Transient Effect Ring Oscillators Leak Too

CryptArchi

25/06/2019

Ugo Mureddu, Brice Colombier, Nathalie Bochard,
Lilian Bossuet, Viktor Fisher

Univ Lyon, UJM-Saint-Etienne, CNRS,
Laboratoire Hubert Curien UMR 5516,
F42023 Saint-Etienne France

LABORATOIRE HUBERT CURIEN

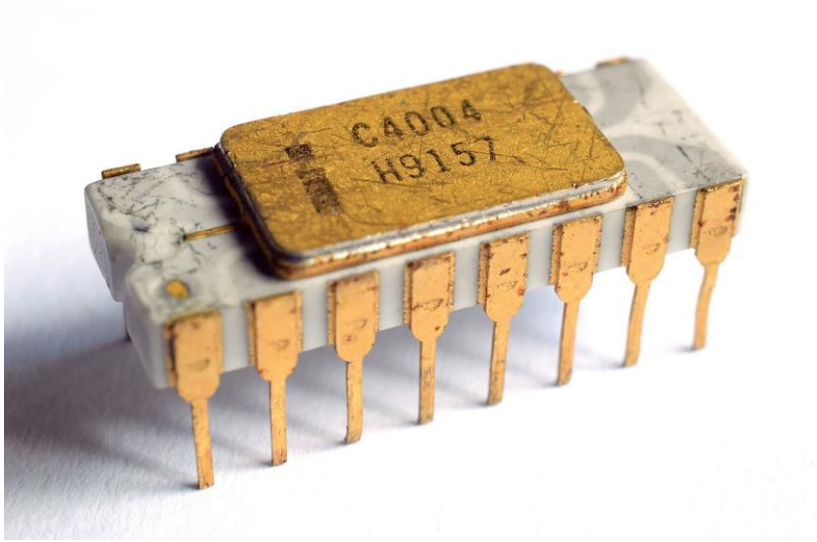
Current industrial context

Context 1/2: electronic advances

1971: Intel 4004

⇨ 2300 transistors

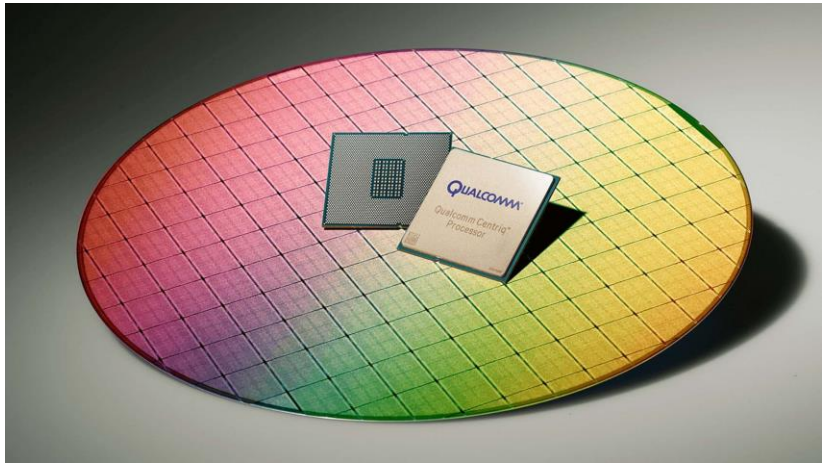
⇨ transistor size: 10 µm



2017: Qualcomm Centriq 2400

⇨ 18 billion transistors

⇨ transistor size: 10 nm



Context 2/2: electronic advances

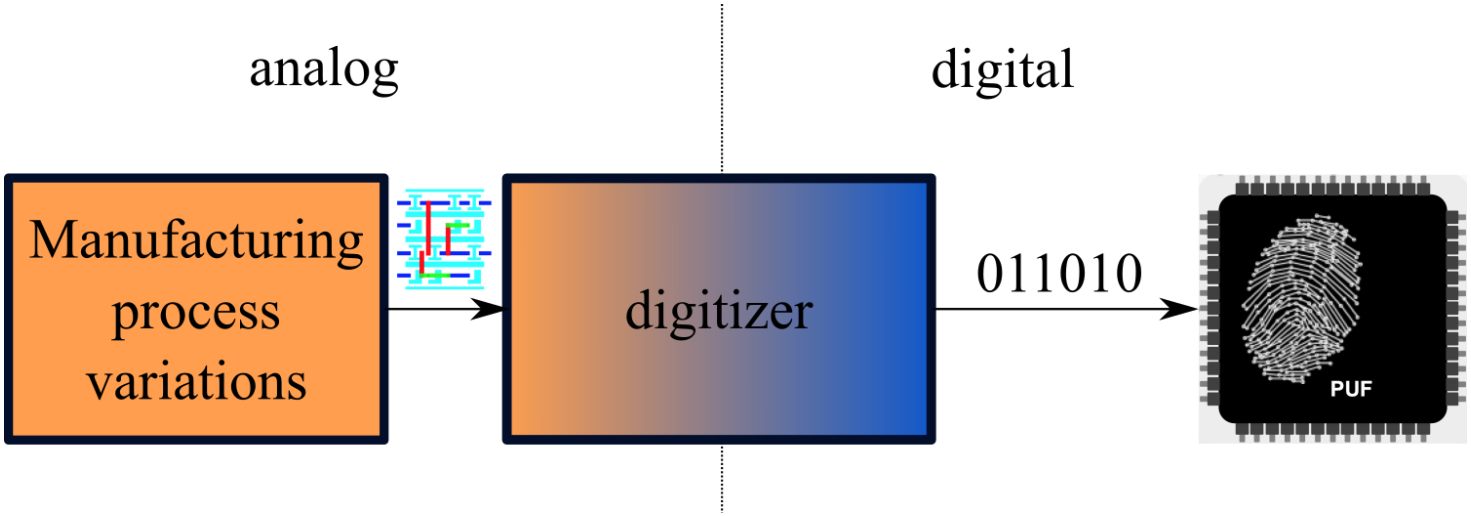
- Internet of Things
  - About **11 Billion** connected objects in 2018 [1]
  - Expected to be 125 Billion in 2030 [1]
  - Huge risks of unauthorized use or abuse

[1] *https://www.forbes.com/sites/louiscolumbus/2018/12/13/2018-roundup-of-internet-of-things-forecasts-and-market-estimates*

PUF

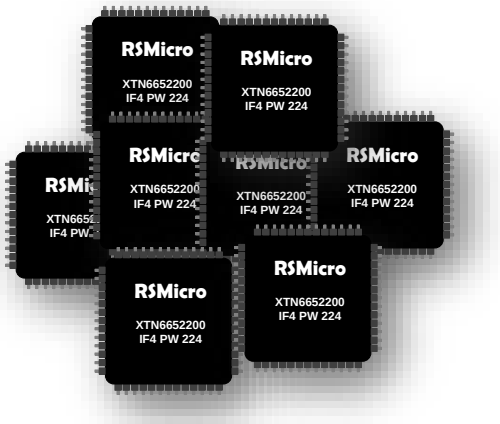
What is a Physical Unclonable Function (PUF)?

- Exploit a random static phenomena: process variations at transistor level
- In digital circuits: **comparison of supposedly identical structures**
- Applications: Intrinsic identification of chips



What is a Physical Unclona Function (PUF)?

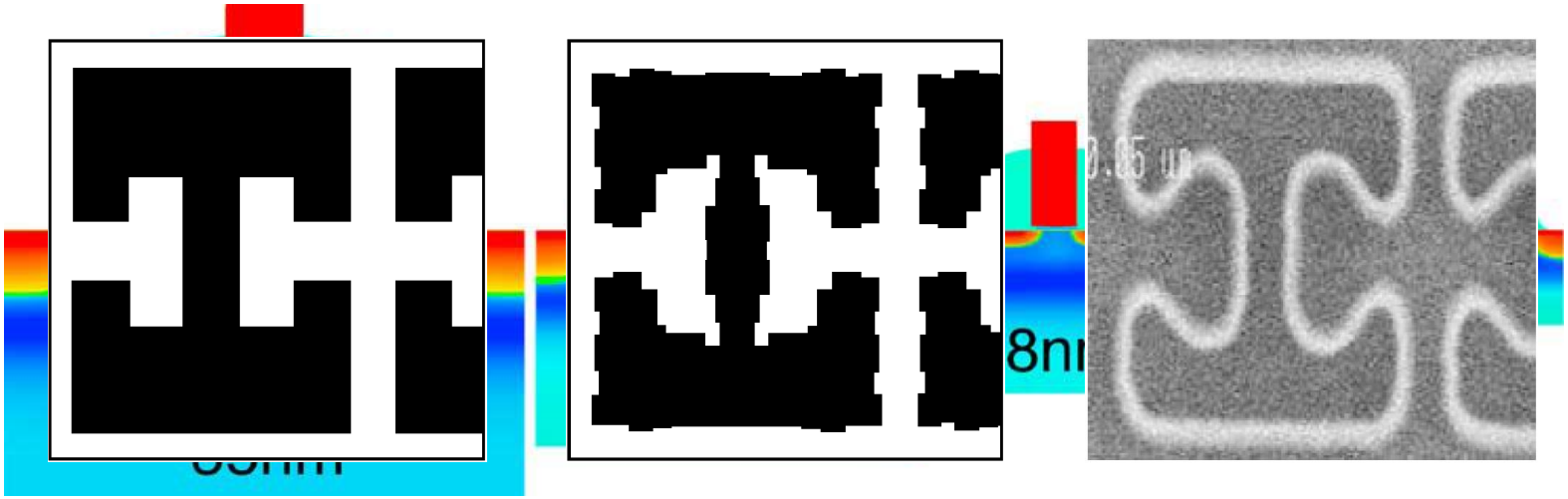
- Intrinsic identification of chips
- Hardware traceability
- Example from a set of identical integrated circuits



ID	IC
AF30	
37B1	
8992	
FE72	
E90B	
5129	
8C9D	
253A	

Manufacturing process variations

- Manufacturing process variations (MPV)
  - Reducing the size of electronic components ⇨ Increases MPV



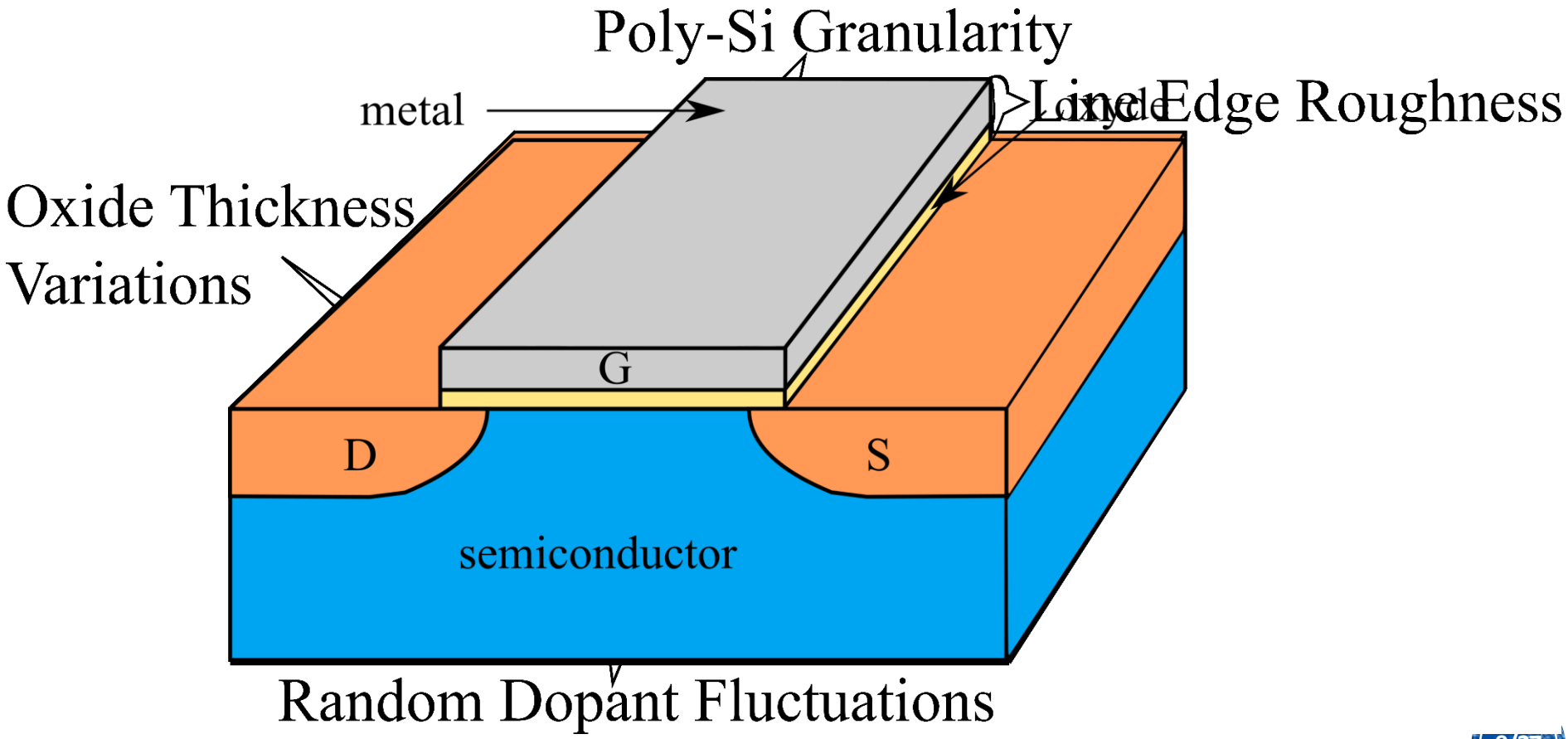
Expected Optical proximity correction On wafer

[W13] M.Wirnshofe, "Variation-aware adaptive voltage scaling for digital

[BRA07] A.Brown, G.Roy, and A.Asenov,,"Poly-Si-Gate-Related Variability in Decananometer MOSFETs With Conventional Architecture," IEEE transactions on electron devices 2007

CMOS process variations

- Affect the switching speed of the transistors



PUF architectures in logic devices

Mostly based on oscillating rings!
Very sensitive to process variations.

- Moroz[illegible] [MMS10]
  - Arbiter VS RO VS Butterfly
  - Target Xilinx Spartan-3E FPGA
  - *"Symmetry requirements for Arbiter and Butterfly PUF cannot be satisfied using available FPGA routing schemes …. Such a RO based PUF can produce a working PUF"*

[MMS10] S. Morozov, A. Maiti, P. Schaumont, "A Comparative Analysis of Delay Based PUF Implementations on FPGA," 6th International Symposium on Applied Reconfigurable Computing, March 2010

- Maiti et al. HOST 2010 [MCMP10]
  - RO PUF
  - 125 Xilinx Spartan-3E FPGA, 512 RO/FPGA
  - *"RO-PUF output signatures are fairly uniformly distributed with high rate of uniqueness in terms of inter-die Hamming distance"*

[MCMP10] A. Maiti, J. Casarona, L. McHale and P. Schaumont, "A large scale characterization of RO-PUF," in Proc. of Int. Sym. on Hardware-Oriented Security and Trust (HOST), IEEE, 2010, pp.94-99.

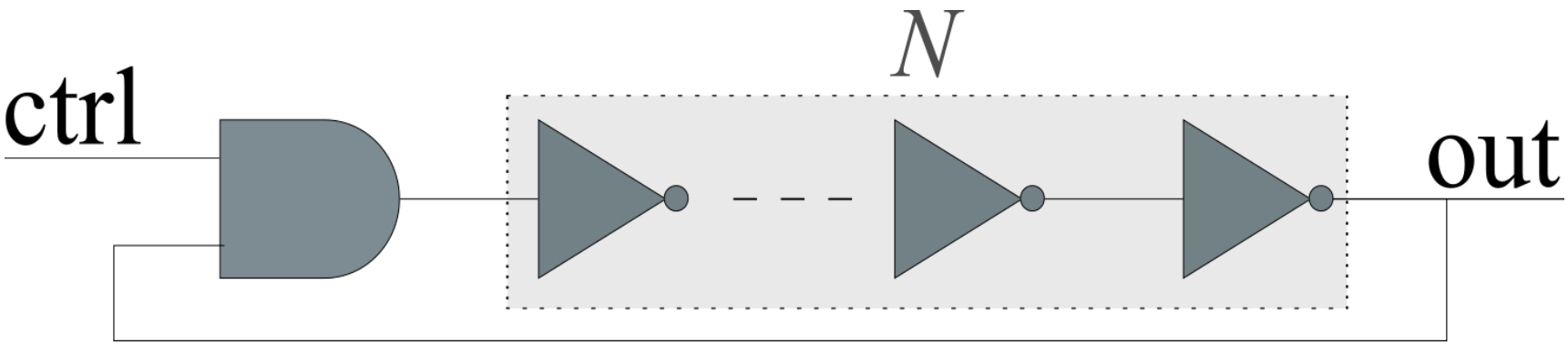
- Maiti et al. NIST worshop 2011 [MCMP11]
  - Arbiter VS RO
  - 193 Xilinx Spartan-3E FPGA
  - *"RO-PUF exhibited better performance compared to Arbiter PUF even if the former is implemented on a bigger device"*

[MCMP11] A. Maiti, J. Casarona, L. McHale and P. Schaumont, "A Framework for the Evaluation of Physical Unclonable Functions," in Proc. of NIST Work. on Crypto. For Emerging Tech. and Appl., 2011.

- Katzenbeisser et al. CHES 2012 [KKR+12]
  - Arbiter VS RO VS SRAM VS FF and latch
  - Target: 96 ASIC TSMC 65 nm CMOS
  - *"The SRAM and RO PUFs achieve almost all desired properties of a PUF"*

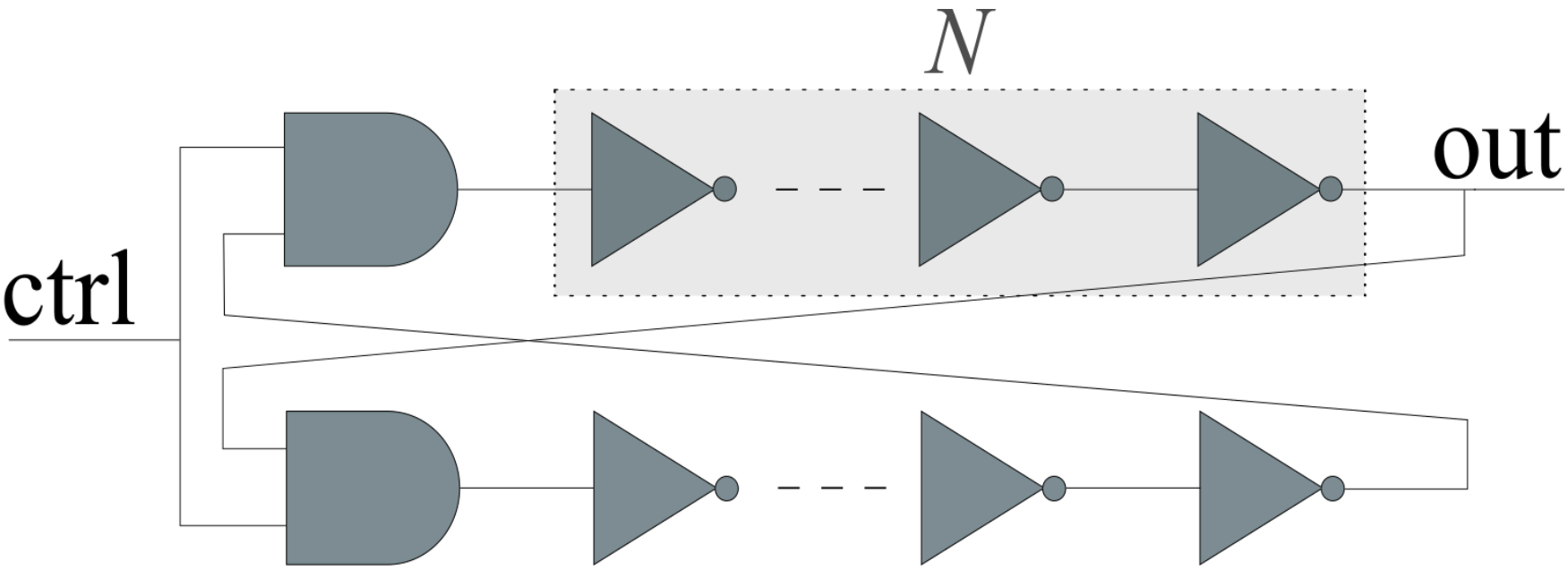
[KKR+12] S. Katzenbeisser, Ü. Kocabaş, V. Rožić, A.R. Sadeghi, I. Verbauwhede, C. Wachsmann. "PUFs: Myth, Fact or Busted? A Security Evaluation of Physically Unclonalble Functions Cast in Silicon" in Proc. of Int. Conf. on Cryptographic Hardware an Embedded Systems (CHES), Spinger, LNCS, vol. 7428, 2012, pp. 283-301.

Studied cells: Ring Oscillator (RO)



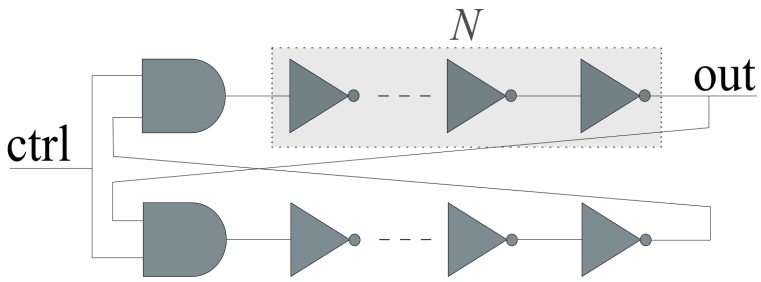
- Composed of an odd N number of inverters and a gate to activate it

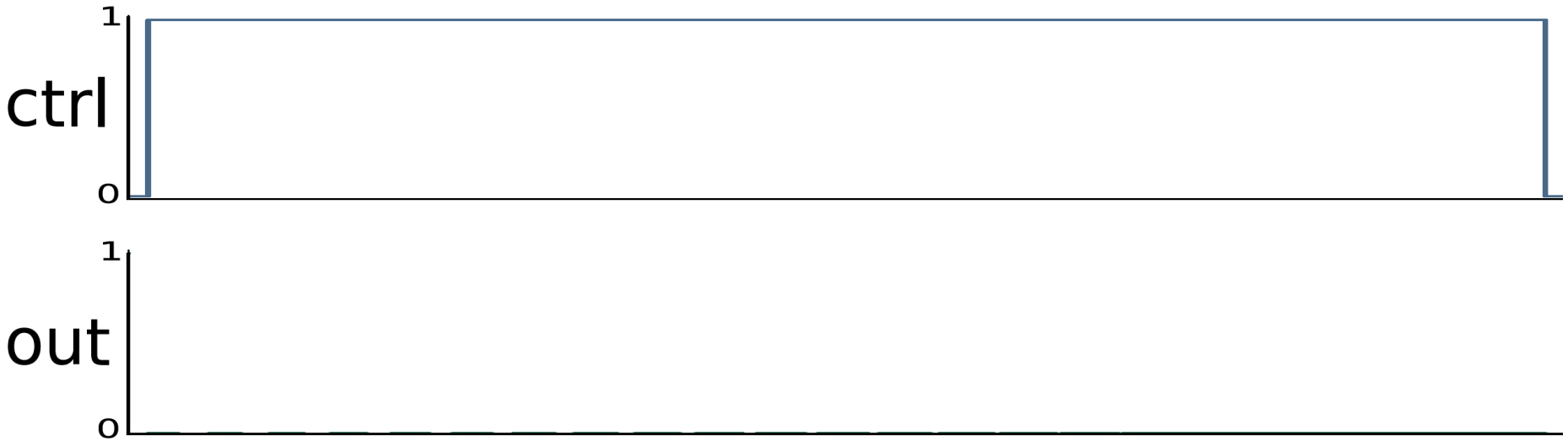
Studied cells: Transient Effect Ring Oscillator (TERO)



- An electronic circuit that oscillates temporarily
- Composed of an even 2xN number of inverters and a couple of gates to activate it

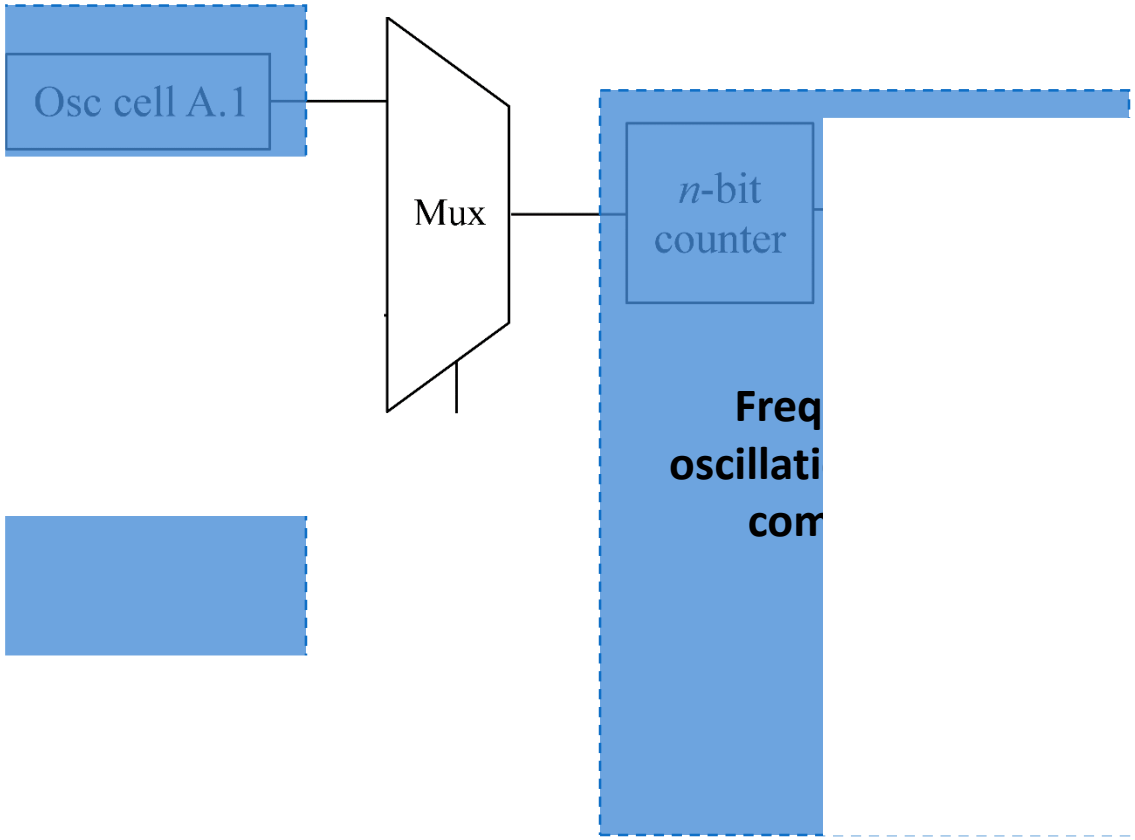
Studied cells: Transient Effect Ring Oscillator (TERO)





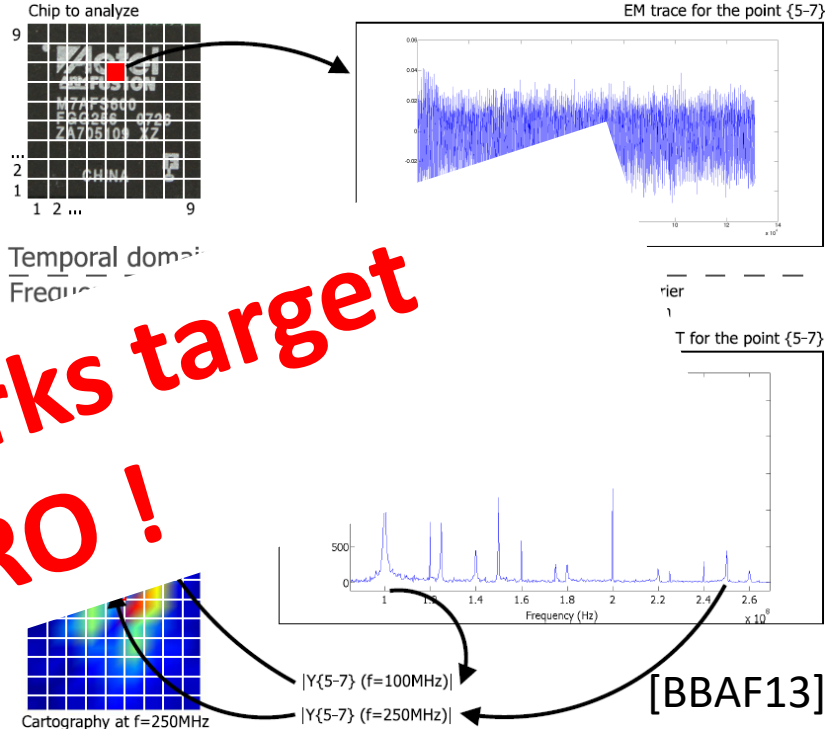
- Two events propagate into the cell
- Duty cycle of the output will move from 50% to 0% or 100% and stop the oscillations

Oscillator based PUF architecture



EM analysis on RO

- Method: using the electromagnetic radiation to analyze RO
- Finding : RO frequencies and physical localization
- EM frequency cartography
- Near-field probe



[BBAF13]

All those works target only RO !

[MSSS11]

[MSSS11] D. Merli, D. Schuster, F. Stumpf, and G. Sigl, "Semi-invasive EM attack on FPGA RO PUFs and countermeasures," in Proceedings of the Workshop on Embedded Systems Security, WESS '11, (New York, NY, USA), pp. 2 :1–2 :9, ACM, 2011.

[BBAF13] P. Bayon, L. Bossuet, A. Aubert, V. Fischer. EM radiation analysis on true random number generators: Frequency and localization retrieval method. In Proceedings of the IEEE Asia-Pacific International Symposium and Exhibition on Electromagnetic Compatibility (APEMC 2013),Melbourne, Australia, May 2013.

Objectives

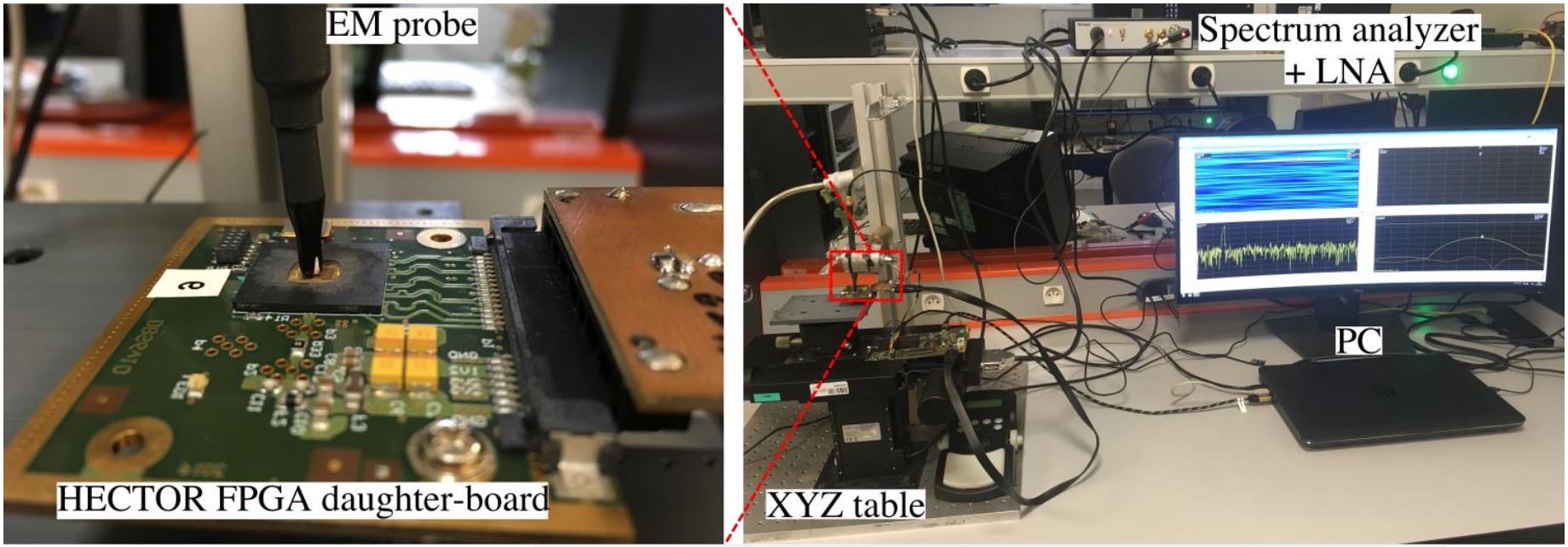
- Evaluate the possibility of an EM analysis on TERO
  - Finite number of oscillations
  - Is it possible to intercept EM radiation?

What about TERO?

Electromagnetic analysis of TERO

Experimental setup

- FPGA platform HECTOR [LDFV18] : experiments made on Xilinx Spartan 6 and Intel Cyclone V FPGAs
- EM probe RS H 2.5-2 from Rohde & Schwartz
- Real time spectrum analyzer RSA607a from Tektronix
- XYZ table

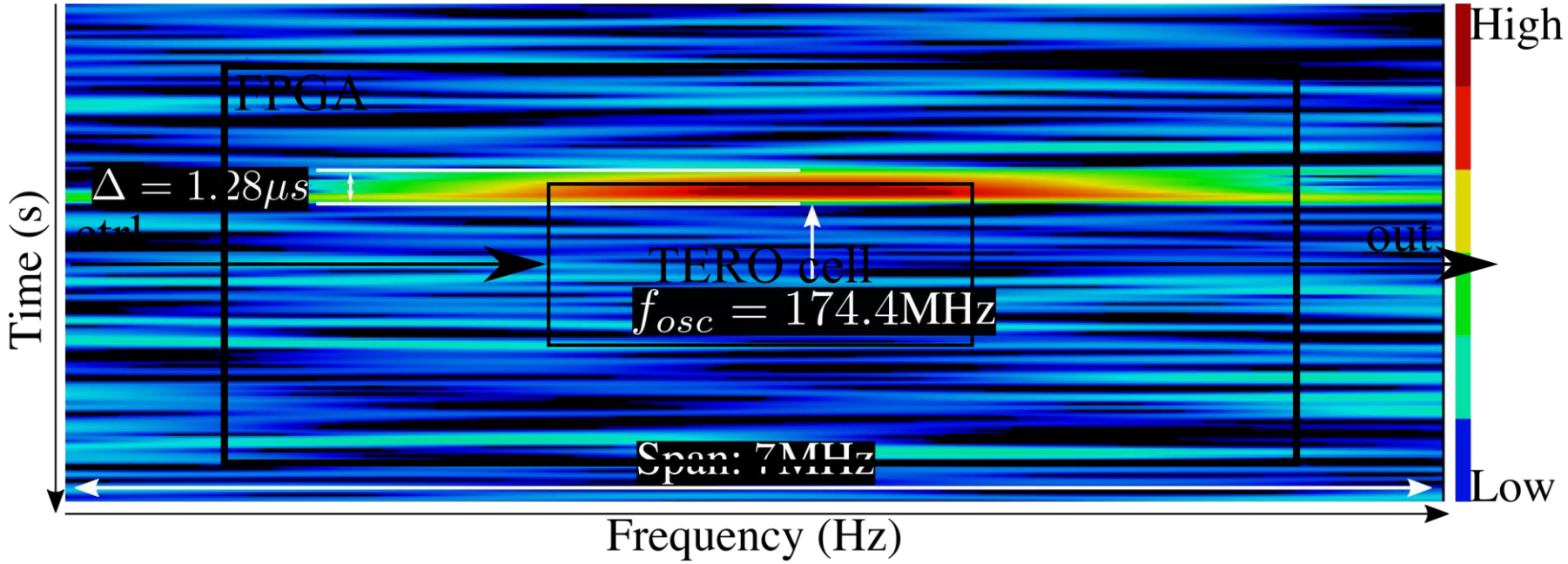


[LFV18] : M.Laban,M.Drutarovsky,V.Fischer,andM.Varchola,"Modular evaluation platform for evaluation and testing of physically unclonable functions," in 28th International Conference Radioelektronika, April 2018, pp. 1–6.

EM analysis of one TERO cell

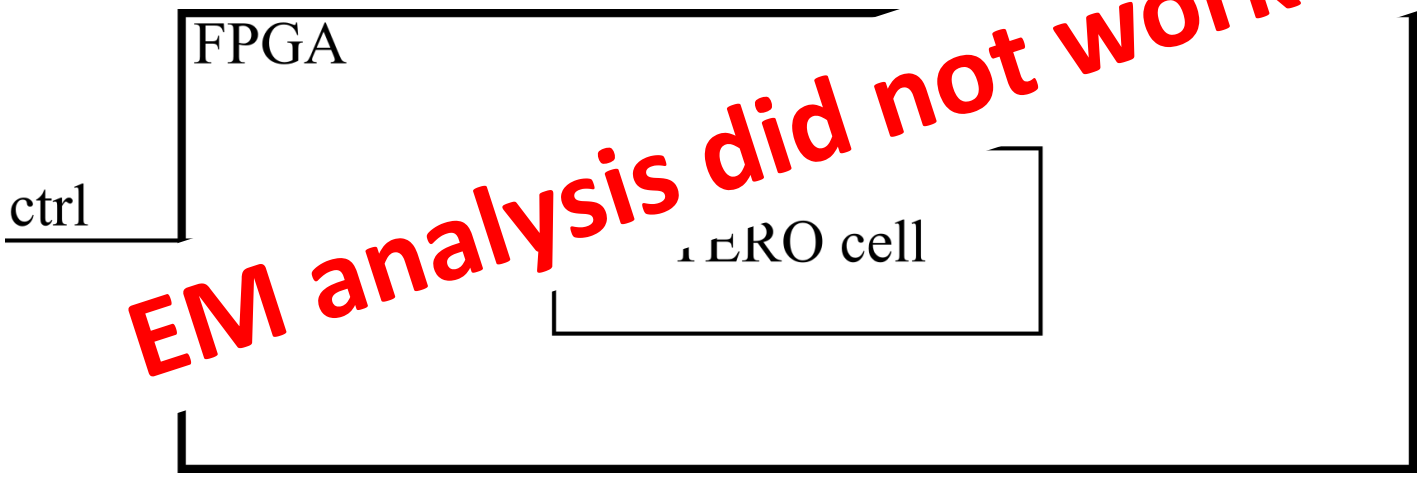
⚠ N_{osc} **can be retrieved**

- TERO cell periodically restarted
- Frequency + duration of oscillation ⇨ N_{osc} = 223



EM analysis of one TERO cell

- Same TERO cell
- TERO output stays inside the FPGA

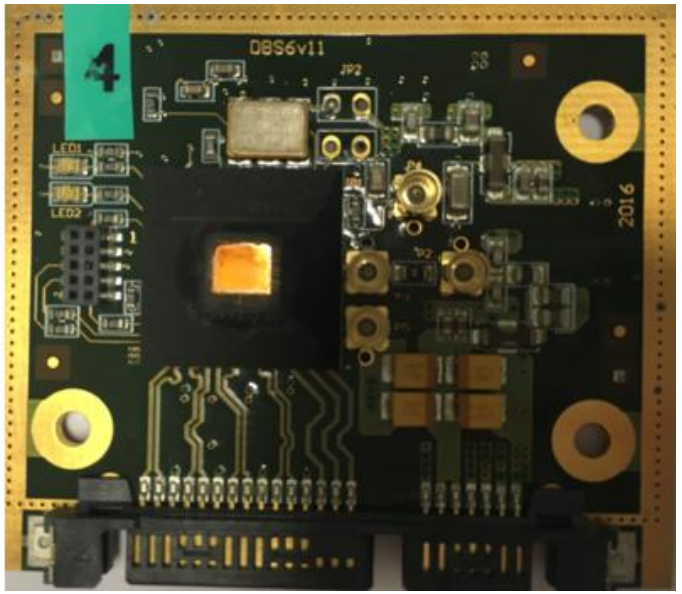


EM analysis of one TERO cell

⚠ N_{osc} **can be retrieved**

- FPGA decapsulation with acid mix: nitric (HNO_3)/sulfuric (H_2SO_4)

Cyclone V

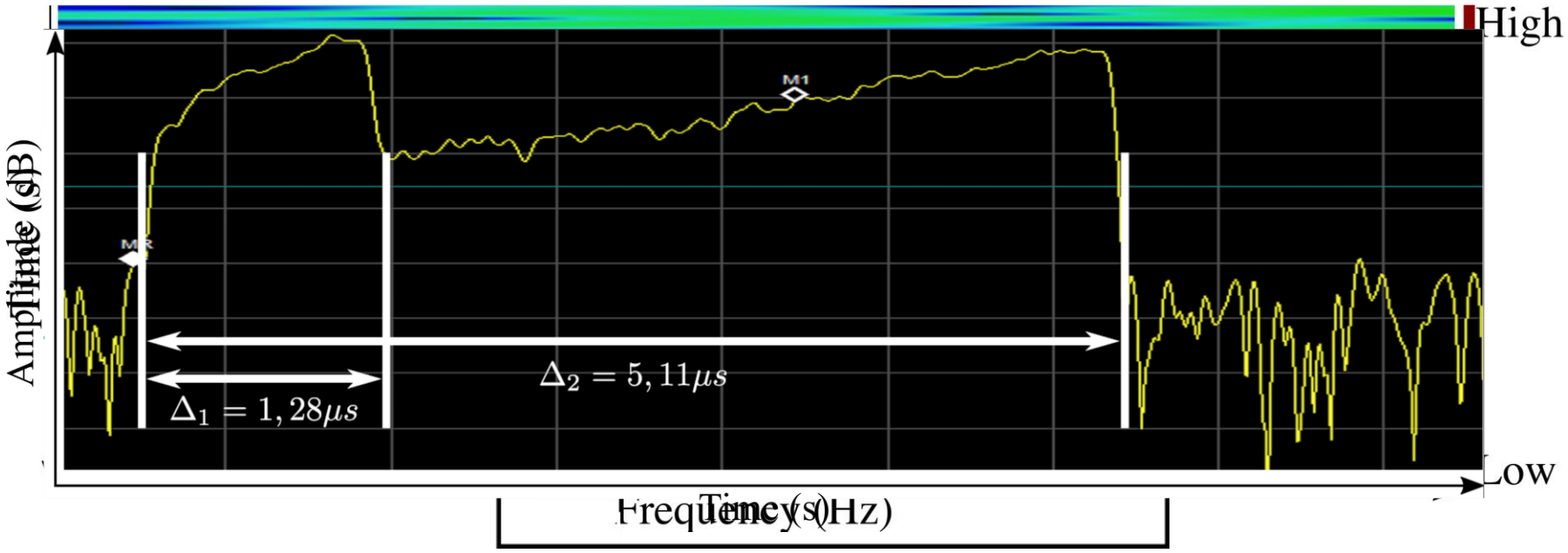


Spartan 6

EM analysis of two TERO cells

⚠ The two N_{osc} can be dissociated

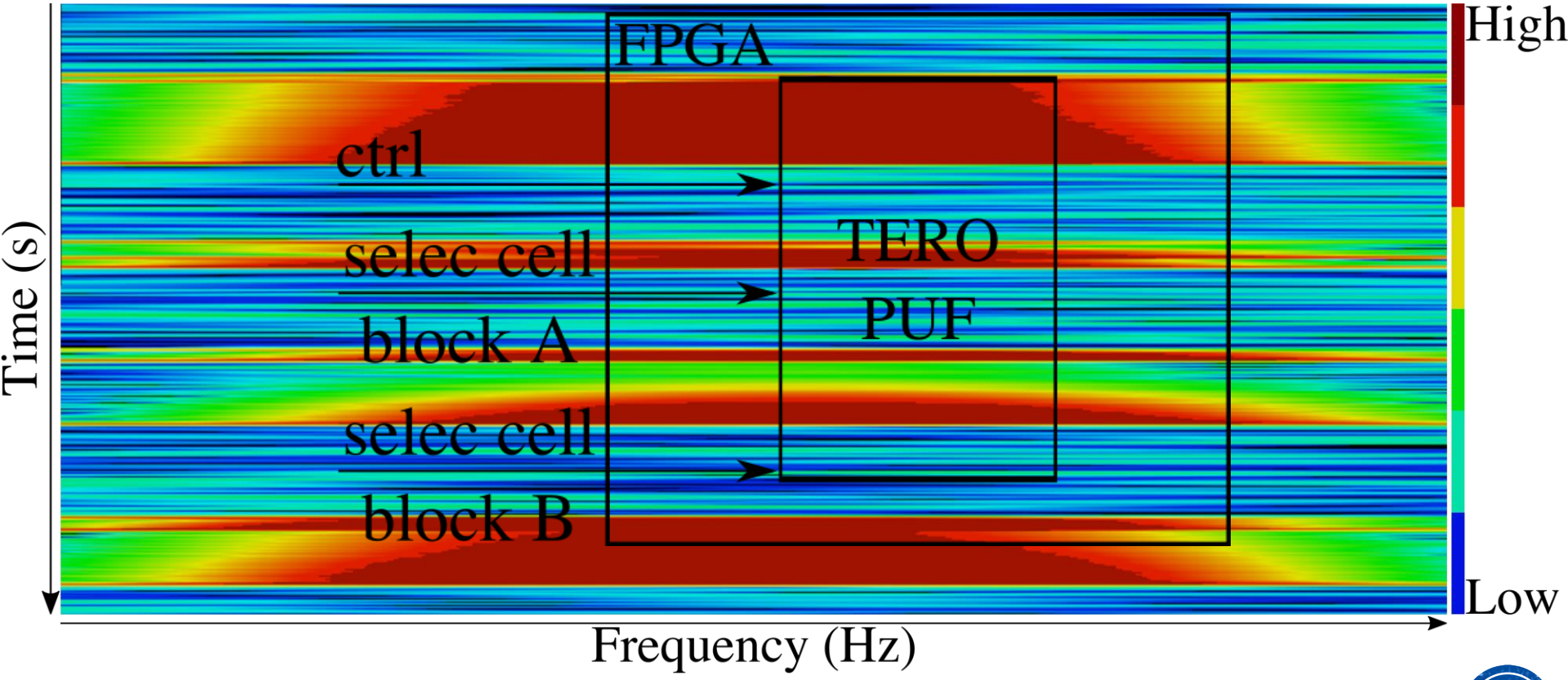
- Two TERO cells periodically restarted at the same time
- ⇨ N_{osc1} = 223 and N_{osc2} = 892



EM analysis of a TERO PUF

⚠ Successive comparaisons can be caught

- Four successive comparisons



EM analysis of a TERO PUF

- Successive comparisons scheme to clone a complete TERO-PUF:

A_1 versus B_1 ⇨ identification of two N_{osc}

A_1 versus B_2 ⇨ N_{osc} of A_1, B_1 and B_2

A_2 versus B_1 ⇨ N_{osc} of A_2

.

.

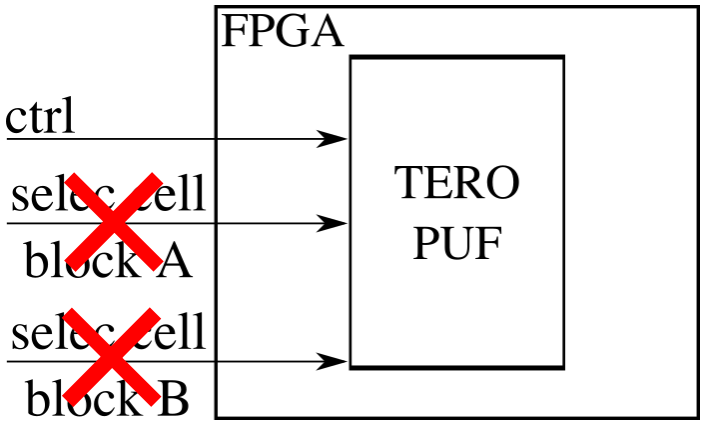
.

A_m versus B_m ⇨ N_{osc} of A_m and B_m

- 2x*m*-1 comparisons to clone the whole PUF: linear complexity.

Leakage prevention measures

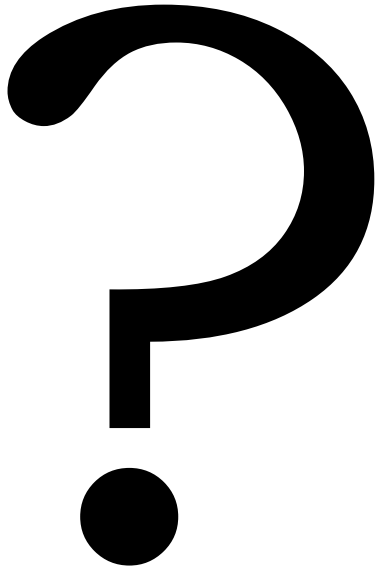
- Make the device physically inaccessible: aluminum lid to shield EM emissions (not always possible)
- Not to allow users to access challenges
- Activation of all TEROs for each comparison



Conclusion

- Hardware traceability needs increase with IoT deployments
- PUF allow intrinsic identification of chips
- Many PUF based on digital oscillators
- Show for the first time TERO is vulnerable to EM analysis: to be anticipated during design conception!

Thank you!



ugo.mureddu@univ-st-etienne.fr