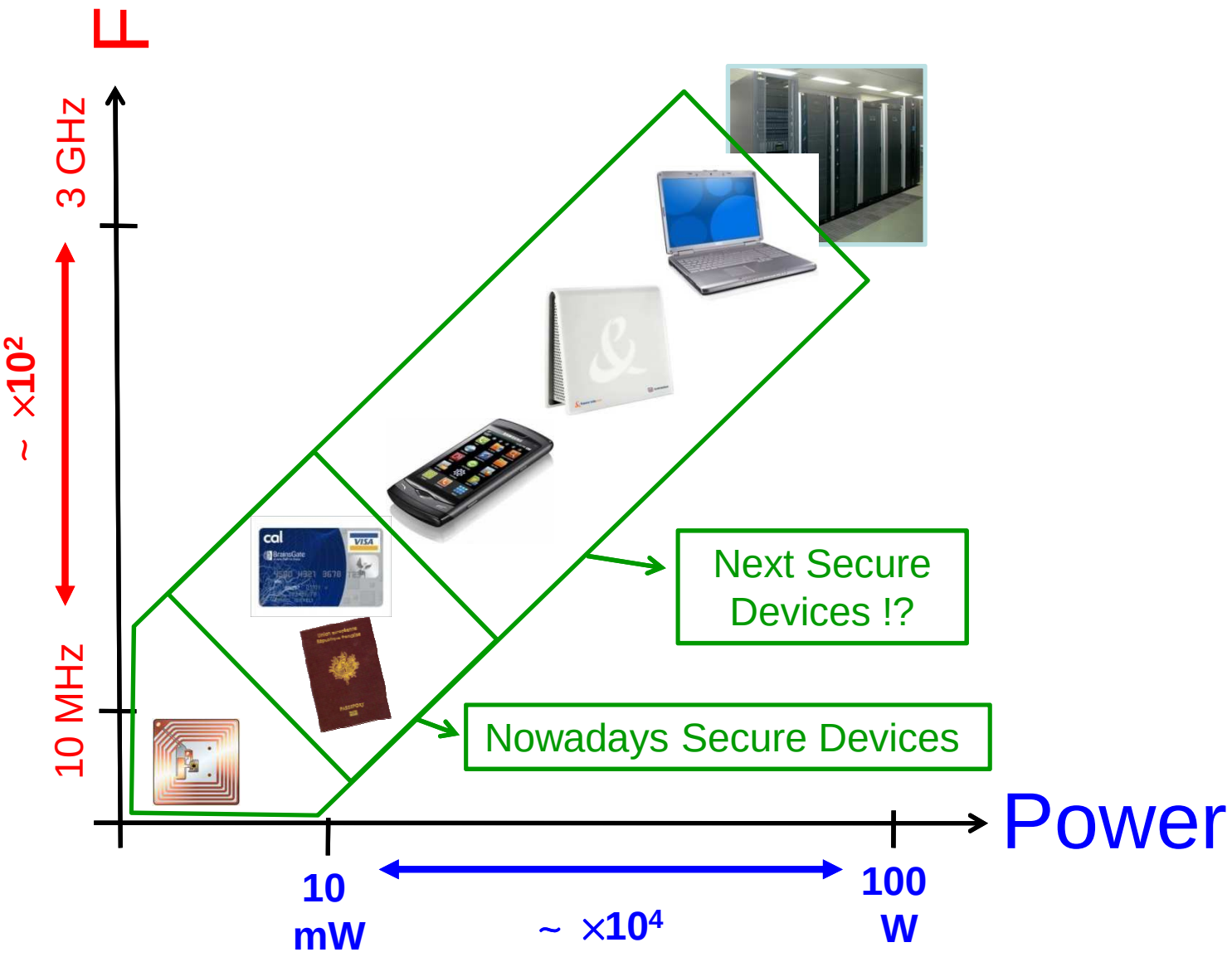
Techniques for EM Fault Injection: Equipments and Experimental Results

FDTC 2012

P. Maurine (pmaurine@lirmm.fr)

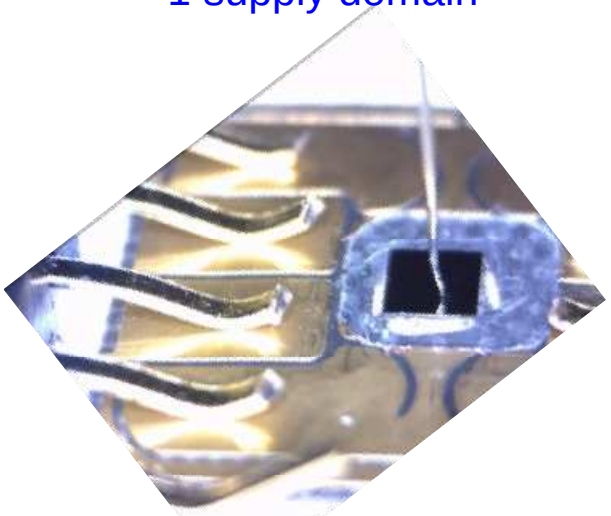
1- Context toward secure Systems on Chips (SoC)



1- Context SmartCards vs secure SoC


~100 kgates, ~ 30 MHz, ~ 5 mm²
~ 90 nm / 4-5 metal Layers
~ 2-3 clock domains
~ 1 supply domain


~ 1 Mgates, ~ 1 GHz, ~ 25 mm²
~ 32-28 nm / 7-12 metal layers
~ 10 clock domains
~ 2-4 supply domains
~ bulk -- FDSOI



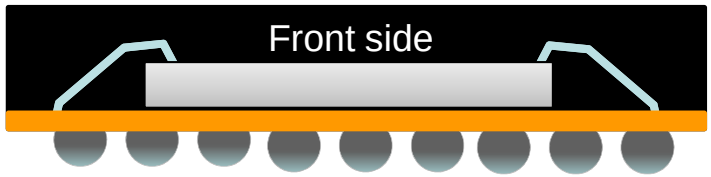
Physical Attacks still efficient against such components ?

1- Context packaging

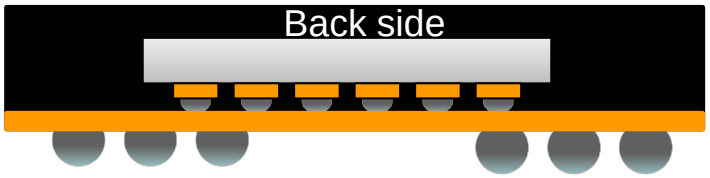
Embedded cryptography
- Symetric crypto-blocks
- Modular arithmetic accelerator
- TRNG …

Embedded Countermeasures
- Internal clock generator
- Voltage regulators / Sensors
- Light sensors …

Wire bonded BGA



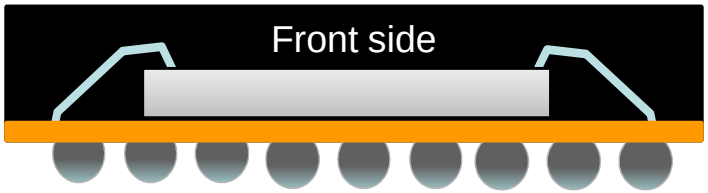
Flipped Chip BGA



How to inject faults into such components?

1- Our choices

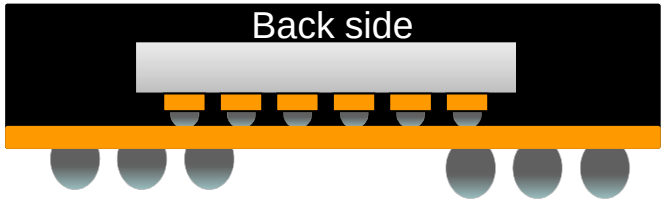
Wire bonded BGA



local EM coupling with the P/G ground network to modify locally the supply voltage of some CMOS gates (timing faults)

ElectroMagnetic Injection

Flipped Chip BGA



Locally modify the substrate bias to modify locally the supply voltage of some CMOS gates (timing faults)

Forward Body Biais Injection

First works by:
David Samyde (2002)
Jorn-Marc Schmidt (2007)

Agenda

1- Context & motivations

2- Front side Injection: EM Injection platforms

-a- Different EM Injections
-b- Probe Modeling
-c- Developed platforms

3- Back side Injection: Forward Body Bias Injection platform

4- Experimental Results

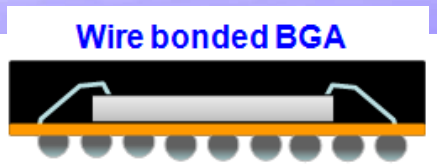
5- Conclusion

2- Front side Injection : EM Injection

Different targets ⇔ Different EM Injections

Targets	Analog Blocks		Digital Blocks
	Internal Clock Generator	TRNG	logic and memories
Goal	Increase the frequency to produce timing fault	Dynamically bias TRNGs (locking and latching)	Generate timing fault (setup time constraint)
How	Providing directly and locally Power to the P/G network	Providing a frequency on the P/G network	EM pulse / Voltage drop / timing violation
EM Injection Type	**Harmonic Injection** Intense & long duration & local Electrical Field		**Pulse Injection** Intense & local & short & sudden Magnetic Field variation

2- Front side Injection : EM Injection



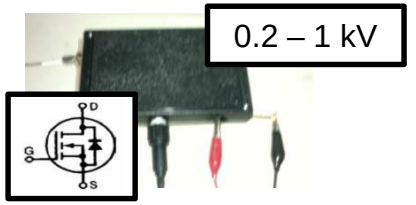
HARMONIC INJECTION

RF Generator

Power Amplifier

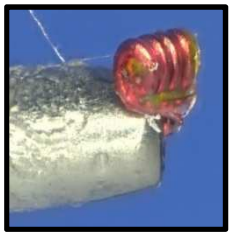
Micro-probe

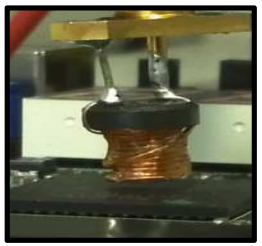
PULSE INJECTION



Market Pulse Generators

Nanopulse generators



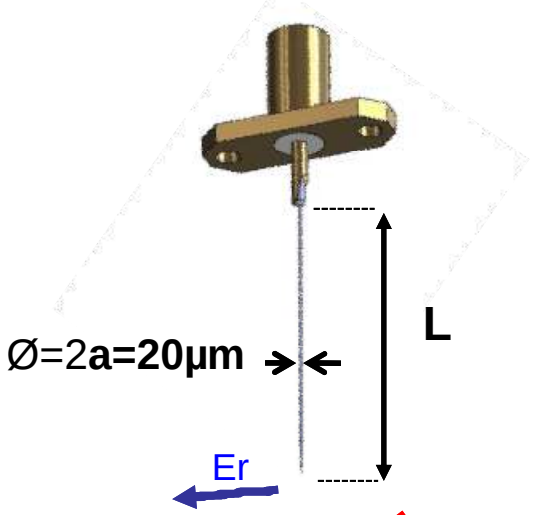


The probes are key elements !!

- fix the spatial resolution
- fix the amplitude of the EM field

2- Front side Injection : EM Injection

HARMONIC INJECTION PROBES



Avoid the thermal dissipation problem associated to continuous waves

LOCAL and radial electrical field Er

Wire bonded BGA

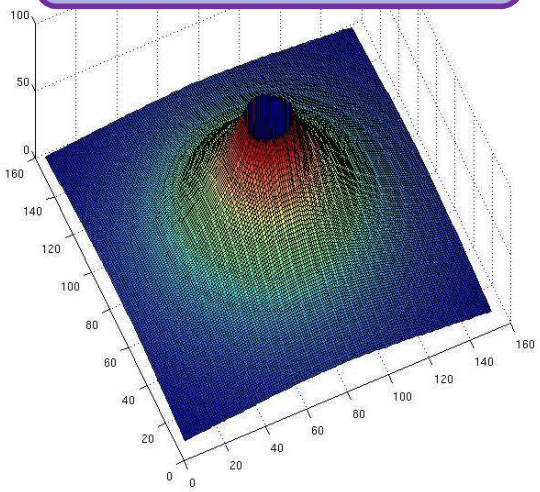
‘L’ chosen to maximise Er:

The lowest the frequency is the longest the probe must be … (take care of mechanical vibrations)

‘a’ fixes the spatial resolution :

90% of the Power is within a donut with Øint. 2*a & Øext. 5*a

Illumination model

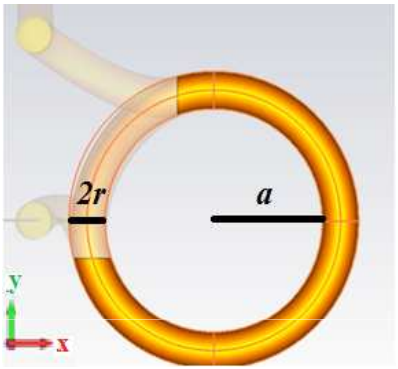


a= 10 µm
Øint=40 µm
Øext=100 µm

2- Front side Injection : EM Injection

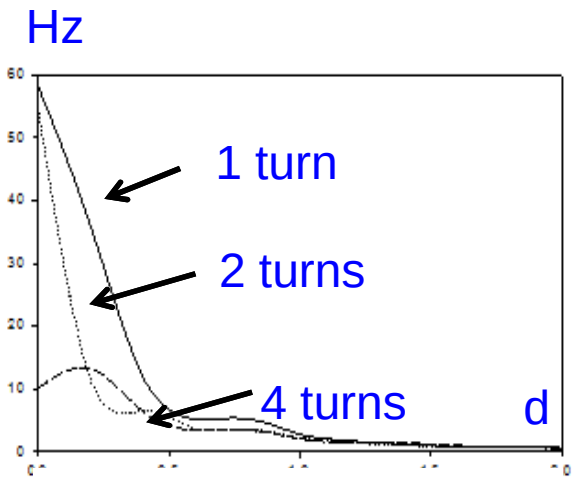
Wire bonded BGA

PULSE INJECTION PROBES



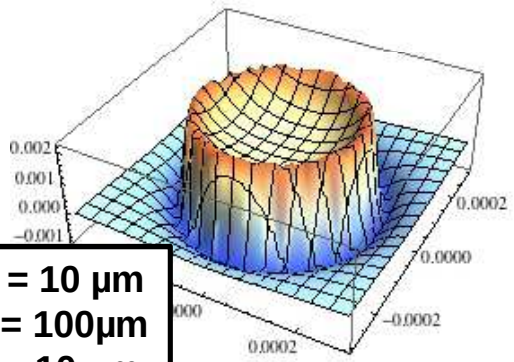
Produces a local and vertical magnetic field Hz

Take care to the Pulse repetition rate (heating problem)

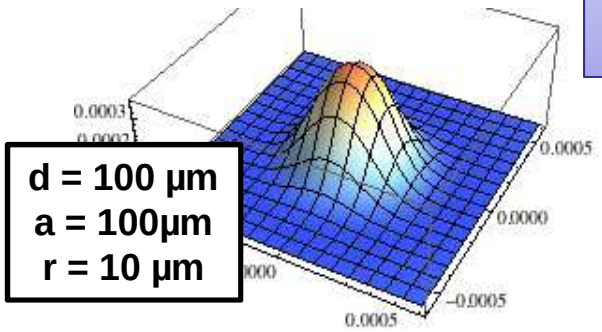


Hz ~1/d³

1 turn is optimal !



d = 10 µm
a = 100µm
r = 10 µm



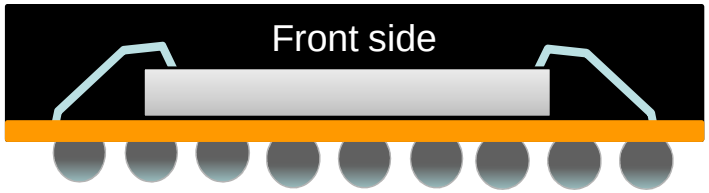
d = 100 µm
a = 100µm
r = 10 µm

90% of the power within 0 and ≈ 5a

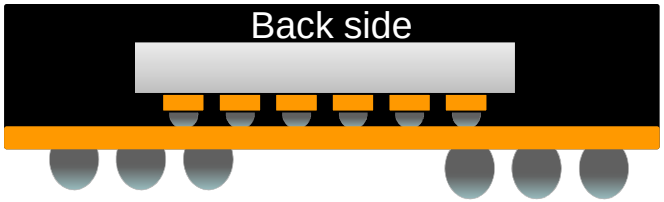
a=100µm → resolution 1 mm

3- Back side Injection : FBBI

Wire bonded BGA



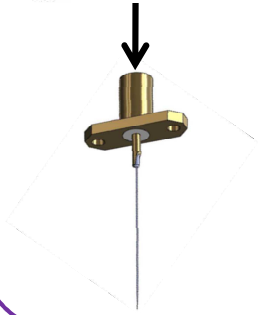
Flipped Chip BGA



HARMONIC INJECTION

RF Generator

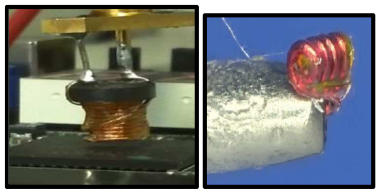
Power Amplifier



Micro-probe

PULSED INJECTION

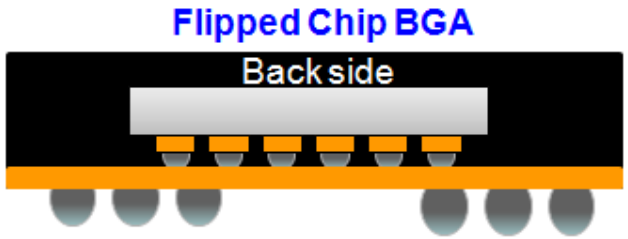
Market Pulse Generators



Locally modify the substrate bias to modify locally the supply voltage of some CMOS gates

Forward Body Bias Injection

3- Back side Injection : FBBI platform

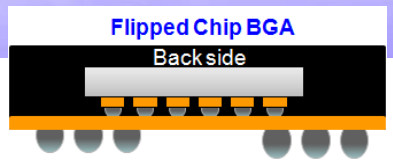


Is electromagnetic injection has an interest in case of Flipped Chip BGA ?

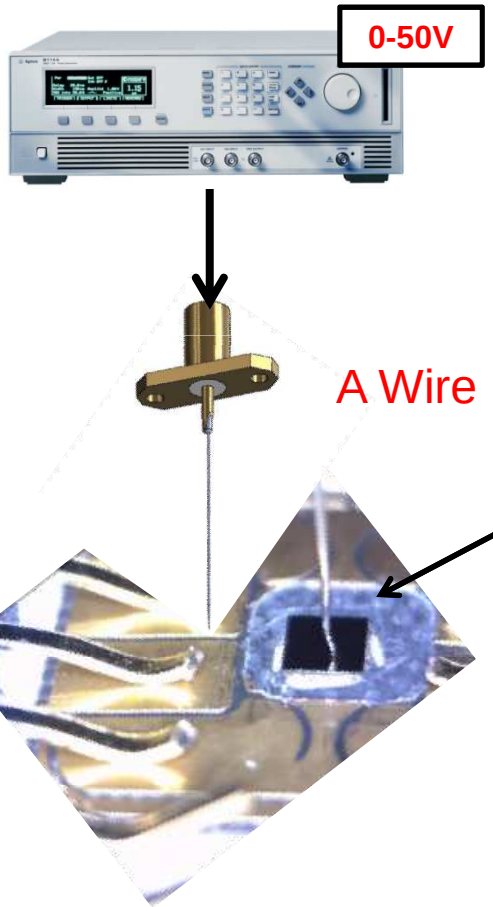
No !!!! …

So, don’t use an
Antenna and just use a wire …
to do create a direct contact at a given point of the back side …

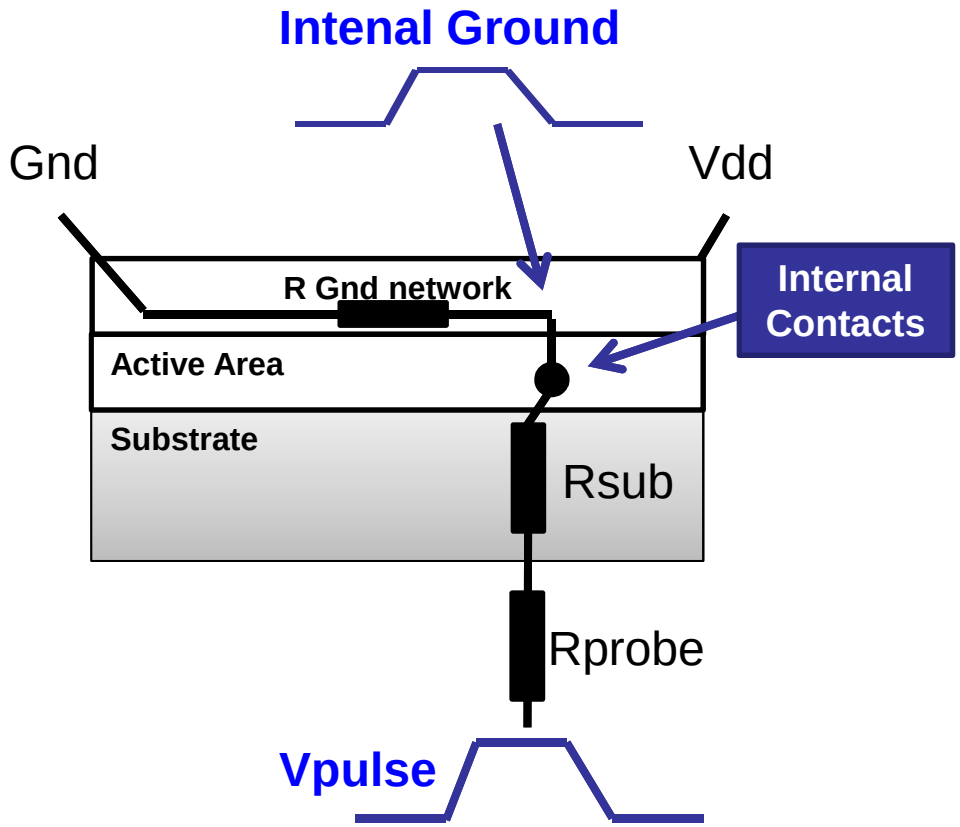
3- Back side Injection : FBBI



FBBI PLATFORM



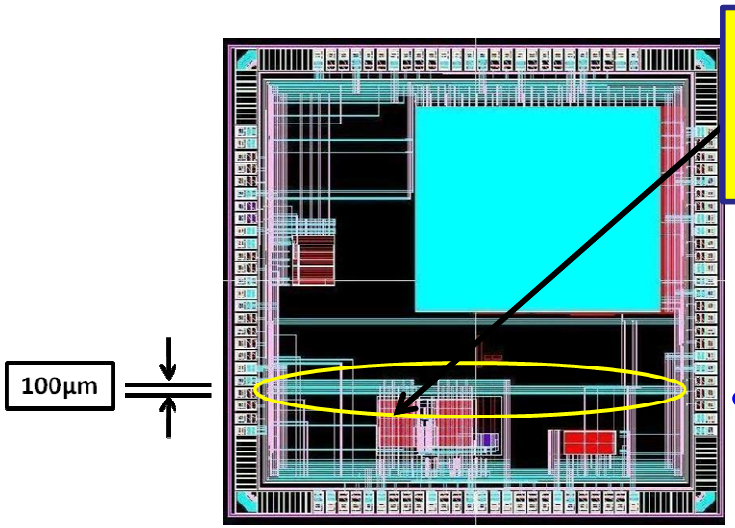
Electrical contact with the substrate

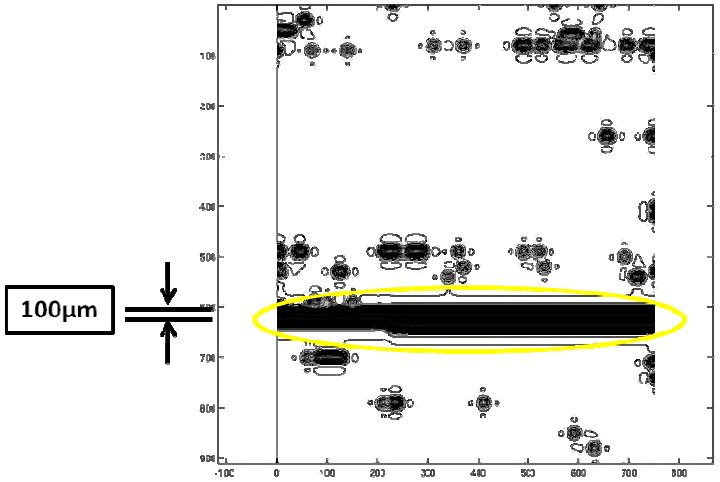


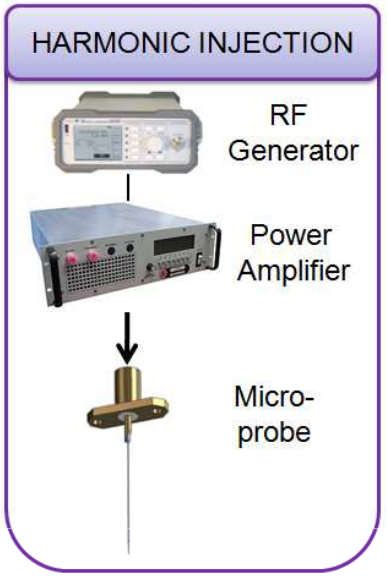
More details will be available in :

Yet Another Fault Injection Technique: by Forward Body Bias Injection
Yacc 2012 (24- 28 September, Porquerolles Island, France)

4- Results : Front Side Injection







- **Parameters**
  - 1GHz Sine.
  - Distances probe / IC surface 2mm.
  - Forward Power 0dbm to 6.63 dbm
  - Through package

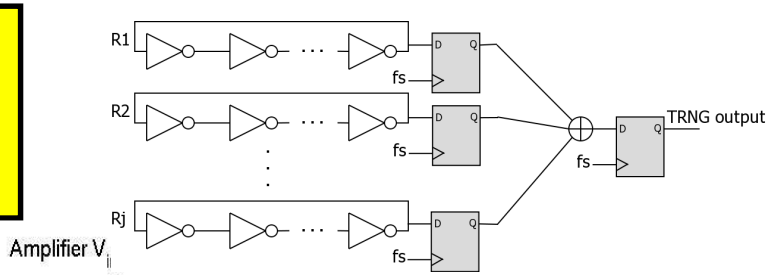
- **Results**
  - Increase of the frequency up to 45%
  - Effective and local coupling with the power/ground network

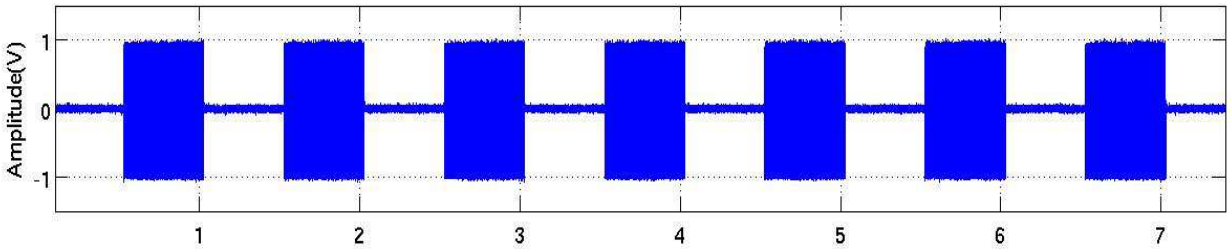
More details in : Local and Direct EM Injection of Power Into CMOS Integrated Circuits. FDTC 2011: 100-104

4- Results : Front Side Injection

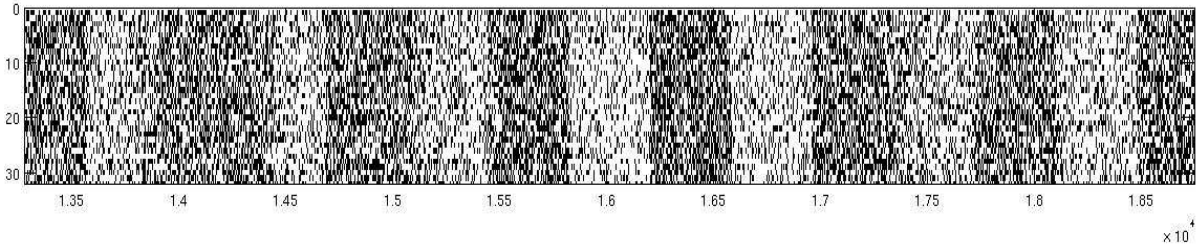
Wold TRNG

- **TRNG = 50 ROs**
- **Sampling frequency 24 kHz.**
- **FPGA Actel**

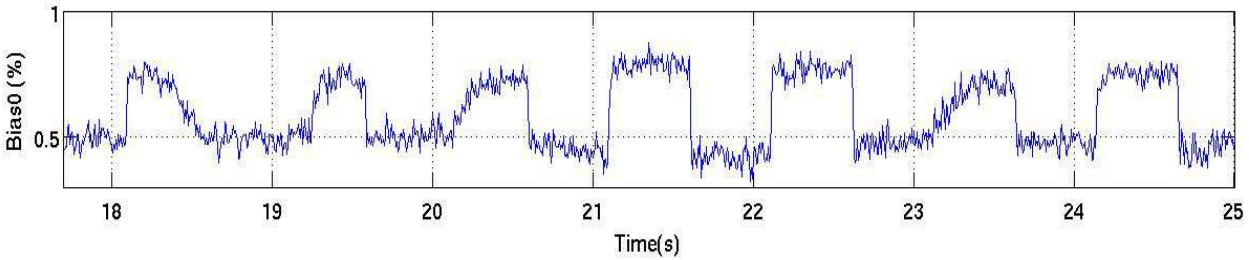


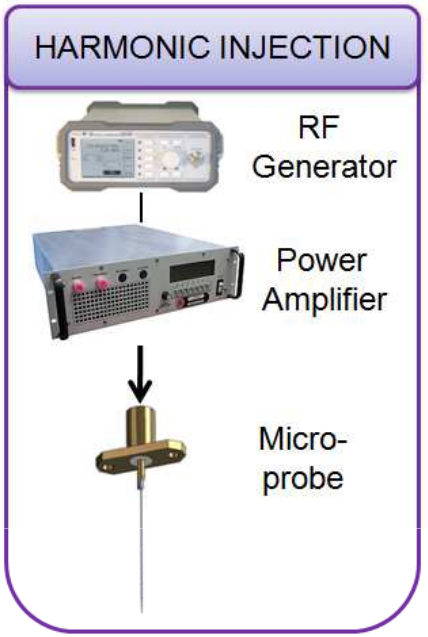


Flot bitstream



ZOOM Bias0(Time) 5 lines package



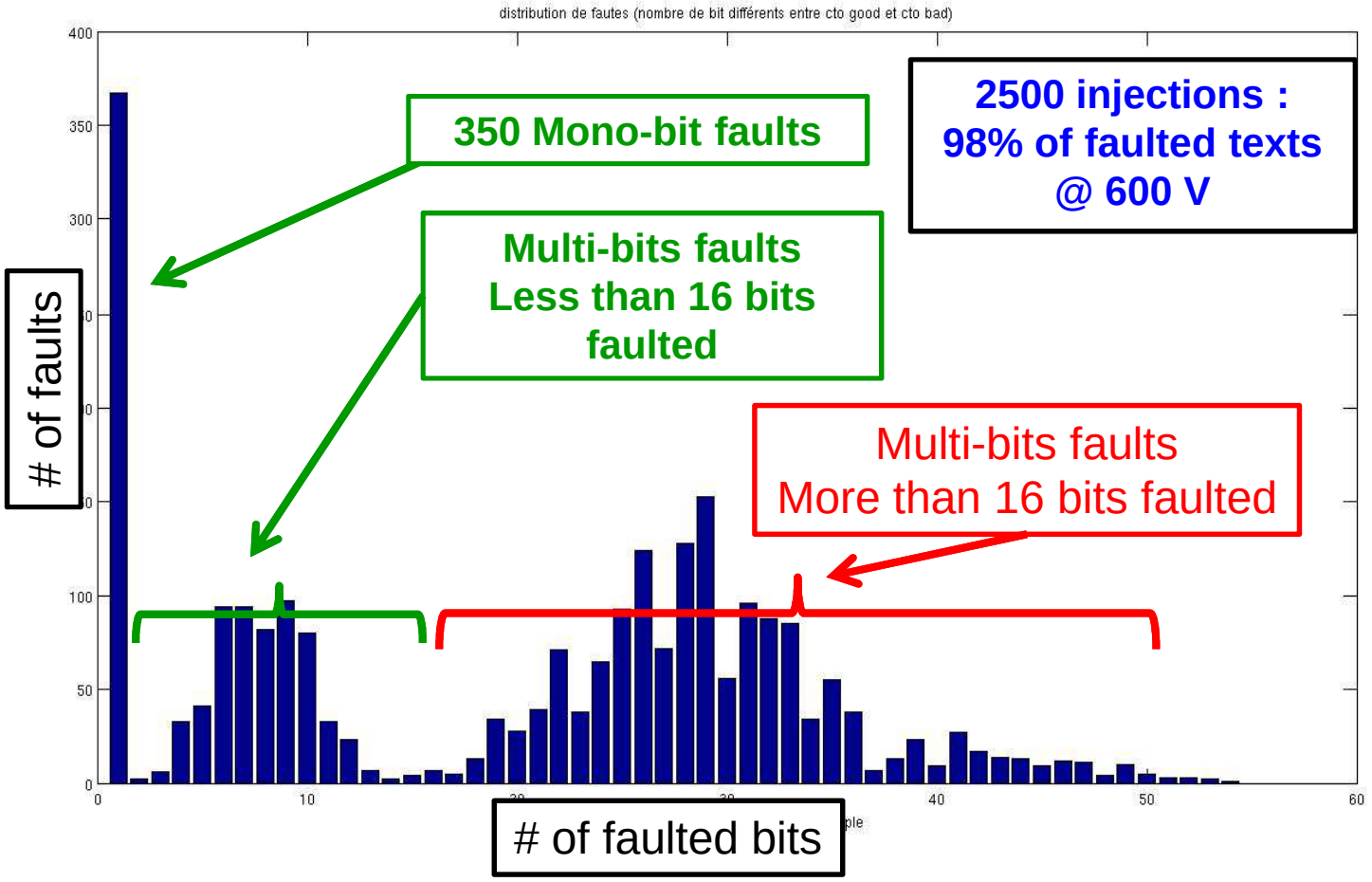


Dynamic Control of the bias

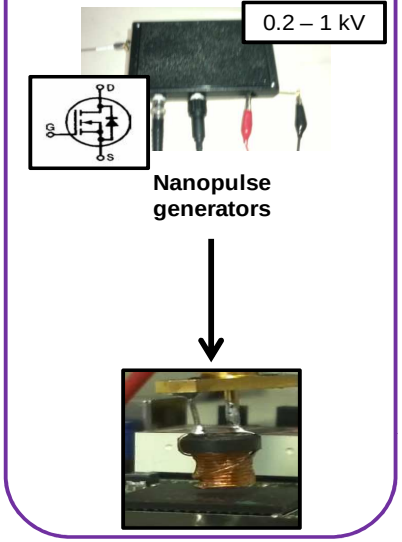
More details in : Contactless Electromagnetic Active Attack on Ring Oscillator Based True Random Number Generator. COSADE 2012: 151-166

4- Results : Front Side Injection

Hardware AES
FPGA Xilinx
50 MHz

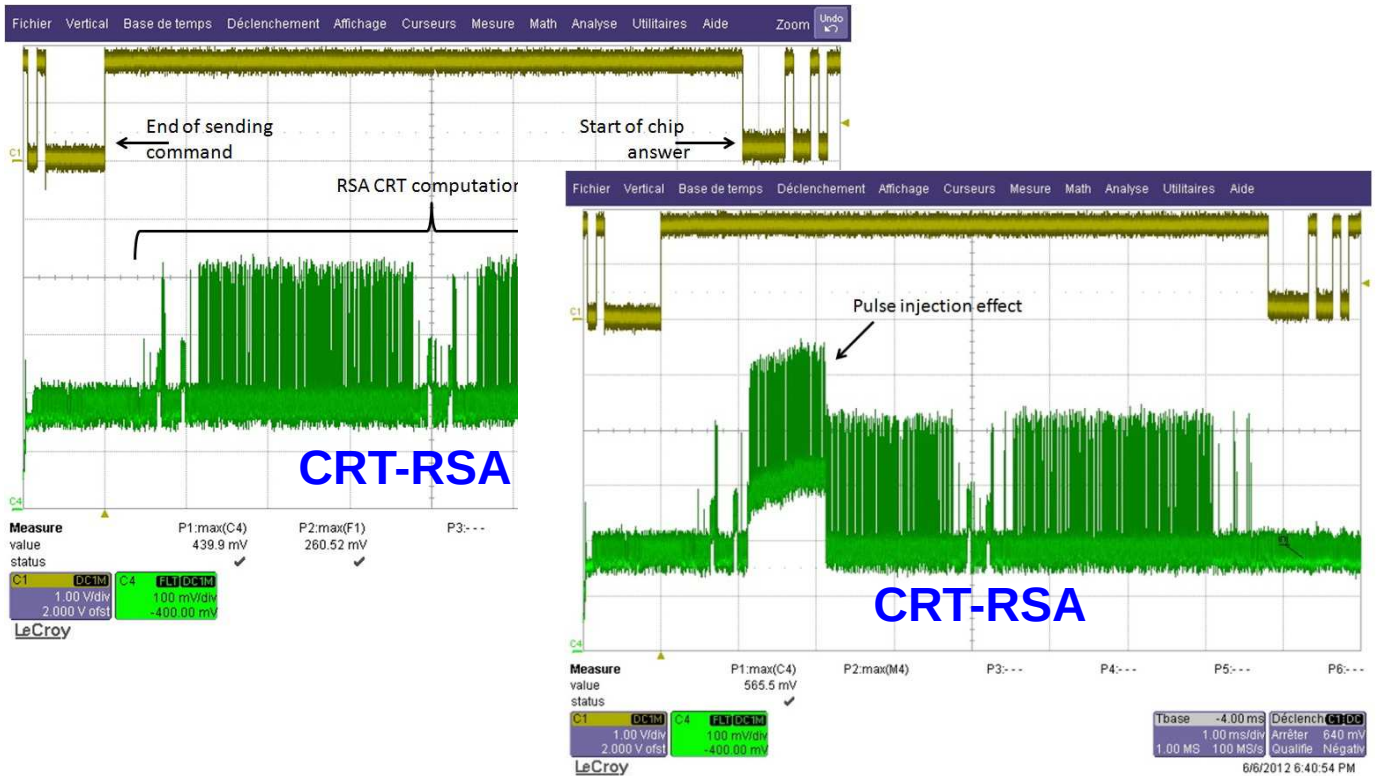


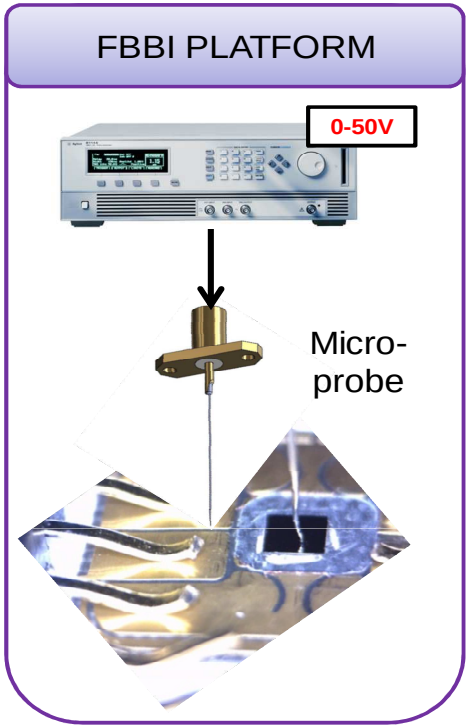
PULSED INJECTION



4- Results : Back Side Injection

Microcontroller (90nm)
(countermeasures were disabled)





Application of the Bellcore attack !
Glitch detectors have flagged the injection (optimizations are on going)

More details will be available in : Yet Another Fault Injection Technique: by FBBI Yacc 2012 (24- 28 September, Porquerolles Island, France)

4- Conclusion

- Three different Injection platforms

- to pertubate an internal clock generator (130nm ASIC)
- to Bias a Wold TRNG (FPGA Actel Fusion)
- to Pass a Piret & Quisquater Attack (FPGA xilinx spartan)
- new : Forward Body Bias Injection Technique

- Spatial resolution is limited to few hundreds of µm

- Countermeasure : Voltage Glitch detectors

- There is room for optimization (resolution, efficiency)

- increase of the frequency range of EM platforms to couple with smaller metallic structures)

- specific and more sophisticated probes to increase the resolution and the efficiency

- FBBI seems an promising fault injection technique (works are on going)

Thanks

People involved in the EMAISeCi and E-MATAHARI Projects

A. Aubert, P. Bayon, L. Bossuet, L. Chusseau, A. Dehbaoui, J.M. Dutertre, V. Fisher, S. Jarrix, P. Y. Liardet, M. Lisart, P. Maistri,T. Ordas, F. Poucheret, J. Raoult, B. Robisson