IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received August 7, 2020, accepted August 24, 2020, date of publication August 27, 2020, date of current version September 10, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3020020

Proposal and Analysis of a Novel Class of PUFs Based on Galois Ring Oscillators

MIGUEL GARCIA-BOSQUE, GUILLERMO DÍEZ-SEÑORANS, CARLOS SÁNCHEZ-AZQUETA, AND SANTIAGO CELMA

Group of Electronic Design, Electrical Engineering and Communications Department, University of Zaragoza, 50009 Zaragoza, Spain

Corresponding author: Miguel Garcia-Bosque (mgbosque@unizar.es)

This work has been supported by Ministerio de Economía y Competitividad-Fondo Europeo de Desarrollo Regional (MINECO-FEDER) (TEC2017-85867-R) and Diputación General de Aragón (DGA) fellowship to Guillermo Díez-Señorans

ABSTRACT In this article, the possibility of using Galois ring oscillators to construct physically unclonable functions (PUFs) has been studied. The idea is to use novel PUF architectures, similar as the ring oscillator PUFs that, instead of comparing frequencies, compare the statistical bias of pairs of oscillators implemented in different locations. To study the viability of these systems, three different Galois oscillators have been implemented in several locations in several FPGAs and we have studied the main properties of their bias: repeatability, variability with the location, variability with the FPGA and spatial autocorrelation. Based on this study, we have determined that the bias of these oscillators meet the requirements that are needed to be used to construct a PUF. Finally, a PUF based on comparing the bias of neighboring 7-LUT Galois ring oscillators have been implemented and analyzed. The experimental results show that this PUF generates uniform responses that are highly reproducible and unique, making this PUF suitable for being used in identification applications.

INDEX TERMS Fibonnaci ring oscillators, FPGA, Galois ring oscillators, hardware security, physically unclonable function, ring oscillator.

I. INTRODUCTION

In the last years, physically unclonable functions (PUFs) have gained a great interest in both the academic and in the industry communities and are now considered an essential building block in modern secure systems [1]–[3]. By profiting the physical variations that occur during the manufacturing process of silicon chips, PUFs can generate an embedded secret that is easy to verify but difficult to predict. This way, these primitives can be used in some important applications such as identification [4]–[6] and key generation/storage [7], [8].

Depending on the method used for amplifying the manufacturing variations, PUFs can use several techniques such as memory metastability [9]–[11], matched delay line arbiter [12], differential-NAND [13] or ring oscillators (RO-PUFs) [7], [14]. However, in case of implementing a PUF in an FPGA, some complications can arise. While in an ASIC design, a designer can exploit the layout design techniques or work at a gate level, in an FPGA, a designer only has access to some bigger design blocks such as LUTs, flip-flops, multipliers or block RAM. Therefore, not all the proposed PUFs can be implemented on FPGAs.

Among the FPGA-based PUFs, RO-PUFs are often preferred [15], [16]. In these PUFs, typically the differences between the oscillator frequencies of identical ring oscillators are used to generate the PUF response. Unfortunately, the frequencies of the oscillators implemented in the FPGA present a clear systematic frequency variation when moved over the FPGA. To mitigate this effect, often, each oscillator is only compared with nearby oscillators [15].

In this article, we propose and study the possibility of using a class of digital nonlinear oscillators proposed by Golić in [17] to construct physically unclonable functions. We prove that, in a similar way as ring oscillators, Golić's oscillators exhibit a certain variation depending on its location that can be exploited for PUF applications. Furthermore, while the frequency variation of ring oscillators has a significant systematic component, we prove that the behavior of

The associate editor coordinating the review of this manuscript and approving it for publication was Yong Chen.

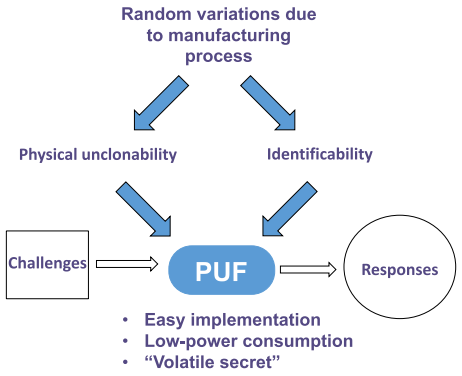

FIGURE 1. General scheme of a PUF with its properties.

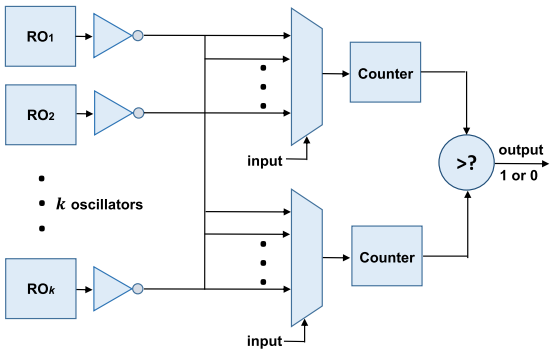

FIGURE 2. Basic scheme of a ring oscillator based PUF.

these oscillators do not have a noticeable systematic component along the location in the FPGA.

The paper is organized as follows: Section II presents the basic structure of a RO-PUF, an overview of the Fibonacci and Galois ring oscillators and, finally, proposes a method to use the variability presented by these systems to construct a PUF; Section III studies experimentally the bias of three different Galois ring oscillators to prove the capability of these systems to be used to construct a PUF; in Section IV, a PUF consisting of an array of 7-LUT GAROs is implemented and analyzed. Finally, conclusions are drawn in Section V.

II. BASIC CONCEPTS

A. ARCHITECTURE OF A RO-PUF

A ring oscillator consists of an odd number of inverters connected in a loop. Its output oscillates at a frequency that, in the ideal model, only depends on the number of inverters. In practice, however, due to random variations introduced during the manufacturing process, the oscillation frequency of each oscillator is not exactly the same. Typically, a RO-PUF compares the frequencies of pairs of identical oscillators to produce the output. A common scheme is the one shown in Fig 2, proposed in [7]. As it can be seen, the PUF contains an array of k identical ring oscillators, a couple of multiplexers used to select the oscillators and a couple of frequency counters to measure the frequencies of each oscillator. Typically, several pairs of oscillators are compared, producing several response bits. There are RO-PUFs with several challenges, where each challenge determines the pairs of oscillators to compare but, often, these PUFs have a single challenge, i.e., always the same pairs of oscillators are compared.

By considering all possible combinations, a total of $\binom{k}{2} = \frac{k(k-1)}{2}$ pairs can be formed to generate an output bit. However, from all these possible comparisons, not all of them produce independent outputs. For example, if oscillator RO_1 is faster than oscillator RO_2 and oscillator RO_2 is faster than oscillator RO_3, then it is clear that oscillator RO_1 is faster than oscillator RO_3. The number of independent comparisons that can be made is theoretically limited by the number of possible ways of ordering the oscillators, which is $k!$ Therefore, the maximum possible independent output bits is $\log_2 k!$ However, in practice, the exact list of independent comparisons to achieve this is difficult to obtain and is device-specific. A simple method of guaranteeing that all the output bits are independent consist of comparing fixed pairs of oscillators, using each oscillator only once, therefore, producing $\frac{k}{2}$ output bits. In order to further improve the reproducibility and uniqueness of the PUF, another approach consist of dividing the array of oscillators in groups of d oscillators and consider only the pair with the largest difference in frequency. This way, the quality of the PUF is enhanced at a cost of reducing the number of response bits by a factor of d [7]. Finally, a common approach consist of comparing neighboring oscillators, producing a response of $k-1$ bits [14]. With this approach, although the output bits are not completely independent, the entropy per output bit is very high and the throughput is almost twice as much as with the $\frac{k}{2}$ strategy.

As it is clear, there are many different RO-PUFs architectures that can be implemented and each architecture prioritizes some aspects such as: number of response bits, independence of the output bits, reproducibility and uniqueness of the PUF, big number of challenges-response pairs, etc. Unfortunately, when implemented in an FPGA, the frequency of the ring oscillators presents a clear systematic component (i.e., ring oscillators implemented in some locations are usually faster than ring oscillators implemented in other locations). As a consequence, some architectures that could theoretically be good for a certain application behave worse in a real implementation. Therefore, in practice, only a few architectures are usually used. Typically, in these architectures, only nearby oscillators are compared to reduce the systematic component.

B. FIBONACCI AND GALOIS RING OSCILLATORS

In 2006, J D. Golić proposed a new method for true random number generation using new structures called Fibonacci ring oscillators (FIRO) and Galois ring oscillators (GARO) [17]. These structures where based on the structure of ring oscillators but, instead of using a single circular feedback, they used a more complex feedback incorporating XOR gates in an analogous way to the Fibonacci and Galois configurations of an LFSR (Fig. 3). The idea behind this proposal was to

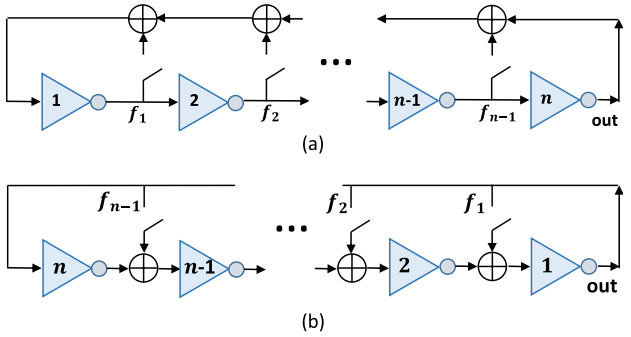

FIGURE 3. Scheme of (a) Fibonacci ring oscillators and (b) Galois ring oscillators.

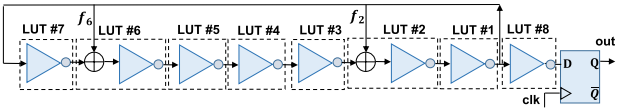

FIGURE 4. 7-LUTs GARO. An extra inverter (LUT #8) is used to avoid possible frequency couplings.

combine the pseudo-randomness properties of the LFSRs with the true randomness properties of ring oscillators due to oscillation jitter.

For both FIRO and GARO, the feedback connections are specified with coefficients f_i and, therefore, the configuration can be unequivocally defined using a binary polynomial $f(x) = \sum_{i=0}^{n} f_i x^i, f_0 = f_1 = 1$. If $f_i = 1$, the corresponding switch in Fig. 3 is closed while, if $f_i = 0$, the corresponding switch is open. Note that these switches are only shown for illustration purposes and are not actually implemented. In an actual implementation, if $f_i = 1$, there is an XOR and a feedback connection implemented in the ith position while, if $f_i = 0$, the ith feedback connection and XOR gate are not implemented. An advantage of using GAROs with respect to FIROs is that, given a feedback polynomial of order n, it is possible to easily implement it in an FPGA using exactly n LUTs. If $f_i = 1$, the implemented function in the ith LUT is an XNOR operation while, if $f_i = 0$, the implemented function in the ith LUT is a NOT operation. According to Xilinx specifications [18], the LUT propagation delay does not depend on the function implemented so the total time-delay will only depend on the total number of LUTs (which is determined by the order of the primitive polynomial), making the study of these systems easier. For this reason, in this work, only GARO topologies have been studied.

C. ISSUES OF FIRO AND GARO TRNGs

Both FIRO and GARO TRNGs have been widely studied and implemented in both FPGAs [19] and ASIC devices [20]. Unfortunately, these kind of structures have not yet proven to be robust since there is no theory that explains how to choose a feedback polynomial for GARO or FIRO that guarantees that the system behaves properly, generating a minimum amount of entropy [21], [22].

Furthermore, even using the same feedback polynomial, it has been recently proven that, depending on the location

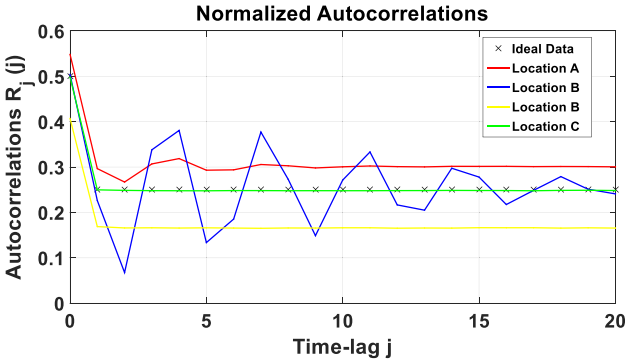

FIGURE 5. Autocorrelations of sequences obtained from the same GARO polynomial implemented in four different locations. Red sequence presents some statistical dependence and some autocorrelation, blue sequence presents no bias but a high statistical dependence, yellow sequence presents some bias and no statistical dependence and green sequence does not present bias or statistical dependence.

within the FPGA where the system is implemented, the behavior of the system can change drastically, sometimes resulting in poor random sequences [23], [24].

As an example, let's consider a TRNG consisting of a 7-LUT GARO with the feedback polynomial $f(x) = 1+x^2+x^6+x^7$ that obtains the random sequences by sampling the signal with a flip-flop (Fig. 4). By comparing the sequences obtained by the same system implemented at several locations within the FPGA, it can be seen that they clearly present different statistical properties. A possible measurement that can be used to illustrate this fact is the normalized autocorrelations, R_j, defined as: $R_j = \frac{1}{N-j}\sum_{i=0}^{N-j-1} a_i a_{i+j}$ where N is the total number of bits of the sequence and a_i is the ith element of the sequence (note that the coefficient R_0 represents the bias of the sequence). Fig. 5 represents the normalized autocorrelations, R_j, of four sequences, each of them generated by the same system sampled at 10 MHz but implemented at different locations in the same FPGA. As it can be seen, all of the graphs present clearly distinguishable patterns.

D. CONSTRUCTION OF A GARO-PUF

As we have shown, GAROs implemented in different locations present some clearly noticeable statistical differences. The main scope of this work is to study the possibility of using these statistical differences to construct a PUF. In particular, due to its simplicity, we will study the variation of the bias (R_0) depending on the location. As long as the bias distribution presents some properties such as being repeatable within the same location in the same FPGA but variable when changing the location or the FPGA, it could be possible to use an analogous structure as the one used in the RO-PUF (Fig. 1) that compares the value of the bias of GAROs instead of the frequencies of ring oscillators.

In the following section, we will prove experimentally that the biases of several GAROs meet all the required properties and, therefore, it can be possible to construct PUFs based on these systems. Finally, as a proof of concept, a particular

GARO-PUF that uses an analogous structure as the RO-PUF presented in [14] has been implemented and analyzed. All the systems have been implemented in a Pynq Z2 board that includes a Zynq-7000 series ARM/FPGA System on Chip.

III. PROPERTIES OF THE BIAS OF SEVERAL OSCILLATORS

A. STUDY OF THE REPRODUCIBILITY OF A POSSIBLE GARO-PUF

In order to construct a PUF based on comparing the bias of pairs of oscillators (i.e., pairs of identical oscillators implemented on different locations), the biases of the oscillators must meet some properties, in a similar way as the frequencies of the ring oscillators in a RO-PUF. In particular, if we want this kind of PUFs to be reproducible, the bias of the oscillators must meet these two properties:

- First, if the measurement of the bias of an oscillator in a given location and a given FPGA is repeated several times, the results should always be the same or very similar. In this article, this property will be called "repeatability".
- Second, the measured bias should change when changing the location within the FPGA. In this article, we will call this property "variability".

The changes in the bias that occur when changing the location (i.e., variability) should be clearly larger than the changes that might occur when repeating the measurement in the same location. This way, the results of the comparisons between pairs of oscillators will most of the time be the same and, therefore, an implemented PUF based on comparing pair of oscillators will be reproducible.

To study these properties, the same GARO has been implemented in 101 different locations in the same FPGA. Each GARO has been sampled with a flip-flop and, if the sampled bit is "1", a counter has been increased. This way, by observing the value of the counter, it is possible to know the behavior of the bias as long as the following conditions are met: first, the sampling frequency must be much lower than the frequency of the oscillations to avoid that the measurements occur during the same high or low state; second, a high number of samples must be taken so that the final value of the counter is a good estimation of the bias. The same process has been repeated 100 times to measure the repeatability.

In order to determine a proper sampling frequency, we first did a small test consisting of measuring the bias at different sampling frequencies (from 100 MHz to 10 kHz) for several systems. We observed that a sampling frequency of f_s= 100 kHz was good enough for measuring the bias precisely (lower sampling frequencies did not improve the precision of the measurements while, in some systems, higher sampling frequencies affected the result of the bias). Regarding the number of samples, we determined that 100,000 samples was a good choice to have a good estimation of the bias. With 100,000 samples, assuming an ideal unbiased sequence the expected value of the sum would be $50,000 \pm 158$ (around $\sim$ 0.3% error). If, instead, we had used 10,000 samples, the error in the estimation of the bias would be $\sim 1\%$, which could affect the repeatability of the PUF.

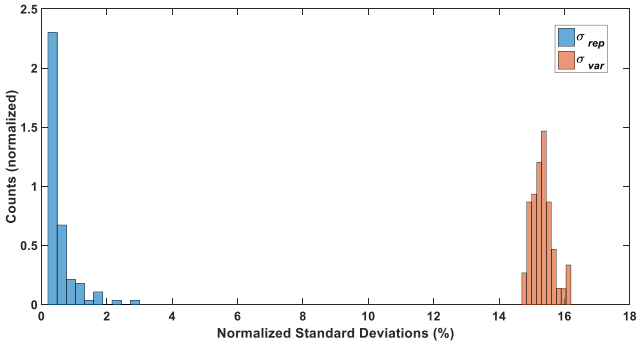

FIGURE 6. Distribution of the normalized standard deviations σ^j_{rep}, and σ^j_{var} of a 5-LUT GARO at room temperature.

To sum up, at the end of the experiment, a matrix of integer numbers, $A = \{A^j_i\}$ has been obtained where each element A^j_i represents the final value of the counter at the ith measurement of the oscillator that is located in the jth location.

To evaluate the repeatability and the variability, the normalized standard deviations σ^j_{rep}, σ^i_{var} have been used, defined as:

$$\sigma^j_{rep} = \frac{1}{\mu^j}\sqrt{\frac{1}{N-1}\sum_{i=1}^{N}\left|A^j_i - \mu^j\right|^2} \times 100(\%)$$
$$\sigma^i_{var} = \frac{1}{\mu_i}\sqrt{\frac{1}{N'-1}\sum_{j=1}^{N'}\left|A^j_i - \mu_i\right|^2} \times 100(\%) \quad (1)$$

where

$$\mu^j = \frac{1}{N}\sum_{i=1}^{N} A^j_i$$
$$\mu_i = \frac{1}{N'}\sum_{j=1}^{N'} A^j_i \quad (2)$$

In this experiment, the number of repetitions is $N = 100$ and the number of different locations is $N' = 101$.

Fig. 6 shows the distribution of σ^j_{rep} and σ^i_{var} in an experiment using an array of 5-LUT GAROs at room temperature ($\sim$ 25°C). As it can be seen, the values of σ^j_{rep} are much smaller than the values of σ^i_{var}, which indicates that a PUF based on comparing the bias of pairs of oscillators would be reproducible. It must be noticed that all these measurements have been obtained in the same experiment (using the same synthesized code) so the fact that the values of σ^j_{rep} are not cero means that the system is sensitive to changes in the operation conditions that can occur between measurements such as slightly different temperatures or supply voltages. The spread of the histogram of σ^j_{rep} indicates that oscillators implemented in some locations are more sensitive to these changes than oscillators implemented in other locations.

The same experiment has been repeated for three different GAROs (a 5-LUT GARO, a 7-LUT GARO and a 17-LUT GARO) at different temperatures. According to [17], a GARO does not present a fixed point if an only if $f(1) = 1$ and n is odd. In this work, we have only used feedback

TABLE 1. Standard deviations $\bar{\sigma}_{rep}$, $\bar{\sigma}_{var}$ of different oscillators at different temperatures.

	5-LUT GARO $f(x) = 1 + x + x^3 + x^5$			7-LUT GARO $f(x) = 1 + x^2 + x^6 + x^7$			17-LUT GARO $f(x) = 1 + x + x^3 + x^{17}$			5-LUT RO $f(x) = 1 + x^5$		
Temperature (°C)	$\bar{\sigma}_{rep}$ (%)	$\bar{\sigma}_{var}$ (%)	Q	$\bar{\sigma}_{rep}$ (%)	$\bar{\sigma}_{var}$ (%)	Q	$\bar{\sigma}_{rep}$ (%)	$\bar{\sigma}_{var}$ (%)	Q	$\bar{\sigma}_{rep}$ (%)	$\bar{\sigma}_{var}$ (%)	Q
-20	0.758	13.2	17.4	0.405	16.4	40.6	0.578	32.7	56.6	1.00	4.53	4.52
0	0.503	13.4	26.6	0.533	14.9	28.0	0.558	33.0	59.3	1.16	4.42	3.80
20	0.525	13.2	25.1	0.424	15.1	35.6	0.579	31.2	53.8	0.982	4.31	4.39
40	0.566	11.4	20.1	0.397	15.9	40.0	0.396	15.9	40.2	0.703	4.23	6.02
60	0.548	11.2	20.4	0.457	16.0	35.0	2.535	33.0	13.0	0.691	4.23	6.13
80	0.615	11.0	17.9	0.393	16.3	41.5	1.120	31.2	27.8	0.019	3.98	211.23
Average values	0.586	12.2	**21.3**	0.435	15.8	**36.8**	0.961	29.5	**41.8**	0.7599	4.29	**39.3**

polynomials that satisfy this condition to avoid any possible fixed points. Furthermore, for comparison purposes, an analogous structure that measures 100 times the frequencies of a 5-LUT ring oscillator implemented in the same 101 locations has been implemented. In order to have a figure of merit of the repeatability and variability, the average values $\bar{\sigma}_{rep} = \frac{1}{N'}\sum_{j=1}^{N'}\sigma_{rep}^{j}$ and $\bar{\sigma}_{var} = \frac{1}{N}\sum_{i=1}^{N}\sigma_{var}^{i}$ have been obtained for each temperature. Finally, we have defined the quality ratio $Q = \bar{\sigma}_{var}/\bar{\sigma}_{rep}$, which can be a good estimator of how reproducible a PUF would be. The experimental results are summarized in Table 1.

As it can be seen, although the temperature can affect the repeatability and the variability of the bias of a GARO, the changes are quite small in all three cases (5-LUT, 7-LUT and 17-LUT) and, from the collected data, it is not clear if increasing the temperature improves or deteriorates the reproducibility of the PUF. In a similar way, the 5-LUT ring oscillator does not present a high variability on the temperature, as long as the temperature is not very high. However, when operating at 80 °C, the repeatability is much higher and, therefore, the quality ratio Q is also very high.

By comparing the average values of the quality ratios, $\bar{Q} = \frac{1}{6}\sum_{i=1}^{6} Q(T_i)$, of the different oscillators, we can see that both the 7-LUT GARO, the 17-LUT GARO and the 5-LUT RO present similar values $\bar{Q} \approx 40$ while the 5-LUT GARO presents a lower value ($\bar{Q} \approx 20$). However, it must be noticed that, in the case of the ring oscillator, the high value of Q obtained at 80 °C affects greatly the value of $\bar{Q}$. By considering lower temperatures, the value of $\bar{Q}$ would be around 5.0, which is clearly lower than the values obtained by the GAROs. Therefore, it can be concluded that, as long as the temperatures are not very high, a GARO-PUF would probably present a higher reproducibility than a RO-PUF.

B. STUDY OF THE UNIQUENESS OF A POSSIBLE GARO-PUF

In order to study the uniqueness of a GARO-PUF, the same experiment as before has been repeated on 20 different FPGAs at room temperature. First, for each FPGA and each jth location, the mean value of the bias, μ_k^j has been calculated as.

$$\mu_k^j = \frac{1}{N}\sum_{i=1}^{N} A_i^j(k) \tag{3}$$

where $A_i^j(k)$ is the ith measurement of the oscillator that is located in the jth location in the kth FPGA. Then, we have obtained the normalized standard deviations of the mean values measured on different FPGAs (σ_{FPGA}^j) which indicate the variability of the bias in a certain location when changing the FPGA:

$$\sigma_{FPGA}^j = \frac{1}{\overline{\mu_k^j}}\sqrt{\frac{1}{K-1}\sum_{k=1}^{K}\left|\mu_k^j - \overline{\mu_k^j}\right|^2} \times 100(\%) \tag{4}$$

with $\overline{\mu_k^j} = \frac{1}{K}\sum_{k=1}^{K}\mu_k^j$ and $K = 20$.

In a similar manner as in the previous subsection, these deviations should be big compared to the deviations that occur when repeating the same measurement in the same location and same FPGA (σ_{rep}^j). Fig. 7 shows the histogram of the values of σ_{FPGA}^j along with the values of σ_{rep}^j in all FPGAs using a 5-LUT GARO. As it can be seen, although the values of σ_{FPGA}^j are generally higher than the values of σ_{rep}^j, in some cases they are quite similar. Therefore, the uniqueness of a PUF using these oscillators would not be ideal. By repeating the experiment for the case of a 7-LUT GARO and

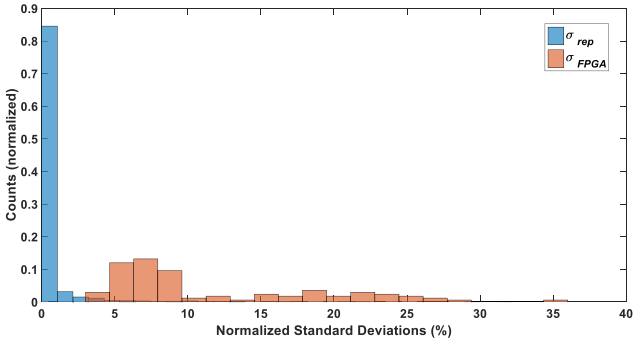

FIGURE 7. Distribution of the normalized standard deviations σ_{rep}^j, and σ_{FPGA}^j of a 5-LUT GARO at room temperature.

TABLE 2. Standard deviations $\bar{\sigma}_{rep}$, $\bar{\sigma}_{FPGA}$ of different oscillators.

	$\bar{\sigma}_{rep}$	$\bar{\sigma}_{FPGA}$	Q'
5-LUT GARO $f(x) = 1 + x + x^3 + x^5$	0.8624	11.7	**13.6**
7-LUT GARO $f(x) = 1 + x^2 + x^6 + x^7$	0.4717	9.61	**20.4**
17-LUT GARO $f(x) = 1 + x^3 + x^{17}$	0.592	12.2	**20.5**
5-LUT RO $f(x) = 1 + x^5$	0.991	30.3	**40.6**

17-LUT GARO, similar results have been obtained. The mean values of σ^j_{FPGA} and σ^j_{rep}, (i.e., $\bar{\sigma}_{FPGA}$ and $\bar{\sigma}_{rep}$) at room temperature and its ratio $Q' = \bar{\sigma}_{FPGA}/\bar{\sigma}_{rep}$ for each case are shown in Table 2. For comparison, the values of a 5-LUT ring oscillator have also been included. From these values, it seems that the 5-LUT GARO-PUF would present the lowest uniqueness and the 7-LUT and 17-LUT GARO-PUFs would both present a slightly higher uniqueness. However, the ring oscillator presents the highest ratio ($Q' \approx 40$) which indicates that, probably, a RO-PUF would outperform a GARO-PUF in terms of uniqueness. Nevertheless, there could be other GAROs with other feedback polynomials that might exhibit a higher uniqueness. Future research works could focus on finding new feedback polynomials that have higher uniqueness while maintaining a high reproducibility.

C. STUDY OF THE SYSTEMATIC COMPONENTS IN THE BIAS

As explained before, one of the main issues of the ring oscillator PUF is that the frequencies of the ring oscillators present a high systematic component, i.e., ring oscillators implemented in some areas of the FPGA are usually faster than oscillators implemented in other regions. To visualize this fact, a color map of the average frequencies of a 5-LUT ring oscillator implemented on 101 different locations is shown in Fig. 8a. Each rectangle represents a ring oscillator and its coordinates correspond approximately to their physical coordinates within the FPGA (no oscillators were implemented in the top right corner of the FPGA). The color of each rectangle represents its frequency (darker color corresponds to higher frequency).

By looking at this map, there are some correlations that can be easily detected. For example, oscillators implemented in the right tend to have higher frequencies than oscillators implemented on left of the FPGA. On the other hand, the bottom row follows a dark-light-dark-light... pattern.

The same map has been obtained with the bias of 5-LUT GAROs implemented in the exact same locations (Fig. 8b). As seen in this Figure, no patterns can be easily appreciated indicating that the spatial autocorrelation of the bias of these oscillators is much lower than the spatial autocorrelation of the frequencies of ring oscillators. Similar figures have been obtained for the 7-LUT GARO and the 17-LUT GARO.

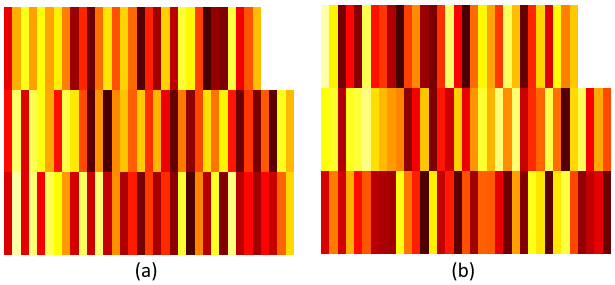

FIGURE 8. (a) Frequency map of the ring oscillators. (b) Bias map of GAROs. Each rectangle represents a ring oscillator/GARO and its color represents its frequency/bias (darker colors represent higher frequencies/bias).

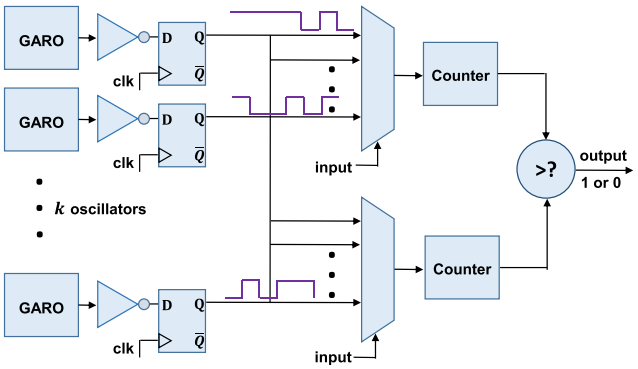

FIGURE 9. Structure of the implemented GARO-PUF.

Therefore, GAROs seem to present a great advantage with respect to ring oscillators in that sense. While most of the RO-PUF constructions need to compare only nearby oscillators to mitigate the spatial correlations, GARO-PUFs would not have this restriction and, therefore, could offer a much bigger challenge-response set.

IV. IMPLEMENTATION OF A GARO-PUF

Finally, as proof of concept, a GARO-PUF has been implemented and tested. This PUF contains an array of 101 7-LUT GAROs and a 100-bit response is obtained by comparing the bias of neighboring oscillators in an analogous manner as the one presented in [14]. The measurement scheme adapted in this article is shown in Fig. 9. As in the previous section examples, to obtain the bias of each oscillator, 100,000 samples are collected with a sampling frequency of 100 kHz. This way, by measuring each oscillator in parallel a 100-bit response is obtained per second. This implementation, however, requires to implement a counter for each oscillator and, therefore, uses a lot of area. If, instead, the bias of each oscillator is measured sequentially, a single counter can be used for all the measurements. This way, the implementation area is greatly reduced at a cost of decreasing the throughput. Both implementations with parallel measurement and sequential measurement have been made. The implementation resources are shown in Table 3.

Since the architecture of this PUF is almost identical to the architecture of a RO-PUF, the implementation resources in both cases are very similar, as long as the same measurement

TABLE 3. GARO-PUF implementation resources.

	Parallel measurement		Sequential measurement	
	LUTs	FFs	LUTs	FFs
Oscillators	606	101	606	101
Counters	202	2020	2	40
Comparators	2100	200	21	2
Extra logic for measuring	832	87	70	23
Total	**3740**	**2408**	**699**	**166**

strategy (sequential or parallel) is used. Regarding the throughput, in both GARO-PUFs and RO-PUFs it can be increased or decreased by changing the time spent to measure the bias/frequency. However, decreasing too much the time spent to measure the bias/frequency would worsen the quality of the PUF. In all comparisons shown in this article, a similar measuring time has been used for GAROs and ROs to have fair comparisons. We have chosen a quite high measuring time to measure the bias/frequencies quite precisely so that in both cases we are approaching to a best-case scenario. Lower measuring times would decrease the precision of the measurements, especially in the of the GAROs and, therefore, worsen their reproducibility.

Once implemented, this PUF has been analyzed in terms of reproducibility, uniqueness, uniformity and identifiability.

A. REPRODUCIBILITY

First, the reproducibility of the implemented PUF has been measured. For this purpose, the 100-bit response of the PUF has been measured 100 times and, for each possible pair of measurements, the Hamming Distance, *HD*, has been obtained. Given two m-bits output words, $x = (x_1, x_2, \ldots x_m)$ and $y = (y_1, y_2, \ldots y_m)$, their hamming distance is defined as:

$$HD = \sum_{i=1}^{m} x_i \oplus y_i \tag{5}$$

where, in this case, $m = 100$.

The distribution of the Intra-chip Hamming Distances (Intra-*HD*s) of the GARO-PUF measured at room temperature has been plotted in Fig. 10a. As it can be seen, all of the hamming distances are close to 0, indicating that the reproducibility is very high. The average value is 1.11% with a minimum value of 0 and a maximum value of 5%. For comparison, in the case of the ring oscillator we obtain an average value of 1.98% with also a minimum value of 0% and a maximum value of 5% (Fig. 10b). Furthermore, the histogram of the ring oscillator presents a larger dispersion.

Furthermore, the Intra-chip Hamming Distances have been measured at different temperatures. Its values are plotted in Fig. 11. As it can be seen, the average Intra-*HD* does not change greatly with the temperature. If we compare the values with the ones obtained by the RO-PUF, we can see that for lower temperatures the GARO-PUF is more reproducible than the RO-PUF while, for very high temperatures, the RO-PUF is more reproducible. These results, however, could depend on many factors such the FPGA or the oscillators implemented so it is not possible to extrapolate these results to other cases. Another thing that must be pointed out is that, by repeating this experiment, the values obtained in Fig. 11 are not repeatable. This is likely caused by the fact that the internal temperatures and voltages are not exactly the same in each measurement. However, the tendency commented before (i.e., GARO-PUF presents lower Intra-*HD*s for

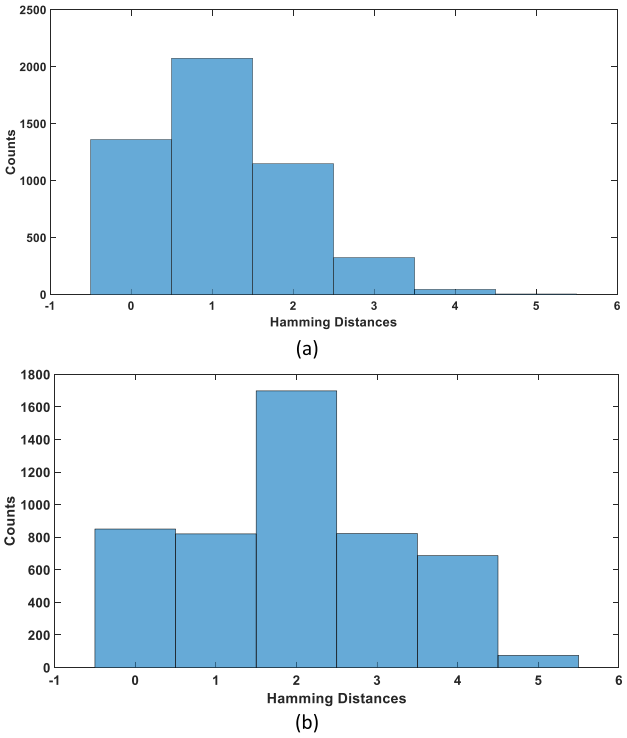

FIGURE 10. (a) Distribution of the Intra-chip Hamming Distances of the 7-LUT GARO PUF measured at room temperature (b) Distribution of the Intra-chip Hamming Distances of the 5-LUT RO-PUF measured at room temperature.

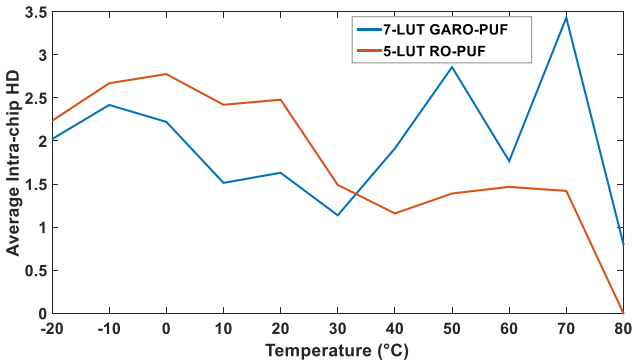

FIGURE 11. Distribution of the Intra-chip Hamming Distances measured at room temperature.

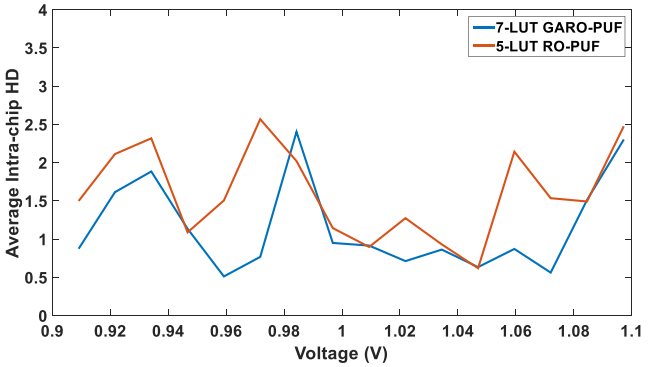

FIGURE 12. Distribution of the Intra-chip Hamming Distances for different voltages.

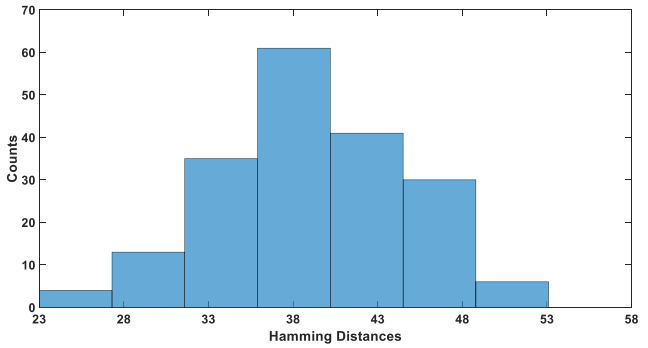

FIGURE 13. Distribution of the Inter-chip Hamming Distances measured at room temperature.

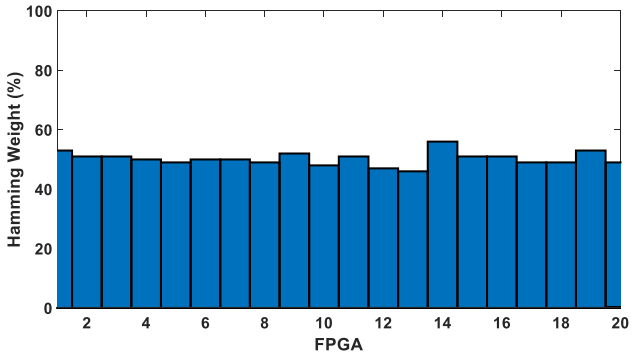

FIGURE 14. Hamming Weights of the most common response in each FPGA.

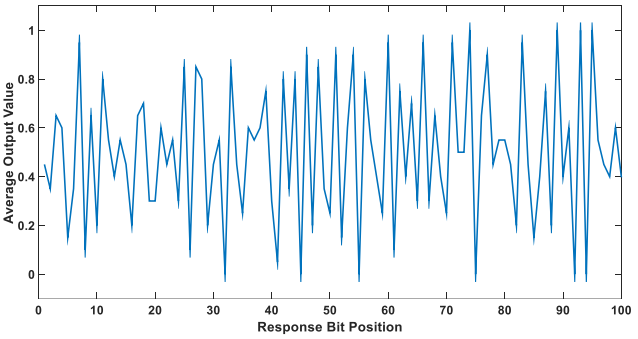

FIGURE 15. Average output value at each bit position.

low temperatures and RO-PUF presents lower Intra-*HD*s for high temperatures) prevails.

Finally, we have measured Intra-chip Hamming Distances at different FPGA core voltages. The Pynq Z2 board has a TPS65400 Power Management Unit (PMU) that creates the required 3.3 V, 1.8 V, 1.5 V and 1.0 V supplies needed for the FPGA from the main power input [25]. In particular, the 1.0 V signal used for the FPGA core supply, V_{CCINT}, depends on a reference voltage, V_{REF}, that can be changed in 10 mV steps (which produces changes of around 13 mV in V_{CCINT}) through an I2C command [26]. This way by using a microcontroller we have managed to measure the interdistances at different voltages at a $\pm 10\%$ range. The results are shown in Fig. 12. We can see that, in both the RO-PUF and in the GARO-PUF, the average Intra-*HD* does not change greatly with the supply voltage. In fact, these changes could be caused by the fact that the internal temperature was not exactly the same in all measurements.

B. UNIQUENESS

To measure the uniqueness of the PUF, it has been implemented on 20 different FPGAs and we have obtained the most common response for each case. Then, the Inter-chip Hamming Distances have been obtained as shown in Fig. 13.

As it can be seen, although the Inter-*HD*s are quite larger than the Intra-*HD*s, their values are far from the ideal 50%. For comparison, the average Inter-*HD* is 39.1% while, for the ring oscillator, the average value is 47.2%. It must be noticed that the measured value is not very precise since we do not have enough statistical data (only 20 FPGAs have been used). However, although the actual average value could be higher, it seems very unlikely that by increasing the number of FPGAs, the average value will approach too much to 50%.

The fact that the average Inter-*HD* deviates from the 50% value could be caused by two non-idealities. First, it could be caused by non-uniform distributions in the PUF responses (i.e., responses tend to have more 1's than 0's or vice versa). Second, it could be caused by bit-aliasing (i.e., most of the FPGAs produce the same bit in some positions).

To check if the output responses are uniform, Fig. 14 shows the Hamming Weights (percentage of ones), *HW*, of the most common response in each FPGA. As it can be seen, all Hamming Weights are close to 50%, which indicates that the responses are uniform so it cannot be the reason why the average Inter-chip *HD* is low.

Regarding the bit-aliasing, for each response bit position (from 1 to 100), the average value of the output bit across the 20 FPGAs has been obtained (Fig. 15).

We can see that, although the average value is 0.502, there are many spikes, i.e., some response bits are almost always 0 or almost always 1 in all FPGAs. Therefore, this explains why the Inter-chip *HD*s are smaller than the ideal value.

A possible reason for the bit-aliasing could be that some locations (the ones that almost always produce a 0 or a 1 output bit) could be physically placed near other FPGA elements (the input/output ports, the power supply, the

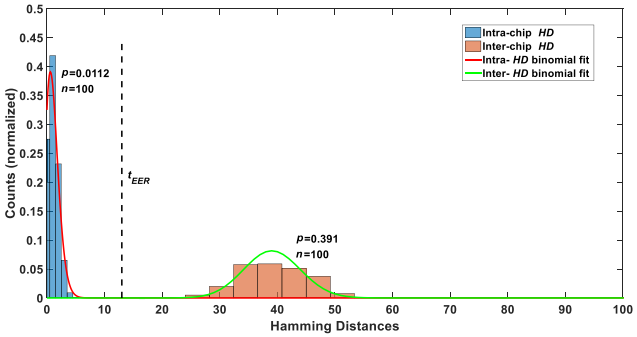

FIGURE 16. Intra-chip and Inter-chip Hamming Distances.

implemented counters, ...) and some of those elements could affect the behavior of nearby oscillators in a similar way. Another possible reason could be that, during the manufacturing process, some areas of the FPGA could present lower variations than other areas. Finally, in some cases, the particular routing of a certain oscillator (which we not fully control) could determine its behavior. Since the exact same routing for each location is used when repeating the measurements in different FPGAs (the same.bit file is used to program each FPGA), the oscillators placed in some locations could have a particular routing that determines their behavior quite deterministically.

C. IDENTIFIABILITY

Since, the PUF presents a fuzzy behavior, in order to use it for identification applications, a threshold t must be set. Then, two responses x, y, will be considered to come from the same FPGA if $HD(x, y) < t$. Otherwise the two responses will be considered to come from a different FPGA [27]. With all the responses obtained experimentally, it can be noticed that all of the Intra-*HD*s (Fig. 10) are smaller than all the Inter-*HD*s (Fig. 13). Therefore, by choosing any threshold such as max {Intra-*HD*}$< t <$ min{Inter-*HD*} all the responses are perfectly identifiable.

However, by increasing the number of measurements, new Hamming Distances will be obtained. To estimate the probability of obtaining different Hamming Distances, both the Intra-*HD*s and the Inter-*HD*s have been adjusted to binomial functions (Fig. 16). From this adjustment, we have calculated that the Equal Error Threshold t_{EER}, i.e., the threshold for which the False Acceptance Rate (FAR) and False Rejection Rate (FRR) are closest is: $t_{EER} = 13$. With this threshold, we obtain the values of FAR $= 1.81 \times 10^{-9}$ and FRR $= 1.61 \times 10^{-9}$. As it can be seen, both errors are negligible and, therefore, this PUF is highly identifiable.

V. CONCLUSION

In this article, we have proven the suitability of using the GAROs proposed in [17] to construct a PUF. In particular, by analyzing three different oscillators, we have shown that their bias change depending on their location as well as the FPGA in a similar way as the frequencies of a ring oscillator.

As a demonstration, a 7-LUT GARO-PUF have been implemented and analyzed. Its reproducibility has been high and, although the uniqueness is not ideal, the identifiability is very high. Nevertheless, it must be noticed that, by measuring the bias with more precision (decreasing the sampling frequency and increasing the number of counts), both the reproducibility and uniqueness would improve.

From the experimental results obtained in this work, GARO-PUFs seem to be at least comparable to RO-PUFs. Their reproducibility seems to be higher and their uniqueness smaller. Furthermore, it seems that the distribution of the bias of these systems does not present as much spatial autocorrelation within the FPGA compared to the frequencies of the ring oscillator. This opens the possibility of constructing PUFs with a wider set of challenge-response sets since it is not required to compare only nearby oscillators as in the case of the RO-PUFs. This would be a great improvement since it would be possible to design PUFs with better performance and more robust to modeling attacks.

This work opens a very interesting line of research in the design of robust PUFs for FPGAs. Other structures such as other GAROs, FIROs or other Digital Nonlinear Oscillators such as the ones presented in [23] could be studied. It is likely that other oscillators would offer better results than the ones shown in this article. Furthermore, other strategies to distinguish between oscillators (e.g., measuring the other normalized autocorrelations, R_j, or the Shannon entropy instead of measuring the bias) could be the used. However, this would require a more complex measuring system.

REFERENCES

[1] M. Garcia-Bosque, G. Díez-Señorans, C. Sánchez-Azqueta, and S. Celma, "Introduction to physically Unclonable functions: Properties and applications," in *Proc. 24th Eur. Conf. Circuit Theory Design (ECCTD)*, Sofia, Bulgaria, 2020, pp. 1–4.

[2] Y. Gao, D. C. Ranasinghe, S. F. Al-Sarawi, O. Kavehei, and D. Abbott, "Emerging physical unclonable functions with nanotechnology," *IEEE Access*, vol. 4, pp. 61–80, 2016.

[3] S. Satpathy, S. K. Mathew, V. Suresh, M. A. Anders, H. Kaul, A. Agarwal, S. K. Hsu, G. Chen, R. K. Krishnamurthy, and V. K. De, "A 4-fJ/b delay-hardened physically unclonable function circuit with selective bit destabilization in 14-nm trigate CMOS," *IEEE J. Solid-State Circuits*, vol. 52, no. 4, pp. 940–949, Apr. 2017.

[4] J. Zhang, X. Tan, X. Wang, A. Yan, and Z. Qin, "T2FA: Transparent two-factor authentication," *IEEE Access*, vol. 6, pp. 32677–32686, 2018.

[5] K. Yang, Q. Dong, D. Blaauw, and D. Sylvester, "14.2 a physically unclonable function with BER <10^{-8} for robust chip authentication using oscillator collapse in 40nm CMOS," in *IEEE ISSCC Dig. Tech. Papers*, Feb. 2015, pp. 1–3.

[6] A. Alvarez, W. Zhao, and M. Alioto, "14.3 15fJ/b static physically unclonable functions for secure chip identification with <2% native bit instability and 140× Inter/Intra PUF Hamming distance separation in 65nm," in *IEEE ISSCC Dig. Tech. Papers*, Feb. 2015, pp. 1–3.

[7] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Proc. 44th ACM/IEEE Design Autom. Conf.*, Jun. 2007, pp. 9–14.

[8] J. Delvaux, D. Gu, D. Schellekens, and I. Verbauwhede, "Helper data algorithms for PUF-based key generation: Overview and analysis," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 34, no. 6, pp. 889–902, Jun. 2015.

[9] K.-U. Choi, S. Baek, J. Heo, and J.-P. Hong, "A 100% stable sense-amplifier-based physically unclonable function with individually embedded non-volatile memory," *IEEE Access*, vol. 8, pp. 21857–21865, 2020.

[10] Y. Su, J. Holleman, and B. Otis, "A 1.6pJ/bit 96% stable chip-ID generating circuit using process variations," in *IEEE ISSCC Dig. Tech. Papers*, Feb. 2007, pp. 406–411.
[11] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, "FPGA intrinsic PUFs and their use for IP protection," in *Proc. Cryptograph. Hardware Embedded Syst. (CHES)*, Berlin, Germany, 2007, pp. 63–80.
[12] J. W. Lee, D. Lim, B. Gassend, G. E. Suh, M. van Dijk, and S. Devadas, "A technique to build a secret key in integrated circuits for identification and authentication applications," in *Symp. VLSI Circuits. Dig. Tech. Papers*, Jun. 2004, pp. 176–179.
[13] J. Lee, M. Kim, G. Shin, and Y. Lee, "A 20F2 area-efficient differential NAND-structured physically unclonable function for low-cost IoT security," *IEEE Solid-State Circuits Lett.*, vol. 2, no. 9, pp. 139–142, Sep. 2019.
[14] A. Maiti, J. Casarona, L. Mchale, and P. Schaumont, "A largescale characterization of RO-PUF," in *Proc. IEEE Int. Symp. Hardw. Oriented Secur. Trust (HOST)*, Anaheim, CA, USA, Jun. 2010, pp. 94–99.
[15] A. Maiti and P. Schaumont, "Improved ring oscillator PUF: An FPGA-friendly secure primitive," *J. Cryptol.*, vol. 24, no. 2, pp. 375–397, Apr. 2011.
[16] W. Liu, Y. Yu, C. Wang, Y. Cui, and M. O'Neill, "RO PUF design in FPGAs with new comparison strategies," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, May 2015, pp. 77–80.
[17] J. D. J. Golic, "New methods for digital generation and postprocessing of random data," *IEEE Trans. Comput.*, vol. 55, no. 10, pp. 1217–1229, Oct. 2006.
[18] *7 Series FPGAs Configurable Logic Block User Guide*, Xilinx, San Jose, CA, USA, 2016.
[19] M. Dichtl and J. D. J. Golić, "High-speed true random number generation with logic gates only," in *Cryptographic Hardware and Embedded Systems (CHES)*, Vienna, Austria: Springer-Verlag, 2007, pp. 45–62.
[20] U. Guler, S. Ergun, and G. Dundar, "A digital IC random number generator with logic gates only," in *Proc. 17th IEEE Int. Conf. Electron., Circuits Syst.*, Dec. 2010, pp. 239–242.
[21] M. Dichtl, "Fibonacci ring oscillators as true random number generators—A security risk," IACR, Lyon, France, Tech. Rep. 2015/270, 2015.
[22] L. Matuszewski and M. Jessa, "An auxiliary source of randomness for combined TRNG based on ring oscillators," *Proc. Poznaskie Warsztaty Telekomunikacyjne*, Poznanń, Poland, 2011, pp. 1–4.
[23] T. Addabbo, A. Fort, M. Mugnaini, V. Vignoli, and M. Garcia-Bosque, "Digital nonlinear oscillators in PLDs: Pitfalls and open perspectives for a novel class of true random number generators," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, May 2018, pp. 1–5.
[24] T. Addabbo, A. Fort, R. Moretti, M. Mugnaini, V. Vignoli, and M. G. Bosque, "Lightweight true random bit generators in PLDs: Figures of merit and performance comparison," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, May 2019, pp. 1–5.
[25] (May 17, 2017). *PYNQ-Z2 Reference Manual V1.0*. [Online]. Available: https://d2m32eurp10079.cloudfront.net/Download/pynqz2_user_manual_v1_0.pdf
[26] *TPS65400 4.5- to 18-V Input Flexible Power Management Unit With PMBus/I2C Interface*. Accessed: Aug. 30, 2020. [Online]. Available: https://www.ti.com/lit/ds/symlink/tps65400.pdf
[27] R. Maes, "Physically unclonable functions: Constructions, properties and applications," Ph.D. dissertation, Dept. Elect. Eng., Katholieke Univ. Leuven, Leuven, Belgium, 2012.

MIGUEL GARCIA-BOSQUE was born in Zaragoza, Spain. He received the B.Sc., M.Sc., and Ph.D. degrees in physics from the University of Zaragoza, Zaragoza, in 2014, 2015, and 2019, respectively.

He is currently a member of the Group of Electronic Design, Aragon Institute of Engineering Research, University of Zaragoza. He has coauthored nine technical articles and more than 20 international conference contributions. He has participated in eight national and international research projects. His research interests include chaos theory, true random number generation, cryptography algorithms, and physically unclonable functions.

GUILLERMO DÍEZ-SEÑORANS was born in Huesca, Spain. He received the B.Sc. and M.Sc. degrees in physics from the University of Zaragoza, Zaragoza, Spain, in 2016 and 2017, respectively, where he is currently pursuing the Ph.D. degree with the Group of Electronic Design, Aragón Institute of Engineering Research. He has participated in five national research projects and coauthored two technical articles. His research interests include physically unclonable functions, cryptography, and physics of complex systems.

CARLOS SÁNCHEZ-AZQUETA was born in Zaragoza, Spain. He received the B.Sc., M.Sc., and Ph.D. degrees in physics from the University of Zaragoza, Zaragoza, in 2006, 2010, and 2012, respectively, and the Dipl.Ing. degree in electronic engineering from the Complutense University of Madrid, Madrid, Spain, in 2009. He is currently a member of the Group of Electronic Design, Aragon Institute of Engineering Research, University of Zaragoza. His research interests include mixed signal integrated circuits, high-frequency analog communications, and cryptography applications.

SANTIAGO CELMA was born in Zaragoza, Spain. He received the B.Sc., M.Sc., and Ph.D. degrees in physics from the University of Zaragoza, Zaragoza, in 1987, 1989, and 1993, respectively.

He is currently a Full Professor with the Group of Electronic Design, Aragon Institute of Engineering Research, University of Zaragoza. He has coauthored more than 100 technical articles and 300 international conference contributions. He is a coauthor of four technical books and the holder of four patents. He appears as a Principal Investigator in more than 30 national and international research projects. His research interests include circuit theory, mixed-signal integrated circuits, high-frequency communication circuits, wireless sensor networks, and cryptography for secure communications.