Chaotic mathematical circuitry

René Lozi

To cite this version:

René Lozi. Chaotic mathematical circuitry. Andrew Adamatzky, Guanrong Chen. Chaos CNN, Memristors and Beyond, A festschrift for Leon Chua, World scientific, pp.307-323, 2013, 978-981-4434-79-9. hal-00682309v2

Chapter 24

Chaotic mathematical circuitry

R. LOZI
Laboratoire J.A. Dieudonné - UMR CNRS 7351
Université de Nice Sophia-Antipolis
Parc Valrose
06108 NICE Cedex 02
FRANCE
lozi@unice.fr

Following the worldwide tradition of use of Chua's circuits for various purposes, we introduce the paradigm of chaotic mathematical circuitry which shows some similarity to the paradigm of electronic circuitry -the design of electronic circuit- especially in the frame of chaotic attractors. An electronic circuit is composed of individual electronic components, such as capacitors, diodes, inductors, resistors, transistors and connected by conductive wires. Recently, in 2009, three more components discovered by L. O. Chua have been added to the set of devices, namely: memristors, memcapacitors and meminductors. In the same way a mathematical circuit is composed of individual components we design: generators, couplers, samplers, mixers, reducers and cascaders, connected by streams of data. The combination of such mathematical components allows many new applications in chaotic cryptography, genetic algorithms in optimization or in control.

Published in: "Chaos CNN, Memristors and Beyond, A festschrift for Leon Chua" (commemorating the 75th birthday of Prof Leon O. Chua), *Eds. A. Adamtzky, & Guanrong (Ron) Chen., World Scientific, 2013, Chapter 24, pp. 307-323.*

1. Introduction

Since the seminal work of E. N. Lorenz[16] in 1963, who discovered by accident the first chaotic strange attractor, chaotic dynamical systems have been fully studied. Fifty years after, only few chaotic attractors involving differential equations remain actively explored. Among them Chua's attractor is nowadays incredibly used, because both of its realizations: electronic circuit or system of differential equations can be combined for multiple purpose.[8] Following the first studies applying such combinations to crypted transmission, our aim is to build an analog of paradigm of electronic circuitry, which is the design of electronic circuit: the paradigm of chaotic mathematical circuitry, in order to improve the performance of well known chaotic attractors for application purpose (cryptography, generic algorithms in optimization, control,...).

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. In the same way a mathematical circuit is composed of individual components we introduce (generators, couplers, samplers, mixers, reducers and cascaders,...) 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 (Belykh,[17] Lorenz, Rössler,[28] ...) for application purpose (chaotic cryptography, genetic algorithms in optimization, control,...).

In Sec. 2 we recall a first historic example of chaotic mathematical circuitry: the cascading of two identical receivers in Chua's circuit. In Sec. 3, we introduce the new paradigm of chaotic mathematical circuitry, some examples of applications of which are given in Sec. 4.

2. A first historic example of chaotic mathematical circuitry: the cascading of two identical receivers in Chua's circuit

2.1. *Chua's circuit*

In october 1983, visiting T. Matsumoto at Waseda University, L. O. Chua invented an electronic circuit (Fig. 1(a) and (b)) mimicking directly on an oscilloscope screen a chaotic signal (Fig. 1(c)).

Only two autonomous systems of ordinary differential equations were generally accepted then as being chaotic, the Lorenz equations[16] and the Rössler equations.[28] The nonlinearity in both systems is a the product function of two variables which is very difficult to build in electronic circuit. L. O. Chua[4] says, " The fault lies on the dearth of a critical nonlinear IC component with a near-ideal characteristic and a sufficiently large dynamic range; namely, the analog multiplier. Unfortunately, this component was the key to building an autonomous chaotic circuit in 1983." He adds, "Suddenly [in the evening of the precise day he attended an unsuccesful presentation of an electronic circuit realization of the Lorenz Equations] it dawned upon me that since the main mechanism which gives rise to chaos, in both the Lorenz and the Rössler Equations, is the presence of at least two unstable equilibrium points -3 for the Lorenz Equations and 2 for the Rössler Equations-it seems only prudent to design a simpler and more robust circuit [than that built by Matsumoto's team] having these attributes. Having identified this alternative approach and strategy, it becomes a simple exercise in elementary nonlinear circuit theory to enumerate systematically all such circuit candidates, of which there were only 8 of them, and then to systematically eliminate those that, for one reason or another, can not be chaotic."

The Chua's equations he laid down

$$\begin{cases} \dot{x} = \alpha\left(y - x - f\left(x\right)\right), \\ \dot{y} = x - y + z, \\ \dot{z} = -\beta y, \end{cases} \tag{1}$$

where

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

and

$$\alpha = 15.60,\ \beta = 28.58,\ a = -\frac{1}{7},\ b = \frac{2}{7}\,, \tag{3}$$

were soon numerically analyzed by T. Matsumoto.[26] The "nonlinear" characteristic which is in fact only piecewise linear allows some exact computations. Henceforth, L. O. Chua *et al.*[3] proved in the same breath that the mechanism of chaos exists in this attractor.

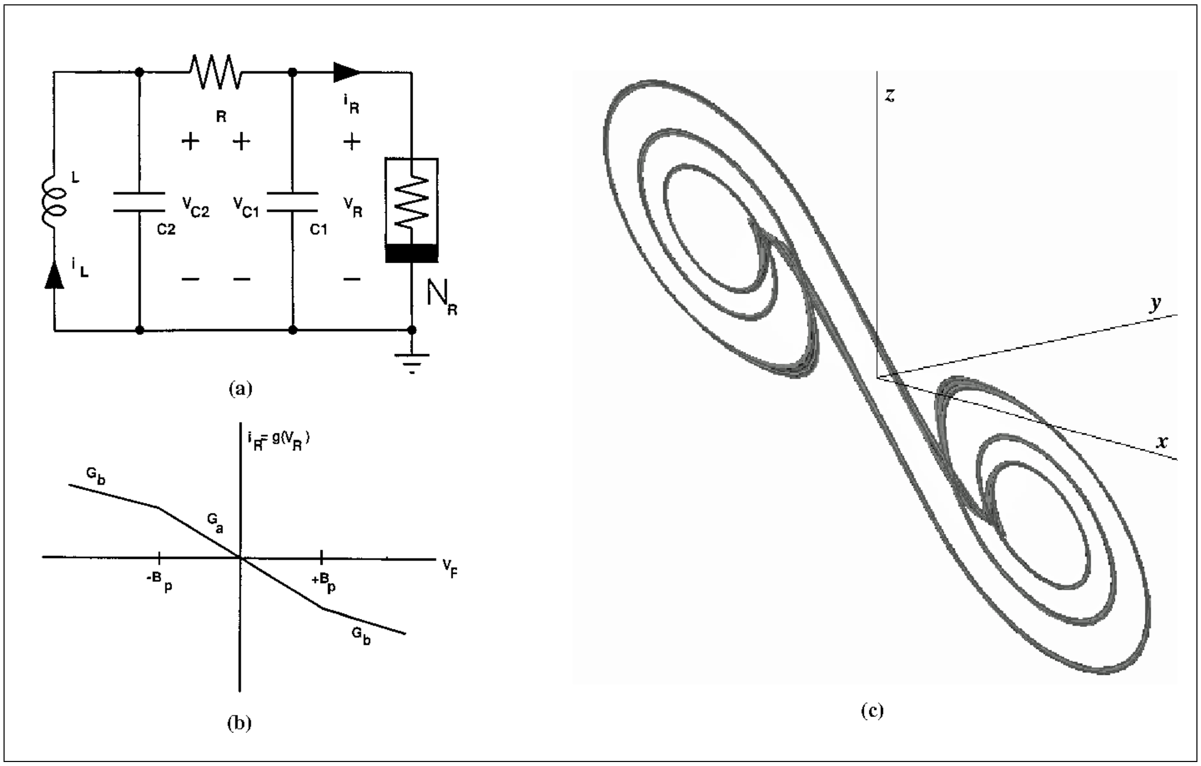


Fig. 1. (a) Realization of Chua's circuit from.[5] (b) Three-segment piecewise-linear *v*-*i* characteristic of nonlinear resistor in Chua's circuit. (c) Chua attractor.

2.2. *Secure communication via chaotic synchronization*

2.2.1. *Synchronization*

The synchronization of two Chua's circuit was studied experimentaly height years later in 1992,[5] soon followed by its application to crypted transmission. The first laboratory demonstration of a secure communication system which uses a chaotic signal for masking purposes[27] and which exploits the chaotic synchronization techniques to recover the signal was reported in 1992.[15] While the "transmitter" in this system is a direct implementation of the method proposed in oppenheim *et al.*,[27] the "receiver" differs from their computer simulation approach in that it actually contains two subsystems of the "chaotic" transmitter (Chua's circuit in that case).

2.2.2. *Single chaotic synchronization*

The mathematical translation of the dynamics of the circuit used by Kocarev *et al.,*[15] for the experimental demonstration of secure communication is as follows: the basic building block is a Chua's circuit, the dynamics of which is given by the Chua's equations (1) and (2). Here $x(t)$ is used as noise-like "masking" signal. Let $s(t)$ be an information-bearing signal. The transmitted signal is $r(t) = x(t) + s(t)$, where the power level of $s(t)$ is assumed to be significantly lower than that of $x(t)$, in order to have the signal effectively hidden. The receiver consists of two subsytems.

The first one is driven by the transmitted signal $r(t)$:

$$\begin{cases} \dot{y_1} = r\left(t\right) - y_1 + z_1, \\ \dot{z_1} = -\beta y_1. \end{cases} \tag{4}$$

The second subsytem is driven by the signal $y_1(t)$:

$$\dot{x_2} = \alpha\left(y_1\left(t\right) - x_2 - f\left(x_2\right)\right). \tag{5}$$

Then $s(t)$ is recovered as

$$s_2\left(t\right) = r\left(t\right) - x_2\left(t\right) \approx s\left(t\right). \tag{6}$$

Actually the dynamics of the experimental set-up (see Fig. 2) is described by

$$\begin{cases} \dot{x_2} = \alpha\left(y_1\left(t\right) - x_2 - f\left(x_2\right)\right), \\ \dot{z_2} = -\beta y_1\left(t\right). \end{cases} \tag{7}$$

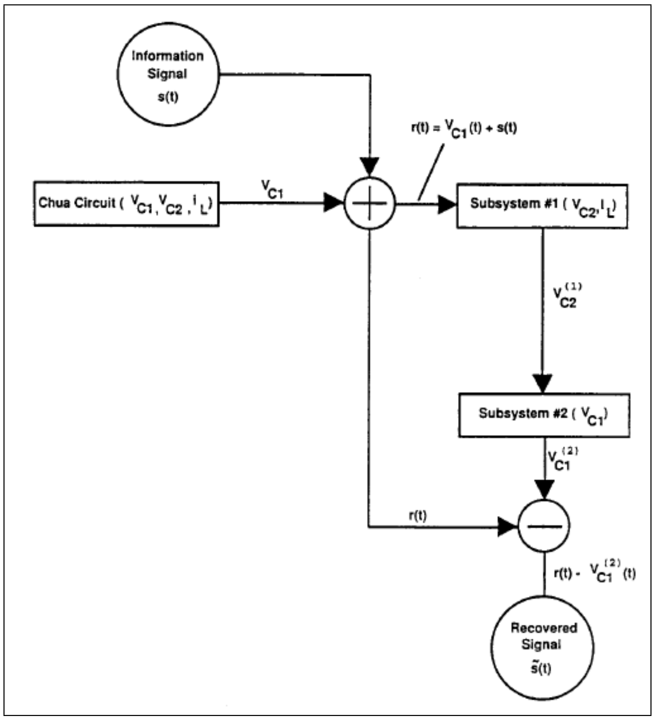


Fig. 2. Experimental set up. Block diagram of the system. It contains one Chua's circuit and two partial Chua's circuits, that is, subsystems #1 et #2 of Fig. 3, from.[15]

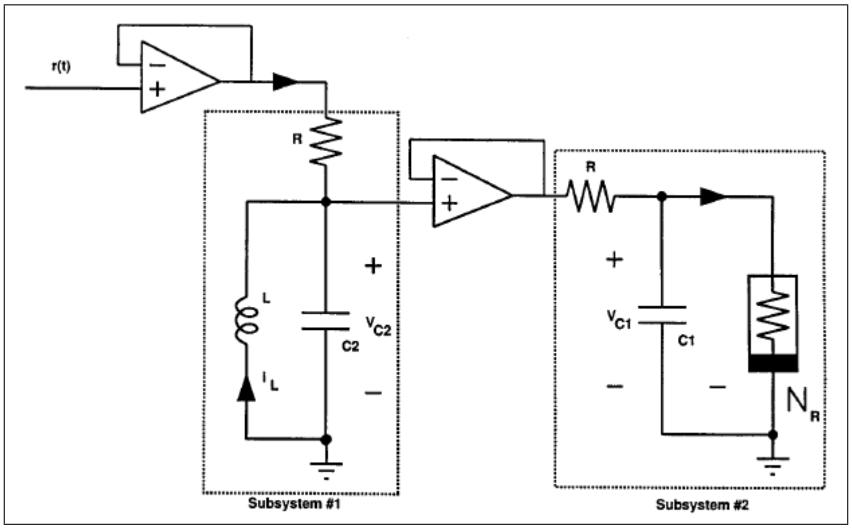


Fig. 3. Practical realization of the receiver. The first subsystem is a partial Chua's circuit consisting of the $\left(v_{C_2}, i_L\right)$-subsytem driven by the transmitted signal $r\left(t\right)$. The second subsystem is a partial Chua's circuit consisting of the $\left(v_{C_1}\right)$-subsytem driven by the transmitted signal $v_{C_2}^{(1)}$. The triangular symbols are OpAmps which decoupled the systems, acting as the signal drive elements, from.[15]

However, as long as we do not need $z_2(t)$ to recover $s_2(t)$, we continue to use Eq. 6 instead of Eq. 7 in the following improved system.

2.2.3. *Cascade chaotic synchronization*

Ten years after the invention of his ubiquitous real-world example of a chaotic system, leading some to declare it "a paradigm for chaos", and few months

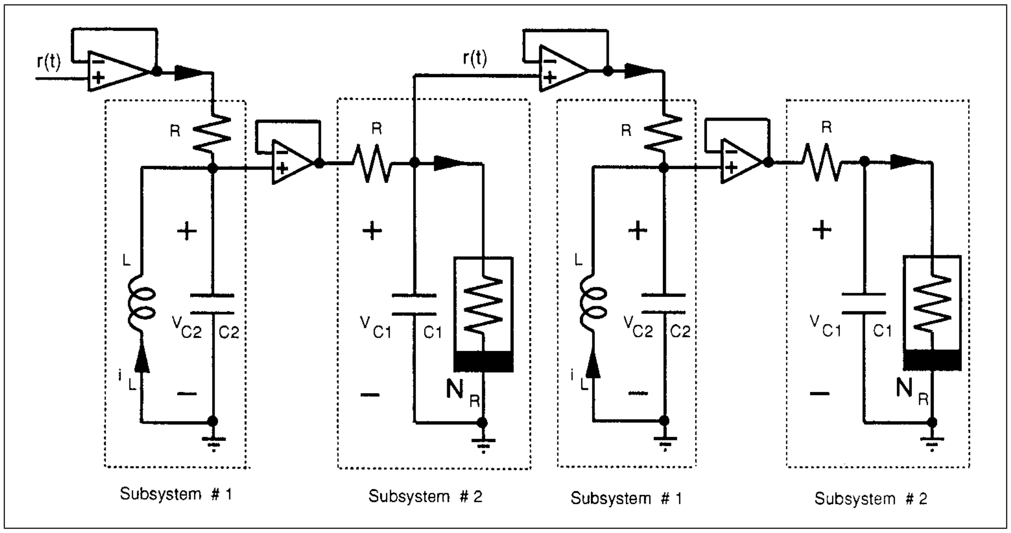


Fig. 4. Electronic circuit implementation of the two stage "receiver" consisting of two identical copies of the circuit given in Fig.3.

after the experimental demonstration of secure communication using the properties of this chaotic generator, Professor L. O. Chua was visiting us for one month, in May 1993, at the University of Nice.

In both implementations -electronic circuit realization (Fig. 3) or computer simulation (Fig. 2)- of the circuit used by Kocarev *et al.*,[15] there is an inevitable error introduced by the signal $s(t)$. Then the claim was to enhance the performance of the chaotic masking technique by improving the convergence of the recovered signal $s_2(t)$ towards the information-bearing signal $s(t)$. Having in mind the knowledge of relaxation methods used in numerical analysis (in numerical mathematics, relaxation methods are iterative methods for solving systems of equations, including nonlinear systems), we 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 Eqs. 4-5 driven by $x_2(t)$ instead of $r(t)$, as displayed in Fig. 5. The second receiver also consists of two subsytems. The first one is driven by the signal $x_2(t)$ which is assumed to be more synchronized to $x(t)$ than the transmitted signal $r(t)$:

$$\begin{cases} \dot{y_3} = x_2\left(t\right) - y_3 + z_3 \\ \dot{z_3} = -\beta y_3 \end{cases} \tag{8}$$

The second subsystem of the second receiver is then driven by the signal $y_3(t)$ from Eq. 8:

$$\dot{x_4} = \alpha\left(y_3\left(t\right) - x_4 - f\left(x_4\right)\right) \tag{9}$$

Then $s(t)$ is recovered as

$$s_4\left(t\right) = r\left(t\right) - x_4\left(t\right) \approx s\left(t\right) \tag{10}$$

In practice we simply make two copies of the receiver as shown in Fig. 4. By identifying the symbols (V_{C_1}, V_{C_2}, I_l) in Chua's circuit (see Figs. 2 and 3) with (x, y, z), the electronic circuit implementation in Fig. 4 can be translated into the block diagram shown in Fig. 5. Although no two electronic circuits can be made perfectly identical in practice, this ideal situation can be approached with the help of the integrated circuit technology demonstrated in Delgado-Restituto & Rodriguez-Vasquez.[6] By fabricating several identical Chua's circuits on the *same* silicon chip, the resulting circuits are almost "clones" of each other. This technique has the additional security adavantage in that even if someone else has discovered the parameters (α, β) used in the system, integrating it into *another* silicon chip invariably introduces discrepancies due to the different processing parameters from different silicon "foundries". We have shown by computer experiments that by connecting two identical receivers, a significant amount of noise can be reduced, thereby allowing the recovery of a much higher quality signal.[18]

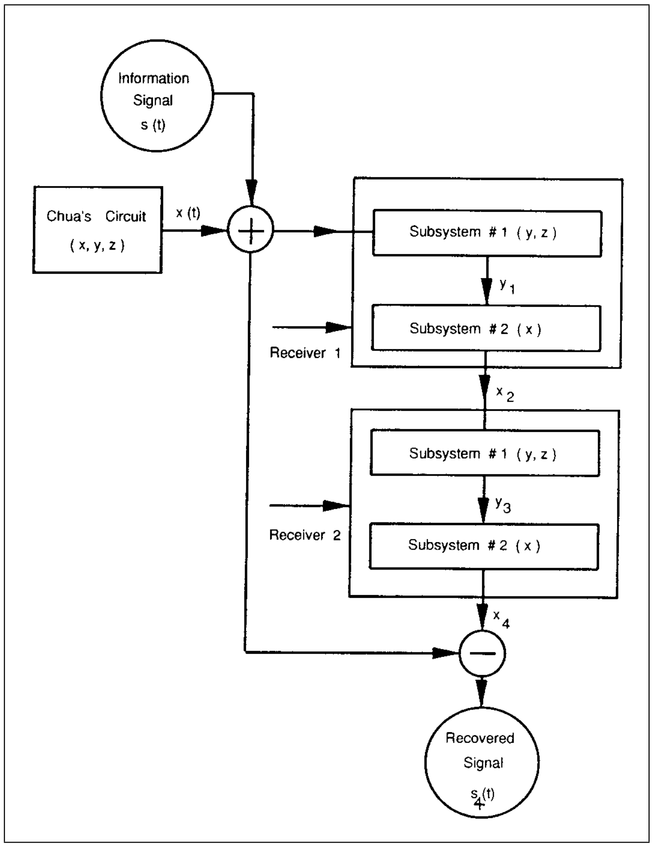


Fig. 5. Block diagram of the electronic circuit implemented in Fig. 4.

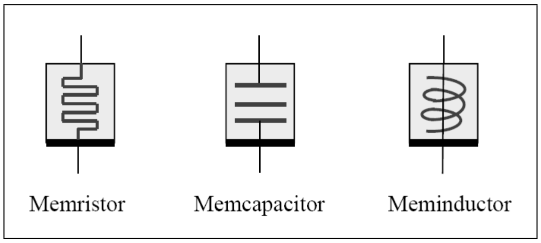


Fig. 6. Symbols of the three recently discovered circuit elements with memory.

2.2.4. *Numerical experiments*

Due to the limited extend of this chapter, we give only a sketch of results of numerical experiments. Assuming that the input (information-bearing) signal $s(t)$ is a single tone (sine wave) of amplitude $k \ll 1$:

$$s(t) = k\sin(\omega t) \ \text{ with } \ k > 0. \tag{11}$$

Therefore $s(t)$ has a power level significantly lower than that of $x(t)$.

Let us define the *errors*

$$\left\|e_s\left(k,\omega\right)\right\|_2 = \left\|s_2(t) - s(t)\right\|_2 \tag{12}$$

$$\left\|e_c\left(k,\omega\right)\right\|_2 = \left\|s_4(t) - s(t)\right\|_2 \tag{13}$$

where

$$\left\|f\left(t\right)\right\|_2 \triangleq \lim_{T\to\infty}\frac{1}{T}\left[\int_0^T f^2\left(t\right)dt\right]^{\frac{1}{2}} \tag{14}$$

denotes the quadratic norm of $f(t)$.

Extensive computer studies show that both $\left\|e_s\left(k,\omega\right)\right\|_2 / \left\|s(t)\right\|_2$ and $\left\|e_c\left(k,\omega\right)\right\|_2 / \left\|s(t)\right\|_2$ are independent of k, and that both norms $\left\|e_s\left(k,\omega\right)\right\|_2$ and

$\|e_c(k,\omega)\|_2$ are decreasing in accordance to a power law with an exponent greater than 2 when ω is increasing. Moreover $\|e_c(k,\omega)\|_2$ is always less than $\|e_s(k,\omega)\|_2$. This shows that the cascade chaotic synchronization technique offers a good improvment over the single-stage chaotic synchronization results.

3. Mathematical circuitry

Our aim is to build an analog of paradigm of electronic circuitry, which is the design of electronic circuit: the paradigm of mathematical circuitry and especially chaotic mathematical circuitry in order to improve the performance of well known chaotic attractors (Belykh,[17] Lorenz,[16] Rössler,[28] ...) for application purpose (chaotic cryptography, genetic algorithms in optimization, control, emergence of ramdoness from chaos,...).

An electronic circuit is composed of individual electronic components, such as capacitors, diodes, inductors, resistors, transistors and connected by conductive wires through which electric current can flow. Recently, in 2009, three more components discovered by L. O. Chua *et al.,*[7] have been added: memristors, memcapacitors and meminductors (Fig. 6). 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. In the same way a mathematical circuit is composed of individual components we introduce now: generators, couplers, samplers, mixers, reducers and cascaders, connected by streams of data. The combination of such mathematical components leads to several performing news applications, such as Chaotic Pseudo Random Number Generators (CPRNG), as we will show in the rest of this article.

3.1. *Generator*

Analog circuits are very commonly represented in schematic diagrams, in which wires are shown as lines, and each component has a unique symbol. We present in this section the symbols we design in order to draw mathematical schematic diagrams. The first symbols we describe, generator symbols, are, from a mathematical point of view, equivalent to a battery or a current generator in electronic circuit. However we consider that they generate a numerical signal (in one or more dimensions) rather than a voltage or an intensity variation (nonetheless, a voltage or intensity variation can be considered as a physical signal which can be discretized). This signal can be either continuous, as in Chua's circuit, or discrete as in Hénon map.[13]

In the expanded symbol of continuous generator (see Fig. 7(a)), the solid line arrows coming out from the generator represent the three components of the signal $\underline{x}(t) = (x(t), y(t), z(t))$ (see Eq. 1), the dashed line arrow points at λ which stands for the parameter value defined by Eq. 3, and the dot line arrow 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. 7(b).

We need also to design chaotic circuitry for discrete signal. To this aim two generators can be considered: in dimension 2, the Hénon map (see Figs. 7(c) and (d))

$$H_{a,b} : \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} y + 1 - ax^2 \\ bx \end{pmatrix} \tag{15}$$

with

$$a = 1.4,\ b = 0.3, \tag{16}$$

which is associated to the dynamical system,

$$\begin{cases} x_{n+1} = y_n + 1 - ax_n^2 \\ y_{n+1} = bx_n \end{cases} \tag{17}$$

and the logistic map

$$f_r(x) = rx(1-x) \tag{18}$$

linked to the one dimensional system which is chaotic when $r = 4$ (see Fig. 7(e)).

$$x_{n+1} = rx_n(1-x_n) \tag{19}$$

Thereafter, another 1-dimensional chaotic generator, the symmetric tent map, will be, also, represented by the same symbol.

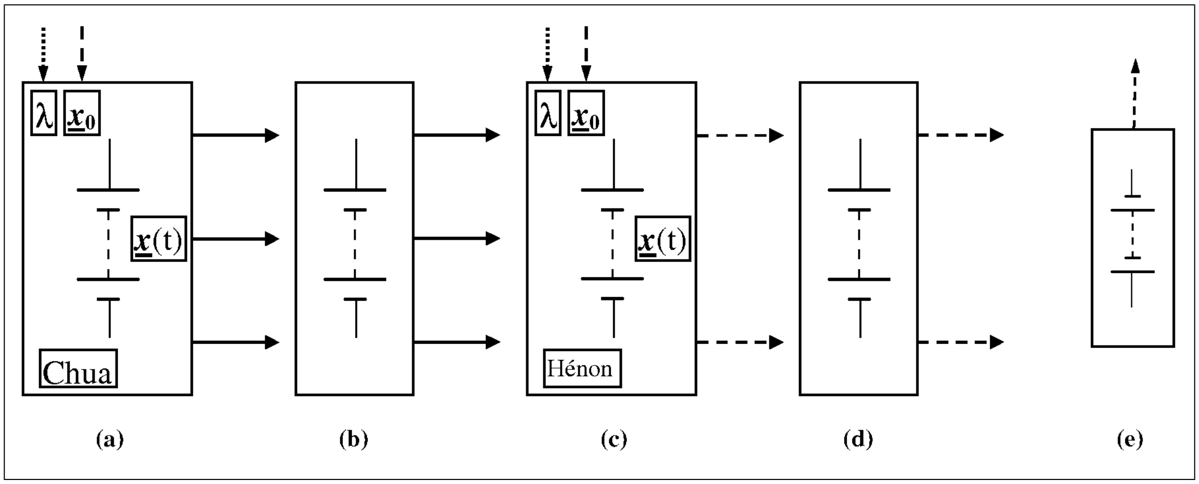


Fig. 7. Generators. (a) Continuous generator (Chua's circuit, expanded symbol). (b) Simplified continuous generator. (c) Discrete generator (Hénon map, expanded symbol). (d) Simplified discrete generator. (e) 1-dimensional logistic generator.

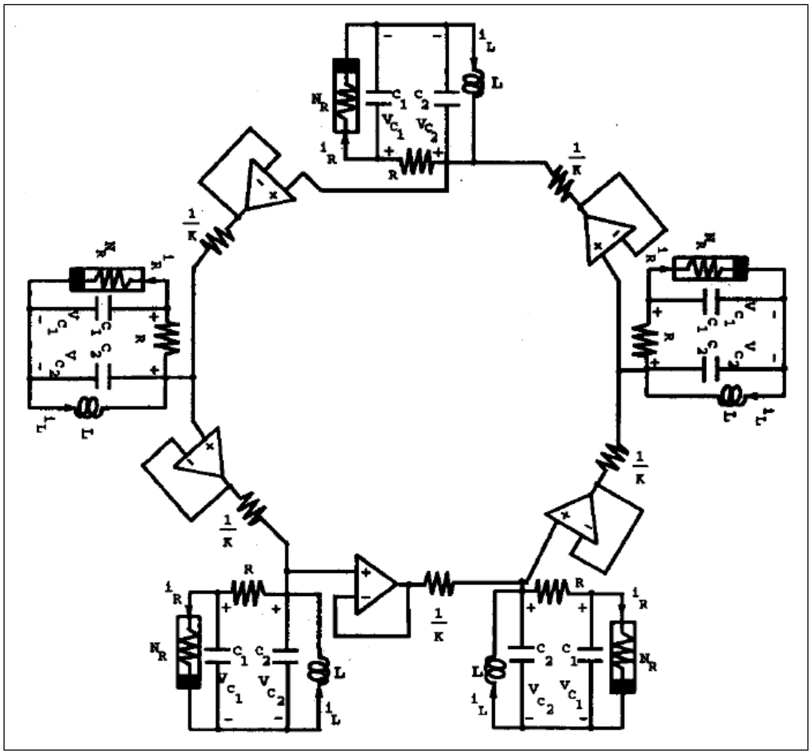


Fig. 8. Five identical coupled Chua's circuits forming a ring, from.[14]

3.2. *Coupler*

Two years after the experimental study of the synchronization of two Chua's circuit, in 1994, experimental observation of hyperchaotic attractors in open and closed chain of Chua's circuit was reported.[14] The layout of the five identical coupled Chua's circuit forming a ring is displayed on Fig. 8, the state equations of this circuit are as follows

$$\left\{\begin{array}{l}
C_1\frac{dv_{C_1}^{(1)}}{dt} = G\left(v_{C_2}^{(1)} - v_{C_1}^{(1)}\right) - f\left(v_{C_1}^{(1)}\right),\\
C_2\frac{dv_{C_2}^{(1)}}{dt} = G\left(v_{C_1}^{(1)} - v_{C_2}^{(1)}\right) + i_L^{(1)} + K_1\left(v_{C_2}^{(2)} - v_{C_2}^{(1)}\right),\\
L\frac{di_L^{(1)}}{dt} = -v_{C_2}^{(1)},\\
C_1\frac{dv_{C_1}^{(2)}}{dt} = G\left(v_{C_2}^{(2)} - v_{C_1}^{(2)}\right) - f\left(v_{C_1}^{(2)}\right),\\
C_2\frac{dv_{C_2}^{(2)}}{dt} = G\left(v_{C_1}^{(2)} - v_{C_2}^{(2)}\right) + i_L^{(2)} + K_2\left(v_{C_2}^{(3)} - v_{C_2}^{(2)}\right),\\
L\frac{di_L^{(2)}}{dt} = -v_{C_2}^{(2)},\\
\qquad\qquad\qquad\cdots\\
\qquad\qquad\qquad\cdots\\
\qquad\qquad\qquad\cdots\\
C_1\frac{dv_{C_1}^{(5)}}{dt} = G\left(v_{C_2}^{(5)} - v_{C_1}^{(5)}\right) - f\left(v_{C_1}^{(5)}\right),\\
C_2\frac{dv_{C_2}^{(5)}}{dt} = G\left(v_{C_1}^{(5)} - v_{C_2}^{(5)}\right) + i_L^{(5)} + K_5\left(v_{C_2}^{(1)} - v_{C_2}^{(5)}\right),\\
L\frac{di_L^{(2)}}{dt} = -v_{C_2}^{(5)}.
\end{array}\right. \tag{20}$$

Each Chua's circuit (see Fig. 1 (a)) contains three linear energy-storage elements (an inductor and two capacitors), a linear resitor, and a single nonlinear resistor, namely, Chua's diode with three segment linear characteristic defined by

$$f\left(v_R\right) = m_0 v_R + \frac{1}{2}\left(m_1 - m_0\right)\left[\left|v_R + B_p\right| - \left|v_R - B_p\right|\right] \tag{21}$$

where the slopes in the inner and the outer regions are m_0 and m_1, respectively, and $\pm B_p$ denotes the breakpoints (see Fig. 1 (b)). Equation 21 is equivalent to Eq. 2. By identifying the symbols $\left(V_{C_1}^{(i)}, V_{C_2}^{(i)}, I_l^{(i)}\right)$ in each Chua's circuit with $\left(x^i, y^i, z^i\right)$, the state equations of the circuit can be translated into the differential equations (22) and the electronic circuit symbolized by the mathematical circuit of Fig. 9.

$$\left\{\begin{array}{l}
\dot{x}^1 = \alpha\left(y^1 - x^1 - f\left(x^1\right)\right),\\
\dot{y}^1 = x^1 - y^1 + z^1 + k_1\left(y^2 - y^1\right),\\
\dot{z}^1 = -\beta y^1,\\
\dot{x}^2 = \alpha\left(y^2 - x^2 - f\left(x^2\right)\right),\\
\dot{y}^2 = x^2 - y^2 + z^2 + k_2\left(y^3 - y^2\right),\\
\dot{z}^2 = -\beta y^2,\\
\qquad\qquad\cdots\\
\qquad\qquad\cdots\\
\qquad\qquad\cdots\\
\dot{x}^5 = \alpha\left(y^5 - x^5 - f\left(x^5\right)\right),\\
\dot{y}^5 = x^5 - y^5 + z^5 + k_5\left(y^1 - y^5\right),\\
\dot{z}^5 = -\beta y^5.
\end{array}\right. \tag{22}$$

In this figure the double arrows symbolize the coupling $k_i\left(y^{i+1} - y^i\right)$ of one Chua's circuit to the next one. In order to represent the coupling between mathematical equation, depending on the nature of the coupling, we can use both symbols: the ring coupler corresponding to the coupling of one generator to the next one (Fig. 10(a)), and the full coupler when the coupling involves more connections between the couplers (Fig 10(b)).

Remark 1.1. In the rest of this article, we use solid

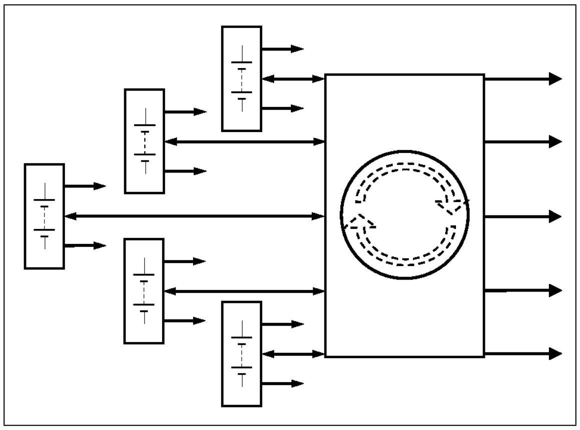


Fig. 9. Numerical circuit corresponding to electronic circuit of Fig. 8.

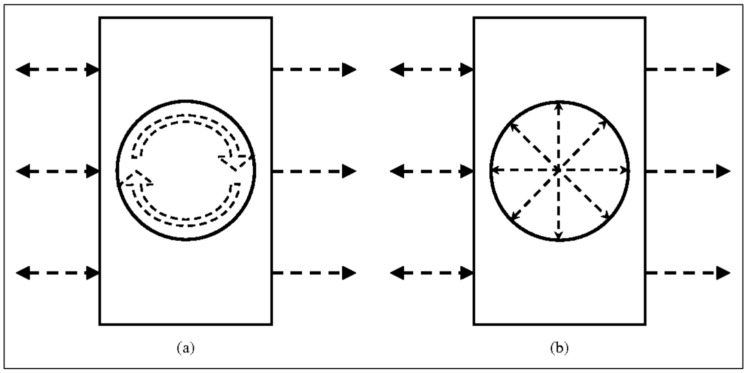


Fig. 10. (a) Ring coupler. (b) Full coupler.

line arrow for continuous signal $x\left(t\right)$, and dashed line arrow for discrete signal x_n.

It has been shown, a few years ago[20] that the ultra-weak coupling of several logistic maps (Eq. 18) or symmetric tent maps

$$f_a\left(x\right) = 1 - a\left|x\right| \tag{23}$$

$$x_{n+1} = f_a\left(x_n\right) \tag{24}$$

when $a = 2$, allows the production of long series of chaotic numbers equally distributed over the interval $J = [-1, 1] \subset \mathbb{R}$.

When a dynamical system is realized on a computer using floating point numbers, the computation is of discretization, where finite arithmetic replaces continuum state space. For chaotic dynamical systems, the discretizations often have collapsing effects to a fixed point or to short cycles.[25] Instead, the ultra-weak coupling of logistic or symmetric tent map

$$\begin{cases} x_{n+1}^1 = \left(1 - 2\varepsilon_1\right) f\left(x_n^1\right) + \varepsilon_1 f\left(x_n^2\right) + \varepsilon_1 f\left(x_n^3\right) \\ x_{n+1}^2 = \varepsilon_2 f\left(x_n^1\right) + \left(1 - 2\varepsilon_2\right) f\left(x_n^2\right) + \varepsilon_2 f\left(x_n^3\right) \\ x_{n+1}^3 = \varepsilon_3 f\left(x_n^1\right) + \varepsilon_3 f\left(x_n^2\right) + \left(1 - 2\varepsilon_3\right) f\left(x_n^3\right) \end{cases} \tag{25}$$

symbolized by Fig. 11(a) gives rise to sterling model of generator of chaotic numbers with a uniform distribution of these numbers of the interval $[-1, 1]$. Ultra-weak coupling means $\varepsilon_i \in \left[10^{-15}, 10^{-7}\right]$ for computations using double precision numbers.[24] The periodic solutions of such generator have period far greater than ten billions. Of course, more than three 1-dimensional generators can be coupled under the same process, enhancing the ergodic properties of the generator.

The considered system of the p-coupled dynamical systems is

$$X_{n+1} = F(X_n) = A.\left(\underline{f}(X_n)\right) \tag{26}$$

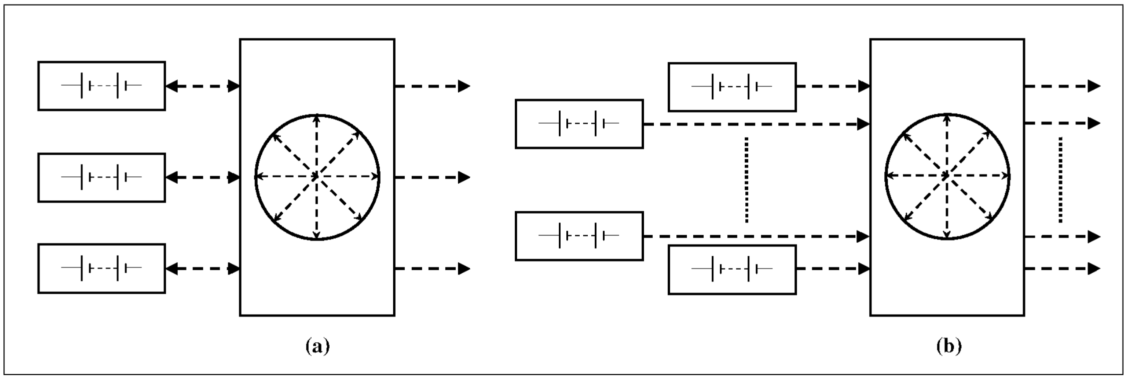


Fig. 11. (a) Circuit of ultraweak coupling of three 1-dimensional chaotic maps. (b) Circuit of ultraweak coupling of p 1-dimensional chaotic maps.

with

$$X_n = \begin{pmatrix} x_n^1 \\ \vdots \\ x_n^p \end{pmatrix} \qquad \underline{f}(X_n) = \begin{pmatrix} f(x_n^1) \\ \vdots \\ f(x_n^p) \end{pmatrix} \tag{27}$$

and the coupling matrix A. F is a map of $J^p = [-1,1]^p \subset \mathbb{R}^p$ into itself. The mathematical circuit of this system is displayed on Fig. 11(b).

$$A = \begin{pmatrix} \varepsilon_{1,1} = 1 - \sum_{j=2}^{j=p} \varepsilon_{1,j} & \varepsilon_{1,2} & \cdots & \varepsilon_{1,p-1} & \varepsilon_{1,p} \\ \varepsilon_{2,1} & \varepsilon_{2,2} = 1 - \sum_{j=1, j\neq 2}^{j=p} \varepsilon_{2,j} & \cdots & \varepsilon_{2,p-1} & \varepsilon_{2,p} \\ \vdots & \ddots & & \vdots & \vdots \\ \vdots & & \ddots & \vdots & \vdots \\ \varepsilon_{p,1} & \cdots & \cdots & \varepsilon_{p,p-1} & \varepsilon_{p,p} = 1 - \sum_{j=1}^{j=p-1} \varepsilon_{p,j} \end{pmatrix} \tag{28}$$

It is noteworthy that these families of very weakly coupled maps are more powerful than the usual formulas used to generate chaotic 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 common in laptop computers, nowadays.

We display in Table 1 the discrepancies in quadratic norm (Eq. 14) between the distribution of the iterated values x_n^1 and the Lebesgue measure vs. the number of iterates N_{iter}, for 2, 3 and 4-coupled symmetric tent maps. Computations are done using double precision numbers ($\sim 14 - 15$ digits), $\varepsilon_{i,j} = i\varepsilon_1$, $j = 1, 4$, $\varepsilon_1 = 10^{-14}$, initial values: $x_0^1 = 0.330000013113$, $x_0^2 = 0.338756413113$, $x_0^3 = 0.331353442113$, $x_0^4 = 0.333213583113$.

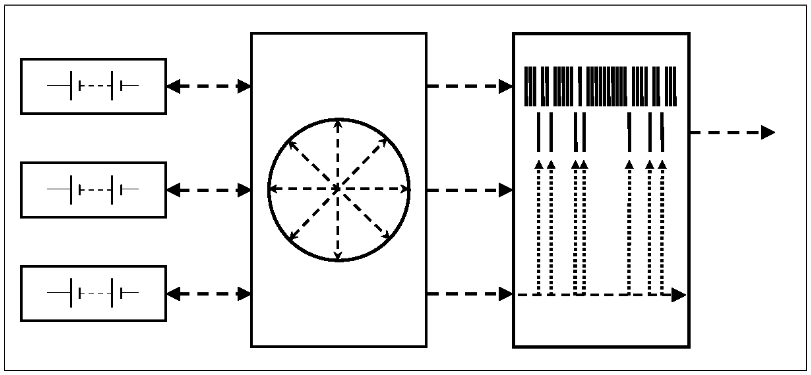


Fig. 12. Circuit of enhanced Chaotic Pseudo Random Number Generators (CPRNG) based on chaotic sampling.

Table 1

N_{iter}	$2 - coupled\ equation$	$3 - coupled\ equation$	$4 - coupled\ equation$
10^5	0.100199	0.099820996	0.099610992
10^6	0.01006199	0.0098781898	0.01022057
10^7	0.0010442081	0.0010014581	0.0010055967
10^8	0.0001055816	9.8853067×10^{-5}	0.00010197872
10^9	1.567597×10^{-5}	1.0047459×10^{-5}	1.0326474×10^{-5}
10^{10}	7.3577797×10^{-6}	9.7251536×10^{-7}	9.9932242×10^{-7}
10^{11}	6.6338453×10^{-6}	1.0434293×10^{-7}	1.0070523×10^{-7}
10^{12}		1.116009×10^{-8}	9.6166733×10^{-9}
3×10^{12}		4.0443118×10^{-9}	3.2530773×10^{-9}

Remark: the ring coupler of Fig. 10(a) corresponds to an hollow matrix, in which only one diagonal and one other coefficient are not empty. The full coupler of the same figure stands for a matrix more filled with non vanishing coefficients as in Eq. 28.

3.3. *Sampler*

However chaotic numbers are not pseudo-random numbers because the plot of the couples of any component (x_n^l, x_{n+1}^l) of iterated points (X_n, X_{n+1}) in the corresponding phase plane reveals the map f used as one-dimensional dynamical systems to generate them via Eq. 26. Nevertheless we have recently introduced a family of enhanced Chaotic Pseudo Random Number Generators (CPRNG) in order to compute very fast long series of pseudorandom numbers with desktop computer[21,22,23] and its properties have been analyzed.[10,11,12] This family is based on the previous ultra-weak coupling which is improved in order to conceal the chaotic genuine function.

In order to hide f of Eq. 26, in the phase space (x_n^l, x_{n+1}^l), two mechanisms are used. The pivotal idea of the first one mechanism is to sample chaotically the sequence $(x_0^l, x_1^l, x_2^l, \ \dots\ , x_n^l, x_{n+1}^l, \ \dots)$ generated by the l-th component x^l, selecting x_n^l every time the value x_n^m of the m-th component x^m, is strictly greater (or smaller) than a threshold $T \in J$, with $l \neq m$, for $1 \leq l, m \leq p$.

That is to say, to extract the subsequence $(x_{n_{(0)}}^l, x_{n_{(1)}}^l, x_{n_{(2)}}^l, \ \dots\ , x_{n_{(q)}}^l, x_{n_{(q+1)}}^l, \ \dots)$ denoted here $(\overline{x_0}, \overline{x_1}, \overline{x_2}, \ \dots\ , \overline{x_q}, \overline{x_{q+1}}, \ \dots)$ from the original one, in the following way:

Given $1 \leq l, m \leq p$, $l \neq m$

$$\begin{cases} n_{(-1)} = -1 \\ \overline{x_q} = x_{n_{(q)}}^l \ , \quad \text{with} \quad n_{(q)} = \min\limits_{r \in \mathbb{N}} \{ r > n_{(q-1)} \ \mid \ x_r^m > T \} \end{cases} \tag{29}$$

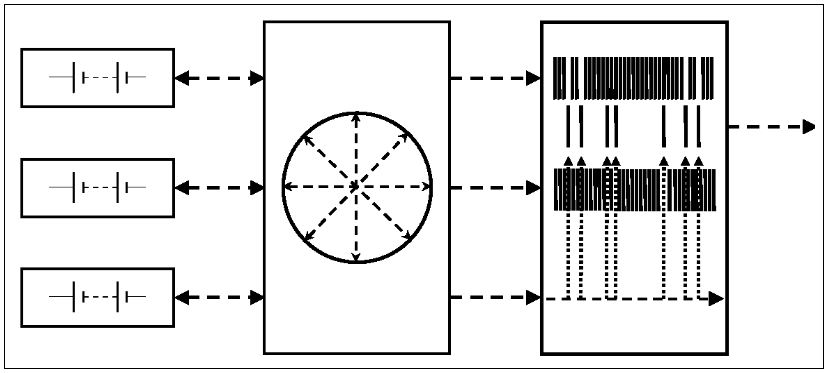


Fig. 13. Circuit of enhanced Chaotic Pseudo Random Number Generators (CPRNG) based on chaotic mixing.

The sequence $(\overline{x_0}, \overline{x_1}, \overline{x_2}, \ ... \ , \overline{x_q}, \overline{x_{q+1}}, \ ...)$ is then the sequence of chaotic pseudo-random numbers.

The mathematical formula (29) can be best understood in algorithmic way. The pseudo-code, for computing iterates of (29) corresponding to N iterates of Eq. 26 is:

```
$X_0 = (x_0^1, x_0^2, ..., x_0^{p-1}, x_0^p) = seed$
$n = 0$; $q = 0$;
do { while $n < N$
    do { while $(x_n^m \leq T)$
        compute $(x_n^1, x_n^2, ..., x_n^{p-1}, x_n^p); n$++}
    compute $(x_n^1, x_n^2, ..., x_n^{p-1}, x_n^p)$;
    then $n(q) = n; \overline{x_q} = x^1_{n(q)}; n$++; $q$++}
```

This chaotic sampling is possible due to the independence of each component of the iterated points X_n vs. the others.[21] We introduce the symbol on the right hand side of Fig. 12 in order to give a schematic representation of this sampling (also called subsampling) process.

3.4. *Mixer*

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

$$T_1 < T_2 < ... < T_{p-1} \ \in \ J$$

and the corresponding partition of

$$J = \bigcup_{k=0}^{p-1} J_k$$

with $J_0 = [-1, T_1]$, $J_1 =]T_1, T_2[$, $J_k = [T_k, T_{k+1}[$ for $1 < k < p-1$ and $J_{p-1} = [T_{p-1}, 1[$,
this simple mechanism is based on the chaotic mixing of the $p-1$ sequences

$(x_0^1, x_1^1, x_2^1, \ ... \ , x_n^1, x_{n+1}^1, \ ...), (x_0^2, x_1^2, x_2^2, \ ... \ , x_n^2, x_{n+1}^2, \ ...),$ $... \ , (x_0^{p-1}, x_1^{p-1}, x_2^{p-1}, \ ... \ , x_n^{p-1}, x_{n+1}^{p-1}, \ ...), \ ...$
using the last one $(x_0^p, x_1^p, x_2^p, \ ... \ , x_n^p, x_{n+1}^p, \ ...)$ in order to distribute the iterated points with respect to this given partition defining the subsequence $(\overline{x_0}, \overline{x_1}, \overline{x_2}, \ ... \ , \overline{x_q}, \overline{x_{q+1}}, \ ...)$ by

$$\begin{cases} n_{(-1)} = -1 \\ \overline{x_q} = x^k_{n_{(q)}} \ , \quad \text{with} \ \ n_{(q)} = \min\limits_{1 \leq k \leq p-1} \left\{ s_k(q) = \min\limits_{r \in \mathbb{N}} \{ r_k > n_{(q-1)} \ \ | \ \ x^p_{r_k} \in J_k \} \right\} \end{cases} \tag{30}$$

The pseudo-code, for computing the iterates of Eq. 30 corresponding to N iterates of Eq. 26 is

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

We introduce the symbol on the right hand side of Fig. 13 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.

We display in Table 2 the discrepancies in quadratic norm (Eq. 14) between the autocorrelation distribution of the iterated values and the Lebesgue measure vs. the number of subsampled or mixed iterates N_{iter}, for 4-coupled symmetric tent maps. Sampling: the first component x^1 is sampled by x^4 for the threshold value 0.998. Mixing: the three components x^1 , x^2, x^3 are mixed and sampled by x^4 for the threshold values $T_1 = 0.998$, $T_2 = 0.9987$, $T_3 = 0.9994$. Computations are done using double precision numbers ($\sim$ 14 − 15 digits), $\varepsilon_{i,j} = i\varepsilon_1$, $j = 1, 4$, $\varepsilon_1 = 10^{-14}$, initial values: $x_0^1 = 0.330$, $x_0^2 = 0.3387564$, $x_0^3 = 0.50492331$, $x_0^4 = 0.0$.

Table 2

N_{iter}	$sampling\ of\ 4 - coupled\ equation$	$mixing\ of\ 4 - coupled\ equation$
10^5	0.70947368	0.68924731
10^6	0.26570546	0.25881773
10^7	0.079871223	0.086706776
10^8	0.023190157	0.026815309
10^9	0.0071386288	0.0089111078
10^{10}	0.002493667	0.0027932033
10^{11}	0.00071561417	0.00085967214
10^{12}	0.00025442753	0.0002346851
10^{13}	0.000088445108	0.000073234736

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.[24]

3.5. *Reducer*

The accelerated development of modern data transaction applications such as telecommunications requires encoding techniques with higher standards of security.

Classically, these encoding sequences are obtained using Pseudo Random Number Generators (PRNG). Since the seminal work presented in Sec. 2, an efficient alternative, the chaotic-based generators (CPRNG) are used to achieve even higher demanding encryption standards. Indeed, the chaotic systems exhibit a plethora of properties which make them suitable to meet the above requirements.

The advantage to use chaotic systems lies in their extreme sensitivity to small parameter and initial conditions variations: in this way, as many different chaotic carriers as wanted can be generated. However, the appropriate selection of a chaotic map that satisfies cryptographic applications requirements is a huge problem. It has to be emphasized that all chaotic maps are not applicable, because the chaotic generator -which is deterministic- has to satisfy at the same time the criteria for closeness to random signals. Therefore many practical problems arise, from the choice of the chaotic generator and its parameters, to the chaotic properties verification after the quantisation. Ideally, for cryptographic applications and higher security, an everywhere dense chaotic attractor is required, so all chaotic signal samples will appear with the same probability. We have shown that highly efficient discrete-time chaotic generators can be obtained from coupling, sampling, and mixing quite simple models such as the logisic map or the symmetric tent map. We have built the corresponding mathematical circuit. Moreover there exist other combinations of such 1-dimensional chaotic attractor.

We introduce now, as an example, another combination which can directly provides random number without sampling or mixing, although it is possible to combine these processes with it.

The idea leading to this system is to confine on $J^p = [-1, 1]^p \subset \mathbb{R}^p$, considered as a torus, a ring of $p-$coupled symmetric tent map (or logistic map).[9]

Consider the equation

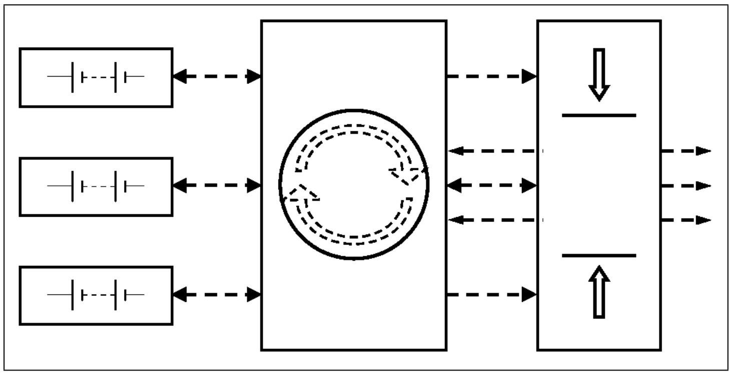


Fig. 14. Reducer for the circuit of Eq. 31, with $n = 3$.

$$\begin{cases} x_{n+1}^1 = 1 - 2\left|x_n^1\right| + k_1 x_n^2 \\ x_{n+1}^2 = 1 - 2\left|x_n^2\right| + k_2 x_n^3 \\ \vdots \\ x_{n+1}^p = 1 - 2\left|x_n^p\right| + k_p x_n^1 \end{cases} \tag{31}$$

where the parameters $k_i \in \{-1, 1\}$. In order to confine the variables x_{n+1}^i on J^p, we do, for every iteration the transform

$$if\ x_{n+1}^i < -1,\ add\ 2 \tag{32}$$

$$if\ x_{n+1}^i > 1,\ substract\ 2 \tag{33}$$

We desing a new symbol: the reducer (on the right hand side of Fig. 14) in order to give a schematic representation of the projection of the variable on the torus J^p. For sake of simplicity we have only displayed a circuit with three 1-dimensional generators. However this new pseudo-random number generator works better when more generators are coupled.

To evaluate the random properties of these generators, a set of statistical based test known as NIST test developed by the National Institute of Standards and Technology have been used.

The random properties validation of a 4-dimensional system has been carried out. Additionally, the chaotic carrier output needs to be quantised and binarised (0 and 1) in order to be validated as being random using NIST tests. Therefore, different methods of binarisation (converting real signals to binary ones) have been implemented and compared.

A first 1−bit binarisation has been applied to the system (31) with $n = 4$, output: the results showed to be highly sensitive to the type of binarisation. Eventually, after testing several different methods, a 32−bit binarisation has been chosen as being the most suitable solution. Because the system is confined to the p−dimensional torus, 31 bits are assigned to represent the decimal part, and 1 bit to the sign. To illustrate the results, the NIST tests for the four dimensional system (31) with parameters $k_i = (-1)^{i+1}$ are shown in Fig. 15. The chosen conditions are:

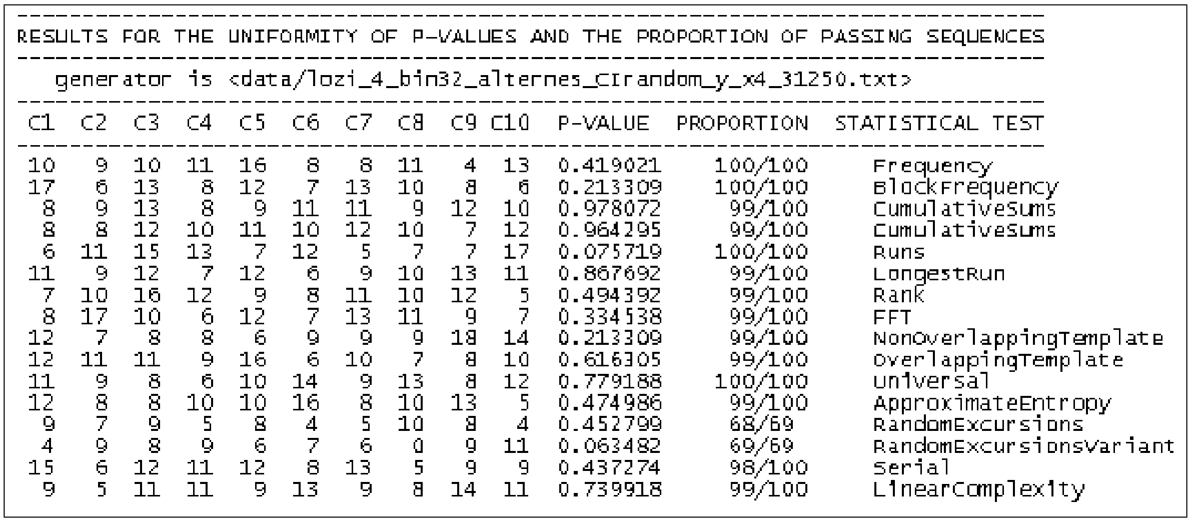
Length of the original sequence: 10^8 bits, length of bit string: 10^6, quantity of bit strings: 100. The output of the system has been arbitrary chosen as being: $y = x_n^4$.

Furthermore, as the results show their independence from 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 sequence can be accepted as being random. As we said above, in order to improve even more the random properties of that random signal, two possible strategies are possible: increasing the system order or under-sampling the output signal, which is possible with the circuit of Fig. 14 in which a sampler is added on hand right side.

3.6. *Cascader*

Finally, turning back to the problem of chaotic masking, via the cascading of Chua's attractor, the last symbol we design in order to schematise mathematically the cascading method is the cascader displayed on Fig. 16(a).



```
------------------------------------------------------------------------------
RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES
------------------------------------------------------------------------------
   generator is <data/lozi_4_bin32_alternes_CIrandom_y_x4_31250.txt>
------------------------------------------------------------------------------
 C1  C2  C3  C4  C5  C6  C7  C8  C9 C10  P-VALUE  PROPORTION  STATISTICAL TEST
------------------------------------------------------------------------------
 10   9  10  11  16   8   8  11   4  13  0.419021    100/100     Frequency
 17   6  13   8  12   7  13  10   8   6  0.213309    100/100     BlockFrequency
  8   9  13   8   9  11  11   9  12  10  0.978072     99/100     CumulativeSums
  8   8  12  10  11  10  12  10   7  12  0.964295     99/100     CumulativeSums
  6  11  15  13   7  12   5   7   7  17  0.075719    100/100     Runs
 11   9  12   7  12   6   9  10  13  11  0.867692     99/100     LongestRun
  7  10  16  12   9   8  11  10  12   5  0.494392     99/100     Rank
  8  17  10   6  12   7  13  11   9   7  0.334538     99/100     FFT
 12   7   8   8   6   9   9   9  18  14  0.213309     99/100     NonOverlappingTemplate
 12  11  11   9  16   6  10   7   8  10  0.616305     99/100     OverlappingTemplate
 11   9   8   6  10  14   9  13   8  12  0.779188    100/100     Universal
 12   8   8  10  10  16   8  10  13   5  0.474986     99/100     ApproximateEntropy
  9   7   9   5   8   4   5  10   8   4  0.452799     68/69      RandomExcursions
  4   9   8   9   6   7   6   0   9  11  0.063482     69/69      RandomExcursionsVariant
 15   6  12  11  12   8  13   5   9   9  0.437274     98/100     Serial
  9   5  11  11   9  13   9   8  14  11  0.739918     99/100     LinearComplexity
```

Fig. 15. Successful result of the NIST tests.

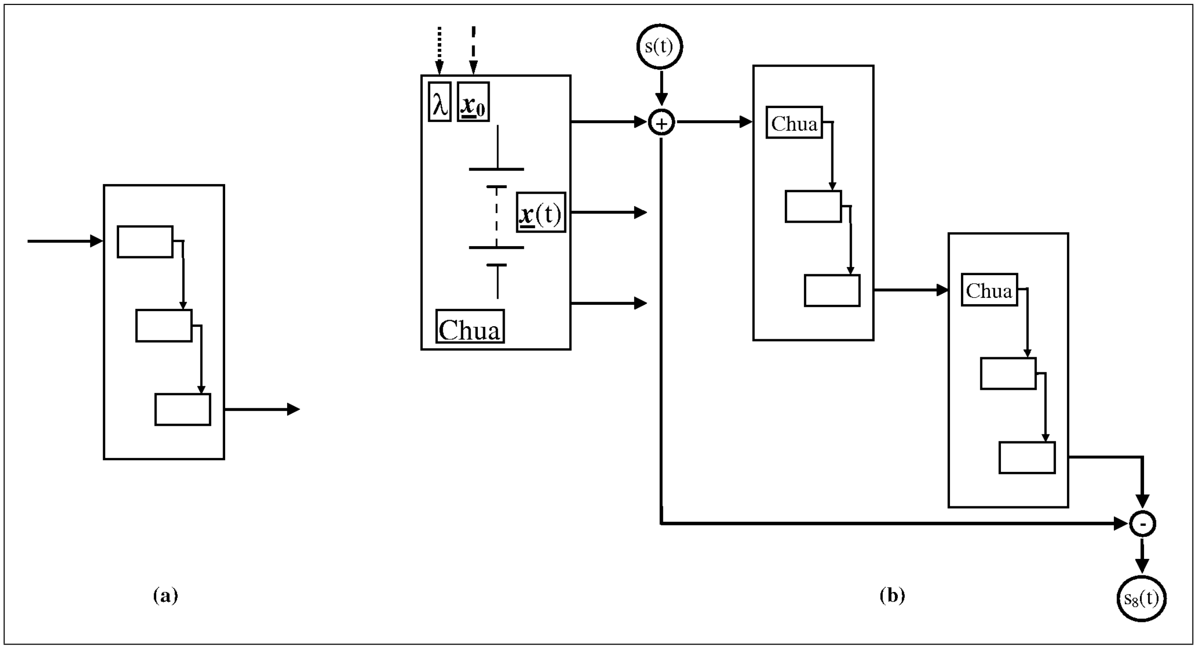


Fig. 16. (a) Cascader symbol. (b) Two cascading receivers combined.

4. mathematical circuit engineering

4.1. *Signal masking*

In the limited extend of this chapter, we give only two examples of the engineery of mathematical circuits we have introduced in the previous Section. The first one 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 deep the combination of circuit elements. It is possible to combine two cascading receiver as in Fig. 16(b).

The equations of this circuit are

$$\begin{cases} \dot{y_5} = x_4\left(t\right) - y_5 + z_5 \\ \dot{z_5} = -\beta y_5 \end{cases} \tag{34}$$

$$\dot{x_6} = \alpha\left(y_5\left(t\right) - x_6 - f\left(x_6\right)\right) \tag{35}$$

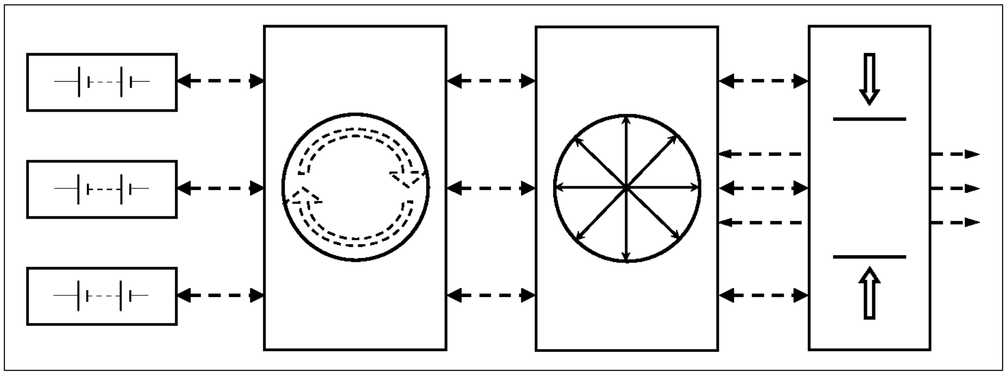


Fig. 17. Chaotic multistream PRNG (Cms-PNRG).

$$\begin{cases} \dot{y_7} = x_6\left(t\right) - y_7 + z_7 \\ \dot{z_7} = -\beta y_7 \end{cases} \tag{36}$$

$$\dot{x_8} = \alpha\left(y_7\left(t\right) - x_8 - f\left(x_8\right)\right) \tag{37}$$

Then $s(t)$ is recovered as

$$s_8\left(t\right) = r\left(t\right) - x_8\left(t\right) \approx s\left(t\right) \tag{38}$$

Numerical experiments show an improvement of the results.[1,19]

4.2. *Noise-resisting cryptography*

The second example which highligt the complex combination of circuit element belongs to the new flourishing field of chaotic based cryptography. We proposed last year,[2] a novel noise-resisting ciphering method resorting to a chaotic multi-stream pseudo-random number generator (denoted Cms-PRNG) described below. This Cms-PRNG co-generates an arbitrarily large number of uncorrelated chaotic sequences. These cogenerated sequences are actually used in several steps of the ciphering process. Noisy transmission conditions are considered, with realistic assumptions. The efficiency of the proposed method for ciphering and deciphering is illustrated through numerical simulations based on a Cms-PRNG involving ten coupled chaotic sequences.

The CPRNG decribed in Fig. 14, can be improved in order to generate uncorrelated sequences of pseudo-random numbers, possessing a large number of keys. This is simply obtained by adding a coupler as a keyer as in the circuit of Fig. 17 corresponding to Eq. 39 for 4-streams, or Eq. 40 for $p-$streams.

$$\begin{cases} x_{n+1}^1 = 1 - 2\left|x_n^1\right| + k_1\left(1 - \varepsilon_{1,3} - \varepsilon_{1,4}\right)x_n^2 + \varepsilon_{1,3}x_n^3 + \varepsilon_{1,4}x_n^4 \\ x_{n+1}^2 = 1 - 2\left|x_n^2\right| + k_2\left(1 - \varepsilon_{2,4} - \varepsilon_{2,1}\right)x_n^3 + \varepsilon_{2,4}x_n^4 + \varepsilon_{2,1}x_n^1 \\ x_{n+1}^3 = 1 - 2\left|x_n^3\right| + k_3\left(1 - \varepsilon_{3,1} - \varepsilon_{3,2}\right)x_n^4 + \varepsilon_{3,1}x_n^1 + \varepsilon_{3,2}x_n^2 \\ x_{n+1}^4 = 1 - 2\left|x_n^4\right| + k_4\left(1 - \varepsilon_{4,2} - \varepsilon_{4,3}\right)x_n^1 + \varepsilon_{4,2}x_n^2 + \varepsilon_{4,3}x_n^3 \end{cases} \tag{39}$$

$$\begin{cases} x_{n+1}^1 = 1 - 2\left|x_n^1\right| + k_1\left(\left(1 - \sum\limits_{j=3}^{p}\varepsilon_{1,j}\right)x_n^2 + \sum\limits_{j=3}^{p}\varepsilon_{1,j}x_n^j\right) \\ \vdots \\ x_{n+1}^m = 1 - 2\left|x_n^m\right| + k_m\left(\left(1 - \sum\limits_{j=1,j\neq m,m+1}^{p}\varepsilon_{m,j}\right)x_n^{m+1} + \sum\limits_{j=1,j\neq m,m+1}^{p}\varepsilon_{m,j}x_n^j\right) \\ \vdots \\ x_{n+1}^{p-1} = 1 - 2\left|x_n^{p-1}\right| + k_{p-1}\left(\left(1 - \sum\limits_{j=1}^{p-2}\varepsilon_{p-1,j}\right)x_n^p + \sum\limits_{j=1}^{p-2}\varepsilon_{p-1,j}x_n^j\right) \\ x_{n+1}^p = 1 - 2\left|x_n^p\right| + k_p\left(\left(1 - \sum\limits_{j=1}^{p-2}\varepsilon_{p,j}\right)x_n^1 + \sum\limits_{j=1}^{p-2}\varepsilon_{p,j}x_n^j\right) \end{cases} \tag{40}$$

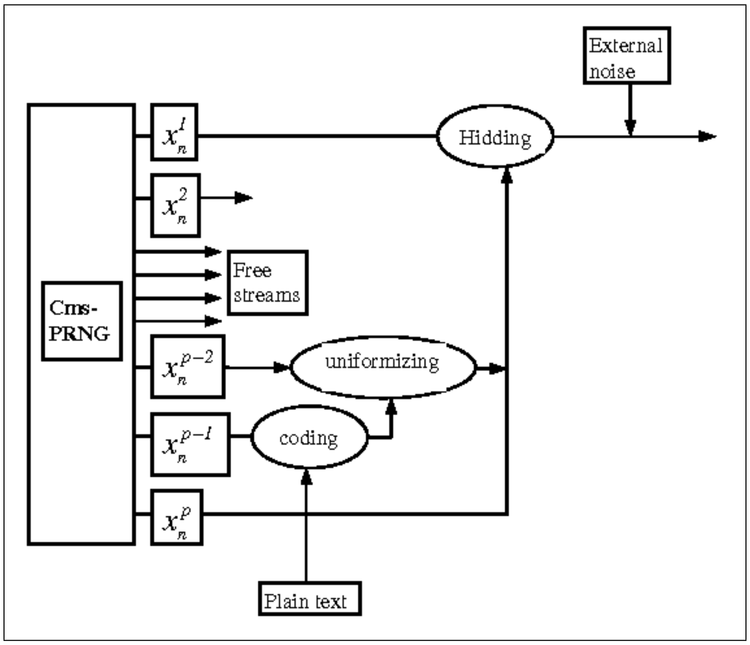


Fig. 18. Transmitter

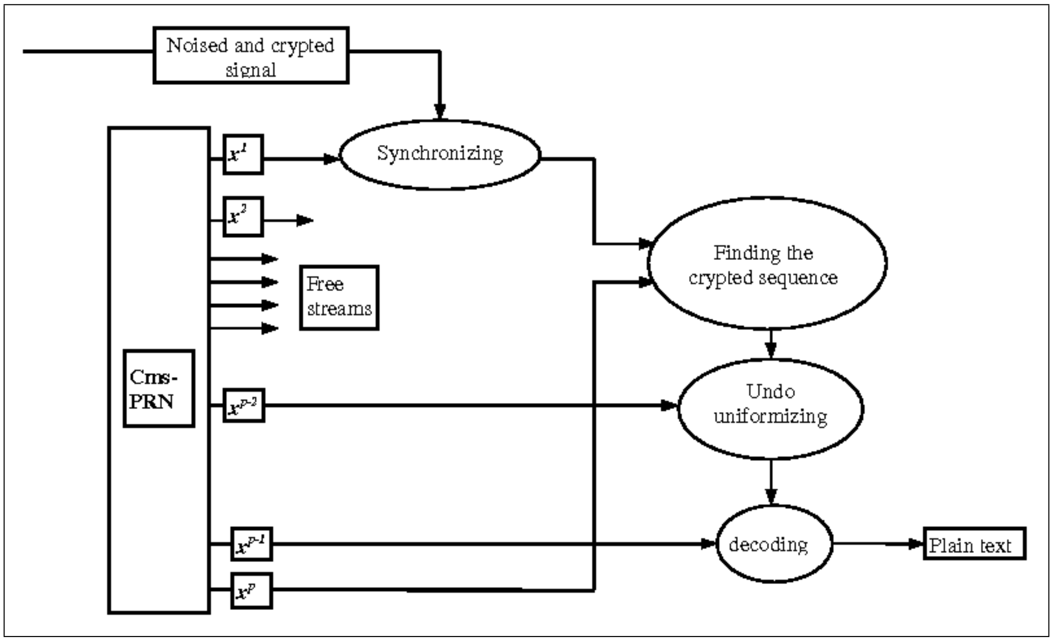


Fig. 19. Receiver

The ring coupling which is expressed as a diagonal matrix in Eq. 31 is completed with numerous other non vanishing coefficients of the matrix used as secret keys in Eq. 40. Then the originality of the noise-resisting ciphering method introduced which uses this Cms-PRNG is twofold. First a novel ciphering method is proposed aimed at resisting to a noisy transmission channel. 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 to restrict the bounds of the aforementioned intervals in order to precisely resist to the effects of the noise. An extra scrambling resorting to a co-generated chaotic sequence enhances the ciphering process. Then a new chaotic substitution method is developed: considering a chaotic carrier, belonging to the set of cogenerated and coupled pseudo-random chaotic sequences, the idea is to randomly/chaotically (in fact, this is determined by a second pseudo-random chaotic sequence) replace some elements of the carrier by a ciphered element (a letter here) of the message. At the receiver end, a copy of the Cms-PRNG, with the same parameters (hence we deal with a symmetrical ciphering method) allows to generate the necessary chaotic sequences and therefore to retrieve the initial message.

This process can be summarized in both circuits of Figs. 18, 19. Due again to the limited extend of this chapter, we cannot expand these figures in order to show the constituting symbols in each oval shaped region of the circuit. The originality of the method lies in the use of a chaotic pseudo-random number generator: several co-generated sequences can be used at different steps of the ciphering process, since they present the strong property of being uncorrelated. Each letter of the initial alphabet of the plain text is encoded as a subinterval of $[-1, 1]$. The bounds of each interval are defined in function of the known bound of the additive noise. A pseudo-random sequence is used to enhance the complexity of the ciphering. The transmission consists of a substitution technique inside a chaotic carrier, depending on another cogenerated sequence. The efficiency of the proposed scheme is illustrated on some numerical simulations.[2] As further work, some studies should be performed of several sets of unknown parameters, since with the considered Cms-PRNG with 10 states, the number of possible parameters amounts to 90 (the $\varepsilon_{i,j}$ and the k_i).

5. Conclusion

Following the worldwide tradition of use of 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, as an example, the building of new chaotic and random number generators. In this beginning of the third Millenium, the old tradition of design of electronic circuits is drastically revolutionized by the introduction by L. O. Chua of new components with memory, namely memristor, memcapacitor and meminductor. These devices are common at the nanoscale and their combination in circuits open up new functionnalities in electronics. Apart from the obvious use of these elements in nonvolatile memories, several applications can be already envisioned, especially in neuromorphic devices to stimulate learning, adaptative and spontaneous behavior.[7]

Alongside to this electronic circuits revolution, the new theory of mathematical circuits allows many new applications in chaotic cryptography, genetic algorithms in optimization and in control,... Due to the versatility of the new components we introduce, the combined operation of these chaotic mathematical circuits is still largely unexplored. We hope our work will motivate experimental and theoretical investigations in this direction. For the 75th birthday of Professor L. O. Chua, one can highlight that his seminal work since more than forty years is fruitful exceeding his wide-ranging field of research. In this chapter (as suggested in the title of the anniversary book) we followed him from chaos to memristor and we went beyond.

References

1. Aziz Alaoui, M. A.& Lozi, R., (1994), "Secure Communications via Chaotic Synchronization in Chua's Circuit: Numerical Analysis of The Errors of the Recovered Signal," in *Proc. Nonlinear Theory and its Application*, Kagoshima, Japan, 145-148.
2. Cherrier, E. & Lozi, R., (2011), "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.
3. Chua, L. O., Kumoro, M. & Matsumoto, T., (1984), "The Double Scroll Family," *IEEE Trans. Circuit and Systems*, **32** (11), 1055-1058.
4. Chua, L. O., (1992), "The genesis of Chua's Circuit," *AEÜ*, **46** (4), 250-257.
5. Chua, L. O., Kocarev, L., Eckert, K. & Itoh, M., (1992), "Experimental chaos synchronization in Chua's circuit," *Int. J. Bifurcation & Chaos*, **2** (3), 705-708.
6. Delgado-Restituto, M. & Rodriguez-Vasquez, A. (1993), "A CMOS monolithic Chua's circuit," *J. Circuits, Systems and Computerss*, **(3)** 2, 259-268.
7. Di Ventra, M., Pershin, Y. V. & Chua, L. O., (2009), "Circuit elements with memory: memristors, memca-

pacitors, and meminductors," *Proceedings of IEEE*, **97** (10), 1717-1724.

8. Duan, Z., Wang, J. and Huang, L. (2004), "Multi-input and multi-output nonlinear systems interconnected Chua's ciruits," *Int. J. Bifurcation & Chaos*, **14** (9), 3065-3081.
9. Espinel, A., Taralova, I. & Lozi, R. (2011), "Dynamical and Statistical Analysis of a New Lozi Function for Random Numbers Generation," in *Proceeding or Physcon 2011, León, Spain, 5-8 september.*, IPACS open Access Electronic Library.
10. Hénaff, S., Taralova, I. & Lozi, R. (2009a), "Observers design for a new weakly coupled map function", in *Conference Proceedings of ICCSA 2009, 3rd International Conference on Complex Systems and Applications*, June 29 - July 02, C. Bertelle, X. Liu, M.A. Aziz-Alaoui (Eds), 47-50.
11. Hénaff, S., Taralova, I. & Lozi, R., (2009b), "Dynamical Analysis of a new statistically highly performant deterministic function for chaotic signals generation", *IPACS Open Access Electronic Library, Physics and Control 2009.*
12. Hénaff, S., Taralova, I. & Lozi, R. (2010), "Exact and Asymptotic Synchronization of a new weakly coupled maps system", *Journal of Nonlinear Systems and Applications*, **1**, 3-4, 87-95.
13. Hénon, M., (1976), "A Two-dimensional mapping with a strange attractor," *Commun. Math. Phys.*, **50**, 69-77.
14. Kapitaniak, T., Chua, L. O. & Zhong, G.-H., (1994), "Experimental hyperchaos in coupled Chua's circuits," *IEEE Trans. Circuit and Systems*, **41** (7), 499-503.
15. Kocarev, Lj., Hale, K.S., Chua, L.O. & Parlitz, U., (1992), "Experimental demonstration of secure communication via chaotic synchronization," *Int. J. Bifurcation & Chaos*, **2** (3), 709-713.
16. Lorenz, E. N., (1963), "Deterministic nonperiodic flow," *J. Atmospheric Science*, **20**, 130-141.
17. Loskutov, A., Yu. & Popkova, A., V., (2011), "Stabilization of chaotic oscillations in systems with a hyperbolic-type attractor," *JETP Letters*, **94** (1), 86-90.
18. Lozi, R. & Chua, L.O., (1993), "Secure communications via chaotic synchronization II: noise reduction by cascading two identical receivers," *Int. J. Bifurcation & Chaos*, **3** (5), 1319-1325.
19. Lozi, R., (1995), "Secure communications via chaotic synchronization in Chua's circuit and Bonhoeffer-Van der Pol equation: numerical analysis of the errors of the recovered signal," *ISCAS'95, IEEE International Symposium on Circuits and Systems, April 30 - May 3 1995,* Vol. 1, 684 - 687.
20. Lozi, R., (2006),"Giga-periodic orbits for weakly coupled tent and logistic discretized maps," *Modern Mathematical Models, Methods and Algorithms for Real World Systems*, eds. A. H. Siddiqi, I. S. Duff & O. Christensen, (Anamaya Publishers, New Delhi, India), 80-124.
21. Lozi, R., (2008a), "New Enhanced Chaotic Number Generators", *Indian Journal of Industrial and Applied Mathematics,* Vol.1, no.1, 1-23.
22. Lozi, R., (2008b), "Chaotic Sampling, Very Weakly Coupling, and Chaotic Mixing: Three Simple Synergistic Mechanisms to Make New Families of Chaotic Pseudo Random Number Generators", in *6th EUROMECH Non Linear Dynamics Conference*, Saint-Petersburg, ENOC 2008, 30 June - 4 July 2008, IPACS open Access Electronic Library, 1715-1724.
23. Lozi, R. (2009), "Chaotic Pseudo Random Number Generators via Ultra Weak Coupling of Chaotic Maps and Double Threshold Sampling Sequences," in *Conference Proceedings of ICCSA 2009, 3rd International Conference on Complex Systems and Applications*, June 29 - July 02, C. Bertelle, X. Liu, M.A. Aziz-Alaoui, (Eds), 20-24.
24. Lozi, R., (2011),"Complexity leads to randomness in chaotic systems" *Mathematics in Science and Technology: Mathematical Methods, Models and Algorithms in Science and Technology.* Proceedings of the Satellite Conference of ICM, 15-17 August 2010 Delhi, India (A.H. Siddiqi, R.C. Singh, P. Manchanda Eds.), World Scientific Publisher, Singapore, 93-125.
25. Lozi, R., (2012),"Can we trust in numerical computation of chaotic solutions of Dynamical systems ?," in *Conference Proceedings of From Laser Dynamics to Topology of Chaos*, June 28 - 30, 2011, (Rouen), Ch. Letellier, (Eds), *In press.*
26. Matsumoto, T., (1984), "A chaotic attractor from Chua's circuit," *IEEE Trans.*, **CAS-31** (12), 1055-1058.
27. Oppenheim, A. L., Wornell, G. W., Isabelle, S. H. & Cuomo, K. M., (1992), "Signal processing in the context of chaotic signals," *Proc. 1992 IEEE ICASSP IV,* 117-120.
28. Rössler, O. E., (1976), "Chaotic behavior in simple reaction system," *Zeitschrift für Naturforschung*, **A 31**, 259–264.