BITFLIP 2025

Nov 19th 2025

Paul Grandamme

Ph.D. in microelectronics

Fault Injection Attacks on Unpowered Devices

MINES Saint-Étienne
Une école de l'IMT

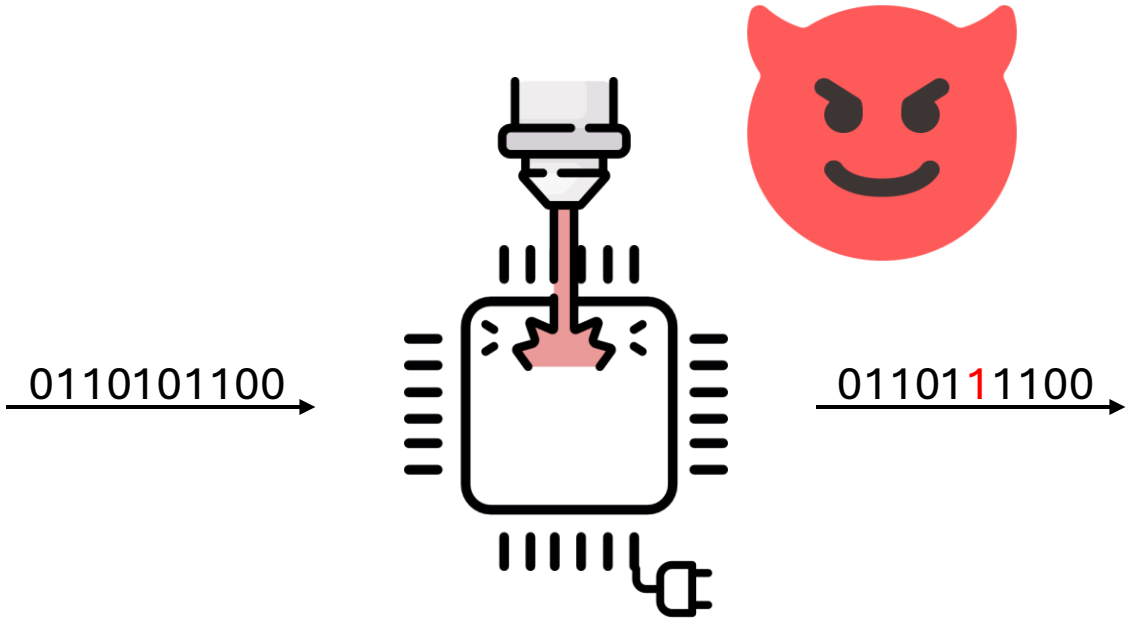
50 years 1976-2026

Laboratoire Hubert Curien
UMR ▪ CNRS ▪ 5516 ▪ Saint-Étienne

Context

State of the art

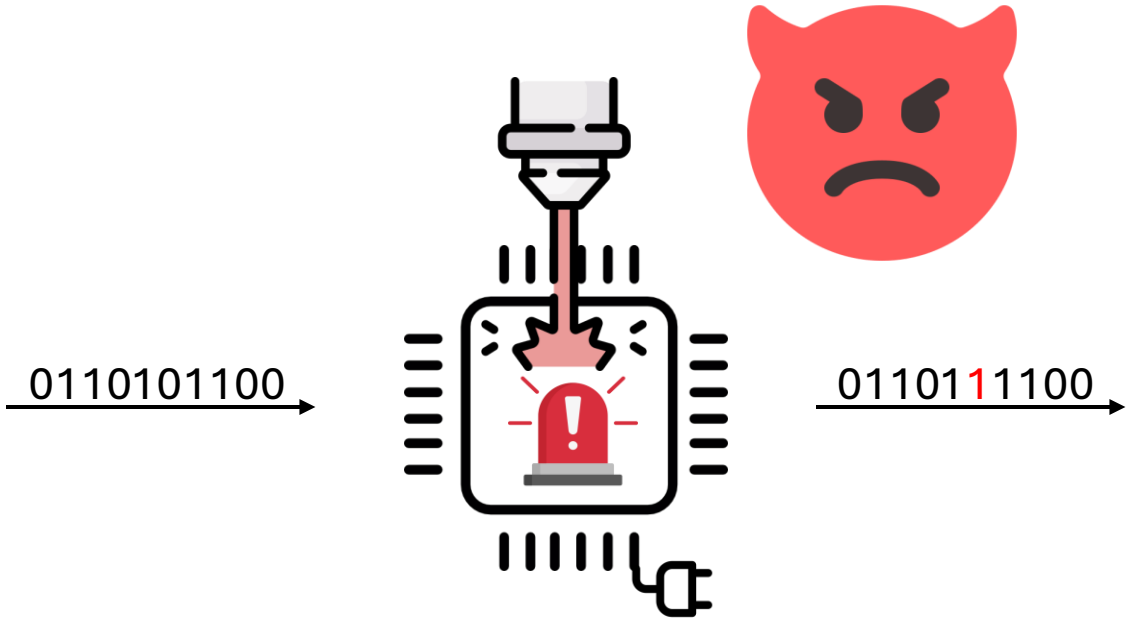
Almost all the attacks performed on powered devices



Context

State of the art

Almost all the attacks performed on powered devices

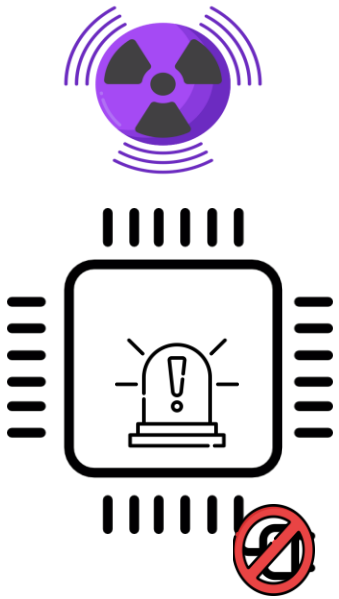


Context

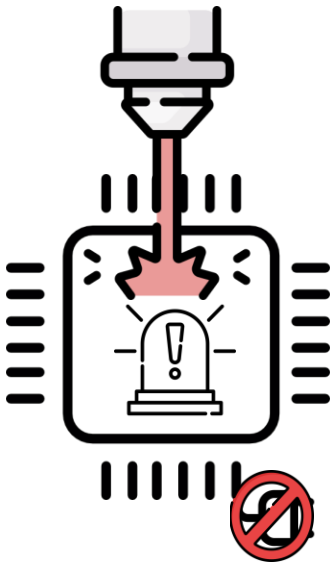
State of the art

Almost all the attacks performed on powered devices

X-Ray



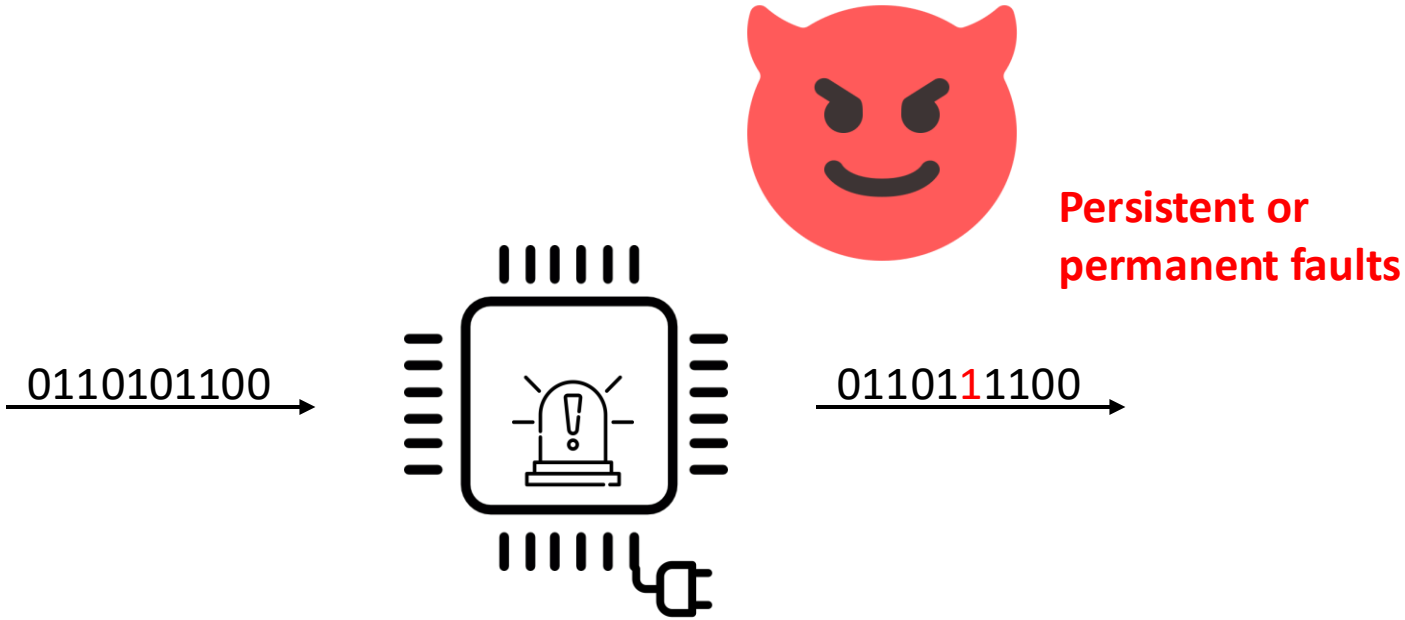
Laser



Context

State of the art

Almost all the attacks performed on powered devices



Context

Problem

How to bypass the sensors?

Solution

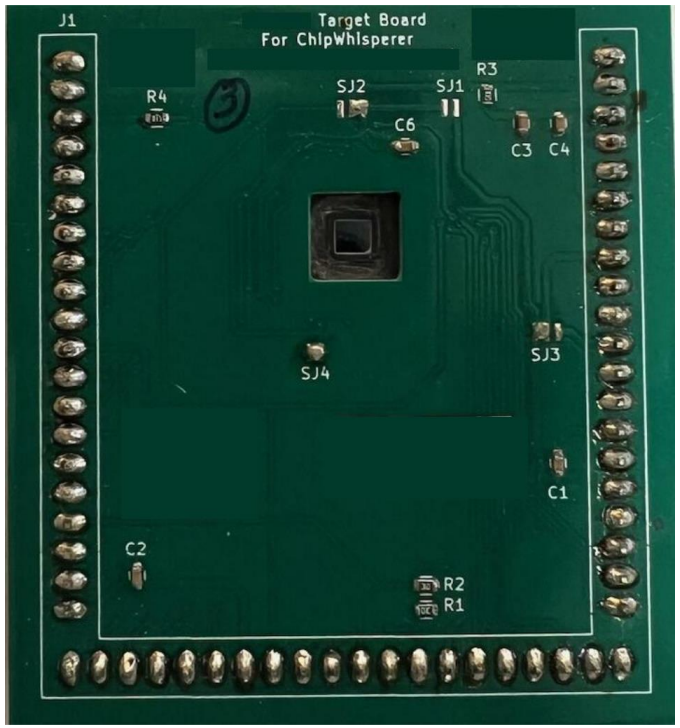
Attack unpowered devices

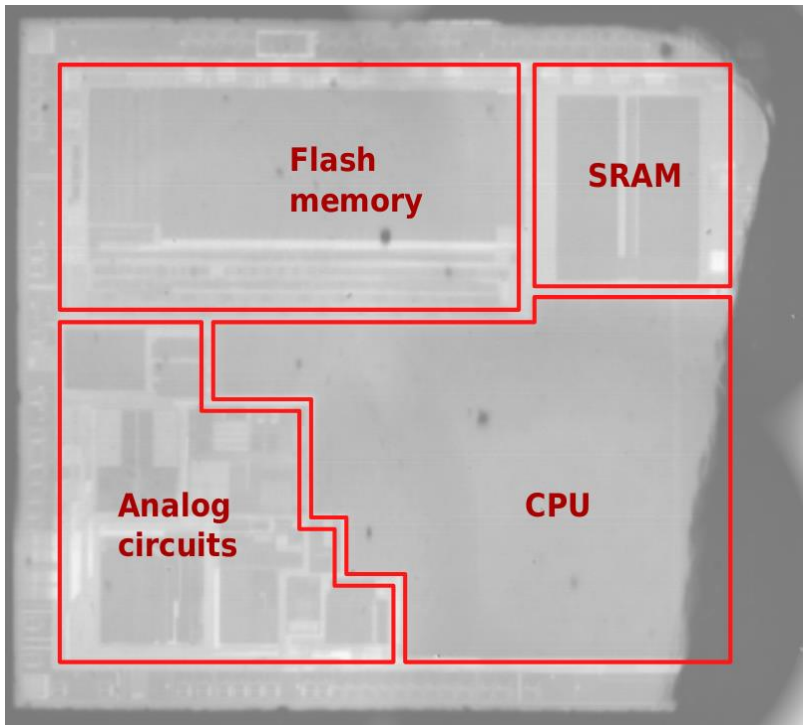
- No detection possible
- No synchronization required

Ideas

- Break the sensors
- Corrupt stored information: Non-Volatile Memories (Flash)

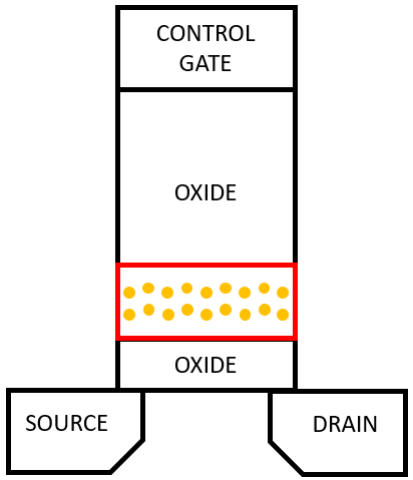
Hardware target



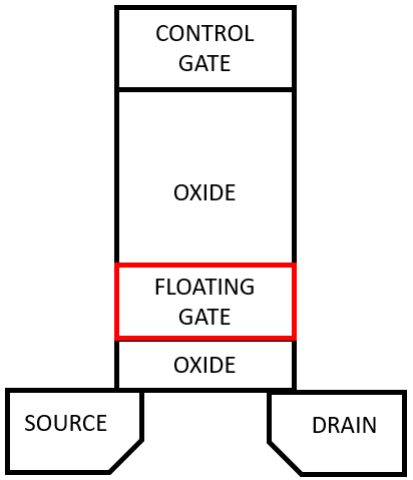


- STM32F1 open on the backside (32-bit microcontroller)
- 128 kB of Flash memory (128 pages of 1 kB)

Floating gate transistors in Flash memories



Charged cell

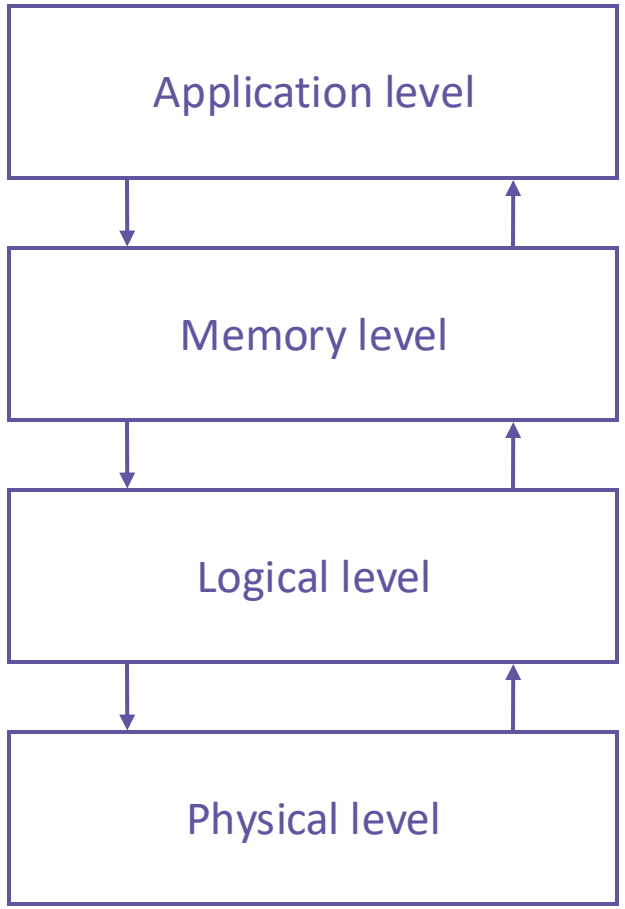


Discharged cell

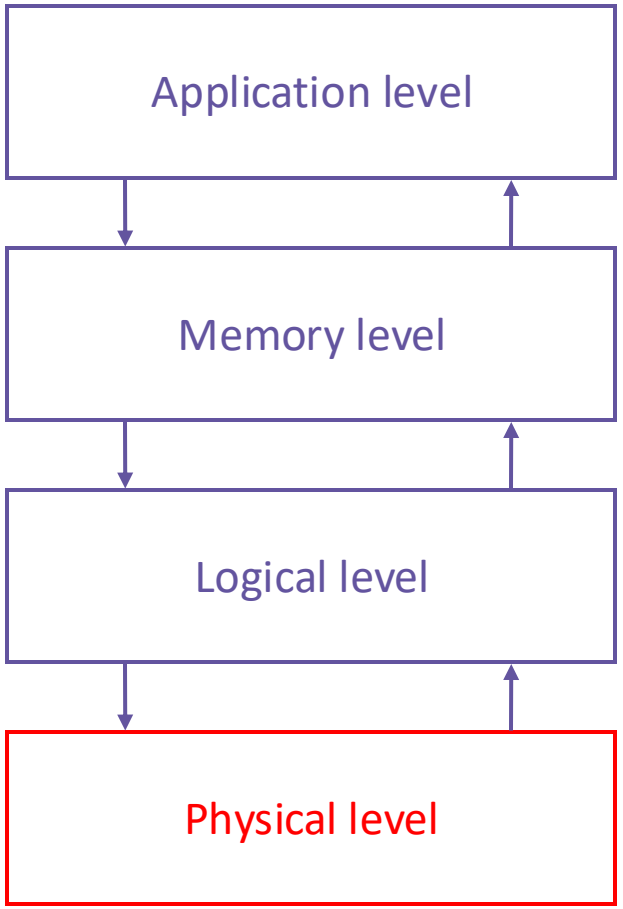
Convention:

- Charged = '0'
- Discharged = '1'

Abstraction levels

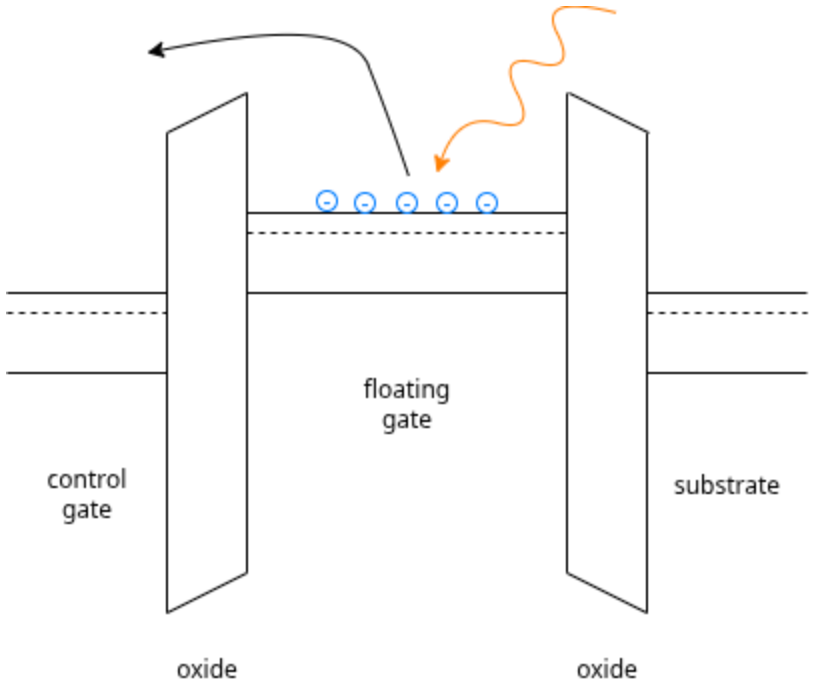


Abstraction levels



X-Ray Fault Injection

Total Ionizing Dose effect on FGmos[1]



Photoemission effect

Three different mechanims:

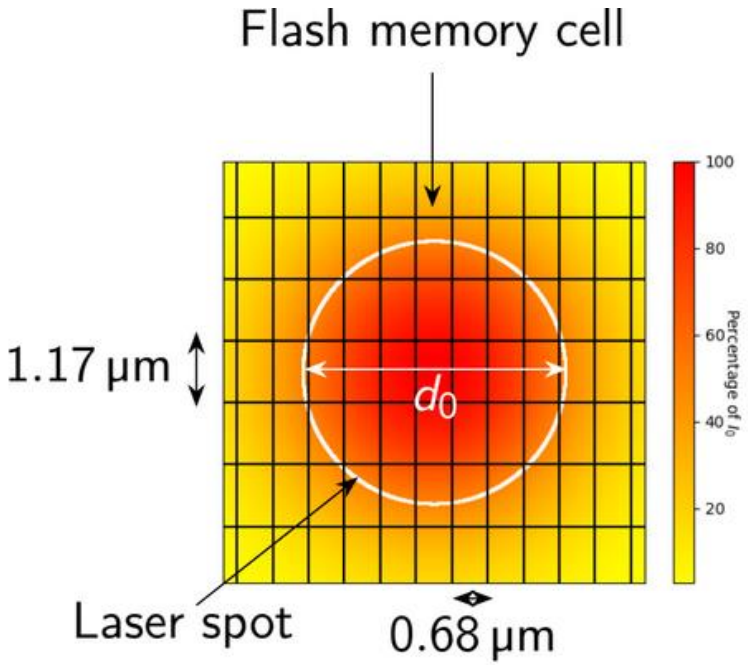
- Electron/hole pair generation in the oxides
- Charge trapping in the oxides
- Photoemission

[1]Gerardin et al., "Radiation Effects in Flash Memories", IEEE Transactions on Nuclear Sciences 2013

Laser Fault Injection

Temperature effect on FGmos

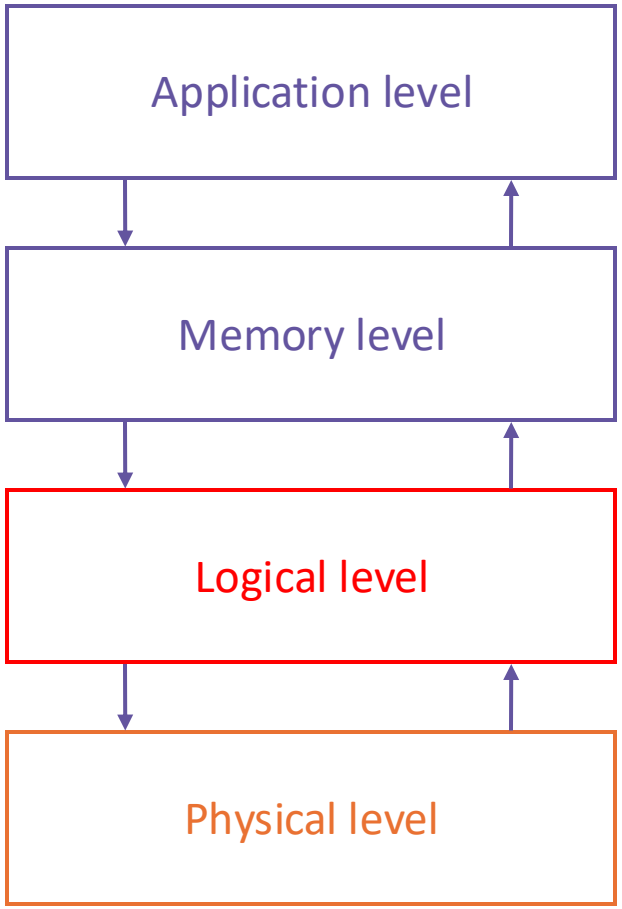
- Laser beam energy → Temperature increase → Floating gate discharge[2]



Heatmap induced by the laser exposition (d_0=5µm)

[2]Sands, "Pulsed laser heating and melting", Heat Transfer: IntechOpen 2011

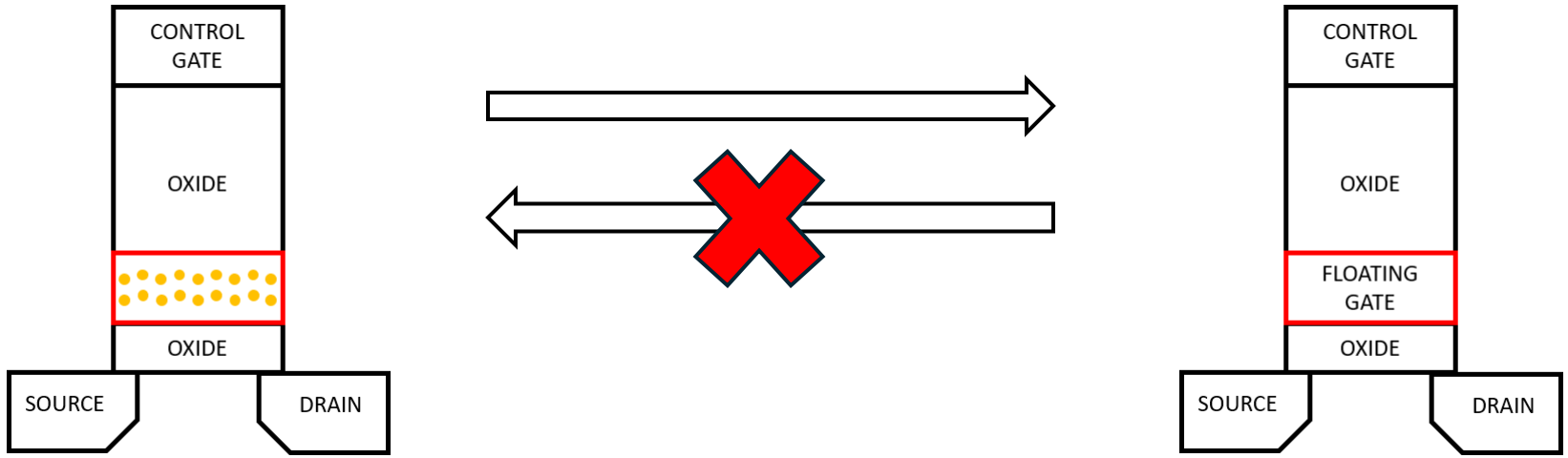
Abstraction levels



Floating gate transistors discharge by photoemission or heating

Abstraction levels : Logical level

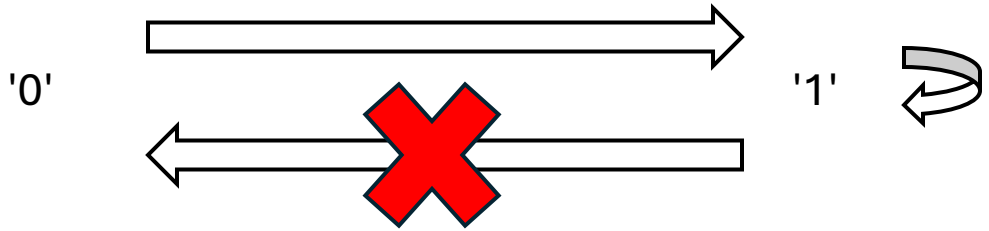
- From the physical level:



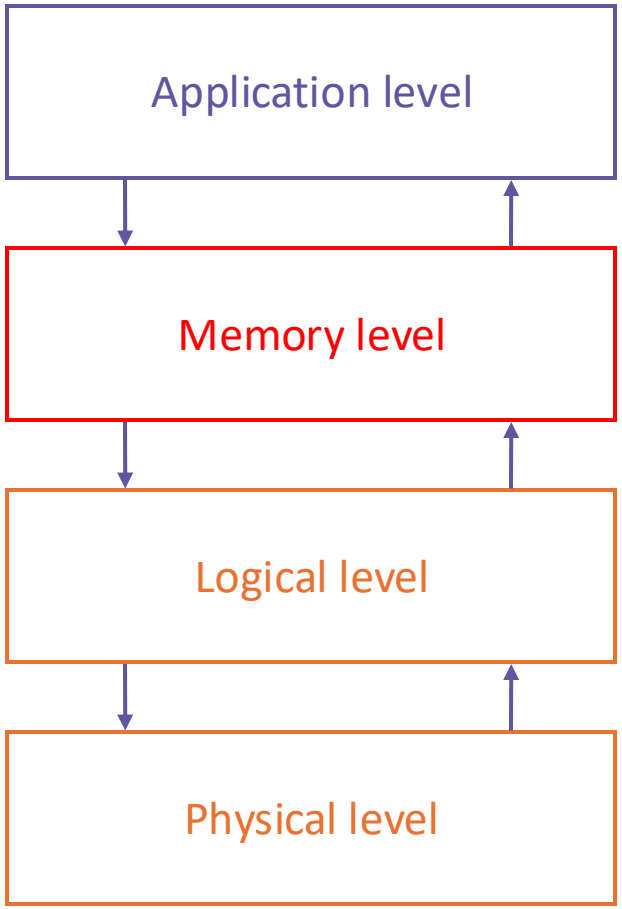
Charged cell

Discharged cell

- To the logical level:



Abstraction levels



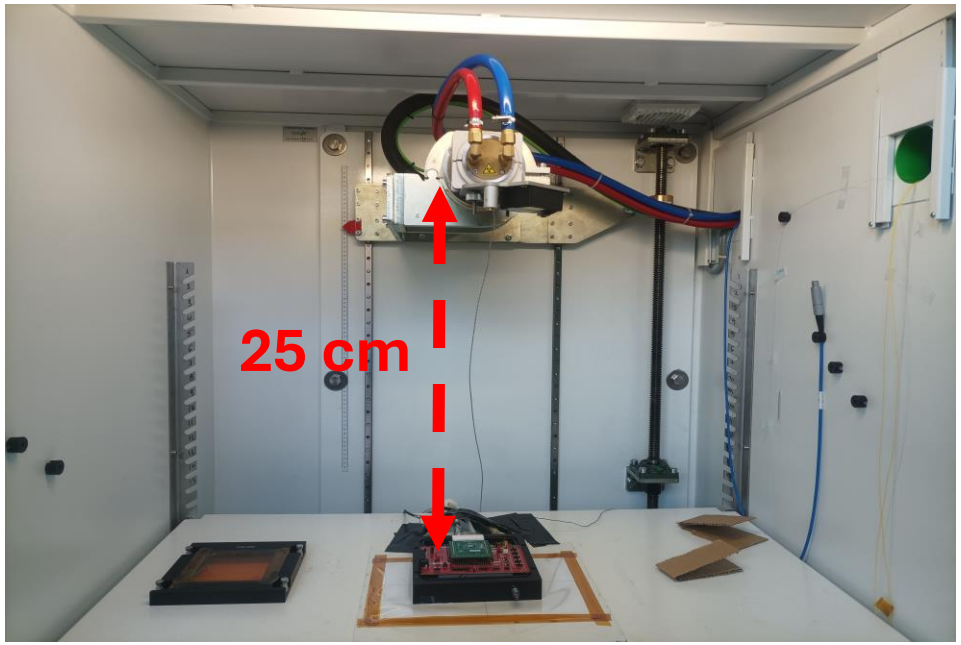
Bitsets ('0'→ '1')

Floating gate transistors discharge by photoemission or heating

X-Ray Fault Injection

Experimental setup

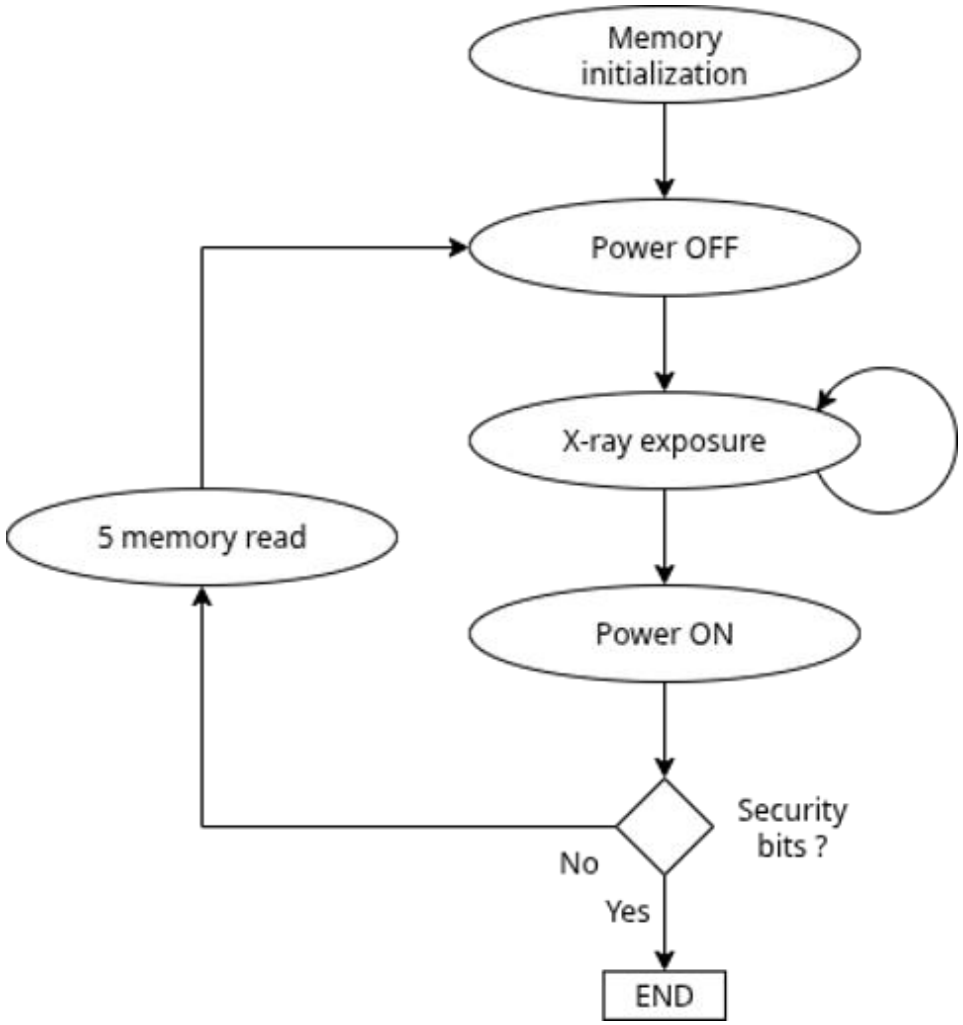
LABORATOIRE HUBERT CURIEN
UMR • CNRS • 5516 • SAINT-ETIENNE



⚠ **The entire target is irradiated !**

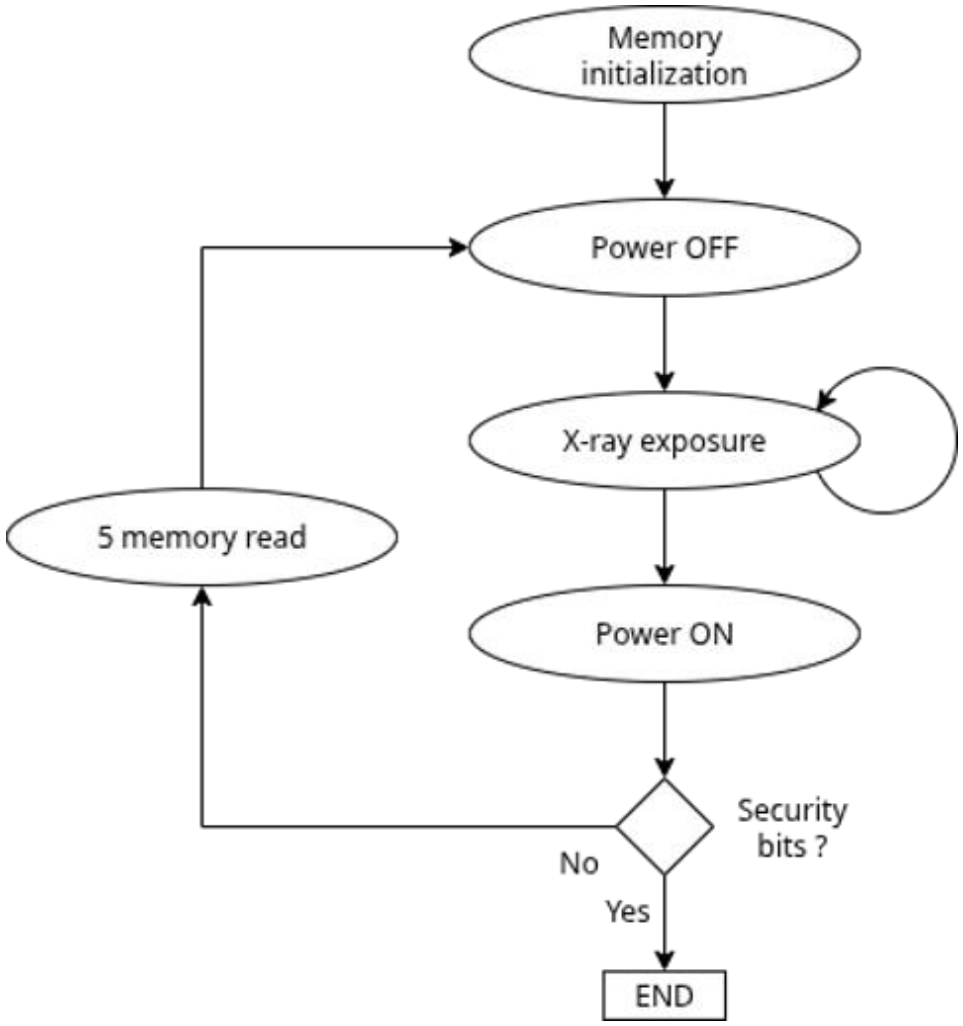
X-Ray Fault Injection

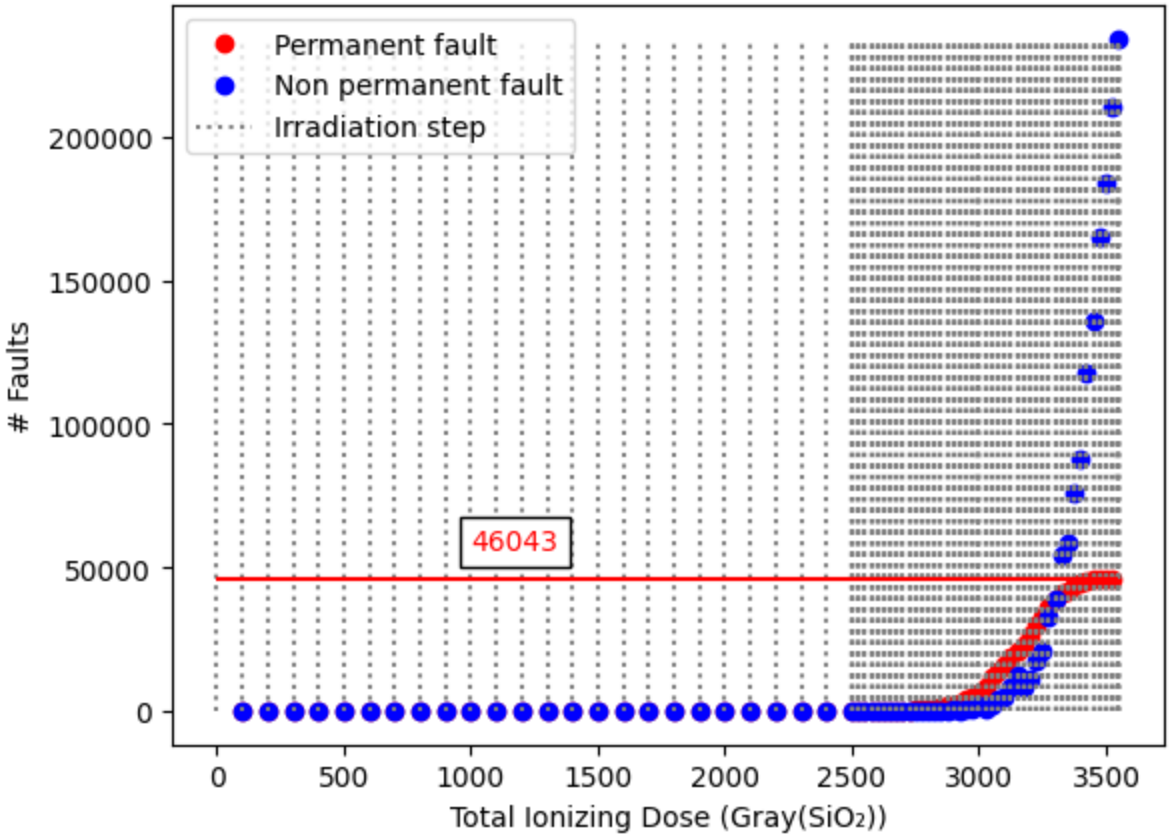
Results

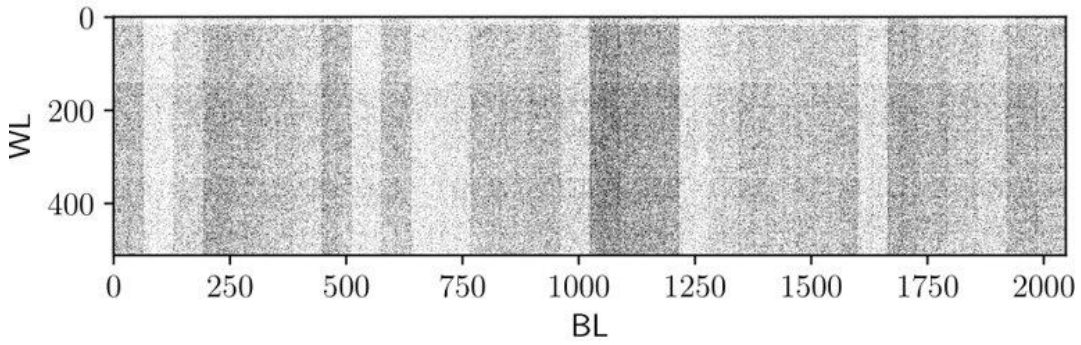


X-Ray Fault Injection

Results







X-Ray Fault Injection

Synthesis

Fault mechanism
• Floating gate transistors discharge by photoemission

X-Ray Fault Injection

Synthesis

Fault mechanism

- Floating gate transistors discharge by photoemission

Limitations

- Faults injected but not localized, therefore non exploitable

X-Ray Fault Injection

Synthesis

Fault mechanism

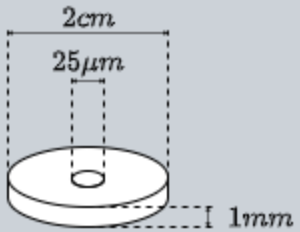
- Floating gate transistors discharge by photoemission

Limitations

- Faults injected but not localized, therefore non exploitable

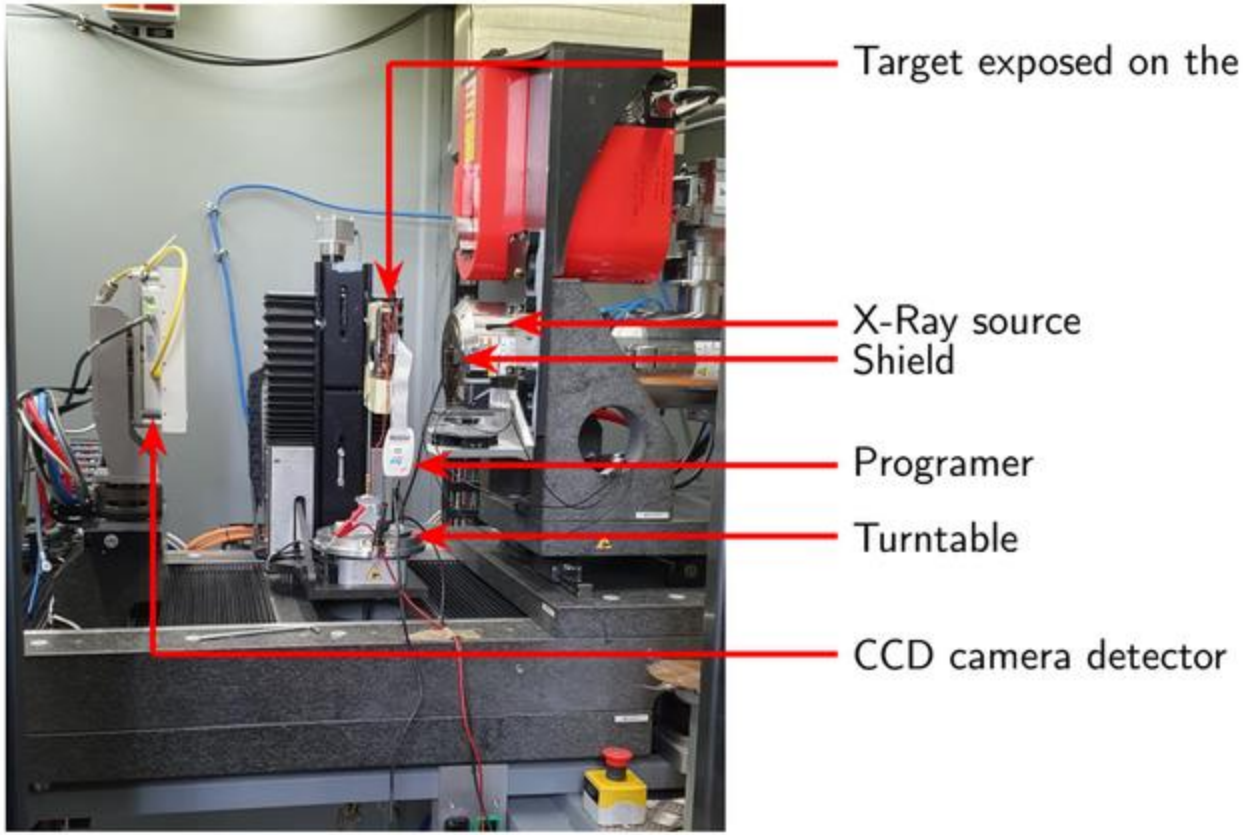
Design of a focalization shield

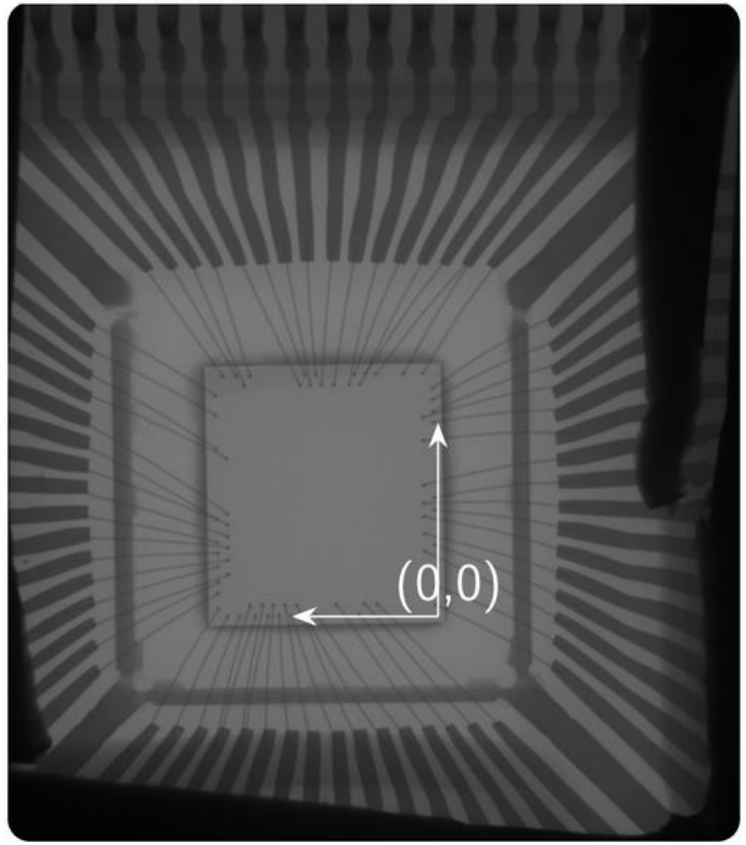
- Tungsten (W)



X-Ray Fault Injection

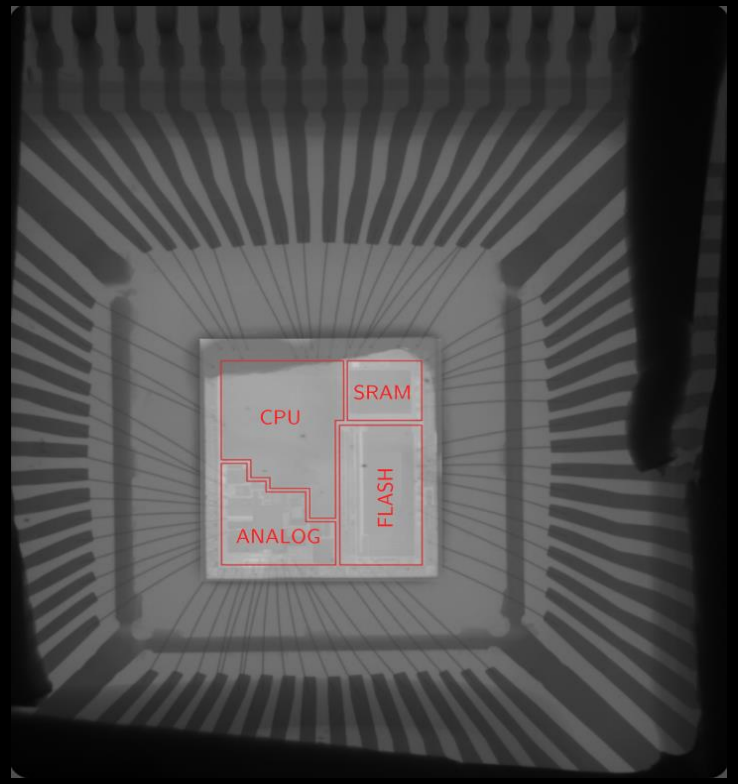
Experimental setup

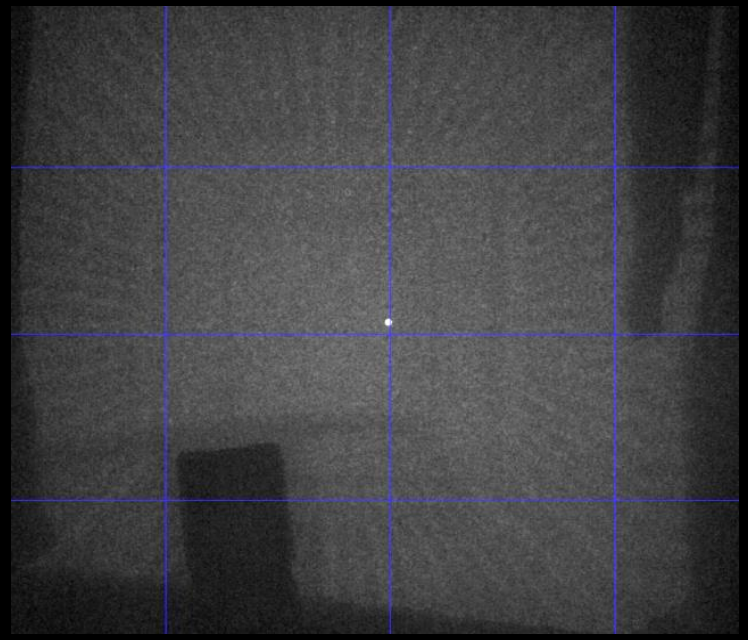




X-Ray Fault Injection

Obtained pictures



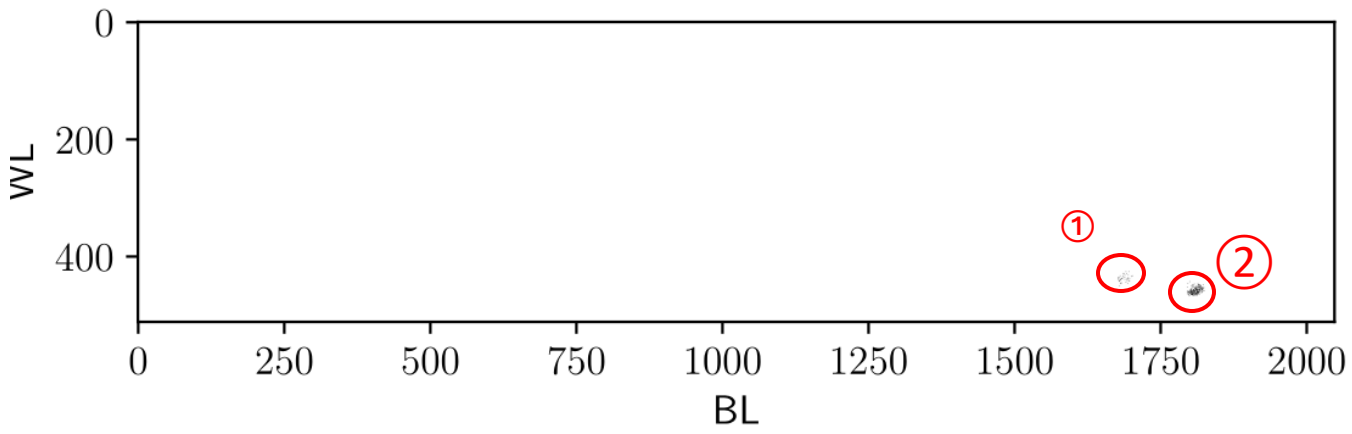


X-Ray Fault Injection

Results

2 different positions:

- Position ① : (0.6 mm,1.1 mm) ⇒ 1h of irradiation
- Position ② : (0.6 mm,1.2 mm) ⇒ 2h15 of irradiation



Results

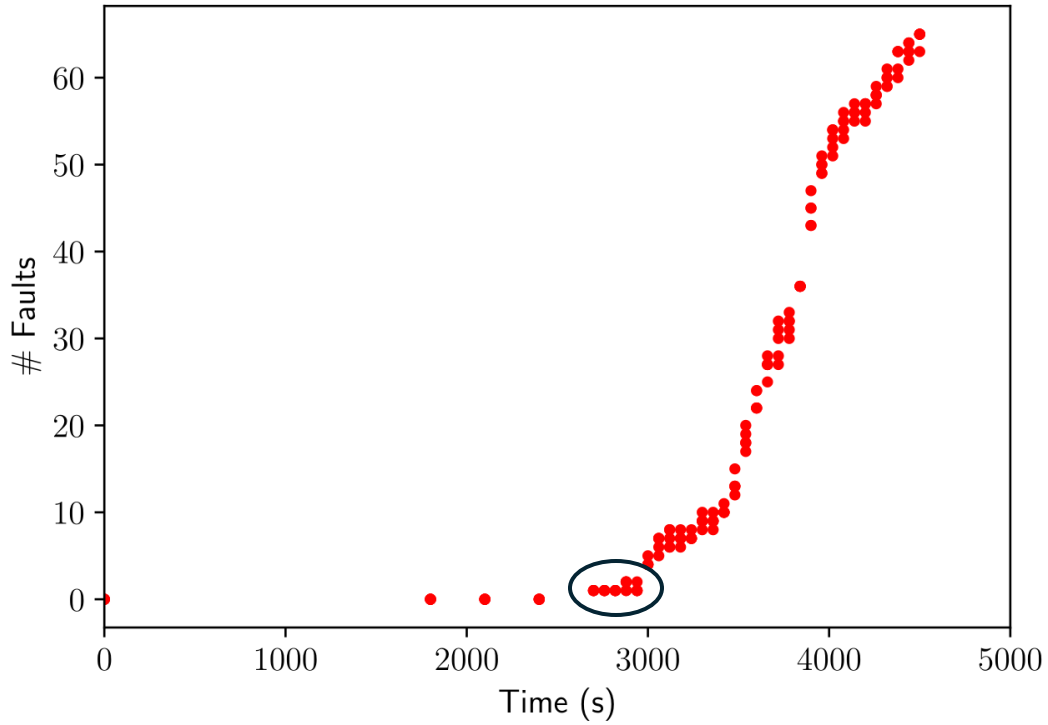
- Position ①: ≃ 70 localized faults
- Position ②: ≃ 300 localized faults

X-Ray Fault Injection

Results

Position ①:

- (0.6 mm,1.1 mm) ⇒ 1h of irradiation ⇒ ≃ 70 localized faults

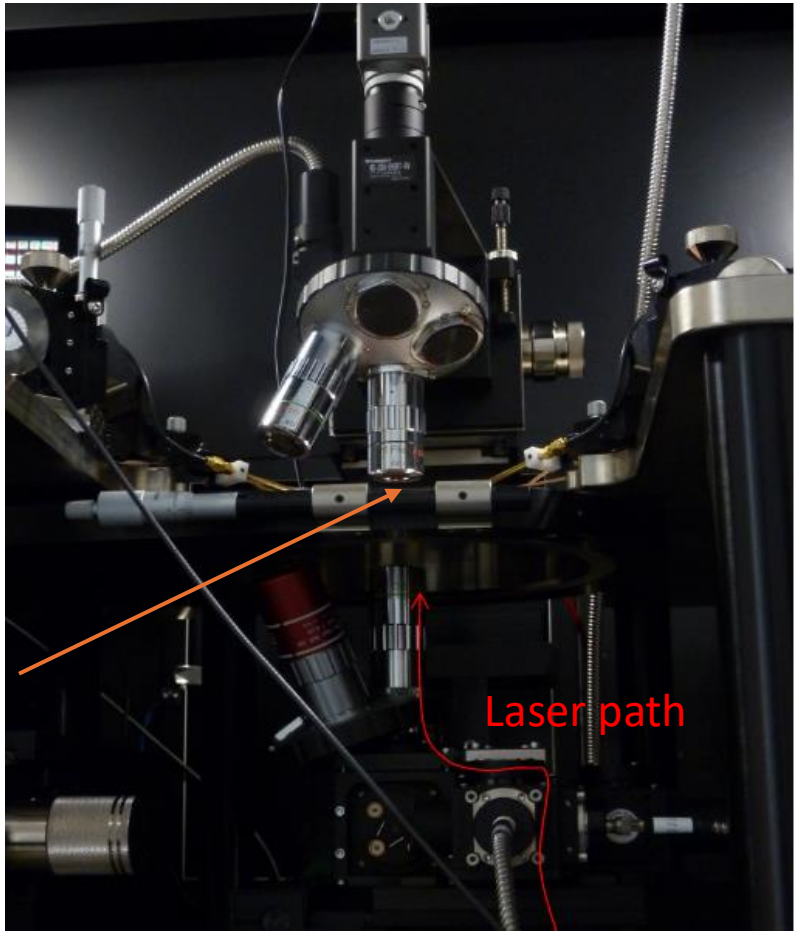


Results

Only few faulty bits for a given exposure time!

Laser Fault Injection

Experimental setup



- 1,064 nm laser source (near-IR)
- 5 µm spot with a x20 magnifying lens
- Backside view with an IR camera
- Same setup as usual powered LFI

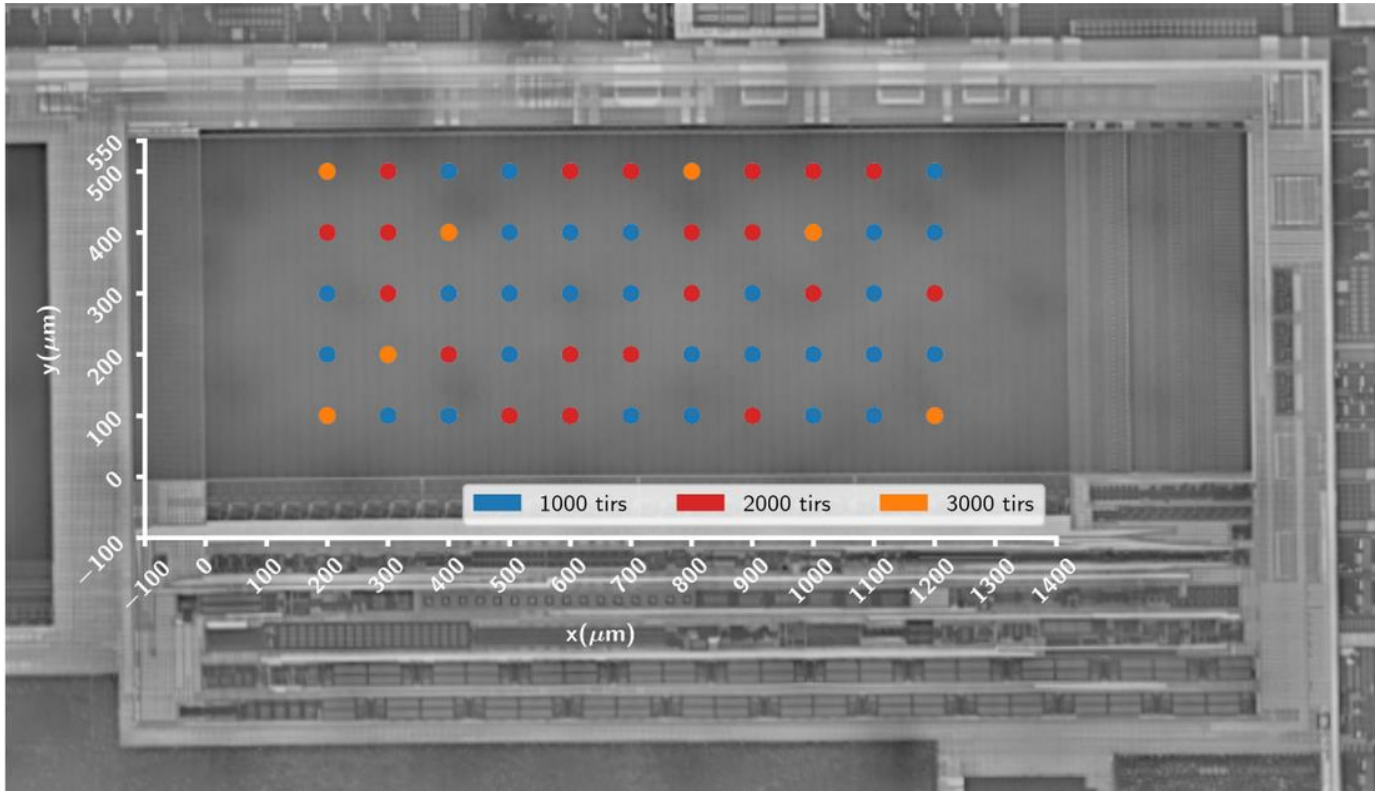
MINES Saint-Étienne
Une école de l'IMT

European Cyber Week

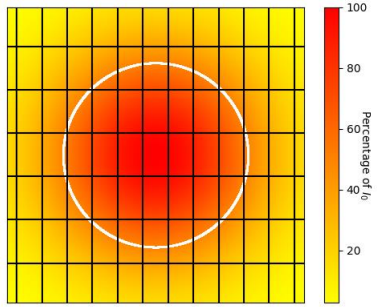
Laser Fault Injection

Results

- Memory initialized to 0x00000000 before laser exposure



- Reverse engineering of the Flash memory mapping possible



- Single bit faults in 33%
- 2.2 faulty bits on average

Laser Fault Injection

Abstraction levels : Memory level

Code corruption (ARMv7 ISA)

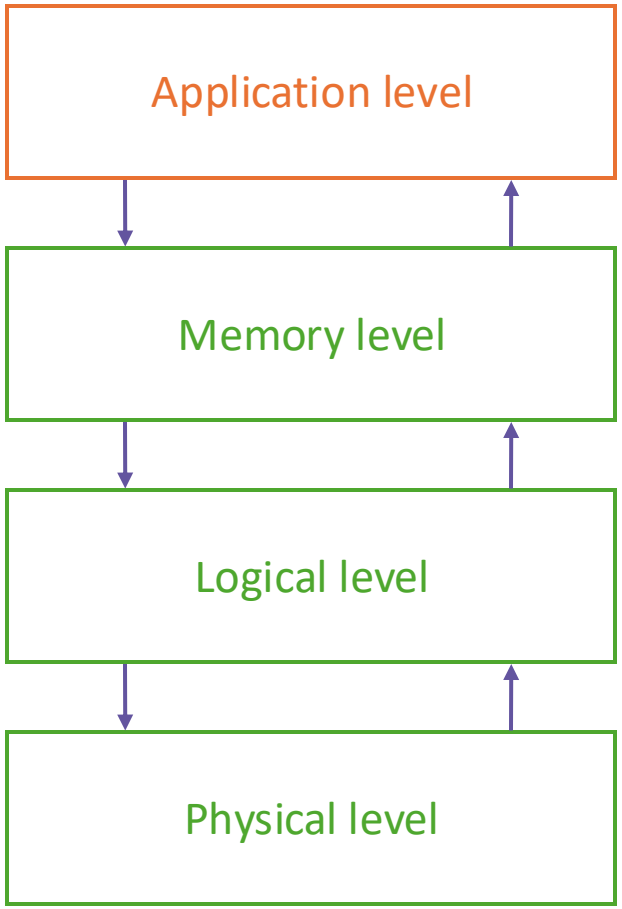
31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Generic MOVW																															
1	1	1	1	0	i	1	0	0	1	0	0	imm4				0	imm3			Rd				imm8							
MOVW,R0,0																															
1	1	1	1	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
MOVW,R0,4																															
1	1	1	1	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
MOVW,R1,0																															
1	1	1	1	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
MOVT,R0,0																															
1	1	1	1	0	0	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Example of possible corruptions on a MOVW instruction[3]

- Also possible to corrupt permanent data

[3]Colombier et al., "Laser-induced Single-bit Faults in Flash Memory: Instructions Corruption on a 32-bit Microcontroller", IEEE HOST 2019

Abstraction levels



Code or data corruption

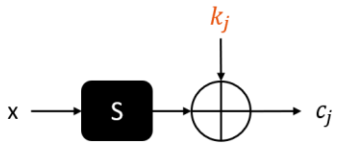
Bitsets ('0'→ '1')

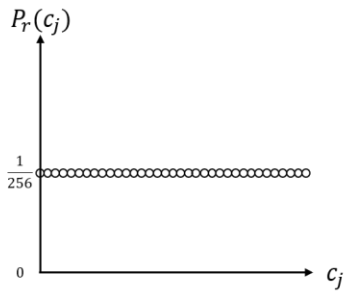
Floating gate transistors discharge by photoemission or heating

Laser Fault Injection

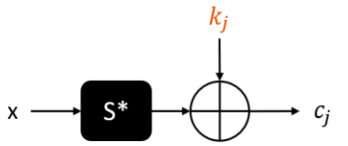
Abstraction levels : Application level

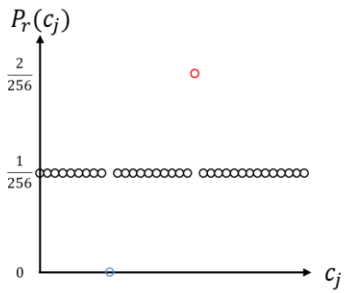
- Persistent Fault Analysis[4] (PFA)
- Persistent fault injection on the S-Box (AES, DES, ASCON,…)
- Statistical study on the bytes of the ciphertexts





Without fault





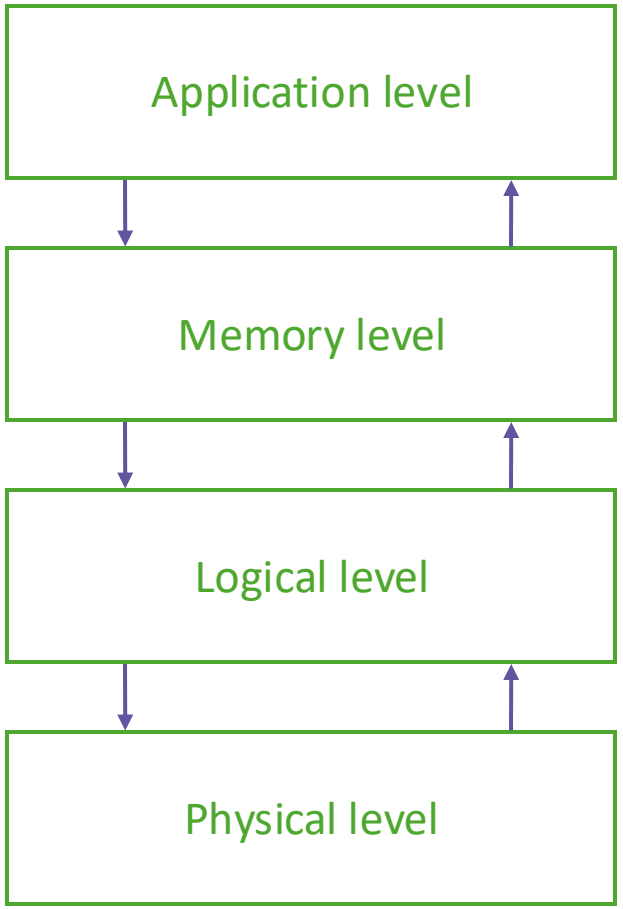
With one faulty byte

Successful PFA

First experimental realization of the PFA on unpowered devices

[4]Zhang et al., "Persistent Fault Analysis on Block Ciphers", TCHES 2018

Abstraction levels



PFA on AES

Code or data corruption

Bitsets ('0'→ '1')

Floating gate transistors discharge by photoemission or heating

Conclusion

Unpowered devices

- Reality of the threat of these attacks
- Hardware sensors not effective
- No synchronization required

X-Ray Fault Injection

- Possibility of focusing fault injection using a tungsten mask with a thickness of 1 mm
- Fault injection on powered and unpowered devices
- Attack scenarios become feasible

Grandamme et al., "X-Ray Fault Injection in Non-Volatile Memories of Power OFF Devices", IEEE PAINE 2023
Grandamme et al., "X-Ray Fault Injection Localization with a Shield on Powered and Unpowered Devices", IEEE PAINE 2025

Laser Fault Injection

- New fault model from the physical level up to the application level
- Validation of a PFA-type attack scenario

Grandamme et al., "Switching Off your Device Does Not Protect Against Fault Attacks", TCHES 2024

Thank you for your attention !

This work was supported by research grants of the projects :

- POP (ANR-21-CE39-0004)
- MITIX (ANR-20-CE39-0012)
- FAMAS.