Random number generation: a potential target of electromagnetic emanation analysis ?

Pierre BAYON - Lilian BOSSUET - Alain AUBERT - Viktor FISCHER

Laboratoire Hubert Curien, UMR 5516 CNRS
Jean Monnet University, Member of University of Lyon
Saint-Etienne, France

pierre.bayon@univ-st-etienne.fr

17 June 2011

Outline

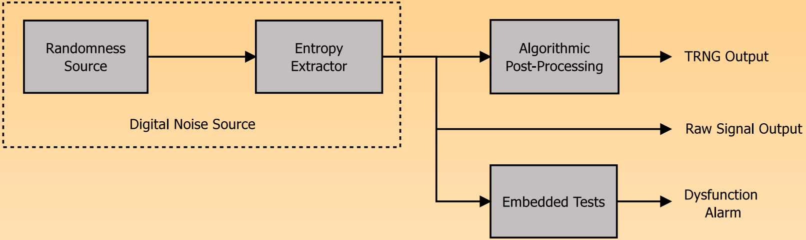
Outline

1. Introduction
   - TRNGs General Structure
   - EMA on TRNG: State of the Art
2. Case Study
   - TRNG Principle
   - Implementation and Floorplan
   - EMA Test Bench
   - Setup of the Bench
3. Tools Used
   - Frequential Analysis
   - Cross-Correlation Cartography
4. Results
5. Conclusion

This work has been done within the ANR EMAISeCi project (http://www.lirmm.fr/emaiseci/).

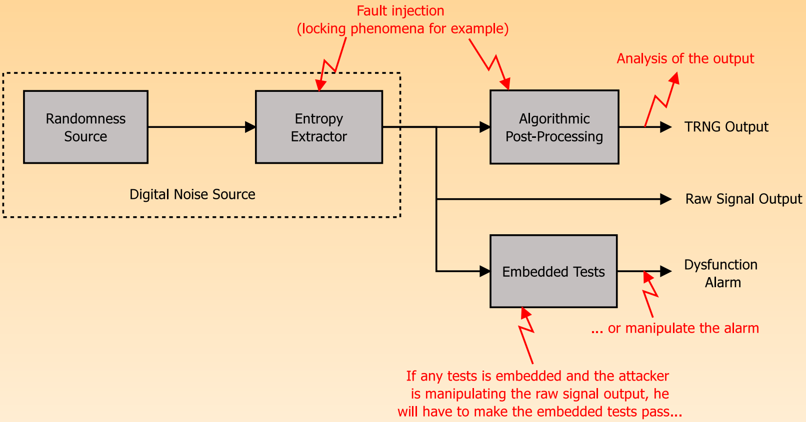
This presentation is an overview of my recent work on EMA on TRNG.

TRNGs General Structure



- Source of randomness and entropy extractor:
  - Should give as much entropy per bit as possible.
  - Should enable sufficient bit-rate.
  - Shouldn't be manipulable (robustness).
- Algorithmic post-processing:
  - Enhances statistical properties of the output without reducing the entropy.
- Embedded tests:
  - Detect immediately the generator's total failure.
  - Evaluate the quality of the source of randomness in real time.

How to Attack a TRNG

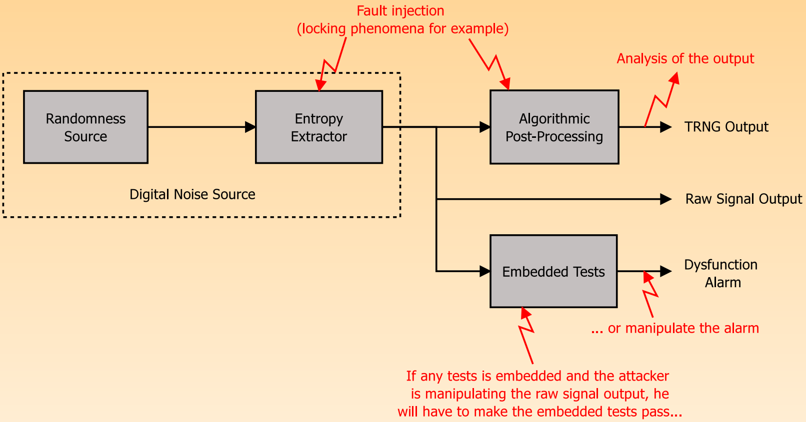


State of the Art

- No paper dealing with passive or active EM attacks on TRNG to date.
- Some tests regarding the sensibility of the TRNG to different parameters such temperature, core voltage, ..., can be viewed as attacks.
- Only one dealing with periodic signal injection on the power line rises: [MM09] - The Frequency Injection Attack on Ring-Oscillator-Based True Random Number Generators.

- EMA on cryptographic systems is something well-tried.
- It should not be a problem then to apply these methodologies to TRNG EMA.
  - FPGA implementation of a block cipher is a complex structure (more than 1000 logic cells and registers).
  - So, area of interest gives a relatively high electromagnetic emanation compared to the surrounding blocks.
- But ...
  - TRNG area is much smaller (usually not more than 300 logic cells and 100 registers).
  - So, area of interest gives an electromagnetic emanation that is lower than that of the cipher for example.
  - TRNG are to be embedded in a cryptographic system, so with a surrounding using much more logic cells.

How to Attack a TRNG



Fault injection
(locking phenomena for example)

Analysis of the output

Randomness Source

Entropy Extractor

Digital Noise Source

Algorithmic Post-Processing

TRNG Output

Raw Signal Output

Embedded Tests

Dysfunction Alarm

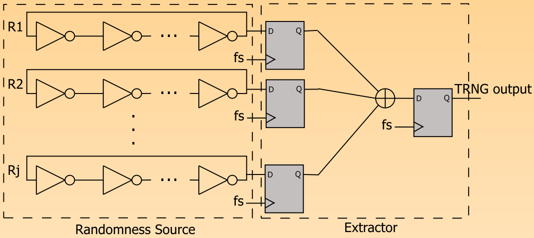
... or manipulate the alarm

If any tests is embedded and the attacker is manipulating the raw signal output, he will have to make the embedded tests pass...

Outline

1. Introduction
   - TRNGs General Structure
   - EMA on TRNG: State of the Art
2. **Case Study**
   - TRNG Principle
   - Implementation and Floorplan
   - EMA Test Bench
   - Setup of the Bench
3. Tools Used
   - Frequential Analysis
   - Cross-Correlation Cartography
4. Results
5. Conclusion

TRNG principle - [WT08] Wold and Tan TRNG



Principle

- Improvement of an existing TRNG ([SMS07] A Provably Secure True Random Number Generator with Built-in Tolerance to Active Attacks)
- Use the RO-generated clock jitter as a source of randomness.

Implementation

- Study performed on an Actel Fusion M7AFS600.
- Two versions of topology were made, differing in TRNG position on the chip.
- The TRNGs were composed of 54 rings of 5 elements (frequency of the ring roughly equal to 200MHz).
- Other frequencies involved in the chip: 36MHz and 127MHz (PLL frequencies), 100MHz (internal RC oscillator).

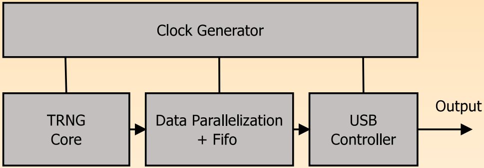


Figure: TRNG testing environment.

Floorplan

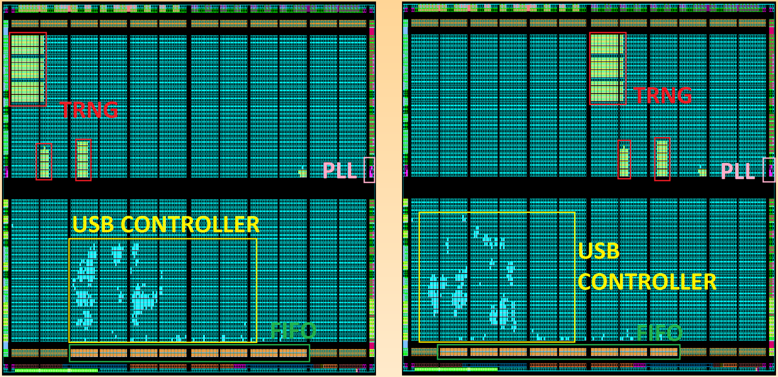
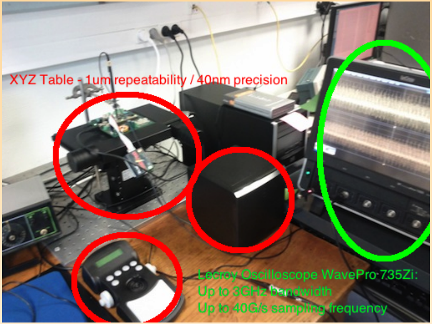
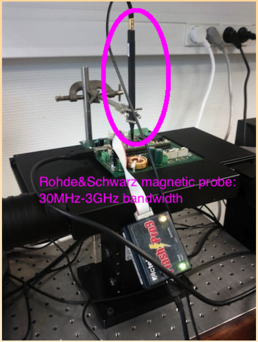


Figure: On the left the first position, on the right the second one.

EMA Test Bench





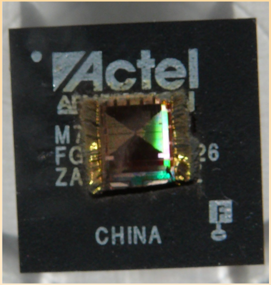
Acquisition Setup

- Sampling used: 20G sample / s
- Number of points on each trace: 100000
- Before being acquired, each trace is averaged 16 times.

All the results presented in the following have been obtained using a Rohde&Schwarz amplifier (BW: 30MHz - 3GHz, gain 20dB, noise figure 4.5dB).

Calibration of the Measurement

The calibration of the test bench has been done thanks to a decapsulated chip.



We are able to place precisely the probe over the DIE.

Outline

Frequential Analysis

From the method proposed in [1]

- A Fast Fourier Transform of each traces is computed.
- Then to obtain a cartography at a certain frequency, one just needs to take the module of the FFTs at this frequency.

---

[1] [SGM09] Electromagnetic Raditions 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.

Cross-Correlation Function (NXC Function)

From the method proposed in [2]
Let's take two temporal measurements A and B.

Cross-Correlation Function

$$\Gamma_{A,B}(d) = \frac{cov(A,B_{-d})}{\sigma_A.\sigma_B} = \frac{\sum_{n=d}^{d+inf(n_A,n_B)-1}(A(n)-\overline{A(n)}).(B(n-d)-\overline{B(n)})}{\sqrt{\sum_{n=0}^{n_A}(A(n)-\overline{A(n)})^2}\sqrt{\sum_{n=0}^{n_B}(B(n-d)-\overline{B(n)})^2}}$$

With:

- σ_A and σ_B the standard deviations of the observations A and B.
- n_A and n_B the number of temporal samples of A and B.
- $\overline{A(n)}$ and $\overline{B(n)}$ the mean values of A and B.

Basically xcorr or xcov functions in Matlab.

---

[2] [SGF+10] Cross-Correlation Cartography, L. Sauvage, S. Guilley, F. Flament, J-L Danger and Y. Mathieu, 2010 International Conference on Reconfigurable Computing

Example

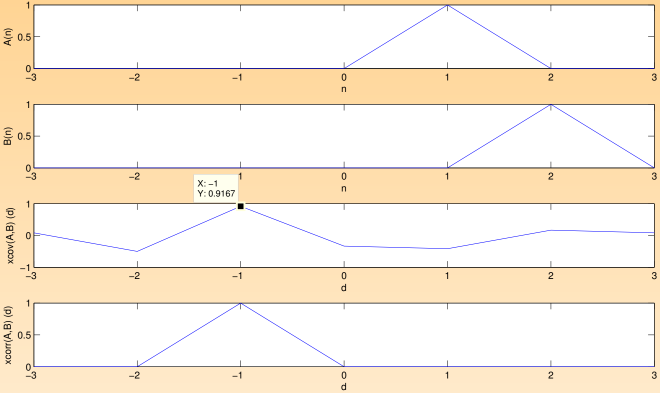


Figure: From top to bottom: Measurement A, Measurement B, xcov on A and B, xcorr on A and B

NXC Cartography

What we need in order to obtain a map

- A fixed reference observation point (Xref,Yref).
- Scanning over all the (X,Y) positions...
- ... and evaluate the maximum of the NXC((Xref,Yref),(X,Y)).

Then we will have to compute a map for each position as reference point. If we have N_P points, we will get at the end N_P maps.

NXC Cartography

- Analyzing N_P maps, especially if N_P is big, is very time consuming
- Maps where observations points are close to each others will look alike (or be correlated).
- So, maps could be classified in different groups using a bidimensional correlation function.

Bidimensional Correlation Function

$$\Gamma^{2D}_{M,N}(p,q) = \frac{cov(M,N_{-p,-q})}{\sigma_M.\sigma_N}$$

With:

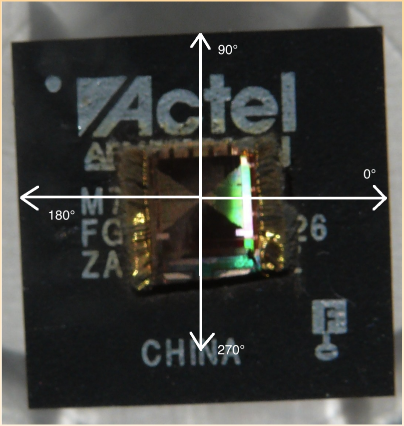
- M, N two maps.
- σ_M and σ_N, their standard deviation.

Outline

1. Introduction
    - TRNGs General Structure
    - EMA on TRNG: State of the Art
2. Case Study
    - TRNG Principle
    - Implementation and Floorplan
    - EMA Test Bench
    - Setup of the Bench
3. Tools Used
    - Frequential Analysis
    - Cross-Correlation Cartography
4. Results
5. Conclusion

Reference for the Orientation of the Probe

To deal with the different orientations of the probe we have set the reference for the angle as:



Floorplan

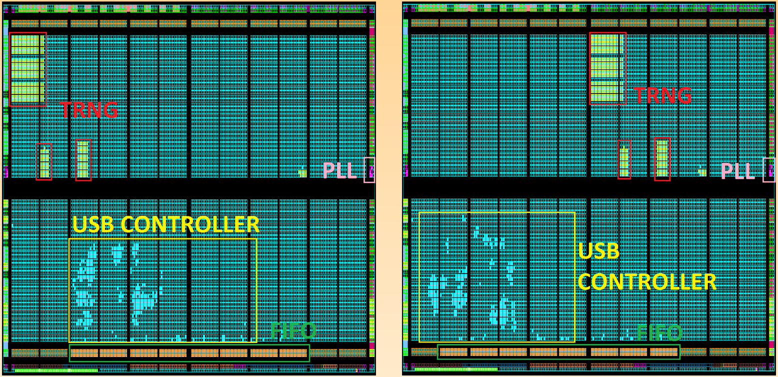


Figure: On the left the first position, on the right the second one.

Spotting the PLL using Frequential Analysis

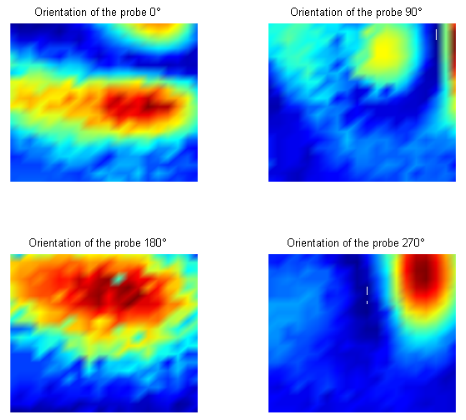


Figure: Frequential cartography at 127MHz for different orientations of the probe.

Spotting the PLL using Cross Correlation

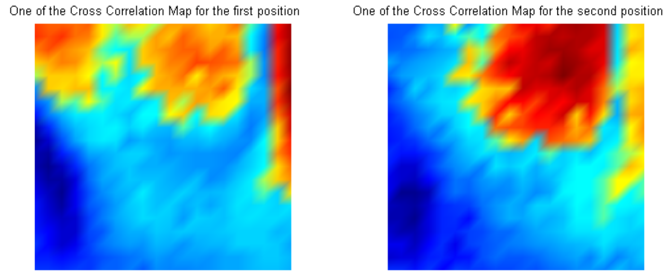


Figure: One of the Cross Correlation map obtained for position 1 on the left, and position 2 on the right with probe at 90°.

Spotting the Ring using Frequential Analysis

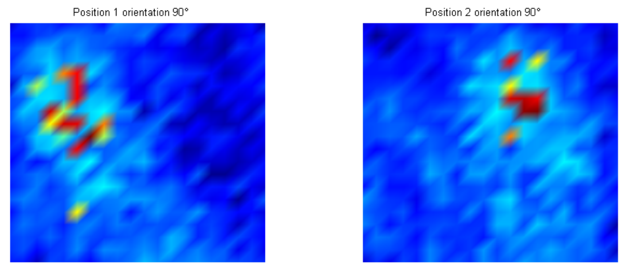


Figure: Frequential cartography between 195MHz and 197MHz for position 1 on left and position 2 on right.

Outline

Conclusion

- Using frequential analysis and knowing what was inside the chip we were able to locate:
    - The position of the PLL and the flip-flop that use given frequencies.
    - The position of the ring oscillators for the two different positions.
- Using Cross Correlation we were able to locate the PLL and the flip-flop.

Future Work

- Obtain a more accurate cartography.
- Active EM attacks on TRNG.
- Usage of EM analysis to characterize ring oscillators (locking, ...).

Thank you, any questions ?