Master 2 Internship proposal

Side channel analysis on non volatile memories

Keywords: Hardware security, side channel analysis, non volatile memories, cpa?,

Contact: Valentin Egloff (**valentin.egloff@lcis.grenoble-inp.fr**), LCIS laboratory, Valence, France

Context and motivation:

New memory technologies have emerged recently to replace multiple level of the memory hierarchy. These promise high density, low energy and high bandwidth memories into a single type of memory. Moreover, compared to SRAM or DRAM, they are also non volatile, *i.e.* they retain data even when power is cut. However, they present some asymmetries in power depending on the data read or written. As such, it may be possible for an attacker to guess secret information stored within the memory [1].

Side channel attacks are passive attacks in which the attacker has access to some physical channels emanating from the victim which may carry information. Most common channels are time, power, EM radiation, temperature, etc. The attacker will try to retrieve meaningful information from one or multiple channels to break cryptographic systems or get access to secret information such as a private key. Badly implemented algorithm or CPU core may naturally leak data while some information leaks are unavoidable (e.g. EM radiation).

In this internship, we aim to **characterize** the susceptibility of **non volatile memories to side channel attacks** of different kinds, mainly EM radiation, timing and instantaneous power consumption. This exploratory work will be used to target in-memory computing targets in the future [2]. Based on the knowledge of the physical phenomenon used to store the information, we want to propose models to **exploit vulnerabilities** of these new memories.

The intern will perform side channel attacks on non volatile memories and try to extract information through correlation, differential measurement or any other model used in side channel attacks.

In this internship, the main tasks will be:

- Prototyping RISC-V core (CV32E40P) in FPGA
- Implementing basic software to drive the NVM
- Conducting side channel attacks on different NVM
- Analyzing and determining the best model to steal information from the NVM
- Eventually, testing different encoding to increase resistance to SCA

Who can apply: Applicants must be enrolled in a Master’s degree or engineering school in cyber security, computer engineering or embedded systems and have interests in hardware security.

Required skills:

- C and assembly
- Electronics design and measurement
- Embedded systems
- Cybersecurity

Internship duration: 5 to 6 months (starting February 2024)

Internship location: LCIS Laboratory, in CTSYS team (https://lcis.fr/ctsys)

Laboratoire LCIS, 50 Rue Barthélémy de Laffemas, 26902 Valence cedex 9, France

Financing: About 650€ per month.

For more information or in case you are interested:

please contact or send your CV to: valentin.egloff@lcis.grenoble-inp.fr

Bibliography:

[1] M. N. I. Khan, S. Bhasin, B. Liu, A. Yuan, A. Chattopadhyay, et S. Ghosh, « Comprehensive Study of Side-Channel Attack on Emerging Non-Volatile Memories », *Journal of Low Power Electronics and Applications*, vol. 11, n° 4, Art. n° 4, déc. 2021, doi: 10.3390/jlpea11040038.

[2] Z. Wang, F.-H. Meng, Y. Park, J. K. Eshraghian, et W. D. Lu, « Side-Channel Attack Analysis on In-Memory Computing Architectures », *IEEE Transactions on Emerging Topics in Computing*, vol. 12, n° 1, p. 109-121, janv. 2024, doi: 10.1109/TETC.2023.3257684.

[3] B. Sapui, S. Meschkov, et M. B. Tahoori, « Side-Channel Attack with Fault Analysis on Memristor-based Computation-in-Memory », présenté à IOLTS, Rennes, 2024.

[4] M. T. Arafin et Z. Lu, « Security Challenges of Processing-In-Memory Systems », in *Proceedings of the 2020 on Great Lakes Symposium on VLSI*, in GLSVLSI ’20. New York, NY, USA: Association for Computing Machinery, sept. 2020, p. 229-234. doi: 10.1145/3386263.3411365.