2024-2025 Internship Proposal at TIMA Laboratory

Side-Channel Attack Mitigation in Physically Unclonable Functions

Abstract:

The security of Physically Unclonable Functions (PUFs) is a critical challenge in modern hardware, particularly in the face of side-channel attacks. These attacks leverage physical information, such as power consumption or electromagnetic emissions, to extract sensitive data or manipulate system behavior. The increasing prevalence of PUFs in applications requiring device authentication and security highlights the need for effective countermeasures against such attacks. This internship aims to analyze large datasets of side-channel attack information and develop AI-based methods to detect and mitigate these threats. By identifying attack patterns and categorizing different attack types, the research will propose innovative techniques to disrupt and prevent potential side-channel attacks, thereby strengthening the security and robustness of PUFs in various applications.

Project description:

The goal of this internship is to analyze large datasets of side-channel attack data and develop AI-based methods to mitigate these threats, particularly in the context of PUF security. The intern will explore patterns in the attack data, categorize different types of attacks, and propose countermeasures and techniques to disrupt and prevent potential side-channel attacks. Python and HDL languages can be used to implement the proposed methods and countermeasures.

Tasks of the internship:

- Developing and selecting suitable features from side-channel attack data to improve the accuracy of detection models.
- Designing and fine-tuning machine learning, neural network, and data mining models to optimize performance in identifying attack patterns, categorizing the attack types, and mitigating threats.
- Proposing countermeasures based on the detected patterns and threats.
- Implementing validation and testing procedures to evaluate the effectiveness of the proposed countermeasures and techniques.
- Collecting and analyzing experimental results from the implemented models and comparing their performance.

Scientific environment:

The candidate will work within the TIMA Laboratory (https://tima.univ-grenoble-alpes.fr/) in collaboration with the AMfoRS (Architectures and Methods for Resilient Systems) research group.

Profile & requested skills:

We are looking for a highly motivated Engineering School or M2 Master's student. Applicants must hold a Master 1 degree (or equivalent) obtained within the last three years at the application deadline, in a related field such as computer science, microelectronics technologies, hardware security, or emerging advances in Artificial Intelligence. Interpersonal skills, dynamism, rigor, and teamwork abilities will be highly valued. Candidates should be fluent in English and have strong English writing skills.

Allowance: Internship allowance will be provided.

Application instructions:

If you are interested in the topic please send your complete application to: mohammadreza.heidari-iman@univ-grenoble-alpes.fr.

A complete application consists of:

Cover letter: A brief motivation statement by the applicant, explaining their connection to the position, how the position aligns with their background, and how it supports their future career goals (maximum 1 page).

CV: Academic and professional background, detailing relevant experience, particularly research.

Relevance for Application: The applicant should include a clear description of how his or her scholarly background and expertise apply to the project outlined above and how they might add value to it.
Our laboratory welcomes applicants with diverse backgrounds and experiences. We regard gender equality and diversity as a strength and an asset.
Depending on the student's motivation, the internship may lead to a doctoral project.

Contact:

Mohammad Reza Heidari Iman,
Postdoctoral Researcher at TIMA Laboratory,
Université Grenoble Alpes,
Grenoble, France
Email: mohammadreza.heidari-iman@univ-grenoble-alpes.fr