MARECA, P. y BORDEL, B., 2019. Robust hardware-supported chaotic cryptosystems for streaming commutations among reduced computing power nodes. Analog integrated circuits and signal processing, vol. 98, no. 1, ISSN 0925-1030. DOI 10.1007/s10470-018-1262-x.

Robust hardware-supported chaotic cryptosystems for streaming commutations among reduced computing power nodes

Pilar Mareca [1], Borja Bordel [1,*]

[1] Universidad Politécnica de Madrid. Avenida Complutense nº 30. 28040 - Madrid (España); E-Mails: mpmareca@fis.upm.es, bbordel@dit.upm.es

***** Author to whom correspondence should be addressed; E-Mail: bbordel@dit.upm.es; Tel. 91 549 57 00 ext. 2011

ABSTRACT

Most recent technological proposals, such as Cyber-Physical Systems or Wireless Sensor Networks, consist of a collection of tiny nodes designed to be seamless integrated into daily living objects. These nodes then, due to their miniaturized configuration, use to present very limited processing capabilities. Because of that, in general complex algorithms, as which are employed today to secure communications, cannot be implemented in these new systems. Thus, new instruments for security are needed, with a special mention to hardware-supported solutions. Therefore, in this paper different robust hardware-supported cryptosystems based on Chua's circuit are proposed, studied ad compared. The described solutions are specifically designed to be employed in streaming communications among reduced computing power nodes. Moreover, an experimental validation is proposed comparing the performance of the proposed technologies and other existing solutions.

KEYWORDS

Cryptography; Chaos; Hardware-supported technologies; Chaotic cryptosystems; Chaotic masking; Chua's circuit

MATHEMATICS SUBJECT CLASSIFICATION 2010

34H10; 34D06; 37C75

ABBREVIATED TITLE

Robust hardware-supported chaotic cryptosystems

1. INTRODUCTION

In the last decade, many different new technological paradigms have been proposed. From Cyber-Physical Systems (defined as integrations of computation and physical processes [1]) to Wireless Sensor Networks (consisting of a set of spatially distributed autonomous tiny sensor nodes to monitor and recording physical or environmental conditions, which act as both data generators and network relays [2]). There is, however, a common characteristic among all these proposals: they consider miniaturized and reduced computational power devices as main elements into the system.

In fact, although many times nodes making up a unique system are a heterogeneous collection of devices with very different functionalities and capabilities, various aspects are common to every element [3]: self-configurable, delay-tolerant, decentralized, etc. Among all of these characteristics, one of the most important aspects is the reduced size and the limited processing (and communication) capabilities [4] of the nodes. In this context, traditional algorithms or network solutions are not directly applicable to these new systems, as telecommunication networks (such as Internet or Frame Relay) incorporate additional infrastructures (such as the power supply) and devices with high capacities which cannot be considered in the future engineered systems.

In that way, some of the most important technological solutions for communication networks (such as routing protocols or handovers) should be redesigned and adapted to these new systems. One of the most affected fields by these limitations is security. Security is a key problem in most recent proposals [5] (see Figure 1, where the proposed reference architecture for Cyber-Physical Systems by the NIST is showed), and several different solutions addressing this challenge may be found.

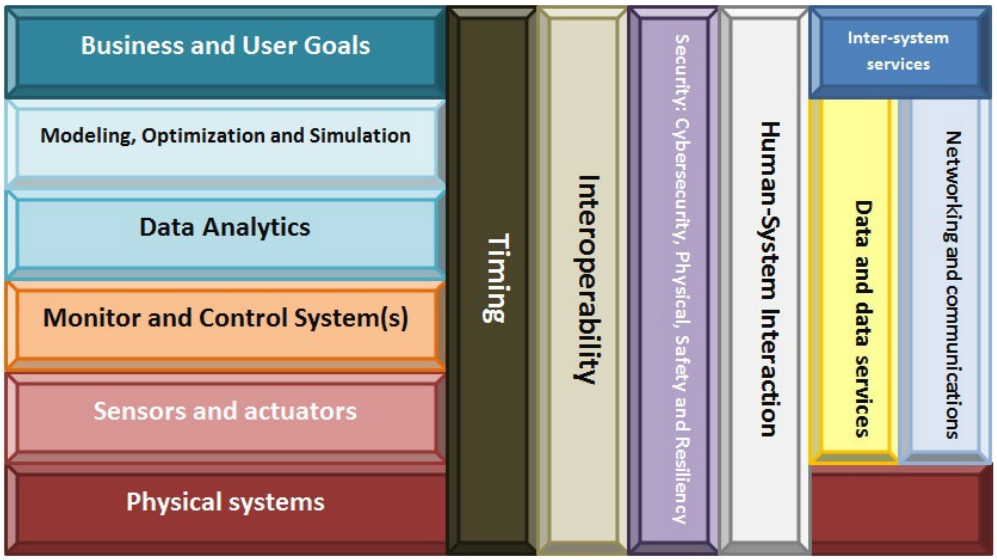

Figure 1. NIST reference architecture for Cyber-Physical Systems

Firewalls, secure routing protocols or encryption technologies demand too many computational resources to be applied to new engineered systems (usually composed of small microprocessors), so new approaches are demanded. In particular, hardware-supported

technologies seem to be one of the most promising solutions [6]. Nevertheless, in general, hardware-assisted technologies are based on the inclusion of additional co-processors being able to perform a complex algorithm in a very efficient way. In respect to security, for example, hash functions in order to protect message transmissions are usually implemented using these technologies. This type of solutions, however, increases the size of device to be integrated into technological systems and, besides, they are not applicable to one of the most promising applications of pervasive computing.

Continuous sensing of environmental or biological signals (such as border control or monitoring vital signals) is nowadays one of the most investigated applications for future technological deployments [5]. In these cases, nevertheless, nodes must establish streaming communications among them, instead of employing packet-oriented links. The use of co-processors, then, is not a valid solution, but secure communications are still required (mainly, in order to maintain the privacy level required by the particular application). In this context, other technologies should be investigated. The proposed solution has to be fast, efficient and protect data against intruders in the communications channel (the most common attack on these wireless systems).

In previous works [7], the authors have briefly investigated some possible solutions to this problem. In this paper, those proposals are extended and complemented.

Therefore, the objective of this paper is to describe a hardware-based cryptosystem for streaming communications in new technological (pervasive) systems. The proposed technology employs chaotic cryptography in order to cipher the information signals before being transmitted through the wireless communications interface. An adapted secure communication theory to chaotic communications is presented, and different proposals in order to obtain a robust cryptosystem are studied. Besides, in order to validate the usability of our proposals, a chaotic masking device is designed, addressing the implementation challenges related to these solutions. As a result, a reduced size and a very low power consumption module based on Chua's circuit is described, where loading effects typical of this circuit are removed by means of a robust implementation of the electronic circuit.

The rest of the paper is organized as follows: Section 2 describes the state of the art on security solutions for future engineered systems and chaotic cryptosystems; Section 3 includes the mathematical formalization of the proposed secure communication theory and the theoretical study of the three proposed schemes. Section 4 describes the robust electronic implementation of one the proposed solutions and presents an experimental validation in order to test the performance of the described technology; Section 5 contains the experimental results and Section 6 concludes the paper.

2. STATE OF THE ART

Security is one of the key topics nowadays. Different privacy, security and trust solutions have been proposed in relation to Cyber-Physical Systems (CPS), Internet of Things (IoT) and Wireless Sensor Networks (WSN) and other similar paradigms. In this section, it is presented the state of the art on this popular topic. Besides, it is described the previous security solutions based on our selected supporting technology: the chaotic systems.

2.1 SECURITY AND FUTURE TECHNOLOGICAL SYSTEMS

First, works proposing different taxonomies describing the new cyber-attacks that may suffer systems such as CPS or WSN may be found [10]. Other important classifications investigate the uncertainties in those systems [9] or the future challenges in relation to cyber security [8]. Finally surveys about security issues and cyberattacks in WSN or IoT scenarios may also be found [12][18]. In all these cases, the conclusion is that traditional corporate IT (Information Technology) security is different from security solutions for new engineered systems (higher availability, operate at real-time, be lighter, etc.) [8]. Thus, several proposals for each one of the required new solutions have been reported.

In particular, most works on security for new engineered systems describe secure routing protocols trying to avoid cyberattacks such as the sinkhole attack or the Sybil attack [11]. Other similar works propose intrusion-tolerant routing techniques [13] or new layers supporting secure data exchange at low-level [14] (typically employing block codes and message encryption solutions). Works on generic security protocol (in order to support, for example, authentication) [15] are also common. In general, information encryption in those systems is quite common, and only some works about hardware-supported solutions might be found [16]. These proposal, however, are focused on applications where nodes communicates opportunistically and traffic around the network remains low. Continuous monitoring applications (or streaming communications) are not usually covered by these technologies. Different studies analyzing the problem of IP-based communication technologies for future technological systems have been also reported [20].

More exhaustive works even study how to secure the information flow which initiates the secure connections [17] or the design cycle which should be followed in order to define the most appropriate security solution for a collection of devices with a given characteristics [19].

Different architectures being able to support security policies, suing centralized entities [21] or a distributed management system have been also described [22]. Multimedia traffic (which requires a streaming communication) is usually considered only if enough powerful devices are included.

Finally, other concepts related to security such as privacy or trust [23][24] are also investigated in different works. Most interesting papers are which describe solutions to anonymize communications in these new engineered systems. Applications to anonymous streaming communications [25] (considering high computational power devices) and authentication protocols based on different encryption techniques [26][27] have been described.

The main cause of the impossibility of apply these previous solutions to resource constraint devices Is that using any encryption scheme requires extra bits, extra memory, extra battery power, etc. so encryption could increase delay, jitter and packet loss in the system [28] (especially if streaming communications are considered). Then, novel technologies should be applied in these scenarios in order to, for example, guarantee a secure access to the physical layer (among other possibilities). One of these technologies may be chaotic cryptography.

2.2 CHAOTIC CRYPTOSYSTEMS

The origin of chaotic cryptography is the synchronization phenomenon which appears in chaotic dynamics [35]. In fact, various chaotic systems may be synchronized if they are connected in the appropriate way [36]. Very different schemes have been proposed in order to generate this effect [37][38], although one of the most commonly employed is Pecora and Carroll's proposal [39][40].

Actually, apart from the synchronization phenomenon, very complex schemes of chaotic cryptography have been defined [29][30]. Discrete dynamics have been employed as pseudo-aleatory code [31], unidimensional maps have been integrated into spread spectrum techniques [32] and other solutions based on external keys have been described [33]. Additionally, digital and analog systems have been described [34]; and high-order systems have been proposed to be employed in advanced cryptosystems [42]. However, all these proposals are based on complicated software algorithms. Thus, for constraint resource devices, most simple hardware-supported solutions are required. It is in this point where synchronization turns very important.

Several works have investigated the use of synchronized chaotic systems to support secure communications [43][44]. Different proposals, named as chaotic modulation or chaotic masking, have been described [45]. In this sense, Cuomo and Oppenheim [46] propose a couple of synchronized chaotic circuits as cryptosystem (based on Lorenz dynamics), capable of hiding the transmitted information. Moreover, Kokarev [47] has demonstrated the viability of chaotic masking solutions for other dynamics, such as the Chuas's circuit [48].

In fact, Chua's circuit has been proved to be able to be implemented in a very compact way using microelectronics techniques [51]. Moreover, different relevant works have studied the synchronization phenomenon in this chaotic system [49][50], so (if the adequate configuration is reached) it should be possible to design a small-size functional cryptosystem based on this dynamics.

All the previously cited proposals, however, are always implemented using numerical programming and/or simple numerical simulation environments. Thus, practical deployment problems (such as the loading effects) are not addressed (and may severally affect practical systems). Our proposal covers this gap as a robust hardware implementation (valid to be implemented in sensor nodes) is described.

3. CHAOTIC CRYPTOSYSTEMS FOR STREAMING COMMUNICATIONS

Various works have demonstrated that cryptographic techniques for protecting the transmitted information among resource constraint nodes cannot be based on traditional digital schemes (which employ keys and complex algorithms) [28]. Instead, analog hardware-supported techniques are required. Specially, steganography seems to be one of the better alternatives. Steganography aims at hiding the existence of the data flows among the nodes by embedding information into other signals, so transmissions are not perceptible and hence, the medium looks just like usual. In this context, chaotic masking can be a steganography solution for streaming communications among low computational power devices.

In this Section it is proposed a hardware-supported steganography solution based on chaotic dynamics. First a basic theory for secure communications based on chaos is described. Then, the synchronization possibilities of Chua's circuit are evaluated, and one configuration is selected and numerically studied.

3.1. THEORETHICAL BASIS FOR SECURE COMMUNICATIONS BASED ON CHAOS

The basic working scenario is showed on Figure 2. Two constraint resource nodes are communicating through a wireless interface. Both nodes are provided with a chaotic circuit. Then, many authors [46][47] have proved that both circuits can get synchronized if one of them (the transmitter) sends some information about the generated chaotic signals to the other (the receptor). Thus, the chaotic signal creates a perturbation in the spectrum which may hide the information streaming, so intruders cannot capture the communication (as in steganography solutions). However, as both nodes can get synchronized, the receptor may recover the information using a subtractor.

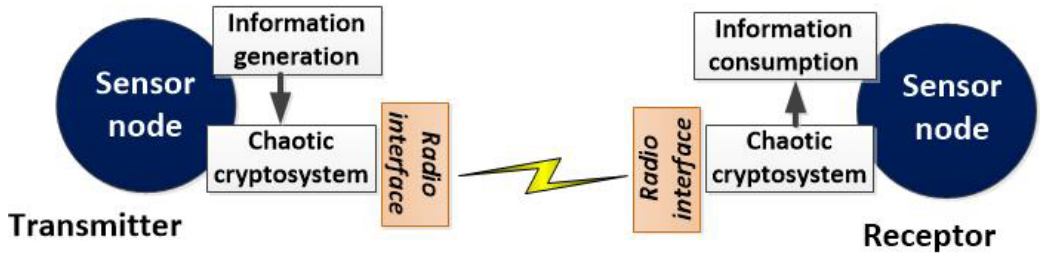

Figure 2. Basic scenario

Since the synchronization phenomenon in chaotic systems was discovered, several works have investigated the use of chaotic signals as information carriers [52]. Although various authors [53] criticize the use of chaos in cryptosystems, mainly because a pretended lack of versatility; each day more researchers employ chaos as supporting technology for their secure communication systems [54]. Besides, secure communication systems based on chaos are broadband systems by default. In particular, they belong to a very useful group of techniques named as Spread Spectrum Communications [55] (mainly employed in military applications although techniques such as CDMA -Code Division Multiple Access- are moving them to the

civil world). In that way, chaotic cryptosystems are the lighter way of designing secure multimedia communications (or streaming communications, in general).

The basic scheme for a chaotic cryptosystem is showed on Figure 3. An information signal is introduced into the transmitter, which produces a chaotic signal. As said, this signal contains the information to be transmitted, but it is totally hidden by the "chaotic noise". The receptor which is provided with the necessary key, may recover the information signal (o a good approximation of it, depending on the case).

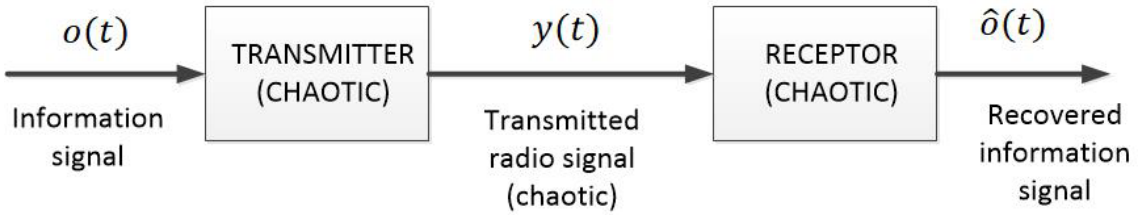

Figure 3. General scheme of a chaotic cryptosystem

Thus, a transmitter in a chaotic cryptosystem performs two actions: (i) encrypts the information and (ii) spread the information signal power along the entire chaotic frequency spectrum (which, in a good chaotic cryptosystem, is much wider than information signal one). In fact, these activities are the base of the most sophisticated cryptosystems nowadays [56]. However, chaos based solution may perform both actions in a unique phase (simultaneously) and (moreover) very simple, small and low-energy circuits can be employed as main element in the cryptosystem. Thus, this type of solutions perfectly fits the requirements or the study scenario: they consume very few resources and they may be miniaturized.

Although in some configurations the information signal may be obtained in a non-coherent way (using statistical methods), these applications are not useful for secure communications. Then, in order to design a valid cryptosystem, demodulation must be coherent. In that way, when a chaotic cryptosystem is designed or its operation stars, firstly a good synchronization state must be reached. See Figure 4. Mathematically, $\vec{X}$ represents the chaotic transmitter and $\vec{\xi}$ the receptor (1). y and η are the reference signal of each system. Mathematical model is described considering time as a continuous variable (analog systems), but may be easily transformed to represent discrete signals (digital systems).

$$\begin{gathered}\dot{\vec{X}} = \vec{F}(\vec{X}) \\ \dot{\vec{\xi}} = \vec{F}(\vec{\xi}, y) \\ y = g(\vec{X}) \quad \eta = \hat{g}(\vec{\xi}, y)\end{gathered} \tag{1}$$

Besides, it is necessary to consider that both systems follow the same evolution if initial conditions are identical in both dynamics (2).

$$\begin{gathered}\vec{F}\left(\vec{X}, g(\vec{X})\right) = \vec{F}(\vec{X}) \\ \hat{g}(\vec{X}, g(\vec{X})) = g(\vec{X})\end{gathered} \tag{2}$$

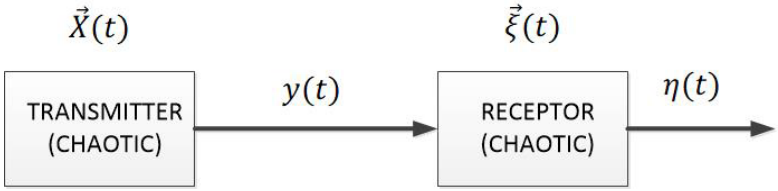

Figure 4. Synchronization scheme

In period systems, two remote dynamics may be synchronized if they are phase locked, but in remote chaotic system with different initial conditions, both dynamics tend to diverge exponentially. Thus, in the proposed scenario, the transmitter synchronizes with the receptor if they converge exponentially (3).

$$\|\eta(t) - y(t)\| \leq e^{-\omega t}\|\eta(0) - y(0)\| \quad \textbf{(3)}$$

The ω parameter is named as synchronization rate. If the synchronization rate depends only on the distance $\|\eta(t) - y(t)\|$ but not on the particular selected initial conditions, then the transmitter and the receptor synchronize uniformly. In that way, limits to the required time to reach a "good synchronization" (for a giver precision) may be considered. In general, besides, if both systems get synchronized not only their reference signals are synchronized, also their entire states.

The particular expression or pattern selected for $g(\cdot)$ and $\hat{g}(\cdot)$ and the relation between $\vec{F}(\cdot)$ and $\hat{\vec{F}}(\cdot)$ determines the synchronization scheme. Basically, there are three possible configurations [57]: (i) imposition of a state, (ii) drive-response coupling and (iii) lineal error feedback coupling. As it is which requires a smaller size and a little number of extra components, we are selecting a synchronization configuration based on the imposition of a state (see Figure 5).

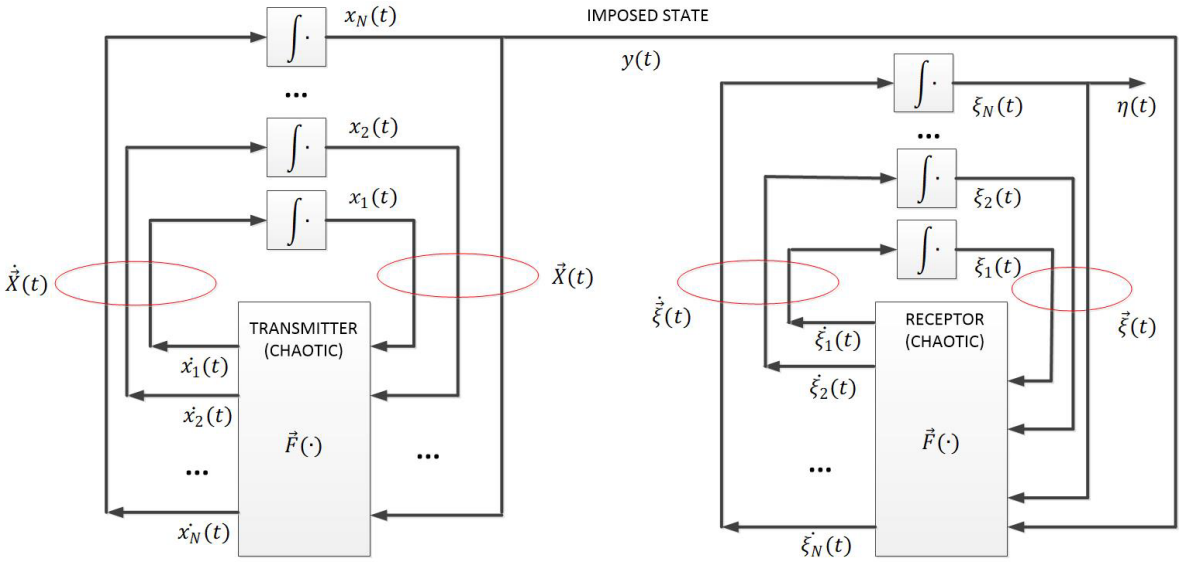

Figure 5. Synchronization configuration based on the imposition of a state

Mathematically (4), this scheme implies to remove one of the variables of the receptor from a subset of its components and introduce in its place a signal (state) from the transmitter.

Moreover, as can be seen, both functions $\vec{F}(\cdot)$ and $\vec{\hat{F}}(\cdot)$ are considered to be equal, and $g(\cdot)$ and $\hat{g}(\cdot)$ functions are defined as the identity function (they do not introduce any modification).

$$\dot{\vec{X}} = (x_1, x_2, \dots, x_j, \dots, x_N) = \vec{F}(\vec{X})$$

$$\dot{\vec{\xi}} = \vec{F}(\vec{\xi}, y) = \vec{F}(\vec{\xi}, x_j) = \begin{cases} F_1(\xi_1, \xi, \dots, \xi_j, \dots, \xi_N) \\ F_2(\xi_1, \xi, \dots, \xi_j, \dots, \xi_N) \\ \dots \\ F_k(\xi_1, \xi, \dots, x_j, \dots, \xi_N) \\ \dots \\ F_N(\xi_1, \xi, \dots, x_j, \dots, \xi_N) \end{cases} \quad \textbf{(4)}$$

Once synchronization is reached, the coupled chaotic systems may be used as the base for a cryptosystem for resource constraint devices. Using the same synchronization scheme different secure communication systems may be constructed. In particular, using the configuration showed on Figure 5 three are the most employed schemes of chaotic cryptosystems: chaotic masking [58], chaotic shift keying [59] and modulation of a chaotic carrier [60].

Although solutions based on the modulation of a chaotic carrier are the most simple, they present some practical problems related to the amount of noise they can tolerate and their robustness. On the other hand, chaotic shift keying schemes are the most robust, but involve three different circuits instead of two of them as the other proposals. As a compromise, we select for the proposed cryptosystem for constraint resource devices a chaotic masking scheme. This approach, in some occasions, present also instability and robustness problems (which as analyzed and solved in this work), but the designed cryptosystems may be implemented in smaller spaces.

Figure 6 shows the general scheme for a chaotic masking scheme.

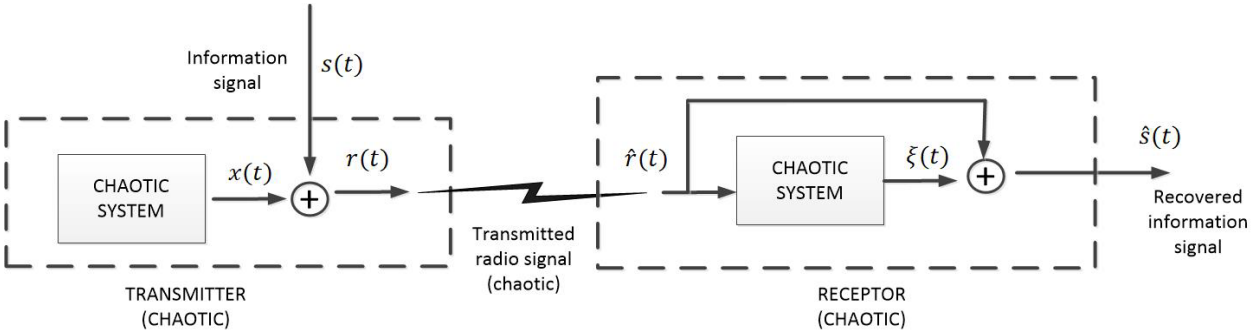

Figure 6. General scheme for a chaotic masking

In chaotic cryptosystems, an information signal $s(t)$ is added to the output $x(t)$ of a chaotic dynamic by the transmitter. This signal is transmitted through the radio channel. In the receptor, an identical chaotic system tries to synchronize with the transmitter using the received $\hat{r}(t)$ signal, which could present some "random noise" due to wireless transmission. From this point of view, besides the problems associated with the radio channel, $s(t)$ is a

perturbation which is introduced in the synchronization scheme, so the final synchronization state is slightly affected and the recovered information signal $\hat{s}(t)$ may be different to the original one $s(t)$. However, it is proved that if the induced synchronization error is small, compared to the original information signal $s(t)$, then, the obtained recovered signal is a good approximation of the sent information. As a consequence, in general, in this kind of systems, a weaker (not uniform) synchronization definition is considered (5).

$$\lim_{t\to\infty} \|\eta(t) - y(t)\| = 0 \tag{5}$$

Mathematically (6) the representation of a chaotic masking scheme is an elemental extension of the synchronization scheme through the imposition of a chaotic state. n is a realization of a stochastic process representing Gaussian white noise.

$$\dot{\vec{X}} = (x_1, x_2, \dots, x_j, \dots, x_N) = \vec{F}(\vec{X})$$

$$r = x_j + s$$
$$\hat{r} = r + n$$

$$\dot{\vec{\xi}} = \vec{F}(\vec{\xi}, y) = \vec{F}(\vec{\xi}, x_j) = \begin{cases} F_1(\xi_1, \xi, \dots, \xi_j, \dots, \xi_N) \\ F_2(\xi_1, \xi, \dots, \xi_j, \dots, \xi_N) \\ \dots \\ F_k(\xi_1, \xi, \dots, x_j, \dots, \xi_N) \\ \dots \\ F_N(\xi_1, \xi, \dots, x_j, \dots, \xi_N) \end{cases} \tag{6}$$

$$\hat{s} = \hat{r} - \xi_j$$

The challenge is to select a chaotic dynamic and design a particular implementation being able to offer a good synchronization scheme under certain level of perturbations. The next subsection deals with this issue.

3.2. CHUA'S CIRCUIT: SYNCHRONIZATION AND APPLICATIONS TO SECURE COMMUNICATIONS

Almost every chaotic dynamic may be employed in masking systems. Nevertheless, considering the reduced size and low resources of the nodes in future engineered systems, it is important to select a dynamic with a compact, low-energy and computationally easily to manage (but robust) electronic implementation. Among the paradigm systems (such as Lorenz's system [61][62] or Chen [63]) and the most recent proposals looking for very complex high-order dynamics [42], Chua's dynamic (7) is which better meets those requirements. In fact, many synchronization schemes for the Chua's dynamic are available, even some of them are implemented using microelectronic techniques putting them into a much reduced casing [51].

$$\begin{gathered} \dot{x_1} = \alpha\left(x_2 - x_1 - \left(m_1 x_1 + \frac{1}{2}(m_0 - m_1)(|x_1 + 1| - |x_1 - 1|)\right)\right) \\ \dot{x_2} = x_1 - x_2 + x_3 \\ \dot{x_3} = -\beta x_2 \end{gathered} \tag{7}$$

Different masking schemes based on Chua's system have been propose. In particular, adaptive control techniques [43], passive-active decompositions [52] and other synchronization techniques [64] have been used as base for the chaotic masking systems. However, as said in the previous subsection, the most simple, and possible robust, synchronization scheme is based on the imposition of a chaotic scheme.

Nevertheless, due to practical implementation considerations, this scheme is usually slightly modified following the solutions proposed by Pecora and Caroll [40][41] (usually named as "transmitter-receptor decomposition"). Basically, as the basic configuration, it consists of two identical chaotic systems acting one of them as transmitter and the other one as receptor. Then, at least one chaotic signal (called synchronization signal) is extracted from the transmitter and injected in the receptor. Then, Pecora and Caroll propose that, if desired, the corresponding equations or subsystem of the receptor (those which generates the injected signals) may be removed. In the simplest approach only one signal from the transmitter is injected into the receptor. In that way, as Chua's dynamics presents three dimensions, three different synchronization schemes may be proposed (see Figure 7).

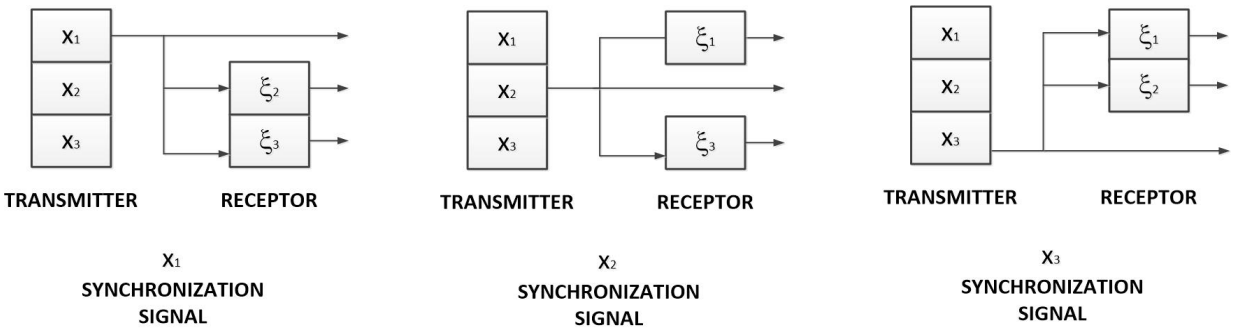

Figure 7. Possible synchronization schemes using the Pecora and Caroll approach and the Chua's circuit

These schemes allow, in general, a complete synchronization (module and phase) of both dynamics, but present some particularities which make this approach to require a special analysis method. In particular, it is not guaranteed that every designed scheme could reach a synchronization state. Thus, before advancing towards the construction of a robust chaotic cryptosystem it is necessary to find what configurations from which showed on Figure 7 may reach a synchronization state.

Louis M. Pecora and Thomas L. Caroll [66] proposed a particular method known nowadays as conditional or transversal Lyapunov exponents. Topologically, in this case it is only necessary to study the instability evolution due to perturbations transversal to the synchronization manifold [65]; i.e. perturbations affecting signals which are not employed as synchronization signal. If perturbations tend to grow exponentially or to oscillate, synchronization is never reached. The conditional Lyapunov exponents are the easiest way to perform this analysis (without being necessary to develop a deep topological study).

Basically, the calculation of the conditional Lyapunov exponents consists of finding the Lyapunov exponents [67] of the receptor when it is evaluated inside the synchronization

manifold. In that way, one of the numerous numerical algorithms employed to obtain the Lyapunov exponents of a system may be employed to perform this analysis.

In its traditional formulation, it is sufficient (but not necessary) for a synchronization scheme to present only negative conditional Lyapunov exponents to reach a good (module and phase) synchronization state. However, if weaker synchronization definitions are considered (which are not valid at all to design cryptosystems), this criterion may be relaxed. Table 1 shows the conditional Lyapunov exponents for each one of the schemes showed on Figure 7.

Table 1. Conditional Lyapunov exponents for the possible transmitter-receptor synchronization schemes of Chua's circuit

Synchronization signal	**Conditional Lyapunov exponents**
x_1	-0.4982 -0.5014
x_2	-2.6316 0
x_3	1.4713 -5.3246

As can be seen, only the scheme considering x_1 as synchronization signal it is guaranteed to reach a stable synchronization state. In fact, the rigorous demonstration process proposed by Vayda [68] (based on the Lyapunov's stability theorems) also indicates that this is a stable synchronization scheme. Below it is proposed a particular realization of this demonstration process for the scheme under study.

It must be considered the error vector $\vec{e} = \vec{x} - \vec{\xi}$. Then, deriving and substituting the dynamics of both systems, it can be obtained the expression of the temporal evolution for the error vector (8), where $e_1 = 0$ as $x_1 = \xi_1$

$$\begin{aligned} e_1 &= 0 \\ \dot{e_2} &= -e_2 + e_3 \\ \dot{e_3} &= -\beta e_2 \end{aligned} \tag{8}$$

Now we propose the following Lyapunov function (9) for $\beta > 0$

$$L(e_1, e_2, e_3) = \frac{1}{2}\left(e_1 e_1 + e_2 e_2 + \frac{1}{\beta} e_3 e_3\right) \tag{9}$$

Then:

(i) $L(e_1, e_2, e_3)$ presents an absolute minimum in the origin as $L(0,0,0) = 0$ and $L(e_1, e_2, e_3) > 0 \quad \forall \vec{e} \; if \; \vec{e} \neq 0$

(ii) $\frac{dL(e_1,e_2,e_3)}{dt} < 0$ in every perforated domain around the origin. In fact, $\frac{dL(e_1,e_2,e_3)}{dt} = \frac{\partial L(e_1,e_2,e_3)}{\partial e_1} \cdot \frac{de_1}{dt} + \frac{\partial L(e_1,e_2,e_3)}{\partial e_2} \cdot \frac{de_2}{dt} + \frac{\partial L(e_1,e_2,e_3)}{\partial e_3} \cdot \frac{de_3}{dt} = e_2\dot{e_2} + \frac{1}{\beta} e_3\dot{e_3} == e_2(-e_2 + e_3) + \frac{1}{\beta} e_3(-\beta e_2) = -e_2\, e_2$

Therefore, the Lyapunov theorem guarantees that $\lim_{t \to \infty} \vec{e} = \vec{0}$, and then $\vec{x} \to \vec{\xi}$ if $t \to \infty$. Finally, that ensures that $\lim_{t\to\infty} \|\eta(t) - y(t)\| = 0$, which is the synchronization criteria we are employing.

Once selected the synchronization scheme to be employed, the chaotic masking configuration may be easily deducted (see Figure 8).

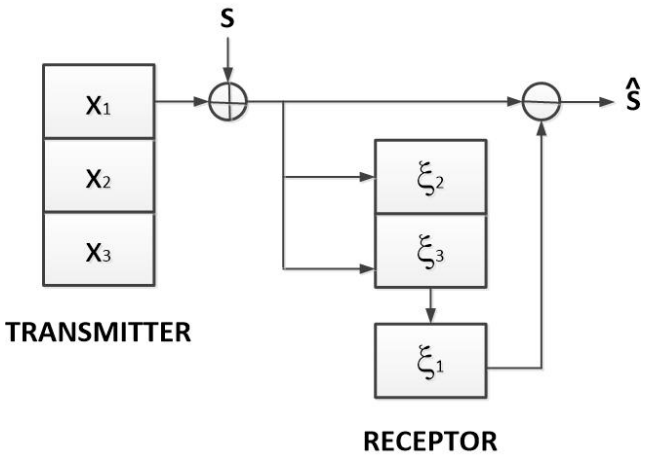

Figure 8. Proposed schemes for chaotic masking using the Chua's circuit

Mathematically (10), in order to create a chaotic masking solution using the selected synchronization scheme, it is enough to include the removed equations or subsystems in the receptor, but isolated from the synchronization signal (see Figure 8). Thus, in the transmitter, the information streaming would be added to the synchronization signal, and the masked information would be recovered by the receptor using a subtractor.

$$\begin{gathered} \dot{x_1} = \alpha\big(x_2 - x_1 - f(x_1)\big) \\ \dot{x_2} = x_1 - x_2 + x_3 \\ \dot{x_3} = -\beta x_2 \end{gathered}$$

$$x_s = x_1 + s \quad \text{(masked information)}$$

$$\begin{gathered} \dot{\xi_1} = \alpha\big(\xi_2 - \xi_1 - f(\xi_1)\big) \\ \dot{\xi_2} = x_s - \xi_2 + \xi_3 \\ \dot{\xi_3} = -\beta\xi_2 \end{gathered} \qquad \textbf{(10)}$$

$$\hat{s} = x_s - \xi_1 \quad \text{(recovered information)}$$

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

Using numerical programming it is possible to evaluate the performance of the proposed scheme. In Figure 9 it is showed the spectrum which could be seen in the radio channel during transmissions. As can be seen, signals with bandwidths up to 25kHZ cannot be protected with this scheme, as the chaotic synchronization signal cannot hide frequencies above this limit. However, usually, constraint resource devices use to transmit low data rates, in order to consume the as little energy as possible, so this value is enough for typical applications. Of course, a radiofrequency chain may translate in frequency the spectrum to be transmitted using wireless communications.

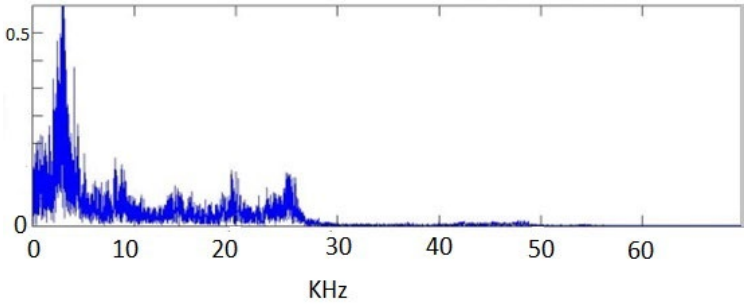

Figure 9. Results of a numerical implementation of the chaotic masking scheme: spectrum of the masked signal

Additionally, Figure 10(a) and Figure 10(b) show a comparison between the original information signal and the recovered signal in both cases using the proposed scheme: an analog and a digital information flow. As can be seen, as planned, the introduction of the information signal generates a perturbation which makes the synchronization state not to be perfect, so the original and the recovered signals present slight differences.

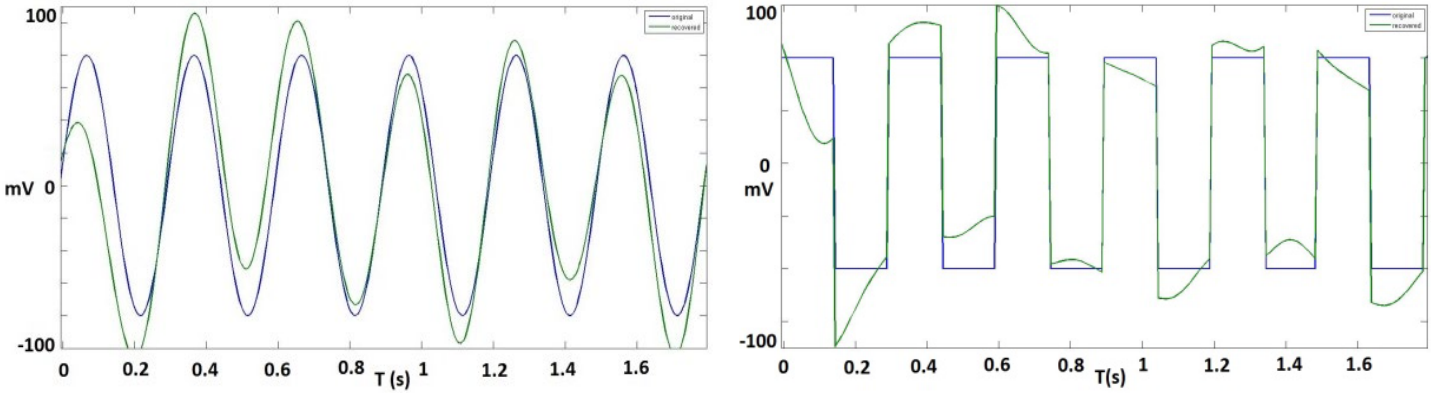

Figure 10. Results of a numerical implementation of the chaotic masking scheme: Original information and recovered information. (a)Analog signal (b) Digital signal

4. ROBUST HARDWARE IMPLEMENTATION AND EXPERIMENTAL VALIDATION

In its origin, the Chua's circuit was designed as a real electronic circuit (see Figure 11), so the Chua's dynamics may be expressed as the evolution laws of this circuit (11).

$$\begin{aligned}\frac{dv_1}{dt} &= \frac{1}{C_1}\left(\frac{1}{R}(v_2 - v_1) - f(v_1)\right)\\ \frac{dv_2}{dt} &= \frac{1}{C_2}\left(i_3 + \frac{1}{R}(v_1 - v_2)\right)\\ \frac{di_3}{dt} &= -\frac{1}{L}v_2\end{aligned} \quad \textbf{(11)}$$

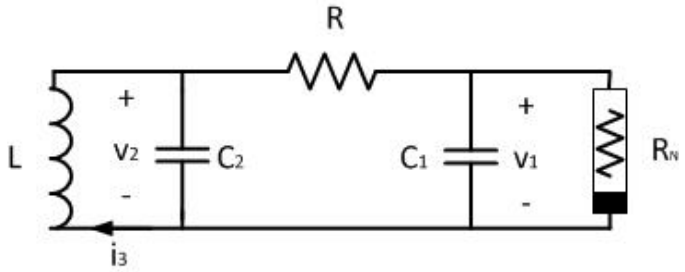

Figure 11. Electronic implementation of Chua's circuit

Thus, the proposed synchronization and masking schemes could be directly implemented using standard electronic techniques (see Figure 12), and simply connecting two identical circuits. Previous works use to validate the proposed implementations by means of electronic simulation. In fact, the numerical solutions and results obtained from circuit simulators have a good behavior and validate the usability of the configuration showed on Figure 12.

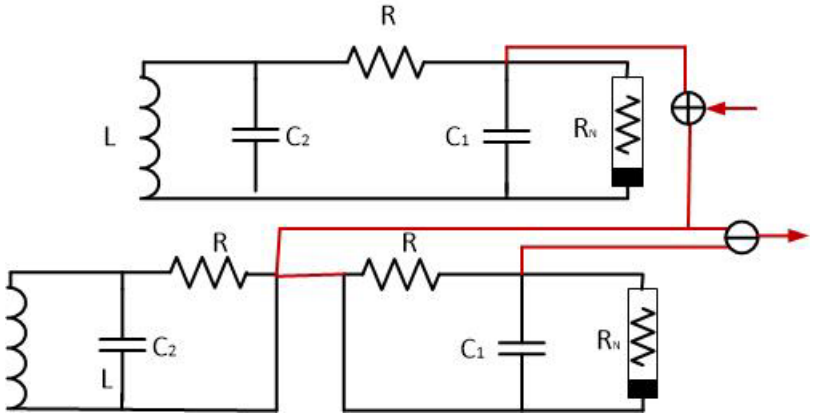

Figure 12. Electronic implementation of a traditional masking system based on Chua's circuit

However, it has been proved that real electronic implementations of Chua circuit are very sensitive to the accuracy of its components [70]. Furthermore, if complex models are considered for components in typical circuit simulator, second order effects appear and the previously proposed scheme cannot reach a stable synchronization state. Therefore, if real deployments are considered, it is necessary to put special attention to the interconnection technique employed to couple both circuits (the receptor and the transmitter) [71][72].

4.1. A ROBUST HARDWARE IMPLEMENTATION

The performed studies by the authors showed three main problems that have impeded until now the implementation of an electronic chaotic masking system based on a standard implementation of Chua's circuit (complex solutions based, for example, on CNN -Cellular Neural Networks- [69] require much more resources): (i) the induced effects of the load due to the interconnection of both circuits, (ii) the required inductances (which are hard to construct with precise values and using high-integration techniques) and (iii) the high-frequency chaotic noise which tends to appear mixed with the recovered information. In this section we propose a robust solution which addresses these problems.

First, in order to avoid the effects of the load, voltage followers are included to extract and inject signals in or from the Chua's circuits. Operational amplifiers into voltage followers present very low output impedance and very high input impedance. In that way, these new elements turn independent some parts of the circuit to the others, and especially turn independent both circuits, the transmitter and the receptor. Thus, the effects of the load are minimized.

Second, the need of including various inductances in the system makes impossible to implement the circuit using high-integration techniques. Particularly, inductances require much more space than other components in order to be implemented (especially if inductances with a high value are needed), so (usually) it is recommendable to employ alterative implementations using other types of elements such as capacitors. Moreover, inductances use to be very difficult to construct with precise values, so the construction of the proposed cryptosystem turn pretty difficult. The solution, then, is to try to remove those inductances. In order to do that, the inductance in the traditional Chua's circuit (see Figure 11) is substituted by an inmitances converter [71], which may be implemented employing capacitors and operations amplifiers. Both elements, now, can be implemented using high integration techniques in a very easy way and more precise elements can be produced.

Finally, in order to remove the high-frequency chaotic noise, a second-order Sallen-Key low-pass filter is included after the final subtractor which recovers the information signal in the receptor. Figure 13 shows the resulting robust implementation.

Various modules are distinguished in the circuit:

- Module A: It is the Chua's circuit acting as transmitter. It generates the chaotic signal to mask the secured information. It includes the inmitances converter.
- Module B and module C: Voltage followers to turn independent some parts of the circuit and prevent the effect of the load.
- Module D: It is an operational amplifier acting as voltage adder, in order to incorporate the secure information to the chaotic signal
- Module E: It represents the transmission medium (usually wireless, such as a radio channel)
- Module F: It includes the subsystem of the Chua's circuit which receives the synchronization signal. It includes the inmitances converter.
- Module G: It includes the subsystem of the Chua's circuit which it is not part of the Pecora and Caroll's synchronization scheme

- Module H: Two operational amplifiers configured ad a subtractor and an inverting amplifier in order to recover the secure information.
- Module I: A second-order Sallen-Key low-pass filter in order to remove the chaotic noise.

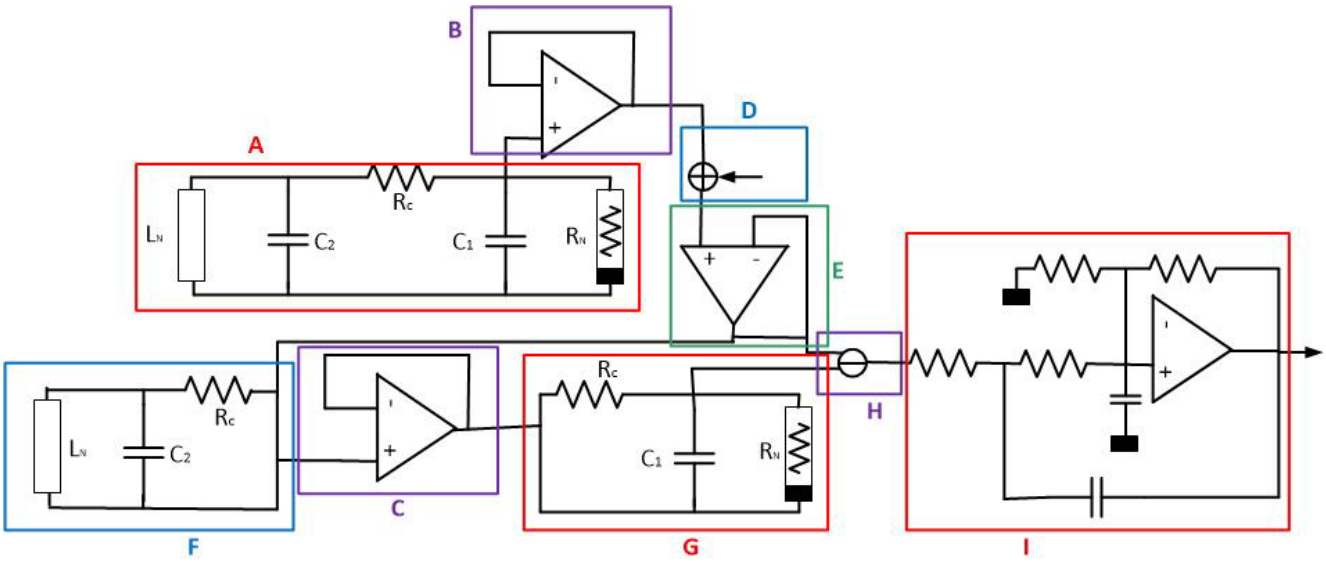

Figure 13. Robust electronic implementation of the masking system based on Chua's circuit

4.2. EXPERIMENTAL VALIDATION

In order to validate the proposed cryptosystem, its operation was studied using two different techniques. First, the PSPICE circuit simulator suite was configured to take into account more complex models than usual, so the validity of the proposed robust implementation for our cryptosystem might be evaluated. Moreover, a real electronic circuit was implemented using discrete electronic components (see Figure 14)

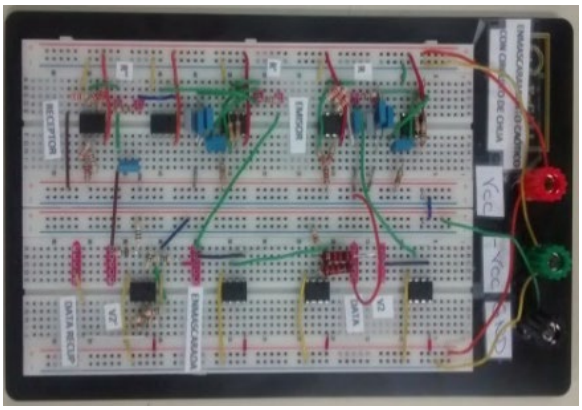

Figure 14. Electronic implementation of the masking system

Considering the electronic circuit simulation of the proposed system, two different types of secure information were included: a sinusoidal signal (analog information) and a TTL signal

(digital information). Detailed parameters of both signals are included on Table 2. Moreover, ten different values for the control parameter (in this case we employed the resistor R_c as control parameter, see Figure 13) were considered. Thus, in total, twenty different simulations were performed.

Table 2. Simulation details for the experimental validation

Parameter	Sinusoidal signal	TTL signal
Amplitude	75 mV	75mV
Frequency	2KHz	2KHz
Duty cycle	--	50%
Offset	0V	0V

Simulations were configured to calculate the evolution of the cryptosystem during the first three seconds of operation. Each simulation, moreover, was performed five times. In order to evaluate the performance of the cryptosystem, the recovering error (difference between the original information signal and the recovered one) was calculated. In that way, a mathematical expression for the medium value of the recovering error is also proposed (12).

$$[\varepsilon(t)] = \sum_{n=0}^{N_{max}} \frac{1}{N_{max}} |s[n] - \hat{s}[n]| \quad \textbf{(12)}$$

In respect to the implemented real circuit, a measurement bench was designed. Basically it consisted of an oscilloscope working in dual mode and representing signal in XY mode on the screen. One of the two independent channels of the oscilloscope was connected to the information signal generator. The other one was connected to the output of the cryptosystem, where the recovered information signal may be sensed. In that way, if both signal are "enough similar", on the screen will be represented the bisector of the first and third quadrant of the screen.

5. RESULTS AND DISCUSSION

In this Section results of the proposed experimental validation are presented and discussed. The final objective is to determine the validity of the proposed cryptosystem.

First, we are studying the results obtained from the circuit simulations. Figure 15 shows the comparison between the recovered signal and the original secure information in the case of considering $R_c = 1800\Omega$, for both, a TTL signal and a sinusoidal signal. Simulations results are displayed using the Probe tool (included into the PSPICE suite). As can be seen, the recovered information signal (red) follows almost perfectly the original information (green).

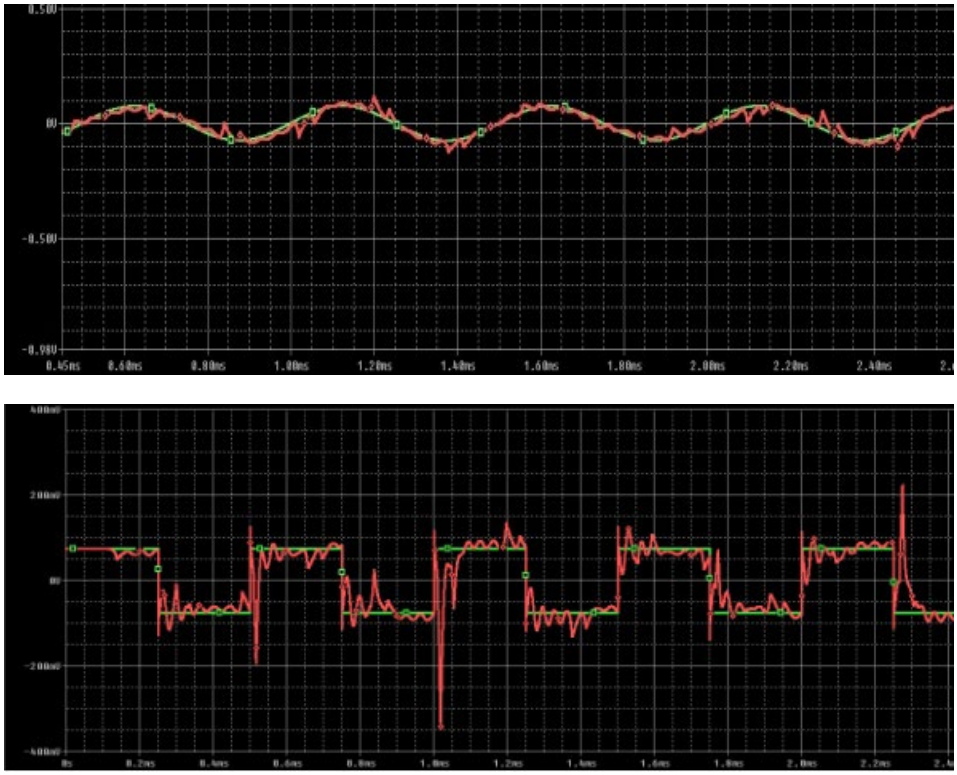

Figure 15. Results obtained from the proposed solution

However, it may be seen some high frequency components which are overlapped on the information signal. These components may be produced by thermal noise or by some spurious chaotic components which are not totally removed by the Sallen-Key filter. Any case, if desired, a new tuned filter (with the appropriate cut frequency) may improve the quality of the recovered signals (see Figure 16). In the case of considering TTL signals, moreover, some digital components (such as Smith-Triger circuits) could be included in order to recover a perfect TTL signal another time.

As said above, the recovered signal presents good quality, although a high frequency parasite frequency is mixed with the recovered information (and using the appropriate filter this effect could be removed). However, in order to obtain a quantitative estimation of the quality of the recovered information signal, the mean recovering error is calculated (see Table 2).

Table 2. Recovery error

Experiment	**Recovery error (%)**
Sinusoidal signal	2.7%
TTL signal	11.5%
Total	7.2%

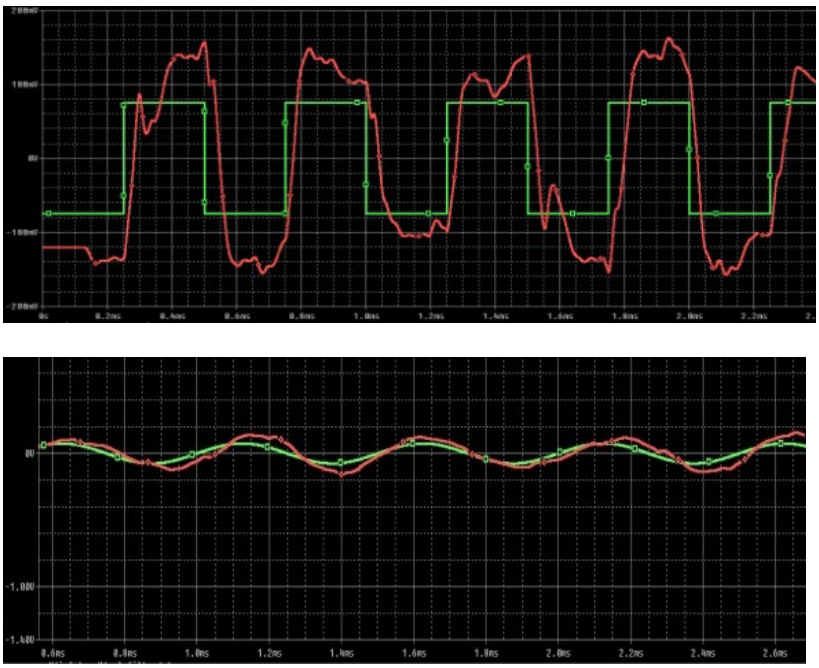

Figure 16. Results obtained from the proposed solution considering a final tuner filter

As can be seen, sinusoidal signals may be recovered with better quality than the TTL signals. However, in order to obtain the recovering error, both types of signals are considered analog. Then, in general, the quality of the recovered information signal, if a digital sequence is masked, could be improved if TTL signals were considered as digital. In fact, as said also before, recovered TTL signals may be highly improved considering specialized digital circuits such as the Smith-trigger (employed to obtain pure TTL signals from TTL-like signals).

Then, the real implemented cryptosystem based on hardware (circuit) technologies was measured. Both chaotic circuits were configured to generate a double-roll topology (using a resistor $R_c = 1680\Omega$). The obtained measure on the oscilloscope screen is showed on Figure 17.

As can be seen, the recovered and the original information signals are perfectly synchronized (both are almost identical), as an almost perfect line appears on the screen. Two small perturbations may be detected, nevertheless. First, the line does not cross the origin. This is due to the appearance of a little continuous power on the recovered signal. Second, the figure it is not a perfect line, as it present a certain width. This is due to the variations (modulations) and other perturbations that appear on the recovered signal.

Any case, results shows that the proposed cryptosystem is a valid solution for both digital and analog transmissions.

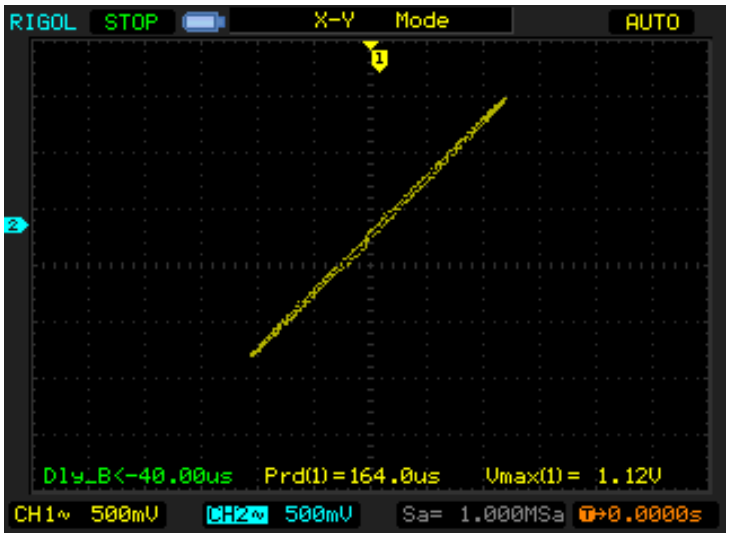

Figure 17. Results obtained from the real implemented circuit

6. CONCLUSIONS

In this article we propose a robust chaotic hardware-based cryptosystem, which employs the chaotic masking technology as main supporting technique. The designed cryptosystem is especially designed to low computational power devices which cannot execute traditional and heavy cryptographic algorithms. Different synchronization schemes and chaotic dynamics are studied. Moreover a robust implementation of the proposed cryptosystem based on the Chua's circuit using standard electronic components is described.

The resulting cryptosystem allows encrypting str8eaming communications among resource constraint nodes in future engineered systems (such as pervasive sensing platforms). The first obtained result has been a good chaotic synchronization between the emitter and the receiver systems. Moreover, we have detected and solved the most important practical implementation problems, associated with the most standard Chua's circuit. We have reduced, first, the loading effects by introducing several voltage followers in the receiver system. We have replaced very costly inductances by inmitances converser and capacitors and, finally, we have introduced a low-pass filter in order to remove the high frequency chaotic noise typical of these solutions. In addition, the circuit is characterized by a reduced size and a very low power consumption.

We have implemented the cipher system using an electronic circuit simulator (PSPICE), where sine and TTL information signals were considered. The recovery error was 3% for the sinusoidal signal and 7% for the TTL one. The work is focused on protecting private communications that is essential in current devices using sensor networks. Future works should be focused on masking speech and sound signals which require wider chaotic signal in frequency and higher transmission rates.

ACKNOWLEDGMENTS

Borja Bordel has received funding from the Ministry of Economy and Competitiveness through SEMOLA project (TEC2015-68284-R), from the Centre for the Development of Industrial Technology (CDTI) through PERIMETER SECURITY project (ITC-20161228), from the Autonomous Region of Madrid through MOSI-AGIL-CM project (grant P2013/ICE-3019, co-funded by EU Structural Funds FSE and FEDER) and from the Ministry of Education through the FPU program (grant number FPU15/03977).

CONFLICTS OF INTEREST

The authors declare that there is no conflict of interest regarding the publication of this paper.

REFERENCES

[1] Bordel, B., Alcarria, R., Martín, D., Robles, T., & de Rivera, D. S. (2017). Self-configuration in humanized cyber-physical systems. Journal of Ambient Intelligence and Humanized Computing, 8(4), 485-496.

[2] Akyildiz, I. F., Vuran, M. C. Wireless sensor networks (Vol. 4). John Wiley & Sons. (2010)

[3] Yick, J., Mukherjee, B., Ghosal, D. Wireless sensor network survey. Computer networks, 52(12), pp. 2292-2330, (2008).

[4] Vieira, M. A. M., Coelho, C. N., da Silva, D. C., da Mata, J. M. Survey on wireless sensor network devices. In IEEE Conference Emerging Technologies and Factory Automation, Vol. 1, pp. 537-544. IEEE. (2003)

[5] Bordel, B., Alcarria, R., Robles, T., & Martín, D. (2017). Cyber–physical systems: Extending pervasive sensing from control theory to the Internet of Things. Pervasive and Mobile Computing, 40, 156-184.

[6] Portilla, J., Otero, A., de la Torre, E., Riesgo, T., Stecklina, O., Peter, S., Langendörfer, P. Adaptable security in wireless sensor networks by using reconfigurable ECC hardware coprocessors. International Journal of Distributed Sensor Networks, (2010).

[7] Mareca, P., & Bordel, B. (2017, April). A Robust Implementation of a Chaotic Cryptosystem for Streaming Communications in Wireless Sensor Networks. In World Conference on Information Systems and Technologies (pp. 95-104). Springer, Cham.

[8] Cardenas, A., Amin, S., Sinopoli, B., Giani, A., Perrig, A., & Sastry, S. (2009, July). Challenges for securing cyber physical systems. In Workshop on future directions in cyber-physical systems security (Vol. 5).

[9] Zhang, M., Selic, B., Ali, S., Yue, T., Okariz, O., Norgren, R. Understanding Uncertainty in Cyber-Physical Systems: A Conceptual Model. (2016)

[10] Avizienis, A., Laprie, J. C., Randell, B., & Landwehr, C. (2004). Basic concepts and taxonomy of dependable and secure computing. IEEE transactions on dependable and secure computing, 1(1), 11-33.

[11] Karlof, C., Wagner, D. Secure routing in wireless sensor networks: Attacks and countermeasures. Ad hoc networks, 1(2), pp. 293-315, (2003).
[12] Wang, Y., Attebury, G., Ramamurthy, B. A survey of security issues in wireless sensor networks. (2006).
[13] Deng, J., Han, R., & Mishra, S. (2003). A performance evaluation of intrusion-tolerant routing in wireless sensor networks. In Information Processing in Sensor Networks (pp. 552-552). Springer Berlin/Heidelberg.
[14] Karlof, C., Sastry, N., & Wagner, D. (2004, November). TinySec: a link layer security architecture for wireless sensor networks. In Proceedings of the 2nd international conference on Embedded networked sensor systems (pp. 162-175). ACM.
[15] Perrig, A., Szewczyk, R., Tygar, J. D., Wen, V., Culler, D. E. SPINS: Security protocols for sensor networks. Wireless networks, 8(5), pp. 521-534, (2002).
[16] Portilla, J., Otero, A., de la Torre, E., Riesgo, T., Stecklina, O., Peter, S., Langendörfer, P. Adaptable security in wireless sensor networks by using reconfigurable ECC hardware coprocessors. International Journal of Distributed Sensor Networks, (2010).
[17] Akella, R., Tang, H., & McMillin, B. M. (2010). Analysis of information flow security in cyber–physical systems. International Journal of Critical Infrastructure Protection, 3(3), 157-173.
[18] Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. Computer networks, 54(15), 2787-2805.
[19] Babar, S., Stango, A., Prasad, N., Sen, J., & Prasad, R. (2011, February). Proposed embedded security framework for internet of things (iot). In Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2011 2nd International Conference on (pp. 1-5). IEEE.
[20] Heer, T., Garcia-Morchon, O., Hummen, R., Keoh, S. L., Kumar, S. S., & Wehrle, K. (2011). Security Challenges in the IP-based Internet of Things. Wireless Personal Communications, 61(3), 527-542.
[21] Zhou, L., & Chao, H. C. (2011). Multimedia traffic security architecture for the internet of things. IEEE Network, 25(3).
[22] Ning, H., Liu, H., & Yang, L. T. (2013). Cyberentity security in the internet of things. Computer, 46(4), 46-53.
[23] Medaglia, C. M., & Serbanati, A. (2010). An overview of privacy and security issues in the internet of things. In The Internet of Things (pp. 389-395). Springer, New York, NY.
[24] Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer Networks, 76, 146-164.
[25] Cao, J., Carminati, B., Ferrari, E., & Tan, K. L. (2011). Castle: Continuously anonymizing data streams. IEEE Transactions on Dependable and Secure Computing, 8(3), 337-352.
[26] Alcaide, A., Palomar, E., Montero-Castillo, J., & Ribagorda, A. (2013). Anonymous authentication for privacy-preserving IoT target-driven applications. Computers & Security, 37, 111-123.

[27] Peng, L., Ru-chuan, W., Xiao-yu, S., & Long, C. (2013, October). Privacy Protection Based on Key-changed Mutual Authentication Protocol in Internet of Things. In China Conference Wireless Sensor Networks (pp. 345-355). Springer, Berlin, Heidelberg.

[28] Pathan, A. S. K., Lee, H. W., Hong, C. S. Security in wireless sensor networks: issues and challenges. In 8th International Conference Advanced Communication Technology, Vol. 2, IEEE. (2006)

[29] Vaidya, P. G., Angadi, S. Decoding chaotic cryptography without access to the superkey. Chaos, Solitons & Fractals, 17(2), pp. 379-386. (2003)

[30] Wong, K. W., Ho, S. W., Yung, C. K. A chaotic cryptography scheme for generating short ciphertext. Physics Letters A, 310(1), pp. 67-73, (2003).

[31] Li, S., Li, Q., Li, W., Mou, X., Cai, Y. Statistical properties of digital piecewise linear chaotic maps and their roles in cryptography and pseudo-random coding. In IMA International Conference on Cryptography and Coding, pp. 205-221. Springer Berlin Heidelberg. (2001)

[32] Pareek, N. K., Patidar, V., Sud, K. K.Cryptography using multiple one-dimensional chaotic maps. Communications in Nonlinear Science and Numerical Simulation, 10(7), pp. 715-723, (2005)

[33] Pareek, N. K., Patidar, V., Sud, K. K. Discrete chaotic cryptography using external key. Physics Letters A, 309(1), pp. 75-82, (2003).

[34] Amigó, J. M., Kocarev, L., Szczepanski, J. Theory and practice of chaotic cryptography. Physics Letters A, 366(3), pp. 211-216, (2007)

[35] Kocarev, L., & Parlitz, U. (1995). General approach for chaotic synchronization with applications to communication. Physical review letters, 74(25), 5028.

[36] Voss, H. U. (2000). Anticipating chaotic synchronization. Physical review E, 61(5), 5115.

[37] Rosenblum, M. G., Pikovsky, A. S., & Kurths, J. (1997). From phase to lag synchronization in coupled chaotic oscillators. Physical Review Letters, 78(22), 4193.

[38] Pikovsky, A. S., Rosenblum, M. G., & Kurths, J. (1996). Synchronization in a population of globally coupled chaotic oscillators. EPL (Europhysics Letters), 34(3), 165.

[40] Pecora, L. M., & Carroll, T. L. (1990). Synchronization in chaotic systems. Physical review letters, 64(8), 821.

[41] Carroll, T. L., & Pecora, L. M. (1991). Synchronizing chaotic circuits. IEEE Transactions on circuits and systems, 38(4), 453-456.

[42] Mareca, M. P., & Bordel, B. (2017). Improving the Complexity of the Lorenz Dynamics. Complexity, 2017.

[43] Liao, T. L., & Tsai, S. H. (2000). Adaptive synchronization of chaotic systems and its application to secure communications. Chaos, Solitons & Fractals, 11(9), 1387-1396.

[44] Sivaprakasam, S., Shahverdiev, E. M., Spencer, P. S., & Shore, K. A. (2001). Experimental demonstration of anticipating synchronization in chaotic semiconductor lasers with optical feedback. Physical Review Letters, 87(15), 154101.

[45] Kolumbán, G., Kennedy, M. P., & Chua, L. O. (1998). The role of synchronization in digital communications using chaos. II. Chaotic modulation and chaotic synchronization. IEEE

Transactions on Circuits and Systems I: Fundamental Theory and Applications, 45(11), 1129-1140.
[46] Cuomo, K. M., Oppenheim, A. V., Strogatz, S. H. Synchronization of Lorenz-based chaotic circuits with applications to communications. IEEE Transactions on circuits and systems II: Analog and digital signal processing, 40(10), pp. 626-633, (1993)
[47] L. Kocarev, K. Halle, K. Eckert, and L. Chua, Experimental demonstration of secure communications via chaotic synchronization, Int. J. Bifurcation Chaos, vol. 2, pp. 709-713, (1992).
[48] Chua, L. O. (1992). The genesis of Chua's circuit. Electronics Research Laboratory, College of Engineering, University of California.
[49] Chua, L. O., Itoh, M., Kocarev, L., & Eckert, K. (1993). Chaos synchronization in Chua's circuit. Journal of Circuits, Systems, and Computers, 3(01), 93-108.
[50] Chua, L. O., Kocarev, L., Eckert, K., & Itoh, M. (1992). Experimental chaos synchronization in Chua's circuit. International Journal of Bifurcation and Chaos, 2(03), 705-708.
[51] Cruz, J. M., & Chua, L. O. (1993). An IC chip of Chua's circuit. IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing, 40(10), 614-625.
[52] letti, S., Kurths, J., Osipov, G., Valladares, D. L., & Zhou, C. S. (2002). The synchronization of chaotic systems. Physics reports, 366(1), 1-101.
[53] Wheeler, D. D. (1989). Problems with chaotic cryptosystems. Cryptologia, 13(3), 243-250.
[54] Mishra, M. (2017). Review on Chaotic Ciphers and its Analysis. Journal of Science & Engineering Education (ISSN 2455-5061), 2, 30-34.
[55] Peterson, R. L., Ziemer, R. E., & Borth, D. E. (1995). Introduction to spread-spectrum communications (Vol. 995). New Jersey: Prentice Hall.
[56] Kim, A. (2011). Photonic CDMA systems with security physical layers. IEEE Communications Letters, 15(1), 1-3.
[57] Hasler, M. (1998). Synchronization of chaotic systems and transmission of information. International Journal of Bifurcation and Chaos, 8(04), 647-659.
[58] Morgül, Ö., & Feki, M. (1999). A chaotic masking scheme by using synchronized chaotic systems. Physics Letters A, 251(3), 169-176.
[59] 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.
[60] Kolumbán, G., Kennedy, M. P., & Chua, L. O. (1998). The role of synchronization in digital communications using chaos. II. Chaotic modulation and chaotic synchronization. IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 45(11), 1129-1140.
[61] Lorenz, E. N. J. (1963). Deterministic nonpenodic chaos. Atmos. Sci, 20, 167.
[62] Lorenz, E. (1963). Chaos in meteorological forecast. J. Atmos. Sci, 20, 130-144.
[63] Chen, G., & Ueta, T. (1999). Yet another chaotic attractor. International Journal of Bifurcation and chaos, 9(07), 1465-1466.

[64] Bai, E. W., & Lonngren, K. E. Synchronization of two Lorenz systems using active control. Chaos, Solitons & Fractals, 8(1), 51-58, (1997)
[65] Patidar, V., & Sud, K. K. (2006). Identical synchronization in chaotic jerk dynamical systems. Electronic journal of theoretical physics, 3(11).
[66] Pecora, L. M., & Carroll, T. L. (1990). Synchronization in chaotic systems. Physical review letters, 64(8), 821.
[67] Pesin, Y. B. (1977). Characteristic Lyapunov exponents and smooth ergodic theory. Russian Mathematical Surveys, 32(4), 55-114.
[68] He, R., & Vaidya, P. G. (1992). Analysis and synthesis of synchronous periodic and chaotic systems. Physical Review A, 46(12), 7387.
[69] Chua, L. O. (1998). CNN: A paradigm for complexity (Vol. 31). World Scientific.
[70] I. M. Kyprianidis, P. Haralabidis & I. N. Stouboulos. Dynamics and Synchronization of a Second-Order Nonlinear and Nonautonomous Electric Circuit. 3rd World Multiconference on: Circuits, Systems, Communications and Computers. CSCC'99 , 3241-3247. (1999)
[71] V. Alcober, P. Mareca y G. González. Una Optimización en la Sincronización y Enmascaramiento con el circuito de Chua. XXVIII Reunión Bienal de la Real Sociedad Española de Física. Simposio de Dinámica no-lineal. Sevilla (Spain). (2001)
[72] K.Murali and M. Lakshamanan, and L.O. Chua. Synchronizing Chaos in driven Chua's circuit, Int. J. Bifurcation Chaos 05 (2), 563 (1995).

BORJA BORDEL received the B.S. degree in telecommunication engineering in 2012 and the M.S. telecommunication engineering in 2014, both from Technical University of Madrid. He is currently pursuing the Ph.D. degree in telematics engineering at Telecommunication Engineering School, UPM. His research interests include cyber-physical systems, wireless sensor networks, radio access technologies, communication protocols and complex systems

PILAR MARECA received the PhD in fundamental physics in 1983, from Universidad Complutense de Madrid. She is current full professor at Telecommunication Engineering
School, UPM. Her research interests include chaotic circuits, Numerical Analysis, Mathematical Modelling, Molecular Dynamics and Nonlinear Analysis