IETR IRISA Inria cnrs CentraleSupélec Nantes Université INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES RENNES

Master internships on Deep Learning Hardware Security

Side-Channel Resistant DNN Hardware Accelerators

Number of openings: 2/3

Starting date: flexible, anytime from March/April 2024

Duration: 5-6 months

One of the internships could continue with a Ph.D. in the upcoming course 2024/2025.

Scientific context

Machine/Deep Learning (ML/DL) is deployed in different applications that increasingly deal with sensitive data and control critical infrastructures. As a result, **ML security and privacy** has emerged as a key cybersecurity concern, as private data and secret Intellectual Property of ML models can be compromised through hardware and software attacks at training and inference time. The accessibility and connectivity systems at the edge and the cloud expose a large attack surface with the potential for major societal and economic impacts on security, safety, and privacy. These large deployments are also increasing the need to reduce the computational complexity and energy requirements of ML systems, for which **Approximate Computing** (AxC) and **flexible hardware accelerators** are gaining traction.

In this context, the **hardware security of ML/DL systems** is emerging as an important field, as increasing amounts of attacks on Deep Neural Network (DNN) implementations are reported. **Side-Channel Analysis (SCA) attacks** compromise *confidentiality* by looking for correlations between processed data and observable side effects of computations like power consumption, Electromagnetic (EM) emanations or timing. **SCA attacks to DNN implementations** enable the recovery of secret assets like models' structure, parameters, and private data inputs, jeopardizing privacy and enabling reverse-engineering of models and microarchitectural details, which can in turn help adversaries fool systems more easily towards misclassification. We are interested in both local SCA attacks to edge devices, highly exposed to attackers and remote SCA attacks to cloud FPGAs.

These internships are framed in the ANR JCJC project ATTILA[1] (2021–2025, young investigators grant from the French national research agency), focused on studying the security threats to DNN accelerators in heterogeneous reconfigurable platforms. Our **goal is to investigate the implementation vulnerabilities of ML systems** and to **design secure implementations against SCA attacks** using heterogeneous MPSoC-FPGAs.

Objectives

The internships can focus on different aspects depending on the background and interests of the candidates, e.g., on hardware and architecture (FPGAs, hardware security, secure accelerators and microarchitecture, microcontrollers) or on computer science/mathematics (side-channel analysis, cryptanalysis, artificial intelligence):

- **DNN implementation and side-channel evaluation**. Extend our current setup to implement further DNN models in FPGAs (or microcontrollers) leveraging AxC techniques and evaluate their side-channel leakage under different settings.

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

- **Implementation of countermeasures**. Study the existing countermeasures in the literature and propose new ones leveraging AxC and other techniques to be explored.
- **Advanced side-channel analysis techniques and evaluation methodologies**. Study the literature on analysis techniques and attacks to propose and implement new side-channel evaluation methodologies adapted to the DNNs context (recovery of parameters/inputs, reverse-engineer models or hardware accelerators, discover new vulnerabilities, etc.).

Please contact us if you are in doubt about whether your background can fit or not. Most likely, it will!!

Candidates Profile

Master 1 or 2 students (or 4th/5th year Engineering) in Computer/Electrical Engineering, Embedded Systems, Electronics/Microelectronics or Computer Science. You should have a strong background in at least one of the following topics:

- Side-channel attacks, other HW/SW security
- Design for FPGAs and hands-on experience in prototyping and implementations
- Implementation of DNN/CNN in FPGAs and/or other accelerators/systems
- Machine Learning/Artificial Intelligence frameworks (PyTorch, TensorFlow, TFLite...)

Other interesting skills to have:

- Programming in C/C++/Python
- Use of Linux/Git as development environment
- Good use of laboratory instruments (oscilloscopes, power supplies, etc.)

You are able to speak, write, and read English at a very good level (french language is not required).

Interested?

You will **work closely with an ongoing Ph.D. and a Postdoc** and will be able to participate in some scientific activities of the project to get a taste of research projects.

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

Team information

You will integrate the IETR laboratory in CentraleSupélec in Rennes, and work with members from the ASIC team of IETR and the SUSHI team of IRISA/Inria. You would be based in the Rennes campus of CentraleSupélec.

Contacts:

- **Dr. Rubén Salvador**: ruben.salvador@inria.fr
- **Dr. Maria Méndez Real**: maria.mendez@univ-nantes.fr
- **Prof. Jean-Christophe Prévotet**: Jean-Christophe.Prevotet@insa-rennes.fr
- **Dr. Amor Nafkha**: Amor.Nafkha@centralesupelec.fr

How to apply

Please send an email to the supervisors indicated above 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 can think can prove your experience

Application deadline: End of April 2024. Interviews start as applications arrive, so the candidates might be selected before the deadline.