Physically Unclonable Functions Characterisation
Zhoua Cherif Jouini, Jean-Luc Danger, Lilian Bossuet

To cite this version:
Zhoua Cherif Jouini, Jean-Luc Danger, Lilian Bossuet. Physically Unclonable Functions Characterisation. Colloque du GDR SoC-SiP, Jun 2012, Paris, France. hal-00753222

HAL Id: hal-00753222
https://hal.archives-ouvertes.fr/hal-00753222
Submitted on 18 Nov 2012

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
Characterization of Physically Unclonable Functions at Design Stage

Zouha Cherif Jouini1,2, Jean-Luc Danger1 and Lilian Bossuet2
1Institut TELECOM, TELECOM ParisTech, CNRS LTCI, 46 rue Barrault 75 634 Paris, France.
2Université 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.

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.

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.

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.

Randomness
Randomness = 1 - \left| Pr(D = 0) - Pr(D = 1) \right|.

With, D_R the pdf of \sum_{i=1}^{M} d_i.

Randomness = 1 - \left| \frac{E(D_R)}{\sigma \sqrt{2 \cdot M}} \right|.

Experiments and Results
- 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.

Performance indicator Arbiter PUF Loop PUF
Randomness 0% 100%
Intra-Uniqueness 97.73% 95%
Steadiness 99.07% 98.75%

Conclusion & Future Research
Conclusion:
- New 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 Monte-Carlo simulation. Environmental variation can also be simulated. Then, results of simulation will be compared with ASIC results.

References

This work has been supported by the European project “TOISE” and the Mines-Telecom French Institute.