2025-2026 Optimization and Implementation of Ring Oscillator PUF Architectures on FPGA

Abstract:

Physical Unclonable Functions (PUFs) represent a promising alternative to non-volatile memories, as they enable on-demand generation of cryptographic keys without requiring their storage. Several types of PUFs exist, including Ring Oscillator-based PUFs (RO-PUFs), which rely on comparing the frequencies of multiple ring oscillators. These RO-PUFs can be implemented on FPGAs using various architectures, and their performance depends on several parameters such as the implementation choices, the underlying technology, and environmental conditions.

Project description:

The primary objective of this internship is to implement and optimize a Ring Oscillator Physical Unclonable Function (RO-PUF) architecture in order to improve its overall performance, particularly in terms of reliability, uniqueness, and entropy. The work will focus on two critical components of the acquisition chain, which have a direct impact on the quality of the generated bits. The first research axis will address the optimization of the comparison logic. This includes analyzing and implementing different strategies for selecting pairs of ring oscillators (ROs), as well as developing innovative comparison mechanisms to maximize bit stability and reduce the bit error rate, especially under environmental variations. The second axis will focus on improving the measurement blocks, specifically the frequency counters. The goal is to design and optimize frequency counters that enhance the precision of discrimination between ring oscillators. Particular attention will be paid to the trade-offs between measurement accuracy, silicon area, and power consumption, with the aim of achieving an efficient and practical implementation.

Tasks of the internship:

- Analyze and implement optimized RO-PUF architectures, focusing on improving reliability, uniqueness, and entropy.
- Design and evaluate efficient comparison logic and ring oscillator pairing strategies to enhance bit stability and reduce error rates.
- Develop and optimize frequency measurement blocks (counters), and study the trade-offs between measurement accuracy, silicon area, and power consumption.

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 seeking a highly motivated student from an Engineering School or a Master's program (M2). Applicants should hold a Master 1 degree (or an equivalent qualification) obtained within the last three years at the time of application, in a relevant field such as microelectronics, digital electronics, or related disciplines. A strong foundation in HDL languages (Verilog/VHDL) and data processing tools such as Python is required. Candidates with a genuine interest in hardware security and experimental FPGA-based projects will be particularly encouraged to apply.

Allowance: Internship allowance will be provided.

Application instructions:

If you are interested in the topic, please send your complete application to:
Aghiles.Douadi@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.

Contacts:

Aghiles,Douadi
Postdoctoral Researcher at TIMA Laboratory
Université Grenoble Alpes
Grenoble, France
Email: Aghiles.Douadi@univ-grenoble-alpes.fr