World Journal of Engineering Research and Technology
WJERT
www.wjert.org
SJIF Impact Factor: 4.326

A NEW CHAOTIC ATTRACTOR FOR RANDOM NUMBER GENERATION BASED ON MEMRISTIVE CIRCUIT

Zehra Gülru Çam Taşkıran*, Murat Taşkıran, Nihan Kahraman and Herman Sedef

Yildiz Technical University, Davutpasa Campus, Electronics and Communications Department, 34220, Esenler, Istanbul, Turkey.

Article Received on 03/11/2017 **Article Revised on 24/11/2017** **Article Accepted on 15/12/2017**

***Corresponding Author**
Zehra Gülru Çam Taşkıran
Yildiz Technical University, Davutpasa Campus, Electronics and Communications Department, 34220, Esenler, Istanbul, Turkey.

ABSTRACT

In this study, the well-known chaotic circuit, Muthuswamy-Chua circuit, is used with a different memristor element and obtained a new chaotic attractor. Equilibrium points, lyapunov exponents, phase portraits and bifurcation diagrams of the new ODE system is analysed mathematically. Obtained chaotic signals are sampled by a low-frequency sampling clock and formed number sequence is numerically tested for randomness. According to test results, the proposed circuit can be used as pseudo random number generator at various applications such as criptology, modulator design and steganography.

KEYWORDS: chaos, attractor, memristor, Muthuswamy- Chua circuit, random number generator.

INTRODUCTION

Memristor is a two-terminal passive element which is firstly defined at 1971 by Leon Chua.[1] Memristor provides the functional relationship between charge and flux. When Stanley Williams group from HP Lab has built a nano scale TiO_2 component[2] which have properties explained by the memristor theory, an interest in using the memristor for potential applications, such as sensors, memory devices,[3] cellular neural networks,[4] analog circuits,[5] and chaotic circuits,[6] has increased among scientists worldwide.

Chaos does not yet have a universally accepted definition. The commonly accepted definition is systems that produce periodic outputs that are sensitive to initial conditions. A well-known chaotic structure is Muthuswamy-Chua circuit.[7] In the mentioned study, Chua diode in the Chua circuit is replaced with a memristor and a double scroll chaotic attractor is realized. After that, lots of study have taken part in the literature as memristor based chaotic circuit.[8]

PROPOSED MEMRISTOR ELEMENT

For this study, it is assumed a memristor that provides the relation given in Eq. 1.

$$M(t) = \frac{v(t)}{i(t)} = \frac{k_1}{\varphi(t) + k_2}$$

If k_1 chosen as 110 and k_2 chosen as 0.0047, and trigger voltage v(t) is taken as a sinusoidal voltage source with amplitude as 1.2V and frequency with 40 Hz, memristance equation is obtained as a fifth-order polynomial as Eq. 2.a. If the frequency is decreased, order of the memristance polynomial is also decreased. For 120 Hz, a fourth-order polynomial is obtained as in Eq. 2.b. and for 500 Hz, a third-order polynomial is obtained as in Eq.2.c.

$$M(\phi) = -3.9912e14\varphi^5 + 1.1212e13\varphi^4 - 1.3417e11\varphi^3 + 9.559e8\varphi^2 - 5.0735e6\varphi + 2.4219e4$$

$$M(\phi) = 1.5428e13\varphi^4 - 1.7369e11\varphi^3 + 1.0478e9\varphi^2 - 5.1397e6\varphi + 2.4226e4$$

$$M(\varphi) = 9.0461e8\varphi^2 - 0.0511e8\varphi + 0.0002e8$$

The characteristic hysteresis curves of the memristor element obtained according to the proposed equation and given parameters are given in Fig.1. According to this, when the element frequency increases, it becomes a hysteresis loop which lobe area reduced and it is suitable to be defined as a memristor.[9]

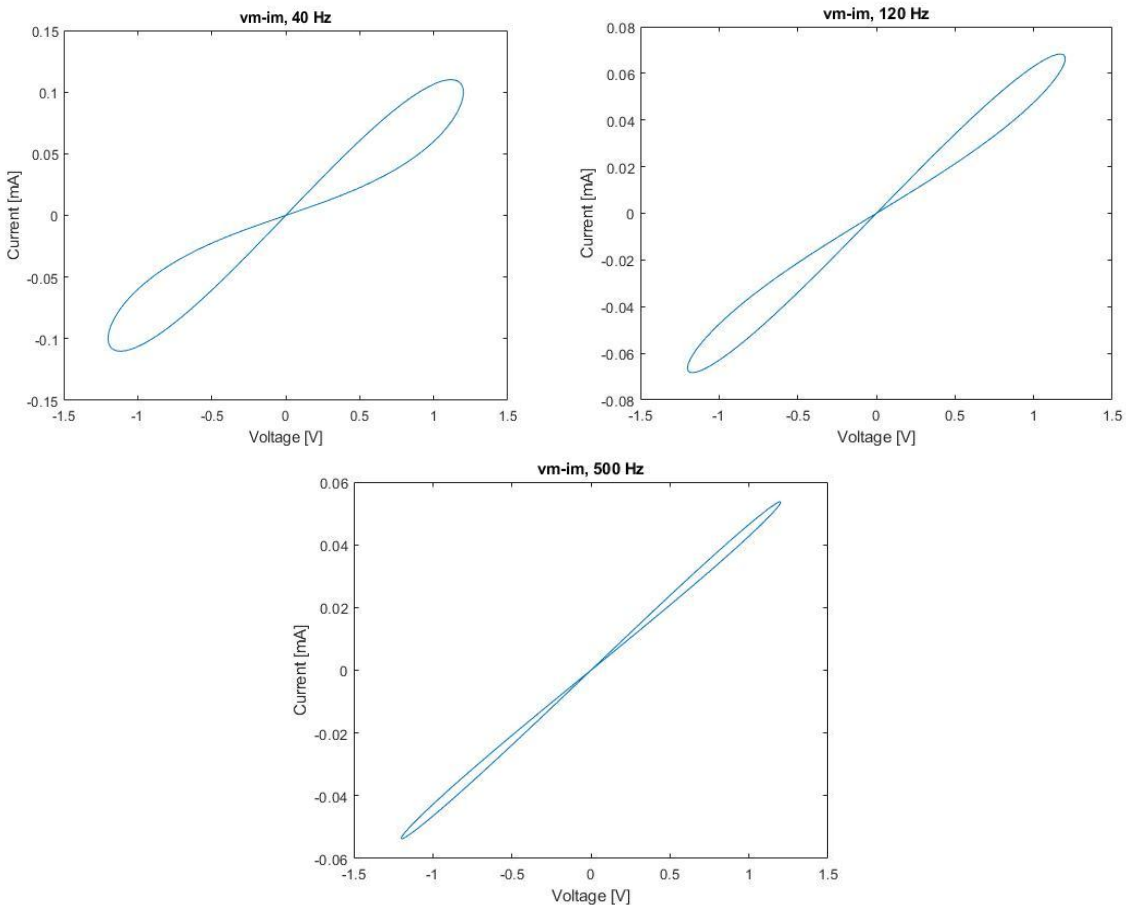

Figure 1: Characteristic pinched histeresis curves of the defined memristor element for a. 40 Hz, b. 120 Hz, C. 500 Hz.

It is thought that this system will allow different Chua circuits by producing polynomials at different non-linearity levels.

THEORETICAL ANALYSIS OF THE CIRCUIT

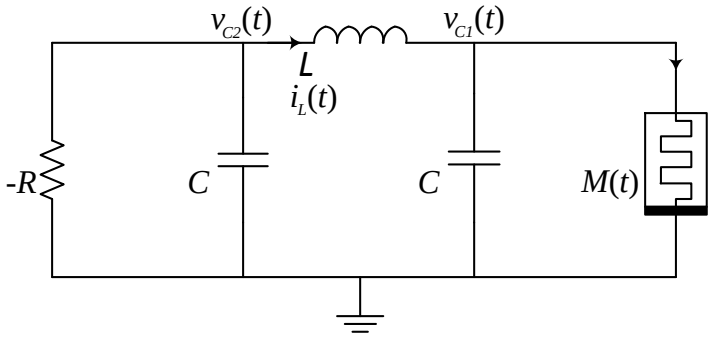

Figure 2: Proposed chaotic circuit topology.

The state equations of the circuit given in Fig.2 are obtained as in Eq. 3.

$$\dot{v_{C1}} = \frac{1}{C_1} i_L(t) - \frac{v_{C1}(t)}{C_1 k_1}(\varphi(t) + k_2)$$

$$\dot{i_L} = \frac{1}{L} v_{C2}(t) - \frac{1}{L} v_{C1}(t)$$

$$\dot{v_{C2}} = -\frac{1}{RC_2} v_{C2}(t) - \frac{1}{C_2} i_L(t)$$

$$\dot{\varphi} = v_{C1}(t)$$

For the calculation simplicity, circuit constants are parametrized as $v_{C1} = x_1,\ i_L = x_2, v_{C2} = x_3,\ \varphi = x_4, \frac{1}{C_1} = a_1,\ \frac{1}{RC_1} = a_2, \frac{1}{L} = a_3,\ \frac{1}{C_2} = a_4, \frac{1}{RC_2} = a_5.$

According to these parameters, the Jacobian matrix is as Eq. 4.

$$J = \begin{bmatrix} \frac{\partial \dot{x_1}}{\partial x_1} & \frac{\partial \dot{x_1}}{\partial x_2} & \frac{\partial \dot{x_1}}{\partial x_3} & \frac{\partial \dot{x_1}}{\partial x_4} \\ \frac{\partial \dot{x_2}}{\partial x_1} & \frac{\partial \dot{x_2}}{\partial x_2} & \frac{\partial \dot{x_2}}{\partial x_3} & \frac{\partial \dot{x_2}}{\partial x_4} \\ \frac{\partial \dot{x_3}}{\partial x_1} & \frac{\partial \dot{x_3}}{\partial x_2} & \frac{\partial \dot{x_3}}{\partial x_3} & \frac{\partial \dot{x_3}}{\partial x_4} \\ \frac{\partial \dot{x_4}}{\partial x_1} & \frac{\partial \dot{x_4}}{\partial x_2} & \frac{\partial \dot{x_4}}{\partial x_3} & \frac{\partial \dot{x_4}}{\partial x_4} \end{bmatrix} = \begin{bmatrix} -a_1(x_4 + k_2)/k_1 & a_1 & 0 & -a_1 x_1/k_1 \\ -a_3 & 0 & a_3 & 0 \\ 0 & -a_4 & -a_5 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

Therefore the equilibrium points of the system are obtained as [*a*, 0, 0, 0], when *a* is a constant value. The system has infinite number of equilibrium points.

For the analysis chosen parameters are

$a_1 = 5.5556,\ a_2 = 26.7867,\ a_3 = 10,\ a_4 = 3.5,\ a_5 = -5.5,\ \ k_1 = 0.2074,\ \ \ k_2 = -5.5.$

When these parameters and the characteristic polynomial of the circuit are examined, there is one pole in the left half s-plane, one pole on the origin, and two conjugate poles right half s-planes. So, these points can be called unstable saddle focuses.[10] When the initial conditions are chosen as [0.1, 0, 0, 0.1], obtained time series are given in Fig. 3.

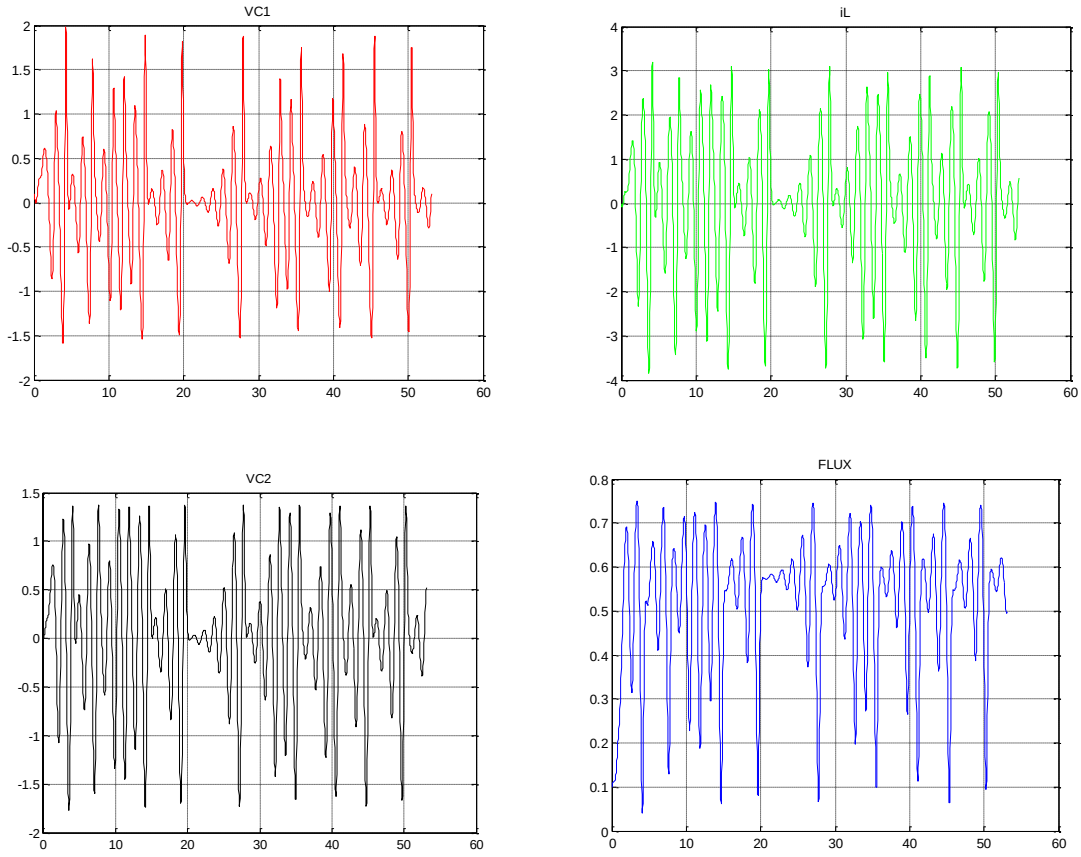

Figure 3: Time series of obtained 4 chaotic signals, a. v_{c1}, b. i_L, c. V_{c2}, d. Flux.

When $\nabla V < 0$ is satisfied, the system supports chaotic attractors. If $\nabla V = 0$, circuit is conservative. If $\nabla V > 0$, the phase space volume expands continuously. These conditions and parameters provide ∇V <0.[11]

In these system $\nabla V = \frac{dx_1}{x_1} + \frac{dx_2}{x_2} + \frac{dx_3}{x_3} + \frac{dx_4}{x_4} = -a_2(x_4 + k_2) - \frac{1}{RC_2} < 0$ is saitsfied and verified that system supports chaotic attractors.

Phase portraits and chaotic attractors obtained by taking the projections of state variables according to each other are given in Fig.4.

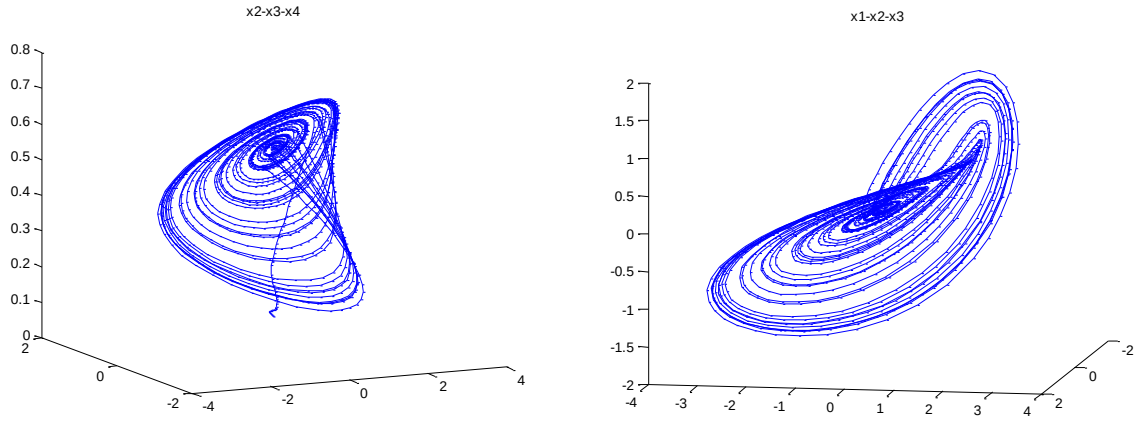

Figure 4: Phase portraits for a. x2-x3-x4 b. x1-x2-x3.

In each cycle, lyapunov exponents, which express how far the orbits are separated from each other, are thus given as the greatest indicator of chaos determination in Fig. 5. The fact that the greatest exponent is always positive confirms the existence of chaos. Accordingly, the existence of chaos in the circuit is confirmed by this metric.

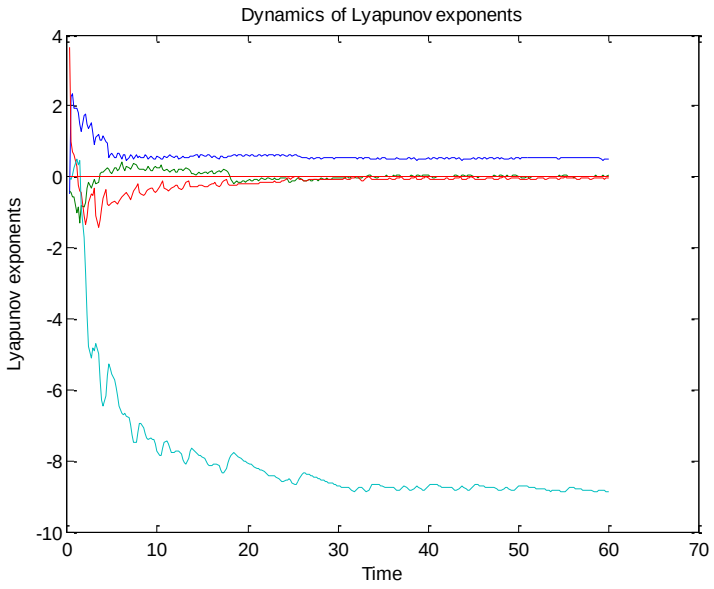

Figure 5: Maximum Lyapunov exponent is positive when the system is chaotic.

Figure 6 shows the bifurcation when flux passes through equation line in x_4-x_3 plane.

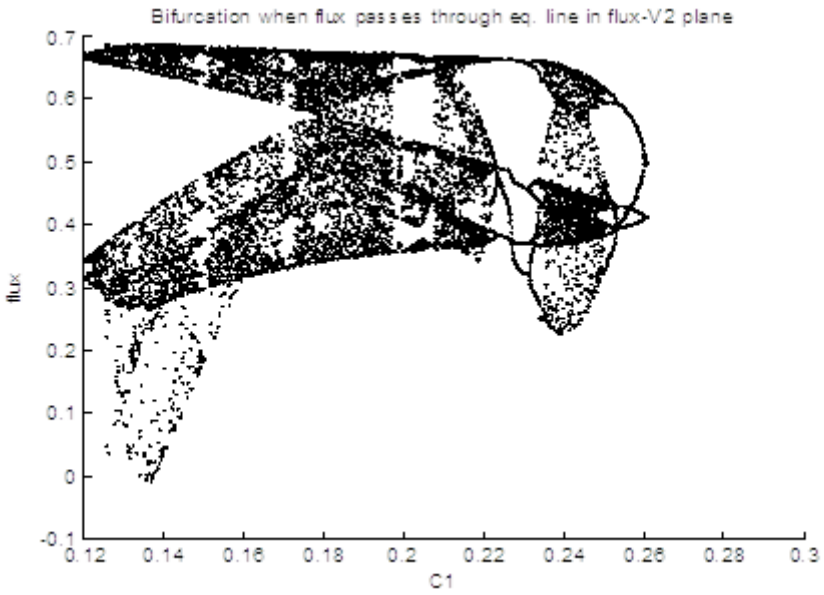

Figure 6: Bifurcation diagram shows the x_4 state variable with respect to normalized C_1 value.

NUMERİCAL TESTS FOR RANDOMNESS

Runs Test

This tests the number array according to a hypothesis for randomness, starting from the ratios of increases and decreases in the number sequence produced. Thus, when the obtained *h* parameter is '0', it is said that the null hypothesis is rejected and a metric is obtained that it is random. The chaotic signals obtained with the same initial conditions mentioned above are sampled with a sampling frequency of 2 Hz, and when this test is performed, the parameter *h* is obtained as '0'. In other words, the number sequence is random according to this test.

0.1 Test

A 0-1 test, as recommended by Gottwald-Melbourne,[12] was performed to assess whether the produced signal was chaotic. Expressions used to obtain the dimensionless variables *p* and *q*;

$$p(n) = \sum_{j=1}^{n} x(j)cosjc$$

$$q(n) = \sum_{j=1}^{n} x(j)sinjc$$

Where *c* is a randomly selected number between 0 and π. The number of data points received in the chaotic signal is expressed by *n*. The mean quadratic displacement *M(n)*, if the system is chaotic, will be linearly increasing.

$$M(n) = \lim_{n\to\infty} \frac{1}{n} \sum_{j=1}^{n} [p_c(j+n) - p_c(j)]^2 + [q(j+n) - q_c(j)]^2$$

Asymptotic growth rate K;

$$K = \lim_{n\to\infty} \frac{\log M(n)}{\log n}$$

If the *K* constant is close to 1, the sign is chaotic. If it is close to 0, it is periodic.

The *K* constant obtained by sampling the chaotic signal according to the given parameters with 2 Hz sampling frequency is 0.9663. The change in mean square displacement over time is also given in Fig. 7.a. When this graph is obtained, the parametres change according to the randomly selected *c* values as in Fig.7.b.

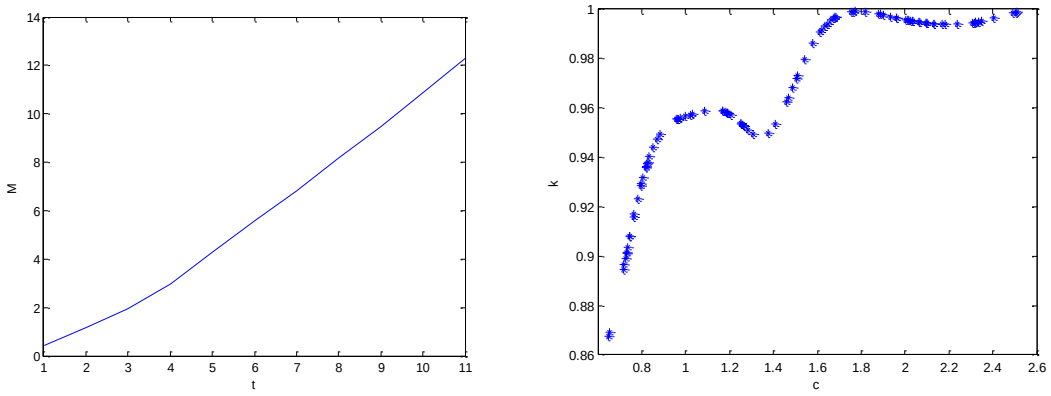

Figure 7: a. Average squared displacement curve from 0-1 Test b. Asymptotic growth rate according to randomly selected c value in 0-1 Test.

Autocorrelation Test

If two number sequences are independent of each other, there is no correlation between them. If the number sequence obtained is not periodic, the autocorrelation coefficients of this sequence should also be small except for the value '0'. For this, two chaotic signals with different initial conditions were produced with the same parameters, and again with 2 Hz.

1. $[v_{c1}(0)\ i_L(0)\ v_{c2}(0)\ \phi(0)]=[0.1\ 0\ 0\ 0.001]$
2. $[v_{c1}(0)\ i_L(0)\ v_{c2}(0)\ \phi(0)]=[0.07\ 0\ 0.0002\ 0.0008]$

Moreover, the two chaotic signals produced with different initial conditions must not correlate with each other.

These two conditions have been tested with the two signals produced and it is seen that it is as expected. The results obtained are given in Fig. 8.

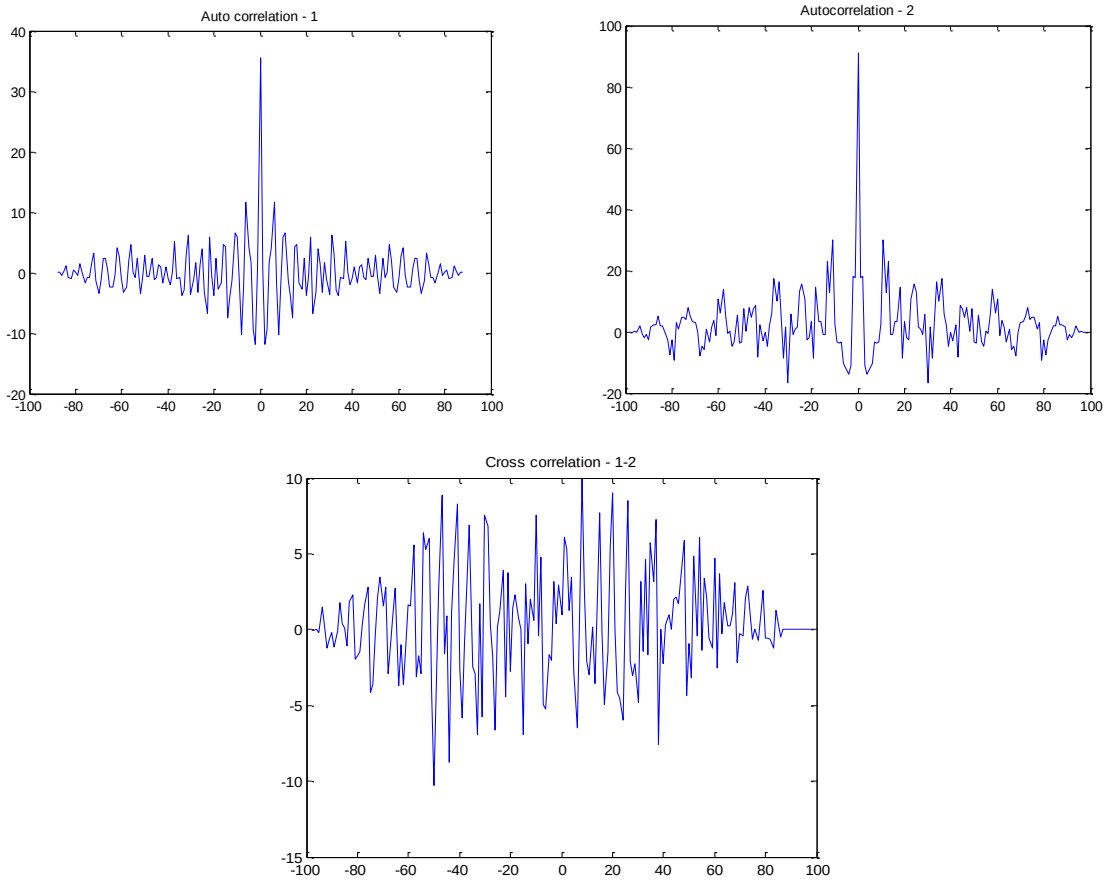

Figure 8: a. b. Autocorrelation of sampled signals to denormal and c. cross correlation.

As a result of all these analyzes, it has been proved that random signs are obtained with the designed chua circuit.

RESULTS AND CONCLUSION

In this study, a new chaotic attractor was designed using well-known Chua circuit with a defined memristor element and attempted to obtain random numbers from the chaotic attractor. The memristive behavior of the described element is confirmed by pinched hysteresis loop curves. The chaotic behaviour are verified by Lyapunov exponents, bifurcation diagram and phase-portraits. The fact that the memristor element can be implemented at different non-linearity levels can also allow the formation of different attractors with the same structure. Numerical tests show that low frequency sampled chaotic signals can be used as random numbers. All analyzes on the run were made with normalized values. All parameters must be denormalized for physical implementation of the circuit. The

new random number generator can be used in cryptology, secure communications and steganography areas.

REFERENCES

1. Chua L. O., "Memristor — The missing circuit element," IEEE Trans. Circuit Th. CAT, 1971; 18: 507–519.
2. Strukov D. B., Snider G. S., Stewart D. R., and Williams S. R., "The missing memristor Found", Nature, 2008; 453(7191): 80-83.
3. Ebong I. E. and Mazumder P., "Self-controlled writing and erasing in a memristor crossbar memory", IEEE Trans. Nanotechnol., 2011; 10(6): 1454-1463.
4. Kim H., Sah M.P., Yang C., Roska T. and Chua L.O., "Neural Synaptic Weighting With a Pulse-Based Memristor Circuit", IEEE Transactions on Circuits and Systems I: Regular Papers, 2012; 59(1): 148-158.
5. Fouda M.E., Khatib M.A., Mosad A.G. and Radwan A.G., "Generalized Analysis of Symmetric and Asymmetric Memristive Two-Gate Relaxation Oscillator", IEEE Transactions on Circuits and Systems I: Regular Papers, 2013; 60(10): 2701-2708.
6. Iu H.H.C., Yu D.S., Fitch A.L., Sreeram V. and Chen H., "Controlling Chaos in a Memristor Based Circuit Using a Twin-T Notch Filter", IEEE Transactions on Circuits and Systems I: Regular Papers, 2011; 58(6): 1337-1344.
7. Muthuswamy B., "Implementing memristor based chaotic circuits," International Journal of Bifurcation and Chaos, 2009; 20: 1335-1350.
8. Yener Ş. C., Kuntman H., "Fully CMOS Memristor Based Chaotic Circuit", Radıoengıneerıng, 2014; 23(4): 1140-1149.
9. Adhikari S.P., Sah M.P., Kim H. and Chua,L.O., "Three Fingerprints of Memristor", Ieee Transactions On Cırcuıts And Systems—I: Regular Papers, 2013; 60(11).
10. Maciej J Ogorzalek, "Chaos and Complexity in Nonlinear Electronic Circuits", World Scientific Series on Nonlinear Science Series A, 1997; 22.
11. Hilborn R C., "Chaos and Nonlinear Dynamics—An Introduction for Scientists and Engineers." Oxford, United Kingdom: Oxford University Press, 1994.
12. Gottwald G. A. and Melbourne I., "On the Implementation of the 0–1 Test for Chaos", SIAM Journal on Applied Dynamical Systems, 2009; 8(1).