ElectroMagnetic Analysis and Fault Injection onto Secure Circuits

Paolo Maistri[1], Régis Leveugle[1], Lilian Bossuet[2], Alain Aubert[2],

Viktor Fischer[2], Bruno Robisson[3], N. Moro[3],

Philippe Maurine[3,4], Jean-Max Dutertre[5], Mathieu Lisart[6]

(1) (2) (3) (4) (5) (6)

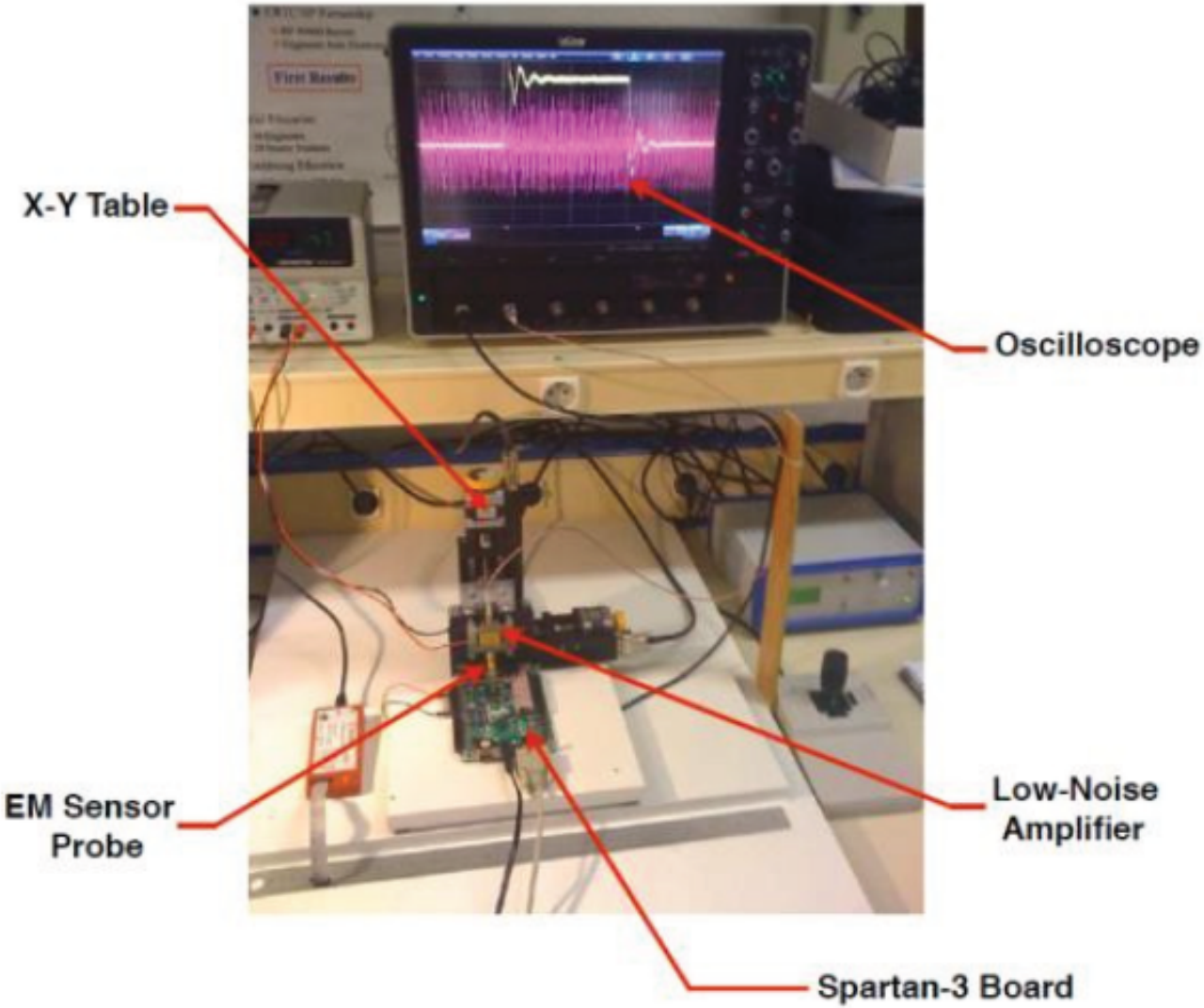
Outline

- Context
- Side Channel Analysis
- Fault Injection
- Advanced discussion
- Conclusion/Perspectives

Context

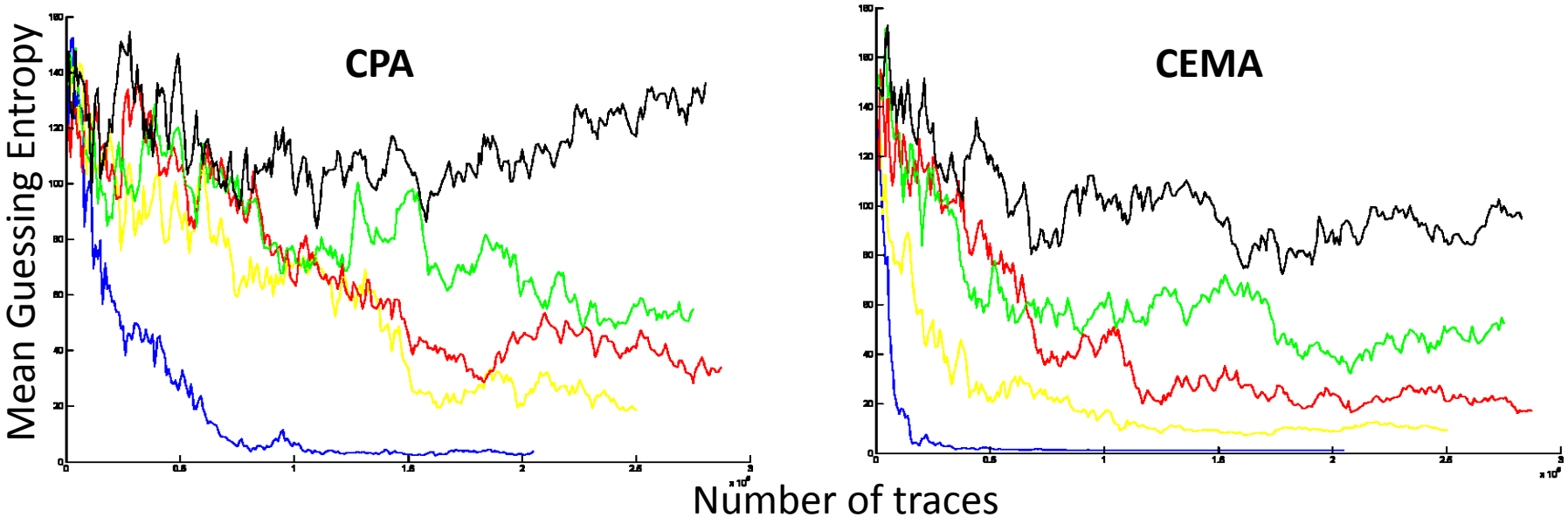
- Implementation attacks are a serious threat to secure designs
  - Side channel analysis, Fault injection, …
- EM is
  - A very rich information source in passive analysis
    - Power is global, EM is local
  - A versatile medium for active attacks
    - Laser requiring decapsulation and lapping
- Know-How has been largely developed only in recent years

Analysis Platform

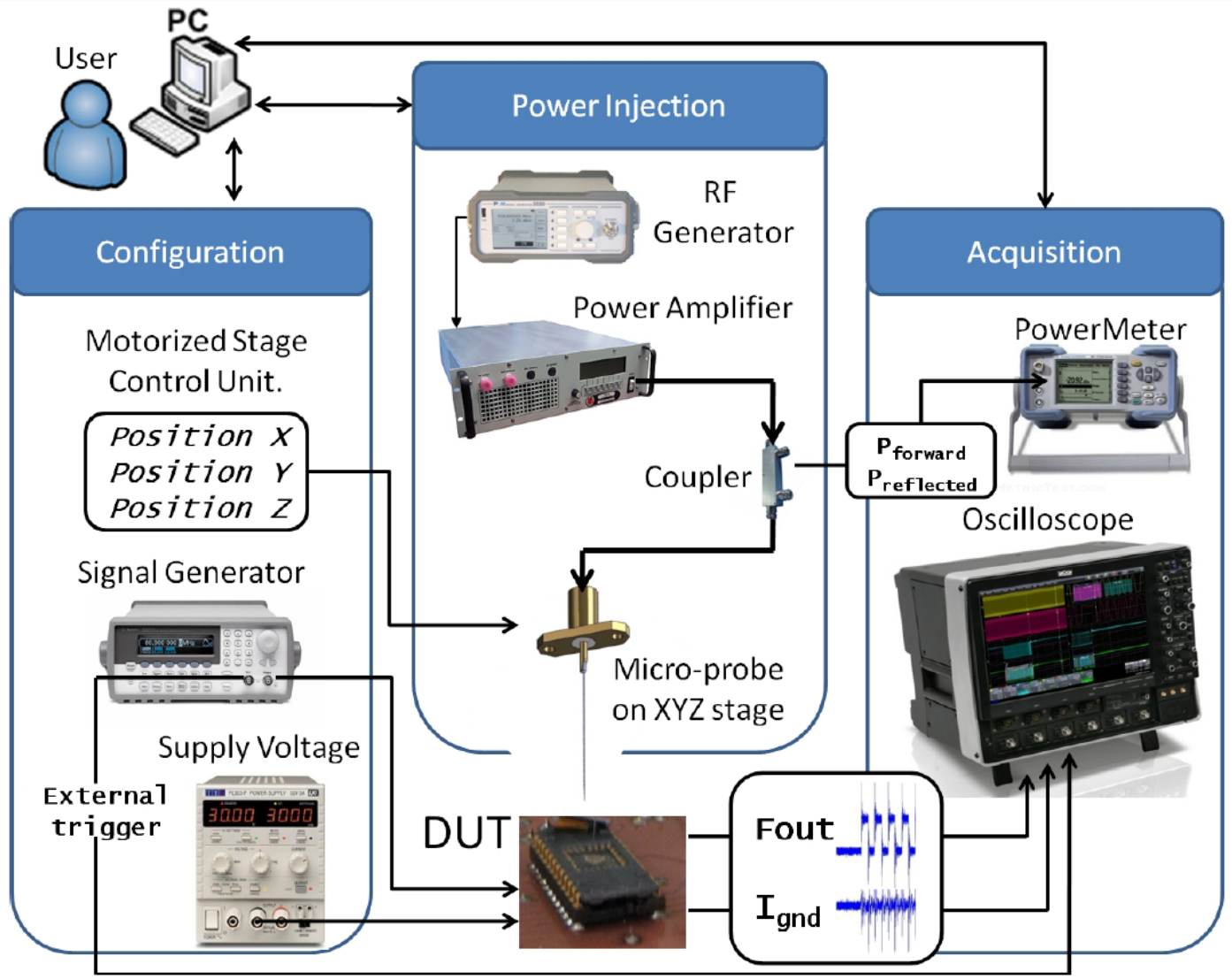


EM Side Channel Analysis

Design	Power Analysis			EM Analysis		
	Key bytes found	Mean Guessing Entropy	# traces ($x10^3$)	Key bytes found	Mean Guessing Entropy	# traces ($x10^3$)
Unprotected	15	1	205	16	1	155
+ Linear Masking	4	54	275	8	52	275
+ Dynamic Map	5	34	287	9	17	287
+ Dynamic Reloc	7	19	250	12	9	250
+ All	0	136	283	0	94	283



Injection Platform

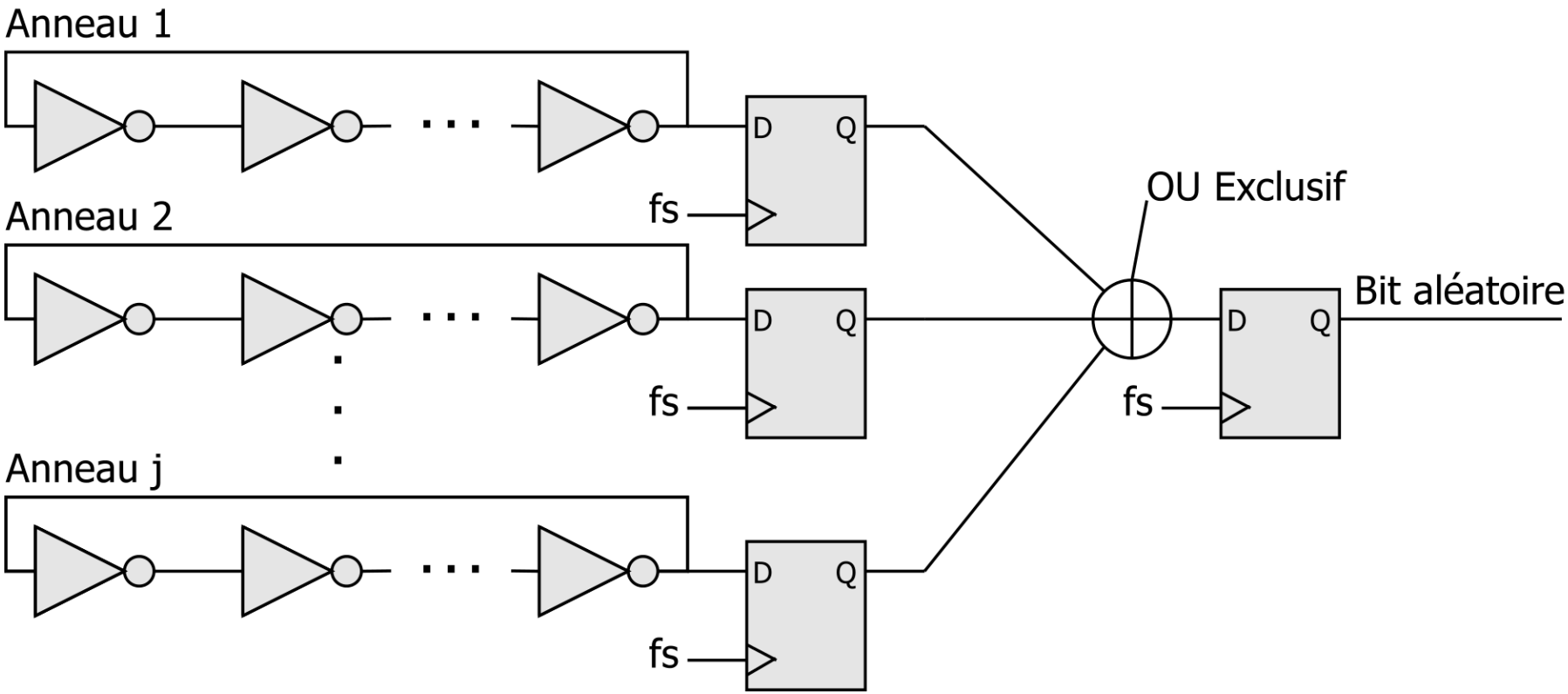


Fault Injection Results

- Ring Oscillators
- Random Number Generators
- Cryptographic Coprocessors
- General purpose CPUs

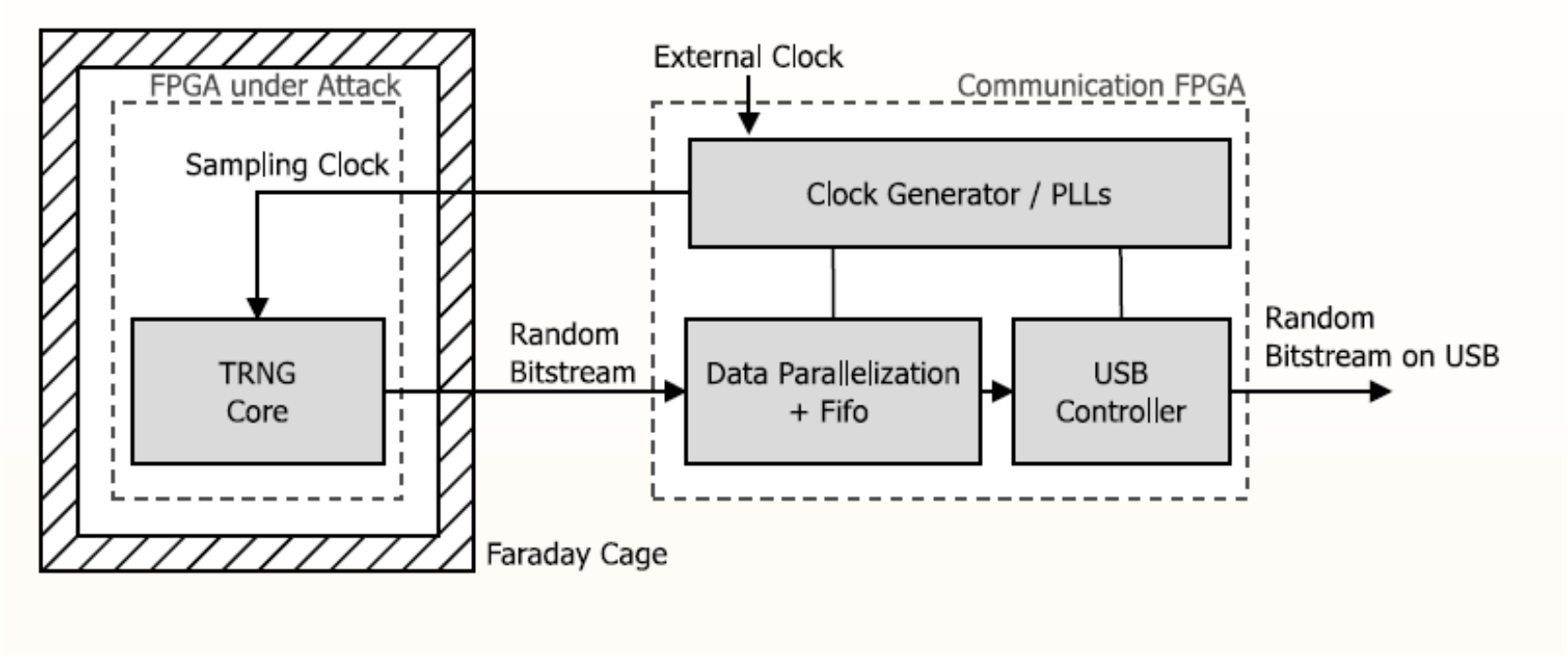
Target: Ring Oscillators based TRNG

- Use the Ro-generated clock jitter as a source of randomness
- ROs should be independent



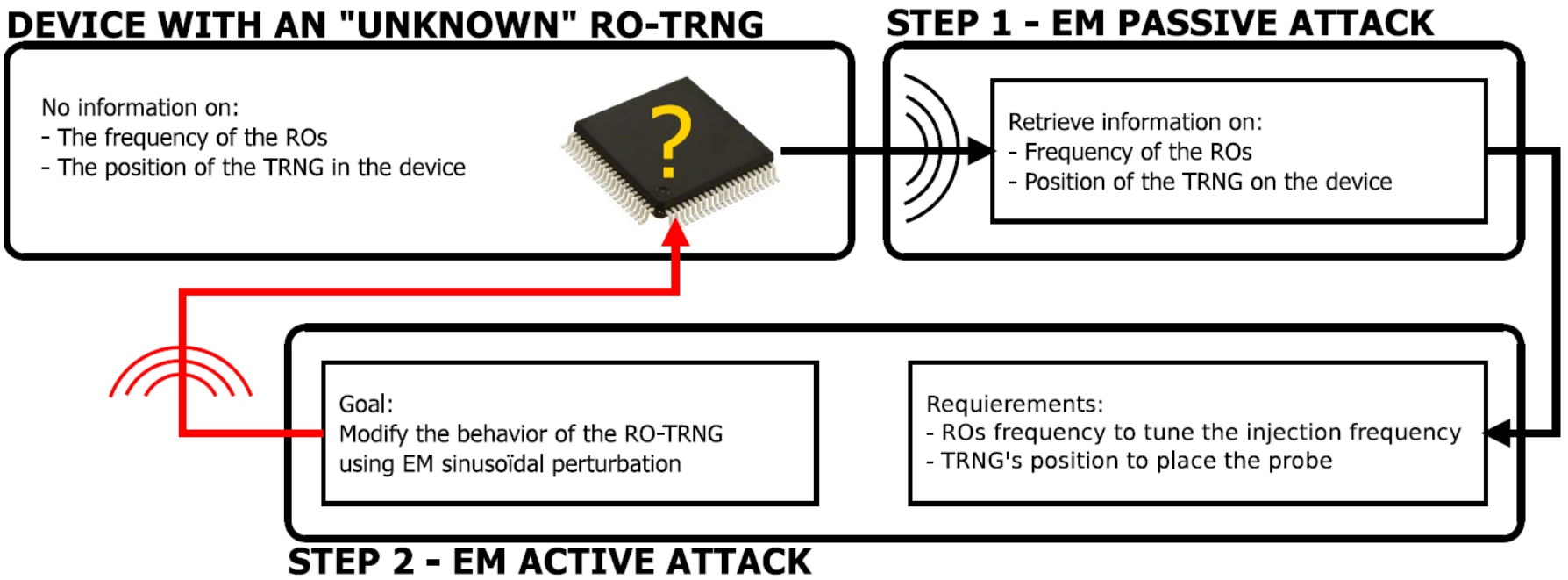
Design architecture

- The TRNG core is a 50 ROs Wold TRNG
- Working frequencies of the ROs are around 320 MHz
- Sampling frequency: 24 KHz

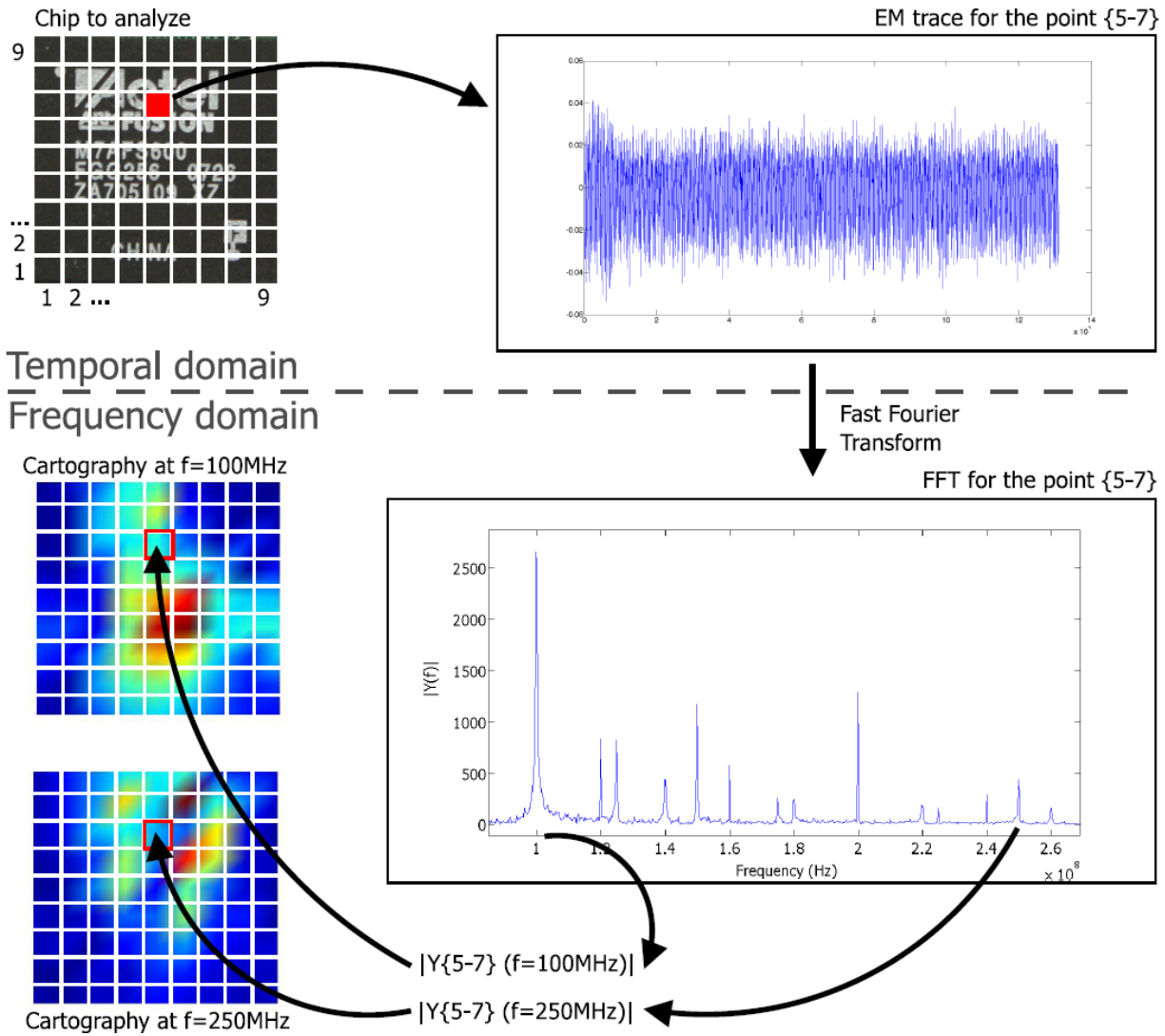


Attack scenario

- Complementary passive and active EM attacks



Passive attack: EM cartography

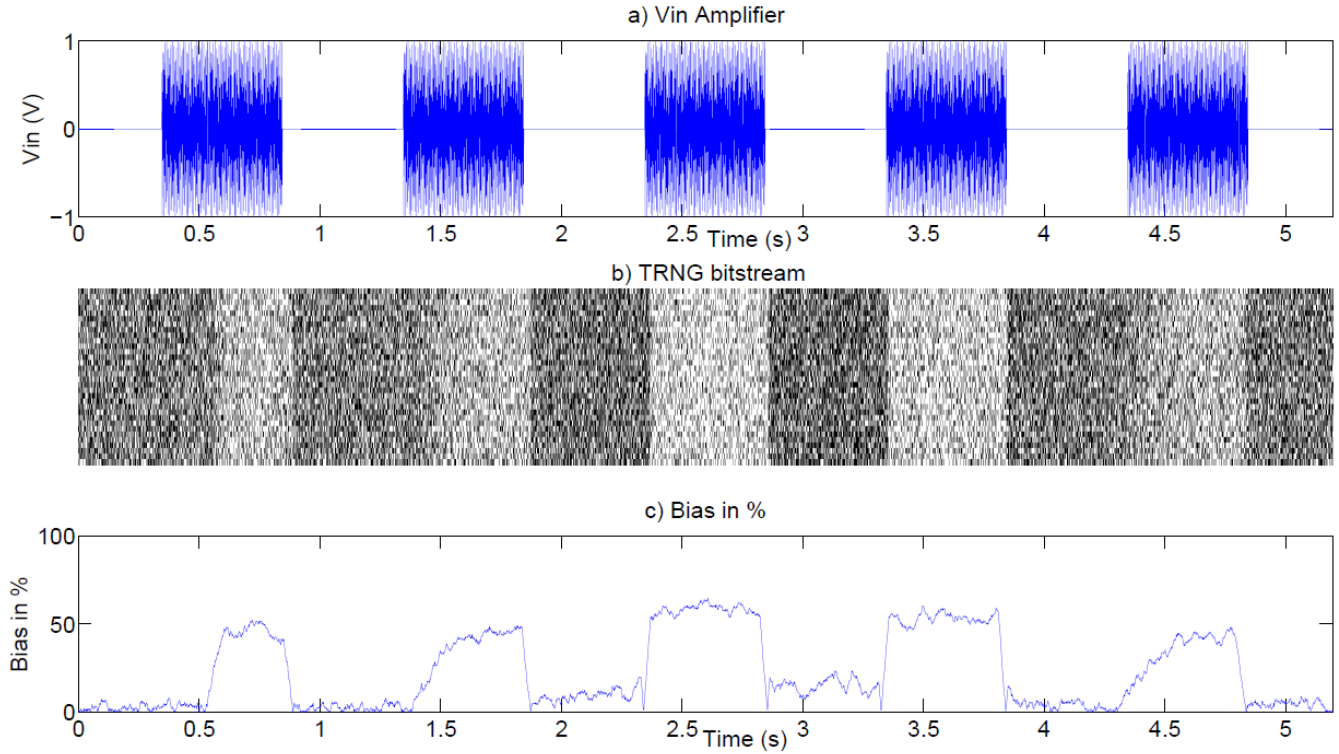


Active attack: EM harmonic injection

PForward	No Injection	210 μW	260 μW	300 μW
Bias%	0.1%	15.87%	51.57%	55%
NIST tests	SUCCESS	FAIL	FAIL	FAIL

Dynamic behavior in case of active attack

- The attacks is effective only during the period of the attack.
- The setup and falling time of the attack is directly proportional to the performance of the EM bench



Fault Injection Results

- Ring Oscillators
- Random Number Generators
- Cryptographic Coprocessors
- General purpose CPUs

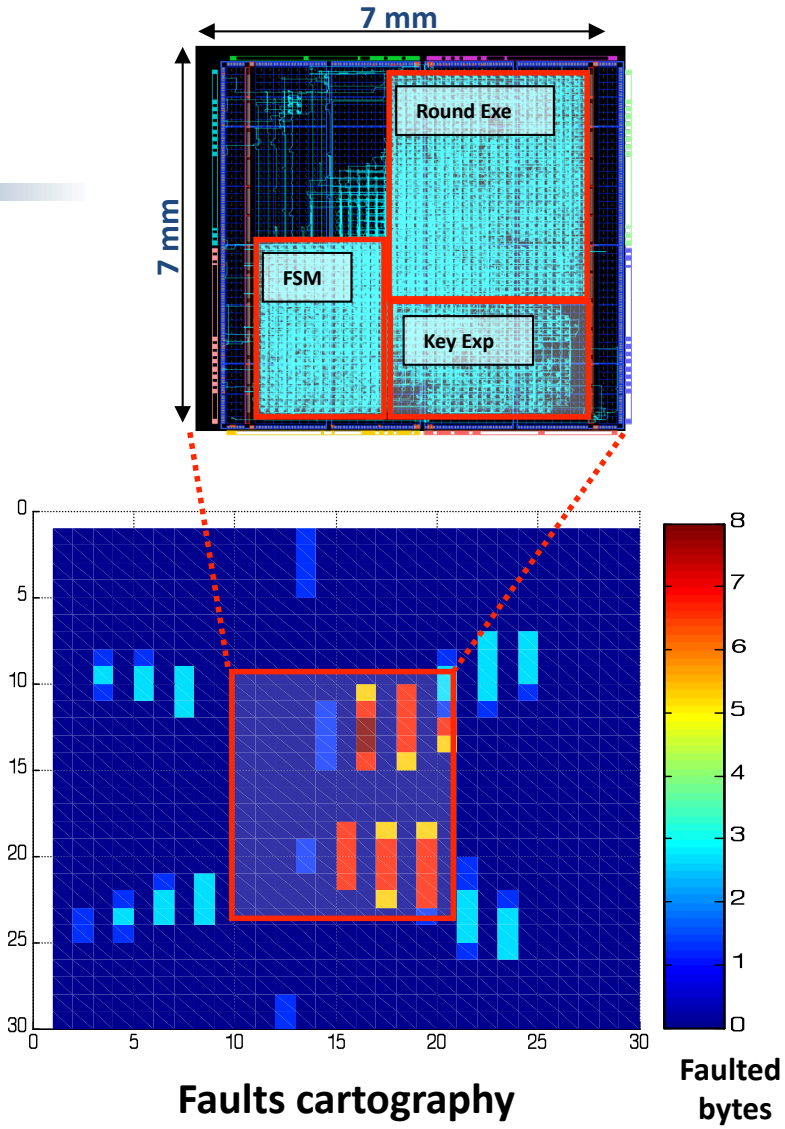
Crypto-Coprocessors

- FPGA Spartan 3 (**130nm)**
- Iterative **Hardware AES** implementation
- **100 MHz @ 1.2 volts**

- At each position, an **EMP** is injected **100V-10ns**
- The corresponding faulted ciphertext is retrieved
- **1,000 encryptions** of the same plaintext
- 30x30 different locations
- Antenna **diameter** : **500 µm**
- Displacement **step** : **500 µm**

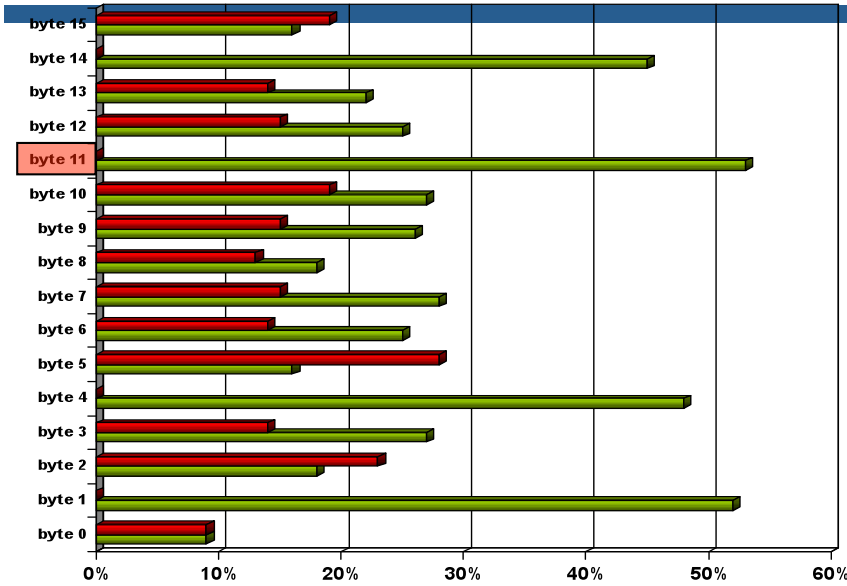
EMP parameters

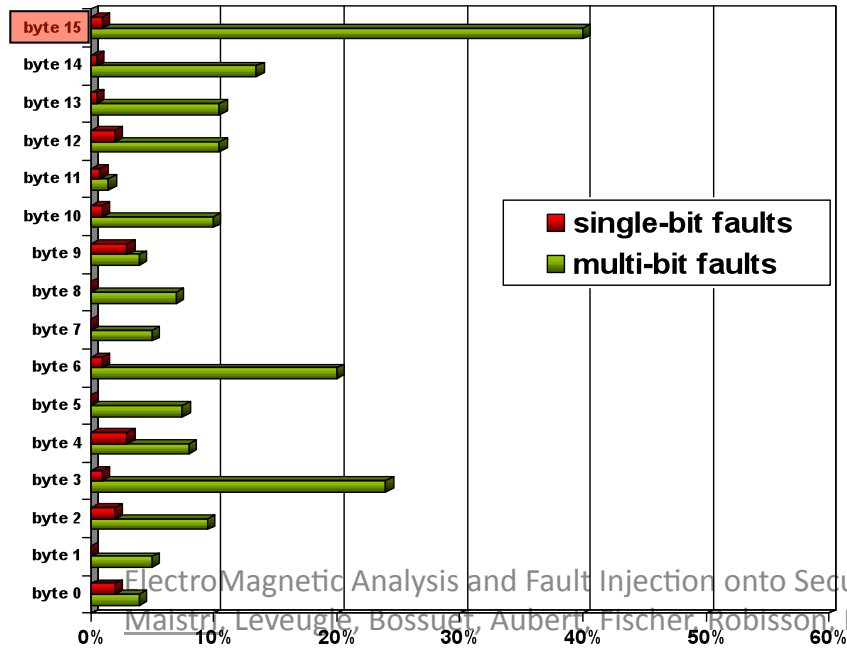
Z position	EMP amplitude	EMP width	Clk period	Rise/fall times
< 500 µm	100V	10ns	10ns	5ns

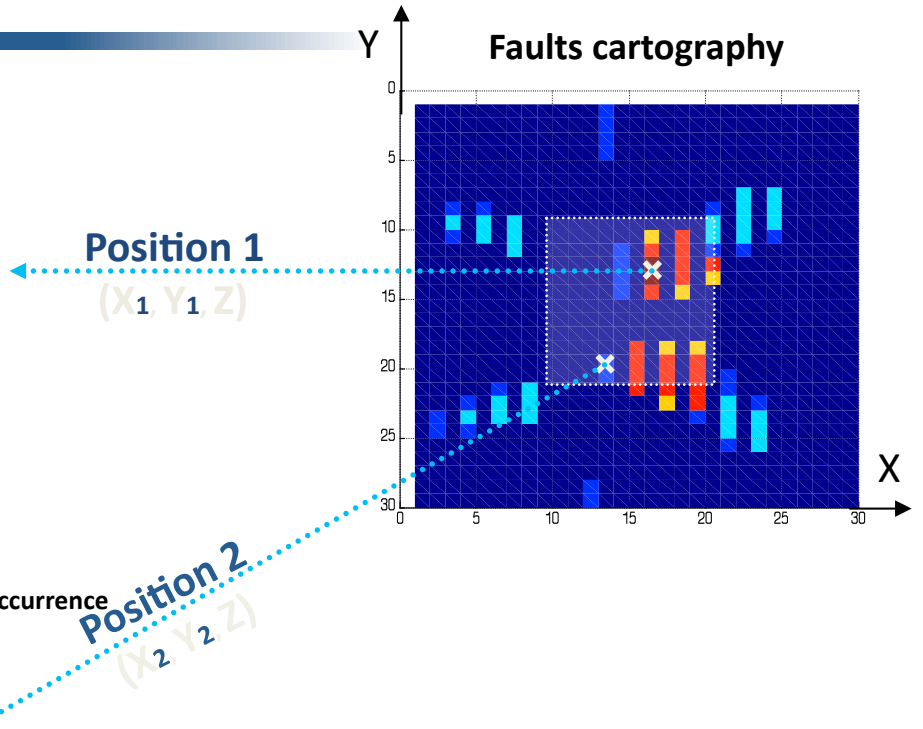


- Localized effect of the **EMP**
- Good correlation between the Floorplan and the cartography
- Deterministic and **reproducible effect**

Crypto-Coprocessors







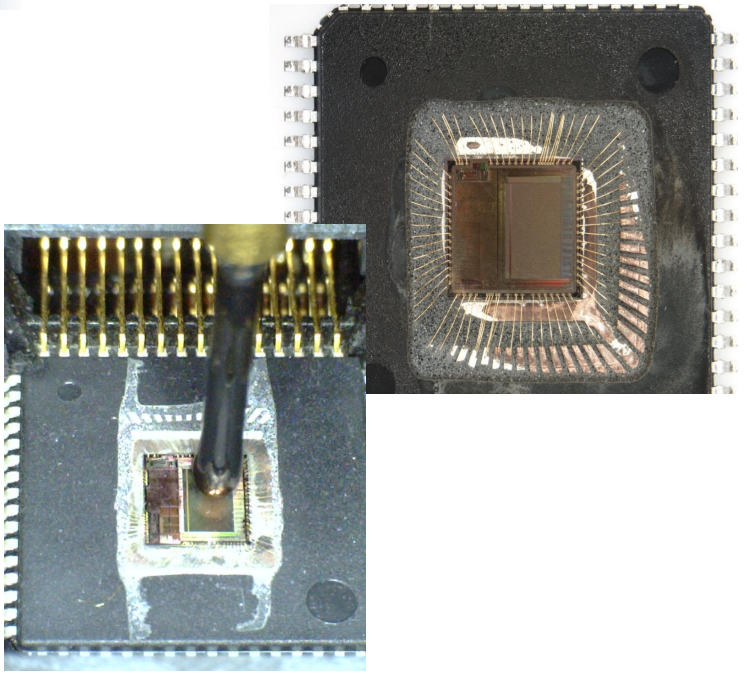
- Ability to inject **single-bit** and **multi-bits** faults into AES calculations
- Induced faults are **timing faults** (see later)
- May fault any paths (even **subcritical** paths)

Fault Injection Results

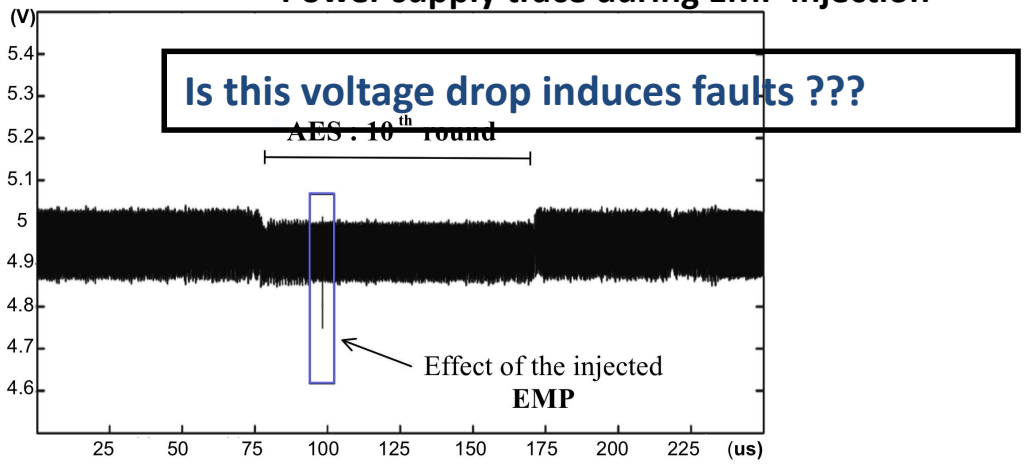
- Ring Oscillators
- Random Number Generators
- Cryptographic Coprocessors
- General purpose CPUs

General Purpose CPU (1/2)

- Smartcard emulation board
- 8-bits AVR Atmega 128 MCU (techno **0,35µm**)
- Harvard architecture
- 128 KB Flash program memory
- 4 KB SRAM
- Operating voltage : **4.5 – 5.5 V**
- Operating frequency : **3.57 MHz** => **Tclk = 280 ns**
- **Software AES** implementation



Power supply trace during EMP injection



Voltage drop of about 200 mV

EMP parameters

Z position	EMP amplitude	EMP width	Clk period	Rise/fall times
< 500 µm	100V	50ns	280ns	5ns

General Purpose CPU (2/2)

Faulted byte #	Injection time
0	$0.3\mu s$
1	$9.78\mu s$
2	$19.3\mu s$
3	$33.7\mu s$
4	$55.7\mu s$
5	$12.4\mu s$
6	$63.4\mu s$
15	$87.5\mu s$

- Deterministic and **reproducible effect**
- **EMP injection prevents the CPU from executing some instructions by violating the timing constraints**

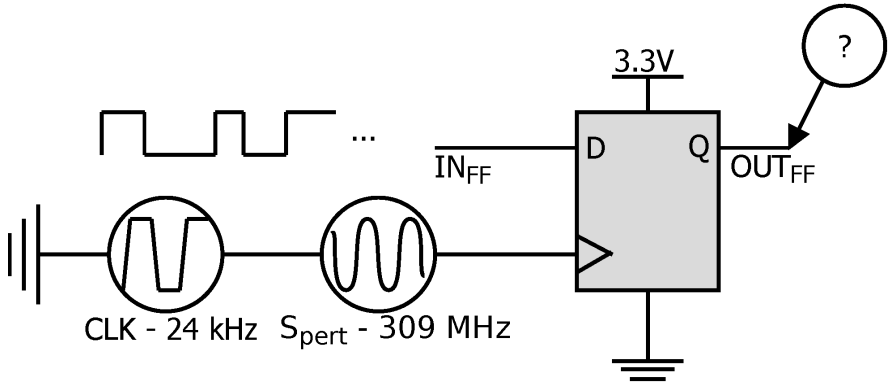
Advanced Modeling

- Harmonic injections
- Pulsed injections
- Power coupling

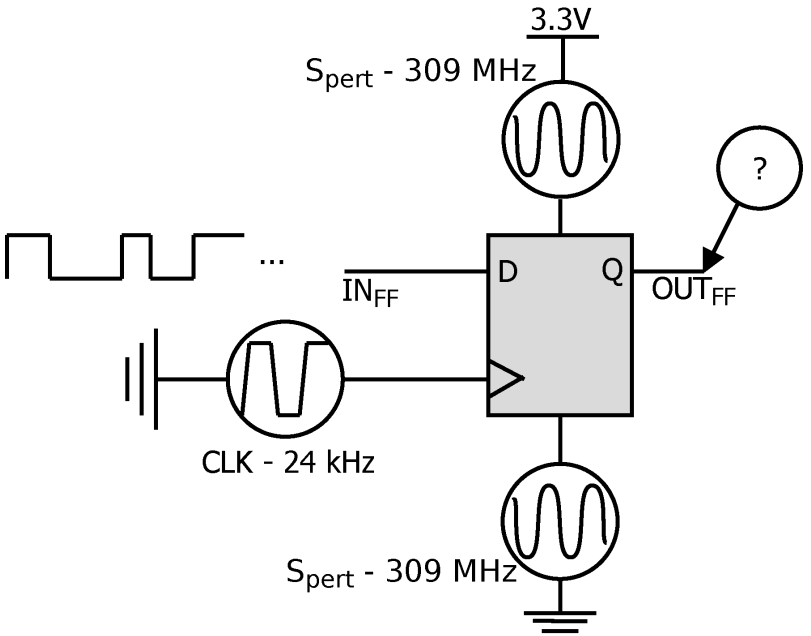
Harmonic injections

- Faults on DFF used for RO sampling
  - Erroneous sample on (some) clock falling edges
  - Some values not correctly sampled on rising edge (rarer)
- Two possible models describing the behavior:

Model for Electric field



Model for Magnetic field

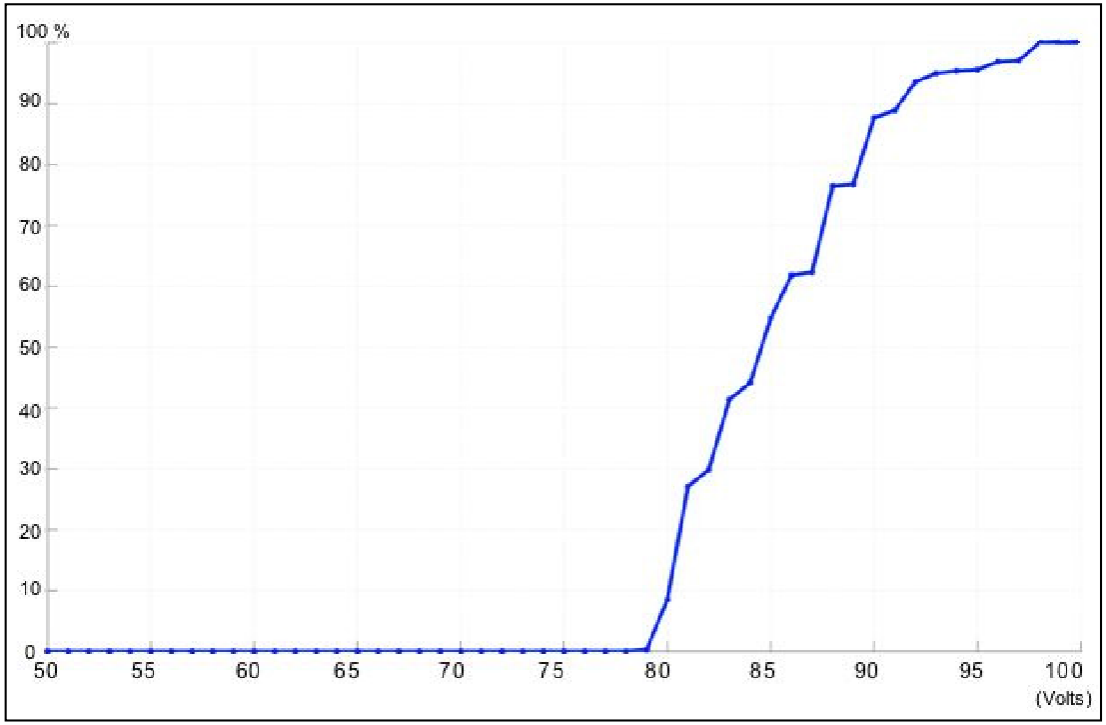


Advanced Modeling

- Harmonic injections
- Pulsed injections
- Power coupling

Pulsed injections

- Strong resemblance to errors from delay faults
  - Increased injected power => Increased error probability
  - Precise clock glitches => very similar error patterns



Pulsed injections

- Strong resemblance to errors from delay faults
  - Increased injected power => Increased error probability
  - Precise clock glitches => very similar error patterns
- Interaction EM pulse <> power-ground network
  - Additional delivered energy alters the differential voltage supply
  - Logic under the EM pulsed injection is subject to a lower tension
  - Signal transitions are slower
  - Slowdown larger than available slack → Timing violation
- EM pulsed injections vs Clock/Voltage perturbations:
  - EM local delay fault → Specific locations can be targeted

Advanced Modeling

- Harmonic injections
- Pulsed injections
- Power coupling

Power Coupling

	EM Pulse	IR-drop
Spatial connotation	Local	Local
Temporal connotation	Transient	Transient/Dynamic
Effect	Voltage drop	Voltage drop
Source	External	Internal
Origin	Fault injection	Data-dependent computation

- Use IR-drop analysis to
  - Predict most vulnerable regions of the circuit
  - Simulate EM pulses (What-If analysis)
  - Correlate EM/IR-drop cartographies

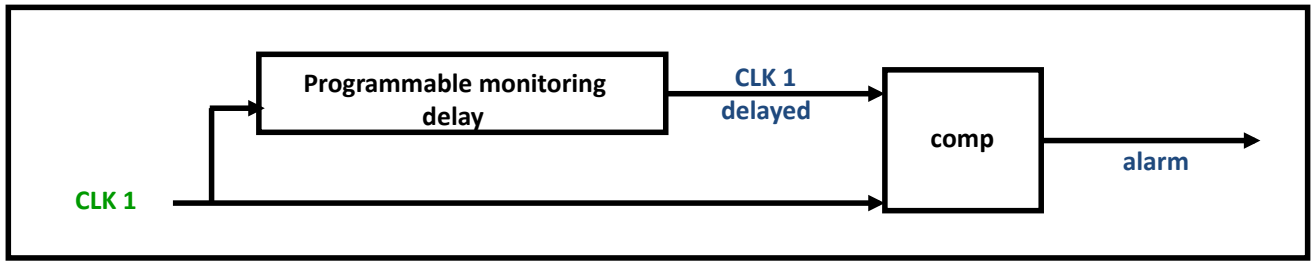
Conclusion

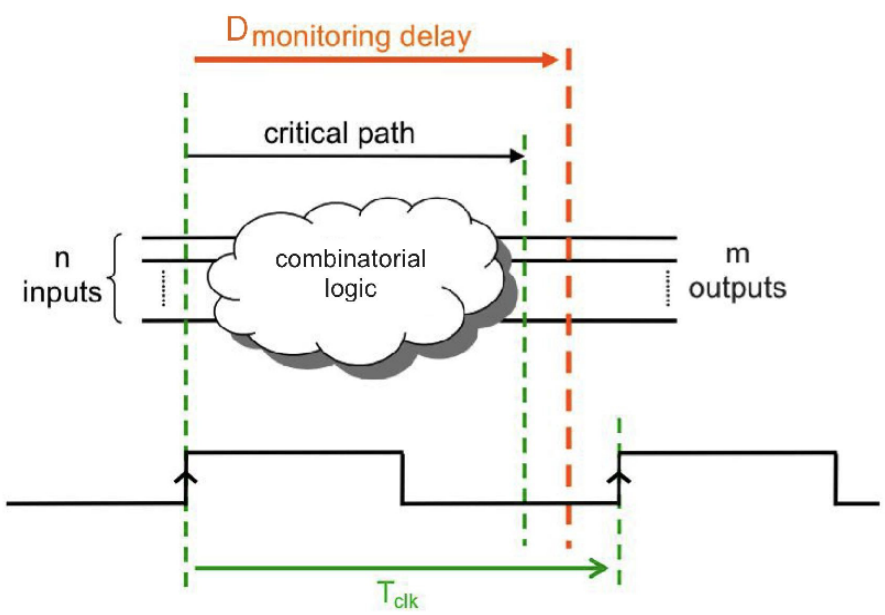
- We demonstrate that it is possible to dynamically control the bias of a RO-TRNG embedded in an FPGA
- The effectiveness of our proposed coupled attack questions the use of ring oscillators in the design of TRNGs

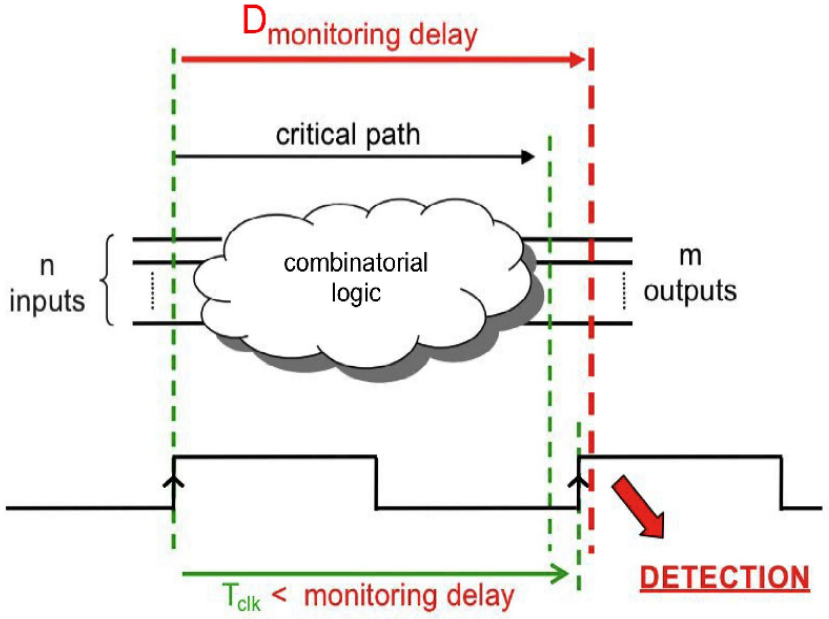
Q & A

BACKUP SLIDES

Hardware Countermeasure (1/2)

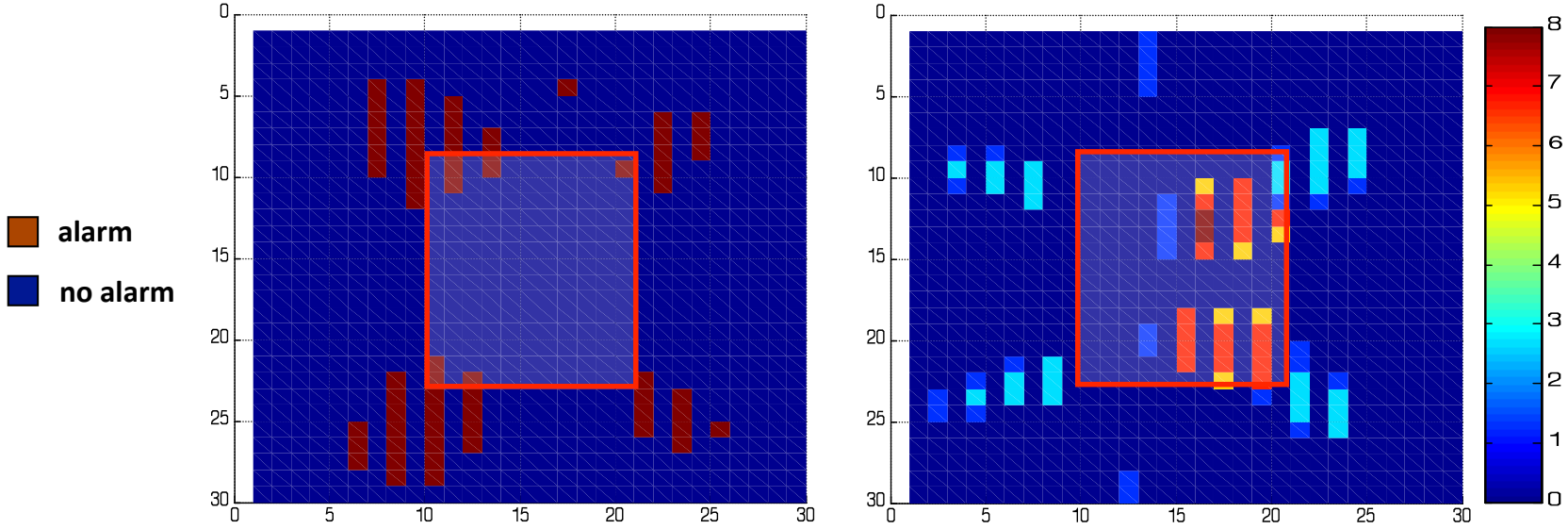






Hardware Countermeasure (2/2)

- At each position, an **EMP** is injected
- **1,000 encryptions** of the same plaintext
- **30x30 different locations** of the injection probe (step 500 µm)



- Localized effect of the **EMP**
- The EMP is detected only in some positions
- Possibility to induce faults without triggering the alarm