IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received August 6, 2021, accepted October 25, 2021, date of publication October 27, 2021, date of current version November 8, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3123867

Digitization Algorithms in Ring Oscillator Physically Unclonable Functions as a Main Factor Achieving Hardware Security

GUILLERMO DIEZ-SENORANS[1], MIGUEL GARCIA-BOSQUE[1,2], CARLOS SÁNCHEZ-AZQUETA[3], AND SANTIAGO CELMA[1]

[1]Group of Electronic Design, Department of Electrical Engineering and Communications, University of Zaragoza, 50009 Zaragoza, Spain
[2]Centro Universitario de la Defensa, Academia General Militar, 50009 Zaragoza, Spain
[3]Department of Applied Physics, University of Zaragoza, 50009 Zaragoza, Spain

Corresponding author: Guillermo Diez-Senorans (gds@unizar.es)

This work was supported by the Ministerio de Economía y Competitividad - Fondo Europeo de Desarrollo Regional (MINECO-FEDER) under Grants TEC2017-85867-R and PID2020-114110RA-I00. The work of Guillermo Diez-Senorans was supported by the Diputación General de Aragón (DGA) fellowship.

ABSTRACT Since the discovery of the physical random functions and their subsequent refinement into physical unclonable functions (PUF), a great effort has been made in developing and characterizing these objects attending to their physical properties as well as conceiving a myriad of different examples in the search for a better application-specificity and suitability. However, comparatively little time has been devoted to the analysis of entropy extraction algorithms beyond the recognition of some limitations due to the environment influencing the PUF behavior. In this article we focus on well known PUF candidates based on ring oscillator delay, which are ideal for FPGA prototyping due to their tolerance to asymmetries in routing. We have studied the impact that different digitization algorithms of the responses have over their security properties. Specifically, we have analyzed the response probability distributions that arise from some popular techniques of digitization called ''compensated measuring'' methods, highlighting their lack of uniformity and how this might translate into cryptanalytically exploitable vulnerabilities. Furthermore, we propose a new family of digitization schemes named *k-modular* that exhibit both uniformity in response distribution and high entropy density on both physical and response space.

INDEX TERMS Compensated measuring, entropy, FPGA, hardware security, physically unclonable function, ring oscillator.

I. INTRODUCTION

The continuous growth in the capacity to store, process and transmit digital data is radically transforming our environment into an information ecosystem. Massive access of everyday devices to the internet (Internet of Things, IoT) has potential applications in areas of great importance such as logistics, industry, health or defense [1]–[3]. However, the distributed nature of this technology and the severe restrictions on power and area associated make the physical layer of these systems a major vulnerability [4]. In this context, physically unclonable functions (PUFs) arise as a promising security solution, capable of providing secure storage of key data and identification of trusted instances [5]–[7].

The associate editor coordinating the review of this manuscript and approving it for publication was Ahmed M. Elmisery.

PUFs are a cryptographic primitive with security properties on the physical layer, which are of application in getting a device to be robust against hardware-level, physically invasive attacks as well as side channel attacks [8]–[10]. To achieve this goal PUFs exploit microelectronic manufacturing process random variations in such a way that different physical realizations of a same design present slight yet measurable deviations, which are impossible to control in order to be physically replicated even by the original manufacturer [11], [12]. These characteristics resemble those of biometric security systems, which has motivated to call PUFs ''a device's fingerprint''.

From a formal point of view, PUFs can be thought as pieces of hardware which exhibit a *response* when exposed to adequate stimuli called *challenges*. PUFs have been traditionally classified according to the size of this challenge space as

weak PUFs if this is small (i.e., if this can be exhausted in polynomial or less time) or *strong PUFs*, if challenge space scales faster than polynomial as a function of PUF device physical parameters (e.g., area, number of cells, etc.). However, it is a controversial statement, as some authors argue that density of information in a region of space is upper bounded by fundamental physical arguments [13] to be asymptotically polynomial, thus deprecating this widespread classification. Despite the formalization of both kinds of PUF in terms of complexity theory, things are usually much clearer in practice where PUFs classified ''weak'' present a very limited number of possible challenges (usually only one), while those called ''strong'' exhibit a (more or less) straightforward mechanism to expose the instance to multiple challenges. As a consequence, both types of PUF behave in a dramatically different way, and thus they find application in very different fields: weak PUFs provide a secure key storage mechanism in which keys are re-generated from hardware-specific features of the device rather than stored in non-volatile memories [6], [9], whereas strong PUFs can be used in identification/authentication protocols as well as key generation [10], [14].

In this paper we focus on the security properties that arise regarding the methodology chosen to turn physical disorder into binary responses, which we will refer to as *digitization algorithms* through the text. The concrete PUF representative that we work with is the ring oscillator PUF (RO-PUF), which was first proposed by Gassend *et al.* in [12], and exhibits a number of advantages that make it highly convenient. First, it is an FPGA-friendly PUF that allows fast and easily modifiable hardware implementation, as well as straightforward interfacing via UART and PMOD ports. Besides, RO-PUFs have been extensively studied in terms of physical properties, and the digitization algorithms developed to it (based on frequency comparison of identically designed ring oscillators) are of application to a broader family of PUF candidates, specifically, any PUF whose response is constructed by comparing measurements, i.e., compensated measuring -digitized PUFs, [14]. In regards of the discussion of the previous paragraph, RO-PUFs are capable of providing a large number of challenge-response pairs and thus might be classified as strong PUFs. In this work we are interested in studying the security properties of a single RO-PUF instance in terms of the entropy delivered from it, for which we have made use of different permutations of ring oscillators array as challenges which altogether with a digitization scheme will produce well defined bit strings.

Furthermore, a method based on entropy analysis has been developed to test some popular comparison algorithms reported in RO-PUF design works, highlighting their strengths and weaknesses. Finally we propose a novel algorithm that aims to compensate for unbalance in security to performance trading-off found on previous schemes.

The main contributions of this work are: (i) we have studied the entropy regarding the digitization schemes typically used in RO-PUF and other compensated measuring PUFs, (ii) we have proved that entropy scales linearly with the size (*i.e.*, number of oscillators) of such PUF circuit, (iii) we have given examples of how the most common digitization algorithm gives raise to dictionary-like vulnerabilities due to the non-uniformity of its distribution, (iv) we have given plausible arguments that make evident that there exists an inverse relation between usage of resources and cryptographic performance (in terms of entropy extraction), and (v) we have proposed a digitization algorithm (so called *k-modular*) that exhibits good trade-off between these two aforementioned desirable properties. On the other hand, the prime difficulty faced in this research was to handle the huge size of challenge space which makes it hard to approximate the outcome distribution of probability.

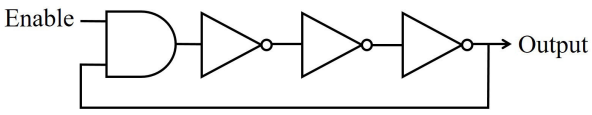

FIGURE 1. A three-inverter ring oscillator with enable control scheme.

This paper is organized as follows: in Section II we make an exhaustive review on the physical aspects of RO-PUFs, Section III describes the experimental setup that has been used to implement and evaluate our RO-PUF proposals in FPGA. Section IV contains a description and subsequent analysis of the results obtained in our experiments. Finally, Section V will highlight some conclusions that might be drawn from our work.

II. BACKGROUND

A. RING OSCILLATORS

A ring oscillator (*RO*) is an astable digital circuit composed of an odd number of inverters feedbacked in a loop (Fig. 1). Adopting a mathematical model similar to that described in [15], we can characterize a ring oscillator delay (Δ) as

$$\Delta = \delta_0 + \delta_{gD} + \delta_{lD} + \delta_{gG} + \delta_{lG}$$

where δ_0 is the nominal delay of an ideal ring, δ_{gD} is a global and deterministic contribution to delay due to global deviation from ideal conditions (i.e., temperature and voltage supply of the whole chip), δ_{lD} is the local and deterministic contribution due to systematic features of the oscillator (this is, the term that comprises all the ''manufacturing noise''), δ_{gG} is the delay caused by global Gaussian fluctuations (such as fluctuation in temperature or voltage), and δ_{lG} is the contribution of local Gaussian noise, such as EM noise influencing the circuit pointwisely. Ring oscillator architecture allows us to write down the expected time for the oscillator to complete M laps as

$$t_M = \sum_{i=1}^{M} \Delta_i = M(\delta_0 + \delta_{gD} + \delta_{lD}) + \sum_{i=1}^{M} \delta_{gG}(t_{i-1}) + \delta_{lG}(t_{i-1}) \quad (1)$$

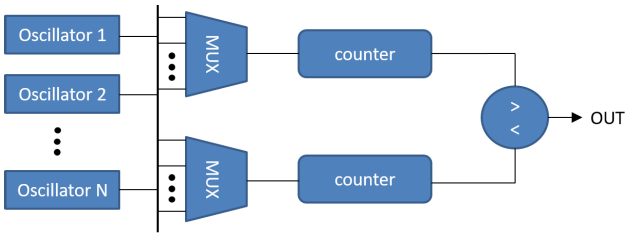

FIGURE 2. RO-PUF schematic.

Since these quantities are modeled like normal distributed variables of zero mean (note that any bias can be absorbed by the corresponding global or local systematic contribution), it follows

$$\langle \delta_G \rangle = 0 = \frac{\sum_{i=1}^{M} \delta_G(t_{i-1})}{M} \rightarrow \sum_{i=1}^{M} \delta_G(t_{i-1}) = 0 \tag{2}$$

where $\langle x \rangle$ stands for the average of the quantity x. Thus for large enough number of periods M we can rewrite total oscillator delay as

$$t_M = M(\delta_0 + \delta_{gD} + \delta_{lD}) \equiv M\Delta = \frac{M}{f} \tag{3}$$

where $f = 1/\Delta$. On the other hand, the time elapsed by a reference clock of period δ_r in completing M_r oscillations might be written as

$$t_{M_r} = M_r \delta_r = \frac{M_r}{f_r} \tag{4}$$

If the total delay t_M equals t_{M_r} then, from (3) and (4) we have

$$\frac{M}{f} = \frac{M_r}{f_r} \rightarrow f = \frac{M}{M_r} f_r \tag{5}$$

Since M_r and M are natural numbers $M = M_r q + r$, and (5) can be written

$$f = \frac{M_r q + r}{M_r} f_r = \left(q + \frac{r}{M_r} \right) f_r \tag{6}$$

Experimental estimation of RO frequency ($\hat{f}$) if M oscillations are measured in M_r periods of the reference clock will be

$$\hat{f} = q f_r \tag{7}$$

So deviation (e) with respect to actual frequency,

$$e = e(M_r) = \left| f - \hat{f} \right| = \frac{r}{M_r} f_r \sim 1/M_r \tag{8}$$

and thus on the limit of large M_r is

$$\lim_{M_r \to \infty} e = 0 \tag{9}$$

This exposes the fact that resolution of measuring can be arbitrary increased by letting the reference clock run for a longer time.

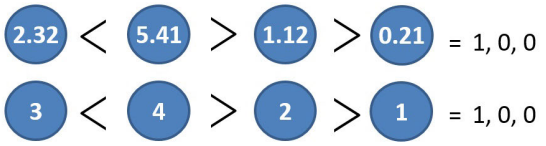

FIGURE 3. Example of digitization scheme where one bit is extracted per frequency comparison: only relative frequency between oscillators has relevance.

B. RO-PUF

The RO-PUF architecture that we have adopted in this work is the modification proposed by Suh and Devadas in [6]. This dates back to 2007 and further research has been made in order to increase the number of bits, *i.e.*, the number of comparisons that can be made out of a fixed number of oscillators such as configurable RO-PUF [16], or the more modern Transformer PUF introduced in [17]. However, we will restrict to the original ring oscillator PUF for simplicity, since the results of our research are of application to any comparison-based digitization procedure and thus involve newer RO-PUF adaptations. The core of such design is a bank of N ring oscillators designed to be identical, together with a measuring element capable to capture their oscillation frequencies (Fig. 2). Since ring oscillators are very sensitive to deterministic global noise caused by temperature variations, it is a common practice to build a differential function out of the frequency measurements. A well-known differential function introduced by Gassend *et al.* consists of subtracting the frequencies of pairs of oscillators, taking the sign of this operation as the binary output (say, "0" for minus and "1" for plus) [12], [18]. This approach has the advantage of showing a straightforward way to define the challenge space in which each challenge is simply the pair of oscillators to be compared. This differential technique is referred to as *compensated measuring* in the context of PUF design practice [12], [19]. From an N cells arrangement this means that it can deliver $N(N-1)/2$ bits, however it is clear that many of these bits will be correlated because of the transitivity of the ordering operation which dictates that, given a set of three oscillators a, b and c such that $f_a > f_b$ and $f_b > f_c$ it implies that $f_a > f_c$ (where f_i stands for the oscillation frequency of oscillator "i"), and the bit from the comparison of oscillators a and c (namely, the bit ac) is not random. This means that the maximum entropy possibly delivered by such a system is somewhat lower than $N(N-1)/2$ bits; actually we can do better in bounding the maximum entropy, since only relative differences are of interest rather than actual frequency measurements, so it is apparent that each oscillator can be unequivocally labeled from 1 to N according to its relative speed (see Fig. 3). This leads to the assertion that the complexity of this system is that of ordering each of the N oscillators, i.e., this PUF can be set at $N!$ different states, which implies an upper bound on entropy:

$$S \leq \log_2 N! \tag{10}$$

as stated in [6]. The problem of guessing which of all the possible $N(N-1)/2$ comparisons will deliver the maximum

entropy is hard to make and device-dependent [10], so a simpler approach within a specific application is to compare fixed pairs of oscillators. From now on we will refer to this list of fixed comparisons as the *topology* ($\mathcal{T}$) of the RO-PUF. Let $\mathcal{N}^2$ the set of all possible pairs,

$$\mathcal{N}^2 = \{(i, j) \mid 1 < i < N, j > i\} \tag{11}$$

then any topology is defined as

$$\mathcal{T} \subseteq \mathcal{N}^2 \tag{12}$$

Through the rest of the text we will refer coherently to RO arrays $\boldsymbol{N}$ of length N oscillators, and bit strings $\boldsymbol{N_b}$ of length N_b bits as the random variables:

$$\boldsymbol{N} = \{n_i \in \mathbb{N} \mid 1 < i < N\} \tag{13}$$

$$\boldsymbol{N_b} = \{b_i \in \{0, 1\} \mid 1 < i < N_b\} \tag{14}$$

These two concepts are made concrete through the PUF physical instantiate, and are bounded by the definition of a topology which can be thought as an operator acting on RO arrays as

$$\mathcal{T}(\boldsymbol{N}) = \boldsymbol{N_b} \tag{15}$$

The application scenarios of RO-PUF comprise both its use as either authentication or secure key storage, *e.g.*, RO-PUF can be used to authenticate end nodes in an IoT environment, which requires CRP transmission through an insecure channel and thus CRP reuse is forbidden [20]; this application makes use of a large CRP space and thus the RO-PUF design must include a mechanism to accept different challenges. On the other hand, the secure key storage application can be set with a minimum number of challenge-response pairs (maybe only one) and these might be hard-coded in the hardware design [21].

Once a topology has been chosen (probably implemented as an intrinsic property of the RO-PUF), it might be argued that many potentially independent comparisons are being ignored. This can be addressed by defining a challenge space as the space of permutations $\sigma(1, \ldots, N)$, in the sense that the topology defined as the subset of pairs i, j can be applied to the permuted indices $\sigma(i), \sigma(j)$, *e.g.*, given a toy model of three inverters $N = 3$ and a topology defined as $\{(1, 2), (2, 3)\}$ that produces two bits, we can feed this RO-PUF with the identity permutation $(1, 2, 3)$ and thus obtain the response bit string $(12,\ 23)$ (where "12" stands for the bit resulting from comparing oscillators 1 and 2, etc); or we could ask the RO-PUF to output a different permutation, say $(3, 1, 2)$ which will lead to the word $(31,\ 12)$. Since the entropy of the system is bounded by (10), this definition of a challenge space is well behaved in the sense that the whole performance in entropy extraction is provided by the topology definition: a good topology (in terms of entropy extraction) will map each challenge to a different, independent response string and thus will deliver the theoretical maximum entropy, while a poorly defined topology will map the challenge space to a skewed response space. Throughout this work we will analyze some of the most common topologies found in the literature in terms of entropy extraction and other security metrics, and we will propose a new topology to address some of the flaws found. It is interesting to notice that in the assumption of an ideal manufacturer which produces oscillators whose frequencies are uniformly distributed through the chip, the space of RO-PUF instances matches the challenge space defined as above (because the ordering of any oscillators array produced by the manufacturer will match *some* permutation $(1, \ldots N)$), and thus the following discussion is applicable to both scenarios where a large CRP space is needed for authentication purposes, or either a single challenge is used in a weak PUF fashion as secure storage.

According to this, the evaluation of every permutation will give raise to a space of bit strings (responses) whose distribution will depend on the chosen topology [22]. We will refer to the probability of a response as the chance of extracting a concrete outcome if a permutation is randomly picked and evaluated. Thus, the security properties of each topology might be characterized attending to some statistical metrics over the responses probability distribution. There are a number of popular metrics that are useful to characterize security properties in cryptographic systems depending on the adversarial model (i.e., the information an adversary is supposed to posses from the system): *Shannon entropy* (S) measures the minimum number of bits required by a system to label every state [23]; *min-entropy* (s) can be thought as a measure of the best chance an adversary has in guessing the key at one try (and furthermore, its superiority over Shannon entropy as security metric has been claimed by some authors) [24], [25]; and *guesswork* (G) measures the mean time needed to break a key in a dictionary attack (i.e., a kind of "brute force attack" in which the illegitimate key candidates are tried out from the most probable to the least) [26]. Nevertheless, in this work we have mainly attached to the Shannon entropy (and some related curves) as a measure of "cryptographic-goodness", since this metric is well studied and widespread through the literature [27]–[31]. Entropy is defined on the response probability distribution $p_{\mathcal{T}}(\boldsymbol{N_b})$ as

$$S_{\mathcal{T}} = -\sum_{\boldsymbol{N_b}} p_{\mathcal{T}}(\boldsymbol{N_b}) \log_2 [p_{\mathcal{T}}(\boldsymbol{N_b})] \tag{16}$$

where

$$p_{\mathcal{T}}(\boldsymbol{N_b}) = \frac{\|\{\boldsymbol{N} \mid \mathcal{T}(\boldsymbol{N}) = \boldsymbol{N_b}\}\|}{N!} \tag{17}$$

and $\|.\|$ stands for set cardinality.

In the following, we will use square brackets, $S[\boldsymbol{N}]$ to indicate "the entropy of the response space spanned by the whole set of oscillator arrays, $\{\boldsymbol{N}\}$".

In practice, the previous discussion leaves two main design options which are most popular through literature:

- The *1-out-of-k* masking was introduced by Suh and Devadas in [6] as a way of obtaining uncorrelated bits and increase the robustness of the system against environmental variations. In this approach, the set of N

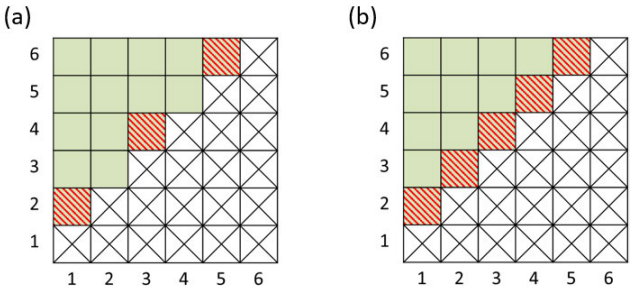

FIGURE 4. Representation of a topology as the number of used comparisons (dashed squares) out of all possible comparisons (green squares). These two examples show: (a) the *1-out-of-2* topology (1st oscillator is compared to 2nd, 3rd to 4th and so on) and (b) the *N-1* topology (1st is compared to 2nd, 2nd to 3rd, 3rd to 4th and so on) for a set of $N = 6$ oscillators.

oscillators is divided into groups of k oscillators. One bit is obtained out of each group by comparing only the pair of oscillators whose frequencies are further apart (which reduces the probability of a bit flip event in the case that environmental changes affect the frequency of oscillators). In this work we will attach to the simplest form of masking using $k = 2$; we will refer symbolically to this *1-out-of-2* masking as $\mathcal{N}_{/2}$ topology; this constructions will provide $N/2$ bit length responses out of an array of N oscillators (see the schematic representation of this topology in Fig. 4.a) [6], [10], [32].

- The "$N-1$" topology which we will refer to as $\mathcal{N}_{\searrow 1}$, where only neighboring oscillators are compared yielding $N-1$ bit responses (Fig. 4.b) [33], [34].

In the next subsections we will introduce these topologies, as well as the case $\mathcal{N}^2$ in which all possible comparisons are taken into account. Finally, we will propose a novel family of topologies named "*k-modular*" (referred as $\mathcal{N}^2_{/k}$) that are introduced in Section IV.

III. EXPERIMENTAL SETUP

In this work we are interested in the security properties that arise from a RO-PUF architecture depending on the digitization technique selected to turn a set of N oscillators into a bit string. In orde to perform such analysis. In this work we have implemented a set of ring oscillators in an FPGA model xc7z020 mounted on a development board PYNQ-Z2, which includes a 125 MHz clock signal inputted to the FPGA. The ring oscillator architecture consists of three inverters in a loop plus an AND gate which provides *enable* control. The frequency of a ring oscillator is measured by estimating its period; this is done by comparing the number of cycles looped by the ring oscillator (M) in M_r cycles of the reference clock, while maintaining the system at constant (room) temperature and voltage. Afterwards the quotient M/M_r is easily transformed into frequency multiplying by the factor $f = M \times 125/M_r$ MHz (where the factor 125 stands for the frequency of the reference clock measured in MHz).

According to (8) the maximum possible error due to lap counting will be $e = f_r/M_r$, however at some point Gaussian

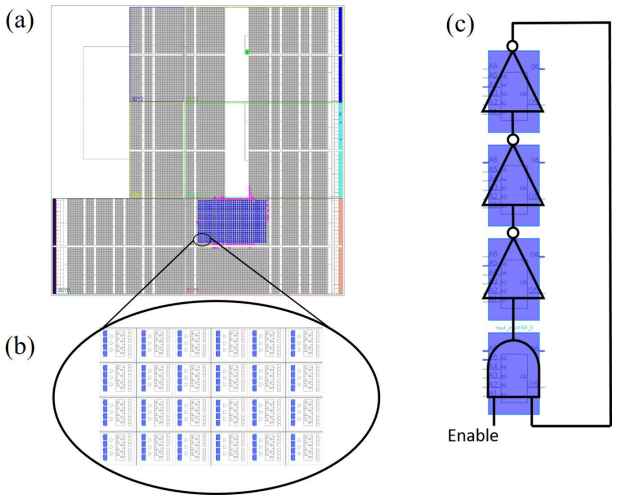

FIGURE 5. (a) Implementation of measuring system in FPGA. (b) Zoom to matrix of ring oscillators. (c) Scheme of an oscillator implemented using three LUTs.

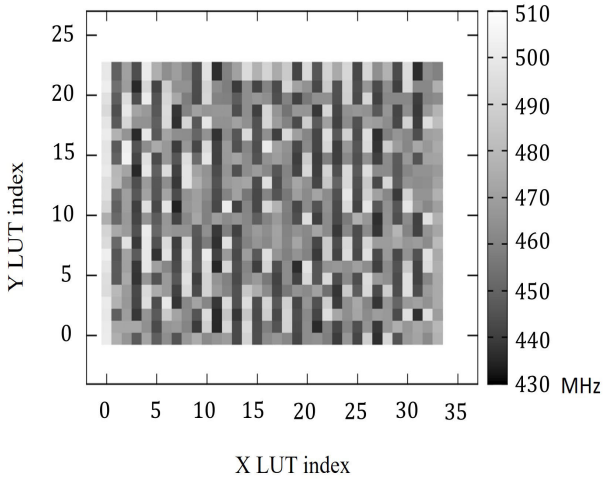

FIGURE 6. Spatial distribution of frequencies throughout the matrix of oscillators in FPGA.

noise will become dominant (notice that Gaussian fluctuations are expected to behave like $\sim 1/M_r^{1/2}$). In our experiments where we took $M_r = 10^7$ reference laps the resolution of measurement is $\sim 1.25 \times 10^{-5}$ MHz, while the smallest standard error measured in the RO matrix arrangement was ± 0.01 MHz, so it is clear that our reference time is enough to measure deterministic features of RO properly.

The schematic implemented in the FPGA as well as the construction of a ring oscillator using the FPGA look up tables (LUTs) is shown in Fig. 5. For this work we have implemented a matrix of 34×23 RO which oscillate at an average frequency of $\hat{f} = 463.93$ MHz. The distribution of frequencies shows some degree of correlation in the frequency spatial distribution, in the sense that nearby oscillators, specifically oscillators within the same column, seem to run at close frequencies, see Fig. 6.

In the present study we are focused on the security properties arising from the choice of digitization method only,

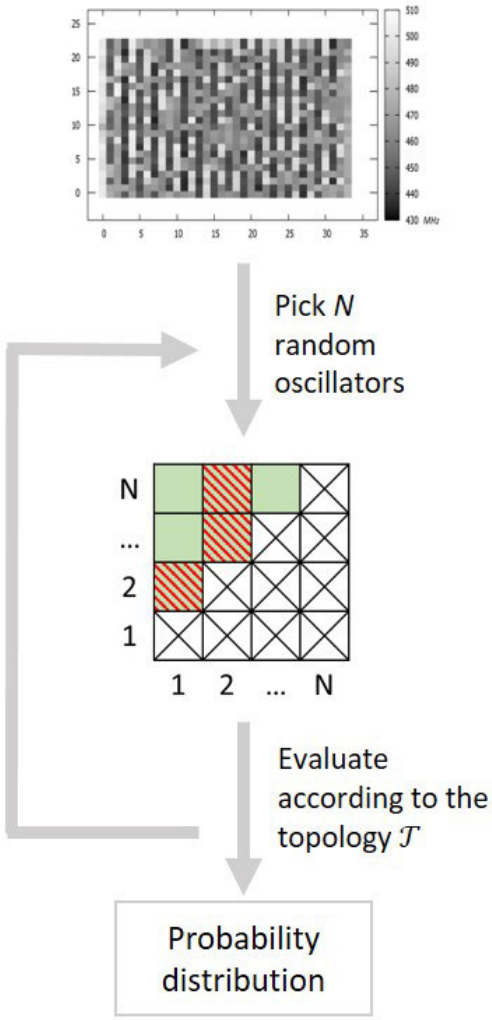

FIGURE 7. Scheme of the evaluation procedure designed to obtain the probability distribution associated to each topology.

and thus we want to save our results from hardware implementation flaws such as spatial correlation. To achieve this, we design an evaluation procedure that randomize the actual frequency measurements by picking a random subset of N oscillators. The N values will be used to simulate a N-oscillator RO-PUF, which is then evaluated according the dictation of a given topology. This process is iterated to generate a histogram that approximate the underlying probability distribution associated to an ideal N-oscillators RO-PUF operating under a given topology (Fig. 7). PUF instance responses are generated in post processing by randomly picking subsets of N oscillators from the whole set, and comparing them under the dictation of a given topology $\mathcal{T}$ for different permutations (challenges). This process is iterated for various values of N to study how the distributions change depending on the number of oscillators.

IV. RESULTS

A. COMPARE ALL PAIRS: $\mathcal{N}^2$ TOPOLOGY

This is the trivial topology in which all possible comparisons are made to build the response bit string. Digitization process

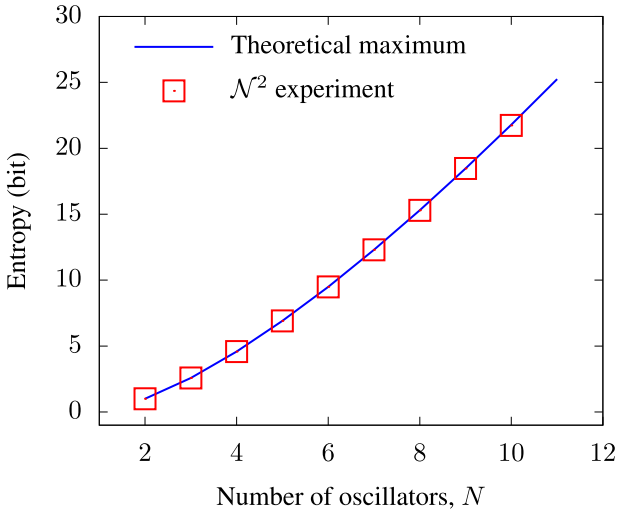

FIGURE 8. Entropy delivered by $\mathcal{N}^2$ topology equals the maximum theoretical possible.

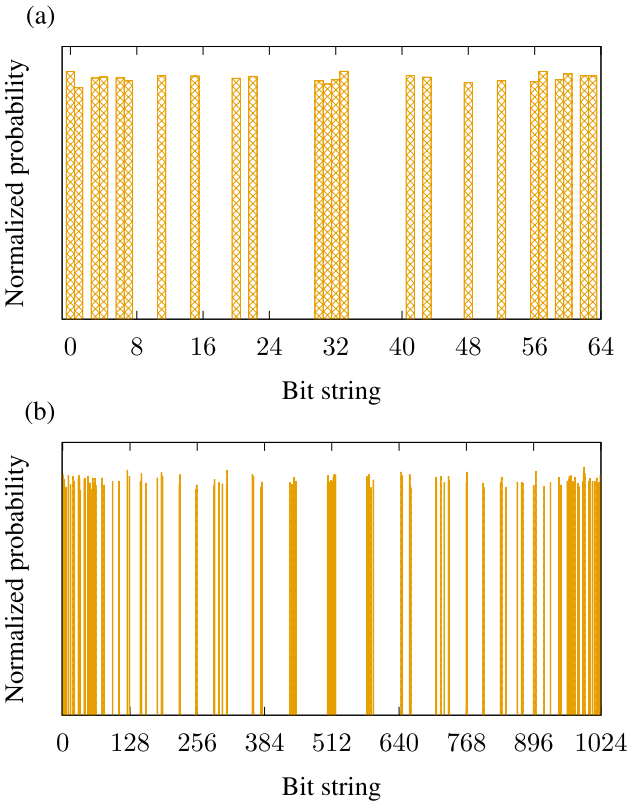

FIGURE 9. Response histograms under topology $\mathcal{N}^2$ with: (a) $N = 4$ and (b) $N = 5$ oscillators.

is carried out by exhausting all possible comparisons in the matrix of oscillators, thus $N(N-1)/2$ bits are deployed. This way of extracting strings from the RO-PUF is infrequent in the literature, since it suffers from a high bit correlation due to the transitivity of ordering. However, since the state space contains *all* possible comparisons that can be made out of an N oscillators matrix, any other topology construction will

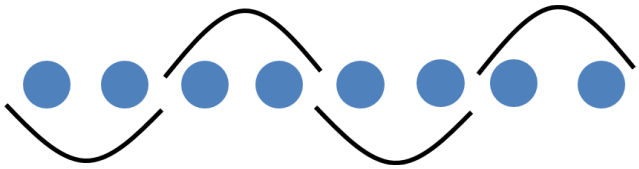

FIGURE 10. Comparison scheme of $\mathcal{N}_{/2}$ topology.

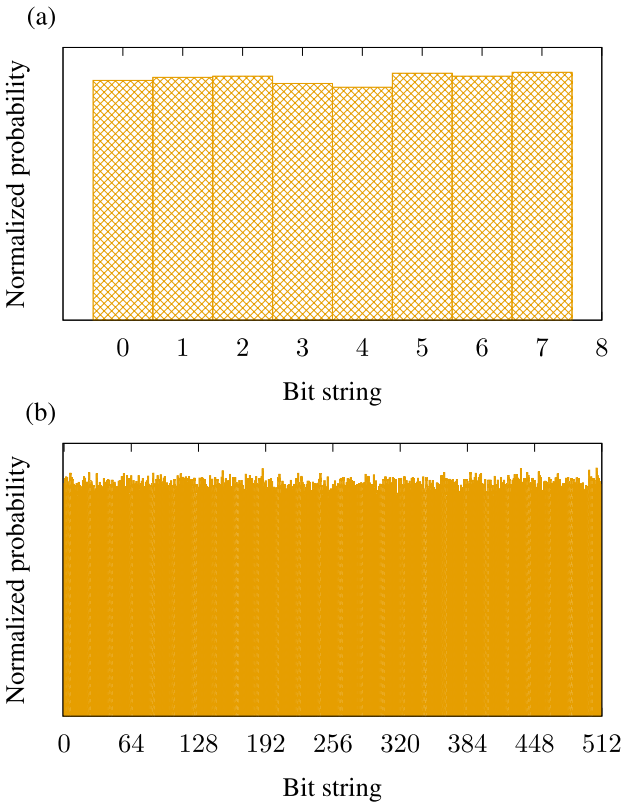

FIGURE 11. Response histograms under $\mathcal{N}_{/2}$ topology for N oscillators: (a) $N = 8$ and (b) $N = 18$.

span a smaller state space, thus $S_{\mathcal{N}^2} \geq S_{\mathcal{T}}$. This still stands even if topology $\mathcal{T}_{\max}$ deploys the maximum entropy, thus it necessarily follows

$$S_{\mathcal{N}^2}(N) = \log_2 N! \tag{18}$$

This is clearly pointed out in the strong agreement between experimental entropy estimation (red markers) and theoretical bound (solid line) in Fig. 8, where the interpolation curve has been extended to the real domain using the Legendre's gamma function: $N! \to \Gamma(N+1)$.

The distribution of bit strings that arise according to $\mathcal{N}^2$ topology for different number of oscillators is shown in Fig. 9. These histogram leaves a large number of blank spaces throughout the PUF image $y \in [0, 2^{N(N-1)/2} - 1]$, which is nonetheless expected because bit correlation prevents $2^{N(N-1)/2} - N!$ states from being visited. However it is interesting that the system is uniformly distributed over the remaining $N!$ values.

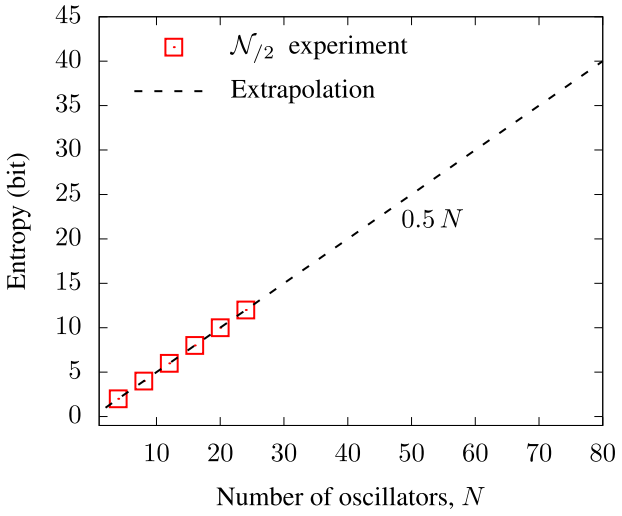

FIGURE 12. Entropy delivered by $\mathcal{N}_{/2}$ topology against the number of oscillators: it remarkably escalates as the responses bit-length.

B. COMPARISON WITHOUT REPETITION: $\mathcal{N}_{/2}$ TOPOLOGY

In this topology the array of N available oscillators $n_i\,|_{i=1}^{N}$ is digitized by comparing two adjacent oscillators without repetition (see Fig. 10):

$$\mathcal{N}_{/2}(\boldsymbol{N}) \ni b_{i/2} = \begin{cases} 0 & \text{if } n_{i+1} > n_i \\ 1 & \text{otherwise} \end{cases} \tag{19}$$

This scheme (altogether with others that generalize to *1-out-of-k* masking in which one bit is produced out of $k \geq 2$ different oscillators) are the most commonly found in PUF literature [6]. It produces $N/2$ bit words, thus a large amount of entropy is paid in the trade-off between security proficiency and environmental robustness. Unfortunately, since switching activity can be correlated to the number of oscillators in the matrix, this system will also suffer from a poor performance mark [35]. However, absolute no cell repetition translates into no bit correlation at all, and thus entropy per bit scoring tends to 100%, which arises as a guarantee of good resistance to cryptanalysis (notice the plain distribution of measured responses shown in Fig. 11).

In Fig. 12 we have plotted entropy against different size of the oscillator arrays. The linear interpolation curve is justified as follows:

We define the composition operation, "$\circ$", on ROs arrays as

$$\boldsymbol{X} \circ \boldsymbol{Y} \longleftarrow \mathcal{T}(\boldsymbol{X} \circ \boldsymbol{Y}) = \mathcal{T}(\boldsymbol{X}), \mathcal{T}(\boldsymbol{Y}) \quad \forall \mathcal{T} \tag{20}$$

where the comma separator (,) stands for mere juxtaposition of either ring oscillators arrays or bit strings.

On the basis of the well-known entropy property of joint systems, $S(X, Y) \leq S(X) + S(Y)$, with equality happening if and only if both subsystems are independent [36], the next property can be derived for the composition operation defined above,

$$S_{\mathcal{T}}[\boldsymbol{X} \circ \boldsymbol{Y}] = S_{\mathcal{T}}[\boldsymbol{X}] + S_{\mathcal{T}}[\boldsymbol{Y}] \tag{21}$$

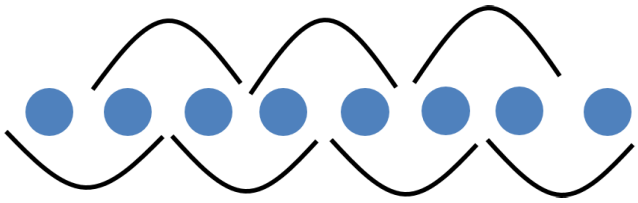

FIGURE 13. Comparison scheme for $\mathcal{N}_{\diagdown 1}$ topology.

Concerning the particular case of $\mathcal{N}_{/2}$ topology, any oscillators array might be splitted into two juxtaposed subsystems such that they will be independent one to each other because every oscillator is used only once, $\mathcal{N}_{/2}(\boldsymbol{X},\boldsymbol{Y}) = \mathcal{N}_{/2}(\boldsymbol{X}),\mathcal{N}_{/2}(\boldsymbol{Y})$. Regarding definition (20) this can be written

$$\begin{aligned} \mathcal{N}_{/2}(\boldsymbol{X},\boldsymbol{Y}) &= \mathcal{N}_{/2}(\boldsymbol{X}\circ\boldsymbol{Y}) \\ &\downarrow \\ S_{\mathcal{N}_{/2}}[\boldsymbol{X},\boldsymbol{Y}] &= S_{\mathcal{N}_{/2}}[\boldsymbol{X}\circ\boldsymbol{Y}] \end{aligned} \tag{22}$$

And using (21) this leads to the linearity of entropy function

$$S_{\mathcal{N}_{/2}}[\boldsymbol{N}] = S_{\mathcal{N}_{/2}}[\boldsymbol{X}] + S_{\mathcal{N}_{/2}}[\boldsymbol{Y}] \quad \forall \boldsymbol{X},\boldsymbol{Y} \mid \boldsymbol{X},\boldsymbol{Y} = \boldsymbol{N} \tag{23}$$

C. COMPARISON WITH REPETITION OF ONE OSCILLATOR: $\mathcal{N}_{\diagdown 1}$ TOPOLOGY

In this latter scenario, which was introduced by Maiti *et al.* in [33], the system is maintained under reasonable environmental resistance while deploying an entropy of approximately N bits. In this scheme every comparison involves a new oscillator, thus measurements will not be trivially correlated due to transitivity over triads as in the previous case (see Fig. 13)

$$\mathcal{N}_{\diagdown 1}(\boldsymbol{N}) \ni b_i = \begin{cases} 0 & \text{if } n_{i+1} > n_i \\ 1 & \text{otherwise} \end{cases} \tag{24}$$

In this case the responses will be $N-1$ bits long, however it is interesting that some bit correlation still exists because of the digitization algorithm: there are some RO-PUF challenges (i.e., some permutations of the N oscillators array) such that the resulting adjacent-comparing produces the same bit string. In order to provide an example of this collision scenario and the correlation that it implies we have examined the behavior of a three oscillators long array (see Fig. 14). These might be labeled from 1 to 3 according to each relative frequency (such as Fig. 3). Since any realization of this PUF instance will correspond to some ordering, any possible PUF outcome will be specified by a permutation of (1, 2, 3). The table in Fig. 14 shows all possible challenge and its corresponding PUF output. From this example it is apparent that, after extracting a first bit (say, "0") the probability of getting a second bit is not uniform: obtaining a "1" is more probable (66%) than obtaining a "0" (33%). This fact reveals

(a)

Permutation	Bitstring
$1<2<3$	0 0
$1<3>2$	0 1
$2>1<3$	1 0
$2<3>1$	0 1
$3>1<2$	1 0
$3>2>1$	1 1

(b)

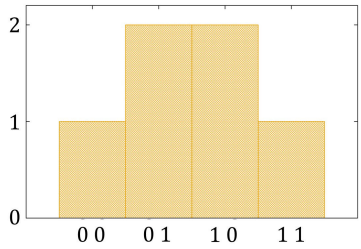

FIGURE 14. Toy example of $\mathcal{N}_{\diagdown 1}$ topology for $N = 3$: (a) all possible realizations of such a RO-PUF. (b) Histogram of the RO-PUF responses, which exhibits evident non-uniformity.

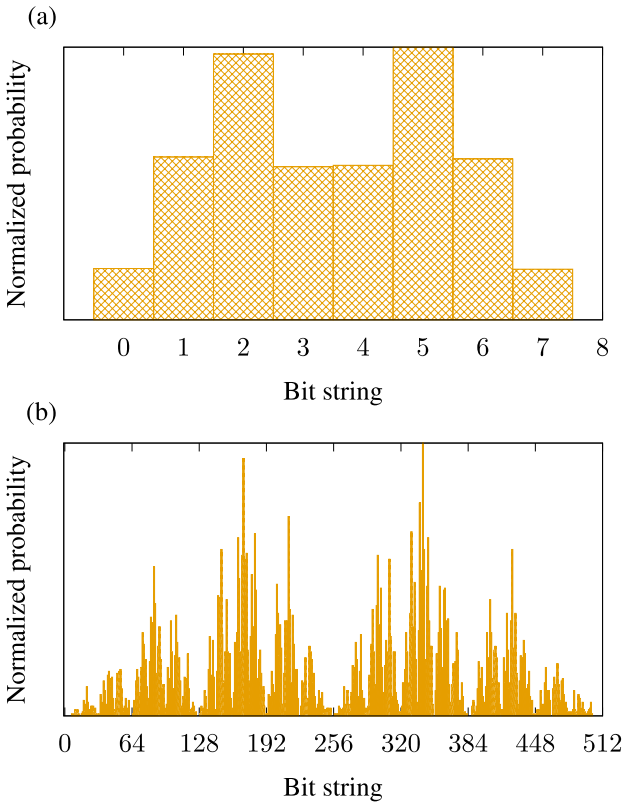

FIGURE 15. Response histograms under topology $\mathcal{N}_{\diagdown 1}$ for N oscillators: (a) $N = 4$, (b) $N = 5$, (c) $N = 6$ and (d) $N = 10$.

a fundamental shortcoming of this security structure, and it is remarkably caused by the digitization algorithm only, no matter the physical properties of the device holding this architecture.

In Fig. 15 we have plotted the histograms resulting of various distinct number of oscillators N, which shows how this effect is amplified as the response length increases; this collision probability can be used by an adversary to gain advantage over the RO-PUF solution by exposing illegitimate key candidates to the PUF interface in a "better-than-random" checkout. The entropy delivered by this topology against the length of the oscillator array is shown in Fig. 16.

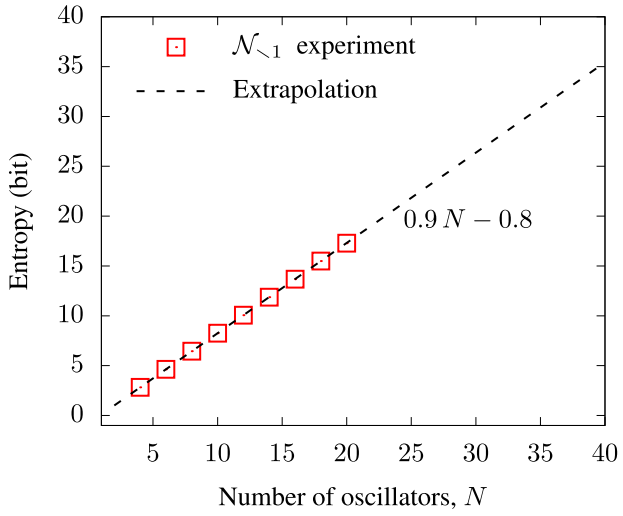

FIGURE 16. Entropy delivered by $\mathcal{N}_{\diagdown 1}$ topology against the number of oscillators. Its progression law can be proved to be linear, which allows for extrapolation.

In regards of the interpolation model, pretty much of the argument given in the previous section stands here: given a system $\boldsymbol{N}$ composed of N oscillators whose elements are numbered from 1 to N as usual, this system can be separated into two sub systems $\boldsymbol{X}$ and $\boldsymbol{Y}$, of lengths X and Y such that $X + Y = N$. No matter what permutation happened to instantiate the $\boldsymbol{N}$ PUF system, the oscillators within each sub array can be re-numbered from 1 to X and 1 to Y respectively, according to discussion in Fig. 3. Unlike the previous case, now $\mathcal{N}_{\diagdown 1}(\boldsymbol{X}, \boldsymbol{Y}) \neq \mathcal{N}_{\diagdown 1}(\boldsymbol{X}), \mathcal{N}_{\diagdown 1}(\boldsymbol{Y})$ because there are two oscillators in each sub-string (namely, the "frontier oscillators": last oscillator in $\boldsymbol{X}$ and first one in $\boldsymbol{Y}$) that interact one to each other. However, these are the only connection between both sub-strings indeed: all the remaining bits produced by $\mathcal{N}_{\diagdown 1}$ are independent. Thus the operation of $\mathcal{N}_{\diagdown 1}$ on the juxtaposed string $\boldsymbol{X}, \boldsymbol{Y}$ is *almost* that on the whole system $\boldsymbol{N}$ in the absence of this "interaction bit". Of course this bit will not be independent because the actual realizations of $\boldsymbol{X}$ and $\boldsymbol{Y}$ sub-arrays will constraint the frontier oscillator candidates, and thus uncertainty of this single bit will be lesser than unity: call this bit's contribution to entropy u and let it be (by now) a function of the subsystems sizes,[1] $u = u(X, Y)$. This lets us write the entropy of the whole system $\boldsymbol{N}$ as

$$S_{\mathcal{N}_{\diagdown 1}}[\boldsymbol{N}] = S_{\mathcal{N}_{\diagdown 1}}[\boldsymbol{X}] + S_{\mathcal{N}_{\diagdown 1}}[\boldsymbol{Y}] + u(X, Y) \tag{25}$$

and using (21),

$$S_{\mathcal{N}_{\diagdown 1}}[\boldsymbol{N}] = S_{\mathcal{N}_{\diagdown 1}}[\boldsymbol{X} \circ \boldsymbol{Y}] + u(X, Y) \tag{26}$$

Equivalently we could decompose the system in two different sub-arrays, $\boldsymbol{N} = \boldsymbol{X}', \boldsymbol{Y}'$ which drives to

$$S_{\mathcal{N}_{\diagdown 1}}[\boldsymbol{N}] = S_{\mathcal{N}_{\diagdown 1}}[\boldsymbol{X}' \circ \boldsymbol{Y}'] + u(X', Y') \tag{27}$$

[1]Notice that every subsystem of the same size is equivalent, since only relative ordering of the system members is relevant.

TABLE 1. Number of operations needed to find a random key in brute force attack and dictionary attack on $\mathcal{N}_{\diagdown 1}$ topology. Non uniformity on responses distribution leads to effective dictionary attack.

N	Random (r)	Dictionary (d)	r/d
5	7.53	4.93	1.53
9	126.76	61.14	2.07
17	32923	9710	3.39
21	52203	129151	4.04

Systems $\boldsymbol{X} \circ \boldsymbol{Y}$ and $\boldsymbol{X}' \circ \boldsymbol{Y}'$ are equivalent, for both consist of the same number of oscillators,

$$X + Y = N = X' + Y' \tag{28}$$

and span the same number of bits,

$$\begin{aligned} X_b + Y_b &= X - 1 + Y - 1 \\ &= N - 2 \\ &= X' + Y' - 2 \\ &= X' - 1 + Y' - 1 \\ &= X'_b + Y'_b \end{aligned} \tag{29}$$

Thus $S_{\mathcal{N}_{\diagdown 1}}[\boldsymbol{X} \circ \boldsymbol{Y}] = S_{\mathcal{N}_{\diagdown 1}}[\boldsymbol{X}' \circ \boldsymbol{Y}']$, and equating (26) to (27) we have

$$u(X, Y) = u(X', Y') \quad \forall X, Y \tag{30}$$

Once it has been proved that the increment of entropy is constant with the addition of new oscillators to the array, it is evident that the entropy function of $\mathcal{N}_{\diagdown 1}$ topology grows linearly with N,

$$S_{\mathcal{N}_{\diagdown 1}}(N) \sim N \tag{31}$$

DICTIONARY ATTACK ON $\mathcal{N}_{\diagdown 1}$ TOPOLOGY

This topology, despite the introduction of a new physical oscillator to every comparison, must be treated carefully because the digitization algorithm gives raise to non-uniformities in the probability distribution which are sensible to be exploited by an adversary, as stated before. As an example we have performed an easy dictionary attack over a series of PUF responses, i.e., an optimal brute force search where guessing candidates are chosen consistently with the probability distribution of this scheme (see Fig. 17). This experiment consists of three different stages: in the first place we construct and reorder the histogram of the N-oscillators distribution using a subset of the experimental data. Afterwards, we use a different subset of data to generate a number of PUF responses (in this case 10^4 numbers). Finally we try to find out each PUF response by two different methods: random guessing and dictionary attack. The average number of trials needed to find all the responses for some N are shown in

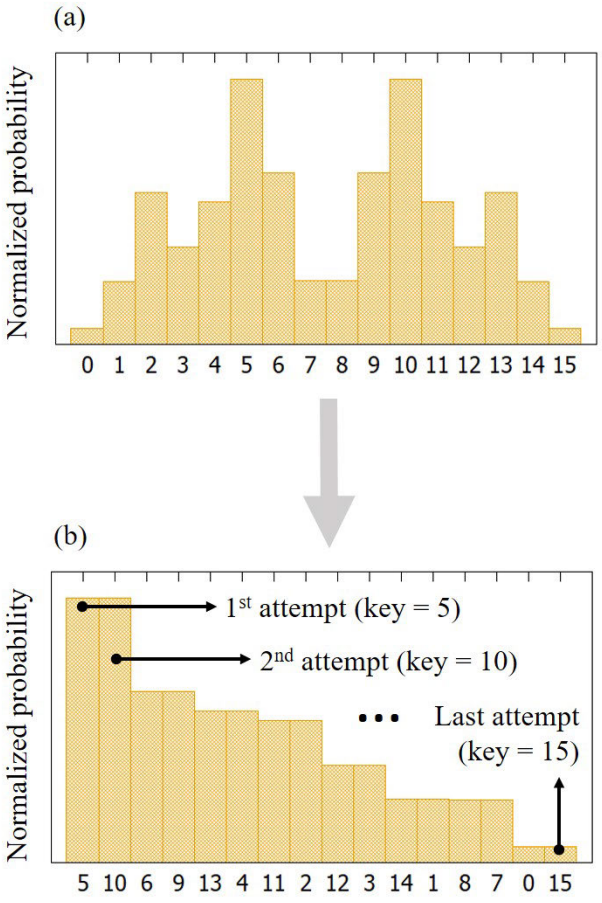

FIGURE 17. Visualization of a dictionary attack on $\mathcal{N}_{\diagdown 1}$ topology: the response distribution of $N = 5$ oscillators in (a) is re-sort in descending order of probability, such that illegitimate keys chosen from left to right in (b) minimize the time required to break this security system.

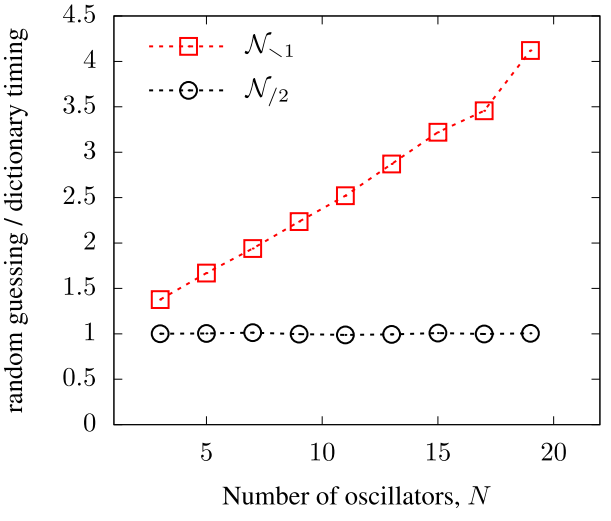

FIGURE 18. Ratio between the number of trials needed to break RO-PUF for brute force attack / dictionary attack in topologies $\mathcal{N}_{\diagdown 1}$ and $\mathcal{N}_{/2}$.

Table 1. In Fig. 18 we have plotted the ratios "random" to "dictionary" for PUF responses of different bit length under

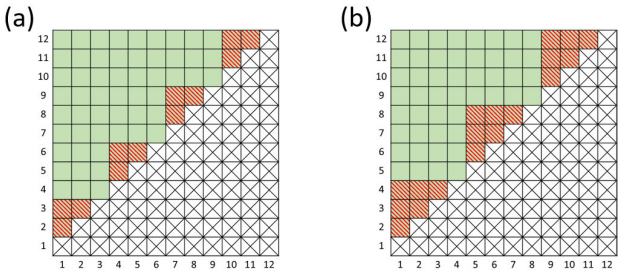

FIGURE 19. Comparison scheme for an array of $N = 12$ oscillators under $\mathcal{N}^2_{/k}$ topology: (a) k=3, (b) k=4.

topologies $\mathcal{N}_{\diagdown 1}$ and $\mathcal{N}_{/2}$. This makes clear how $\mathcal{N}_{\diagdown 1}$ non-uniformity speeds up the searching, thus weakening the PUF further than expected despite an apparently efficient use of physical resources. This is merely an example of how digitization has an impact on security properties beneath circuit architecture; other ways of exploiting this lack of uniformity can be imagined, e.g. bit correlation might be used to support modeling attacks, etc.

D. TOPOLOGY $\mathcal{N}^2_{/k}$

Although we have just seen an approach where good entropy and entropy-related quantities might fail in proving a system to be secure due to poor distribution uniformity, entropy still stands as a lower bound to guesswork. Thus, this shortcoming can be bypassed if the production of entropy (relative to physical properties of the PUF, in this case the number of oscillators) happens to be enough to compensate for the bit correlation.

Driven by this idea we have combined the benefits of avoiding repetition in oscillator comparison as much as possible (a task where the *1-out-of-k* masking performs good), while keeping a high entropy per oscillator rate (such as the case of comparing all possible pairs). Putting these two constructions together gives raise to the *k-modular* ($\mathcal{N}^2_{/k}$) topologies family. These are constructed by taking apart the array of ring oscillators in N/k groups of k oscillators; each group will be treated like an independent RO-PUF of $N = k$ oscillators, and will be evaluated in an $\mathcal{N}^2$ fashion to produce $k(k-1)/2$ bits. Thus, the total number of bits extracted from this topology in $N(k-1)/2$ bits. Since every group is unconnected to the rest, the total entropy deployed by this system will be $S_{\mathcal{N}^2_{/k}} = N/k \times \log_2 k!$. It is noticeable that the topologies referred as $\mathcal{N}^2$ and $\mathcal{N}_{/2}$ are particular cases of $\mathcal{N}^2_{/k}$ for $k = N$ and $k = 2$ respectively. In this work we have focused on $k = 3$ and $k = 4$ -modular properties (see the schematic representations in Fig. 19), whose probability distributions for different N-long arrays are shown in Fig. 20. It exhibits a similar shape as that of $\mathcal{N}^2$ topology, where all possible states are visited with the same probability (yet, the states space is smaller than 2^{N_b} which leads to some "white spaces" in the histograms). However, it suffices to

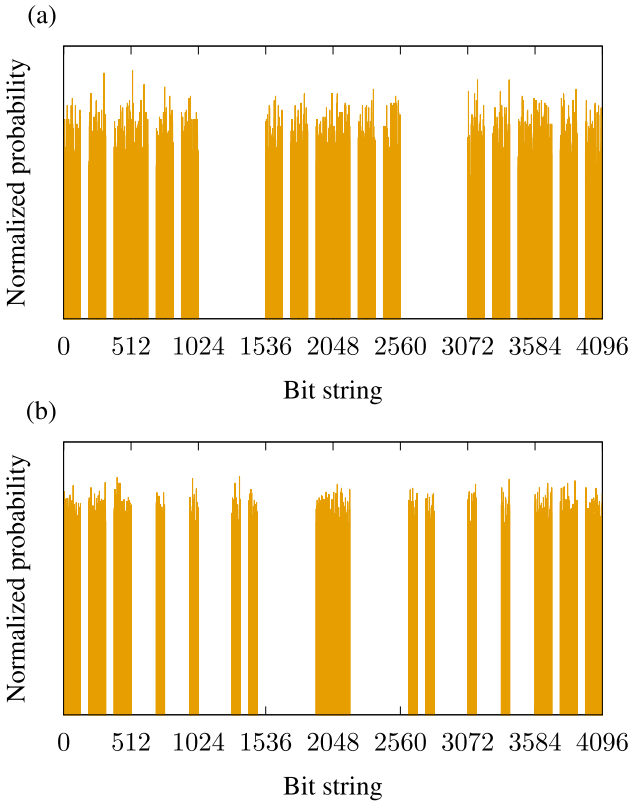

FIGURE 20. Responses histograms under $\mathcal{N}^2_{/k}$ topology for $N = 12$ oscillators: (a) topology $\mathcal{N}^2_{/3}$ and (b) topology $\mathcal{N}^2_{/4}$.

prevent exploitation from distribution variability such as the dictionary attack exemplified in the previous section.

E. COMPARISON BETWEEN TOPOLOGIES

The Shannon entropy -related quantities that we have used to characterize each topology security properties are:

- *Shannon entropy per oscillator rate* (S/N) [29], [31] as a measure of the system performance in terms of resource consumption, since power consumption is related to switching activity [35], which grows with the number of oscillators.
- *Shannon entropy per bit rate* (S/N_b) [9], [27] as a measure of the resistance that the system is capable to exhibit to cryptanalysis.

In Fig. 23 we have plotted: *a)* entropy per oscillator rate (S/N) and *b)* entropy per bit (S/N_b) against the string length of PUF responses, for the topologies studied: $\mathcal{N}^2$ (black), $\mathcal{N}_{/2}$ (red), $\mathcal{N}_{\setminus 1}$ (blue), $\mathcal{N}^2_{/3}$ (green) and $\mathcal{N}^2_{/4}$ (magenta). The points in these figures are interpolated by solid lines in agreement with the arguments given above: $\mathcal{N}_{/2}$ topology is interpolated according to Fig. 16, $S_{\mathcal{N}_{/2}} = 0.5N$, which leads to rates $S/N = 0.5$ bits per oscillator (red curve in Fig. 23.a), and $S/N_b = 1$ bits per bit response (red in Fig. 23.b). On the other hand, topology $\mathcal{N}_{\setminus 1}$ is linearly extrapolated beyond the experimental measurements supported by the arguments given in Section II as $S_{\mathcal{N}_{\setminus 1}} = 0.9N - 0.8$. On the asymptotic

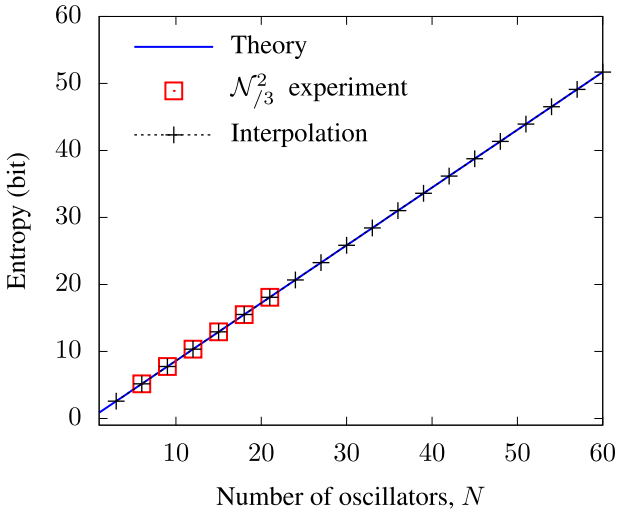

FIGURE 21. Entropy delivered by $\mathcal{N}^2_{/3}$ topology against the number of oscillators. Progression is linear on N as expected.

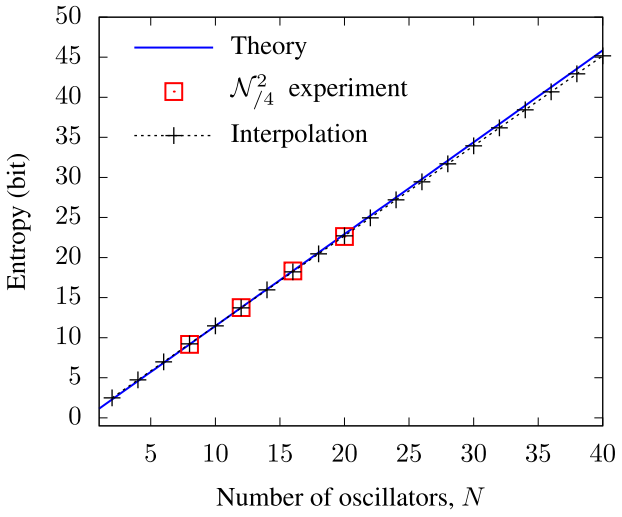

FIGURE 22. Entropy delivered by $\mathcal{N}^2_{/4}$ topology against the number of oscillators. Progression is linear on N.

limit of large N, $S/N \sim 0.9$ bits per oscillator (blue line in Fig. 23.a), and $S/N_b \sim 0.9$ bits per bit response (blue in Fig. 23.b).

For the remaining analyzed topologies $\mathcal{N}^2$ and $\mathcal{N}^2_{/k}$ with $k = 3$ and $k = 4$, we dispose theoretical interpolation curves whose excellent agreement with experimental data is plotted in Figs. 8, 21 and 22 respectively. In the limit of large N, entropy rates of $\mathcal{N}^2$ can be stated making use of Stirling's formula, $S_{\mathcal{N}^2}/N \sim \log_2 N$ (black line in Fig. 23.a) and $S_{\mathcal{N}^2}/N_b \sim \log_2 N/(N-1) \to 0$ (black line in Fig. 23.b).

Regarding the proposed new topologies, $\mathcal{N}^2_{/3}$ behaves like $S_{\mathcal{N}^2_{/3}}/N \sim 0.86$ bits per oscillator (green line in Fig. 23.a), which happens to be the same as entropy per bit rate (green line in Fig. 23.b), while $\mathcal{N}^2_{/4}$ topology exhibits a nice trade-off between both quantities, delivering $S_{\mathcal{N}^2_{/4}}/N \sim 1.15$ bits per

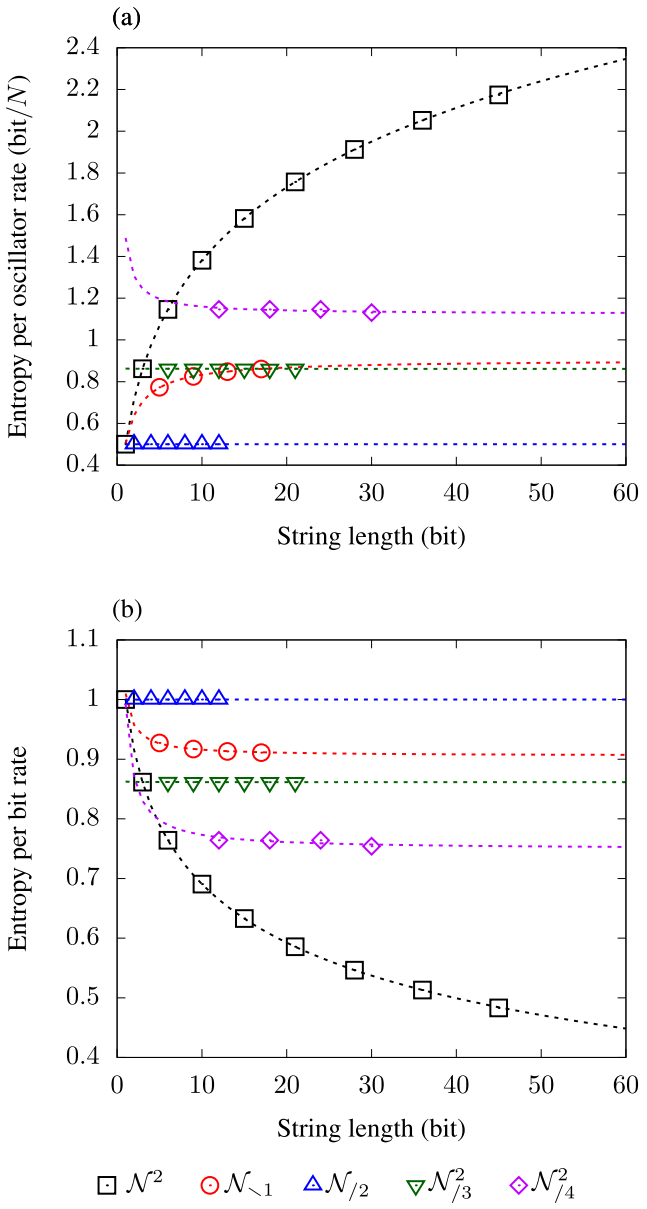

FIGURE 23. Entropy densities for every studied topology against the response length for: (a) entropy per oscillator rate, (b) entropy per bit rate. Experimental data are represented with points, and interpolation curves with dashed lines.

oscillator (magenta in Fig. 23.a) and $S_{\mathcal{N}^2_{/4}}/N_b \sim 0.76$ bits per bit-response (magenta in Fig. 23.b).

Finally for the sake of completeness, we have estimated the Hamming intra-distance as a measure of reliability, which is defined as

$$\mu_{\text{intra}} = \frac{1}{\text{No. repetitions}} \sum_{i<j}^{\text{No. repetitions}} \text{HD}\left(\boldsymbol{N_b}^i, \boldsymbol{N_b}^j\right) \quad (32)$$

where HD stands for the Hamming distance, which is the number of different symbols between two strings.

The results provided in Table 2 have been obtained through one thousand frequency measurement repetitions (using the same technique stated in Section III); afterwards the PUF response has been generated to each corresponding topology in order to obtain approximately 64 bits, which implies using a different number of oscillators depending on the topology. This analysis shows that the reliability of the PUF is not derated by the introduction of the new topologies (as would be expected since these metrics only depend on the physical properties of the circuit), which allows us to conclude that the proposed digitization schemes $\mathcal{N}^2_{/3}$ and $\mathcal{N}^2_{/4}$ do not introduce artifacts in the production of bit-strings.

TABLE 2. Average Hamming intra-distance μ_{intra} measured for the studied topologies (within the same physical FPGA).

Topology	N_b (N)	μ_{intra} (%)
$\mathcal{N}^2$	66(12)	6.46
$\mathcal{N}_{\diagdown 1}$	64(65)	7.14
$\mathcal{N}_{/2}$	64(128)	6.81
$\mathcal{N}^2_{/3}$	64(64)	6.07
$\mathcal{N}^2_{/4}$	66(44)	5.73

V. CONCLUSION

In this work we have analyzed the outcome probability distribution of a ring oscillator PUF implemented in FPGA, on the light of the digitization algorithms only. All the methods studied, referred here as topologies of the PUF, belong to an extremely popular set of digitization techniques known as *compensated measuring*, which allow for both obtain a binary response intrinsically, as well as strengthen the security system against environmental undesired influences. The parameters of the experiments performed to characterized these algorithms were the topology ($\mathcal{T}$), and the number of oscillators (N) which compose the RO array of the PUF (or equivalently the bit-length of the responses, N_b, which is fixed given a topology). All measurements were carried out at room temperature and constant voltage. In regards to the metrics used, we have characterize each $(\mathcal{T}, N)$ couple according to its density of entropy per oscillator (S/N, as a quantification of the performance in terms of consumption of resources, i.e., power and area) and entropy per bit-response (S/N_b, as a measure of security proficiency). Also, a cryptanalytic experiment was conducted on the popular $\mathcal{N}_{\diagdown 1}$ topology to make explicit the existence of weaknesses regarding digitization algorithms only.

The most remarkable aspect of the topologies studied is the behavior of entropy-related metrics for large N_b, since practical cryptological applications would lay on the asymptotic limit of these. At this respect, it is clearly pointed out that there is an inverse relation between efficient use of resources and security potential (which, in retrospective,

seems a very natural trade-off). Regarding this, our proposed topology family (particularly the $\mathcal{N}_{/4}^{2}$ one) occupies a central position in both plots, which highlights its potential to gather the best of both worlds and makes it a promising candidate for the practice of compensated measuring PUF design, furthermore, these conclusions clear the way for a study on hardware performance and machine learning attacks robustness.

REFERENCES

[1] D. Evans, "The Internet of Things: How the next evolution of the internet is changing everything," CISCO, San Jose, CA, USA, White Paper 2011, vol. 1, 2011, pp. 1–11.

[2] C. Perera, C. H. Liu, and S. Jayawardena, "The emerging Internet of Things marketplace from an industrial perspective: A survey," *IEEE Trans. Emerg. Topics Comput.*, vol. 3, no. 4, pp. 585–598, Dec. 2015.

[3] P. A. Laplante, M. Kassab, N. L. Laplante, and J. M. Voas, "Building caring healthcare systems in the Internet of Things," *IEEE Syst. J.*, vol. 12, no. 3, pp. 3030–3037, Sep. 2018.

[4] H. V. Poor and R. F. Schaefer, "Wireless physical layer security," *Proc. Nat. Acad. Sci. USA*, vol. 114, no. 1, pp. 19–26, Jan. 2017.

[5] M. Garcia-Bosque, G. Diez-Senorans, C. Sanchez-Azqueta, and S. Celma, "Introduction to physically unclonable fuctions: Properties and applications," in *Proc. Eur. Conf. Circuit Theory Design (ECCTD)*, Sep. 2020, pp. 1–4.

[6] 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.

[7] 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.

[8] U. Rührmair, J. Sölter, and F. Sehnke, "On the foundations of physical unclonable functions," in *Proc. IACR*, 2009, p. 277.

[9] H. Handschuh, G.-J. Schrijen, and P. Tuyls, "Hardware intrinsic security from physically unclonable functions," in *Towards Hardware-Intrinsic Security*. Berlin, Germany: Springer, 2010, pp. 39–53.

[10] R. Maes, "Physically unclonable functions: Constructions, properties and applications," Ph.D. dissertation, Dept. Elect. Eng., Katholieke Universiteit Leuven, Heverlee, Belgium, 2012.

[11] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, "Physical unclonable functions and applications: A tutorial," *Proc. IEEE*, vol. 102, no. 8, pp. 1126–1141, Aug. 2014.

[12] B. Gassend, D. Clarke, M. Van Dijk, and S. Devadas, "Silicon physical random functions," in *Proc. 9th ACM Conf. Comput. Commun. Secur. (CCS)*, 2002, pp. 148–160.

[13] J. D. Bekenstein, "How does the entropy/information bound work?" *Found. Phys.*, vol. 35, no. 11, pp. 1805–1823, Nov. 2005.

[14] 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.

[15] C. Martinez-Gomez and I. Baturone, "Calibration of ring oscillator PUF and TRNG," in *Proc. Eur. Conf. Circuit Theory Design (ECCTD)*, Sep. 2020, pp. 1–4.

[16] M. Choudhury, N. Pundir, M. Niamat, and M. Mustapa, "Analysis of a novel stage configurable ROPUF design," in *Proc. IEEE 60th Int. Midwest Symp. Circuits Syst. (MWSCAS)*, Aug. 2017, pp. 942–945.

[17] Z. Wei, Y. Cui, Y. Chen, C. Wang, C. Gu, and W. Liu, "Transformer PUF: A highly flexible configurable RO PUF based on FPGA," in *Proc. IEEE Workshop Signal Process. Syst. (SiPS)*, Oct. 2020, pp. 1–6.

[18] J. Teo, N. Hashim, A. Ghazali, and F. Hamid, "Ring oscillator physically unclonable function using sequential ring oscillator pairs for more challenge-response-pairs," *Indonesian J. Electr. Eng. Comput. Sci.*, vol. 13, pp. 892–901, Mar. 2019.

[19] B. L. P. Gassend, "Physical random functions," Ph.D. dissertation, Dept. Elect. Eng. Comput. Sci., Massachusetts Inst. Technol., Cambridge, MA, USA, 2003.

[20] H. Zhao and L. Njilla, "Hardware assisted chaos based IoT authentication," in *Proc. IEEE 16th Int. Conf. Netw., Sens. Control (ICNSC)*, May 2019, pp. 169–174.

[21] M. Barbareschi, V. Casola, A. De Benedictis, E. L. Montagna, and N. Mazzocca, "On the adoption of physically unclonable functions to secure IIoT devices," *IEEE Trans. Ind. Informat.*, vol. 17, no. 11, pp. 7781–7790, Nov. 2021.

[22] G. Diez-Senorans, M. Garcia-Bosque, C. Sanchez-Azqueta, and S. Celma, "A new approach to analysis the security of compensated measuring PUFs," in *Proc. Eur. Conf. Circuit Theory Design (ECCTD)*, Sep. 2020, pp. 1–5.

[23] T. Schürmann and P. Grassberger, "Entropy estimation of symbol sequences," *Chaos, Interdiscipl. J. Nonlinear Sci.*, vol. 6, no. 3, pp. 414–427, 1996.

[24] R. Konig, R. Renner, and C. Schaffner, "The operational meaning of min and max-entropy," *IEEE Trans. Inf. Theory*, vol. 55, no. 9, pp. 4337–4347, Sep. 2009.

[25] B. Espinoza and G. Smith, "Min-entropy as a resource," *Inf. Comput.*, vol. 226, pp. 57–75, May 2013.

[26] D. Malone and W. G. Sullivan, "Guesswork and entropy," *IEEE Trans. Inf. Theory*, vol. 50, no. 3, pp. 525–526, Mar. 2004.

[27] S. S. Kumar, J. Guajardo, R. Maes, G.-J. Schrijen, and P. Tuyls, "The butterfly PUF protecting IP on every FPGA," in *Proc. IEEE Int. Workshop Hardw.-Oriented Secur. Trust*. Jun. 2008, pp. 67–70.

[28] U. Ruhrmair, J. Sölter, F. Sehnke, X. Xu, A. Mahmoud, V. Stoyanova, G. Dror, and J. Schmidhuber, "PUF modeling attacks on simulated and silicon data," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 11, pp. 1876–1891, Nov. 2013.

[29] T. McGrath, I. E. Bagci, Z. M. Wang, U. Roedig, and R. J. Young, "A PUF taxonomy," *Appl. Phys. Rev.*, vol. 6, no. 1, Mar. 2019, Art. no. 011303.

[30] Y. Gao, S. F. Al-Sarawi, and D. Abbott, "Physical unclonable functions," *Nature Electron.*, vol. 3, no. 2, pp. 81–91, 2020.

[31] R. Maes and I. Verbauwhede, "Physically unclonable functions: A study on the state of the art and future research directions," in *Towards Hardware-Intrinsic Security*. Berlin, Germany: Springer, 2010, pp. 3–37.

[32] C.-E. Yin and G. Qu, "LISA: Maximizing RO PUF's secret extraction," in *Proc. IEEE Int. Symp. Hardware-Oriented Secur. Trust (HOST)*, Jun. 2010, pp. 100–105.

[33] A. Maiti and P. Schaumont, "Improving the quality of a physical unclonable function using configurable ring oscillators," in *Proc. Int. Conf. Field Program. Log. Appl.*, Aug. 2009, pp. 703–707.

[34] A. Maiti and P. Schaumont, "Improved ring oscillator PUF: An FPGA-friendly secure primitive," *J. Cryptol.*, vol. 24, no. 2, pp. 375–397, 2011.

[35] Y. Nasser, J.-C. Prévotet, M. Hélard, and J. Lorandel, "Dynamic power estimation based on switching activity propagation," in *Proc. 27th Int. Conf. Field Program. Log. Appl. (FPL)*, 2017, pp. 1–2.

[36] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 27, no. 3, pp. 379–423, Jul./Oct. 1948.

GUILLERMO DIEZ-SENORANS 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.

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 eleven 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.

CARLOS SÁNCHEZ-AZQUETA was born in Zaragoza, Spain. He received the B.Sc. and M.Sc. degrees in physics from the University of Zaragoza, Zaragoza, Spain, in 2006 and 2010, respectively, the Dipl.Ing. degree in electronic engineering from the Complutense University of Madrid, Madrid, Spain, and the Helsinki University of Technology, Helsinki, Finland, in 2009, and the Ph.D. degree in physics from the University of Zaragoza, in 2012.

He is currently an Assistant Lecturer with the Department of Applied Physics, University of Zaragoza. He has coauthored more than 40 technical papers and 130 conference contributions. He has participated in 25 national and international research projects, ten of which as a Principal Investigator. His research interests include cryo-CMOS circuits in quantum computing applications, RF analog and mixed signal processing, active antennas for satellite communications, and hardware security. He is also a member of the Group of Electronic Design, Aragon Institute of Engineering Research, University of Zaragoza.

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, Aragon Institute of Engineering Research, University of Zaragoza. He has coauthored more than 130 technical papers and 320 international conference contributions. He is the coauthor 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.