Algerian Journal of Research and Technology
https://doi.org/10.58681/ajrt.24080104
A.J.R.T Volume 8 (N°1) (2024) 27 - 41

Study and practical implementation of a CHUA circuit synchronized between Master-Slave

F. Benkhedir[1]*, N. Hadj Said[1], A. Ali Pacha[1], M. Maamri[2]

[1] *Laboratory of Coding and Security of Information.*
University of Sciences and Technology of Oran Mohamed Boudiaf PoBox 1505 Oran M'Naouer 31000 Algeria
[2]*LABGET Laboratory, Department of Electrical Engineering Larbi Tebessi University-Tebessa, Tebessa, Algeria.*

***Corresponding author:** fairouz.benkhedir@univ-usto.dz,*

Received. December 20, 2023. Accepted. February 15, 2024. Published May 15, 2024.

DOI: https://doi.org/10.58681/ajrt.24080104

Abstract. The Chua circuit is a simple classical electronic circuit exhibiting chaotic behaviour and considered as a true paradigm of chaos in the real world. In this paper, we propose an innovative practical implementation of two Chua circuits in master-slave configuration using the OrCAD environment.
An original procedure allowing the mutual synchronisation of these two circuits is developed and experimentally validated. The detailed study of the synchronised behaviour reveals interesting cryptographic properties, in particular a high sensitivity to initial conditions. A final demonstrator consisting of the two synchronised circuits is then produced, characterised and exploited to extract relevant information for innovative chaos-based cryptographic applications.
This work opens up promising prospects for the practical use of the Chua circuit, a recognised simple chaotic system, in the development of advanced cryptographic approaches exploiting the unique properties of synchronised chaotic systems.

Keywords. Chua circuit, Synchronization, Chaos Signals, Chua attractor, Tthe double scroll.

INTRODUCTION

Today, the generation of random signals is crucial in many fields, particularly chaotic cryptography. This involves superimposing the original data with a chaotic signal, then transmitting the resulting signal.

Chaos theory is one of the three major scientific breakthroughs of the 20th century, alongside information theory and control theory, according to logician Daniel Parrochia.

Since Edward Lorenz revealed chaos theory in the 1960s, it has found numerous applications, notably in materials science, chemistry and finance, as well as a growing number of uses in electronic devices, particularly for cryptography and secure communications.

Since 1981, when a basic RLD circuit was revealed to be capable of causing chaotic dynamics in electronic systems, it has been a source of fascination (Linsay, 1981).

In 1983 Chua and Matsumoto designed the first autonomous chaotic electronic circuit. The Chua circuit is an electronic chaotic oscillator portrayed by a system of non-linear elements with three coupled first-order differential conditions. The Chua circuit may be a basic, non-linear, independent electrical circuit that shows an assortment of energetic practices, counting chaos, which has been tentatively affirmed (Chua al., 1986).

In 2010 Alexander Jimenez-Triana and others developed a method for controlling chaos by applying periodic impulsive parametric disturbances (Jimenez-Triana et al., 2010).

Today, other chaos-based cryptographic schemes have been proposed by researchers in this field. Some notable examples include:

In 2007 , Adnan Abdul-Aziz Gutub focused on improving an earlier evolutionary inversion hardware architecture proposed in 2004 for the finite field GF(p), whose architecture comprises two parts - a computation unit and a memory unit.

In 2009, Loai Ali Tawalbeh and al proposed a new high-speed, high-throughput crypto-processor architecture for elliptic curve cryptography multiplication computations defined over GF(p) primes.

In 2011, Adnan.Abdul-Aziz Gutub, and al proposed and evaluated a new and improved modular cryptographic pipelined multiplier architecture. The aim is to implement this solution on FPGA.

En 2014, Loai Tawalbeh et al ont proposé des algorithmes optimisés pour la quadrature modulaire dans GF(p), une opération essentielle dans les algorithmes de cryptage à clé publique les plus répandus. Trois algorithmes sont proposés : deux pour la mise au carré et un pour la réduction combinée à la mise au carré, formant un algorithme général de mise au carré modulaire.

A chaotic system is extremely sensitive to initial conditions and its future behaviour is therefore very difficult to predict. It is this unpredictability that makes it useful for securing communications. However, traditional random signal generators based on looped shift registers have well-known shortcomings and will eventually enter predictable repetitive cycles.

The use of a master-slave hardware representation enables controlled synchronisation of two chaotic generators. Sensitivity to initial conditions means that two identical systems will quickly diverge if subjected to slightly different conditions. The master-slave configuration forces the two systems to remain identical and to emit the same chaotic signals, which are essential for encoding and decoding in cryptography.

For example, imagine a pair of identical chaotic circuits with very similar initial conditions. By regularly injecting small corrections into the slave, we can keep it perfectly synchronised

with the master at all times. This configuration allows us to take advantage of the long-term unpredictability of chaos while controlling the process.

So this original approach based on two synchronised chaotic circuits provides a level of cryptographic security that is far superior to conventional random generation methods. It makes full use of the unique and advantageous properties of controlled chaos while circumventing its drawbacks.

CHUA'S CIRCUIT

Presentation of the Chua Circuit

The Chua chaotic oscillator is a simple electronic circuit invented by Leon Chua in 1983. This random generator generates complex chaotic behavior thanks to the presence of a non-linear element, the Chua diode. A dynamic chaotic system must contain at least: An inductor, two active resistors, one linear and the other non-linear., one or more storage components (Chua et al., 1986 ; Chua, 1994).

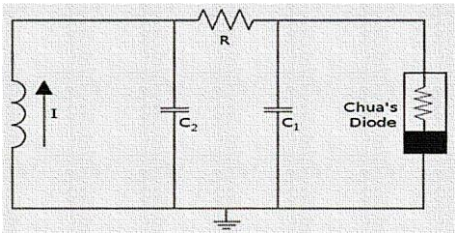


Fig.1. Chua circuit.

The Chua circuit is a chaotic generator described by a non-linear dynamic system with three differential equations, of which: X and Y the equations across the capacitors C1 and C2, Z: the equation across the gyrator (de Magistris et al., 2011; Sharkovsky, 1993 ; Galias, 2016).
We can represent this system of equations as a function of X, Y, and Z:

$$\begin{cases} X = \alpha(y - x - g(x)) \\ Y = x - y + z \\ Z = -\beta y \end{cases} \quad (1)$$

α and β: depend on the actual components of the circuit.
g(x): is a linear function representing the variation of the resistance as a function of the current across the diode Chua:

$$g(x) = m_1 x + \frac{m_0 - m_1}{2} = (|x + 1| - |x - 1|) \quad (2)$$

Chua's diode

The Chua diode is not manufactured or marketed because, unlike other standard components, it is a type of non-linear active resistor. There are several models of Chua diode, for our work, we have chosen the famous model, which contains standard components such as resistors and operational amplifiers.

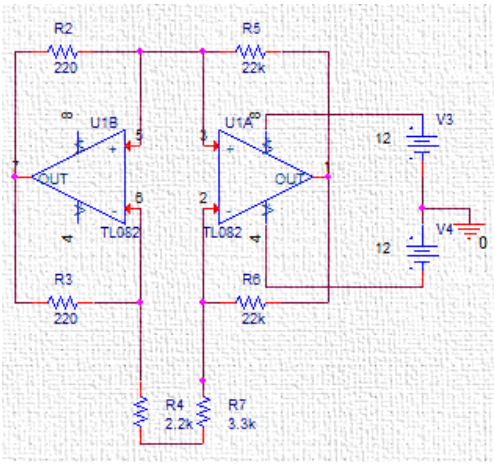


Fig.2. Equivalent diode Chua.

Where g(x) represents the non-linear element of the circuit:

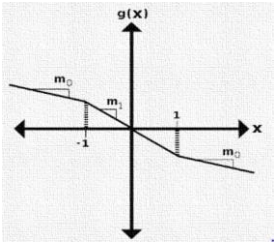


Fig.3. Diode characteristic.

Equivalent inductor gyrator

The gyrator replaces the L inductor, which we use instead of a real inductor. The gyrator consists of active resistors, capacitors and operational amplifiers (Siderskiy, 2012).

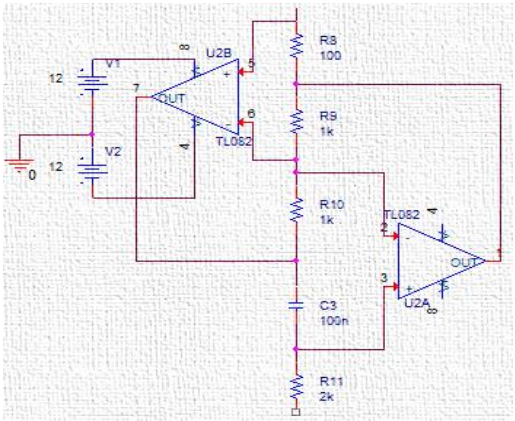


Fig.4. The gyrator.

SIMULATION AND RESULTS

In this section, the Chua generator is simulated on OrCAD with two models, one containing an inductor and the other containing a gyrator.

OrCAD definition

OrCAD is a computer-aided design (CAD) software package that simulates analogue and digital electronic circuits, and produces the corresponding printed circuit boards (Mitzner, 2011).

Chua circuit simulation and results on OrCAD

Initially, the first circuit will contain two capacitors, C1 and C2, with respective capacities of 10nF and 100nF, as well as a variable "potentiometer" resistor (R = 1.8kohm) and a variable inductor.

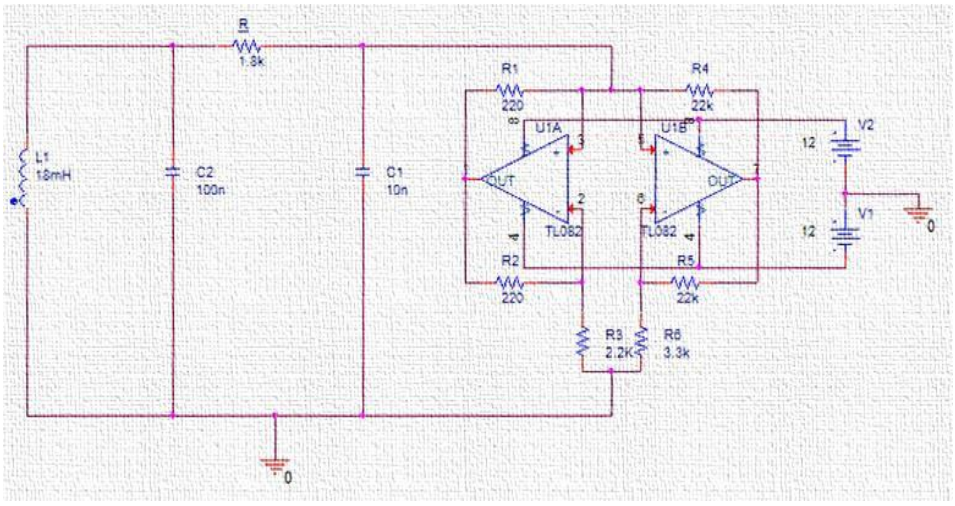
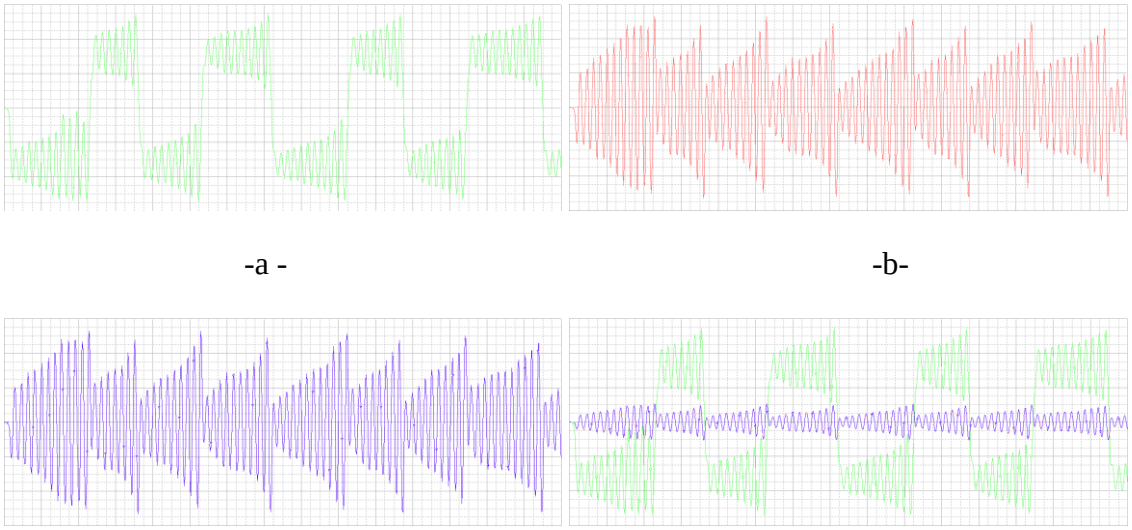


Fig.5. Circuit diagram of Chua under OrCAD (with inductance).

The results of the first circuit are shown in the following figures, of which figures (a), (b) and (c) show the X, Y and Z signals and figure (7) shows the Chua attractor.



-a - -b-

-c- -d-

Fig.6. Time series of voltages V_1 and V_2, a) - Signal X, b) - Signal Y, c) - Signal Z and d)- The three signals X, Y, and Z.

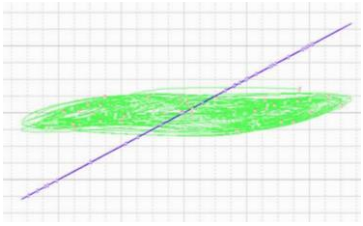


Fig.7. Double attractor of a Chua circuit.

In the second circuit, we chose to replace the inductor with a gyrator (this type of inductor can be difficult to find and buy). As the diagram shows, the equivalent circuit for the inductor should comprise three resistors and one variable resistor (we chose R = 2.5kohm), two operational amplifiers (TL082) and a 100nf capacitor.

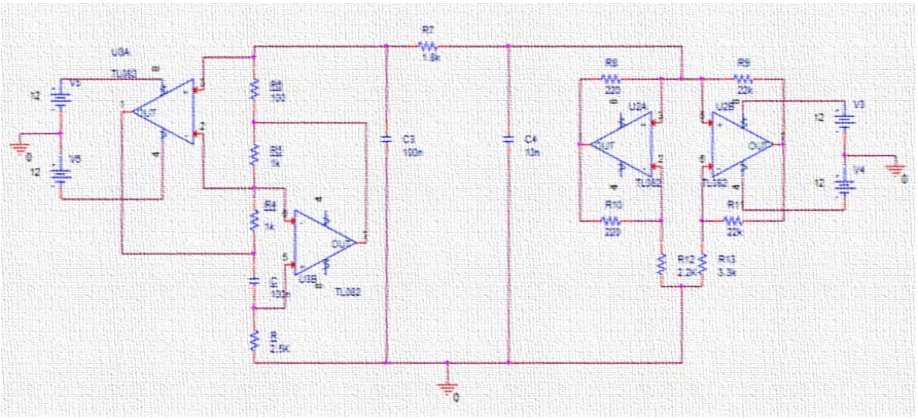
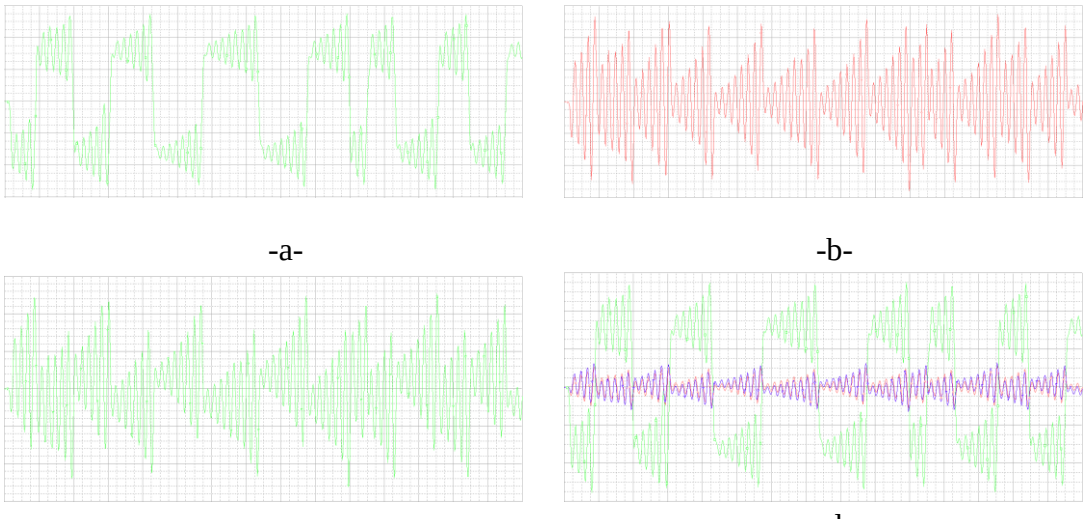


Fig.8. Diagram of the Chua circuit under OrCAD (with gyrator).

We place the voltage across resistors C1, C2 on the Chua circuit with the Gyrator, The following figures show the results of simulating the X, Y and Z signals of this circuit:



-a- -b-

-c- -d-

Fig.9. Time series of voltages V1 andV2, a) - Signal X, b) - Signal Y, c) - Signal Z,d) - The three Signals X, Y, and Z.

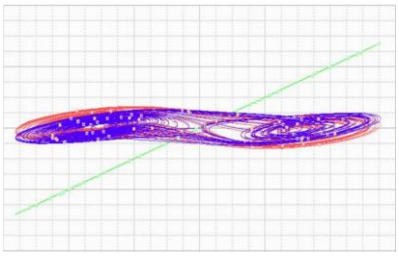


Fig.10. Double attractor of the Chua circuit.

Figures 6 and 9 show the time series generated by Chua's chaotic generator (circuit 1 employs an L=18mh inductance, whereas circuit 2 employs a gyrator), with V_1 at the capacitor C_1 terminals and V_2 at the capacitor C_2 terminals. The pathways in Figures 9 and 13 around the two foci of attraction show that the voltages are random and the signals are chaotic.

SYNCHRONIZATION OF CHAOTIC DYNAMICAL SYSTEMS

Definition 1: (Larousse) (a Greek word) the word Synchronization means together and Chrono means time. It is the action of putting in phase to create a simultaneity between several operations, according to time.

General definition: Synchronization is now an important part of data transmission success. Because chaotic oscillators are predictable but very sensitive to beginning circumstances, it is theoretically conceivable to synchronize two of them (have one or more positive Lyapunov exponents and are unstable). Two chaotic signals are considered to be synchronized if they are asymptotically identical as it approaches infinity (Carroll and Pecora, 1993).

Synchronization may be divided into two categories: (Sanchez et al., 2000)

Bidirectional synchronization: An element that permits energy to be exchanged in both directions is required when two identical systems a and b are linked in bidirectional synchronization (means that each system can play a role of a master or slave system at the same time)

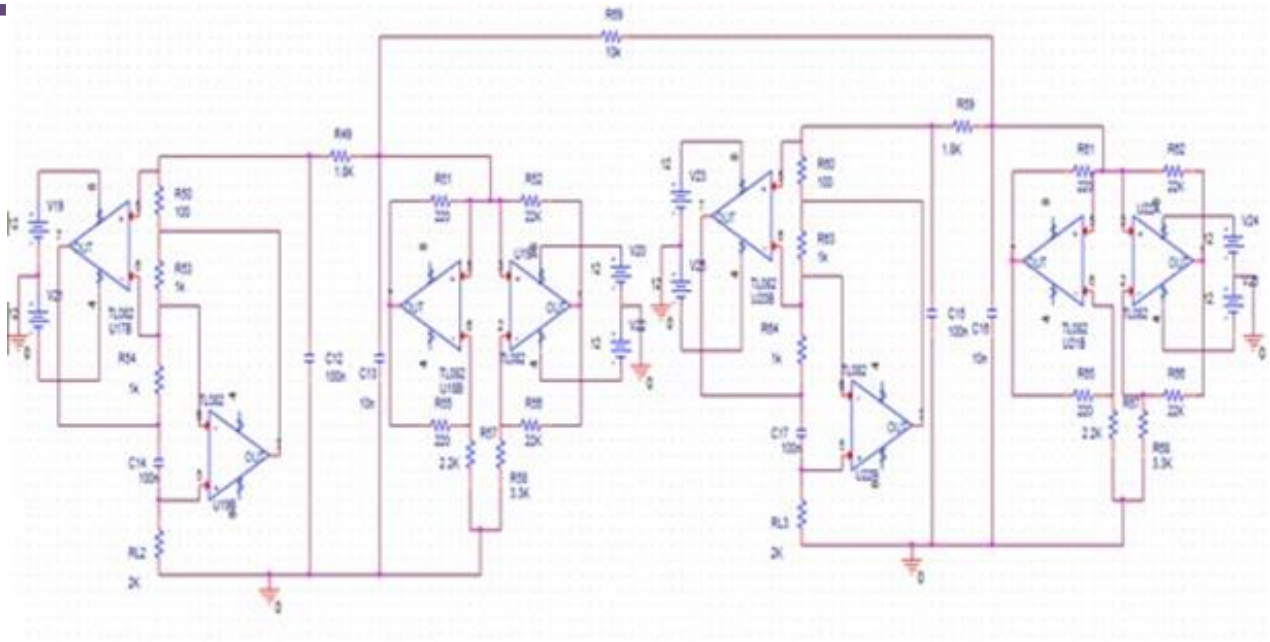


Fig.11. Synchronisation bidirectionnelle.

One-way synchronization: in the case of unidirectional synchronization the coupling between two identical systems a and b requires an element operating in one direction only.
The master: is an independent system
The slave: is a system that is dependent on the master system.

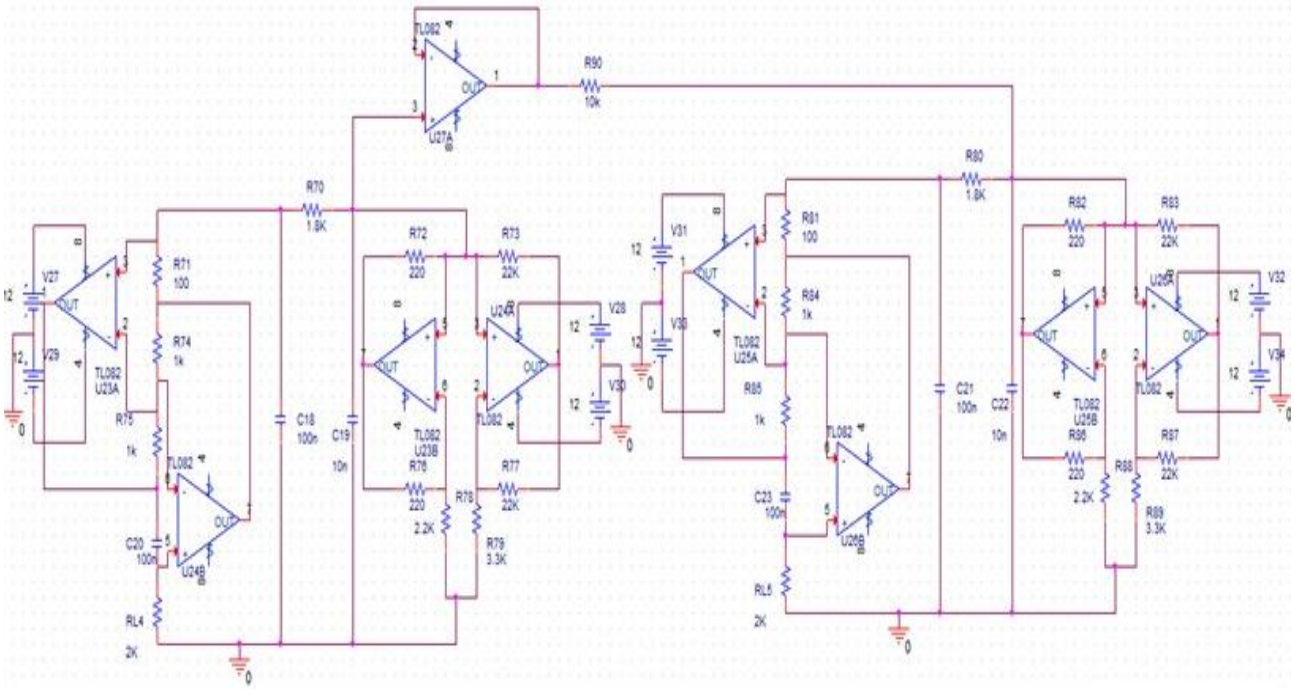


Fig.12. Realization of Chua circuit (master/slave) under OrCAD.

At first, we start with the slave diagram signals:

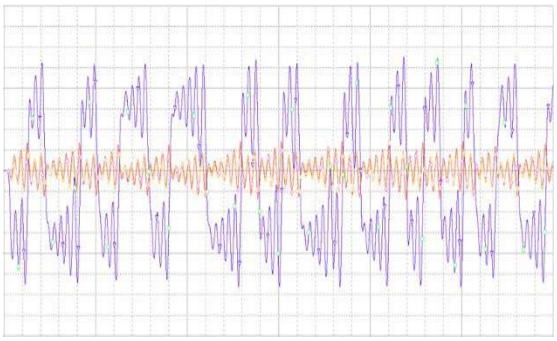


Fig.13. The 3 signals X, Y, Z.

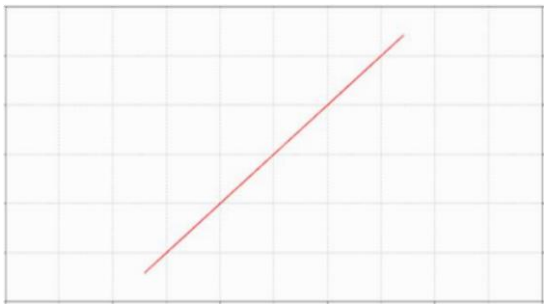


Fig.14. Synchronization of the two circuits.

Figure (15) shows the curve of the voltage V_1 of the master circuit versus the voltage V'_1 of the slave circuit, according to the result of the output the two circuits are synchronized (Carroll and Pecora, 1991; Gutub, 2007)

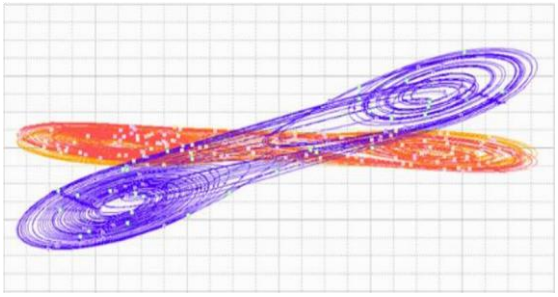


Fig.15. Desynchronization of the two circuits.

By slightly modifying the values of the two potentiometers of the master circuit, figure 16 shows that the two circuits are not synchronized, which confirms the sensitivity to the initial conditions of the synchronized system.

DISCUSSION OF THE RESULTS

In this part, we apply the knowledge we saw in the previous part about Chua's circuit and its theoretical and simulated behavior, and the synchronization of two chaotic circuits to realize an electronic card containing two Chua's circuits. Chua's circuits can be created in a variety

of ways using standard or custom electronic components. Our main concern is to achieve Chua's nonlinear resistance, as all linear circuit elements are available on both ports.

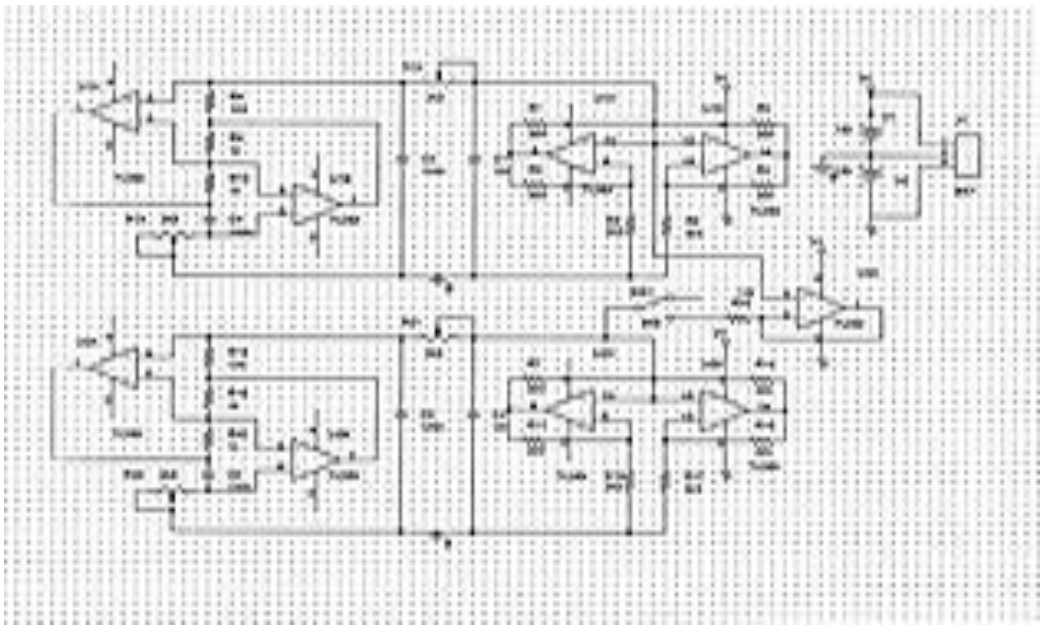


Fig.16. Diagram of the Chua circuit with OrCAD (Master/Slave).

The above image shows us a simple realization of a Chua synchronizer (Master/Slave) circuit using operational amps.

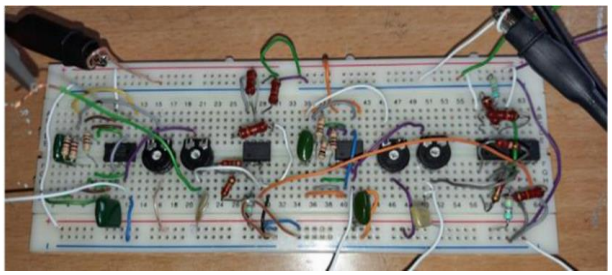
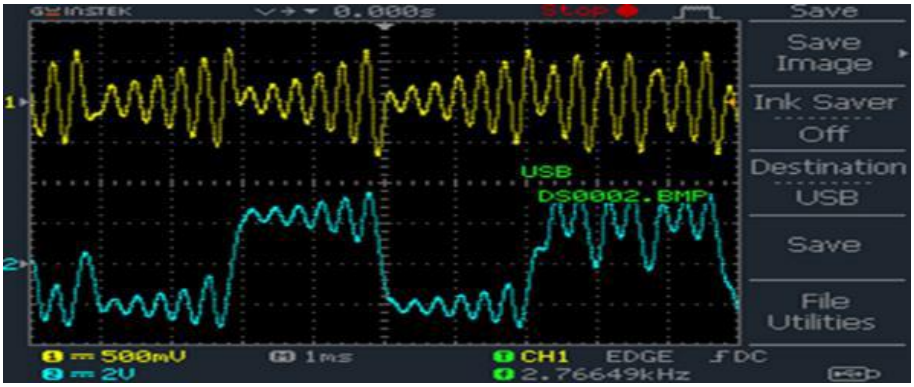
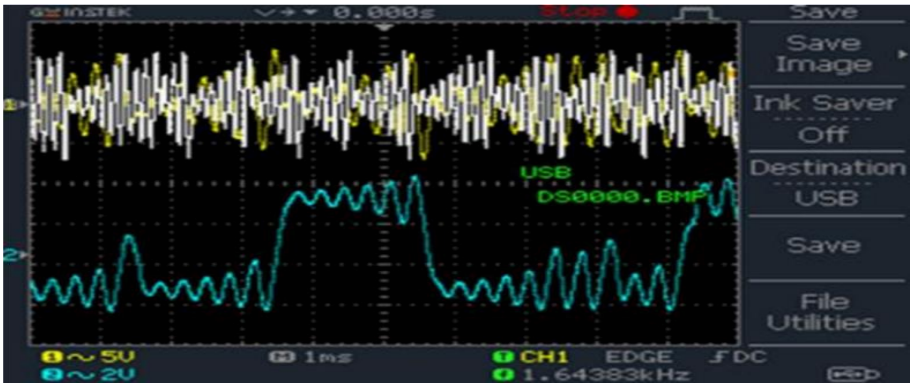


Fig.17. Chua circuit on the test plate (Master/Slave).

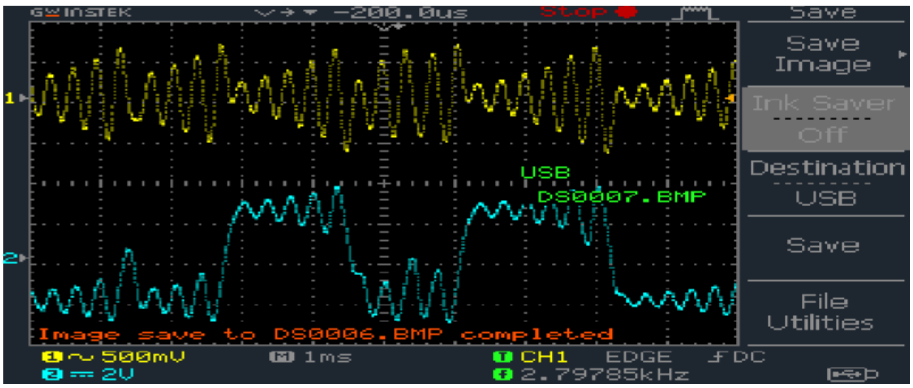
Fig. 18. Chua circuit manipulation 1.



-a-



-b-



-c-

Fig.19. Example of simulation result.

Figure 20 shows the simulation results of a chaotic generator called the Chua circuit whose figure -a- presents the X, and Y signals, and figure -b- presents the result of the, Y and Z signals.

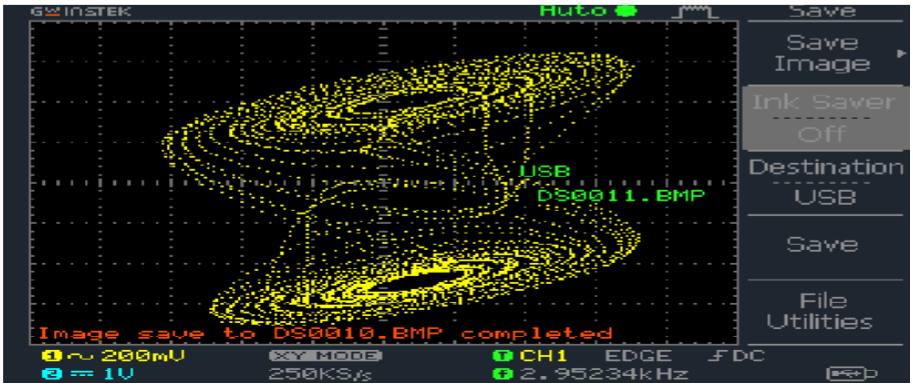


Fig.20. Chua attractor.

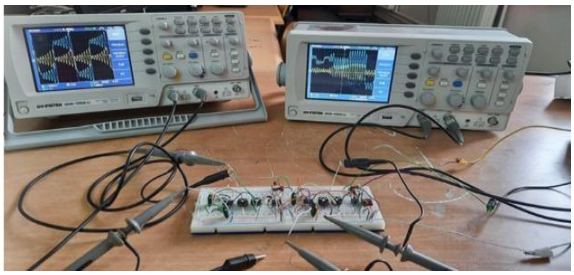


Fig.21. Chua circuit manipulation 2.

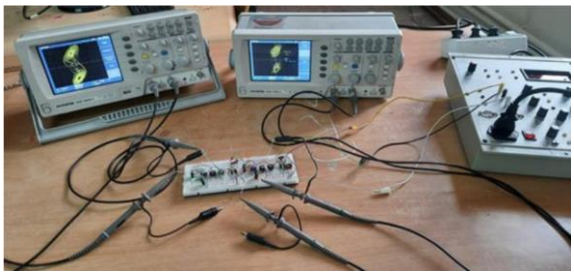


Fig.22. Chua attractor of two generators.

The outline over appears the nearness of a twofold attractor within the first circuit (master), which suggests that it'll indeed generate a chaotic flag A comparative double attractor is additionally shown within the moment circuit, inferring the nearness of a chaotic flag. To form this circuit, we utilize the OrCAD program which permits us to create PCB circuits with extraordinary ease, and we get the PCB diagram following:

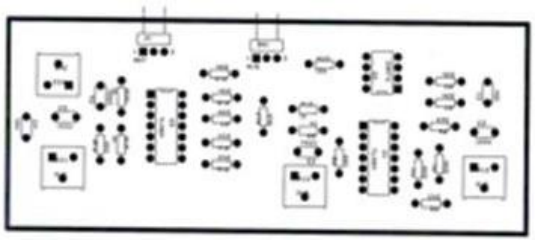


Fig.23. The circuit PCB diagram in OrCad.

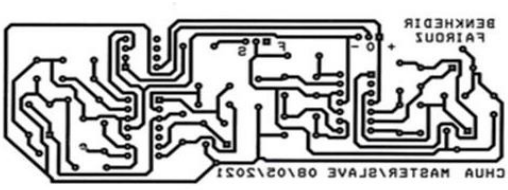


Fig.24. Circuit film with OrCAD.

In a single electronic plate, two circuits of Chua were made, after completing the schematics of the later circuits, we get the various models outlined underneath:

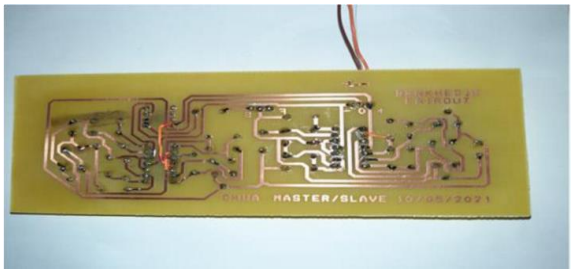


Fig.25. Back view of the electronic card.

Fig.26. Implementation of components on the electronic card.

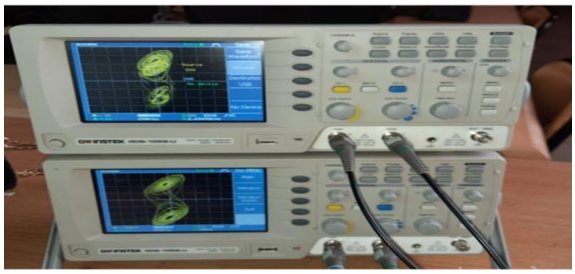


Fig.27. Card simulation result.

CONCLUSION

This work enabled an in-depth exploration of Chua's chaotic circuit, both from a theoretical and practical point of view. The implementation and detailed simulation of the circuit in the OrCAD environment made it possible to generate and analyse the various chaotic signals. The visualisation of the associated strange attractor confirmed the highly non-linear and complex behaviour of this model system. The practical implementation of a synchronised Chua circuit and its simulation validated the feasibility of such a concrete implementation. These results open up interesting new prospects. One promising avenue would be to exploit the cryptographic potential of the chaotic signals generated by using them as a source of random keys in robust encryption algorithms. The statistical properties and complexity of the chaotic sequences obtained could be further analysed with this objective in mind. Another possible avenue of research would be to implement the synchronised circuit on a dedicated hardware platform, enabling real-time applications and offering better performance in terms of throughput and stability.

REFERENCES

Jimenez-Triana, A., Tang, W. K. S., Chen, G., & Gauthier, A. (2010). Chaos control in Duffing system using impulsive parametric perturbations. *IEEE Transactions on Circuits and Systems II: Express Briefs*, *57*(4), 305-309.

Chua, L. E. O. N. O., Komuro, M., & Matsumoto, T. (1986). The double scroll family. *IEEE transactions on circuits and systems*, *33*(11), 1072-1118.

Mitzner, K. (2011). *Complete PCB design using OrCad capture and layout*. Elsevier.

Chua, L. O. (1994). Chua's circuit 10 years later. *International Journal of Circuit Theory and Applications*, *22*(4), 279-305.

De Magistris, M., Di Bernardo, M., Di Tucci, E., & Manfredi, S. (2012). Synchronization of networks of non-identical Chua's circuits: Analysis and experiments. *IEEE Transactions on Circuits and Systems I: Regular Papers*, *59*(5), 1029-1041.

Sharkovsky, A. N. (1993). Chaos from a time-delayed Chua's circuit. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, *40*(10), 781-783.

Galias, Z. (2016). Rigorous analysis of Chua's circuit with a smooth nonlinearity. *IEEE Transactions on Circuits and Systems I: Regular Papers*, *63*(12), 2304-2312.

Siderskiy, V. (2012). The Antoniou Inductance-Simulation Circuit Derivation. *Creating Chaos LLC*.

Singh, P. P. (2021). A novel chaotic system with wide spectrum, its synchronization, circuit design and application to secure communication. *Indian Journal of Science and Technology*, *14*(28), 2351-2367.

Carroll, T. L., & Pecora, L. M. (1993). Synchronizing nonautonomous chaotic circuits. *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, *40*(10), 646-650.

Sánchez, E., Matías, M. A., & Pérez-Muñuzuri, V. (2000). Chaotic synchronization in small assemblies of driven Chua's circuits. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, *47*(5), 644-654.

Carroll, T. L., & Pecora, L. M. (1995). Synchronizing chaotic circuits. In *Nonlinear dynamics in circuits* (pp. 215-248).

Dedieu, H., Kennedy, M. P., & Hasler, M. (1993). Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits. *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, *40*(10), 634-642.

Gutub, A. A. (2007). High speed hardware architecture to compute galois fields GF (p) montgomery inversion with scalability features. *IET Computers & Digital Techniques*, *1*(4), 389-396.

Tawalbeh, L. A. A., Mohammad, A., & Gutub, A. A. A. (2010). Efficient FPGA implementation of a programmable architecture for GF (p) elliptic curve crypto computations. *Journal of Signal Processing Systems*, *59*, 233-244.

Gutub, A., El-Shafei, A. R. M., & Aabed, M. A. (2011). Implementation of a pipelined modular multiplier architecture for GF (p) elliptic curve cryptography computation. *Kuwait Journal of Science and Engineering*, *38*(2B), 125-153.

Tawalbeh, L. A., Swedan, S., & Gutub, A. (2009). Efficient Modular Squaring Algorithms for Hardware Implementation in GF (p). *Information Security Journal: A Global Perspective*, *18*(3), 131-138.