A New Class of Digital Circuits for the Design of Entropy Sources in Programmable Logic

Tommaso Addabbo, *Member, IEEE*, Ada Fort, *Member, IEEE*, Riccardo Moretti, *Student Member, IEEE*, Marco Mugnaini, *Senior Member, IEEE*, Hadis Takaloo, *Student Member, IEEE*, and Valerio Vignoli, *Member, IEEE*

***Abstract*— We propose a novel class of Digital Nonlinear Oscillators (DNOs) supporting complex dynamics, including chaos, suitable for the definition of high-performance and low-complexity entropy sources in Programmable Logic Devices (PLDs). We derive our proposal from the analysis of simplified models, investigated as non-autonomous nonlinear dynamical systems under different excitation conditions. The study lead the authors to the design of a fully digital entropy source consuming only two slices of a Xilinx FPGA, including post-processing, sufficient to define a class of TRNGs capable to pass the NIST standard tests for randomness in any worst case experimentally tested by the authors (6 chips, 96 generators). The solution has been compared with others published in the literature, confirming the validity of the proposal.**

***Index Terms*— Digital nonlinear oscillators, nonlinear dynamical systems, information entropy sources.**

I. Introduction

ELECTRONIC information entropy sources find application in cryptography, e.g., for the design of systems devised to issue sequences of truly random bits [1], [2]. These systems, also known as True Random Number Generators (TRNGs), are circuits exploiting *sources of entropy* obtained measuring stochastic physical phenomena. Among the most investigated solutions, we recall TRNGs based on chaos, metastability, electronic noise, signal jitter and ionizing radiation [2]. TRNGs exploiting each of the above phenomena have been proposed in literature, and different combinations of them have been used.

The design of a cryptographic TRNG entropy source is a trade-off between hardware security, fabrication cost, reliability, throughput and energy efficiency, being these aspects dependent on the physical stochastic phenomenon taken into account for the TRNG concept design. With the advent of the Internet of Things, new principles and paradigms oriented the research toward the investigation of new solutions suitable for the industrial production of standardized scalable architectures, also convenient for the so-called lightweight cryptography. From this point of view, the investigation of reliable 'fully-digital' sources of entropy, i.e., for which design a Verilog or VHDL code almost suffices, represents a lively research direction targeting all the goals mentioned before [3]–[18].

In this work we investigate a novel class of circuits, defined as Digital Nonlinear Oscillators (DNOs), as possible candidates for a new class of 'fully-digital' entropy sources, suitable for cryptographic applications, aiming at the design of TRNGs in Programmable Logic Devices (PLDs). Framing our research within the published literature, in this work we discuss the topic from a nonlinear dynamical system analysis point of view. Indeed, we discuss theoretical models and propose numerical investigation techniques providing evidence that, for specific circuit topologies, the chief source of randomness in these systems is mainly due to deterministic chaos. In detail, taking as a reference a novel DNO topology, we show with simulations and experimental results that in this kind of systems the information generation rate can be high and structurally stable with respect to circuit variability, therefore resulting suitable for the design of reliable cryptographic TRNGs consuming an extremely reduced amount of logic resources.

This paper is organized as in the following. In Section II we introduce DNOs and investigate the simplified analog model of a circuit topology capable to support complex dynamics. The introduced circuit is proposed as a 'fully digital' nonlinear oscillator, and further investigated under possible external excitations, referring to actual digital circuits simulated in Cadence (Sec. III). On the basis of the obtained results, in Sec. IV we propose a novel DNO topology as a novel class of 'fully digital' circuits capable to support complex dynamics. Experiments, conclusion and references close the paper.

II. Digital Nonlinear Oscillators

An informal definition of Digital Nonlinear Oscillators have been first introduced in [19].

Definition 1: A Digital Nonlinear Oscillator (DNO) is a network of electronic digital circuits, each one originally designed to behave as an asynchronous logic gate, implementing an autonomous nonlinear dynamical system exhibiting oscillations in the time-continuous domain.

According to the definition, the network nodes do not refer to abstract logic functions. Rather, each node is associated to

Manuscript received October 3, 2019; revised January 22, 2020; accepted February 17, 2020. Date of publication March 11, 2020; date of current version July 1, 2020. This article was recommended by Associate Editor A. Oliveri. *(Corresponding author: Tommaso Addabbo.)*

The authors are with the Department of Information Engineering and Mathematics, University of Siena, 53100 Siena, Italy (e-mail: addabbo@dii.unisi.it).

Color versions of one or more of the figures in this article are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TCSI.2020.2977920

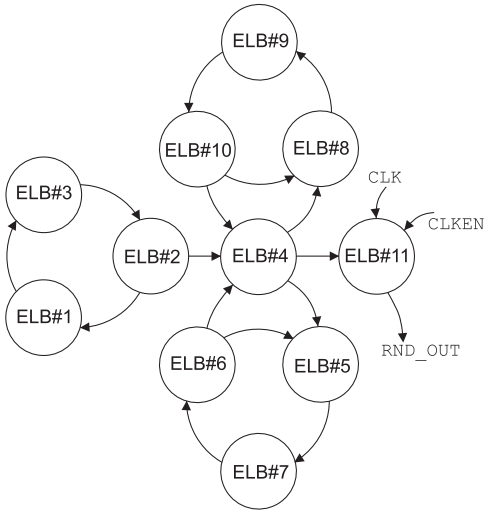

Fig. 1. A possible Digital Nonlinear Oscillator network topology, in which each node is referred as an Elementary Logic Block (ELB) implementing an asynchronous logic function. The ELB#11 is a leaf node not involved in any loop, described in Sec.III.

an electronic circuit, or a sub-circuit in a wider asynchronous architecture (e.g., a digital cell belonging to a standard library developed for a CMOS silicon process technology). In the next Section, since we refer to PLDs, we will deal with Elementary Logic Blocks (ELBs) implementing the network nodes (Fig. 1).

The well know Ring Oscillator circuit, a loop of an odd number of inverting logic gates, is among the simplest examples of a DNO. Other systems classifiable as DNOs have been presented in [14], [19]–[21].

Bringing together PLD design, circuit modeling and the analysis of nonlinear dynamical systems, a first investigation of different DNO architectures have been presented in [19], [21], [22]. The authors showed that, depending on both the network topology and the hardware implementation, DNOs can exhibit complex dynamical behavior.

The design of DNOs faces several challenges, probably the most important one being theoretical. In [19] a clear confutation of the algebraic approaches proposed to study some DNOs has been shown with both simulations and experiments. On the other hand, as discussed in [22], even for simple topologies a DNO is a nonlinear dynamical system operating in high dimension, being the dynamics dependent on parasitic elements in most cases (e.g., distributed nonlinear capacitors and resistors). For this reason, even for low-complexity DNO topologies, an accurate theoretical modeling is often unfeasible and the analysis must resort, eventually, to numerical simulations and experiments.

Regrettably, when simulating high-dimension nonlinear dynamical systems, the numerical analysis of any investigated model should be trusted with caution, due to the uncertain or scarcely controllable effects related to finite precision computation and time-integration algorithmic accuracy [23]. Furthermore, the dynamics of any DNO can be sensitive to noise, temperature or supply voltage variations, aging and silicon fabrication process variability. This latter

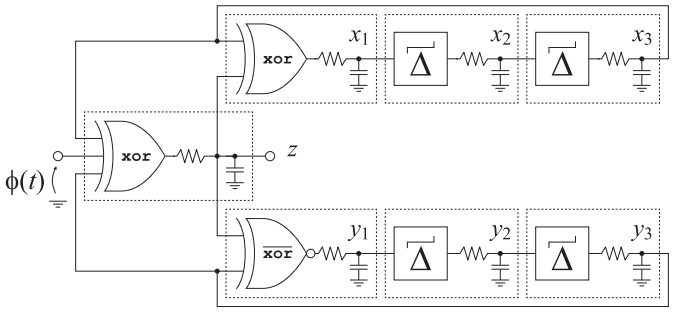

Fig. 2. A simplified model to investigate the core DNO sub-network implementing the non-autonomous dynamical system (2).

effects are well known, and also exploited, e.g., in Physically Unclonable Functions (PUFs) based on nonlinear dynamical systems [24]–[26]. As a result, for any DNO proposal three investigation levels are mandatory: modeling, simulations and experimental verification.

A. A Novel DNO Sub-Circuit Topology Compatible With Complex Dynamics

In this subsection we present a novel circuit topology suitable to design DNOs. The proposal, sketched in Fig. 2, originally derives from heuristic considerations collected by the authors during their research activities.

The circuit in Fig. 2 includes two `xor` gates, one negated `xor` (`nxor`) gate and three active delay nodes (`del`) resulting, e.g., from routing elements in PLDs (connection and switch boxes) [22]. A special symbol for the delay nodes has been introduced to remark that they are digital rectifying delay gates [19], [21], [22].

Resistors and capacitors have been introduced to define a simplified low-dimension theoretical model of the circuit. *It is understood that in effective implementations their role is played by parasitic nonlinear elements distributed on the chip*.

More accurate dynamical models must be taken into account to investigate the transient dynamics of DNO integrated implementation (e.g., by means of analog SPICE simulations based on advanced BSIM4 models, also considering post-layout extractions of digital standard cells). For this reason, we remark that the simplified analysis discussed in this Section aims to assess the compatibility of the proposed topology to support complex dynamics, without referring to any specific silicon process technology.

Accordingly, to reduce the system complexity, we assumed to relate each DNO node to a first-order cell, shown in Fig. 3, such that

$$\frac{dv_o}{dt} = \frac{g(\mathbf{v}_i) - v_o}{RC}, \tag{1}$$

where $\mathbf{v}_i = (v_1, v_2, \ldots, v_m) \in \mathbb{R}^m$ and $v_o \in \mathbb{R}$ are the inputs and output, respectively, and $g : \mathbb{R}^m \to [0, 1]$ describes the node DC analog transfer function $v_o = g(\mathbf{v}_i)$. It is clear from the function codomain that we assume to deal with a normalized phase space.

In this simplified model, any DNO node has high-impedance inputs, decoupled from its output. Furthermore, each of the

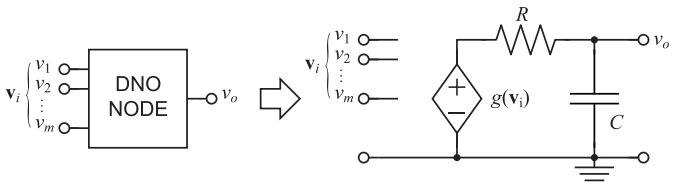

Fig. 3. A first-order nonlinear dynamical model.

two loops involving the nets x_1, x_2, x_3 and y_1, y_2, y_3 agrees with the oscillating topology investigated in [22].

Under this theoretical framework, the circuit in Fig. 2 can be modeled as a non-autonomous nonlinear dynamical system that operates in the normalized bounded phase space $[0, 1]^7 \subset \mathbb{R}^7$, i.e.,

$$\begin{cases} \dot{x}_1 = \alpha_1 \left[\texttt{xor2}(x_3, z) - x_1\right], \\ \dot{x}_2 = \alpha_2 \left[\texttt{del}(x_1) - x_2\right], \\ \dot{x}_3 = \alpha_3 \left[\texttt{del}(x_2) - x_3\right], \\ \dot{y}_1 = \beta_1 \left[\texttt{nxor2}(y_3, z) - y_1\right], \\ \dot{y}_2 = \beta_2 \left[\texttt{del}(y_1) - y_2\right], \\ \dot{y}_3 = \beta_3 \left[\texttt{del}(y_2) - y_3\right], \\ \dot{z} = \gamma \left[\texttt{xor3}(x_3, \phi(t), y_3) - z\right], \end{cases} \tag{2}$$

where $\alpha_i, \beta_i, \gamma \in \mathbb{R}^+$ are positive parametric constants, $\phi : \mathbb{R} \to [0, 1]$ is an arbitrary excitation signal, whereas $\texttt{xor3} : \mathbb{R}^3 \to [0, 1]$, $\texttt{xor2} : \mathbb{R}^2 \to [0, 1]$, $\texttt{nxor2} : \mathbb{R}^2 \to [0, 1]$, $\texttt{del} : \mathbb{R} \to [0, 1]$ are functions properly fitting the analog DC transfer functions of reference `xor`, `nxor` and `del` logic gates, respectively. The parameters $\alpha_i, \beta_i, \gamma$ are equal to the reciprocals of time constants RC of their respective first-order cells, given in (1).

B. Modeling the Node DC Transfer Function

For the different g functions in (1) we considered the analytical compositions of parametric sigmoids of the form

$$\sigma(x, a, b) = \frac{1}{1 + e^{a(x-b)}}, \tag{3}$$

where $a, b \in \mathbb{R}$, with $0.3 < b < 0.7$ and $a > 20$. Accordingly, once set a, b, we define for any $i, j, k \in \mathbb{N}$

$$x_i(v_i) = x_i = \frac{1}{1 + e^{-a(v_i - b)}}, \tag{4}$$

$$\bar{x}_i(v_i) = \bar{x}_i = \frac{1}{1 + e^{a(v_i - b)}}, \tag{5}$$

and

$$\texttt{del}(v_i) = x_i, \quad \texttt{xor2}(v_i, v_j) = x_i\bar{x}_j + \bar{x}_i x_j, \tag{6}$$

$$\texttt{nxor2}(v_i, v_j) = x_i x_j + \bar{x}_i\bar{x}_j, \tag{7}$$

$$\texttt{xor3}(v_i, v_j, v_k) = (x_i x_j + \bar{x}_i\bar{x}_j)x_k + (x_i\bar{x}_j + \bar{x}_i x_j)\bar{x}_k. \tag{8}$$

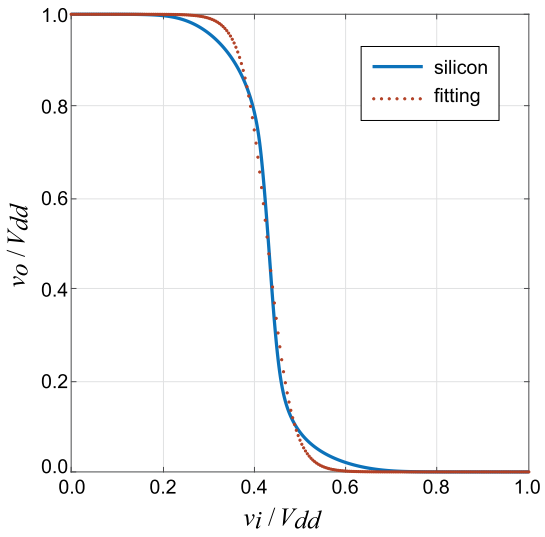

Fig. 4. The DC transfer function of a CMOS inverter (UMC 180nm technology, 1.8V) and the fitting model (5), with $a \approx 36.81$, $b \approx 0.43$.

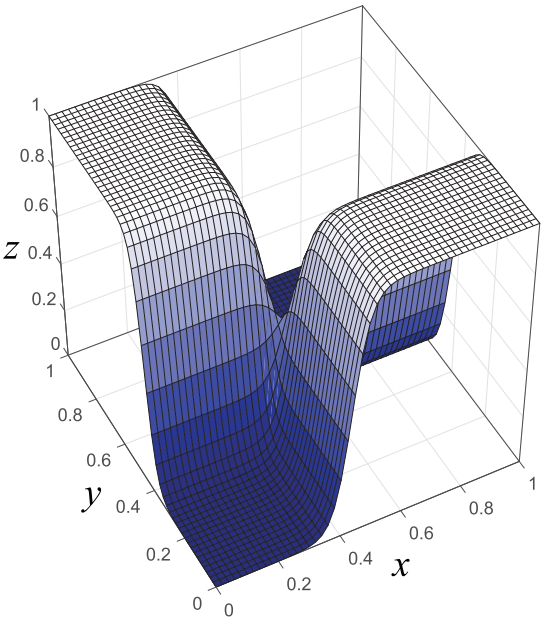

Fig. 5. The function $z = \texttt{xor2}(x, y)$ in (6) for $a \approx 36.81$, $b \approx 0.43$.

As shown in Figs. 4 and 5 proper values for a, b can be estimated to approximate the DC transfer function of actual CMOS digital circuits.

The study of the dynamical system (2) produced significant evidence to justify the design methodology followed by the authors to achieve the solution presented in this work.

C. System Analysis: Turned-Off Excitation

If the excitation in the circuit in Fig. 2 is turned off (i.e., $\phi(t) = 0$), the dynamical behavior of the system (2) depends on the system parameters $\alpha_i, \beta_i, \gamma$ and a, b in (3). For non-pathological parametric values (e.g., if $\alpha_i, \beta_i, \gamma$ have similar magnitudes) the obtained autonomous system has a stable and globally attractive limit cycle. In other words, when

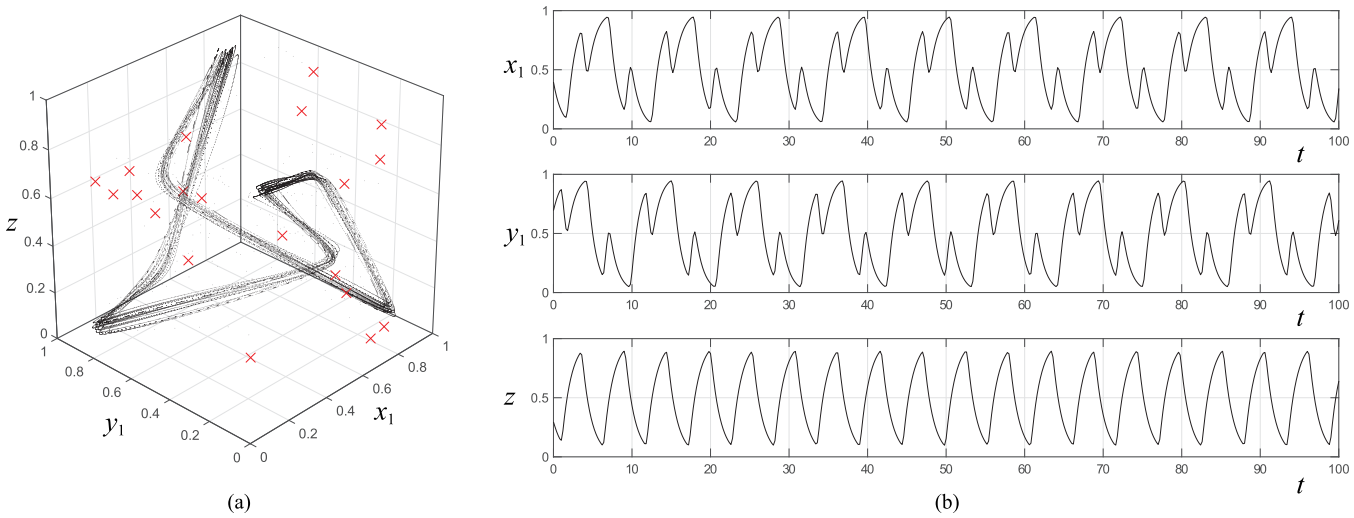

Fig. 6. Different globally attractive limit cycles for the system (2) (excitation turned off), under random Gaussian parametric perturbations ($3\sigma = 6\%$ relative perturbation for $a = 30, b = 0.5$, $3\sigma = 30\%$ relative perturbation for $\alpha_i, \beta_i, \gamma = 1$). Subplot (a): 3D projection (nets x_1, y_1, z) for 20 trajectories obtained from different random initial conditions. Subplot (b): transient evolution of selected state components, for one of the presented cases.

the excitation ϕ is turned off, the simplified circuit in Fig. 2 is a DNO. Exhaustive simulations, obtained integrating the system (2) with standard numerical methods, verified that the dynamical system is structurally stable with respect to parametric perturbations, as shown in Figs. 6.a. It can be noticed that the transient dynamics for the net z exhibits regular oscillations (Fig. 6.b).

D. System Analysis: Periodic Excitation

If the excitation in the circuit in Fig. 2 is turned on, the system (2) describes a forced nonlinear oscillator. In literature, different systems of this kind have been investigated from different points of view. Among the arbitrary set of forcing signals, periodic excitations represent a demanding research topic in terms of theoretical efforts and numerical investigation tools, even in elementary problems based on the well known Duffin and Van der Pol oscillators [27]–[30].

The equations in (2) do not allow for any feasible analytical approach, also considering the problem dimension, if the parametric space is included in the analysis. On the other hand, different numerical investigation methods are nowadays widely accepted to assess the dynamical behavior of complex systems.

A basic numerical anaysis was performed reducing the parametric set, assuming $\alpha_i = \beta_i = \gamma = \xi > 0$ in (2) and $a = 30$, $b = 0.5$ in (3). For the excitation, an adapted full-scale sinusoidal signal with frequency $f_0 = 1/T_0$ was considered, i.e.,

$$\phi(t) = \frac{1}{2}(1 + \sin(2\pi f_0 t)), \quad \phi(t) \in [0, 1]. \tag{9}$$

Accordingly, since the parametric set was reduced to two elements, f_0 and ξ, the adimensional ratio

$$Q = \frac{\xi}{f_0} \tag{10}$$

has been considered as the bifurcation parameter to investigate the system dynamics. The obtained results for $3.3 < Q < 30$ are reported in the bifurcation diagram shown in Fig. 7, in which the long-term dynamical behavior for the set of values $\{z(t_k) : t_k = kT_0 + \theta, 100 < k < 200\}$ has been recorded, referring to random initial conditions in $[0, 1]^7$.

The diagram exhibits a complex structural organization including period-doubling cascades and alternations of periodic-chaotic windows. Presence of chaos at the culmination of period-doubling cascades has been detected by numerical investigations of trajectory stability, sensitivity to the initial condition and frequency spectrum analysis. Also, the study revealed the coexistence of multiple attracting ω-limit sets, partitioning the extended phase state $[0, 1]^7 \cup [0, T_0)$ in disjoint basins of attraction. For the sake of a better presentation, in Fig. 8 we reported the route to chaos that follows the period-doubling cascade for $18 < Q < 20$. In the subplot (e), a broadband spectrum with some sharp peaks located at multiples of the excitation frequency f_0, indicates the clear onset of a chaotic motion [31], [32].

III. Toward the Definition of Novel 'Fully Digital' Chaotic Entropy Sources

Until nowadays, the chief sources of randomness claimed to be exploited in 'fully digital' solutions were timing-skew, metastability and electronic noise, causing jitter and phase noise in oscillators [2]–[12], [14]–[18], [33]–[37]. The results previously presented pose a fundamental question: is it possible to achieve chaos by the proper interconnection of digital gates?

Regarding the issue, to the best of our knowledge, no-evidence has been presented in literature adopting a dynamical system analysis point of view. For this reason, we spent an effort designing specific numerical simulations investigating digital circuits represented at their *analog* transistor level. Since we were focusing on PLDs, we have considered

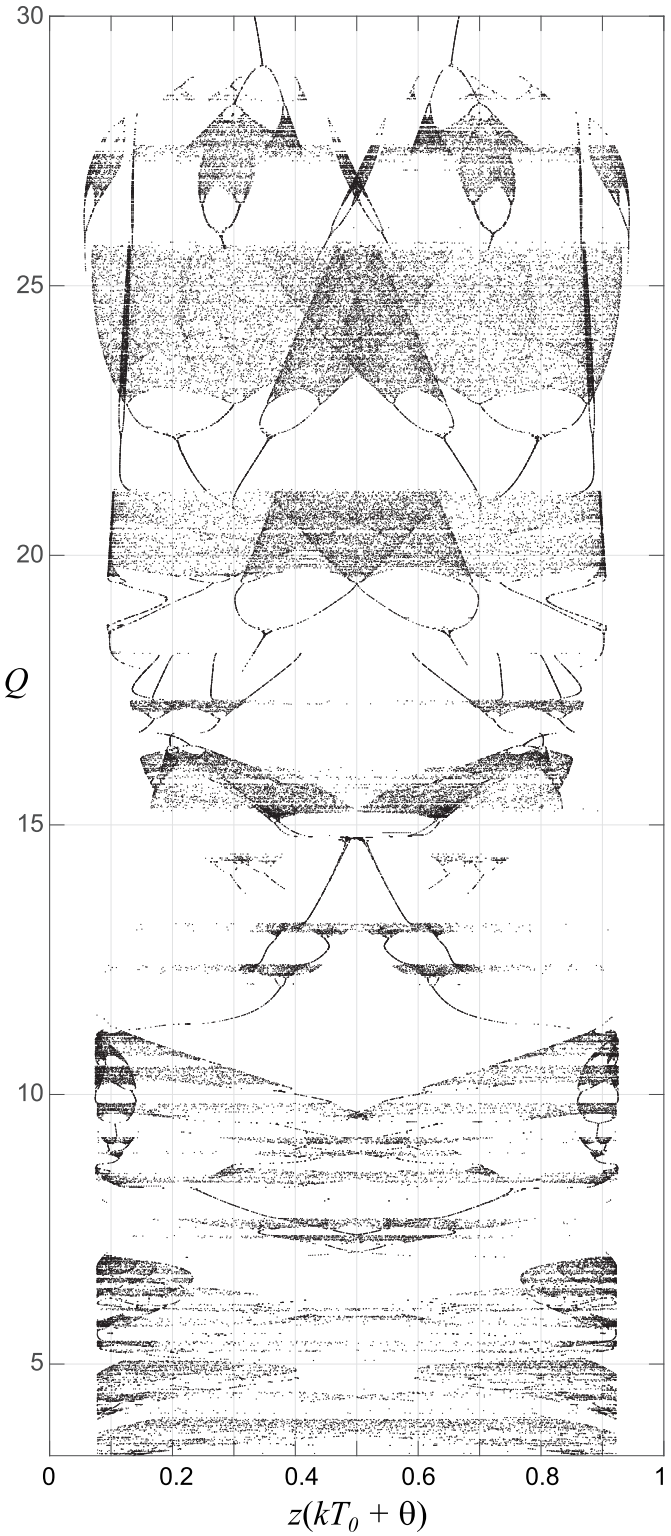

Fig. 7. Bifurcation diagram for the system (2) forced with the periodic excitation (9), reporting the set $\{z(t_k) \in [0, 1], t_k = kT_0 + \theta, 100 < k < 200\}$, for $\theta = 150$ deg and $3.3 < Q < 30$, assuming $\alpha_i = \beta_i = \gamma$ and $a = 30$, $b = 0.5$ in (3). Diagram obtained from 10.000 random initial conditions in $[0, 1]^7$ in $t = 0$.

low-complexity realistic models of the digital circuits available, e.g., in a FPGA [19], as described in the following.

The digital design resources in a FPGA include Registers, Connection/Switch Boxes and Look-Up Tables (LUTs).

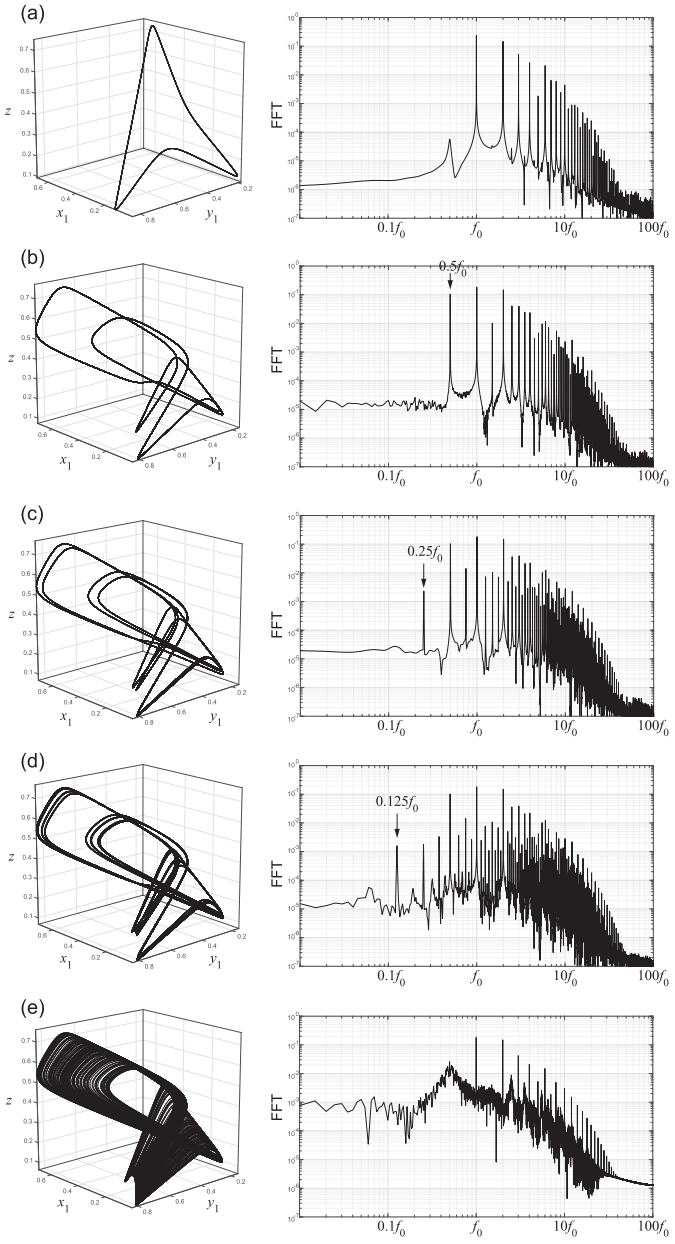

Fig. 8. The route to chaos that follows the period-doubling cascade revealed for $Q = 18.43, 19.42, 19.58, 19.61, 19.90$ in sub-plots (a) to (e), respectively, related to the bifurcation diagram shown in Fig. 7, for the system (2).

At a rough representation level, the combinatorial and the memorization functionality in a FPGA is organized in a 2D array of configurable logic circuits, each one offering multiple programming lines, as in the simplified architecture shown in Fig. 9. In the following, we name these reference structures as Elementary Logic Blocks (ELBs). Due to their topology, the nominal time-delay of an ELB does not depend on the combinatorial function set by its LUT (i.e., by the programming signals C0-C3 in Fig. 9).

The third type of ELB configuration shown in Fig. 9 has a clocked register along the signal path (D flip-flop). This configuration can not be included in any asynchronous loop of the DNO circuit topology. Nevertheless, it can be used as a leaf node of the DNO network, to obtain the sampling

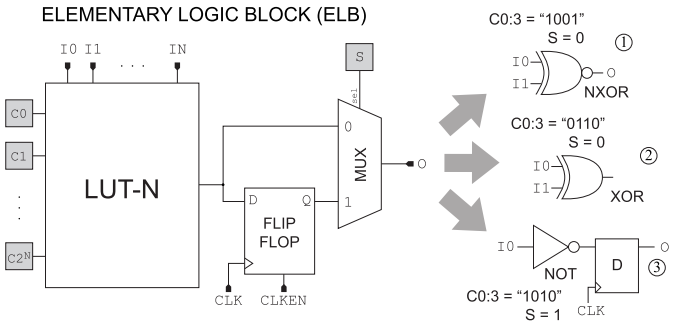

Fig. 9. Simplified structure of a FPGA configurable Elementary Logic Block (ELB). In a Digital Nonlinear Oscillator (DNO), different ELB configurations can be used to design different network nodes.

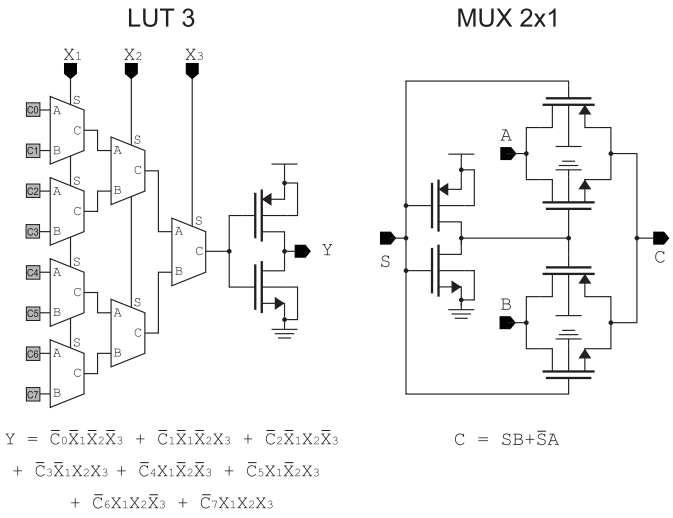

Fig. 10. The logic circuits implementing the ELB core shown in Fig. 9. Depending on the programming lines C0-C7, any logic function $f : \{0, 1\}^3 \rightarrow \{0, 1\}$ can be obtained.

and the analog-to-digital conversion (1-bit resolution) of those voltages that are *observable*, performing a measurement tasks. Indeed, most of the dynamical system state components refer to parasitic distributed elements in ELBs or Connection/Switch Boxes, i.e., they are actually *unobservable states* of the dynamical system.

FPGA vendors (e.g., Xilinx, Altera) provide special directives for the digital synthesizer, to be included in the RTL design (either in VHDL or Verilog), to neglect combinatorial loop errors and the deletion of design entities during the synthesis and optimization processes, also allowing precise resource placement and routing in the FPGA device.

We have designed in Cadence Virtuoso different CMOS circuits implementing the ELB reference structure shown in Fig. 9, using standard digital CMOS topologies (UMC 180nm technology, core voltage 1.8V) [38]. In detail, we considered ELBs containing 3-inputs LUTs (3 2×1 MUX-layers and 8 programming lines C0-C7), shown in Fig. 10.

In Cadence Virtuoso we designed the topology shown in Fig. 2, using three ELBs for the `xor` and `nxor` gates, whereas the delay nodes (`del`) were obtained adding multiplexing active routing elements along the loops (Fig. 11).

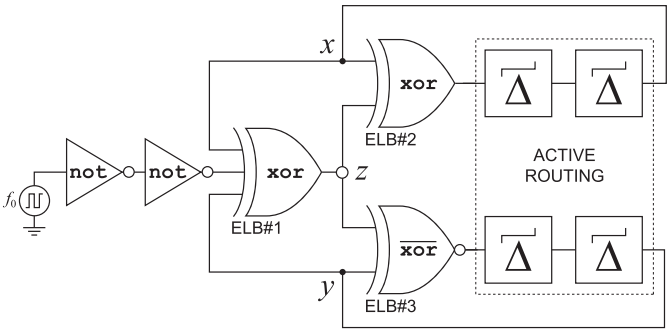

Fig. 11. The circuit simulated in Cadence Virtuoso, referring to UMC 180nm CMOS technology, core voltage 1.8V.

To take control of the high-dimension state initial condition in the simulation, negligible grounded capacitors (5 attofarad) have been added in *all* circuit nets.

A. Simulation Results

Transient simulations confirmed that by turning off the excitation $\phi(t) = 0$V the designed circuit resulted in a structurally stable nonlinear oscillator. On the other hand, an excitation was simulated adding a periodic square wave generator (levels 0V - 1.8V, variable frequency f_0) followed by two CMOS inverting gates, as shown in Fig. 11.

Following the same approach discussed in Sec. II-D, an adimensional ratio $Q' = \frac{\xi'}{f_0}$ has been defined as the bifurcation parameter to investigate the system dynamics, being ξ' a constant proportional to the natural period of the autonomous nonlinear oscillator ($\phi(t) = 0V$), estimated with previous simulations. The obtained bifurcation diagram, shown in Fig. 12, recorded the long-term dynamical behavior for the set of values $\{z(t_k) : t_k = kT_0 + \theta, 100 < k < 200\}$, for a random initial condition. The reported range for Q' corresponds to a range for f_0 between 400MHz and 425MHz.

Similarly to the theoretical case, the obtained bifurcation diagram exhibits a complex structural organization including period-doubling cascades and alternations of periodic-chaotic windows. Again, presence of chaos at the end of period-doubling cascades has been detected by numerical investigations of trajectory stability, sensitivity to the initial condition and frequency spectrum analysis. Again, the study revealed the coexistence of multiple attracting ω-limit sets, partitioning the extended phase state in disjoint basins of attraction, triggering different dynamics. For the sake of a more complete presentation, in Fig.13 we reported three cases showing period-doubling and chaos for $Q' = 13.17, 13.1813.27$ in the 3D-projections of the voltages x, y, z in Fig. 11. Due to the high-gains involved in the digital transfer functions, the dynamics is most of the time saturated at the boundaries of the cube $[0V, 1.8V]^3$.

IV. A New Class of Digital Circuits for the Design of Entropy Sources in Programmable Logic

The authors exploited the previous results to design a novel DNO topology. The idea was to substitute the excitation source in Fig.11 with a ring oscillator, as shown in Fig. 14. As a result,

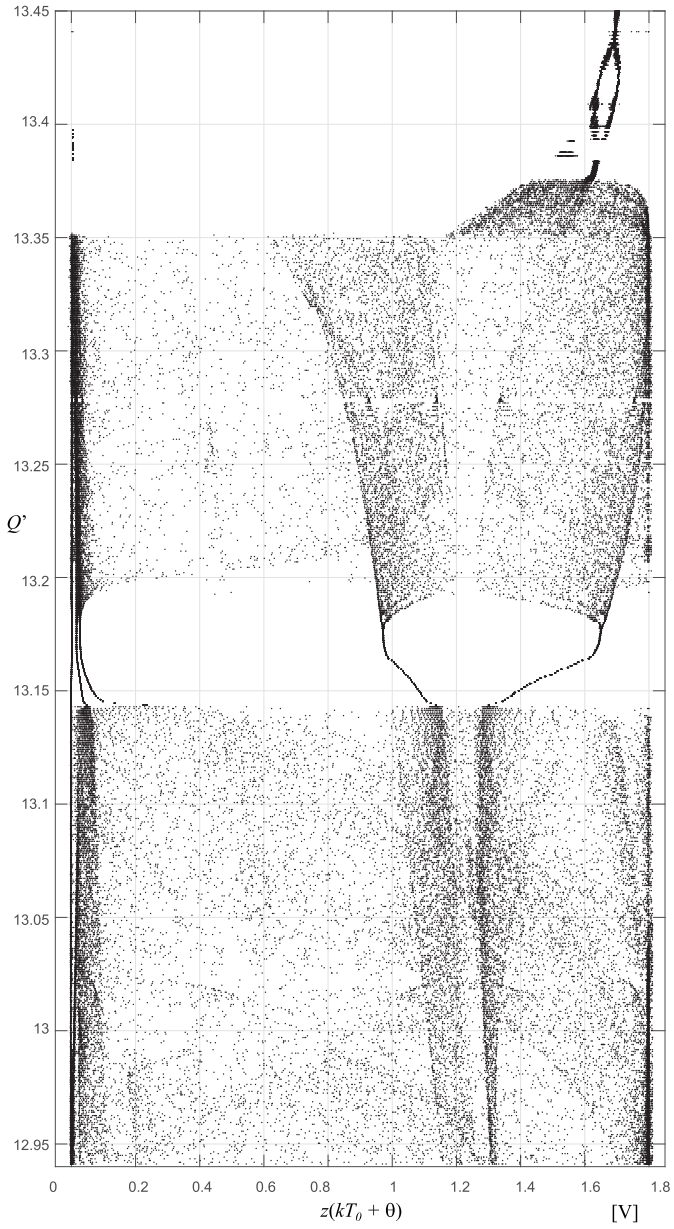

Fig. 12. Bifurcation diagram obtained by simulating the circuit in Fig. 11, reporting the set $\{z(t_k) \in [0V, 1.8V], t_k = kT_0 + \theta, 100 < k < 200\}$, for $\theta = 30\,\text{deg}$, setting the same initial condition in all cases.

the obtained DNO topology agrees with the network shown in Fig. 1, in which the ELBs #9, #10, #6 and #7 (i.e., the delay nodes derived from the first proposal in Fig. 2), were implemented *exploiting active routing elements* (details about the hardware implementation are discussed in Sec. IV-B).

The DNO in Fig. 14 is a 'fully digital' autonomous nonlinear dynamical system, that can be designed in a digital flow as a *network of HDL entities*. In principle, the resulting system can not be directly related to the forced oscillator case shown in Fig. 11, since between the 'driving' Ring Oscillator and the 'driven' oscillator a different sort of coupling may occur by means of parasitic capacitances in actual circuit implementations. However, as also confirmed by exhaustive Cadence simulations and experiments, the circuit is suitable for

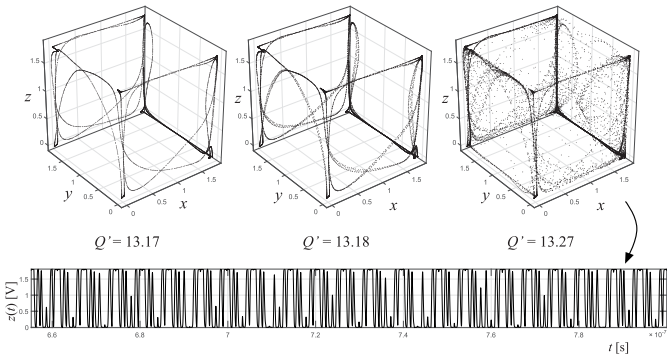

Fig. 13. Three cases showing period-doubling for $Q' = 13.17, 13.18$ and chaos for $Q' = 13.27$ in the 3D-projections of the voltages x, y, z in Fig. 11. For the last chaotic case, the transient simulation of the signal z is reported.

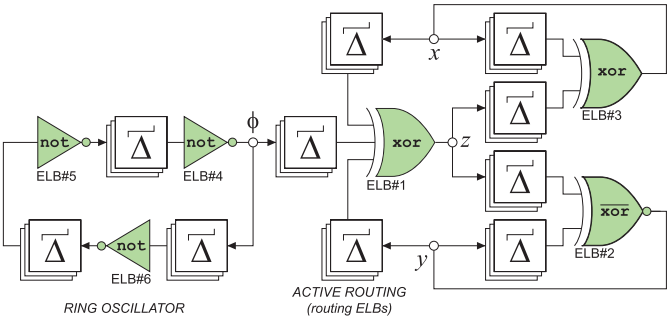

Fig. 14. The complete topology, proposed as representative of a novel class of DNOs, in which a nonlinear oscillating structure (the nonlinear oscillator in Fig.11), is excited by a ring oscillator to produce complex dynamics.

supporting complex periodic dynamics and chaos, depending on the dynamical characteristics of the involved digital circuits.

A. Simulation Results

The circuit proposed in Fig. 14 offers interesting design challenges. The ratio between the 'driving' ring oscillator frequency and the natural frequency of the 'driven' oscillator can be varied playing with the number of nodes in the three loops. However, the simulation results (including Montecarlo analysis) showed that other important aspects can play a significant role in determining the system dynamics. In detail:

- given the nominal circuit design, transistor mismatches and process variability, as well as other implementation results not under the direct control of the PLD designer (i.e., the delays of the Connection/Switch Boxes involved by the routing), can lead to different complex dynamics, including chaos. In Fig. 15 we reported two example simulations (same nominal circuit, different mismatches);
- given any simulated hardware realization, multiple attracting ω-limit sets can coexist, partitioning the system phase state in disjoint basins of attraction related to different dynamical behaviour;
- given the simulated hardware realization, if noise is added in the simulation, switching between different attracting ω-limit sets may occur.

The provided evidence establishes that the resulting dynamics is highly sensitive to relevant aspects that are out of the designer's control.

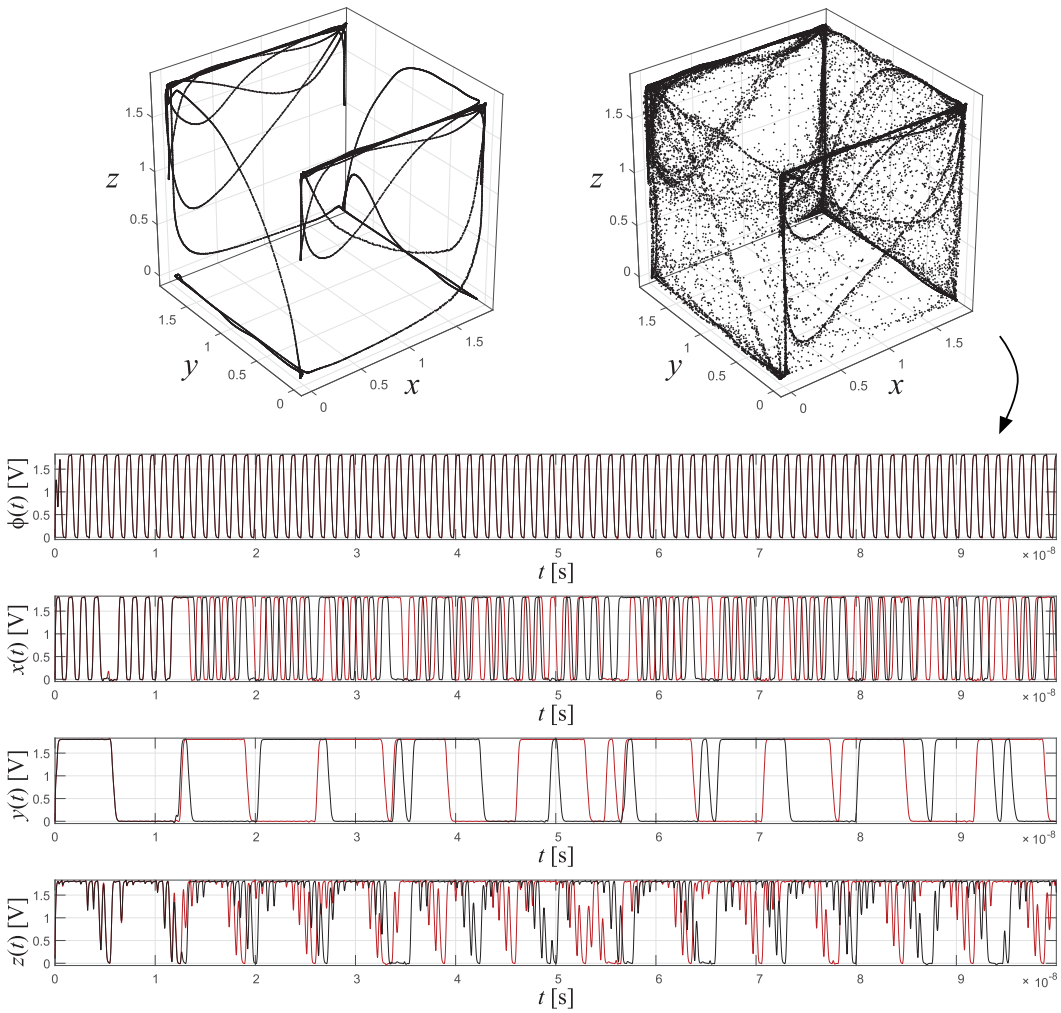

Fig. 15. In the upper plots, the 3D-projections of the voltages x, y, z in Fig. 14 under different realizations (mismatches and process variability). Upper-left: complex periodic dynamics. Upper-right: chaotic dynamics exhibiting sensitivity to initial conditions, highlighted in the trajectories below.

In facts, this issue does not represent a real drawback when targeting information entropy sources, if *in any worst case* the circuit performs better than any other known solution involving the same hardware complexity.

B. Experiments: Raw Entropy Source Low-Level Characterization

The DNO in Fig. 14 has been first compared with two other DNOs, namely a 7-nodes Ring Oscillator (DNO A) and a 7-nodes Golíc Galois Ring Oscillator (DNO B) [19], [21], by means of the measurement campaign hereafter discussed. We have chosen these solutions for the comparison because of the following reasons: 1) they involve a similar hardware complexity; 2) they exhibit stable simple and complex periodic dynamics, respectively; 3) in both of them the chief information generation mechanism has been shown to be due to phase noise and jitter caused by electronic noise. Furthermore, these DNOs have been characterized taking as a reference figures of merit assessing specific low-level entropy harvesting mechanisms, also suitable for investigating their statistical structural stability with respect to the technological process variability.

The comparison of the DNOs has been performed, assuming to add a leaf-node to the network (the third ELB configuration in Fig. 9) to perform uniform sampling and one-bit A/D conversion, designing a binary information source.

The 'non-IID track' included in the NIST SP800-90B publication [39] proposes a battery of tests to estimate the entropy of raw-bit sources. The procedure, taking the minimum among multiple entropy estimates, provides an articulated estimation of the source entropy, necessary to validate any design in absolute terms. However, the approach turns out not to be the best option when comparing different classes of DNOs, if the comparison focuses on those fundamental aspects regarding the information generation mechanisms in phase-noise oscillators: the correlation between the generated bits and the diversification of the generated symbols, considering groups of contiguous bits. For this reason, in this work we adopted the two figures of merit discussed in [21]: the Decorrelation Time and the Average Shannon Entropy. Obviously, the two figures of merit are related to the estimators in [39].

The measurements have been performed designing the DNOs in Xilinx Artix 7 xc7a35 FPGAs running at 100MHz clock frequency. For each system 16 DNO instances were

TABLE I
DEVICE UTILIZATION AND MEASUREMENTS RESULTS

	Ring Oscillator (DNO A)	Galois Ring Oscillator (DNO B)	Proposed Circuit (DNO C)
CLBs	1	1	1
Slices	2	2	2
ELBs (LUTs)	7 (+1)	7 (+1)	6 (+1)
ASE-10_{max} [b/sym]	0.695	0.700	0.955
ASE-10_{mean} [b/sym]	0.613	0.664	0.949
ASE-10_{min} [b/sym]	0.530	0.610	0.937
τ_{min} [ns]	7380	6730	< 10
τ_{mean} [ns]	8893	8350	53
τ_{max} [ns]	9780	9740	80

designed in different chip areas of the FPGA, to assess the impact of intra-device variability on circuit performance. Furthermore, to investigate the device-dependency, the measurements were repeated for six different chips (using the same slice locations for the three DNO types), reaching a total of 96 DNO instances, for each class. The authors implemented different layouts, carefully investigating the place and route phase of the hardware design.

We collected random bits from the oscillators at different sampling frequencies (i.e., decimation rates), ranging from 100 kHz to 100 MHz, acquiring sequences of 1 million bits each. Buffering the binary stream on the FPGA RAM, and implementing a RS232 serial interface, we transferred the collected sequences to a PC running software developed with National Instruments LabVIEW, whose purpose was to read the serial interface and save the received data in different binary files, structured to be processed with Mathworks Matlab.

The Figs. 16 and 17 report the results for the estimated Average Shannon Entropy estimated on the basis of binary words of 10 bits (ASE-10), and the Decorrelation Time τ, differentiating the results for each DNO and for each chip number (16 instances per chip), for the maximum tested sampling rate of 100MHz. The Decorrelation Time was estimated as the time at which the vanishing autocorrelation function of the binary source expresses the 99.9% of its energy, referring to an observation time-window of 10μs, following the set-up discussed in [21].

The device utilization and the overall measurements statistics for the two figures of merit are reported in Table I. It can be noticed from the Table that the three DNOs consume the same amount of resources in the FPGA: one Xilinx Configurable Logic Block (CLB), two Slices, including the leaf-node to perform the uniform sampling.

As far as the figures of merit are considered, the proposed DNO dramatically outperforms the other two circuits, both in term of Decorrelation Time and Average Shannon Entropy. In detail, the proposed DNO is characterized by Decorrelation Times two orders of magnitudes lower than the best tested DNOs of other kinds, also considering different results published in literature [21]. In all cases, the bits collected at a sampling rate of 100MHz from the DNO-C resulted affected by negligible or undetectable correlation, as shown

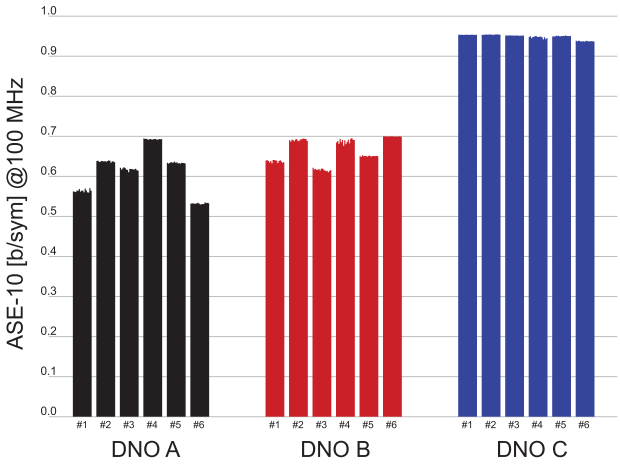

Fig. 16. Results for the Average Shannon Entropy, estimated on the basis of binary words of 10 bits (ASE-10).

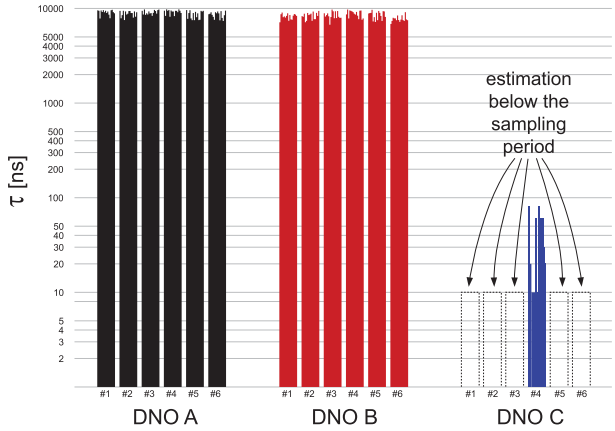

Fig. 17. Results for the Decorrelation Time τ, estimated as the time at which the autocorrelation function of the binary source expresses the 99.9% of its variation-energy, referring to an observation time-window of 10μs, following the set-up discussed in [21].

in Figs. 17 and 18. As a result, the chief limitation of the DNO-C resulted to be a residual offset of the sequences. This aspect is related to the combined effect of the analog signal mean value, dependent on the trajectory shape, and the quantization threshold level of the sampling D flip-flop. The issue is more evident in the DNO-B and less important for the Ring Oscillator generating an almost square wave with 50% duty cycle. If the DNO-B has a reduced correlation time, with respect to the DNO-A, it is affected by a strong bias limiting its ASE. In the DNO-C, an adequate bias appears to be guaranteed by the topological symmetry and by the mutual interaction through the `xor-3` gate of the balanced feedback loops in Fig. 14. The outstanding results obtained for our proposal indicate that, most probably, all the implemented instances of the DNO-C operated in a structurally stable chaotic region.

The comparison between the sources can be appreciated by inspecting the byte-patterns shown in figure 19, in which we reported the results for the DNOs with the highest ASE-10 entropy, including the worst DNO with the lowest ASE-10

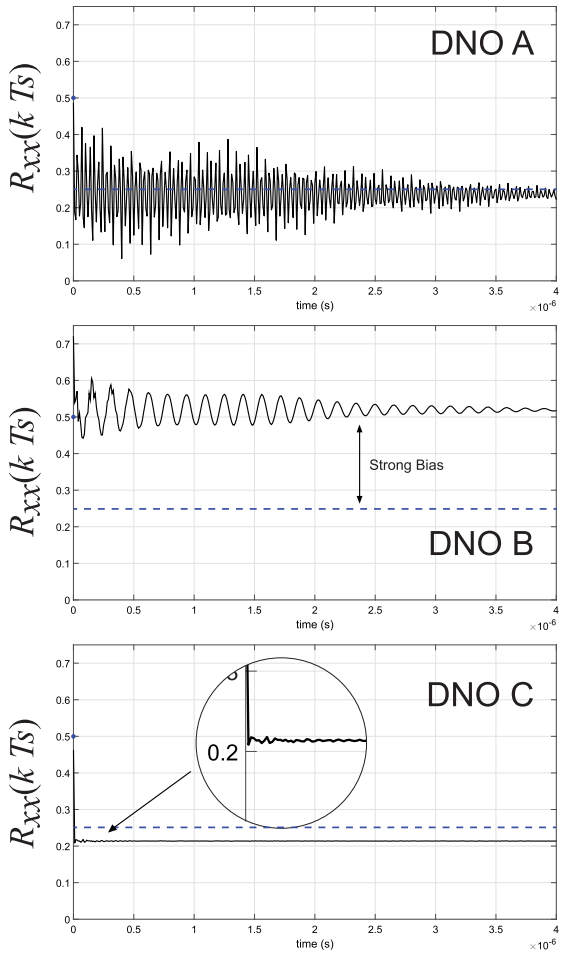

Fig. 18. Autocorrelation functions for the three DNOs (typical results for a sampling frequency of $1/T_s = 100$MHz). For an ideal random binary source the autocorrelation is $R_{xx}(kT_s) = 0.5$ if $k = 0$, 0.25 otherwise (blue/dashed levels) [21].

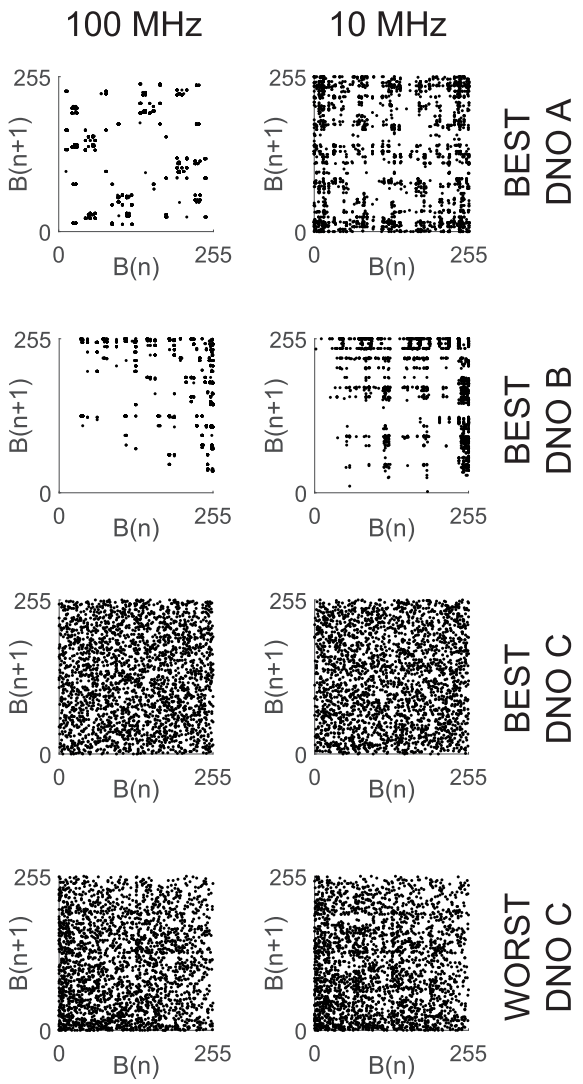

Fig. 19. Comparison between the byte-pattern generations, reporting the result for the DNOs with the highest ASE-10 entropy, including the worst DNO with the lowest ASE-10 entropy for the DNO C type (proposal), for 100MHz and 10MHz sampling rates.

entropy for the DNO-C type (proposal), for 100MHz and 10MHz sampling rates.

C. Experiments: TRNG Statistical Testing

In any cryptographic TRNG the output binary stream results from a digital post-processing of the raw random bits collected from the entropy source. The post-processing can be used both to reduce information redundancy (e.g., by means of information compression) and to mask residual statistical defects (e.g., by means of stream ciphers) [1], [40]. Given any set of randomness tests, the higher is the entropy of the core information source, the minor is the role played by the post-processing to allow the TRNG passing the tests [1], [39].

In this work, we took into account the NIST 800.22 standard tests for cryptographic randomness [1], aiming to design the minimum hardware, based on the DNO in Fig. 14, capable to pass the tests *in any worst case*, considering the variability among the 6 tested FPGA chips and 16 tested locations. The minimum post-processing satisfying the constraint resulted to be a low-complexity stream cipher, performing the bit-by-bit XORing of the collected raw bits with a 8-bit pseudo-random generator (a Fibonacci LFSR based on the primitive polynomial $x^8+x^6+x^5+x^4+1$). In most cases (90% of the tested generators) a 4-bit XOR mixing suffices [37] and in general any more complex (or cryptographically secure)

TABLE II
NIST 800.22 REV.1A STATISTICAL TESTS RESULTS

Test Name	p-Value	Proportion	Result
Frequency	0.474986	1.00	*pass*
BlockFrequency	0.911413	0.97	*pass*
CumulativeSums[a]	0.191687	0.99	*pass*
Runs	0.935716	1.00	*pass*
LongestRun	0.015598	1.00	*pass*
Rank	0.474986	0.99	*pass*
FFT	0.534146	0.98	*pass*
NonOverlappingTemplate[a]	0.955835	0.96	*pass*
OverlappingTemplate	0.350485	0.99	*pass*
Universal	0.699313	0.99	*pass*
ApproximateEntropy	0.798139	0.98	*pass*
RandomExcursions[a]	0.888137	0.96	*pass*
RandomExcursionsVariant[a]	0.324180	0.96	*pass*
Serial[a]	0.145326	0.97	*pass*
LinearComplexity	0.289667	0.99	*pass*

[a] Worst case reported for tests with multiple outcomes.

TABLE III
COMPARISON OF THE PROPOSED SOLUTION WITH SIMILAR RECENTLY PROPOSED TRNGS (NIST-TESTS PASSING)

Reference	Chief Entropy Source	FPGA Device	Hardware Resources[a]	Throughput [Mb/s]	Post-Processing
Ref. [6]	Jitter	Xilinx Spartan-3A	528 LUTs	6	Von Neumann
Ref. [33]	Jitter and Metastability	Xilinx UltraScale	1PLL + 5 primitives + 17 LUTs	100	XOR Compression
Ref. [34]	Jitter	Xilinx Virtex-6	131202 LUTs	167.4	Stream Ciphering
Ref. [35]	Metastability	Altera Cyclone IV	298 LUTs	150	Hashing
Ref. [36]	Metastability	Xilinx Spartan-6	1 Dig. Clock Manager + 36 LUTs	12.6	Custom
Ref. [37]	Timing Skew	Xilinx Virtex-6	224 Slices	50	XOR Mixing
Ref. [16]	DNO (Undetermined Complex Dynamics)	Altera Cyclone IV	≈120 LUTs	200	Stream Ciphering
This Work	**DNO (Chaos Evidence)**	**Xilinx Artix-7**	**15 LUTs**	**100**	**Stream Ciphering**

[a] Overall hardware resources necessary to design the TRNG subsystem, post-processing included.

post-processing proposed in literature can be taken into account, with a further increase of the hardware complexity (as it holds for any TRNG [2]). In Table II typical results for the NIST tests are reported, on the basis of 100 binary sequences of 10^6 bits collected for each run.

For the sake of completeness, we compared the proposed solution with the most relevant and recent works published in literature, as reported in Table III. As it can be appreciated, the proposed solution requires only 15 LUTs, providing an outstanding throughput of 6.66 Mbit/s per LUT. The result is justified by the simplicity of the topology, enhancing the dynamical speed of the resulting nonlinear dynamical system, that the design set to operate in a structurally stable chaotic region in any tested case.

V. CONCLUSION

We have propossed a novel class of Digital Nonlinear Oscillators (DNOs) supporting complex dynamics, including chaos, suitable for the definition of high-performance and low-complexity entropy sources in Programmable Logic Devices (PLDs). We have derived our proposal from the analysis of simplified models, investigated as non-autonomous nonlinear dynamical systems under different excitation conditions. The study lead the authors to the design of a fully digital entropy source consuming only two slices of a Xilinx FPGA, including post-processing, sufficient to define a class of TRNGs capable to pass the NIST standard tests for randomness in any worst case experimentally tested by the authors (6 chips, 96 generators). The solution has been compared with others published in the literature, confirming the validity of the proposal.

REFERENCES

[1] (Apr. 2010). *NIST Special Publication 800-22 Rev.1a: A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-22r1a.pdf

[2] A. J. Acosta, T. Addabbo, and E. Tena-Sánchez, "Embedded electronic circuits for cryptography, hardware security and true random number generation: An overview," *Int. J. Circuit Theory Appl.*, vol. 45, no. 2, pp. 145–169, Dec. 2016.

[3] R. Sivaraman, A. Sridevi, S. Rajagopalan, S. Janakiraman, and A. Rengarajan, "Design and analysis of ring oscillator influenced beat frequency detection for true random number generation on FPGA," in *Proc. Int. Conf. Comput. Commun. Informat. (ICCCI)*, Jan. 2019, pp. 1–6.

[4] H. Hata and S. Ichikawa, "FPGA implementation of metastability-based true random number generator," *IEICE Trans. Inf. Syst.*, vol. E95.D, no. 2, pp. 426–436, 2012.

[5] J.-L. Danger, S. Guilley, and P. Hoogvorst, "High speed true random number generator based on open loop structures in FPGAs," *Microelectron. J.*, vol. 40, no. 11, pp. 1650–1656, Nov. 2009.

[6] N. Nalla Anandakumar, S. K. Sanadhya, and M. S. Hashmi, "FPGA-based true random number generation using programmable delays in oscillator-rings," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 67, no. 3, pp. 570–574, Mar. 2020.

[7] B. Sunar, W. Martin, and D. Stinson, "A provably secure true random number generator with built-in tolerance to active attacks," *IEEE Trans. Comput.*, vol. 56, no. 1, pp. 109–119, Jan. 2007.

[8] M. Raitza, M. Vogt, C. Hochberger, and T. Pionteck, "RAW 2014: Random number generators on FPGAs," *ACM Trans. Reconfigurable Technol. Syst.*, vol. 9, no. 2, pp. 15:1–15:21, Dec. 2015.

[9] Y. Liu, R. C. C. Cheung, and H. Wong, "A bias-bounded digital true random number generator architecture," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 64, no. 1, pp. 133–144, Jan. 2017.

[10] K. H. Tsoi, K. H. Leung, and P. H. W. Leong, "Compact FPGA-based true and pseudo random number generators," in *Proc. 11th Annu. IEEE Symp. Field-Program. Custom Comput. Mach. (FCCM)*, Apr. 2003, pp. 51–61.

[11] K. Wold and C. H. Tan, "Analysis and enhancement of random number generator in FPGA based on oscillator rings," in *Proc. Int. Conf. Reconfigurable Comput. (FPGAs)*, Dec. 2008, pp. 385–390.

[12] U. Guler, S. Ergun, and G. Dundar, "A digital IC random number generator with logic gates only," in *Proc. 17th IEEE Int. Conf. Electron., Circuits Syst.*, Dec. 2010, pp. 239–242.

[13] T. Addabbo, M. Alioto, A. Fort, S. Rocchi, and V. Vignoli, "The digital tent map: Performance analysis and optimized design as a low-complexity source of pseudorandom bits," *IEEE Trans. Instrum. Meas.*, vol. 55, no. 5, pp. 1451–1458, Oct. 2006.

[14] M. Dichtl and J. D. Golić, "High-speed true random number generation with logic gates only," in *Proc. 9th Int. Workshop Cryptograph. Hardw. Embedded Syst. (CHES)*, Berlin, Germany: Springer-Verlag, 2007, pp. 45–62.

[15] H. Martín, T. Korak, E. S. Millán, and M. Hutter, "Fault attacks on STRNGs: Impact of glitches, temperature, and underpowering on randomness," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 2, pp. 266–277, Feb. 2015.

[16] S. Tao, Y. Yu, and E. Dubrova, "FPGA based true random number generators using non-linear feedback ring oscillators," in *Proc. 16th IEEE Int. New Circuits Syst. Conf. (NEWCAS)*, Jun. 2018, pp. 213–216.

[17] K. Demir and S. Ergun, "Random number generators based on irregular sampling and Fibonacci–Galois ring oscillators," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 66, no. 10, pp. 1718–1722, Oct. 2019.

[18] N. Fujieda, M. Takeda, and S. Ichikawa, "An analysis of DCM-based true random number generator," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, to be published.
[19] T. Addabbo, A. Fort, M. Mugnaini, V. Vignoli, and M. Garcia-Bosque, "Digital nonlinear oscillators in PLDs: Pitfalls and open perspectives for a novel class of true random number generators," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, May 2018, pp. 1–5.
[20] 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.
[21] T. Addabbo, A. Fort, R. Moretti, M. Mugnaini, V. Vignoli, and M. Garcia Bosque, "Lightweight true random bit generators in PLDs: Figures of merit and performance comparison," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, May 2019, pp. 1–5.
[22] T. Addabbo, A. Fort, R. Moretti, M. Mugnaini, and V. Vignoli, "Analysis of a circuit primitive for the reliable design of digital nonlinear oscillators," in *Proc. 15th Conf. Ph.D Res. Microelectron. Electron. (PRIME)*, Jul. 2019, pp. 189–192.
[23] N. Shawagfeh and D. Kaya, "Comparing numerical methods for the solutions of systems of ordinary differential equations," *Appl. Math. Lett.*, vol. 17, no. 3, pp. 323–328, Mar. 2004.
[24] T. Addabbo, A. Fort, M. Di Marco, L. Pancioni, and V. Vignoli, "Physically unclonable functions derived from cellular neural networks," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 60, no. 12, pp. 3205–3214, Dec. 2013.
[25] S. Lee, M.-K. Oh, Y. Kang, and D. Choi, "Implementing a phase detection ring oscillator PUF on FPGA," in *Proc. Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, Oct. 2018, pp. 845–847.
[26] C. Q. Liu, Y. Cao, and C. H. Chang, "ACRO-PUF: A low-power, reliable and aging-resilient current starved inverter-based ring oscillator physical unclonable function," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 64, no. 12, pp. 3138–3149, Dec. 2017.
[27] L. Cveticanin, "Forced pure nonlinear symmetrical oscillators," *Math. Comput. Model.*, vol. 55, nos. 3–4, pp. 1580–1593, Feb. 2012.
[28] C. H. Miwadinou, A. V. Monwanou, J. Yovogan, L. A. Hinvi, P. R. N. Tuwa, and J. B. Chabi Orou, "Modeling nonlinear dissipative chemical dynamics by a forced modified van der Pol-Duffing oscillator with asymmetric potential: Chaotic behaviors predictions," *Chin. J. Phys.*, vol. 56, no. 3, pp. 1089–1104, Jun. 2018.
[29] C. Ainamon, C. H. Miwadinou, A. V. Monwanou, and J. B. C. Orou, "Analysis of multiresonance and chaotic behavior of the polarization in materials modeled by a duffing equation with multifrequency excitations," *Appl. Phys. Res.*, vol. 6, no. 6, pp. 74–86, Nov. 2014.
[30] I. Bashkirtseva and L. Ryashko, "Sensitivity and chaos control for the forced nonlinear oscillations," *Chaos, Solitons Fractals*, vol. 26, no. 5, pp. 1437–1451, Dec. 2005.
[31] E. Ott, *Chaos in Dynamical Systems*. Cambridge, U.K.: Cambridge Univ. Press, 1993.
[32] J. H. Hale and H. Koçak, *Dynamics and Bifurcations*. New York, NY, USA: Springer-Verlag, 1996.
[33] G. Di P. Stanchieri, A. De Marcellis, E. Palange, and M. Faccio, "A true random number generator architecture based on a reduced number of FPGA primitives," *AEU-Int. J. Electron. Commun.*, vol. 105, pp. 15–23, Jun. 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1434841118327080
[34] M. Tuna, A. Karthikeyan, K. Rajagopal, M. Alcin, and İ. Koyuncu, "Hyperjerk multiscroll oscillators with megastability: Analysis, FPGA implementation and a novel ANN-ring-based true random number generator," *AEU-Int. J. Electron. Commun.*, vol. 112, Dec. 2019, Art. no. 152941.
[35] X. Wu and S. Li, "A new digital true random number generator based on delay chain feedback loop," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, May 2017, pp. 1–4.
[36] P. Z. Wieczorek, "An FPGA implementation of the resolve time-based true random number generator with quality control," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 61, no. 12, pp. 3450–3459, Dec. 2014.
[37] X. Yang and R. C. C. Cheung, "A complementary architecture for high-speed true random number generator," in *Proc. Int. Conf. Field-Program. Technol. (FPT)*, Dec. 2014, pp. 248–251.
[38] J. M. Rabaey, A. Chandrakasan, and B. Nikolic, *Digital Integrated Circuits*, 3rd ed. Upper Saddle River, NJ, USA: Prentice-Hall, 2008.
[39] *Recommendation for the Entropy Sources Used for Random Bit Generation*, NIST Special Publication 800-90b, Apr. 2018, doi: 10.6028/NIST.SP.800-90B.
[40] T. Addabbo, M. Alioto, A. Fort, S. Rocchi, and V. Vignoli, "A variability-tolerant feedback technique for throughput maximization of TRBGs with predefined entropy," *J. Circuits, Syst. Comput.*, vol. 19, no. 4, pp. 879–895, Nov. 2011.

Tommaso Addabbo (Member, IEEE) received the Ph.D. degree in information engineering from the University of Siena, Italy. He is currently an Associate Professor of electronics with the University of Siena. He has been a Visiting Scholar with the Institute of Nonlinear Science, University of California at San Diego and the Macedonian Academy of Sciences and Arts, Skopje. His main research interests include analysis of nonlinear circuits and systems, stochastic aspects of chaotic dynamics and analog circuits design, and design of electronic embedded systems.

Ada Fort (Member, IEEE) received the Ph.D. degree in nondestructive testing from the University of Florence, Italy, in 1992. She is currently an Associate Professor with the Department of Information Engineering and Mathematics, University of Siena, Italy. Her research interests concern the development of measurement systems based on chemical and ultrasonic sensors and the development of automatic fault diagnosis systems. Recently, she has been involved in the study of random number generators based on chaotic maps.

Riccardo Moretti (Student Member, IEEE) received the M.Sc. degree in electronics and communications engineering from the University of Siena, Siena, Italy, in 2017, where he is currently pursuing the Ph.D. degree with the Department of Information Engineering and Mathematics. His main research interests include nonlinear circuits and systems, digital embedded systems, measurement front-end electronics, and electronic applications for industry.

Marco Mugnaini (Senior Member, IEEE) received the Ph.D. degree in reliability, availability, and logistics from the University of Florence, Italy, in 2003. Since 2003, he has been a Product Safety Engineer with General Electric Oil and Gas Business, Florence. He is currently an Associate Professor with the Department of Information Engineering, University of Siena, Siena, Italy. His current research interest includes the development of measurement systems. He received his green belt certificate from General Electric Oil and Gas Business.

Hadis Takaloo (Student Member, IEEE) received the M.Sc. degree in electrical and electronics engineering from Razi University, Kermanshah, Iran, in 2015. She is currently pursuing the Ph.D. degree with the Department of Information Engineering and Mathematics, University of Siena, Italy. In 2019, she has been a Visiting Scholar with the Instituto de Microelectrónica de Sevilla (IMSE-CNM), Spain. Her main research interests include analog and mixed-signal integrated circuit design, hardware implementation of complex dynamical systems, and hardware security and analysis of nonlinear circuits and systems.

Valerio Vignoli (Member, IEEE) received the Ph.D. degree in nondestructive testing from the University of Florence, Italy, in 1994. He is currently an Associate Professor of electronics with the Department of Information Engineering and Mathematics, University of Siena, Italy. His main research interests include analog and digital electronic design, design, characterization, and modeling of advanced sensors for monitoring physical quantities, and development of data acquisition and processing systems.