IEICE Proceeding Series

Random Number Generation Based on the Rossler Attractor

Vincent Canals, Antoni Morro, Josep L. Rosselló

Vol. 1 pp. 272-275
Publication Date: 2014/03/17
Online ISSN: 2188-5079

2012 International Symposium on Nonlinear Theory and its Applications
NOLTA2012, Palma, Majorca, Spain, October 22-26, 2012

Random Number Generation Based on the Rossler Attractor

Vincent Canals, Antoni Morro and Josep L. Rosselló
Departament de Física, Universitat de les Illes Balears, Palma de Mallorca, Spain
Phone:+34 971 171 373 email: j.rossello@uib.es

Abstract— **A random number generator using a chaotic circuit is proposed and analyzed, for this purpose, a robust implementation of the Rôssler attractor is designed and measured. The chaotic circuit is designed to provide both a chaotic and a periodic binary output. The chaotic analogue circuit is connected to a digital system to provide random bit sequences.**

1. Introduction

Chaos refers to the impossibility of making accurate long-term predictions of the behavior of non-linear systems. During the last decades there has been a high interest in the design and analysis of chaotic systems given their parallelism with nature behavior. The fields of application include secure communications [1], robot control [2], and implementation of noise sources [3], frequently employed in speech processing applications or to test the dynamic behavior of electronic systems. Chaotic circuits are also used as random number generators for applications in the security domain of networks and wireless communications [4]. “Truly” random number generators may also be used for both analog and digital IC testing [5] and as an efficient and secure key generator. Electronics systems exhibiting a chaotic behavior can also be applied to optimization problems [6]. One of the most famous chaotic circuits is the Chua’s circuit [7,8] containing four linear elements (two capacitors, one resistor and one inductor) and a nonlinear resistor called Chua’s diode. An integrated implementation of Chua’s circuit was presented in [9] fabricated using a 2µm CMOS technology. Other researchers [10-12] also present different chaotic oscillators using inductances, resistors and nonlinear elements (similarly to Chua’s circuit).

In this work we present a robust implementation of the Rôssler attractor. This attractor is of special interest since it can be used to provide both analogue and digital signals that can be used for the design of an efficient random number generator.

The rest of this paper is organized as follows: in section II we show the basic principles of the proposed chaotic system, in section III we present the circuit design. Section IV shows the experimental results and finally, in section V we present the conclusions.

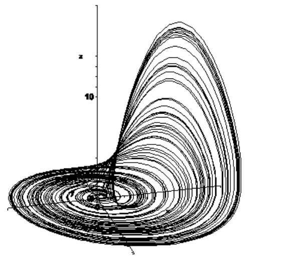
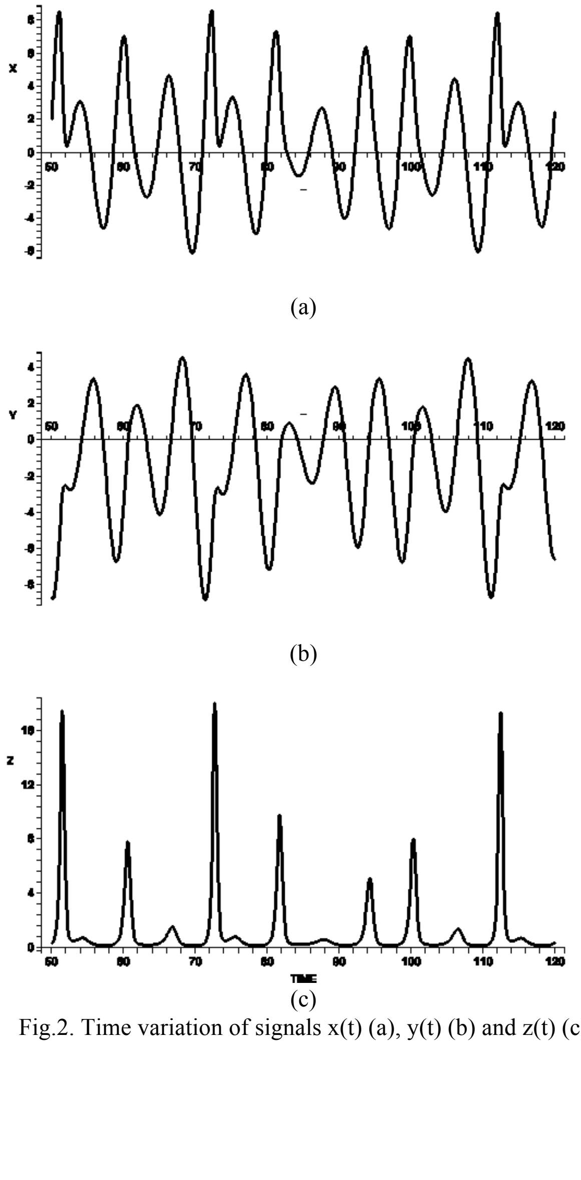


Fig.1. Rôssler Attractor behavior for a=0.38 b=1.5 c=5.



(a)

(b)

(c)

Fig.2. Time variation of signals x(t) (a), y(t) (b) and z(t) (c)

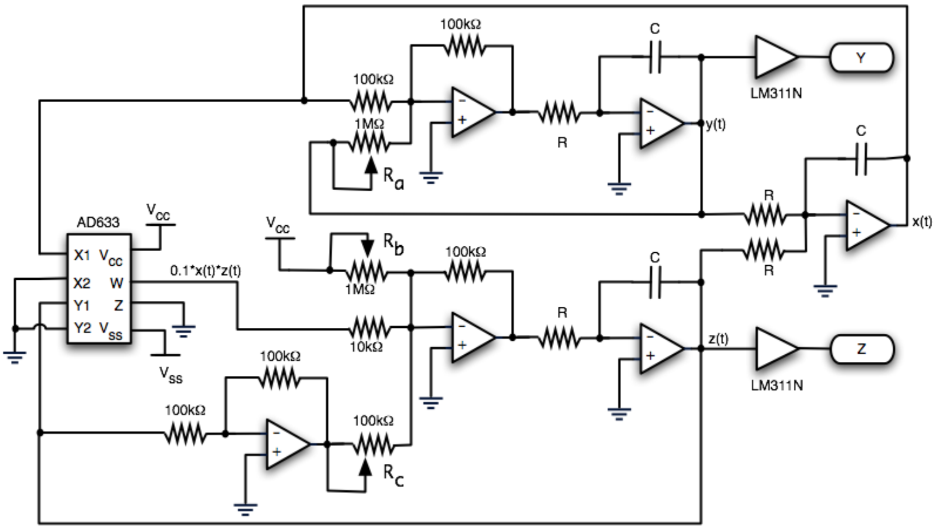


Fig.3. Circuit implementation of the Rôssler attractor

2. Basic Concepts

The Rôssler model [13] is characterized by three non-linear differential equations:

$$\dot{x} = -y - z$$
$$\dot{y} = x + ay$$
$$\dot{z} = b + (x - c)z$$

(1)

where x,y and z are time-varying parameters and a, b and c are constants. For some special values of the constants the system presents a chaotic behavior (Fig.1 and 2) . It should be remained that chaotic models defy all analytical methods and present a rich and complex dynamic behavior. These systems are characterized by its sensitivity to initial conditions that implies that two virtually identical starting points in the attractor will present very different values in the future.

The Rôssler system has some properties that are important to be highlighted. Both the x(t) and the y(t) signals have a fixed frequency of oscillation if z is fixed to zero, with value:

$$\omega = \frac{a}{2}\sqrt{\frac{4}{a^2} - 1}$$

(2)

As can be appreciated in Fig. 2, for some values of the constants in which a chaotic behavior is present, the z value remains to zero except for several cases in which x(t) and y(t) are close to a minimum. The presence of a peak in the z(t) signal is unpredictable. This special property of z(t) will be used to generate random digital numbers.

3. Circuit implementation

We implemented the Rôssler model using the circuit shown in Fig. 3. The main novelty of the proposed circuit relays on the usage of an analog multiplier as the non-linear feedback element. The circuit of Fig. 3 implements the following differential equations:

$$RC\dot{x} = -y - z$$
$$RC\dot{y} = x + \frac{100k\Omega}{R_a}y$$
$$RC\dot{z} = V_{CC}\frac{100k\Omega}{R_b} + \left(x - \frac{100k\Omega}{R_c}\right)z$$

(3)

Where x, y and z are the voltages values at the three nodes indicated in Fig. 3. The parameter RC defines the time speed of the system (for the fabricated circuit we selected RC=100μs), and the OAs supply voltage is set to V_{CC}=15V and V_{SS}=-15V. The resistance values R_a, R_b and R_c are used to set parameters a, b and c in (1) so that we get

$$a = \frac{100k\Omega}{R_a}$$
$$b = 15\frac{100k\Omega}{R_b}$$
$$c = \frac{100k\Omega}{R_c}$$

(4)

From y(t) and z(t) we generate two digital signals Y and Z respectively. A voltage comparator LM311N provide two logic levels fixed to 3.3V (H) and 0V(L) when the signal considered is over a specific voltage reference. The two threshold voltages were V_{ref}=0V and 1.3V for y(t) and x(t) respectively. The outputs of these two comparators are labeled as Y and Z. Y is nearly a regular signal with a frequency of oscillation equal to:

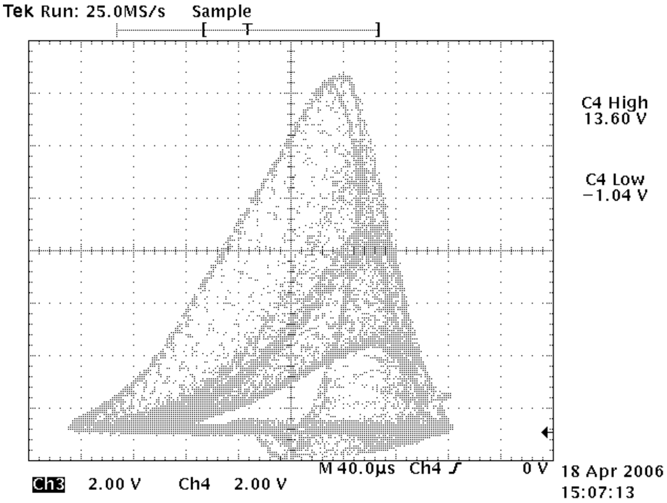


Fig. 4 Rôssler attractor behavior (y(t) vs. z(t)) for a=0.38 b=1.5 c=5.

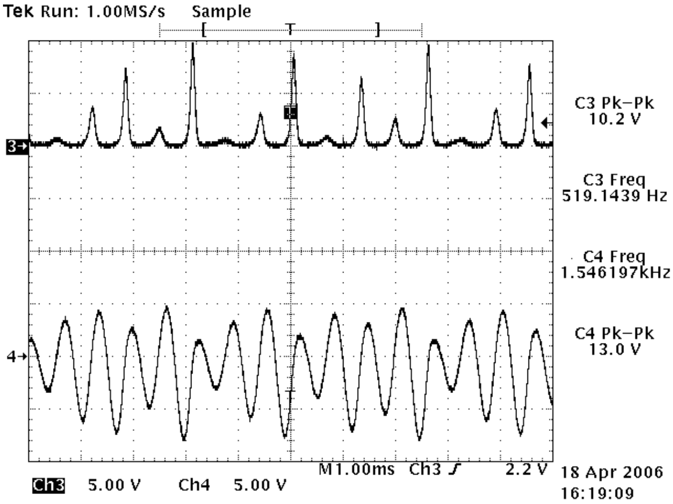


Fig. 5 Measured analog signals z(t) and y(t).

$$f = \frac{a\sqrt{\frac{4}{a^2}-1}}{4\pi RC} \tag{5}$$

The signal Z is an unpredictable digital signal. During the oscillation period of Y, the Z value is LOW or may present a single glitch (see Fig. 6).

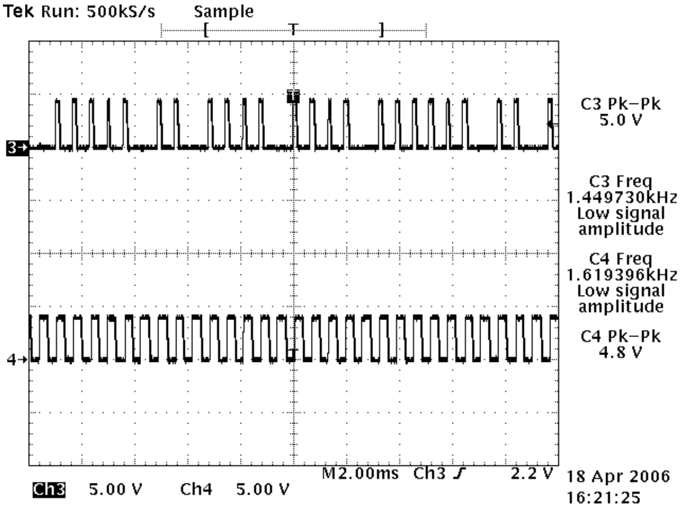


Fig. 6 Measured digital signals Z and Y

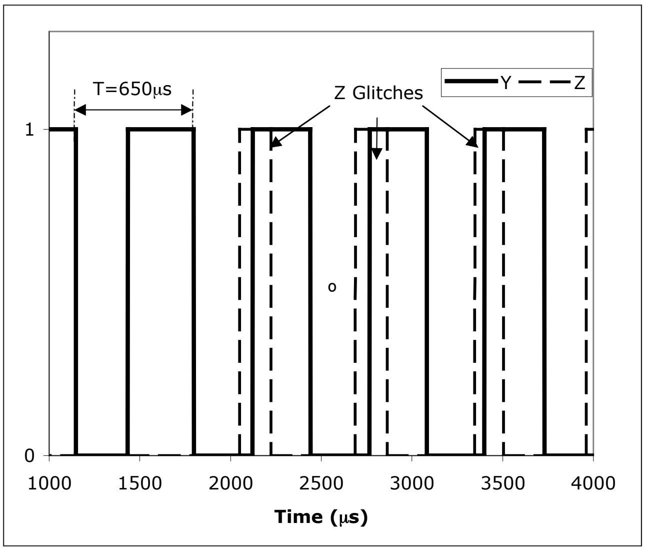


Fig.7 Temporal variation of digital signals Y and Z.

4. Experimental results

We fixed the variable resistances to R_a=263kΩ, R_b=1MΩ and R_c=20kΩ, leading to the values a=0.38, b=1.5 and c=5. For this case we obtain a chaotic behavior like the one shown in Fig. 4. The measured signals z(t) and y(t) that are very similar to those shown in Fig. 2 (see Figs. 4 and 5). The digital signals Z and Y extracted from z(t) and y(t) are shown in Figs.6 and 7. The presence of peaks in the Z signal during the clock period defined by Y is unpredictable. The Y signal is nearly regular with a frequency found to be 1.6kHz, that is in accordance with the frequency of 1.56kHz predicted by expression (5) (see Fig. 6).

The Y signal may be used to capture the presence or absence of the peak in the Z signal and therefore to store it into a register (see Fig.8). The functionality of the two flip-flops and the XOR gate is to capture, in the shift register, the presence (a_i=1) or absence (a_i=0) of the peak in the Z value during a cycle in the Y value.

We computed the autocorrelation of the stored digital signal, as it provides information about the similarity of a digital signal a_i to itself evaluated at time $i+k$ (a_{i+k}). We define the autocorrelation of a digital signal as follows:

$$C(k) = \left| \sum_{i=1}^{N-k} a_i \otimes a_{i+k} - \sum_{i=1}^{N-k} a_i \oplus a_{i+k} \right| \tag{6}$$

Where operators ⊗ and ⊕ are the XNOR and XOR logic operators respectively.

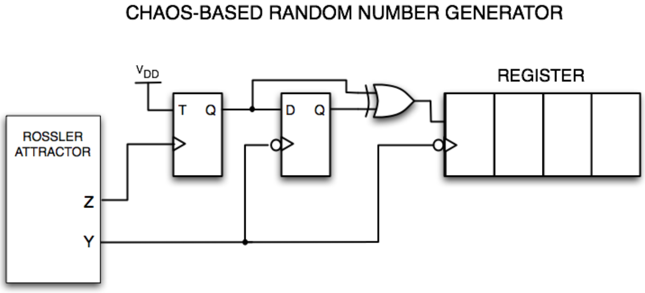


Fig. 8 A chaos-based random number generator is easily constructed from the digital output signals provided by the Rôssler attractor Z and Y.

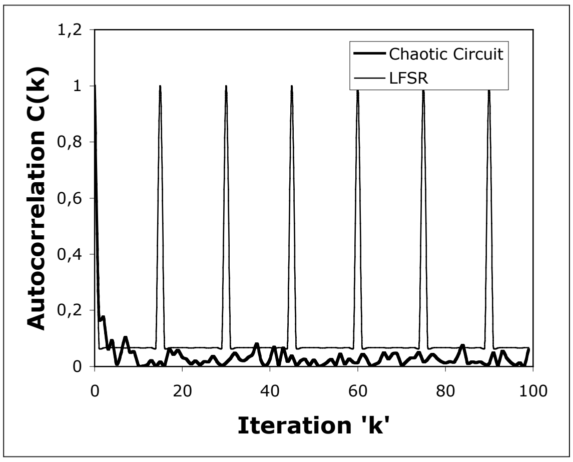


Fig. 9. Autocorrelation of the digital output Z and a 4-bit LFSR.

A periodic signal with period *K* has a correlation function *C(K)=1* while a random signal with a 50% of probability of being HIGH or LOW has a correlation function *C(k)=0 ∀k>0*. In Fig. 9 we show a comparison of the correlation functions between the digital output provided by the random number generator of Fig.8, and the output of a 4-bit LFSR. It is shown that the LFSR has a small correlation value except when *k* is a multiple of the LFSR period (*C(n•15)=1* for the case of the 4-bit LFSR). As is shown in Fig. 9, the proposed circuit provides lower values for *C(k)* when compared to the LFSR with the added value of not showing the repetition period observed in LFSRs.

5. Conclusions

An efficient chaos-based random number generator is proposed and experimentally evaluated. A circuit implementation of the Rôssler system is developed and adapted to generate a random digital signal. The generated chaotic signal presents a negligible value of the autocorrelation function for any period of repetition 'k'. The chaotic signal does not present any predefined sequence of repetition.

Acknowledgment

This work was supported in part by the European Development Funds (FEDER) and in part by the Spanish Ministry of Economy and Competitiveness under project TEC2011-23113

References

[1] J. Wu, J. Hou, Y. Zhang and T. Wang, "Secure communications via synchronized chaotic circuit," in *Proc. Int. Conf. on Signal Processing vol. 2,* Beijing, 2002, pp. 1552-1555.

[2] A.J.K Klomkarn, P Sooraksa "Further investigation on trajectory of chaotic guiding signals for robotic systems," in *Proc. Int. Symp. On Communications and Information Technologies,* Sapporo, Japan, 2004, vol. 2, pp. 1166-1170.

[3] M. Delgado-Restituto, A. Rodriguez-Vazquez, "Integrated chaos generators," *Proceedings of the IEEE*, vol. 90, pp. 747-767, May 2002.

[4] C.C. Wang, J.M. Huang, H.C. Cheng, R. Hu, "Switched-current 3-bit CMOS 4.0-MHz wideband random signal generator," *IEEE J. Solid-State Circuits*, vol. 40, pp. 1360-1365, June 2005.

[5] M.J. Bellido, A.J. Acosta, M. Valencia, A. Barriga and J.L. Huertas, "Simple binary random number generator," *Electronics Lett.*, vol. 28, no. 7, pp. 617-618, March 1992.

[6] T. Tanaka and E. Hiura, "Dynamic behavior of a chaotic neural network and its application to optimization problems," in *Proc. Int. Joint Conf. on Neural Networks*, Montreal, Canada, 2005, pp. 753-757.

[7] L.O.Chua, "The Genesis of Chua's circuit," *Int. J Electronics Communications*, vol 46, pp. 250-257, 1992.

[8] T. Matsumoto, "A Chaotic Attractor from Chua's Circuit," *IEEE Trans. Circuits Syst*., vol CAS-31, no. 12, pp. 1055-1058, Dec. 1984.

[9] J.M Cruz and L.O. Chua, "An IC Chip of Chua's Circuit," *IEEE Trans. Circuits Syst II.* , vol 40, no. 10, pp. 614-625, Oct. 1993.

[10] Y. Hosokawa et. al."A Design Method of Chaotic Circuits using an Oscillator and a Resonator" In *Proc. International Symposium on Circuits and Systems 2001*, vol III, pp. 373-376.

[11] H Nakano et. al."A Simple Nonautonomous Chaotic Circuit with a Periodic Pulse-Train Input" In *Proc. International Symposium on Circuits and Systems 2003*, vol III, pp. 108-111.

[12] A.S. Elwakil "Nonautonomous pulse-driven chaotic oscillator based on Chua's circuit" In *Proc. International Symposium on Circuits and Systems 2003*, vol III, pp. 136-139.

[13] Rôssler, "An Equation for continuous chaos" Phy. Lett. A, 57, pp. 397-398, 1976.