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

UNIVERSITÉ JEAN MONNET
SAINT-ÉTIENNE

cnrs

Evaluation de la sécurité de la technologie ARM TrustZone

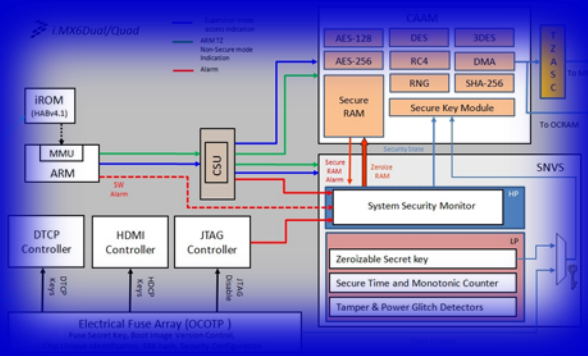
Lilian Bossuet
Laboratoire Hubert Curien, CNRS UMR 5516
Université Jean Monnet, Saint-Etienne, France

25 janvier 2018
Saint-Malo, France

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

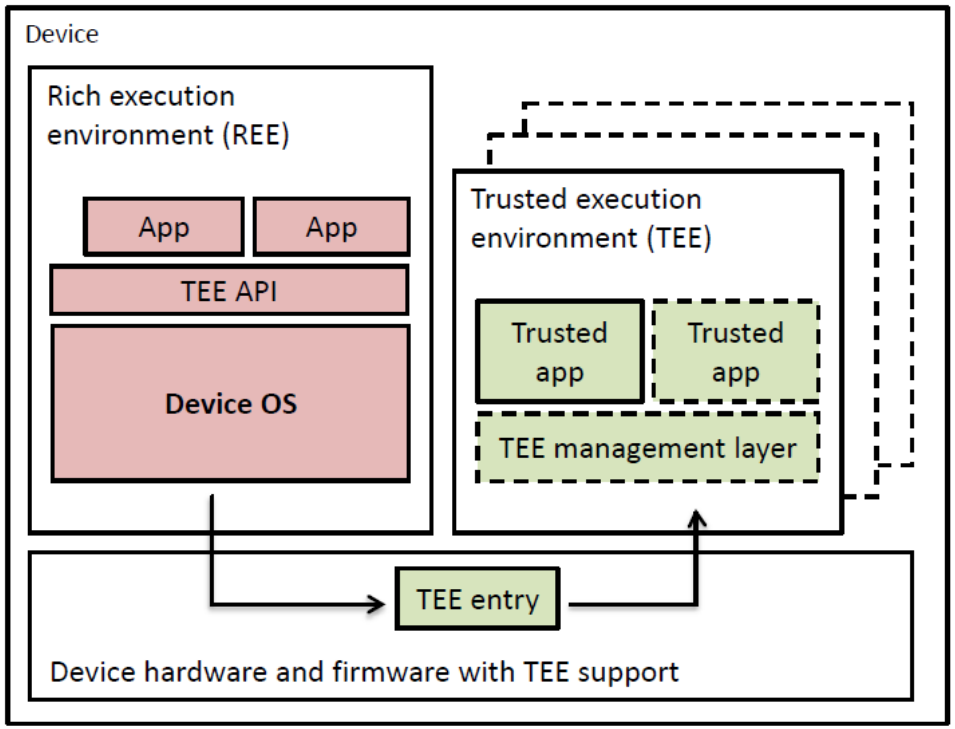
- De multiples attaques sur les systèmes embarqués connectés

Sécurité des systèmes programmables
Trusted Execution Environement – TEE



Architecture TEE

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

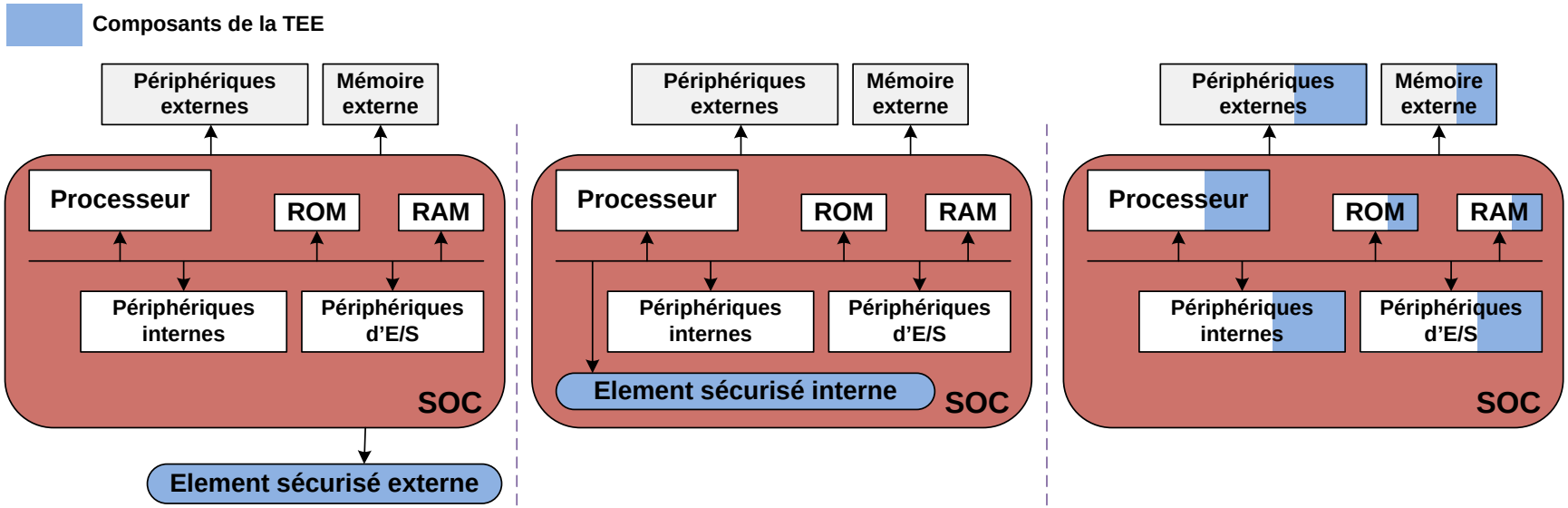


Architectures with single TEE

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

Architectures with multiple TEEs

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



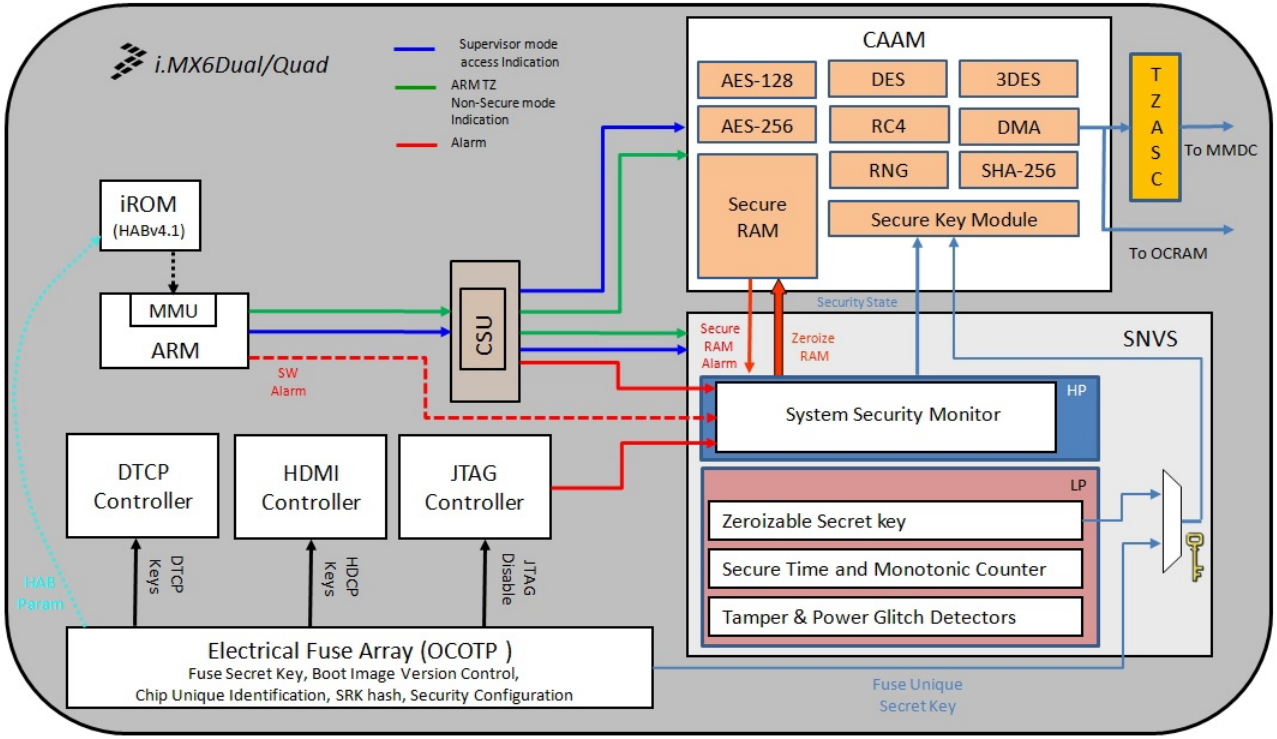
a) architecture de TEE basée sur un élément sécurisé externe

b) architecture de TEE basée sur un élément sécurisé interne

c) architecture de TEE basée sur un SoC avec technologie de sécurité d'exécusion du type *ARM TrustZone*

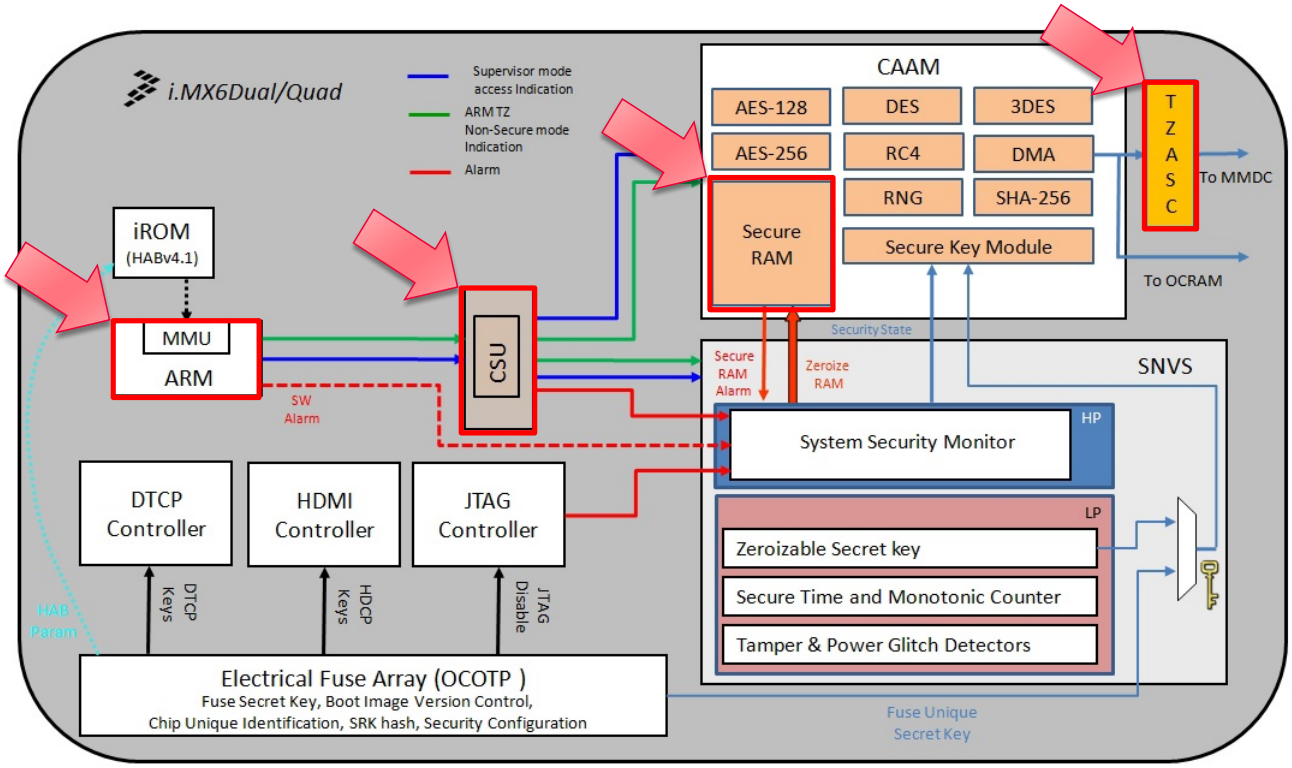
Architecture matérielle de sécurité ARM Cortex A9

- Exemple du Freescale i.MX6



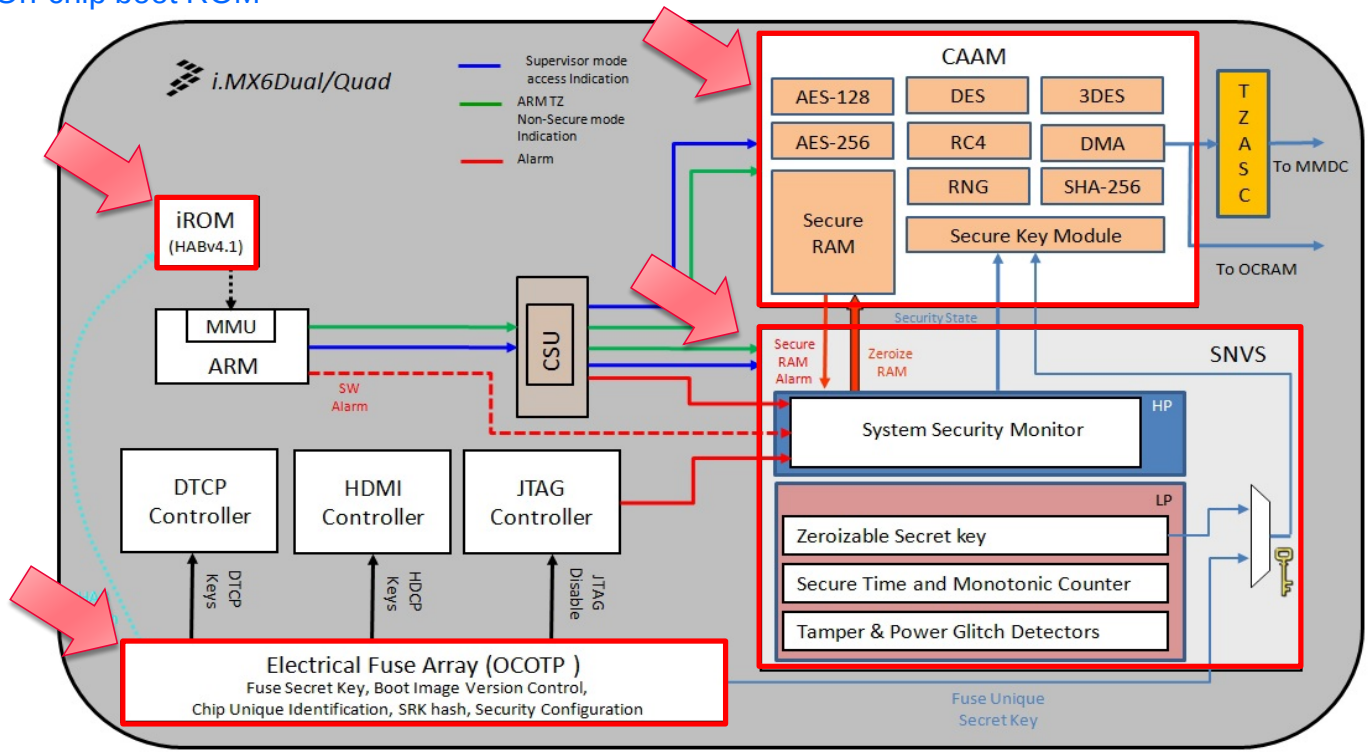
Architecture matérielle de sécurité ARM Cortex A9

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

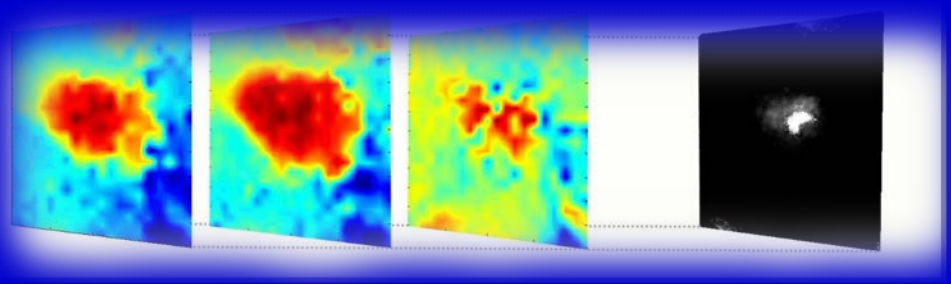


Architecture matérielle de sécurité ARM Cortex A9

- 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



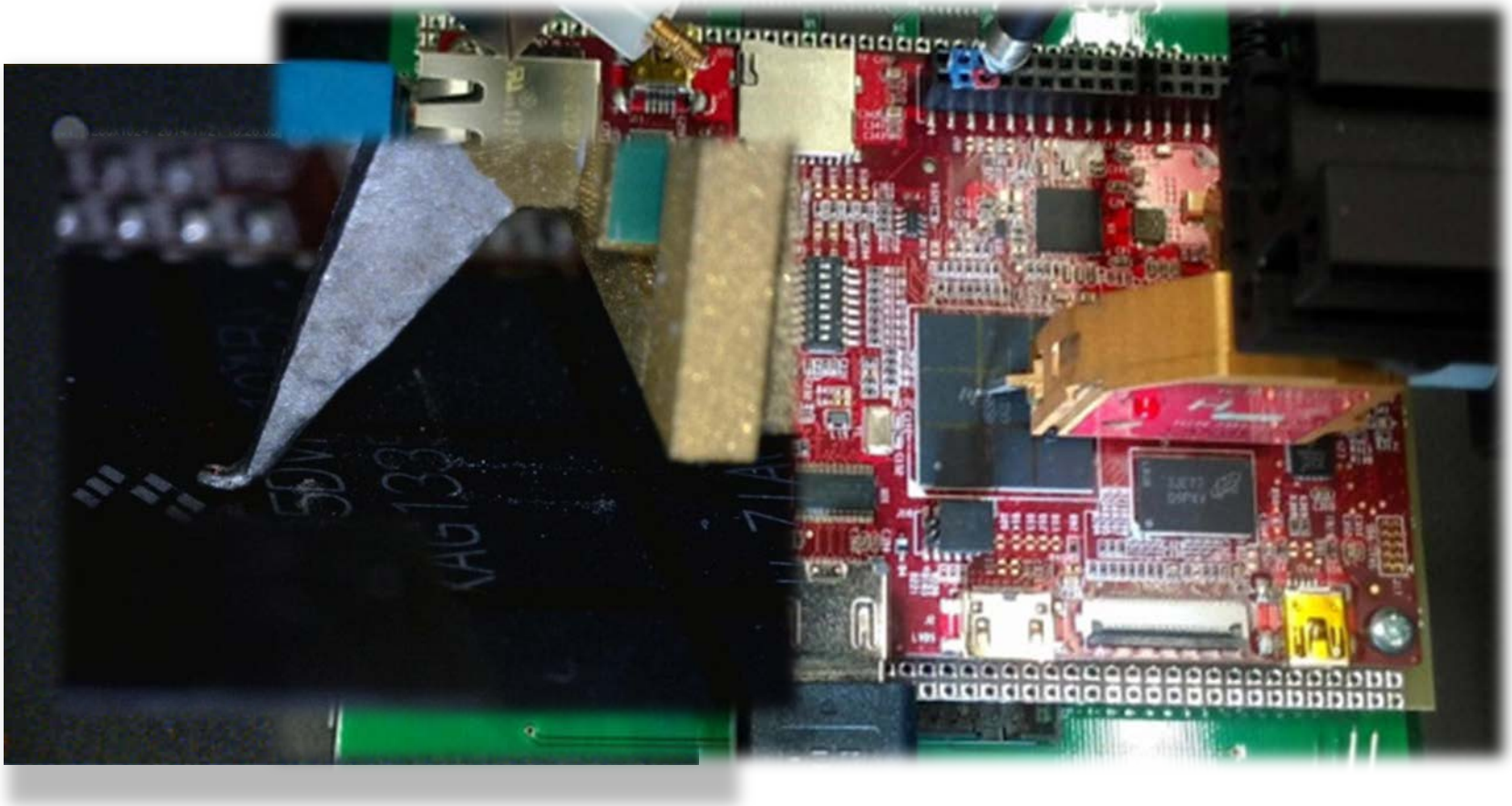
Attaques classiques combinées – étape 1

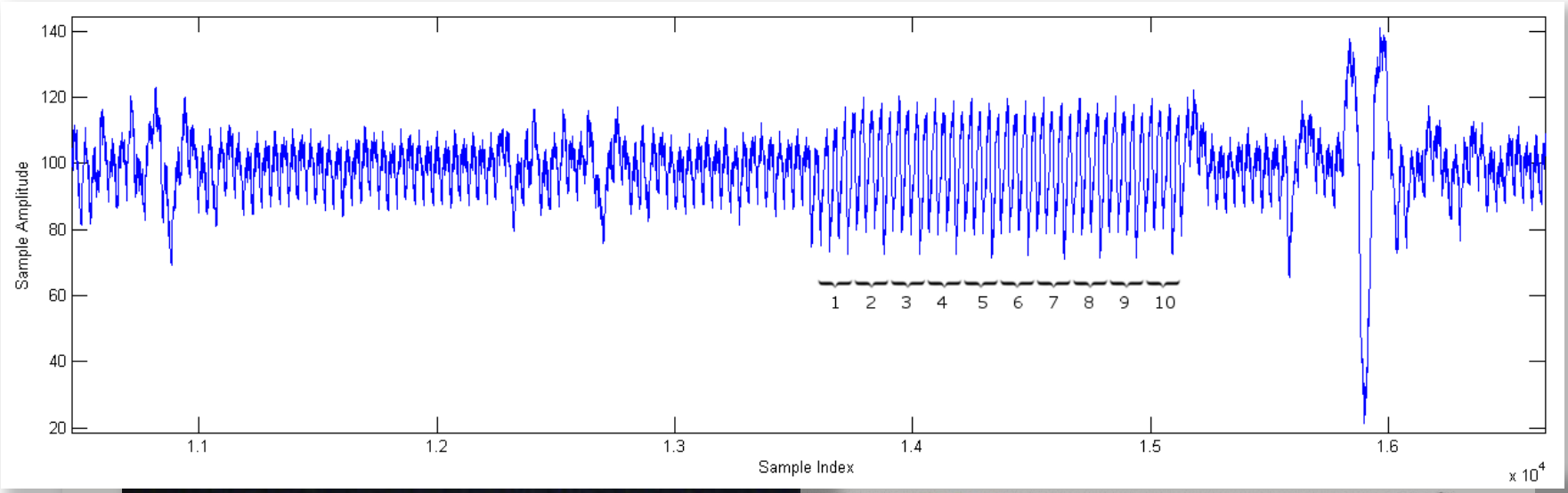
- Analyse du rayonnement EM du chiffreur AES masqué
- Cartographies EM avec trois ensemble de données

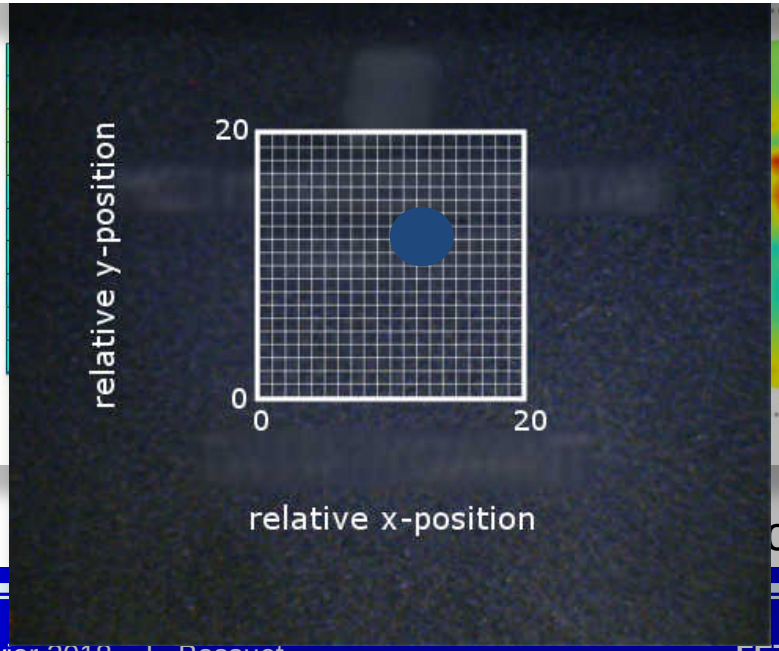
Set 1	HW(clé) : 0 128	HW(message) : 0 0	HW(chiffré) : 65 64
Set 2	HW(message) : 0 128	HW(chiffré) : 65 68	HW(clé) : 0 0
Set 3	HW(chiffré) : 0 128	HW(clé) : 0 128	HW(message) : 65 65

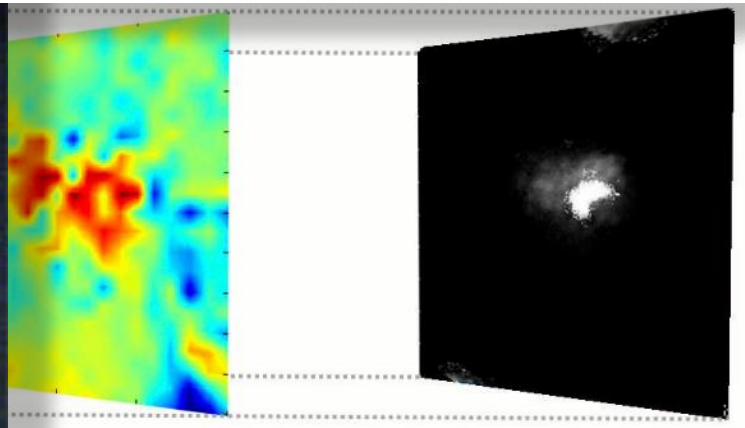
- Objectif : localisation géographique et temporelle du CAAM dans le SoC

Cartographie EM




Sample Amplitude
Sample Index
x 10^4
1 2 3 4 5 6 7 8 9 10


relative y-position
relative x-position
20
0
0
20

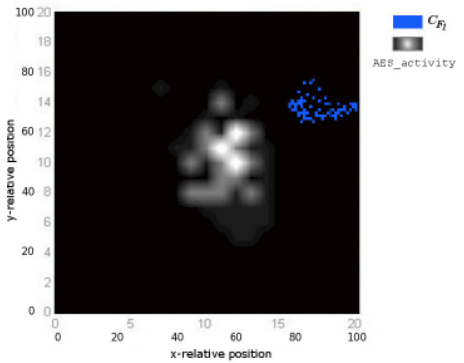


chiffré

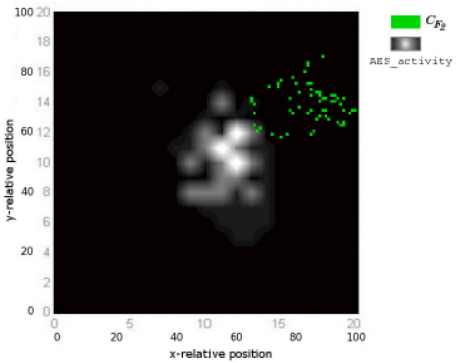
AES

Attaques classiques combinées – étape 2

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

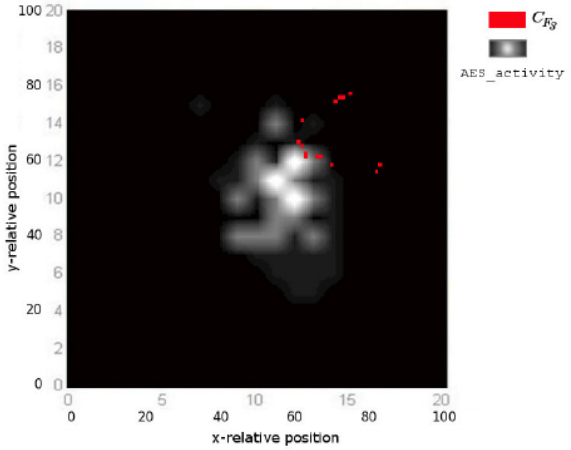


(a) buffer copy faults



(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
	...													



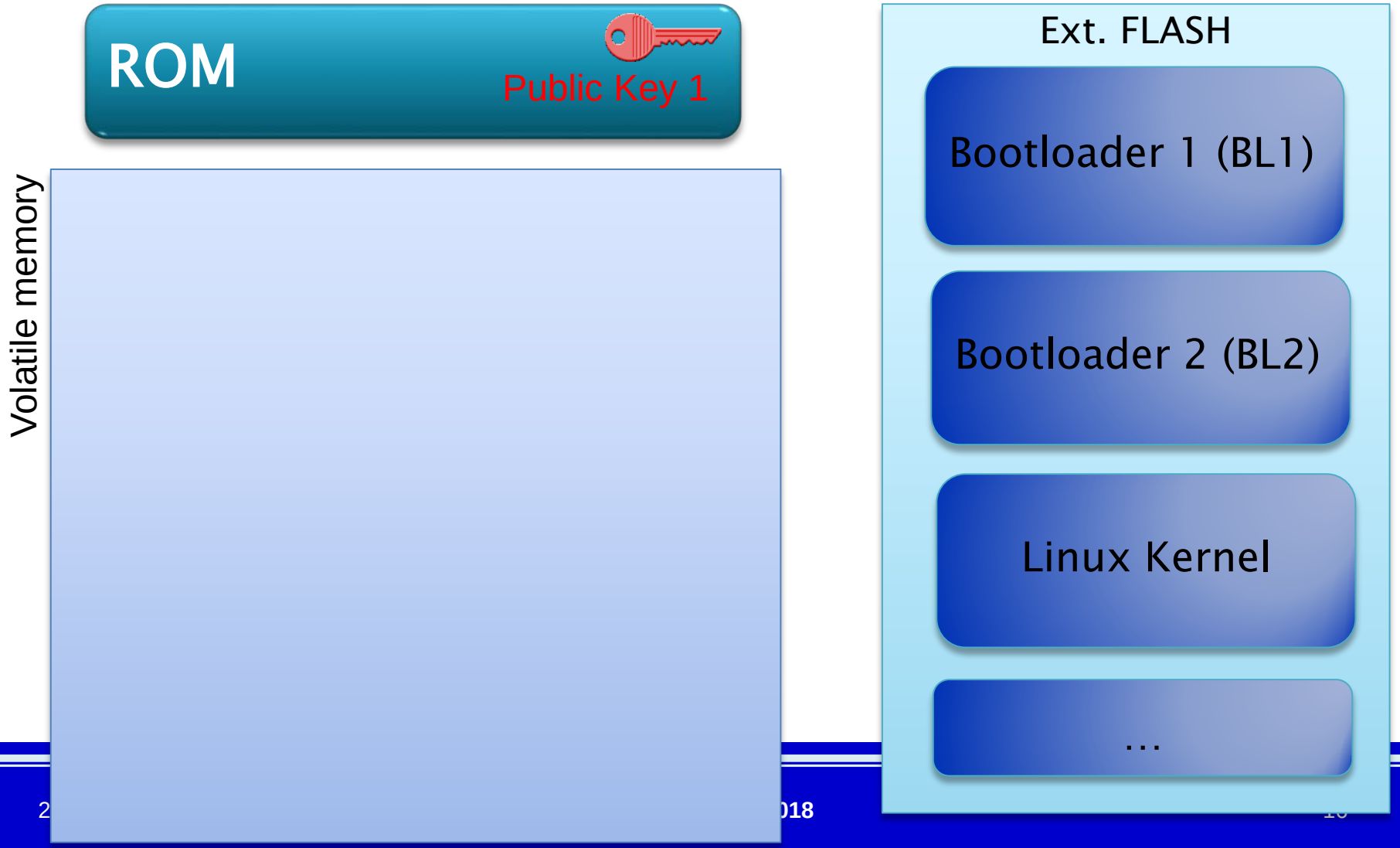
(c) Faults related to the AES process

Conclusion 1/3

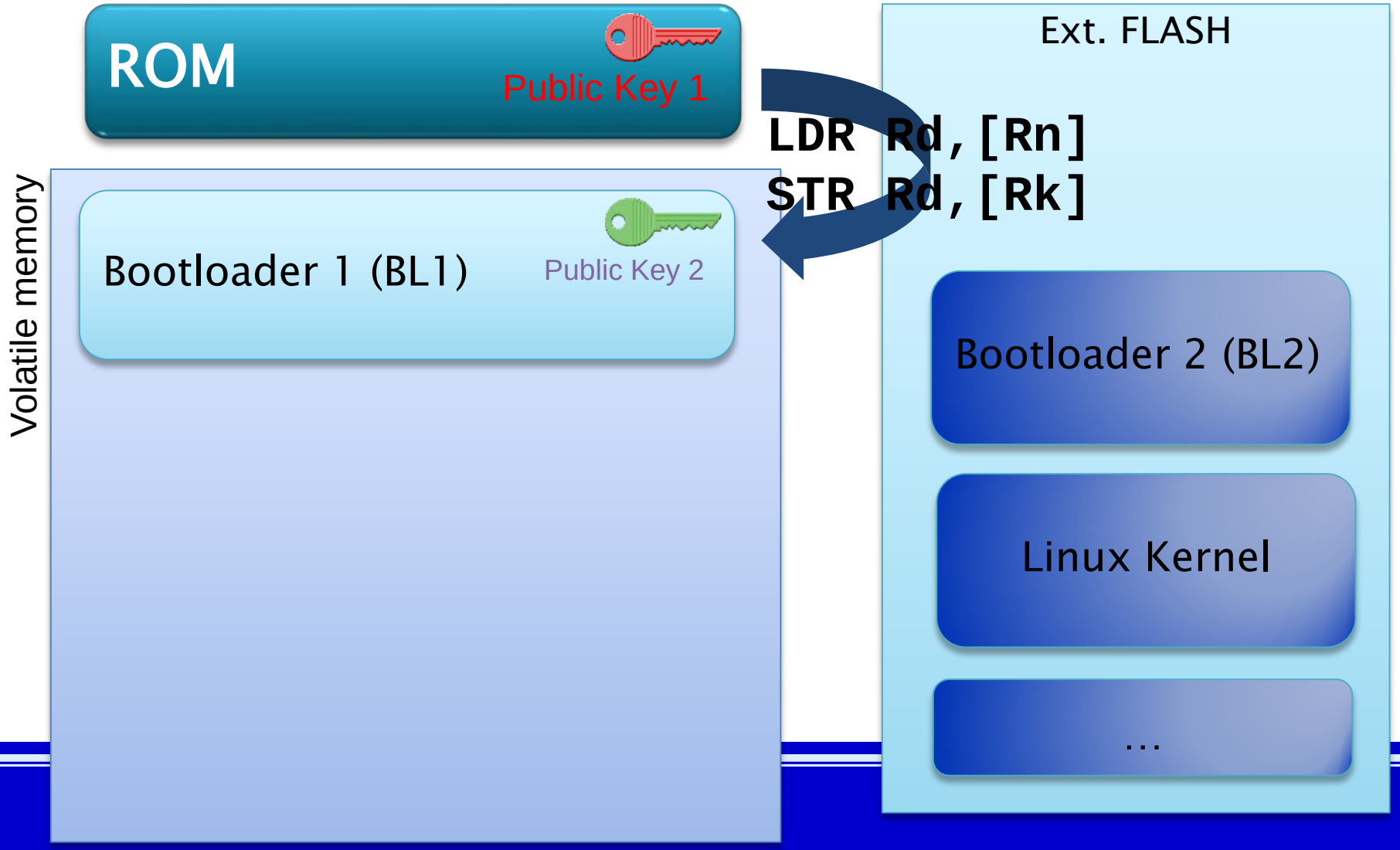
- L'accélérateur cryptographique de la TrustZone est sécurisé contre les attaques par canaux cachés, il existe des possibilités d'attaques en fautes.
  - Pas de protection particulière si l'on exécute un algorithme cryptographique dans le processeur généraliste même dans le monde sécurisé…
- Publication
  - 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 sécure boot de la TrustZone

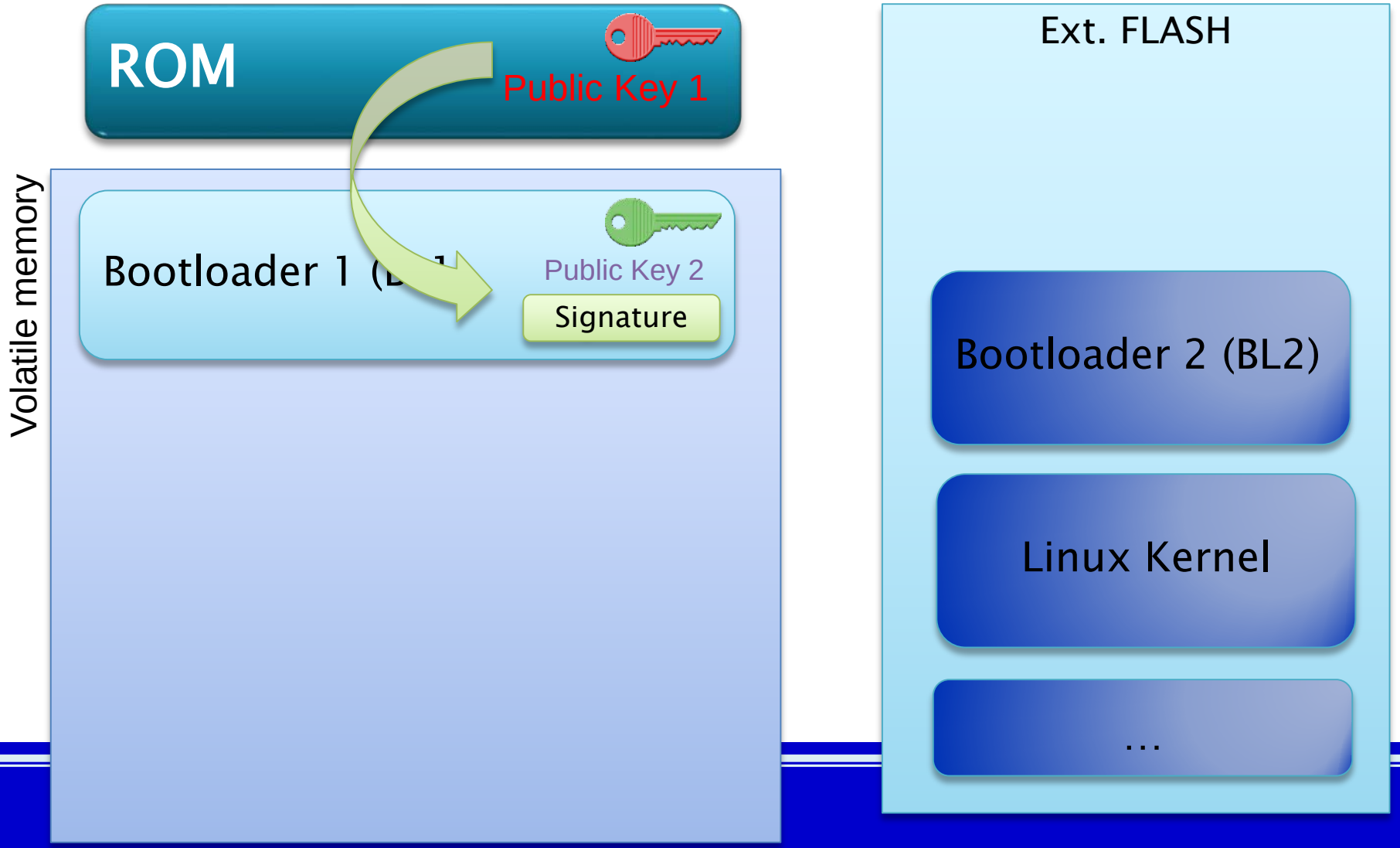
Secure Boot normal



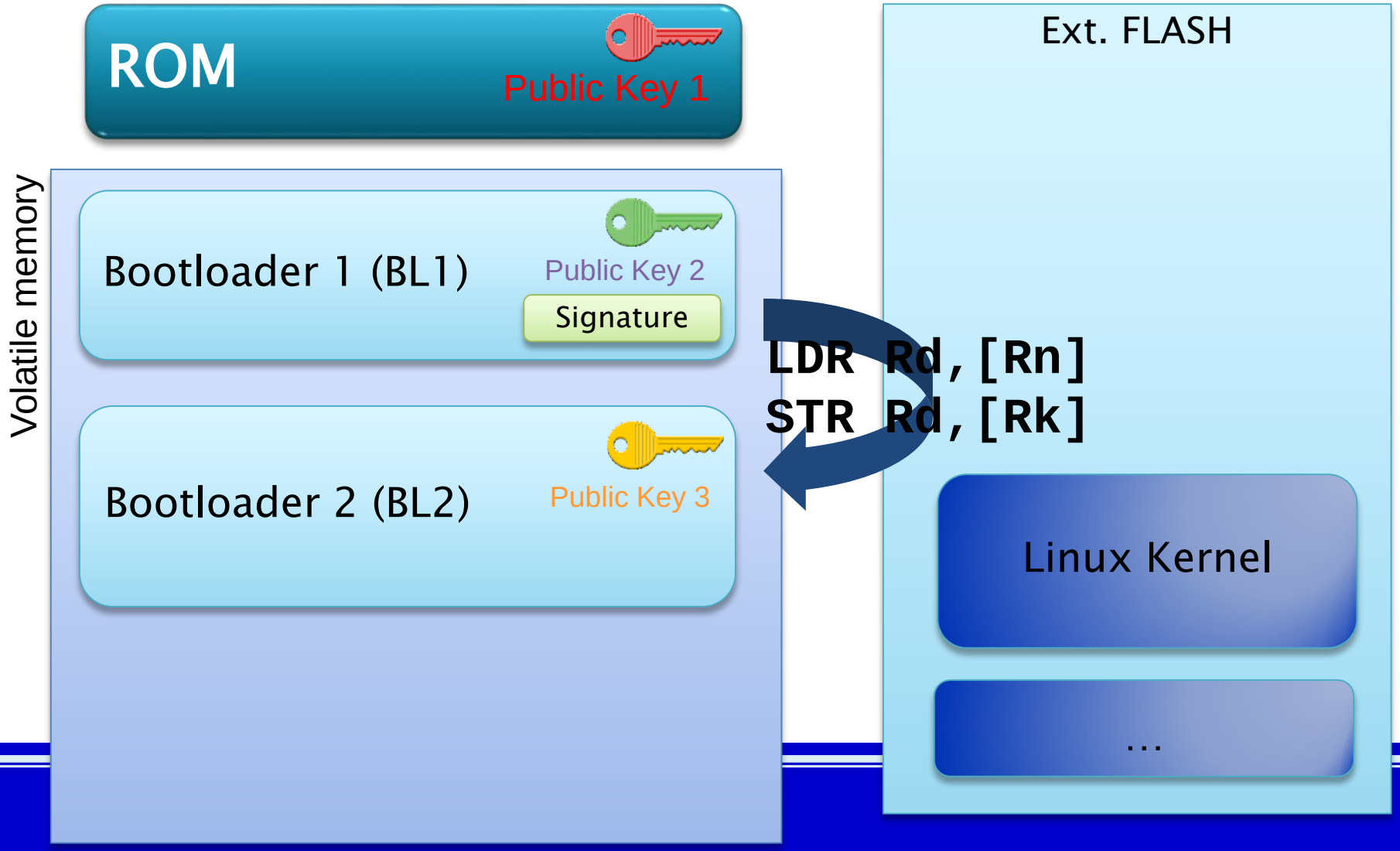
Secure Boot normal



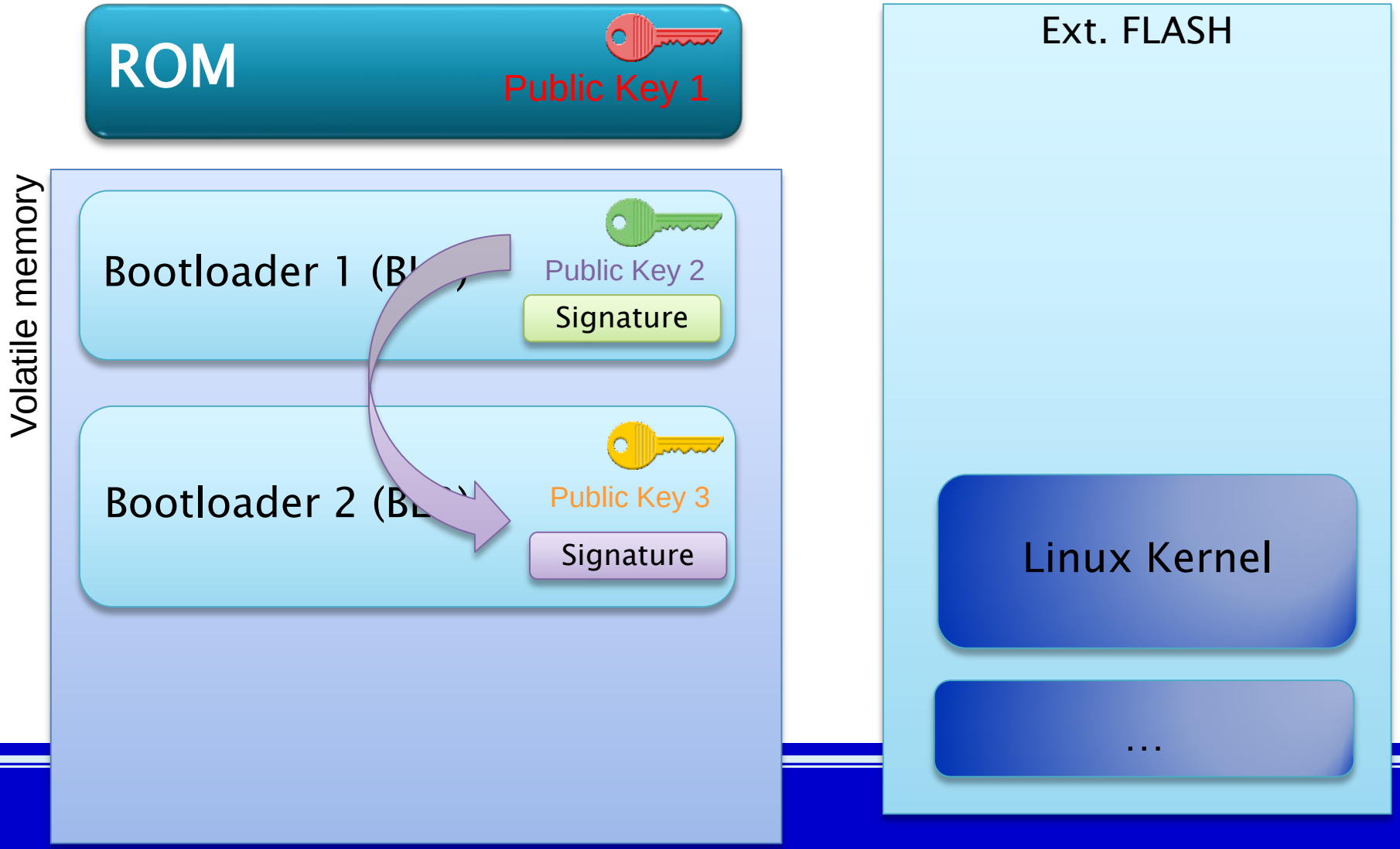
Secure Boot normal



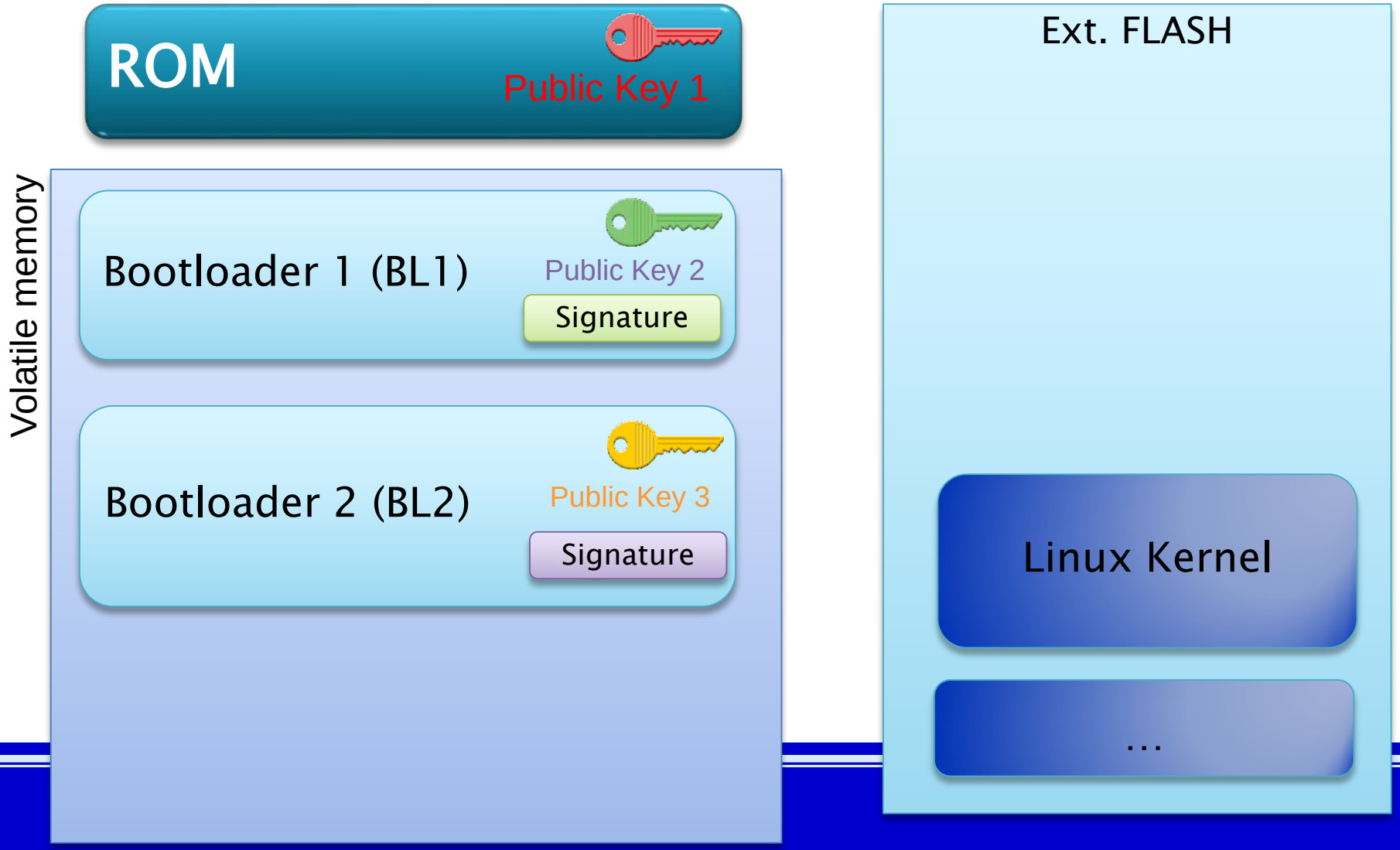
Secure Boot normal



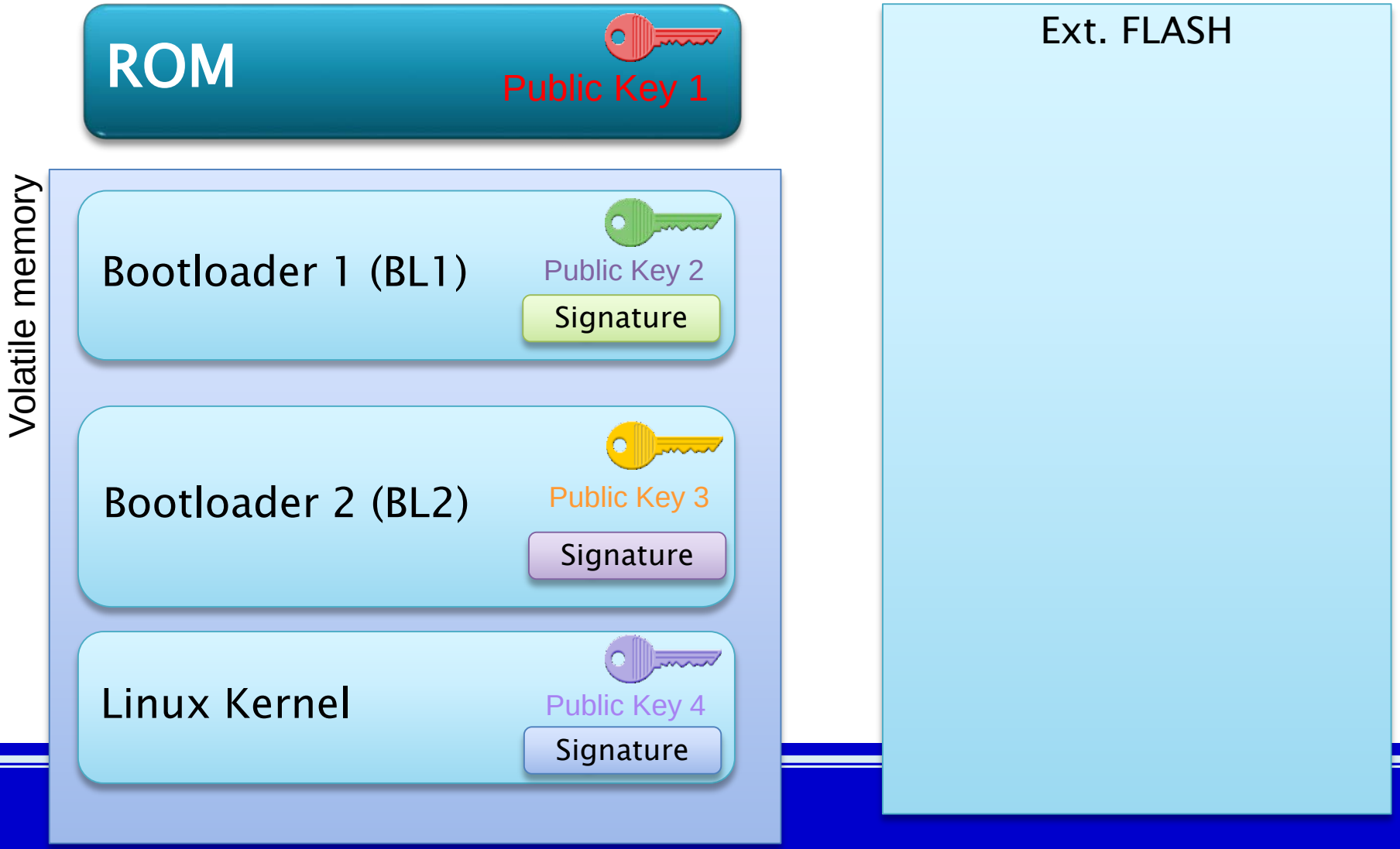
Secure Boot normal



Secure Boot normal

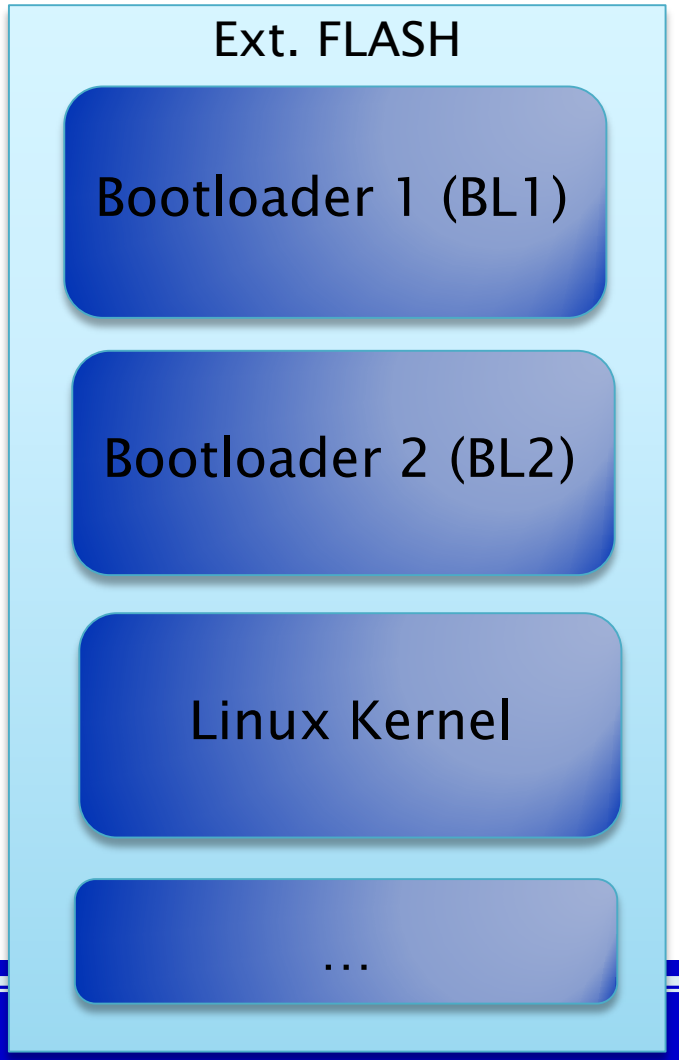


Secure Boot normal



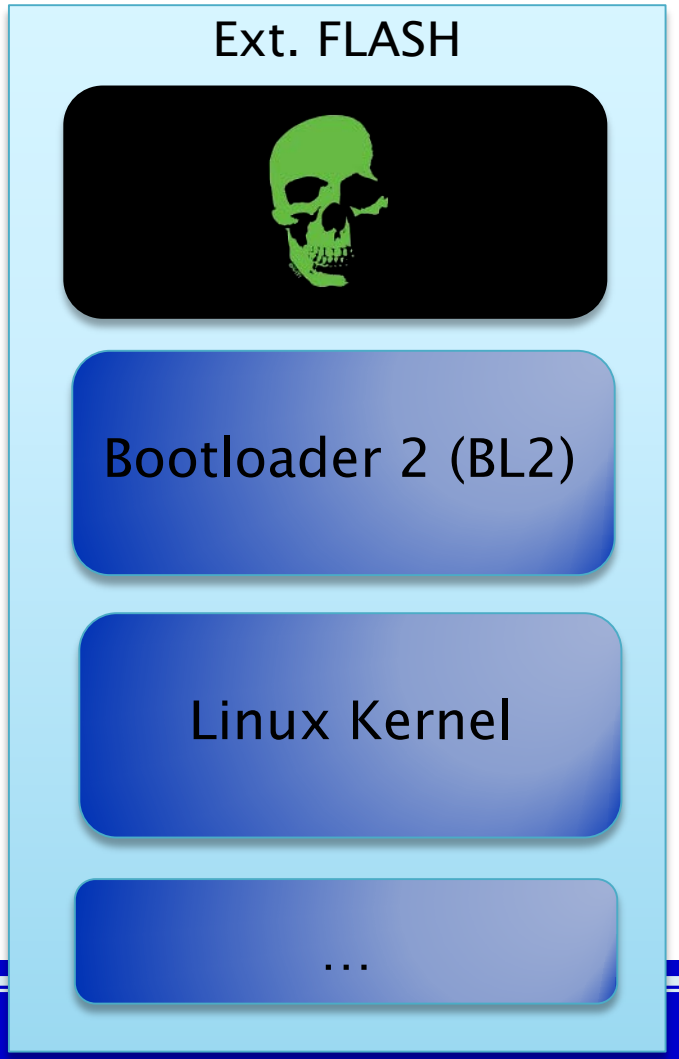
Attaque RISCURE

Volatile memory

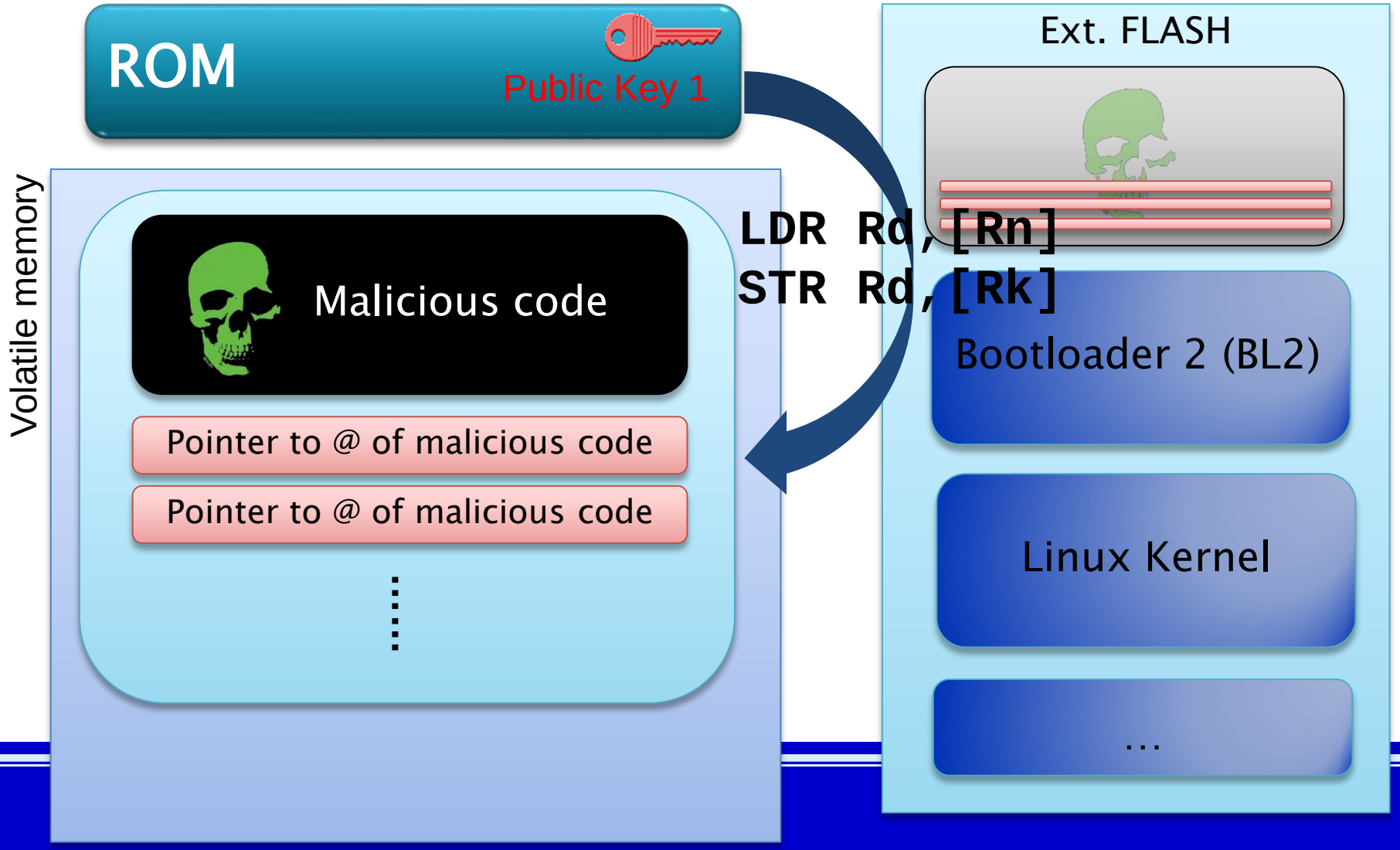


Attaque RISCURE

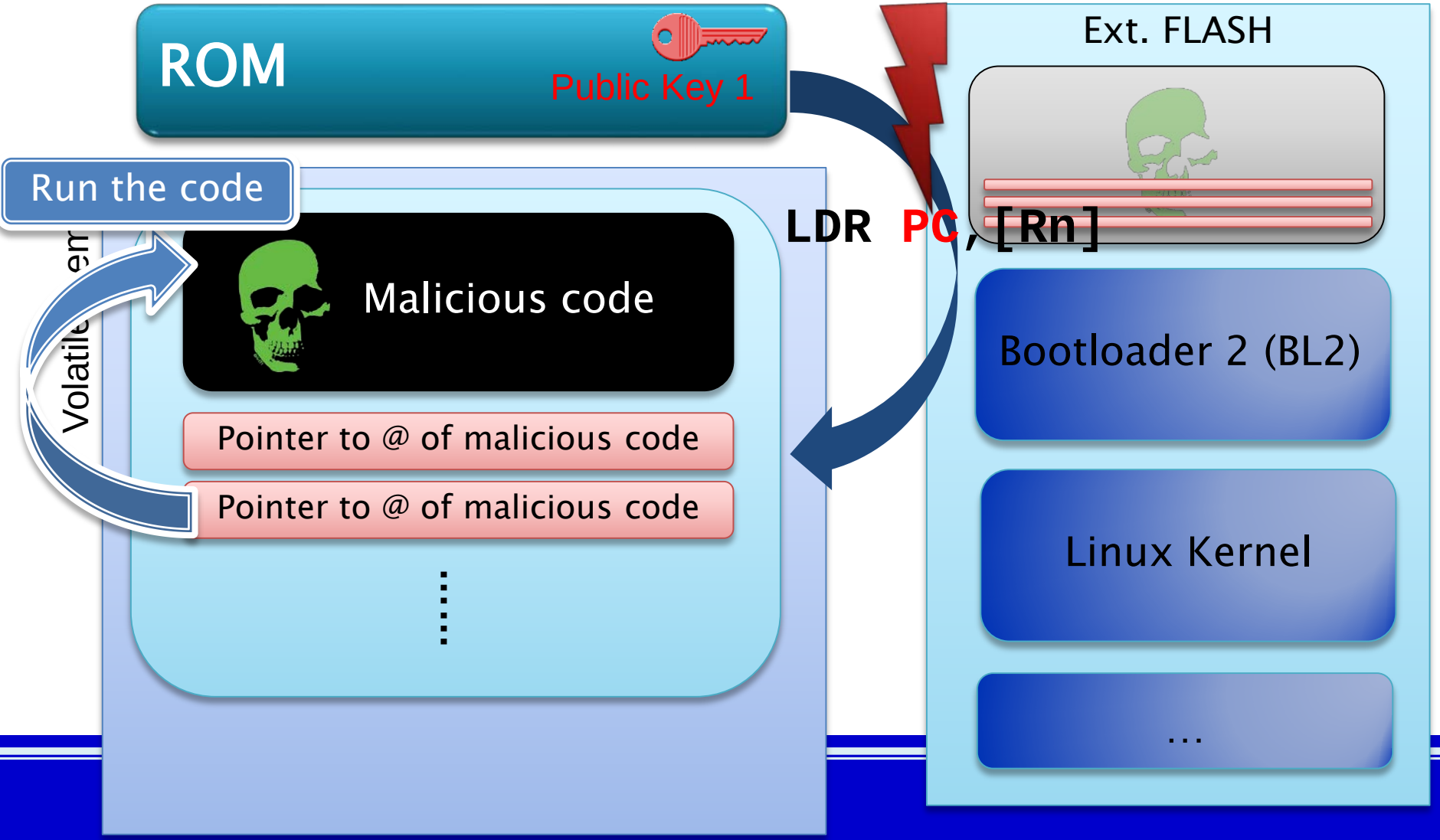
Volatile memory



Attaque RISCURE

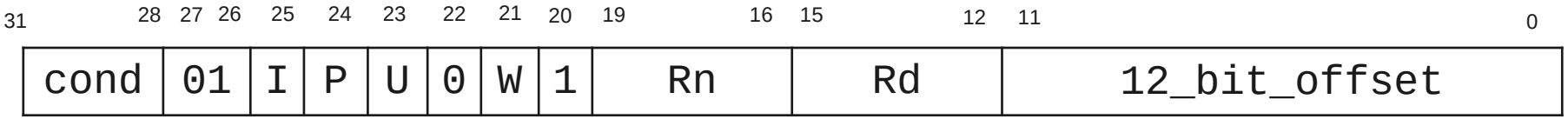


Attaque RISCURE

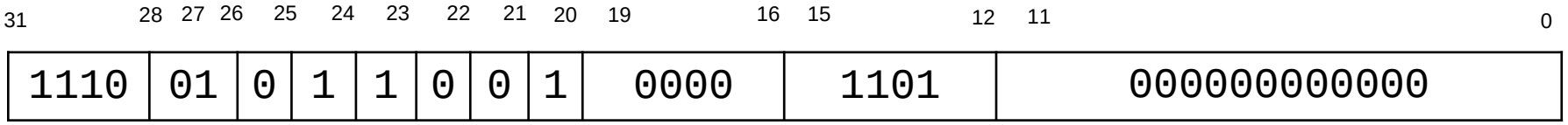


Attaque de RISCURE

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

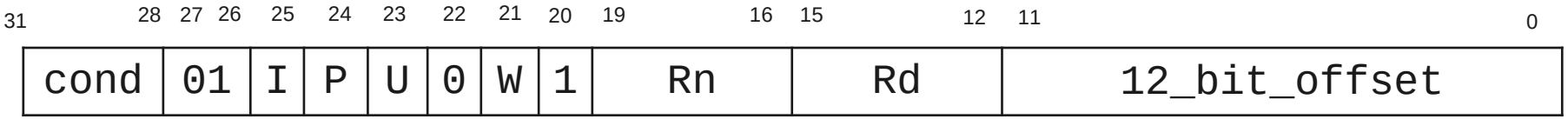


  - `LDR R13, [R0]` (`[R0]` point to the address of the malicious code)

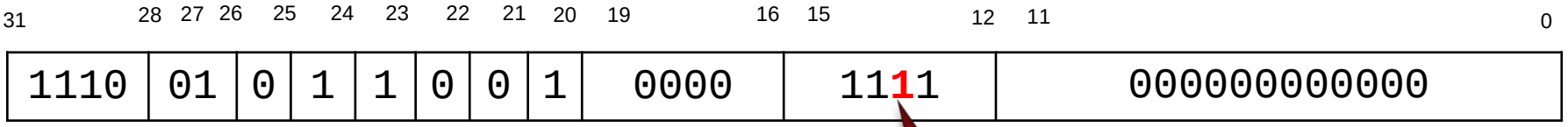


Attaque de RISCURE

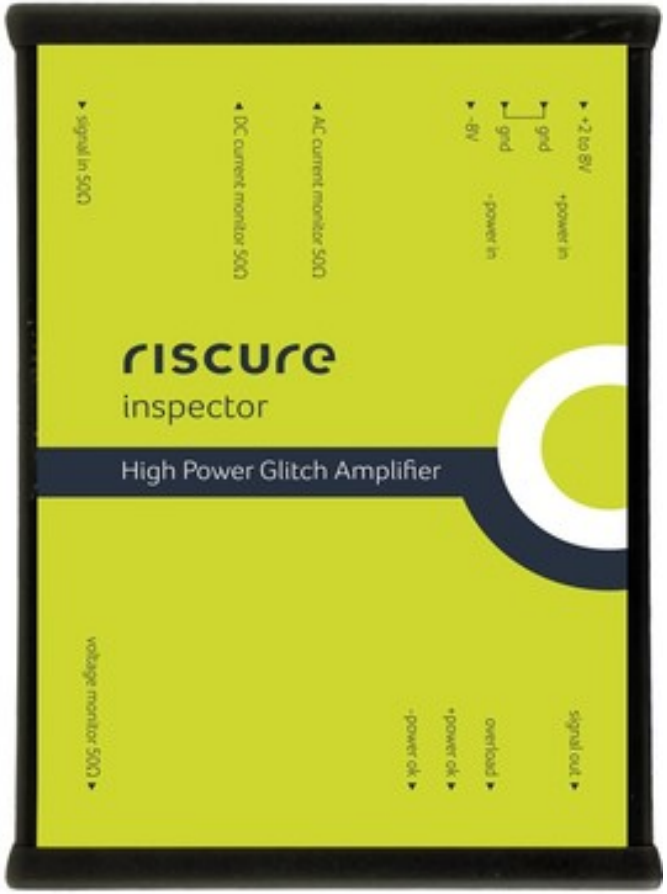
- Comment est-ce possible ?
- *LDR processing instruction*
  - `LDR{<cond>} Rd, [Rn {,#+/-12_bit_offset }]`

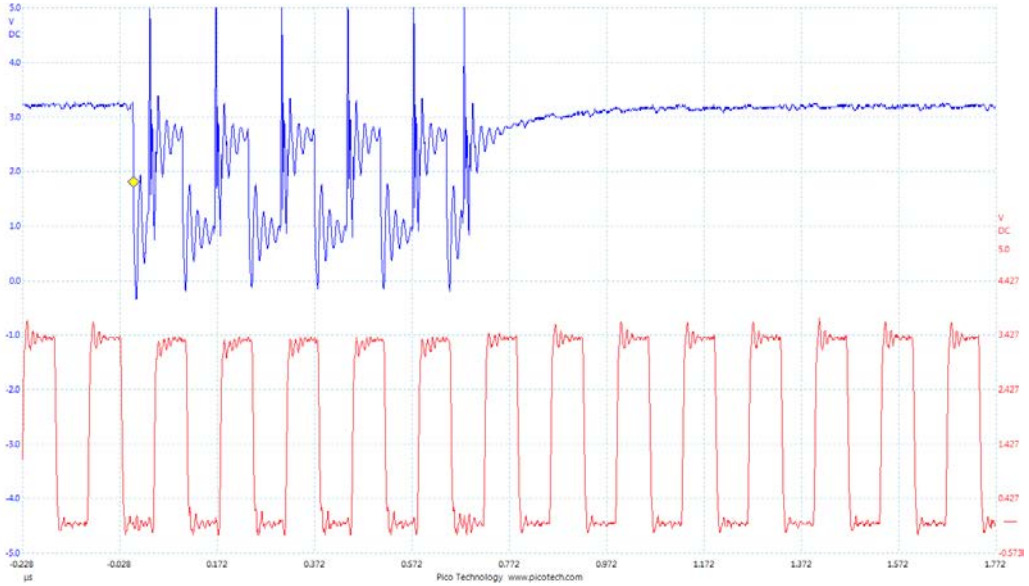


  - `LDR PC , [R0]` (`[R0]` point to the address of the malicious code)



Injection de fautes par *glitch* de tension

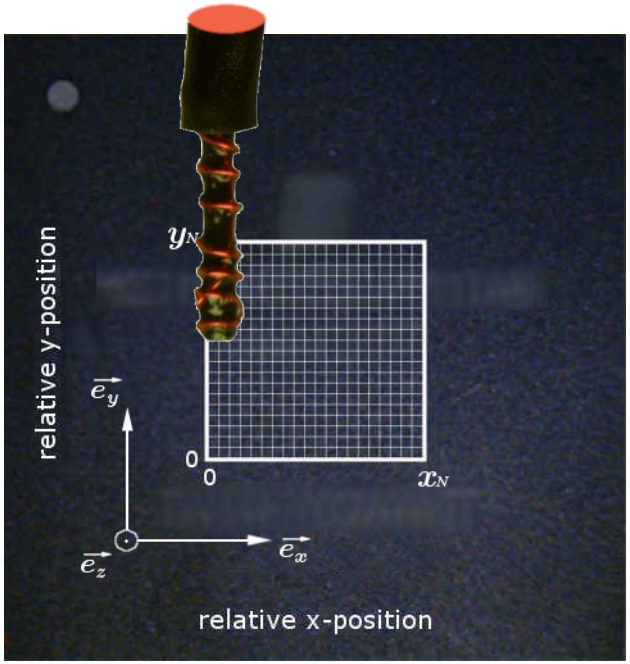


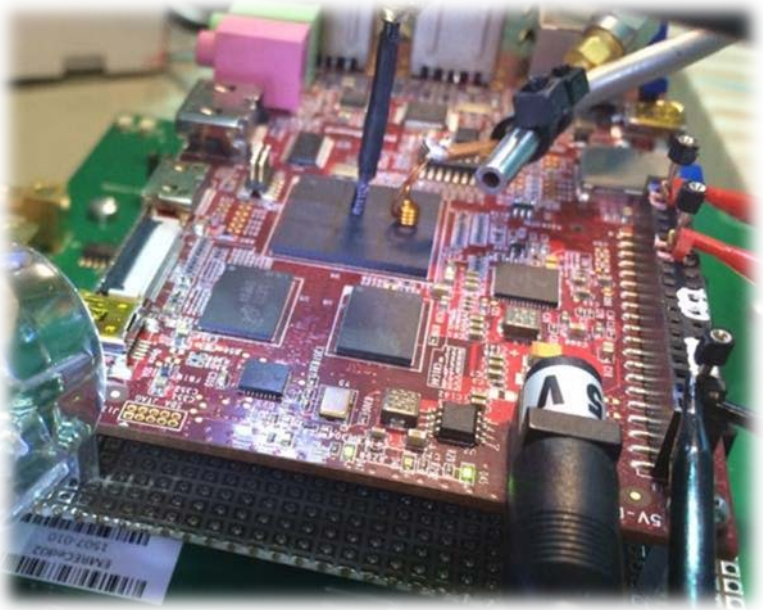


N. Timmers, A. Spruyt and M. Witteman,*Controlling PC on ARM using fault injection*, in Workshop on Fault Diagnosis and Tolerance in Cryptography, (FDTC 2016), Santa Barbara, CA, US, August 16, 2016.

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

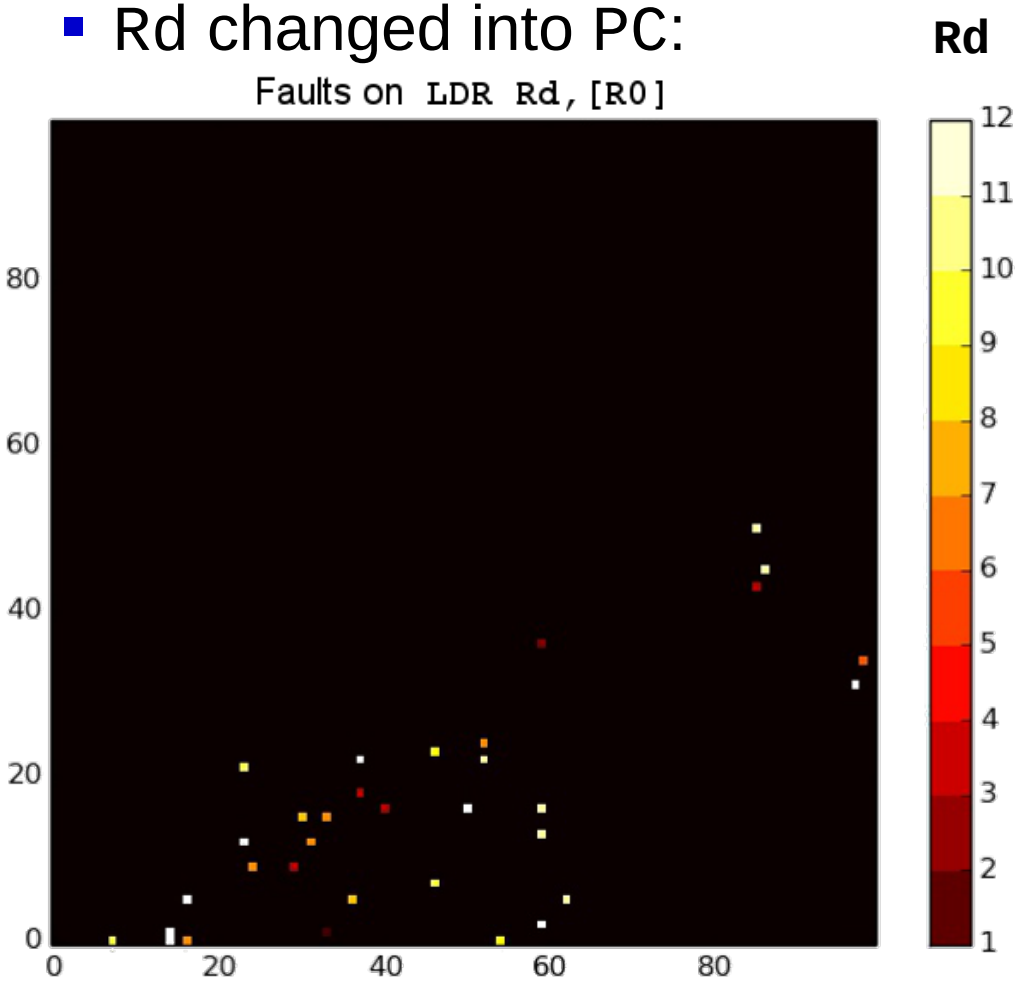
- Injection durant l'exécution de LDR Rd, [R0]
  - Vérfier si LDR Rd, [R0] => LDR PC, [R0]





Résultats expérimentaux

- Rd changed into PC:



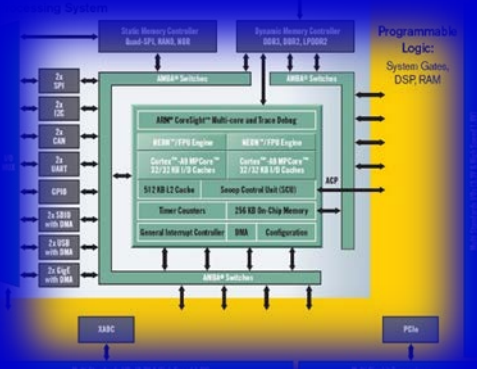
Rd	occurrence
R12	8
R11	6
R10	3
R9	2
R8	2
R7	5
R6	1
R5	0
R4	0
R3	4
R2	1
R1	1

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

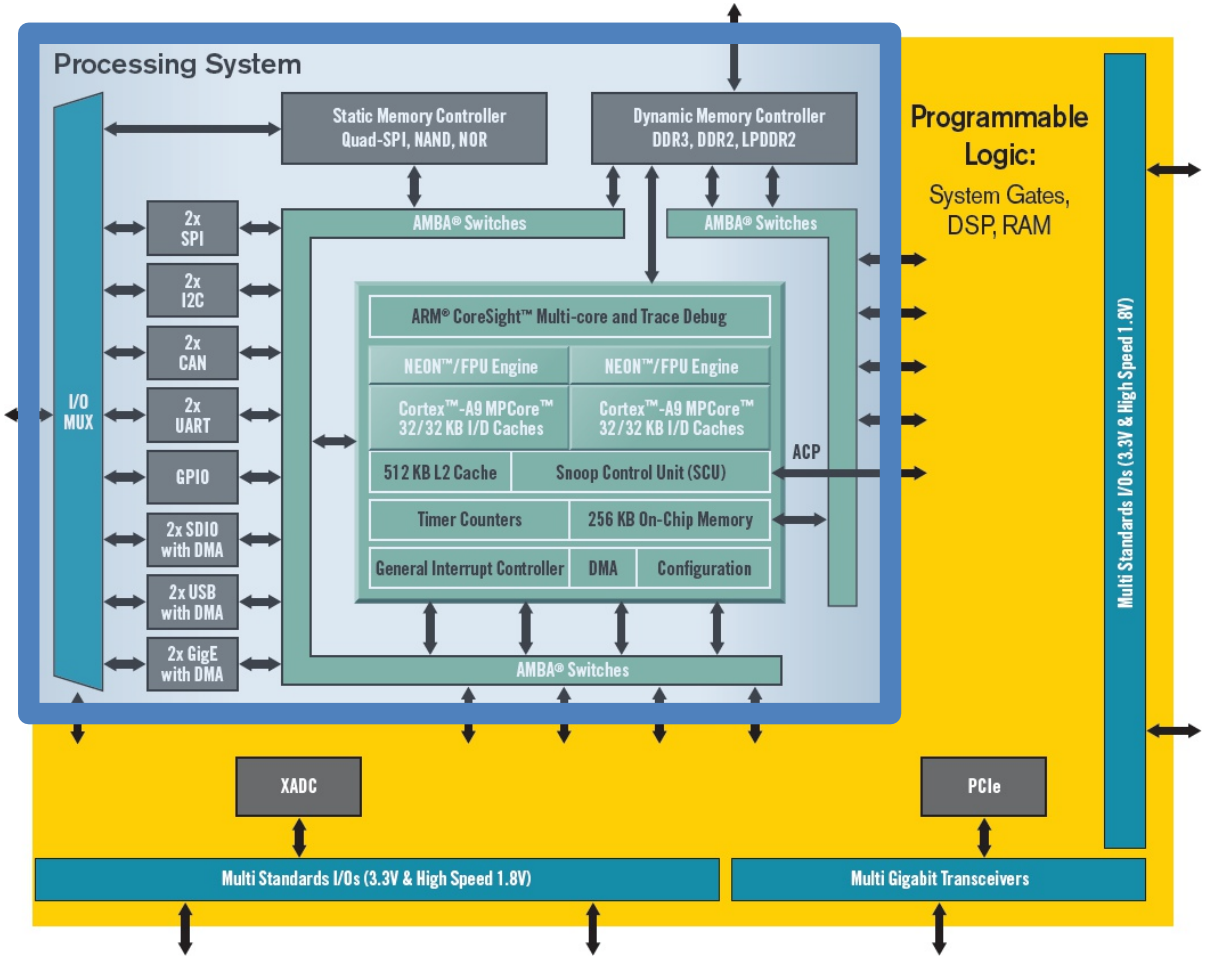


LABORATOIRE HUBERT CURIEN
UMR • CNRS • 5516 • SAINT-ETIENNE

Cibles Intel SoC FPGA et Xilinx Zynq

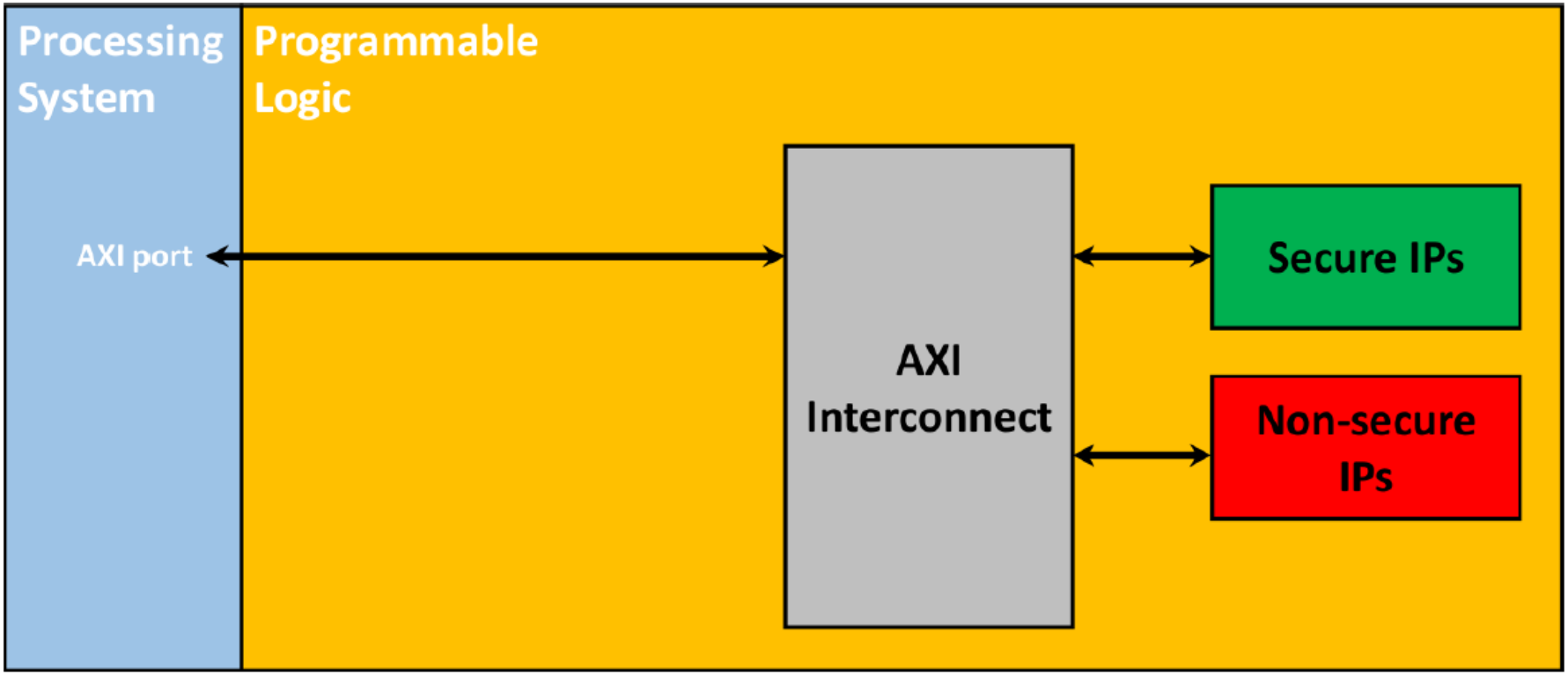
- INTEL SoC
- 9
- Y-A9

Architecture interne d'un SoC hétérogène



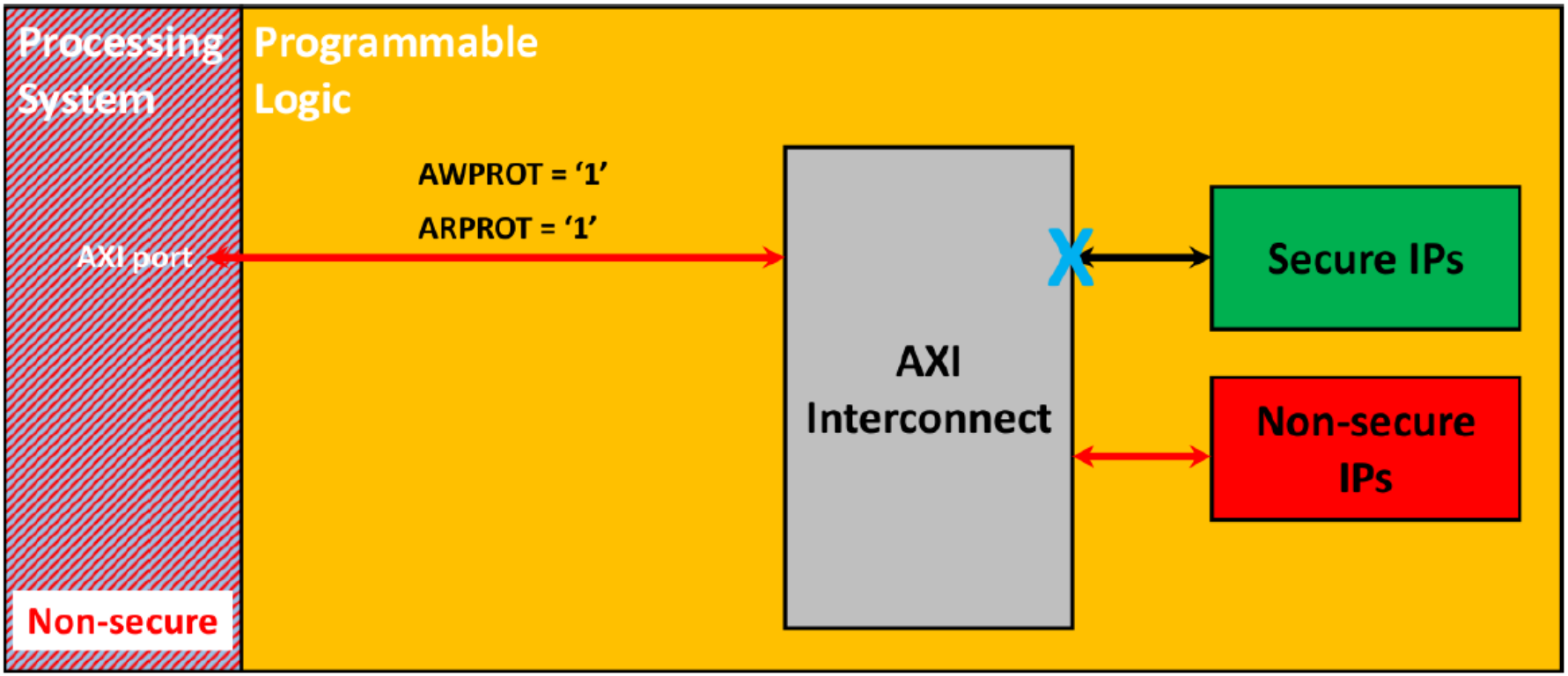
Système cible

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



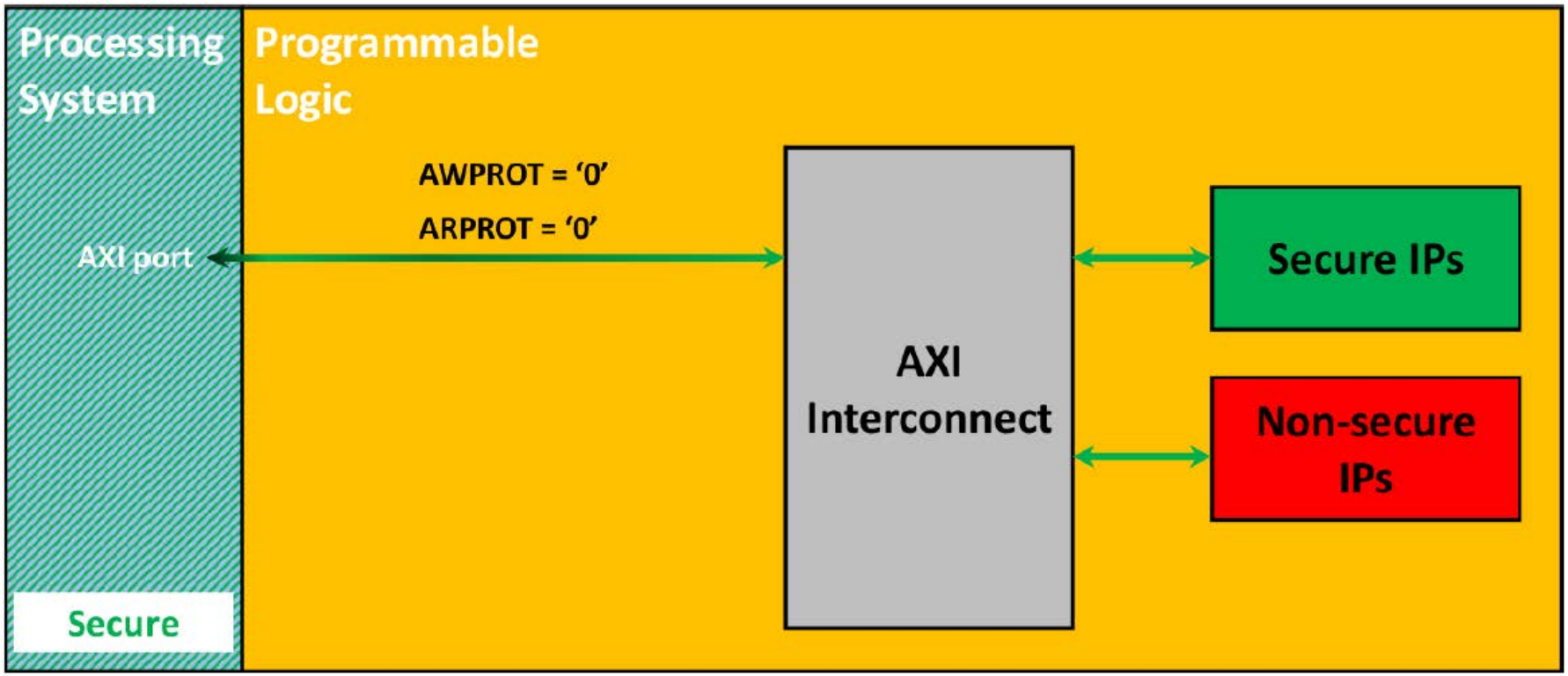
Fonctionnement normal du système (1/2)

- En mode non securisé (REE)



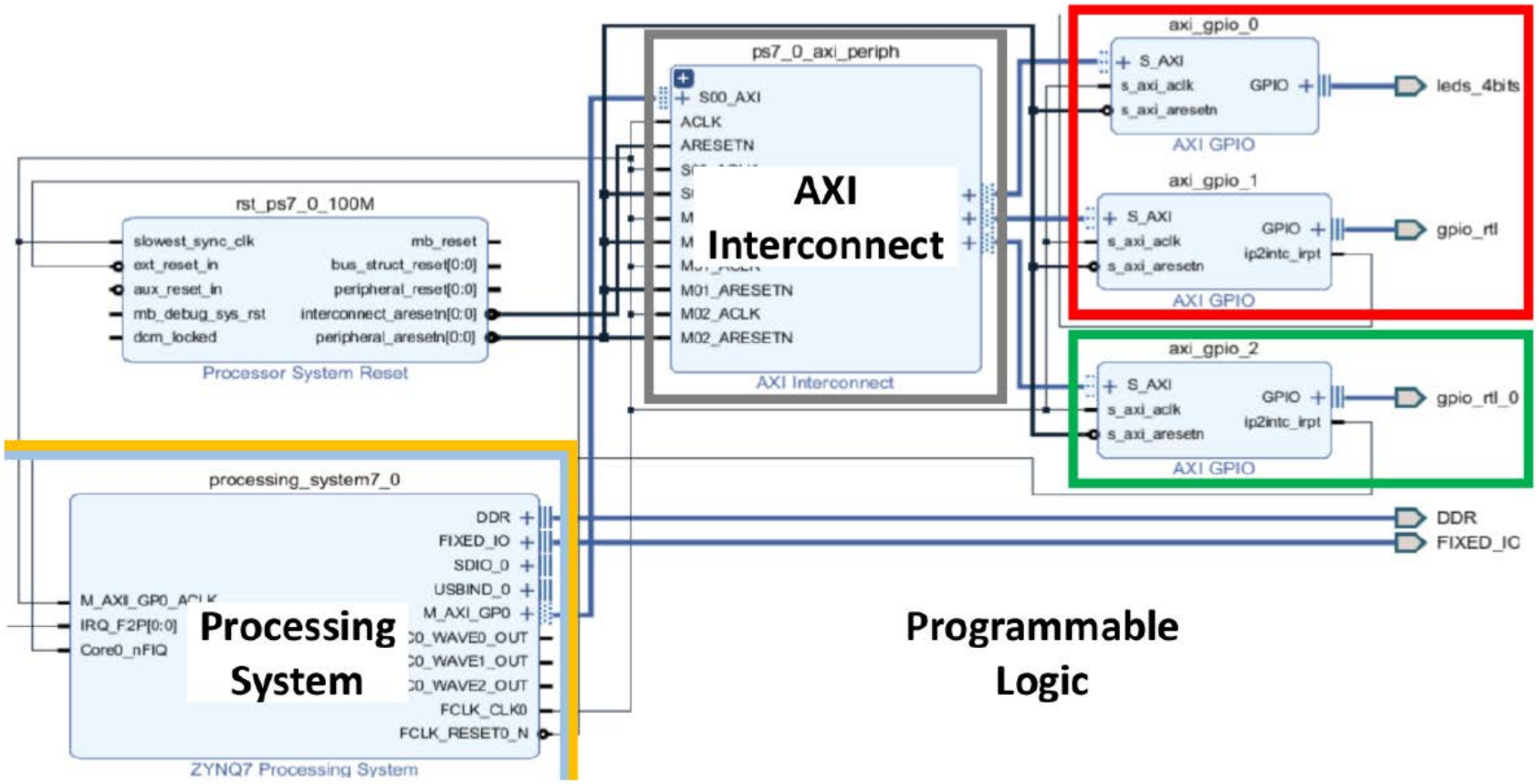
Fonctionnement normal du système (2/2)

- En mode securisé (TEE)

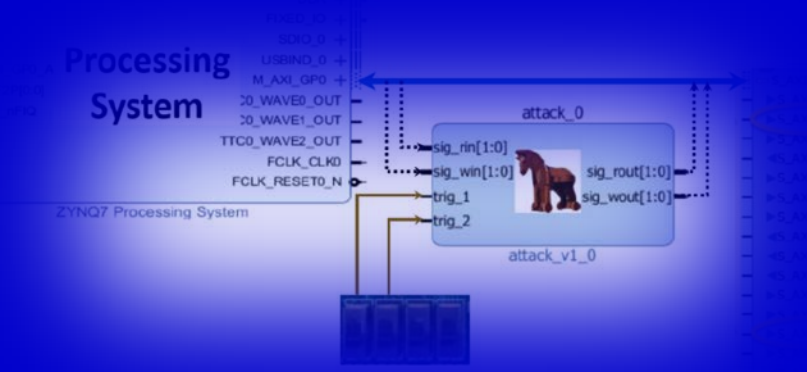


Prototypage (Xilinx Zynq)

- Architecture du système développé (Xilinx Vivado)

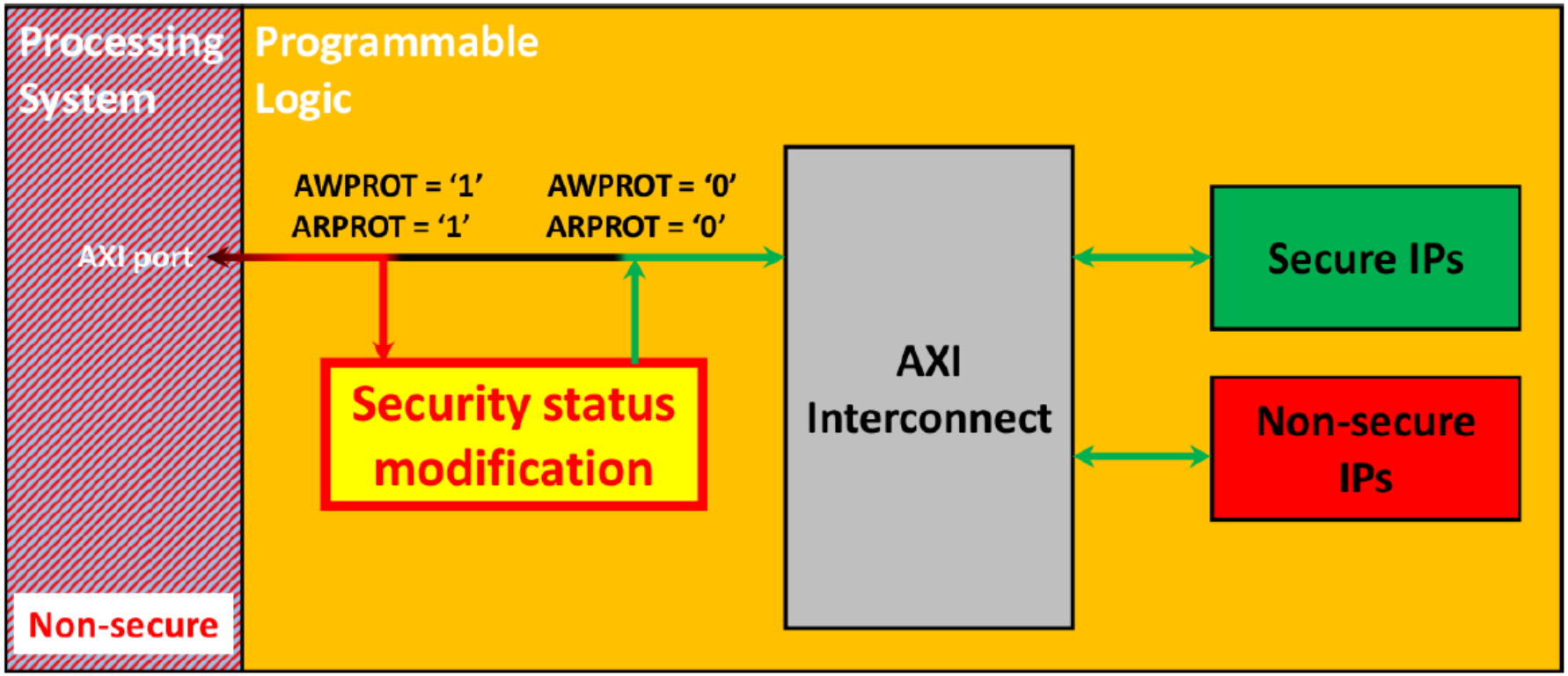


Scénario d'attaques de l'extension de la TrustZone



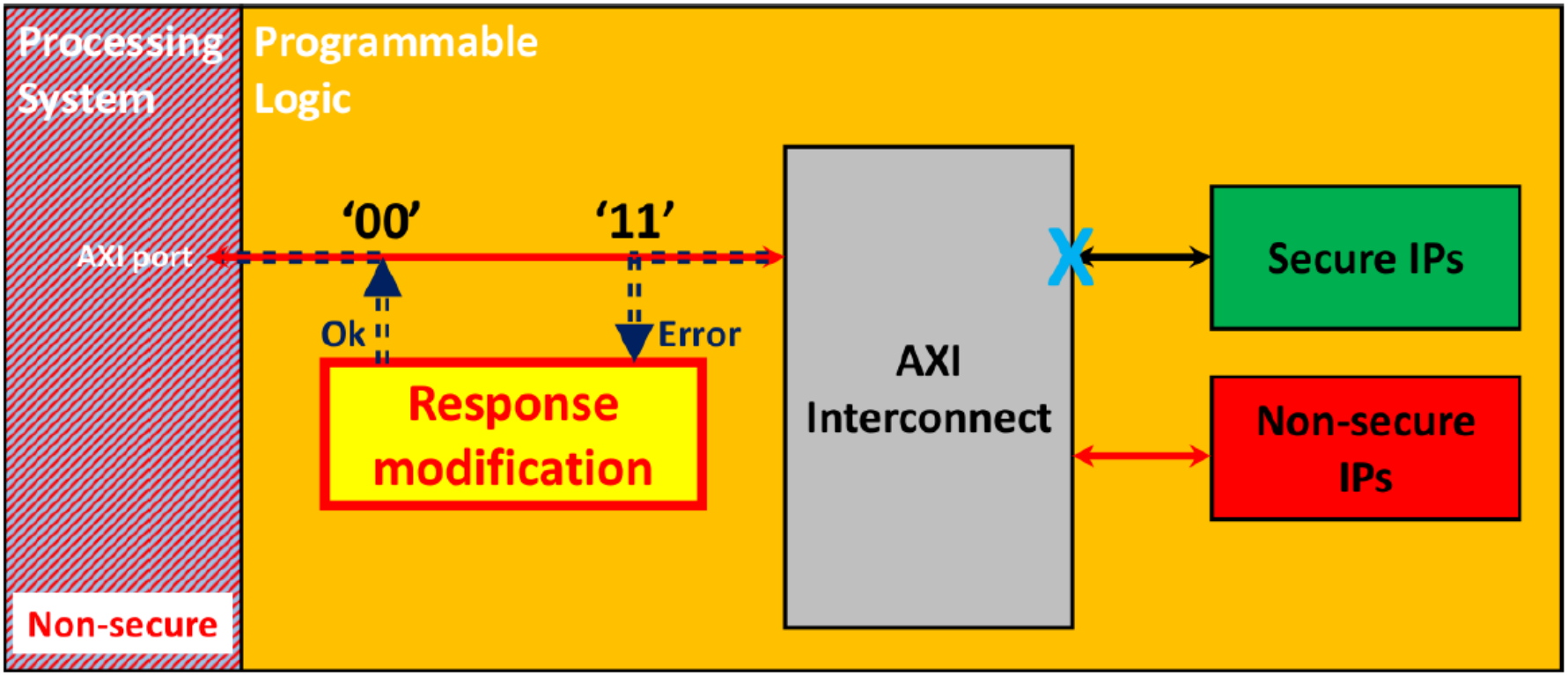
Modification des signaux de contrôle

- Corruption d'AWPROT et ARPROT



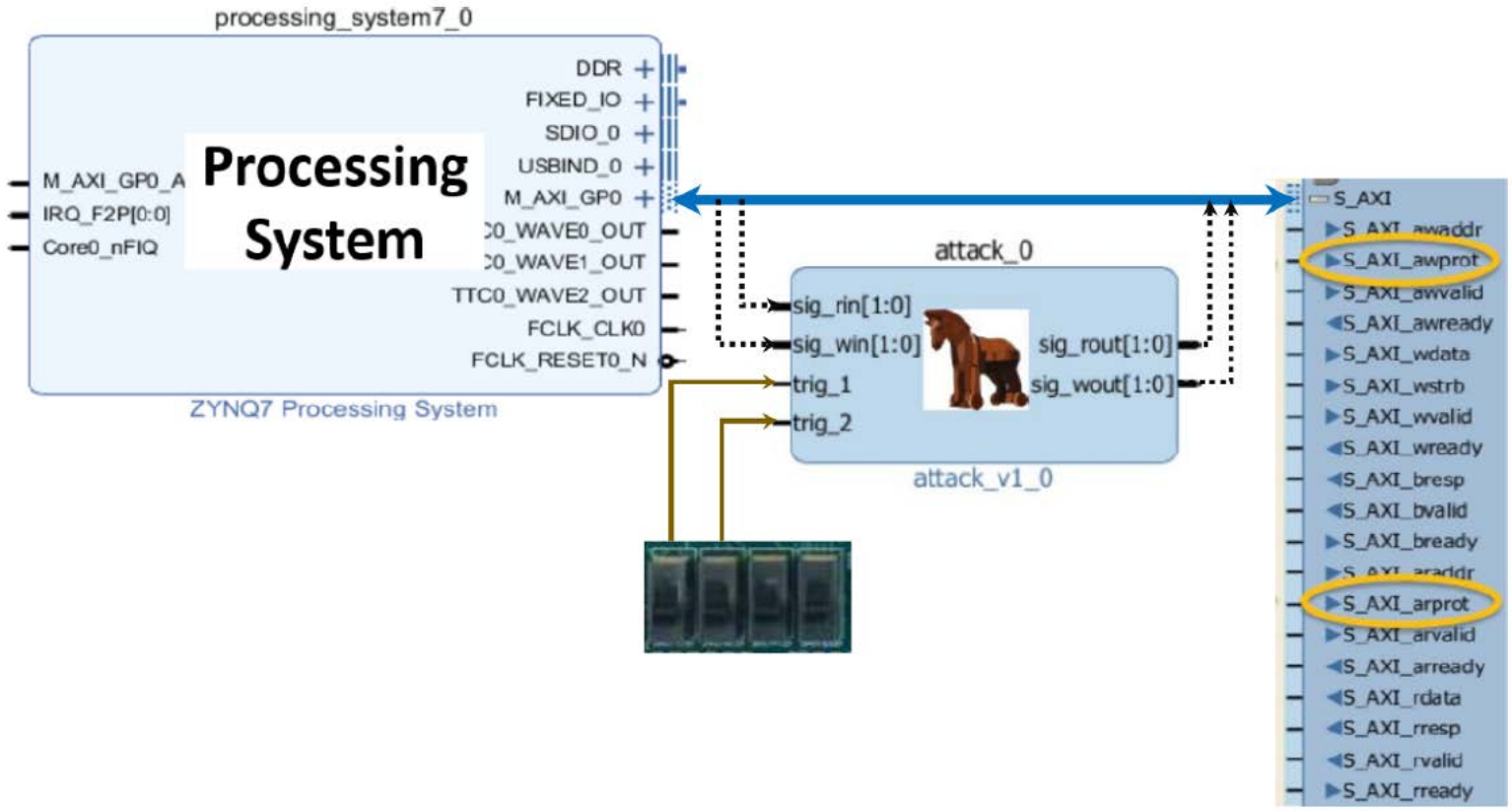
Modification des signaux d'erreur

- Corruption du signal d'erreur



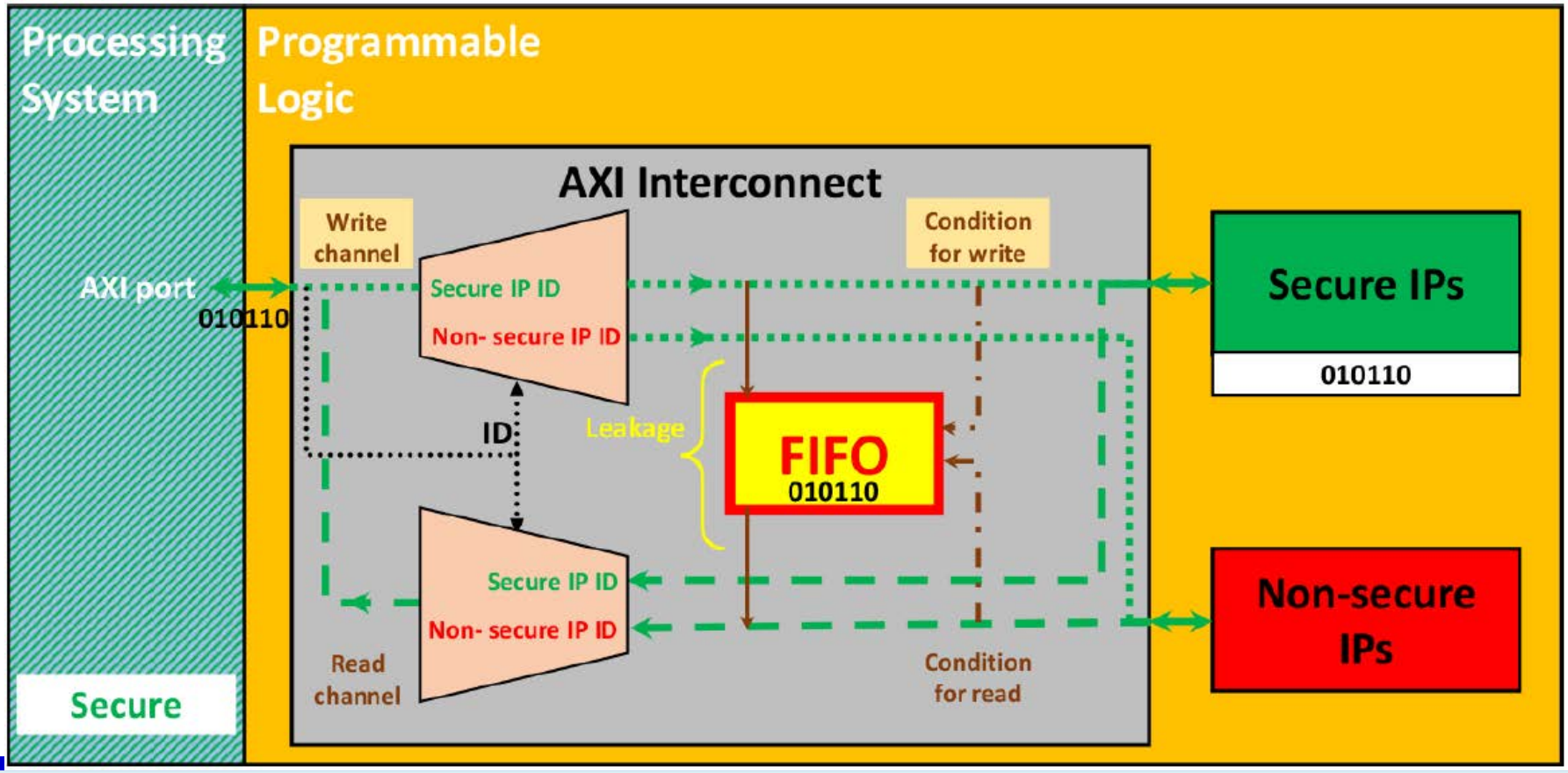
Réalisation (Xilinx Zynq)

- Cheval de Troie matériel



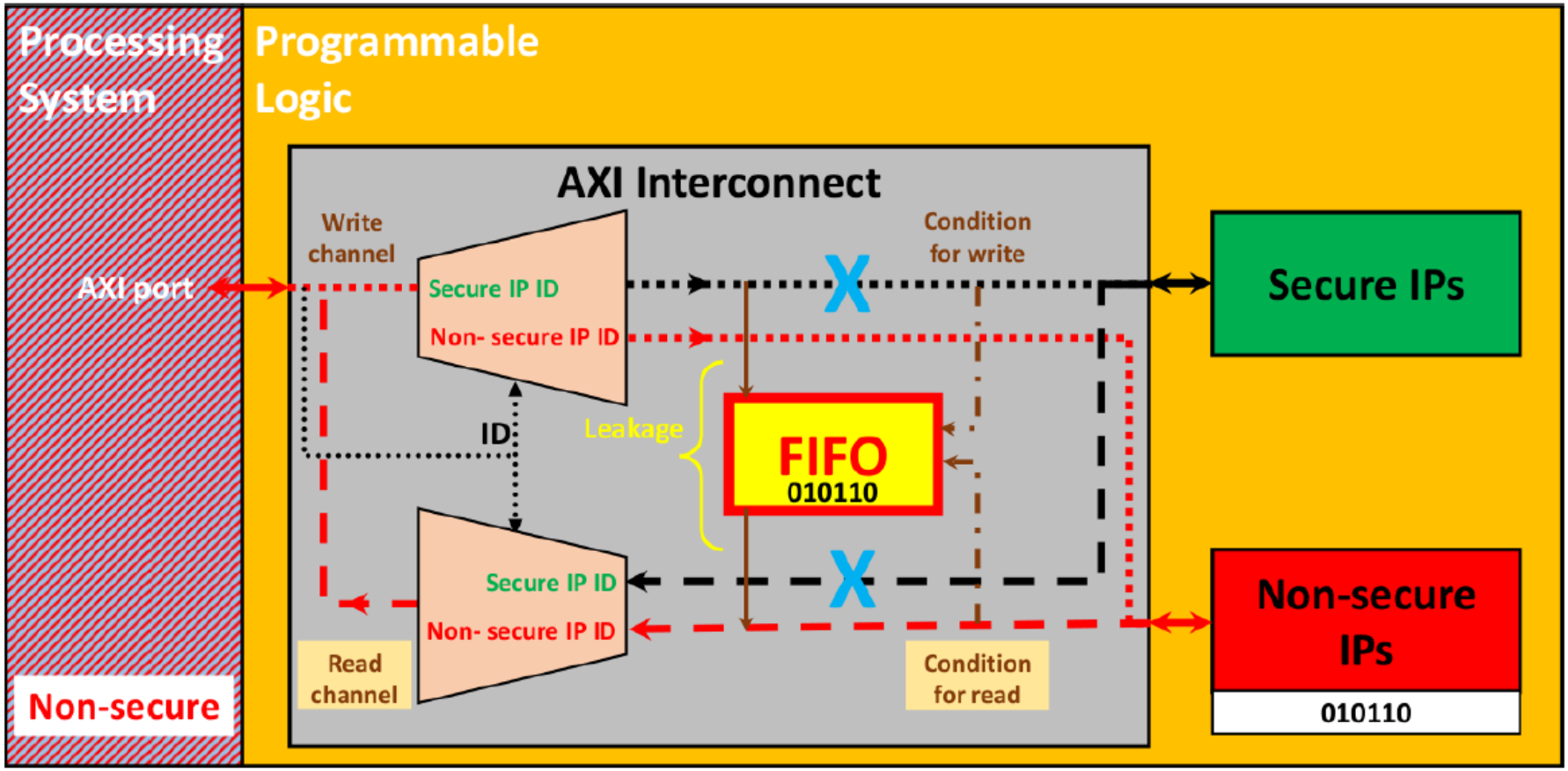
Corruption de l'AXI interconnect

- Mémorisation de l'ID de l'IP sécurisé

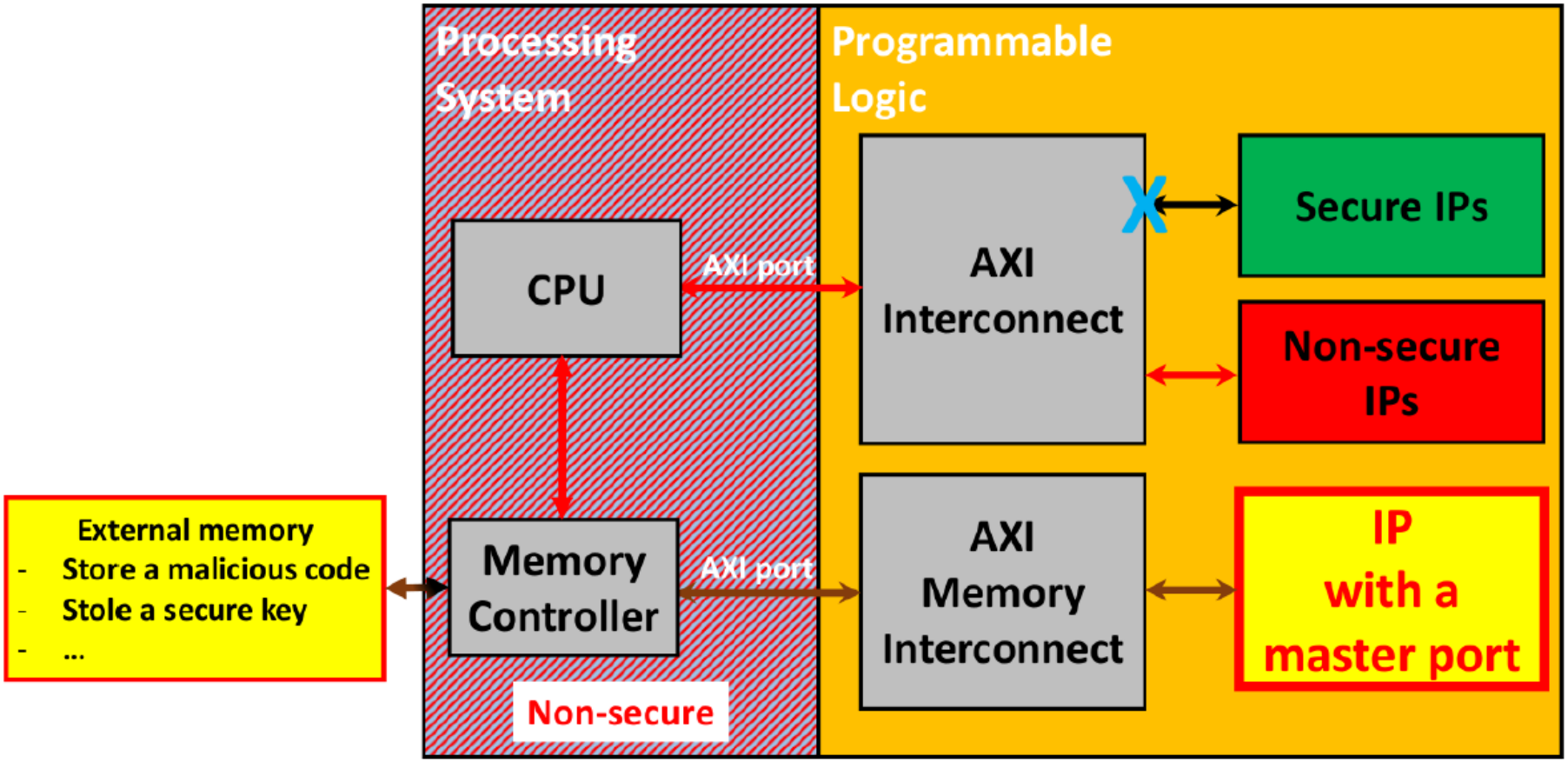


Corruption de l'AXI interconnect

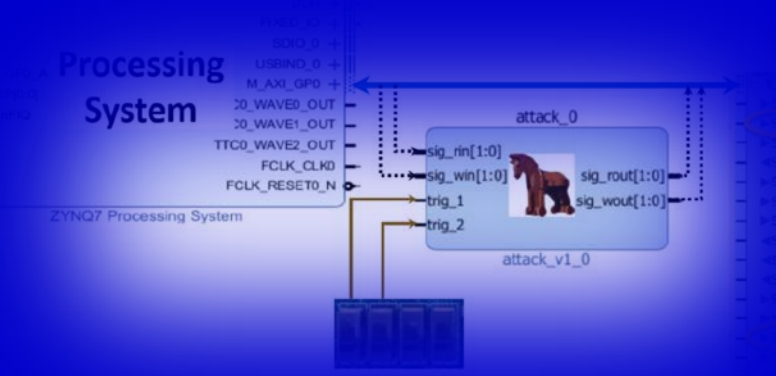
- Récupération d'ID



Accès à la mémoire externe



Démonstration



Conclusion 3/3

- Preuve de concept de plusieurs attaques possibles ciblant l'extension de la TrsutZone 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 TEEMA

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

gemalto security to be free

TRUSTONIC

PHONESEC LA MAÎTRISE DES RISQUES NUMÉRIQUES

MINES Saint-Étienne

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

LIRMM

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

UNIVERSITÉ JEAN MONNET
SAINT-ÉTIENNE

cnrs

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