Physically Unclonable Functions Characterisation

Zhoua Cherif Jouini, Jean-Luc Danger, Lilian Bossuet

Characterization of Physically Unclonable Functions at Design Stage

Zouha Cherif Jouini[1,2], Jean-Luc Danger[1] and Lilian Bossuet[2]
[1]Institut TELECOM, TELECOM ParisTech, CNRS LTCI, 46 rue Barrault 75 634 Paris, France.
[2]Université de Lyon, CNRS UMR 5516, Laboratoire Hubert Curien 42 000 Saint Etienne, France.
Zouha.cherif@telecom-paristech.fr

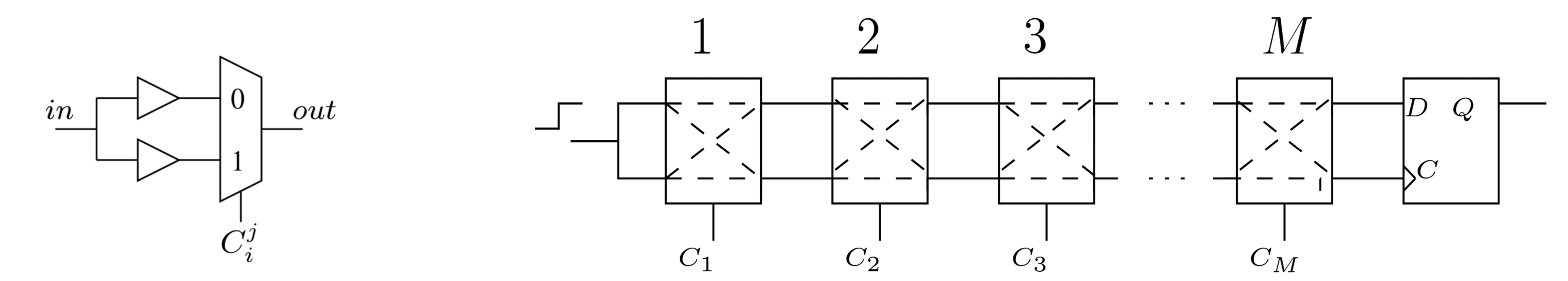
Motivation

The evaluation of Physically Unclonable Function (PUFs) quality is an open problem, as the PUF represents a circuit signature which depends on process variation but also environmental conditions. In the literature, some metrics have been introduced. The considered metrics are often the randomness (max entropy), the uniqueness (two PUFs should be different), and the steadiness (Reliability of the result). The objective of our research topic is to propose a new method which allows to evaluate a silicon PUF, based on delay elements, at design stage without the need to have the circuit.

Background

Arbiter PUF:
- ❖ It is made up of 2*M identical delay elements.
- ❖ Each delay element is controllable.
- ❖ At the end of the delay path, a DFF is used.

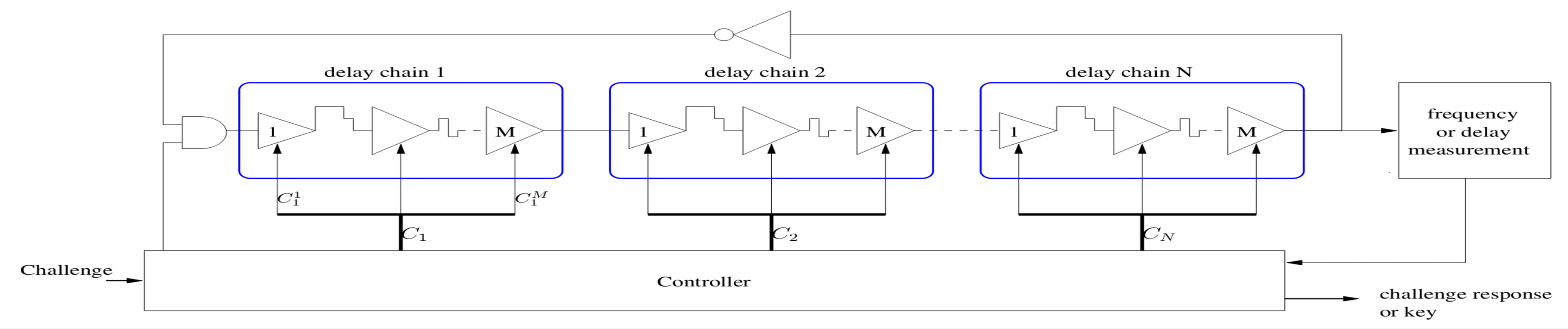
Intrinsic **CMOS variation** ➔ **Delay** of two paths is **different**.
➔ Arbiter is expected to output **unique** IDs to the Device.



A structure of a delay element

A structure of the Arbiter PUF

Loop PUF:
- ❖ It is based on N delay chains forming a loop.
- ❖ Each delay is composed of M controlled delay elements.
- ❖ The ID of the device is in relation with the oscillation frequency.



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 uniqueness** indicates the entropy between two PUFs, either in the same device (intra-uniqueness) or between devices (inter-uniqueness).
- ❖ **The steadiness** expresses the level of PUF reliability which is decayed by the noise coming from the measurement environment.

Our Proposal - Novel metrics

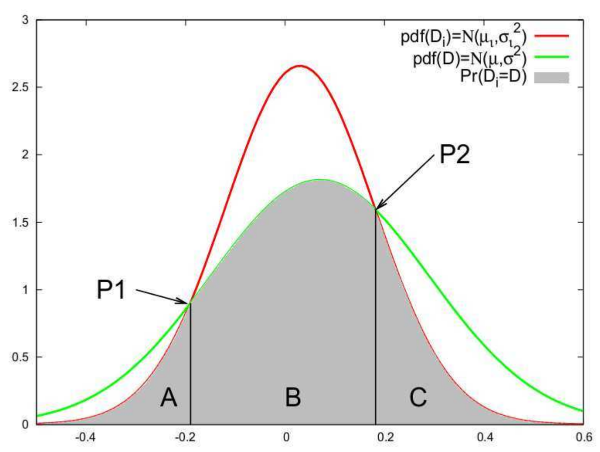
Basics

Classical methods:
- ❖ Perform statistical tests on logical outputs of the PUF.
- ❖ Need a lot of trials in order to run a Monte-Carlo estimation method.

Proposed method:
- ❖ Based on measurement of the physical values (i.e. delays or frequencies).
- ❖ The number of tests is linear with M.
- ❖ The base of the PUF metrics is to calculate a probabilities.

Uniqueness

$$\Rightarrow \quad Uniqueness = \frac{1}{M}\sum_{i=1}^{M} Pr(D_i^L = D).$$



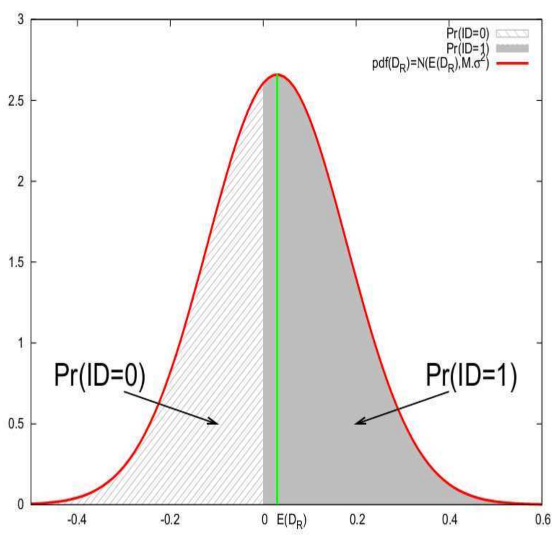
We consider:
- ❖ L PUFs.
- ❖ A delay difference distribution D for M*L delay elements.
- ❖ M normal distributions D_i^L, i in [1,M], of L elements in the same range i.

Randomness

$$Randomness = 1 - |Pr(ID=0) - Pr(ID=1)|.$$

- ❖ With, D_R the pdf of $\sum_{i=1}^{M} d_{c_i}^i$

$$\Rightarrow \quad Randomness = 1 - |erf(\frac{E(D_R)}{\sigma\sqrt{2}\cdot M})|.$$

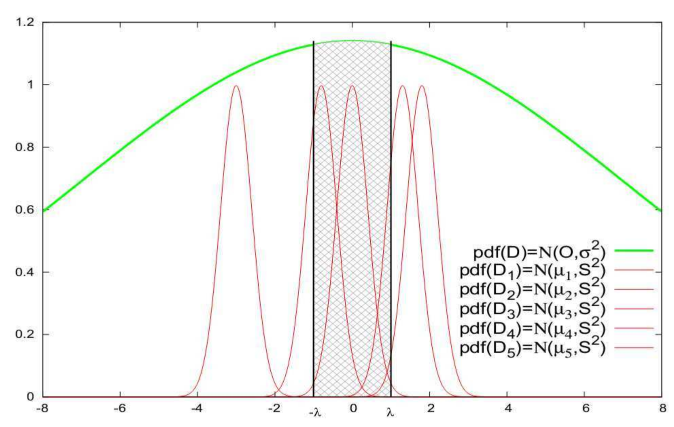


Steadiness

$$Steadiness = 1 - Pr(error).$$

$$Pr(error) = Pr(error \mid delay < |\lambda|) \cdot Pr(delay) < |\lambda|).$$

$$\Rightarrow \quad Steadiness = 1 - \frac{12\sqrt{2\pi} - 9}{8\pi} \times \frac{S}{\sigma}.$$



- ❖ Evry delay difference of element i is measured T times.
- ❖ D_i^T(S2)is the distribution of each element for T tests.
- ❖ Distribution of mean values D (σ2)
- ❖ Error window [-λ,λ].

Experiments and Results

Experiments:
- ❖ Tests have been carried out in a CYCLONE II EP2C35F672.
- ❖ The placement/routing of the all delay chains has been constrained to obtain the exact replication of the same chain. This is possible in ALTERA.

Results:

Intra-device evaluation : Arbiter PUF Vs Loop PUF

Performance indicator	Arbiter PUF	Loop PUF
Randomness	0%	≈ 100%
Intra-Uniqueness	97.73%	95%
Steadiness	99.07%	98.7%

Conclusion & Future Research

Conclusion:
- ❖ Novel metrics for evaluation and characterization delay PUFs has been proposed.
- ❖ These metrics has been validated on an FPGA.

Future Research:
Since this method allows PUF designer to characterize her PUF at design stage and without the need to have the circuit, measurements can be realized with a simulator such as 'Spectre'. Process variation can be done using Mont-Carlo simulation. Environmental variation can also be simulated. Then, results of simulation will be compared with ASIC results.

References

1/ Z. Cherif, J.-L. Danger, and L. Bossuet. Performance evaluation of physically unclonable function by delay statistics. InNEWCAS, Bordeaux, june 2011.

2/ Z. Cherif, J-L. Danger, S. Guilley, and L. Bossuet. An easy to design puf based on a single oscillator: the loop puf. DSD'12, 2012.

3/ 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.

4/ Yohei Hori, Takahiro Yoshida, Toshihiro Katashita, and Akashi Satoh. Quantitative and statistical performance evaluation of arbiter physical unclonable functions on fpgas. Reconfigurable Computing and FPGAs, International Conference on, 0:298–303, 2010.Z. Cherif, J.-L. Danger, and L. Bossuet. Performance evaluation of physically unclonable function by delay statistics. InNEWCAS, Bordeaux, june 2011.

This work has been supported by the European project "TOISE" and the Mines-Telecom french Institute