

Evaluation de la sécurité de la technologie ARM TrustZone

Lilian Bossuet

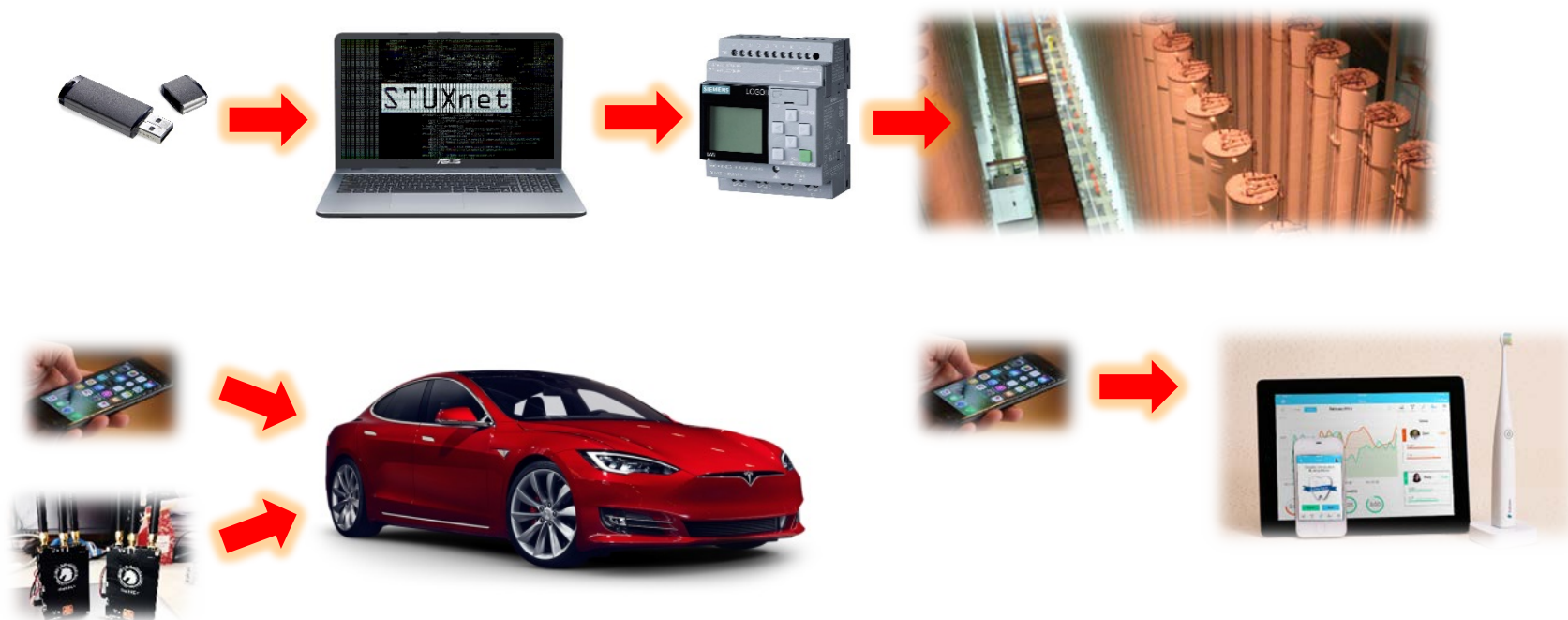
Laboratoire Hubert Curien, CNRS UMR 5516
Université Jean Monnet, Saint-Etienne, France



25 janvier 2018
Saint-Malo, France

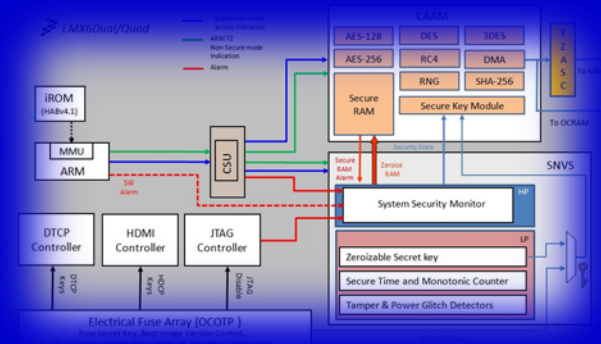
Le slide qui fait peur !!! (*tiré d'histoires vraies*)

- De multiples attaques sur les systèmes embarqués connectés



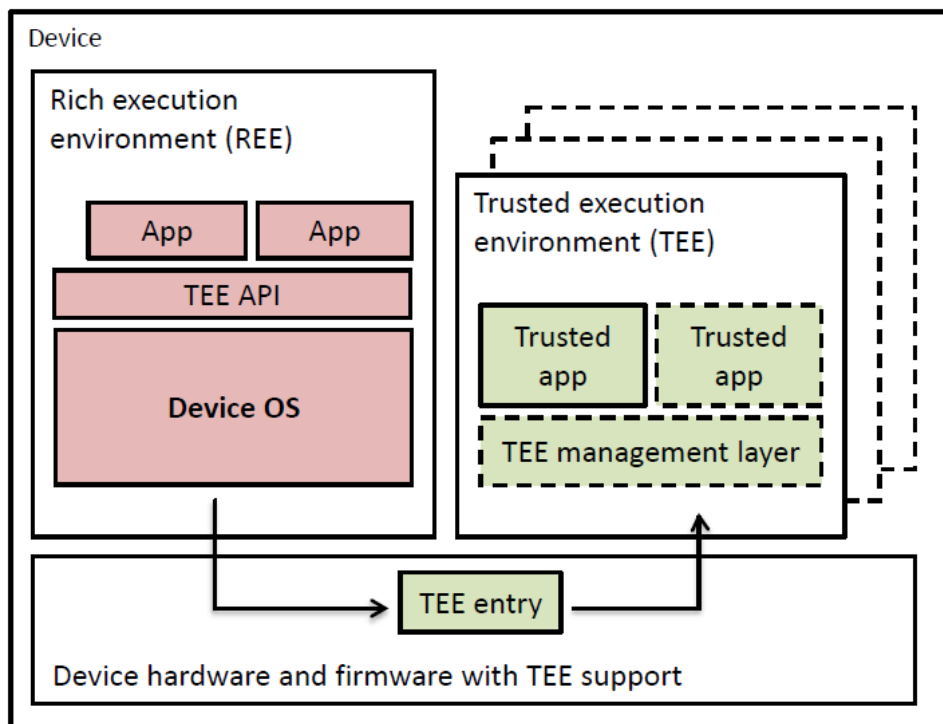
Sécurité des systèmes programmables

Trusted Execution Environment – TEE



Architecture TEE

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



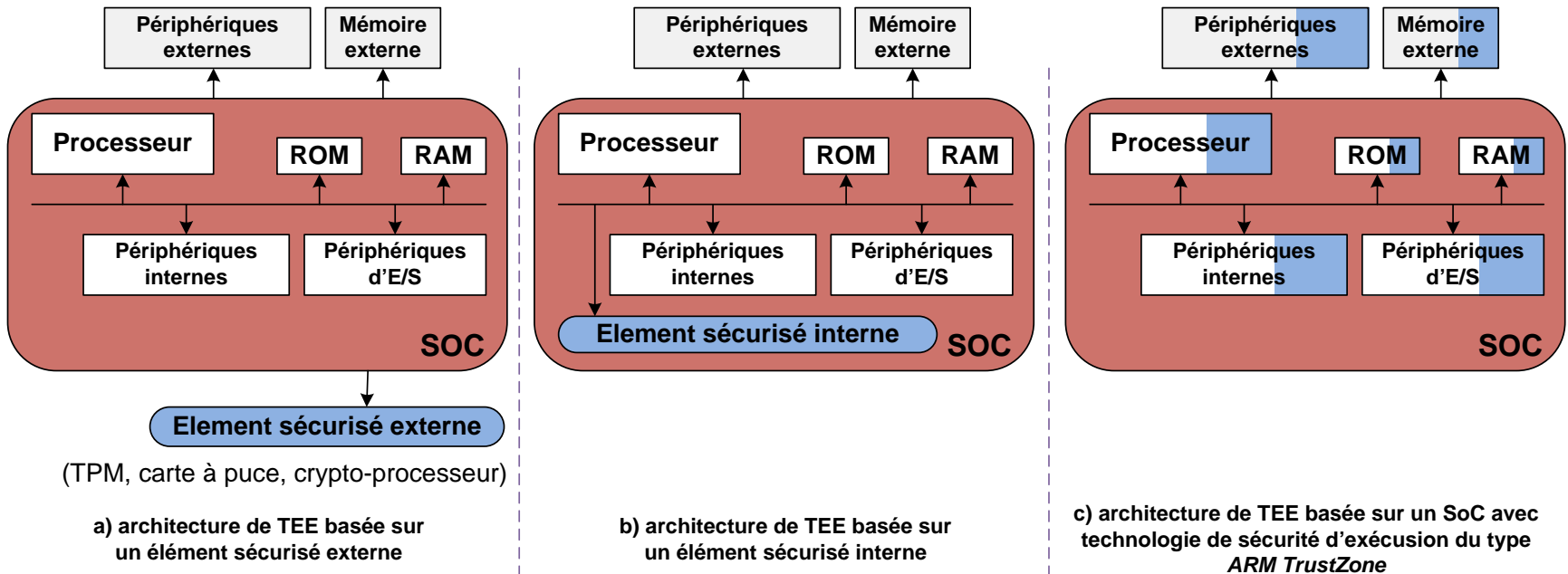
Architectures with single TEE

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

Architectures with multiple TEEs

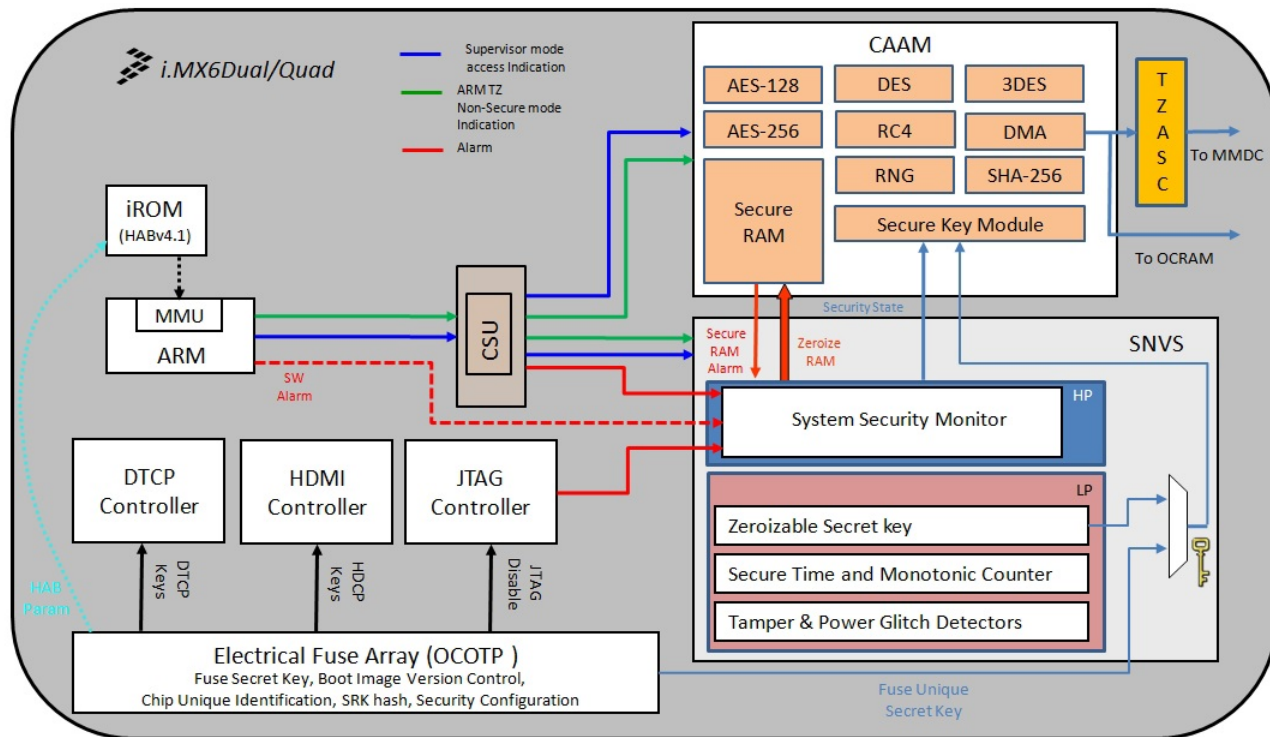
- Intel SGX
- TPM (and “Late Launch”)
- Hypervisor

Composants de la TEE



Architecture matérielle de sécurité ARM Cortex A9

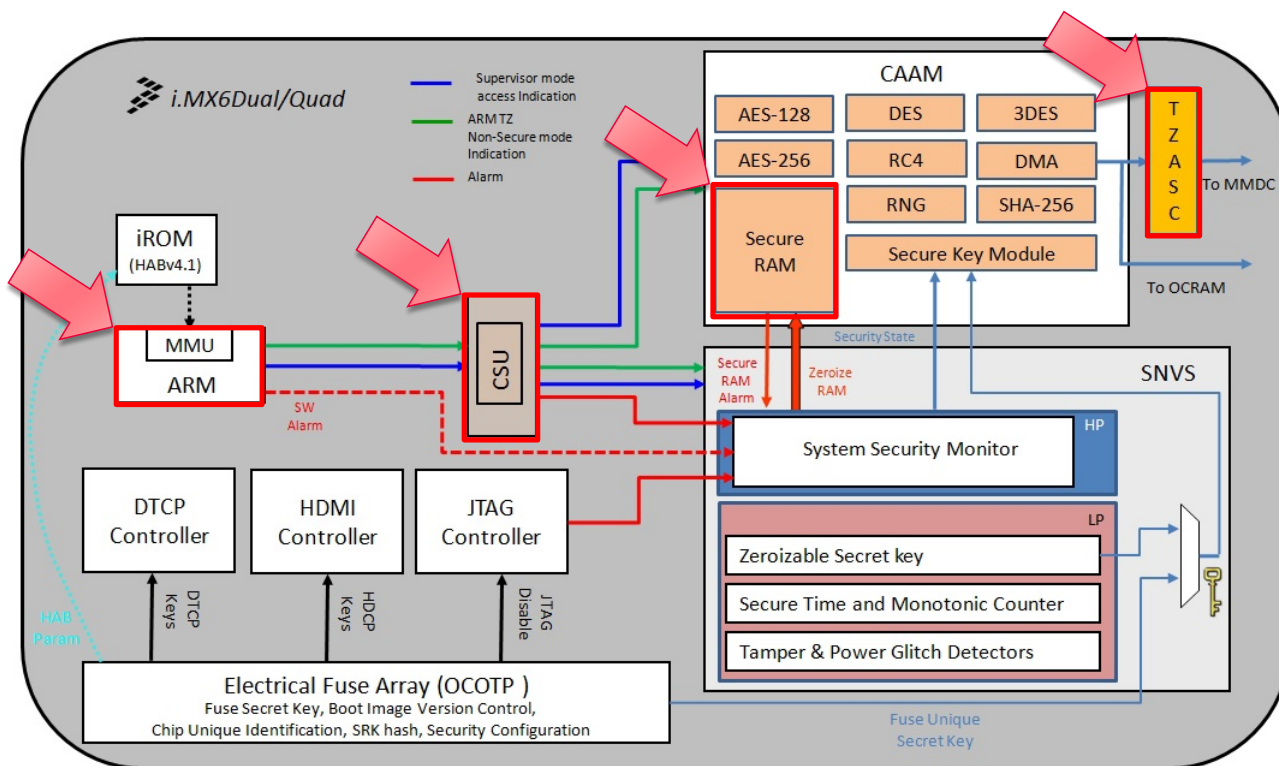
◆ Exemple du Freescale i.MX6



Architecture matérielle de sécurité ARM Cortex A9

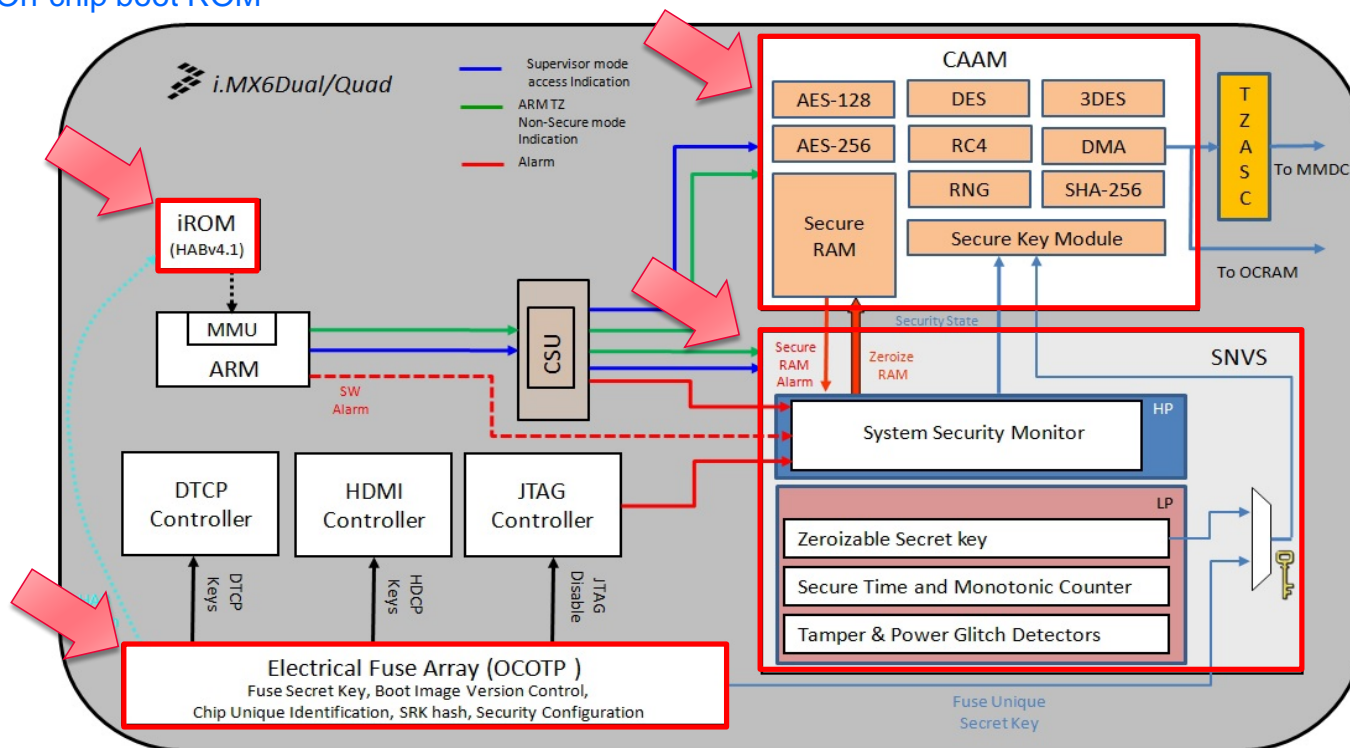
TrustZone

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

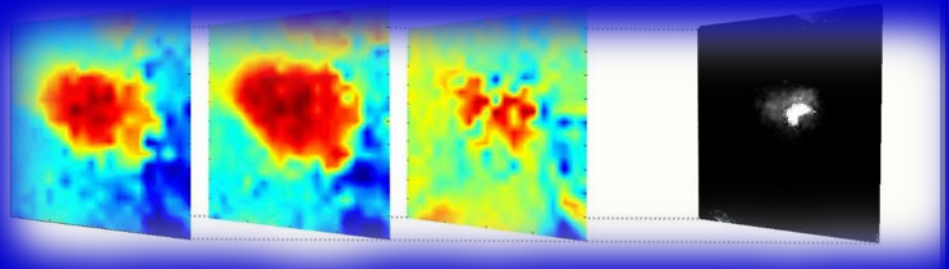


Architecture matérielle de sécurité ARM Cortex A9

- ◆ Cryptographic Acceleration and Assurance Module (CAAM)
- ◆ Secure Non-Volatile Storage (SNVS)
- ◆ System JTAG Controller with secure debug
- ◆ On-chip One-time Programmable (OCOTP)
- ◆ A On-chip boot ROM



Sécurité de l'accélérateur cryptographique (CAAM) de la TrustZone



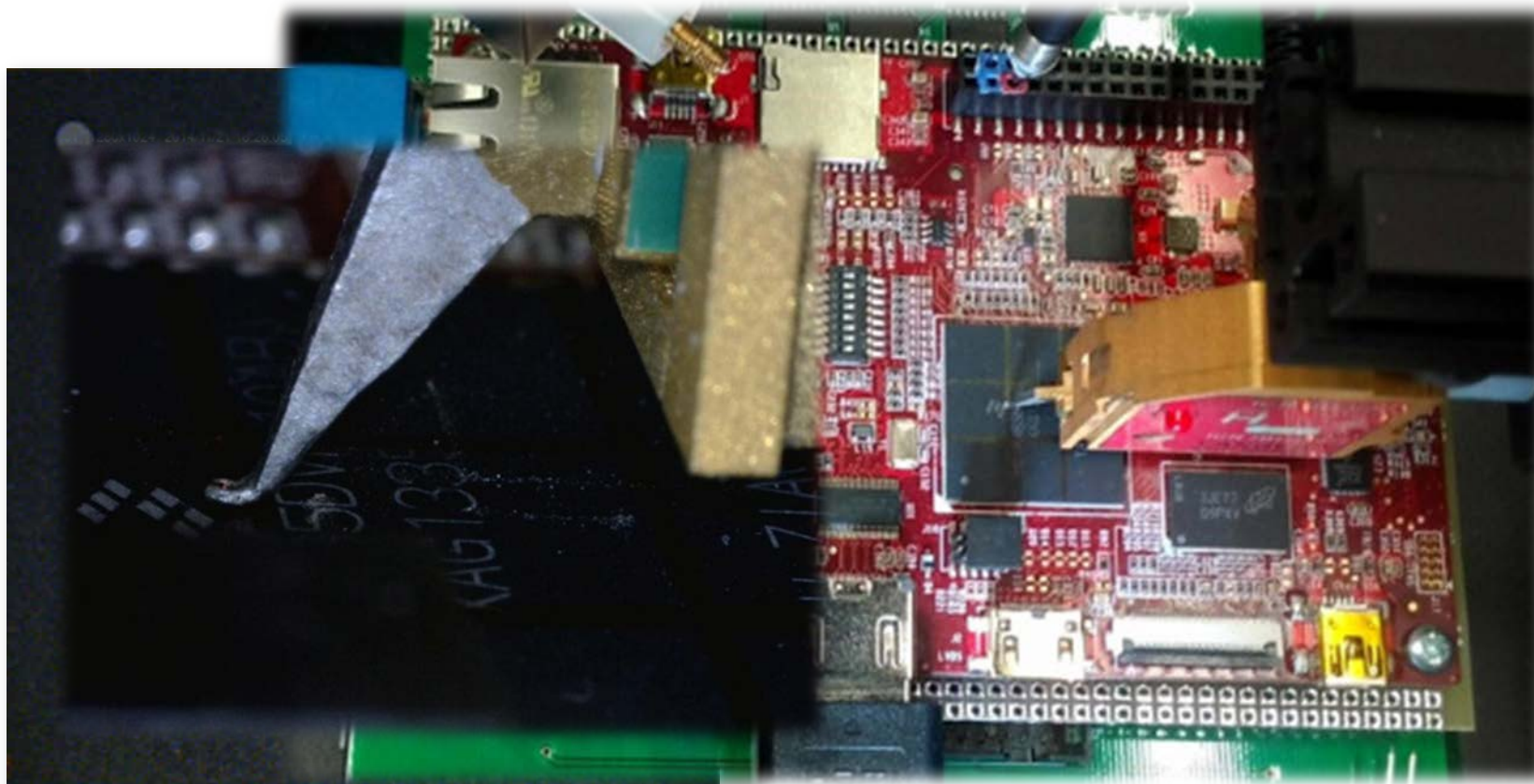
Attaques classiques combinées – étape 1

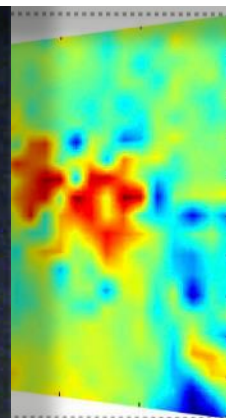
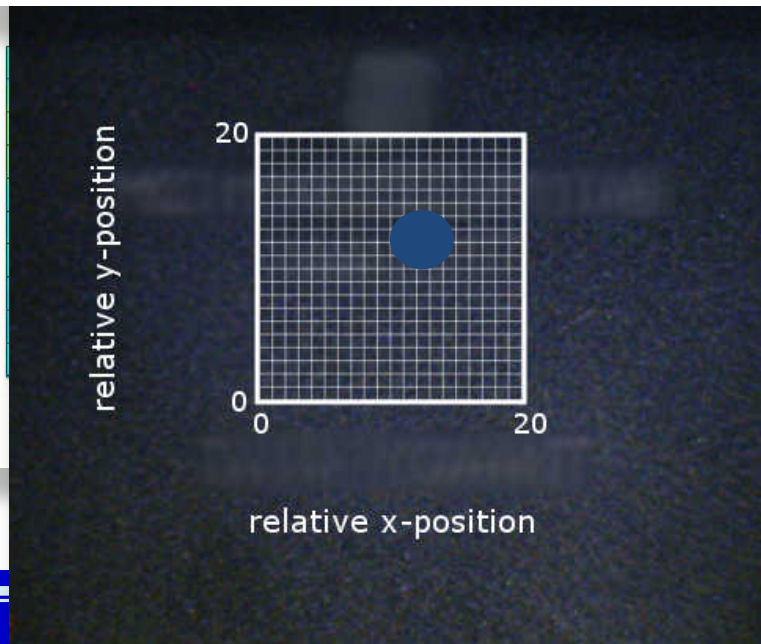
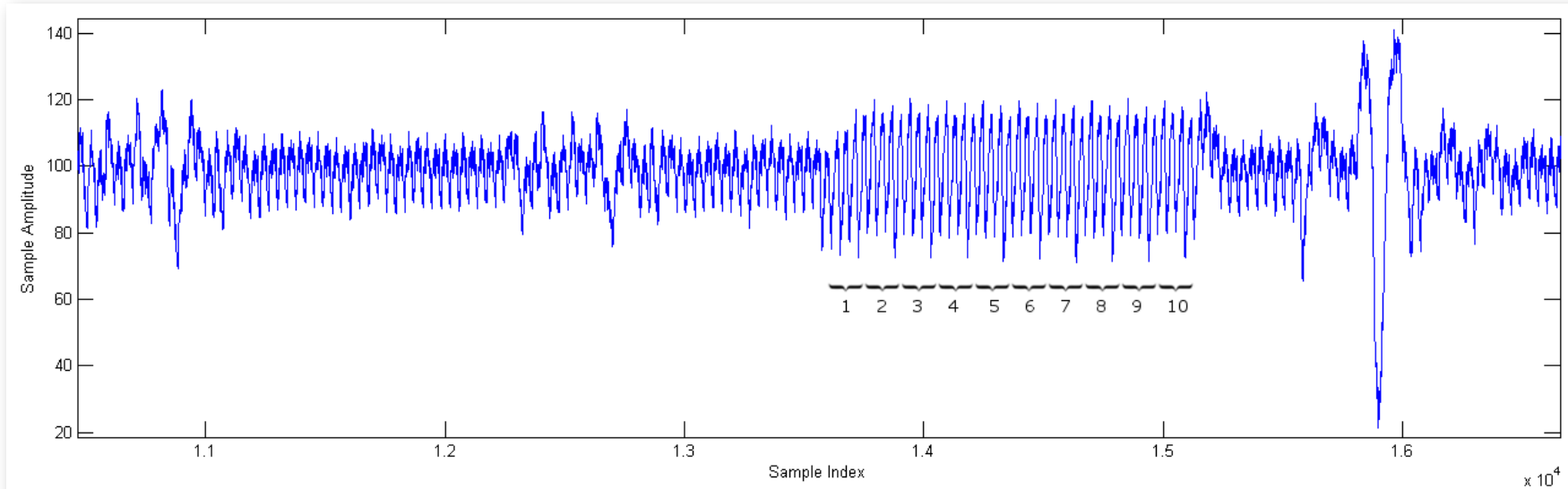
- Analyse du rayonnement EM du chiffreur AES masqué
- Cartographies EM avec trois ensemble de données

Set 1	HW(clé) : 0	HW(message) : 0	HW(chiffré) : 65
	128	0	64
Set 2	HW(message) : 0	HW(chiffré) : 65	HW(clé) : 0
	128	68	0
Set 3	HW(chiffré) : 0	HW(clé) : 0	HW(message) : 65
	128	128	65

- **Objectif : localisation géographique et temporelle du CAAM dans le SoC**

Cartographie EM





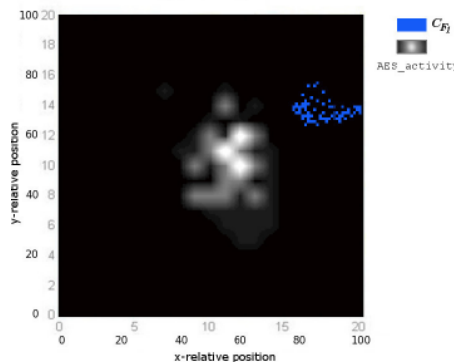
chiffré



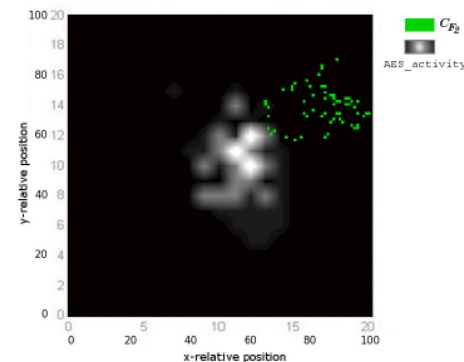
AES

Attaques classiques combinées – étape 2

- Injection d'impulsions EM
 - ◆ pendant le chiffrement
 - ◆ pendant transfert de données

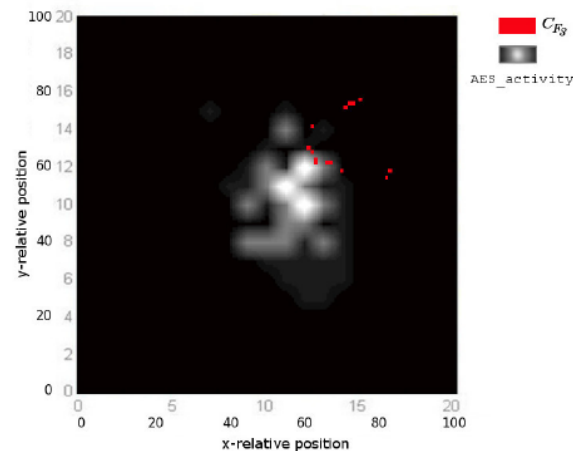


(a) buffer copy faults



(b) bad transfer of cipher

	52	4F	F4	9C	C3	C5	AE	60	B8	A9	81	56	B1	46
CF1 (54%)	52	4F	F4	9C	52	4F	F4	9C	B8	A9	81	56	B1	46
	52	4F	F4	9C	C3	C5	AE	60	B1	46	9E	13	B1	46
...														
CF2 (32%)	CC	CC	CC	CC	50	00	CC	CC	B8	A9	81	56	B1	46
	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC
...														
CF3 (14%)	CA	4F	F4	9C	C3	C5	AE	2A	B8	A9	1D	56	B1	1A
	38	EB	9C	91	56	F6	08	C9	6D	AE	E0	F5	E2	8F
...														



(c) Faults related to the AES process

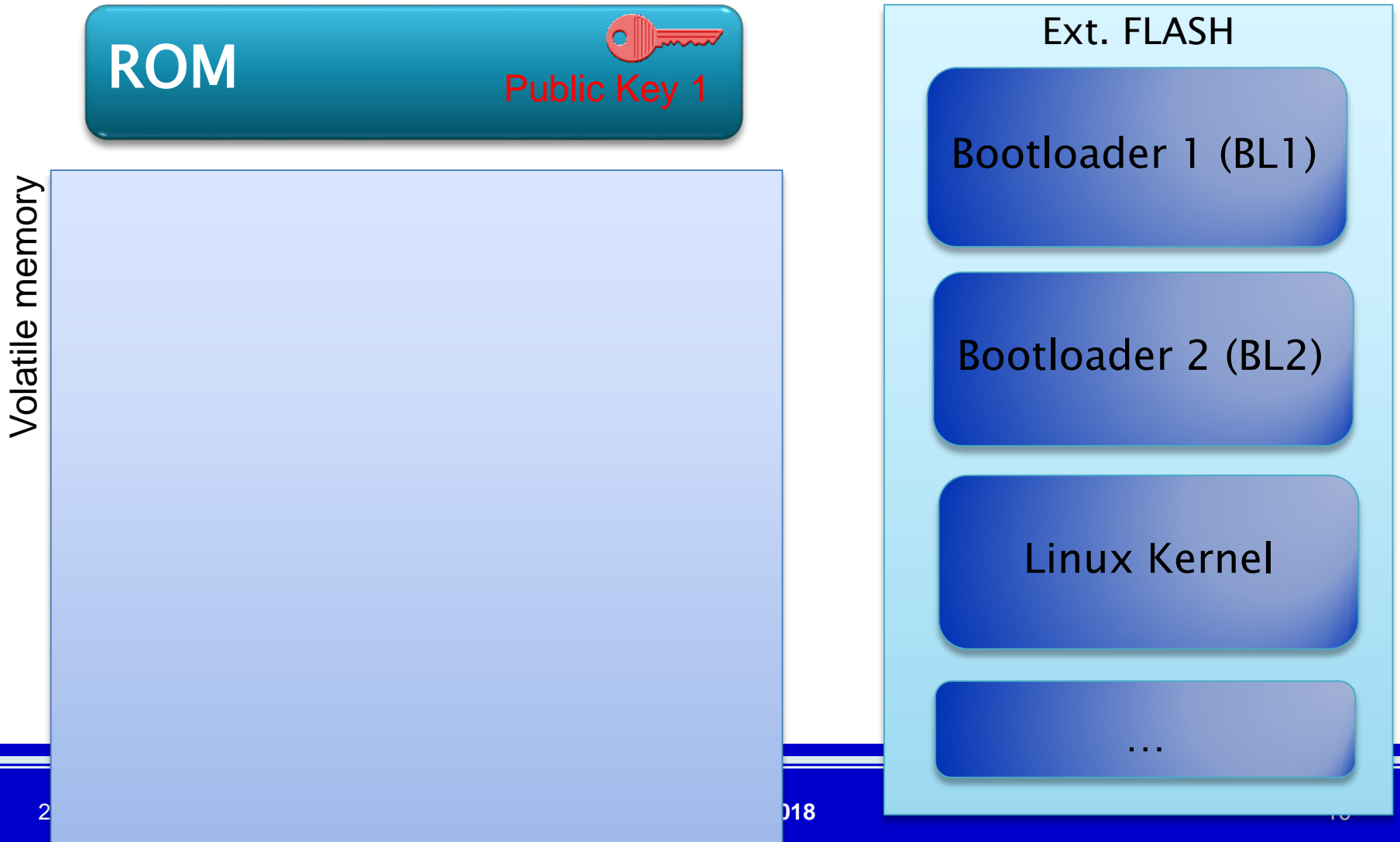
Conclusion 1/3

- L'accélérateur cryptographique de la TrustZone est sécurisé contre les attaques par canaux cachés, il existe des possibilités d'attaques en fautes.
 - ◆ Pas de protection particulière si l'on exécute un algorithme cryptographique dans le processeur généraliste même dans le monde sécurisé...
- Publication
 - ◆ F. Majéric, E. Bourbabo, L. Bossuet. *Electromagnetic security for SoC*. In Proceedings of the 23rd IEEE International Conference on Electronics Circuits and Systems, ICECS 2016, Monte Carlo, Monaco, December 2016.

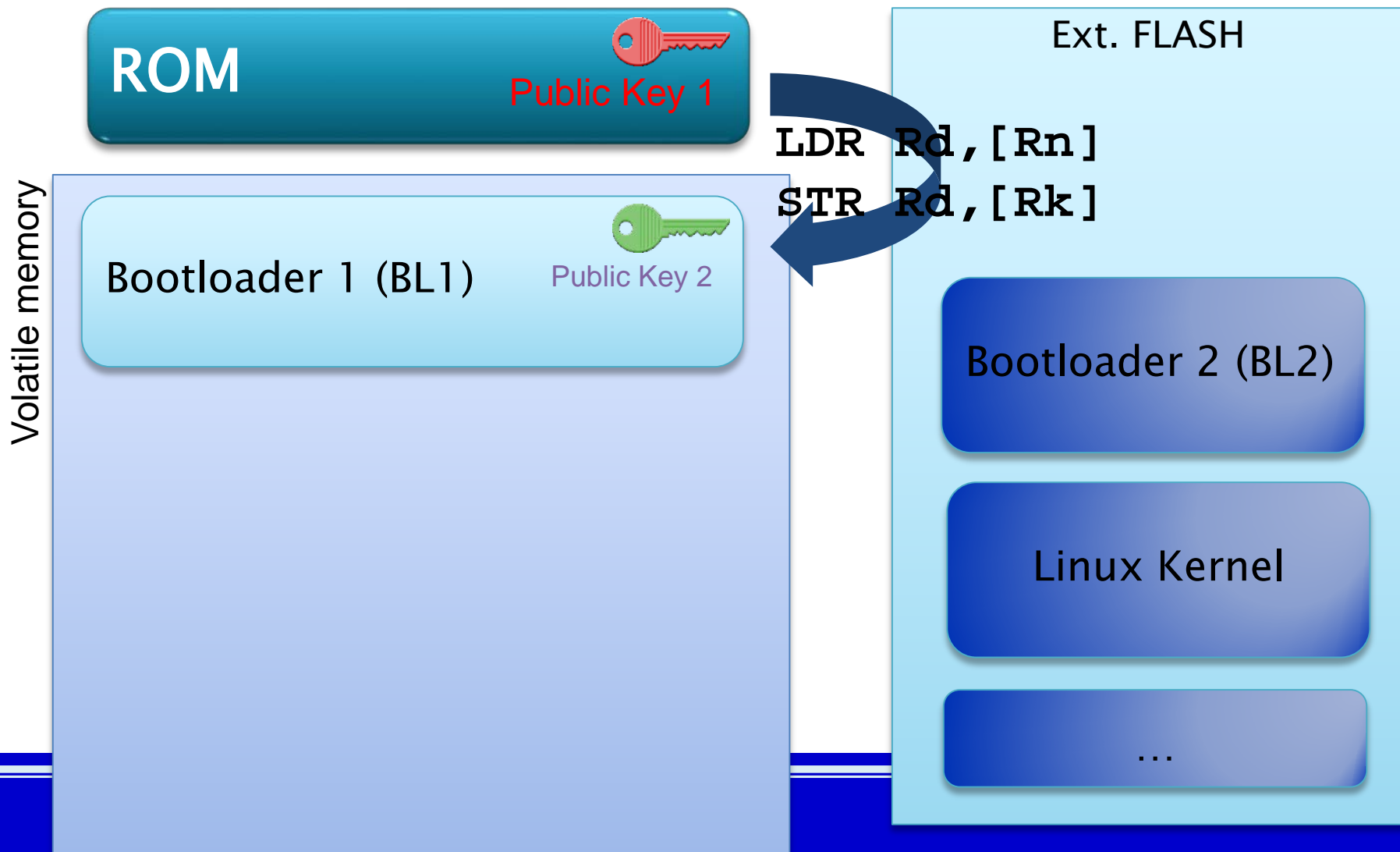
Sécurité du sécuire boot de la TrustZone



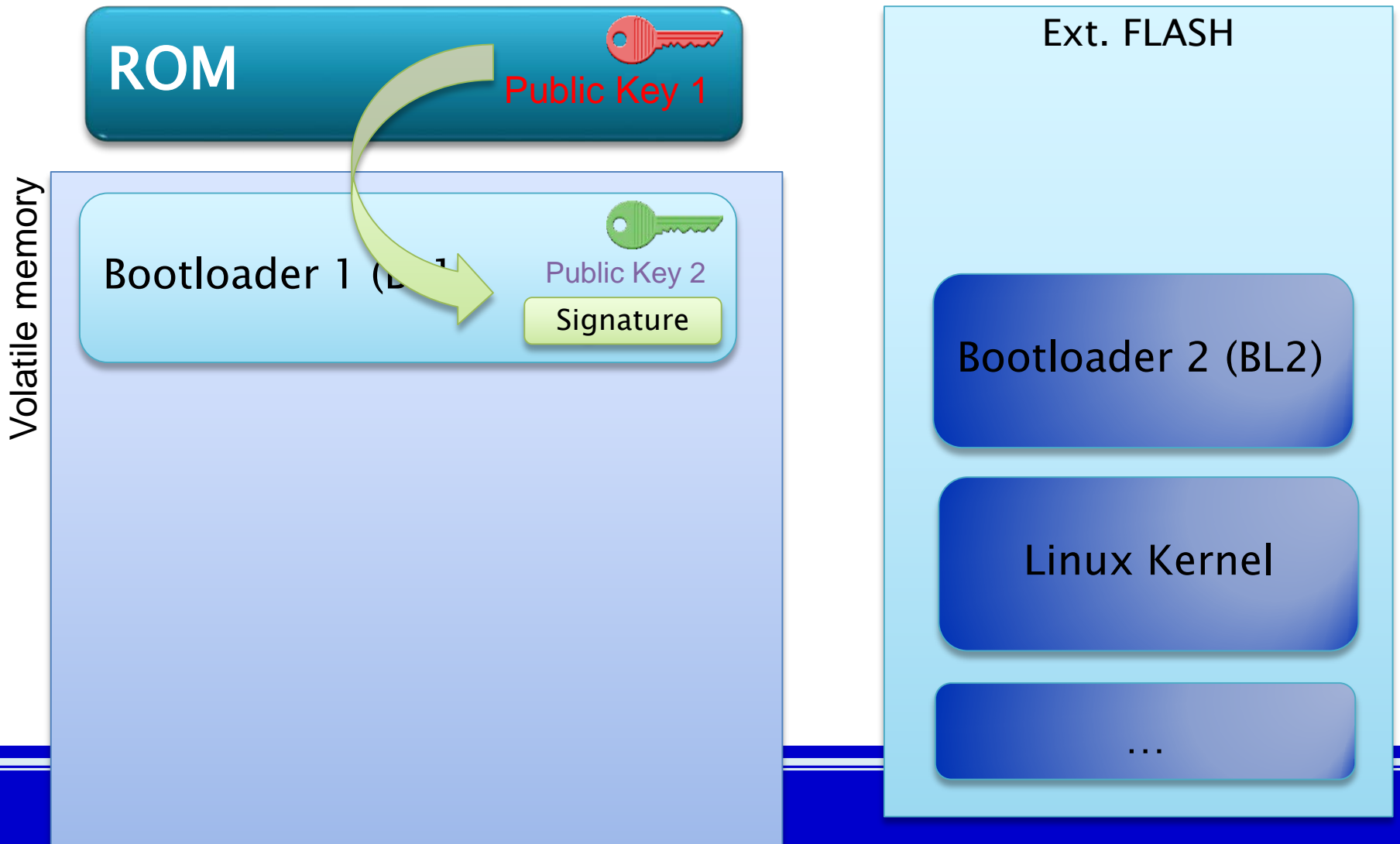
Secure Boot normal



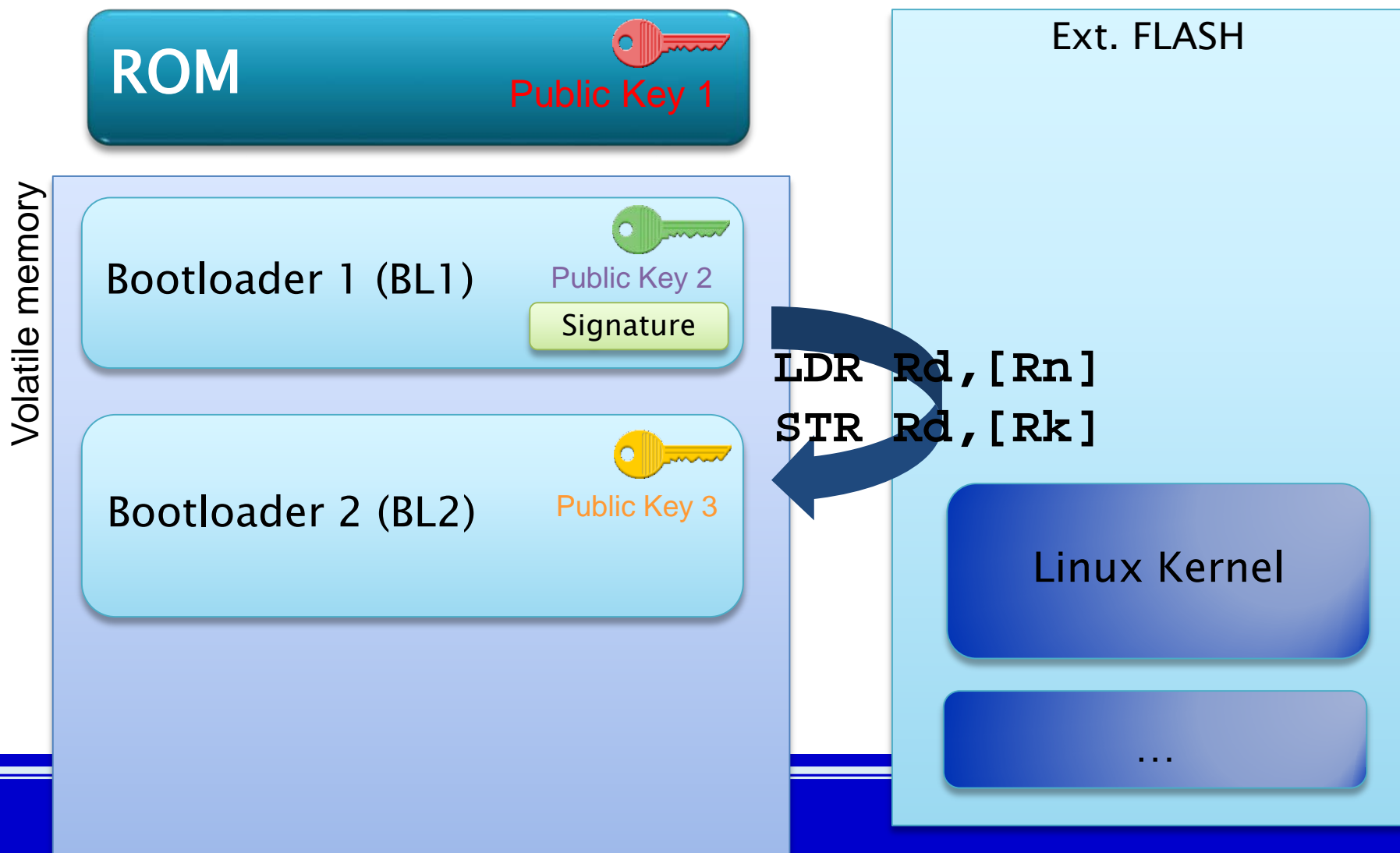
Secure Boot normal



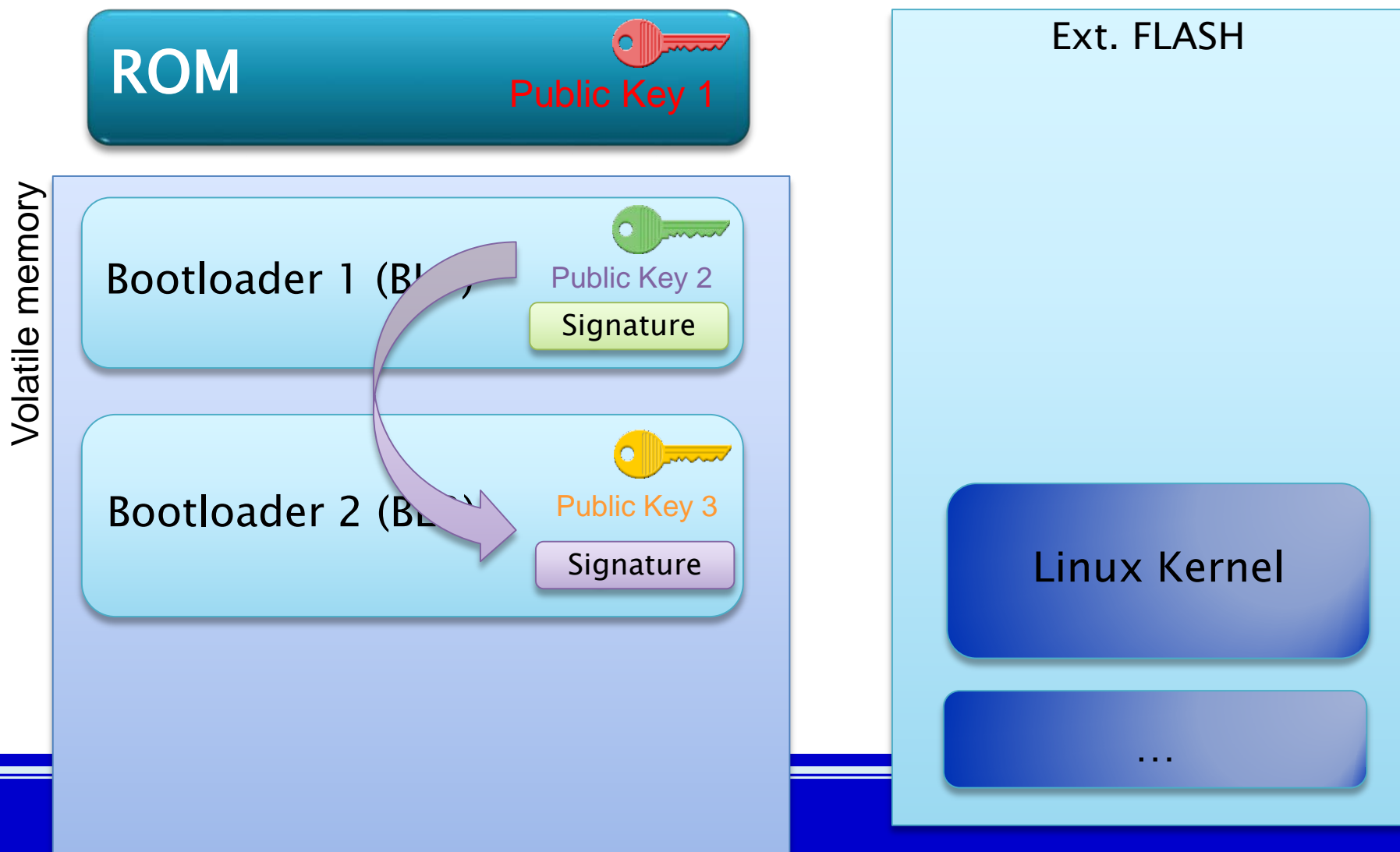
Secure Boot normal



Secure Boot normal



Secure Boot normal



Secure Boot normal

Volatile memory

ROM



Public Key 1

Bootloader 1 (BL1)



Public Key 2

Signature

Bootloader 2 (BL2)



Public Key 3

Signature

Ext. FLASH

Linux Kernel

...

Secure Boot normal

Volatile memory

ROM



Public Key 1

Bootloader 1 (BL1)



Public Key 2

Signature

Bootloader 2 (BL2)



Public Key 3

Signature

Linux Kernel



Public Key 4

Signature

Ext. FLASH

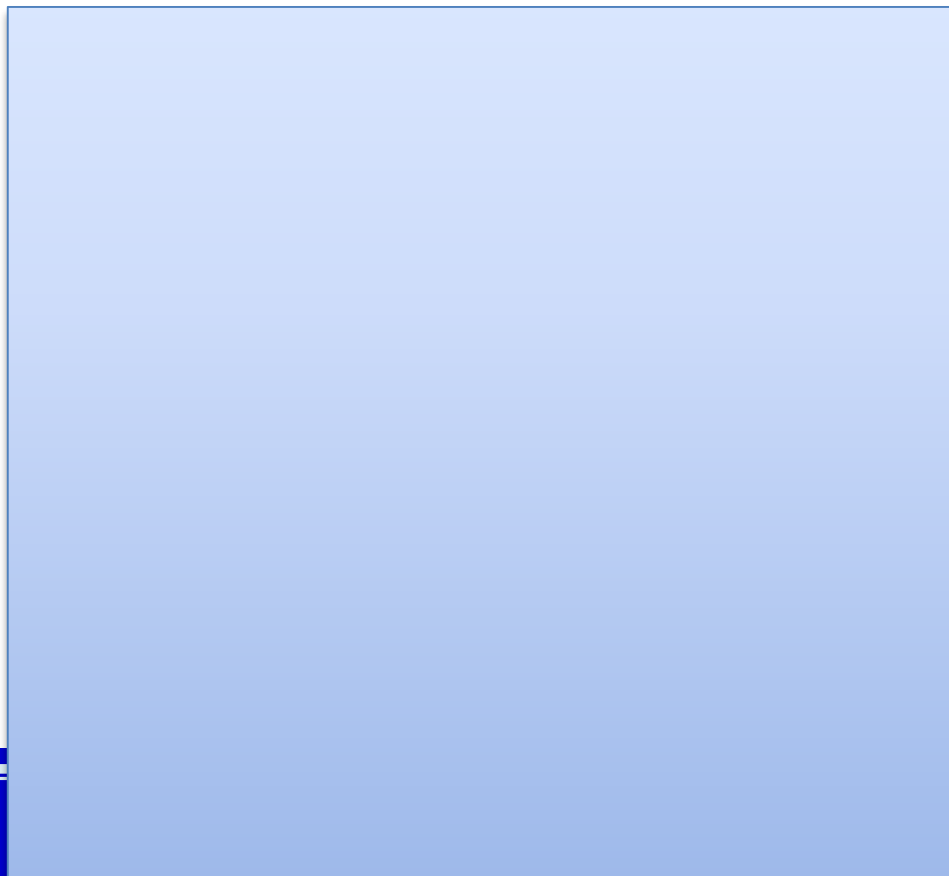
Attaque RISCURE

ROM



Public Key 1

Volatile memory



Ext. FLASH

Bootloader 1 (BL1)

Bootloader 2 (BL2)

Linux Kernel

...

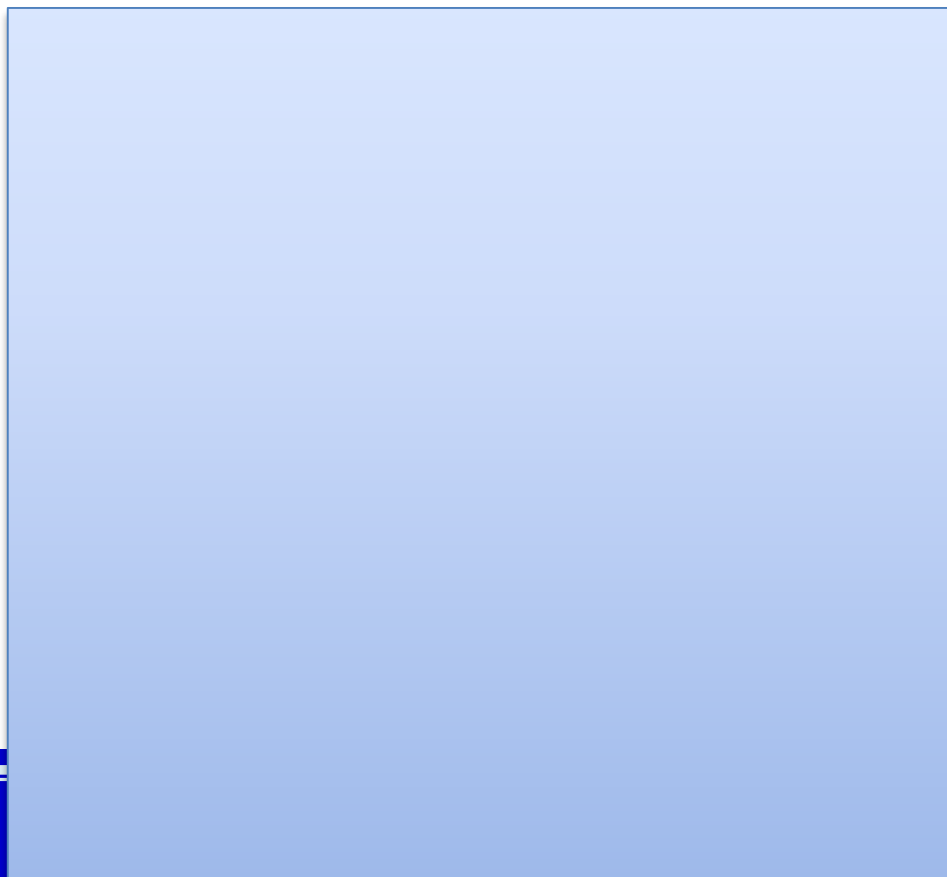
Attaque RISCURE

ROM



Public Key 1

Volatile memory



Ext. FLASH

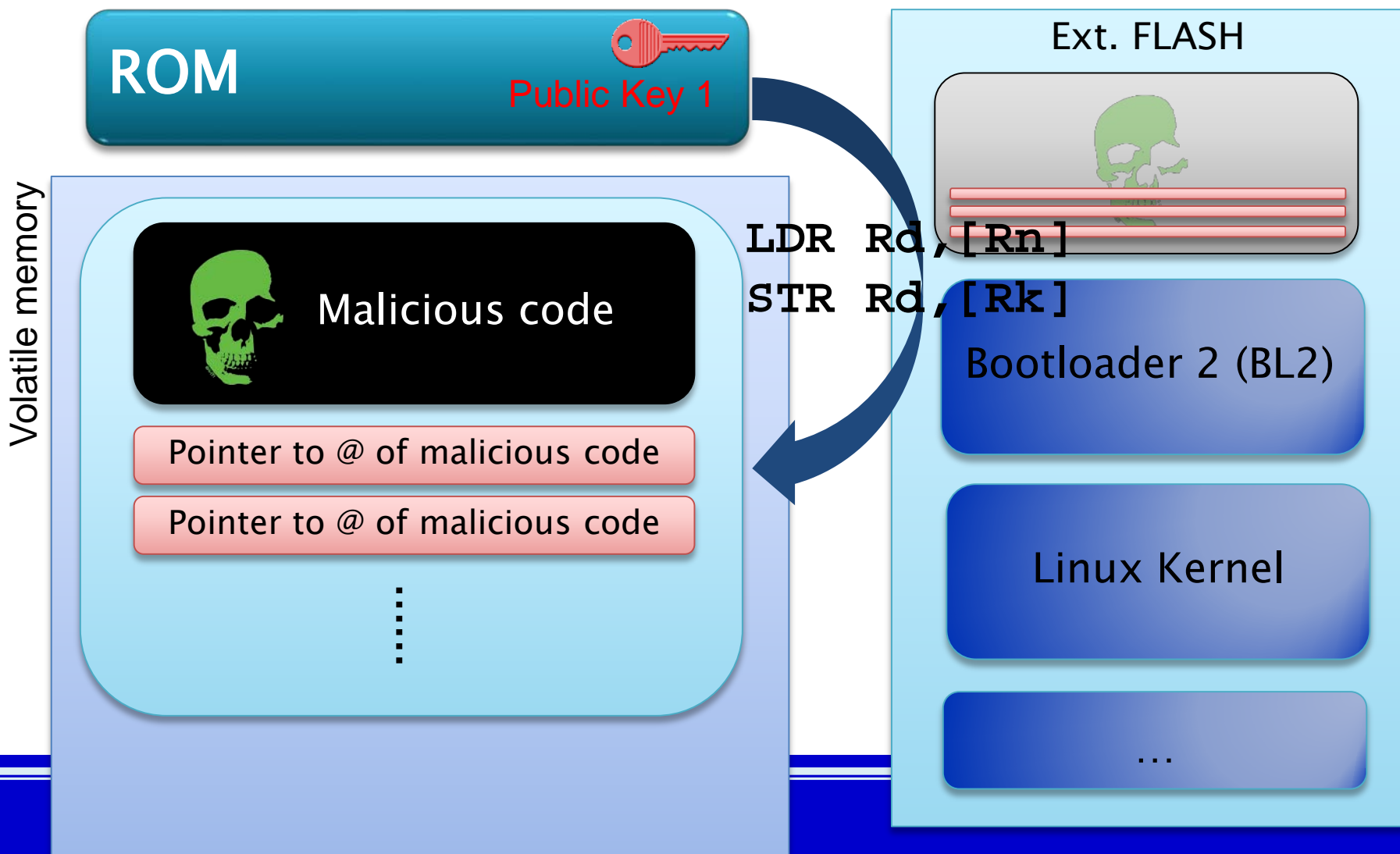


Bootloader 2 (BL2)

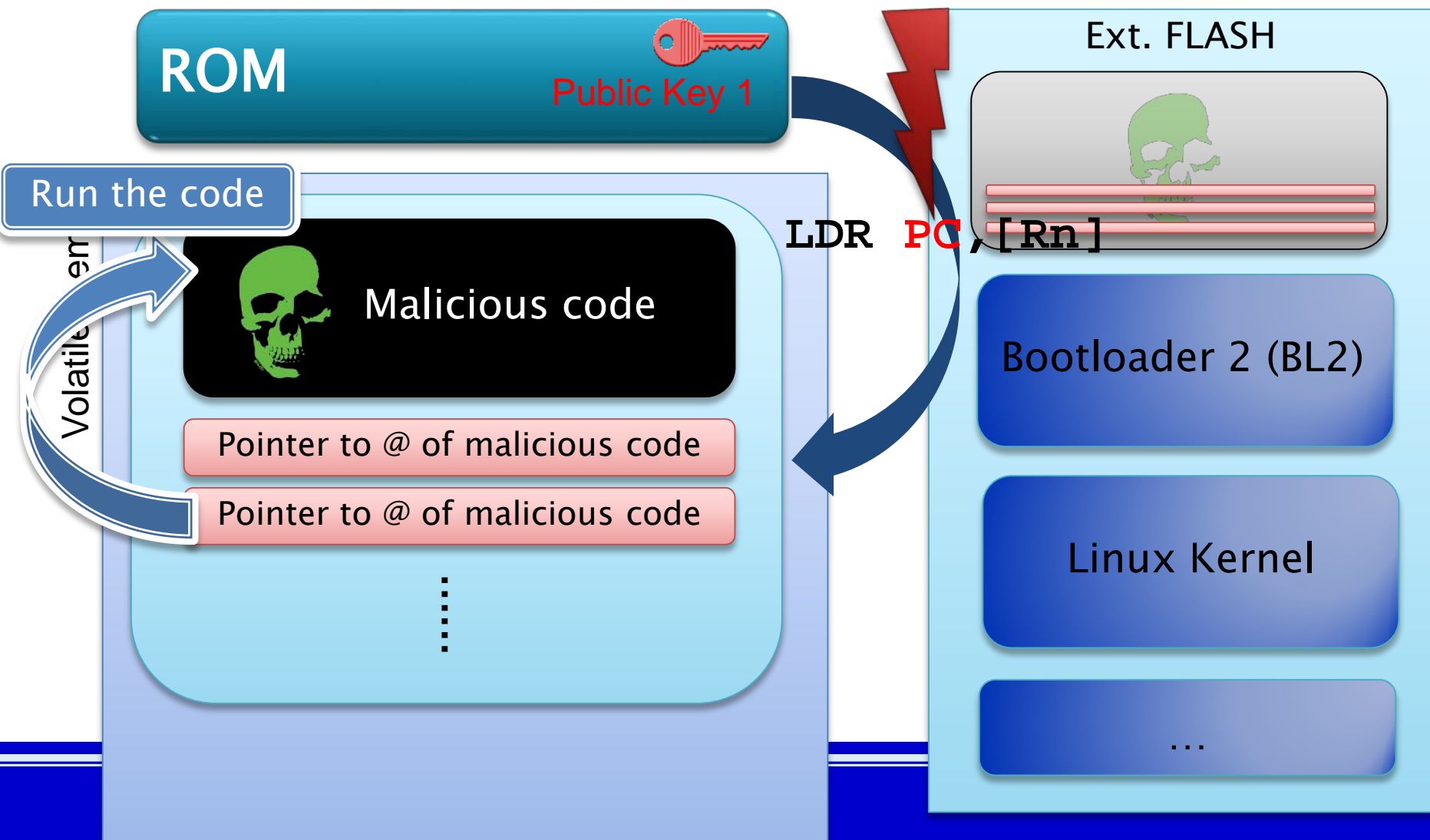
Linux Kernel

...

Attaque RISCURE

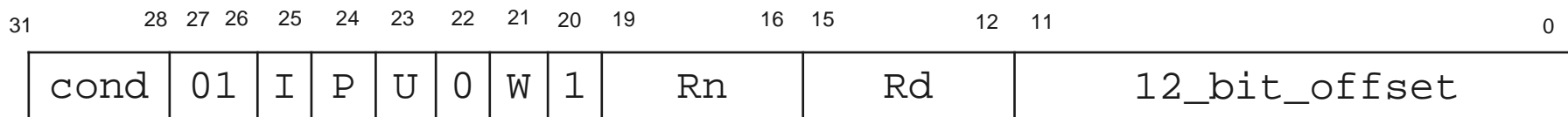


Attaque RISCURE

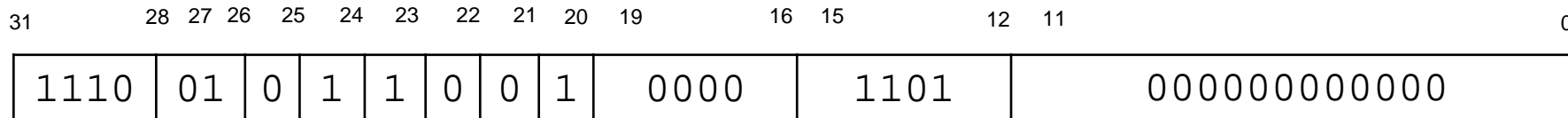


Attaque de RISCURE

- Comment est-ce possible ?
- *LDR processing instruction*
 - ◆ `LDR{<cond>} Rd, [Rn {,#+/-12_bit_offset }]`

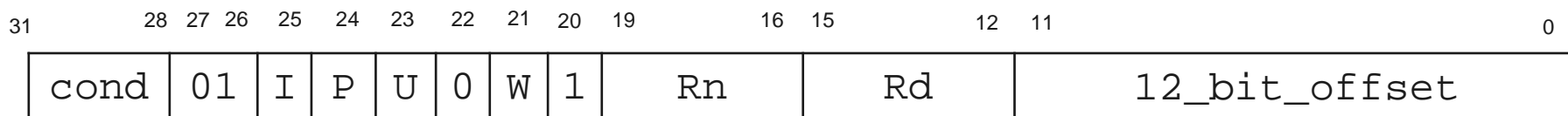


- ◆ `LDR R13, [R0]` (`[R0]` point to the address of the malicious code)

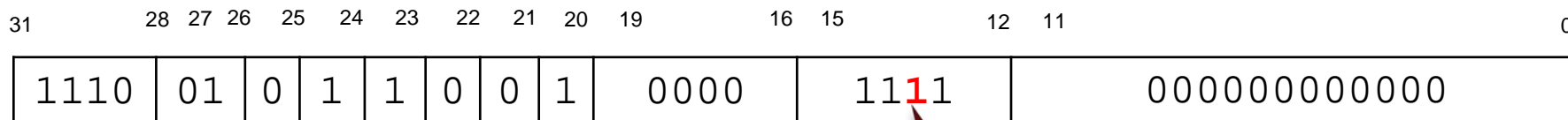


Attaque de RISCURE

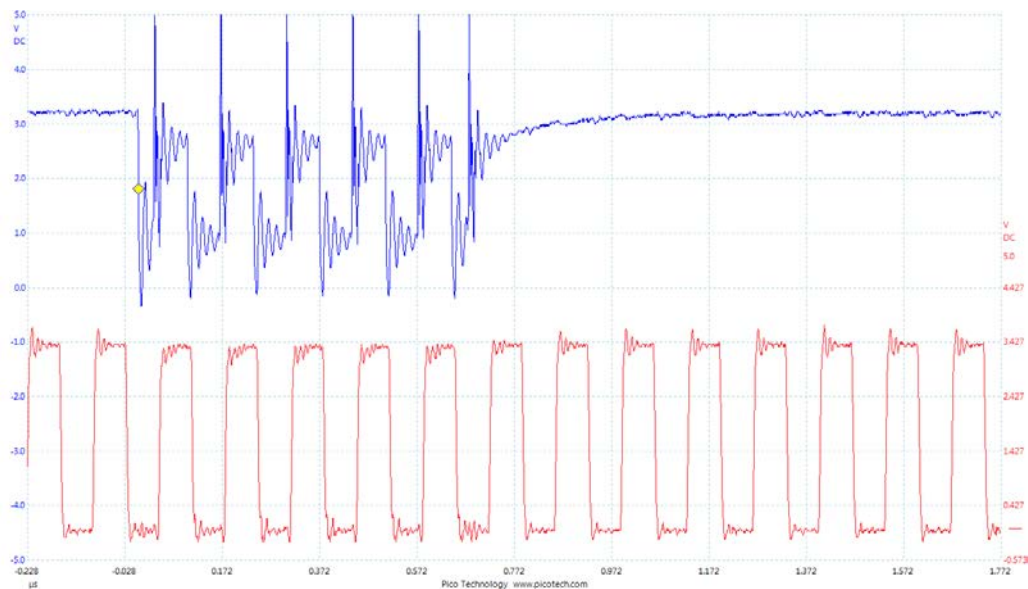
- Comment est-ce possible ?
- *LDR processing instruction*
 - ♦ $LDR\{<cond>\} Rd, [Rn \{, \#+/-12_bit_offset \}]$



- ♦ LDR **PC** , [R0] ([R0] point to the address of the malicious code)



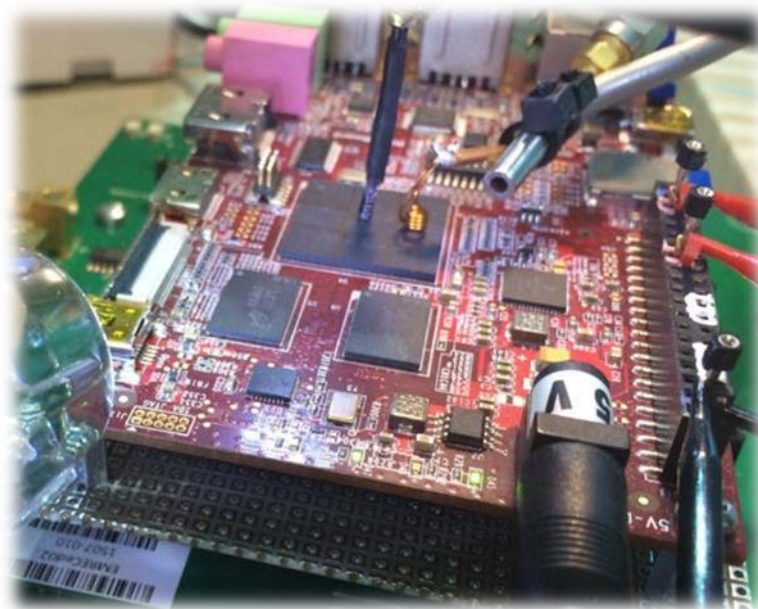
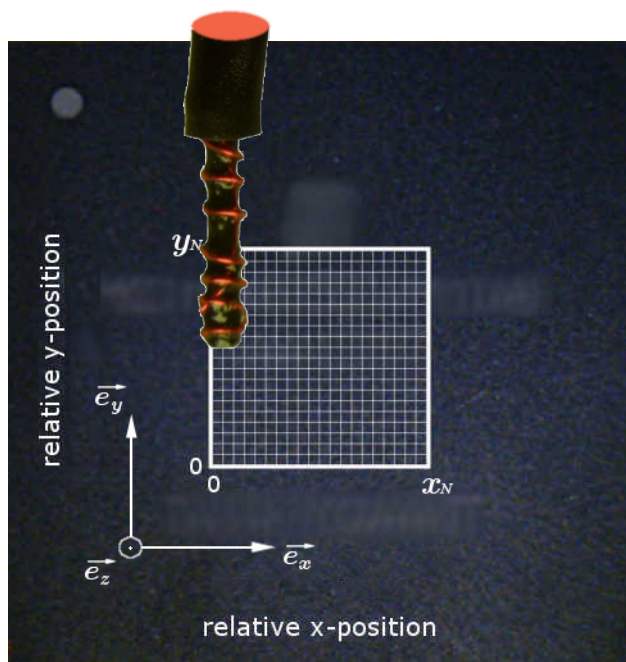
Injection de fautes par *glitch* de tension



N. Timmers, A. Spruyt and M. Witteman, *Controlling PC on ARM using fault injection*, in Workshop on Fault Diagnosis and Tolerance in Cryptography, (FDTC 2016), Santa Barbara, CA, US, August 16, 2016.

Injection de fautes EM (GEMALTO – Lab. H. Curien)

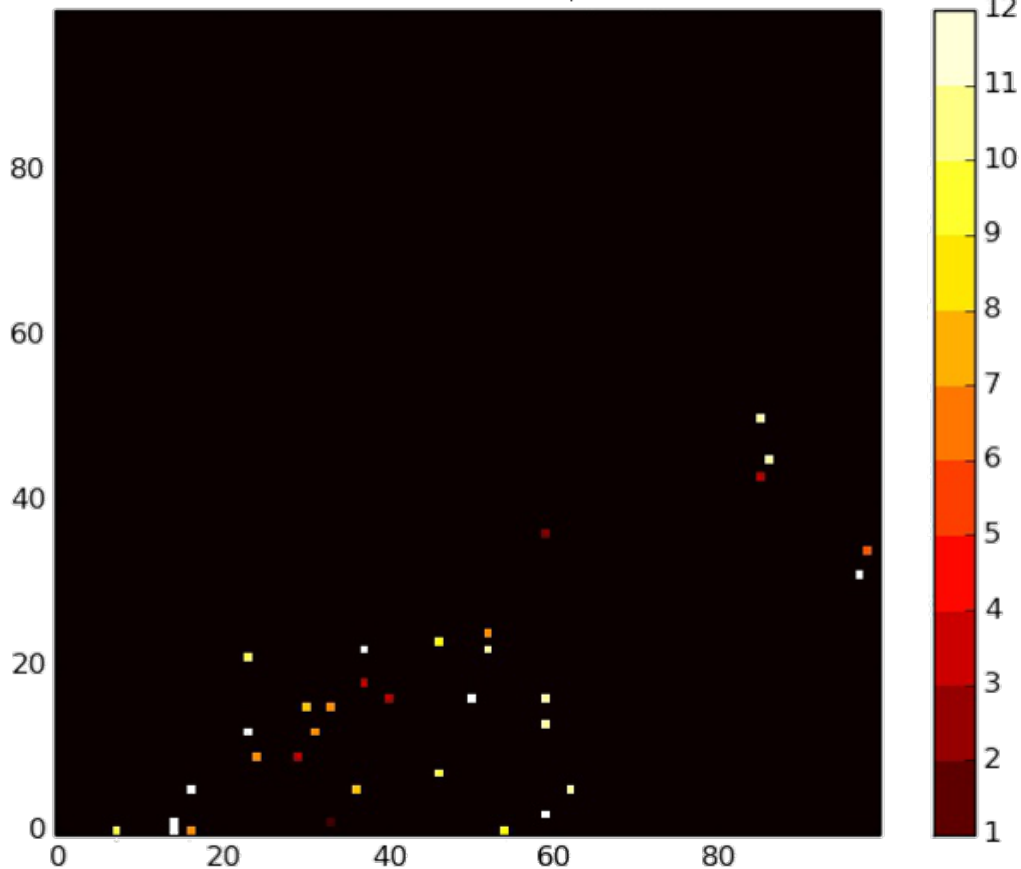
- Injection durant l'exécution de LDR Rd, [R0]
 - ◆ Vérifier si LDR Rd, [R0] => LDR PC, [R0]



Résultats expérimentaux

- Rd changed into PC:

Faults on LDR Rd, [R0]

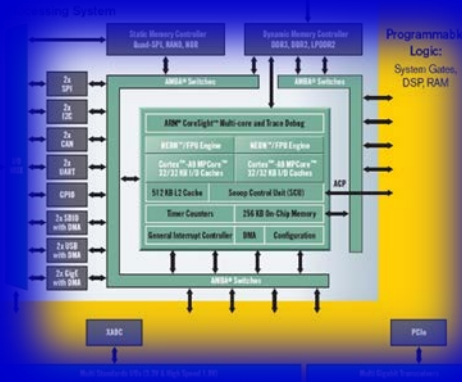


Rd	occurrence
R12	8
R11	6
R10	3
R9	2
R8	2
R7	5
R6	1
R5	0
R4	0
R3	4
R2	1
R1	1

Conclusion 2/3

- La sécurité de la séquence de chargement du boot est assurée par un protocole cryptographique
- Faille de sécurité matérielle due à une trop faible distance de Hamming entre les registres généraux et registres spéciaux du processeur

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



Cibles Intel SoC FPGA et Xilinx Zynq

■ INTEL SoC

Architecture Brief

Shared Memory Protection in Altera SoCs

Introduction

Memory protection is often associated with more advanced processors. The feature prevents errant or illegal processor transactions from reading or corrupting other memory regions. To protect shared resources in SoC FPGAs, Altera extends memory protection to elements in the FPGA that generate memory traffic. This Architecture Brief outlines the protection of shared memory systems and the benefits of incorporating ARM TrustZone® protection technology.

Key aspects of this paper are highlighted in an on-line video, "System Reliability: Memory Protection", which can be found at www.altera.com/socharchitecture under the "Reliability and Flexibility" tab.

Memory Protection for Shared Memory

Memory protection is a feature often associated with more advanced processors. Whether it is called a memory management unit (MMU) or memory protection unit (MPU), it prevents errant or illegal processor transactions from reading or corrupting other memory regions. In the Cortex A9 processor, ARM extends this protection concept with TrustZone® technology, which provides a system-wide approach for security-sensitive systems.

Some SoC FPGAs extend memory protection to the FPGA. This is needed as the processor and FPGA can share a single external DDR memory interface in order to save cost, reduce board space, or save power. What if the custom FPGA logic accidentally overwrites a section of memory belonging to the processor's data application code, or operating system (OS) kernel? This may cause a system crash or worse the processor in sensitive systems.

To prevent this from happening, specific memory regions may be dedicated to an OS or embedded software applications while other memory regions may be dedicated to FPGA-based functions, as shown in Figure 1 (below). Via memory protection, the FPGA-based functions are prevented from corrupting the OS or embedded software regions.

Figure 1: Example DDR Memory Protection Where Processors and FPGA Share a Common Memory

ARM
Dual
M
Hard Mem
Control

■ XILINX Zynq-A9

XILINX
WP429 (v1.0) May 20, 2014

White Paper: Zynq-7000 All Programmable SoCs

TrustZone Technology Support in Zynq-7000 All Programmable SoCs

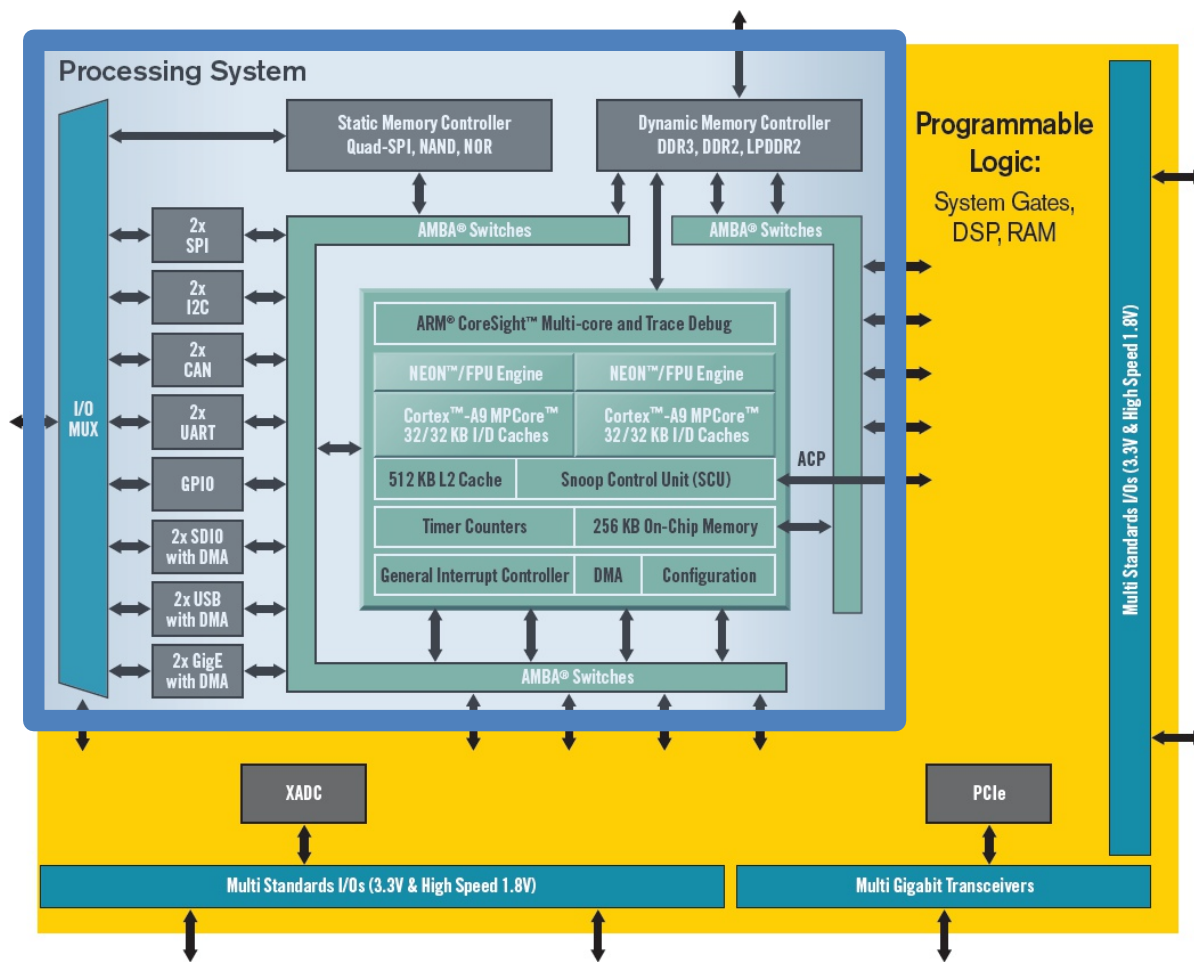
By: Yasha Gosain and Prashoohan Pelanichamy

Embedded systems are becoming more and more vulnerable to unauthorized penetration, in many cases due to preventable weaknesses within the system kernel itself — often a simple lack of appropriate security features and protections that could have been designed in to safeguard the integrity of important data and processes. This dangerous situation is compounded by the fact that each device becomes potentially connectable to other devices outside its intended functional space, making use either of open Internet connectivity or other contrived digital transport strategies.

This white paper describes how the ARM® TrustZone® architecture and technology can be applied to protect custom IP created in Xilinx® Zynq®-7000 All Programmable SoCs.

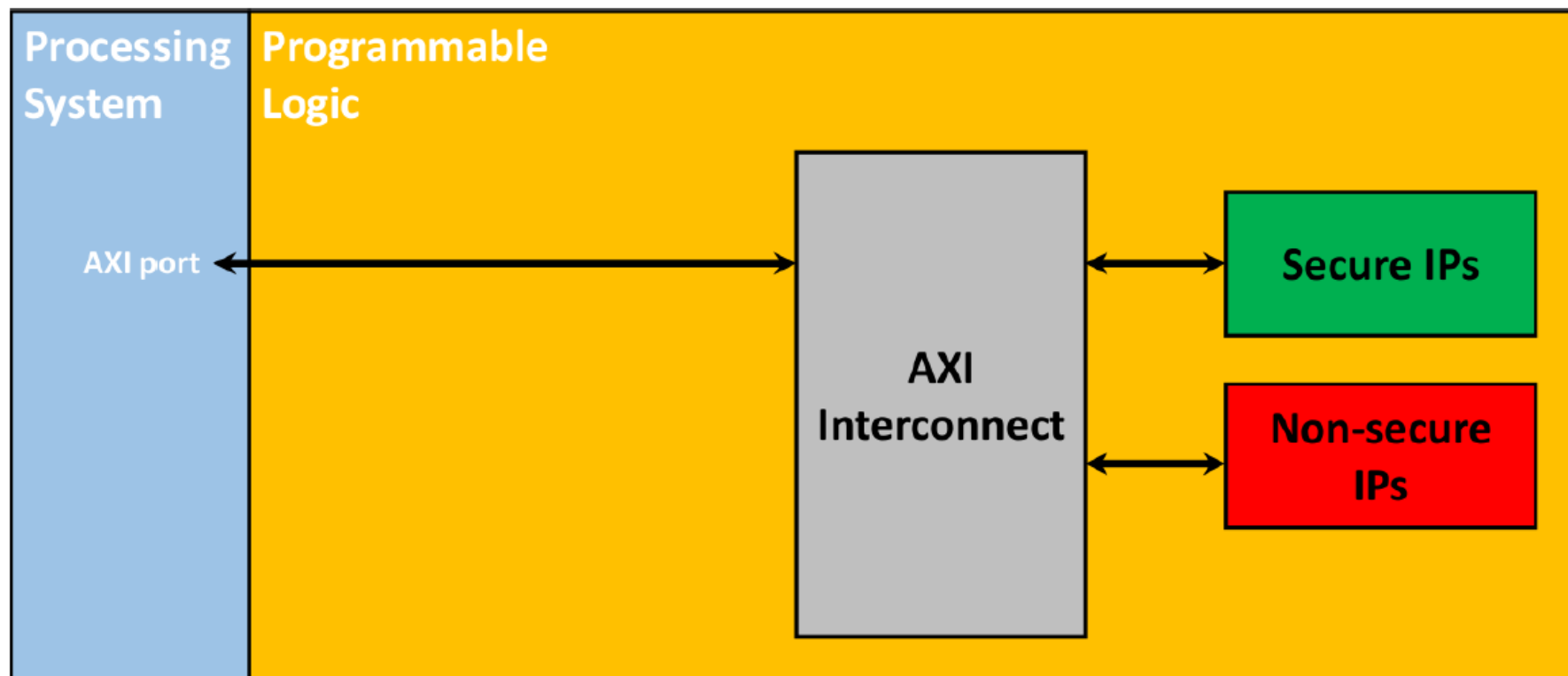
www.xilinx.com

Architecture interne d'un SoC hétérogène



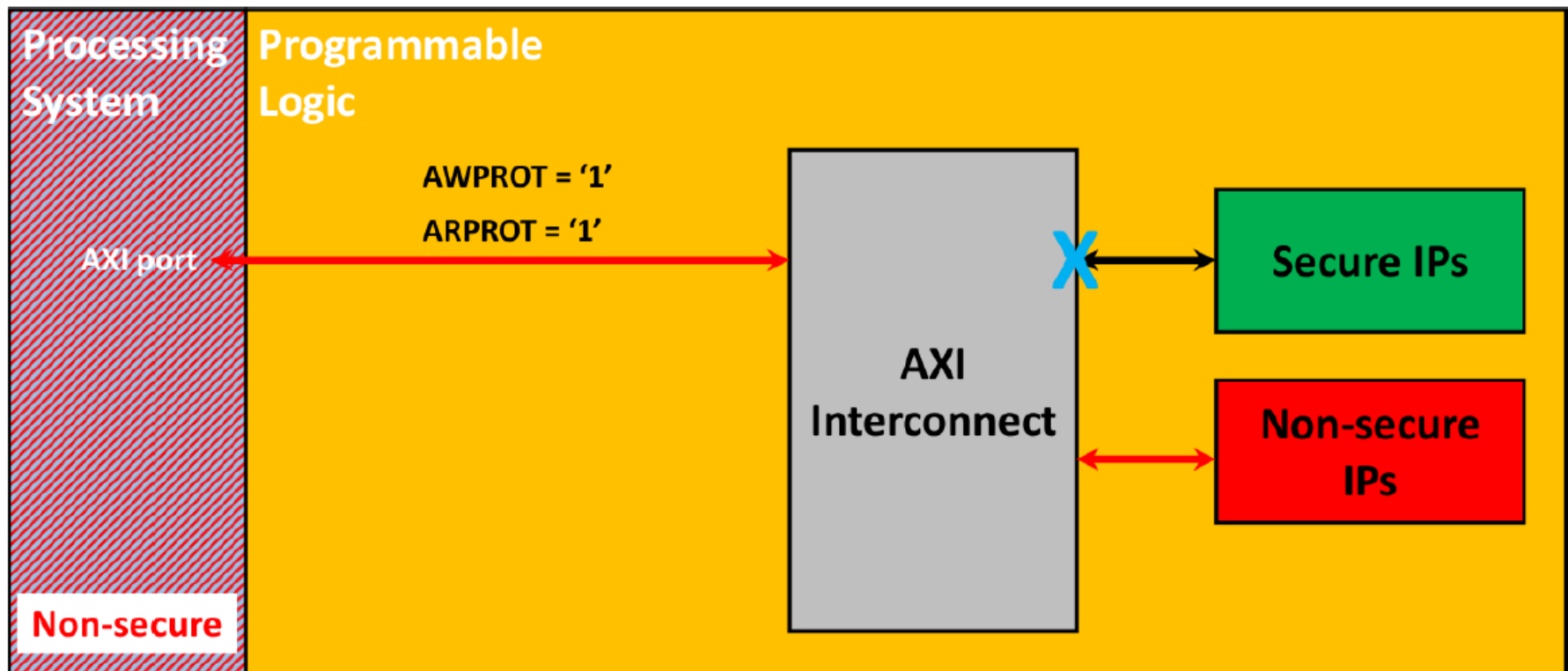
Systeme cible

- Extension de la TrustZone d'un cœur ARM vers le FPGA



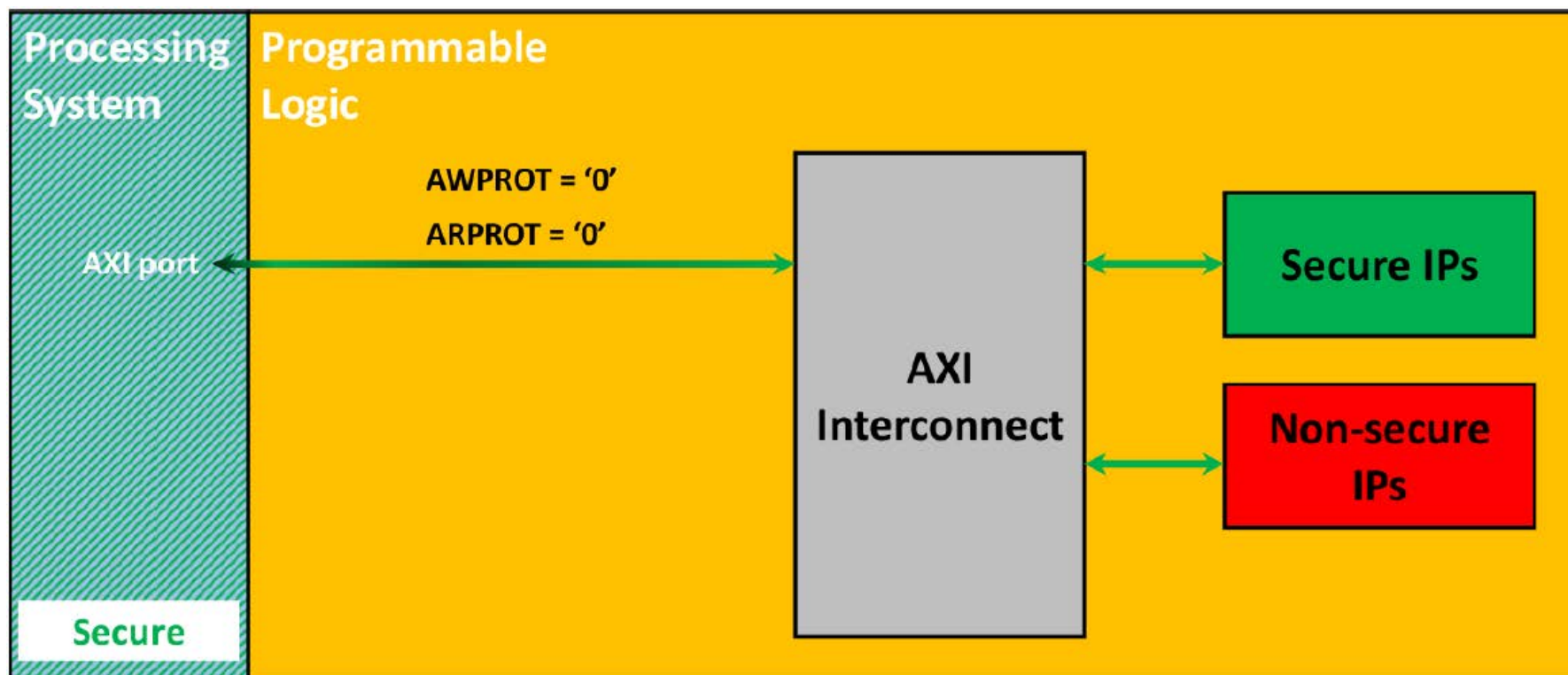
Fonctionnement normal du système (1/2)

- En mode non sécurisé (REE)



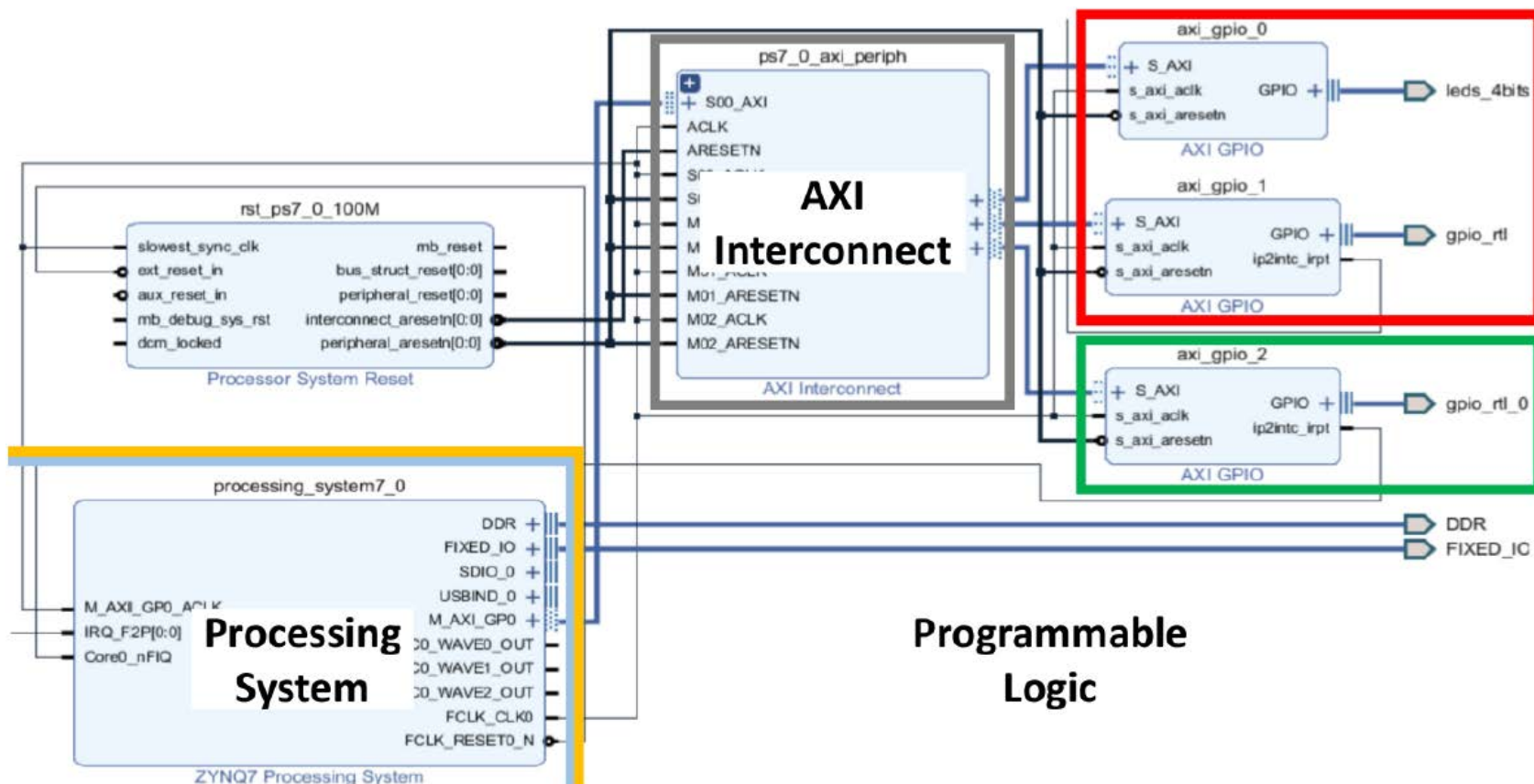
Fonctionnement normal du système (2/2)

- En mode sécurisé (TEE)

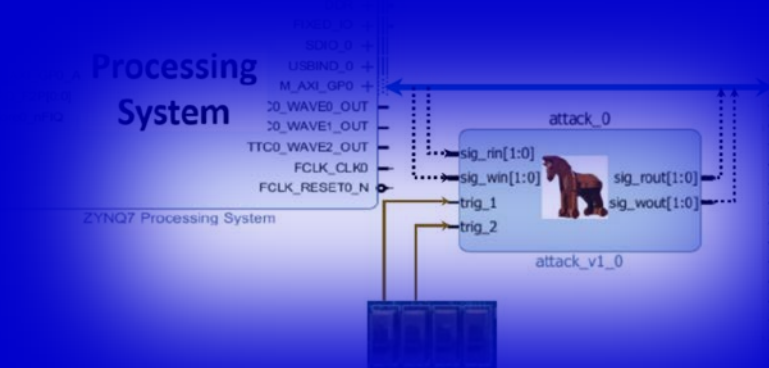


Prototypage (Xilinx Zynq)

- Architecture du système développé (Xilinx Vivado)

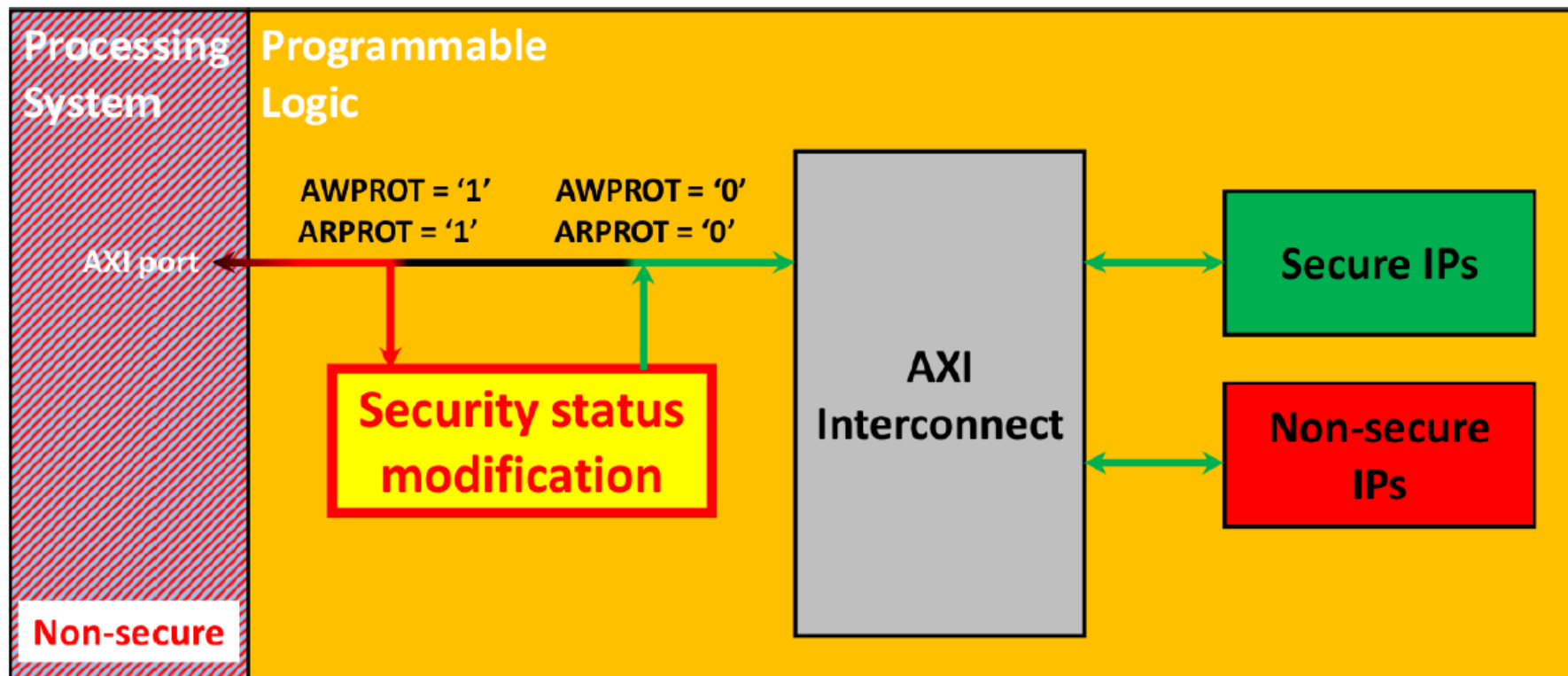


Scénario d'attaques de l'extension de la TrustZone



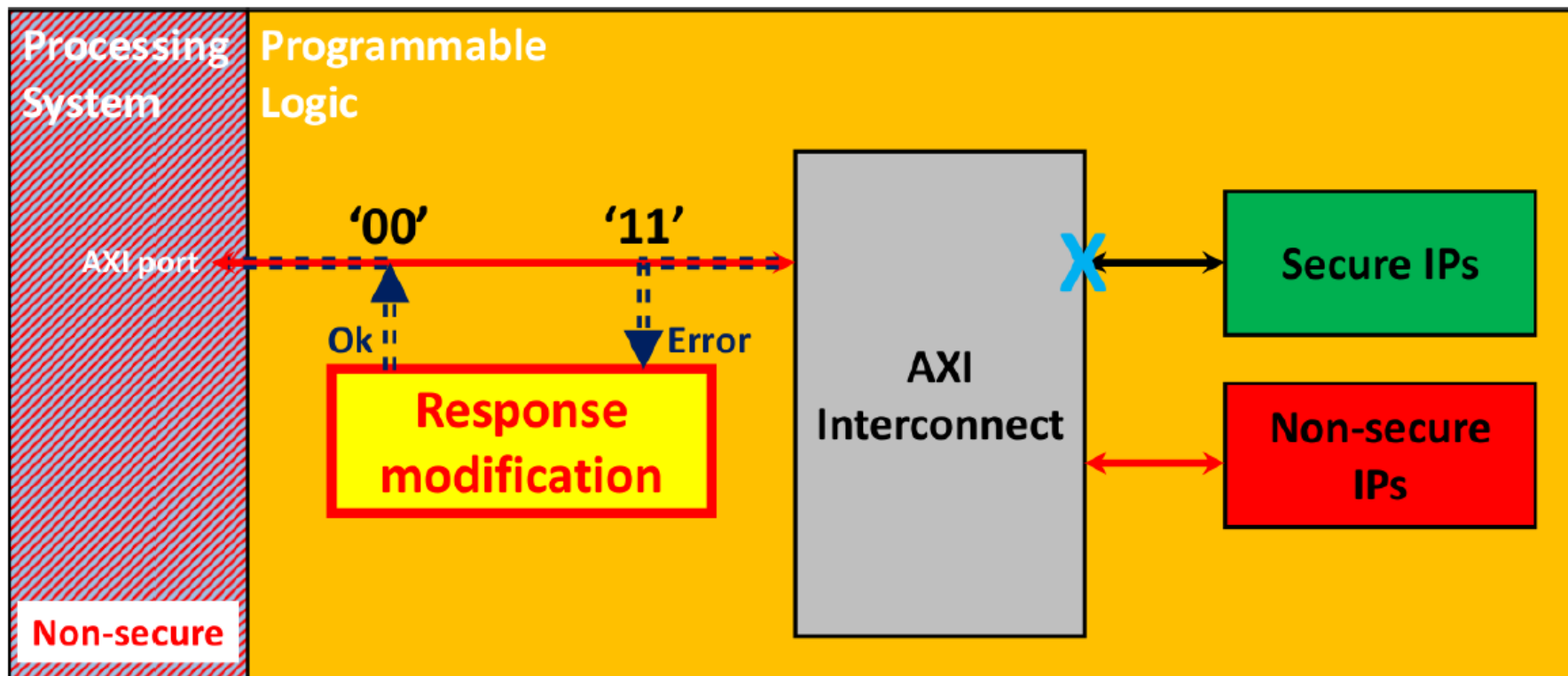
Modification des signaux de contrôle

- Corruption d'AWPROT et ARPROT



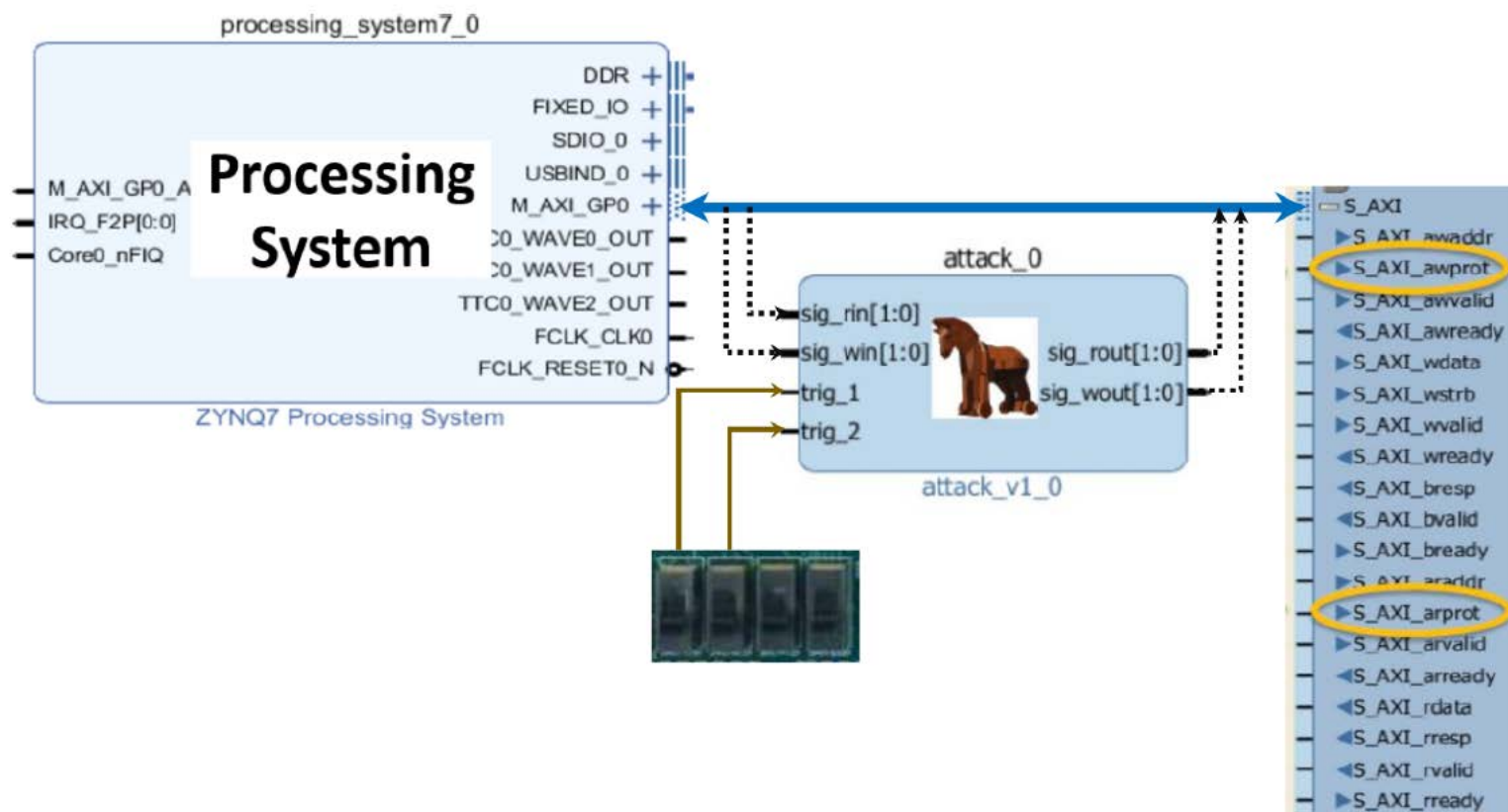
Modification des signaux d'erreur

- Corruption du signal d'erreur



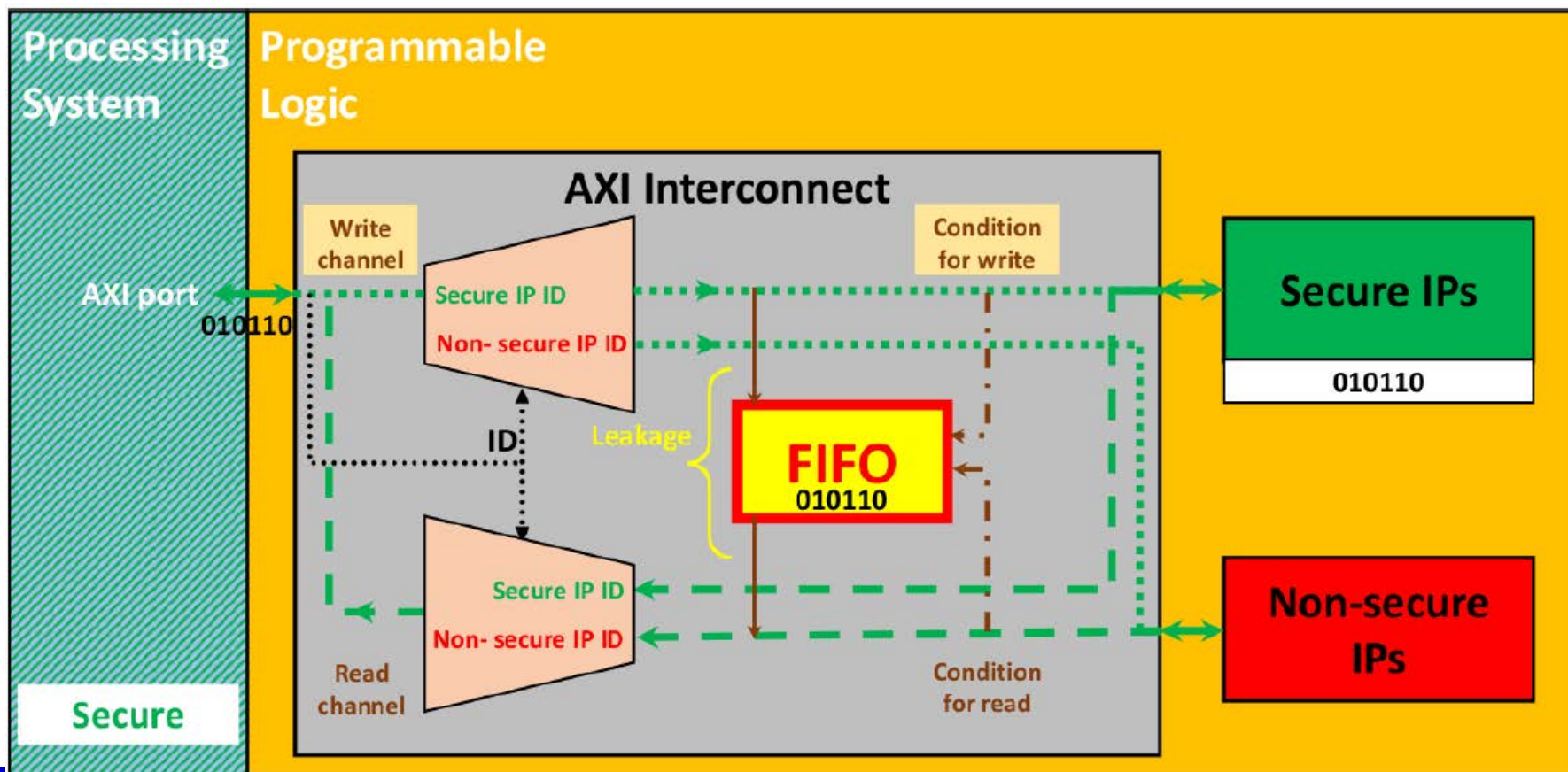
Réalisation (Xilinx Zynq)

- Cheval de Troie matériel



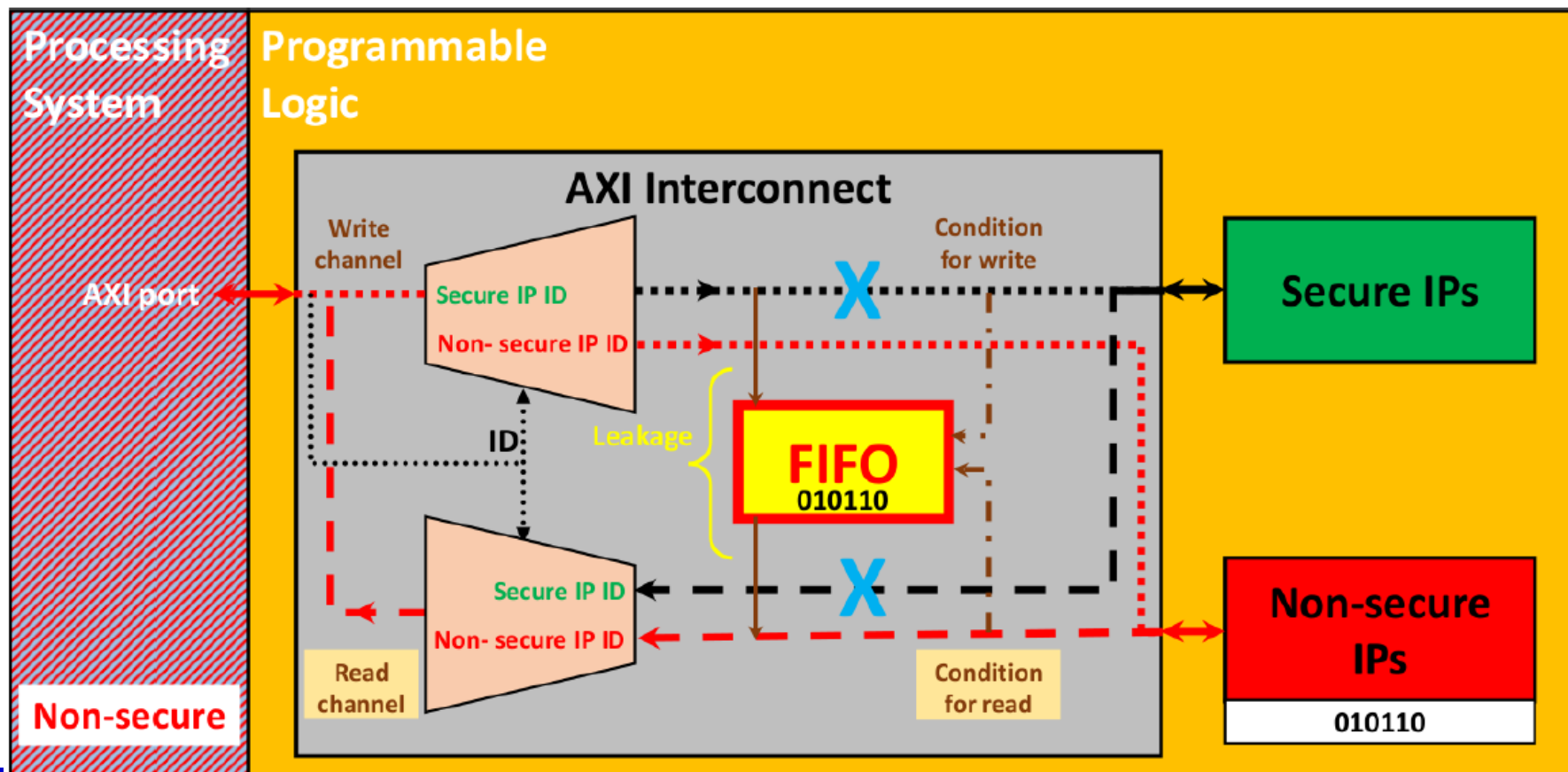
Corruption de l'AXI interconnect

- Mémorisation de l'ID de l'IP sécurisé

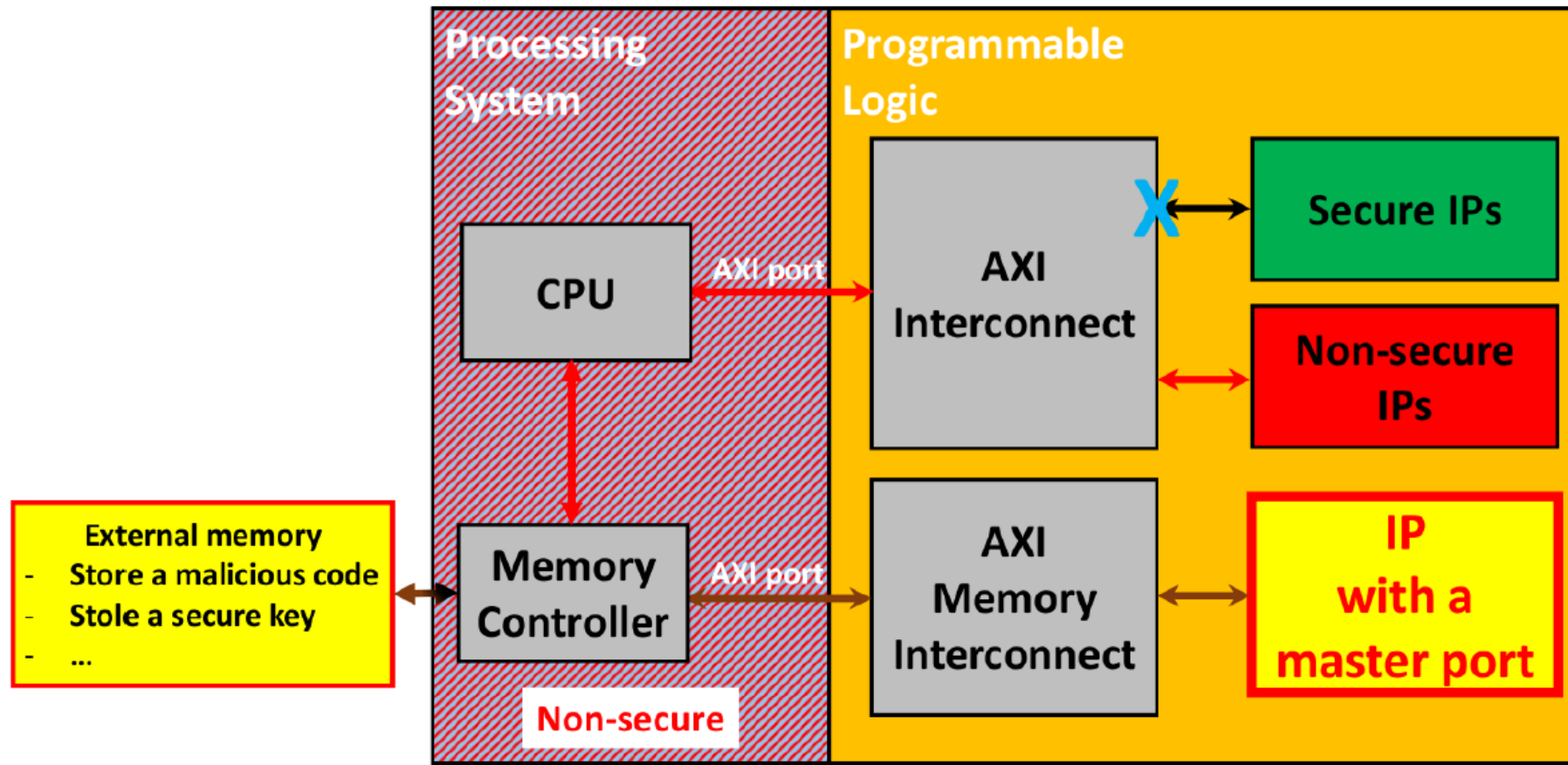


Corruption de l'AXI interconnect

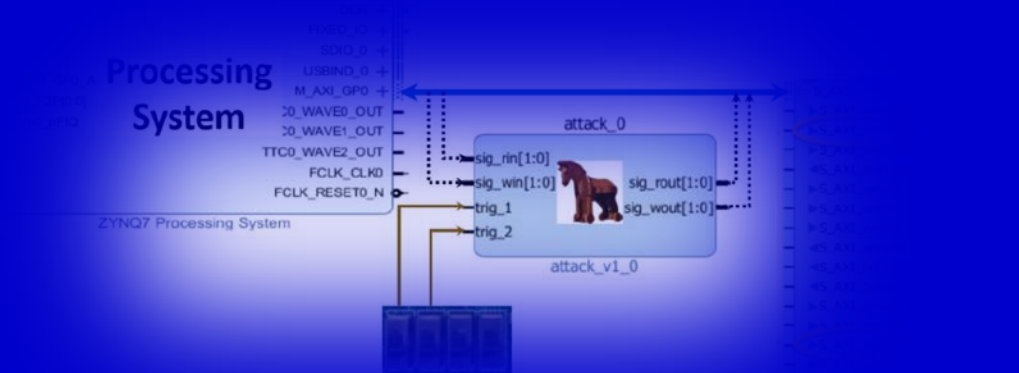
- Récupération d'ID



Accès à la mémoire externe



Démonstration



Conclusion 3/3

- Preuve de concept de plusieurs attaques possibles ciblant l'extension de la TrustZone dans un SoC complexe hétérogène (FPGA + ARM)
- Publication :
 - ◆ El Mehdi Benhani, Cédric Marchand, Alain Aubert, Lilian Bossuet. *On the Security Evaluation of the ARM TrustZone Extension in a Heterogeneous SoC*. IEEE SOCC, Munich, September 2017
- En cours
 - ◆ Mise en évidence de fuites d'informations sur canaux internes

Ces travaux font partie du projet



“Ce projet est financé dans le cadre du 20^{ème} appel à projets de R&D du Fonds Unique Interministériel (FUI)”



Evaluation de la sécurité de la technologie ARM TrustZone

Lilian Bossuet

Laboratoire Hubert Curien, CNRS UMR 5516
Université Jean Monnet, Saint-Etienne, France



25 janvier 2018
Saint-Malo, France