AI-powered design of sustainable secure cryptocircuits

Contact information
Juan Núñez Martínez (Tenured Scientist at Instituto de Microelectrónica de Sevilla, IMSE-CNM)
e-mail: jnunez@csic.es
ORCiD: https://orcid.org/0000-0002-0279-9472

1. Description of the Training Plan

The predoctoral training will be carried out within the framework of the *GreenCrypt* project (*AI-powered design of sustainable secure cryptocircuits*), developed at the Institute of Microelectronics of Seville (IMSE-CNM, CSIC/University of Seville). The work focuses on the **design of secure, reconfigurable, and energy-efficient cryptographic circuits** supported by **artificial intelligence (AI)** methodologies.
The goal is to train the PhD candidate in the **development of cryptographic hardware resilient to physical attacks and adaptable to emerging threats**. The research combines electronic design, cybersecurity, and AI-based automation, addressing the entire flow from conceptual modeling to experimental validation.

Main activities will include:

- Design and simulation of cryptographic modules and their countermeasures.
- Development of **machine-learning tools** for the automatic detection of information leakage.
- Implementation of **hardware patching** techniques to reconfigure countermeasures and evaluate adaptability.
- Design of **PUFs and TRNGs** in CMOS and emerging technologies (memristors, FeFETs, VO_2).
- Experimental validation on **FPGA and ASIC prototypes**.
- Participation in **side-channel and fault-injection attack experiments** using the IMSE hardware security laboratory.

The candidate will gain expertise in **microelectronics, hardware security, and VLSI design**, mastering EDA tools such as **Cadence, Synopsys, or Mentor Graphics**, as well as **AI and data-driven methods** for secure hardware design. The program also includes training in scientific communication, teaching skills, and technology transfer activities with industry.

2. Tentative plan of activities

Year 1 – Foundational Training and Initial Design

- Literature review on hardware security, lightweight cryptography, and AI-assisted design.
- Training in EDA tools and VLSI design methodologies.
- RTL design and simulation of crytographic modules.
- Initial studies on AI techniques for pre-silicon security evaluation.

Year 2 – AI-Based Security and Countermeasure Automation

- Development of deep-learning and machine-learning models for leakage detection.
- Automation of countermeasure insertion against side-channel and fault attacks.
- Exploration of hardware patching and adaptive reconfiguration mechanisms.
- Functional validation of secure architectures on FPGA platforms.

Year 3 – Experimental Design and Validation

- Design and simulation of **PUFs and TRNGs** based on coupled oscillators and emerging devices.
- ASIC design in **CMOS commercial technology** and laboratory testing.
- Experimental evaluation under SCA/FIA conditions.
- Optimization of performance, area, and energy trade-offs.

Year 4 – Dissemination, Internationalization, and Thesis Completion

- Research stay in leading international groups.
- Publication of results in high-impact journals and conferences (ISCAS, HOST, CHES, DCIS).
- Participation in teaching and outreach activities.
- Writing and defense of the doctoral thesis.

3. Skills to Be Acquired

- Advanced knowledge in **VLSI and ASIC design** for secure systems.
- Proficiency in **hardware security evaluation** and cryptographic architecture design.
- Expertise in **AI-based design automation** and data-driven analysis.
- Laboratory experience in **side-channel analysis, fault injection, and device characterization**.
- Competence in **scientific writing, dissemination, and collaboration**.
- Teaching and mentoring skills aligned with university academic training.

4. Expected Results

- Completion of a **doctoral thesis with international distinction**.
- **Three or more publications** in indexed journals (IEEE TETC, TCSI, Sensors, etc.).
- **Conference presentations** at leading venues (ISCAS, HOST, CHES, DCIS, ESSCIRC).
- **Fabricated and validated FPGA/ASIC prototypes** demonstrating physical attack resistance.
- **International research stay** in a top laboratory.
- Full professional qualification for academic or industrial research in **hardware cryptography and microelectronics**.