

Internship Proposal:
"Aging Effect on Delay-based PUF"

Superviser: Jean-Luc Danger
Département Communication et Électronique
Institut TELECOM / TELECOM ParisTech
46, rue Barrault – 75634 Paris Cedex 13
Téléphone : (33) 1 45 81 81 17
Fax : (33) 1 45 80 40 36

State of the Art

A Physically Unclonable Functions (PUF) can be defined as a function which returns the fingerprint of an integrated circuit. It relies on the dispersion of the manufacturing process. The PUF outputs a "response" (or ID) that depends on a control word, called the "challenge". The response differs from one PUF to another.

Challenge-Response Pair (CRP) protocol for authentication and cryptographic key generation are the two main purposes of PUF. PUF avoids the use of non-volatile memory to store a signature, hence they are well suited in low-cost devices as RFIDs or smartcards. PUFs can be generated by the semi-conductor process, it is called "Silicon PUF". There are two main classes of silicon PUFs: the "delay-based" PUFs based on delay comparisons, composed of identical elements, and the "SRAM-PUFs" exploiting the initial state of memory blocks.

The first silicon PUF introduced by Gassend et al. [1] is the arbiter PUF. It is a delay-based PUF where the delays between two identical controlled paths are compared. From the arbiter PUF derives the XOR PUF, as suggested by Suh et al. [10], and the lightweight secure PUF, as proposed by Majzoobi et al. [7]. These PUFs would allow to mitigate the problem of the modeling attack [8]. The ring-oscillator (RO) PUFs proposed by Suh et al. [10] are based on the comparison between the oscillation frequency of selected pairs of ring-oscillators. The loop PUF (LPUF) introduced by Cherif et al. [3] is a delay based PUF which uses a single ring oscillator to generate the PUF response.

Memory based PUF has been introduced first by Guajardo et al. [2] as SRAM PUFs. Its response is directly related with the state of the SRAM at power up. The disadvantage of these SRAM PUFs is that not all FPGAs supports uninitialized SRAM memory. Therefore, Kumar et al. [4] propose the butterfly PUF that can be used on all types of FPGAs. It works as the SRAM PUF with a memory point based on two flip-flops.

Problem

One of the main question about the PUF is its steadiness, as the response is obtained by a measurement, hence noise is added, and not a "read" operation. A correction mechanism has to be added to PUF in order to make it reliable. Another issue is its

stability over the time, especially when we consider the aging effects. Many factors contribute to age the device NBTI, HCI, electromigration, as described in [9]. Indeed the aging can decrease the PUF reliability as shown in [6] which performs experiments on RO-PUFs. The tests have been done by accelerating the aging due to NBTI phenomemon. Another study about SRAM-PUF [5] shows that the aging also affects the SRAM-PUF but the correction mechanism can be relatively efficient. The objective of the paper is to study the aging effect on Loop PUF which as been designed in ASIC technology at Télécom ParisTech.

Organization

During this training period, the student will:

1. Read the literature about the PUF and the aging impact.
2. Study the ways to simulate the aging at design stage.
3. Perform aging experiments on the LPUF prototype.
4. Analyze the results and study ways to mitigate aging if the reliability is impacted.
5. Contribute to a "study period" about PUFs in the framework of ISO/IEC.

Miscellaneous information

- **Theme**: sécurité matérielle
- **Laboratory**: TELECOM-ParisTech, 75013 PARIS
- **Research group**: SEN
- **Internship director**: `jean-luc.danger@TELECOM-ParisTech.fr`
- **Responsible of the laboratory**: `jean-luc.danger@TELECOM-ParisTech.fr`

References

[1] 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.

[2] Jorge Guajardo, Sandeep S. Kumar, Geert Jan Schrijen, and Pim Tuyls. FPGA Intrinsic PUFs and Their Use for IP Protection. In *CHES*, Lecture Notes in Computer Science, pages 63–80. Springer, 2007.

[3] 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.

[4] Sandeep S. Kumar, Jorge Guajardo, Roel Maes, Geert Jan Schrijen, and Pim Tuyls. The Butterfly PUF: Protecting IP on every FPGA. In Mohammad Tehranipoor and Jim Plusquellic, editors, *HOST*, pages 67–70. IEEE Computer Society, 2008.

[5] R. Maes and V. van der Leest. Countering the effects of silicon aging on sram pufs. In *Hardware-Oriented Security and Trust (HOST), 2014 IEEE International Symposium on*, pages 148–153, May 2014.

[6] A. Maiti and P. Schaumont. The impact of aging on a physical unclonable function. *Very Large Scale Integration (VLSI) Systems, IEEE Transactions on*, 22(9):1854–1864, Sept 2014.

[7] Mehrdad Majzoobi, Farinaz Koushanfar, and Miodrag Potkonjak. Lightweight secure pufs. In *Proceedings of the 2008 IEEE/ACM International Conference on Computer-Aided Design*, ICCAD '08, pages 670–673, Piscataway, NJ, USA, 2008. IEEE Press.

[8] Ulrich Rührmair, Frank Sehnke, Jan Sölter, Gideon Dror, Srinivas Devadas, and Jürgen Schmidhuber. Modeling attacks on physical unclonable functions. In *Proceedings of the 17th ACM conference on Computer and communications security*, CCS '10, pages 237–249, New York, NY, USA, 2010. ACM.

[9] S.S. Sapatnekar. What happens when circuits grow old: Aging issues in cmos design. In *VLSI Technology, Systems, and Applications (VLSI-TSA), 2013 International Symposium on*, pages 1–2, April 2013.

[10] G. Edward Suh and Srinivas Devadas. Physical unclonable functions for device authentication and secret key generation. In *DAC*, pages 9–14, 2007.