Nonlinear Dyn (2020) 102:2887–2904
https://doi.org/10.1007/s11071-020-06017-3

ORIGINAL PAPER

A fully CMOS true random number generator based on hidden attractor hyperchaotic system

Ngoc Nguyen · Georges Kaddoum · Fabio Pareschi · Riccardo Rovatti · Gianluca Setti

Received: 23 July 2020 / Accepted: 12 October 2020 / Published online: 31 October 2020

Abstract Low-power devices used in Internet-of-things networks have been short of security due to the high power consumption of random number generators. This paper presents a low-power hyperchaos-based true random number generator, which is highly recommended for secure communications. The proposed system, which is based on a four-dimensional chaotic system with hidden attractors and oscillators, exhibits rich dynamics. Numerical analysis is provided to verify the dynamic characteristics of the proposed system. A fully customized circuit is deployed using 130 nm CMOS technology to enable integration into low-power devices. Four output signals are used to seed a SHIFT-XOR-based chaotic data post-processing to generate random bit output. The chip prototype was simulated and tested at 100 MHz sampling frequency. The hyperchaotic circuit consumes a maximum of 980 μW in generating chaotic signals while dissipates a static current of 623 μA. Moreover, the proposed system provides ready-to-use binary random bit sequences which have passed the well-known statistical randomness test suite NIST SP800-22. The proposed novel system design and its circuit implementation provide a best energy efficiency of 4.37 pJ/b at a maximum sampling frequency of 100 MHz.

Keywords True random number generator · Chaos · Hyper-chaos · CMOS · Security

N. Nguyen · G. Kaddoum
Department of Electrical Engineering, École de Technologie Supérieure (ÉTS), University of Québec, Montreal QC, Canada
e-mail: ngoc.nguyen-thi-thu@lacime.etsmtl.ca

G. Kaddoum
e-mail: georges.kaddoum@etsmtl.ca

F. Pareschi (✉) · G. Setti
Department of Electronics and Telecommunications, Politecnico di Torino, 10129 Turin, Italy
e-mail: fabio.pareschi@polito.it

G. Setti
e-mail: gianluca.setti@polito.it

F. Pareschi · G. Setti · R. Rovatti
Advanced Research Center on Electronic Systems (ARCES), University of Bologna, 40125 Bologna, Italy

R. Rovatti
Department of Electrical, Electronic, and Information Engineering, University of Bologna, 40136 Bologna, Italy
e-mail: riccardo.rovatti@unibo.it

1 Introduction

The security of cryptography algorithms highly depends on the randomness of the keys generated from random number generators (RNGs). Most random number generators available today are software-based, which are commonly referred to as pseudo-random number generators (PRNGs). The term "pseudo-random" refers to the random bits generated from a deterministic algorithm in digital computing software. In this context, the generator knows exactly the next state/the next number, while these numbers appear random to the other side. In a true random number generator (TRNG), conversely,

the computation of the next state/the next number relies typically on a physical process (entropy source) and is unknown until it is revealed. Therefore, these numbers are "random" for both generator and observer. Some TRNG commercial chips have been utilized in high-performance microprocessors [42] where an unpredictable entropy source generates a random seed to a pseudo-random generator. Examples of entropy sources used in these architecture include thermal noise, jitter noise, and metastability. However, all these methods have a critical drawback, as they are inherited from entropy sources whose statistics are known only with a very limited precision. Furthermore, the limited dynamic range of the entropy sources (as in the case, for example, of the thermal noise) makes the entire system extremely sensitive to deterministic system noise sources, such as power variations, bias voltage variations, and device mismatches [1,6,7,16,25,44,45].

In this paper, we deal with chaos as an entropy source. A nonlinear system exhibits chaotic behavior if it features inherent characteristics including (i) high sensitivity to initial conditions—a slight change in initial conditions yields significantly different future trajectories, and (ii) irregular motion in the phase space—phase space trajectories do not converge to a point or a periodic orbit [32]. Thanks to these properties, and despite the deterministic evolution, even a small unavoidable uncertainty on the system's initial condition will make a chaotic system, at a certain point of observation, an actual unpredictable random-like process. The advantage with respect to the previously considered architectures is that, by using chaos as entropy source, it is possible to have a precise knowledge of the process statistics, that are set by the chaotic circuit.

Chaotic systems can be classified into discrete-time and continuous-time where both approaches can be effectively used to produce random numbers. In discrete chaotic systems, the iterated functions are used in the form of $x_{k+1} = F(x_k)$. Examples of such systems include the logistic map, the Renyi map, and piecewise affine Markov maps [17,19,21,22,39,41]. As demonstrated in [12], many researchers have been improving the complexity of chaotic maps, where higher dimensional chaotic maps, such as Logistic 2D map, Chen hyperchaotic map, and Rossler hyperchaotic map, have been used. Conversely, continuous chaotic systems are presented by differential equations $X' = F(X)$ [20]. Nowadays, continuous chaotic systems achieve higher complexity by conveying integer-order systems into the fractional-order domain [34]. However, fractional-order systems are complicated to implement in hardware design due to their memory dependency. The hardware implementation of fractional-order differentiators and integrators requires careful considerations [35]. Here, we focus on high-order continuous chaotic systems—chaotic systems with at least four dimensions and two positive Lyapunov exponents (LE) which are implemented in analog integrated circuit design. In a chaotic system, Lyapunov exponents are important criteria to evaluate the system's dynamics. Sensitivity to initial conditions of a dynamic system is represented by a positive LE. An n-dimensional dynamical system has a spectrum of n-Lyapunov exponents. In order to exhibit chaos, a system requires to be at least three dimensional (3D) with a positive LE. A hyperchaotic system exhibits rich dynamics since system states are expanded exponentially in several directions simultaneously. Due to this property, the hyperchaotic system is an interesting candidate for the generation of random keys used in miscellaneous applications in engineering such as secure communications, cryptosystems, and encryptions [33]. Moreover, continuous chaotic systems are further classified into two sub-categories according to their dynamic characteristics: self-excited and hidden attractors [34]. A nonlinear chaotic system is considered as self-excited if it has a basin of an attractor from an unstable equilibrium point. Lorenz, Rössler, Chen, Lü, or Sprott systems are well-known self-excited systems. Recently, the second group of hidden attractors, which has been developed theoretically and practically, is attracting great attention. The aim of this paper is to introduce a novel hyperchaotic system with hidden attractors suitable for the generation of high-quality random numbers.

1.1 Motivations and contributions

As far as continuous chaotic circuits implementation is concerned, numerous contributions have been reported in the literature, all unfortunately presenting drawbacks and limitation, such as high power consumption, low operation frequency, and inability to operate at low voltage levels, which hinders their capabilities to be adopted in practical engineering applications. As an example, Chua's circuit, the first continuous chaotic system implemented in integrated form, requires the use of complicated nonlinear functions [10,43]. Limit-

ing ourselves to more recent works, in [37] the authors introduced the first integrated versions of a multi-scroll continuous chaotic oscillator showing 3- and 5-scroll attractors in a 0.5 μm CMOS technology. They include a very interesting process, voltage, and temperature (PVT) analysis, showing that the desired chaotic behavior is maintained even in the presence of consistent parameters variation; unfortunately, the circuit topology is still rather complex and the overall circuit is not low-power. In [36], authors compare various integrated circuit design techniques for chaotic oscillators based on with various nonlinear functions (i.e., piecewise linear (PWL), sinusoidal, sawtooth, hysteresis, complex, and tanh(·) functions). In all these implementations, complexity of the circuit implementing the nonlinearity in a issue, as it is the overall characteristic operating frequency of the 5 chaotic oscillators, which is quite low, since one of them works at a 7 MHz frequency using switching currents floating-gate FGMOS transistors, while the others operate between 118 KHZ and 3.5 MHz. The contribution in [5] is interesting since presents guidelines for the CMOS circuit design of basic building blocks (such as current follower, current mirror, and voltage follower) which are used for obtaining particularly simple saturated nonlinear functions (SNLFs). Finally, in [20], some of the authors of this manuscript presented the design of a 3D continuous chaotic system in CMOS technology, and its engineering application in image encryption. The main point in common between the design in [20] and the chaotic system implementation presented in this manuscript is that they both rely on the analog realization of a tanh(·) nonlinear function. Yet, the work presented here offers several improvements. First, the chaotic circuit is now four-dimensional, which is a fundamental fact for implementing a TRNG: in fact, a 3D autonomous chaotic system only possess a self-excited attractor whose basin can be revealed by a computational tool [15], and this may spoil its capability to work effectively as an entropy source. Furthermore, with respect to [20], we provide a thorough characterization in terms of robustness with respect to PVT variations, and of the performances of the system as TRNG by including tests on the entropy of raw (i.e., unaltered by the prost-processing stage) generated data.

Although chaotic systems are unpredictable and have random-like state trajectories, they can be studied and recovered by using computational tools. However, this approach showed very limited success with regards to hidden attractor chaotic systems [15]. The hyperchaotic systems with hidden attractors in [2,26,27] were proposed to overcome these attacks. However, they are deployed using off-the-shelf analog electronic devices that consume high power and require high voltage operation. Therefore, their implementation is inappropriate in highly integrated circuit designs. In conclusion, based on our investigation, hyperchaotic systems with hidden attractors have many advantages when used in generating random bits for highly secure applications. However, the hardware implementation of these systems still has many limitations that need to be addressed. Therefore, our research targets the shortcomings of practical circuit realizations of hyperchaotic systems. We propose a novel hyperchaotic system with four dimensions and hidden attractors which provides high dynamic characteristics. The proposed hyperchaotic system is presented and analyzed in terms of Lyapunov exponents and stability analysis. Comparison against the state-of-the-arts establishes the advantages of the proposed system. Moreover, the proposed system is implemented in a low-power integrated circuit using 130 nm CMOS technology. To generate the ready-to-use binary bitstreams, the proposed chaotic signals are utilized to feed a SHIFT-XOR-based post-processing circuit. Multiple configurations are evaluated to find the best frequency operation, while the randomness is guaranteed. Statistical tests prove the reliability of using the proposed random number generator in information security. The paper contribution can be summarized as follow: (i) design of a novel hyperchaotic system with hidden attractors, which is highly recommended in security and (ii) circuit implementation of the proposed system using 130 nm CMOS technology.

The rest of this paper is organized as follows. Section 2 presents the mathematical model of the proposed hyperchaotic system with numerical analysis to verify the robustness of the system. The circuit implementation using 130 nm CMOS technology is elaborated in Sect. 3. The system performances such as randomness measurement, signal entropy and correlations, power consumption, and throughput are evaluated in Sect. 4. Finally, Sect. 5 concludes this paper.

2 System design and mathematical analysis

This section presents the proposed hidden attractor hyperchaotic system, which is expressed by four differ-

ential equations, depicted in (1). The theoretical analysis is divided into two parts. The first part presents the proposed chaotic system and the theoretical study of its chaotic characteristics, while the second part addresses the stability of its equilibrium points.

2.1 The proposed hyper-chaotic system

The hyperchaotic system is presented in the canonical form $X' = F(X)$, in which the vector $X = [x_1, x_2, x_3, x_4] \in \mathbb{R}^4$, with

$$\begin{cases} x_1' = x_2, \\ x_2' = x_3, \\ x_3' = x_4, \\ x_4' = -a_1 x_3 - a_2 x_4 + b_1 \tanh(b_2 x_1 - b_3) x_2, \end{cases} \tag{1}$$

where $\tanh(\cdot)$ is the standard hyperbolic tangent function. The above system can be described as a hyperjerk system which sastifies

$$x'''' = -a_1 x'' - a_2 x''' + b_1 \tanh(b_2 x - b_3) x'. \tag{2}$$

The proposed 4D chaotic system is inspired by a Jerk 3D chaotic system, which is extended to be four-dimensional. By simulating and observing output signals, the system's parameters are tuned precisely in the range in which the divergent conditions are met. In Sect. 3, we discuss the analog implementation of this system. Here, we propose its analysis by means of MATLAB numerical integration with the aim of highlighting many properties. As summarized in [34], there are many numerical methods that have been applied to solve differential equations such as Forward-Euler, fourth-order Runge–Kutta algorithm, Adams–Bashfort2, and Adams–Bashfort3. As indicated in [34], the fourth-order Runge–Kutta algorithm provides the lowest error. Therefore, the fourth-order Runge–Kutta algorithm is utilized to simulate the proposed design in MATLAB with a step size of 10^{-4}. The proposed system has equilibrium points only located on the line $E = [x_1, 0, 0, 0]$. Therefore, the proposed system is a dynamical system with hidden attractors. According to [3,26], it is impossible to locate the chaotic attractor by choosing an arbitrary initial condition. In other words, from a computational point of view, these attractors are hidden and knowledge about equilibria does not help in their localization. To study the dynamical behavior of the proposed system, we resort to numerical mathematics such as the Lyapunov exponents and bifurcation diagram. The Lyapunov exponents of the system are defined as

$$L_i = \lim_{t \to \infty} \frac{1}{t} \log \frac{\|\partial x_i(t)\|}{\|\partial x_i(0)\|}. \tag{3}$$

For $a_1 = 1, a_2 = 0.5, b_1 = 2, b_2 = 2.5$, and $b_3 = 0.62$, the Lyapunov exponents of the novel 4D chaotic system are: $L_1 = 0.088, L_2 = 0.01, L_3 = 0$, and $L_4 = -0.598$, respectively. The initial conditions of the proposed chaotic system are chosen as $x_1(0) = 0.02, x_2(0) = 0.005, x_3(0) = 0$, and $x_4(0) = 0$. There are two criteria to evaluate the divergence of the dynamic system presented in (1) as follow:

$$\begin{aligned} \sum_{i=1}^{4} \frac{\partial x_i'}{\partial x_i} &= -a_2 < 0, \\ L &= L_1 + L_2 + L_3 + L_4 < 0. \end{aligned} \tag{4}$$

where the first equality holds since, according to (1), $\partial x_1'/\partial x_1 = \partial x_2'/\partial x_2 = \partial x_3'/\partial x_3 = 0$, and $\partial x_4'/\partial x_4 = -a_2$. Moreover, the Kaplan–York dimension, an effective metric to evaluate the complexity of a chaotic oscillator, is calculated as:

$$D_{\mathrm{KY}} = j + \frac{1}{|L_{j+1}|} \sum_{i=1}^{j} L_i, \tag{5}$$

where j is the largest index of the positive Lyapunov exponent. In the proposed system, $j = 3$, and the Kaplan–York dimension is therefore:

$$D_{\mathrm{KY}} = 3 + \frac{L_1 + L_2 + L_3}{|L_4|} = 3.164. \tag{6}$$

Table 1 compares the Lyapunov exponents of the proposed 4D hyperchaotic system with hidden attractors to previous studies. Moreover, the proposed hyperchaotic system obtains a higher Kaplan–York dimension than previous systems. The dynamic characteristics of a chaotic system highly depend on the complexity of the nonlinear function. The nonlinear functions in current state-of-the-art chaotic systems based on a single

Table 1 Lyapunov exponents comparison

Chaos	L_1	L_2	L_3	L_4	D_{KY}
[18]	2.1990	0.071	0	−14.362	3.160
[26]	0.0730	0.0018	0	−0.5755	3.130
[27]	0.0895	0	0	−0.8997	3.099
[46]	1.416	0.5318	0	−39.101	3.0498
[2]	0.0397	0.0001	0	−0.6395	3.0622
This work	0.1528	0.0661	−0.1723	−0.5465	3.164

Table 2 Stability of equilibria with different initial conditions

c	λ_1	$\lambda_{2,3}$	Description
−0.1	− 1.3546	$0.1773 \pm 0.9741i$	Unstable state
0	− 1.2455	$0.1223 \pm 0.8884i$	Unstable state
0.05	− 1.1631	$0.0815 \pm 0.8265i$	Unstable state
0.1	− 1.0514	$0.0257 \pm 0.7439i$	Unstable state
0.2	− 0.3768	$-0.3116 \pm 0.4099i$	Stable state
0.24	0.1489	$-0.5744 \pm 0.5840i$	Unstable state

common function such as multiplication, sign, piecewise linear function, and tanh function. However, in our proposed hyperchaotic system, the nonlinear function includes both multiplication and tanh functions.

2.2 Stability analysis of line equilibria

Stability analysis of the equilibrium points helps evaluate the practical design of the system such as the circuit stability and linearity. To evaluate the stability of equilibria, the Jacobian matrix of the proposed hyperchaotic system is calculated as

$$J = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ A & B & -a_1 & -a_2 \end{bmatrix}, \tag{7}$$

where $A = b_1 b_2 x_2 (1 - \tanh^2(b_2 x_1 - b_3))$, and $B = b_1 \tanh(b_2 x_1 - b_3)$. The eigenvalues of the Jacobian matrix satisfy the condition

$$J - \lambda I = 0 \leftrightarrow \lambda^4 + a_2\lambda^3 + a_1\lambda^2 - B\lambda + A = 0. \tag{8}$$

The proposed system has equilibrium points only located on the line $E = [x_1, 0, 0, 0]$ where the Jacobian matrix at these equilibria is obtained as

$$J = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & b_1 \tanh(b_2 x_1 - b_3) & -a_1 & -a_2 \end{bmatrix}. \tag{9}$$

Let $X_0 = [x_1(0), 0, 0, 0]$ be a fixed point, and ΔX be a small perturbation such that $X = X_0 + \Delta X$. If $\Delta x \approx e^{\lambda} t$, the characteristic polynomial equation is derived as

$$\lambda(\lambda^3 + a_2\lambda^2 + a_1\lambda - B) = 0. \tag{10}$$

Thus, the Jacobian matrix has four eigenvalues where one of them is zero. Let $g(\lambda) = \lambda^3 + a_2\lambda^2 + a_1\lambda - B$ be a polynomial function of three nonzero eigenvalues, the real parts of the roots of $g(\lambda) = 0$ are negative if and only if $a_2 > 0$, $B < 0$, $a_1 a_2 + B > 0$. For the typical parameter set ($a_1 = 1, a_2 = 0.52, b_1 = 2, b_2 = 2.5$, and $b_3 = 0.55$), to make the equilibrium set E unstable, thereby enabling the possibility of chaos occurrence, the initial condition $x_1(0) = c$ must satisfy $c < 0.117834$ or $c > 0.22$. The three nonzero eigenvalues $\lambda_i (i = 1, 2, 3)$ of the equilibrium set E for several typical values of c are listed in Table 2. Depending on the initial value, the proposed system has stable or unstable saddle-focus points. Thus, the dynamical behavior of the equilibrium line chaotic system

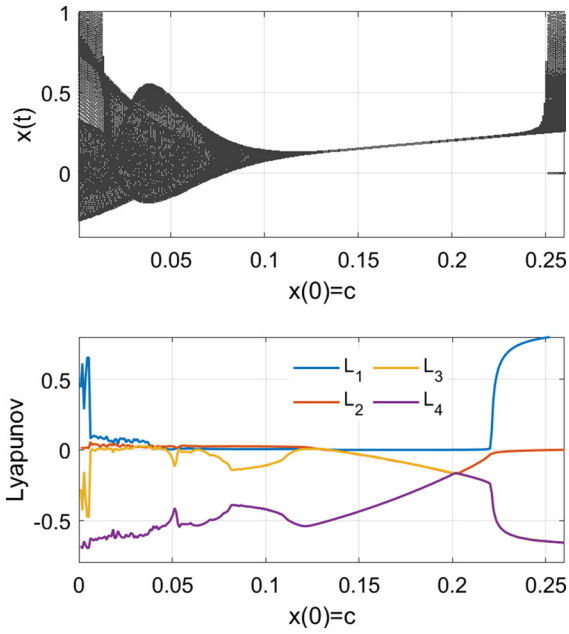

Fig. 1 Bifurcation diagram and Lyapunov spectrum of system state with initial condition $x(0) = c$

is heavily dependent on the initial state of the variable x_1, in addition to the system parameters. When $a_1 = 1, a_2 = 0.52, b_1 = 2, b_2 = 2.5, b_3 = 0.6$ are kept constant, the parameter c in the initial conditions $[x_1(0) = c, x_2(0), x_3(0), x_4(0)]$ varies in the range $[0, 0.26]$. The bifurcation diagram of the state variable $x_1(t)$ of the proposed system is shown in Fig. 1, where it is indicated that the characteristics of the system vary with c. Moreover, the stable region is clearly observed for $0.1178 < c < 0.22$; while for $c > 0.22$, the system is unstable, diverged, and unfolded; therefore, these regions are not interesting. Meanwhile, $0.05 < c < 0.1178$ is a chaotic region with a limited number of periods, and the data space in this region is small. Finally, in the range $0.01 < c < 0.05$, the system exhibits rich dynamic characteristics.

The robustness of the system is illustrated by the choice of system parameters. By evaluating the parameter bifurcations and the corresponding Lyapunov spectrum, we choose the parameter ranges in which the characteristics of the proposed system are preserved. Fig. 2 shows the bifurcation diagrams of state variable x_1 according to the system parameters a_1, and a_2. The variations of b_1, b_2, and b_3 affect the chaotic characteristics of the proposed system as depicted in Fig. 3. Therefore, we select the parameter set as $a_1 = 1, a_2 =$

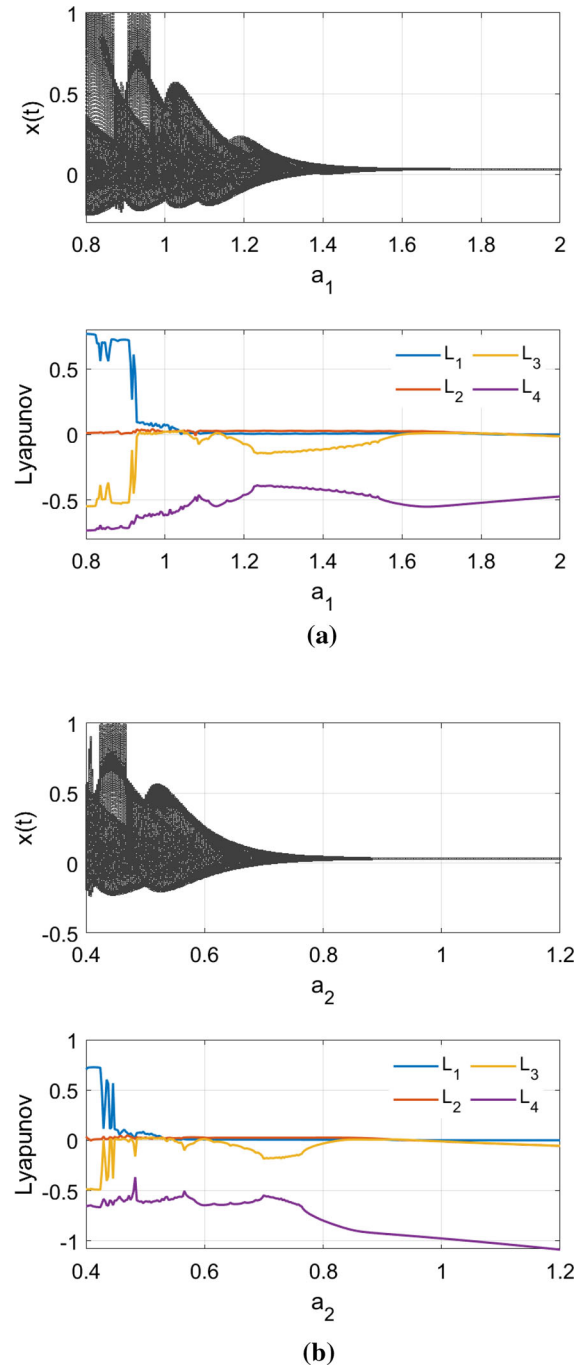

Fig. 2 Bifurcation diagram and Lyapunov spectrum of signal x_1 according to parameters **a** a_1 and **b** a_2

$0.52, b_1 = 2, b_2 = 2.5$, and $b_3 = 0.6$ to determine the chaotic characteristics of the proposed system. The circuit design imperfection and device mismatches con-

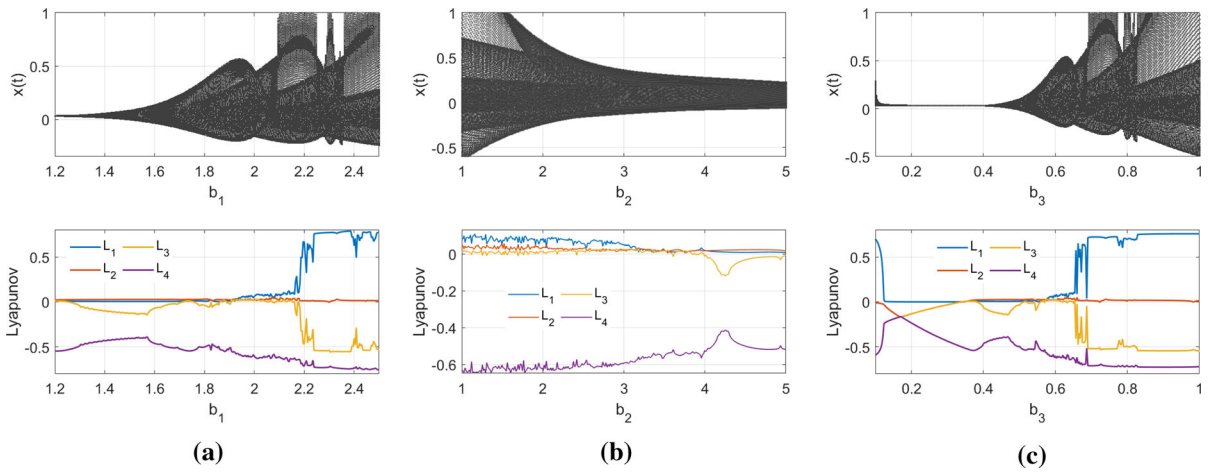

Fig. 3 Bifurcation diagram and Lyapunov spectrum of the signal x_1 according to parameters **a** b_1, **b** b_2, and **c** b_3

tributing to the parameter variations will be evaluated in the next section.

2.3 Periodicity analysis

Wavelet is an effective method for analyzing the periodicity of a dynamic system. Therefore, the scale index i_{scale} is calculated based on the inner scalogram of the continuous chaotic signals [4]. The scale index, which is in the range [0, 1], is used to measure the degree of non-periodicity of the chaotic signal. The value of the scale index is close to zero when the chaotic signal is periodic, and close to one if the observed signal is highly non-periodic. The scale index of the proposed chaotic system with parameters $a_1 = 1, a_2 = 0.52, b_1 = 2, b_2 = 2.5$, and $b_3 = 0.6$ is 0.8289, which indicates the highly non-periodic characteristic of the chaotic system. The spectrum of the scale index in Fig. 4 and the bifurcation diagram in Fig. 3c according to the parameter b_3 determine the non-periodicity of the chaotic system at chosen parameters.

3 Circuit implementation

3.1 Hyperchaotic circuit design

In circuit realization, the proposed system is formulated using Kirchhoff's law, and the results reveal the following system of ordinary differential equations (ODEs):

$$\begin{cases} v_1' = \dfrac{g_{m1}}{C_1} v_2 \\ v_2' = \dfrac{g_{m2}}{C_2} v_3 \\ v_3' = \dfrac{g_{m3}}{C_3} v_4 \\ v_4' = -\dfrac{g_{m4}}{C_4} v_3 - \dfrac{g_{m5}}{C_4} v_4 + \dfrac{i_{out}}{C_4} \end{cases}, \tag{11}$$

in which, $g_m = g_{m1} = g_{m2} = g_{m3} = -g_{m4} = 110\,\mu\text{S}$ and $C = C_1 = C_2 = C_3 = C_4$ for circuit simplicity.

3.1.1 Gm-C integrator

Inverted-based Gm-C configuration is chosen to design the integrator in this circuit due to its low power consumption, high linearity, and high input dynamic as depicted in Fig. 5. In this figure, the current output i_o is the inverse of the current i_1, where

$$i_1 = -g_m v_i. \tag{12}$$

A pair of NMOS and PMOS devices are utilized to provide the total transconductance gain

$$\begin{aligned} g_m &= \mu_n C_{ox} \frac{W_n}{L_n} (V_{\text{GS}n} - V_{\text{TH}n}) \\ &\quad + \mu_p C_{ox} \frac{W_p}{L_p} (V_{\text{GS}p} - V_{\text{TH}p}). \end{aligned} \tag{13}$$

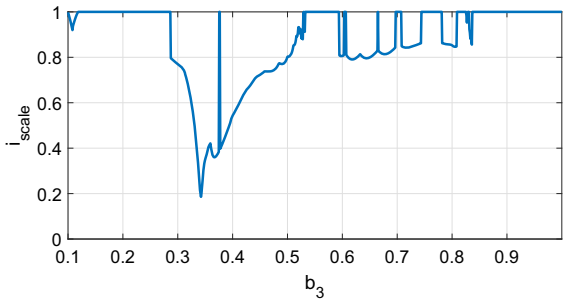

Fig. 4 Scale index spectrum according to the parameter b_3

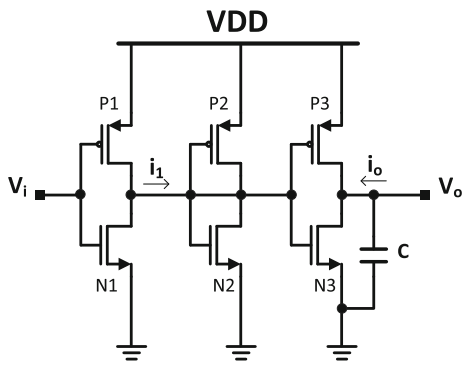

Fig. 5 Integrator circuit design

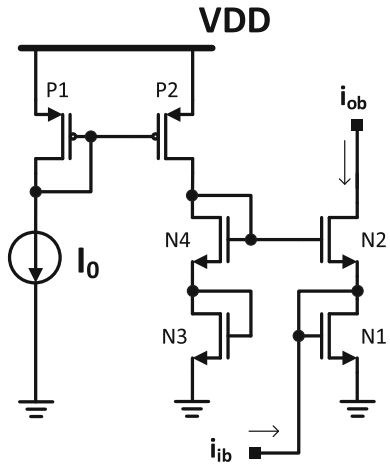

Fig. 6 Circuit design of current square

Two couples of devices ($N2$, $N3$) and ($P2$, $P3$) are used to form bi-directional current mirrors,

$$\begin{aligned} i_o &= -i_1 = g_m v_i, \\ i_o &= \frac{1}{C}\frac{\partial v_o}{\partial t} = g_m v_i \\ \rightarrow \frac{\partial v_o}{\partial t} &= \frac{g_m}{C} v_i. \end{aligned} \tag{14}$$

The transistor size of P_1 and N_1 is chosen to satisfy $K = \mu_p C_{ox}\frac{W_p}{L_p} = \mu_n C_{ox}\frac{W_n}{L_n}$. Then, the transconductance g_m is approximated as $g_m = K(V_{\mathrm{DD}} - V_{\mathrm{TH}n} - V_{\mathrm{TH}p})$. The simple circuit of an inverted-based transconductance integrator has a limited dynamic range of input voltage. To drive all the transistors to the saturation region, the voltage headroom is $[V_{\mathrm{TH}n} \rightarrow V_{\mathrm{DD}} - V_{\mathrm{TH}p}]$. Therefore, low voltage threshold devices are used in the circuit design to increase voltage headroom. The output swing is limited by the overdrive voltages of NMOS and PMOS devices from V_{OD}(NMOS) to ($V_{\mathrm{DD}} - V_{\mathrm{OD}}$(PMOS)). The nonlinearity and variability in the transconductance and the intrinsic capacitor contribute to variations in the DC-transfer function. The transconductance in (14) is assumed to be independent of the gate voltages when the transistors are in the saturation region. However, the drain-to-source voltages of the MOSFETs V_{DS} or the output voltage may drive the devices to linear regions when $V_{DS} \leq (V_{\mathrm{GS}} - V_{\mathrm{TH}})$. Moreover, transistor mismatches in threshold voltages and the transistor parameter K affect the variability of transconductance. A typical mismatch between two physically adjacent transistors is 20%, corresponding to a difference in gate voltage of 10 mV which should be taken into account. A circuit of constant Gm can help increase the linearity of an integrator.

3.1.2 Current square circuit

The nonlinear function $i_{out} = f(v_1, v_2) = i_1 \times i_2$ in (11) was implemented using a low-power multiplier [13,30]. The current multiplier was implemented based on current square cells as shown in Fig. 6. Assuming all transistors are working in the saturation region, the relation between the drain to source current of a transistor (I_D) and the gate-to-source voltage (V_{GS}) is expressed as

$$I_D = K(V_{\mathrm{GS}} - V_{\mathrm{TH}})^2 \tag{15}$$

In Fig. 6, $N3$ and $N4$ are identical diode-connected NMOS devices; therefore, the voltage V_B is calculated as

$$V_B = 2V_{\mathrm{GS3}} = 2\left(\sqrt{\frac{I_0}{K}} + V_{\mathrm{TH}}\right). \tag{16}$$

The drain current of $N1$ is $(i_{ib}+i_{ob})$; therefore, the gate voltage of $N1$ is calculated as

$$V_{\mathrm{GS1}} = \sqrt{\frac{i_{ib}+i_{ob}}{K}} + V_{\mathrm{TH}}, \tag{17}$$

and the gate-to-source voltage of $N2$ is obtained as

$$V_{\mathrm{GS2}} = \sqrt{\frac{i_{ob}}{K}} + V_{\mathrm{TH}}, \tag{18}$$

Calculating the voltage V_B based on the gate-to-source voltages of $N1$ and $N2$, we get

$$\begin{aligned} & V_B = V_{\mathrm{GS1}} + V_{\mathrm{GS2}} \\ & \leftrightarrow \sqrt{i_{ob}} + \sqrt{i_{ib}+i_{ob}} = 2\sqrt{I_0} \\ & \leftrightarrow \sqrt{i_{ob}+i_{ib}} = 2\sqrt{I_0} - \sqrt{i_{ob}} \\ & \leftrightarrow i_{ob}+i_{ib} = 4I_0 + i_{ob} - 4\sqrt{I_0 \times i_{ob}} \\ & \leftrightarrow 16I_0 \times i_{ob} = (4I_0 - i_{ib})^2 \\ & \leftrightarrow i_{ob} = \frac{(4I_0 - i_{ib})^2}{16I_0}. \end{aligned} \tag{19}$$

In the current square circuit, various mismatches including channel length modulation, input current mismatch caused by devices mismatch in current mirrors, and transistor mismatches in the circuit in Fig. 6 introduce current offsets at the output. The current error caused by the input current mismatch decreases with the increase in the input current and depends on the mismatch percentage of the input current which relates to the current mirror mismatch. It can be reduced by choosing large devices in the current mirror. According to [30], the output current error is half of the current mirror mismatch percentage of the input current. The DC-transfer function of current conveying relies on the assumption that (i) N_3 and N_4 are identical and (ii) N_1, N_2, N_3, and N_4 have identical transistor parameter K. The transistor mismatches caused the input current error, and the threshold voltage mismatches lead to a current offset at the output. Therefore, the transistor sizing should take them into account to reduce the current offset. Large devices are preferred to reduce current mirror mismatches.

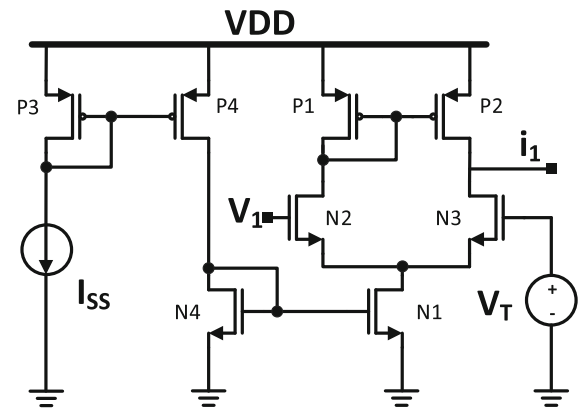

Fig. 7 Hyperbolic function implementation

3.1.3 Hyperbolic circuit

The nonlinear function $i_1 = f(V_1)$ is a hyperbolic tangent function which is based on a differential amplifier circuit as shown in Fig. 7. Assuming the MOSFET devices are working in saturation regions, the drain to source current is calculated as:

$$I_{sat} = I_D e^{\kappa V_G - V_S}. \tag{20}$$

In this circuit, the current output charges the integrated capacitors. Thus, the current mode is preferred. Driving the differential input pair to saturation, the transfer function of this circuit is proportional to the input offset, $i_1 = i_{D1} - i_{D2} = f(V_{\mathrm{in}})$ as

$$\begin{aligned} i_1 = i_{D1} - i_{D2} &= I_{\mathrm{SS}} \frac{e^{\kappa V_1} - e^{\kappa V_T}}{e^{\kappa V_1} + e^{\kappa V_T}} \\ &= I_{\mathrm{SS}} \tanh \frac{\kappa (V_1 - V_T)}{2}. \end{aligned} \tag{21}$$

The deviations from the ideal behavior of the hyperbolic tanh$(\cdot)$ circuit derive from the following: transistors mismatch, voltage limitations due to transistors coming out of saturation, and finite slope of the drain curves in saturation. In Fig. 7, the PMOS devices P_1 and P_2 in the current mirror are not 100% identical which leads to a shift and a difference between the negative and positive asymptotes of the tanh curve. This contributes to the asymmetric geography of the chaotic attractor. The voltage headroom at the output depends on the saturation properties of P_2. Therefore, the drain-source voltage at saturation $V_{\mathrm{OD_{sat}}}$ of PMOS P_2 below

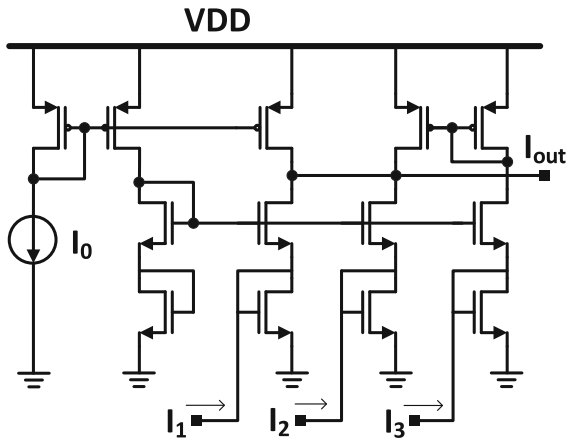

Fig. 8 Multiplier circuit design

V_{DD} sets the upper limit, while drain-source voltages at saturation of NMOS N_1 and N_3 above GND constrain the minimum output voltage.

3.1.4 Multiplier

An inverted-based transconductance amplifier was utilized to obtain current $i_2 = g_{m6}v_2$ and three current square cells were employed to construct the multiplier as shown in Fig. 8, in which $i_3 = i_1 + i_2$, and the current output from multiplier i_{out} is calculated as

$$\begin{aligned} i_{\mathrm{out}} &= I_0 + i_{o3} - i_{o1} - i_{o2} \\ &= I_0 + \frac{(i_1 + i_2 - 4I_0)^2}{16I_0} - \frac{(i_1 - 4I_0)^2}{16I_0} \\ &\quad - \frac{(i_2 - 4I_0)^2}{16I_0} \\ &= \frac{i_1 \times i_2}{8I_0} = \frac{I_{\mathrm{SS}} \tanh \frac{\kappa(V_1 - V_T)}{2} g_{m6} v_2}{8I_0} \end{aligned} \tag{22}$$

The proposed circuit realization in (11) is reformed to the original formulation of the chaotic system in (1) by normalizing by the time constant $\tau = \frac{C}{g_m}$, and dimensionless by an arbitrary voltage V_r, respectively, as

$$\begin{bmatrix} \partial V_1 & V_1 \\ \partial V_2 & V_2 \\ \partial V_3 & V_3 \\ \partial V_4 & V_4 \end{bmatrix} = \begin{bmatrix} \frac{\partial V_1}{\partial \tau} & \frac{V_1}{V_r} \\ \frac{\partial V_2}{\partial \tau} & \frac{V_2}{V_r} \\ \frac{\partial V_3}{\partial \tau} & \frac{V_3}{V_r} \\ \frac{\partial V_4}{\partial \tau} & \frac{V_4}{V_r} \end{bmatrix} \tag{23}$$

The circuit components are chosen to be compatible with the chaotic system parameters as

$$\begin{aligned} a_1 = \frac{C_1}{C_4};\ a_2 = \frac{g_{m5}}{g_m};\ b_1 = \frac{g_{m6} I_{\mathrm{SS}}}{8 g_m I_0};\ b_2 = \frac{\kappa}{2}; \\ b_3 = \frac{\kappa}{2} V_T. \end{aligned} \tag{24}$$

3.1.5 Hyperchaotic circuit

The hyperchaotic core circuit design is presented in Fig. 9 using low-voltage devices in 130 nm CMOS technology with a supply voltage of 1.2 V. All the capacitors were specifically chosen as $C = C_1 = C_2 = C_3 = C_4 = 3.2$ pF. The bias current in the differential circuit to conduct the $\tanh(\cdot)$ function is set to $I_{\mathrm{SS}} = 40\ \mu\mathrm{A}$, the voltage input $V_T = 0.65$ V, and the current source to $I_0 = 10\ \mu\mathrm{A}$. The intrinsic capacitors of the MOSFETs introduce a variation in the system's parameters of the chaotic circuit implementation in (11) g_m/C. According to Fig. 9, the parasitic capacitors at the MOSFET gates introduce the variations in the integrated capacitors. Therefore, to minimize the effect of intrinsic parasitic capacitors, the devices' sizes are minimized to reduce gate capacitors, which are proportional to $W \times L \times C_{ox}$ (W, L, and C_{ox} denote the device width, device length, and the gate-oxide capacitor per unit area, respectively). The effect of parasitic capacitors is also investigated according to the PVT variations as depicted in Fig. 10. As seen from this figure, the PVT variations may contribute up to 6% of the integrated capacitor. Despite these effects, the system successfully generates chaotic signals. The initial condition of the chaotic circuit is controlled by the initial voltages of integrated capacitors. External voltages are used to charge the integrated capacitors to provide initial values. This solution ensures that the biases of all devices in the circuit are correct and that the circuit can correctly start to oscillate. Then, the circuit is switched to an autonomous process and the noise is superimposed to the provided initial condition. Thanks to the high sensitivity of chaotic systems to the initial condition, a different circuital evolution at ever circuit startup is obtained.

The active and passive components in the circuit design affect the intrinsic oscillator frequency of continuous chaotic systems. The sampling frequency of the comparators is expected to be as high as possible at the price of the randomness of the output bitstreams. In our hyperchaotic circuit design, the circuit

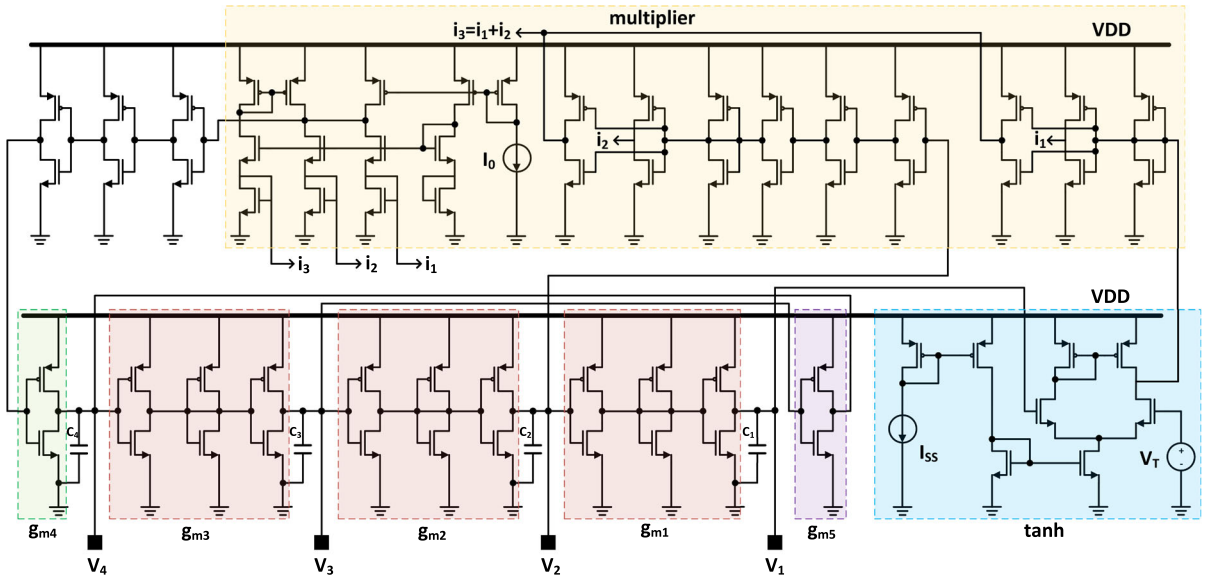

Fig. 9 Circuit design of the proposed 4D hyperchaotic system

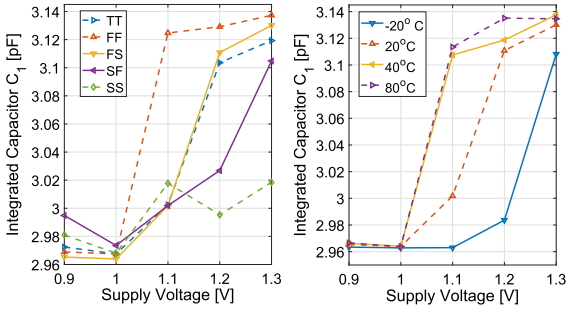

Fig. 10 Integrated capacitor C_1 according to PVT variations

topologies are considered in a trade-off between the power consumption, the circuit stability, and linearity. Indeed, the proposed chaotic system implemented in a fully CMOS circuit design has a self-oscillator frequency of $f = \frac{g_m}{2\pi C} = 5.473$ MHz which is compatible with the state-of-the-art. Therefore, the throughputs of the binary outputs can be increased by using proper post-processing and a high sampling frequency for the comparator. Compared to using off-the-shelf devices as in [11], where the oscillator frequency is limited to a maximum of 830 kHz and the sampling frequency is 19 MHz, the proposed system uses a sampling frequency between 12 and 100 MHz with different configurations of the post-processing circuit.

The chaotic output phase spaces shown in Fig. 11 are compatible with the simulation results in MATLAB. Moreover, the practical circuit design provides higher dynamic characteristics than simulation results. For example, we can still observe hidden attractors with arbitrary trajectories of chaotic signals, while it is in the limited periodic region in the system simulations in MATLAB. The power spectrum density in Fig. 12 shows the chaotic signals from the proposed 4D chaotic system circuit design in the frequency domain. As can be observed from the figure, the peak of the power spectrum is concentrated around the intrinsic oscillator frequency; however, it is possible to find spectral components with a non-negligible power for a wide band of frequencies. This allows us to use a sampling frequency much higher than the intrinsic oscillation frequency, while still expecting good results in terms of randomness. As a final comment, we can notice that using the proposed continuous hyperchaotic system to generate random bits has two advantages compared to chaotic maps. The first advantage comes from superior dynamic characteristics. The second advantage is its four-dimensional chaotic outputs. Although the proposed chaotic system has two positive Lyapunov exponents, corresponding to V_1 and V_2 voltage outputs, all four chaotic signal outputs could be used to generate random bits in parallel. Moreover, in contrast to other continuous chaotic systems, our proposed circuit design uses small embedded CMOS capacitors (3.2 pF) allowing a non-

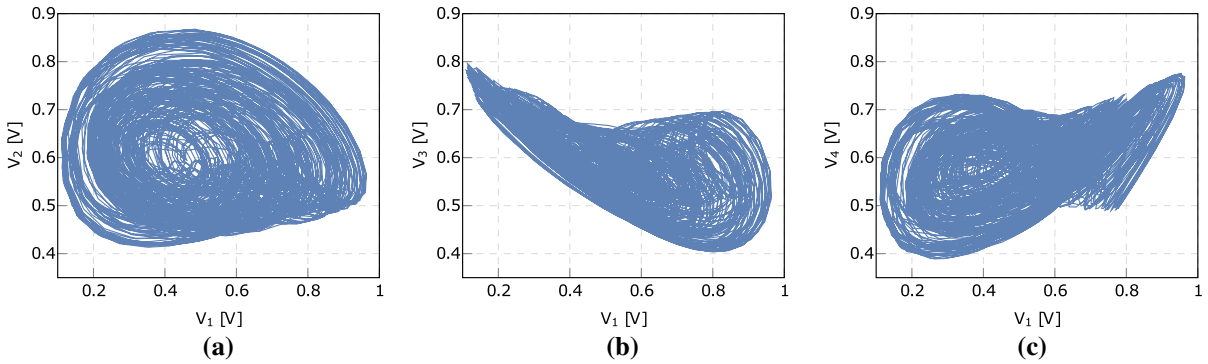

Fig. 11 Trajectories of the chaotic outputs **a** V_1–V_2, **b** V_1–V_3, and **c** V_1–V_4

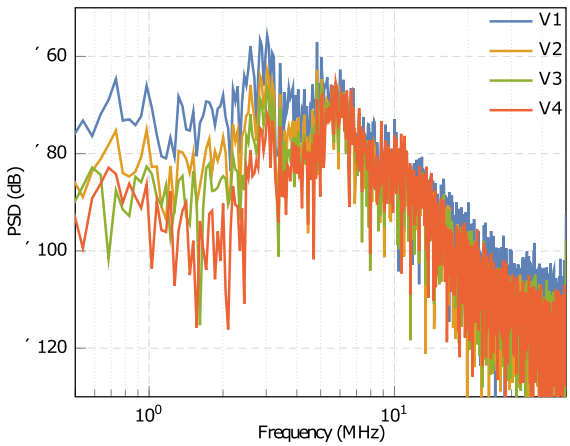

Fig. 12 Chaotic signal output frequency spectrum

negligible increase in the intrinsic frequency oscillator.

3.2 Comparator

Comparators with a maximum sampling frequency of 100 MHz are deployed. The comparator circuit design is detailed in what follows and elaborated in Fig. 13, which includes two stages. The first stage is a preamplifier which is expected to have a small gain with a high input dynamic. The output reset switch using NMOS N_4 in Fig. 13 is employed to reduce regeneration in the comparison phase. The second stage is a latch circuit which provides sufficient gain for the comparison phase at the rising edge of the clock signal. The clock frequency is operating at the maximum of 100 MHz with 50%-duty cycle. The comparator amplifies the input offset at

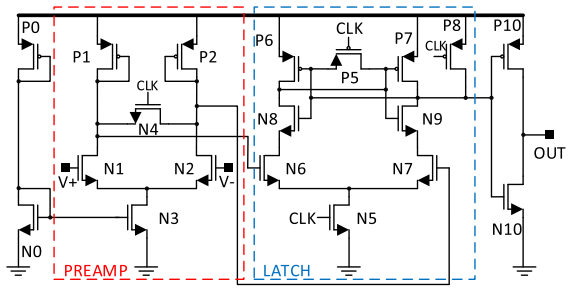

Fig. 13 Comparator circuit design

the first stage by the cross-coupled PMOS transistors P_1 and P_2, and then, the offset output is amplified with a high gain at the second stage when the clock signal CLK is at a high level. The PREAMP block is desirable to track the sampled input which is expected to have a large enough input bandwidth and low gain $g_m(N1)/g_m(P1)$. Relatively small NMOS input devices are used to meet the low input capacitance requirement. However, the random offsets due to transistor mismatches, which is the main source of nonlinearity, may be improved by increasing the device's length at the expense of higher input capacitance. The random offset caused by transistor mismatch (in both voltage threshold mismatch and transistor parameter mismatch) introduces the referred input offset V_{OS}. Two partitions of the attractor are considered $\Lambda_1 = [V_{\min}, V_{\mathrm{ref}} - V_{\mathrm{OS}}]$ and $\Lambda_2 = [V_{\mathrm{ref}} + V_{\mathrm{OS}}, V_{\max}]$, the output bit from the comparator is deduced as

$$B_x = \begin{cases} 0 & \text{if} \quad V_x \subset \Lambda_1 \\ 1 & \text{if} \quad V_x \subset \Lambda_2 \end{cases} \quad (x = 1, 2, 3, 4). \tag{25}$$

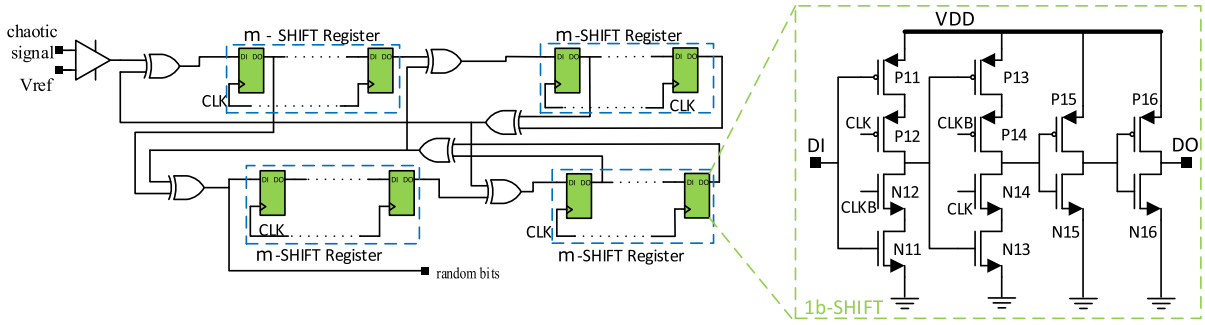

Fig. 14 Circuit design for post-processing based on dynamic D Flip-Flop

The chaotic circuit nonlinearity and mismatches contribute to the imperfection of two partitions Λ_1 and Λ_2 observed compared to the MATLAB simulations. These effects are minimized at each previous block circuit design in trade-off with its circuit requirements in both schematic and layout. The distribution of analog chaotic signals, and the statistical analysis of the mean value and standard deviation are used to setup the reference voltages V_{ref} of the comparators.

3.3 SHIFT-XOR-based post-processing

In this paper, we used a SHIFT-XOR-based PRNG with multiple values for the length of SHIFT registers. This circuit consists of four shift registers m-SHIFT registers and exclusive-ORs [23,28]. The binary output bits from the comparator are evaluated and reused to XOR-operators with the same bit-stream after a few time steps. With such an approach, as observed in [28], it is possible to have a much higher bit-rate preservation efficiency compared to canonical approaches such as a simple Von Neumann post-processing. Three values of length of shift registers $m = 2$, $m = 6$, and $m = 8$ will be evaluated in the statistical test. The circuit design for a one-bit shift register (1b-SHIFT) is elaborated in Fig.14 using a positive-edge trigger dynamic flip-flop. The first period, when CLK is low, and CLKB is high, is the sampling period where the input signal is stored. In the second phase, when CLK is changed to a high and CLKB is low, the signal is transferred to the output. Finally, the input signal is shifted one clock period.

4 Performance evaluation

The proposed circuit was designed and simulated using 130 nm CMOS technology with a 1.2 V voltage supply (VDD). In this section, we present the random bit generator performance including the power consumption, the randomness evaluation by the statistical tests, and the inter-signal correlation test. Moreover, a comparison to state-of-the-art designs is provided to emphasize the work's contribution to engineering applications.

4.1 Power consumption

The hyperchaotic circuit consumes a maximum of 980 μW in generating chaotic signals while dissipates a static current of 623 μA. The comparator utilizes 192 μW for data sampling at 100 MHz. The total power consumption without post-processing is 1240 μW at the normal sampling frequency of 12 MHz which provides a throughput of 48 Mbps by four chaotic output signals. The proposed hyperchaos-based RNG has a high energy efficiency of 25.83 pJ/b in normal operation. The power consumption is summarized in Table 3. We also tested the proposed TRNG at high-speed operation mode of 100 MHz for each chaotic output signal. In this case, a high order polynomial feedback function is used in post-processing circuit. In high-speed operation mode, the total power consumption is 1748 μW at a throughput of 400 Mbps (each chaotic output signal provides a throughput of 100 Mbps after its post-processing), which yields an energy efficiency of 4.37 pJ/b. The circuit layout is illustrated in Fig. 15, in which 8-bit SHIFT registers are used in the post-

Table 3 Power consumption summary

Power (μW)	Hyperchaos	Comparator	Total
Static	748	48	843
Dynamic@12 MHz	980(*)	65	1240
Dynamic@50 MHz	980(*)	120	1459
Dynamic@100 MHz	980(*)	192	1748

(*): The maximum power

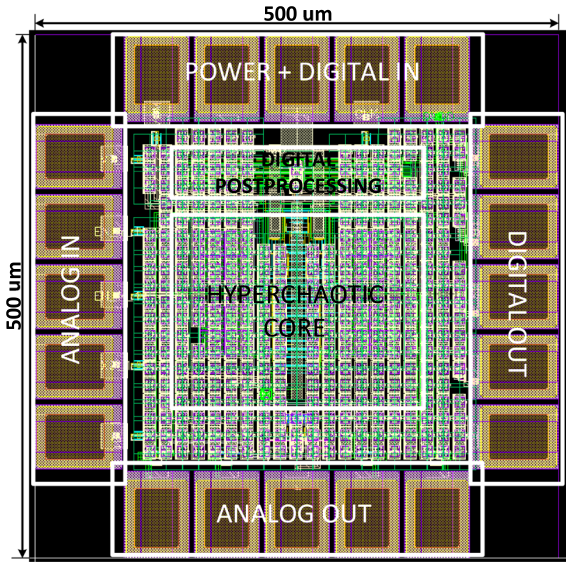

Fig. 15 Layout diagram of the chip

processing circuit. The total size includes the hyperchaotic core circuit and the digital post-processing circuit, in which the digital power is separated from the analog power to reduce noise effects.

4.2 Randomness evaluation

One hundred sixty million bits were collected for the numerical evaluation. Each chaotic dimensional signal contributed forty million bits. The standard operation tests were conducted with a normal supply (VDD=1.2 V) and at a temperature of 20°C. The environment testing included measurements of the influence of temperature and power supply variations. The operation of the proposed TRNG was tested on a wide range of temperature (0 °C, 20 °C, and 60 °C) and a 10% voltage variation (0.9 V, 1.1 V, 1.2 V, and 1.3 V).

4.2.1 Min-entropy estimation

To estimate the number of random bits extracted from chaotic signals, the min-entropy, which provides a lower-bound of the raw binary sequences extracted from chaotic signals before post-processing process, is evaluated as

$$H_{\min}(B_x) = -\log_2[\max_{B_x \subset \Lambda} P_\Lambda(B_x)](\text{bit/symbol}), \quad (26)$$

where B_x is the raw binary random variable which is the binary bit output from the comparator, with probability $P_\Lambda(B_x)$. Chaotic signals are converted into binary streams by the comparator. The conversion rate of binary sequences should be more than $H_{\min}(B_x)$ to obtain maximum entropy. The chaos-based random number generator is determined as a non-IID (non-independent and identically distributed) entropy source as described by NIST SP 800-90B [38]. Since the chaotic signals are digitalized into binary bits by the comparators, four estimation strategies including most common value, collision estimation, Markov estimation, and compression estimation are applied to the raw binary bits. Three raw binary sequences are collected with a sampling frequency $F_s = 3$MHz. Table 4 shows the results of entropy estimation on the raw binary sequences from the chaotic circuit. Since the minimum-entropy estimation is not high due to the asymmetrical geography of chaotic signals and circuit design imperfections, the post-processing circuit is needed to remove bias and increase randomness.

4.2.2 Correlation tests

The correlation, a measure of similarity between two series as a function of the displacement of one relative

Table 4 Entropy per bit estimation of the raw binary sequences

Raw data (binary)	Seq.1	Seq.2	Seq.3
Most common value	0.9976	0.9980	0.9984
Collision estimation	0.7541	0.7045	0.7487
Markov estimation	0.9729	0.9582	0.9312
Compression estimation	0.6086	0.6631	0.6437

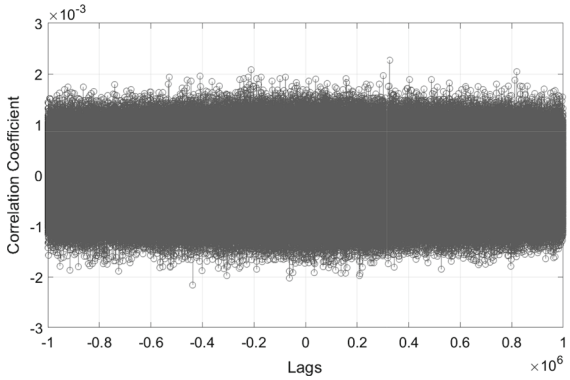

Fig. 16 Cross-correlation measurement of random bitstreams generated from different chaotic signals V_1 and V_2 at the same time

to the other, is used to measure the mutation of two bitstreams [9]. The cross-correlation is calculated as:

$$r_{x_1x_2}(k) = \frac{c_{x_1x_2}(k)}{s_{x_1}s_{x_2}}; \quad k = 0, \pm1, \pm2, \ldots \tag{27}$$

where k is the number of time shifts (lag) and $c_{x_1x_2}$ is the cross-covariance coefficient of the time series $x_{1,t}$ and $x_{2,t}$, calculated as

$$c_{x_1x_2}(k) = \begin{cases} \frac{1}{T}\sum_{t=1}^{T-k}(x_{1,t} - \bar{x_1})(x_{2,t+k} - \bar{x_2}); & k = 0, 1, \ldots \\ \frac{1}{T}\sum_{t=1}^{T+k}(x_{2,t} - \bar{x_2})(x_{1,t-k} - \bar{x_1}); & k = 0, -1, \ldots \end{cases} \tag{28}$$

where s_{x_1} and s_{x_2} are standard deviations of the series $\sqrt{c_{x_1x_1}(0)}$, and $\sqrt{c_{x_2x_2}(0)}$, respectively. To enable the use of four chaotic signals as entropy sources for random bit generators independently, the cross-correlation between these output ports is measured as depicted in Fig. 16. This figure shows the un-correlated relationship between the random bitstreams generated by the chaotic signal V_1 and V_2 after post-processing with a sampling frequency of 100 MHz.

4.2.3 NIST's test results

The final binary output bitstreams are evaluated using statistical tests to verify the randomness, according to the well-known test suite NIST SP 800-22 [24,29]. This statistical test works under a tentative assumption of randomness (H0). Therefore, if the randomness assumption is true for the data, the resulting calculated test statistic value on the data will have a very low probability of exceeding the critical value. If the P-value, which is calculated based on the critical value for each test, is larger than 0.01, there is a 99.9% possibility that the data are random. Then, the data could be used for cryptographic purposes [24]. In total, fifteen statistical tests were separated into two parts. 160M binary bits collected were divided into 1000 streams of 160Kb length for the first ten tests. The second part used 160 bitstreams of 1Mb length.

Fifteen statistical test results presented in Table 5 show the average P-value (PV) for each test and their proportional pass rates (PP). At a normal operation frequency (F_s=12 MHz), the m-SHIFT-XOR passed these tests with high P-values, and high pass proportions with $m = 2$. To evaluate the relation between the length of the shift registers and the possible sampling frequency, we increased the sampling frequency from 12 to 100 MHz. The m-SHIFT-XOR ($m = 2$) does not pass all the tests at 20 MHz. However, it can pass NIST tests with higher value of m, in other words, a higher order of polynomial feedback function. However, due to the trade-off between security and randomness, we could not increase the ratio between the sampling frequency and the intrinsic frequency excessively. The randomness is guaranteed in the high-frequency operation mode of 50 MHz with m-SHIFT-XOR when $m \geq 6$. The maximum operating frequency is tested at 100 MHz, in which the 8-SHIFT-XOR post-processing passed these statistical tests. The first ten tests require minimum proportional pass of 980 samples (98%),

Table 5 Statistical test results of the output bitstreams after post-processing

NIST SP-800.22 Test	m=2 (12 MHz)		m=2 (20 MHz)		m=6 (50 MHz)		m=6 (80 MHz)		m=8 (100 MHz)	
	PV	PP	PV	PP	PV	PP	PV	PP	PV	PP
Monobit test	0.5728	0.991	0.6184	0.985	0.0898	0.984	0.2178	0.975	0.3236	0.995
Frequency within block test	0.3160	0.990	0.0378	0.989	0.8628	0.986	0.0166	0.974	0.7636	0.989
Runs test	0.4280	0.993	0.0393	0.995	0.4924	0.986	0.6703	0.972	0.1644	0.988
Longest run 1's test	0.6308	0.994	**0.0010**	**0.798**	0.1381	0.990	0.9203	0.983	0.6308	0.994
Rank test	0.5756	0.988	0.0582	0.987	0.5422	0.990	0.0433	0.974	0.5756	0.988
Cumulative sum	0.3602	0.995	0.8832	0.988	0.7238	0.988	0.1865	0.980	0.9248	0.993
Discrete Fourier test	0.0127	0.982	**0.0003**	0.985	0.4047	0.990	**0.0004**	0.975	0.6556	0.986
Overlapping template (*)	0.1303	0.989	**0.0001**	**0.825**	0.9786	0.982	0.4082	0.987	0.1303	0.989
Non-overlapping template	0.8237	0.990	0.4262	0.994	0.8377	0.995	0.1825	0.991	0.9999	1
Linear complexity test	0.2518	0.994	0.5101	0.979	0.0356	0.981	**0.0001**	**0.957**	0.6631	0.986
Maurers universal test	0.0206	1	0.5303	1	0.4539	0.966	**0.000**	**0.121**	0.4413	1
Approximate entropy	0.4597	0.992	0.4775	0.991	0.0310	0.987	0.6662	0.975	0.9569	0.987
Serial	0.9379	0.988	0.4262	0.989	0.4118	0.986	0.4012	0.979	0.7405	0.987
Random excursions	0.6668	1	0.6286	1	0.3876	0.969	0.9229	0.981	0.3040	0.993
Random excursion variant	0.8087	1	0.9675	1	0.2492	0.990	0.8990	0.990	0.0494	1

Bold indicates a non-passed test
PV, *P* value; PP, proportion

Table 6 Comparison of modern TRNGs implemented in various entropy sources

	This work*		Chaotic TRNGs [14]*	[19]*	[40]*	Physical entropy TRNGs [31]**	[8]**
Entropy source	Cont. Hyperchaos		Dis.Chaos	Dis. Chaos	Cont. Chaos	Meta.	Thermal noise
Technology	130 nm CMOS		65 nm CMOS	65 nm CMOS	180 nm CMOS	14 nm CMOS	65 nm CMOS
Supply voltage [V]	1.2	1.2	0.4	1.8	0.6	0.65	1
Throughputs [Mbps]	48	400	0.01	50	0.27	1480	100
Power [mW]	1.240	1.748	0.142	1.32	0.000082	3.7	0.036
Energy Efficiency [pJ/b]	25.83	4.37	14.2	26.4	35.5	2.5	0.36

*post-layout simulation results, **measurement results

while the minimum requirement for the second part is 95% or 152 samples passed.

Table 6 shows a comparison between the proposed system and previous chaos-based RNGs in terms of supply voltage, bit throughput, power consumption, and energy efficiency. Our design is comparable to other chaos-based random number generators. Due to the high dimensional chaotic signals and the effectiveness of the post-processing, all four chaotic signal outputs can be used to generate random bits, and therefore the maximum throughput of the generator is increased radically. Moreover, our work is comparable to other kinds of generators which are based on physical entropy such as metastability and thermal noise [8,31]. The work in [8] shows the best energy efficiency at a maximum of 100 Mbps of throughput. Thus, the proposed random bit generator benefits from a low power consumption and a relatively high throughput.

5 Conclusion

In this paper, we presented a fully customized CMOS true random number generator including a new hyperchaotic system with hidden attractors and *m*-SHIFT-XOR post-processing to provide random binary bits for cryptographic applications. The standalone generator is fabricated in 130 nm-CMOS technology. The novelty

of the proposed 4D chaotic system was described using theoretical and mathematical analysis. Moreover, the circuit design was simulated in various working conditions against physical attacks such as power variations and noise attacks. The proposed true random number generator provides a high energy efficiency of 4.37 pJ/b for a throughput of 400 Mbps.

Acknowledgements The authors would like to thank Professor Frederic Nabki and his Ph.D. student Nakisa Shams for their technical support and valuable discussions. The authors would like to give special thank to Schlumberger Foundation for their financial support.

Funding Open access funding provided by Politecnico di Torino within the CRUI-CARE Agreement. This work has been supported by the RJM research chair.

Compliance with ethical standards

Conflict of interest The authors declare that they have no conflict of interest.

References

1. Bae, S.G., Kim, Y., Park, Y., Kim, C.: 3-Gb/s high-speed true random number generator using common-mode operating comparator and sampling uncertainty of D flip-flop. IEEE J. Solid State Circuits **52**(2), 605–610 (2017)
2. Bao, H., Wang, N., Bao, B., Chen, M., Jin, P., Wang, G.: Initial condition-dependent dynamics and transient period in memristor-based hypogenetic jerk system with four line equilibria. Commun. Nonlinear Sci. Numer. Simul. **57**, 264–275 (2018)
3. Barati, K., Jafari, S., Sprott, J.C., Pham, V.T.: Simple chaotic flows with a curve of equilibria. Int. J. Bifurc. Chaos **26**(12), 1630034 (2016)
4. Benítez, R., Bolós, V., Ramírez, M.: A wavelet-based tool for studying non-periodicity. Comput. Math. Appl. **60**(3), 634–641 (2010)
5. Carbajal-Gomez, V.H., Tlelo-Cuautle, E., Muñoz-Pacheco, J.M., de la Fraga, L.G., Sanchez-Lopez, C., Fernandez-Fernandez, F.V.: Optimization and CMOS design of chaotic oscillators robust to PVT variations: invited. Integration **65**, 32–42 (2019)
6. Chen, W., Che, W., Bi, Z., Wang, J., Yan, N., Tan, X., Wang, J., Min, H., Tan, J.: A 1.04 *mu*W truly random number generator for gen2 RFID tag. In: 2009 IEEE asian solid-state circuits conference, pp. 117–120 (2009)
7. Chen, X., Li, B., Wang, Y., Liu, Y., Yang, H.: A unified methodology for designing hardware random number generators based on any probability distribution. IEEE Trans. Circuits Syst. II Exp. Briefs **63**(8), 783–787 (2016)
8. Danesh, M., Venkatasubramaniyan, A.B., Kapoor, G., Ramesh, N., Sadasivuni, S., Chandrasekaran, S.T., Sanyal, A.: Unified Analog PUF and TRNG Based on Current-Steering DAC and VCO. In: IEEE transaction on very large scale integration (VLSI) systems. pp. 1–10 (2020)
9. Demir, K., Ergün, S.: An analysis of deterministic chaos as an entropy source for random number generators. Entropy **20**(12), 957 (2018)
10. Elwakil, A., Kennedy, M.: Chua's circuit decomposition: a systematic design approach for chaotic oscillators. J. Frankl. Inst. **337**(2–3), 251–265 (2000)
11. Ergun, S., Ozoguz, S.: A truly random number generator based on a continuous-time chaotic oscillator for applications in cryptography. In: Computer and information sciences-ISCIS 2005, vol. 3733, pp. 205–214. Springer Berlin Heidelberg, Berlin, Heidelberg (2005)
12. García-Guerrero, E., Inzunza-González, E., López-Bonilla, O., Cárdenas-Valdez, J., Tlelo-Cuautle, E.: Randomness improvement of chaotic maps for image encryption in a wireless communication scheme using PIC-microcontroller via Zigbee channels. Chaos Solitons Fractals **133**, 109646 (2020)
13. Gunhee, H., Sanchez-Sinencio, E.: CMOS transconductance multipliers: a tutorial. IEEE Trans. Circuits Syst. II Analog Digit. Signal Process. **45**(12), 1550–1563 (1998)
14. Hsueh, J.C., Chen, V.H.C.: An ultra-low voltage chaos-based true random number generator for IoT applications. Microelectr. J. **87**, 55–64 (2019)
15. Jafari, S., Sprott, J.: Simple chaotic flows with a line equilibrium. Chaos Solitons Fractals **57**, 79–84 (2013)
16. Kim, E., Lee, M., Kim, J.J.: 8.28 mb/s 28 mb/mJ robust true-random-number generator in 65 nm CMOS based on differential ring oscillator with feedback resistors. In: 2017 IEEE international solid-state circuits conference (ISSCC), pp. 144–145 (2017)
17. Kocarev, L., Szczepanski, J., Amigo, J., Tomovski, I.: Discrete chaos-I: theory. IEEE Trans. Circuits Syst. I Regul. Pap. **53**(6), 1300–1309 (2006)
18. Liu, Y., Tong, X.: Hyperchaotic system-based pseudorandom number generator. IET Inf. Secur. **10**(6), 433–441 (2016)
19. Nguyen, N., Kaddoum, G., Gagnon, F.: Implementation of a Chaotic True Random Number Generator Based on Fuzzy Modeling. In: 2018 16th IEEE international new circuits and systems conference (NEWCAS), pp. 238–242. IEEE, Montreal, QC (2018)

20. Nguyen, N., Pham-Nguyen, L., Nguyen, M.B., Kaddoum, G.: A low power circuit design for chaos-key based data encryption. IEEE Access **8**, 104432–104444 (2020)
21. Nguyen, V.H., Kumar, S., Song, H.: A family of fully integrated CMOS chaos generators with strictly 1-d linear-piecewise chaos maps. J. Comput. Electr. **17**(3), 1343–1355 (2018)
22. Palacios-Luengas, L., Duchen-Sánchez, G.I., Aragón-Vera, J.L., Vázquez-Medina, R.: Digital noise generator design using inverted 1d tent chaotic map. VLSI Des. **2012**, 1–10 (2012)
23. Pareschi, F., Rovatti, R., Setti, G.: Simple and effective post-processing stage for random stream generated by a chaos-based rng. In: The 2006 international symposium on nonlinear theory and its applications (NOLTA2006), p. 5 (2006)
24. Pareschi, F., Rovatti, R., Setti, G.: On statistical tests for randomness included in the NIST SP800-22 test suite and based on the binomial distribution. IEEE Trans. Inf. Forensics Secur. **7**(2), 491–505 (2012)
25. Petrie, C.S., Connelly, J.A.: A noise-based ic random number generator for applications in cryptography. IEEE Trans. Circuits Syst. I Fundam. Theory Appl. **47**(5), 615–621 (2000)
26. Pham, V.T., Vaidyanathan, S., Volos, C.K., Jafari, S., Wang, X.: A Chaotic Hyperjerk System Based on Memristive Device in Advances and Applications in Chaotic Systems, pp. 39–58. Springer International Publishing, Berlin (2016)
27. Prousalis, D.A., Volos, C.K., Stouboulos, I.N., Kyprianidis, I.M.: A hyperjerk memristive system with infinite equilibrium points. In: Mathemathical methods and computational techniques in science and engineering, p. 020024 (2017)
28. Rozic, V., Yang, B., Dehaene, W., Verbauwhede, I.: Iterating von neumann's post-processing under hardware constraints. In: 2016 IEEE international symposium on hardware oriented security and trust (HOST), pp. 37–42. IEEE (2016)
29. Rukhin, A., et al.: A statistical test suite for random and pseudorandom numbergenerators for cryptographic applications. Special Publication 800-22 (2010)
30. Satansup, J., Tangsrirat, W.: 1.5-V CMOS current multiplier/divider. Int. J. Electr. Comput. Eng. (IJECE) **8**(3), 1478 (2018)
31. Satpathy, S.K., Mathew, S.K., Kumar, R., Suresh, V., Anders, M.A., Kaul, H., Agarwal, A., Hsu, S., Krishnamurthy, R.K., De, V.: An all-digital unified physically unclonable function and true random number generator featuring self-calibrating hierarchical Von Neumann extraction in 14-nm tri-gate CMOS. IEEE J. Solid State Circuits **54**(4), 1074–1085 (2019)
32. Stojanovski, T., Pihl, J., Kocarev, L.: Chaos-based random number generators. part II: practical realization. IEEE Trans. Circuits Syst. I Fundam. Theory Appl. **48**(3), 382–385 (2001)
33. Teh, J.S., Teng, W., Samsudin, A.: A true random number generator based on hyperchaos and digital sound. In: 2016 3rd international conference on computer and information sciences (ICCOINS), pp. 264–269. IEEE, Kuala Lumpur, Malaysia (2016)
34. Tlelo-Cuautle, E., Dalia Pano-Azucena, A., Guillén-Fernández, O., Silva-Juárez, A.: Analog/Digital Implementation of Fractional Order Chaotic Circuits and Applications. Springer International Publishing, Cham (2020)
35. Tolba, M.F., AbdelAty, A.M., Soliman, N.S., Said, L.A., Madian, A.H., Azar, A.T., Radwan, A.G.: FPGA implementation of two fractional order chaotic systems. AEU Int. J. Electr. Commun. **78**, 162–172 (2017)
36. Trejo-Guerra, R., Tlelo-Cuautle, E., Carbajal-Gómez, V., Rodriguez-Gómez, G.: A survey on the integrated design of chaotic oscillators. Appl. Math. Comput. **219**(10), 5113–5122 (2013)
37. Trejo-Guerra, R., Tlelo-Cuautle, E., Jiménez-Fuentes, J., Sánchez-López, C., Muñoz-Pacheco, J., Espinosa-Flores-Verdad, G., Rocha-Pérez, J.: Integrated circuit generating 3- and 5-scroll attractors. Commun. Nonlinear Sci. Numer. Simul. **17**(11), 4328–4335 (2012)
38. Turan, M.S., et al.: Recommendation for the entropy sources used for random bit generation. Special Publication 800-90B (2018)
39. Vazquez-Medina, R., Del-Río-Correa, J.L., Rojas-López, C.E., Díaz-Méndez, J.A.: Digital Chaotic Noise Using Tent Map without Scaling and Discretization Process in Hybrid Artificial Intelligent Systems, pp. 105–115. Springer, Berlin (2012)
40. Wannaboon, C., Tachibana, M., San-Um, W.: A 0.18- μ m CMOS high-data-rate true random bit generator through $\delta\sigma$ modulation of chaotic jerk circuit signals. Chaos An Interdiscip. J. Nonlinear Sci. **28**(6), 063126 (2018)
41. Wieczorek, P.Z., Golofit, K.: True random number generator based on flip-flop resolve time instability boosted by random chaotic source. IEEE Tran. Circuits Syst I Regul. Pap. **65**(4), 1279–1292 (2018)
42. Willie, J.: Intel makes a digital coin tosser for future processors. In: IEEE spectrum (2010)
43. Xu, F., Yu, P.: Global stabilization and synchronization of n-scroll chaotic attractors in a modified chua's circuit with hyperbolic tangent function. Int. J. Bifurc. Chaos **19**(8), 2563–2572 (2009)
44. Yang, K., Blaauw, D., Sylvester, D.: An all-digital edge racing true random number generator robust against PVT variations. IEEE J. Solid State Circuits **51**(4), 1022–1031 (2016)
45. Yang, K., Fick, D., Henry, M.B., Lee, Y., Blaauw, D., Sylvester, D.: 16.3 A 23 mb/s 23 pj/b fully synthesized true-random-number generator in 28 nm and 65 nm CMOS. In: 2014 IEEE international solid-state circuits conference digest of technical papers (ISSCC), pp. 280–281 (2014)
46. Yujun, N., Xingyuan, W., Mingjun, W., Huaguang, Z.: A new hyperchaotic system and its circuit implementation. Commun. Nonlinear Sci. Numer. Simul. **15**(11), 3518–3524 (2010)