Reversing the Field to attack the SoCs

- Double use of EM-fields to defeat the complexity -

Fabien Majéric – Eric Bourbao – Lilian Bossuet

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

gemalto
security to be free

CryptArchi 2016
La Grande Motte - 23/06/2016

Reversing the Field to attack the SoCs

- Introduction
- Methodology
- Experimentation
- Analysis of the results

REVERSING THE FIELD TO ATTACK THE SOCS

Introduction

- Context

- SoC specificities

LABORATOIRE HUBERT CURIEN gemalto

Introduction

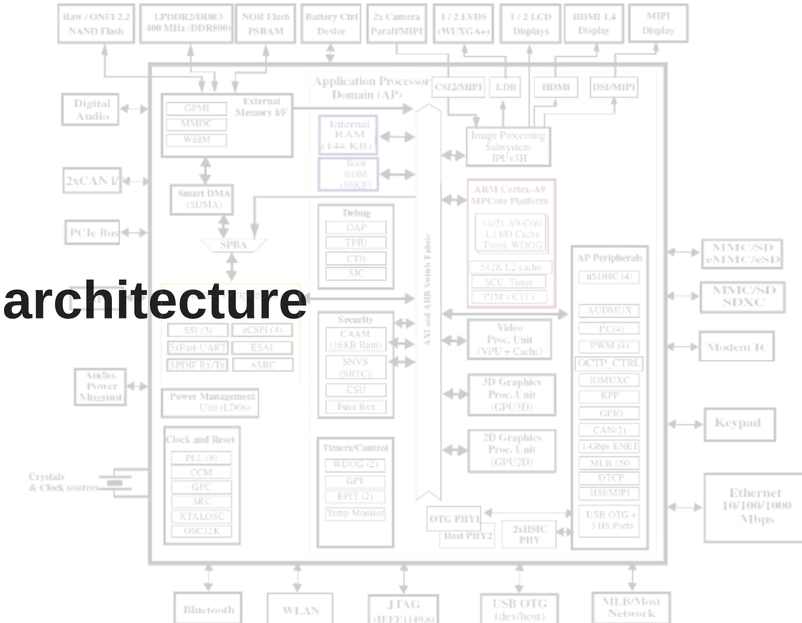
- Internet of Things : more and more complex devices are connected.

- Need to perform security tasks
  → done by embedded microprocessor : System on Chip (SoC)

- Increase of sensitive data processed by these SoC
  - Relative to ID of the users (credentials)
  - Relative to safety of the users (automotive)

Security point of view:
How to characterize the resistance of this devices against the attacks ?
(here: physicals attacks)

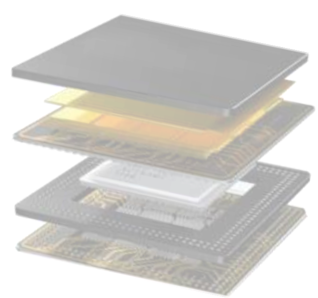
Introduction



SoC features:

- **Rich OS based on complex architecture**
  - Multicores
  - Several clock trees
  - Several power supplies
  - A lot of peripherals
  - etc…

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



- EM is the most suitable physical quantity to spy and disturb a SoC without damage it.
- **For the characterization against the attacks, what could be the advantage to use the same physical quantity to spy and disturb a process ?**

REVERSING THE FIELD TO ATTACK THE SOCS

Target and methodology

- The targeted device

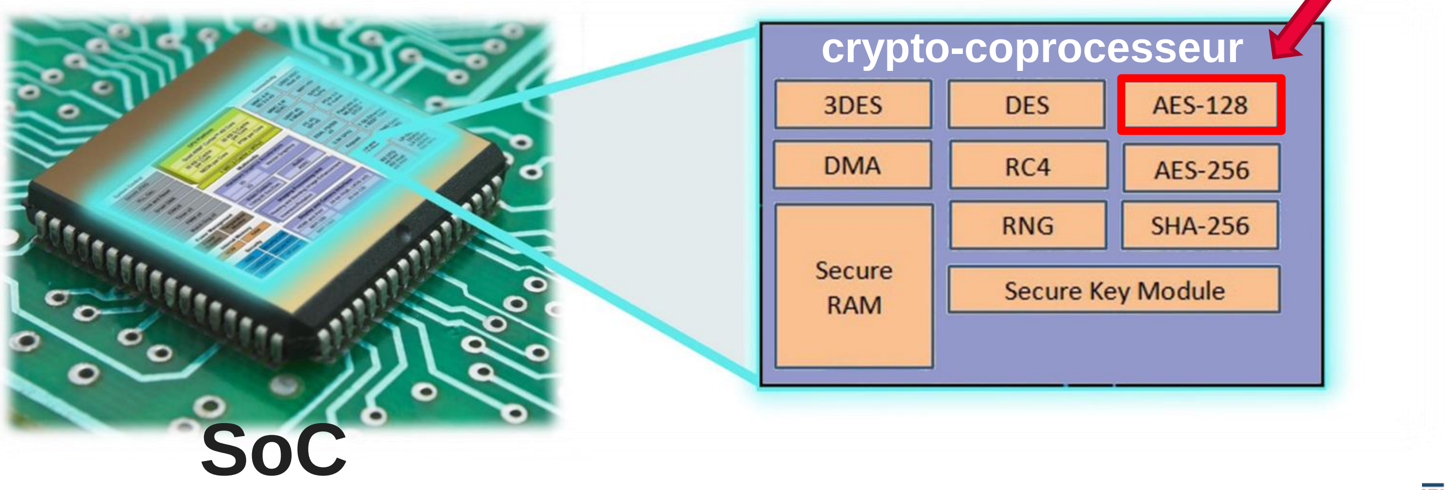
- Principle of our methodology.

Target and methodology

The targeted device:

- SoC : CMOS 40nm, Cortex-A9 (1GHz) , 32-bits, DDR3 memory, Cache L1 & L2…
- An hardware crypto-coprocessor embedded in a SoC.
- Crypto-coprocessor : dedicated clock tree, DMA, interrupts, crypto-accelerators,....
- In particular : an **AES 128-bits hardware accelerator**.

The module targeted !



LABORATOIRE HUBERT CURIEN gemalto

Target and methodology

Principle of our methodology:

1. **EM side-Channel Analysis** to localize in space and **time** the targeted device (AES module)
   - EM side-channel mapping on the SoC by stimuling the AES with suitable data
   - Emissions analysis
   - Timing localization of the round 9 of the AES (DFA)

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** and mappings comparison

Experimentation

→ **<u>EM side-channel analysis</u>**

- EM fault injection

- Results analysis and mappings comparison

LABORATOIRE HUBERT CURIEN gemalto

Side-channel analysis

- Setup:

Control PC

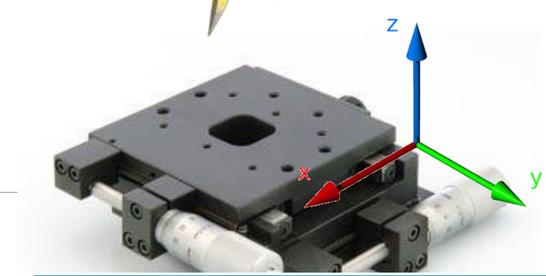
- drivers
- Softs, GUI…
- …

Digital Oscilloscope

- Bandwidth : 4GHz
- Sampling: 40GS/s
- 4 input channels.

EM µ-probes

- size
- orientation
- Bandwidth
- …



XYZ Table

- 3 Stepper motors

Side-channel analysis

Side-channel mapping:

- The Goal is to detect the EM emissions of the hardware AES:
  - Scan on surface of the SoC → variables (x,y)
  - For each point (x_i,y_i), measure of the AES encryption with chosen key and message → variable (t)

LANGER ICR
HH-150 µ-probe
Ø150µm
Bw : 6 GHz

LABORATOIRE HUBERT CURIEN gemalto

Side-channel analysis

- Nb of spatial points: 21 x 21
  Step: 300µm

- Chosen set of key and message to maximize the HW amplitude during operations.

- Set 1 (Key amplitude) :

HW(key) = 0	HW(plaintext) = 0
HW(key) = 128	HW(plaintext) = 0

- Set 2 (plaintext amplitude) :

HW(plaintext) = 0	HW(key) = 0
HW(plaintext) = 128	HW(key) = 0

- Set 3 (cipher amplitude):

HW(cipher) = 0	HW(key) = 0
HW(cipher) = 128	HW(key) = 0

➢ 100 encryptions per parameters per point (x_i,y_i) → 220500 traces in total

LABORATOIRE HUBERT CURIEN gemalto

Side-channel analysis

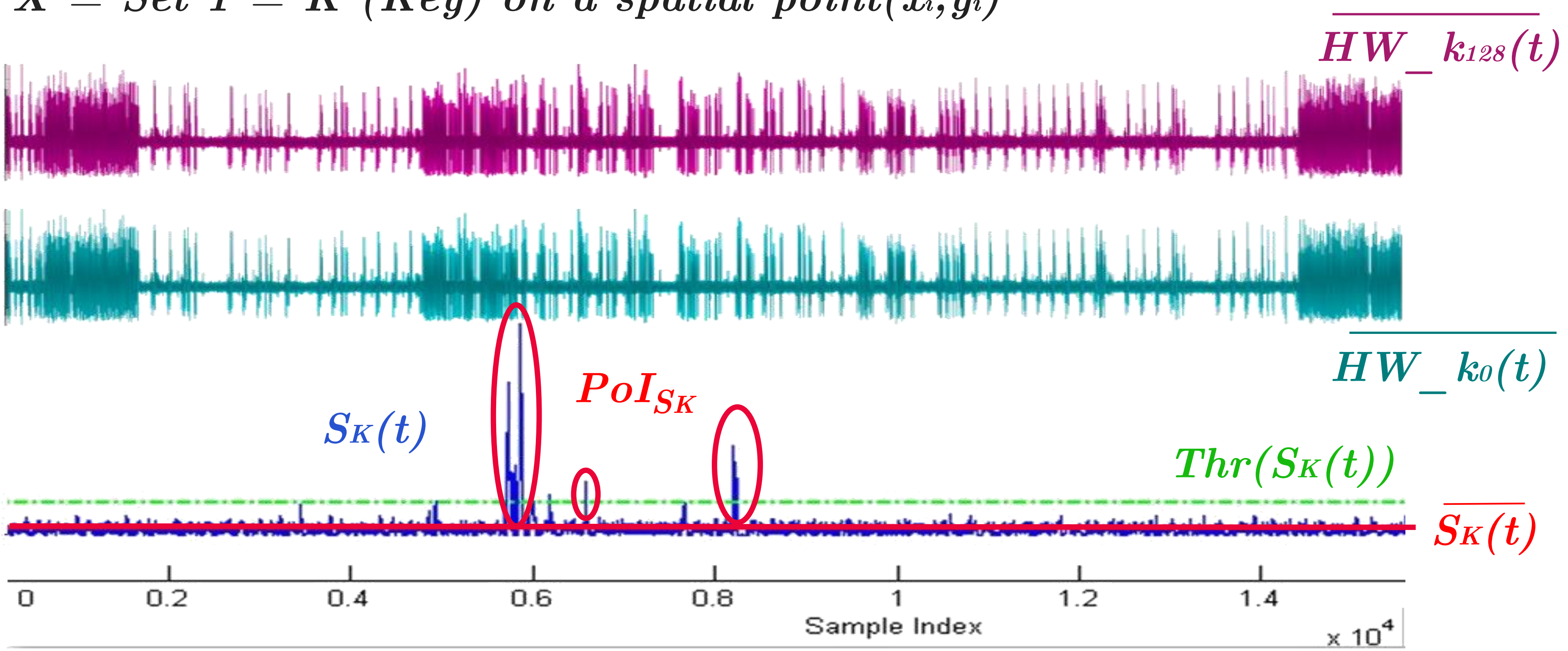
Statistical treatment on each $X \equiv Set\ i,\ i \in \{1,2,3\}$:

(1) $$S_X(t) = \left(\frac{\overline{X_0(t)} - \overline{X_{128}(t)}}{\sqrt{\frac{\sigma_0(t)^2}{n_0} + \frac{\sigma_{128}(t)^2}{n_{128}}}} \right)^2$$

(2) $$Thr(S_X(t)) = \overline{S_X(t)} + 3 \cdot \sigma_{S_X}(t)$$

(3) $$PoI_{S_X} = \{\forall t \mid S_X(t) \geq Thr(S_X(t))\}$$

→ $X = Set\ 1 = K\ (Key)$ *on a spatial point* (x_i, y_i)



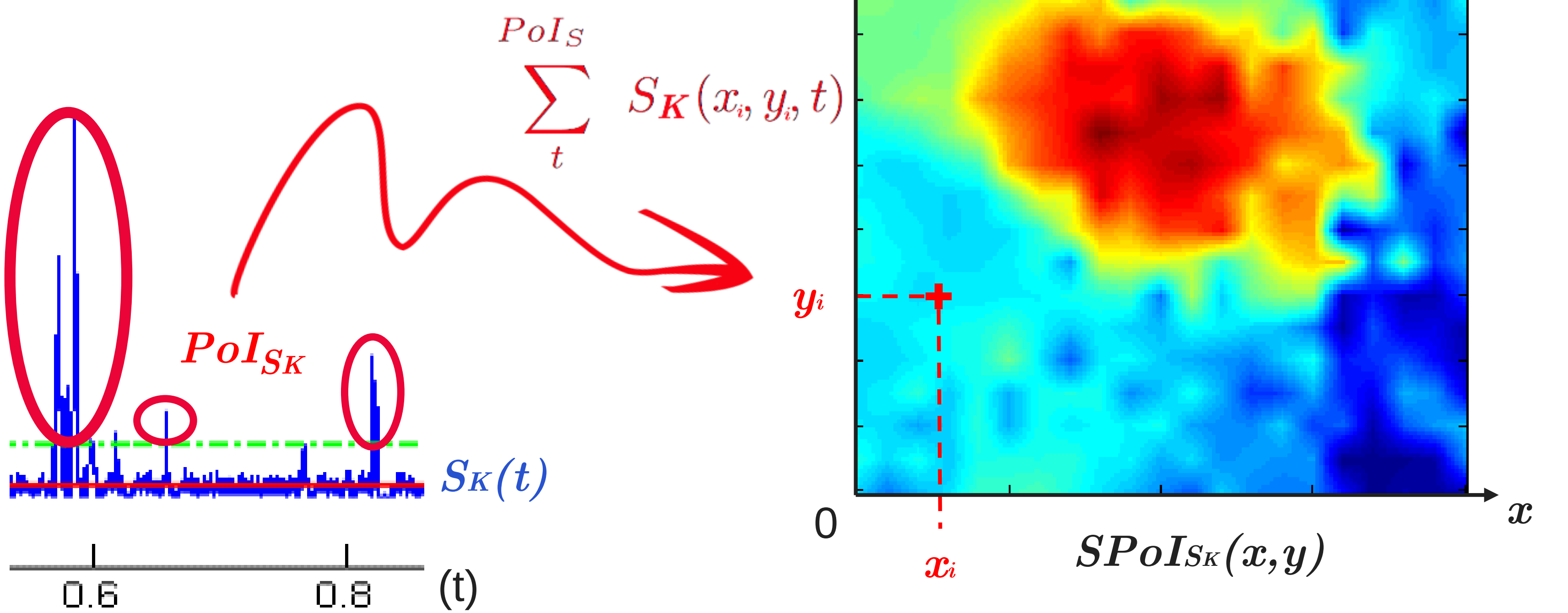
LABORATOIRE HUBERT CURIEN gemalto

Side-channel analysis

X = Set 1 = K (Key) on a spatial point(x_i, y_i)

(3) $PoI_{S_X} = \{\forall t \mid S_X(t) \geq Thr(S_X(t))\}$

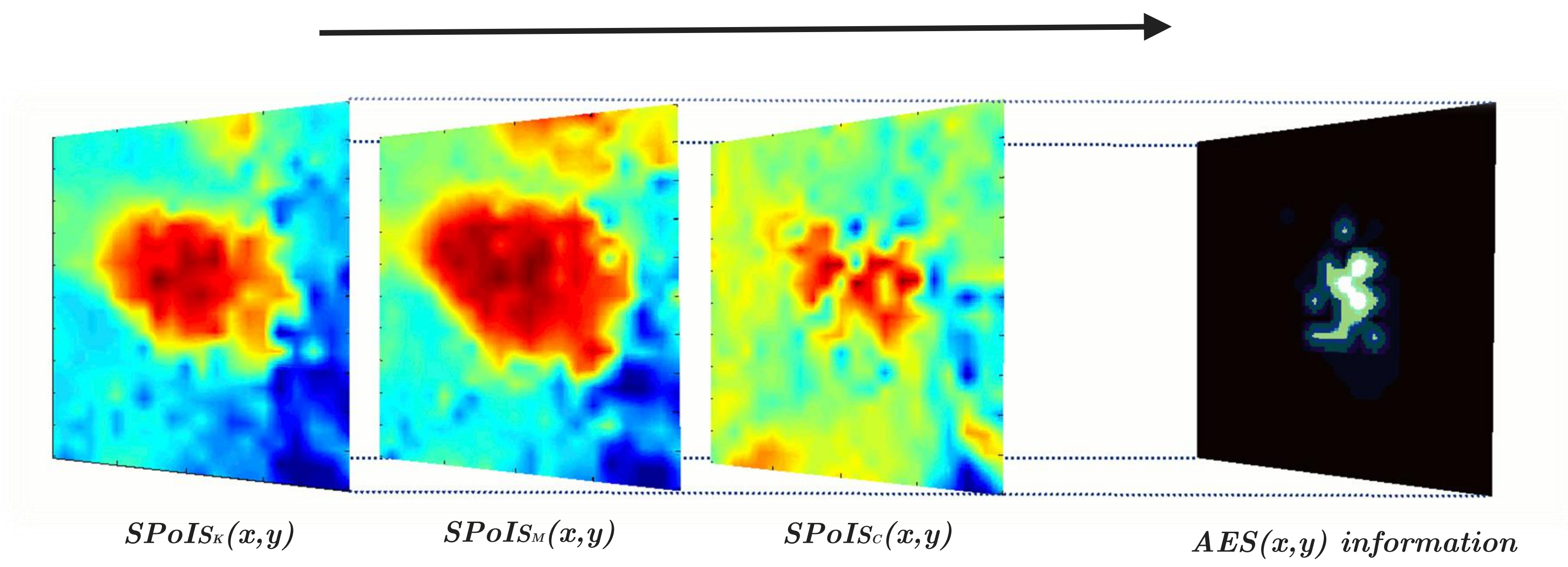
(4) $SPoI_{S_X}(x_i, y_i) = \sum_{t}^{PoI_{S_X}} S_X(x_i, y_i, t)$



Side-channel analysis

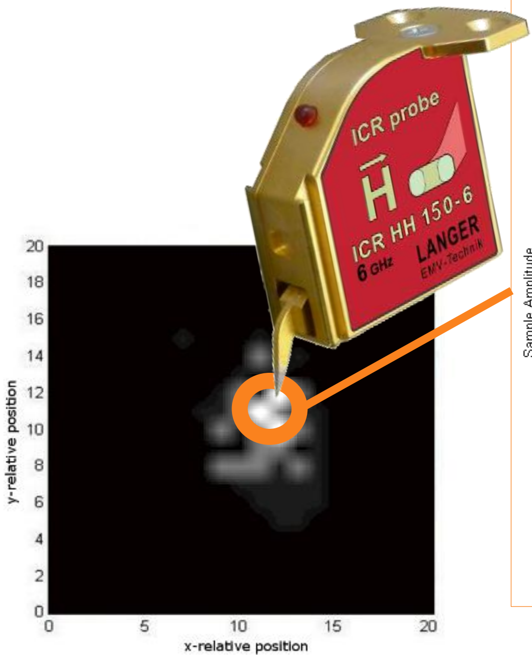
- Analysis and extraction of the desired information

$$\sum_{X=\{K,M,C\}} SPoI_{S_X}(x,y)$$

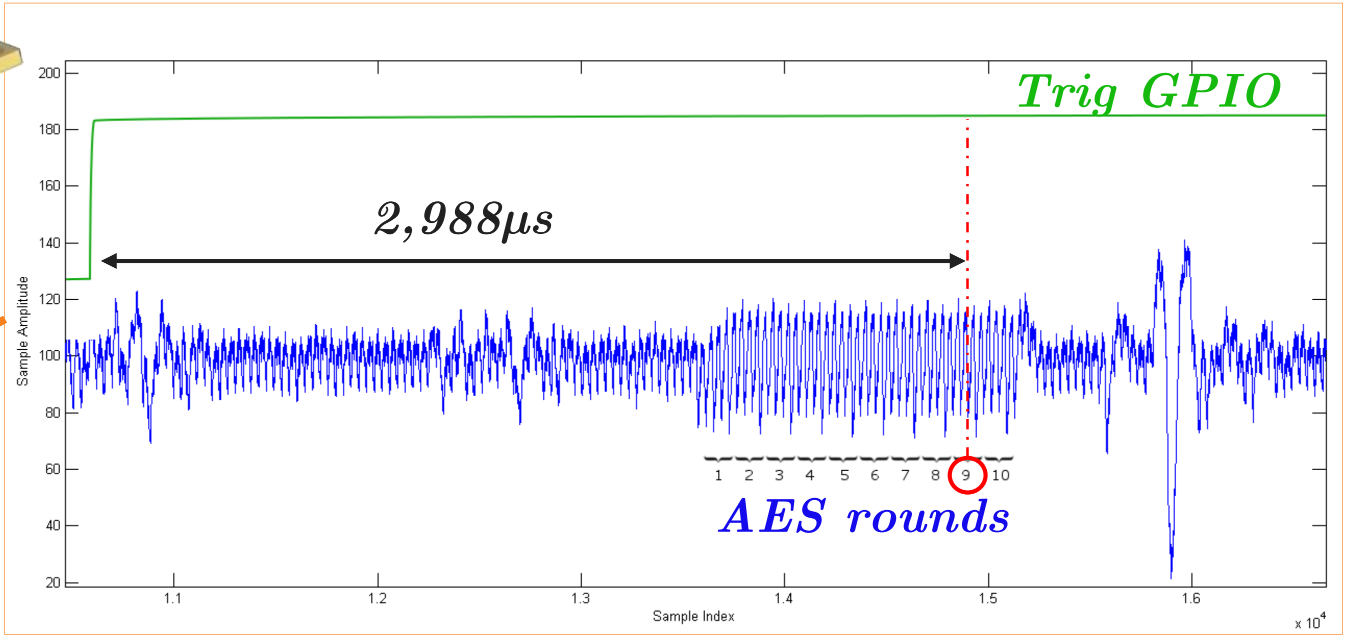


Side-channel analysis

- Timing location of the round 9 of the AES



AES(x,y) information



gemalto

Experimentation

- EM side-channel analysis

→ **EM fault injection**

- Results analysis and mappings comparison

Fault injection

- Setup:

Pulse generator

- Intensity: 0 – 400V
- Duration: 6 – 100 ns.

EM injectors

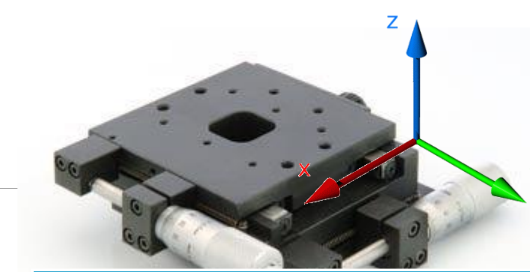
- shape
- size
- nb of turns
- …

Control PC

- drivers
- Softs, GUI…
- …

Digital Oscilloscope

- Bandwidth : 4GHz
- Sampling: 40GS/s
- 4 input channels.



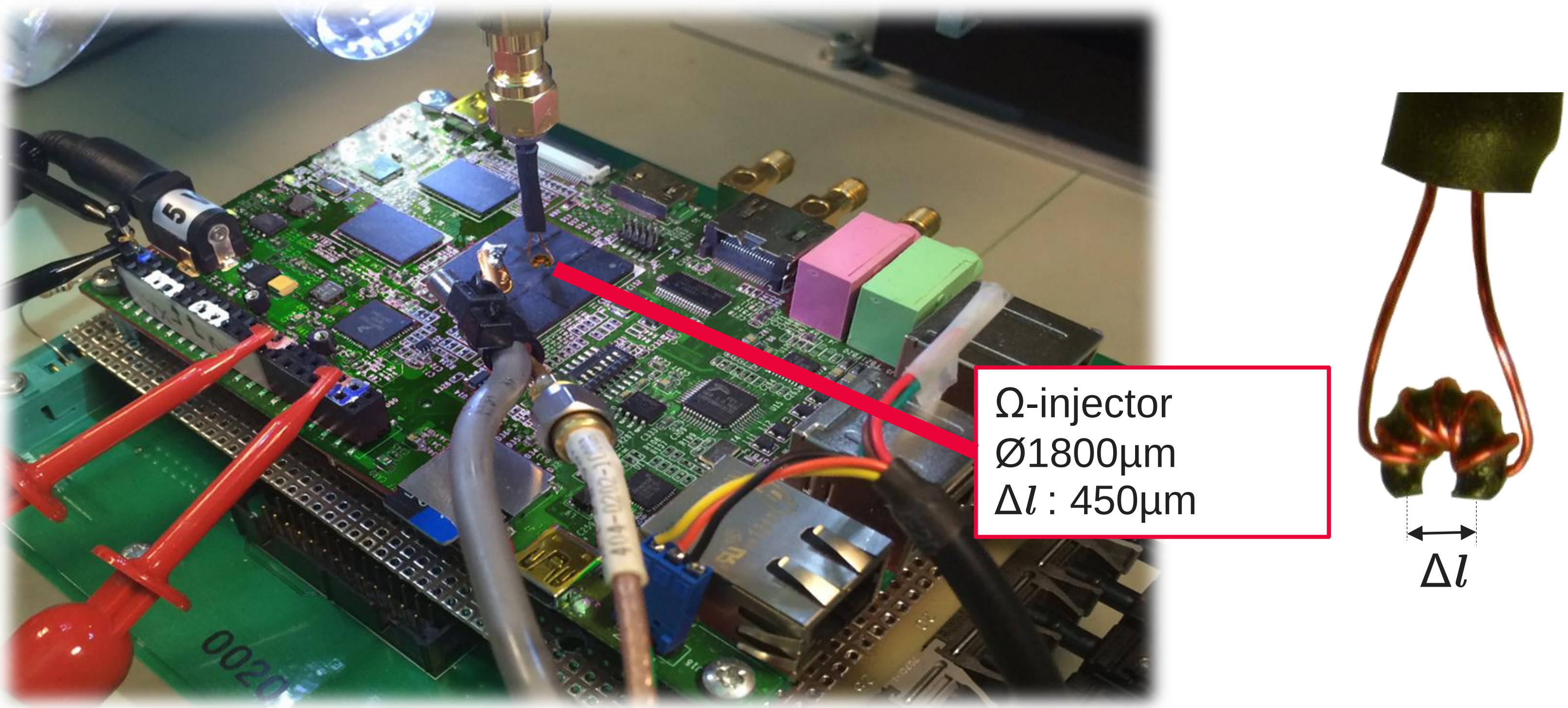
XYZ Table

- 3 Stepper motors

Fault injection

Fault injection mapping:

- The Goal is to detect any disturbance of the AES process:
  - Scan on the surface of the SoC by injecting EM pulses
  - On each point (x_i,y_i), AES encryption with the same fixed key and message
  - Injection of a pulse during the time defined in the side-channel step



LABORATOIRE HUBERT CURIEN gemalto

Fault injection

- Nb of spatial points: 101 x 101
  Step: 60µm

- Fixed key and message to detect faults during operations:

Key	3BE322662F3BE841502E794146052549
Plaintext	00000000000000000000000000000000
Cipher	524FF49CC3C5AE60B8A98156B1469E13

- EM injection features:
  - Time delay after GPIO trigger : $2{,}988\mu s$

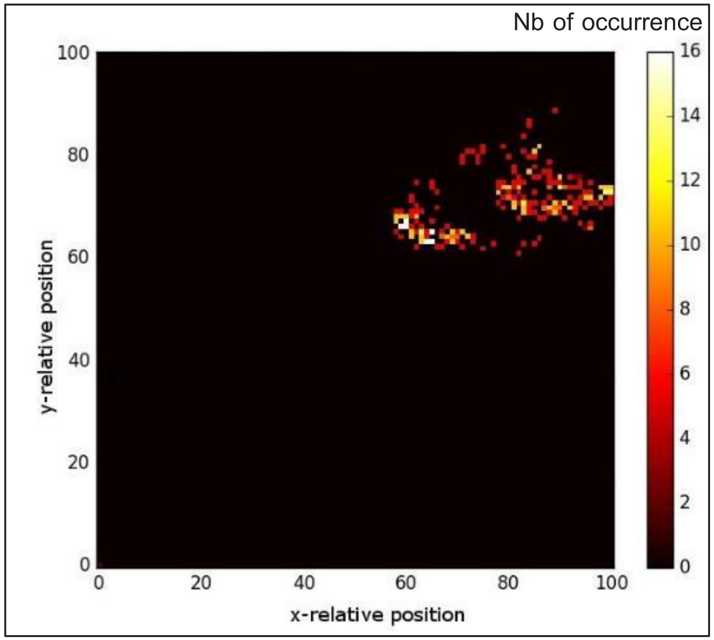
Pulse features

Intensity: +400V
Duration : 6ns

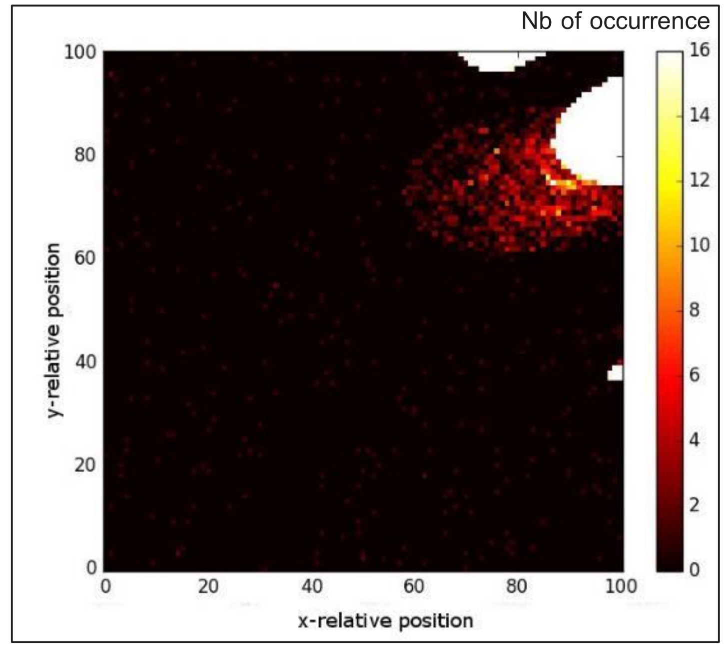
- 50 encryption by point (x_i, y_i) → 510050 EM pulses in total

Fault injection

- Two main type of behaviors:



Faults on the cipher



<no-response>

Experimentation

- EM side-channel analysis

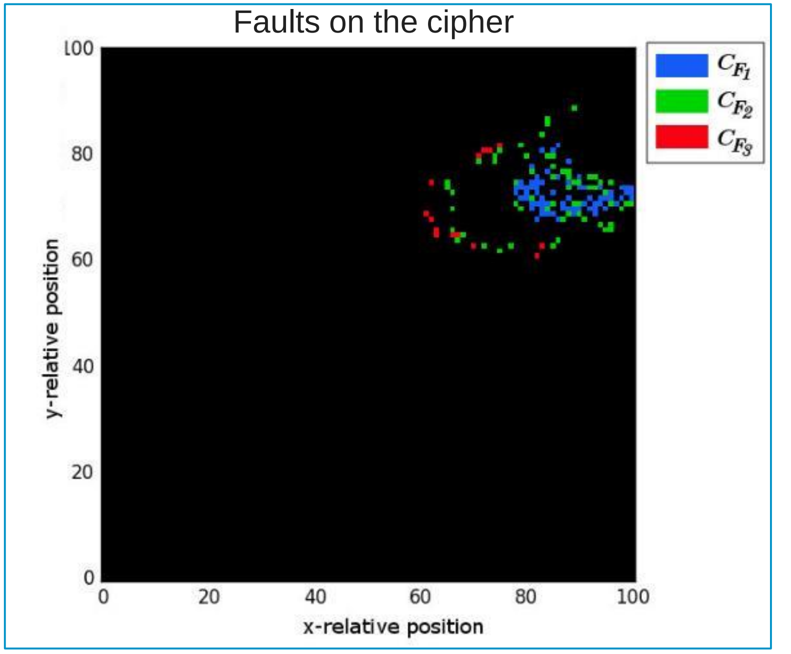
- EM fault injection

→ **Results analysis and mappings comparison**

LABORATOIRE HUBERT CURIEN gemalto

Results analysis

- 3 main type of faults on the cipher:



- Faults classification:

	52	4F	F4	9C	C3	C5	AE	60	B8	A9	81	56	B1	46	9E	13
CF1	52	4F	F4	9C	**52**	**4F**	**F4**	**9C**	B8	A9	81	56	B1	46	9E	13
	52	4F	F4	9C	C3	C5	AE	60	**B1**	**46**	**9E**	**13**	B1	46	9E	13
	...															
CF2	**CC**	**CC**	**CC**	**CC**	**50**	**00**	**CC**	**CC**	B8	A9	81	56	B1	46	9E	13
	CC	**CC**	**CC**	**CC**	**CC**	**CC**	**CC**	**CC**	**CC**	**CC**	**CC**	**CC**	**CC**	**CC**	**CC**	**CC**
	...															
CF3	**CA**	4F	F4	9C	C3	C5	AE	**2A**	B8	A9	**1D**	56	B1	**1A**	9E	13
	38	**EB**	**9C**	**91**	**56**	**F6**	**08**	**C9**	**6D**	**AE**	**E0**	**F5**	**E2**	**8F**	**02**	**B6**
	...															

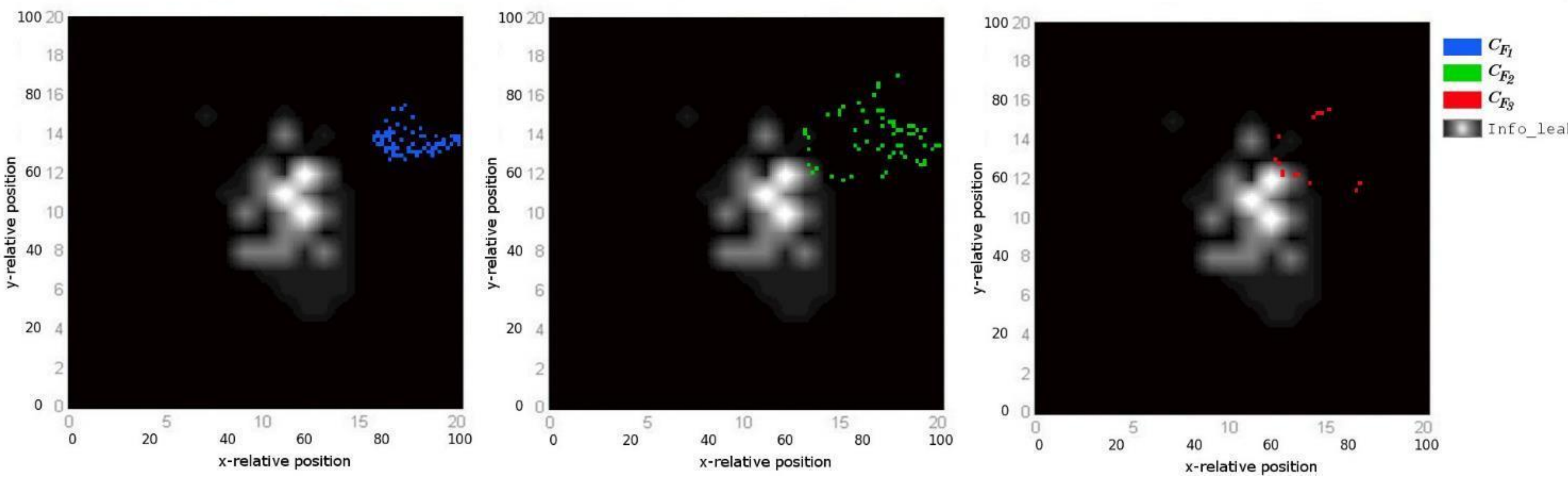
← Cipher without faults (first row)

Results analysis

- No perfect matching between the two maps.

- Potential candidates for the DFA are the ones which are the closest to the side-channel highlighted areas.

- The links between emissions and injections EM need more investigations to define precisely areas of interest.



C_{F1} C_{F2} C_{F3}

REVERSING THE FIELD TO ATTACK THE SOCS

Conclusion

Conclusion

- We try to exploit the same physical quantity (EM) to spy and disturb a process

- The side-channel attack gives information about:
  - The spatial emissions of the AES process
  - The time when to inject a fault

- The fault injection attack gives information about :
  - 3 types of faults
  - Only one kind of them is exploitable for the DFA. This category is the closest to the side-channel highlighted area

- Partial superposition of the exploitable faults and side-channel emissions → more investigations

- Layout access would be valuable for results interpretation
- Additional experimentations on other devices will be done

Thank you

This presentation is available here:

https://dossier.univ-st-etienne.fr/maf13892/public/Presentations/CryptArchi_2016.pdf

fabien.majeric@gemalto.com