Physical Security of Ring-based PUF

L Bossuet

▶ **To cite this version:**

L Bossuet. Physical Security of Ring-based PUF. European Conference on Circuit Theory and Design (ECCTD), Sep 2020, Sofia, Bulgaria. hal-02937858

HAL Id: hal-02937858
https://hal.science/hal-02937858

Submitted on 14 Sep 2020

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.

Physical Security of Ring-based PUF

L. Bossuet
Univ. Lyon, UJM-Saint-Etienne, CNRS, Laboratoire Hubert Curien UMR 5516
F-42023 Saint-Etienne, France
lilian.bossuet@univ-st-etienne.fr

Abstract—**The design of a secure, efficient, lightweight silicon physical unclonable function (PUF) is a serious challenge for the hardware security community. In this context, this paper presents a survey of physical attacks targeting ring-based PUFs because such PUFs are known as some of the more efficient. The paper discuss the threats and try to propose solution to design efficient and secure ring-based silicon PUFs.**

Keywords—PUF; side channel analysis; fault injection;

I. INTRODUCTION

The security of a hardware system depends on the security of all its parts: the processing unit including the cryptographic implementations, the memory unit including the cryptographic keys and sensitive data storage, the data communication, and the scheduling and control unit. For authentication, identification, tractability and licensing of hardware systems, the silicon physical unclonable functions (PUFs) are study for 18 years. Like for others piece of the hardware system security, the security of the silicon PUFs is of paramount importance. Indeed, if attackers can change the behavior of the embedded PUF (for instance, if they can change the PUF response) they can cause denial-of-service, or if attackers can analyze the behavior of the embedded PUF (for instance, if they be able to analyze the PUF side channel) they can clone the PUF and at the end they can dramatically reduce the entire security of the hardware system. Over the past 10 years, some studies suggested active physical attacks and passive physical attacks targeting PUFs with success. These attacks exploit the usual (for the hardware security community) side channels such as power consumption, electromagnetic emanation and photonic emission. All silicon PUF architectures are sensitive to passive and active physical attacks both. This paper focuses only on the two main ring-based PUF architectures: the RO-PUF [1] and the TERO-PUF [2]. Indeed, the ring-based PUFs are known to be efficient and not too hard to design.

The rest of this paper is organized as follows. In Section 2, we present the background on ring-based PUFs. In Section 3, we synthetize the works that propose to attack the ring-based PUFs physically. In Section 4, we discuss design solutions to protect the ring-based PUFs against physical attacks and in Section 5 we present our conclusions.

II. RING-BASED SILICON PUF

The silicon PUFs are used for intrinsic identification of digital integrated circuit. They act as a physical (microelectronic) fingerprinting of integrated circuit. They exploit random static phenomenon: the CMOS process variations at transistor level. Figure 1 presents the silicon PUF principle. All the silicon PUFs use the same principle: a set of identically designed structures generates analog signals and the PUF challenge signal select some of these analog signals to be digitally compare. Because of the manufacture process variations, the identically designed structures have some mismatches, which conduce the digitizer to measure difference in the analog signal and generate the PUF response.

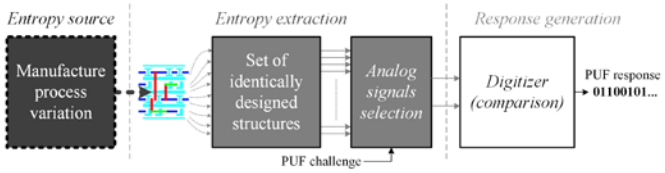

Fig. 1. Silicon PUF principle.

In the case of ring-based silicon PUFs, the identically designed structures are oscillating cells. Two main type of oscillating cells are used for PUF: permanent oscillating cells such as ring-oscillator (RO) and non-permanent oscillating cells such as transient effect ring-oscillator (TERO). In both case of oscillating cells the PUF architecture is the same. Fig. 2 presents the general architecture of a ring-based PUF. Such a PUF uses two sets (*A* and *B*) of identically oscillating cells. The control signal is use to start and to stop the oscillation of the cells. The challenge signal selects one oscillating cell from the set *A*, and one oscillating cell from the set B. Then the PUF digitizer uses two n-bit counters and a response bit extractor. This final part of the PUF depends of the oscillating cells type (i.e. RO or TERO).

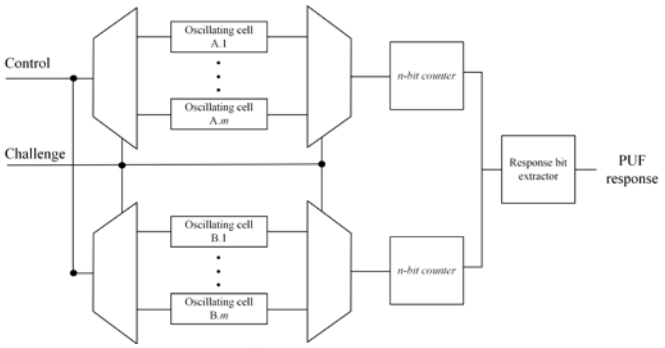

Fig. 2. General architecture of a silicon ring-based PUF using two large set of oscillating cells (RO or TERO).

When RO are used as the PUF oscillating cells (Fig. 3-a) the response bit extractor compare the output of the two n-bit

counters in order to evaluate if the selected RO from the set *A* has a higher oscillating frequency (or not) than the selected RO from the set *B*. Because the ROs oscillating frequency depends of the process variations, the PUF digitizer output can be directly used to generate the PUF response [1]. When TERO are used as the PUF oscillating cells (Fig. 3-b) the response bit extractor subtract the output of the two n-bit counters and then generate many usable bits by period of the control signal. This behavior is possible because the TEROs stop to oscillate after a duration function of the process variation. So at each period of the control signal, the final value of the two n-bit counters are related to the number of oscillation of the two selected TEROs before to stop [2].

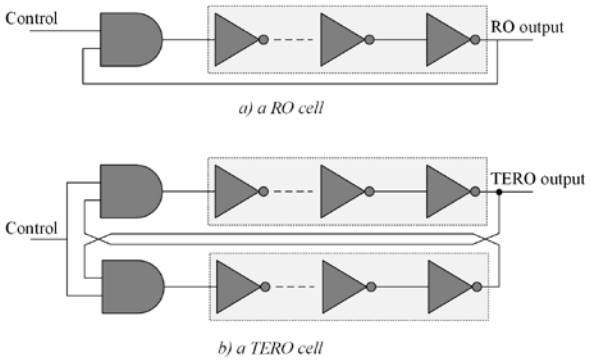

Fig. 3. The RO (a) and TERO (b) oscillating cells usually used in ring-based silicon PUFs.

III. PHYSICAL ATTACKS TARGETING RING-BASED SILICON PUF

A. Physical attacks

Well-known threats in cryptographic engineering are passive and active physical attacks. Passive physical attacks are known as side channel analysis and active physical attacks are known as fault injection attacks.

Side-channel analyses are widely used in cryptographic engineering as passive attacks because they make it possible to retrieve secret information (such as cipher secret keys) with relatively few physical measurements and sometimes using inexpensive equipment. Most of the dynamic characteristics of hardware implementations of security primitives can be used for side channel analysis: power consumption, electromagnetic radiation, optical radiation, etc.

Fault injection attacks are also widely used but as active attacks in cryptographic engineering because they make it possible to retrieve secret information (such as cipher secret keys) by run time perturbation of the system. Moreover, fault injection is increasingly frequently used to bypass security functions (security boot for example) in complex systems or to cause denial of service. Fault injection attacks always need to be able to control the impact of the fault precisely. For a long time, only the optical channel allowed both analysis of locally leaked information and precise injection of faults (single-bit errors). Subsequently, the near-field electromagnetic channel was used. Like the optical channel, the near-field electromagnetic channel allows fault injection attacks, which, in addition, can theoretically be non-invasive and contactless.

During the past ten years, many works propose to perform physical attacks on silicon PUF. Most of them target the entropy extraction of the PUF (see the middle of Fig. 1). Indeed, contrary to the case of the true random number generators (TRNGs), with the PUFs it is not possible to manipulate the entropy source because the realization of the random function occurs only during the manufacture of the device and not on run time. PUF digitizer can be also targeted by the physical attacks, mainly by fault injection, to force the PUF response. In most of the case, active attacks was used only for denial-of-service to output not any or a wrong PUF response. Finally, side channel analysis are more usual because attackers aim to clone the PUF first (they would like to be able to know the secret PUF response for a specific challenge). The remainder of this section provides more detail on the works on physical attacks that targeted ring-based silicon PUF.

B. Fault injection attacks on ring-based PUF

Digital oscillating cells, RO and TERO, are known to be very sensitive on voltage and temperature variations. This sensitivity is an usual issue for the PUF designer [3] and an advantage to design digital voltage or temperature sensor. This sensitivity can be use by an attacker to cause denial-of-service of ring-based PUF. To do it, the attacker can efficiently use a laser injection to modify the voltage and temperature parameters by induce energy as proposed by He and al. in 2016 [4]. They proposed to use a RO in order to detect laser injection because of the RO sensitivity. They show that the laser modifies the phase, the frequency and the amplitude of the RO output signal. They show also that after the injection, the RO settles to its natural oscillating frequency. Such laser injection is not already test on TERO cells, but due to their temporary oscillating state, they must be also sensitive to laser injection. Such active physical attack can cause denial-of-service but using laser is expensive and cheaper equipment can be use efficiently. Indeed, as proven in [3] by Marchand et al. and in [5] by Cao et al., simple power or temperature (cooling, heating) variations can cause dramatic response variation on ring-based PUF especially when the variations go beyond the device specifications for RO-PUF and TERO-PUF both.

Recently Mureddu et al. proven that the digital oscillating cells, including RO and TERO, are sensitive to the locking phenomenon [6]. The attacker can also use this sensitivity to cause denial-of-service of ring-based PUF. To do it, the attacker has to add a harmonic perturbing signal on the PUF power supply. Two different way can be follow to perform such attack. The first way was proposed in 2009 by Markettos and Moore who inject a sine wave signal directly onto the power pad of the device in order to intentionally modify the operating conditions of the two ROs used in a RO-TRNG and thus to get a biased TRNG output signal [7]. In 2012, Bayon et al. improved this first harmonic injection attack by using contactless electromagnetic signal injection [8]. They experimentally shown when the signal frequency is close to an harmonic of the RO oscillating frequency that the attack is possible.

These works on fault injection show us that the digital oscillating cells sensitivity can be malicious used to perform denial-of-service of ring-based PUF. Nevertheless, even if the denial-of-service of PUF could cause a security failure for some application, the main security issue of PUF is the possibility to clone the secret response of the PUF [9]. As we will show in the following, it is possible to do it by using side channel analysis.

C. Side channel analysis on PUF

In physical cryptanalysis, electromagnetic radiation is an efficient side channel since, unlike measurement of power consumption, electromagnetic radiation can be measured locally. One of the main advantages of this side channel is that it is impossible to hide the leak concerning electromagnetic radiation by using a global countermeasure. Moreover, the electromagnetic test bench is not expensive (less than US$ 10K without an oscilloscope, which is the most expensive component). For all its reasons, since 2011, researchers had tried to use electromagnetic radiation to clone ring-based PUF.

In a first time, Merli et al. proven that a spectral analysis of the electromagnetic radiation provides frequency information on the ring-oscillators used in a RO-PUF [10]. In a second time, in 2013, Bayon and al. proposed a differential spectral analysis to obtain frequency and spatial information to characterize and localize the RO-PUF embedded in a device [11]. Fig. 4 illustrates the differential spectral analysis proposed in [11] when two spectral characterizations of the electromagnetic radiation of the device are performed with two different environmental conditions (voltage modification was used in [11] because of the better control on power supply than on ambient temperature). Fig. 5 shown an example of RO-PUF localization provided by the differential spectral EM-cartography proposed in [11]. The same year, Merli et al. proposed another method using also electromagnetic radiation spectral analysis to characterize and localize the RO-PUF embedded in a device [12] by detecting amplitude standard deviation of spectral typical of jitted oscillator. This second method is efficient but less precise than the method proposed in [11].

All these previous first works targeting only RO-PUF, it was not until 2019 that two studies were published at the same time and proved the possibility of cloning a TERO-PUF by the analysis of electromagnetic radiation. Tebelmann et al. proposed to used the signal-to-noise ratio (SNR) to estimate the duration of the TERO oscillation and then estimate the number of oscillation before than the TERO oscillations stop [13]. It is an efficient method but Mureddu et al. proven that the same results can be directly obtain by using a real-time spectral analyzer and moreover they proposed a full methodology to clone the TERO [14]. Fig. 6 illustrate the real time spectral analysis of two TERO of a large TERO-PUF. On this figure, we can see than the two TERO frequency oscillation are 174.4 MHz and 174.6 MHz and that the oscillation occurred during 1.28µs and 5.11µs respectively. Then by performing such a real-time analysis, the attacker can obtain directly the number of oscillation of the two TERO before stopping which are 223 and 892 respectively for the Fig.6 example.

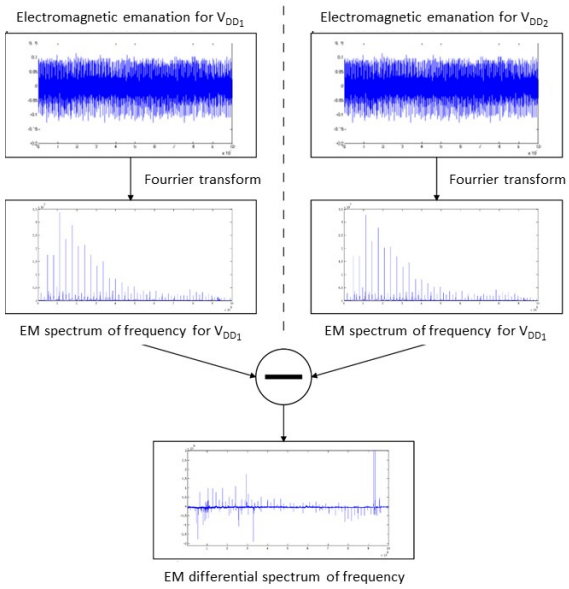

Fig. 4. Illustration of the differential spectral analysis of the electromagnetic radiation of a RO-PUF embedded in an integrated device proposed in [11]. Each of the two spectral analysis were performed with two different voltage condition in order to detect a spectral deviation due to RO sensitivity to voltage modification.

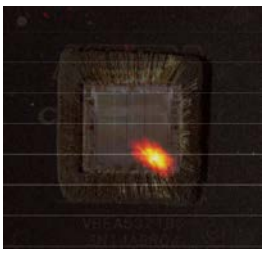

Fig. 5. Illustration of localization of the RO-PUF (hot spot) by using the differential spectral electromagnetic-cartography proposed in [11]. This localization can be used as a preliminary step to perform active attacks presented in Section III-A.

As a conclusion, in the case of ring-based PUF the electromagnetic channel is an efficient side channel for passive attacks. Other side channel could by used but at now not any work proposed to use it with efficiently. Optical channel was also used with success for SRAM-PUF [15] and arbiter-PUF [16] but this channel was not yet study for ring-based PUF, it could be interesting in the future, if experimental optical bench will become more accessible.

IV. Ring-based PUF Protection against Physical Attacks

In the previous sections, the sensibility of TERO and RO cells to active and passive physical attacks have been demonstrated, reflecting the weakness of the ring-based PUF. Here is introduced a list of recommendations to reduce as much as possible attack scenarios based on active and passive attacks of the ring-based PUF.

To protect PUF-based scheme against fault injection, the best solution is to use response correction system. Several types of error-correcting codes can be used to this end, but they all induce significant area overhead on the device. This is

contrasted with the lightweight nature of PUFs, and prevents widespread adoption by industry. Nevertheless, lightweight error correction can be developed as proposed in [17]. Other possibility is to consider the security strategy follow by TRNG designers and be able to prove that the entropy source and extractor are not manipulable as request by the high-security level certification [18]. But this last proposition need new propositions and future works to be dedicated to the PUF.

A first (but radical) solution to prevent side-channel analysis would be to make the device physically inaccessible and close it with an aluminum lid shield to isolate the electromagnetic emission. However, depending on the design constraints this is not always possible. Especially in an IoT context where resources and space are limited. One might think having cells oscillating at close frequencies could also be a solution because it would not allow distinguishing one from another. This is actually an unwanted solution since a too close number of oscillations would render the PUF response unstable. Moreover, for protection against side channel analysis it is more efficient to generate correlated noise on the side channel to be not remove by differential analysis as proposed in [19] for cypher implementation. To do it, a possible way could be to use the intrinsic locking of oscillating cells study in [14]. Finally, an efficient solution would be to not allow the user to access directly to the challenges. By this way, whatever the level of physical accessibility, an attacker could not retrieve the characteristic of the oscillating cells with side channel analysis.

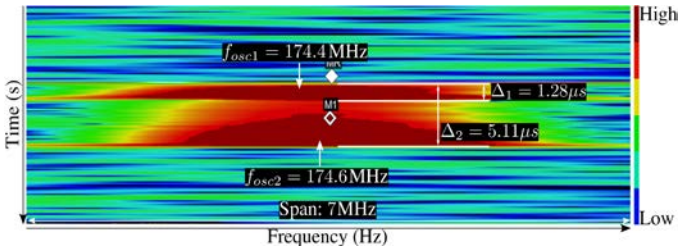

Fig. 6. Real-time spectral analysis of electromagnetic radiation of two TERO of a large TERO-PUF embedded in an integrated circuit (Xilinx Spartan-6 FPGA) proposed in [14].

V. Conclusion

This paper shown the security weaknesses of ring-based PUFs against physical attacks. The PUF designers have to take into account of these weaknesses to proposed efficient and secure scheme based on PUFs. The academic community should spend more effort to find realistic countermeasures for the PUF adoption in the industry.

Acknowledgment

The work presented in this paper was realized in the framework of the FUIAAP22-Project PILAS supported by BpiFrance.

References

[1] G. E. Suh, S. Devadas, “Physical unclonable functions for device authentication and secret key generation,” ACM/IEEE Design Automation Conference, San-Diego, CA, USA, 2007.

[2] A. Cherkaoui, L. Bossuet, C. Marchand, “Design, Evaluation and Optimization of Physical Unclonable Functions based on Transient Effect Ring Oscillators,” IEEE Transactions on Information Forensics and Security, Vol. 11, No. 6, pp. 1291-1305, June 2016.

[3] C. Marchand, L. Bossuet, U. Mureddu, N. Bochard, A. Cherkaoui, V. Fischer, “Implementation and characterization of a physical unclonable function for IoT: a case study with the TERO-PUF,” IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, Vol. 37, No. 1, pp. 97-109, January 2018.

[4] W. He, J. Breier, S. Bhasin, N. Miura and M. Nagata, “Ring Oscillator under Laser: Potential of PLL-based Countermeasure against Laser Fault Injection,” Workshop on Fault Diagnosis and Tolerance in Cryptography, Santa Barbara, CA, USA, 2016, pp. 102-113.

[5] Y. Cao, V. Rožić, B. Yang, J. Balasch and I. Verbauwhede, “Exploring active manipulation attacks on the TERO random number generator,” IEEE International Midwest Symposium on Circuits and Systems, Abu Dhabi, 2016, pp. 1-4.

[6] U. Mureddu, N. Bochard, L. Bossuet, V. Fischer, eExperimental Study of Locking Phenomena on Oscillating Rings Implemented in Logic Devicesee, IEEE Transactions on Circuits and Systems I: Regular Papers, Vol. 66, No. 7, pp. 2560-2571, July 2019.

[7] A. T. Markettos and S. W. Moore, “The Frequency Injection Attack on Ring-Oscillator-Based True Random Number Generators,” Cryptographic Hardware and Embedded Systems, pp. 317-331, 2009.

[8] P. Bayon, F. Poucheret, L. Bossuet, B. Robisson, A. Aubert, P. Maurine, V. Fischer, “Contactless Electromagnetic Active Attack on Ring Oscillator Based true Random Number Generator,” International Workshop on Constructive Side-Channel Analysis and Secure Design, Darmstadt, Germany, May 2012, pp. 151-166.

[9] D. Merli, D. Schuster, F. Stumpf, and G. Sigl, “Side-channel analysis of PUFs and fuzzy extractors,” Trust and Trustworthy Computing, Lecture Notes in Computer Science, 2011, vol. 6740, pp. 33–47.

[10] D. Merli, D. Schuster, and G. Sigl, “Semi-invasive EM attack on FPGA RO PUFs and Ountermeasures,” Workshop on Embedded Systems Security, October 2011.

[11] P. Bayon, L. Bossuet, A. Aubert, V. Fischer, “EM leakage analysis on True Random Number Generator: Frequency and localization retrieval method”, Asia Pacific International Symposium and Exhibition on Electromagnetic Compatibility, Melbourne, Australia, 2013.

[12] D. Merli, J. Heyszl, B. Heinz, D. Schuster, F. Stumpf, and G. Sigl, “Localized electromagnetic analysis of RO PUFs,” International Symposium on Hardware-Oriented Security and Trust, June 2013

[13] L. Tebelmann, M. Pehl, and V. Immler, “Side-channel analysis of the TERO PUF,” Workshop on Constructive Side-Channel Analysis and Secure Design, April 2019, pp. 43–60.

[14] U. Mureddu, B. Colombier, N. Bochard, L. Bossuet, V. Fischer, “Transient Effect Ring Oscillators Leak Too,” IEEE Computer Society Annual Symposium on VLSI, Miami, FL, US, July 2019.

[15] C. Helfmeier, C. Boit, D. Nedospasov and J. Seifert, "Cloning Physically Unclonable Functions," International Symposium on Hardware-Oriented Security and Trust, Austin, TX, USA, 2013, pp. 1-6.

[16] S. Tajik, E. Dietz, S. rohmann, H. Dittrich, D. Nedospasov, C. Helfmeier, J.P. Seifert, C. Boit, and h.W. Hübers, “Photonic Side-Channel Analysis of Arbiter PUFs,” Journal of Cryptology, Vol. 30, pp. 550–571, 2017.

[17] B. Colombier, L. Bossuet, V. Fischer, D. Hely, “Key Reconciliation Protocols for Error Correction of Silicon PUF Responses,” IEEE Transactions on Information Forensics and Security, Vol. 12, No. 8, pp. 1988-2002, August 2017.

[18] O. Petura, U. Mureddu, N. Bochard, V. Fischer, L. Bossuet, “A Survey of AIS-20/31 compliant TRNG Cores Suitable for FPGA Devices,” International Conference on Field-Programmable Logic and Applications, FPL 2016, Lausanne, Switzerland, August 2016.

[19] N. Kamoun, L. Bossuet, and A. Ghazel, “Correlated Power Noise Generator as a Low Cost DPA Countermeasure to Secure Hardware AES Cipher,” International Conference on Signals, Circuits and Systems, 2009.