

**ENSIBS**

PRJ 1401

---

# **RSA power analysis attack with ChipWhisperer**

---

*Cizdziel Matthieu, Richard Etienne, Moguedet Mathis*

*PEI-2*

*Supervised by Guy Gogniat*

29 janvier 2024

---

# Table des matières

# 1 ChipWhisperer

## 1.1 ChipWhisperer's purpose

ChipWhisperer is used to make power analysis attacks easy by making a confined environment that we can analyze. It also provides a lot of crypto-firmware that we can attack with some side channel attack's tutorials.

## 1.2 ChipWhisperer's components

ChipWhisperer is made of 2 main components :

- a capture board used to record the current consumption and make the interface between the computer and the crypto-processor
- a target board used to plug a target chip onto. The target board is useful to quickly switch from a target chip to another one

The target chip is the place where the firmware we want to analyze is running. This chip is only running our firmware so we don't have electrical noise on the analysis. The capture board is used to send the request to the target device and receive the output of the firmware, this board also record the current consumption of the target device. By slicing the work of a computer with two boards, the ChipWhisperer tool allow us to run our firmware in a confined space.

# 2 Building our own Firmware

## 2.1 Communication between the computer and the ChipWhisperer

To send the information from the computer to the ChipWhisperer, we use the "simpleserial.h" library.

# 3 Conclusion