International Journal of Automation and Computing 11(6), December 2014, 588-597
DOI: 10.1007/s11633-014-0839-9

Designing Chaotic Mathematical Circuits for Solving Practical Problems

René Lozi
Laboratory J. A. Dieudonné, UMR CNRS 7351, University of Nice-Sophia Antipolis, Parc Valrose 06108, Nice Cedex 02, France

Abstract: We introduce the paradigm of chaotic mathematical circuitry which shows some similarity to the paradigm of electronic circuitry, especially in the frame of chaotic attractors for solving practical problems (generating hyperchaos; developing chaos based pseudo random number generator (CPRNG) and chaotic multistream PRNG; secure communication via synchronization). They can also be used in cryptography, generic algorithms in optimization, control, etc.

Keywords: Chaotic mathematical circuit, circuit modeling, chaos, Chua′s circuit, pseudo-random number generator.

1 Introduction

Our purpose is to build up an analogue to the paradigm of electric circuitry, which is the design of electronic circuits: the paradigm of chaotic mathematical circuitry, in order to easily improve the performance of well known chaotic attractors for application purposes (chaotic cryptography, evolutionary and genetic algorithms in optimization, control, etc). However, some differences occur in the analogy: Mathematical circuits are generic rather than specific like electric circuits.

An electronic circuit is composed of individual electronic components, such as resistors, transistors, capacitors, inductors and diodes, connected by conductive wires through which electric current can flow. The combination of components and wires allows various simple and complex operations to be performed: Signals can be amplified, computations can be accomplished, and data can be moved from one place to another. Very complex systems can be analyzed using various sophisticated methods[1−3]. We introduce in the same way mathematical circuits which are composed of individual components (generators, couplers, samplers, mixers, reducers and cascaders, etc.) connected through streams of data. The combination of such mathematical components leads to several new applications such as improving the performance of well known chaotic attractors (Chua, Lorenz, Rössler, etc.) for application purposes.

From a mathematical point of view, at least in order to implement applications of chaotic behaviors, all these chaotic attractors have the same structure: Given initial values and a set of parameters, they provide three streams of data symbolized by three arrows. On the contrary, the electric realization of their equation leads to very different electric circuits. In fact, mathematical circuits capture the essential of dynamics of chaotic attractors.

In Section 2, we present several symbols of generators (both continuous and discrete) used in the paradigm of mathematical circuits, and we compare mathematical circuits with the electric ones. In Section 3, we introduce others circuit elements (couplers, sampler, mixer, reducer and cascader) in practical problems: generating hyperchaos, developing chaos based pseudo random number generators (CPRNGs), and chaotic multistream pseudo random number generators (Cms-PRNGs), secure communication via synchronization. The conclusions are given in Section 4.

Regular paper
Special Issue on Recent Advances on Complex Systems Control, Modelling and Prediction II
Manuscript received August 29, 2013; accepted November 4, 2013

2 Elementary mathematical circuit elements

2.1 Continuous generators: Chua′s circuit, Rössler and Lorenz attractors

Analog electric circuits are very commonly represented by schematic diagrams, in which wires are shown as lines, and each component has a unique symbol (Fig. 1).

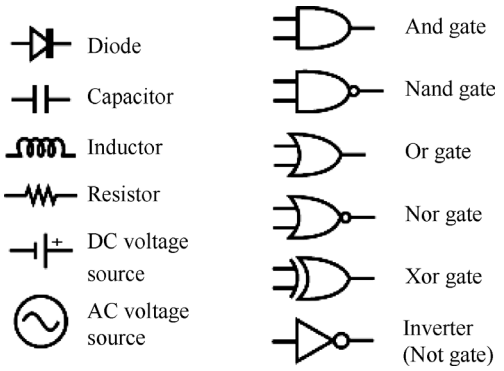


Fig. 1 Electrical symbols (left-hand side column) and electronic circuit symbols (right-hand side column) used for drawing schematic diagram

We present in this section some symbols we design in order to draw mathematical schematic diagrams. First, we describe generator symbols, which are, from a mathematical point of view, equivalent to a battery or a variable current generator in an electric circuit. In the paradigm of mathematical circuitry, they generate a digital signal (in one or several dimensions) rather than an electrical current

characterized by its voltage and intensity variations (nonetheless, a voltage or an intensity variation can be considered as a physical signal which can be discretized).

This signal can be either continuous as in Chua's circuit, Lorenz or Rössler attractors or discrete as in the Lozi mapping or the symmetric tent map. We consider first the continuous ones, inspired by the Chua's famous circuit[4] (Fig. 2 (a)) which contains three linear energy-storage elements (an inductor and two capacitors), a linear resistor, and a single nonlinear resistor, namely Chua's diode (Fig. 2 (b)) with three segment linear characteristics defined by

$$f(v_R) = m_0 v_R + \frac{1}{2}(m_1 - m_0)\left[|v_R + B_p| - |v_R - B_p|\right] \quad (1)$$

where the slopes in the inner and the outer regions are m_0 and m_1, respectively, and $\pm B_p$ denote the breakpoints.

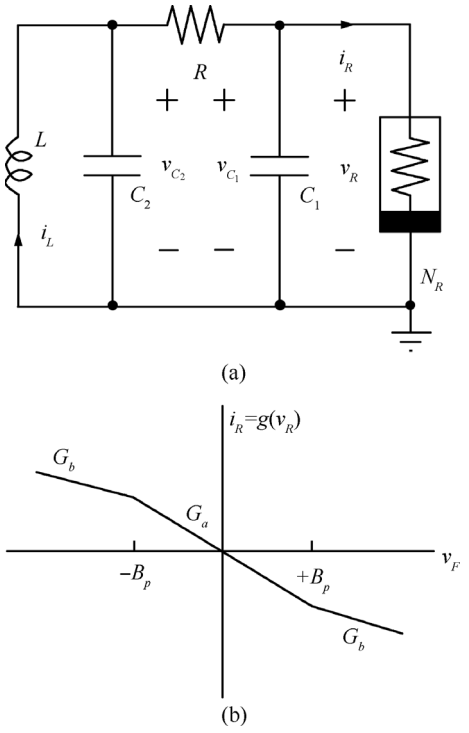


Fig. 2 Chua's circuit. (a) Electronic realization; (b) Three-segment piecewise-linear v-i characteristic of nonlinear voltage controlled resistor (Chua's diode)

The dynamics of Chua's circuit is governed by (2) where V_{C_1}, V_{C_2}, and i_L are the voltages across the capacitors C_1 and C_2, and the intensity of the electrical current through the inductor L, respectively.

$$\begin{cases} C_1 \dfrac{\mathrm{d}v_{C_1}}{\mathrm{d}t} = G(v_{C_2} - v_{C_1}) - f(v_{C_1}) \\ C_2 \dfrac{\mathrm{d}v_{C_2}}{\mathrm{d}t} = G(v_{C_1} - v_{C_2}) + i_L \\ L \dfrac{\mathrm{d}i_L}{\mathrm{d}t} = -v_{C_2}. \end{cases} \quad (2)$$

Equation (2) can be transformed into the system of three first-order autonomous differential equations whose dimension-less form is

$$\begin{cases} \dot{x} = \alpha(y - x - f(x)) \\ \dot{y} = x - y + z \\ \dot{z} = -\beta y \end{cases} \quad (3)$$
$$f(x) = bx + \frac{1}{2}(a - b)\left[|x + 1| - |x - 1|\right]$$

for which the set of parameter values

$$\alpha = 15.60, \quad b = 28.58, \quad a = -\frac{1}{7}, \quad b = \frac{2}{7}$$

is very often used in order to generate chaotic signal. Even if the scheme of Fig. 2 (a) is easily understandable by electric engineers, it is of no help to build a device using mathematical properties of chaos (like a secure communication system based on it[5]). This is why it is more useful to represent Chua's circuit as a chaos generator by the diagram of Fig. 3 (a). On this detailed flowchart of continuous generator, the solid line arrows coming out from the generator represent the three components of the signal $\underline{x}(t) = (x(t), y(t), z(t))$, the dashed line arrow which points at λ stands for the parameter value, and the dot line arrow which points at $\underline{x}_0 = \underline{x}(0)$ indicates the given initial value.

If there is no ambiguity on the nature of the generator used, the symbol can be simplified as in Fig. 3 (b).

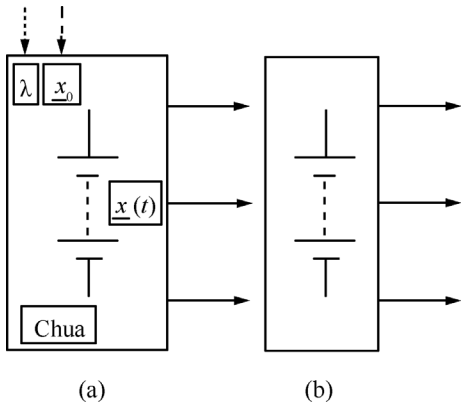


Fig. 3 Continuous generator. (a) Chua's circuit; (b) Simplified symbol

The diagram defined above is suitable, even if we use others types of equations, for generating streams of data, provided the number of streams is the same as in Chua's circuit (if it is not the case, more arrows can be added (Fig. 9)). For example, the Lorenz attractor[6]

$$\begin{cases} \dot{x} = -\sigma(x + y) \\ \dot{y} = \rho x - y - xz \\ \dot{z} = xy - \beta z \end{cases} \quad (4)$$

often studied using the parameter values

$$\sigma = 10, \ \rho = 28, \ \beta = \frac{8}{3}$$

and the Rössler attractor[7]

$$\begin{cases} \dot{x} = -y - z \\ \dot{y} = x + ay \\ \dot{z} = b + z(x - c) \end{cases} \quad (5)$$

for which the parameter values

$$a = 0.2,\ b = 0.2,\ c = 5.7$$

exhibits a strange attractor.

In the next subsection, we show that from a mathematical point of view, in order to build an application of chaotic behaviors, all the attractors generated by these equations have the same structure: Given initial values and a set of parameters, they provide three streams of data symbolized by three arrows. Quite the contrary the electric realization of their equation leads to very different electric circuits.

2.2 Mathematical circuits vs. electric circuits

Although our goal is to build up mathematical circuits that are analogue to the paradigm of electric circuitry, there are some differences between both kinds of circuits. Mathematical circuits are generic rather than specific like electric circuits. The symbol of Fig. 3 (b) shall apply to a class of chaotic (or non-chaotic as well) attractors in 3-dimensional phase space, for instance Chua, Lorenz and Rössler attractors. In contrast, electric implementation of such attractors looks very different. Fig. 2 (a) displays the electric realization of Chua′s circuit which displays Chua attractor on oscilloscope screen.

One among several realizations of Lorenz′s circuit[8] is showed in Fig. 4. The variables, x, y, z of (4) are the voltages across capacitors C_1, C_2, and C_3 after a suitable rescaling.

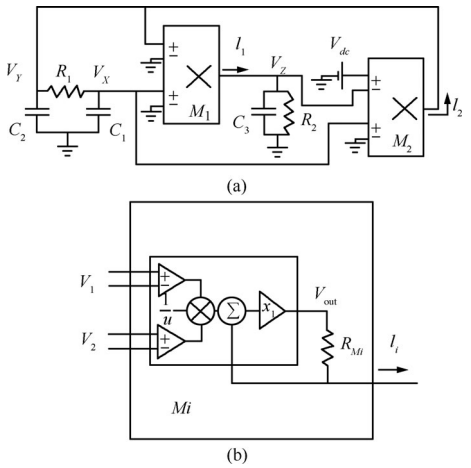


Fig. 4 Lorenz′s circuit. (a) Schematic diagram of a simple circuit. Analog multipliers M_1 and M_2 are configured as current output devices; (b) Schematic diagram of a generic analog multiplier M_i configured as a current output device[8]

An hardware electronic circuit based on slightly modified Rössler equations[9] is shown in Fig. 5. In this circuit, the operational amplifiers OP-1, OP-2 and OP-3 act as integrators for the system with x, y and z as their outputs, respectively.

In fact, mathematical circuits capture the essential of dynamics of chaotic attractors.

2.3 Discrete generators: Symmetric tent map and Lozi mappings

Apart from chaotic circuits running with continuous signal, there are chaotic circuits functioning with discrete signal. There is a need to design such generators. For this purpose, some classical chaotic mappings can be considered: in dimension 1 symmetric tent map, and in dimension 2 Lozi mappings.

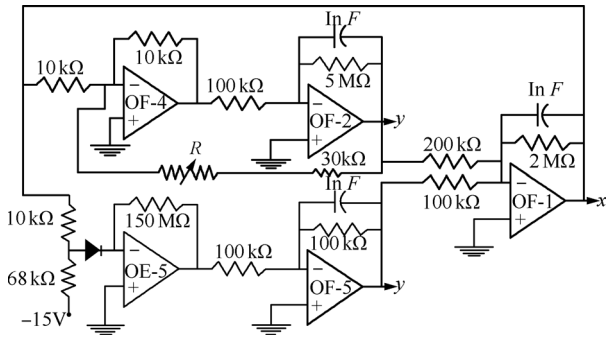


Fig. 5 Electronic circuit representation of a modified Rössler′s system[9]

The symmetric tent map[10]:

$$f(x) = 1 - 2\,|x| \tag{6}$$

associated with the dynamical system

$$x_{n+1} = 1 - 2\,|x_n| \tag{7}$$

is represented by the symbol of Fig. 6.

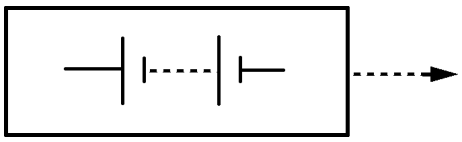


Fig. 6 One-dimensional discrete generator (e.g., symmetric tent map)

For dimension 2, Lozi mappings[11] defined by

$$L_{a,b} : \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} y + 1 - a\,|x| \\ bx \end{pmatrix} \tag{8}$$

which exhibit a strange attractor for the parameter values $a = 1.7$, $b = 0.5$ are represented by the symbols of Fig. 7.

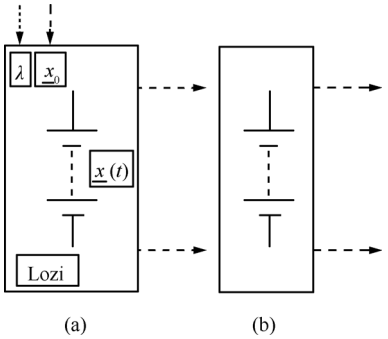


Fig. 7 2-dimensional discrete generator. (a) Lozi map, expanded symbol; (b) Simplified symbol

Remark 1. In the rest of this article, we use solid line arrow for continuous signal $x(t)$, and dashed line arrow for discrete signal x_n.

2.4 Other circuits elements

Rather than to give a tedious list of elementary mathematical components used for mathematical circuit design, we will introduce them each time they are first used for a practical purpose.

That list includes: generators, couplers, sampler, mixer, reducer and cascader. They are connected through streams of data represented by continuous or dashed line and arrows.

3 Solving practical problems

3.1 Building up hyperchaotic electronic and mathematical circuits using a ring coupler

As highlighted in [12], "One of the most interesting features of Chua′s circuit is its easy electronic implementation. Soon after its inception, the circuit was studied experimentally thereby confirming the presence of double scroll in it. Due to the presence of linear passive devices, the task of designing Chua′s circuit was reduced to designing Chua′s diode. In fact, unlike many other chaotic systems, the presence of grounded capacitors and inductors makes Chua′s circuit a very-large-scale integration (VLSI) friendly chaotic system."

However, Chua′s circuit provides only 3-dimensional chaos, as Figs. 3 (a) and (b), with its three arrows emphasized. For studying a more complex chaotic behavior called hyperchaos, which has been reported in hydrodynamics and semiconductor devices, one has to combine the behavior of several Chua′s circuits and couple them in various ways.

The experimental observation of hyperchaotic attractors in open and closed chains of Chua′s circuits was reported in 1994[13]. The layout of the five identical coupled Chua′s circuits forming a ring is shown in Fig. 8.

The state equations of this circuit are as (9). Through identifying symbols $(V_{C_1}^{(i)}, V_{C_2}^{(i)}, I_L^{(i)})$ in each Chua′s circuit with (x^i, y^i, z^i), the state equations of the circuit can be translated into the system of fifteen differential equations shown in (10), and the electronic circuit of Fig. 8 is symbolized by the mathematical circuit of Fig. 9.

In Fig. 9, the double rounded arrows symbolize the coupling of one Chua′s circuit to the next one. In order to represent the coupling between mathematical equations, depending on the nature of the coupling, we can use two different symbols: The ring coupler corresponding to the coupling of one generator to the next one (Fig. 9) and the full coupler when the coupling involves more connections between the couplers as shown in the next subsection (Fig. 10).

$$\begin{cases} C_1\dfrac{\mathrm{d}v_{C_1}^{(1)}}{\mathrm{d}t} = G\left(v_{C_2}^{(1)} - v_{C_1}^{(1)}\right) - f\left(v_{C_1}^{(1)}\right) \\ C_2\dfrac{\mathrm{d}v_{C_2}^{(1)}}{\mathrm{d}t} = G\left(v_{C_1}^{(1)} - v_{C_2}^{(1)}\right) + i_L^{(1)} + K_1\left(v_{C_2}^{(2)} - v_{C_2}^{(1)}\right) \\ L\dfrac{\mathrm{d}i_L^{(1)}}{\mathrm{d}t} = -v_{C_2}^{(1)} \\ C_1\dfrac{\mathrm{d}v_{C_1}^{(2)}}{\mathrm{d}t} = G\left(v_{C_2}^{(2)} - v_{C_1}^{(2)}\right) - f\left(v_{C_1}^{(2)}\right) \\ C_2\dfrac{\mathrm{d}v_{C_2}^{(2)}}{\mathrm{d}t} = G\left(v_{C_1}^{(2)} - v_{C_2}^{(2)}\right) + i_L^{(2)} + K_2\left(v_{C_2}^{(3)} - v_{C_2}^{(2)}\right) \\ L\dfrac{\mathrm{d}i_L^{(2)}}{\mathrm{d}t} = -v_{C_2}^{(2)} \\ \quad\cdots \\ C_1\dfrac{\mathrm{d}v_{C_1}^{(5)}}{\mathrm{d}t} = G\left(v_{C_2}^{(5)} - v_{C_1}^{(5)}\right) - f\left(v_{C_1}^{(5)}\right) \\ C_2\dfrac{\mathrm{d}v_{C_2}^{(5)}}{\mathrm{d}t} = G\left(v_{C_1}^{(5)} - v_{C_2}^{(5)}\right) + i_L^{(5)} + K_5\left(v_{C_2}^{(1)} - v_{C_2}^{(5)}\right) \\ L\dfrac{\mathrm{d}i_L^{(5)}}{\mathrm{d}t} = -v_{C_2}^{(5)} \end{cases} \tag{9}$$

$$\begin{cases} \dot{x}^1 = \alpha(y^1 - x^1 - f(x^1)) \\ \dot{y}^1 = x^1 - y^1 + z^1 + k_1(y^2 - y^1) \\ \dot{z}^1 = -\beta y^1 \\ \dot{x}^2 = \alpha(y^2 - x^2 - f(x^2)) \\ \dot{y}^2 = x^2 - y^2 + z^2 + k_2(y^3 - y^2) \\ \dot{z}^2 = -\beta y^2 \\ \quad\cdots \\ \dot{x}^5 = \alpha(y^5 - x^5 - f(x^5)) \\ \dot{y}^5 = x^5 - y^5 + z^5 + k_5(y^1 - y^5) \\ \dot{z}^5 = -\beta y^5. \end{cases} \tag{10}$$

3.2 Developing chaos based pseudo random number generator (CPRNG) using full coupler, sampler, mixer, and reducer

It is well known that industrial mathematics is greedy of massive amounts of random and pseudorandom numbers, as they are vital in many areas of modern technology such as fast communication systems, economy, equity trading and in a wide range of engineering applications. US and European patents using discrete maps for providing these numbers are registered by specialists of discrete dynamical systems[14,15]. We have recently proposed efficient chaotic pseudo random number generators (CPRNGs)[16]. They are based on the ultra weak multidimensional coupling of p 1-dimensional dynamical systems which preserve the chaotic properties of the continuous models in numerical experiments. Combined with chaotic sampling and mixing processes, ultra weak coupling leads to families of CPRNGs which are very effective[17].

It was shown a few years ago[18] that the ultra-weak coupling of several logistic or symmetric tent maps (6) allows the production of long series of chaotic numbers equally distributed over the interval $[-1, 1]$ of the real line.

The system of p-coupled tent map is given by

$$X_{n+1} = F(X_n) = A(\underline{f}(X_n)) \tag{11}$$

where $X_n = \begin{pmatrix} x_n^1 \\ \vdots \\ x_n^p \end{pmatrix}$, $\underline{f}(X_n) = \begin{pmatrix} f(x_n^1) \\ \vdots \\ f(x_n^p) \end{pmatrix}$, and A is the matrix that is shown at the bottom of this page.

The design of the corresponding mathematical circuit is displayed in Fig. 10.

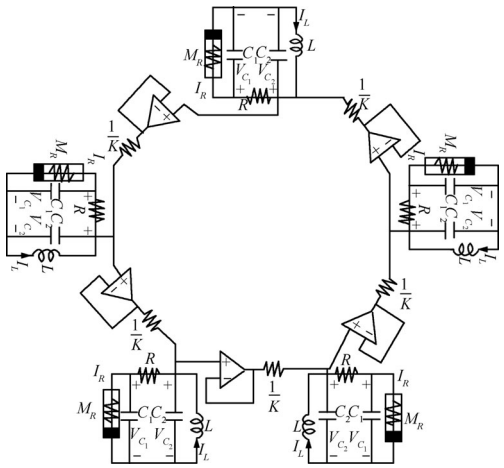


Fig. 8 Five identical coupled Chua′s circuits forming a ring[13]

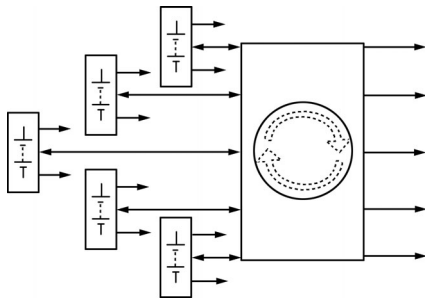


Fig. 9 Mathematical circuit of five identical coupled Chua′s circuits forming a ring

At this point it is important to note that chaotic numbers are not pseudo-random numbers because the plot of the couples of any component $(x_n^l,\ x_{n+1}^l)$ of the iterated f points $(X_n,\ X_{n+1})$ in the corresponding phase f plane reveals the map used as 1-dimensional dynamical systems to generate them via (11). Nevertheless a family of enhanced CPRNG in order to compute very fast long series of pseudorandom numbers with desktop computer has been introduced[19]. The way to conceal the chaotic genuine function is the ultra-weak coupling mechanism which has been improved.

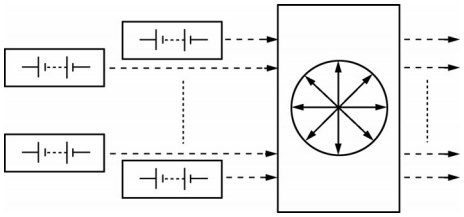


Fig. 10 Circuit of ultraweak coupling of p 1-dimensional chaotic map

In order to hide f of (11) in the phase space $(x_n^l,\ x_{n+1}^l)$, the sequence $(x_0^l,\ x_1^l,\ x_2^l, \cdots,\ x_n^l,\ x_{n+1}^l, \cdots)$ generated by the l-th component of X_n is sampled chaotically, selecting x_n^l every time the value of x_n^m the m-th component of X_n, is strictly greater than a threshold T belonging to the interval $[-1,\ 1]$ of the real line.

The pseudo-code, for computing such chaotically subsampled numbers is

$X_0 = (x_0^1,\ x_0^2, \cdots\ x_0^{p-1},\ x_0^p) = \text{seed}$
$n = 0;\ q = 0;$
do {while $n < N$
do {while $x_n^m < T$
compute $(x_n^1,\ x_n^2, \cdots,\ x_n^{p-1},\ x_n^p);\ n++\}$
compute $(x_n^1,\ x_n^2, \cdots, x_n^{p-1},\ x_n^p);$
then $n(q) = n;\quad \overline{x}_q = x_{n(q)}^1;\ n++;\ q++\}.$

This chaotic under-sampling is possible due to the independence of each component of the iterated points X_n vs. the others[19]. We introduce the symbol of this sampler on the right-hand side of Fig. 11 in order to give a schematic representation of this chaotic under-sampling process.

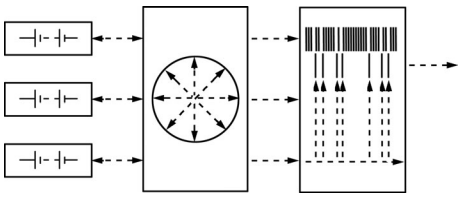


Fig. 11 Circuit of enhanced CPRNG based on chaotic undersampling

$$A = \begin{pmatrix} \varepsilon_{1,1} = 1 - \sum_{j=2}^{j=p} \varepsilon_{1,j} & \varepsilon_{1,2} & \cdots & \varepsilon_{1,p-1} & \varepsilon_{1,p} \\ \varepsilon_{2,1} & \varepsilon_{2,2} = 1 - \sum_{j=1,j\neq 2}^{j=p} \varepsilon_{2,j} & \cdots & \varepsilon_{2,p-1} & \varepsilon_{2,p} \\ \vdots & \ddots & & \vdots & \vdots \\ \vdots & & \ddots & \vdots & \vdots \\ \varepsilon_{p,1} & \cdots & \cdots & \varepsilon_{p,p-1} & \varepsilon_{p,p} = 1 - \sum_{j=1}^{j=p-1} \varepsilon_{p,j} \end{pmatrix}.$$

A second mechanism can improve the unpredictability of the pseudo-random sequence generated as above, using synergistically all the components of the vector X_n instead of two.

Given $p-1$ thresholds

$$0 < T_1 < T_2 < \cdots T_{p-1} < 1$$

which define a partition $J_1, J_2, \cdots, J_{p-1}$ of the interval $[-1, 1]$, the pseudo-code for computing such chaotically subsampled numbers is

$X_0 = (x_0^1,\ x_0^2, \cdots\ x_0^{p-1},\ x_0^p) = \text{seed}$
$n = 0;\ q = 0;$
do {while $n < N$
do {while $x_n^m \in J_0$
compute $(x_n^1,\ x_n^2, \cdots, x_n^{p-1},\ x_n^p);\ n++\}$
compute$(x_n^1, x_n^2, \cdots, x_n^{p-1}, x_n^p)$
let k be such that $x_n^p \in J_k$
then $n(q) = n;\quad \overline{x}_q = x_{n(q)}^k;\ n++;\ q++\}.$

We draw the symbol on the right-hand side of Fig. 12 in order to give a schematic representation of the chaotic mixing process. For sake of simplicity, we have only displayed a circuit with three 1-dimensional generators. However, the mixing process runs better when more generators are coupled.

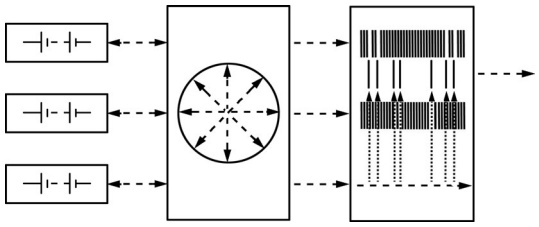


Fig. 12 Circuit of enhanced CPRNG based on chaotic mixing

We can say that the design of mathematical circuit including couplers, samplers or mixers allows the emergence of complexity in chaotic systems which leads to randomness[17].

We introduce now another process which can directly provide random numbers without sampling or mixing, although it is possible to combine those processes with it. The idea underlying this process is to confine on $[-1, 1]^p$ considered as a torus, a ring of p-coupled symmetric tent maps (or logistic maps)[20].

Consider the equalities:

$$\begin{cases} x_{n+1}^1 = 1 - 2\left|x_n^1\right| + k_1 x_n^2 \\ \vdots \\ x_{n+1}^m = 1 - 2\left|x_n^m\right| + k_m x_n^{m+1} \\ \vdots \\ x_{n+1}^{p-1} = 1 - 2\left|x_n^{p-1}\right| + k_{p-1} x_n^p \\ x_{n+1}^p = 1 - 2\left|x_n^p\right| + k_p x_n^1 \end{cases} \tag{12}$$

where the parameters $k_i = \mp 1$. In order to confine the variables x_{n+1}^i on the torus $[-1, 1]^p$, we do for every iteration the transform:

$$\begin{cases} \text{add } 2, & \text{if } (x_{n+1}^j < -1) \\ \text{substract } 2, & \text{if } (x_{n+1}^j > 1). \end{cases} \tag{13}$$

We design a new symbol: the reducer, on the right-hand side of Fig. 13, in order to give a schematic representation of the projection of the variable on the torus. For the sake of simplicity, we have again displayed a circuit with only three 1-dimensional generators. However, this new pseudo-random number generator works better when more generators are coupled as in the previous example.

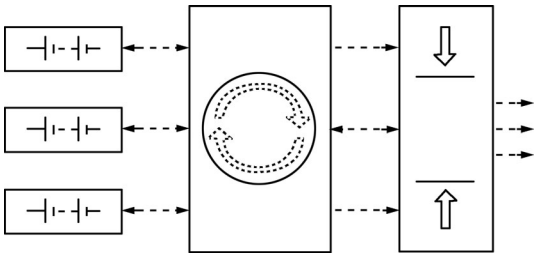


Fig. 13 Reducer for the circuit (12) and the transform (13) with $p = 3$

The particularity of this coupling is that each variable x^j is coupled only with itself and x^{j+1}, i.e., using a ring coupler as shown in Fig. 13. At first glance, in order to enrich the random properties of the map, it could seem interesting to add supplementary cross couplings between these variables, i.e., using a full coupler as in Fig. 10. However, in this case, a full coupling is inappropriate because it would increase the determinism and therefore deteriorate the statistical properties which we are looking for.

To evaluate the random property of these generators, the set of National Institute of Standards and Technology (NIST) tests[21] have been used.

The random property validations of both a 4-dimensional system and a 10-dimensional one have been carried out[22]. For this purpose, the chaotic carrier output needs to be quantized and binarized (0 and 1) in order to be validated as random using NIST tests. Therefore, different methods of binarization (converting real signals to binary ones) have been implemented and compared.

A first 1-bit binarization has been applied to the system output (12, 13), defined as $y_n = x_n^j$ with $j \in [[1, p]]$,

$$\begin{cases} b = 1, & \text{if } (y_n \geqslant 0) \\ b = 0, & \text{else.} \end{cases} \tag{14}$$

The results proved to be highly sensitive to the type of binarization. Eventually, after testing several different methods, a 32-bit binarization was chosen as the most suitable solution. Because the system is confined to the p-dimensional torus $[-1, 1]^p$, 31 bits are assigned to represent the decimal part, and 1 bit to the sign. To illustrate the results, the NIST tests for the 4-dimensional system with parameters $k_i \in (-1)^{i+1}$ are shown in Fig. 14. The chosen conditions are: The length of the original sequence $= 10^8$ bits, the length of bit string $= 10^6$ bits, the quantity of bit

RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES

generator is <data/lozi_10_positif.txt>

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE	PROPORTION	STATISTICAL TEST
8	5	13	9	9	12	6	19	8	11	0.102526	96/100	Frequency
11	16	9	10	10	10	14	6	8	6	0.437274	99/100	BlockFrequency
11	5	8	11	10	5	11	11	13	15	0.419021	97/100	CumulativeSums
8	6	17	10	10	6	7	11	15	10	0.213309	97/100	CumulativeSums
5	8	17	15	6	8	6	14	10	11	0.075719	99/100	Runs
11	11	10	13	9	5	8	8	15	10	0.637119	99/100	LongestRun
6	8	17	14	10	8	9	15	7	6	0.122325	99/100	Rank
9	10	9	13	10	10	9	8	12	10	0.991468	99/100	FFT
14	15	8	10	14	10	11	9	4	5	0.191687	98/100	NonOverlappingTemplate
10	8	11	9	9	13	7	12	10	11	0.964295	99/100	OverlappingTemplate
13	16	6	8	7	10	13	10	8	9	0.455937	100/100	Universal
9	10	12	8	10	11	5	14	11	10	0.816537	97/100	ApproximateEntropy
6	5	6	5	9	11	5	6	8	5	0.637119	65/66	RandomExcursions
3	5	6	7	10	10	9	6	4	6	0.407091	65/66	RandomExcursionsVariant
3	8	8	12	12	9	13	8	13	14	0.319084	100/100	Serial
4	3	12	18	12	8	8	14	9	12	0.028817	100/100	LinearComplexity

Fig. 14 Example of NIST Test for $k^i = (-1)^{i+1},\ i = 1, 2, \cdots, 4$, each sequence of components satisfies the NIST test for randomness

strings = 100. The output of the system has been arbitrary chosen to be $y = x_n^4$.

Furthermore, as the results show their independence of the initial conditions, every bit string in this test is the resulting sequence of a different randomly chosen initial condition. The criterion for a successful test is that the p-value has to be superior to the significance level (0.01 for this case). For the present model, all tests were successful thus the sequences can be accepted as random.

3.3 Chaotic multistream pseudo random number generators (Cms-PRNG)

It is possible to combine several equations in order to design chaotic multistream pseudo random number generators (Cms-PRNGs) or combine several processes in order to generate uncorrelated sequences of pseudo-random numbers, possessing a large number of keys for a cryptographic use.

This is simply obtained by adding a full coupler as a keyer as shown in the circuit of Fig. 15, corresponding to (15) with the reduction process of (13).

$$\begin{cases} x_{n+1}^1 = 1 - 2\left|x_n^1\right| + k_1\left[\left(1 - \sum\limits_{j=3}^{p}\varepsilon_{1,j}\right)x_n^2 + \sum\limits_{j=3}^{p}\varepsilon_{1,j}x_n^j\right] \\ \qquad\qquad \vdots \\ x_{n+1}^m = 1 - 2\left|x_n^m\right| + k_m\left[\left(1 - \sum\limits_{j=1,j\neq m;m+1}^{p}\varepsilon_{m,j}\right)x_n^{m+1} + \right. \\ \qquad \left.\sum\limits_{j=1,j\neq m;m+1}^{p}\varepsilon_{m,j}x_n^j\right] \\ \qquad\qquad \vdots \\ x_{n+1}^{p-1} = 1 - 2\left|x_n^{p-1}\right| + k_{p-1}\left[\left(1 - \sum\limits_{j=1}^{p-2}\varepsilon_{p-1,j}\right)x_n^p + \right. \\ \qquad \left.\sum\limits_{j=1}^{p-2}\varepsilon_{p-1,j}x_n^j\right] \\ x_{n+1}^p = 1 - 2\left|x_n^p\right| + k_p\left[\left(1 - \sum\limits_{j=2}^{p-1}\varepsilon_{p,j}\right)x_n^1 + \sum\limits_{j=2}^{p-1}\varepsilon_{p,j}x_n^j\right]. \end{cases} \tag{15}$$

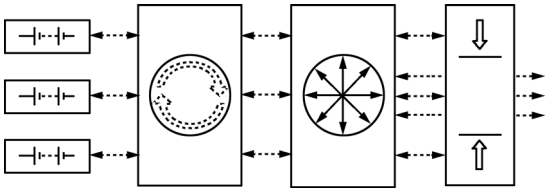


Fig. 15 Circuit of Cms-PRNG with only 3 streams

3.4 Secure communication via chaotic synchronization using a cascader

The synchronization of two Chua′s circuits was studied experimentally eight years after its discovery in 1992[23], soon followed by its application to encrypted transmission. In 1992, the first laboratory demonstration of a secure communication system using a chaotic signal for masking purposes was built[24]. The technique exploited the chaotic synchronization in order to recover the signal[25]. While the "transmitter"[25] is a direct implementation of the method proposed in [24], the "receiver" differs from the computer simulation approach, because it actually contains two subsystems of the "chaotic transmitter" (Chua′s circuit).

The mathematical translation of the dynamics of the circuit used in [25] for the experimental demonstration of secure communication is as follows: The basic building block is a Chua′s circuit, and the dynamics of which is given by the Chua′s equations (3). The noise-like signal $u(t)$ is used to hide the message. If $s(t)$ is an information-bearing signal, the transmitted one is $r(t) = u(t) + s(t)$, where $s(t)$ is assumed to have a significantly lower power level than that of $u(t)$. Hence the signal $s(t)$ is effectively "masked".

Two sub-systems compose the receiver.

The first sub-system is driven by the transmitted signal $r(t)$:

$$\begin{cases} \dot{v}_1 = r(t) - v_1 + w_1 \\ \dot{w}_1 = -\beta v_1. \end{cases} \tag{16}$$

The second one is driven by the signal $v_1(t)$ as

$$\dot{u}_2 = \alpha[v_1 - u_2 - f(u_2)]. \tag{17}$$

The signal $s(t)$ is then recovered using

$$s_2(t) = r(t) - u_2(t) \approx s(t). \tag{18}$$

Actually the dynamics of the experimental set-up (Fig. 16) is described by

$$\begin{cases} \dot{u}_2 = \alpha(v_1 - u_2 - f(u_2)) \\ \dot{w}_2 = -\beta v_1. \end{cases} \tag{19}$$

Remark 2. As long as we do not need $w_2(t)$ to recover $s_2(t)$, we continue to use (18) instead of (19) in the following improved system.

Remark 3. In both implementations (electronic circuit realization (Fig. 17) and computer simulation (Fig. 16)) of

the circuit[25], there is an inevitable error which is introduced by using the signal $s(t)$.

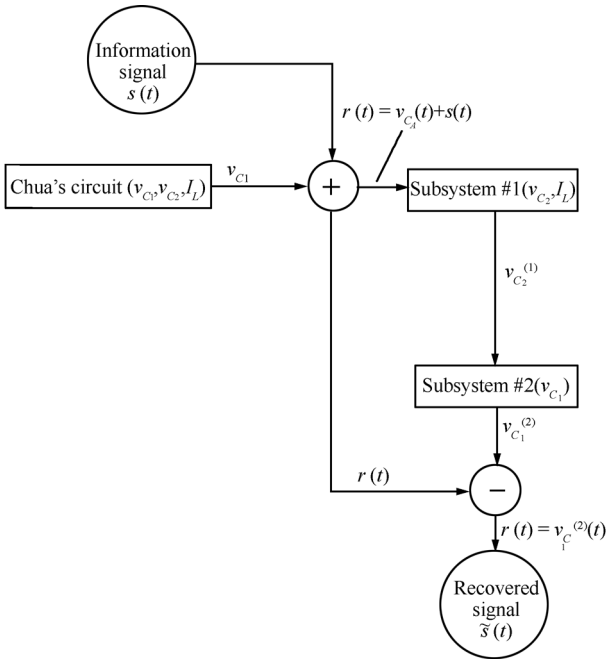


Fig. 16 Experimental set up. Block diagram of the system. It contains one Chua′s circuit and two partial Chua′s circuits, that is, subsystems #1 and #2 of Fig. 17[25]

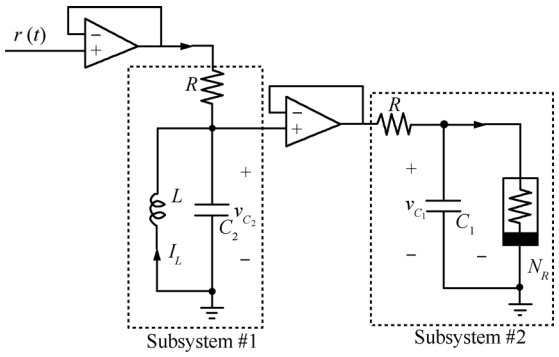


Fig. 17 Practical realization of the receiver. The first subsystem is a partial Chua′s circuit consisting of the (v_{C_2}, i_L) — subsystem driven by the transmitted signal $r(t)$. The second subsystem is a partial Chua′s circuit consisting of the v_{C_1} — subsystem driven by the transmitted signal $(v_{C_2}^{(1)})$. The triangular symbols are OpAmps which decouple the systems, acting as the signal drive elements[25]

The performance of the chaotic masking technique need to be enhanced by means of improving the convergence of the recovered signal $s_2(t)$ towards the information-bearing signal $s(t)$. Using an analog of relaxation method in numerical analysis (in numerical mathematics, relaxation methods are iterative methods for solving systems of equations, including nonlinear systems), it has been proposed to iterate the process of recovering the signal, cascading a second identical receiver to the first one, i.e., introducing a second system of equations comparable to (16, 17) driven by $u_2(t)$ instead of $r(t)$, as shown in Fig. 18.

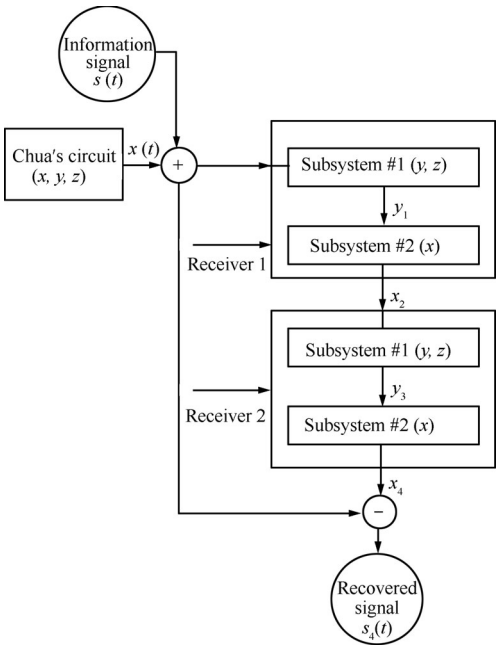


Fig. 18 Block diagram of the electronic circuit implemented in Fig. 19

Two subsystems build the second receiver. The signal $u_2(t)$ drives the first subsystem. It is assumed to be more synchronized to $u(t)$ than the transmitted signal $r(t)$:

$$\begin{cases} \dot{v}_3 = u_2 - v_3 + w_3 \\ \dot{w}_3 = -\beta v_3. \end{cases} \tag{20}$$

The second subsystem of the second receiver is then driven by the signal $v_3(t)$ from (20):

$$\dot{u}_4 = \alpha[v_3 - u_4 - f(u_4)]. \tag{21}$$

Then $s(t)$ is recovered as

$$s_4(t) = r(t) - u_4(t) \approx s(t). \tag{22}$$

In practice, we simply build two copies of the receiver as shown in Fig. 19. By identifying the symbols (v_{C_1}, v_{C_2}, i_L) in Chua′s circuit (see Figs. 16 and 17) with (u, v, w), the electronic circuit implementation in Fig. 19 can be translated into the block diagram shown in Fig. 18. Although no two electronic circuits can be made perfectly identical in practice. One can approach this ideal situation with the help of the integrated circuit technology[26]. By fabricating several identical Chua′s circuits on the same silicon chip, the resulting circuits are almost "clones" of each other. The additional security supported by this technique has the advantage that even if someone else has discovered the parameters (α, β) used in the system, integrating it into another silicon chip will invariably introduce discrepancies due to the different processing parameters from different silicon "foundries". Computer experiments show that by connecting two identical receivers, a significant amount of noise can be reduced. The recovered signal[27] has thereby a much higher quality.

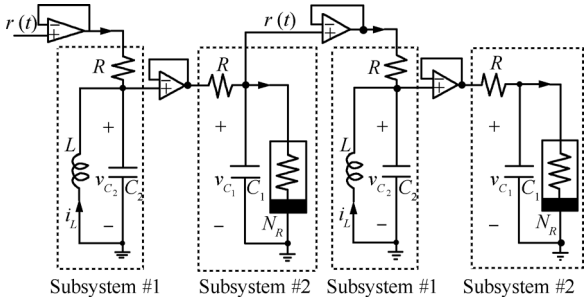


Fig. 19 Electronic circuit implementation of the two-stage "receiver" consisting of two identical copies of the circuit given in Fig. 18

At that point of this article, the last symbol we introduce in order to schematise mathematically that cascading method is the cascader displayed in Fig. 20.

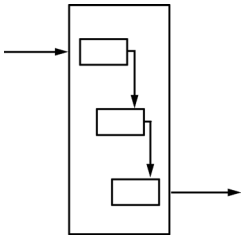


Fig. 20 Cascader symbol

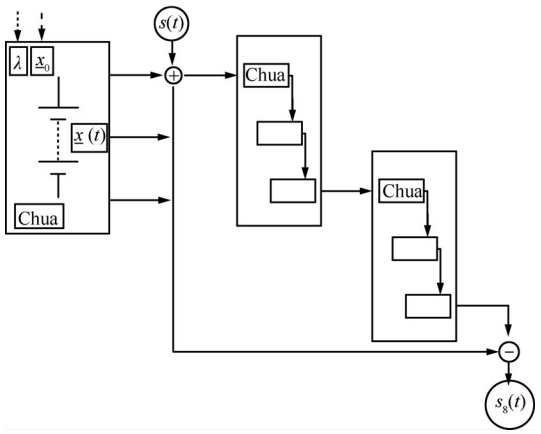


Fig. 21 Two cascading receivers combined

In the limited extent of this paper, the last example of mathematical circuits we give is an improvement of the cascading of two identical receivers of Chua′s circuit. Albeit this improvement is rather from a numerical point of view than a practical one, it is given in order to illustrate more in depth the combination of circuit elements. It is possible to combine two cascading receivers as in Fig. 21.

This circuit is governed by

$$\begin{cases} \dot{v}_5 = u_4 - v_5 + w_5 \\ \dot{w}_5 = -\beta v_5 \end{cases} \tag{23}$$

$$\dot{u}_6 = \alpha[v_5 - u_6 - f(u_6)] \tag{24}$$

$$\begin{cases} \dot{v}_7 = u_6 - v_7 + w_7 \\ \dot{w}_7 = -\beta v_7 \end{cases} \tag{25}$$

$$\dot{u}_8 = \alpha[v_7 - u_8 - f(u_8)]. \tag{26}$$

Then $s(t)$ is recovered as

$$s_8(t) = r(t) - u_8(t) \approx s(t). \tag{27}$$

A clear improvement of the results[27, 28] is shown by numerical experiments.

4 Conclusions

Following the worldwide tradition of using Chua′s circuits for various purposes, we have introduced the paradigm of chaotic mathematical circuitry which shows some similarity to the paradigm of electronic circuitry — the design of electronic circuits. This new paradigm allows, for instance, building new chaotic and random number generators. However, there are some differences in the analogy: Mathematical circuits are generic rather than specific like electric circuits. In fact, they capture the essential of dynamics of chaotic attractors.

We have presented the symbols of generators (both continuous and discrete) used in the paradigm of mathematical circuits, and compared mathematical circuits with the electric ones.

We considered others circuit elements (couplers, sampler, mixer, reducer and cascader) in practical problems: generating hyperchaos; developing chaos based pseudo random number generators (CPRNGs), chaotic multistream pseudo random number generators (Cms-PRNGs) and secure communication via synchronization.

Alongside electronic circuits, the new theory of mathematical circuits allows many new applications in chaotic cryptography[29], genetic algorithms in optimization and in control[30], etc. Due to the versatility of the new components we introduce, the combined operation of these chaotic mathematical circuits remains largely unexplored.

Acknowledgement

The author would like to thank J. P. Lozi (LIP6) for his valuable suggestions.

References

[1] M. Arounassalame. Analysis of nonlinear electrical circuits using Bernstein polynomials. *International Journal of Automation and Computing*, vol. 9, no. 1, pp. 81–86, 2012.

[2] S. Vaidyanathan, S. Sampath. Anti-synchronization of four-wing chaotic systems via sliding mode control. *International Journal of Automation and Computing*, vol. 9, no. 3, pp. 274–279, 2012.

[3] L. Sheng, H. Z. Yang. H_∞ synchronization of chaotic systems via delayed feedback control. *International Journal of Automation and Computing*, vol. 7, no. 2, pp. 230–235, 2010.

[4] L. O. Chua, M. Kumoro, T. Matsumoto. The double scroll family. *IEEE Transactions on Circuit and Systems*, vol. 33, no. 11, pp. 1072–1118, 1986.

[5] R. Lozi, L. O. Chua. Secure communications via chaotic synchronization II: Noise reduction by cascading two identical receivers. *International Journal of Bifurcation and Chaos*, vol. 3, no. 5, pp. 1319–1325, 1993.

[6] E. N. Lorenz. Deterministic nonperiodic flow. *Journal of Atmospheric Sciences*, vol. 20, no. 2, pp. 130–141, 1963.

[7] O. E. Rössler. Chaotic behavior in simple reaction system. *Zeitschrift für Naturforschung*, vol. A31, pp. 259–264, 1976.

[8] J. N. Blakely, M. B. Eskridge, N. J. Corron. A simple Lorenz circuit and its radio frequency implementation. *Chaos*, vol. 17, no. 2, Article no. 023112, 2007.

[9] N. Datta, M. K. Mandal. Realisation of electronic circuit based on modified rössler system and its application in secure communication. *Elixir Computer Science and Engineering*, vol. 49, pp. 9845–9848, 2012.

[10] J. C. Sprott. *Chaos and Time-series Analysis*, Oxford, UK: Oxford University Press, 2003.

[11] R. Lozi. Un attracteur étrange (?) du type attracteur de Hénon. *Journal de Physique*, vol. 39, no. C5, pp. 9–10, 1978.

[12] G. Gandhi. Electronic Realizations of Chaotic Circuits: From Breadboard to Nanotechnology, Ph. D. dissertation, Peter Pazmany Catholic University, Budapest, Hungary, 2008.

[13] T. Kapitaniak, L. O. Chua, G. Q. Zhong. Experimental hyperchaos in coupled Chua′s circuits. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 41 no. 7, pp. 499–503, 1994.

[14] M. V. Petersen, H. M. Sorensen. Method of Generating Pseudo-random Numbers in an Electronic Device, and a Method of Encrypting and Decrypting Electronic Data, Patent No. 7170997, USA, 2007.

[15] D. Ruggiero, D. Mascolo, I. Pedaci, P. Amato. Method of generating successions of pseudo-random bits or numbers, Patent No. 20060251250 A1, USA, 2006.

[16] R. Lozi. Complexity Leads to Randomness in Chaotic Systems. *Mathematics in Science and Technology: Mathematical Methods, Models and Algorithms in Science and Technology*, A. H. Siddiqi, R. C. Singh, P. Manchanda, Eds., Singapore: World Scientific Publisher, pp. 93–125, 2001.

[17] R. Lozi. Emergence of randomness from chaos. *International Journal of Bifurcation and Chaos*, vol. 22, no. 2, Article no. 1250021, 2012.

[18] R. Lozi. Giga-periodic orbits for weakly coupled tent and logistic discretized maps. *Modern Mathematical Models, Methods and Algorithms for Real World Systems*, A. H. Siddiqi, I. S. Duff, O. Christensen, Eds., New Delhi, India: Anamaya Publishers, pp. 80–124, 2006.

[19] R. Lozi. New enhanced chaotic number generators. *Indian Journal of Industrial and Applied Mathematics*, vol. 1, no. 1, pp. 1–23, 2008.

[20] A. Espinel, I. Taralova, R. Lozi. Dynamical and statistical analysis of a new Lozi function for random numbers generation. In *Proceedings of the 5th International Conference on Physics and Control*, León, Spain, IPACS open Access Electronic Library and Applications, pp. 5–8, 2011.

[21] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker. *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, NIST (2001), [Online], Available: http://csrc.nist.gov/rng/, August 28, 2013.

[22] A. E. Rojas, I. Taralova, R. Lozi. New alternate ring-coupled map for multi-random number generation. *Journal of Nonlinear Systems and Applications*, vol. 4, no. 1, pp. 64–69, 2013.

[23] L. O. Chua, L. Kocarev, K. Eckert, M. Itoh. Experimental chaos synchronization in Chua′s circuit. *International Journal of Bifurcation and Chaos*, vol. 2 no. 3, pp. 705–708, 1992.

[24] A. V. Oppenheim, G. W. Wornell, S. H. Isabelle, K. M. Cuomo. Signal processing in the context of chaotic signals. In *Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing*, IEEE, San Francisco, CA, USA, pp. 117–120, 1992.

[25] L. Kocarev, K. S. Halle, K. Eckert, L. O. Chua, U. Parlitz. Experimental demonstration of secure communications via chaotic synchronization. *International Journal of Bifurcation and Chaos*, vol. 2, no. 3, pp. 709–713, 1992.

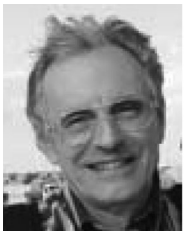
[26] M. Delgado-Restituto, A. Rodríguez-Vasquez. A CMOS monolithic Chua′s circuit. *Journal of Circuits, Systems and Computers*, vol. 3, no. 2, pp. 259–268, 1993.

[27] M. A. Aziz Alaoui, R. Lozi. Secure communications via chaotic synchronization in Chua′s circuit: Numerical analysis of the errors of the recovered signal. In *Proceedings of Nonlinear Theory and Its Application*, Kagoshima, Japan, pp. 145–148, 1994.

[28] R. Lozi. Secure communications via chaotic synchronization in Chua′s circuit and Bonhoeffer-Van der Pol equation: Numerical analysis of the errors of the recovered signal. In *Proceedings of IEEE International Symposium on Circuits and Systems*, IEEE, Seattle, WA, USA, vol. 1, pp. 684–687, 1995.

[29] R. Lozi. Engineering of Mathematical Chaotic Circuits. *Nostradamus 2013: Prediction, Modeling and Analysis of Complex Systems, Advances in Intelligent Systems and Computing*, I. Zelinka, G. Chen, O. E. Rössler, V. Snasel, A. Abraham, Eds., Switzerland: Springer, vol. 210, pp. 17–29, 2013.

[30] M. Pluhacek, R. Senkerik, D. Davendra, I. Zelinka. Designing PID controller for DC motor system by means of enhanced PSO algorithm with discrete chaotic Lozi map. *Soft Computing Models in Industrial and Environmental Applications Advances in Intelligent Systems and Computing*, vol. 188, pp. 475–483, 2013.



René Lozi received his Ph. D. degree in bifurcation theory from University of Nice (France) in 1975 and the French State Thesis from University of Nice under the supervision of Professor René Thom in 1983. As an assistant professor, Laboratoire J. A. Dieudonné, University of Nice (1974–1976), he spent 15 years as a responsible for research at CNRS (1974–1990) and became full professor in 1990 at the same university. He served as the director of Institut Universitaire de Formation des Maîtres (IUFM) during 2001–2006, and as vice-chairman of the French Board of Directors of IUFM (2004–2006). In 2011, he became a full professor of Exceptional Class (the highest rank in French university). He is the member of the Editorial Board of *Indian Journal of Industrial* and *Applied Mathematics* and *Journal of Nonlinear Systems* and *Applications*, and member of the Honorary Editorial Board of *International Journal of Bifurcation and Chaos*. He is also a member of the Interuniversity Group of Research DYCOEC, GdR 2984 of C.N.R.S. (Dynamics and control of complex sets), and the International Physics and Control Society (IPACS, St Petersburg, Russia). He was among the founders of the Indian Society of Industrial and Applied Math (ISIAM) in 1989. In 1977, he discovered a particular mapping of the plane producing a very simple strange attractor (now known as the "Lozi map"). He has worked in this field with renowned researchers, such as Professors Leon Chua (inventor of "Chua circuit"), and Alexander Sharkovsky (who introduced the "Sharkovsky′s order"). He has been a visiting professor for several periods to the University of Kyoto and University of Tokushima in Japan and University of Berkley, USA.

His research interests include complexity and emergences theories, dynamical systems, bifurcation and chaos, control of chaos and cryptography based chaos.

E-mail: rlozi@unice.fr