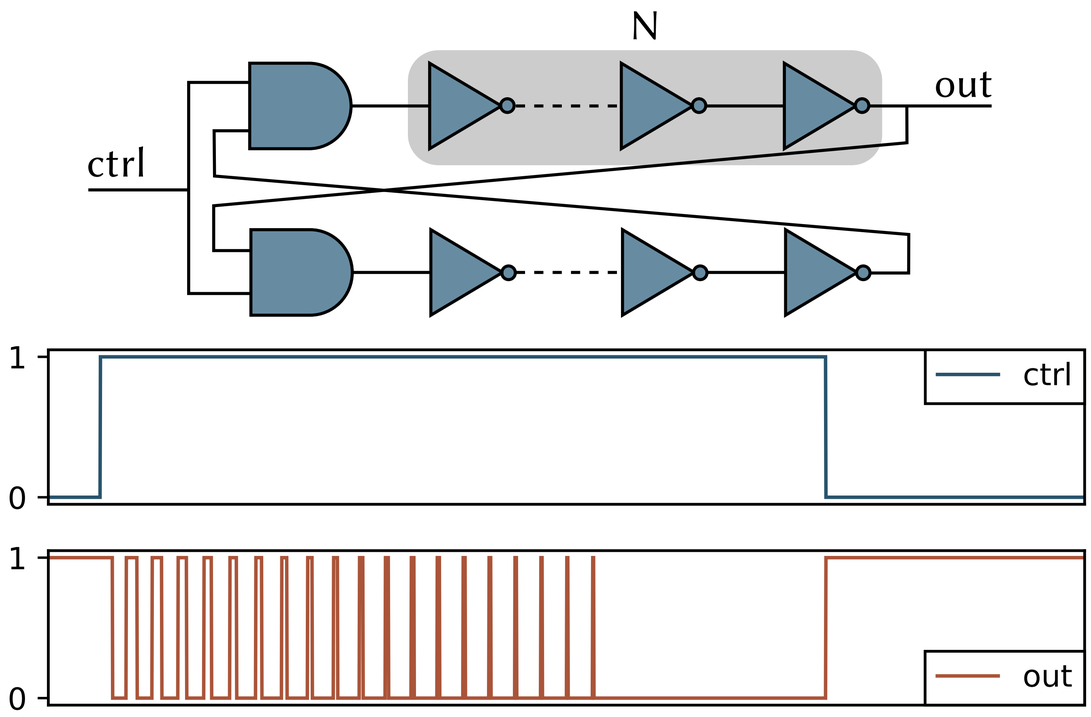
# Transient Effect Ring Oscillators Leak Too

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

Univ Lyon, UJM-Saint-Etienne, CNRS, Laboratoire Hubert Curien UMR 5516, F-42023, SAINT-ETIENNE, France

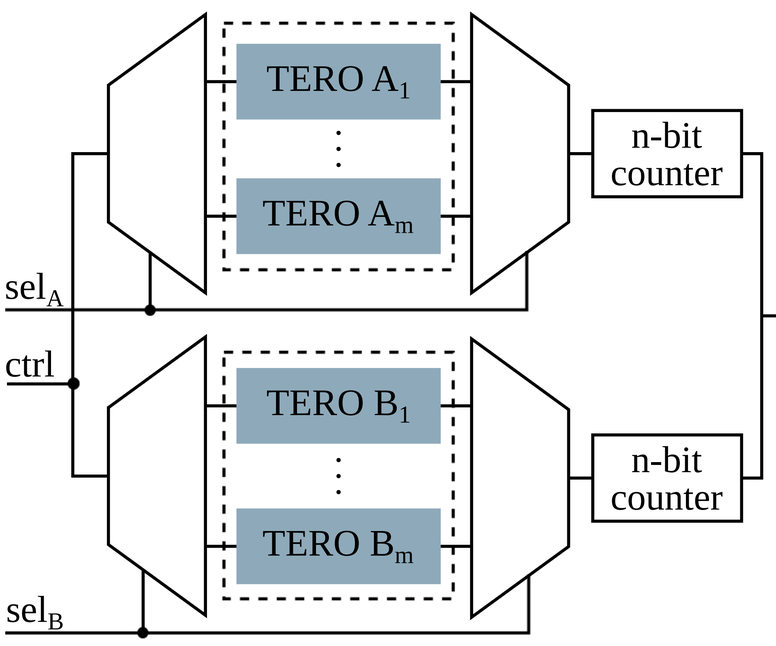
{ugo.mureddu, b.colombier, nathalie.bochard, lilian.bossuet, fischer}@univ-st-etienne.fr

## Transient Effect Ring Oscillator




The **number of oscillations** is **unique** and depends on **manufacturing process variations.**

## TERO-PUF




TERO as building block for a **Physical Unclonable Function**

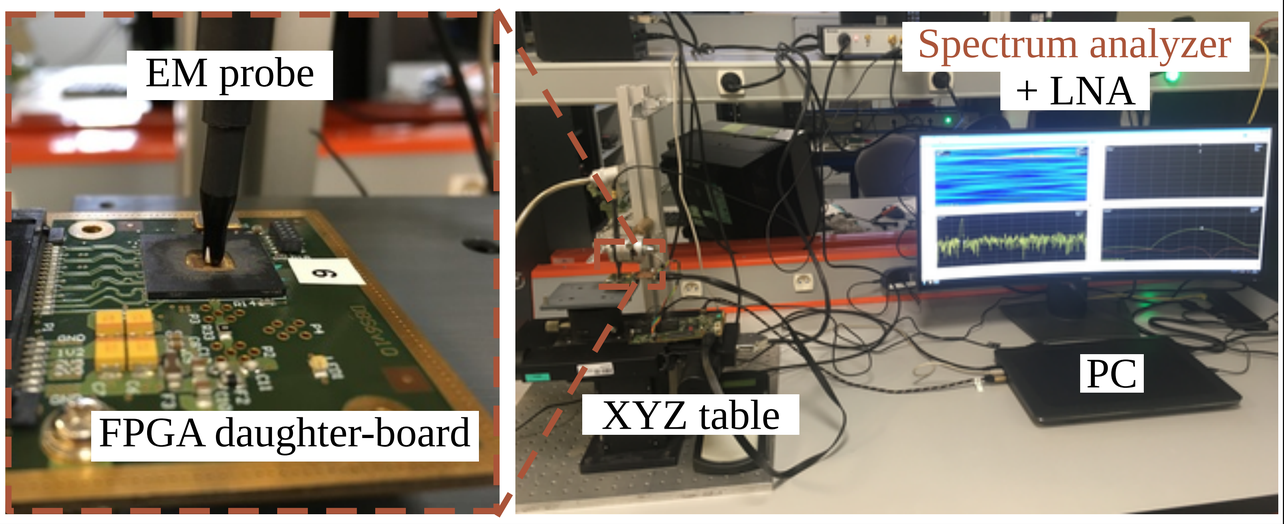
Classical ring oscillators are known to **leak** their frequency [1,2,3]

[1] D. Merli, D. Schuster, F. Stumpf, and G. Sigl,
"**Semi-invasive EM attack on FPGA RO PUFs and countermeasures**,"
Workshop on Embedded Systems Security, 2011.
[2] D. Merli, J. Heyszl, B. Heinz, D. Schuster, F. Stumpf, and G. Sigl,
"**Localized electromagnetic analysis of RO PUFs**,"
IEEE International Symposium on Hardware-Oriented Security and Trust, 2013.
[3] P. Bayon, L. Bossuet, A. Aubert, and V. Fischer,
"**Electromagnetic analysis on ring oscillator-based true random number generators**,"
International Symposium on Circuits and Systems, 2013.

Until now, TERO were thought to be **immune to EM analysis**...

## Experimental setup

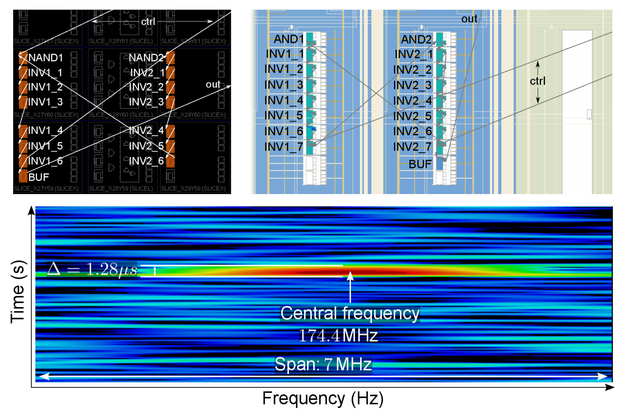
2 FPGA families: Xilinx Spartan 6 and Altera Cyclone V




## Implementations and results

### One TERO + output buffer

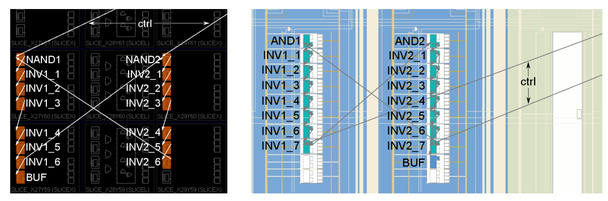
no decapsulation



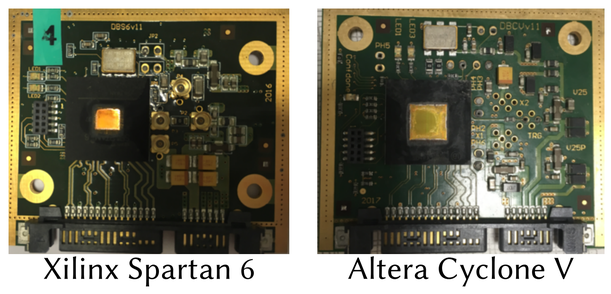

$N_{osc} = \Delta \cdot f_{osc}$

$N_{osc} = 1.28\times10^{-6}\times174.4\times10^{6} = 223$

### One TERO only



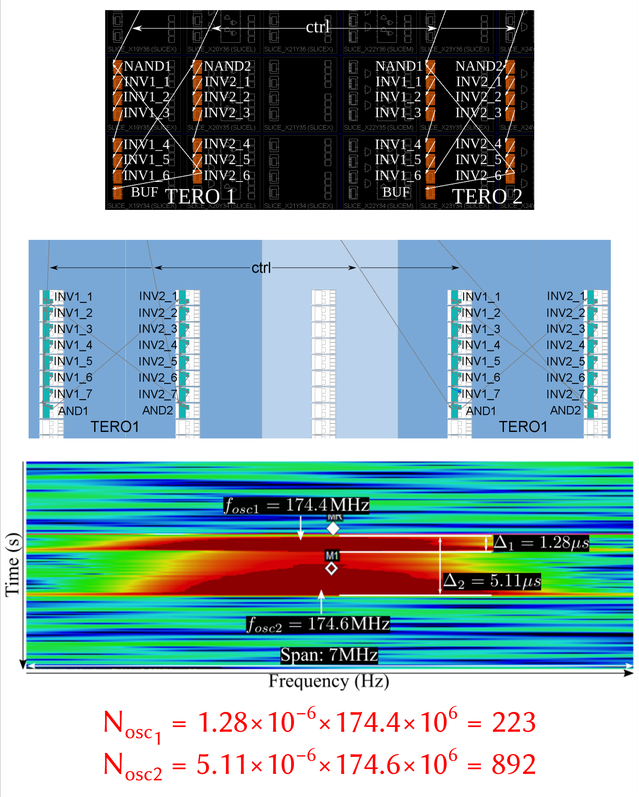
Decapsulation is **required**



Xilinx Spartan 6 | Altera Cyclone V

### Two TEROs

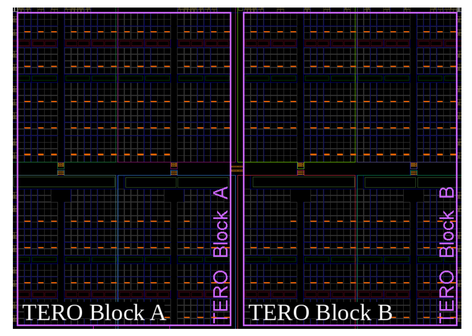
oscillating simultaneously

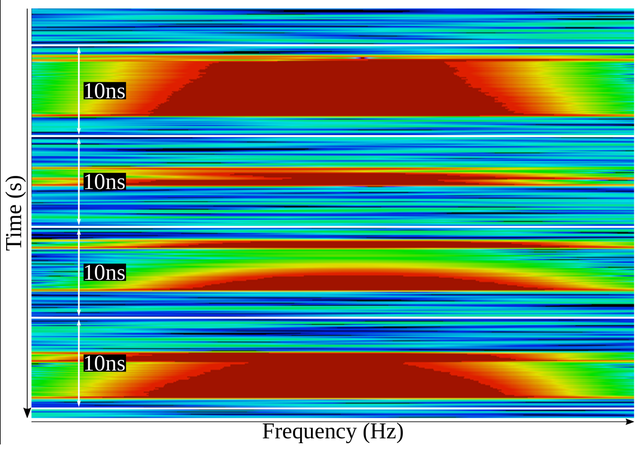



$N_{osc_1} = 1.28\times10^{-6}\times174.4\times10^{6} = 223$

$N_{osc2} = 5.11\times10^{-6}\times174.6\times10^{6} = 892$

### Full TERO-PUF




## Full TERO-PUF cloning

**Step 1**:
$A_1 \leftrightarrow B_1$
$A_1 \leftrightarrow B_2$

**Step 2**:
$A_1 \leftrightarrow B_i$
for $3 < i < m$

**Step 3**:
$A_i \leftrightarrow B_1$
for $2 < i < m$

**2m+1** comparisons overall : **linear** complexity

## Conclusion

TERO is **vulnerable to EM analysis**
TERO-PUF can be **fully cloned** with **linear** complexity

Possible **countermeasures**:
- Electromagnetic **shielding**
- **No access** to the "challenge" ($sel_X$) input
- Activation of **all TEROs** for each comparison

**Full article** available at:
*https://eprint.iacr.org/2019/300.pdf*

## Code availability

All associated VHDL code is **open source** and **available online** at:
*https://gitlab.univ-st-etienne.fr/ugo.mureddu/em-analysis-of-transient-effect-ring-oscillator-based-puf*

UNIVERSITÉ DE LYON | UNIVERSITÉ JEAN MONNET SAINT-ÉTIENNE | bpifrance | cnrs | LABORATOIRE HUBERT CURIEN UMR • CNRS • 5516 • SAINT-ETIENNE