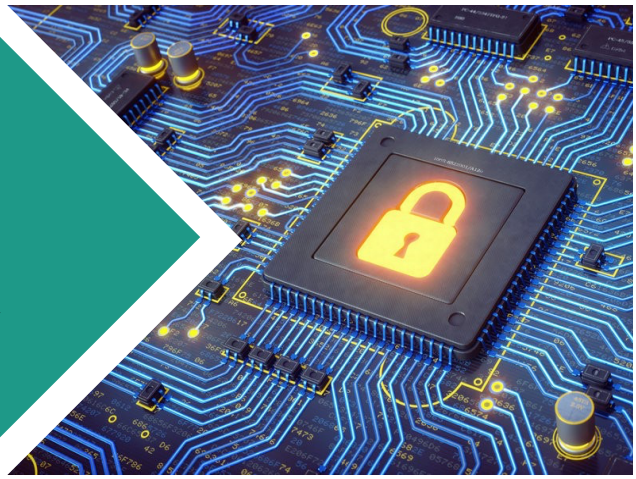
TIMA Scientific Days

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

March 3rd, 2023

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
13h30 – 13h55	SRAM-based Physical Unclonable Functions *Sergio VINAGRERO (PhD. Student - TIMA/Amfors)*
13h55 – 14h20	Challenges and opportunities in implementing Logic-in-Memory: a security perspective – *Pietro INGLESE (PhD. Student - TIMA/Amfors)*
14h20 – 14h55	Electromagnetic fault models *Sami EL AMRAOUI (PhD. Student - TIMA/Amfors)*
14h55 – 15h10	Break
15h10 – 15h35	Faulting real-world devices with X-Rays beams *Laurent Maingault (Full Researcher – CEA/DSYS)*
15h35 – 16h00	Variable-Length Instruction Set: Feature or Bug? *Ihab ALSHAER (PhD. Student – LCIS, TIMA/Amfors)*
16h00 – 16h30	Secure RISC-V processors with respect to Micro Architectural attacks *Valentin MARTINOLI (PhD. Student – Thales DIS, TIMA/Amfors)*

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

Join Zoom Meeting
https://univ-grenoble-alpes-fr.zoom.us/j/94744317591?pwd=R1pPVnhzU29qKzRLWVJXd3hEWXIxdz09

Meeting ID: 947 4431 7591
Passcode: 737434

	Abstracts
13h30 – 13h55 ***Sergio VINAGRERO*** *(PhD. Student - TIMA/Amfors)*	**SRAM-based Physical Unclonable Functions** Physical Unclonable Functions (PUFs) leverage manufacture variability in order to generate secrets. Private keys are usually stored in non-volatile memories, but this comes with security implications. SRAM memories, being a ubiquitous component in the micro-processors nowadays, are a good candidate for secret generation mechanisms. During the manufacture of the SRAM memories, some cells end up being asymmetric and this can be exploited to obtain a unique identifier for each SRAM memory during start up state.
13h55 – 14h20 ***Pietro INGLESE*** *(PhD. Student - TIMA/Amfors)*	**Challenges and opportunities in implementing Logic-in-Memory: a security perspective** As energy efficiency and performance become increasingly important in modern systems, the study of emerging non-volatile memories has gained significant attention. The Logic-in-Memory (LIM) paradigm, a subset of Computation-in-Memory, focuses on performing Boolean operations directly within the memory, which can be allowed by some emerging memories. However, this shift towards LIM technology presents new challenges, including preserving operation accuracy in non-ideal conditions. The potential to integrate crypto-cores into LIM systems has added necessity to studying the security and reliability of LIM architectures.
14h20 – 14h55 ***Sami EL AMRAOUI*** *(PhD. Student - TIMA/Amfors)*	**Electromagnetic fault models** One major threat against secure devices is Fault Injection (FI) since it enables an attacker to recover highly sensitive data. FI can be implemented through various techniques among which ElectroMagnetic Fault Injection (EMFI) has been pointed out as an effective medium because of its inherent advantages; no need to perform chip decapsulation, good spatial and temporal resolutions and the experimental setup is of lower complexity and cost compared to other radiation-based fault injections. Therefore, evaluating the impact of electromagnetic coupling between the probe and the integrated circuit remains crucial to define an accurate fault model that helps the designer in the evaluation and definition of adapted countermeasures.
14h55 – 15h10	Break
15h10 – 15h35 ***Laurent Maingault*** *(Full Researcher – CEA/DSYS)*	**Faulting real-world devices with X-Rays beams** Details will follow soon

15h35 – 16h00 ***Ihab ALSHAER*** *(PhD. Student – LCIS, TIMA/Amfors)*	**Variable-Length Instruction Set: Feature or Bug?** With the increasing complexity of embedded systems, the use of variable-length instruction sets became essential, in order to achieve higher code density and better performance. However, security aspects must also be considered, in particular with the continuous improvement of attack techniques and equipment. Hardware designers and software developers lack accurate hardware and software fault models to evaluate the vulnerabilities of their designs or codes, in presence of fault attacks, especially with the increasing complexity of microprocessors' architectures. In this work, which aims at providing realistic fault models, clock glitch fault injection campaigns, using the ChiWhipserer environment, have been performed. The objective behind these experiments is to provide proper characterization, at the instruction set architecture (ISA) level, for several faulty behaviors that can be observed experimentally when targeting a processor running a variable-length instruction set. Such characterization would help in proposing suitable fault models. Thus, designing cost-effective countermeasures against fault attacks.
16h00 – 16h30 ***Valentin MARTINOLI*** *(PhD. Student – Thales DIS, TIMA/Amfors)*	**Secure RISC-V processors with respect to Micro Architectural attacks** Micro architectural attacks take advantage of optimization mechanisms inside recent CPUs to cause information leakages. Competitive access to limited and shared hardware resources is the root cause of micro architectural covert channels. We propose to study the micro architectural vulnerabilities of the open-source. RISC-V CPU named CVA6. We have built a Prime + Probe covert-channel in a realistic scenario for extracting information and propose an analysis on how to achieve the best extraction possible as well as a hardware modification to mitigate these issues directly at the micro architectural level.