Implementation of Chaotic Encryption Architecture on FPGA for On-Chip Secure Communication*

1st Ravi Monani
California State University at Long Beach
Department of Electrical Engineering
Long Beach, CA, USA
ravi.monani01@student.csulb.edu

2nd Brian Rogers
California State University at Long Beach
Department of Electrical Engineering
Long Beach, CA, USA
Brian.Rogers@student.csulb.edu

3rd Amin Rezaei
California State University at Long Beach
Department of Computer Engineering & Computer Science
Long Beach, CA, USA
Amin.Rezaei@csulb.edu

4th Ava Hedayatipour
California State University at Long Beach
Department of Electrical Engineering
Long Beach, CA, USA
Ava.Hedayatipour@csulb.edu

2022 IEEE Green Energy and Smart Systems Conference (IGESSC) | 978-1-6654-9866-1/22/$31.00 ©2022 IEEE | DOI: 10.1109/IGESSC55810.2022.9955334

***Abstract*— Chaos is an interesting phenomenon for nonlinear systems that emerges due to its complex and unpredictable behavior. With the escalated use of low-powered edge-compute devices, data security at the edge develops the need for security in communication. The characteristic that Chaos synchronizes over time for two different chaotic systems with their own unique initial conditions, is the base for chaos implementation in communication. This paper proposes an encryption architecture suitable for communication of on-chip sensors to provide a POC (proof of concept) with security encrypted on the same chip using different chaotic equations. In communication, encryption is achieved with the help of microcontrollers or software implementations that use more power and have complex hardware implementation. The small IoT devices are expected to be operated on low power and constrained with size. At the same time, these devices are highly vulnerable to security threats, which elevates the need to have low power/size hardware-based security. Since the discovery of chaotic equations, they have been used in various encryption applications. The goal of this research is to take the chaotic implementation to the CMOS level with the sensors on the same chip. The hardware co-simulation is demonstrated on an FPGA board for Chua encryption/decryption architecture. The hardware utilization for Lorenz, SprottD, and Chua on FPGA is achieved with Xilinx System Generation (XSG) toolbox which reveals that Lorenz's utilization is ~9% lesser than Chua's.**

***Index Terms*—CMOS, Hardware security, FPGA, Chua's Chaotic equations, Lorenz, SprottD, edge-compute devices, secure communication, Xilinx System Generator, wearables, security, Chaos implantation, Internet of Things (IoT).**

I. INTRODUCTION

In 1963 Lorenz [1] presented the first well-known chaotic system, this marked the start of chaos theory, a branch of nonlinear system theory that has been studied intensively in recent years. Chaotic systems are nonlinear dynamic systems that are unpredictable, and highly sensitive to initial conditions. These trajectories of two identical chaotic systems with unique initial conditions however can converge over time, making the basis of chaos synchronization. The butterfly-like pattern of the Lorenz attractor is one of the first well-known and most complex symbols of chaos. The main disadvantage of these equations is the implementation of two multipliers in its three differential equations scheme, increasing the power and area consumption.

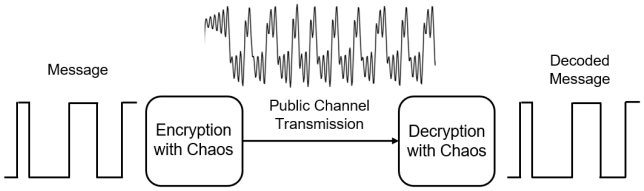


Figure 1:Message is encrypted using a chaotic circuit and transmitted over a public channel to be decrypted back at the receiver.

Modified Lorenz, proposed by Radwan et al. [2], solves this problem by eliminating the need for multipliers but maintaining the "Butterfly effect". Other variations of the Lorenz system are also proposed. As an example, to improve the stability or predictability of the Lorenz system, Stenflo and Leonov derived the following four-dimensional Lorenz–Stenflo system with four parameters.

Chaos synchronization is the basis of using chaos in communication. Figure 1 shows an overview of a chaotic encryption system. The input signal is the raw unencrypted data that is scrambled by the chaotic transmitter before being transmitted over the public channel. The public channel can be wireless as in body sensor networks or wired as in power grids.

Parametric feedback control using chaos [3] eliminated the need for conventional frequency synthesizers as communication carriers. The information that needs to be communicated is transmitted as a chaotic spectral signal that looks like noise to a third party. Though chaotic communication has been around for decades, asymmetric and symmetric key encryption Cryptography have been the fundamental method of message encryption. With the advancement of resource-limited systems like cars, implanted medical devices, and internet of things devices (IoTs) encryption needs to be incorporated in different layers of the system starting from the integrated circuit, where symmetric and asymmetric encryption methods can be challenging to implement. Moreover, with the claim of quantum computing

* This material is based upon work supported by the National Science Foundation under Grant No. 2131156.

on the horizon [4] [5], symmetric and asymmetric cryptography keys can break quickly in the near future by exhaustively trying long bits of all secret keys. Therefore, methods of encryption other than symmetric and asymmetric security are gaining more importance and quickly becoming necessary.

In this paper, we aim to achieve chaos synchronization, that can be implemented on-chip for secure communication. The synchronized communication is confirmed by simulations and FPGA implementations for Lu, Chua, Lorenz and SprottD chaotic equations using EDA tools like LTspice, MATLAB, and XSG .The rest of the paper is organized as follows. Section II discusses the MATLAB implementation of chaotic equations along with their sensitivity to initial conditions. Section III focuses on the spice design of comprehensive design of encryption architecture using Chua's chaotic circuit. The hardware implementation with resource utilization is summed up in sections IV and V with experimental data.

II. Different Chaotic Systems and Their Simulations in MATLAB

To study chaos, different systems are implemented to evaluate which one is the best for the desired outcome. Specifically, Lorenz, Lü, SprottD, and Chua's chaotic equations will be examined. The focus of this paper will be on analyzing which circuit is most efficient in terms of power and cost.

A. Lorenz Chaotic Equations:

Lorenz equations are modeled as shown in Table 1. The initial conditions are given by $\sigma = 10, \rho = 28, and\ \beta = \frac{8}{3}$. [6] Plotting the three differential equations on MATLAB, the "Butterfly effect" is observed as depicted in Figure 2 (a). Due to the nonperiodic motion revolving around the two unstable equilibrium points [7], the curve never intersects itself, illustrating the system's chaotic behavior.

B. Lü Chaotic Equations

Lü chaos equations are given in Table 1. In Figure 2(b), the MATLAB plot of the equations follows a similar "butterfly effect" as in Figure 2(a).

Table 1: Different Chaos Equations

Name	Equations	Scroll Type	Function
Lorenz	$\dot{x} = \sigma(y - x)$ $\dot{y} = (\beta - z)x - y$ $\dot{z} = xy - \rho z$	Double Scroll	OTA, Multiplier
Lü	$\dot{x} = \sigma(y - x)$ $\dot{y} = \beta y - xz$ $\dot{z} = -\rho z + xy$	Multi Scroll	PTA, Product
SprottD	$\dot{x} = -y$ $\dot{y} = x + z$ $\dot{z} = 2y^2 + xz - a$	Multi Scroll	PTA, Product
Chua	$\dot{x} = \sigma(y - x - g_2(x))$ $\dot{y} = x - y + z$ $\dot{z} = -\beta y$	Multi Scroll	PWL

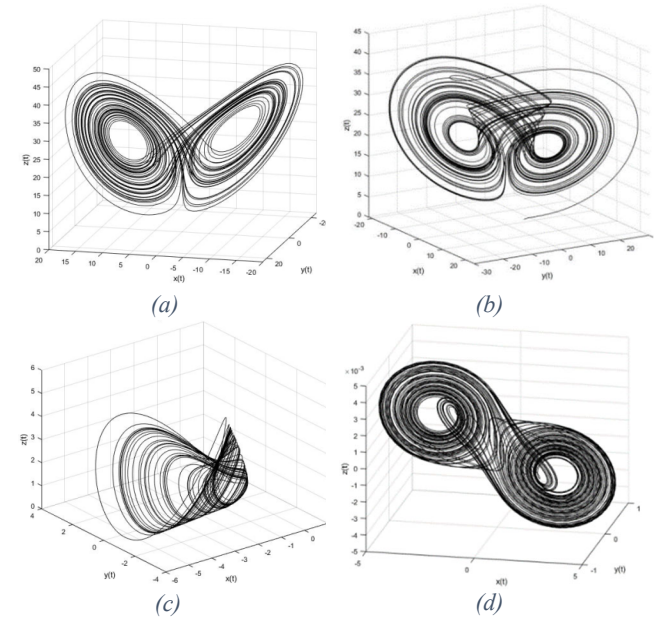


Figure 2: MATLAB simulation of Chaotic equations (a) Lorenz, (b) Lü, (c) SprottD, and (d) Chua

Notably, the sensitivity graphs follow a similar pattern to that of the Lorenz attractor but are more sensitive to the initial conditions.

C. SprottD Chaotic Equations

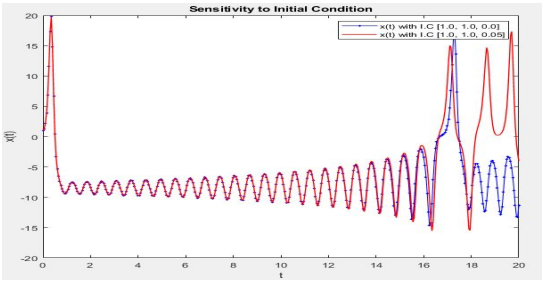
SprottD attractor has grown in popularity during the previous years due to its high performance and low-cost implementation [7]. This circuit is described by the equations mentioned in Table 1. This circuit illustrates chaotic behavior as observed by the "Butterfly effect" in Figure 2 (c). From Figure 3 (c), the value of one parameter is altered from 0.4 to 0.45.

D. Chua's Chaotic Equations

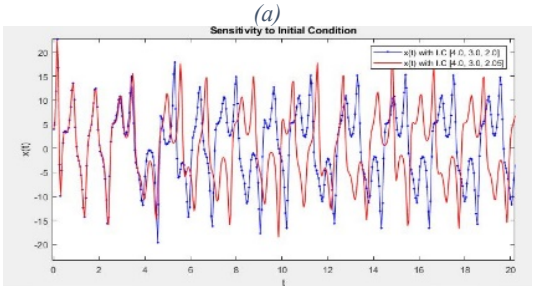
Chua's circuit requires a nonlinear element, a locally active resistor, and three or more energy storage elements. [8] The Chua Diode covers the nonlinear element and locally active resistor. As observed by the plot of Chua's equations in Table 1, the "Butterfly effect" and double scroll attractor are displayed, illustrating the chaotic behavior and three nonlinear ordinary differential equations. Consisting of three unstable equilibrium points, Chua's circuit has more chaos than the preceding systems. [6] Chua circuit is "one of the most robust experimental proof of chaos and can be easily implemented in different ways." [8]

E. Sensitivity to Noise and Robustness to Attack

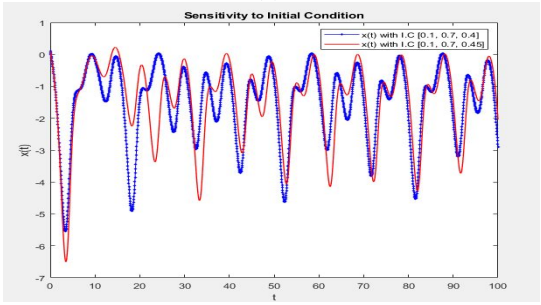
In communication when the signal is discussed, it is always important to pay attention to the noise component involved in the signal. Signal-to-Noise Ratio (SNR) is the ratio of signal power compared to all other electrical signals, which can be identified as noise. SNR can be calculated by the mean of the signal divided by the standard deviation.



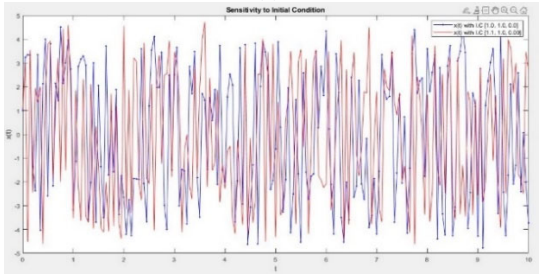
(a)



(b)



(c)



(d)

Figure 3: Sensitivity to Initial Conditions for Chaotic Equations (a) Lorenz, (b) Lü, (c) SprottD, (d) Chua

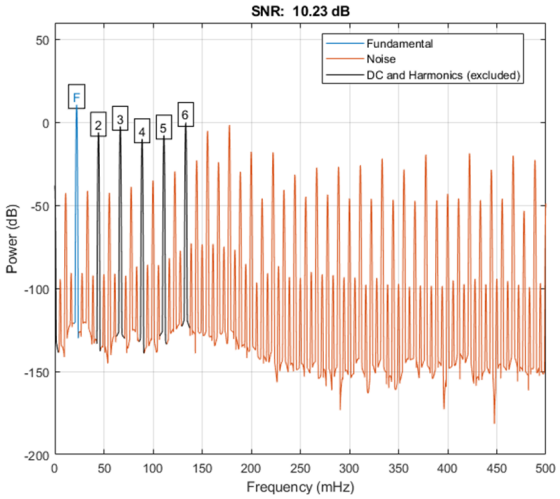


Figure 4: Signal to Noise Ratio (SNR) for Chua's Signal X

Lower SNR tends to introduce more Gaussian noise, as the signal becomes unusable. This is also called 'noise floor'. During the analysis of the chaos, it is observed that the Chua has an SNR near 10 dB which makes the signal more prone to noise.

Figure 4 illustrates the SNR plot of signal X from Chua's equation. The signal with SNR near 10 dB can be identified as noise and the signal becomes unusable. Thus, when transmitted through a public channel these signals are just noise, which symbolizes the robustness of the chaotic equations to the static noise and eliminates the possibilities of data loss.

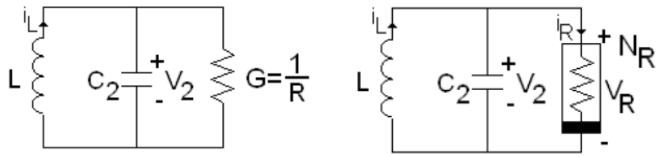
III. Simulation And Encryption Architecture Using Chua Equations

The high-level system block diagram can be seen in Fig. 1. The data collected from the sensor are fed to the chaotic transmitter before transmission. The chaotic transmitter encrypts the original signal using chaotic equations and generates a signal which seems chaotic in nature. This encrypted signal is then transmitted over a public channel where it cannot be decrypted without initial conditions/parameters of encryption to the chaotic equations known. This section discusses the complete encryption architecture implemented in LTSpice using Chua's chaotic equations.

The 3D plot of Chua's equation is presented in Figure 2 (d) using MATLAB. The parameters' values and the initial conditions for the encryption-decryption are discussed in the following section. The equations can be found in Table 1.

A. Equations:

The invention of Chua's circuit started with the topology



(a) *(b)*

Figure 5: (a) Linear parallel RLC circuit (b) LC circuit with a nonlinear element

with LC parallel, the simplest mechanism providing oscillation. The linear parallel RLC circuit in Figure 5 (a) is the least complicated resonant circuit that can oscillate [8]. As an advancement to make a stable oscillator and many real oscillations independent from the initial conditions, a nonlinear element needs to be added, as the RLC circuit is not structurally stable [8]. Figure 5 (b) represents the LC circuit with a nonlinear element to generate stable oscillators.

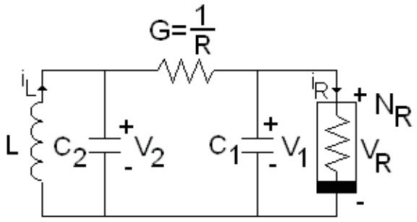


Figure 6 The Chua's circuit

Chua's circuit evolved as an efficient circuit generating chaos [8]. Chua's circuit containing capacitor, inductor, and resistor with nonlinear element N_R is shown in Figure 6 [8]. When Kirchhoff's circuit law is applied, the state equations are as Equation 1 [8].

$$\frac{dv_1}{dt} = \frac{1}{C_1}[G(v_2 - v_1) - g(v_1)]$$
$$\frac{dv_2}{dt} = \frac{1}{C_2}[G(v_1 - v_2) + i_L]$$
$$\frac{di_L}{dt} = -\frac{1}{L}v_2$$

Equation 1

The above Chua's chaotic equations can be rewritten as below Equation 2.

$$\dot{x}_1 = \alpha(x_2 - x_1 - g_2(x_1))$$
$$\dot{x}_2 = x_1 - x_2 + x_3$$
$$\dot{x}_3 = -\beta x_2$$

Equation 2

Where, $g_2(x_1)$ *can be defined as,*

$$g_2(x_1) = m_1 x + \frac{1}{2}(m_0 - m_1)[|x+1| - |x-1|]$$

B. Encryption Architecture*:*

The characteristic property of Chaos, in general, motivates its implementation in cyphering and that has taken many approaches in cryptography. Figure 1 describes the data transmission into the public channel with secure encryption and decryption at the receiver end. Figure 8 represents the architectural design developed with Chua's chaotic equations to encrypt the data signal.

The message signal (V3) has been encoded in the encryption circuit through the β-modulator. [9] The β-modulator is a variable gain circuit designed with inverting summing amplifier and two separate inverting amplifiers, one of which is controlled by the switch. Figure 7 represents the β-modulator. [9]

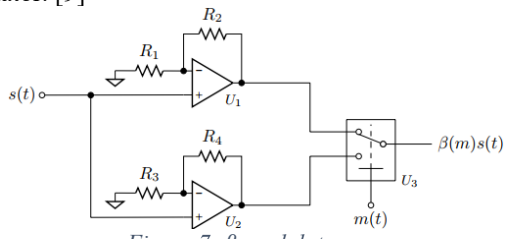


Figure 7: β-modulator

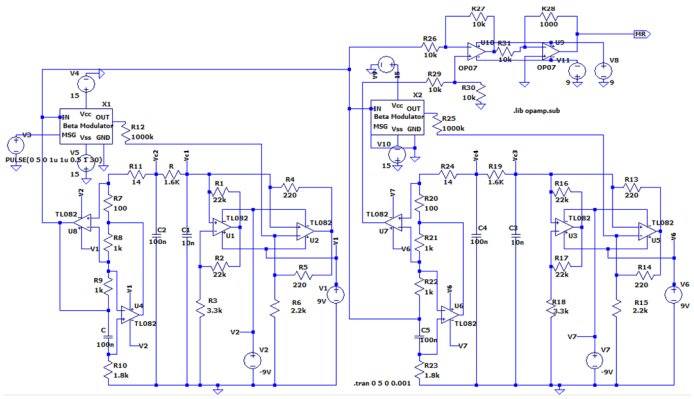


Figure 8: Encryption Circuit with Chua's Equations

The encrypted signal is then transmitted out to the public channel from the transmitter and the receiver decrypts the signal from similar initial conditioned Chua's equations. This generated signal, say X' is then compared to the originally received signal, say X at the receiver end. The difference between these two is then amplified to retrieve the message signal data in order to complete the transaction.

Figure 9 plots the simulations of the encryption architectures message signals, blue square pulse signal represents the original message signal sent to the chaotic encryption system and the red chaotic signal is decrypted signal at the receiver end. Thus, when this signal is drawn down to the receiver chaotic decryption circuit, it reviles the message by proving zero values when the original message is zero and oscillating pulse signal when the original signal has a +5V magnitude.

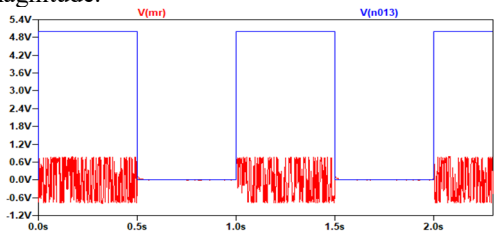


Figure 9: Original message signal and decrypted signal

IV. Hardware Implementation with Xilinx System Generator (XSG)

The attempt of implementing a random number generator using Chua's circuit on FPGA has been performed in [10]. Using this cryptographically secured pseudo-random sequence is generated to encrypt the image and then restored using the private key as initial conditions of Chua's circuit [10].In recent studies, the FPGA implementation of Chua's circuit has been claimed to be achieved for multi-scroll Chua equations with 25MHz in [11] with Xilinx Artix7 board. These implementations are done with the use of the Xilinx System Generator (XSG) [11] [10].

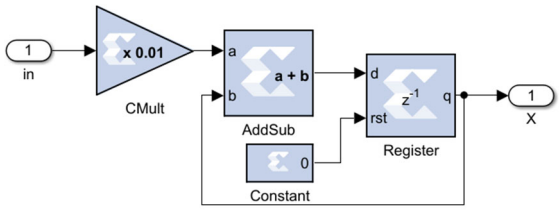


Figure 10: Integrator design

The fraction-order chaotic system based on Chau's circuit is implemented on FPGA with Xilinx Artix7 board in [12]. The fraction-order system with the shifting blocks, replacing multipliers, results in reduced hardware resources and propagation delay with low power on hardware [12]. This motivation drives the encryption architecture proposed in this section with the goal of achieving low-power, CMOS-based chaotic implementation using Chua's circuit.

The aim of the FPGA implementation of chaotic equations is to estimate the cost in terms of power and hardware utilization when it is implemented on a chip.

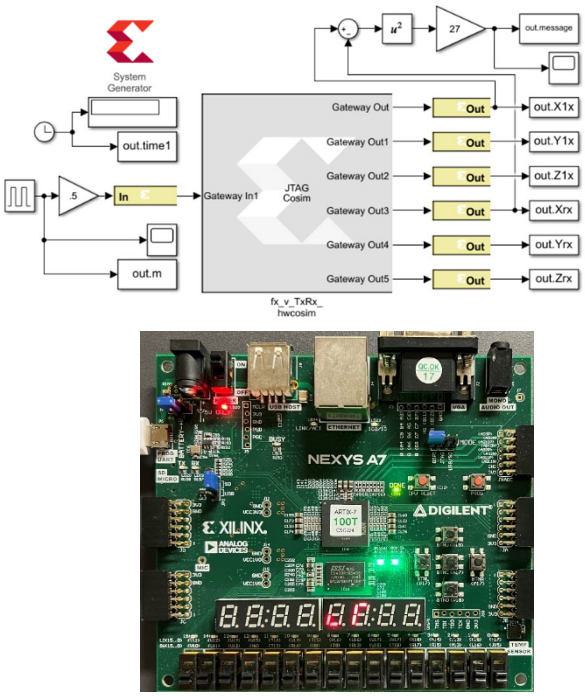


Figure 11: Xilinx Artix-7 FPGA (XC7A35T-1 CPG236C) Basys3

The integrator block, Figure 10, is implemented using register and adder with a sample rate of 0.01. This XSG implementation is discussed further with their simulation results and utilization observations in the result section.

The Xilinx System Generator toolbox provides MATLAB Simulink support to generate the HDL (Hardware Descriptive Language) codes for a design to be implemented on Xilinx FPGA boards. Upon successful completion of a synthesis run for the target board as shown in Figure 11, Xilinx Artix-7 Nexys-A7, power and utilization are estimated for all three chaotic designs. The Result section talks about these comparisons with adequate data.

To achieve the FPGA implementation of chaotic circuits, Xilinx's Nexys-A7 board is selected. It has support for a USB-UART bridge, USB-JTAG port, and an internal clock with 450 MHz. This enables the board to be used also for hardware co-simulation with the XSG toolbox on Simulink. The board is shown in Fig 11. The more detailed circuit of the transmitter and the receiver is shown in Figure 12.

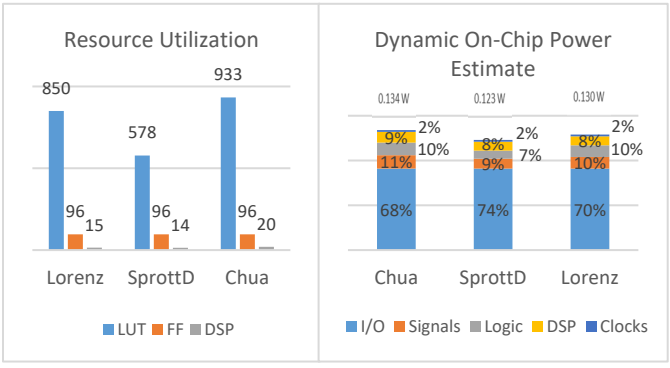
V. Results and Discussion

The experimental data has been probed from the FPGA board Nexys A7 for the system generator design of Lorenz, SprottD, and Chua. Figure 13 compare the resource utilization and power for these three chaotic circuits in Vivado when implemented on the above-mentioned target board.

Figure 14(a)represents the raw decrypted signal and Figure 14(b) represents the complete encryption signals from hardware co-simulation. These plots contain the original message, raw decrypted signal at (Rx), convoluted signal and decrypted message signal. The raw decrypted signal is post-processed with the help of convolution and thresholding. The post-processing of the signal is implemented in MATLAB to retrieve the message signal from the raw signal. Convolution of two signals is carried out, first, large masking window ($u(t)$) and second, the difference between x signal and receiver decrypted signal 'X_r', say (m'(t)). The convolution of any two vectors $u(t)$ and m' (t) represents the overlapped area as shown below.

$$w(k) = \sum_j m'(j)u(k-j+1)$$

Once the differences are averaged with the large sliding window (moving-average), that goes through a squared function to amplify the signal.



(a) *(b)*

Figure 13: (a) Resource Utilization; (b) Dynamic On-Chip Power Estimate

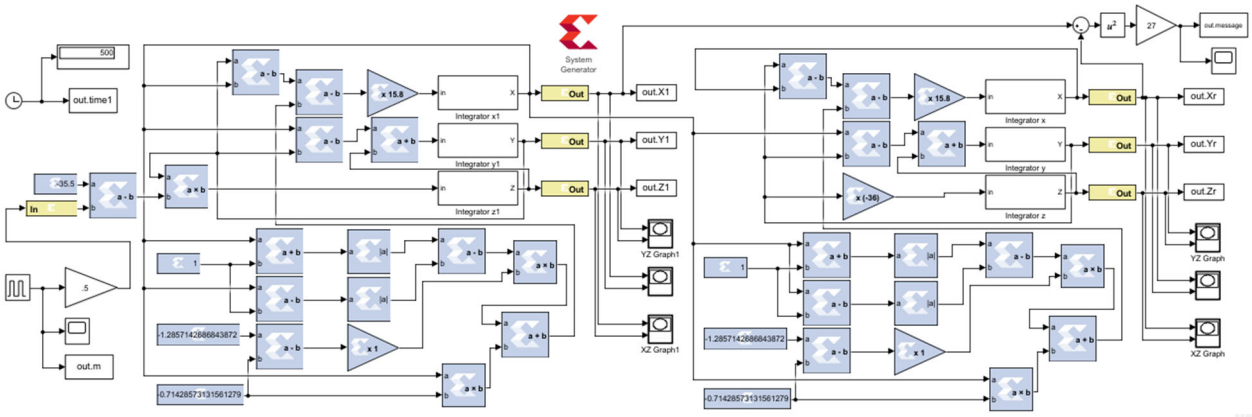
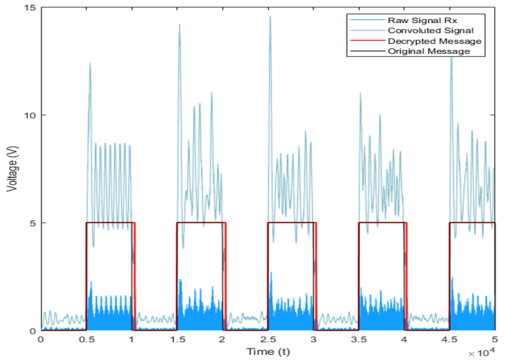
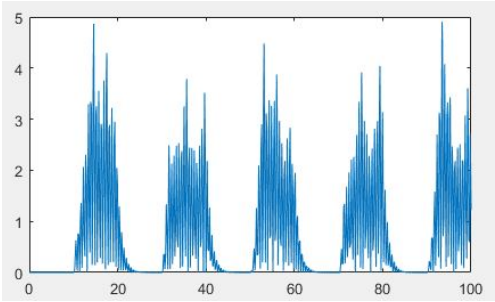


Figure 13: Xilinx System Generator design implantation of Encryption Architecture with Chua



(a)



(b)

Figure 14: (a) The raw decrypted signal (b) post-processed signal

VI. Conclusion

This work contributes toward the goal of achieving the chaos ciphering communication implemented on the chip along with the sensors to encode the data at its very origin. The study of state-of-art chaotic equations with simulation in multiple platforms i.e MATLAB, Simulink, LTSpice, and XSG enables achieve chaos implementation on hardware. The hardware implementation of chaotic transmitter and receiver are implemented using Chua, Lorenz, and SprottD on the Nexys-A7 FPGA board. This implementation provides a comprehensive understanding of resource utilization and power estimation.

The experimental observations from the power and resource utilization lead to the conclusion that Chau's circuit has more hardware utilization when compared to its counterparts on FPGA. Although, the LTspice implementation proves otherwise. The Chua's chaotic circuit uses ~9% and ~38% more hardware resources compared to Lorenz and SprottD respectively.

There have been multiple attempts to practically implement Chua's chaos equations in ciphering. This research supplements that and provides an encryption architecture that can be used in communications. Moreover, the research is more directed and focused on Implantable and Wearable Devices (IWDs), as they are resource-constraint and power-limited devices. With the advancement in electronics chip design technology, this industry is growing rapidly. At the same time, these devices are at the risk most risk of security breaches. Thus, this motivation is enough to justify the efforts in the ciphering industry to consider chaos as a way out even in the post-Quantum era.

Acknowledgment

This material is based upon work supported by the National Science Foundation under Grant No. 2131156.

Bibliography

[1] E. N. Lorenz, "Synchronization of chaos," *J. atmos. Sci 20 (1963),* p. 130.

[2] A. G. Radwan, A. M. Soliman and A. El-Sedeek, "MOS realization of the modified Lorenz chaotic system," *Chaos, Solitons & Fractals 21,* no. 3, pp. 553-561., 2004.

[3] F. J. Romeiras, C. Grebogi, E. Ott and W. P. Dayawansa, "Controlling chaotic dynamical systems," *Physica D: Nonlinear Phenomena,* vol. 58, no. 1-4, pp. 165-192, 1992.

[4] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. Brandao and D. A. B. e. al., ""Quantum supremacy using a programmable superconducting processor," *Nature,* vol. 574, no. 7779, pp. 505-510, 2019.

[5] J. E. Bourassa, R. N. Alexander, M. Vasmer, A. Patil, I. Tzitrin, T. Matsuura and D. S. e. al., "Blueprint for a scalable photonic fault-tolerant quantum computer," *Quantum 5,* p. 392, 2021.

[6] M. S. Azzaz, C. Tanougast, S. Sadoudi and A. Dandache, "Real-time FPGA implementation of Lorenz's chaotic generator for ciphering telecommunications," in *2009 Joint IEEE North-East Workshop on Circuits and Systems and TAISA Conference*, 2009.

[7] M. Jalilian, A. Ahmadi and M. Ahmadi, "Hardware Implementation of A Chaotic Pseudo Random Number Generator Based on 3D Chaotic System without Equilibrium," in *25th IEEE International Conference on Electronics, Circuits and Systems (ICECS)*, 2018.

[8] Luigi Fortuna; Mattia Frasca; Maria Gabriella Xibilia, Chua's Circuit Implementations Yesterday, Today and Tomorrow, World Scientific Publishing Co. Pte. Ltd, 2009.

[9] A. Hedayatipour, "Design and implementation of a multi-modal sensor with on-chip," PhD diss.,University of Tennessee, Tennessee, 2020.

[10] L. Merah, A. Ali-Pacha, N. H. Said and M. Mamat, "A Pseudo Random Number Generator Based on the Chaotic System of Chua's Circuit, and its Real Time FPGA Implementation," *Applied Mathematical Sciences,* vol. 7, no. 55, pp. 2719 - 2734, Jan 2013.

[11] W. A. Al-Musawi, W. Wali and M. A. Al-Ibadi, "Implementation of Chaotic System using FPGA," in *6th Asia-Pacific Conference on Intelligent Robot Systems*, Iraq, 2021.

[12] A. J. A. El-Maksoud, A. A. A. El-Kader, B. G.Hassan, M. A. Abdelhamed, N. G. Rihan, M. F. Tolba, L. A. Said, A. G. Radwan and M. F. Abu-Elyazeed, "FPGA Implementation of Fractional-Order Chua's Chaotic System," in *7th International Conference on Modern Circuits and Systems Technologies (MOCAST)*, Egypt, 2018.

[13] Z.A.S. Rahman, B. H. Jasim, Y. I. Al-Yasir, R. A. Abd-Alhameed, and B.N. Alhasnawi, "A new no equilibrium fractional order chaotic system, dynamical investigation, synchronization, and its digital implementation." *Inventions*, vol. 6. no.3 , p.49, 2021.

[14] E. Tlelo-Cuautle and M. Duarte-Villasenor, "Designing Chua's circuit from the behavioral to the transistor level of abstraction," *Applied Mathematics and Computation,* pp. 715-720, 2007.

[15] H. Xu, Z. Zhang, and M. Peng. "Novel bursting patterns and the bifurcation mechanism in a piecewise smooth Chua's circuit with two scales." *Nonlinear Dynamics, pp.* 1-17, 2022.