An analysis of Ring Oscillator PUF Behavior on FPGAs

Susana Eiroa and Iluminada Baturone
Dept. of Electronics and Electromagnetism, Univ. of Seville
Microelectronics Institute of Seville (IMSE-CNM-CSIC)
Seville, Spain
{eiroa,lumi}@imse-cnm.csic.es

***Abstract*— Many studies have been directed to probe ring oscillator PUF's feasibility in the security field, but most of them suffer from the lack of global approach as they analyze the system isolated, giving an uncompleted theory about their behavior. This paper presents how adjacent hardware elements may affect PUF response, modifying their statistical characteristics and even masking the randomness of manufacturing process. This is a factor that should be taken into account when modeling the behavior of the ring oscillators in the PUF. Experimental results from Xilinx Spartan 3 FPGAs illustrate these issues.**

Keywords: PUF; Ring Oscillator; hardware security

I. INTRODUCTION

As a result of the big evolution in communication society, the use of hardware devices to carry out related-security tasks is growing significantly. In parallel, new attacks have been appearing to break the security not only of the communication channel but also of the devices themselves. Concerning the latter, active as well as passive attacks have been developed. In order to counteract these new attacks, a huge encourage in hardware protection is being needed. In this line, new structures have been proposed such as Physical Unclonable Functions (PUFs). A PUF is a physical random function that maps a set of challenges to a set of responses driven by parametric properties of physical components that are difficult to predict, control, or reproduce. Therefore, the mapping function can only be evaluated with the physical system, and it is unique for each physical instance.

In the field of hardware devices, the most interesting ones are silicon PUFs, which were firstly proposed in [1]. They exploit small variations in the hardware manufacturing process such as different leakage current consumption and different delays. Work in [2] analyzes how the peculiarities of FPGA routing affect the implementations of delay-based PUFs making arbiter and butterfly PUFs not suitable for FPGA implementations. PUFs without the mirror symmetry requirement, such as ring oscillator PUFs, present better qualities in this context.

However, ring oscillator PUFs suffer from the lack of reliability (or reproducibility) due to their high sensibility to temperature, supply voltage fluctuations and influence of surrounding noise sources. Consequently, many studies have been focused on improving this feature. Basically the proposed approaches can be divided into those that recommend to apply relatively complex post-processing (such as using error-correction codes [3]), and those that suggest to use a pre-processing stage where only the "reliable oscillators" are selected to from the PUF structure [4]-[6].

Besides reliability, PUFs used for security purposes must show a high level of uniqueness. In this line, the idea is to avoid spatial gradients. A controlled placement scheme where adjacent oscillators are compared is proposed in [7]. A scheme with four oscillators combined as in the common-centroid layout design of analog circuits is proposed in [8].

Most of these studies (focused on reliability as well as uniqueness) show results where the ring oscillator PUFs are the main circuit implemented in the die. However, the PUF finality is to be included into a security system. This paper presents that the system where the PUF is included can bias significantly the PUF response so that such systematic changes reduce the PUF uniqueness and can make inefficient some of the schemes proposed to improve PUF reliability.

The paper is structured as follows. Section II gives an overview of ring oscillator PUF characteristics and desired features. Section III presents a new approach to model the behavior of the ring oscillators in a PUF to consider the system where they are included. This model includes new systematic changes that may bias the PUF responses and can degrade PUF uniqueness, especially if some schemes to improve PUF reliability are employed. This is supported by experimental results obtained with the Xilinx Spartan 3 XC3S200 FPGA devices from Digilent Starter Boards. Section IV illustrates with more experimental results how these systematic changes can degrade PUF uniqueness, especially if some schemes to improve PUF reliability are employed. Finally, conclusions are given in Section V.

II. BASIS OF RING OSCILLATOR PUFS

The basic idea behind ring oscillator PUFs is that given equally laid and structured elements (equal number of gates and equal distribution), their output frequency comes defined by manufacturing variation. The basic structure, firstly proposed in [4], compares this value by counting the cycles in a certain time period. If the counter associated to the upper oscillator shows higher frequency, the corresponding output PUF code is '1' and, otherwise, the output is '0' (Fig.1).

However, manufacturing variations are not purely random [7]. Results for 90nm FPGAs shown in [9] illustrate graphically the frequencies of a matrix of ring oscillators with identical layout. The obtained surface shows a spatially

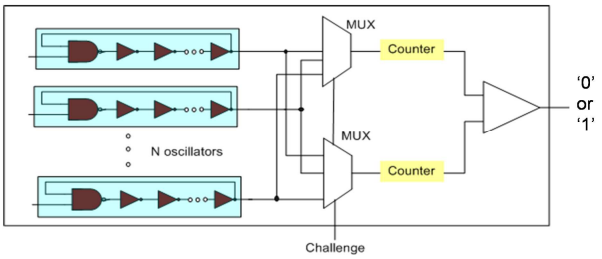


Fig. 1. Basic ring oscillator PUF proposed in [4].

dependent gradient (systematic dependence) together with a roughness all along the gradient plane (stochastic part) that is completely uncorrelated with position. In order to decrease the systematic factor, the authors in [7] proposed to place the oscillators as close as possible and to compare adjacent elements. The model they use to analyze the total delay in a ring oscillator is the following [7] [10]:

$$d_{RO} = d_{AVG} + d_{PV} + d_{NOISE} \qquad (1)$$

The delay d_{AVG} is the nominal value of the delay based on architectural and technological parameters. It is the same for all identical oscillators. The delay d_{PV} is due to process variation. It may vary from one oscillator to another and it is static, that is, it is assumed to be constant over time (neglecting possible ageing effects). The delay d_{NOISE} represents a noisy and dynamic component that changes over time. This generates that the oscillator frequency presents a Gaussian distribution instead of a delta value, which could produce bit flipping (a bit that changes between '0' and '1') because of the overlap of the frequency distributions. In order to filter noise, high counting values should be chosen.

Taking into account the previous considerations, if the frequencies of two oscillators are compared, the resulting bit would depend on static and random process variation, and if several pairs are compared, the PUF response should ensure reliability and uniqueness:

- *Reliability* measures how consistently a response is reproduced by the PUF for the same challenge over several read outs. It is calculated as the average intra-class Hamming distance, HD(R, R'), over *x* samples, as follows:

$$R = \frac{1}{x}\sum_{y=1}^{x}\frac{HD(R_i, R'_{i,y})}{n}\times 100 \qquad (2)$$

- *Uniqueness* measures how distinctly the PUF can identify the device where it is included. It is calculated as the average inter-class Hamming distance, as follows:

$$U = \frac{2}{m(m-1)}\sum_{i=1}^{m-1}\sum_{j=i+1}^{m}\frac{HD(R_i, R_j)}{n}\times 100 \qquad (3)$$

Where *m* is the number of devices and *n* is the number of bits in the PUF responses (R_i).

Uniqueness is reduced if the responses of the PUFs have bits with always the same value ('0' or '1') in all the chips. This problem is also known as bit aliasing.

The ideal PUF behavior should provide *R* of 0%, *U* of 50% and 0% of repeated bits (no bit takes the same value in all the devices)

III. Redefining the Model of Ring Oscillators in PUFs

According to the model proposed in (1), the frequency of a ring oscillator can be expressed as $f_{RO} = f(d_{AVG}, d_{PV}, d_{NOISE})$. The validity of this model has been analyzed by performing several experiments with ring oscillator PUFs implemented in Spartan 3 FPGAs (with XC3S200 devices). The oscillators implemented have 4 inverters and 1 NAND gate meeting all the considerations discussed in the previous section.

A. Contribution of process variations and system over PUF

A PUF with 16 ring oscillators has been implemented in three different FPGAs (F1, F2, and F3). The 16 oscillators are constrained (manually) to form an 8x2 matrix in the centre of the die. The frequencies of the different oscillators are measured by comparing the result of their associated counters with the count of a reference element working at the board frequency of 50 MHz.

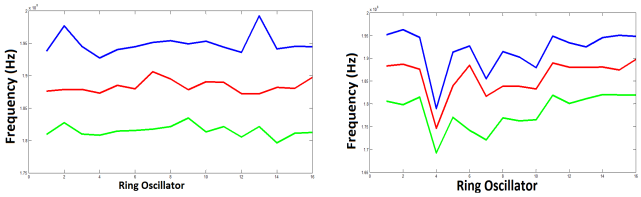
The behavior of the PUF has been analyzed when included into four different and simple systems:

- Case1: only the PUF with 16 oscillators is included in the FPGA. The rest of the circuitry necessary for processing the oscillator comparisons is placed and routed freely by the ISE CAD tools.
- Case2: A PUF with 16+16 oscillators is implemented (16 oscillators, which are disabled, are added to Case1).
- Case3: The place occupied by the 16 added oscillators of Case2 is marked as "prohibit" by the ISE CAD tools, so that it appears empty in the final floorplan of the system (like Case1 but the rest of the circuitry is not placed freely).
- Case4: A PUF with 64 (16+16+16+16) oscillators is implemented (48 oscillators, which are disabled, are added to Case1).

The average frequencies of the 16 ring oscillators in the different devices and cases are shown in Table I. It can be seen that one device (F2) is always the fastest, independently of the case, while F1 is always the slowest. This is due to the contribution of process variations. However, Table I shows how the average frequency of the 16 oscillators changes depending on the system implemented. The frequency variation depends on the relation between the PUF and the system. If the system is bigger, the frequency of the oscillator appears clearly modified.

TABLE I
AVERAGE FREQUENCY (MHZ) OF THE 16 OSCILLATORS

	Case1	Case2	Case3	Case4
F1	181.51	181.52	181.18	178.35
F2	194.91	194.65	194.13	191.86
F3	188.35	188.44	188.11	185.93



(a) (b)

Fig. 2. Frequencies of 16 oscillators in 3 FPGAs: (a) Case1. (b) Case4.

Contribution of the system over the PUF is different to contribution of process variation. The changes in the oscillator frequencies do not correspond to a global displacement with random variations around but it follows a certain pattern. This can be appreciated in Figure 2, which illustrates how the influence of the system imposes a similar pattern in all the devices. Hence, the model shown in (1) to analyze the total delay in a ring oscillator should be refined to include another delay, d_{SYSTEM}, so that the frequency of a ring oscillator is also function of the system:

$$d_{RO} = d_{AVG} + d_{PV} + d_{NOISE} + d_{SYSTEM} \quad (4)$$

The influence of d_{SYSTEM} is the consequence of the special sensitivity that ring oscillator show to power supply variations. This fact makes them really sensitive to changes in its surroundings. Variations of ring oscillator frequencies with power supply fluctuation have been analyzed experimentally with a variation of +/-5% of nominal value. For this purpose, the 1.2V regulator that feeds the FPGA core has been disconnected and changed by an external power source. The result of this analysis is that for a range of 1.14V to 1.26V the change of the ring oscillator frequencies is 17.04MHz.

Concerning temperature variation, the oscillator frequencies decrease almost linearly when temperature increases, with a slope of -0.14MHz per Celsius degree. This means that the influence of temperature variation is very much smaller than the influence of power supply variation (to produce a similar change in oscillator frequencies, the temperature should change in more than 118º C).

IV. REDUCTION OF PUF RELIABILITY AND UNIQUENESS

The influence of the system on the PUF response can deteriorate the PUF performance in terms of reliability and uniqueness. Concerning reliability, the PUF response may vary for the same device if the system implemented in the device changes. Concerning uniqueness, the PUF response may not vary very much for different devices.

Let us illustrate quantitatively these issues for the experiments commented in the previous section. The PUF response analyzed has 14 bits as the result of comparing 7+7 pairs of adjacent oscillators. Reliability is measured with equation (2), considering that the read outs correspond to the PUF responses obtained from the same device with different implemented systems (Case1 to Case4). The results are shown in Table II. Uniqueness is measured with equation (3), considering different devices with the same system implemented (Case1 to Case4). Results are shown in Table III (uniqueness decreases as the influence of the system increases). The third column in Table III illustrates how the influence of the system may produce that the 50% of the bits in the PUF response are equal in all the devices.

Comparing Table II and Table III, it can be observed that in the extreme case (Case4) the intra-class Hamming distance calculated (22.62%) is close to the inter-class Hamming distance (32.14%). This means that given an obtained PUF response, it is almost not possible to distinguish if it comes from the same FPGA with a different implemented system or from the same system implemented in a different FPGA.

In order to validate how the influence of the system can reduce the PUF uniqueness, a new scheme has been tested. It consists in two different PUF structures merged. Each one is composed by 32 ring oscillators distributed into an 8x4 matrix. The columns of the structures are interleaved, that is, the even columns belong to one structure while the odd columns belong to the other. Only one oscillator is active during a measure (the rest of the oscillators are disabled to avoid any kind of coupling). In these circumstances, the influence of ring oscillators could be similar to any other disabled circuitry placed in that position (as happens in Case1 and Case2 of the previous experiments). Two cases have been studied:

- CaseA: The output bits are obtained by comparing one oscillator in an even column with its adjacent oscillator. The output bit stream of the PUF has 28 bits. The odd columns form the “surrounding system”.

- CaseB: The 28 output bits are obtained as previously but evaluating the oscillators in the odd columns. The even columns form the “surrounding system”.

Figures 3 and 4 illustrate the frequencies of the 8x4 oscillators. A similar pattern can be observed for all devices in both cases. As a consequence, 13 out of the 28 bits are the same in the 9 devices analyzed, which conforms a 46.43% of the bitstream and presents a bad figure for authentication or identification purposes. Uniqueness results (measured using (3)) are 24.40% for CaseA and 21.63% for CaseB, which are far from the ideal 50%. This can be seen in Tables IV and V, which show the Hamming distance matrixes of both cases.

Several approaches reported in literature to increase the PUF reliability such as those of [4] [5] suggest to compare the fastest and the slowest oscillator in a matrix. If any of those proposals are used in these situations, the same output would be obtained in all the devices.

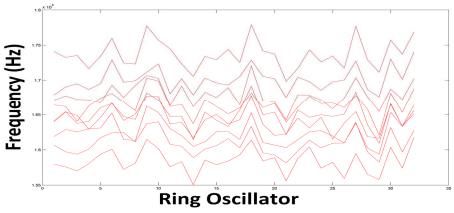


Fig. 3. Frequencies of the 8x4 oscillators in CaseA (each line corresponds to the 32 oscillators in an FPGA).

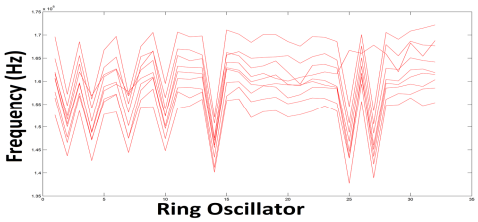


Fig. 4 Frequencies of the 8x4 oscillators in CaseB (each line corresponds to the 32 oscillators in an FPGA).

TABLE II
RELIABILITY (INTRA-CLASS HAMMING DISTANCE) FOR 3 FPGAS

	F1	F2	F3
Case1 and Case2	21.43%	14.29 %	14.29 %
Case1 and Case3	21.43 %	28.57 %	7.14 %
Case1 and Case4	14.29 %	42.86 %	28.57 %
Case2 and Case3	42.86 %	28.57 %	7.14 %
Case2 and Case4	21.43 %	28.57 %	14.29 %
Case3 and Case4	21.43%	28.57%	21.43%
Total	**23.81%**	**28.57 %**	**15.48%**

TABLE III

UNIQUENESS (INTER-CLASS HAMMING DISTANCE AND BIT ALIASING)

	Inter-Class_HD	Repeated bits
Case1	42.86%	35.71%
Case2	47.62%	42.86%
Case3	57.14%	14.29%
Case4	32.14%	50.00%

IV. CONCLUSIONS

After the study of different ring oscillator PUF structures on Spartan 3 FPGAs, it can be concluded that the whole system where the PUF is included determines in clear way the behavior and so statistical security features of the PUF. The cause is the power supply variations that are induced on the die. Since this influence can mask the manufacturing variability, the uniqueness property of the PUF is deteriorated. In addition, the strategies to increase the PUF reliability could even further reduce the PUF uniqueness. Hence, when a ring oscillator PUF structure is designed, the global system where it is included must be taken into account. The system should be the same during the enrollment process (when the bitstream of the PUF response is registered to create an ID or a key) and the authentication process (when the same PUF response is wanted to be reproduced).

ACKNOWLEDGMENT

This work has been partially supported by European Community under the MOBY-DIC Project FP7-IST-248858 (www.mobydic-project.eu), by Ministerio de Ciencia e Innovacion under the Project TEC2008-4920 and DPI2008-3847 and by Junta de Andalucia under the Project P08-TIC03674 (with support from the PO FEDER-FSE)

REFERENCES

[1] B. Gassend, D. E. Clarke, M. van Dijk, and S. Devadas. “Silicon physical unknown functions”, in, CCS 2002, pp. 148–160.
[2] S. Morozov, A. Maiti, P. Schaumont, “An analysis of delay based PUF implementations on FPGA”, in 6th Int. Symp. on Applied Reconfigurable Computing. LNCS, vol. 5992 (2010), pp. 382–387.
[3] M.-D. Yu and S. Devadas, “Secure and robust error correction for physical unclonable functions”, IEEE Design & Test of Computers, pp. 48-65, Jan.-Feb. 2010.
[4] G.E. Suh and S. Devadas,”Physical unclonable functions for device authentication and secret key generation", in Proc. Design Automation Conference, DAC 2007.
[5] C.-E. D. Yin and Q. Gang, “LISA: Maximizing RO PUF’s secret extraction”, In HOST 2010, pp. 100-105.
[6] A. Maiti, and P. Schaumont, “Improving the quality of a physical unclonable function using configurable ring oscillators”, in FPL 2009, pp. 703-707, Washington, DC, USA.
[7] A. Maiti, and P. Schaumont, “Improved ring oscillator PUF: an FPGA-friendly secure primitive”, Journ. of Cryptology, Vol. 4 (2), pp. 375-397, April 2011.
[8] H. Yu, P. H. W. Leong, H. Hinkelmann, L. Moller, M. Glesner, “Towards a unique FPGA-based identification circuit using process variations”, Proc. FPL 2009, pp. 397-402.
[9] P. Sedcole and P. Y. K. Cheung, “Within-die delay variability in 90nm FPGAs and beyond”, Proc. FPT 2006, pp. 97-104.
[10] A. Maiti, J. Casarona, L. McHale, P. Schaumont, “A large characterization of RO-PUF”, HOST 2010, pp. 66-71.

TABLE IV
INTER-CLASS HAMMING DISTANCE MATRIX (IN %) FOR CASEA

	F1	F2	F3	F4	F5	F6	F7	F8	F9
F1	0	21.4	21.4	35.7	25.0	17.9	28.6	17.9	17.9
F2		0	7.1	28.6	32.1	17.9	28.6	25.0	17.9
F3			0	28.6	32.1	17.9	21.4	25.0	25.0
F4				0	17.9	25.0	14.3	32.1	25.0
F5					0	35.7	17.9	35.7	21.4
F6						0	25.0	21.4	28.6
F7							0	32.1	25.0
F8								0	28.6
F9									0

TABLE V
INTER-CLASS HAMMING DISTANCE MATRIX (IN %) FOR CASEB

	F1	F2	F3	F4	F5	F6	F7	F8	F9
F1	0	25.0	10.7	25.0	32.1	21.4	28.6	17.9	25.0
F2		0	28.6	28.6	35.7	25.0	25.0	35.7	28.6
F3			0	21.4	28.6	25.0	17.9	14.3	28.6
F4				0	21.4	25.0	10.7	28.6	14.3
F5					0	10.7	10.7	21.4	7.1
F6						0	14.3	17.9	10.7
F7							0	25.0	10.7
F8								0	21.4
F9									0