IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 19 February 2025, accepted 9 March 2025, date of publication 12 March 2025, date of current version 20 March 2025.

Digital Object Identifier 10.1109/ACCESS.2025.3550677

RESEARCH ARTICLE

Novel Machine Learning-Resistant RO-Based PUF Optimized for IoT Device Authentication

RAÚL APARICIO-TÉLLEZ, MIGUEL GARCIA-BOSQUE, GUILLERMO DÍEZ-SEÑORANS, AND SANTIAGO CELMA

Group of Electronic Design (GDE), I3A, University of Zaragoza, 50009 Zaragoza, Spain

Corresponding author: Raúl Aparicio-Téllez (r.aparicio@unizar.es)

This work was supported by the Agencia Estatal de Investigacion under Grant PDC2023-145838-I00 and Grant PID2023-150244OB-I00. The work of Raúl Aparicio-Téllez was supported by the Diputación General de Aragón (DGA) Fellowship.

ABSTRACT In this work, a novel Physically Unclonable Function (PUF) based on Generalized Galois Ring Oscillators (GenGAROs) optimized for IoT device identification purposes has been proposed and analyzed. A GenGARO is composed of a certain number of logic gates with up to two inputs connected in cascade so that one input corresponds to the output of the previous gate and the other to the output of the last one. The bias of the signal of these oscillators has been used to construct a GenGARO-PUF. Firstly, the combination of logic gates which optimize the response of the GenGARO-PUF in terms of identifiability has been studied. Once the optimal configuration of GenGARO has been found, a GenGARO-PUF of 11 Look-Up Tables (LUTs) has been implemented on FPGA and its properties have been analyzed and compared to a conventional RO-PUF implemented in the exact same locations of the FPGA and using the same hard constraints. The proposal of this work shows an average Inter-Hamming Distance (*HD*) of 49.9 % and an Equal Error Rate $EER = 1.52 \cdot 10^{-12}$ using 100-bit responses. The GenGARO-PUF has proven to outperform the conventional Ring Oscillator (RO) PUF in terms of spatial autocorrelation, uniqueness, uniformity, bit-aliasing, identifiability and resistance to modeling attacks. Furthermore, a 3-LUT GenGARO-PUF has been proposed maintaining the prediction accuracy of the 11-LUT GenGARO-PUF, and showing that a good identifiability can still be achieved using fewer resources of the FPGA.

INDEX TERMS Authentication, Galois Ring Oscillator, hardware security, identification, machine learning, physically unclonable function.

I. INTRODUCTION

The Internet of Things (IoT) has experienced a significant growth in recent years as many IoT devices are becoming part of our daily lives [1], [2]. This has entailed a tremendous advancement, but it has also brought along several security and privacy risks, especially in sensitive environments where it is crucial to maintain the confidentiality of the transmitted data [3], [4]. In these conditions, it is essential to develop new device authentication and identification methods which meet the security requirements while also being cost-effective and compatible with the limitation of resources required by IoT devices, giving birth to Physically Unclonable Functions (PUFs) [5].

A PUF is a physical entity that presents a challenge-response functionality reliant on the intrinsic properties of physical structures which are difficult to clone. This response is unique for each device, serving as its identifier (ID), much like fingerprints do in humans [6], [7]. These IDs can be used to create authentication protocols [8], [9], [10] that not only enhance the security of IoT systems but also reduce the cost of devices, as they avoid the need of storing secret information in Non-Volatile Memories (NVMs). In recent years, several PUF proposals have been already made [11], [12].

Authentication protocols can significantly increase the power consumption of IoT devices. Additionally, the development of new technologies and particularly the Machine

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

Learning (ML), has rendered many of the current IoT authentication and identification systems vulnerable. In this work, a novel architecture of PUF based on Galois Ring Oscillators has been proposed and implemented on FPGA. The main contributions of this work are:

1) A description of the effect of the architecture of the proposed oscillators and the position of the logic gates that contribute to improving the identifiability of a PUF based on these oscillators.
2) The proposal of a novel 11-Look-Up Table (LUT) digital oscillator which has proven to be optimal to implement a PUF, and another 3-LUT oscillator proposal with high identifiability, featuring lower power consumption in a minimal area, two key aspects of IoT environments.
3) An implementation of a PUF in FPGA based on this oscillators with high uniqueness, reproducibility, identifiability, bit-aliasing, uniformity, and no spatial autocorrelation, which also outperforms the conventional Ring Oscillator PUF (RO-PUF) properties. Furthermore, randomness, power and area consumption, as well as the high resistance of the proposal facing ML attacks is exhaustively analyzed. Later on, the resistance to the most common ML attacks in PUFs will be experimentally discussed.

This paper is organized as follows: Section II describes the background of the work; Section III defines some metrics used to determine the quality of a PUF; Section IV shows the implementation on FPGA of a novel oscillator proposed as source of entropy to construct a PUF with high identifiability; Section V and Section VI analyzes the quality of the PUF and compares it with other state-of-the-art PUFs; finally, conclusions are drawn in Section VII.

II. RELATED WORK

A. RO-PUF

Suh and Devadas [13] proposed a refined type of PUF which used the small variations of the oscillating frequency of identical oscillators implemented in different devices due to uncontrollable variations inherent to the manufacturing process. This PUF was named RO-PUF and, compared to other types of PUFs like the Arbiter PUF [14], it was simpler to implement in ASIC and FPGA. Furthermore, compared to other delay-based PUFs, RO-PUFs tend to present higher reliability and they are more suitable for secure processor designs. Regarding other types of PUFs such as SRAM-PUFs, they are more sensitive to environmental factors such as temperature and voltage variations. While SRAM-PUFs are highly resistant to modeling attacks, they tend to be vulnerable to cloning and invasive attacks. In that work, instead of using the frequency of ROs directly as the response of the PUF, the result of the comparison of pairs of frequencies (f_i, f_j) was used to generate the output bit b_{ij}. This comparison technique was named compensated measurement and made the response of the PUF more stable against changes in the operating environment (such as temperature or voltage).

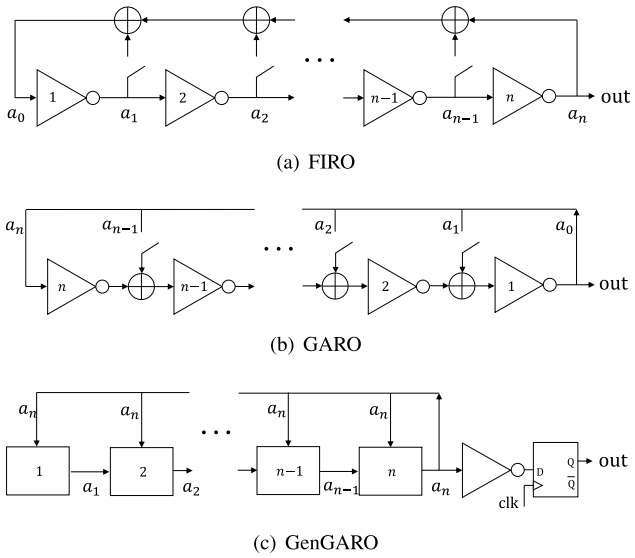


FIGURE 1. Architecture of FIRO, GARO and GenGARO.

Nowadays, this technique is widely used in different types of PUFs. However, if all possible comparisons are performed, correlations between bits of the response emerge. For example, let f_a, f_b and f_c be the frequencies of three oscillators a, b, c; if $f_a < f_b$ and $f_b < f_c$, then $f_a < f_c$. Typically, to avoid this, each oscillator is only used once: RO-1 is compared to RO-2, RO-3 with RO-4 etc. (non-overlapping comparison topology). This way, given N oscillators, $N/2$ independent bits can be easily extracted [13].

B. GARO-PUF AND FIRO-PUF

In [15], Golic introduced two novel techniques for True Random Number Generation (TRNG) based on asynchronous oscillating circuits with feedback, giving rise to Galois Ring Oscillators (GARO) and Fibonacci Ring Oscillators (FIRO). In both types of oscillators, some XOR gates are introduced between the feedback path of the oscillator and the input of some inverters, as it can be seen in Fig. 1(a) and Fig. 1(b).

Later, it was explored the possibility of using these oscillators initially proposed as TRNGs as PUFs. This way, Garcia-Bosque et al. [16] proposed a PUF based on GAROs (GARO-PUF). In this work, the authors compared the biases of GAROs implemented in FPGA in pairs to obtain the PUF response, similarly as it is done in conventional RO-PUFs. Furthermore, Matuszewski et al. [17] proposed a novel PUF based on FIROs, giving birth to the FIRO-PUF.

C. GENERALIZED GARO-PUF

Finally, in [18] the authors proposed a novel structure of oscillator inspired by GAROs which they called Generalized GAROs (GenGARO). This type of oscillator is formed by a certain number of logic gates, each one with up to two

inputs, connected in cascade. One of the inputs of each logic gate is the output signal of the previous logic operation while the other is the feedback signal, as it is shown in Fig. 1(c). Therefore, the first logic gate can perform two types of logic operations (DEL, NOT), while the rest can execute eight different logic operations (DEL, NOT, XOR, XNOR, AND, NAND, OR, NOR).

Additionally, a Flip-Flop (FF) is used to fix the value of the bit when measuring the bias of the output signal of the oscillator. The extra inverter is added before the FF to minimize possible frequency coupling effects. In their work, the authors used the oscillators to construct a GenGARO-PUF which, although presenting PUF-like characteristics, exhibited poorer uniqueness, reproducibility, and, consequently, lower identifiability compared to a conventional RO-PUF. It should be noticed that GenGAROs were only used as a proof of concept and therefore only small oscillators were used (less than 7 LUTs) while the analysis carried out by the authors seemed to indicate that better results could be obtained using larger oscillators. In this work, the use of optimized polynomials and larger oscillators (up to 11 LUTs) results in two new PUF configurations that exhibit significantly improved properties, including enhanced uniqueness and reliability. Additionally, in that work, the authors did not fix the routing of the oscillators to make them as identical as possible and they only fixed the LUT locations.

In Table 1,the comparison between this work and related works is summarized in terms of: (1) characteristics of the design, (2) implementation and analysis of the suitability of the proposal as PUF, and (3) obtained results.

TABLE 1. Comparison of this work to previous works using oscillators proposed by Golic (FIRO, GARO...) or derivatives. ?: not addressed in the work, ✓: made in the work, ×: not made, -: not applicable.

Description	[16]	[17]	[18]	This work
1. Design				
Type of oscillator	GARO	FIRO	GenGARO	GenGARO
Fixed routing	?	?	×	✓
GenGARO configured externally	-	-	×	✓
2. Implementation and analysis				
Analysis of suitability as PUF	✓	✓	✓	✓
Implementation in FPGA	✓	✓	✓	✓
Bit-aliasing/randomness analysis	×	×	×	✓
Modeling resistance analysis	×	×	×	✓
3. Results				
PUF proposal improves RO-PUF	×	×	×	✓
Low hardware alternative proposal	×	×	×	✓

Therefore, the main aim of this work is to find a configuration of logic operations to construct a PUF with optimal identifiability. Furthermore, the research seeks a configuration that minimizes spatial correlation of oscillators in FPGA and is resilient against the most common ML attacks.

III. PRELIMINARIES

In this section, the main metrics which are further used to determine the quality of the GenGARO-PUF are introduced.

A. SPATIAL AUTOCORRELATION

To measure spatial autocorrelation, Moran's I [19] and Geary's C [20] have been used as metrics. The former is used to measure the global spatial autocorrelation while the latter is more sensitive to local spatial autocorrelation. In a perfectly random pattern with no spatial autocorrelation, $I = 0$ and $C = 1$. However, $I > 1$ and $C < 1$ indicates a growing positive spatial autocorrelation, while $I < -1$ and $C > 1$ indicates a growing negative one.

B. UNIQUENESS

Analyzes whether the response generated by one device is different from the response generated by other devices. In this work, it has been measured with the Inter-chip Hamming Distance (HD) which compares the n-bit responses R_i and R_j obtained from two different devices $i \neq j$: $HD^{\text{inter}}_{i,j} = HD(R_i, R_j)$. The average HD^{inter} among k devices is defined as [21]:

$$\mu^{\text{inter}} = \frac{2}{k(k-1)} \sum_{i=1}^{k-1} \sum_{j=i+1}^{k} \frac{HD(R_i, R_j)}{n} \times 100\%. \quad (1)$$

Ideally, it should be 50 % on average. Ideally, before measuring a certain response in a device, the value of each bit in that response can be 0 or 1 with equal probability, regardless of the result obtained when measuring the response in other devices. If this condition is met, the Inter-HD will follow a binomial distribution with $p = 0.5$ [21].

C. REPRODUCIBILITY

Analyzes the ability of a device to always generate the same response. In this work, it has been measured with the Intra-chip HD which compares the n-bit responses R_i of device i measured at m different times t, t': $HD^{\text{intra}}_i = HD(R_i(t), R_i(t'))$. The average HD^{intra} is defined as:

$$\mu^{\text{intra}}_{\text{device } i} = \frac{2}{m(m-1)} \sum_{t=1}^{m-1} \sum_{t'=t+1}^{m} \frac{HD(R_i(t), R_i(t'))}{n} \times 100\%. \quad (2)$$

In some works, this definition slightly differs and tends to be confused with the Bit-Error Rate (BER), defined in (3), where the m iterations of responses $R_i(t)$ measured at different temperature and voltage conditions are compared with a single response $R_i(t')$ measured at nominal conditions. Ideally, both parameters should be 0 %.

In this work, μ^{intra} is used to estimate the reproducibility of the PUF at nominal conditions while BER is used to measure the PUF robustness facing voltage-temperature variations.

$$BER_{\text{device } i} = \frac{1}{m} \sum_{t=1}^{m} \frac{HD(R_i(t), R_i(t'))}{n} \times 100\%. \quad (3)$$

D. BIT-ALIASING

Bit-aliasing is a measure of the correlation of a given bit in the response across multiple devices. Given the l-th bit of a

response across k devices, the bit-aliasing of bit l is defined as [21]:

$$BA_{\text{bit } l} = \frac{1}{k}\sum_{i=1}^{k} r_{i,l} \times 100\%. \tag{4}$$

Ideally, bit-aliasing should be 50 % on average.

E. UNIFORMITY

The uniformity estimates how uniform the distribution of bits in the response of the PUF is. Given the n-bits $r_{i,l}$ of the PUF response, the uniformity of the response provided by device i is defined as [21]:

$$U_{\text{device } i} = \frac{1}{n}\sum_{l=1}^{n} r_{i,l} \times 100\%. \tag{5}$$

Ideally, uniformity should be 50 % on average.

F. IDENTIFIABILITY

In an identification system, it is evident that the probability of false rejections and false acceptances should be minimized. This is measured with the false rejection rate (*FRR*) and false acceptance rate (*FAR*) respectively. Both rates are estimated from the intra-chip *HD* distributions ($\hat{p}_P^{\text{intra}}$) and inter-chip *HD* ($\hat{p}_P^{\text{inter}}$):

$$FRR(t_{\text{id}}) = 1 - F_{\text{bino}}(\hat{p}_P^{\text{intra}}), \tag{6}$$

$$FAR(t_{\text{id}}) = F_{\text{bino}}(\hat{p}_P^{\text{inter}}) \tag{7}$$

where F_{bino} is the cumulative distribution function (CDF).

This way, given *FAR*, *FRR* and the identification threshold t, the equal error rate (*EER*) is defined as [6]:

$$EER = \max\{FAR(t_{EER}), FRR(t_{EER})\} \tag{8}$$

where $t_{EER} = \text{argmin}_t\{\max\{FAR(t), FRR(t)\}\}$. The lower *EER*, the better the PUF in terms of identifiability.

IV. PROPOSAL OF GENERALIZED GARO

First, we experimentally observed that larger oscillators (i.e., oscillator with a large number of stages) appeared to exhibit better properties. However, using oscillators with a large number of LUTs results in higher power and area consumption. For these reasons, we considered 11 LUTs to be an appropriate number of stages for each oscillator, as they can be implemented in exactly 3 slices, taking into account the final inverter, which was added to prevent potential frequency coupling effects. Second, regarding the order of the logic gates and the type of logic gates implemented at each position of the oscillator, an experimental process was carried out to determine which configurations are most suitable for constructing the PUF response. This process is explained in the following subsections.

A. PROPOSED OSCILLATOR

To obtain the configuration of GenGARO (where "configuration" is referred to the combination of logic operations in each LUT of the oscillator) which optimizes the PUF response in terms of identifiability, considering the time required to analyze each configuration and the impossibility of analyzing all the oscillator configurations that lead to an oscillating output in a reasonable amount of time, 72,000 configurations have been randomly generated.

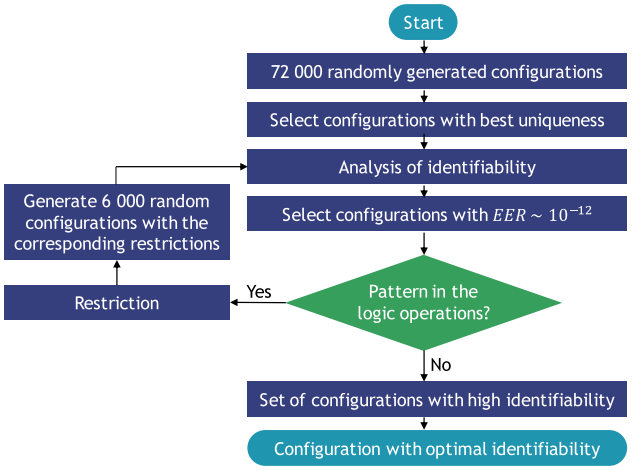
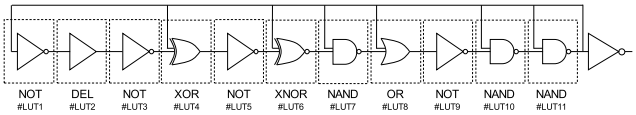
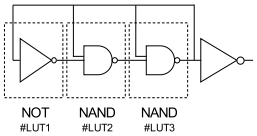


FIGURE 2. Process to obtain the configuration of GenGARO with optimal properties.



(a) 11-LUT



(b) 3-LUT

FIGURE 3. Configuration of 11-LUT and 3-LUT GenGAROs selected to construct a PUF with optimal identifiability.

Later, the identifiability of the configurations with the best uniqueness (i.e. configurations of oscillators with average Inter-*HD* in the interval [45, 55] %) has been analyzed. It was observed that the logic operations of the last LUTs were crucial to obtain a PUF with good properties. Therefore, the configurations have been randomly generated by applying successive restrictions to the logic operations of the LUTs. Subsequently, the patterns in the logic operations of the configurations with best identifiability have been analyzed, and successive restrictions have been applied to the last LUTs of the GenGAROs.

The process followed to obtain the configuration with optimal properties is summarized in Fig. 2.

1) Firstly, it has been observed that the configurations with {NAND,NAND} or {NAND,XOR} gates in the

last two LUTs {LUT_{10},LUT_{11}} lead to a PUF with high identifiability.
2) Secondly, among these configurations, it has been found that the best configurations presented a NOT gate in LUT_9.
3) Finally, applying these restrictions to the last three LUTs, it has been observed that the best configurations presented an OR gate in LUT_8. Other patterns have not been found in the rest of LUTs.

These results show that when these restrictions are applied to the last four LUTs of the 11-LUT GenGAROs, all resulting 6,000 configurations exhibit high identifiability with $EER \sim 10^{-11}$ or $EER \sim 10^{-12}$. Finally, among the 6,000 configurations generated with the described restrictions, the configuration of GenGARO with the lowest *EER* has been selected. This configuration, shown in Fig. 3, has been used to construct a 11-LUT GenGARO-PUF whose properties have been analyzed in Section V.

Therefore, since it is necessary to find a trade-off between the PUF being reliable and secure at the same time, the optimization has been performed in terms of the *EER*, a parameter that simultaneously combines the properties of uniqueness and reproducibility.

B. FPGA IMPLEMENTATION

To test this proposal, 200 11-LUT GenGAROs have been implemented in 40 Artix-7 FPGAs. LUTs in FPGA allow for flexibility and rapid testing of different configurations of GenGAROs. Rather than employing a limited number of devices to estimate the reproducibility and uniqueness of the PUF, this experiment has been conducted on a larger scale, simultaneously taking measurements across the 40 FPGAs. The bias of the oscillators has been compared using the non-overlapping comparison topology, thus obtaining 100-bit responses.

Each GenGARO has been implemented using three slices: LUTs A, B, C and D of slice X_iY_j; LUTs A, B, C, D of slice X_iY_{j+1}; and LUTs A, B and C of slice X_iY_{j+2}. The extra inverter has been implemented in LUT D of slice X_iY_{j+2}. The FF has been placed close to this inverter to avoid the degradation of the signal which could affect the bias of the oscillator. Furthermore, hard constraints have been applied to the location and routing of GenGAROs so that all of them are as identical as possible.

By using 11-LUT oscillators, each GenGARO will be limited to three slices, as the extra inverter would be implemented in LUT #12. This way, a large number of configurations can be achieved without using a high number of FPGA slices.

C. REDUCTION TO ONE SLICE

As it has been mentioned, the logic operations corresponding to the last LUTs of GenGAROs were found to be crucial to construct a PUF with good properties. Consequently, it has been studied the possibility of reducing the length of GenGAROs to one slice, thus reducing the number of CLBs used on the FPGA and improving the power consumption and area usage, two crucial aspects for IoT.

Consequently, in addition to 11-LUT GenGAROs, 3-LUT GenGAROs have been implemented on FPGA using only one slice per oscillator. The architecture of 3-LUT GenGARO correspond to the last three LUTs of 11-LUT GenGAROs {NOT, NAND, NAND}, as it can be observed in Fig. 3(b). This oscillator has been used to construct a 3-LUT GenGARO-PUF and its properties have been analyzed together with the properties of the 11-LUT GenGARO-PUF.

V. EXPERIMENTAL RESULTS

In this section, the quality metrics obtained for the 11-LUT and 3-LUT GenGARO-PUF are shown. To analyze the quality of the PUFs, 100 measurements of the bias/frequencies of 200 oscillators have been measured in 40 Artix-7 FPGAs.

The design has been synthesized and implemented using Vivado 2019.1. Synthesis has been performed using the *Vivado Synthesis Defaults (Vivado Synthesis 2019)* settings, while implementation has been performed using the *Vivado Implementation Defaults (Vivado Implementation 2019)* settings. In case the exact parameters used are not accessible, the authors are willing to provide these predefined parameters upon request.

Furthermore, the obtained results are compared to a conventional 11-LUT RO-PUF whose frequencies are compared using the same non-overlapping comparison topology, implemented in the exact same locations of the FPGA and using the same hard constraints as the 11-LUT GenGARO-PUF. The obtained parameters are summarized in Table 2. Given the considerable number of works included in the comparison, to facilitate a quick insight for the reader, in addition to indicating the numerical values of each quality metric, a color code has been used to qualitatively indicate how good each parameter is: green (good), yellow (acceptable), and orange (improvable).

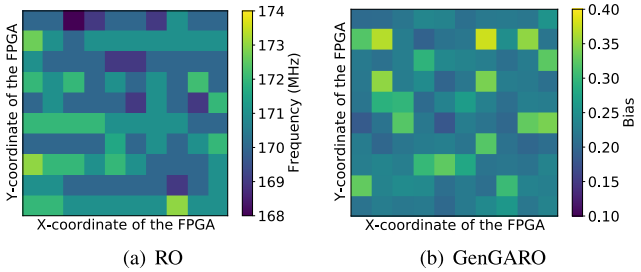
A. FREQUENCY/BIAS SPATIAL AUTOCORRELATION

Firstly, the correlation of the biases/frequencies of the oscillators within their location in the FPGA has been analyzed. In Fig. 4, a map of the frequencies and biases of the ROs and GenGAROs respectively within their location in the same FPGA is shown. In the case of the ROs, in the upper and right areas, the oscillators seem to tend to have a lower frequency. Furthermore, in Fig. 5, the values of Moran's I and Geary's C have been calculated for each PUF instance. In this figure, the existence of spatial correlation is clearly observed in the case of the RO-PUF, while its absence is noted for the GenGARO-PUF. As it can be seen, 11-LUT GenGAROs present almost no spatial correlation (average $\overline{I} = 0.01$ and $\overline{C} = 0.98$). However, 11-LUT ROs exhibit a certain positive spatial correlation ($\overline{I} = 0.63$, $\overline{C} = 0.38$), causing the oscillators located in the upper right corner of the FPGA to have lower frequencies than those in the lower left corner, as it can be seen in Fig. 4.

TABLE 2. Obtained quality metrics for 11-LUT and 3-LUT GenGARO-PUFs and comparison with other state-of-the-art PUFs. "RO" in the first row refers to a conventional 11-LUT RO-PUF implemented in the exact same locations and routing as 11-LUT GenGARO-PUF.

Property	Metric	11-LUT	3-LUT	RO	[22]	[23]	[24]	[25]	[26]	[27]	[28]
Year	-	**2024**	**2024**	2024	2022	2021	2020	2018	2018	2017	2013
Type of PUF	-	**GenGARO**	**GenGARO**	RO	XOR	DD	RO	RO	TERO	RO	RO
FPGA [a]	-	**A7**	**A7**	A7	A7	A7	A7	V5	S6	S6	S3
Uniqueness	$\mu^{\text{inter}}(\%)$	**49.89**	**48.94**	42.00	49.47	49.48	48.05	49.33	49.65	47.13	48.30
Reproducibility	$\mu^{\text{intra}}(\%)$ [b]	**1.68**	**2.37**	0.66	2.05	1.67	0.70	4.55	3.68	0.84	2.12
Uniformity	$d_{\text{K-S}}$, $\overline{U}$	**0.15**	**0.41**	0.25	-	50.59 [c]	-	49.50 [c]	-	50.61 [c]	51.80 [c]
Bit-Aliasing	$d_{\text{K-S}}$, $\overline{BA}$	**0.09**	**0.29**	0.33	-	-	-	-	-	-	50.13 [c]
Identifiability	$\sim EER_{100\text{-bit}}$ [d]	$\mathbf{10^{-12}}$	$\mathbf{10^{-11}}$	10^{-11}	10^{-11}	10^{-12}	10^{-13}	10^{-9}	10^{-10}	10^{-13}	10^{-11}
Modeling Resist.	-	**High**	**High**	Medium	-	-	Low	Medium [e]	Low	Medium [e]	Medium [e]
Response Length	-	**100**	**100**	100	128	128	128	136	128	256	283
Number of FPGAs [f]	-	**40**	**40**	40	16	16	217	1 (40) [g]	30	5	31

[a] A7: Artix-7, V5: Virtex-5, S6: Spartan-6, and S3: Spartan-3.
[b] In some works, to estimate μ^{intra} not all responses are compared to each other. Instead, the responses obtained in the different measurements are compared to a single response.
[c] These works estimate the bit-aliasing and uniformity using the average of the distributions $\overline{U}$ and $\overline{BA}$. However, it is not the best metric to measure these properties as it has been previously explained, and in this work $d_{\text{K-S}}$ is preferred.
[d] The length of the PUF response can significantly modify μ^{inter} and *EER*. In this work, the *EER* that each PUF would have if they generated 100-bit words has been estimated, maintaining the same μ^{inter} since there is no data on uniqueness for different lengths of the PUF response.
[e] In some works, Weak PUFs are considered to present a "High" resistance to modeling attacks. However, in RO-PUFs, if the index of the selected oscillators is used as challenge, the PUF behaviour presents lower resistance to these attacks.
[f] Number of FPGAs used for the evaluation of the PUF. In this work, all metrics have been calculated and averaged over 40 FPGAs. The number of FPGAs used can greatly worsen the μ^{intra} estimation.
[g] The PUF is implemented in one "Virtex-5 FPGA which is divided into 40 areas to simulate 40 FPGAs".



(a) RO (b) GenGARO

FIGURE 4. Spatial distribution of the frequencies and biases of the ROs and GenGAROs respectively in the FPGA.

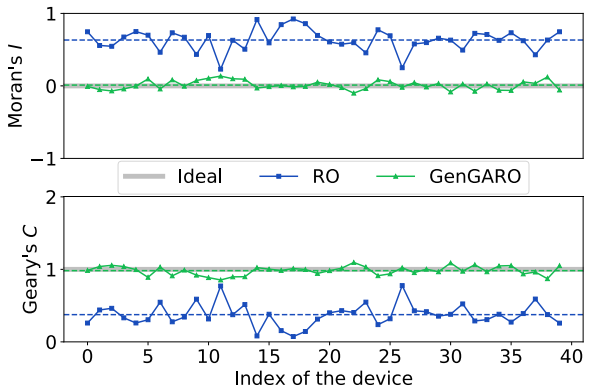


FIGURE 5. Values of Moran's *I* and Geary's *C* for each PUF instance for the frequencies/biases of the oscillators. The dashed green line corresponds to the ideal values that would be obtained if there would be no spatial autocorrelations. The dashed blue line is the experimental average.

Therefore, by measuring the bias of the GenGAROs instead of directly using the frequencies of ROs, the effect of spatial correlation of the oscillators in the FPGA is nearly completely eliminated. Similarly, no spatial correlation in the bias of the oscillators is observed using 3-LUT GenGAROs. This allows fewer restrictions when selecting the challenges of the PUF. Additionally, it also hints at the low predictability of the GenGARO-PUF facing ML attacks.

B. UNIQUENESS

In Fig. 6, the Inter and Intra-*HD* distributions for the proposed 11-LUT GenGARO-PUF and 11-LUT RO-PUF are shown together with the parameters p and n obtained in the binomial fit of the distributions. As it can be seen, while the RO-PUF presents a poor $\mu^{\text{inter}} = 42.0\,\%$, the 11-LUT GenGARO-PUF present an almost perfect uniqueness with $\mu^{\text{inter}} = 49.9\,\%$. Consequently, the 11-LUT GenGARO-PUF improves by up to 8 percentage points the uniqueness of a RO-PUF implemented in the exact same locations.

Similarly, using the 3-LUT GenGARO-PUF, a high uniqueness is still observed with $\mu^{\text{inter}} = 48.9\,\%$. It must be noticed that in this work, an exactly identical routing

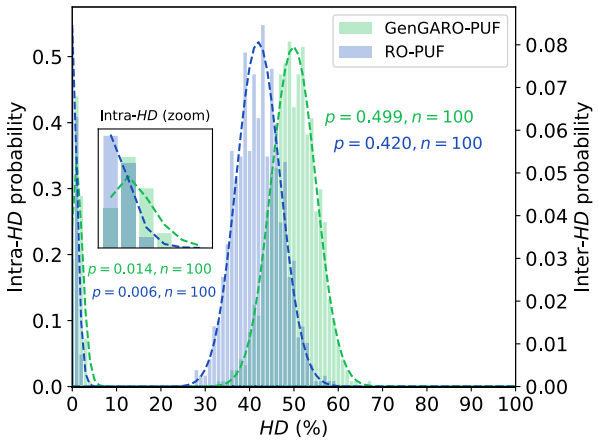


FIGURE 6. Intra and Inter-*HD* distributions for the 11-LUT GenGARO-PUF and RO-PUF.

for all oscillators has been used while other works simply fix the location of the LUTs but the routing is performed automatically. This could negatively affect the uniqueness of the RO-PUF but it should be considered that the obtained reproducibility is extremely low compared to other RO-PUFs. Consequently, while a better uniqueness could be achieved, it would be at the expense of worsening reproducibility and, effectively, a similar identifiability would be obtained.

C. REPRODUCIBILITY

In terms of reproducibility, the RO-PUF presents a low $\mu^{\text{intra}} = 0.66\,\%$. The proposed 11-LUT GenGARO-PUF presents worse reproducibility with a slightly higher $\mu^{\text{intra}} = 1.68\,\%$. However, in both cases a high reproducibility is obtained. Using the 3-LUT GenGARO-PUF the reproducibility is slightly worsened with $\mu^{\text{intra}} = 2.37\,\%$. It must be noticed that all metrics have been obtained averaging over 40 FPGAs.

To be use for device identification purposes, a PUF must exhibit simultaneously good reproducibility and good uniqueness. As it can be seen in Table 2, the proposed PUF achieves a better trade-off between both properties compared to other PUFs in the literature.

D. IDENTIFIABILITY

Therefore, given the Intra and Inter-*HD* distributions, *FAR* and *FRR* curves have been calculated and the *EER* has been obtained. Firstly, using the conventional 11-LUT RO-PUF, an identifiability of $EER\,(t_{EER} = 11) = 1.07 \cdot 10^{-11}$ is obtained.

Secondly, using the 3-LUT GenGARO-PUF, the identifiability is worsened ($EER\,(t_{EER} = 16) = 2.26 \cdot 10^{-11}$) with the advantage that is uses much less resources and presents a lower spatial correlation so it is more difficult to attack using modeling attacks as it is further shown.

Thirdly, using the 11-LUT GenGARO-PUF, the identifiability is improved by one order of magnitude ($EER\,(t_{EER} = 17) = 1.52 \cdot 10^{-12}$) so it is more suitable to be used for device identification purposes compared to the conventional RO-PUF. As this parameter determines the probability that an identification attempt results in a false rejection and false acceptance, it has also been calculated for other PUFs in the state of the art, as it is shown in Table 2.

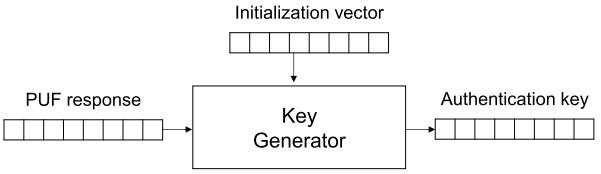


FIGURE 7. Possible key generation for authentication scheme using Weak PUF response as "seed" of a block cypher encryption. The PUF could also be used as a key in a cryptosystem.

However, it could be also be considered the implementation of an authentication scheme based on this Weak PUF. This way, in this hypothetical authentication scheme, the PUF response would be used as ''seed''. This ''seed'' would be introduced along with an initialization vector into a cryptographic module, so that a potential attacker could only read the output of the cryptographic block and would not have access to the PUF response (''seed''). Furthermore, the PUF could also be used as the key in a cryptosystem. In Figure 7, it is shown how this hypothetical authentication scheme would look. The analysis in this paper has focused on identification, which is related to authentication in most protocols.

E. BIT-ALIASING

It should be noticed that the mean value of bit-aliasing is not an adequate measure to determine bit-aliasing since a distribution could have an ideal mean bit-aliasing of 50 % and still have some positions within the responses that always tend to be 1 and other positions that always tend to be 0. Therefore, the obtained distributions have been compared to the bit-aliasing distribution obtained with a PUF constructed with 40 100-bits responses randomly generated.

To compare the experimental distributions with the expected distribution, the Kolmogorov-Smirnov Distance ($d_{\text{K-S}}$) is used. This parameter allows quantifying the similarity between an experimental and a theoretical distribution. The lower $d_{\text{K-S}}$, the more similarity exists between both distributions. The greatest distance has been obtained for the conventional 11-LUT RO-PUF ($d_{\text{K-S}} = 0.33$), while for the 11-LUT GenGARO-PUF, a considerably lower value has been obtained ($d_{\text{K-S}} = 0.09$). It is worth noticing that with the 3-LUT GenGARO-PUF a higher distance ($d_{\text{K-S}} = 0.29$) is obtained compared to the initially-proposed 11-LUT GenGARO-PUF. This indicates that the bit-aliasing distribution for the 11-LUT GenGARO-PUF is more similar to the ideal distribution than the distribution of the conventional RO-PUF.

Therefore, the proposal also outperforms the RO-PUF in terms of bit-aliasing. In Fig. 8, the bit-aliasing distributions

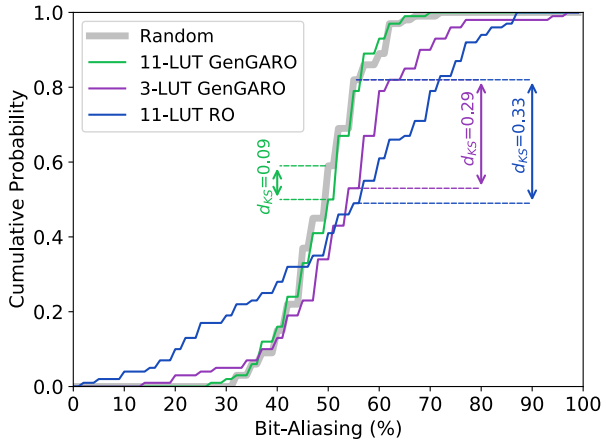


FIGURE 8. Bit-Aliasing distributions for 11-LUT GenGARO-PUF and RO-PUF, and 3-LUT GenGARO-PUF.

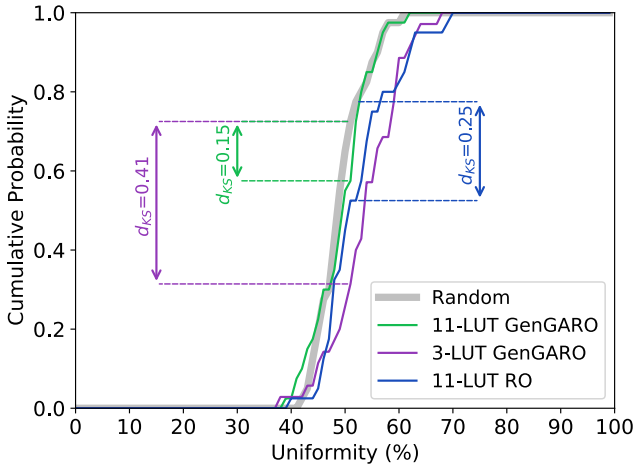


FIGURE 9. Uniformity distributions for 11-LUT GenGARO-PUF and RO-PUF, and 3-LUT GenGARO-PUF.

together with their corresponding Cumulative Distributions Functions (CDFs) are shown for the analyzed PUFs.

F. UNIFORMITY

Next, an analysis similar to the presented in the previous section has been carried out. In terms of uniformity, the greatest distance is obtained for the 11-LUT RO-PUF ($d_{\text{K-S}} = 0.25$), while the 11-LUT GenGARO-PUF presents the smallest distance ($d_{\text{K-S}} = 0.15$). Therefore, the proposed 11-LUT GenGARO-PUF also succeeds in improving the uniformity compared to a conventional RO-PUF.

In Fig. 9, the uniformity distributions together with their corresponding CDFs are shown for the analyzed PUFs. It is worth noticing that the worst uniformity is obtained with the 3-LUT GenGARO-PUF ($d_{\text{K-S}} = 0.41$).

G. RANDOMNESS

To evaluate the randomness of the responses of the proposed PUF, some tests provided by NIST statistical test suite have been used, specifically the NIST SP 800-22 test [29].

TABLE 3. Result of a subset of NIST SP 800-22 test passed for 11-LUT and 3-LUT GenGARO-PUFs responses. To consider that the tests have been passed with a significance level of $\alpha = 0.01$, the proportion of sequences that must pass the tests is 37 out of 40.

Test	11-LUT		3-LUT	
	P-val	Prop.	P-val	Prop.
1. Frequency Monobit	0.276	40/40	0.004	40/40
2. Block Frequency	0.350	39/40	0.941	40/40
3. Runs	0.312	40/40	0.485	40/40
12. Approximate entropy	0.911	40/40	0.568	40/40
13. Cusum (forward)	0.002	40/40	0.004	40/40
13. Cusum (reverse)	0.122	40/40	0.135	40/40

In this work, a subset of tests has been chosen since, as mentioned in [26], these are tests that can be performed using data of reduced length, as is the case here, since we only have 100-bit responses from 40 different FPGAs. Therefore, the following tests have been conducted: *1. Frequency (Monobit) Test, 2. Frequency Test within a Block, 3. Runs Test, 12. Approximate Entropy Test,* and *13. Cumulative Sums (Cusum) Test.*. It should be noted that the *Frequency (Monobit) Test* would correspond to the uniformity of the PUF. However, in this work, the uniformity property is still maintained, as it is a standard property that appears in many works on PUFs with the aim of comparing with other state-of-the-art PUFs.

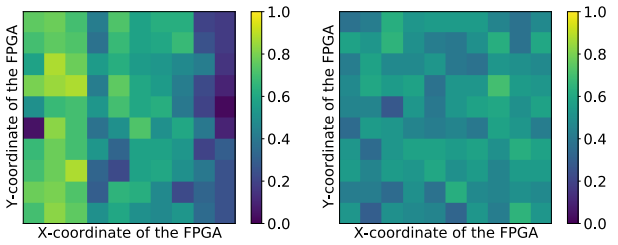
Additionally, in tests 2 and 12, the size of the bit subblocks must be selected. Regarding the subblock size M in test 2, taking into account the recommendations specified in [29], $M = 20$ has been selected. Similarly, regarding test 12, a block size of $M = 1$ has been used.

In [26], the *Test for the Longest Run of Ones in a Block* is also performed, where the block size is predetermined based on the length of the response, such that the response must be at least 128 bits long. Since in this case, the responses are 100 bits long, this test has not been conducted.

In Table 3, the P-value obtained for each of the NIST tests conducted on the 3-LUT and 11-LUT GenGARO-PUF are shown. Additionally, the number of sequences (proportion) that passed the tests is also displayed. For a sample size of 40 binary sequences, the minimum pass rate for each statistical test conducted is 37 with the selected level of significance (α=0.01, in this case). Furthermore, as it is explained in [25] , "based on χ^2 Goodness-of-Fit Test, the underlying distribution is deemed uniform if the P-value of the P-values is equal or greater than 0.0001". This is also explained in Section 4.2.2. of [29]. Therefore, it can be considered that the sequences from both PUFs pass the tests.

H. BIT SPATIAL AUTOCORRELATION

To obtain the response of a RO-based PUF, the frequencies/biases of oscillators located close in the FPGA are compared. Consequently, for each pair of oscillators and location of the FPGA, a bit of the response of the PUF can be assigned. Furthermore, in Fig. 10 the bit maps obtained



(a) RO-PUF (b) GenGARO-PUF

FIGURE 10. Spatial distribution of the bits of the response of the 11-LUT RO-PUF and GenGARO-PUF in multiple FPGAs.

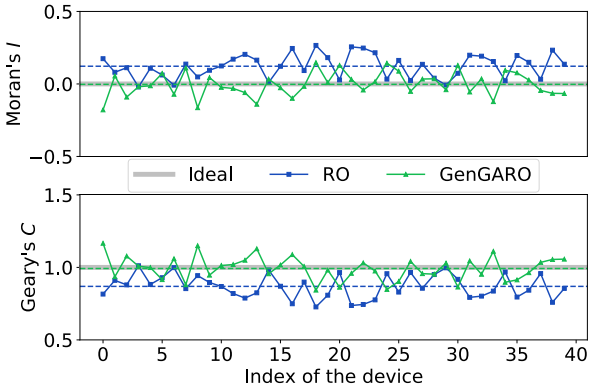


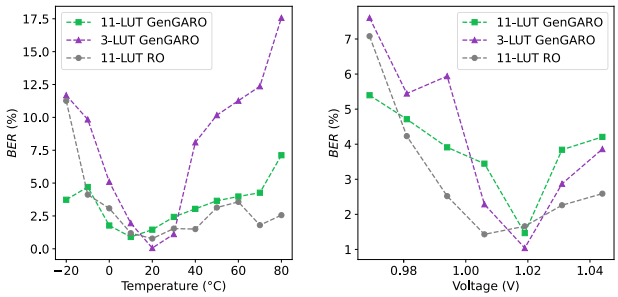
FIGURE 11. Values of Moran's *I* and Geary's *C* for each PUF instance using the 11-LUT RO-PUF and GenGARO-PUF responses. The dashed lines correspond to the average values.

for 40 FPGAs have been averaged. It is important to note that in this figure it is being represented the spatial correlation of the bits of the PUF response, so what is being calculated is the spatial correlation of 100 points that can only take the values 0 or 1.

As it can be seen in Fig. 10(a), the response bits of the RO-PUF also present a certain spatial autocorrelation in the FPGA (in the right area of the FPGA there are more 0's than in the left). This is corroborated using the Geary's and Moran's indexes, thus obtaining $\overline{I} = 0.14$, $\overline{C} = 0.86$.

It should be noticed that this is a consequence of the spatial autocorrelation of the frequencies of the oscillators in the FPGA. Furthermore, in this map the effect of bit-aliasing can also be appreciated as it is observed that when performing the average of the responses of several devices, there are still some bits fixed to 0 or 1. On the other hand, as it can be seen in Fig. 10(b), the response bits of the 11-LUT GenGARO-PUF present no spatial autocorrelation within the FPGA. Again, no spatial autocorrelation is observed as it is corroborated with the values of Moran's I and Geary's C: $\overline{I} = -0.07$, $\overline{C} = 1.06$.

Similarly, no spatial autocorrelation is observed using the 3-LUT GenGARO-PUF ($\overline{I} = -0.02$, $\overline{C} = 1.01$). Furthermore, no bit-aliasing effect is observed. In Fig. 11, the



(a) Temperature variations (b) Voltage variations

FIGURE 12. *BER* facing variations in the operating environment.

values of Geary's C and Moran's I for the 11-LUT RO-PUF and GenGARO-PUF are shown for each PUF instance.

I. ROBUSTNESS TO VOLTAGE-TEMPERATURE VARIATIONS

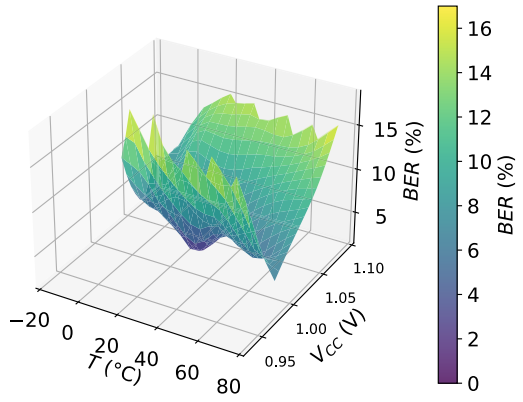
Subsequently, the stability of the proposed GenGARO-PUFs facing changes in the operating environment such as temperature and supply voltage variations has been analyzed. With this purpose, 100 responses of the 11-LUT and 3-LUT GenGARO-PUFs have been generated at different temperatures and voltages. Furthermore, the *BER* has been calculated for each temperature and voltage with respect to the response obtained at nominal conditions.

Facing temperature variations, it can be seen in Fig. 12 that the *BER* increases as the temperature deviates from the nominal value (20 ° C). However, in almost all cases it remains low. However, for the 3-LUT GenGARO-PUF, a greater variation of *BER* is observed in the range of temperatures analyzed.

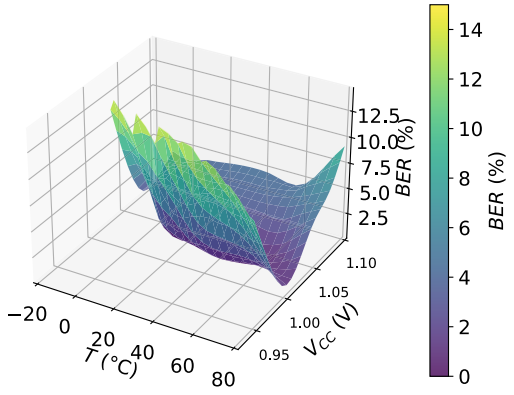
Similarly, facing voltage variations, the *BER* increases as the supply voltage is far from the nominal value. Furthermore, in all cases the obtained *BER* remains below the identification threshold showing that the proposed PUF still presents the properties of identifiability obtained in the studied range. A similar behavior is observed for the 3-LUT GenGARO-PUF.

Firstly, the temperature and supply voltage of the FPGA were simultaneously varied, and the $BER(T, V_{CC})$ value was obtained for each temperature T of the thermal chamber and voltage V_{CC} of the FPGA. The 3D surface obtained for the 11-LUT GenGARO-PUF is shown in Figure 13(a) , and the results obtained for the 3-LUT GenGARO-PUF are shown in Figure 13(b). Once again, it can be observed that points closest to ($T = 20$°C, $V_{CC} = 1.02$) exhibit a lower *BER*, which increases as the points move away from this location.

Secondly, the variation of the average Intra-*HD* for each temperature and FPGA supply voltage has been studied. The temperature results are shown in Fig. 14(a). As observed, all average Intra-*HD* for both the 11-LUT GenGARO-PUF and the 3-LUT GenGARO-PUF remain below 4 %. It can also be observed that for almost all temperatures, the

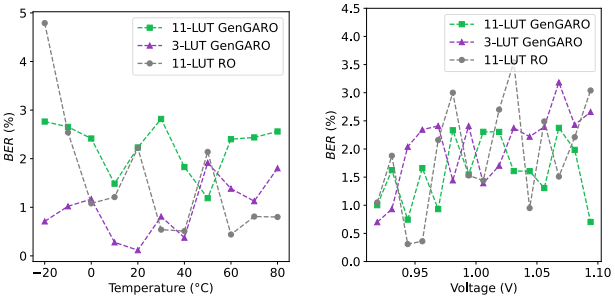


(a) 11-LUT



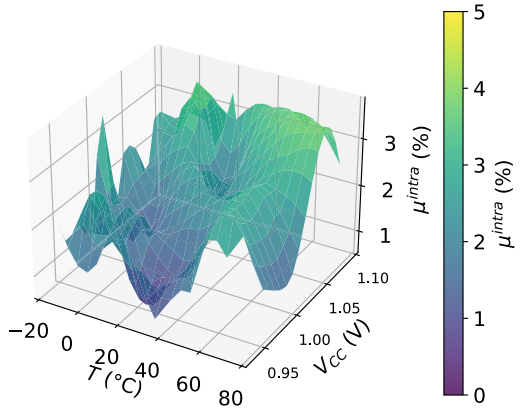
(b) 3-LUT

FIGURE 13. Bit Error Rate (*BER*) in % with respect to the golden key measured at $T = 20°C$ and $V_{CC} = 1.02$ for each temperature and voltage of the FPGA.

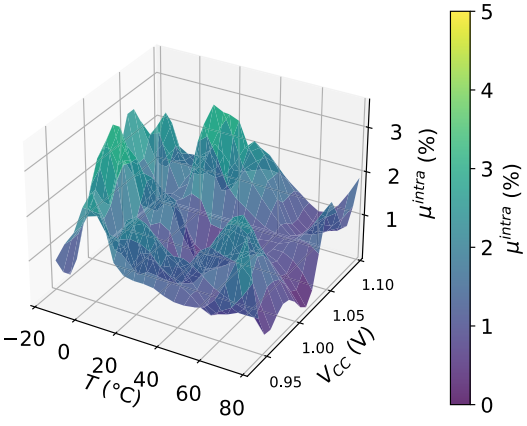


(a) Temperature variations (b) Voltage variations

FIGURE 14. μ^{intra} facing variations in the operating environment.



(a) 11-LUT



(b) 3-LUT

FIGURE 15. Average Intra-*HD* in % with respect to the golden key measured at $T = 20°C$ and $V_{CC} = 1.02$ for each temperature and voltage of the FPGA.

3-LUT GenGARO-PUF tends to exhibit better μ^{intra} than the 11-LUTs.

Furthermore, in the worst-case scenario, a high identifiability with an $EER \sim 10^{-10}$ would be achieved. Similarly, Fig. 14(b) shows the voltage results. Again, the Intra-*HD* does not exceed 4 % for any supply voltage. In this case, both the 3-LUT and 11-LUT GenGARO-PUF exhibit a more similar behavior. However, it can be observed that at high voltages, the 3-LUT GenGARO-PUF tends to show a slightly higher average Intra-*HD*. Additionally, in the worst-case scenario, the GenGARO-PUF would also achieve high identifiability with an $EER \sim 10^{-10}$.

Finally, the three-dimensional surface of the average Intra-*HD* has also been obtained under simultaneous changes in temperature and the FPGA supply voltage. The results obtained for the 11-LUT GenGARO-PUF are shown in Figure 15(a) while those for the 3-LUT are shown in Figure 15(b). For the 3-LUT, in the worst case, an $\mu^{\text{intra}} = 3.55$ % would be obtained, while for the 11-LUT it would be $\mu^{\text{intra}} = 3.80$ %.

In Figures 12 and 14, the curves obtained for the conventional 11-LUT RO-PUF are also shown. As can be seen, a similar behavior to the GenGARO-PUF is observed, both under temperature changes and changes in supply voltage. However, as analyzed in previous sections, the GenGARO-PUF presents better properties of uniqueness, uniformity, bit-aliasing, identifiability, spatial correlation, etc.

J. RESISTANCE TO ML ATTACKS

Finally, the resistance of the proposed 3-LUT and 11-LUT GenGAROs to ML Attacks has been analyzed. Typically, ML resistance is only analyzed only for Strong PUFs. While the proposed PUF is a Weak PUF, the goal of the analysis is to demonstrate that it is more robust than the conventional RO-PUF facing these types of attacks. This way, ML is used in this work to demonstrate that the PUF response cannot be modeled based on a certain subset of oscillator biases, unlike what happens with the conventional RO-PUF given a subset of the frequencies of the ring oscillators.

As the proposal is a Weak PUF, it only has one Challenge-Response Pair (CRP) per device. However, to study the robustness to ML Attacks, a scheme with several CRPs is needed [30]. Therefore, to perform this analysis an alternative scheme has been used. In this case, the selection of a pair of oscillators is used as a challenge and the result of this comparison is used as (1-bit) response.

To generate the database used as input of the ML algorithms, three parameters have been used: index of the device k, index of the first oscillator i and index of the second oscillator j used to obtain the output bit b_{ij}^k. From the 200 GenGAROs, 100 pairs of oscillators have been randomly chosen in a ''non-overlapping'' manner, that is, each oscillator has been used in only one comparison.

To test the proposal, five different algorithms [31] have been performed: Decision Tree (DT), Random Forest (RF) with 100 trees to improve stability and prediction accuracy, K-Nearest Neighbor (KNN) with $k = 1$, Support Vector Machine (SVM) using Radial Basis Function (RBF) kernel, and a Multilayer Perceptron (MLP) with two hidden layers of size 100 and 50 using each one the ReLu activation function, and a final layer with one output corresponding to the probability of the output bit to be '1'. and sigmoid activation function. It is evident that the probability of the output bit to be '0' will be the opposite.

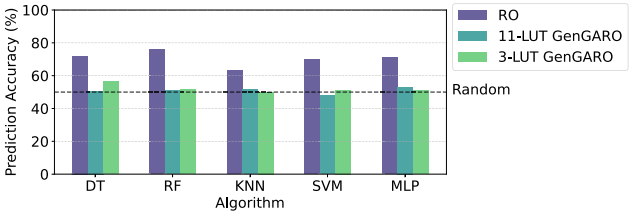
To perform the optimization, the Adam Optimizer has been used [32]. All algorithms have been implemented on Google Colab, which allows programming and executing code in Python. A total of 3500 CRPs have been generated. Of the total dataset, 2975 CRPs (85%) have been used as training data while 525 CRPs (15%) have been used as validation data. To compare the oscillators and generate the output bit b_{ij}^k for each $\{i, j, k\}$, two approaches have been followed: random selection and selection of oscillators located close in the FPGA. In addition, the Early Stopping functionality has been implemented to stop training the model if it does not improve after a certain number of ''epochs''. This way, the point at which the model starts to overfit can be identified and prevented from continuing.

In Table 4 and Figure 16, the prediction accuracy obtained with the GenGARO-PUF and the RO-PUF implemented in the exact same locations of the FPGA is shown. As it can be seen, the prediction accuracy obtained for the conventional RO-PUF using random comparisons is approximately 63-76 %. However, the prediction accuracy for the GenGARO-PUF is 47-54 %, which is the expected accuracy from random uniform bit choice, improving by 11-25 percentage points the values of the accuracy obtained with the conventional RO-PUF. This indicates that it is approximately capable of predicting half of the comparisons. Since the output of the algorithm can only be 0 or 1, a 50% prediction rate suggests that the output is highly resistant to prediction, making it effectively impossible for ML algorithms to predict the response of the GenGARO-PUF.

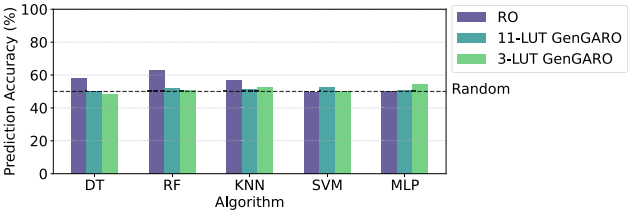
In a second experiment, instead of choosing the 100 pairs ''randomly'', we have chosen 100 pairs of ''close oscillators'' (i.e., oscillators within each pair are neighbors). This way, the effect of the correlated intra-die variation is mitigated, so a reduction in the prediction accuracy would be expected.

TABLE 4. Prediction accuracy of the attack of different algorithms on the RO-PUF tested in Table 2, 11-LUT and 3-LUT GenGARO-PUF.

Algorithm	Prediction Accuracy (%)					
	Random selection			Close oscillators		
	RO	11-LUT	3-LUT	RO	11-LUT	3-LUT
DT	72.00	50.67	56.38	57.90	49.90	48.57
RF	75.81	50.86	51.43	62.67	51.81	50.86
KNN	63.24	51.62	50.10	56.76	51.43	52.76
SVM	69.71	47.89	51.24	49.76	52.57	50.10
MLP	70.86	53.14	50.86	50.10	50.67	54.48



(a) Random selection

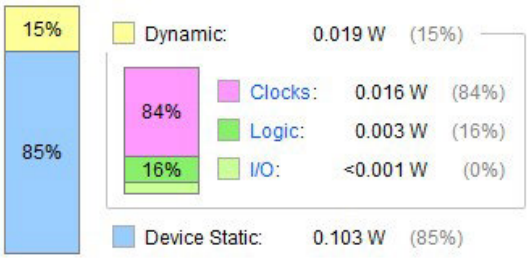


(b) Close oscillators

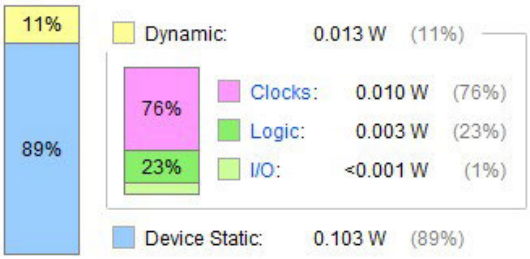
FIGURE 16. Prediction accuracy of the attack of different algorithms on the RO-PUF tested in Table 2, 11-LUT and 3-LUT GenGARO-PUF.

K. AREA AND POWER OVERHEAD

Finally, the area and power consumption has been analyzed. It is important to note that in the literature there is no consensus or standardized method for estimating the hardware overhead and power of a design. In Figure 17, the power consumption reports generated by Vivado of a design containing only the PUF primitive are shown. The power report has been generated opening the implemented design and navigating



(a) 11-LUT GenGARO-PUF



(b) 3-LUT GenGARO-PUF

FIGURE 17. Estimation of the post-implementation power consumption by Vivado for the design with the PUF primitive.

TABLE 5. FPGA utilization resources of the design containing the PUF primitive for 11-LUT and 3-LUT GenGARO-PUF.

Resource	Utilization	
	11-LUT	3-LUT
LUT	2793 (5.25%)	1166 (2.19%)
LUTRAM	-	-
FF	4200 (3.95%)	4200 (3.95%)
IO	1 (0.80%)	1 (0.80%)
BUFG	1 (3.13%)	1 (3.13%)

to Reports > Report Power in the Vivado 2019.1 version. Predefined settings have been used regarding the environment and power supply options used to generate the report. The authors are willing to provide the exact values used to generate these reports upon request.

If we look at the static consumption, which corresponds to the design itself, it is observed that the highest consumption is due to the clock signal. However, if we focus on the logic consumption, it is 3 mW in both cases, for the 3-LUT and the 11-LUT GenGARO-PUF. This is because the largest contribution to consumption comes from the registers used to store the bias values of the oscillators, which are the same for both cases. The fundamental difference will therefore lie in the occupied area.

Finally, Table 5 shows the FPGA resources used for each of the two designs. The flip-flops (FF) used are the same since both designs have the same number of oscillators. The difference lies in the number of LUTs used, as one design employs oscillators with 3 logic gates, while the other uses oscillators with 11 logic gates.

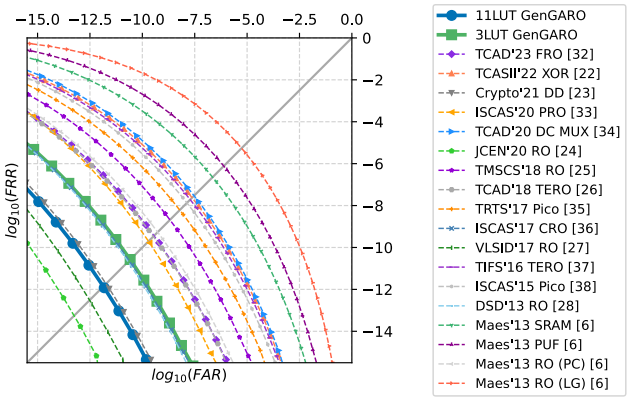


FIGURE 18. Identifiability ROC for the proposed PUFs compared to other state-of-the-art PUFs if 100-bit responses were used.

VI. COMPARISON WITH OTHER STATE-OF-THE-ART PUFS

Firstly, the identifiability of the proposed PUF architectures has been compared to the identifiability of other state-of-the-art PUFs. As the length of the response affects the *EER* of the PUF, to make a fair comparison between the proposed PUF and other state-of-the-art PUFs, the identifiability ROC curves have been calculated supposing that 100-bit responses have been used.

The obtained ROC curves are shown in Fig. 18. As it can be seen, the 11-LUT GenGARO-PUF presents a low *EER* ($EER = 1.52 \cdot 10^{-12}$) i.e. a high identifiability compared to PUFs of other works. Moreover, the 3-LUT GenGARO-PUF also presents high identifiability ($EER = 2.66 \cdot 10^{-11}$) while using fewer resources.

The proposed PUF architecture has been compared to other state-of-the-art FPGA-based Weak PUFs [22], [23], [24], [25], [26], [27], [28], [40], [41]. The comparison, outlined in Table 2, highlights several key findings. Firstly, the 11-LUT GenGARO-PUF shows better reproducibility, uniformity, and bit-aliasing compared to the 3-LUT GenGARO-PUF. Furthermore, the 11-LUT GenGARO-PUF has better uniqueness, uniformity, bit-aliasing, frequency spatial autocorrelation, bit spatial autocorrelation, and resistance against ML attacks compared to the conventional RO-PUF.

Compared to other PUFs in the literature [22], [23], [24], [25], [26], [27], [28], while it is true that some properties of other PUFs might be occasionally better than GenGARO-PUF, the PUF proposal of this work is the one that concurrently exhibits good uniqueness, reproducibility, identifiability, uniformity, bit-aliasing, spatial autocorrelation and resistance against modeling attacks when compared to the others. The key to this PUF proposal compared to others is that it can maintain high identifiability while providing a response that is nearly unpredictable with ML attacks.

VII. CONCLUSION

In this work, a novel architecture of GenGARO-PUF with optimal properties has been proposed, implemented and

analyzed. This type of oscillator is based on replacing each of the LUTs of a GARO with any logical function of up to two inputs.

As it has been shown, the proposed GenGARO-PUF presents lower spatial correlation of the oscillators and the bit responses on FPGA, better uniqueness, bit-aliasing and uniformity, and higher resistance to ML attacks compared to a conventional RO-PUF implemented in the exact same locations of the FPGA and using the same hard constraints. With respect to other PUFs in the literature [22], [23], [24], [25], [26], [27], [28], the proposal of this work demonstrates a remarkable uniqueness, reproducibility, and resistance against modeling attacks compared to the rest.

Furthermore, the 3-LUT GenGARO-PUF demonstrates significant advantages in terms of resource efficiency compared to the 11-LUT GenGARO-PUF, making it particularly well-suited for resource-constrained IoT environments. Its minimal area requirements provide a compelling case for its adoption in practical IoT applications where both security and efficiency are critical.

These results highlight that the proposed GenGARO-PUF exhibits optimal properties for device identification purposes. Future lines of research would involve to extend this analysis to other devices and manufacturers and exploring the use of GenGAROs to construct a Strong PUF.

REFERENCES

[1] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, Sep. 2013.

[2] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Context aware computing for the Internet of Things: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 414–454, 1st Quart., 2014.

[3] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019.

[4] F. A. Alaba, M. Othman, M. Hashem, and F. Alotaibi, "Internet of Things security: A survey," *J. Netw. Comput. Appl.*, vol. 88, pp. 10–28, Apr. 2017.

[5] A. Babaei and G. Schiele, "Physical unclonable functions in the Internet of Things: State of the art and open challenges," *Sensors*, vol. 19, no. 14, p. 3208, Jul. 2019.

[6] R. Maes, *Physically Unclonable Functions: Constructions, Properties and Applications*. Berlin, Germany: Springer, 2013.

[7] C. Bhm and M. Hofer, *Physical Unclonable Functions in Theory and Practice*. Cham, Switzerland: Springer, 2012.

[8] S. Roy, D. Das, A. Mondal, M. H. Mahalat, B. Sen, and B. Sikdar, "PLAKE: PUF-based secure lightweight authentication and key exchange protocol for IoT," *IEEE Internet Things J.*, vol. 10, no. 10, pp. 8547–8559, May 2023.

[9] M. Ebrahimabadi, M. Younis, and N. Karimi, "A PUF-based modeling-attack resilient authentication protocol for IoT devices," *IEEE Internet Things J.*, vol. 9, no. 5, pp. 3684–3703, Mar. 2022.

[10] F. Farha, H. Ning, K. Ali, L. Chen, and C. Nugent, "SRAM-PUF-based entities authentication scheme for resource-constrained IoT devices," *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5904–5913, Apr. 2021.

[11] J. Liu, Y. Zhao, Y. Zhu, C.-H. Chan, and R. P. Martins, "A weak PUF-assisted strong PUF with inherent immunity to modeling attacks and ultra-low BER," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 69, no. 12, pp. 4898–4907, Dec. 2022.

[12] Y. Shifman, A. Miller, O. Keren, Y. Weizman, and J. Shor, "An SRAM-based PUF with a capacitive digital preselection for a 1E-9 key error probability," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 67, no. 12, pp. 4855–4868, Dec. 2020.

[13] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Proc. 44th ACM/IEEE Design Autom. Conf. (DAC)*, Jun. 2007, pp. 1–9.

[14] Z. He, W. Chen, L. Zhang, G. Chi, Q. Gao, and L. Harn, "A highly reliable arbiter PUF with improved uniqueness in FPGA implementation using bit-self-test," *IEEE Access*, vol. 8, pp. 181751–181762, 2020.

[15] 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.

[16] M. Garcia-Bosque, G. Díez-Señorans, C. Sánchez-Azqueta, and S. Celma, "Proposal and analysis of a novel class of PUFs based on Galois ring oscillators," *IEEE Access*, vol. 8, pp. 157830–157839, 2020.

[17] Ł. Matuszewski, J. Nikonowicz, P. Kubczak, and W. Woźniak, "Physical unclonable function based on the internal state transitions of a Fibonacci ring oscillator," *Sensors*, vol. 21, no. 11, p. 3920, Jun. 2021.

[18] M. Garcia-Bosque, A. Naya, G. Díez-Señorans, C. Sánchez-Azqueta, and S. Celma, "Suitability of generalized GAROs on FPGAs as PUFs or TRNGs considering spatial correlations," *IEEE Open J. Ind. Electron. Soc.*, vol. 4, pp. 112–122, 2023.

[19] P. A. P. Moran, "Notes on continuous stochastic phenomena," *Biometrika*, vol. 37, nos. 1–2, p. 17, Jun. 1950.

[20] R. C. Geary, "The contiguity ratio and statistical mapping," *Incorporated Statistician*, vol. 5, no. 3, p. 115, Nov. 1954.

[21] A. Maiti, V. Gunreddy, and P. Schaumont, *A Systematic Method to Evaluate and Compare the Performance of Physical Unclonable Functions*. New York, NY, USA: Springer, 2013.

[22] R. D. Sala, D. Bellizia, and G. Scotti, "A lightweight FPGA compatible weak-PUF primitive based on XOR gates," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 69, no. 6, pp. 2972–2976, Jun. 2022.

[23] R. D. Sala, D. Bellizia, and G. Scotti, "A novel ultra-compact FPGA PUF: The DD-PUF," *Cryptography*, vol. 5, no. 3, p. 23, Sep. 2021.

[24] C. Gu, C.-H. Chang, W. Liu, N. Hanley, J. Miskelly, and M. O'Neill, "A large-scale comprehensive evaluation of single-slice ring oscillator and PicoPUF bit cells on 28-nm Xilinx FPGAs," *J. Cryptograph. Eng.*, vol. 11, no. 3, pp. 227–238, Sep. 2021.

[25] J. Zhang, X. Tan, Y. Zhang, W. Wang, and Z. Qin, "Frequency offset-based ring oscillator physical unclonable function," *IEEE Trans. Multi-Scale Comput. Syst.*, vol. 4, no. 4, pp. 711–721, Oct. 2018.

[26] C. Marchand, L. Bossuet, U. Mureddu, N. Bochard, A. Cherkaoui, and V. Fischer, "Implementation and characterization of a physical unclonable function for IoT: A case study with the TERO-PUF," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 37, no. 1, pp. 97–109, Jan. 2018.

[27] N. N. Anandakumar, M. S. Hashmi, and S. K. Sanadhya, "Compact implementations of FPGA-based PUFs with enhanced performance," in *Proc. 30th Int. Conf. VLSI Design 16th Int. Conf. Embedded Syst. (VLSID)*, Jan. 2017, pp. 161–166.

[28] B. Habib, K. Gaj, and J.-P. Kaps, "FPGA PUF based on programmable LUT delays," in *Proc. Euromicro Conf. Digit. Syst. Design*, Sep. 2013, pp. 697–704.

[29] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, document 800-22, DTIC, Fort Belvoir, VA, USA, 2001.

[30] P. Ren, Y. Xue, L. Jing, L. Zhang, R. Wang, and Z. Ji, "A strong physical unclonable function with machine learning immunity for Internet of Things application," *Sci. China Inf. Sci.*, vol. 67, no. 1, pp. 1–13, Jan. 2024.

[31] S. Ray, "A quick review of machine learning algorithms," in *Proc. Int. Conf. Mach. Learn., Big Data, Cloud Parallel Comput. (COMITCon)*, Feb. 2019, pp. 35–39.

[32] D. P. Kingma and J. Ba, "Adam: A method for stochastic optimization," 2014, *arXiv:1412.6980*.

[33] Z. Huang, J. Bian, Y. Lin, H. Liang, and T. Ni, "Design guidelines and feedback structure of ring oscillator PUF for performance improvement," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 43, no. 1, pp. 71–84, Jan. 2024.

[34] Y. Cui, Y. Chen, C. Wang, C. Gu, M. O'Neill, and W. Liu, "Programmable ring oscillator PUF based on switch matrix," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, Oct. 2020, pp. 1–4.

[35] Y. Xu, Y. Lao, W. Liu, Z. Zhang, X. You, and C. Zhang, "Mathematical modeling analysis of strong physical unclonable functions," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 39, no. 12, pp. 4426–4438, Dec. 2020.

[36] C. Gu, N. Hanley, and M. O'Neill, "Improved reliability of FPGA-based PUF identification generator design," *ACM Trans. Reconfigurable Technol. Syst.*, vol. 10, pp. 1–23, May 2017.
[37] L. Zhang, C. Wang, W. Liu, M. O'Neill, and F. Lombardi, "XOR gate based low-cost configurable RO PUF," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, May 2017, pp. 1–4.
[38] A. Cherkaoui, L. Bossuet, and C. Marchand, "Design, evaluation, and optimization of physical unclonable functions based on transient effect ring oscillators," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 6, pp. 1291–1305, Jun. 2016.
[39] C. Gu and M. O'Neill, "Ultra-compact and robust FPGA-based PUF identification generator," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, May 2015, pp. 934–937.
[40] N. N. Anandakumar, M. S. Hashmi, and M. Tehranipoor, "FPGA-based physical unclonable functions: A comprehensive overview of theory and architectures," *Integration*, vol. 81, pp. 175–194, Nov. 2021.
[41] F. Zerrouki, S. Ouchani, and H. Bouarfa, "A survey on silicon PUFs," *J. Syst. Archit.*, vol. 127, Jun. 2022, Art. no. 102514.

RAÚL APARICIO-TÉLLEZ was born in Zaragoza, Spain. He received the B.Sc. and M.Sc. degrees in physics from the University of Zaragoza, Zaragoza, in 2022 and 2023, respectively, where he is currently pursuing the Ph.D. degree with the Group of Electronic Design, Aragón Institute of Engineering Research. His research interests include digital electronics, microelectronic design, hardware security, cryptography, and physically unclonable functions.

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, Aragón Institute of Engineering Research (I3A); and an Associate Professor with the University of Zaragoza. He has co-authored 14 technical papers and more than 35 international conference contributions. He has participated in ten national and international research projects, two of them as a principal investigator. 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., M.Sc., and Ph.D. degrees in physics from the University of Zaragoza, Zaragoza, Spain, in 2016, 2017, and 2024, respectively. He is currently a member of the Group of Electronic Design, Aragón Institute of Engineering Research, University of Zaragoza; and an Assistant Professor with the Centro Universitario de la Defensa, Zaragoza. He has participated in five national research projects and co-authored several technical papers. His research interests include physically unclonable functions, cryptography, and physics of complex systems.

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, Spain, in 1987, 1989, and 1993, respectively. He is currently a Full Professor with the Group of Electronic Design, Aragón Institute of Engineering Research, University of Zaragoza. He has co-authored more than 130 technical papers and 320 international conference contributions. He is the co-author of four technical books and the holder of four patents. He has participated in 70 national and international research projects, 40 of which as a principal investigator. His research interests include cyber-physical systems, hardware security and cryptosystems, analog and mixed signal processing, front-ends for wireline and wireless communications, RFIC and MMIC integrated circuits, devices and integrated circuits in emerging technologies, embedded systems for secure communications, and cryo-CMOS circuits for interfaces in quantum technologies.