Mathematical chaotic circuits: an efficient tool for shaping numerous architectures of mixed chaotic/peudo random number generators

René Lozi

MATHEMATICAL CHAOTIC CIRCUITS: AN EFFICIENT TOOL FOR SHAPING NUMEROUS ARCHITECTURES OF MIXED CHAOTIC/PSEUDO RANDOM NUMBER GENERATORS

René Lozi

University of Nice-Sophia Antipolis
Laboratory J.A. Dieudonné, UMR CNRS 7351
Parc Valrose, 06108 NICE Cedex 02
France
rlozi@unice.fr

Abstract: *During the last decades, it had been highlighted the duality between chaotic numbers and pseudo-random numbers. Emergence of pseudo-randomness from chaos via various under-sampling methods has been recently discovered. Instead of opposing both qualities (chaos and pseudo-randomness) of numbers, it should be more interesting to shape mixed Chaotic/Pseudo-random number generators, which can modulate the desired properties between chaos and pseudo-randomness.*
Because nowadays there exist increasing demands for new and more efficient number generators of this type it is important to develop new tools to shape more or less automatically various families of such generators.
Mathematical chaotic circuits have been recently introduced for such a purpose among several others. There some analogy between them and electric circuits, but the components. Mathematical circuits use new ones we describe therein.
The combination of such mathematical components leads to several news applications which improve the performance of well known chaotic attractors (Hénon, Chua, Lorenz, Rössler, ...).
They can be also used in larger scale to shape numerous architectures of mixed Chaotic/Pseudo Random Number Generators.

Keywords: *Mathematical circuits, chaos, pseudo-random numbers, attractors, mathematical engineering, Chua's circuit.*

1 Introduction

During the last decades, on one hand, it had been highlighted the duality between chaotic numbers and pseudo-random numbers (e.g. sometimes chaotic numbers used in particle swam optimisation are more efficient than pseudo-random numbers, sometimes high quality pseudo-random numbers are needed for cryptography).

On the other hand, emergence of pseudo-randomness from chaos via various under-sampling methods has been recently discovered. Instead of opposing both qualities (chaos and pseudo-randomness) of numbers, it should be more interesting to shape mixed Chaotic/Pseudo-random number generators, which can modulate the desired properties between chaos and pseudo-randomness.

Because nowadays there exist increasing demands for new and more efficient number generators of this type (these demands arise from different applications, such as multi-agents competition, global optimisation via evolutionary algorithms or secure information transmission, etc.), it is important to develop new tools to shape more or less automatically various families of such generators.

Mathematical chaotic circuits have been recently introduced for such a purpose among various others. By analogy of electronic circuitry: i.e. the design of electronic circuits which are composed of individual electronic components, such as resistors, transistors, capacitors, inductors and diodes, connected by conductive wires through which electric current can flow; mathematical chaotic circuits are composed of individual components (generators, couplers, samplers, mixers, reducers and, shapers, etc.) connected through streams of data. The combination of such mathematical components leads to several news applications such as improving the performance of well known chaotic attractors (Chua, Lorenz, Rössler, Hénon, Lozi, Logistic or Symmetric Tent map, etc.).

They can be also used in larger scale to shape numerous architectures of mixed Chaotic/Pseudo Random Number Generators.

In Sect. 2 we recall briefly those famous chaotic attractors. In Sect. 3 we introduce the chaotic mathematical circuits. In Sect. 4 we show some applications of chaotic circuits.

2 Chaotic and random numbers

Chaos theory studies the behavior of dynamical systems that are highly sensitive to initial conditions. Small differences in initial conditions (such as those due to rounding errors in numerical computation) yield widely diverging outcomes for chaotic systems, rendering long-term prediction impossible in general. This property is popularly referred to as the “butterfly effect”. This happens even though these systems are deterministic (i. e. their future behavior is fully determined by their initial conditions), with no random elements involved. In other words, the deterministic nature of these systems does not make them predictable. We recall first the most studied examples of systems of differential equations (continuous dynamical systems) and mappings (discrete dynamical systems) which we will use in this article to explain the new paradigm of chaotic circuitry. We then introduce several types (chaotic, mixing and geometric) of undersampling in order to overcome the poor quality of chaotic generators. Those mechanisms allow the emergence of pseudo-randomness from chaos. A number of (chaos based) Chaotic Pseudo Random Number Generators (CPRNG) can be built using those undersampling methods.

2.1 Continuous dynamical systems: Lorenz, Rössler models and Chua’s electronic circuit

The first example of such well known chaotic continuous system in the dissipative case was pointed out by the meteorologist E. Lorenz in1963 [1] who introduced the following non linear system of differential equations as a extremely simplified model of atmospheric dynamics. It is precisely these equations which led Lorenz to the discovery of the sensitive dependence of initial conditions - an essential factor of unpredictability in many systems.

$$\begin{cases} \dot{x} = -\sigma(x+y), \\ \dot{y} = \rho x - y - xz, \\ \dot{z} = xy - \beta z, \end{cases} \tag{1}$$

Numerical simulations for an open neighbourhood of the classical parameter values

$$\sigma = 10\,,\ \rho = 28\,, \text{ and } \beta = \frac{8}{3}\ , \tag{2}$$

suggest that almost all points in phase space tend to a strange attractor the: Lorenz attractor (see Fig. 1).

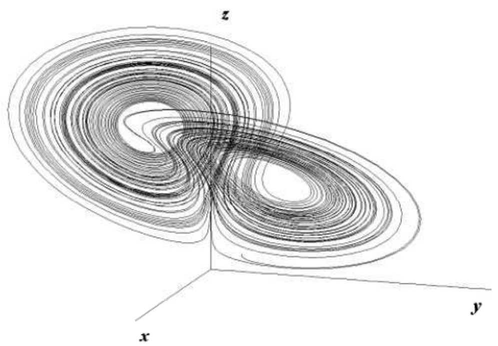


Figure 1: The Lorenz attractor

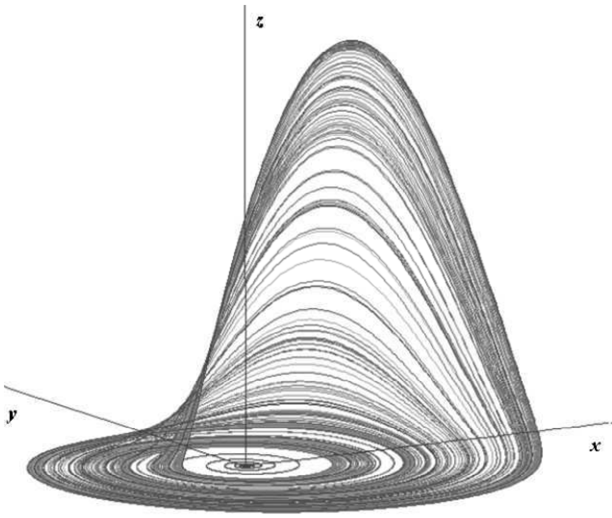


Figure 2: The Rössler attractor

In 1976, O. E. Rössler followed a different direction of research to obtain a chaotic model. Considering that, due to extreme simplification used by Lorenz in order to obtain equation (1), there is no actual link between this equation and the Rayleigh-Benard problem from which it is originate; he followed a new way in the study of a chemical multi-vibrator. He started to design some three-variable oscillator based on a two-variable bistable system coupled to a slowly moving third-variable. The resulting three-dimensional system was only producing limit cycles at the time. At an international congress on rhythmic functions held on September 8-12, 1975 in Vienna, he met A. Winfree, a theoretical biologist who challenged him to find a biochemical reaction reproducing the Lorenz attractor. Rössler failed to find a chemical or biochemical reaction producing the Lorenz attractor but, he instead found a simpler type of chaos in a paper he wrote during the 1975 Christmas holidays [2]:

$$\begin{cases} \dot{x} = -y - z, \\ \dot{y} = x + ay, \\ \dot{z} = b + z(x - c), \end{cases} \tag{3}$$

The obtained chaotic attractor for the parameter value

$$a = 0.2\ ,\ b = 0.2\ ,\ \text{and}\ c = 5.7\ , \tag{4}$$

(see Fig. 2), does not have the rotation symmetry of the Lorenz attractor defined by (5), but it is characterized by a map equivalent to the Lorenz map.

$$S(x, y, z) = (-x, -y, -z) \tag{5}$$

The Chemical reaction scheme leading to (3) is meticulously analyzed by Ch. Letellier and V. Messager [3]. The structure of the Rössler attractor is simpler than the Lorenz's one. However even if hundreds of papers has been written on it, the rigorous proof of its existence is not yet established as done for Lorenz equations [4].

Few years later, in October 1983, visiting T. Matsumoto at Waseda University, L. O. Chua found an electronic circuit [5] mimicking directly on an oscilloscope screen a chaotic signal (Fig 3).

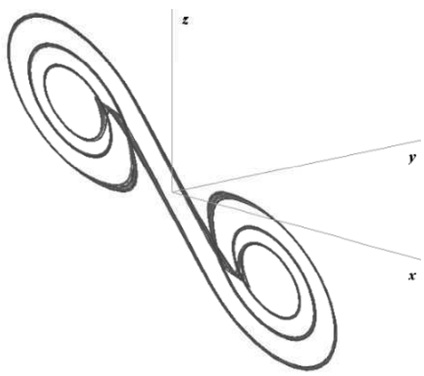


Figure 3: The Chua attractor

This circuit (Fig. 4) contains three linear energy-storage elements (an inductor and two capacitors), a linear resistor, and a single nonlinear resistor, namely Chua's diode (Fig. 5) with three segment linear characteristics defined by

$$f(v_R) = m_0 v_R + \frac{1}{2}(m_1 - m_0)\Big[|v_R + B_p| - |v_R - B_p|\Big] \tag{6}$$

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

The dynamics of Chua's circuit is governed by (7) where V_{C_1}, V_{C_2}, and I_L are respectively the voltages across the capacitors C_1 and C_2, and the intensity of the electrical current through the inductor L:

$$\begin{cases} C_1 \dfrac{dv_{C_1}}{dt} = G(v_{C_2} - v_{C_1}) - f(v_{C_1}), \\ C_2 \dfrac{dv_{C_2}}{dt} = G(v_{C_1} - v_{C_2}) + i_L, \\ L \dfrac{di_L}{dt} = -v_{C_2}. \end{cases} \tag{7}$$

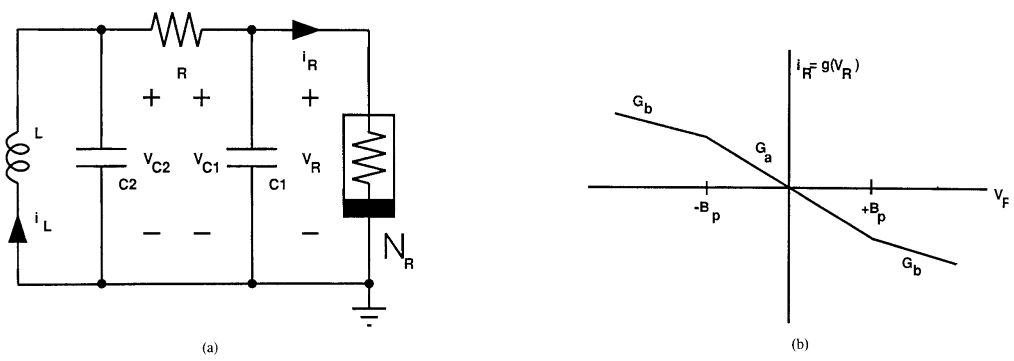


Figure 4 (left): Realization of Chua's circuit the Lorenz attractor
Figure 5 (right): Three-segment piecewise-linear *v-i* characteristic of nonlinear voltage controlled resistor (Chua's diode)

Equation (7) can be transformed into the system of three first-order autonomous differential equations whose dimension-less form is

$$\begin{cases} \dot{x} = \alpha(y - x - f(x)), \\ \dot{y} = x - y + z, \\ \dot{z} = -\beta y, \end{cases} \tag{8}$$

$$f(x) = bx + \frac{1}{2}(a - b)\left[|x+1| - |x-1|\right],$$

for which the set of parameter values

$$\alpha = 15.60\ ,\ \beta = 28.58\ ,\ a = -\frac{1}{7}\text{, and, } b = \frac{2}{7} \tag{9}$$

is very often used in order to generate chaotic signals. All those models are studied very thoroughly since their discovery 30 years ago. However, even if their equations are very simple, their dynamics is not easily understandable, hundreds of articles have published in this aim. The technique often used to simplify those models is the use of the Poincaré map [6].

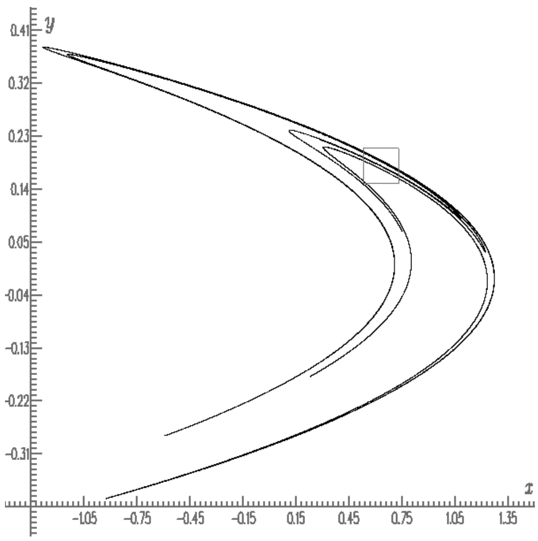
2.2 2-Dimensional discrete dynamical systems: Hénon and Lozi mapping.

In order to study numerically the properties of the Lorenz attractor, M. Hénon an astronomer of the observatory of Nice, France, introduced in 1976 a simplified model of the Poincaré map of this attractor [7]. The Lorenz attractor being imbedded in dimension 3, the corresponding Poincaré map is a mapping from the plane $\mathbb{R}^2$ into $\mathbb{R}^2$. Therefore the Hénon mapping is also defined in dimension 2 as

$$H_{a,b} : \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} y + 1 - ax^2 \\ bx \end{pmatrix} \tag{10}$$

It is associated to the dynamical system

$$\begin{cases} x_{n+1} = y_n + 1 - a x_n^2 \\ y_{n+1} = b x_n \end{cases} \tag{11}$$



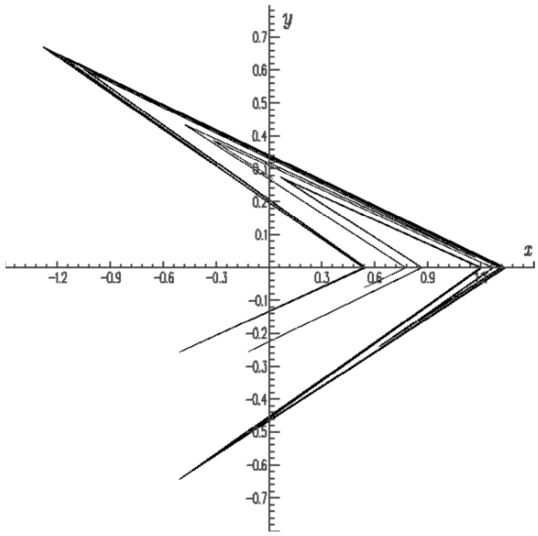


Figure 6 (left): Hénon strange attractor, 10000 successive points obtained by iteration of the mapping
Figure 7 (right): Lozi strange attractor

For the parameter value $a = 1.4$ and $b = 0.3$ (see Fig. 6) M. Hénon pointed out numerically that there exists an attractor with fractal structure. This was the first example of strange attractor (previously introduced by D. Ruelle and F. Takens [8]), for a mapping defined by an analytic formula. The like-Cantor set structure in one direction orthogonal to the invariant manifold in this simple mapping was a dramatic surprise in the community of physicists and mathematicians. In order to go further in the way of simplifying such a model, few years later, using one of the first desktop electronic calculator HP-9820, we found out, that the linearized version of the Hénon mapping (known as Lozi mapping)

$$L_{a,b} : \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} y+1-a|x| \\ bx \end{pmatrix} \quad (12)$$

displayed numerically (for a = 1.7 and b = 0.5) the same structure of strange attractor, but the curves were replaced by straight lines (Fig. 7).

2.3 1-Dimensional discrete dynamical systems: Logistic and Tent Map

In mathematics, computations done on one dimensional objects are more tractable than those done on two-dimensional features. Hence it is interesting to consider one-dimensional discrete dynamical systems. The most studied examples are the logistic and the tent (symmetric or skew) map of the interval. In 1838 the belgium mathematician Pierre François Verhulst [9] introduced a differential equation modelling the grow of population in a simple demographic model, as an improvement of the Malthusian growth model, in which some resistence to the natural increase of population is added. He later, in 1845 [10], called logistic function the solution of this equation. In 1973, the biologist Sir R. M. May introduced the nonlinear, discrete time dynamical system

$$x_{n+1} = rx_n(1-x_n) \quad (13)$$

as a model for the fluctuations in the population of fruit flies in a closed container with constant food [11]. Due to the similarity of both equations although one is a continuous dynamical system, and the other a discrete one, he called Eq. (13) logistic equation. The logistic map (Fig. 7) $f_r : [0,1] \to [0,1]$

$$f_r(x) = rx(1-x) \quad (14)$$

associated to (13) and generally considered for $r \in [0,4]$ is often cited as an archetypal example of how complex, chaotic behavior can arise from very simple non-linear dynamical equations.

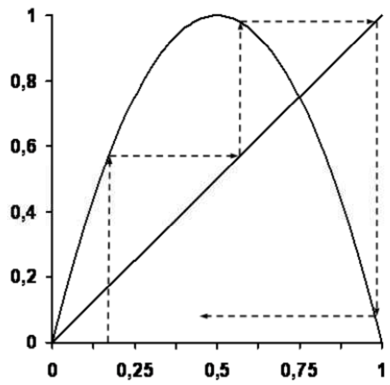


Figure 7: Cobweb of the logistic map for $r = 4$

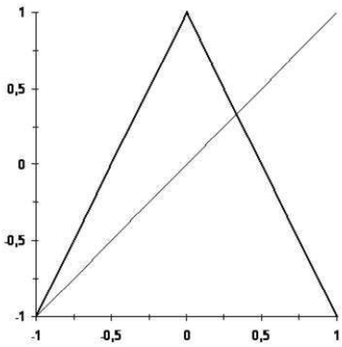


Figure 8: Graph of the symmetric tent map

Similarly to the linearization of the Hénon map into Lozi map, one can consider the linearized version of the logistic map which is called, due to its shape (see Fig. 8), the Tent map

$$f(x) = 1-2|x| \quad (15)$$

associated to the dynamical system

$$x_{n+1} = 1-2|x_n| \quad (16)$$

When the summit of this tent is not exactly in the middle of the interval of definition, the corresponding map is also called the skew tent map.

Chaotic dynamical systems in low dimension are often used since their discovery in the 70' in order to generate chaotic numbers, because they are very easy to implement in numerical algorithms [12]. However, as we point out in [6], the computation of numerical approximation of their periodic orbits leads to very different results from the theoretical ones. The collapsing of iterates of dynamical systems or at least the existence of very short periodic orbits, their non constant invariant measure, and the easily recognized shape of the function in the phase space avoid the use of one-dimensional map (logistic, baker, or tent, …) as a Pseudo Random Number Generator (PRNG). However, the very simple implementation in computer program of chaotic dynamical systems led some authors to use it as a base of cryptosystem [13, 14]. In addition it seems that for some applications, chaotic numbers are more efficient than random numbers. That is the case for evolutionary algorithms [15, 16] or chaotic optimization [17].

2.4 The route from chaos to pseudo-randomness via chaotic or mixing undersampling

In this subsection we show how to overcome the poor quality of chaotic generators using two types (chaotic, mixing) of undersampling. Before presenting both undersampling mechanisms, we have to show how to stabilize the chaotic properties of chaotic number when realized on a computer. In order to simplify the presentation below, we use as an example a system of 2-coupled symmetric tent map (15), even though other chaotic maps of the interval (as the logistic map, the baker transform, etc.) can be used for the same purpose (as a matter of course, the invariant measure of the chaotic map considered is preserved).

The system is simply described by

$$\begin{cases} x_{n+1} = (1-\varepsilon_1) f(x_n) + \varepsilon_1 f(y_n) \\ y_{n+1} = \varepsilon_2 f(x_n) + (1-\varepsilon_2) f(y_n) \end{cases} \tag{17}$$

We use generally $\varepsilon_1 = 10^{-14}$, $\varepsilon_2 = 2\varepsilon_1$ when computations are done with double precision numbers. With these numerical values, the collapsing effect disappears and the invariant measure of any component is the Lebesgue measure [18]. When computations are done with double precision number it is not possible to find any periodic orbit, up to $n = 5\times 10^{11}$ iterations.

More generally, the coupling of *p* maps takes the form

$$X_{n+1} = F(X_n) = A \cdot \left(\underline{f}(X_n) \right) \tag{18}$$

where

$$\underline{f}(X_n) = \begin{pmatrix} f(x_n^1) \\ \vdots \\ \vdots \\ f(x_n^p) \end{pmatrix}, \qquad X_n = \begin{pmatrix} x_n^1 \\ \vdots \\ \vdots \\ x_n^p \end{pmatrix}, \tag{19}$$

and

$$A = \begin{pmatrix} \varepsilon_{1,1} = 1 - \sum_{j=2}^{j=p} \varepsilon_{1,j} & \varepsilon_{1,2} & \cdots & \varepsilon_{1,p-1} & \varepsilon_{1,p} \\ \varepsilon_{2,1} & \varepsilon_{2,2} = 1 - \sum_{j=1, j\neq 2}^{j=p} \varepsilon_{2,j} & \cdots & \varepsilon_{2,p-1} & \varepsilon_{2,p} \\ \vdots & \ddots & & \vdots & \vdots \\ \vdots & & \ddots & \vdots & \vdots \\ \varepsilon_{p,1} & \cdots & \cdots & \varepsilon_{p,p-1} & \varepsilon_{p,p} = 1 - \sum_{j=1}^{j=p-1} \varepsilon_{p,j} \end{pmatrix} \tag{20}$$

with $\varepsilon_{i,i} = 1 - \sum_{j=1, j\neq i}^{j=p} \varepsilon_{i,j}$ on the diagonal (the matrix A is always a stochastic matrix iff the coupling constants verify $\varepsilon_{i,j} > 0$ for every *i* and *j*).

It is noteworthy that these families of very weakly coupled maps are more powerful than the usual formulas used to generate pseudo-random sequences, mainly because only additions and multiplications are used in the computation process, no division being required. Moreover the computations are done using floating point or double precision numbers, allowing the use of the powerful Floating Point Unit (FPU) of the modern microprocessors. In addition, a large part of the computations can be parallelized taking advantage of the multicore microprocessors which are used nowadays. Moreover, a determining property of such coupled map is the high number of parameters used ($p\times(p-1)$ for *p* coupled equations) which allows to choose them as cipher-keys, when used in chaos based cryptographic algorithms, due to the high sensitivity to the parameters values [19].

However Chaotic numbers are not pseudo-random numbers because the plot of the couples of any component $\left(x_n^j, x_{n+1}^j\right)$ of iterated points $\left(X_n, X_{n+1}\right)$ in the corresponding phase plane reveals the map *f* used as one-dimensional dynamical systems to generate them *via* (18). Nevertheless, we have recently introduced a family of enhanced Chaotic Pseudo Random Number Generators (CPRNG) in order to compute faster long series of pseudorandom numbers with desktop computer [20]. This family is based on the previous ultra weak coupling which is improved in order to conceal the chaotic genuine function.

The first process of undersampling, the chaotic one is used in order to hide f of (18), in the phase space (x_n^j, x_{n+1}^j) for any *j*, the sequence $(x_0^j, x_1^j, x_2^j, \dots x_n^j, x_{n+1}^j, \dots)$ generated by the *j*-th component x^j, is sampled chaotically, selecting x_n^j every time the value x_n^m of the m-th component x^m, is strictly greater than a threshold *T* belonging to the interval $[-1,1]$ of the real line.

The pseudo-code, for computing such chaotically sub-sampled iterates is:

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

This chaotic under-sampling is possible due to the independence of each component of the iterated points X_n *vs*. the others [21].

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 $0 < T_1 < T_2 < \cdots T_{p-1} < 1$ forming a partition $J_1, J_2, \dots, J_{p-1}$ of the interval $[-1,1]$, the pseudo-code, for computing such chaotically sub-sampled iterates is

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

This second mechanism is called the mixing undersampling.

2.5 Geometric undersampling

Geometric undersampling is based on the coupling in another way of *p* tent maps on the p-dimensional torus $J^p = [-1,1]^p \subset \mathbb{R}^p$, which can directly generate random numbers, without sampling or mixing, provided *p* is large enough, although it is possible to combine those processes with it. After presenting this ring coupling in high dimension, we introduce the geometric undersampling fitted to obtain randomness with small values of *p* (e.g. $p = 2$).

We first define the mapping $M_p : J^p \to J^p$

$$M_p \begin{pmatrix} x_n^1 \\ x_n^2 \\ \vdots \\ \vdots \\ x_n^p \end{pmatrix} = \begin{pmatrix} x_{n+1}^1 \\ x_{n+1}^2 \\ \vdots \\ \vdots \\ x_{n+1}^p \end{pmatrix} = \begin{pmatrix} 1-2\left|x_n^1\right| + k_1 \times x_n^2 \\ 1-2\left|x_n^2\right| + k_2 \times x_n^3 \\ \vdots \\ \vdots \\ 1-2\left|x_n^p\right| + k_p \times x_n^1 \end{pmatrix} \tag{21}$$

with the parameters $k_i = \pm 1$. In order to confine every variable x_n^j on $J^p = [-1,1]^p \subset \mathbb{R}^p$ we do, for every iteration, the transform

$$
\begin{cases} if\,(x_{n+1}^{j} < -1) & add \quad 2 \\ if\,(x_{n+1}^{j} > -1) & substract \quad 2 \end{cases} \tag{22}
$$

The particularity of this coupling is that each variable x_n^j is coupled only with itself and x_n^{j+1}, as displayed on Fig. 9.

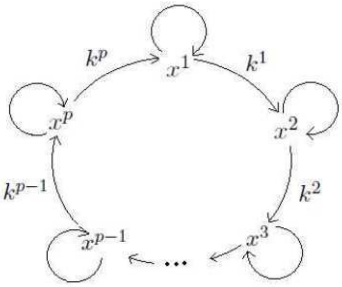
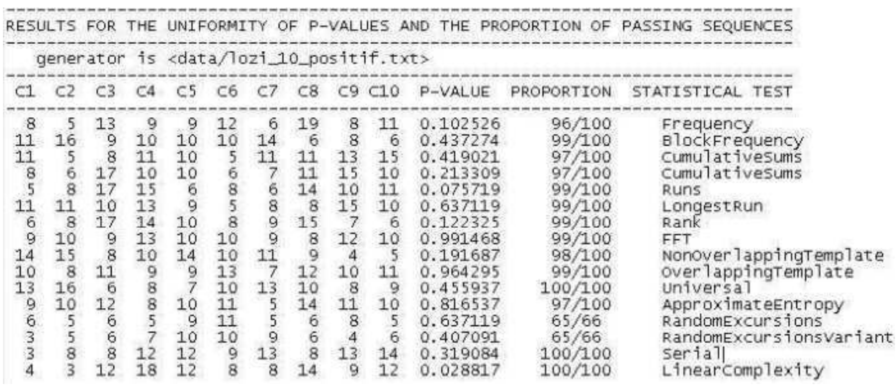


Figure 9: Ring coupling between the variables x_n^j

To evaluate the random properties of these generators, the set of NIST tests have been used (Fig. 10). The random properties validations of both a 4-dimensional system and a 10-dimensional one have been carried out [22].



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

Figure 10: Example of NIST Test for $k_i = (-1)^{i+1}$, $i = 1,4$, each sequence of components satisfies the NIST test for randomness

Although system (21) is a good PRNG when $p \geq 4$, in lower dimension 2 and 3, the chaotic numbers are not equidistributed on the torus (see Fig. 11).

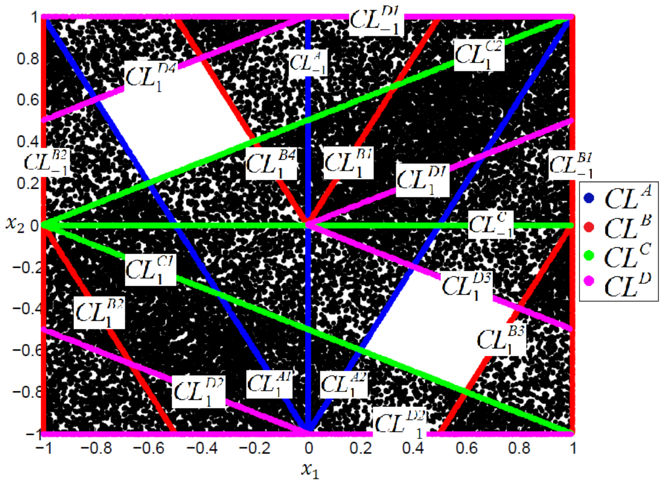


Figure 11: Invariant densities of iterates in 32 sub-regions bounded by critical lines of M_2 on the torus J^2 [22]

In order to improve the ring coupling mechanism in low dimension, a geometric undersampling based on geometric nature of the invariant measure is used. We present briefly this new mechanism which allows the emergence of randomness from chaos, in the simplest case, the 2-dimensional ring mapping M_2 on the torus J^2 (i.e. a square) into itself, with $k_1 = k_2 = 1$. For this mapping

$$\begin{cases} x_{n+1}^1 = 1 - 2\left|x_n^1\right| + x_n^2 \\ x_{n+1}^2 = 1 - 2\left|x_n^2\right| + x_n^1 \end{cases} \tag{23}$$

with

$$\begin{cases} if\,(x_{n+1}^j < -1) \quad add \quad 2 \\ if\,(x_{n+1}^j > -1) \quad substract \quad 2 \end{cases} \tag{24}$$

it is possible to define several critical lines which split the square in a partition of 32 sub-regions, in which the density is uniform [22]. Each density can be computed explicitly using a cell-to-cell analysis by the means of a Markov process.

The geometric undersampling process consists in magnifying a square G included in one region (as for example the square G = [0.36,0.64] × [0.36,0.64]) included in region *m* on Fig. 12, up to the size of the square J^2.

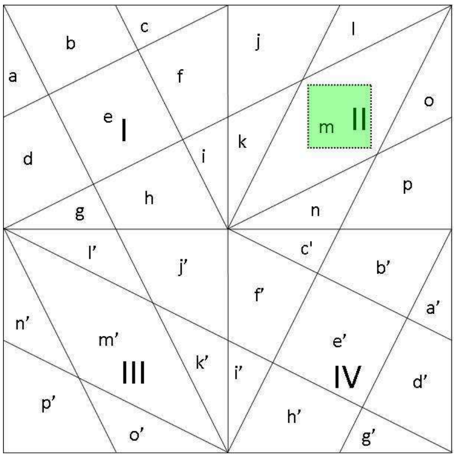


Figure 12: The square G = [0.36,0.64]´[0.36,0.64] in which the iterates of (23) are geometrically undersampled

We have also used NIST test to confirm the random property of the geometrical undersampling process. They are all successful (Fig. 13).

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

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE	PROPORTION	STATISTICAL TEST
12	9	7	9	12	11	8	11	13	8	0.924076	99/100	Frequency
1	4	3	4	7	5	9	16	16	35	0.000000 *	100/100	BlockFrequency
9	9	10	12	11	8	9	10	10	12	0.996335	99/100	CumulativeSums
10	9	12	12	9	7	10	10	9	12	0.983453	99/100	CumulativeSums
11	12	11	8	12	7	12	6	10	11	0.883171	99/100	Runs
9	9	13	8	9	8	17	8	10	9	0.595549	100/100	LongestRun
6	11	11	11	9	8	8	14	9	13	0.798139	100/100	Rank
15	10	7	8	8	8	15	16	7	6	0.153763	97/100	FFT
12	9	10	13	9	11	7	15	4	10	0.474986	98/100	NonOverlappingTemplate
12	6	10	6	13	6	8	8	17	14	0.145326	99/100	OverlappingTemplate
18	12	13	11	9	10	5	8	9	5	0.145326	99/100	Universal
11	8	12	11	11	14	8	10	7	8	0.883171	99/100	ApproximateEntropy
3	5	6	9	4	3	7	5	6	11	0.145326	59/59	RandomExcursions
7	6	6	2	6	7	6	7	4	8	0.637119	59/59	RandomExcursions
2	6	4	5	5	6	10	6	7	8	0.334538	59/59	RandomExcursionsVariant
8	15	13	12	9	12	13	5	9	4	0.224821	98/100	Serial
9	9	6	13	13	7	12	9	10	12	0.798139	99/100	LinearComplexity

The minimum pass rate for each statistical test with the exception of the random excursion (variant) test is approximately = 96 for a sample size = 100 binary sequences.

Figure 13: Geometrical undersampling: each sequence of components

satisfies the NIST test for randomness

In the case of 2 coupled maps the geometric undersampling allows the building of a PRNG which passes all NIST Test. It is very effective for generating 2 parallel streams of pseudo-random numbers, as shown in [23], in which sequences up to 10^{12} consecutives iterates of (23) have been computed, providing more than 3.5×10^{10} random numbers in a very short time.

3 Mathematical chaotic circuits

In this Section we introduce the new paradigm of mathematical (chaotic) circuits, which should constitute a new branch of mathematical engineering, in the sense of building models using equations like electronics engineering do using transistors, diodes, etc.

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 [24]. We introduce in the same way mathematical circuits which are composed of individual components (generators, couplers, samplers, mixers, reducers, cascaders and shapers, 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, Hénon, logistic) presented in Sect. 2 for application purposes.

Analog electric circuits are very commonly represented by schematic diagrams, in which wires are shown as lines, and each component has a unique symbol (See Fig.14).

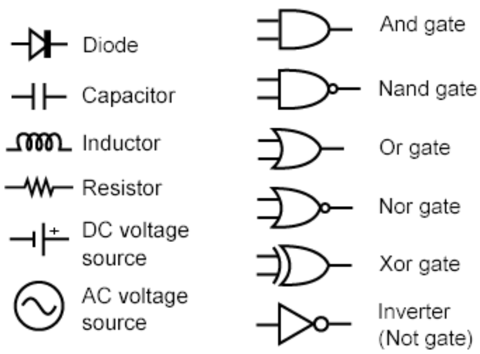


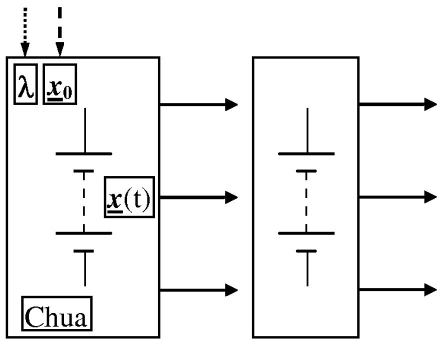
Figure 14: Electrical symbols (left-hand side column) and electronic circuit symbols (right-hand side column) used for drawing schematic diagram

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 Hénon, Lozi, Logistic or the symmetric Tent mapping. We consider first the continuous ones.

3.1 Continuous generators: Chua’s circuit, Rössler and Lorenz attractors

From a mathematical point of view, at least in order to implement applications of chaotic behaviors, all the chaotic attractors (1), (3), (8) 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. For example, concerning the Chua’s circuit, even if the scheme of Fig. 4 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 [25]). This is why it is more useful to represent Chua’s circuit as a chaos generator by the diagram of Fig. 15(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 $\underline{x}_0 = \underline{x}(0)$, the given initial value of the signal.

If there is no ambiguity on the nature of the generator used, the symbol can be simplified as in Fig. 15(b).



(a) **(b)**

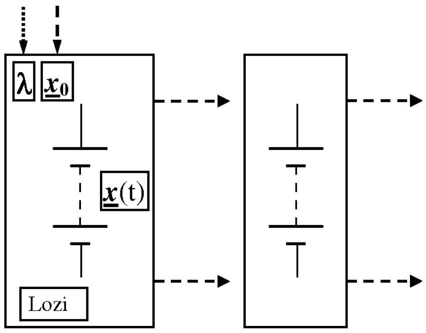
Figure 15: (a) Electrical Chua's circuit: continuous generator
(b) Simplified symbol of a continuous generator

The diagram defined above is suitable, even if we use others types of equations like the Lorenz (1) or the Rössler (3) attractor, 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 (see Fig. 18)).

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

3.2 Discrete generators: Hénon, Lozi, Logistic and Tent map

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 the classical chaotic mappings presented in Sect. 2.2 and 2.3 can be considered: the Lozi map (12) is represented by the symbols of Fig. 16, the Hénon map (10) also (provided the name inside the symbol is changed). In dimension 1 the symbol of Fig. 17 stands for both the symmetric tent map (15) and the logistic map (14).



(a) **(b)**

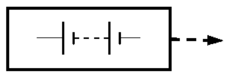


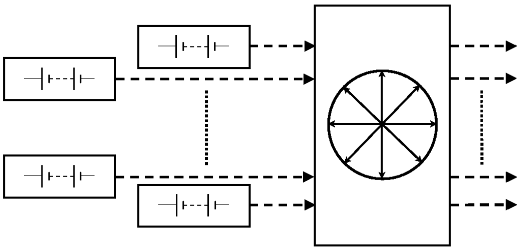
Figure 16 (left): (a) Discrete generator (Lozi map, expanded symbol)
(b) Simplified symbol of 2-dimensional discrete generator
Figure 17 (right) One-dimensional discrete generator (e.g. symmetric tent map)

Remark: 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.

3.3 Elementary circuit elements: coupler, mixer, sampler and reducer

We present in this section some other symbols we design in order to draw mathematical schematic diagrams. Rather than to give a tedious list of elementary mathematical components used for mathematical circuit design, we introduce them each time they are first used for a practical purpose. That list includes: coupler, sampler, mixer and reducer. They are connected through streams of data represented by continuous or dashed line and arrows.

There are two types of couplers: ring coupler or full coupler. The coupling of p maps given by Eq. (18) can be symbolized by the following circuit (Fig. 18) in which there are p generators on the left hand side and one full coupler on the right hand side.



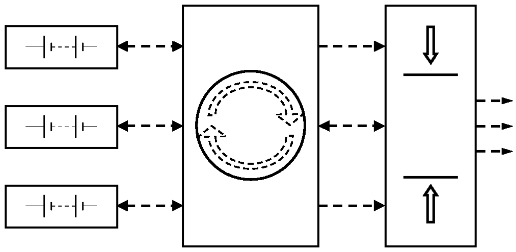
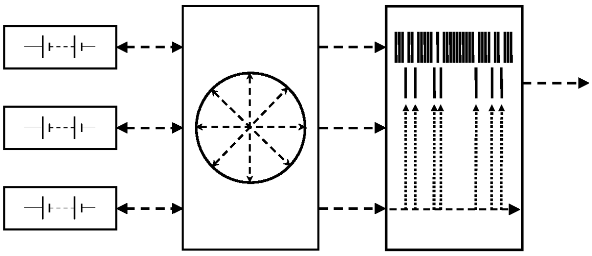


Figure 18 (left): Circuit of coupling of *p* 1-dimensional chaotic map (18) displaying a full coupler
Figure 19 (right): Reducer for the circuit (21) and the transform (22) with $p = 3$

The circuit of Fig. 19 displays a ring coupler in the middle of the circuit corresponding to the coupling defined by the mapping $M_p : J^p \to J^p$ (21), meanwhile the symbol on the right hand side is a reducer which corresponds to the reduction of the signal to the tore J^p by means of Eq. (22). Note the similarity between the ring coupler of Fig. 19 with Fig. 9.

Mixer and sampler are used to symbolize the undersampling processes. The circuit of Fig. 20 symbolizes the chaotic undersampling defined in Sec. 2.4, with a sampler on the right hand side, while on Fig. 21 the mixing undersampling is displayed with a mixer at the same position. Both circuits on those figures are designed with 3 generators constituted with 1-dimensional symmetric Tent map.



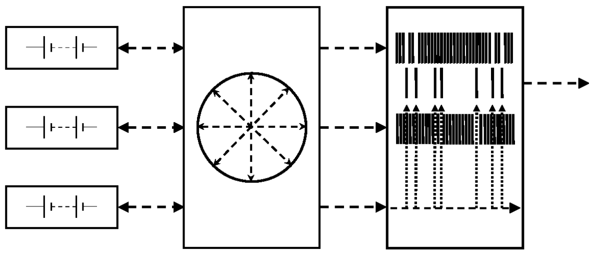
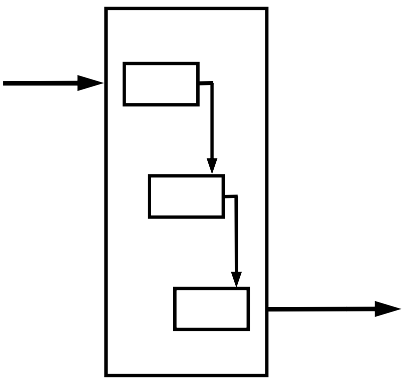


Figure 20 (left): Circuit of chaotic undersampling using a sampler
Figure 21 (right): Circuit of mixing undersampling using a mixer

3.4 Other circuit elements

As done for the schematization of electric circuits, several other mathematical circuit elements can be drawn for special purpose: **cascader** (see Fig. 22) for secure communication using two or four synchronized Chua's circuits in cascade (see Fig. 23) [25]; **geometric sampler** (Fig. 24), in order to represent the geometric undersampling of Sect. 2.5; **shaper** in order to modify the invariant measure of a chaotic generator (Fig. 25), etc.



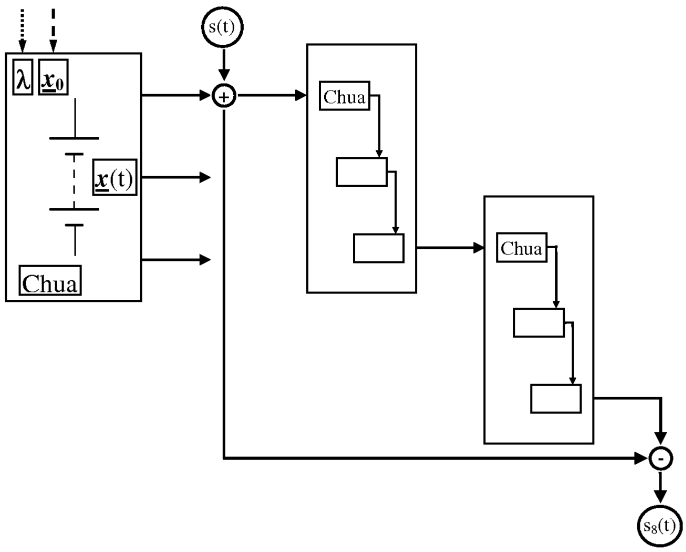


Figure 22 (left): Cascader symbol
Figure 23 (right): Two cascading receiver based on several Chua's circuits combined [25]

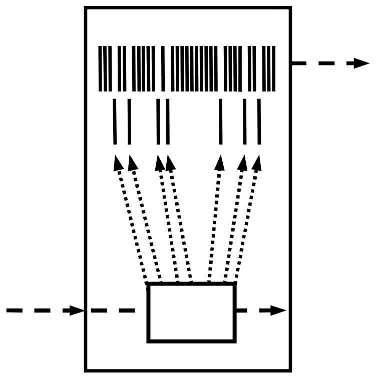
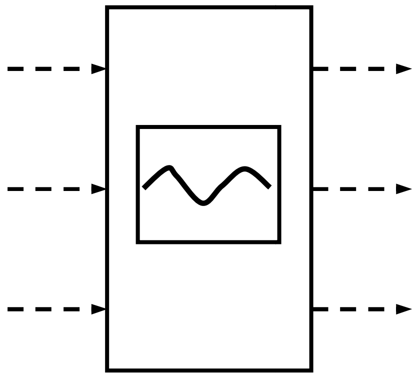



Figure 24 (left): Geometric sampler symbol
Figure 25 (right): Shaper symbol

4 Building families of mixed chaotic/random numbers generators

In the limited extend of this paper; it is difficult give examples of fully developed mathematical circuits. We first consider the circuit of Cms-PRNG recently defined . The Cms-PRNG have been used for a novel ciphering method recently introduced in order to resist to noise which is always present during the transmission of the signal in any channel [26]. The main idea is to establish, between the transmitter and the receiver, a correspondence between the alphabet constituting the plain text and some intervals defining a partition of $[-1,1]$. Some realistic assumption about the noise boundedness allows restricting the bounds of the aforementioned intervals in order to precisely resist to the effects of the noise. Another combination of logistic and symmetric Tent map is also considered [27]. Nowadays, it seems more interesting to shape mixed Chaotic/Pseudo-random number generators, which can modulate the desired properties between chaos and pseudo-randomness for optimization using evolutionary algorithms [28, 29].

4.1 Chaotic multistream pseudorandom number generators (Cms-PRNG)

It is possible to combine several equations in order to design chaotic multistream pseudo random number generators (Cms-PRNG) which generates 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. 26, corresponding to Eq. (25) (with the reduction process of Eq. (24)) when $p = 3$. Finally we consider

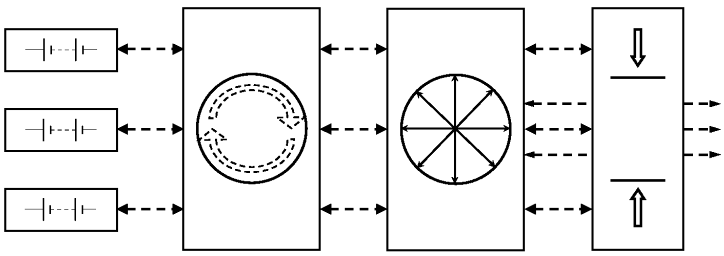


Figure 26: Circuit of Cms-PRNG with only 3 streams

$$\begin{cases} x_{n+1}^{1} = 1 - 2\left|x_n^1\right| + k_1\left(\left(1 - \sum_{j=3}^{p} \varepsilon_{1,j}\right)x_n^2 + \sum_{j=3}^{p} \varepsilon_{1,j} x_n^j\right) \\ \vdots \\ x_{n+1}^{m} = 1 - 2\left|x_n^m\right| + k_m\left(\left(1 - \sum_{j=1, j\neq m; m+1}^{p} \varepsilon_{m,j}\right)x_n^{m+1} + \sum_{j=1, j\neq m; m+1}^{p} \varepsilon_{m,j} x_n^j\right) \\ \vdots \\ x_{n+1}^{p-1} = 1 - 2\left|x_n^{p-1}\right| + k_{p-1}\left(\left(1 - \sum_{j=1}^{p-2} \varepsilon_{p-1,j}\right)x_n^p + \sum_{j=1}^{p-2} \varepsilon_{p-1,j} x_n^j\right) \\ x_{n+1}^{p} = 1 - 2\left|x_n^p\right| + k_p\left(\left(1 - \sum_{j=2}^{p-1} \varepsilon_{p,j}\right)x_n^1 + \sum_{j=2}^{p-1} \varepsilon_{p,j} x_n^j\right) \end{cases} \tag{25}$$

Another combination recently studied [27] is obtained using in the same time both logistic (14) and symmetric Tent map (15) with the reduction process (24):

$$\begin{cases} x_{n+1}^{1} = 1 - k_1^1\left(2\left|x_n^1\right| - k_1^2 (x_n^2)^2\right) \\ x_{n+1}^{2} = 1 - k_1^2\left(2\left|x_n^2\right| - k_2^2 (x_n^3)^2\right) \\ \vdots \\ x_{n+1}^{p} = 1 - k_1^p\left(2\left|x_n^p\right| - k_2^p (x_n^1)^2\right) \end{cases} \tag{26}$$

The corresponding circuit is displayed on Fig. 27, each horizontal generator being, for example, the logistic map, and the vertical generator, the Tent map.

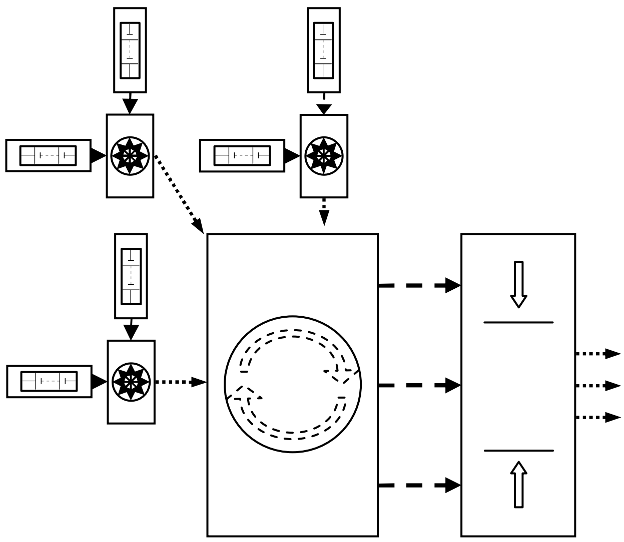
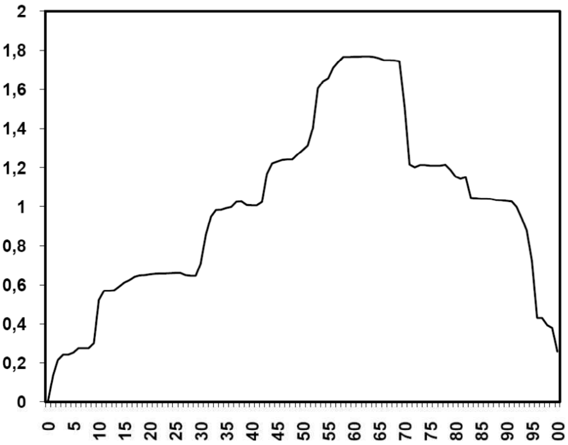


Figure 27: Circuit of Cms-PRNG with only 3 streams

4.2 Mixed Chaotic/Pseudo-random number generators

Taking advantage of properties as ergodicity and stochasticity of chaos, some new algorithms called chaos optimization algorithms (COA) are developed [28, 29]. Those algorithms depend strongly on the shape of the invariant measure of the chaotic mapping they use (see Fig. 28 for the shape of the numerical computed invariant measure of the Lozi map

(12) and Fig. 29 for the invariant measure of the logistic map). In fact there is a need of to choose the good shape of invariant measure for each specific optimization problem.



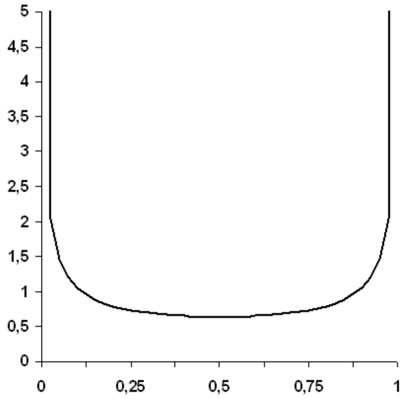


Figure 28 (left): density of iterated values of y(k) of Lozi map (10) fitted to the interval [0; 1] which is split in 100 boxes for 10,000,000,000 iterated values
Figure 29 (right): density of iterated values of logistic map (14)

Hence, instead of looking for family of chaotic generators having the requested shape, it is more simple to use a standard CMS-PRNG which provides pseudo-random numbers with Lebesgue invariant measure, and to transform this equal repartition on the interval adding a new transform to these iterated points. As an exemple of such method, one can consider the transform S defined by Eq. (27) applied after Eq. (26). Such “shaper” transform can be symbolized by adding a shaper circuit element after any circuit of CPRNG (Fig. 28).

$$\begin{pmatrix} y_{n+1}^1 \\ y_{n+1}^2 \\ \vdots \\ y_{n+1}^p \end{pmatrix} = \mathrm{S}\begin{pmatrix} x_{n+1}^1 \\ x_{n+1}^2 \\ \vdots \\ x_{n+1}^p \end{pmatrix} = \begin{pmatrix} s(x_{n+1}^1) \\ s(x_{n+1}^2) \\ \vdots \\ s(x_{n+1}^p) \end{pmatrix} \qquad \textit{with} \qquad s(x) = \begin{cases} 0.5x - 0.5 & \textit{if} \quad -1 \le x < -0.4 \\ 1.75x & \textit{if} \quad -0.4 \le x < 0.4 \\ 0.5x + 0.5 & \textit{if} \quad 0.4 \le x \le 1 \end{cases} \tag{27}$$

5 Conclusion

We have introduced the paradigm of chaotic mathematical circuitry which shows some similarity to the paradigm of electric circuitry –the design of electronic circuits. This new paradigm allows, as an example, the building of new chaotic and random number generators. Mathematical circuitry should constitute a new branch of mathematical engineering, in the sense of building models using equations like electronics engineering do using transistors, diodes, etc.

Alongside to electronic circuits, the new theory of mathematical circuits allows many new applications in chaotic cryptography, 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.

Emergence of pseudo-randomness from chaos via various under-sampling methods has been recently discovered. Instead of opposing both qualities (chaos and pseudo-randomness) of numbers, it should be more interesting to shape mixed Chaotic/Pseudo-random number generators, which can modulate the desired properties between chaos and pseudo-randomness. Chaotic circuitry is the perfect mathematical frame in which such improvement can be easily designed.

References

[1] Lorenz, E. N.: Deterministic nonperiodic flow. Journal of Atmospheric Science, 20, 130-141 (1963).
[2] Rössler, O. E.: Chaotic behavior in simple reaction system. Zeitschrift fur Naturforschung A, 31, 259-264 (1976).
[3] Letellier, Ch. & Messager, V.: Influences on Otto Rössler’s earliest paper on chaos. International Journal of Bifurcation & Chaos, 20 (11), 1-32 (2010).
[4] Tucker, W.: *The Lorenz attractor exists*, PhD thesis, Uppsala University, Sweden, (1999).
[5] Chua, L. O., Kumoro, M. & Matsumoto, T.: The Double Scroll Family. IEEE Trans. Circuit and Systems, 32 (11), 1055-1058, (1984).

[6] Lozi, R.: Can we trust in numerical computations of chaotic solutions of dynamical systems?, *Topology and Dynamics of Chaos*, Eds. Ch. Letellier, R. Gilmore, World Scientific Series on Nonlinear Sciences , Series A, 84, 63-98 (2013).
[7] Hénon, M.: A Two-dimensional mapping with a strange attractor. Commun. Math. Phys., 50, 69-77 (1976).
[8] Ruelle, D. & Takens, F.: On the nature of turbulence. Comm. Math. Phys., 20, 167-192 (1971).
[9] Verhulst, P.-F.: Notice sur la loi que la population poursuit dans son accroissement. Correspondance mathématique et physique de l'observatoire de Bruxelles, 4 (10), 113-121 (1838).
[10] Verhulst, P.-F.: Recherches mathématiques sur la loi d'accroissement de la population. Nouveaux Mémoires de l'Académie Royale des Sciences et Belles-Lettres de Bruxelles, 18, 1-42 (1845).
[11] May, R. M.: *Stability and Complexity of Models Ecosystems*, Princeton University Press, Princeton, NJ (1973).
[12] Sprott, J. C.: *Chaos and Time-Series Analysis*, Oxford University Press, Oxford, UK (2003).
[13] Baptista, M. S.: Cryptography with chaos. Phys. Lett. A, 240, 50-54 (1998).
[14] Ariffin, M. R. K., Noorani, M. S. M.: Modified Baptista type chaotic cryptosystem via matrix secret key. Phys. Lett. A, 372, 5427-5430 (2008).
[15] Pluhacek, M., Budikova, V., Senkerik, R., Oplatkova, Z., and Zelinka, I.: Extended Initial Study on the Performance of Enhanced PSO Algorithm with Lozi Chaotic Map, *Advances in Intelligent Systems and Computing*, 192, Nostradamus: Modern Methods of Prediction, Modelling and Analysis of Nonlinear Systems, 167-177 (2012).
[16] Tang, T. W., Allison, A., and Abbott, D.: Parrondo's games with chaotic switching, *Proc. SPIE Noise in Complex Systems and Stochastic Dynamics II*, 5471, 520-530, Maspalomas, Gran Canaria, Spain, 26-28 May 2004.
[17] Araujo, E., Coelho, L. dos S.: Particle swarm approaches using Lozi map chaotic sequences to fuzzy modelling of an experimental thermal-vacuum system. Applied Soft Computing, 8, 1354–1364 (2008).
[18] Lozi, R.: 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 and O. Christensen (Eds.), Anamaya Publishers, New Delhi, India, 80-124 (2006).
[19] Lozi, R.: Emergence of randomness from chaos. International Journal of Bifurcation and Chaos, 22 (2), 1250021-1/1250021-15 (2012).
[20] Lozi, R.: 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.), World Scientific Publisher, Singapore, 93-125 (2011).
[21] Lozi, R.: New Enhanced Chaotic Number Generators. Indian Journal of Industrial and Applied Mathematics, 1, (1), 1-23 (2008).
[22] Taralova, I., Espinel, A. and Lozi, R.: Dynamical and statistical analysis of a new Lozi function for random numbers generation", *Proceeding of Physcon 2011*, León, Spain, 5-8 september, IPACS open Access Electronic Library (2011).
[23] Lozi, R., & Taralova, I.: From chaos to randomness via geometric undersampling. ESAIM: Proceedings and surveys, 1-10, to appear (2014).
[24] Vaidyanathan, S. & Sampath, S.: Anti-synchronization of four-wing chaotic systems via sliding mode control. Intern. J. of Automation and Computing, 9, (3), 274-279 (2012).
[25] Lozi, R. & Chua, L. O.: Secure communications via chaotic synchronization II: noise reduction by cascading two identical receivers. Int. J. Bifurcation & Chaos, 3 (5), 1319-1325 (1993).
[26] Cherrier, E. & Lozi, R.: Noise-resisting ciphering based on a chaotic multi-stream pseudo-random number generator. In: Proc. IEEE Conference Internet Technology and Secured Transactions (ICITST), 11-14 Dec. Abu Dhabi, 91-96 (2011).
[27] Garasym, O., Taralova, I., and Lozi, R.: Design of Gigaperiodic Robust Chaotic Pseudo Random Number Generator and applicable to cryptography. Preprint (2014).
[28] Hamaizia, T., Lozi, R. & Hamri, N.-E.: Fast chaotic optimization algorithm based on locally averaged strategy and multifold chaotic attractor. Applied Mathematics and Computation, 219, 188–196 (2012).
[29] Hamaizia, T. & Lozi, R.: An improved chaotic optimization algorithm using a new global locally averaged strategy. Journal of Nonlinear Systems and Applications, 58-63 (2012).
[30] Pluhacek, M., Senkerik, R., Davendra, D., Zelinka, I.: 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, 188, 475-483 (2013).