# Electromagnetic Attacks on Ring Oscillator-Based True Random Number Generator

Pierre Bayon, Lilian Bossuet, Alain Aubert, Viktor Fischer
François Poucheret, Bruno Robisson, Philippe Maurine

Université de Lyon - Université Montpellier 2 - CEA Leti

pierre.bayon@univ-st-etienne.fr
francois.poucheret@lirmm.fr

20 June 2012

# Outline

1. Introduction
   - True Random Number Generator ?
   - Threat model
2. Attacks on TRNG
   - Case study
   - Markettos & Moore attack
3. Our active attack
   - Experimental Setup
   - Effect of the Electromagnetic harmonic injection on ring oscillators
   - Effect of the Electromagnetic injection on the TRNG
4. Some Insight on EM analysis

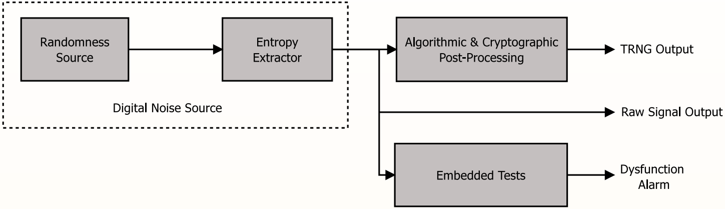
# Outline

1. Introduction
   - True Random Number Generator ?
   - Threat model
2. Attacks on TRNG
   - Case study
   - Markettos & Moore attack
3. Our active attack
   - Experimental Setup
   - Effect of the Electromagnetic harmonic injection on ring oscillators
   - Effect of the Electromagnetic injection on the TRNG
4. Some Insight on EM analysis

# True Random Number Generator in Cryptography

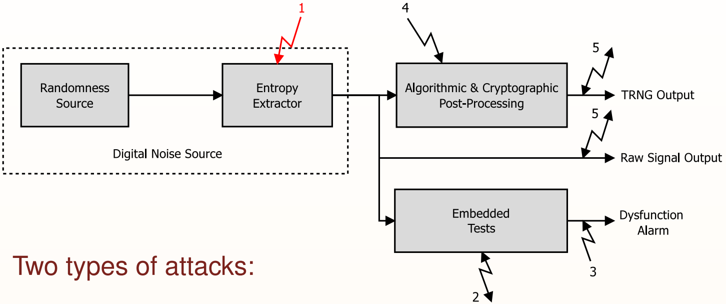
- Use of True Random Number Generators (TRNGs) in cryptography:
  - Key generation for cipher
  - Generation of initialization vectors, padding values, ...
  - Counter-measures against side-channel attacks
- Requirements on TRNGs:
  - Good statistical properties of the output bitstream
  - Output unpredictability
  - Security:
    - Robustness
    - Testability of the randomness source

# General structure of a TRNG



- Randomness source and entropy extractor:
  - High entropy per bit.
  - Good output bit rate.
  - Not manipulable.
- Post processing to enhance statistical properties.
- Embedded tests:
  - Detect total failure.
  - Evaluate the quality of the randomness source.

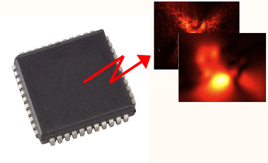
# Threat model of TRNG

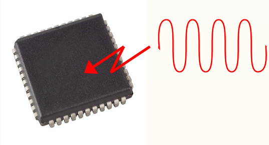


- Two types of attacks:

Passive: Reading of a Side-Channel information

**Active: Perturbation of the design behavior to create a fault**





# Outline

1. Introduction
   - True Random Number Generator ?
   - Threat model
2. Attacks on TRNG
   - Case study
   - Markettos & Moore attack
3. Our active attack
   - Experimental Setup
   - Effect of the Electromagnetic harmonic injection on ring oscillators
   - Effect of the Electromagnetic injection on the TRNG
4. Some Insight on EM analysis

# TRNG used as case study

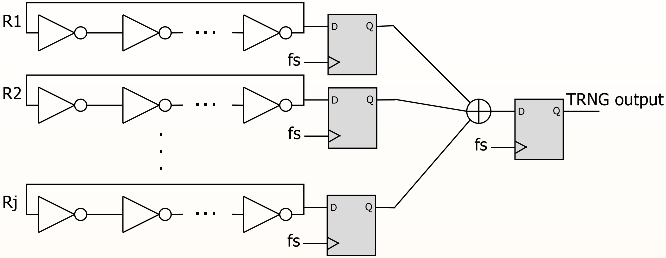


Figure: RO-Based TRNG

## Remarks:

- Use the RO-generated clock jitter as a source of randomness
- ROs should be independent - they should have different frequencies, and these frequencies **should not be correlated**

# Markettos & Moore attack

Up to our knowledge there is only one paper dealing with a practical attack on TRNG: [1]

- Limited to a 2-RO based TRNG.
- The frequency of the harmonic signal that could be injected on the power line is limited by the power pads.
- The power line could be filtered - no effect on the injection.
- Require modification of the board.

[1] [MM09] "The Frequency Injection Attack on Ring-Oscillator-Based True Random Number Generators", A. T. Markettos and S. W. Moore, Cryptographic Hardware and Embedded Systems

# Electromagnetic waves as a new attack medium ?

- Electromagnetic Potentials:
  - Penetration capabilities
  - Hard to detect in electronic environment
  - Low-cost equipment
- Feasibility of Electromagnetic attacks?
  - Is it possible to create a local coupling with just a part of IC ?
  - Is it possible to disturb the behavior of a CMOS IC without removing package ?
- What about an attack on **realistic** TRNG ?

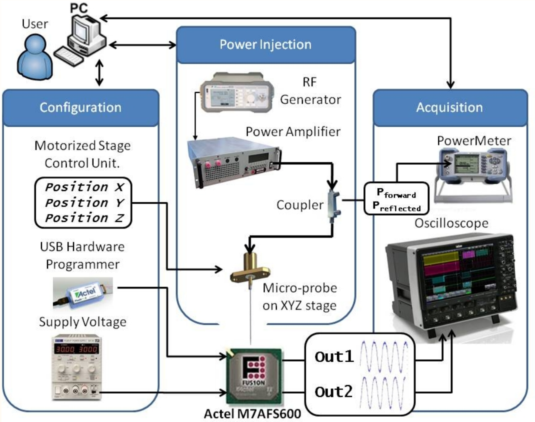
# Outline

1. Introduction
   - True Random Number Generator ?
   - Threat model
2. Attacks on TRNG
   - Case study
   - Markettos & Moore attack
3. Our active attack
   - Experimental Setup
   - Effect of the Electromagnetic harmonic injection on ring oscillators
   - Effect of the Electromagnetic injection on the TRNG
4. Some Insight on EM analysis

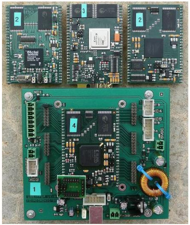
# Electromagnetic harmonic signal injection bench

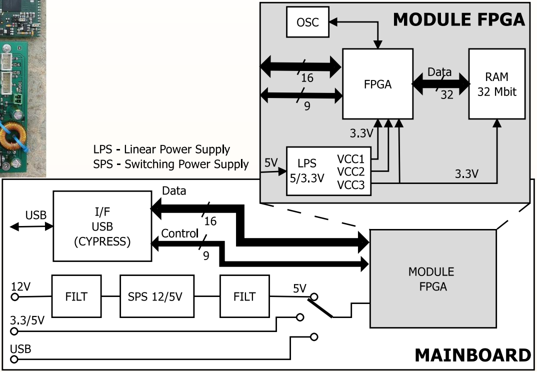
Electromagnetic Injection bench:

- 50W power amplifier
- Electromagnetic probe:
  - Length: 30mm
  - Diameter: 10 to 200 $\mu$m



# FPGA board





FPGA used: Actel Fusion M7AFS600 (Flash Technology - 0.13 $\mu$m)

# Target #1 - ROs measurement

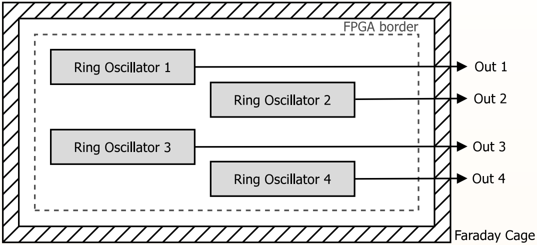


Figure: Target #1 setup

The ROs were composed by 3 elements - working frequency around 325MHz.

# Choice of the injection frequency - Target#1

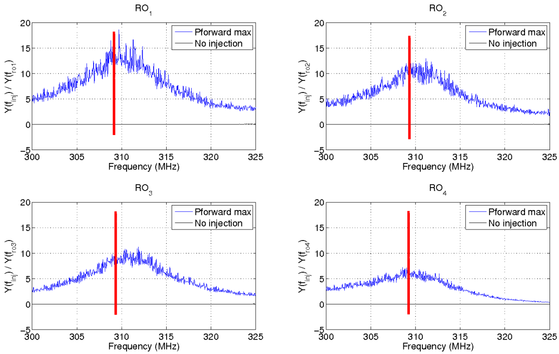


Figure: Amplitude of the DFT for Finj over the amplitude of the DFT for Fro vs Finj

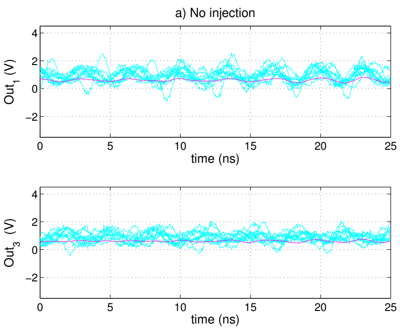
We have decided to choose Finj = 309MHz - seems to have good performance while not being the best injection frequency.

# From behavioral perturbation to locking phenomenon

To ensure good statistical properties of the TRNG, the ring oscillators should not be dependent.
However, two ring oscillators that have close frequencies could be synchronized together or on another signal - this phenomenon is called locking. It could be induced by modifying:

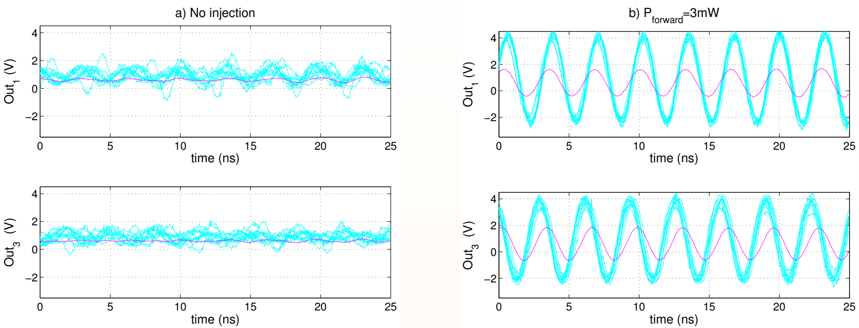
- The working temperature,
- The voltage of the FPGA core,
- etc ...

# Persistance plot for Finj = 309MHz - Target#1



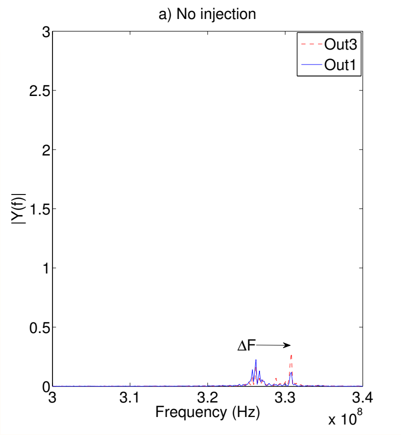
Here is a persistent plot: the cyan traces are the traces acquired with the oscilloscope and the purple trace is the mean of the cyan traces.

# Persistance plot for Finj = 309MHz - Target#1

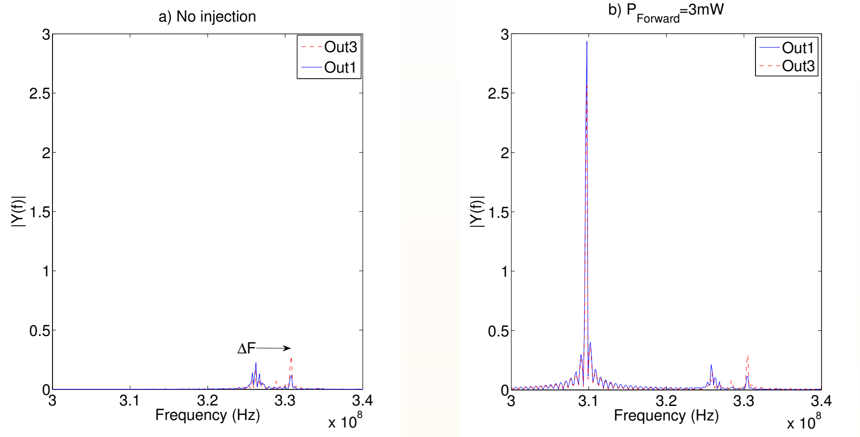


Evidence of the **locking phenomenon** induced by the injection. The RO outputs are now synchronized.

# DFT plot for Finj = 309MHz - Target#1



# DFT plot for Finj = 309MHz - Target#1



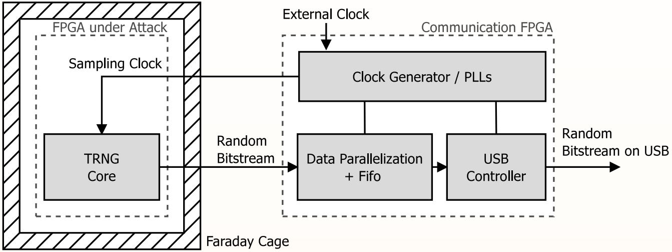
Appearance of the injection frequency in the DFT of the RO outputs.

**The working frequency of the ROs is now Finj**.

# Question ?

Now that we are able to lock ring oscillators on an injected signal, what will be the effect on a RO-based TRNG?

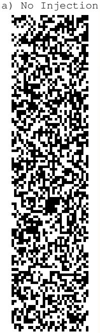
# Target #2 - TRNG measurement



- The TRNG core is a 50 ROs Wold TRNG [2]
- Working frequencies of the ROs around 320MHz.
- Sampling frequency: 24KHz.
- The TRNG passes usual statistical tests (FIPS, NIST, ...).

[2] **50 ROs is two time the number of ROs recommended** in "Analysis and Enhancement of Random Number Generator in FPGA Based on Oscillator Rings", K. Wold and C. H. Tan, ReConFig 2008

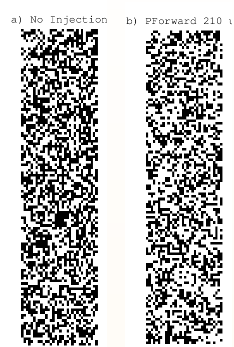
# TRNG output bitstream - Target#2



| PForward | No Injection | 210 $\mu$W | 260 $\mu$W | 300 $\mu$W |
|---|---|---|---|---|
| Bias[3] | 0.005 | | | |
| NIST tests | SUCCESS ☺ | | | |

[3] Bias = probability to obtain a '0' - 0.5

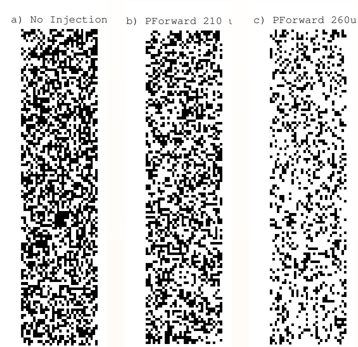
# TRNG output bitstream - Target#2



| PForward | No Injection | 210 $\mu$W | 260 $\mu$W | 300 $\mu$W |
|---|---|---|---|---|
| Bias[3] | 0.005 | 0.079 | | |
| NIST tests | SUCCESS ☺ | FAIL ☹ | | |

[3] Bias = probability to obtain a '0' - 0.5

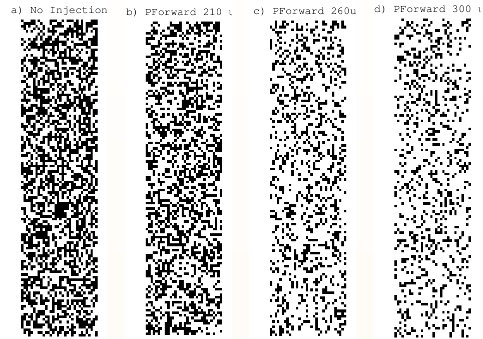
# TRNG output bitstream - Target#2



| PForward | No Injection | 210 $\mu$W | 260 $\mu$W | 300 $\mu$W |
|---|---|---|---|---|
| Bias[3] | 0.005 | 0.079 | 0.256 | |
| NIST tests | SUCCESS ☺ | FAIL ☹ | FAIL ☹ | |

[3] Bias = probability to obtain a ’0’ - 0.5

# TRNG output bitstream - Target#2

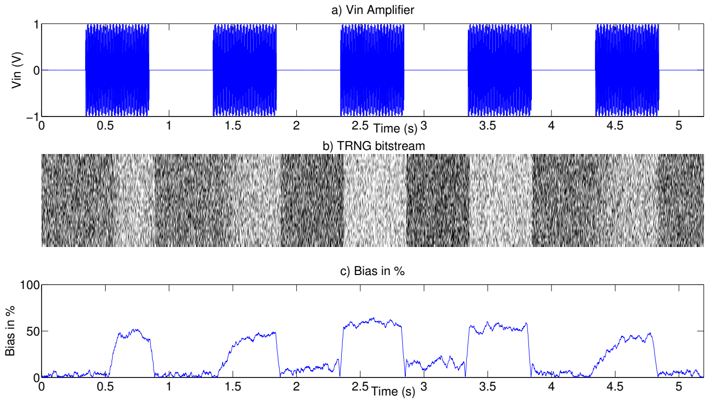


| PForward | No Injection | 210 $\mu$W | 260 $\mu$W | 300 $\mu$W |
|---|---|---|---|---|
| Bias[3] | 0.005 | 0.079 | 0.256 | 0.275 |
| NIST tests | SUCCESS ☺ | FAIL ☹ | FAIL ☹ | FAIL ☹ |

We are able to bias **continuously the TRNG up to 50%.** What about the dynamic behavior of the attack ?

[3] Bias = probability to obtain a '0' - 0.5

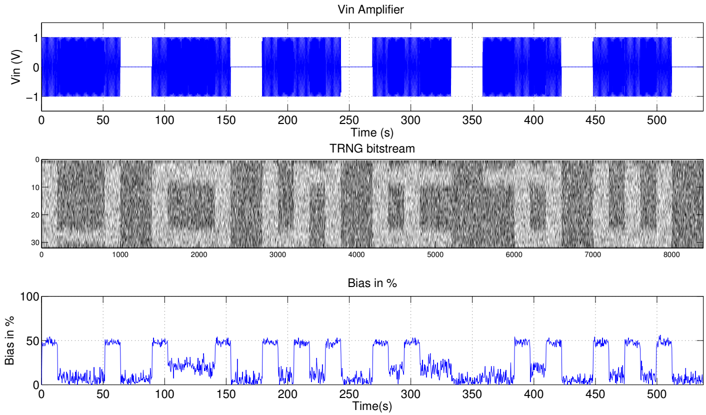
# Dynamic control of the bitstream - Target#2



The effect of the attack is visible only during the period of the attack.

The setup and falling time of the attack is directly proportional to the performance of the injection bench.

# Just for the fun - Target#2



To perform this complex attack, the sampling clock of the TRNG was reduce to 500Hz.

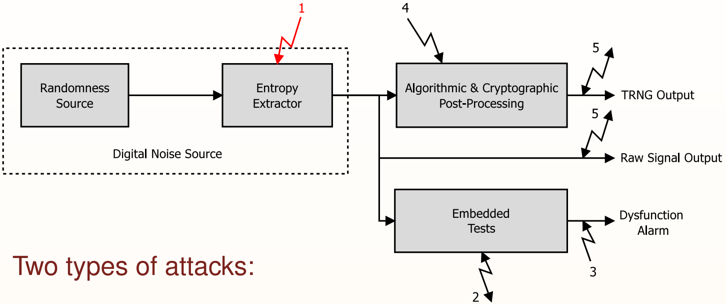
# Conclusion

- We have shown that Electromagnetic injection can make ROs locked.
- We achieved to control a 50-RO TRNG:
  - Up to 50% bias of the output bitstream: **make an attack on a cryptographic system easier**.
  - Fast setup and falling time.
- Electromagnetic waves are good candidates to perform such attacks:
  - Not invasive:
    - Board
    - Device
  - No limit on the frequency of the injected signal.
  - Low-cost equipment.

# Outline

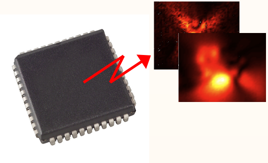
1. Introduction
   - True Random Number Generator ?
   - Threat model
2. Attacks on TRNG
   - Case study
   - Markettos & Moore attack
3. Our active attack
   - Experimental Setup
   - Effect of the Electromagnetic harmonic injection on ring oscillators
   - Effect of the Electromagnetic injection on the TRNG
4. Some Insight on EM analysis

# Threat model of TRNG

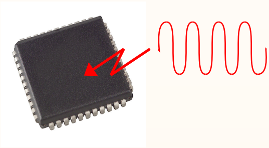


- Two types of attacks:

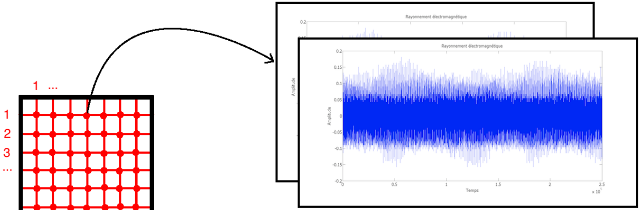
**Passive: Reading of a Side-Channel information**



Active: Perturbation of the design behavior to create a fault



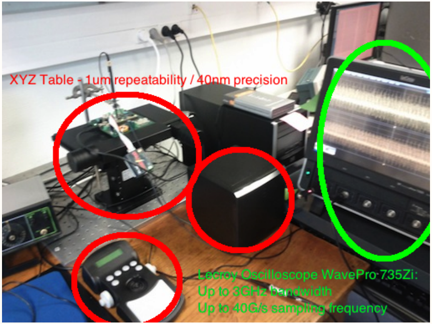
# Cartography Principle

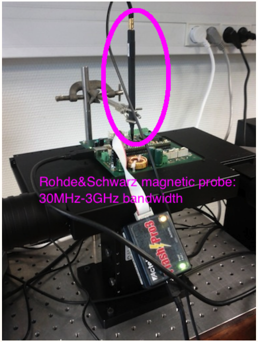


Chip to analyze

Set of EM traces for the point {1 - 4}

# EM Analysis test bench


XYZ Table - 1um repeatability / 40nm precision
Lecroy Oscilloscope WavePro 735Zi:
Up to 3GHz bandwidth
Up to 40G/s sampling frequency



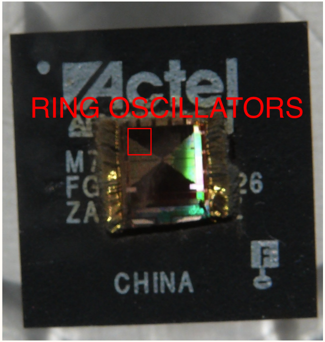
# Frequency analysis

From the method proposed in [4]

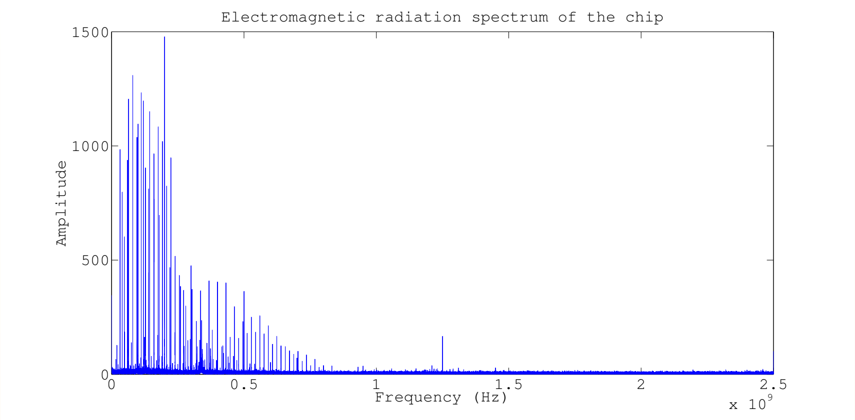
- A Fast Fourier Transform is computed for each electromagnetic trace.
- To obtain a cartography at a given frequency, all you have to do is to take for each "point", the amplitude of the spectrum at this frequency.

[4] [SGM09] Electromagnetic Radiations of FPGAs: High Spatial Resolution Cartography and Attack on a Cryptographic Module, L. Sauvage, S. Guilley and Y. Mathieu, ACM Transactions on Reconfigurable Technology and Systems 2009.

# Floorplan



# Lost?



Ok... What if i don't know the working frequencies of my ring oscillators ?

# Idea

The frequency of a ring oscillator depends on:

- The temperature of the chip
- The voltage of the chip
- The age of the chip
- ...

To enhance the frequency analysis on ring oscillators, the idea is to realize a differential analysis.

Two different set of traces are acquired with a modification on the parameters above.

The easiest parameter to modify is the temperature:

- No modification of the board is required
- Max cost: 30 euros for a good space heater.

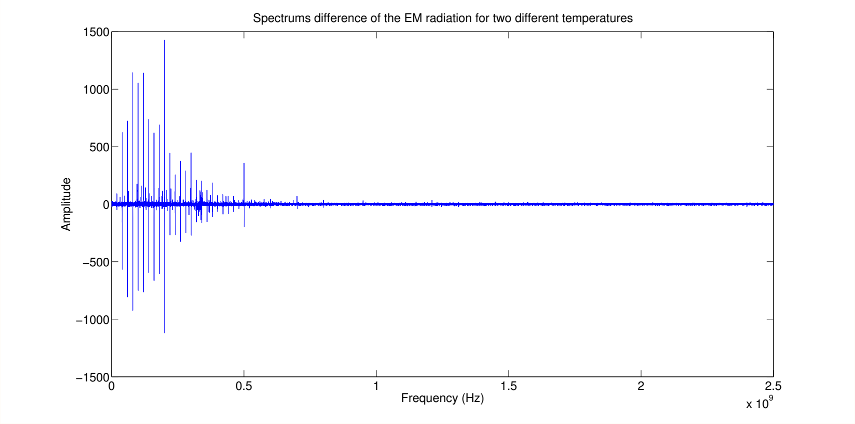
# Idea

For the two acquisitions:

- Frequencies of the oscillators should be different.
- Other frequencies should not change.

By making the difference of the spectrums, we should only highlight the frequency of the oscillators.

# Spectrum difference

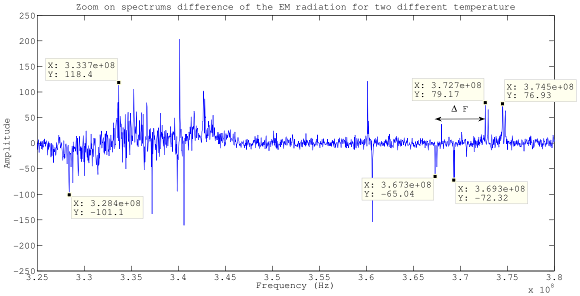


I can see clearly now the "static" frequencies are gone

# Differential analysis

- Less "useless" peaks.
- Spotting of the interest area easier.
- Yet all the "useless" peaks are not deleted ... small difference of frequency for some peaks between two acquisitions.

# Differential analysis - zoom

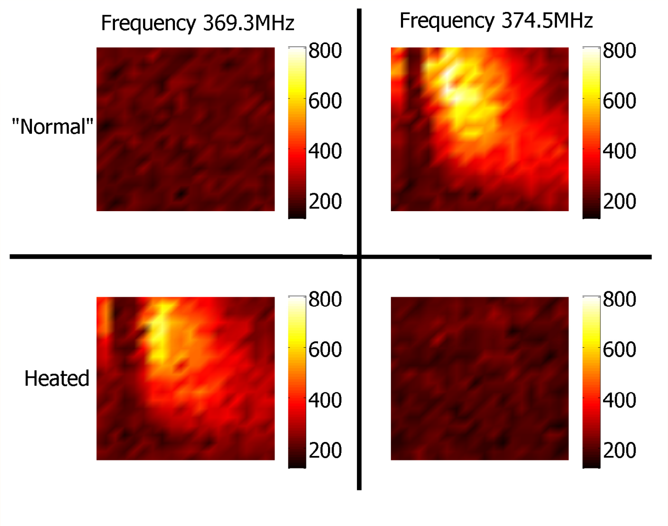


Several "pairs" of frequencies:

- 369.3 MHz and 374.5 MHz
- 367.3 MHz and 372.7 MHz
- 328.4 MHz and 333.7 MHz

Frequency difference = 5.3 MHz roughly.

# Frequency cartography for 369.3MHz and 374.5MHz



# Thank you, any questions ?