# Security analysis of a dynamic execution context processor

**Place:** IMS Laboratory

**Supervisor:** Mathieu Escouteloup mathieu.escouteloup@ims-bordeaux.fr

**Duration:** February 2026 - August 2026

**Description of the internship:**

*Context:* Modern processors are the result of several decades of optimization aimed at improving their performance. Thus, many mechanisms have been introduced solely to enhance their computing capabilities: pipelining, cache memory, branch prediction, etc. However, security has also become a key issue within electronic and computer systems. Many works have shown that it is possible to exploit these mechanisms at the microarchitecture level of processors.

At the same time, while processor design has for many years been centered around proprietary architectures, the open and free ISA RISC-V now represents a credible alternative. Many academic or industrial projects aim to propose new implementations.

In this context, the HERSE research project within the CSN team of the IMS laboratory aims to propose a new architecture for security. Its approach is based on a new notion of *dynamic execution context*: the ability to specifically configure the execution environment in which a program runs. The goal is to design processors capable of adapting to the needs of applications, both in terms of security and performance. This architectural change therefore involves rethinking all parts of the system, from hardware to the earliest layers of software.

*Subject:*

A first version of a processor based on this new architecture has been developed. It is therefore necessary to evaluate its operation and its contributions to security, but also its limitations. Thus, the objective of this internship will be to contribute to its improvement and evaluation. It will be organized into four main phases:

1. First, the intern will need to understand the architecture and the developed hardware platform. This will involve executing assembly language programs on the modified processor, as well as studying its hardware implementation.
2. The second phase will focus on developing a low-level software layer for managing dynamic contexts. The goal will be to be able to use this new architecture directly from a C program. Again, the operation will be validated with a simulation to ensure proper functioning.
3. The third phase will focus on implementing the prototype on FPGA. The idea will be to run a simple program using dynamic contexts and validate its operation by interacting with simple peripherals (UART, GPIO, SPI, etc.).
4. Finally, a last phase will be devoted to the evaluation of information leaks (e.g. analysis of timing variations). Using internal resources from the team, the objective will be to attempt to reproduce certain side-channel attacks on this new architecture.

**Required Knowledge and Skills:**

Knowledge in the following areas is expected:
- Processor architecture,
- Digital circuit design,
- Microcontroller programming.

Knowledge of embedded systems and operating systems is a plus. Similarly, prior experience (project or internship) with the following tools is expected:
- C and assembly language,
- VHDL/Verilog/SystemVerilog,
- FPGA implementation software (Vivado).