Evaluation of Delay PUFs on CMOS 65 nm Technology: ASIC vs FPGA

Zouha Cherif[1,2], Florent Lozac'h[1], Jean-Luc Danger[1,3], Lilian Bossuet[2], Yves Mathieu[1] and Tarik Graba[1]

[1] MINES-TELECOM Institute / TELECOM-ParisTech
[2] Jean Monnet University / Hubert Curien Laboratory
[3] Secure IC

Monday, June 24, 2013

Goal of the Talk

Physically Unclonable Functions on ASIC or FPGA?
Loop PUF or arbiter PUF on ASICs ?

Outline

Overview of PUFs

- The PUF can be defined as a device signature.
- The signature depends on the manufacturing process.
- They are used for authentication or key generation purposes.
- They output a response (**ID**) from a control word called "Challenge".

Figure 1: PUF principle

- We focus our interest on **silicon** PUFs:
  - Do not require any specific technology.

Arbiter PUF Structure

- Race between two identical and parallel delay lines.
- Challenge = Control word.
- Response = Result of the race : 1 bit.

- Gassend et al.(2002)

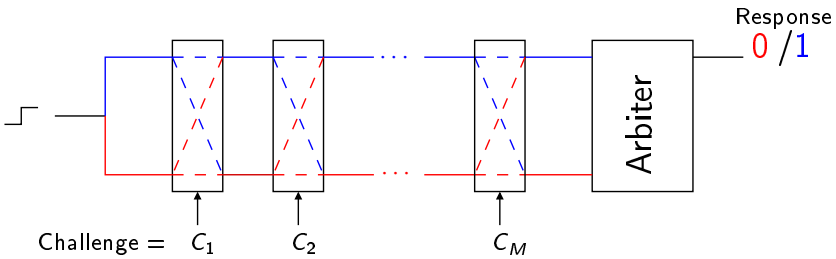


Figure 2: Arbiter PUF (2002)

- Majzoobi et al. (2010)

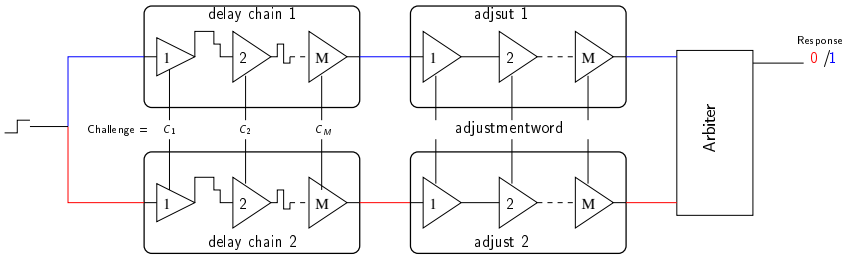


Figure 3: Arbiter PUF (2010)

Loop PUF: Structure

- Delay chains are placed sequentially → No routing constraints out of the chains.
- Challenge = Control word.
- Response = Variable length: In depends on the number of performed comparison between oscillation frequencies.
- Proposed by Cherif et al. (2012)

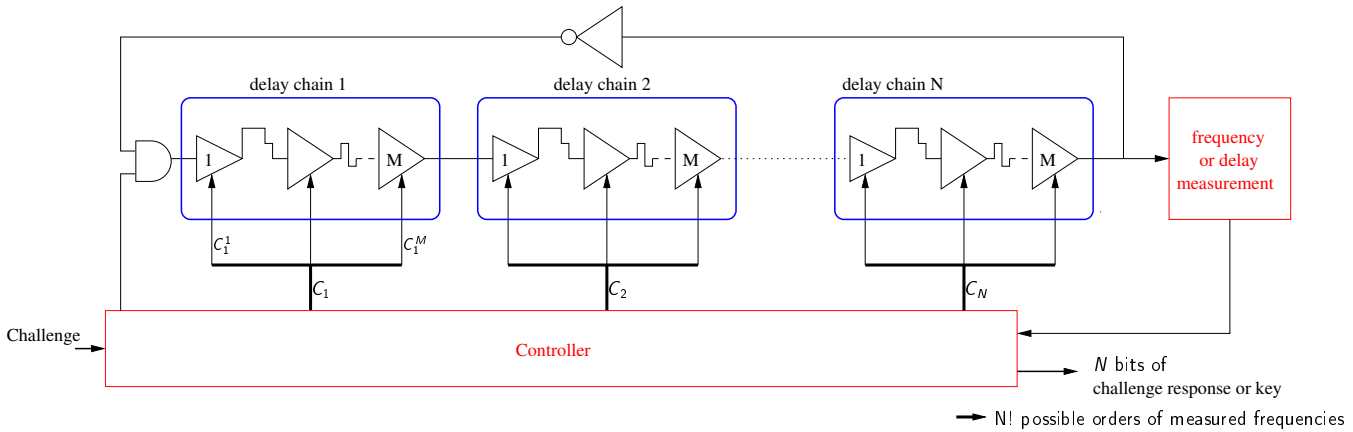


Figure 4: Loop PUF structure.

Performance Indicators

- **The randomness** gives an estimate of the imbalance between the number of IDs at '0' and the IDs at '1' for all the challenges.
- **The steadiness** (or **reliability**) expresses the level of PUF reliability which is reduced by the noise coming from the measurement environment.
- **The uniqueness** indicates the entropy between two PUFs, either in the same device (intra-uniqueness) or between devices (inter-uniqueness).

Evaluation Metrics

- **Randomness:**
  - Uses the **min-entropy** H of a response bit sequence when applying different challenges.
    $\rightarrow$ Highest (ideal) randomness at **100%**.
- **Steadiness:**
  - Based on the **min-entropy** H of a bit sequence obtained when applying the same control word T times.
  - the steadiness metric is 1-H.
    $\rightarrow$ Highest (ideal) steadiness at **100%**.
- **Uniqueness:**
  - Based on the Sum of Hamming Distance (**SHD**) of the possible ID-combinations, when applying the same challenge set to different PUFs.
    $\rightarrow$ Highest (ideal) uniqueness at **100%**.

Outline

PUF_{mix} Structure

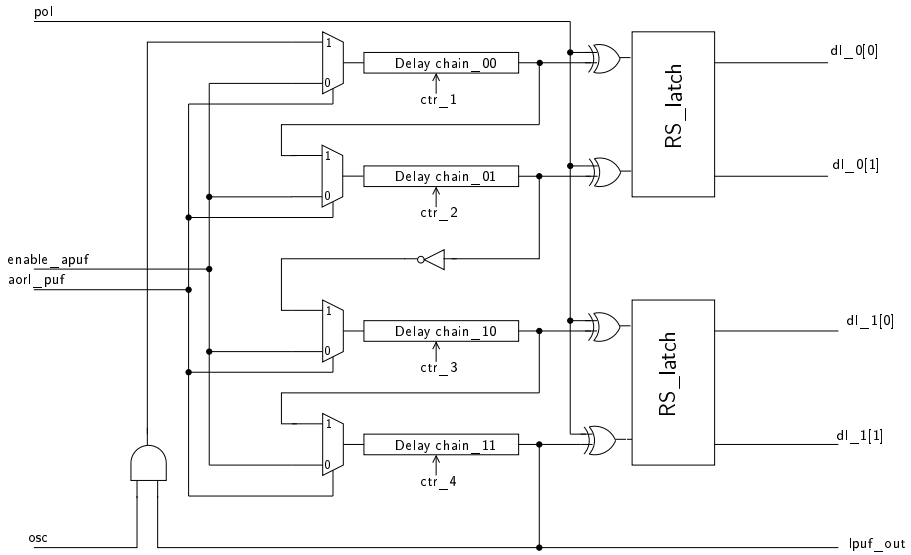


Figure 5: PUF_{mix} design

- It includes 3 Independents PUFs:
  - Arbiter PUF #1 (uses the two upper delay chains).
  - Arbiter PUF #2 (uses the two bottom delay chains).
  - Loop PUF (uses the four delay chains).

ASIC

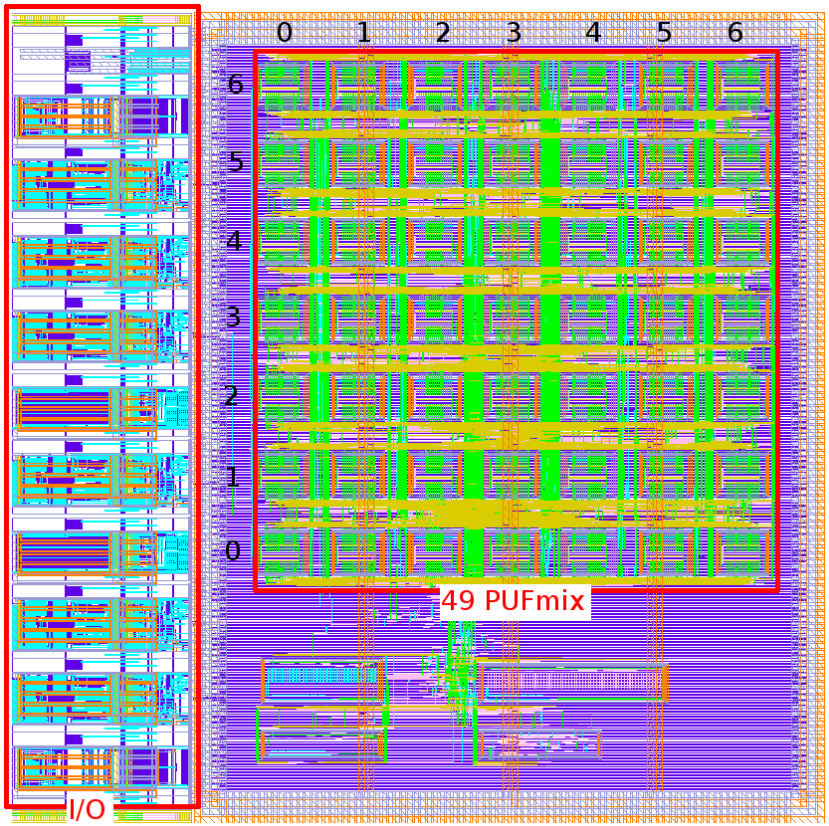
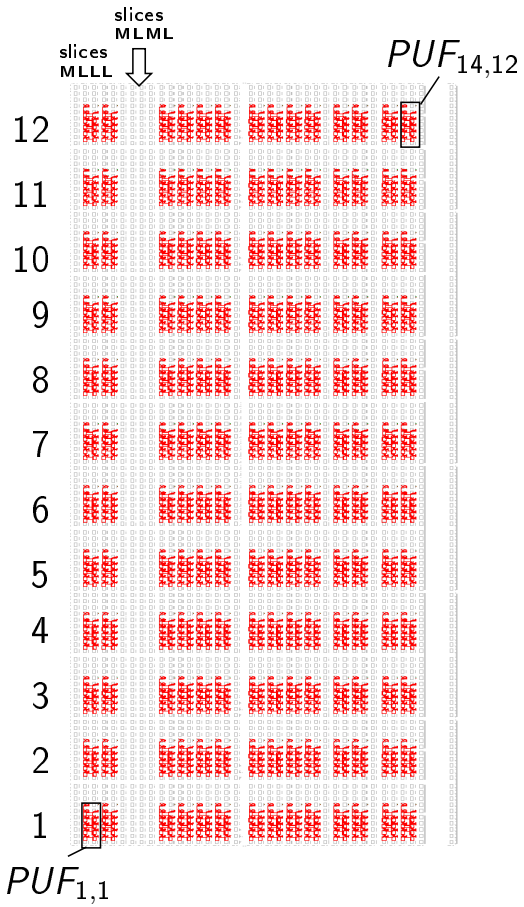


Figure 6: ASIC layout.

- 18 ASICs.
- Each ASIC embeds 49 PUF_{mix}.
- One PUF_{mix}:
  - 215 ST standard cells.
  - Occupies 2249.424 μm^2.

FPGA



- Xilinx Virtex-5 vlx50t FPGA.
- 168 PUF_{mix}.
  $\rightarrow$ 49 only are considered for fair comparison
- One PUF_{mix} occupies 24 slices
  $\rightarrow$ 0.4% of slice resources.

Figure 7: FPGA layout.

Outline

Arbiter PUF ♯1

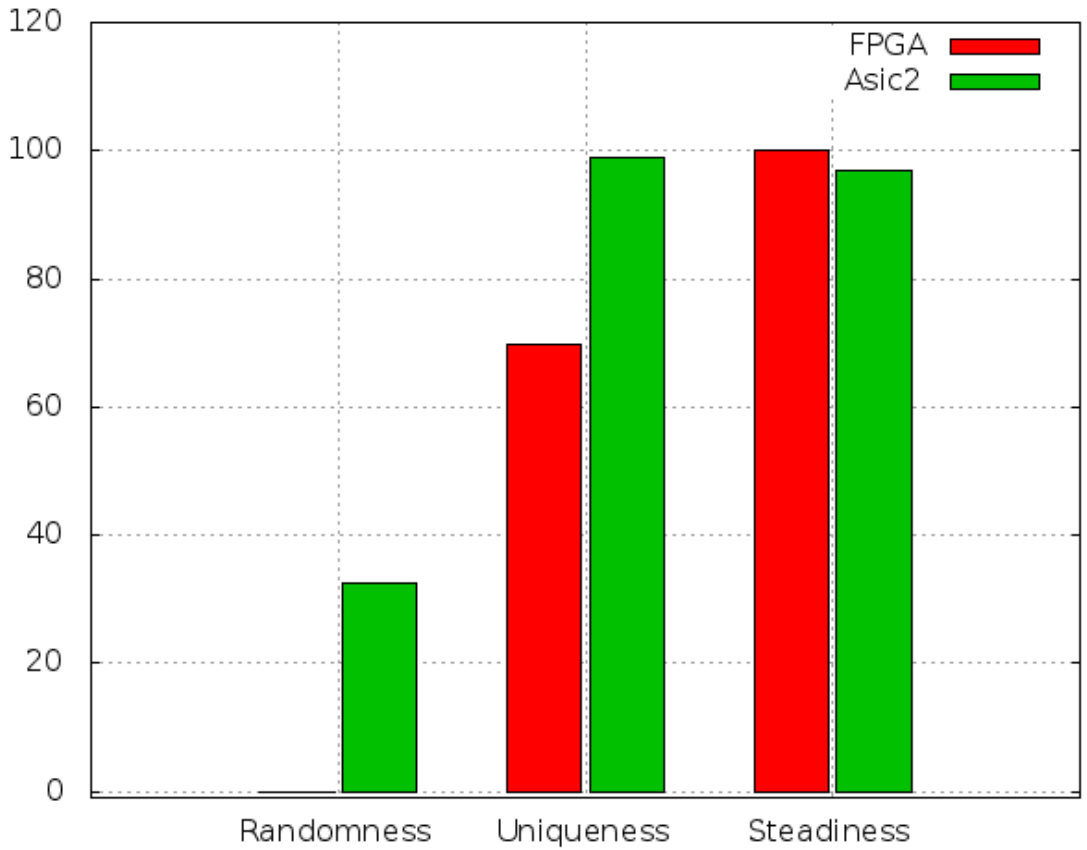


Figure 8: Intra-device evaluation of arbiter PUF ♯1

Arbiter PUF ♯2

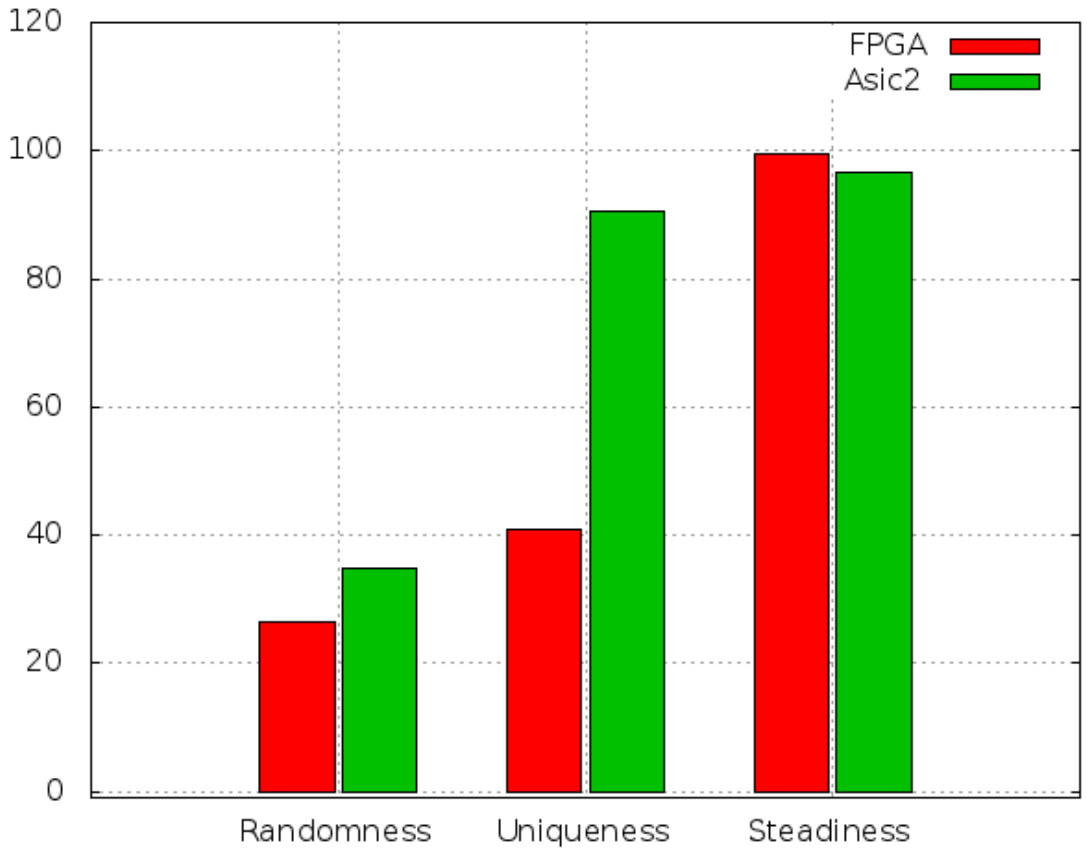


Figure 9: Intra-device evaluation of arbiter PUF ♯2

Loop PUF

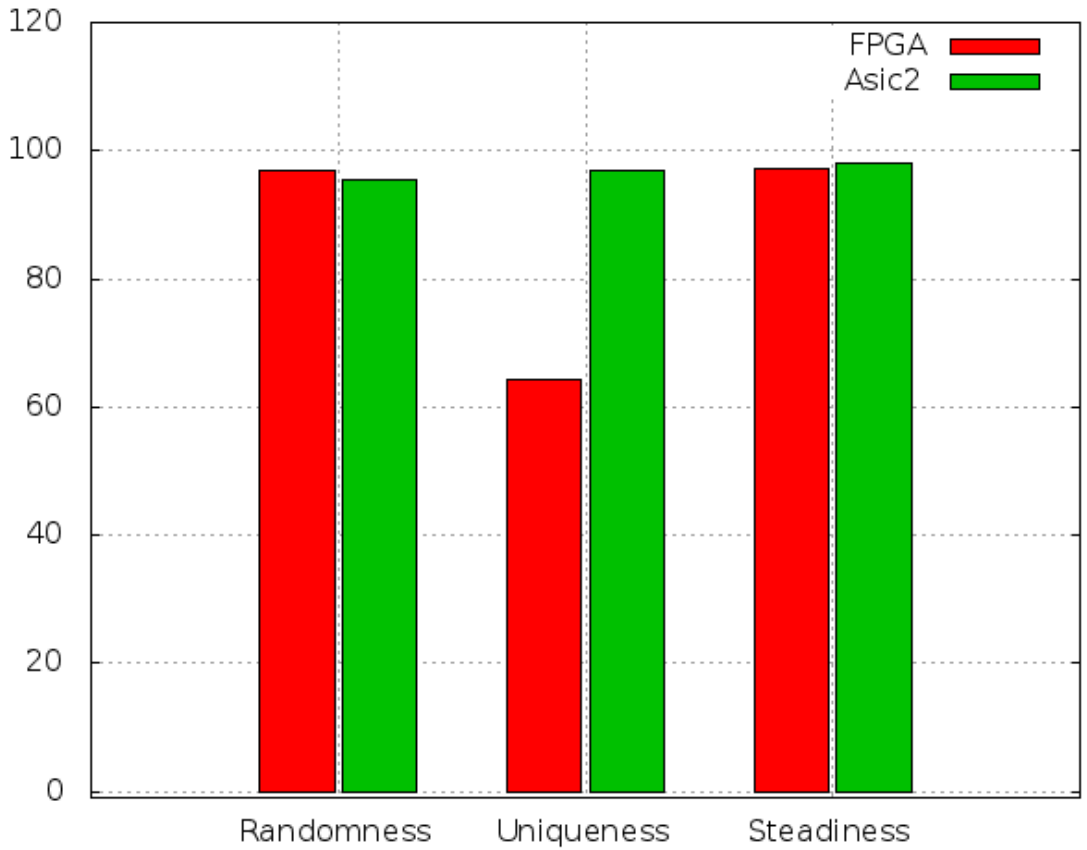


Figure 10: Intra-device evaluation of the loop PUF

Randomness Analysis

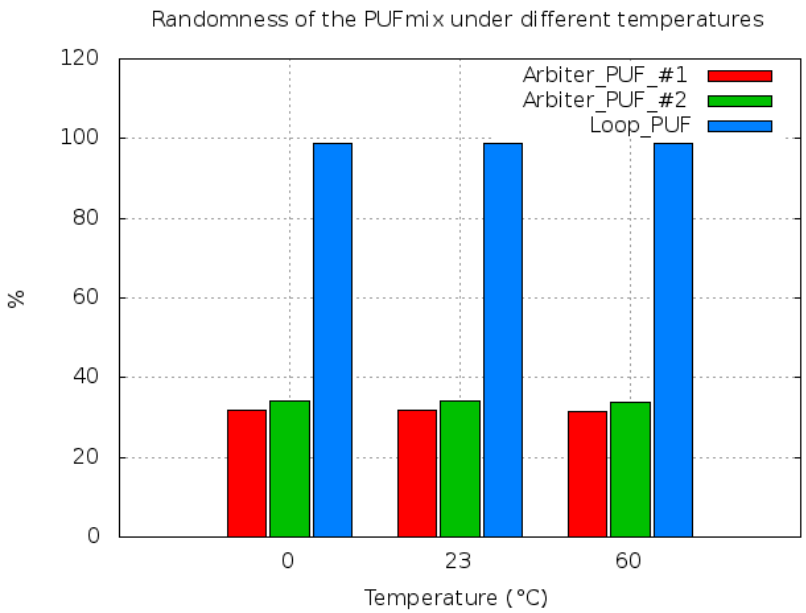


Figure 11: Temperature impact

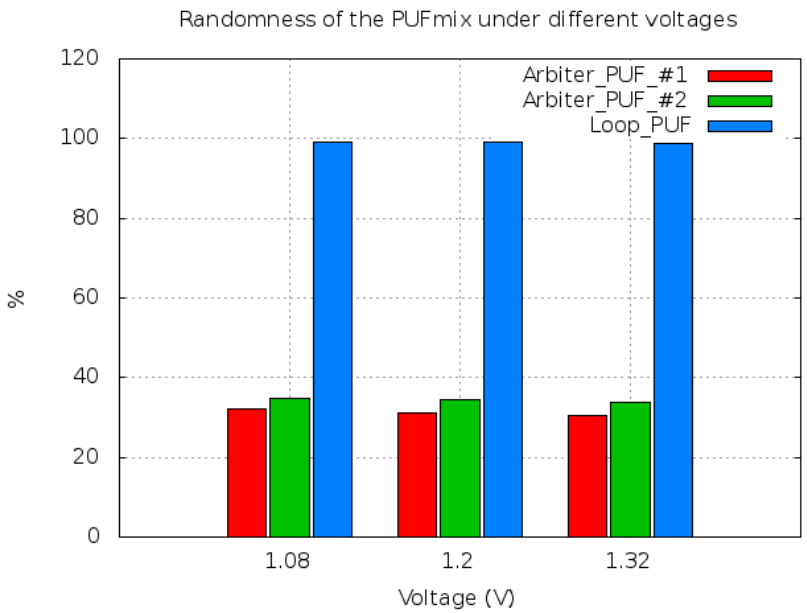


Figure 12: Voltage impact

Steadiness Analysis

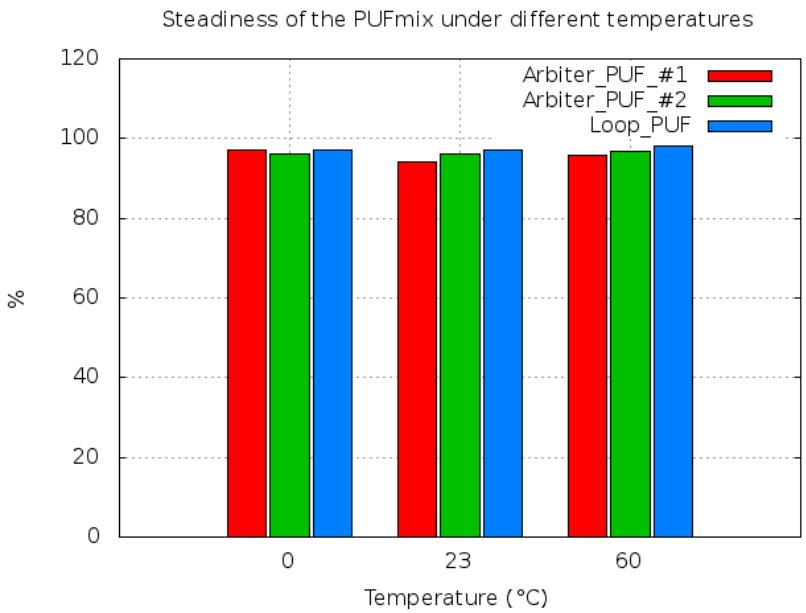


Figure 13: Temperature impact

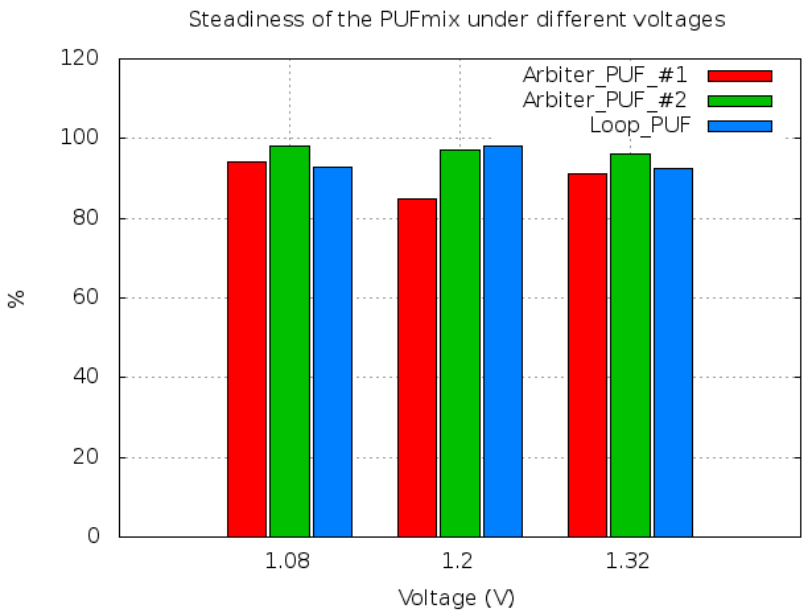


Figure 14: Voltage impact

Inter-Uniqueness Analysis (1)

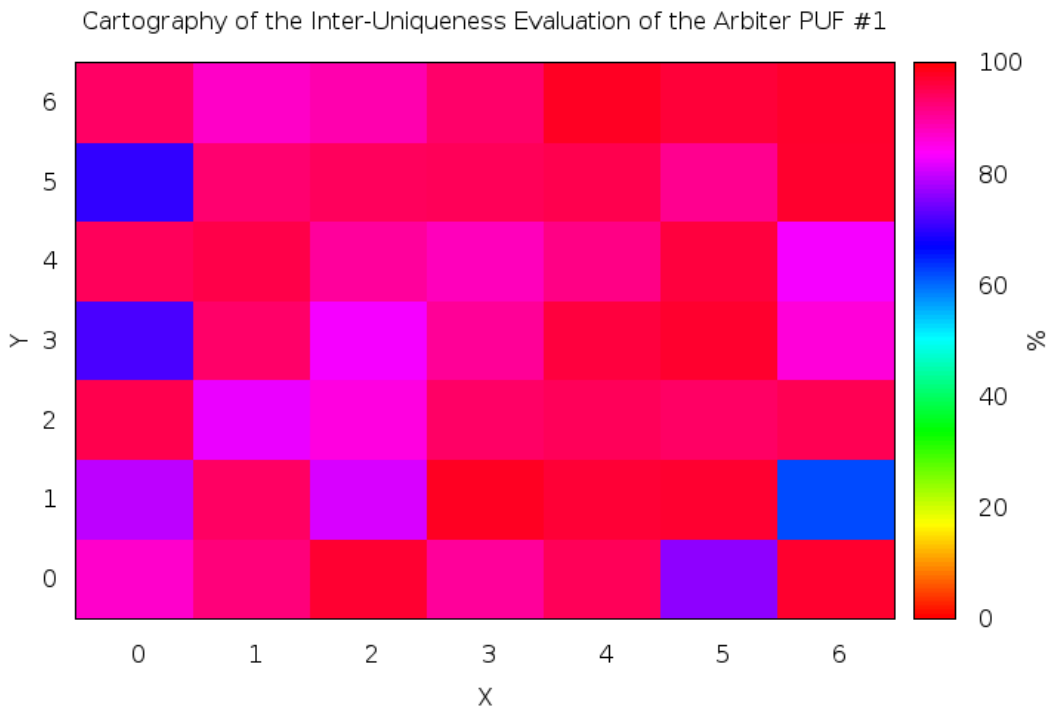


Figure 15: Arbiter PUF ♯1

Inter-Uniqueness Analysis (2)

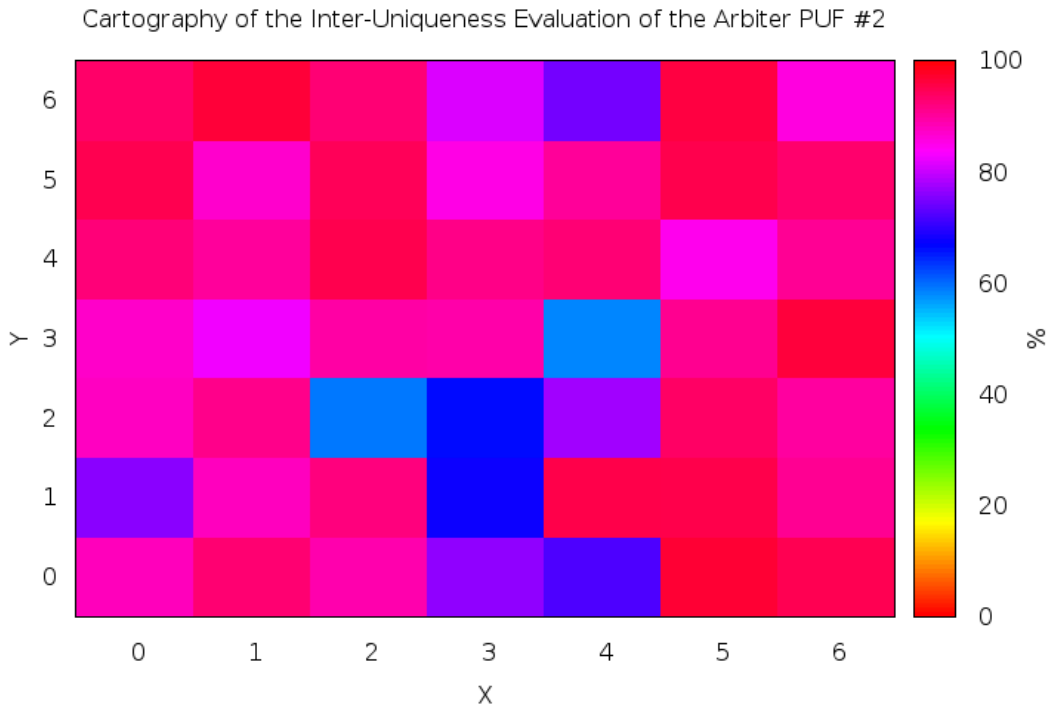


Figure 16: Arbiter PUF ♯2

Inter-Uniqueness Analysis (3)

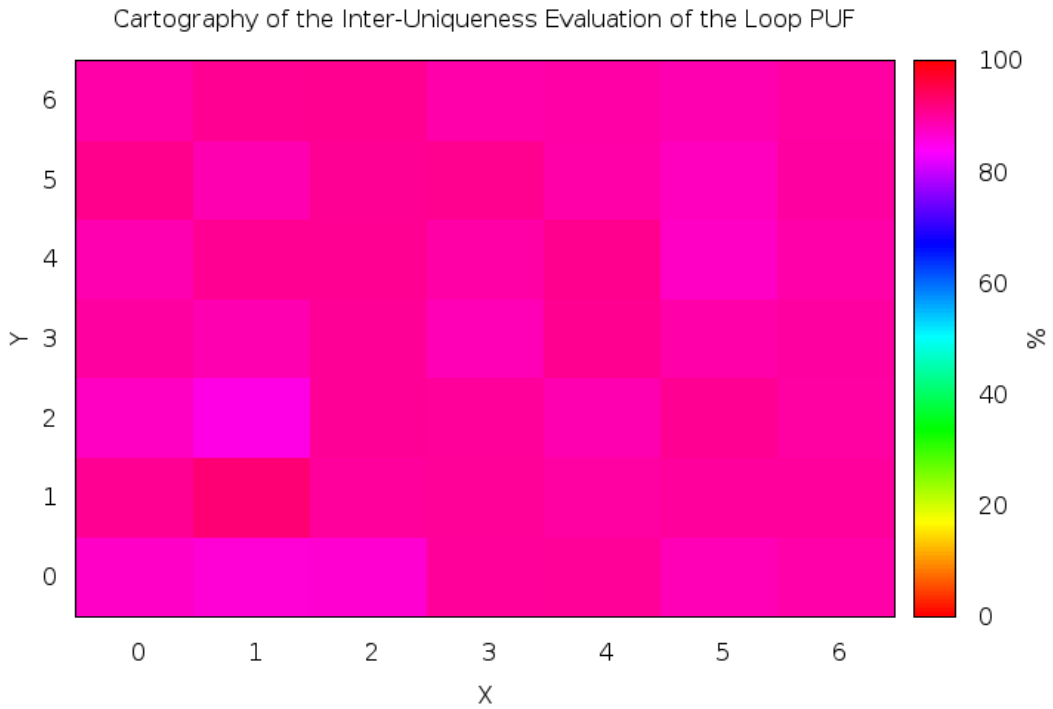


Figure 17: Loop PUF

Outline

Conclusions

ASIC vs FPGA

Inter-platforms evaluation:

- Arbiter PUF: much Better on ASIC than on FPGA.
  $\Longrightarrow$ Randomness: Hard routing constraints are **easier** to define in **ASIC**.
  $\Longrightarrow$ Uniqueness: Extraction process **better** on **ASIC** than on FPGA.
- Loop PUF: slightly better on ASIC than on FPGA.
  $\Longrightarrow$ Uniqueness: Extraction process **better** on **ASIC** than on FPGA.

Loop vs arbiter PUF on ASIC

Deeper analysis on ASIC (18 ASICs).

- The loop PUF is better in terms of randomness, uniqueness and steadiness.
- The randomness of both structures is independent from the supply voltage and the temperature variations.
- The steadiness of both structures slightly influenced by the supply voltage variation.
- The loop PUF has a same inter-uniqueness characteristics in different places on the ASIC.

Perspective

- Improves the arbiter PUF implementation on the FPGA.


Blaise Gassend, Dwaine E. Clarke, Marten van Dijk, and Srinivas Devadas.
Silicon physical random functions.
In *ACM Conference on Computer and Communications Security*, pages 148–160, 2002.


Zouha Cherif Jouini, Jean-Luc Danger, Sylvain Guilley, and Lilian Bossuet.
An easy to design puf based on a single oscillator: the loop puf.

DSD'12, 2012.


M. Majzoobi, F. Koushanfar, and S. Devadas.
Fpga puf using programmable delay lines.
In *Information Forensics and Security (WIFS), 2010 IEEE International Workshop on*, pages 1 –6, 2010.