Memorias del Congreso Nacional de Control Automático
ISSN: 2594-2492

On the FPGA-based Implementation of the Synchronization of Chaotic Oscillators in Master-Slave Topology ⋆

Omar Guillen-Fernandez * **Alejandro Silva-Juarez** *
Ashley Melendez-Cano ** **Jose Cruz Nuñez-Perez** **
Esteban Tlelo-Cuautle *

* *INAOE, Department of Electronics, Luis Enrique Erro No. 1. Tonanztintla, Puebla, 72840 México (e-mail: etlelo@inaoep.mx)*
** *CITEDI-IPN, Department of Telecommunications, Instituto Politecnico Nacional No. 1310, Nueva Tijuana, México*

Abstract: Chaotic oscillators have been implemented using embedded systems like field-programmable gate arrays (FPGAs). Their applications in secure communications require the synchronization of them in a master-slave topology, for instance. However, this is not a trivial task because one must guarantee a low synchronization error that depends on the selection of an appropriate step-size of a numerical method. That way, this paper describes how to select the step-size for a successful simulation and how to implement the master-slave synchronization of two chaotic oscillators using FPGAs. We discuss details on the numerical simulation of the synchronization using the seminal work of Pecora & Carroll and also discuss FPGA issues. Finally, we implement a chaotic secure communication system to show that synchronization methods with high error produce loss of data, as shown by the transmission and reception of a color image using two chaotic oscillators.

Keywords: Chaos, synchronization, FPGA, secure communication system, numerical method, image processing.

1. INTRODUCTION

Chaotic oscillators have been implemented with different electronic devices and nowadays with embedded systems like field-programmable gate arrays (FPGAs) Tlelo-Cuautle et al. (2016). For instance, several chaotic oscillators introduced in Sprott (2003), are simulated and analyzed to generate their bifurcation diagrams, compute their Lyapunov exponents, fractal dimension and entropy. Those chaotic oscillators can be synchronized and implemented using FPGAs. However, one must guarantee that chaotic behavior will not be suppressed and that the synchronization error is low to avoid loss of data.

Among the currently available synchronization methods, this paper is based on the seminal work of Pecora & Carroll Pecora and Carroll (1990) in order to highlight that the synchronization error generates loss of data when implementing a secure communication system. In this manner, the cases of study are two Sprott's chaotic oscillators whose nonlinear functions are the multiplication of two state variables or a squared state variable. They are simulated using the simple Forward Euler method, from which we detail the FPGA-based implementation as already shown in Tlelo-Cuautle et al. (2016), where one can find applications to random number generators, neural networks and secure communications.

Chaotic oscillators have challenges in the development of new security applications. For example, as mentioned in Alam et al. (2018), chaotic circuit-based cryptography is a promising candidate to overcome the deficiency of conventional cryptography. Chaotic circuits are high sensitive to initial conditions and parameters, so that their behavior becomes difficult to predict and the phenomena can be compared with key-dependent confusion and diffusion in cryptography. In fact, generating the same cipher key in both transmitter and receiver is a challenge to guarantee security. This issue is highlighted herein by showing that a high synchronization error produces loss of data due to the bad selection of the step-size in a numerical method and the length of the digital word or computer arithmetic in an FPGA.

The development of accurate synchronized chaotic systems is quite useful for industrial Internet of Things, as shown in Wang et al. (2018). In general, for chaotic security systems, the design of the synchronization stage and the selection of appropriate parameters of the driv-

⋆ This work is partially supported by CONACyT under project 237991.

ing and response systems, are challenges to ensure the stability and minimization of the synchronization error. The following section summarizes the synchronization of two chaotic oscillators in a master-slave topology applying the seminal work of Pecora & Carroll. Afterwards, we detail the FPGA-based implementation and finally discuss issues that produce loss of data in a chaotic secure communication system.

2. SYNCHRONIZATION IN CHAOTIC SYSTEMS

The Pecora & Carroll synchronization scheme has often been described as a "master-slave" system topology. Essentially, this topology consists of two identical chaotic systems Pecora and Carroll (1998). Therefore, both chaotic systems are described by the same set of differential equations, with the same parameter values, but they can have different initial conditions. For synchronization to occur, the output from, at least, one of the coupled differential equations of the first chaotic system must be made available to the second chaotic system, as sketched in Fig. 1 Jovic (2011).

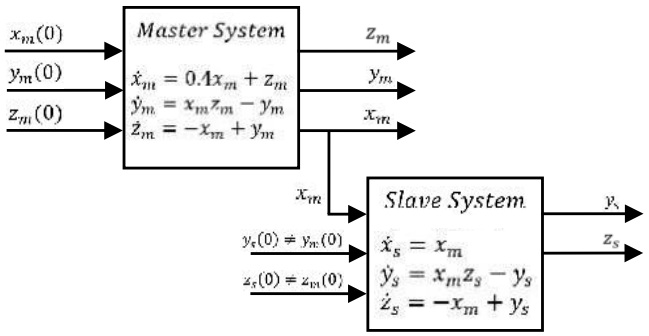


Fig. 1. The block diagram of the master−slave chaotic synchronization scheme using the state variable x as the driving signal.

To perform the synchronization it is possible to take any of the three variables x, y, z as driving, from the master system. The recommendation to the correct selection of the driver variable is the observation and determination of the influence that it has over the differential equations. Unlike other kind of synchronization, the method introduced by Pecora & Carroll is slow, because oscillation of the slave has to wait the output of the master. Although, the time iteration will increase at double.

Having defined the topology for the synchronization as the master-slave system in Fig. 1, the pattern that indicates that the system will be synchronized are the eigenvalues of the Jacobian of the slave system. If the eigenvalues of the real parts are negative, synchronization will be successful. This is a necessary condition but not enough since there may be a system with eigenvalues equal to zero and synchronization can occur.

The synchronization method proposed by Pecora & Carroll is tested herein by using two chaotic systems from Sprott's Collection Sprott (1994). The Sprott's case G is described in (1) and case L in (2), respectively,

$$\begin{aligned} \dot{x_m} &= 0.4x_m + z_m \\ \dot{y_m} &= x_m z_m - y_m \\ \dot{z_m} &= -x_m + y_m \end{aligned} \tag{1}$$

$$\begin{aligned} \dot{x_m} &= y_m + 3.9z_m \\ \dot{y_m} &= 0.9x_m^2 - y_m \\ \dot{z_m} &= 1 - x_m \end{aligned} \tag{2}$$

where m denotes the master block from Fig. 1. In this cases we consider the state variable x as drive because it is the variable that is present throughout the system and has an influence on the state variables y and z. The slave systems for both cases of Sprott are described by (3) and (4), respectively.

$$\begin{aligned} \dot{y_s} &= x_m z_s - y_s \\ \dot{z_s} &= -x_m + y_s \end{aligned} \tag{3}$$

$$\begin{aligned} \dot{y_s} &= 0.9x_m^2 - y_s \\ \dot{z_s} &= 1 - x_m \end{aligned} \tag{4}$$

To determine the step-size for the numerical simulation of the synchronization, one needs to evaluate the Jacobian of the slave system, which in for Sprott's case G it becomes,

$$\textbf{Jacobian } (J_G) = \begin{bmatrix} -1 & x_m \\ 1 & 0 \end{bmatrix}.$$

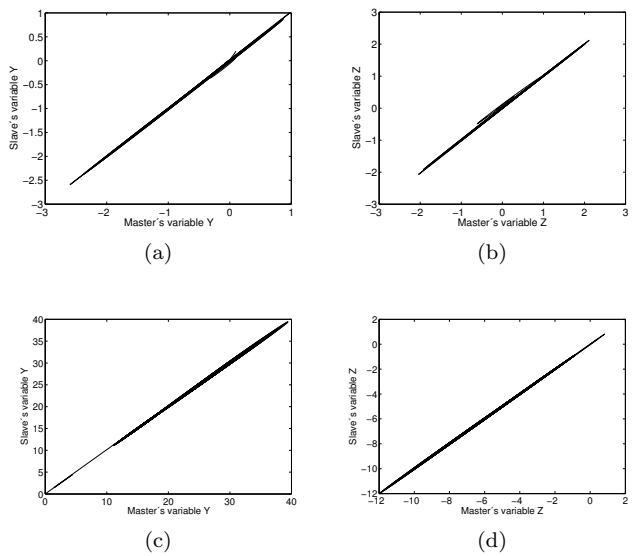
According to the equilibrium point, we have the value of x=2 and it is replaced in the Jacobian.

$$\textbf{Jacobian } (J_G) = \begin{bmatrix} -1 & 2 \\ 1 & 0 \end{bmatrix}$$

The eigenvalues of Sprott's case G are: $\lambda_{1,2}$ = -0.5±1.32j, as one sees $\{Re\} < 0$. Similarly, it is solved for the Sprott's case L but in this case $\lambda_{1,2} = 0$, so that $\{Re\} = 0$. Considering that these roots have a real and negative part, is very probable that the system can be synchronized.

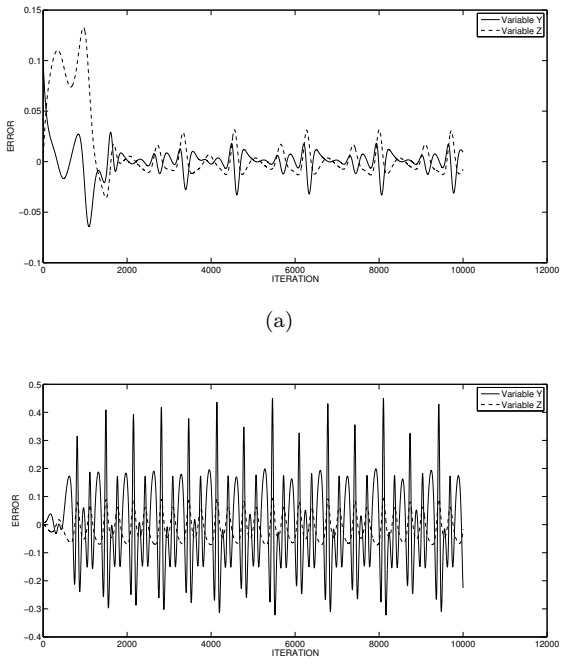
Realizing the simulation of the synchronization using $MATLAB^{TM}$ but programming the numerical method known as forward Euler, the solution of the system of differential equations is computed using a step size h = 0.01. The simulation results in this case are shown in Fig. 2. Figure 3 shows the synchronization errors obtained for both Sprott's cases. It can be observed that there exist a big error thus indicating that synchronization does not exist.

Changing the step-size the synchronization may occur. For example, reducing the step size 100 times, i.e. from 0.01 to 0.0001, the synchronization for both Sprott's cases occurs as shown in Fig. 4. In this case one can infer that a reduction in the value of the step size leads to a reduction in the synchronization error, which decreases in a similar amount, i.e. three magnitude orders, as shown in Fig. 5. Compared to the error shown in Fig. 3, it really diminished three orders. However, still the synchronization error is not as good as by using



(a) (b) (c) (d)

Fig. 2. Phase plane diagrams for the master and slave state variables: (a) y and (b) z for the Sprott's case G, and (c) y and (d) z for the Sprott's case L, both using a step size of 0.01.

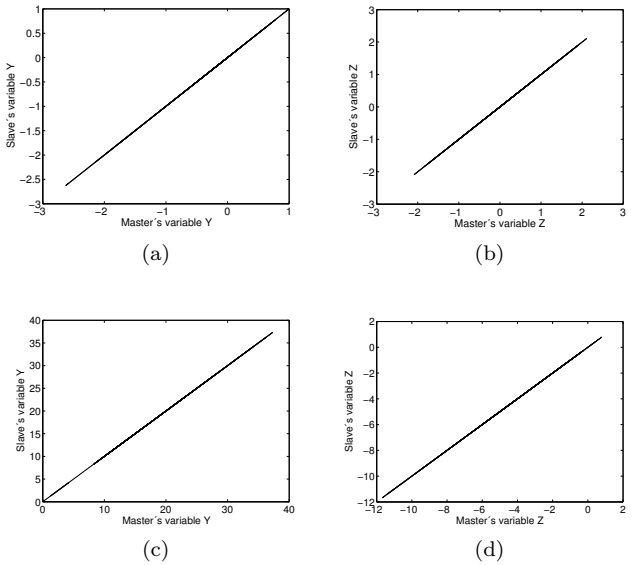


(a)

(b)

Fig. 3. Magnitude of the synchronization error using as drive x with step size 0.01 for the Sprott's cases: (a) G and (b) L.

other synchronization methods like the one based on Hamiltonian forms and observer approach applied in Tlelo-Cuautle et al. (2016).



(a) (b) (c) (d)

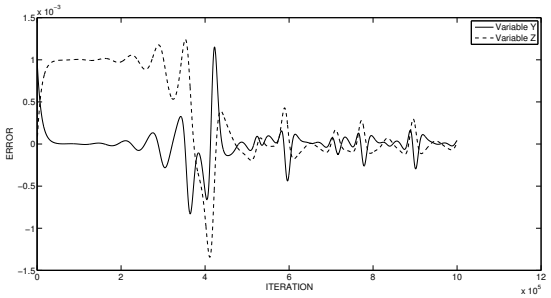
Fig. 4. Phase plane diagrams for the master and slave state variables: (a) y and (b) z for the Sprott's case G, and (c) y and (d) z for the Sprott's case L, both using a step size of 0.0001.

3. FPGA-BASED IMPLEMENTATION

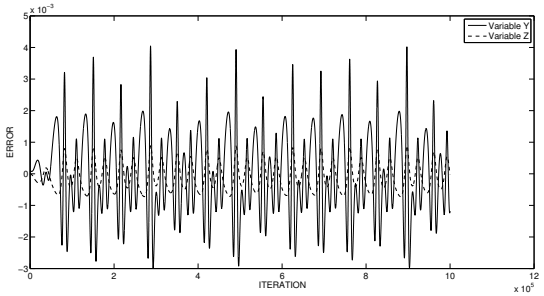
After performing the numerical simulation, the FPGA-based implementation of the chaotic oscillators requires the use of digital blocks that can be described by hardware description languages as Verilog or VHDL, and then synthesized into an FPGA. The same occurs for the master-slave system that performs the synchronization of two dynamical systems. The experiments were performed using the FPGA "Cyclone IV GXEP4CGX150DF31C7 " from Altera. The experimental observation of the chaotic attractors requires the use of a digital-to-analog converter, which have resolution of 16 bits.

The VHDL description of the synchronized system in the master-slave topology for Sprott's case G is performed as shown in Fig. 6. More details can be found in Tlelo-Cuautle et al. (2016). Those descriptions are synthesized into the FPGA and then they are observed by a Lecroy's oscilloscope as shown in Figs. 7 and 8. Recall that the synchronization is performed according to Pecora & Carrol.

The resources used in the Altera FPGA to the implementation of the chaotic systems synchronization based on Sprott's cases G and L, are shown in Table 1 and obtained from the synthesizer of Quartus II software. It is observed that the Forward-Euler discretization method uses less resources in the FPGA than 4th-order Runge-Kutta (RK4), more details can be found in Boubaker and Jafari (2018). In addition, the first method is enough to



(a)



(b)

Fig. 5. Magnitude of the synchronization error using as drive x with step size 0.0001 for the Sprott's cases: (a) G and (b) L.

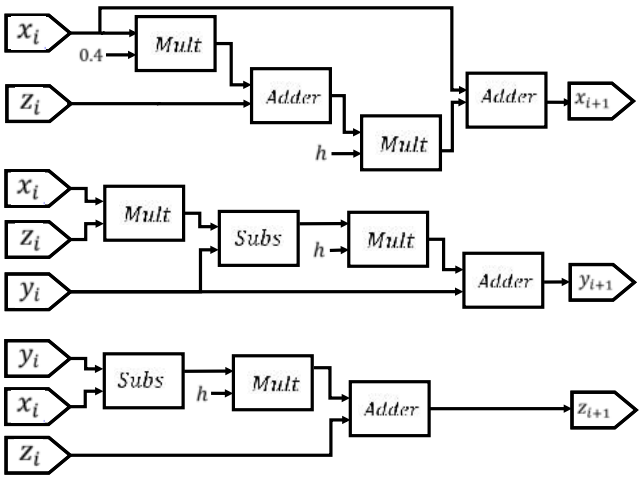
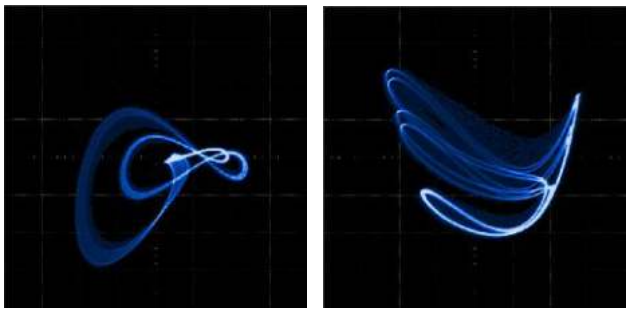


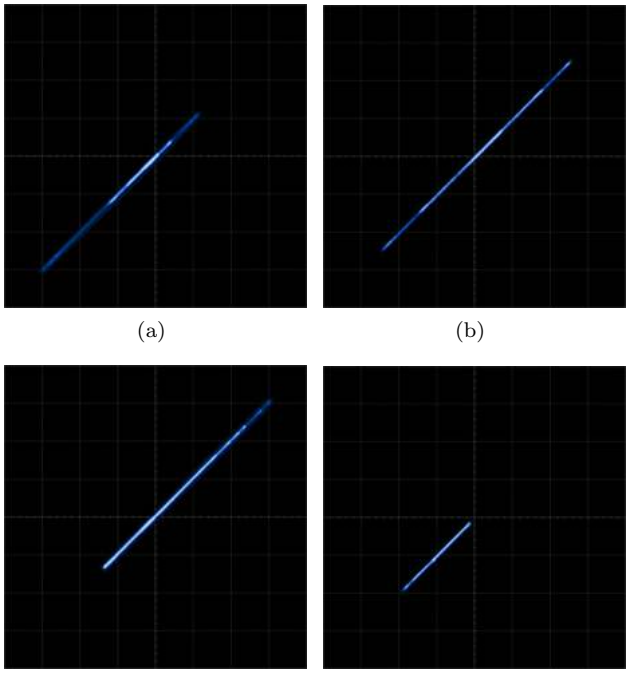
Fig. 6. VHDL description of the main blocks to evaluate the equations of the Sprott's case G for the state variables $x_{i+1}, y_{i+1}, z_{i+1}$ from (1).

solve the chaotic systems and generate chaos. The last column presents the time occupied by an iteration, obtained from the multiplication of the maximum frequency and the number of cycles.



(a) (b)

Fig. 7. Experimental observation of the Sprott's attractors in their phase-space portraits ($x(t)$ vs. $y(t)$) with the following initial conditions: Sprott case G using $x_m(0) = 0.1$, $y_m(0) = 0$ and $z_m(0) = 0$ and Sprott case L using $x_s(0) = 0.1$, $y_s(0) = 0$ and $z_s(0) = 0$, respectively. In the oscilloscope channel A and B: 1 Volt/Div.



(a) (b)

(c) (d)

Fig. 8. Synchronization of the master-slave topologies: Sprott G (a) $y_m(t)$ vs. $y_s(t)$, (b) $z_m(t)$ vs. $z_s(t)$, and Sprott L (c) $y_m(t)$ vs. $y_s(t)$ and (d) $z_m(t)$ vs. $z_s(t)$. In the oscilloscope channel A and B: 1 Volt/Div.

4. APPLICATION TO IMAGE TRANSMISSION AND DISCUSSION

The synchronization applying the method of Pecora & Carroll Pecora and Carroll (1990) makes the slave able to follow the master oscillator. If this occurs, then one can implement a chaotic secure communication system as described in Tlelo-Cuautle et al. (2016), which basically can

Table 1. Resources associated to the Pecora-Carroll synchronization implementation using the FPGA Ciclone IV GX-EP4CGX150DF31C7

Chaotic system	Numerical method	Logic elements	Registers	Maximun frequency (MHz)	Cicles for iteration	Iteration latency (ns)
Case G	Forward-Euler	1096	751	111.31	20	180
	RK4	3131	1763	108.31	36	332
Case L	Forward-Euler	1108	772	113.6	22	194
	RK4	3350	1919	115.83	40	345

be a system that transmit contaminated data (addition of chaos to the original image) and then the information is recovered by eliminating chaos (subtraction of chaos to the chaotic channel), also known as masking data, like audio, image or video. This chaotic communication system is sketched in Fig. 9 Jovic (2011).

The process begin masking the original data (in this case an image) with the chaotic drive (master) of the transmitter system; then, the resultant contaminated signal with chaos travels through a secure medium or channel to the slave system, where the chaotic receiver unmask the data to obtain or recover the original image. If perfect synchronization is performed then the original and the recovered images must be exactly equal, while ideally the correlation between the chaotic channel and the image should be zero.

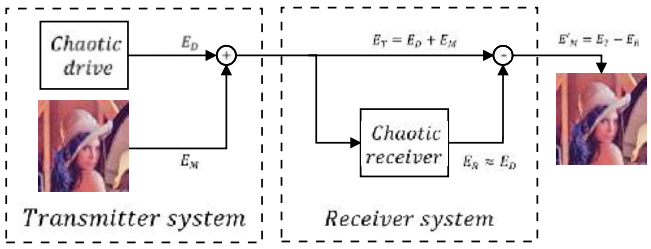


Fig. 9. Scheme for chaotic secure communications.

Figures 10 and 11 show experimental results of the application of the chaotic secure communication system using both cases of Sprott, namely: case G and L described above. In both cases, the original or the image being transmitted is observed a the left side of the Figures. This image is introduced into the FPGA from a personal computer applying the serial communication protocol RS-232 with a speed of 128,000 Baud, but any protocol can be used. The masking of the image with the chaotic information generates the chaotic channel data that is shown in the middle of the Figures. As one sees, the original image is almost well encrypted. Finally, in the receiver stage, the chaos generated by the slave oscillator is subtracted from the chaotic channel and then the recovered image is shown at the rigth side of the images in Figs. 10 and 11. The recovered image is again send to the personal computer to observe the data.

As one can see in the recovered images using both cases of Sprott, some information is lost due to the

Fig. 10. Master−Slave Synchronization of the Sprott G System.

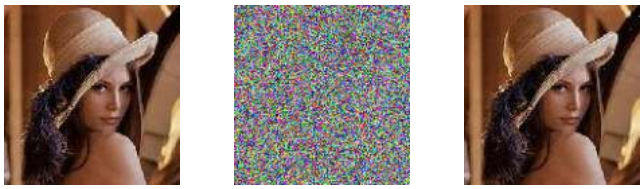


Fig. 11. Master−Slave Synchronization of the Sprott L System.

synchronization error, which is not as small as required. In fact, the magnitude of the synchronization error using as drive x with step size 0.0001 for the Sprott's cases G and L shown in 5, is not constant, so that perfect synchronization does not occur. This is not a surprise because the method proposed by Pecora & Carroll was the very first one and the salve system is reduced to two differential equations. This limitation produces such an error as demonstrated herein even for a more small step size. Another source of error in the FPGA-based implementation of a chaotic secure communication system is the one caused by the numerical integration method. As one knows forward Euler is the simplest numerical method and it has the biggest error if the step size is not the appropriate one. Therefore, in a bigger system as the whole synchronization, if the step size is not the good one, then the numerical error increases. Another issue is that the FPGA needs to define the computer arithmetic, which is not infinite and then the selection of a small digital word may also increase the error in both, the chaotic oscillator and the synchronization.

Other problem that one must take into account when observing the experimental data in an oscilloscope, is the use of a digital-to-analog converter, which in the majority of cases it is of 16 bits in resolution. Therefore, if one uses fixed-point notation of 32 bits for processing the chaotic signals and then in the secure communication system, then 16 bits may be loss when using the digital-to-analog converter. In this manner, the synchronization error still having a step size lower than 0.0001, may not be avoided due to the limitations in both the computer arithmetic in the FPGA and the resolution of the digital-to-analog converter. In other words, the truncation on the number of bits in the FPGA and its connection to the digital-to-analog converter is insufficient to get a successful recovery of the data free of errors. The solution is the selection of another synchronization method that be able to reduce the synchronization error.

5. CONCLUSION

This paper showed the application of the synchronization method introduced in the seminal work of Pecora & Carrol to two chaotic oscillators taken from Sprott's cases. Simulation results were presented with different step sizes using the forward Euler numerical method, thus concluding that a low step size leads to better results. The whole synchronization method was implemented in an FPGA and then a chaotic secure communication system was developed and used to test the transmission of an image. We highlighted that the synchronization method generates and error that affects the transmission of data in a chaotic system and that to avoid loss of information another synchronization method must be used to reduce numerical errors.

REFERENCES

Alam, M.M., Chowdhury, S., Park, B., Munzer, D., Maghari, N., Tehranipoor, M., and Forte, D. (2018). Challenges and opportunities in analog and mixed signal (ams) integrated circuit (ic) security. *Journal of Hardware and Systems Security*, 2(1), 15–32.

Boubaker, O. and Jafari, S. (2018). *Recent Advances in Chaotic Systems and Synchronization: From Theory to Real World Applications*.

Jovic, B. (2011). *Synchronization techniques for chaotic communication systems*. Springer Science & Business Media.

Pecora, L.M. and Carroll, T.L. (1990). Synchronization in chaotic systems. *Physical review letters*, 64(8), 821.

Pecora, L.M. and Carroll, T.L. (1998). Master stability functions for synchronized coupled systems. *Physical review letters*, 80(10), 2109.

Sprott, J.C. (1994). Some simple chaotic flows. *Phys. Rev. E*, 50, R647–R650. doi:10.1103/PhysRevE.50.R647. URL `https://link.aps.org/doi/10.1103/PhysRevE.50`.

Sprott, J.C. (2003). *Chaos and time-series analysis*, volume 69. Citeseer.

Tlelo-Cuautle, E., de la Fraga, L., and Rangel-Magdaleno, J. (2016). *Engineering applications of FPGAs*. Springer.

Wang, T., Wang, D., and Wu, K. (2018). Chaotic adaptive synchronization control and application in chaotic secure communication for industrial internet of things. *IEEE Access*, 6, 8584–8590.

