Internship proposal at TIMA Laboratory – 2024-2025

Pulsed EMFI on Ring Oscillator-based TRNG implemented in an FPGA

Context

In modern cryptographic systems, True Random Number Generators (TRNGs) play a fundamental role in ensuring security by generating unpredictable and high-entropy random numbers. These random values are crucial for cryptographic key generation, secure authentication, and data encryption. TRNGs derive their randomness from physical sources (usually some kind of analog noise), which is monitored and digitized to obtain a digital noise after a sufficiently long jitter accumulation time**.** Among various TRNG architectures, Ring Oscillator-based TRNGs (RO-TRNGs) exploiting the jittered clock signal generated by the freely running oscillators are the most studied ones due to their ease of integration, low resource utilization, and high-speed operation [1]. However, their reliance on metastability and jitter makes them vulnerable to different kind of fault injection attacks, particularly pulsed Electromagnetic Fault Injection (EMFI). Pulsed EMFI is a powerful technique that can induce transient faults in the FPGA fabric, potentially disturbing the entropy source of the TRNG and biasing its output. Therefore, understanding the impact of pulsed EMFI on RO-TRNGs is critical as attackers exploiting these vulnerabilities can undermine the integrity of secure systems [2]. This case study aims to analyze the susceptibility of RO-TRNGs implemented on FPGAs to pulsed EMFI, assess the resulting security implications, and explore possible countermeasures to enhance their robustness against EMFI threat.

Project description

The **main objective** of this internship is to take advantage of the open source TRNG project OpenTRNG - Open-source TRNG offering different reference architectures of RO-based TRNGs (Elementary based Ring Oscillator (ERO), Multi Ring Oscillator (MURO) and Coherent Sampling Ring Oscillator (COSO)) to understand the behavior of each one of them after a pulsed EMFI attack. To achieve this objective, the following tasks needs to be executed:

- Use OpenTRNG to compile and run the different TRNG architecture on an FPGA
- Analyze and evaluate the random outcomes of each architecture
- Mount the EMFI attack and analyze the impact on each architecture

Profile:

We are looking for a highly-motivated Engineering School or M1 Masters student.

Required skills:

- Experience in VHDL or Verilog for FPGA design.
- Experience with FPGA design tools such as Xilinx Vivado.
- Proficiency in Python for data analysis and automation of experiments.
- Knowledge of physical attacks is a plus;
- Strong analytical thinking and troubleshooting skills.

Interpersonal skills, dynamism, rigor and teamwork abilities will be appreciated. Candidates should be fluent in English and/or in French.

Scientific environment:

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

Application instructions: If you are interested in the topic, please send your complete application to the 3 contacts below.

A complete application consists of:
Cover letter: Short motivation of the applicant and connection with the position, including how this position serves future career goals. Include name and contact information of applicant (1 page max)
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 is applicable, and might add value, to the project set out above.
Our team welcomes applicants with diverse backgrounds and experiences. We regard gender equality and diversity as strength and an asset.

CONTACT

Sami El Amraoui (TIMA): sami.el-amraoui@univ-grenoble-alpes.fr
Paolo Maistri (TIMA): paolo.maistri@univ-grenoble-alpes.fr
Régis Leveugle (TIMA): regis.leveugle@univ-grenoble-alpes.fr

References:

[1] Benea, L., Carmona, M., Fischer, V., Pebay-Peyroula, F., & Wacquez, R. (2024). Impact of the Flicker Noise on the Ring Oscillator-based TRNGs. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2024(2), 870-889. https://doi.org/10.46586/tches.v2024.i2.870-889
[2] M. Madau *et al*., "The Impact of Pulsed Electromagnetic Fault Injection on True Random Number Generators," *2018 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*, Amsterdam, Netherlands, 2018, pp. 43-48, doi: 10.1109/FDTC.2018.00015.