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

1 PhD/Postdoc positions on Deep Learning Hardware Security

Side-Channel Resistant DNN Hardware Accelerators

Duration: *Ph.D.* full 3-year thesis, and *Postdoc* 2 years with possibility of extension.

Start date: Flexible during 2024, ideally *Ph.D.* Oct./Nov., and *Postdoc* as soon as possible.

Deadline: Interviews will start as applications arrive and run until filling the positions.

Permanent junior research positions open yearly at Inria and CNRS, and a permanent professorial position will likely open in the coming 1–3 years. This postdoc is an excellent opportunity to prepare for such tenured positions.

Scientific context

Machine/Deep Learning (ML/DL) is deployed in applications that increasingly deal with sensitive data and control critical infrastructures. As private data and secret Intellectual Property of ML models can be compromised through hardware and software attacks at training and inference time [1], **ML security and privacy** is emerging as a key cybersecurity concern [2]. Accessibility and connectivity of deployments at the edge and cloud expose a large attack surface with potential for major societal and economic impacts on security, safety, and privacy. Such large deployments also increase the need to reduce the computational complexity and energy requirements , for which **Approximate Computing** (AxC) [3, 4] and **flexible hardware accelerators** [5, 6] are gaining traction.

In particular, **hardware/software security of ML/DL systems** is emerging as an important field, as increasing amounts of attacks to Deep Neural Network (DNN) implementations are reported [7, 8]. **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 [9] and the structure and dataflow scheduling of encrypted IP hardware accelerators [10]. Such side-channel-assisted information can also help adversaries fool systems more easily toward misclassifications. We are interested in both local SCA attacks to edge devices, highly exposed to attackers [11], and remote SCA attacks to cloud FPGAs [12, 13].

Objectives of the position

Our **goal is to investigate the side-channel vulnerabilities of DL systems in heterogeneous reconfigurable platforms (MPSoC-FPGAs)** and to **design secure accelerators against SCA attacks**. We focus on AxC techniques for implementation and aim to understand the interplay between AxC and SCA resistance. The **security implications of AxC** is an emerging area aiming at understanding the interplay between approximation techniques, vulnerabilities, and defense mechanisms [14, 15]. Although the focus is on SCA attacks exploiting power consumption [12, 13, 16] or EM emanations [17, 18], the candidate can explore other side-channel vulnerabilities, too.

We **welcome candidates with different backgrounds and interests**, 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). Depending on the background, the research directions to explore can revolve around:

- **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.

- **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.).

The position offers a clear path to **complete a PhD in an important emerging field** and the chance to **set up and develop their own research agenda** to postdoc candidates.

Project environment

The position is framed in the ANR JCJC project ATTILA[1] (young investigators grant from the French national research agency). You will be fully integrated into the scientific activities of the project (discussions, meetings, seminars) and **work closely with one ongoing Ph.D. and Master students**. You will be **able to supervise other students, participate and lead grant writing to attract funds if you are a postdoc, and, if interested, enroll in teaching activities** (with an added salary bonus).

Team information

You will integrate the IETR laboratory in CentraleSupélec, Rennes campus and work with members from the ASIC team, and the SUSHI team of IRISA/Inria. We are part of a larger collaborative environment with researchers in Rennes and Nantes working on DL hardware and hardware/software security. The campus has a long, established tradition in cybersecurity, offering two cybersecurity tracks and specializations on the engineering degree, a specialized (executive education) master, and participates in the *Graduate Research School* EUR Cyberschool. You will work alongside several PhDs and postdocs in the security domain.

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

Location

Rennes is a vibrant city with great surroundings and a great international environment. As a research and innovation hub in cybersecurity, it is a great place for a postdoc to work closely with like-minded colleagues and benefit from a rich cybersecurity, artificial intelligence, and computing systems architecture environment. The **cybersecurity ecosystem in Rennes** includes the DGA, the Rennes branch of the French National Cybersecurity Agency (ANSSI), major industrial groups (Orange, Airbus, Thales, etc.), an increasing number of specialized companies like Secure-IC, and academic partners like Inria, IRISA, IETR, and the LHS (High-Security Laboratory, Inria). The *Cybersecurity Excellence Center* (Pôle d'Excellence Cyber) federates the different initiatives in cybersecurity. Academic partners are creating a multidisciplinary *Cybersecurity Competence Center* (C3) with a dedicated building hosting many cybersecurity research and teaching activities in the same place. Rennes also hosts the *Graduate Research School* EUR Cyberschool.

Details of the position

Salary: Gross salary (before taxes) is 2100-2300€/month for PhD and 2750€-3200€/month for the postdoc, depending on previous experience.

Benefits package:

- Social Security coverage

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

- Subsidized meals
- Partial reimbursement of public transport costs
- Paid holiday leave
- Accommodation facilities available on-campus
- Access to vocational training, social, cultural, and sports facilities and activities

Candidates profile

Graduate (Master 2 or 5th year Eng.) or **Ph.D.** in Computer/Electrical Engineering, Computer Science, Microelectronics, Embedded Systems. **You have a strong background in at least one of the following domains:**

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

Other interesting skills:

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

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

How to apply

Please send an email to the contacts indicated above with the following information:

- Your CV
- Reference letter/s from previous supervisors
- Copies/links to reports/papers/repositories showing your experience
- **Postdoc:**
  - Motivation letter and research statement (4 pages max)
  - Your Ph.D. thesis manuscript
- **Ph.D.:**
  - Motivation letter
  - Bachelor/Master transcripts

Please do not hesitate to contact us for further details and information.

References

[1] M. Shafique et al. "Robust Machine Learning Systems: Challenges,Current Trends, Perspectives, and the Road Ahead". *IEEE Des Test* 37.2 2020, pp. 30–57. DOI: 10.1109/MDAT.2020.2971217.

[2] N. Papernot, P. McDaniel, A. Sinha, and M. P. Wellman. "SoK: Security and Privacy in Machine Learning". *2018 IEEE EuroS&P)*. Apr. 2018, pp. 399–414. DOI: 10.1109/EuroSP.2018.00035.

[3] E. Wang et al. "Deep Neural Network Approximation for Custom Hardware: Where We've Been, Where We're Going". *ACM Comput. Surv.* 52.2 May 30, 2019, 40:1–40:39. DOI: 10.1145/3309551.

[4] G. Armeniakos, G. Zervakis, D. Soudris, and J. Henkel. "Hardware Approximate Techniques for Deep Neural Network Accelerators: A Survey". *ACM Comput. Surv.* Mar. 2022. DOI: 10.1145/3527156.

[5] K. Guo, S. Zeng, J. Yu, Y. Wang, and H. Yang. "[DL] A Survey of FPGA-based Neural Network Inference Accelerators". *ACM TRETS* 12.1 Mar. 28, 2019, 2:1–2:26. DOI: 10.1145/3289185.

[6] S. Mittal. "A Survey of FPGA-based Accelerators for Convolutional Neural Networks". *Neural Computing and Applications* 32.4 Feb. 2020, pp. 1109–1139. DOI: 10.1007/s00521-018-3761-1.

[7] 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.

[8] 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.

[9] 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.

[10] C. Gongye, Y. Luo, X. Xu, and Y. Fei. "Side-Channel-Assisted Reverse-Engineering of Encrypted DNN Hardware Accelerator IP and Attack Surface Exploration". *2024 IEEE SP)*. IEEE Computer Society, Oct. 2023, pp. 1–1. DOI: 10.1109/SP54263.2024.00001.

[11] 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.

[12] 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.

[13] 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.

[14] W. Liu et al. "Security in Approximate Computing and Approximate Computing for Security: Challenges and Opportunities". *Proceedings of the IEEE* 108.12 2020, pp. 2214–2231. DOI: 10.1109/JPROC.2020.3030121.

[15] P. Yellu et al. "Security Threat Analyses and Attack Models for Approximate Computing Systems: From Hardware and Micro-architecture Perspectives". *ACM TODAES* 26.4 2021, 32:1–32:31. DOI: 10.1145/3442380.

[16] L. Wei, B. Luo, Y. Li, Y. Liu, and Q. Xu. "I Know What You See: Power Side-Channel Attack on Convolutional Neural Network Accelerators". *ACSAC*. ACM, 2018, pp. 393–406. DOI: 10.1145/3274694.3274696.

[17] H. Yu, H. Ma, K. Yang, Y. Zhao, and Y. Jin. "DeepEM: Deep Neural Networks Model Recovery through EM Side-Channel Information Leakage". *IEEE HOST*. 2020, pp. 209–218. DOI: 10.1109/HOST45689.2020.9300274.

[18] V. Yli-Mäyry, A. Ito, N. Homma, S. Bhasin, and D. Jap. "Extraction of Binarized Neural Network Architecture and Secret Parameters Using Side-Channel Information". *ISCAS*. May 2021, pp. 1–5. DOI: 10.1109/ISCAS51556.2021.9401626.