Laboratoire d'Informatique de Robotique et de Microélectronique de Montpellier

LIRMM

UNIVERSITÉ MONTPELLIER 2
SCIENCES ET TECHNIQUES

cnrs
dépasser les frontières

Local and Direct EM Injection of Power into CMOS Integrated Circuits.

F. Poucheret[1,4], K.Tobich[2], M.Lisart[2],L.Chusseau[3], B.Robisson[4], P. Maurine[1]

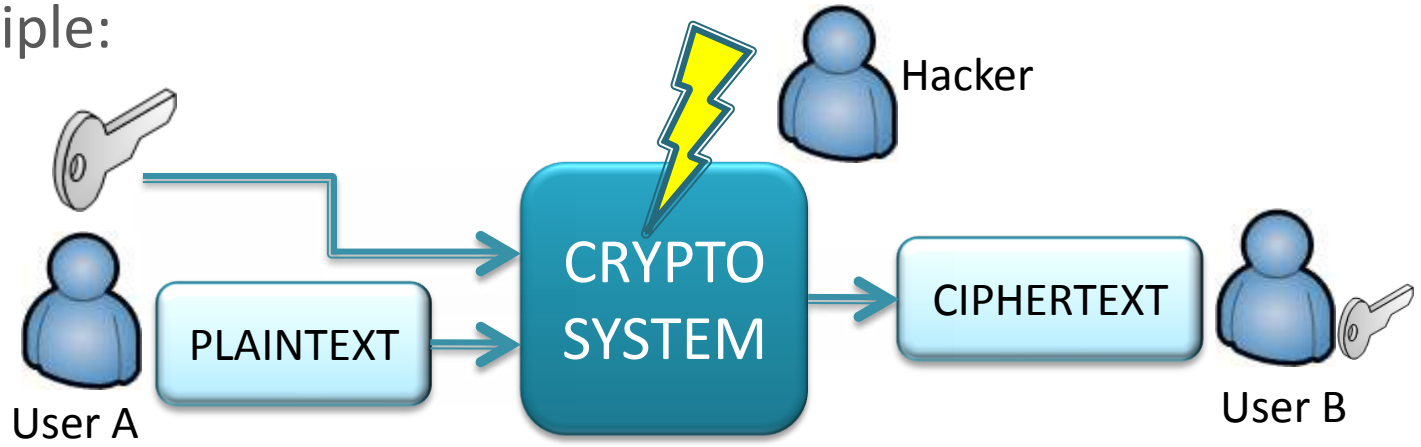
LIRMM Montpellier[1]
ST Microelectronics Rousset[2]
IES Montpellier[3]
CEA Gardanne[4]

Outline

- 1/ Introduction
  - Context of secure IC.
  - EM waves properties.
- 2/ EM injection Platform
  - Power Injection chain.
  - Illumination model.
- 3/ Experimental results
  - Injections on packaged IC.
  - Injections on unpackaged IC.
- 4/ Conclusion

Context: Fault Attacks

- Principle:

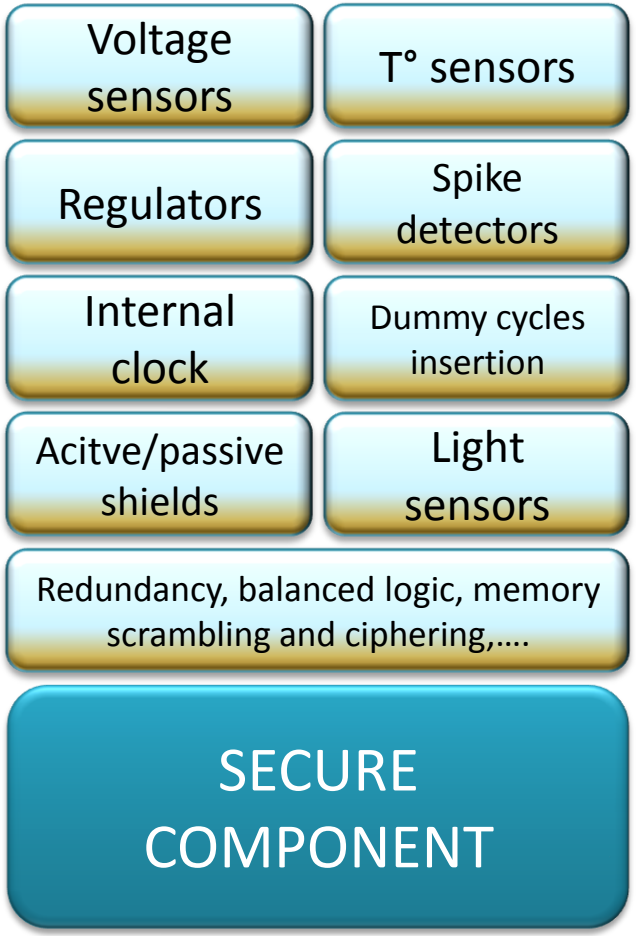


- **Disturbing the crypto-computation to extract secret information.**
- Characteristics:
  - Very efficient on unprotected systems.
  - Unpredictable behavior.
  - Complex to protect.

Context : Attacks Vs Countermeasures

- **Global attacks:**
  - **Operating limits(V, F, T°).**
  - **Voltage spike.**
  - **Clock glitch.**
- **Local attacks:**
  - **Laser shoot.**

- **EM attack ?**



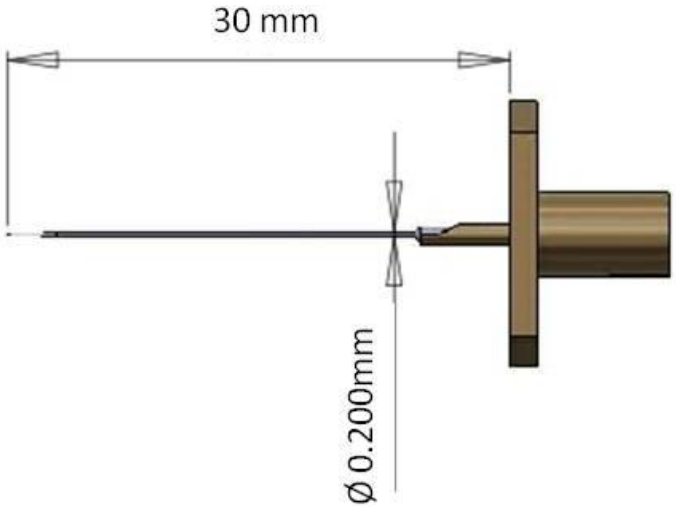
Context : ElectroMagnetic (EM) Waves

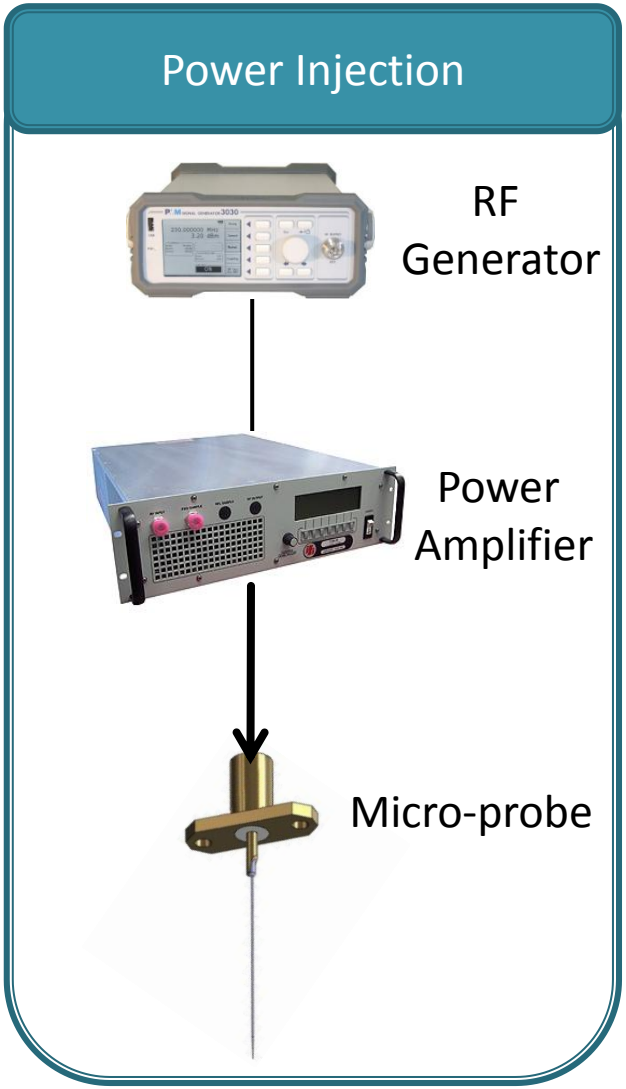
- **EM potentials:**
  - *Penetration capabilities.*
  - *Difficult to detect in electronic environment.*
  - *Low-cost equipment.*
- **Feasibility of EM attacks?**
  - *Is it possible to create a local coupling with an IC?*
  - *Is it possible to disturb an IC without removing the package?*

EM Harmonic Injection

Power Injection Chain

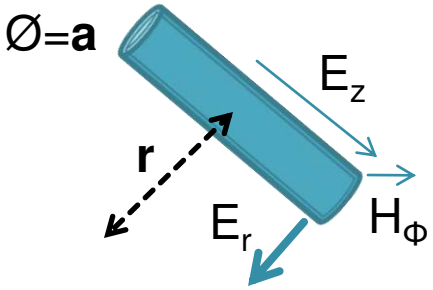
- List of elements:
  - RF generator.
  - 50W power amplifier.
  - RF cables.
  - Micro-probe.

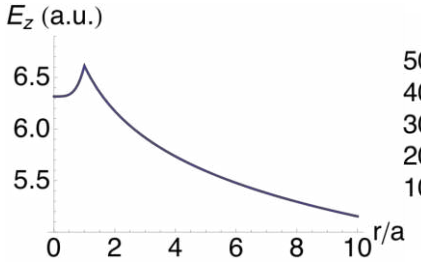


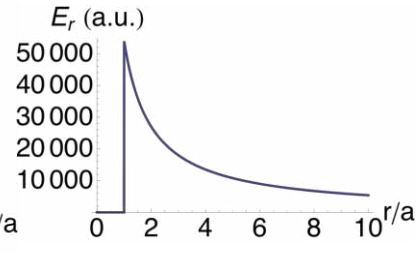


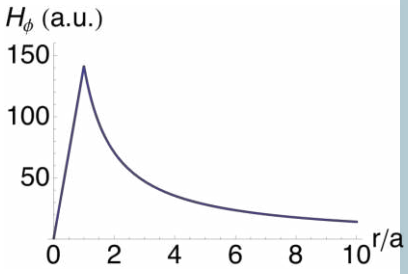
EM Illumination Model

- EM fields:

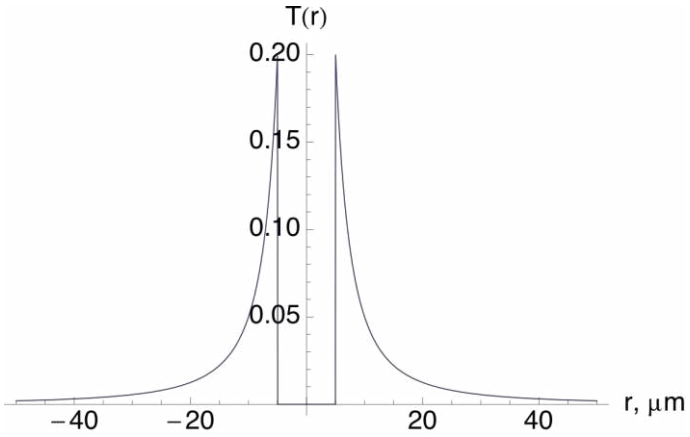


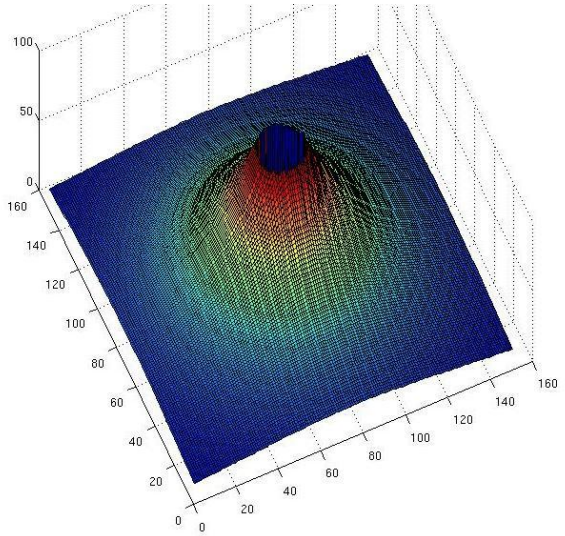






- EM illumination:

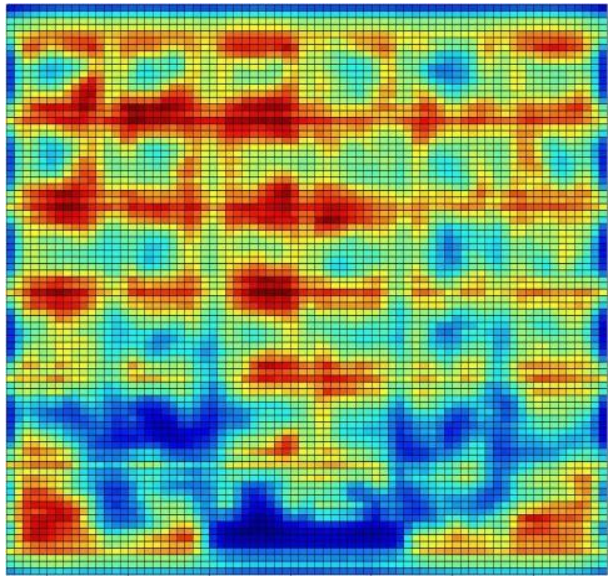




- 90% of power in a ring of internal Ø=2*a and external Ø= 5*a.
- Local and intense EM injections.

EM coupling: In brief

- Our first works demonstrate the possibility of creating local EM couplings.



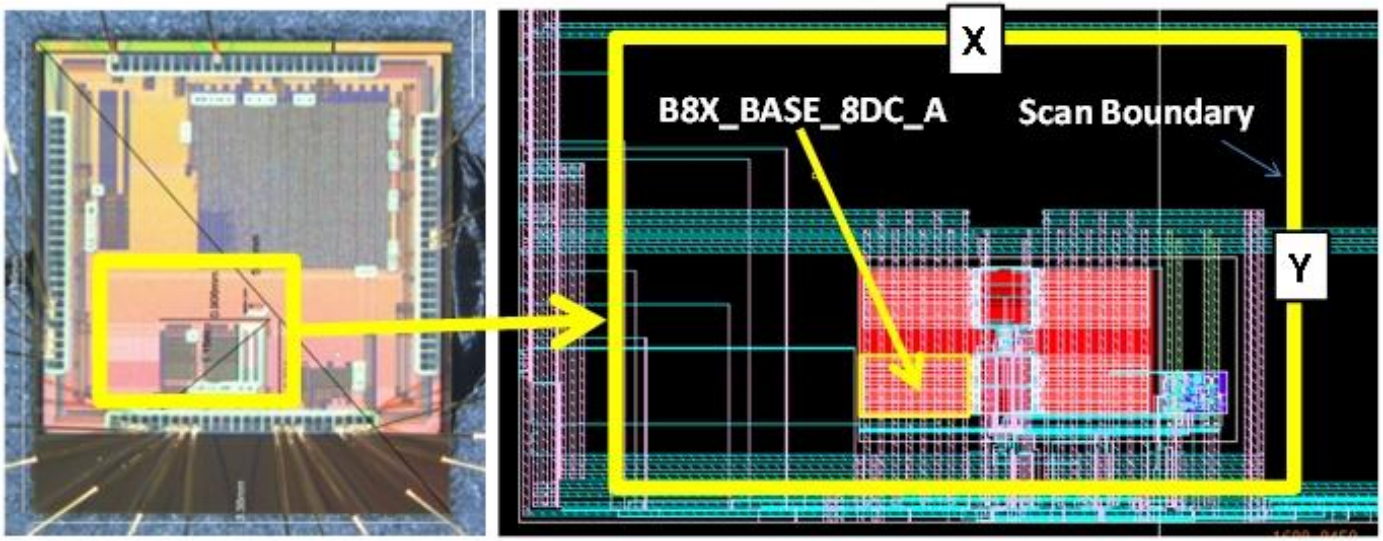
- The coupling depends on:
  - Probe position and geometry.
  - IC and receptive geometry pattern.
  - Frequency and power.

- ***"Local ElectroMagnetic Coupling with CMOS Integrated Circuits"***, *F. Poucheret, B. Robisson, L. Chusseau, P. Maurine, EMC-Compo 2011, Dubrovnik, Croatia.*

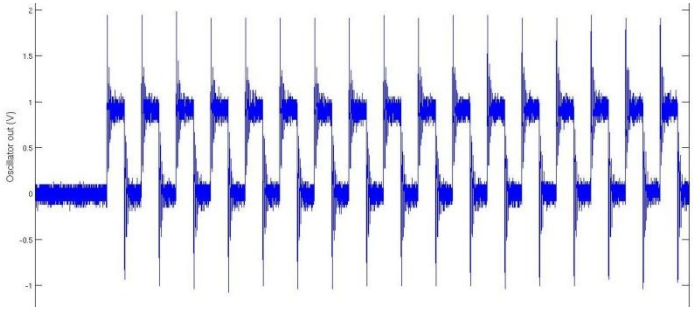
Experimental Results

DUT: Ring Oscillator

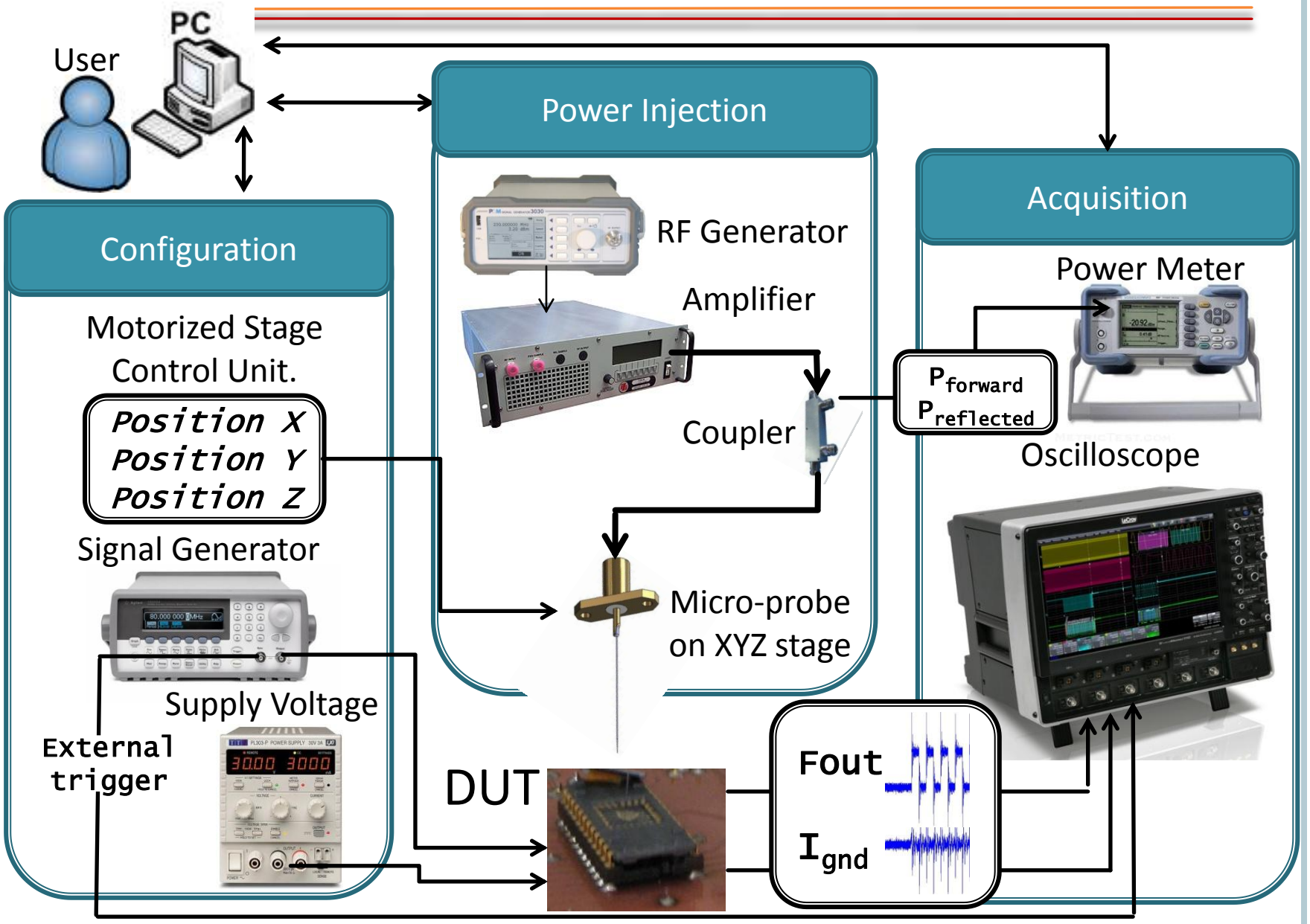
- **Choice of a Ring Oscillator:**
  - CMOS technology characterization.
  - True Random Number Generator, Internal Clock Generator.



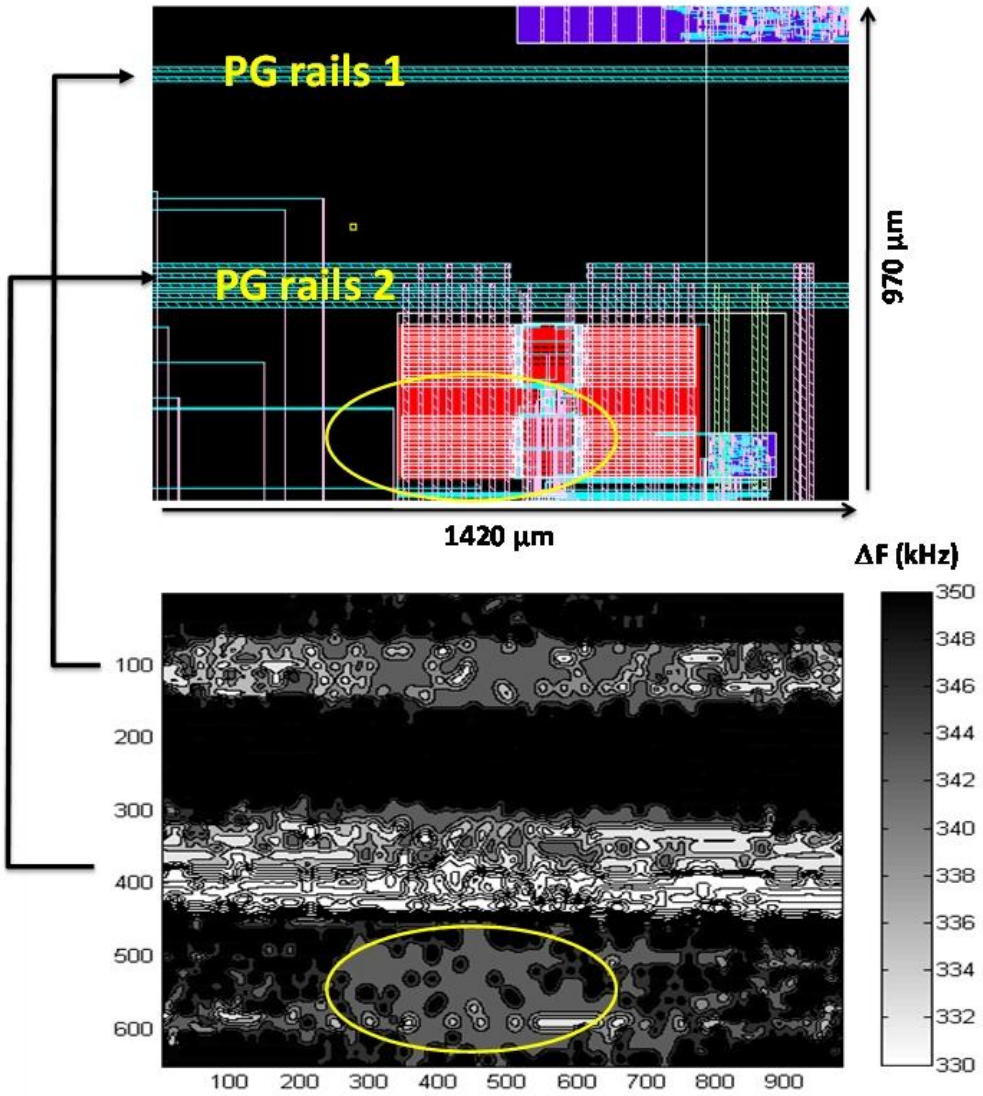
- **101 inverters + counter.**
- **Output frequency (Fout)=3.81MHz.**



Experimental Configuration

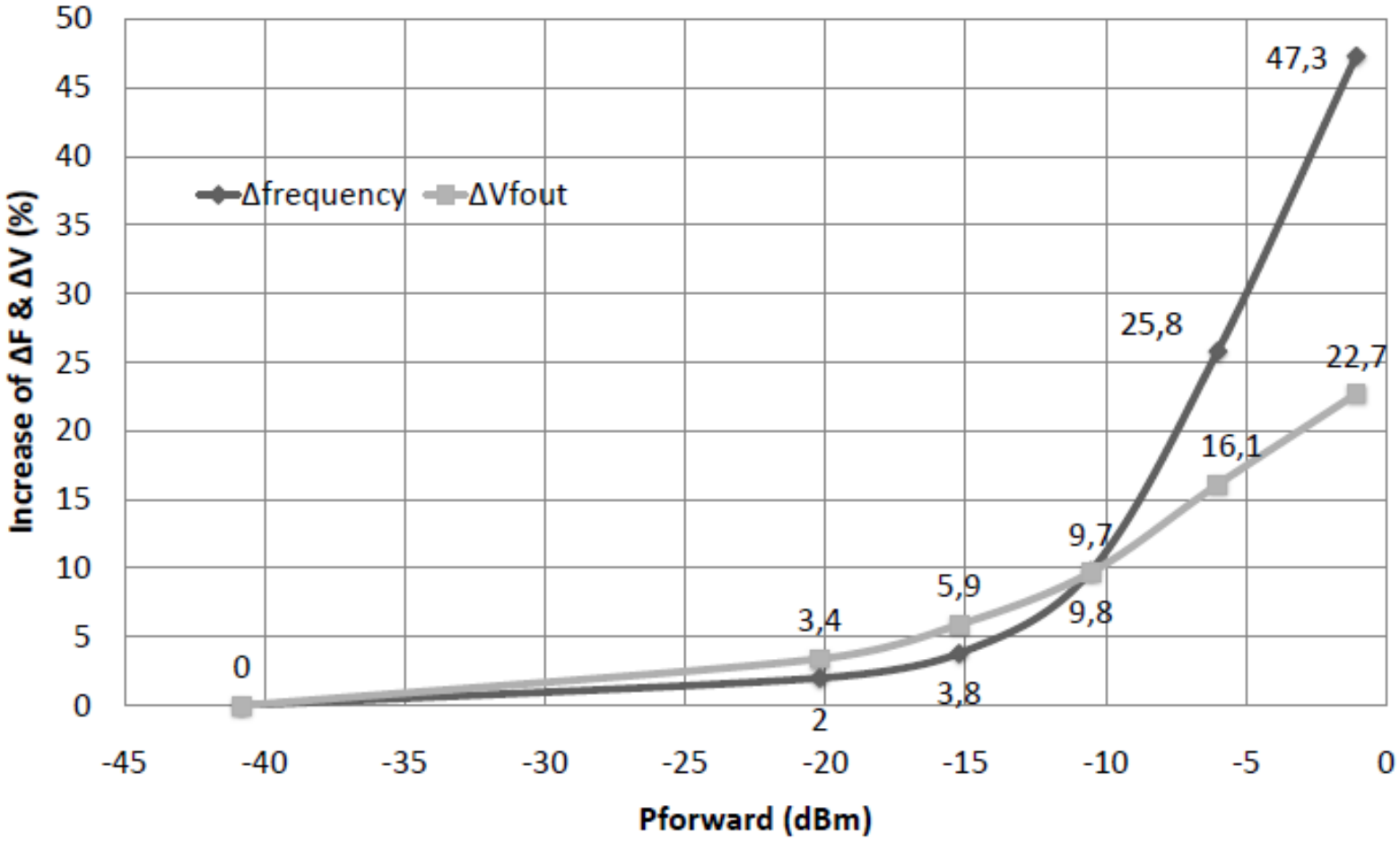


ΔF Cartography on unpackaged IC



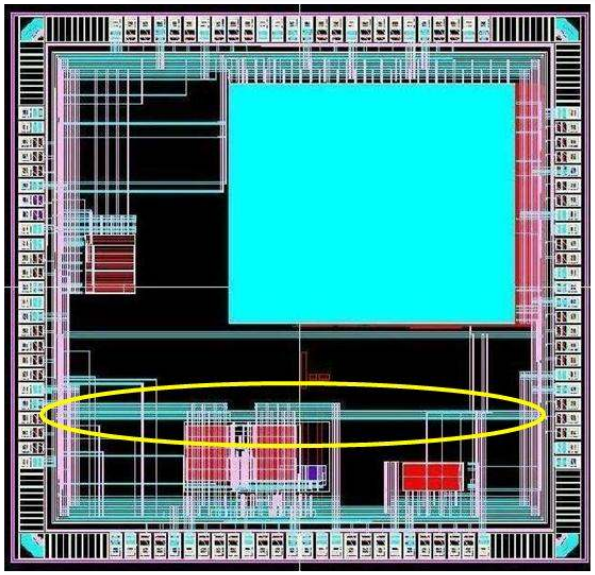
- **Parameters:**
  - 1GHz sine.
  - $P_{forward}$ = 0.1mW.
  - Gap probe/IC = 50µm.
- Global increase of frequency: 350kHz (9.2%).
- Local variations between 310-380kHz.

ΔF AND ΔV SWING EVOLUTIONS (PACKAGED IC).

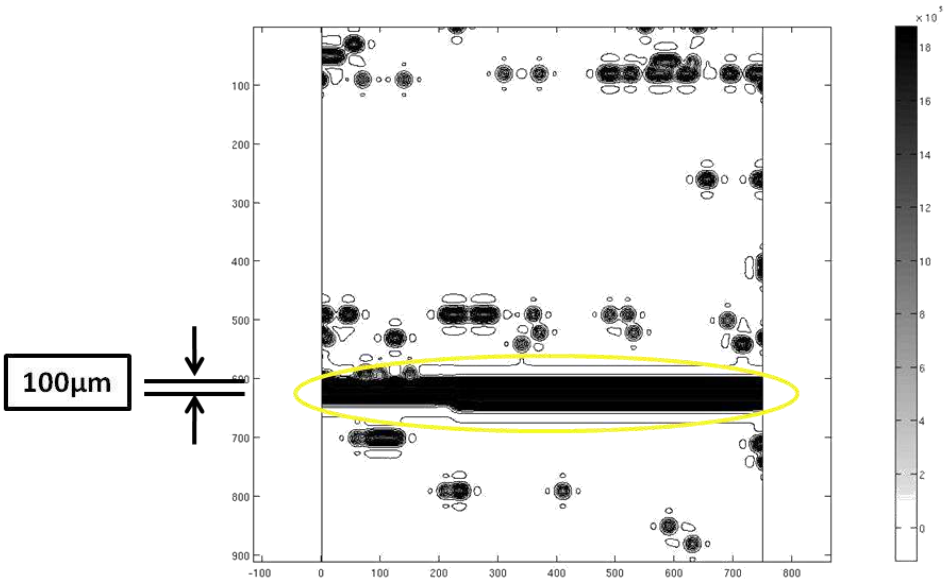


- Increase of Vdd .
- Proportional to $P_{forward}$.

ΔF Cartography on packaged IC



- **Parameters:**
  - 1GHz sine.
  - $P_{forward}$ = 6.63mW.
  - Gap probe/IC = 2mm.



- Local increase of 1.8 MHz (46,6%).
- Detection of patterns (width≈100µm).

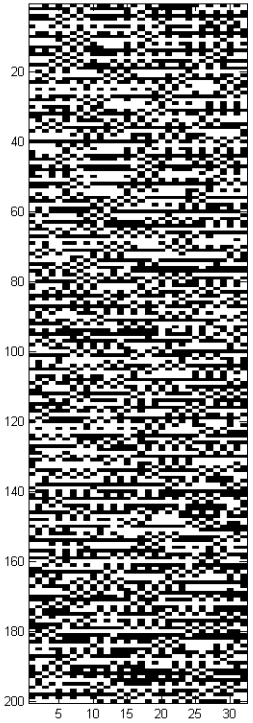
Conclusion

- **EM harmonic Injection into CMOS IC at High Frequency.**
  - Energy supply directly to power ground network.
  - Contactless (several mm).
  - Detection of 100µm wide patterns.

UNDERGOING WORK ON "WOLD" TRNG

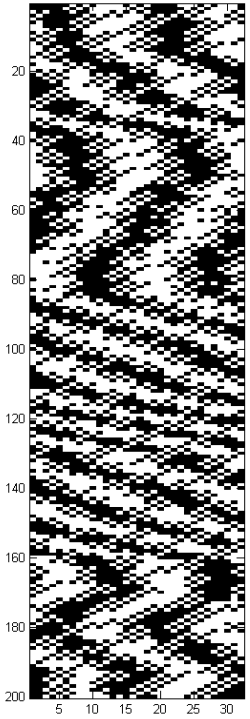
- First EM Harmonic Injection into TRNG

Output stream without injection



LOCKING

Output stream with injection



- Modified bit stream at the output.
- Fail the statistical tests.