Master Internships on Deep Learning Side-Channel Security

Number of openings: 2/3

Start date: Flexible, anytime from March/April 2026.

Duration: 5-6 months.

Scientific context

After more than 20 years of research, Side-Channel Attacks (SCA) are still one of the most critical vulnerabilities in embedded systems. SCAs exploit correlations between processed data and physical, observable side effects of computing – power consumption, electromagnetic (EM) emanations or timing to name a few – to extract sensitive information. Traditionally directed to retrieve the cryptographic key of mathematically-secure cryptographic implementations, the increasing adoption of Machine Learning (ML) and Deep Learning (DL) is making Artificial Intelligence (AI) a new target. As these systems increasingly deal with sensitive data and control critical infrastructure, and as new vulnerabilities are reported, the **hardware/software security of ML/DL systems** is emerging as a key cybersecurity concern to build trustworthy AI-based systems [1, 2].

Side-channel attacks to DL implementations pave the way to attacks aiming at stealing the intellectual property of DL-based products/services [3, 4], violating the privacy of the end-user and facilitating attacks to DL-based systems.

Objectives of the internships

These internships are framed in the ANR JCJC project ATTILA[1] (young investigators grant from the French national research agency). The **objectives** are to **investigate the susceptibility of DL-based system to side-channel attacks** and to **design SCA-secure DL implementations**. In these internships, we are interested in both local SCA attacks to edge devices, highly exposed to attackers [5–8], and remote SCA attacks to cloud-based DL implementations [9, 10]. The internships cover both software implementations (e.g., in microcontrollers) and hardware implementations (e.g., accelerators in FPGA) of DL algorithms.

Although the main focus is on physical side-channel vulnerabilities (e.g., power consumption or EM emanations), we are open to explore microarchitecural timing side channels exposing, e.g., cache, DRAM or other processor microarchitecture vulnerabilities.

This position offers a good opportunity to discover an emerging topic and gain skills to help you **complete a PhD in the field of (AI) hardware/microarchitecture security**.

Candidates profile

We welcome **Master 1 and 2 students** (4th/5th year Engineering) in **Computer/Electrical Engineering, Embedded Systems, Electronics/Microelectronics or Computer Science**.

The candidate should have a strong background in (at least) one of the following topics:

- Side-channel attacks and evaluation methodologies of secure implementations, cryptanalysis;
- HW or SW implementations of DNNs (FPGAs, microcontrollers, other accelerators/systems);
- Other HW/SW security background (e.g., hardware-secure implementation of cryptographic algorithms);
- Design for FPGAs and hands-on experience in prototyping and implementations.

Other interesting skills to have:

[1] ATTILA: https://rsalvador.org/projects/ATTILA/

- Programming in C/C++/Python
- Use of Linux/Git as development environment
- Good use of laboratory instruments (oscilloscopes, power supplies, etc.)
- ML/AI frameworks (TinyML, PyTorch, TensorFlow, TFLite...)

You can speak, write, and read English at a professional level (french language is not required).

Position details

Stipend: according to regulations, between 650-700 €/month

Supervisors

You will integrate the SUSHI team of IRISA/Inria in Rennes. We are part of a larger collaborative environment with researchers in Rennes and Lorient working on DL hardware/software security, so you will also work with members from the ASIC team of IETR and SHAKER of Lab-STICC.

Contacts of main supervisors:

- **Dr. Rubén Salvador**: ruben.salvador@inria.fr
- **Dr. Lorenzo Casalino**: lorenzo.casalino@centralesupelec.fr
- **Dr. Maria Méndez Real**: maria.mendez-real@univ-ubs.fr
- **Prof. Jean-Christophe Prévotet**: jean-christophe.prevotet@insa-rennes.fr

How to apply

Please send us an email with the following information:

- Your CV
- Your Bachelor/Master transcripts (important to know your background)
- A motivational letter
- Any additional document/report or link to repositories that you think can prove your experience

Application deadline: End of January 2026. Interviews will start as applications arrive so candidates might be selected before the deadline. Please do not hesitate to contact us for further details and information.

References

[1] S. Mittal, H. Gupta, and S. Srivastava. "A Survey on Hardware Security of DNN Models and Accelerators". *J. Syst. Archit.* 117 2021, p. 102163. DOI: 10.1016/j.sysarc.2021.102163.

[2] V. Meyers, D. Gnad, and M. Tahoori. "Active and Passive Physical Attacks on Neural Network Accelerators". *IEEE Design & Test* 2023, pp. 1–1. DOI: 10.1109/MDAT.2023.3253603.

[3] M. Méndez Real and R. Salvador. "Physical Side-Channel Attacks on Embedded Neural Networks: A Survey". *Appl. Sci.* 11 15, 2021, p. 6790. DOI: 10.3390/app11156790.

[4] P. Horváth, D. Lauret, Z. Liu, and L. Batina. "SoK: Neural Network Extraction Through Physical Side Channels". *33rd USENIX Security Symposium (USENIX Security 24)*. 2024, pp. 3403–3422.

[5] M. Isakov, V. Gadepally, K. M. Gettings, and M. A. Kinsy. "Survey of Attacks and Defenses on Edge-Deployed Neural Networks". *IEEE HPEC*. 2019, pp. 1–8. DOI: 10.1109/HPEC.2019.8916519.

[6] L. Batina, S. Bhasin, D. Jap, and S. Picek. "CSI NN: Reverse Engineering of Neural Network Architectures Through Electromagnetic Side Channel". *USENIX Security Symp.* 2019, pp. 515–532.

[7] R. Joud, P.-A. Moëllic, S. Pontié, and J.-B. Rigaud. "A Practical Introduction to Side-Channel Extraction of Deep Neural Network Parameters". *Smart Card Research and Advanced Applications*. Ed. by I. Buhan and T. Schneider. Cham: Springer International Publishing, 2023, pp. 45–65. DOI: 10.1007/978-3-031-25319-5_3.

[8] R. Joud, P.-A. Moëllic, S. Pontié, and J.-B. Rigaud. "Like an Open Book? Read Neural Network Architecture with Simple Power Analysis on 32-Bit Microcontrollers". *Smart Card Research and Advanced Applications*. Ed. by S. Bhasin and T. Roche. Cham: Springer Nature Switzerland, 2024, pp. 256–276. DOI: 10.1007/978-3-031-54409-5_13.

[9] Y. Zhang, R. Yasaei, H. Chen, Z. Li, and M. A. A. Faruque. "Stealing Neural Network Structure Through Remote FPGA Side-Channel Analysis". *IEEE Trans. Inf. Forensics Secur.* 16 2021, pp. 4377–4388. DOI: 10.1109/TIFS.2021.3106169.

[10] S. Moini, S. Tian, D. Holcomb, J. Szefer, and R. Tessier. "Power Side-Channel Attacks on BNN Accelerators in Remote FPGAs". *IEEE J. Emerg. Sel. Top. Circuits Syst.* 11.2 2021, pp. 357–370. DOI: 10.1109/JETCAS.2021.3074608.