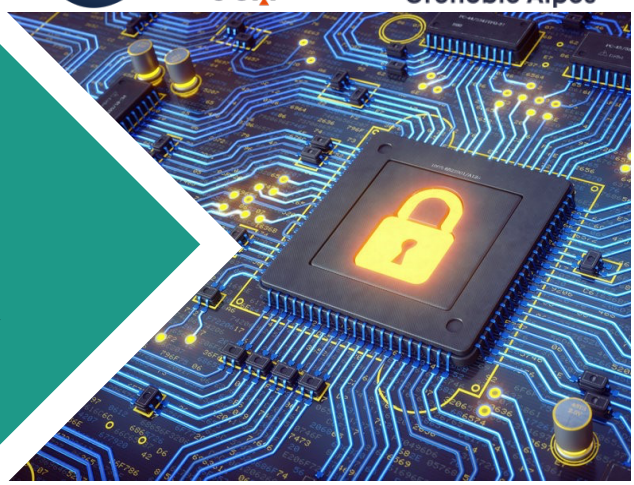
TIMA Scientific Days

These Scientific Days are meant to present the research topics and to disseminate the recent advances of TIMA researchers. **These presentations are open to everybody**, whether they are members of TIMA or not.



Hardware Security

– TIMA Laboratory, 46 avenue Félix Viallet –

Room T312 + Zoom meeting

Thursday May 30th, 2024

Hardware Security | Robustness, Reliability, Test | Emerging Computing | Hardware/ software codesign | Simulation and verification | Async design, non-uniform sampling | AMS/RF circuits and systems | Sensors and Actuators

	Program
14h00 – 14h25	Choose your Path: Control of Ring Oscillators EMFI Susceptibility through FPGA P&R Constraints – *Sami EL AMRAOUI*
14h25 – 14h50	On the Relation Between Reliability and Entropy in Physical Unclonable Functions – *Sergio VINAGRERO GUTIERREZ*
14h50 – 15h15	Modeling Thermal Effects For Biasing PUFs – *Aghiles DOUADI*
15h15 – 15h40	Internal State Monitoring in RISC-V Microarchitectures for Security Purpose – *Roua BOULIFA*
15h40 – 15h50	**Break**
15h50 – 16h15	Enhancing side-channel attacks through X-ray-induced leakage amplification – *Nasr-Eddine OULDEI TEBINA*
16h15 – 16h40	Non-Invasive Attack on Ring Oscillator-based PUFs through Localized X-Ray Irradiation – *Nasr-Eddine OULDEI TEBINA*
16h40 – 17h05	IEEE 1838 compliant scan encryption and integrity for 2.5/3D ICs – *Juan Suzano DA FONSECA*

For more information, please contact: Paolo MAISTRI – paolo.maistri@univ-grenoble-alpes.fr

Zoom meeting
https://univ-grenoble-alpes-fr.zoom.us/j/98139393333?pwd=SIV5TjdzK2lneCtNK2xMZk13Q25SUT09
ID: 981 3939 3333
Code: 289758

	Abstracts
14h00 – 14h25 ***Sami EL AMRAOUI***	**Choose your Path: Control of Ring Oscillators EMFI Susceptibility through FPGA P&R Constraint** Ring Oscillators (ROs) are widely used in various electronic systems, contributing to their functionality, security, and reliability. Therefore, the characterization of the robustness of RO-based designs against fault attacks such as ElectroMagnetic Fault Injection (EMFI) is a real concern. In this paper, we study the impact of electromagnetic (EM) pulses on ROs implemented in FPGAs. We show that the induced harmonic response depends on the placement and routing of the inverters for different parameters of the pulse. Such a characterization can help developing RO-based structures optimized either for better robustness against attacks or on the opposite for higher sensitivity in order to implement on-chip detectors.
14h25 – 14h50 ***Sergio VINAGRERO GUTIERREZ***	**On the Relation Between Reliability and Entropy in Physical Unclonable Functions** Physical Unclonable Functions (PUFs) are integral for generating unique signatures, secret keys, and device identification, leveraging inherent manufacturing process variability. Mathematically defined as functions linking inputs (challenges) to outputs (responses), PUFs exhibit random properties. Key properties for high-quality PUFs include intra-device entropy (random distribution of responses within the same circuit), inter-device entropy (random distribution across different circuits for identical challenges), and reliability (response consistency for identical challenges and the same circuit). Inter-device entropy and reliability may be influenced by design discrepancies, systematic variability, noise, and aging. In this presentation we showcase the correlation between entropy and reliability and verify it with extensive data from real Ring Oscillators.
14h50 – 15h15 ***Aghiles DOUADI***	**Modeling Thermal Effects For Biasing PUFs** Security primitives such as Physical Unclonable Functions (PUFs) or True Random Number Generators (TRNGs), have emerged as hardware roots of trust for ensuring the security of modern applications. However, these primitives display susceptibility to physical attacks, among them, in the face of temperature variations. Previous research has established the feasibility of attacks exploiting temperature fluctuations to compromise the security of these primitives. Specifically, when implemented on FPGAs, programmable components can be vulnerable to alterations induced by thermal changes. These findings underscore the need to deepen the understanding of the implications of temperature sensitivity on the security and robustness of these security mechanisms. This paper studies how heat affects, both instantaneously and permanently, the working of ring oscillators, which are the building blocks of PUFs based on Ring Oscillators. The study also suggests how to exploit these effects to bias the PUf responses, enabling thus the possibility of its cloning.

15h15 – 15h40 ***Roua BOULIFA***	**Internal State Monitoring in RISC-V Microarchitectures for Security Purpose** Embedded systems play a significant role in our everyday lives, making them prime targets for malicious actors. Consequently, ensuring the security of such systems becomes a crucial concern. Among various threats, fault injection attacks on microprocessors are particularly notable. Understanding the effects of these attacks within the microarchitecture is thus essential to assess their impact on the overall security.
15h40 – 15h50	**Break**
15h50 – 16h15 ***Nasr-Eddine OULDEI TEBINA***	**Enhancing side-channel attacks through X-ray-induced leakage amplification** We propose a novel approach that utilizes localized X-ray irradiation to amplify data-dependent leakage currents in CMOS-based cryptography circuits. Our proposed technique strategically targets specific regions in a circuit using X-rays, inducing variations in dynamic and static power consumption due to Total Ionizing Dose (TID) effects, which increases or even reveals hidden data leakage. In this work, we present several experimental campaigns highlighting the benefits of our approach to combinational and sequential logic. Our experiments show a significant increase in information leakage in the targeted regions, which improves the signal-to-noise ratio coefficient and thus makes recovering the processed bytes easier. We envision the possibility of using this technique on full cryptographic designs on both FPGA and ASICs.
16h15 – 16h40 ***Nasr-Eddine OULDEI TEBINA***	**Non-Invasive Attack on Ring Oscillator-based PUFs through Localized X-Ray Irradiation** Physical Unclonable Functions (PUFs) are emerging as a fundamental component of secure architectures that provide services such as authentication and key generation. A specific class of PUF is based on Ring Oscillators (ROs), where minimal behavioral differences due to process variations are harnessed to generate unique responses. The inherent strength of PUFs lies in the fact that it is practically impossible to control these phenomena to forge a specific response from the device. In this paper, we present a novel approach by introducing localized X-Ray attacks on PUFs for the first time. These attacks significantly alter the behavior of a selected RO within the array of oscillators on an FPGA. By biasing the properties of the target block, we demonstrate the feasibility of modifying the response of a specific PUF. In particular, these attacks can be executed when the target is powered off, bypassing several circuit monitoring countermeasures. This capability introduces a new class of attacks that exploit vulnerabilities even in systems with stringent security measures, raising concerns about the robustness of current security frameworks.

16h40 – 17h05 ***Juan Suzano DA FONSECA***	**IEEE 1838 compliant scan encryption and integrity for 2.5/3D ICs** 2.5D and 3D integrated circuits (IC) are the natural evolution of traditional 2D SoCs. 2.5D and 3D integration is the process of assembling pre-manufactured chiplets in an interposer or in a stack. This process can damage the chiplets or lead to faulty connections. Thus, the importance of post-bond test of chiplets. The IEEE Std 1838(TM)-2019 (IEEE 1838) design-for-testability (DFT) standard defines mandatory and optional structures for accessing DFT functions on the chiplet. Compliant chiplets form a DFT network that can be exploited by attackers to violate the confidentiality or integrity of the message transmitted over the serial path. In this work, we combine a message integrity verification system with a scan encryption mechanism to protect the scan chain of an IEEE 1838-compliant DFT implementation. The scan encryption prevents unauthorized actors from writing meaningful data into the scan chain. Message integrity verification makes messages from untrustworthy sources detectable. In conjunction, both security primitives protect the scan chain from malicious chiplets on the stack, scan-based attacks, and brute force attacks. The proposed solution causes less than 1% area overhead on designs composed of more than 5 million gates and less than 1% test time overhead for typical DFT implementations.