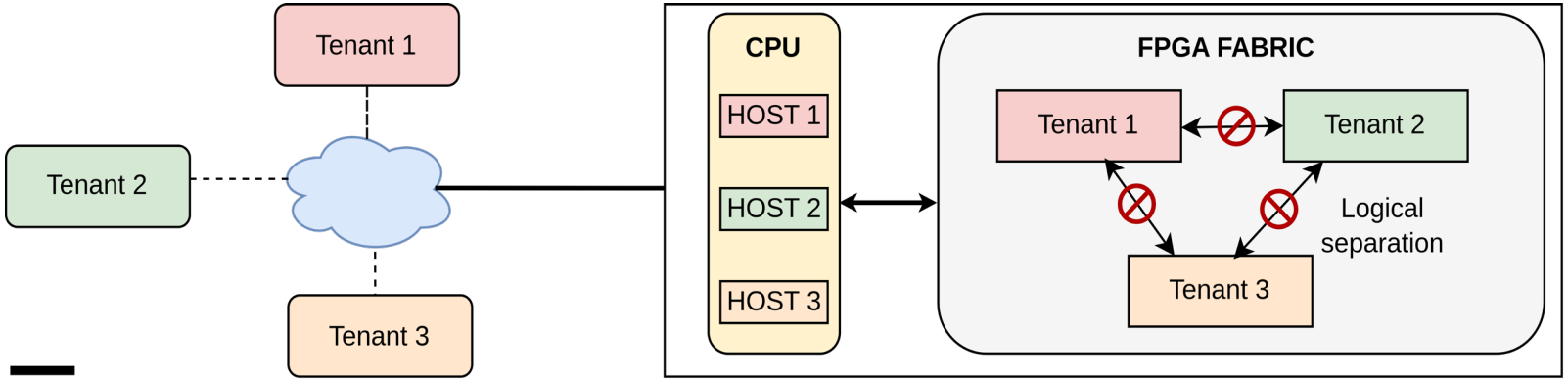
Advanced method for power trace alignement in Remote Power Analysis over Heterogenous SoCs

Anis Fellah-Touta, Prof. Lilian Bossuet, Dr. Carlos Andres Lara-Nino
Laboratoire Hubert Curien, UMR CNRS 5516
Université Jean Monnet, Saint-Etienne, France

Cryptarchi workshop
June 13th, 2023

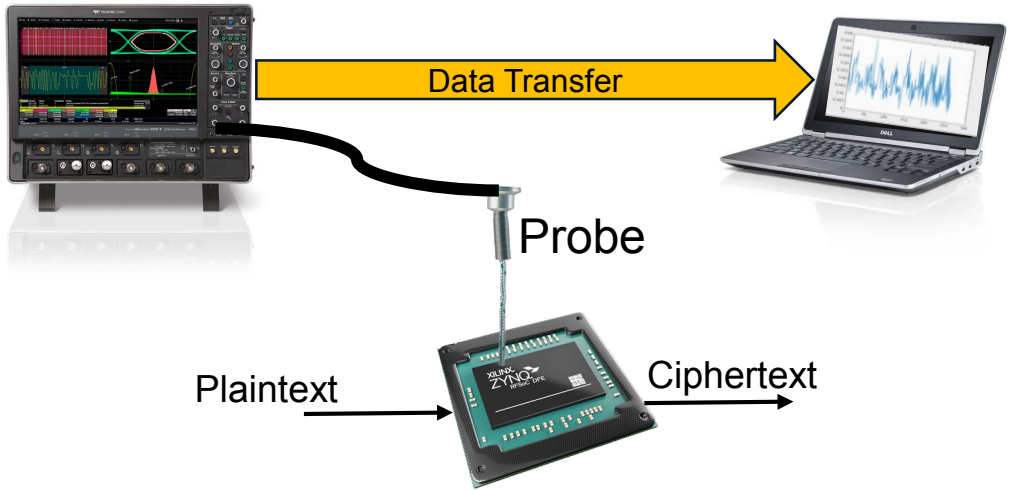
Hardware Accelerators

- Hardware accelerators have been adopted in cloud computing
  - They accelerate computationally intensive tasks, allowing for energy-efficient execution
- Field-Programmable Gate Arrays(FPGAs) have been widely used in datacenters
  - They offer hardware-level parallelism
  - They can be customized to accelerate a wide range of applications, such as cryptography
- Cloud providers allow customers to rent FPGAs for hardware acceleration purposes



Traditional Power Analysis Attacks

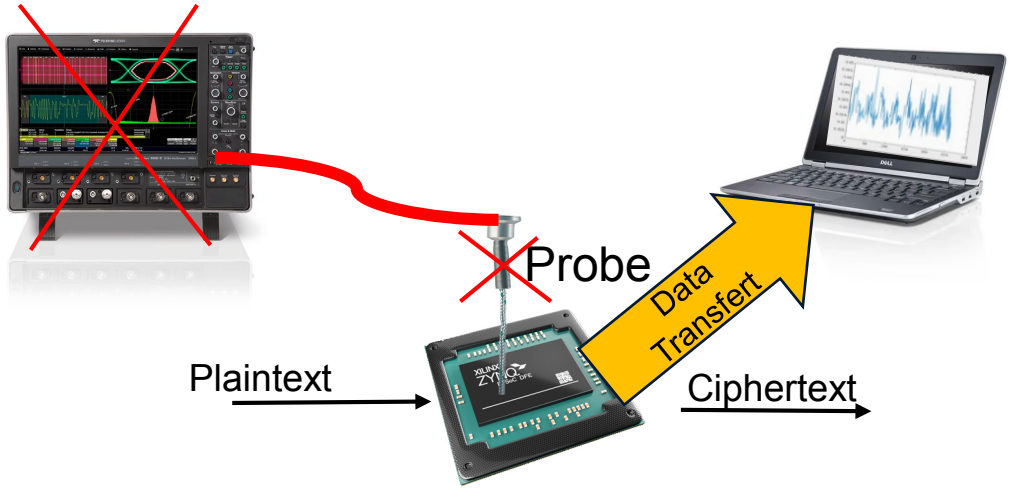
- Deduce secret information by monitoring the power consumption during the execution of cryptographic algorithms
- The attacker needs a physical access to the device



Remote Power Analysis Attacks

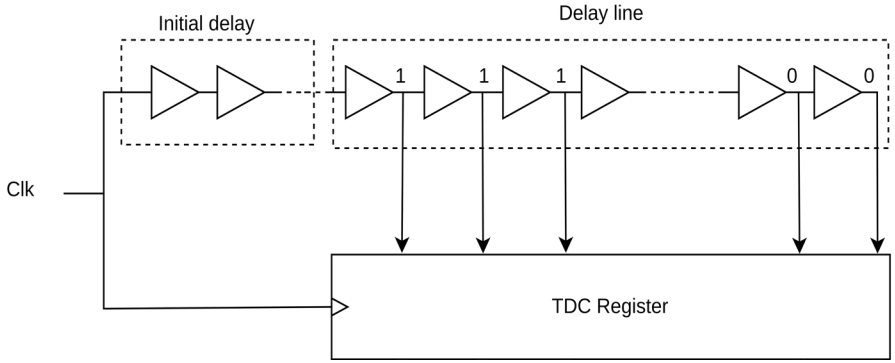
- Deduce secret information by observing the power consumption during the execution of cryptographic algorithms

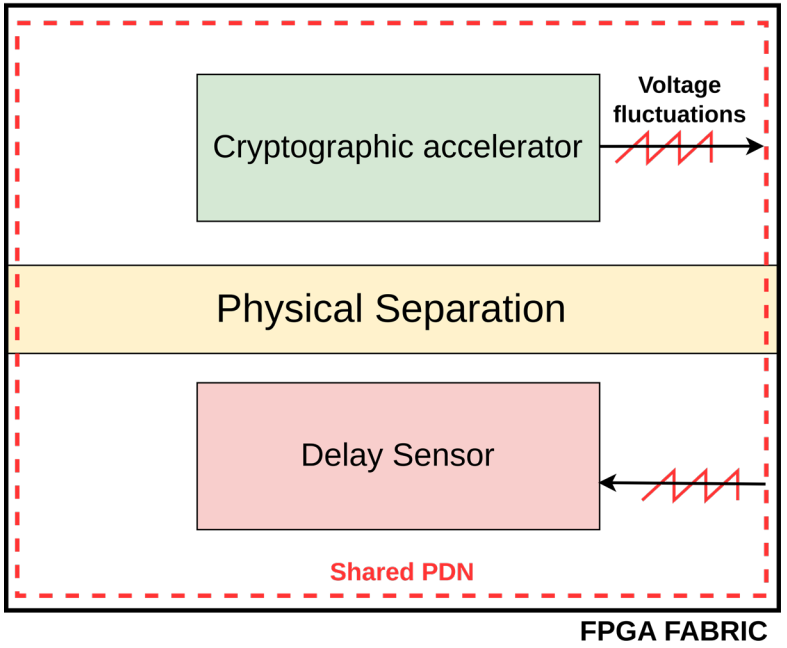
- Remote power attacks **does not require physical access** to the device
  - Internal Voltage sensor can be built using FPGA ressources



FPGA-Based Power Monitor

- Voltage variations affect Propagation delay
- The propagation delay can be measured digitally
- Delay sensors : Time to Digital Converter (TDC), and Ring Oscillator based sensor (RO) [1]





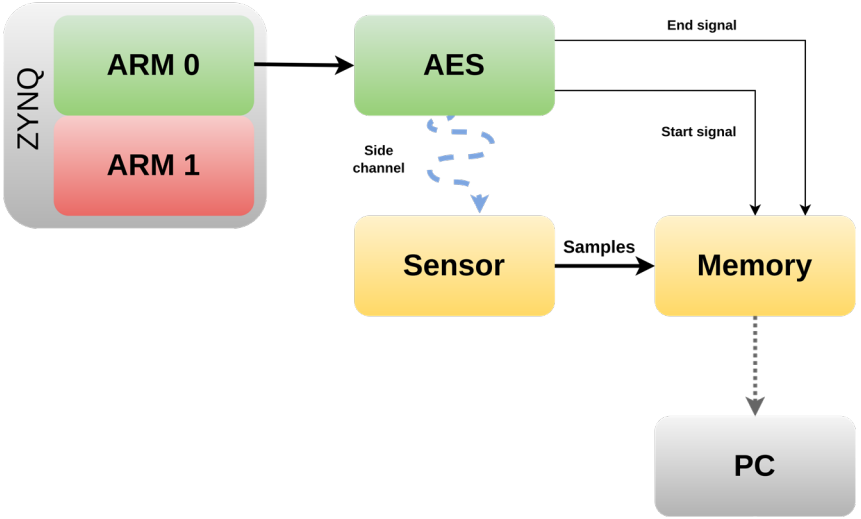
[1] Joseph Gravellier, Jean-Max Dutertre, Yannick Teglia, Philippe Loubet-Moundi, and Olivier Francis. Remote Side-Channel Attacks on Heterogeneous SoC. In CARDIS 2019, Pragues, Czech Republic, November 2019

Limitations of Remote Power Analysis Attacks

• The alignment of power traces is one of the major challenges that an attacker can face

• So far, one of the solution is to create a trigger mechanism based on the sensor output value [2]

• This technique is not completely reliable as it is susceptible to the circuit noise

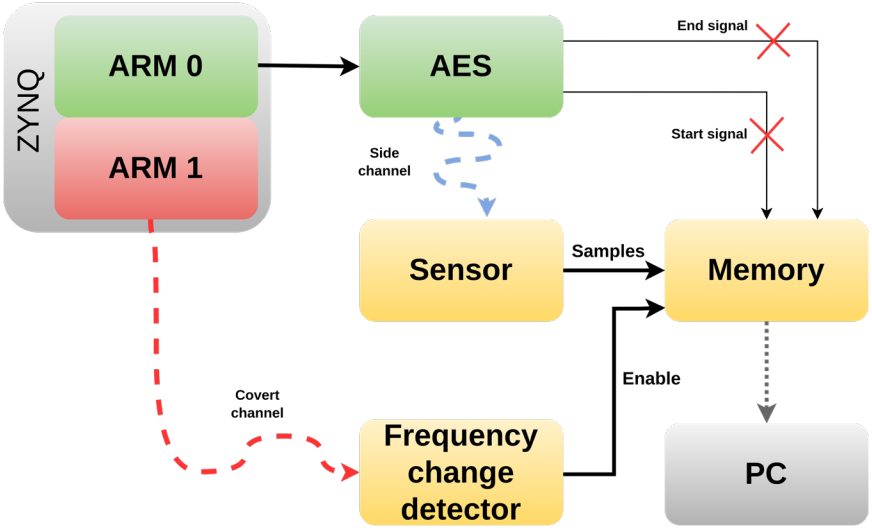


[2] Falk Schellenberg, Dennis R.E. Gnad, Amir Moradi, and Mehdi B. Tahoori. An inside job: Remote power analysis attacks on FPGAs. In 2018 Design, Automation Test in Europe Conference Exhibition (DATE), pages 1111–1116, 2018

Proposed Solution

- Suggest to send covertly the synchronization information to the voltage sensor

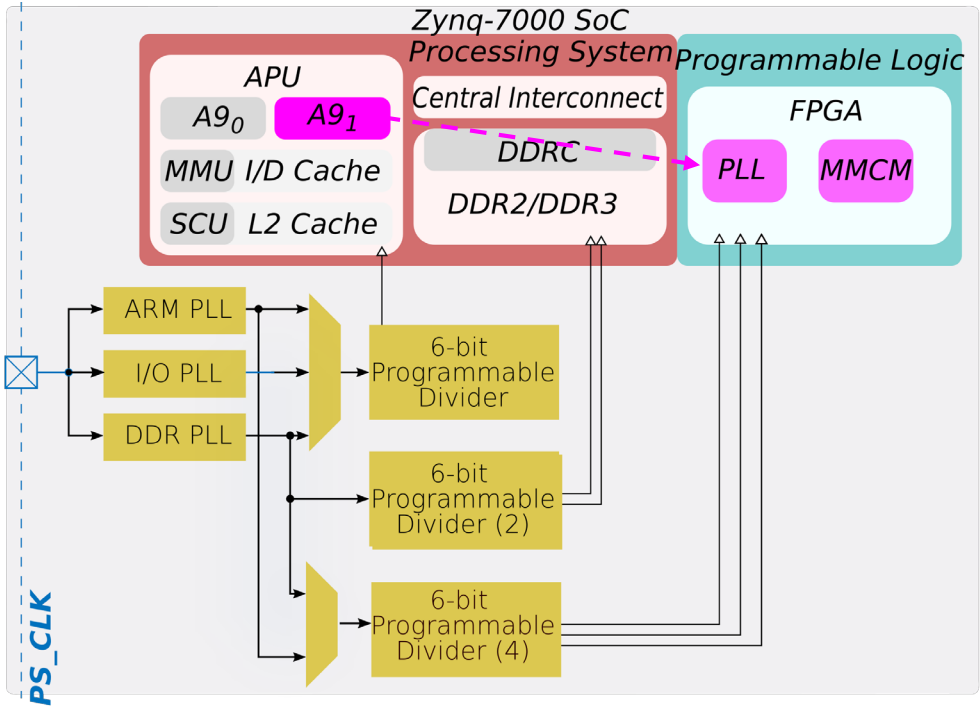
- Create a frequency-based covert channel by modulating the frequency of the clock signal



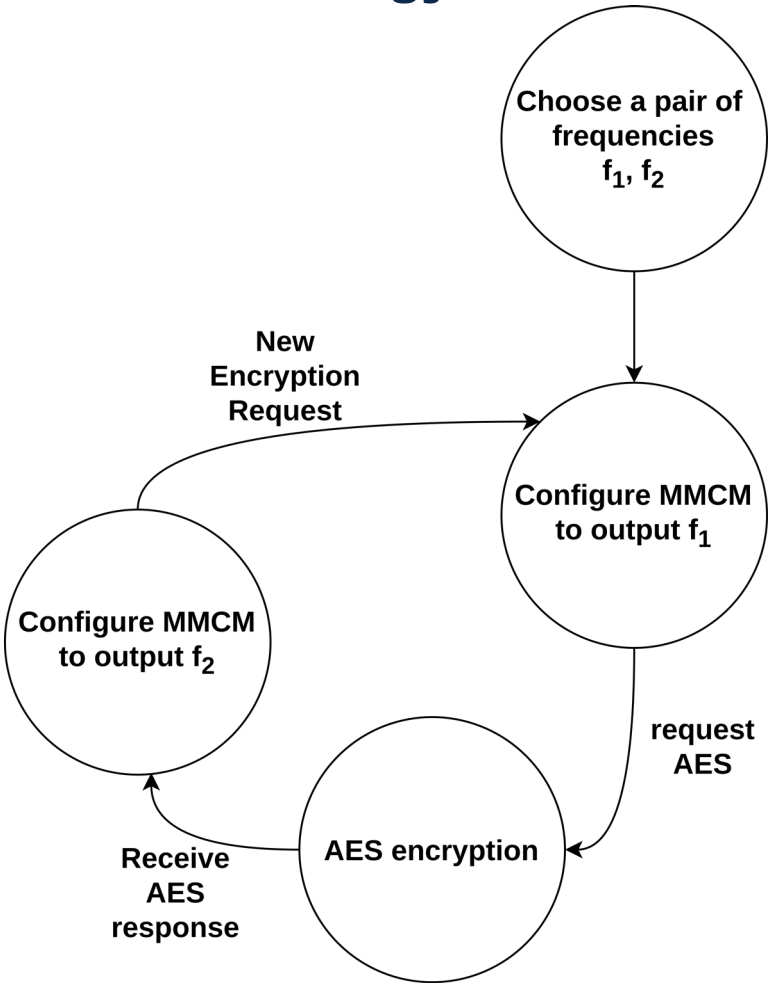
Frequency-based Covert channel

- Use the clocking resources of the FPGA : MMCM and PLL

- Modify the clock without any root privileges and at runtime

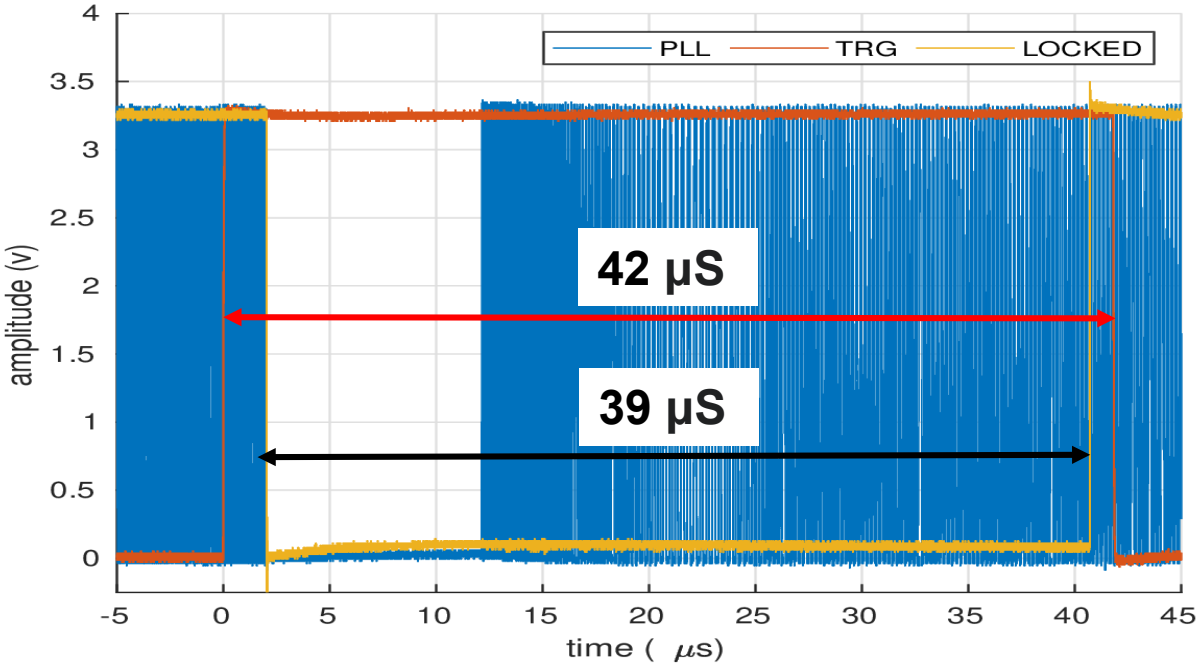


Frequency modulation strategy

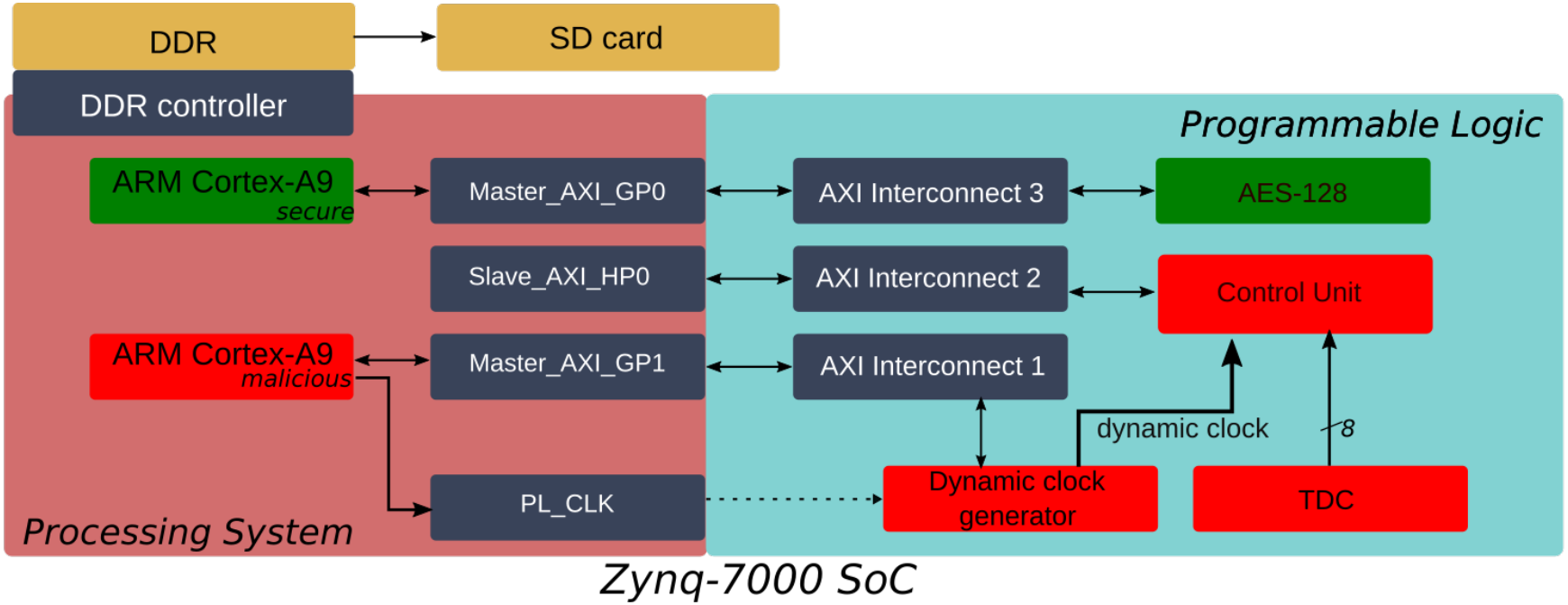


PLL dynamic characterization

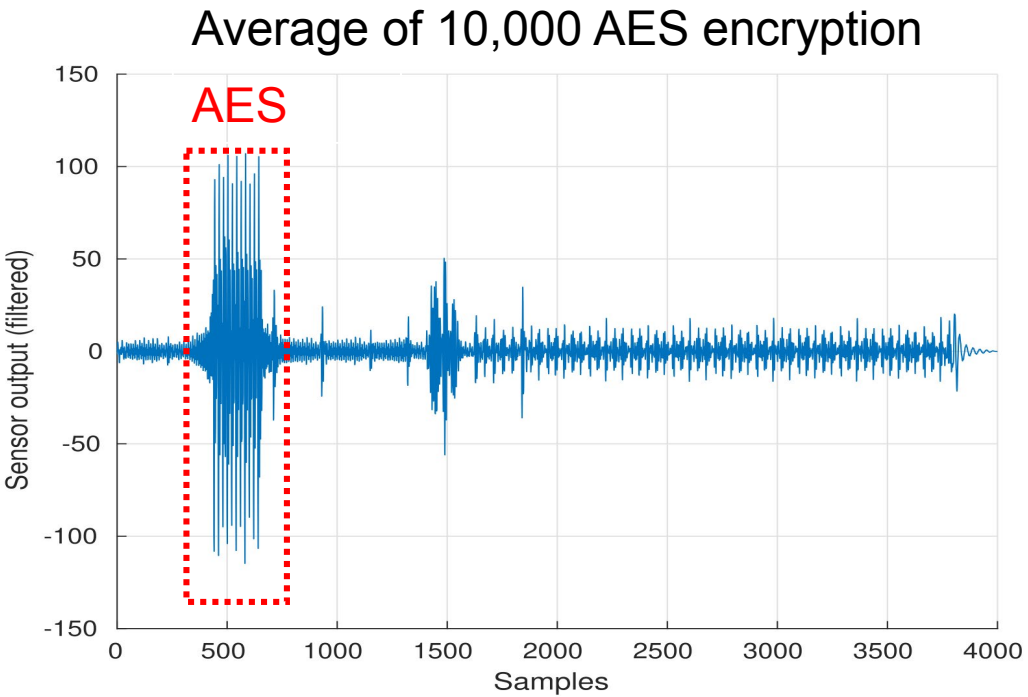
Transition from 66MHZ to 200MHZ



Experimental Setup



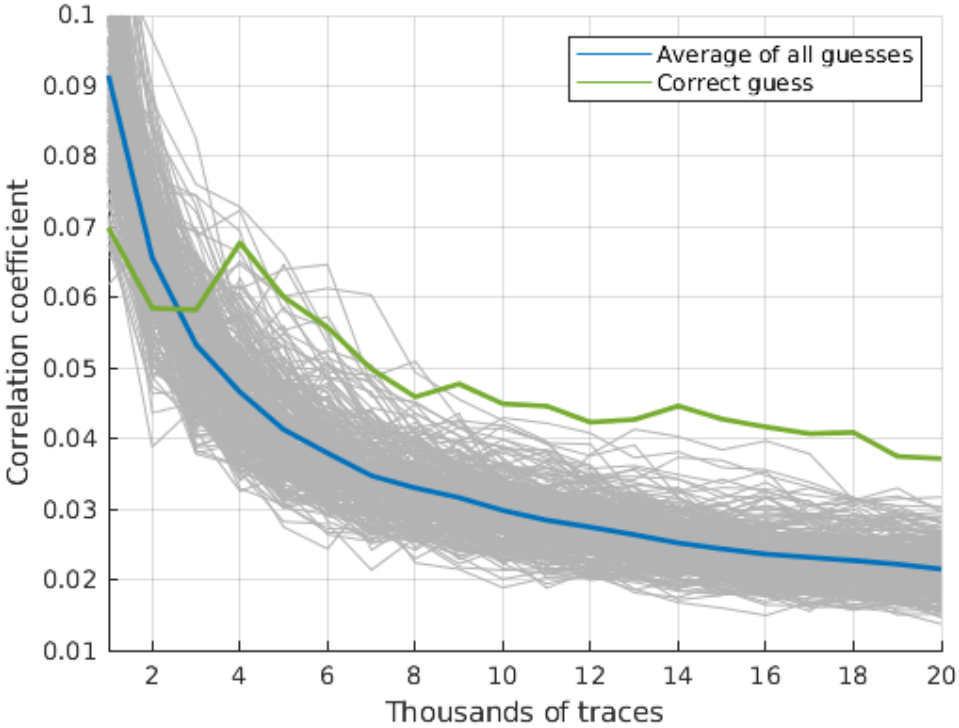
Results



- F_{sample} = 200MHZ F_{AES} = 10MHZ

Results

- Perform Correlation Power Analysis (CPA) to reveal the AES key
- Conduct the CPA on the first-round key
- Target the first key byte
- The correct guess emerges with ~ 9K



Conclusions

- Remote Power Attacks are possible even with logical protections
- Covert channels can be used to strengthen this kind of attack
- Protecting only the main clocks of the SoC is not enough

Thank you for your attention

anis.fellah.touta@univ-st-etienne.fr