LABORATOIRE HUBERT CURIEN
UMR • CNRS • 5516 • SAINT-ETIENNE

UNIVERSITÉ JEAN MONNET SAINT-ÉTIENNE

cnrs

Extension de la TrustZone et de la TEE :

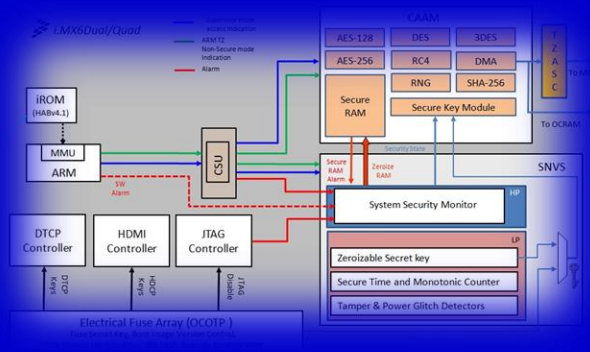
Secure or not secure?

Lilian Bossuet
Laboratoire Hubert Curien

Le slide qui fait peur !!! (*tiré d'histoires vraies*)

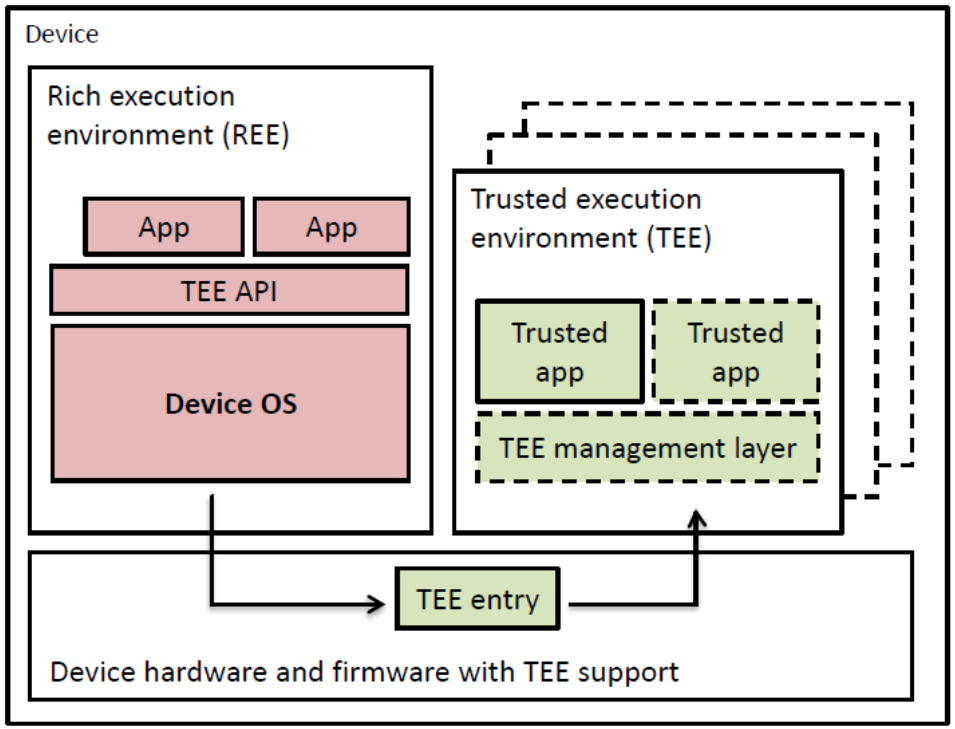
- De multiples attaques sur les systèmes embarqués connectés

Trusted Execution Environement – TEE



Architecture TEE

- Une TEE est un microkernel pour la sécurité
  - Utilise des ressources matérielles dédiées



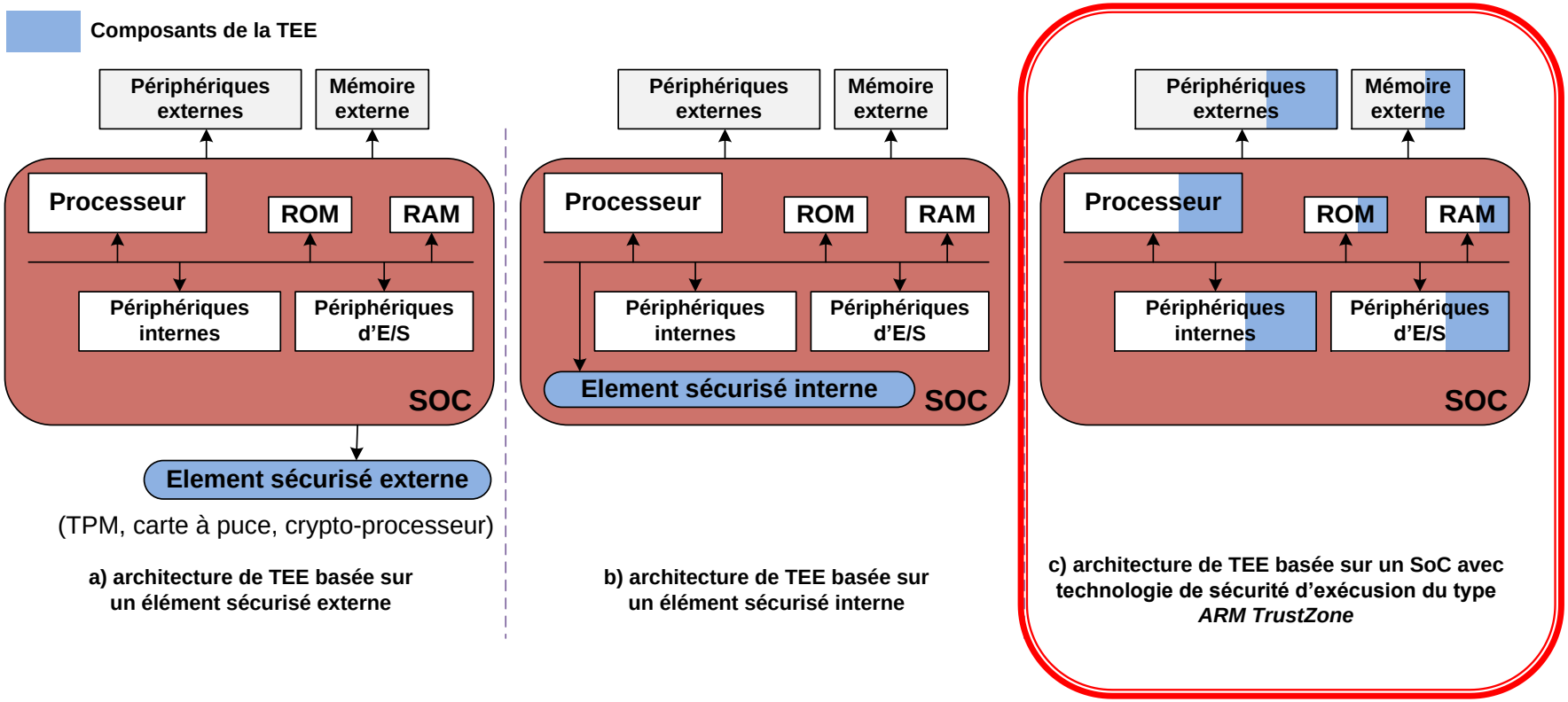
Architectures with single TEE

- ARM TrustZone
- TI M-Shield
- Smart card
- Crypto co-processor
- TPM

Architectures with multiple TEEs

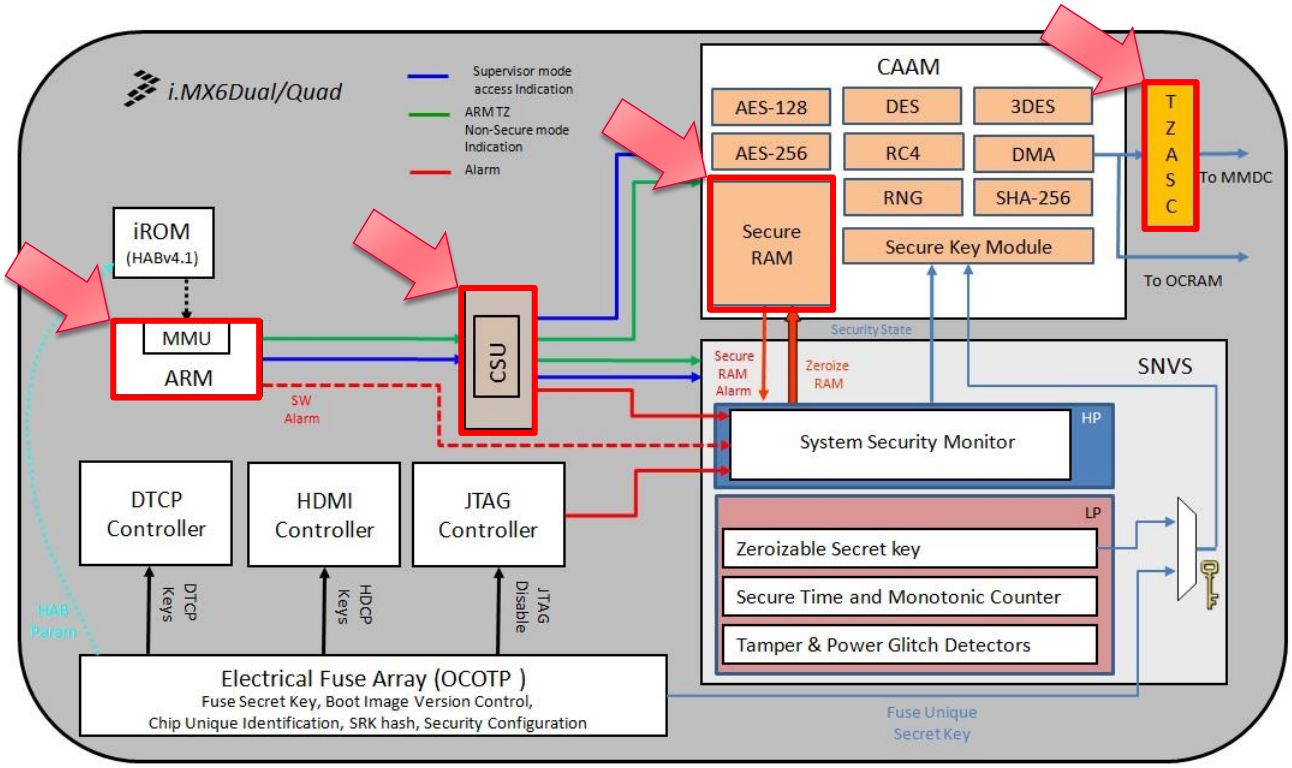
- Intel SGX
- TPM (and “Late Launch”)
- Hypervisor

Implémentations possibles

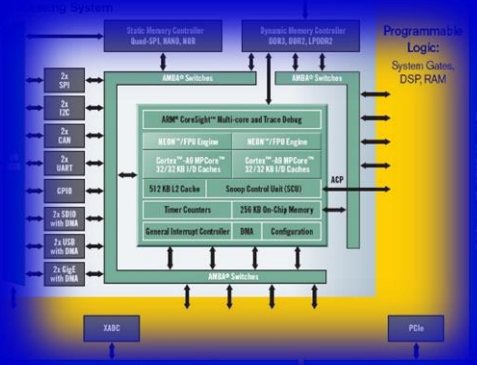


Architecture matérielle de sécurité ARM Cortex A9

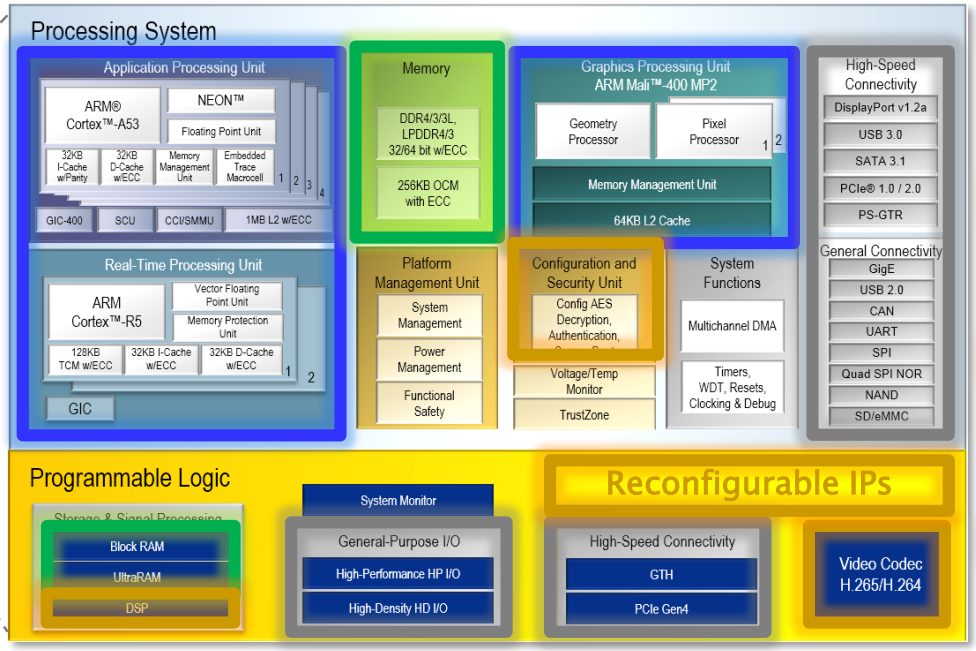
- TrustZone
  - Central Security Unit (CSU) – TZ Address Space Controller (TZASPC), TZ Watchdog



Sécurité de l'extension de la TrustZone dans un SoC complexe hétérogène



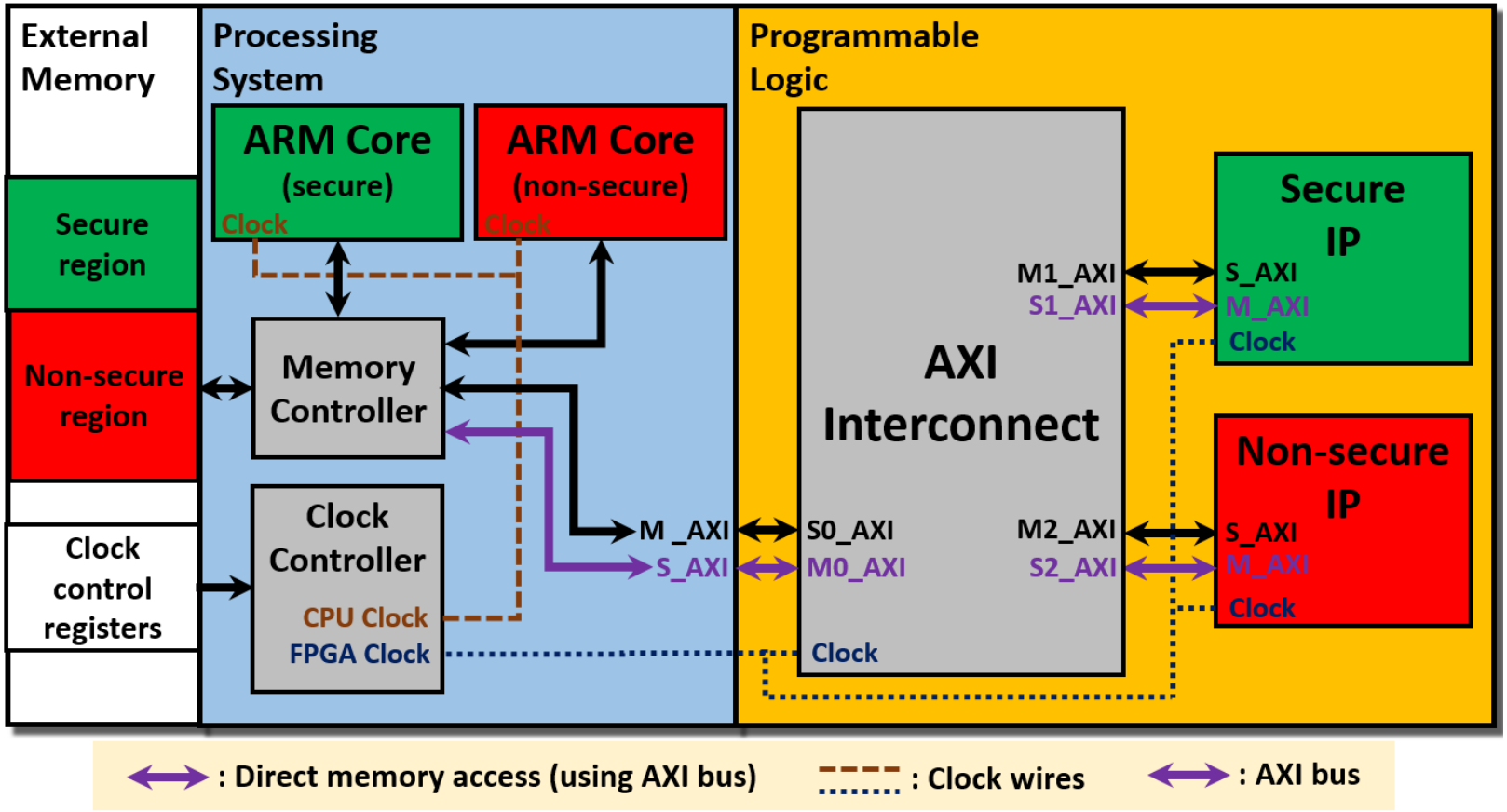
SoC complexe hétérogène



- **General purpose and dedicated processors**
- **Memory ressources**
- **Hardware accelerator (cryptography, video, signal processing …)**
- **Connectity to external peripherals and memories**

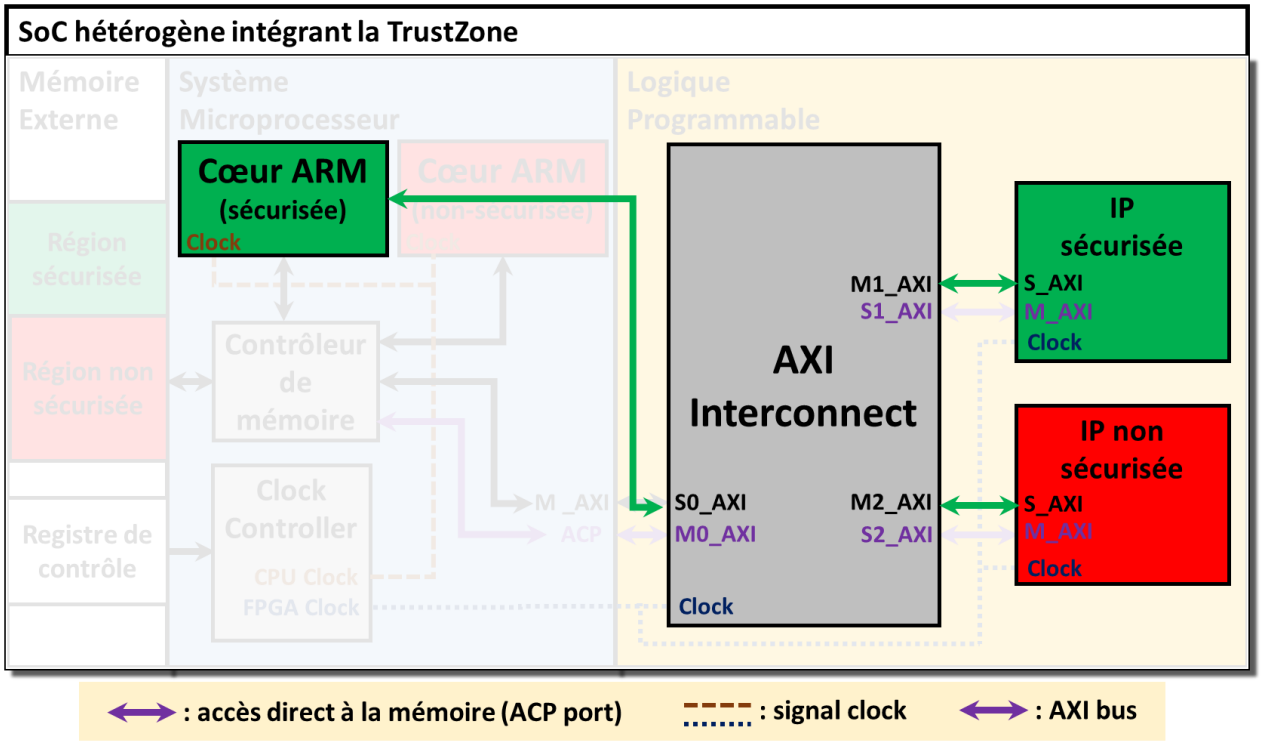
Architecture interne d'un SoC hétérogène

Système cible



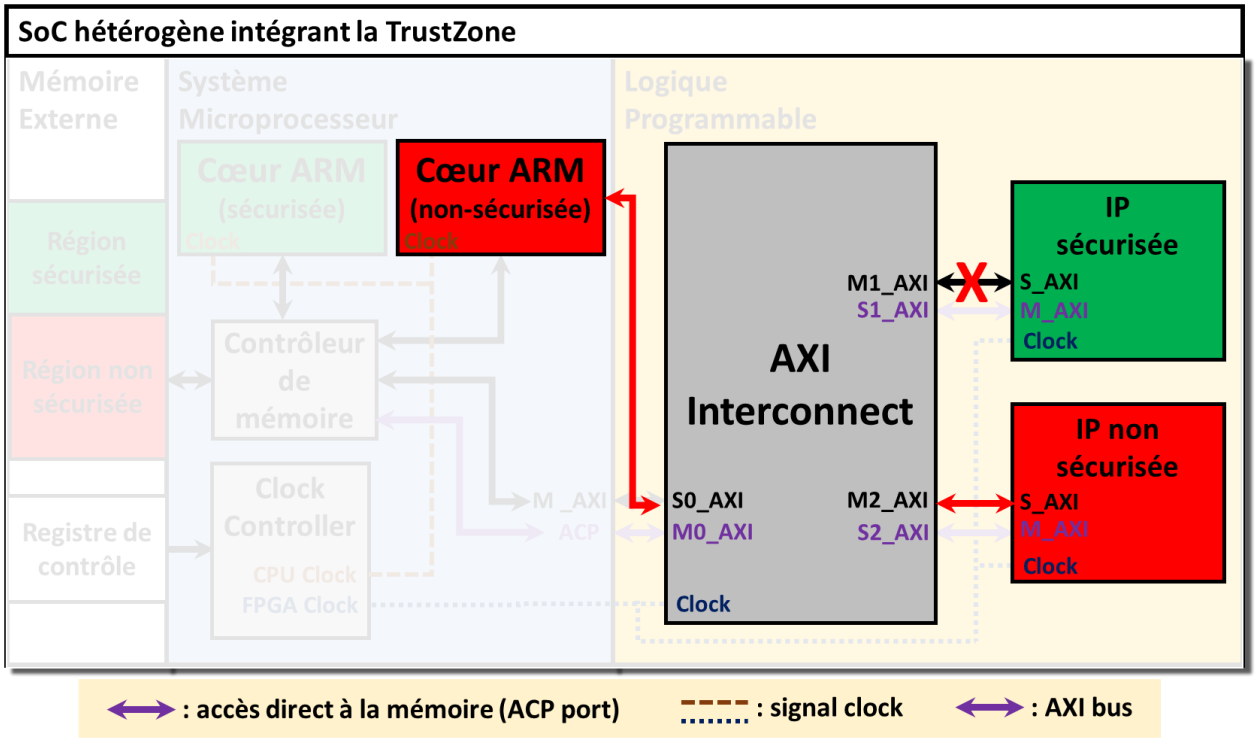
Fonctionnement du système

- Le monde sécurisé a un accès total au différentes IP de la partie reconfigurable



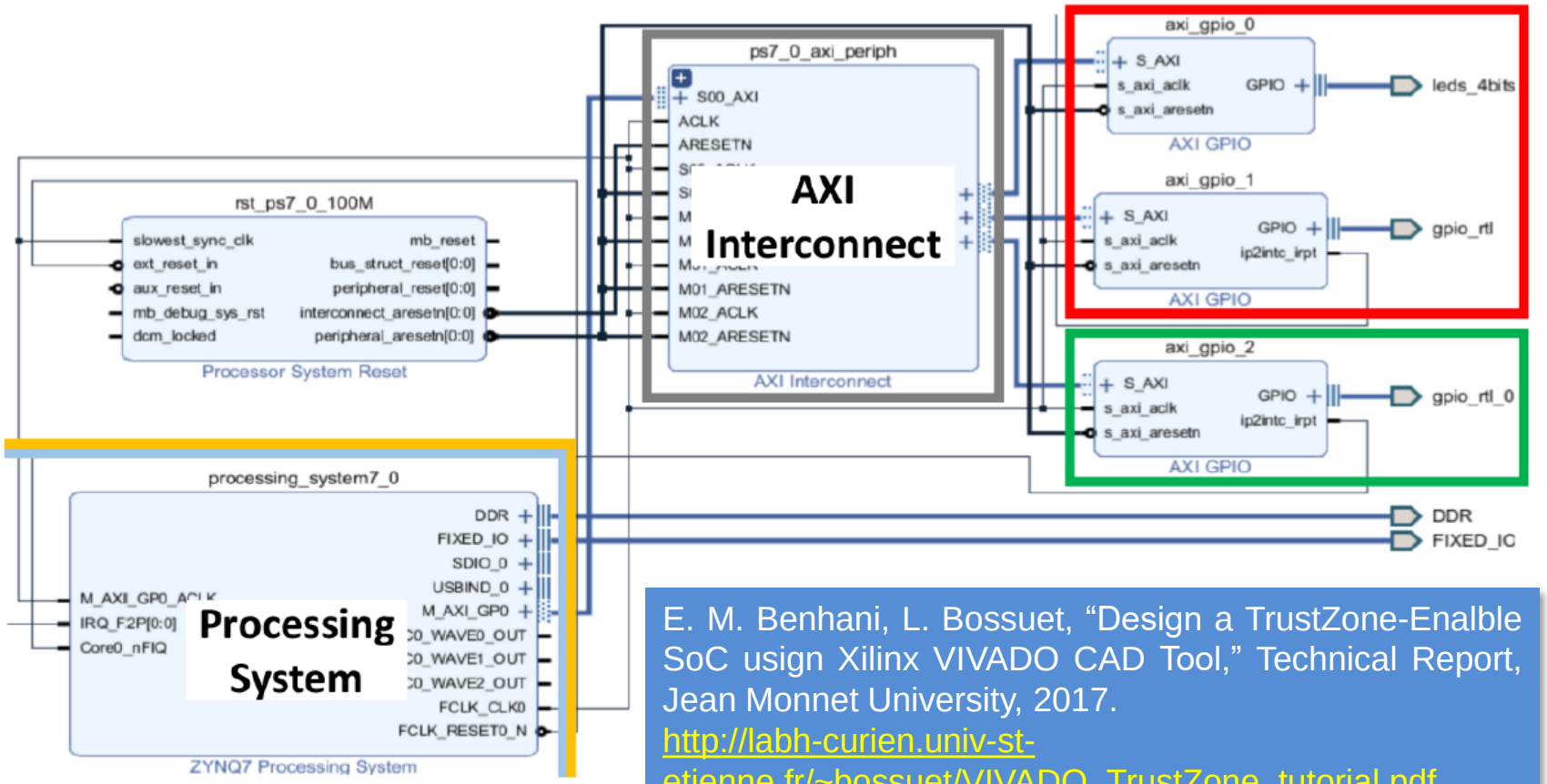
Fonctionnement du système

- Le monde non-sécurisé a accès seulement aux IP non-sécurisées de la partie reconfigurable



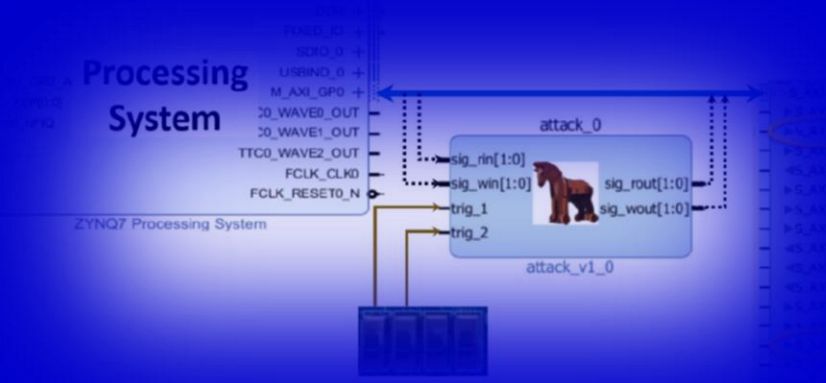
Prototypage (Xilinx Zynq)

- Architecture du système développé (Xilinx Vivado)

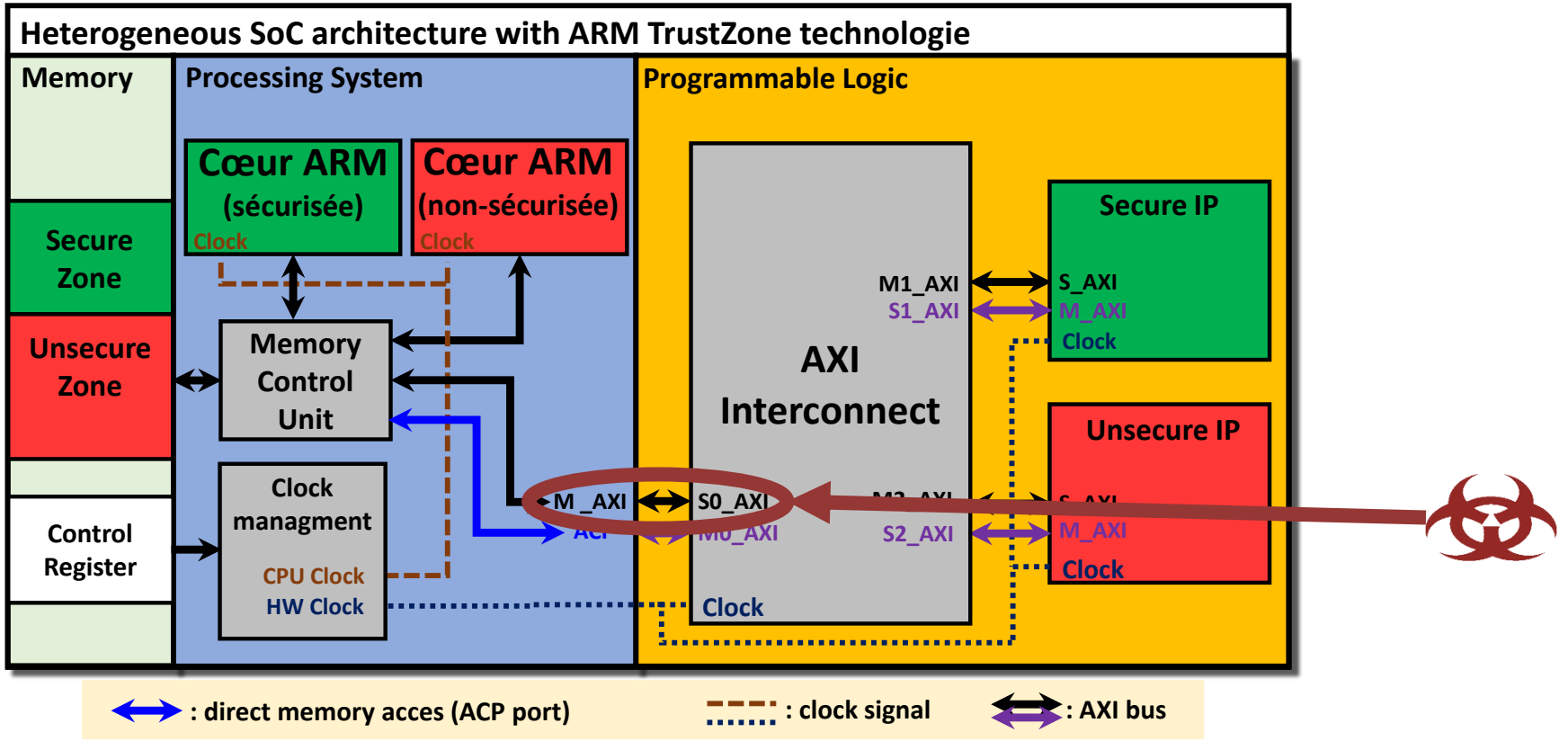


E. M. Benhani, L. Bossuet, “Design a TrustZone-Enalble SoC usign Xilinx VIVADO CAD Tool,” Technical Report, Jean Monnet University, 2017.
http://labh-curien.univ-st-etienne.fr/~bossuet/VIVADO_TrustZone_tutorial.pdf

Attaques par corruption matérielle



1) Corruption du port AXI

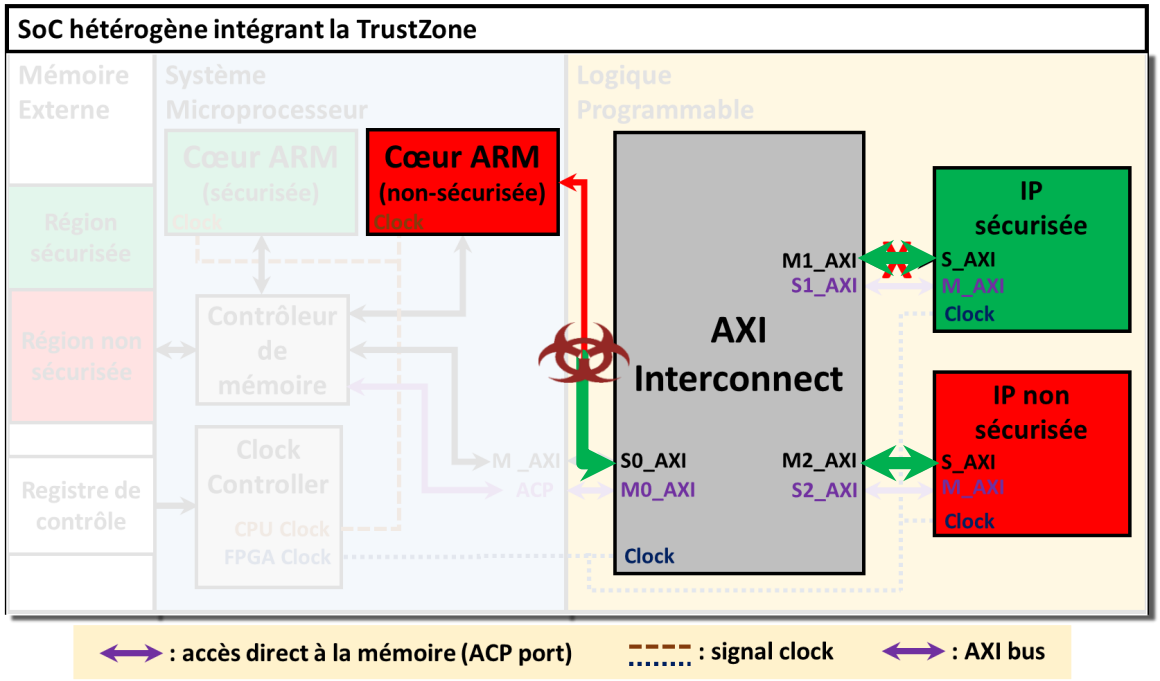


AXI : ARM advanced Micro-controller Bus Architecture (AMBA) Advanced eXtensible Interface (AXI)

Exemples de modification du signal AWPROT

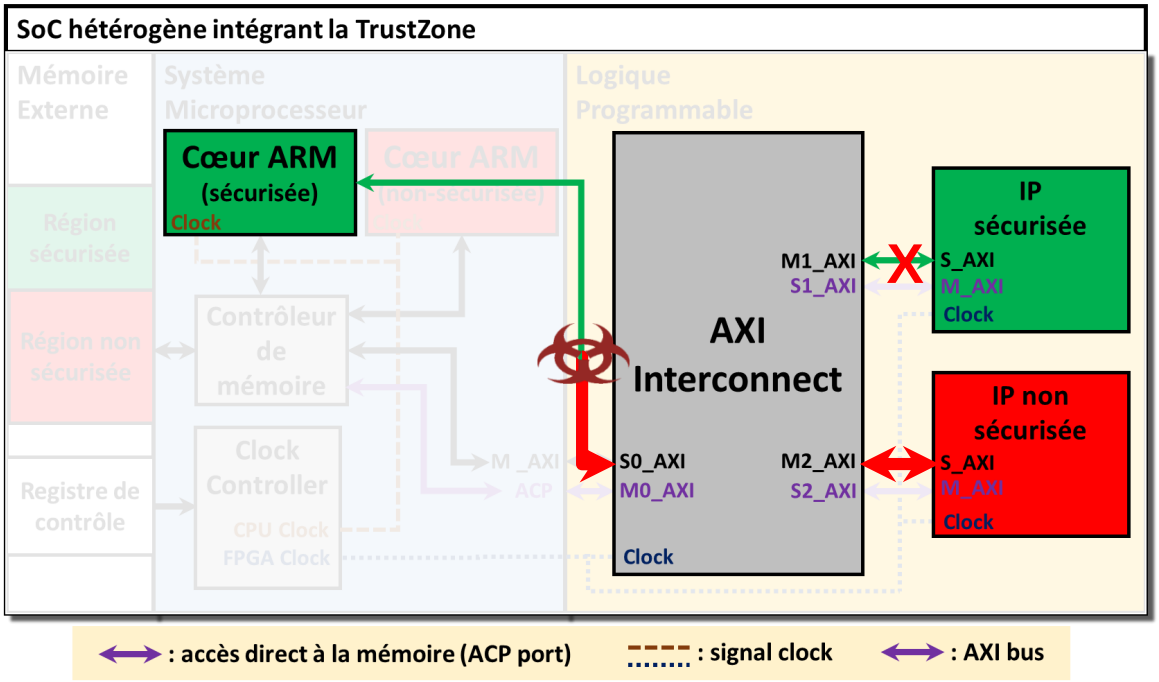
Effet de la modification du signal AWPROT 1/2

- Le monde non-sécurisé a un accès total aux différentes IP de la partie reconfigurable



Effet de la modification du signal AWPROT 2/2

- Le monde sécurisé ne peut plus utiliser les IP sécurisées de la partie reconfigurable

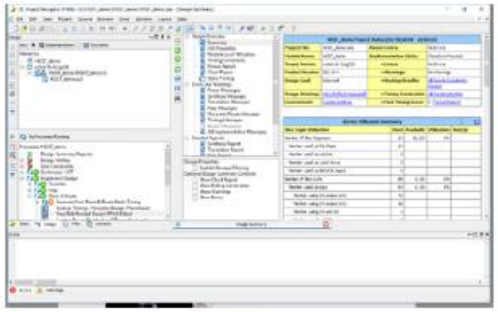


Demonstration of Security Threats from Malicious FPGA Tools and Corresponding Countermeasures

Zhiming Zhang, Jaya Dofe, and Qiaoyan Yu
Dept. of Electrical and Computer Engineering
University of New Hampshire
Durham, NH 03824, USA
zz1017@wildcats.unh.edu

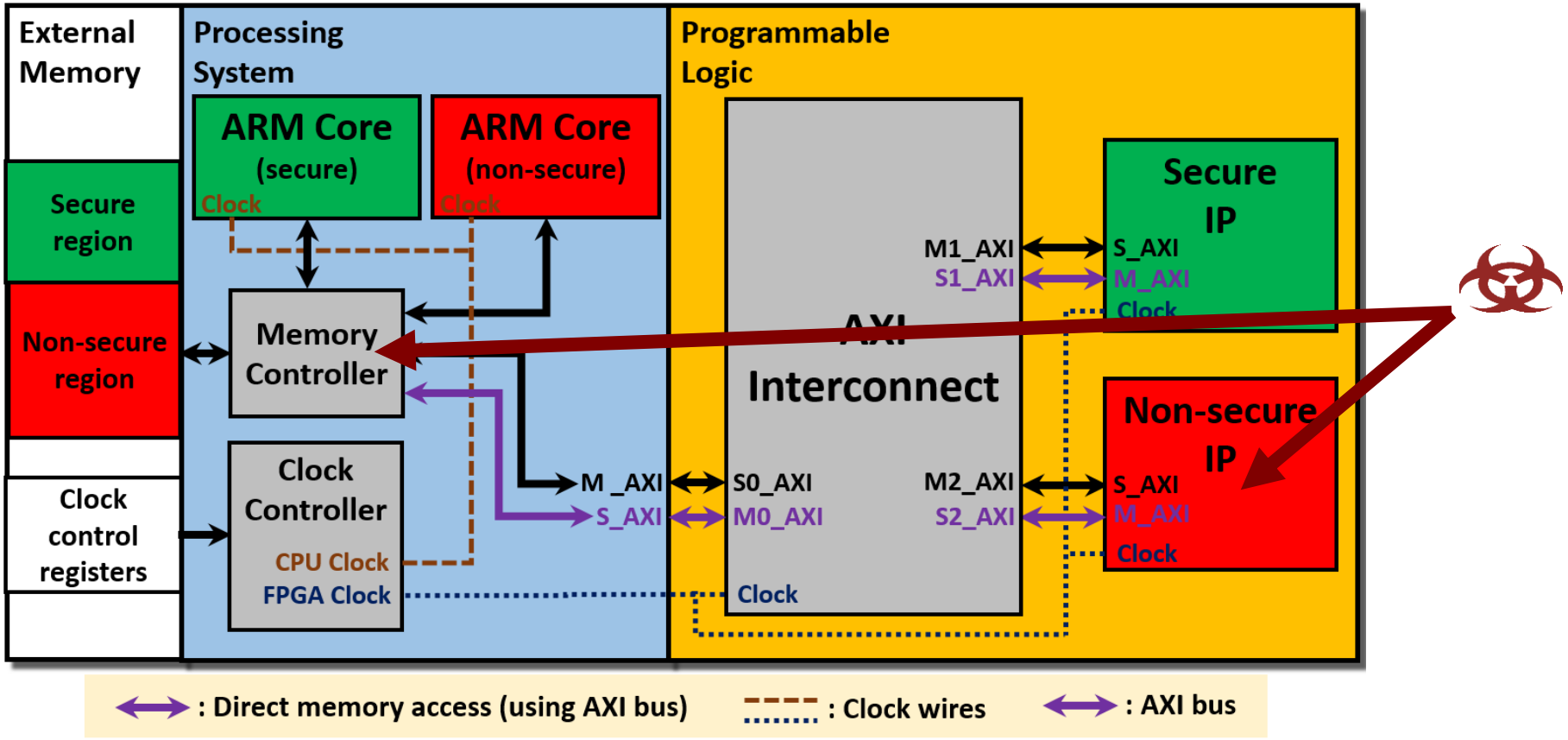
I. Description of the Research

Field Programmable Gate Arrays (FPGAs) enter a rapid growth era due to their attractive flexibility and CMOS-compatible fabrication process. Because of the high demand on the FPGA usage in data processing, industrial, automotive, consumer electronics, telecom, military and aerospace, FPGA market achieves a compound annual growth rate of 8.4% [1]. The increasing popularity of FPGAs also attracts attacker's attention because high improper benefits may be obtained once the FPGA-based system is manipulated. To protect FPGAs from being attacked, a great amount of works on FPGA security have been done [2]. Existing works primarily focus on reverse engineering the downloaded FPGA configuration, retrieving the authentication code or crypto key stored on the FPGA memory, and countermeasures for the security threats above. However, there are limited works addressing the security threats from malicious FPGA design software, which could harm the integrity of a design running on SRAM FPGAs [3]. In this demo, we introduce the potential security vulnerabilities of computer-aided design (CAD) tool. This group of attacks are implemented on the CAD tool which is used to generate bitstream so that the FPGA behavior can be

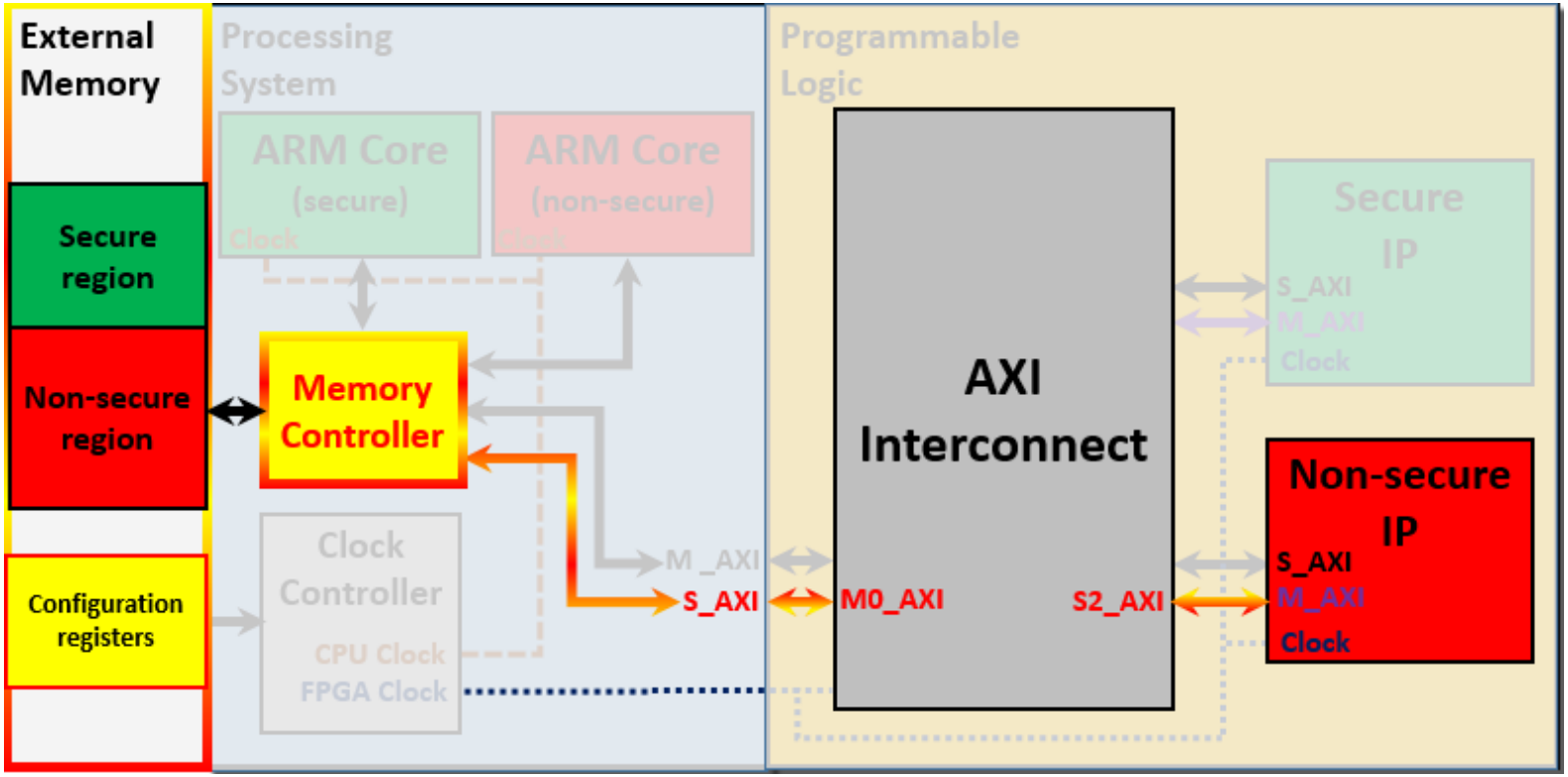


(a)

IP matériel malicieux et accès direct à la mémoire



IP matériel malicieux et accès direct à la mémoire



- **Nécessite la connaissance du mapping mémoire des registres de configuration de la TrustZone**
- **Utilisation du ARM ACP Accelerator Coherency Port => on ne passe pas par le CPU**

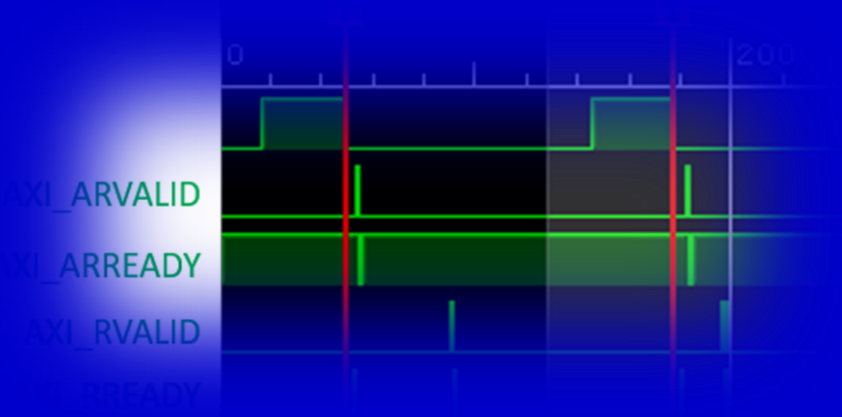
Conclusion 1/3

- Preuve de concept de plusieurs attaques possibles ciblant l'extension de la TrustZone dans un SoC complexe hétérogène (FPGA + ARM)
  - Corruption su signal AWPROT
  - Corruption du composant AXI interconnect
  - Accès direct à la mémoire

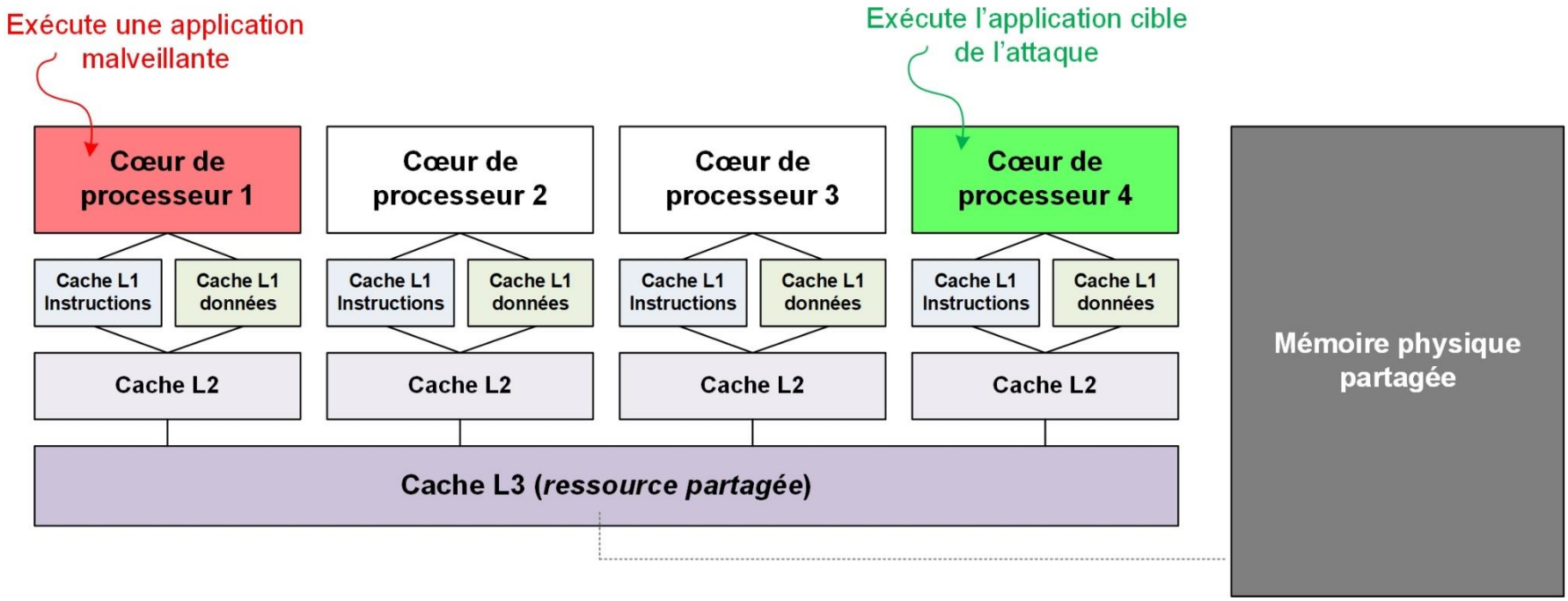
- Référence

E.M. Benhani, L. Bossuet, A. Aubert. *The Security of ARM TrustZone in a FPGA-based SoC*. IEEE Transactions on Computers, February 2019

Attaque par analyse temporelle des mémoires caches

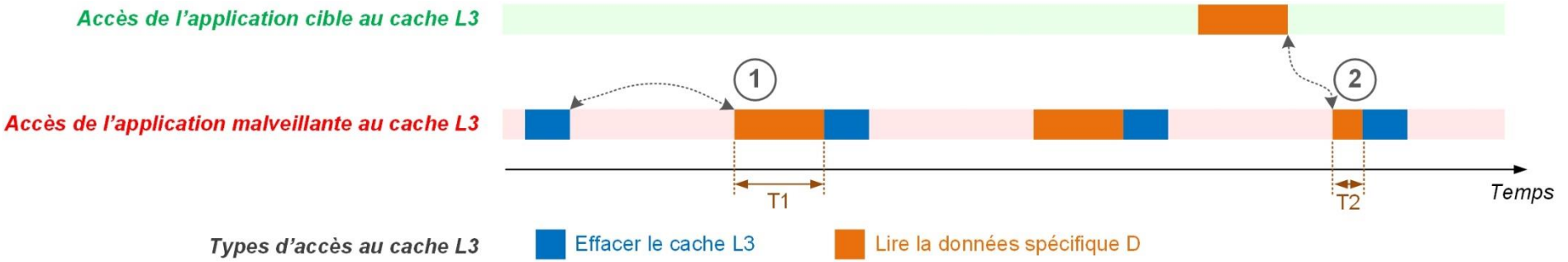


Analyse des temps d'accès à la mémoire caché partagée dans les SoC multi-processeurs



Analyse des temps d'accès à la mémoire caché partagée dans les SoC multi-processeurs

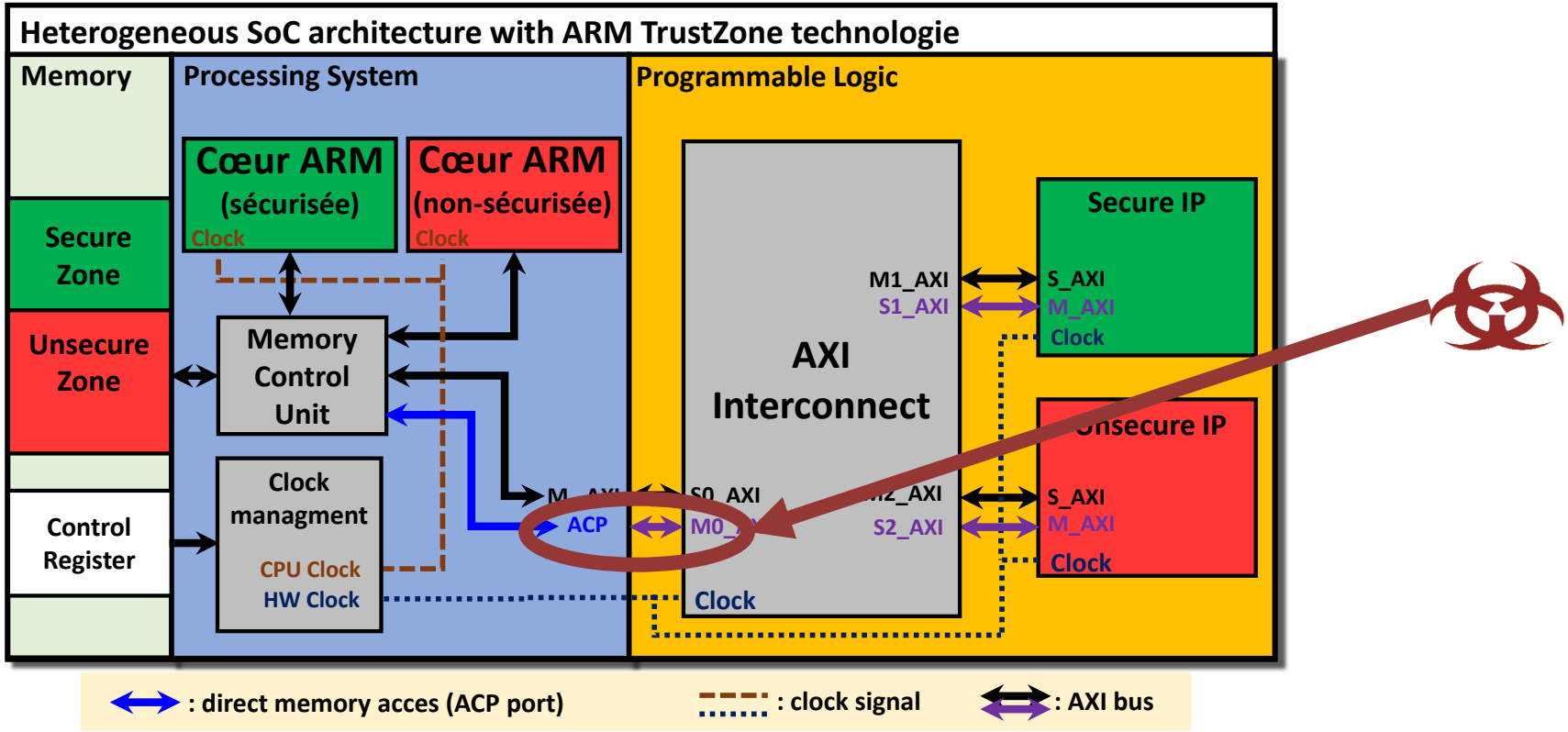
- L'application malveillante analyse le temps d'accès à une donnée D un certain temps après avoir effacé la cache L3 …



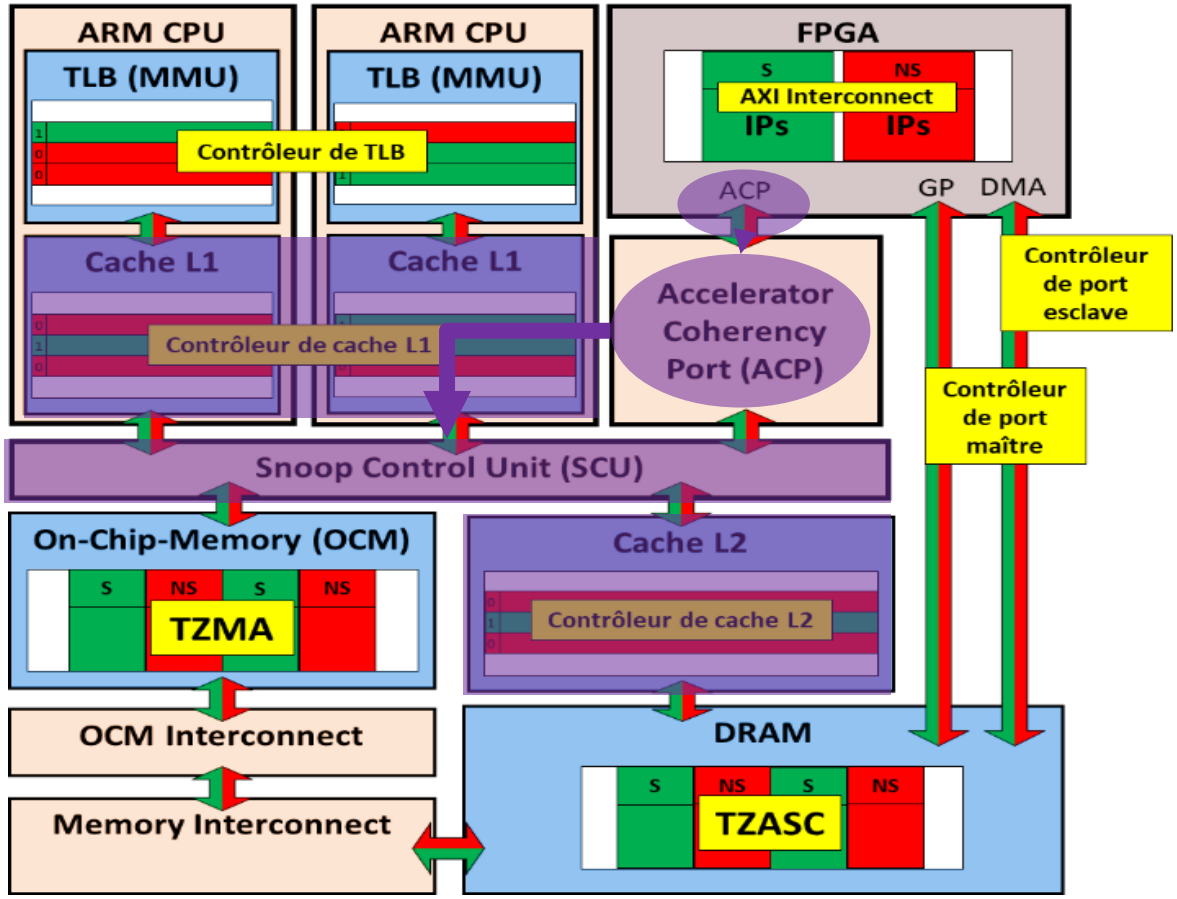
1. L'application malveillante a vidé le cache L3, son temps d'accès T1 à la donnée D est long car il faut aller chercher la donnée en mémoire physique
2. L'application cible a accédé à la donnée D qui est donc présente en cache L3, le temps accès T2 de l'application malveillante à la donnée est plus rapide

- Peut conduire à trouver des clés de chiffrements pour des implantations très particulière de l'AES (T-box) ou des implantations de RSA non sécurisées

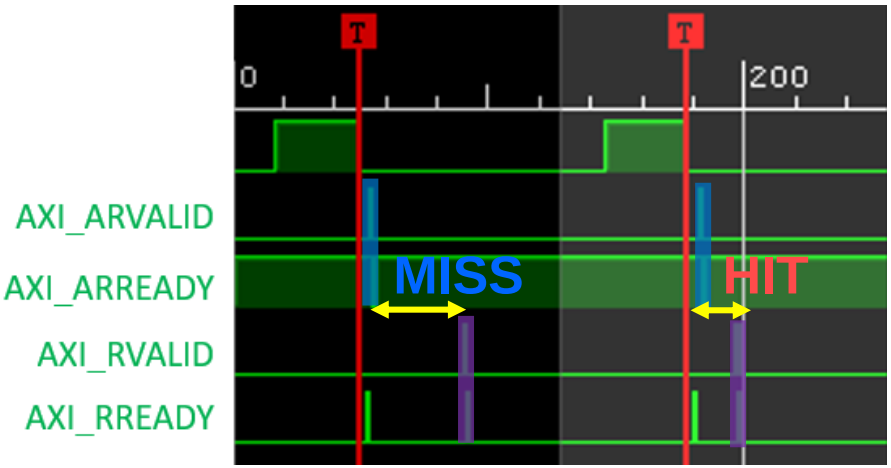
Utiliser le port ACP pour l'analyse en temps

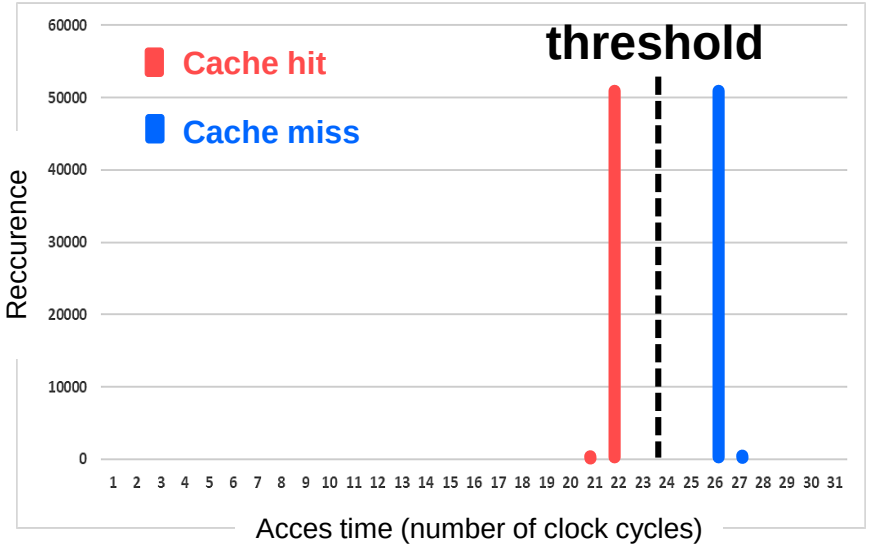


ACP - Accelerator Coherency Port



Proof of concept





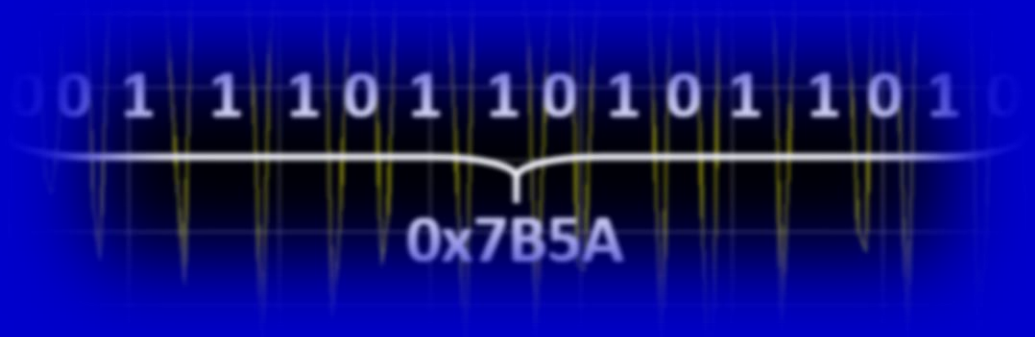
Conclusion 2/3

- Preuve de concept de la possibilité de réaliser des attaques par analyse de la mémoire cache depuis la partie matérielle (FPGA) d'un SoC hétérogène
  - Réalisation de l'attaque compléte sur un AES T-box s'exécutant sur un des cœurs ARM

- Référence :

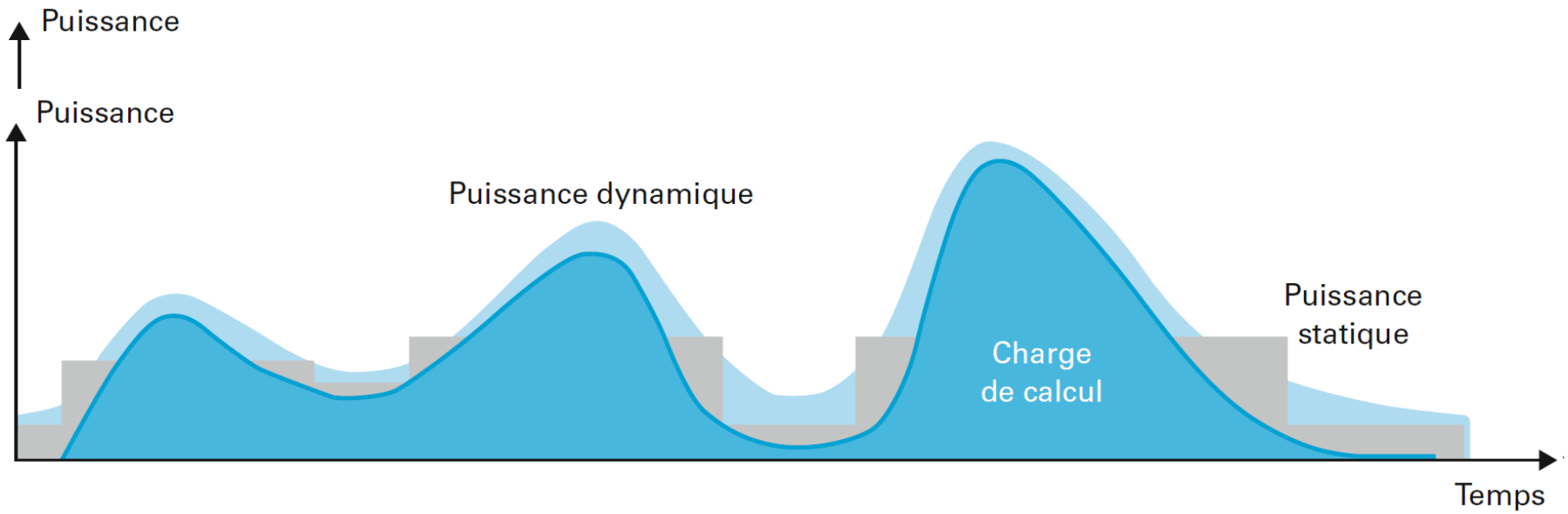
Lilian Bossuet, El Mehdi Benhani. *Security Assessment of Heterogenous SoC-FPGA: On the Practicability of Cache Timing Attacks*. In Proceedings of 29th IFIP/IEEE International Conference on very Large Scale Integration, VLSI-SoC 2021, Singapore, October 2021.

Transmission discrète d'informations (*DVFS as a cover channel*)



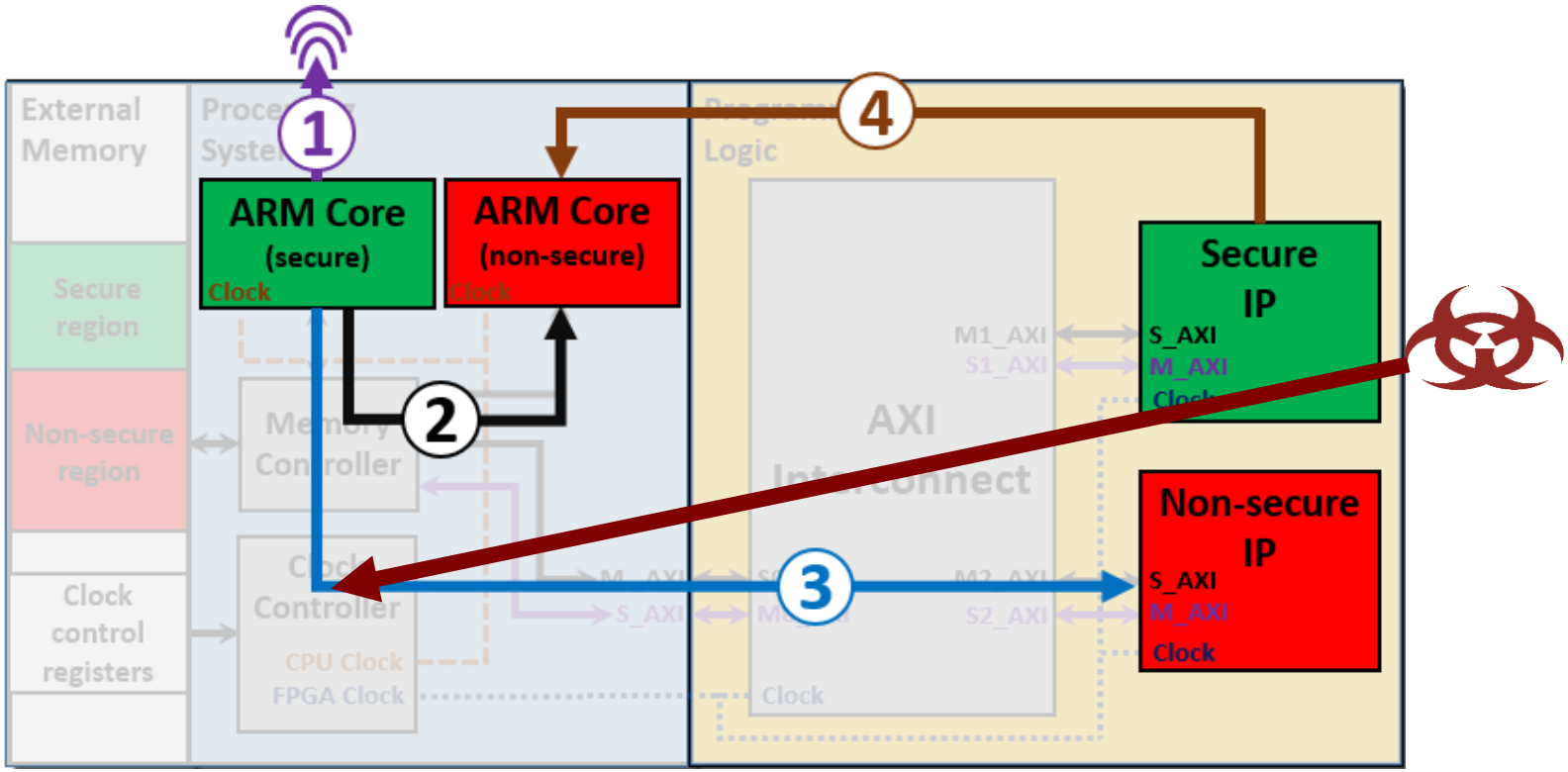
Dynamic Voltage and Frequency Scaling

- Management de la consommation de puissance des processeurs et SoC modernes

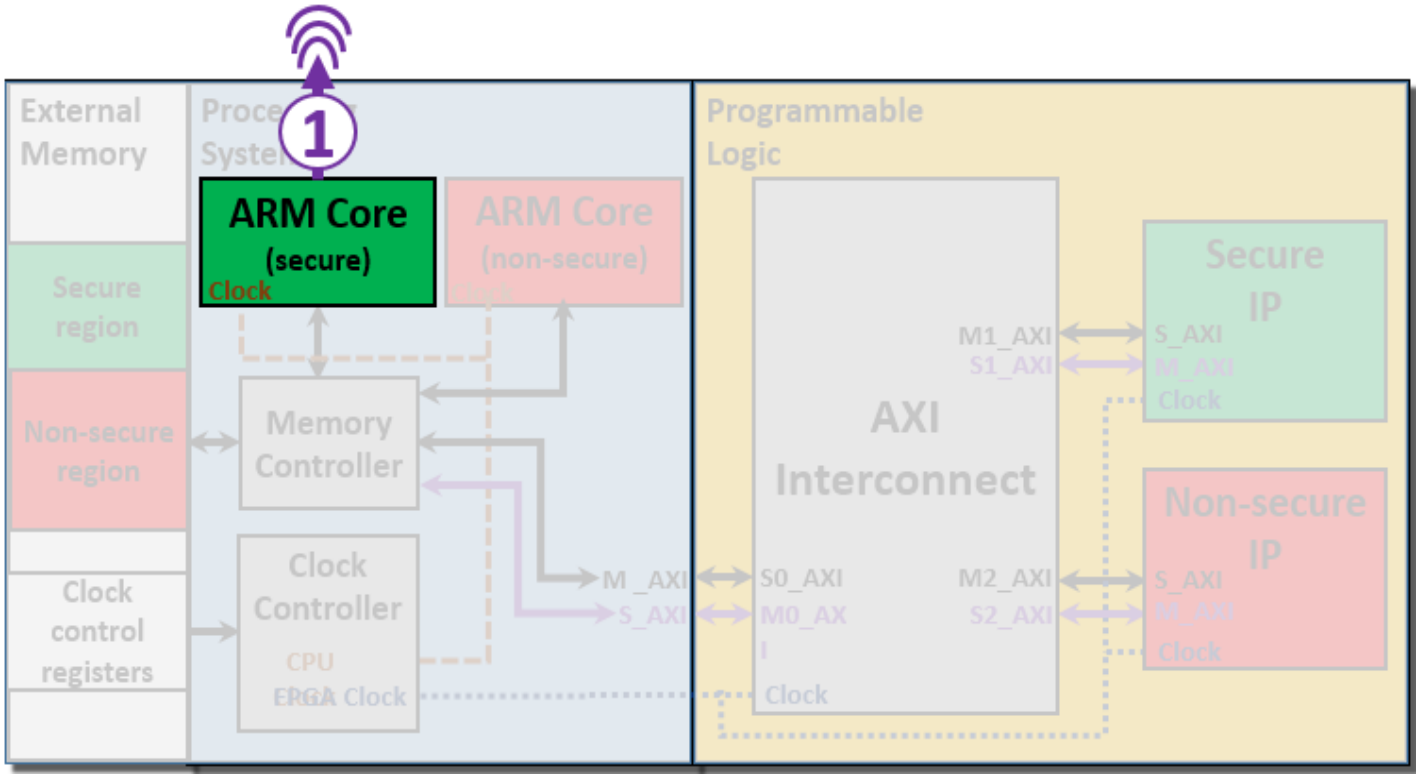


Utilisations malicieuses du DVFS

Cible : Clock Controller



① Transfert de données sensibles du cœur ARM sécurisé vers l'extérieur du SoC



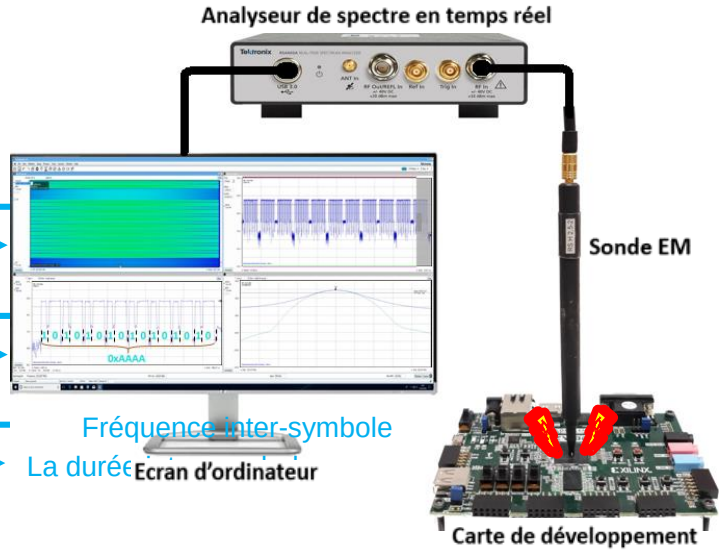
① Transfert de données sensibles du cœur ARM sécurisé vers l'extérieur du SoC

Processus d'espionnage au niveau du cœur ARM sécurisé

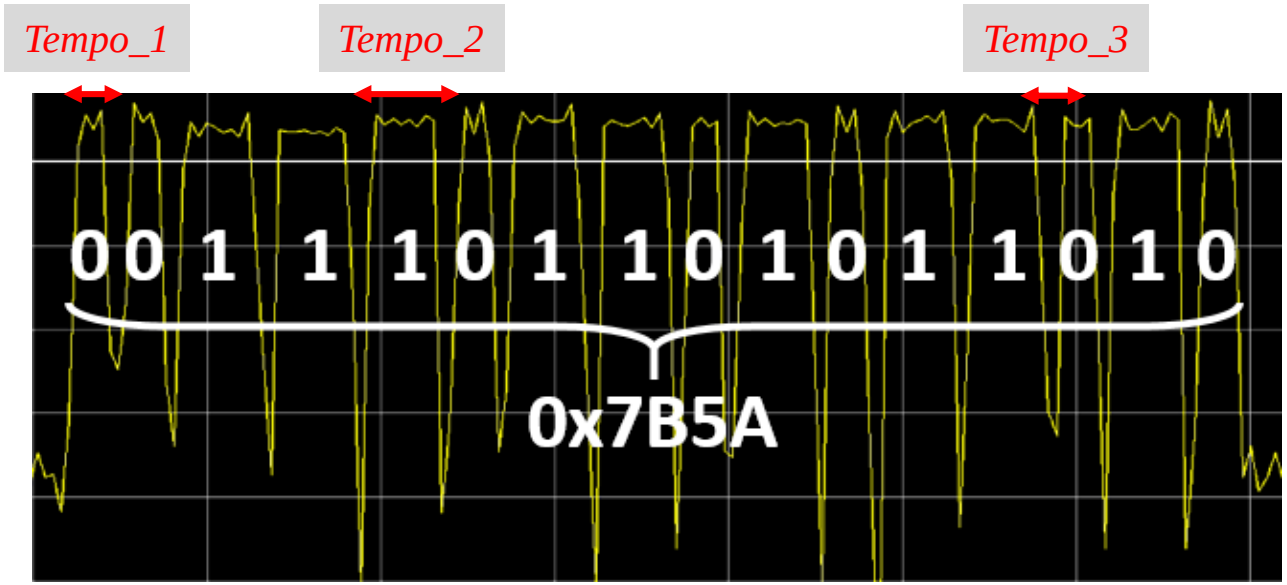
Algorithme 1: Modulation de fréquence

Input: *donnée_à_transférer*
For i = *donnée_à_transférer_size* **To** 0 **Do**
If (*donnée_à_transférer*[i] = 1) **Then**
freq_actuelle = *freq_1*
loop for *Tempo_1*
Else
freq_actuelle = *freq_1*
loop for *Tempo_2*
End If
freq_actuelle = *freq_2*
loop for *Tempo_3*
End For
freq_actuelle = *freq_normal*

Processus récepteur



① Transfert de données sensibles du cœur ARM sécurisé vers l'extérieur du SoC



Variation temporelle de l'amplitude de la raie spectrale à Freq_1 = 433MHz

freq_1 = 325MHz, *freq_2* = 433MHz,
Tempo_1 = 400, *Tempo_2* = 200, *Tempo_3* = 200

Débit binaire = 142 kbps

Conclusion 3/3

- Preuve de concept de la mise en œuvre d'un canal de communication caché exploitant le DVFS du SoC
  - Depuis/vers la partie logicielle ou la partie matérielle
  - Vers l'extérieur
  - Différents types de modulation de fréquence sont possibles

- Référence :

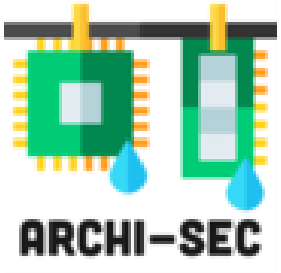
El Mehdi Benhani. Lilian Bossuet, *DVFS as a Security Failure of TrustZone-enabled Heterogeneous SoC*. In Proceedings of 25th IEEE International Conference on Electronics Circuits and Systems , ICECS 2018, Bordeaux, December 2018.

Conclusion

Conclusion

- Une technologie comme TrustZone ne garantie pas l'extension de la TEE au-delà du processeur
  - Cependant cette extension est nécessaire
  - Proposer des contre-mesures
    - Architecture sécurisée
    - Outils de confiance
    - Barrières d'isolation physiques et cryptographiques
  - Valider les protections avec une plateforme de simulation Gem5
  - Explorer les attaques physiques internes

Sponsors & collaborations



LABORATOIRE HUBERT CURIEN
UMR • CNRS • 5516 • SAINT-ETIENNE

UNIVERSITÉ JEAN MONNET SAINT-ÉTIENNE

cnrs

Extension de la TrustZone et de la TEE :

Secure or not secure?

Lilian Bossuet
Laboratoire Hubert Curien