Injection de fautes : attaques physiques, protections logicielles et mécanismes d'évaluation de la robustesse

LABORATOIRE HUBERT CURIEN

gemalto
security to be free

EM injections on cryptographic implementations on SoC

Journée thématique – Mardi 29 mai 2018, Campus de Jussieu, Paris

Fabien MAJÉRIC
29.05.2018

cnrs

GDR SOC²
System On Chip
Systèmes embarqués et Objets Connectés

PROSECCO

Cybersecurity Institute
Univ. Grenoble Alpes

EM injections on cryptographic implementations on SoC

1. Introduction
2. Methodology
3. Experimentations
4. Analysis

1. INTRODUCTION

- Context
- SoC characteristics

1. Introduction

- Fault injection on digital security devices is a prolific subject

(2006) The Sorcerer's Apprentice Guide to Fault Attacks [H. Bar-El *et al*.]

→Focused on microcontrollers and smartcard…

- Today, complex **S**ystem **o**n **C**hip (SoC) are implied into several security task:
  - Relative to ID of the users (credentials)
  - Relative to safety of the users (automotive)

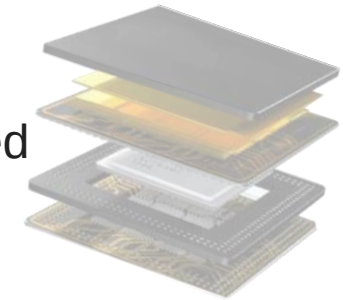
What threats FAs represent on such devices?

1. Introduction

SoC features:

- **Rich OS based on complex architecture**
  - Powerful Multicores
  - Several clock trees
  - Several power supplies
  - A lot of peripherals
  - Cryptographic accelerator
  - Secure internal memories
  - etc…

- **Context**
  - SoC are soldered
  - Package
  - Size
  - etc…



How efficient are FAs on these devices ?

LABORATOIRE HUBERT CURIEN gemalto

2. TARGET AND METHODOLOGY

- Which physical quantity is the most appropriated?
- DUT description
- Our methodology

2. Target and methodology

Which physical quantity is appropriate ?

- To makes a Fault Attack on a process:
  - Analysis (to localize the time and the area)
  - Inject a disturbance on a suitable physical quantity

- Several technologies to inject a fault: Glitch, Laser, EM…

- Electromagnetic field (EM field)
  Analysis **(EM Side-channel)** and Disturbance **(EM Fault Injection)**
  - Through the package
  - Without unsoldering componants
  - Localized disturbances

Electromagnetic field is the most convenient physical quantity to observe and disturb a SoC without damaging it.

2. Target and methodology

The targeted device:

- SoC : CMOS 40nm, Cortex-A9 (1GHz) , 32-bits, DDR3 memory, Cache L1 & L2…

- 2 possible cryptographic implementations:
  CPU and/or crypto accelerator

The test consists in studying the effect of EM injection on an AES encryption executed by the CPU and by the crypto-accelerator.

1. **AES on CPU:**
   - **Straightforward code without counter measures**
2. AES on crypto accelerator:
   - Security Module : dedicated clock tree, DMA, interrupts, crypto-accelerators,....

2. Target and methodology

Principle of our methodology:

1. **EM side-Channel Analysis** to localize in space and **time** the targeted device (module computing the AES)
   - EM side-channel mapping of the SoC by stimulating the AES with suitable data
   - Emissions analysis
   - Timing localization for the FA

2. **EM Injection** to check if an exploitable fault is possible
   - Inject a pulse during the round 9 of the AES (DFA)
   - Injection mapping to cover the entire SoC surface

3. **Results analysis**

3. AES ON CPU : EXPERIMENTATION

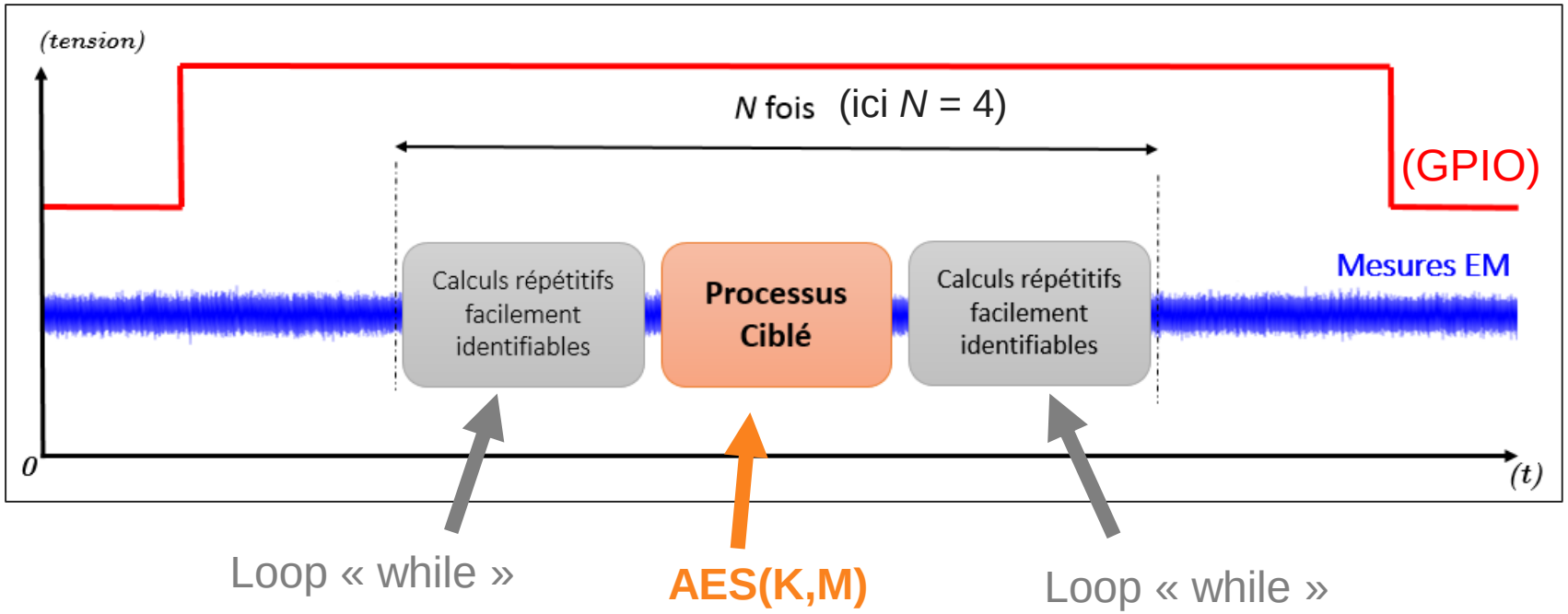
- 3.1 EM side-channel analysis
- 3.2 EM fault injection
- 3.3 Analysis

3.1. Side-channel analysis

- Setup: AES computed by CPU.

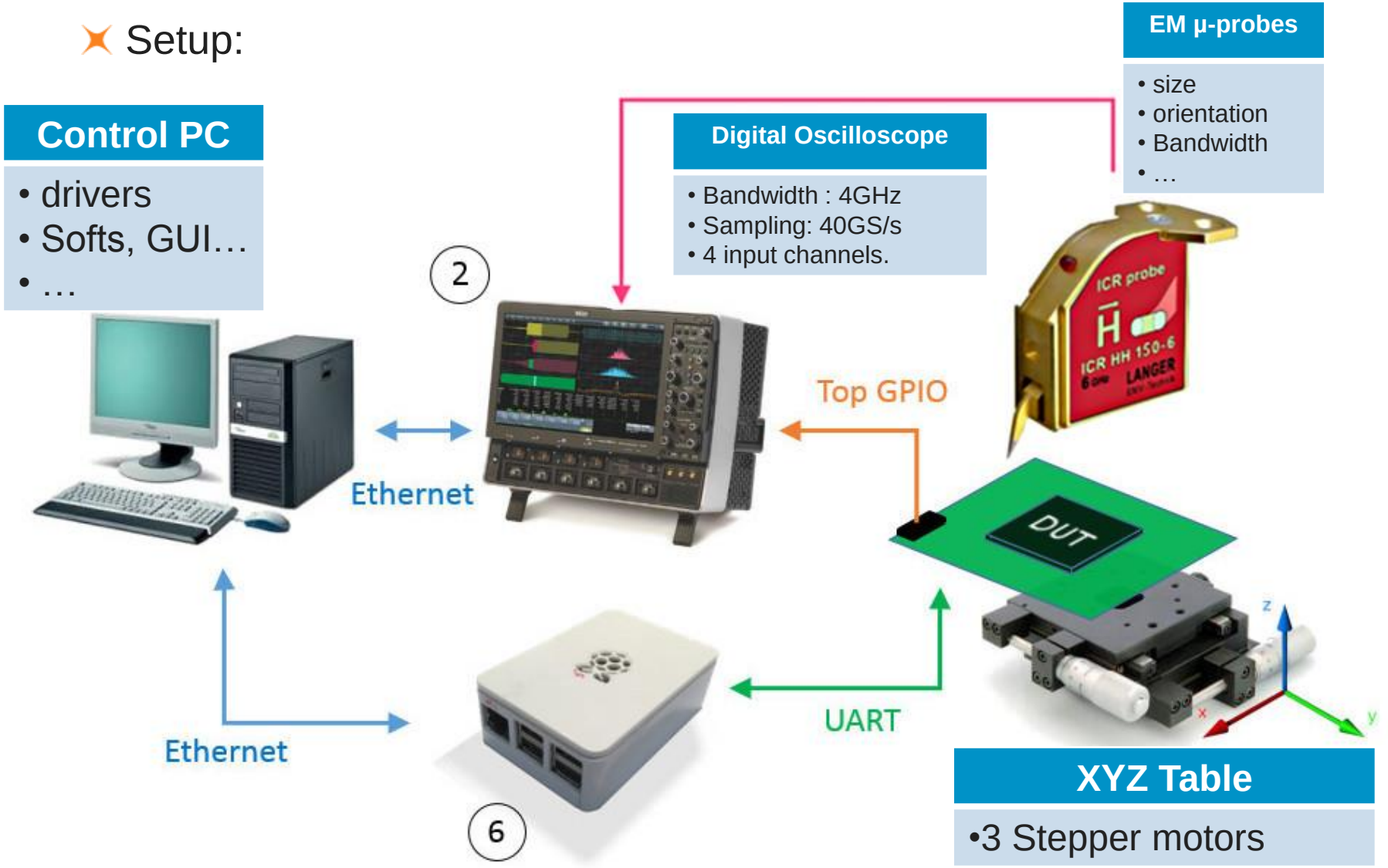
AES encryption:

```
K = 3B E3 22 66 2F 3B E8 41 50 2E 79 41 46 05 25 49
M = RR RR RR RR RR RR RR RR RR RR RR RR RR RR RR RR
```

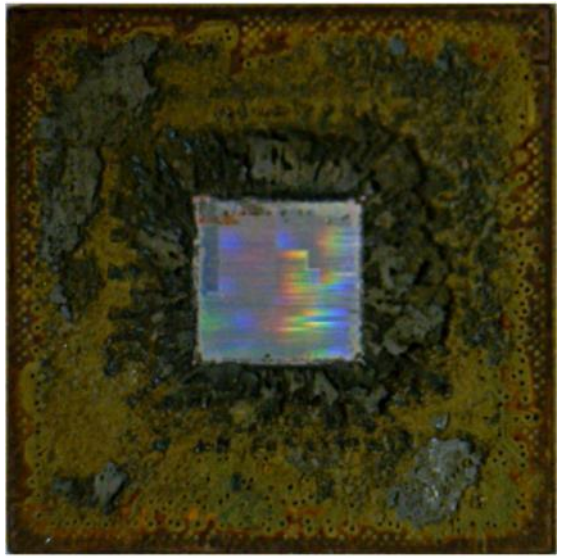


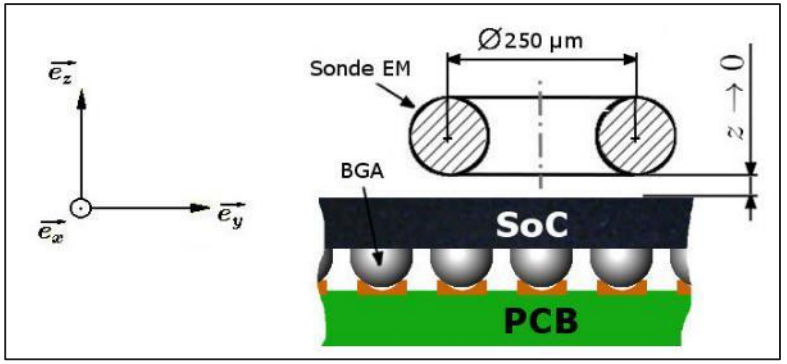
3.1. Side-channel analysis

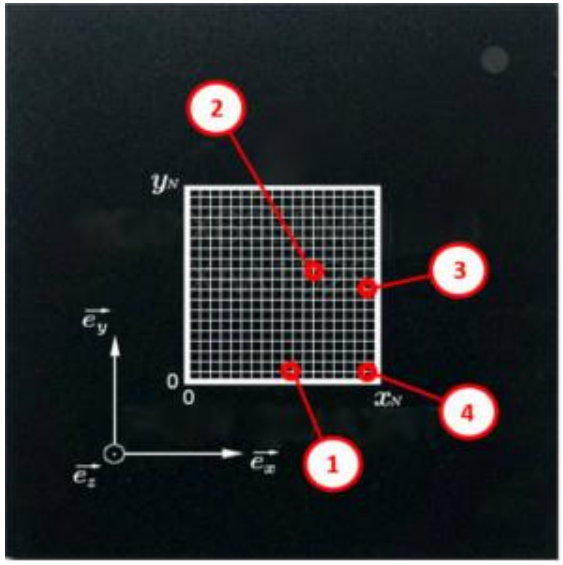
- Setup:



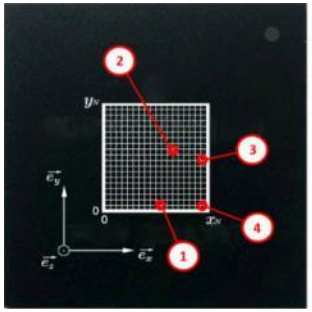
3.1. Side-channel analysis

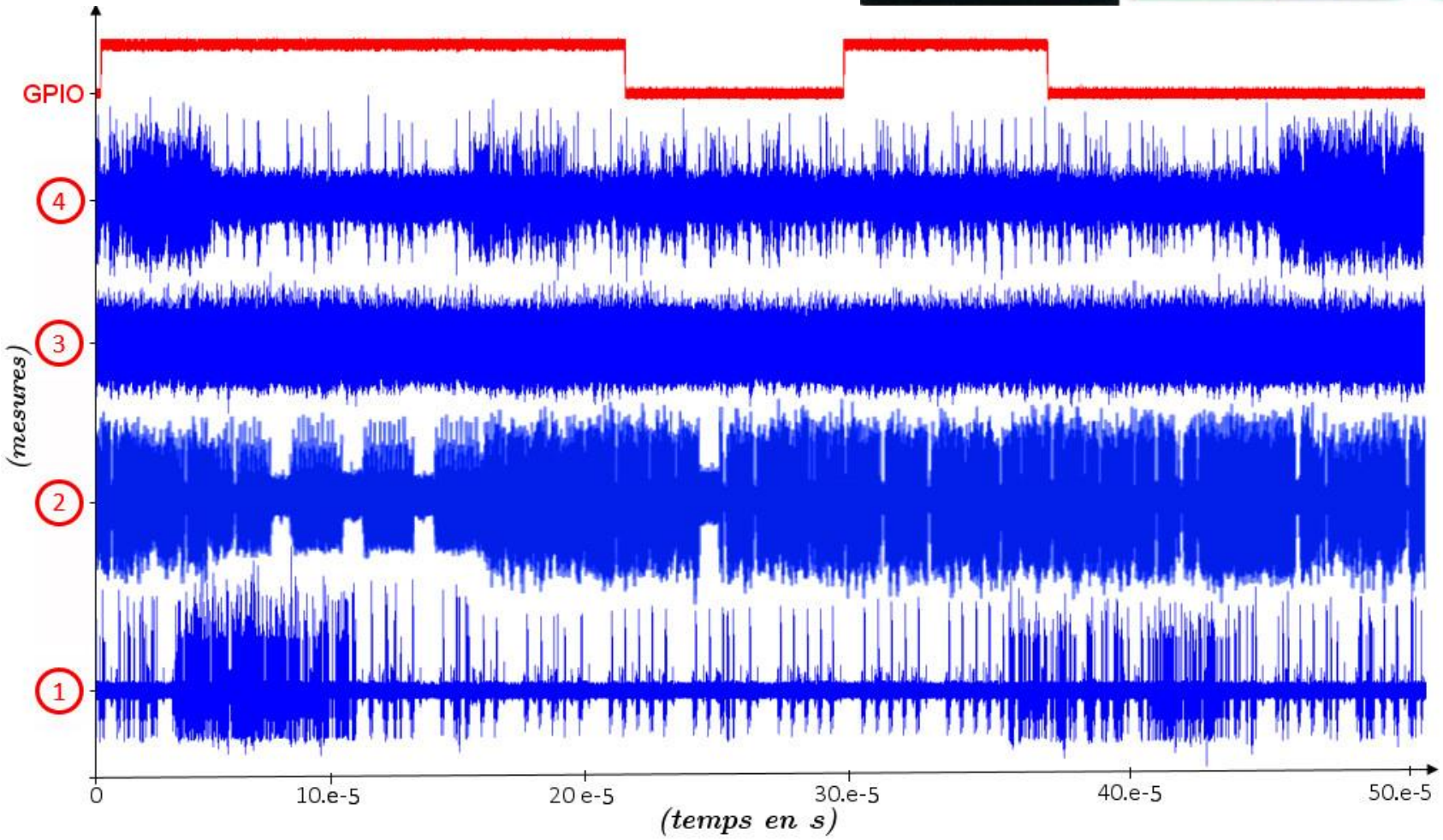






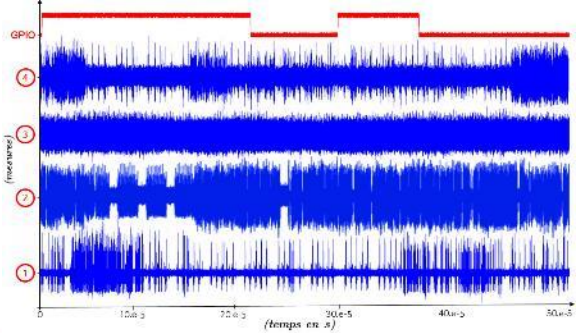
3.1. Side-channel analysis

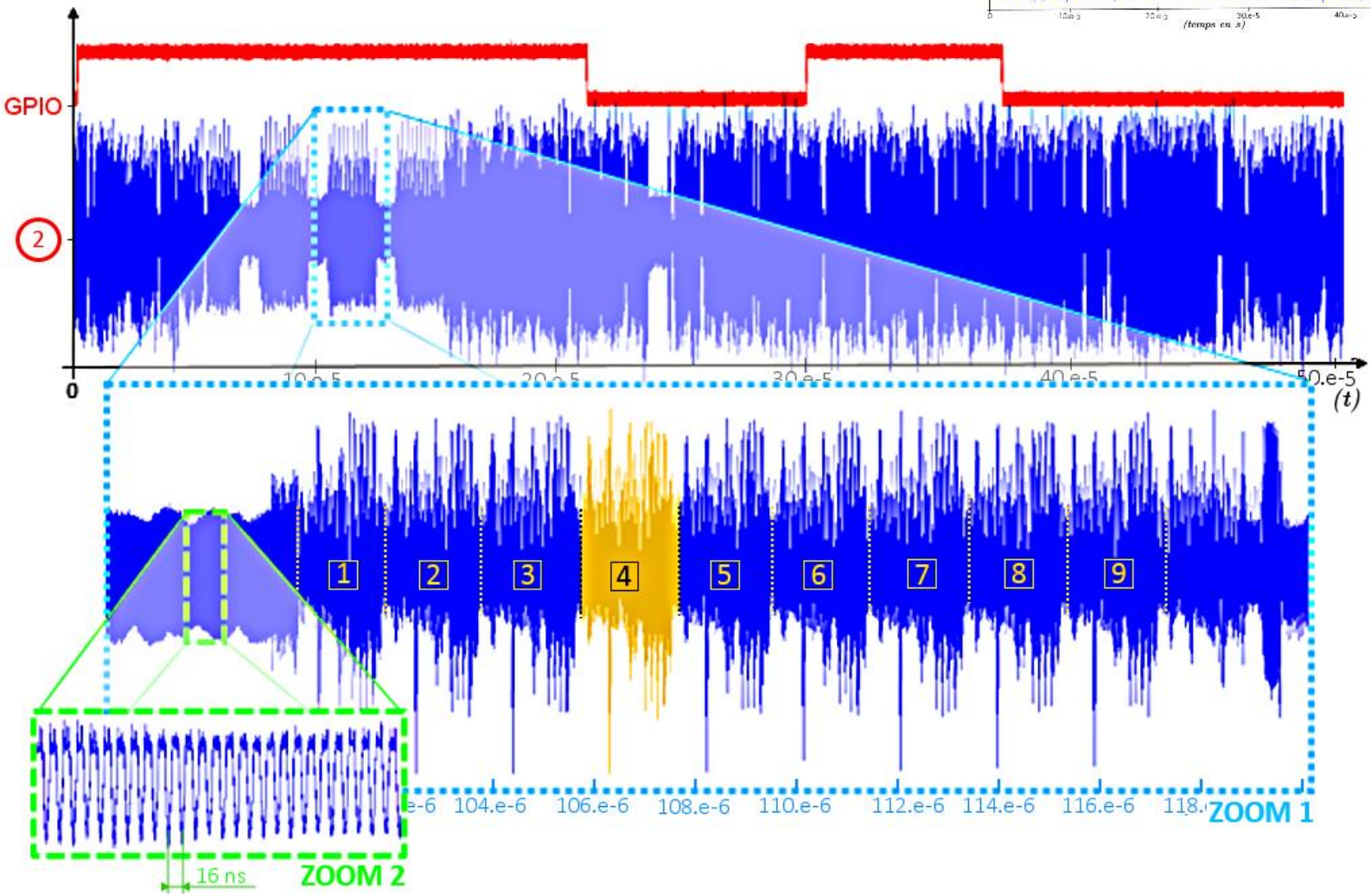




LABORATOIRE HUBERT CURIEN gemalto

3.1. Side-channel analysis





LABORATOIRE HUBERT CURIEN

gemalto

3. AES ON CPU : EXPERIMENTATION

- 3.1 EM side-channel analysis
- 3.2 EM fault injection
- 3.3 Analysis

3.2. Fault injection

- DFA

→ change 1 Byte value of the « state »

[ShiftRow-9] **X** [Mixcolumn-9]

AES encryption:

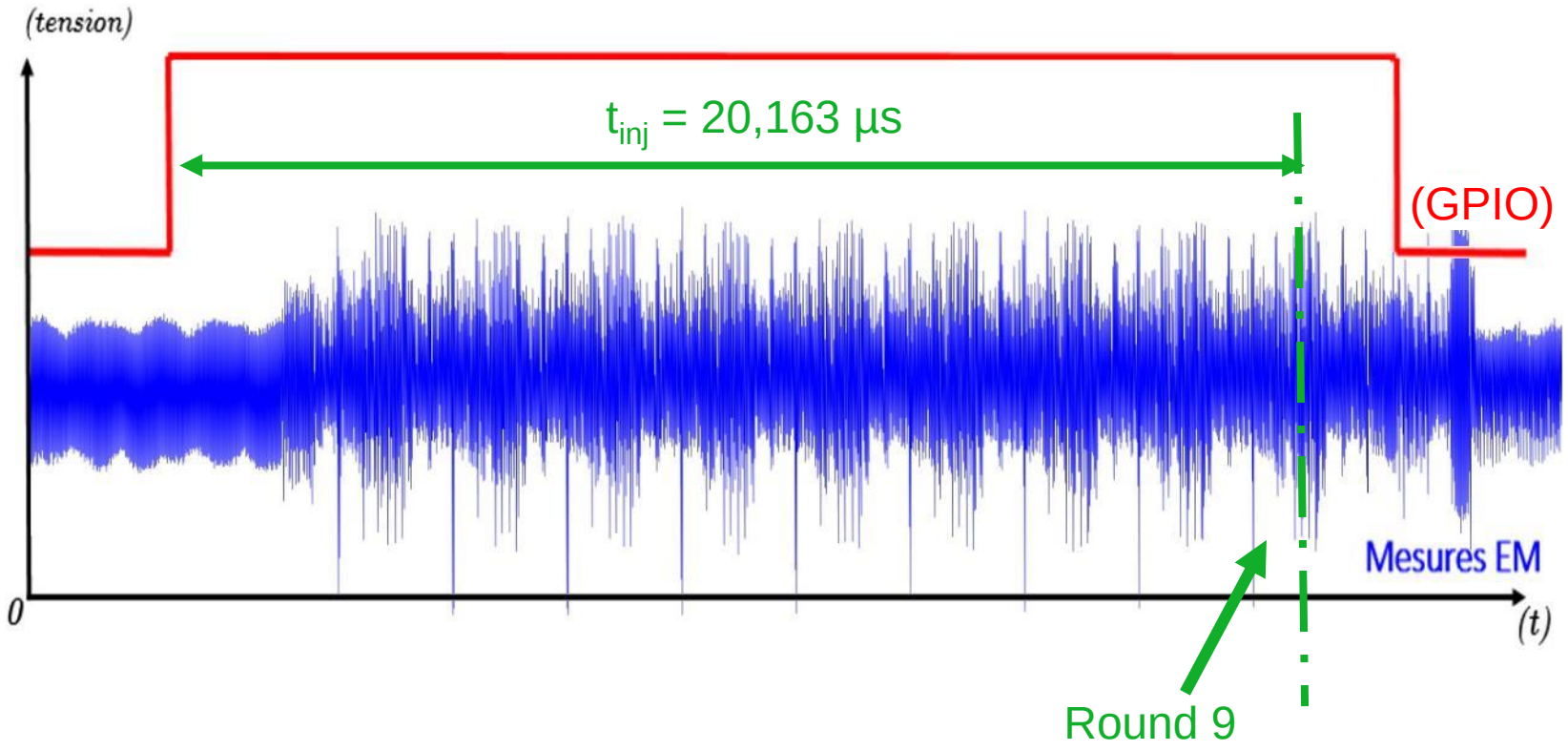
```
K = 3B E3 22 66 2F 3B E8 41 50 2E 79 41 46 05 25 49
M = 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11
C = AF E6 93 58 DE C5 71 93 28 2C 2F B6 B8 AB 62 16
```

Exploitable Faults: (≈ 50 different faults requested)

	$C_{0,0}$	$C_{1,0}$	$C_{2,0}$	$C_{3,0}$	$C_{0,1}$	$C_{1,1}$	$C_{2,1}$	$C_{3,1}$	$C_{0,2}$	$C_{1,2}$	$C_{2,2}$	$C_{3,2}$	$C_{0,3}$	$C_{1,3}$	$C_{2,3}$	$C_{3,3}$
F_1	XX	E6	93	58	DE	C5	71	XX	28	2C	XX	B6	B8	XX	62	16
F_2	AF	XX	93	58	XX	C5	71	93	28	2C	2F	XX	B8	AB	XX	16
F_3	AF	E6	XX	58	DE	XX	71	93	XX	2C	2F	B6	B8	AB	62	XX
F_4	AF	E6	93	XX	DE	C5	XX	93	28	XX	2F	B6	XX	AB	62	16

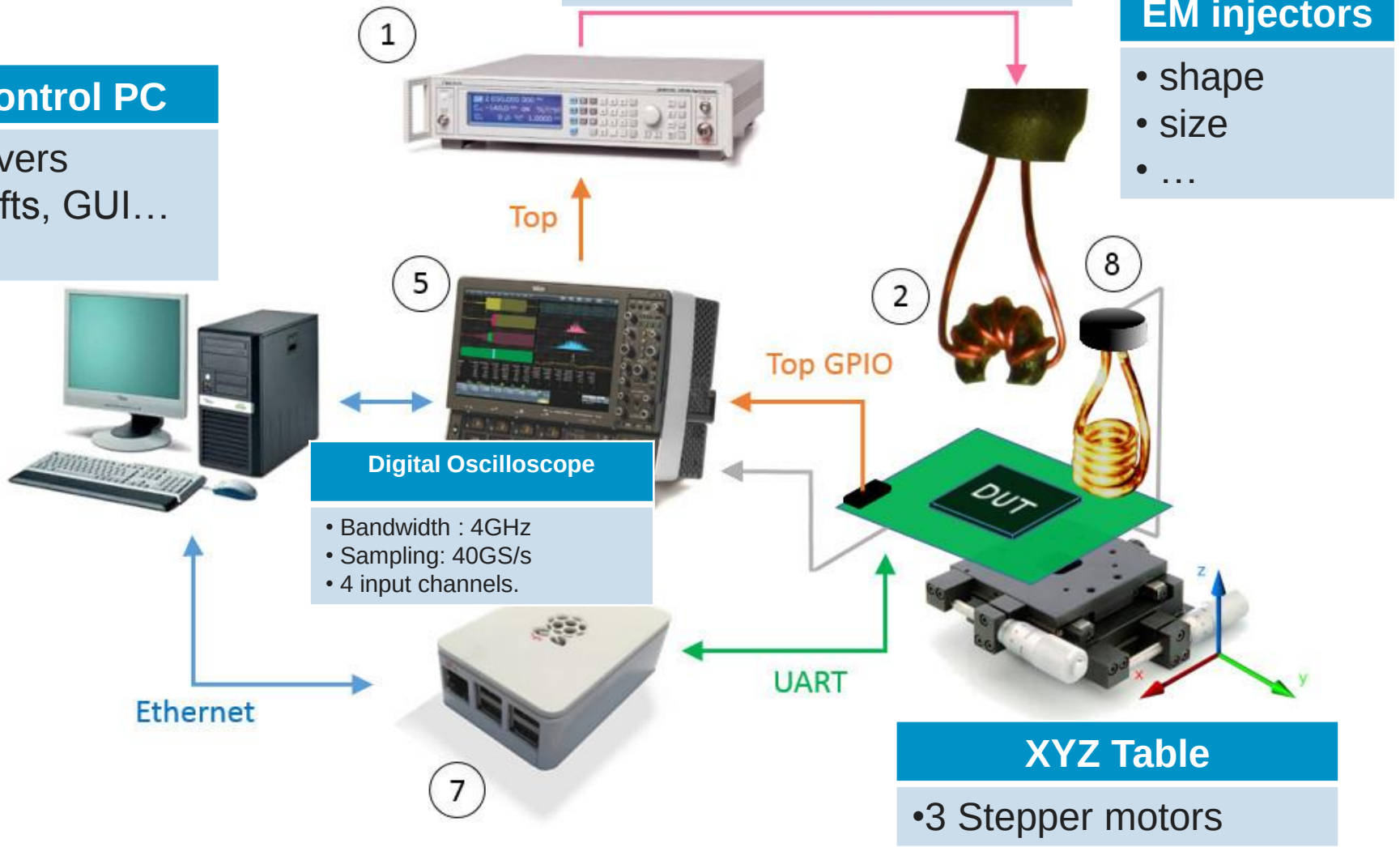
3.2. Fault injection

- From the side-channel analysis:



3.2. Fault injection

- Setup:



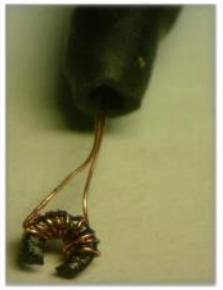
3.2. Fault injection

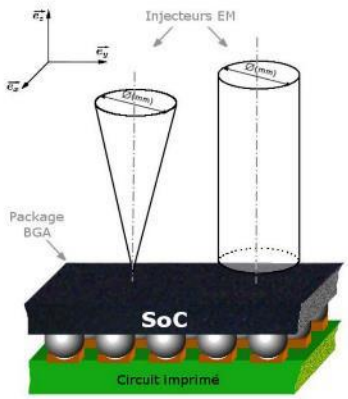
- Several EM injectors with different parameters
  - Size
  - number of spire
  - Symmetry

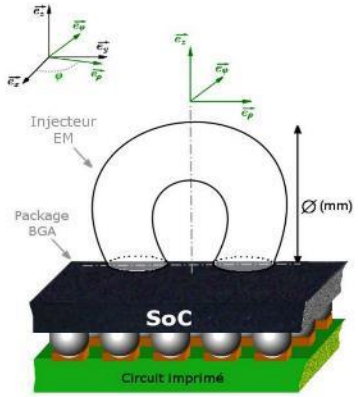
Experimental setup build on trial and error to:

→ Find the most suitable EM injector
→ Find a place where to inject faults.

1. EM pulse +400V, 6ns
2. Localize the `<mute>`
3. Adjust the pulse

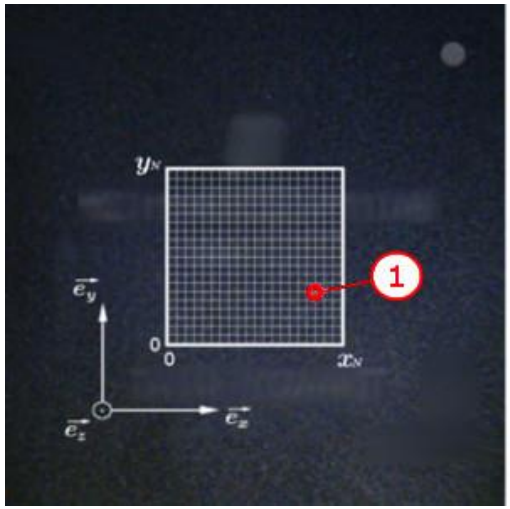


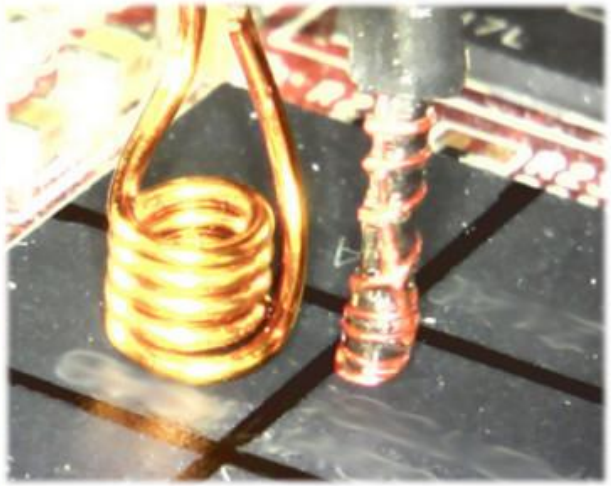




3.2. Fault injection

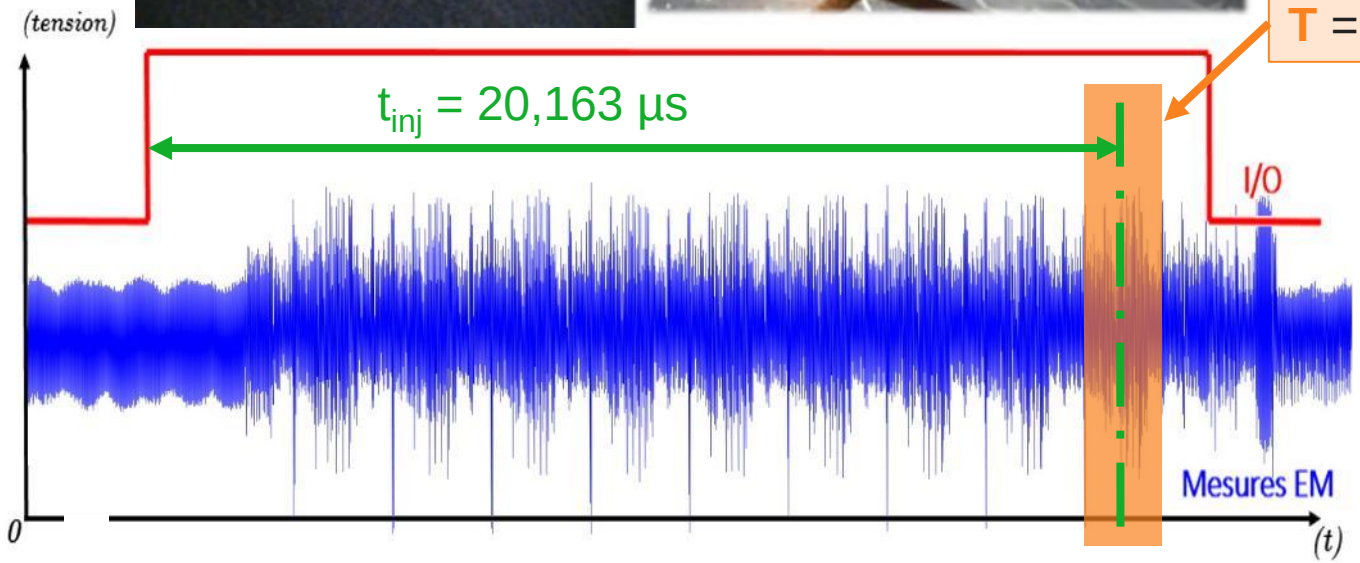
- Most significant results obtained on this point.





ΔA_{inj} = +290V (10% mutes)
ΔT_{inj} = 6ns
T_{inj} = 20,163 µs
Time window: **T**
Step: 1ns
Times : 10

T = [t_{inj}-500ns;t_{inj}+500ns]



3. AES ON CPU : EXPERIMENTATION

- 3.1 EM side-channel analysis
- 3.2 EM fault injection
- 3.3 Analysis

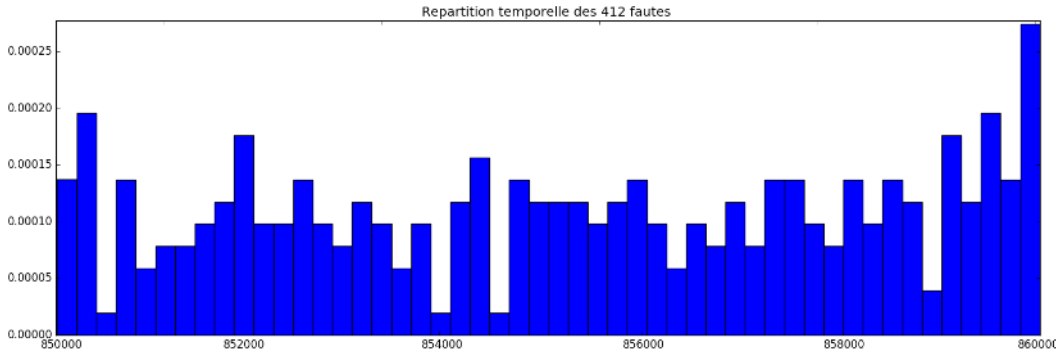
3.2. Fault injection

10 000 tries done in 18h
1207 mutes (12%)
412 faults (4%)
45 exploitable faults

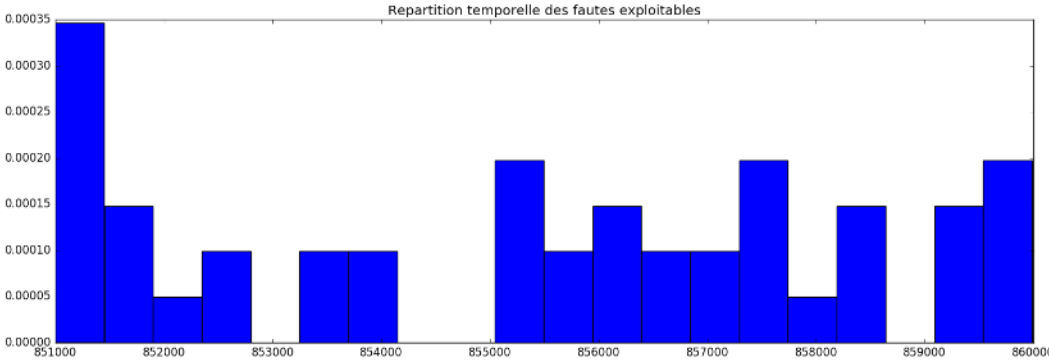
n° identifant	Valeur du <fauté>																(occurences)	Type
(Chiffré Ref.)	AF	E6	93	58	DE	C5	71	93	28	2C	2F	B6	B8	AB	62	16		
0012	..	..	72	..	..	B7	..	..	70	..	..	..	..	..	..	8B	(1 times)	F_3
0014	..	..	..	1E	..	..	73	..	..	75	..	..	A3	..	..	..	(1 times)	F_4
0027	CE	..	..	..	..	..	..	..	78	..	..	78	..	..	9E	..	(3 times)	F_1
0044	..	..	..	F1	..	..	F1	..	..	29	..	..	68	..	..	..	(3 times)	F_4
0067	..	..	..	14	..	..	D1	..	..	49	..	..	A7	..	..	..	(2 times)	F_4
0075	02	..	..	..	..	..	..	..	88	..	..	A6	..	..	C0	..	(6 times)	F_1
0099	06	..	..	..	..	..	..	..	26	..	..	B6	..	..	8F	..	(2 times)	F_1
0161	..	..	..	1C	..	..	DB	..	..	6A	..	..	2A	..	..	..	(1 times)	F_4
0163	..	..	..	13	..	..	31	..	..	6D	..	..	6F	..	..	..	(5 times)	F_4
0171	16	..	..	..	..	..	..	..	66	..	..	EE	..	..	CA	..	(1 times)	F_1
0181	..	..	..	90	..	..	AF	..	..	79	..	..	2B	..	..	..	(5 times)	F_4
0198	..	07	..	..	E9	..	..	..	..	..	..	EE	..	..	83	..	(1 times)	F_2
0208	07	..	..	..	..	..	..	..	AC	..	..	AC	..	..	21	..	(1 times)	F_1
0220	..	C3	..	..	AD	..	..	..	..	..	..	3C	..	..	EF	..	(1 times)	F_2
0223	25	..	..	..	..	..	..	..	20	..	..	6E	..	..	1C	..	(1 times)	F_1
0224	1A	..	..	..	..	..	..	..	E4	..	..	A6	..	..	0D	..	(1 times)	F_1
0273	..	C3	..	..	EB	..	..	..	..	..	..	..	7C	..	..	99	(1 times)	F_2
0297	48	..	..	..	..	..	..	..	2C	..	..	2E	..	..	C3	..	(2 times)	F_1
0301	..	C3	..	..	E9	..	..	..	..	..	..	3C	..	..	40	..	(1 times)	F_2
0308	..	C6	..	..	E8	..	..	..	..	..	..	4E	..	..	A3	..	(1 times)	F_2
0316	..	..	5E	..	..	D1	..	..	7A	..	..	..	..	..	..	C3	(5 times)	F_3

temporal distribution

All faults



Exploitable faults



3.2. Fault injection : Conclusion

- No difficulties to disturb the AES computed by CPU
- We obtained the faults we expected
- In only 10 000 pulse injections → 45 exploitable faults
- Possible improvements : pattern matching to trig the pulse injection.

4. Analysis / Conclusion

- The AES on CPU is “easy” to disturb.
  - Powerful CPU that emit a lot of information.
  - AES software no protected
  - Easy to localize the EM emission (capacity to set up the FA)

- The crypto-accelerator is more difficult to disturb
  - Optimized /autonomous crypto-processor
  - AES hardware protected
  - Need to automatize the EM scan for side channel
  - More complex methodology to localize the EM emissions
  - Need Improvements on EM bench to automate the most as possible the injection EM parameters

- Complex systems require advanced methodology to succeed in fault injection on cryptographic implementation

Contact : fabien.majeric@gemalto.com