Universal receptor for chaotic cryptosystems based on Chua's circuit in embedded mobile devices

Borja Bordel*and Ramón Alcarria
Universidad Politécnica de Madrid
{borja.bordel, ramon.alcarria}@upm.es

Abstract

Mobile communications are envisioned to be implemented in a large catalog of different applications: from traditional end-user services such as video streaming, to emerging digitalization solutions such as precision agriculture. Typically, mobile devices are considered powerful enough to execute all the modules and services required to support secure and broadband communications, but future scenarios require embedded devices as the primary hardware component. And those embedded devices are resource-constrained. Their limited computing power can only manage minimal communication services, excluding other additional functionalities as heavy security mechanisms. Lightweight security and encryption are the most adopted approaches to mitigate this problem, including stream cipher and chaotic cryptosystems. This is because those techniques are based on hardware elements and do not consume computational resources. But while software implementations are fully replicable with no error, hardware components may change their properties and behavior depending on the manufacturing techniques and design. For standard digital circuits, these small variations are not relevant, but chaotic cryptosystems are extremely sensitive, and the transmitter and the receptor are expected to be totally identical. However, this scenario prevents technological development, as all mobile embedded devices should be manufactured by the same industry agent to ensure interoperability. In this paper, we address this challenge and propose a universal receptor for chaotic cryptosystems in embedded mobile devices. The described receptor will be able to operate with transmitters based on any existing implementation of the Chua's circuit. Using a combination of entropy metrics and binary distances, the receptor is able to identify the circuit implementation in the transmitter and dynamically adapt the receptor to this configuration. Simulation tools are used to validate the proposed technology, and the results show that interoperability errors are reduced by more than 63%.

Keywords: chaotic cryptosystems, Chua's circuit, information theory, embedded devices, mobile security, simulation tools

1 Introduction

Next-generation mobile technologies (including 5G communications in the Ka-band [1] and 6G networks [2] are expected to provide high performance communication services to a large catalog of different applications. Each of these scenarios has very different characteristics and requirements, creating 5G network slices [3] or 6G verticals [4]. However, provided Quality-of-Service (QoS) must be intense regardless of the final application under consideration, and Ultrareliable Low Latency Communications (URLLC) [5], massive Machine-Type Communications (mMTC) [6], and enhanced Mobile Broadband Communications (eMBBC) [7] must always be guaranteed.

The 7th International Conference on Mobile Internet Security (MobiSec'23), Dec. 19-21, 2023, Okinawa, Japan, Article No. 32

*Corresponding author: Borja Bordel. E.T.S.I. Sistemas Informáticos, UPM. Calle Alan Turing s/n (Ctra. de Valencia, Km. 7) 28031 - Madrid (Spain), Tel. (+34) 91 067 35 24

These hard QoS requirements require complex network architectures and great computing capabilities to be feasible. Both base stations and mobile devices must execute several different modules, services, and protocols to support a smooth communication flow [8]. But in addition, they must run other complementary and essential services such as security mechanisms or tarification controls [9]. In standard mobile devices, computing resources are considered redundant enough to support all these algorithms and solutions. Nevertheless, this kind of device is not universal. While in end-user services such as video streaming or phone calls, traditional mobile devices are the dominant user equipment, in order to develop emerging applications other types of devices are preferred [10]. For example, in sensorization scenarios, industry digitalization solutions (Industry 4.0 [11] and Industry 5.0 [12]) or precision agriculture, mobile embedded devices that enable a pervasive computing deployment are the most feasible technology [13]. However, these mobile embedded devices tend to be resource-constrained. The lack of power supply and their reduced size imply a very limited computational power in terms of memory and/or MIPS (Million instructions per second) [14].

In these embedded mobile devices, the minimal software needed to enable efficient mobile communication is hardly implemented, and other supplementary services such as heavy security policies (certificates, asymmetric encryption, etc.) cannot be implemented in a generic case [15]. However, this proposal opens several risks, especially in a global context where cyber-physical attacks are rapidly developing and increasing in number every day [16]. As a way to mitigate these risks and partially solve the problem, lightweight security and, mostly, encryption techniques are proposed and implemented [17]. Among all possible approaches, stream cipher [18] and chaotic cryptosystems [19] are preferred, as they can be based on hardware components and circuits that do not require additional consumption of computational resources. However, this hardware-based approach also faces some open questions. While in software algorithms and schemes, replicability is fully ensured (even if devices can execute the same assembler language the binary code can be exactly identical), in hardware technologies the situation is more difficult. Hardware devices that meet the same specifications can be implemented using different physical or circuit designs or technologies. Therefore, finally, the real behavior may be slightly different depending on the manufacturer.

Usually, these differences are not relevant for digital circuits as the one employed to create stream ciphers, but chaotic cryptosystems are totally the opposite. In fact, the strength of chaos-based security systems is the sensitivity of these elements to any variation [20]. So, the final encryption signal or key stream is totally different if a small change is applied to the initial conditions. But most chaotic circuits have several different implementations, so in any real functional application or system or transmitters and receptors need to be implemented using the same strategy and then the manufacturing company if the interoperability wants to be guaranteed. Although this is possible, it is also a barrier for technological development, as it causes high prices and low incentives for innovation. This paper addresses this challenge.

In this paper, we propose a new universal receptor for chaotic cryptosystems in mobile embedded devices. This innovative receptor employs information theory and vector spaces to determine which circuit implementation is available in the transmitted and dynamically adapts to it. This detection algorithm is based on the Shannon entropy definition and the Hamming distance to analyze and calculate the most probable circuit implementation in the transmitter using the standard Euclidean distance. The proposed receptor is specifically designed to support any cryptosystem based on chaos synchronization and the Chua's circuit. Any hardware implementation of this chaotic circuit is supported: the standard circuit, the cubic nonlinearity, the immittance-converter design and the cellular neural network (CNN) cells.

The remainder of the paper is organized as follows. Section 2 describes the state of the art on chaotic cryptosystems for mobile embedded devices. Section 3 describes the proposed receptor, including all the supported circuit implementations and the description of the cryptosystems. Section 4 presents the experimental methodology and simulation scenario validating the performance of the proposed solution, and the results and discussions. Finally, Section 5 concludes the paper.

2 State of the art

Traditionally, works on cryptosystems were focused on reducing the encryption errors and increasing the randomness [21]. Because of the erratic behavior of chaotic systems, the ability of dynamics to generate stable electrical or numerical signals is desired. Authors have proposed solutions based on discrete iterated maps [22], jerk dynamics [23], analog circuits [24], or continuous differential systems [25], among other approaches. But, in general, all of these schemes are not specifically designed for embedded devices or mobile devices. And all results provided are theoretical or numerical. Problems associated with the real circuit implementation of those solutions are not addressed.

On the other hand, some authors do address real implementation problems, but in most cases, these works are restricted to software implementations. Challenges associated with the limited entropy of chaos (increased through DNA-based encryption) [26], problems related to weaknesses against statistical attacks (diffusion algorithms mitigate the situation) [27], or errors induced by the limited numerical precision in microprocessors (addressed using correction techniques) [28] are studied.

Hardware implementations of chaotic cryptosystems are also investigated. Different techniques are reported to implement chaotic dynamics with a well-known good cryptographic behavior (such as Lorenz dynamics) are reported [29]. Some authors investigate how to reduce the size and consumption of these implementations [30], while others propose alternatives to allow for the mass production of circuits using transistors and silicon-based components [24]. In recent years, several researchers have proposed solutions to implement chaotic cryptosystems using digital Boolean circuits and components, such as FPGAs [31] or very large-scale integration (VLSI) circuits [32]. However, all of these works are related to the electronic optimization of chaotic circuits, instead of their cryptographic applications and interoperability.

Moreover, nowadays, the most common approach consists of a standard lightweight cipher, which is fed by a pseudorandom chaotic key [33]. Digital circuits in FPGAs where native chaotic dynamics is employed [34] can be found. Even some proposals describe specific modifications or adaptations of well-known dynamics (such as the Lorenz system) to make them compatible with FPGAs [35] or standard electronic implementations [36]. Ad hoc chaos key generators have also been proposed employing FPGAs [37] or microcontrollers [38]. Other hybrid schemes where chaotic circuits are employed together with S-box functions [39], sine chaotization [40], or wavelet fusion may also be found [41]. Other cryptographic solutions, such as hash functions [42], have also been implemented using hardware-enabled chaos. But again, in all those works, the focus is on the electronic optimization and adaptation of chaotic dynamics. No reference to the cryptographic implications of all these challenges is made to registers. This paper aims to fill this gap.

Finally, works where chaotic cryptosystems are specifically designed and tested for mobile embedded devices are sparse. But some system-on-chip implementations of chaotic cryptosystems have been described [31], as well as ciphers for wireless devices operating in real time [43]. Although most of the usual works are, again, software-based [44] and application-specific [45]. To overcome the limitations of resource-constrained devices, the proposed solutions are typically limited to multiprocessor devices [46] or other similar enhanced hardware components. Nevertheless, neither interoperability problems nor challenges are addressed.

3 Universal receptor for chaotic cryptosystems

All chaotic cryptosystems are based on the need for two identical dynamics to be reconstructed in both the receptor and the transmitter [47]. Thus, a real fully universal receptor for chaotic cryptosystems is impossible to implement because building that receptor is one of the most critical weaknesses of chaos. But if one specific dynamic is chosen, it is theoretically possible to build a universal receptor which can operate with any possible implementation of that dynamic.

In this first paper, we focus on a universal receptor for cryptosystems based on the Chua circuit [48]. Chua's circuit is one of the simplest physical systems generating chaos. Besides, because it is a real circuit, no transformation or adaptation from the mathematical model to a real circuit implementation is required. Because of these advantages, Chua's circuit has been extensively studied and used to build a cryptosystem for embedded (mobile) devices.

Section 3.1 describes the Chua's circuit and all the possible implementations considered in this work. Section 3.2 presents the model for the proposed cryptosystem based on chaos synchronization and the Chua's circuit, and Section 3.3 introduces the architecture and operation of the proposed universal receptor for the previously mentioned cryptosystem.

3.1 Chua's circuit. Considered implementations

Although the Chua's circuit was first introduced by Leon Chua in 1983 [48], it became really popular twenty years later; when its real applications began to be discovered and described [49]. Then, different authors investigated how to exploit the properties of this new circuit, introducing up to ten different electronic implementations to achieve the same chaotic behavior [50]. But with small variations, which were appropriate for different use cases.

In its original and standard implementation, the Chua's circuit (Figure 1) is a simple passive circuit with three reactances (two capacitors and one inductance) producing a three-dimensional dynamic (1). Besides, one non-linear element whose implementation is not defined is included too (2). Being $G_a, G_b < 0$, $E > 0$, $|G_b| < |G_a|$ and variables V_1, V_2 and I_3 electrical signals at different circuit points (see Figure 1). This non-linear resistance is essential, and in its most classical implementation it consists of operational amplifiers and passive components (see Figure 2).

$$\begin{aligned} \frac{dV_1}{dt} &= \frac{1}{C_1}(\frac{1}{R}(V_2 - V_1) - f(V_1)) \\ \frac{dV_2}{dt} &= \frac{1}{C_2}(I_3 + \frac{1}{R}(V_1 - V_2)) \\ \frac{dI_3}{dt} &= -\frac{1}{L}V_2 \end{aligned} \tag{1}$$

$$f(V_1) = G_b \cdot V_1 + \frac{1}{2}(G_a - G_b)(|V_1 + E| - |V_1 - E|) \tag{2}$$

However, this approach has two main problems. On the one hand, capacitors, but mostly instances, are difficult to manufacture and tend to giant in comparison to resistances or amplifiers.

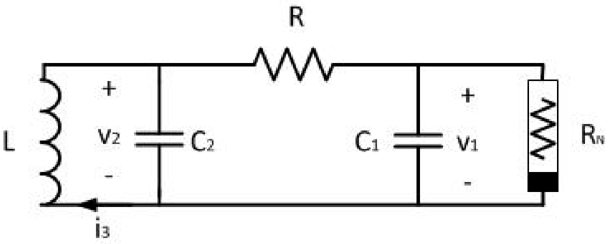

Figure 1: Standard Chua's circuit implementation

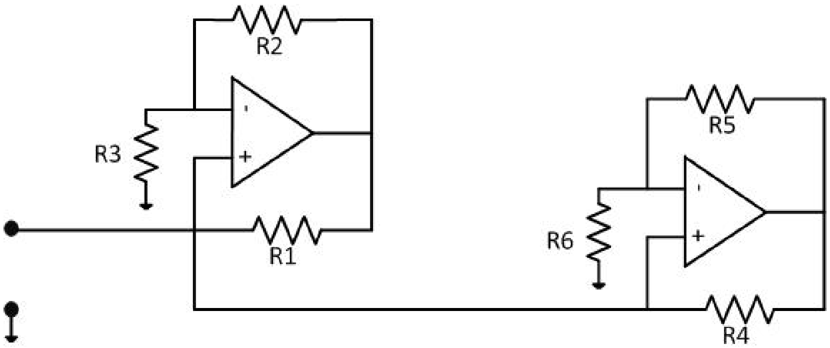

Figure 2: Non-linearity implementation in standard Chua's circuit

On the other hand, the non-linear resistance, implemented with amplifiers, is an active component with a very sensitive behavior. And it usually causes stability problems and electrical interferences.

Therefore, different authors proposed different approaches to address these challenges.

The oldest proposal consists of replacing the non-linear resistance by a cubic non-linearity [51] (3), where V_{max} is a positive parameter. As cubic functions are continuous (the original non-linear resistance is piecewise (4) and then, non-continuous) some electronic components (such as the triode) could produce the non-linearity with stability and no electrical problems. But (see Figure 3) the cubic non-linearity is not fully identical to the original piecewise function, and some small differences in the generated chaos appear (especially in the most complex structures).

$$f(V_1) = -\frac{G_a}{V_{max}^2}{V_1}^3 + G_a V_1 \tag{3}$$

$$f(V_1) = \begin{cases} G_a V_1 \quad if \quad |V_1| < E \\ G_b \cdot V_1 + (G_a - G_b)E \quad if \quad V_1 > E \\ G_b \cdot V_1 - (G_a - G_b)E \quad if \quad V_1 < -E \end{cases} \tag{4}$$

The two remaining implementations are based on circuit transformations using operational amplifiers. The first proposal consists of removing the inductance, whose manufacturing is extremely complicated, by employing a capacitor and an immittance converter. Figure 4 shows the proposed circuit. This converter transforms the capacitor into an equivalent inductance

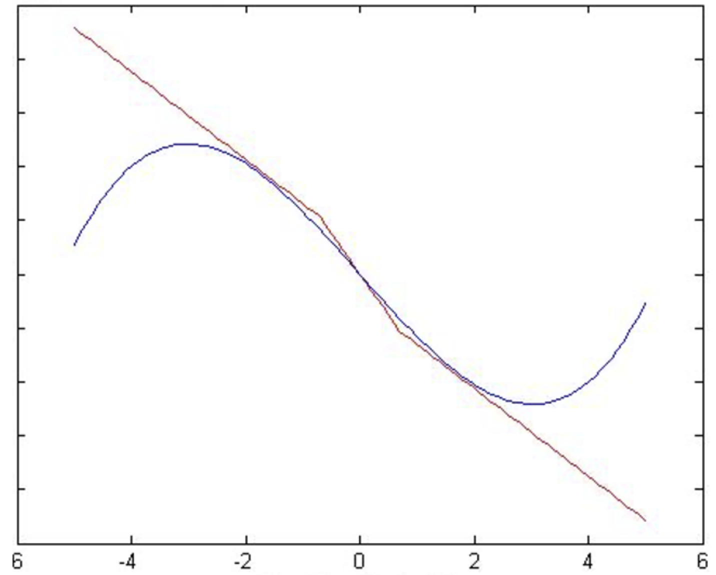

Figure 3: Non-linearity implementation in standard Chua's circuit compared to the cubic non-linearity

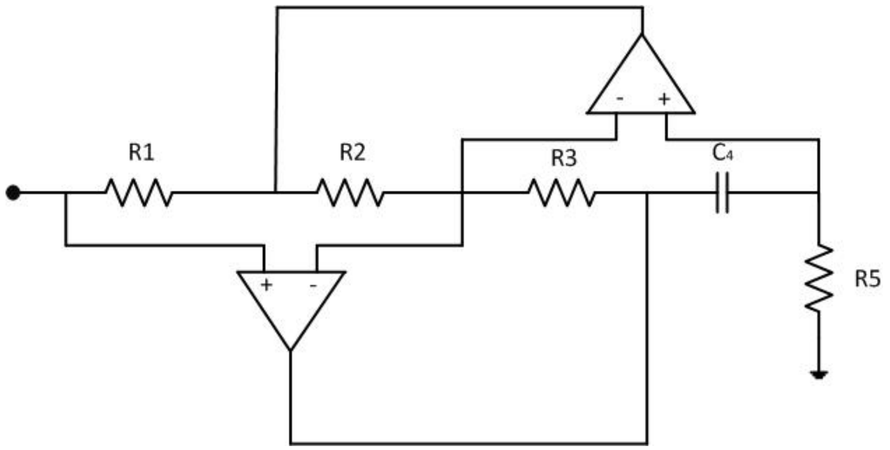

Figure 4: Immittance converter for the Chua's circuit

L_N (5), but also introduces spurious effects, as operational amplifiers can saturate while passive inductance not. Thus, circuits employing this implementation show perturbations at the extreme points of all structures.

$$L_N = \frac{R_3 R_5 R_1 C_4}{R_2} \tag{5}$$

Finally, some authors argue that the behavior of the Chua's circuit cannot depend on passive components, whose manufacturing errors are above 5% in most common components. On the contrary, a Chua's circuit only based on operational amplifiers may benefit from the stable

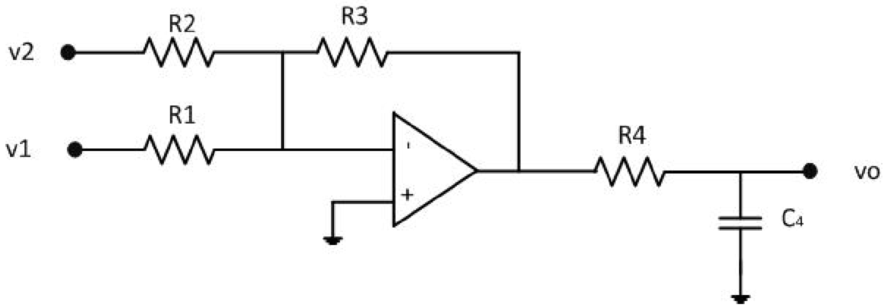

Figure 5: Circuit implementation of a cellular neural network

behavior of feedback control loops. But, as in all feedback loops, this kind of Chua's circuit can only operate correctly within the operating range of operational amplifiers. Distortion tends to appear in the extremes of any chaotic structure and saturation could eventually occur (with fatal consequences for the communication systems). The most usual Chua's circuit implementation using operation amplifiers is based on cellular neural network (CNN) cells. A CNN is a circuit unit (see Figure 5) whose behavior is similar to a differential equation (6). Combining three of these CNN, as well as other required interconnection elements, we can achieve an implementation of the Chua's circuit only based on operational amplifiers (see Figure 6).

$$\frac{d}{dt}v_0 = \frac{-1}{C_4 R_4}(v_0 + R_3(\frac{v_2}{R_2} + \frac{v_1}{R_1})) \tag{6}$$

In this work, the proposed universal receptor can operate with any transmitter based on the Chua's circuit and using any of the previously described implementations.

3.2 Chaos synchronization and cryptosystem

Several different cryptosystems based on chaos have been reported (see Section 2). But in this article, we are focusing on the most traditional and studied one: chaos synchronization and masking. This technique is supported by the full synchronization of two identical chaotic dynamics (Chua's circuits in this case), where the information to be protected is added to the chaotic signal, and then it is masked. The resulting signal is used to synchronize the receptor and recover the original information signal. Figure 7 shows the proposed scheme for this cryptosystem. Different mathematical descriptions and models of this cryptosystem have been reported [52].

However, the key to this cryptosystem is the ability to achieve full synchronization, in the term described by Pecora and Caroll [53]. To allow full synchronization between receptor and transmitter, the masking signal must be injected into the receptor. But the chaotic dynamics in the receptor must also be stable and converge to the state represented by the masking signal. This is only feasible if the conditional Lyapunov exponents of the receptor are strictly negative. Table 1 shows the value of these exponents in the proposed cryptosystem. As can be seen, masking signal must be V_1 in order to ensure that the cryptosystem operates as expected. Figure 8 shows the evolution of the synchronization error in the cryptosystem when this scheme is used, which tends to zero (as expected as well).

However, this good behavior is only achieved if the receptor and transmitter behavior is fully identical. Any minimal change, including small variations caused by different implementations,

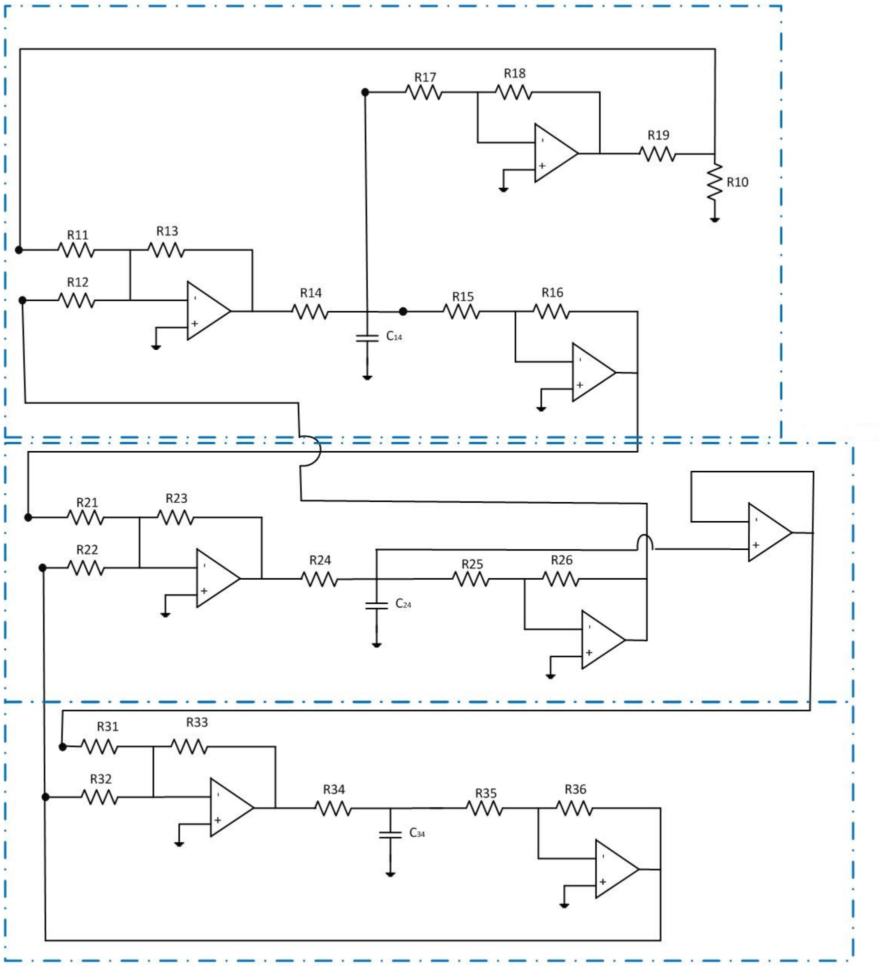

Figure 6: Chua's circuit implementation based on CNN

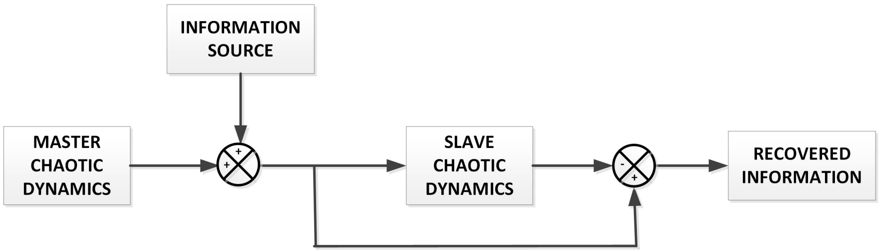

Figure 7: Architecture for the proposed chaotic cryptosystem (chaotic masking)

Table 1: Conditional Lyapunov exponents

Masking signal	**Lyapunov exponents**
V_1	-0.4982 -0.5014
V_2	-2.6316 0
I_3	1.4713 -5.3246

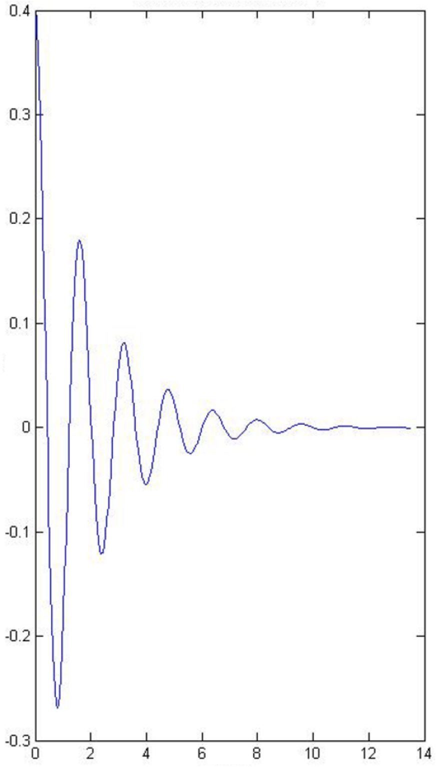

Figure 8: Synchronization error in the proposed chaotic cryptosystem

prevents the system from synchronizing and operating. The proposed universal receptor solves the problem.

3.3 Dynamic receptor adaptation

The architecture of the proposed universal receptor is shown in Figure 9. As can be seen, the receptor must include an instance or implementation of all the possible circuit realizations to be found in the transmitters. In this case: standard Chua circuit, cubic non-linearity, immittance converter, and CNN. The masking signal is tentatively introduced in all possible receptors (or circuit implementations), but a multiplexer chooses the most probable and better output after a statistical analysis. The final output of the receptor is dynamically adapted to the circuit

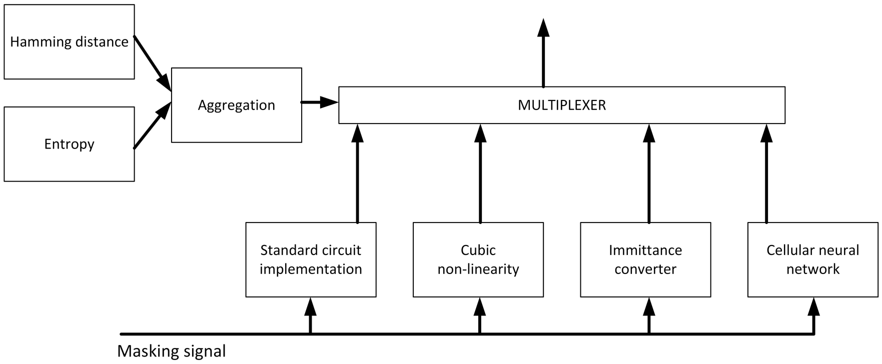

Figure 9: Architecture for the universal receptor

implementation which is identified as the most probable to be implemented in the transmitter.

This dynamic adaptation is based on two different indicators: the Shannon's entropy H and the Hamming distance d_H.

The Shannon's entropy of the recovered information M_r (7) is calculated using the traditional model (8), where probabilities $P(m_i)$ are obtained through the Laplace definition (9). Fully random sources (for which entropy is the unit) and information sources generating only one symbol (for which entropy is zero) are not probable. So, the probability $P_{imp}(H)$ of each circuit implementation to be the one implemented by the transmitter according to the Sannon's entropy can be obtained using a polynomial function with root in zero and the unit (10). Being λ a real parameter taking values in the range [1,4], and $\delta[\cdot]$ the Kronecker delta function.

$$M_r = \{m_i \quad i = 1, \dots, N_{Mr}\} \tag{7}$$

$$H(M_r) = -\sum_{\forall m_i \in M_r} P(m_i) \cdot log_2(P(m_i)) \tag{8}$$

$$P(m_i) = \frac{\sum_{\forall m_i \in M_r} \sum_{\forall m_k \in M_r} \delta[m_i - m_k]}{N_{Mr}} \tag{9}$$

$$P_{imp}(H) = \lambda \cdot (H - H^2) \tag{10}$$

On the other hand, the recovered information M_r should be composed by symbols s_j (with n_j bits) belonging to the code C_{tx} (11) employed in the transmitter. Some errors may occur, but (in general) the probability of a successful decryption decreases as the code in the receptor and the code in the transmitter are "further". This distance can be measured using the Hamming definition d_H (12). And the probability $P_{imp}(d_H)$ of each circuit implementation to be the one implemented by the transmitter according to the Hamming distance can be obtained using the usual mean calculation (13).

$$C_{tx} = \{s_j \quad j = 1, \dots, N_{Ctx}\} \tag{11}$$

$$d_H(s_j, s_z) = \sum_{k=1}^{n_j} \delta[s_j(k) - s_z(k)] \tag{12}$$

$$\begin{aligned} P_{imp}(d_H) = \frac{1}{N_{Ctx}} \sum_{\forall s_j \in M_r} \frac{1}{n_j} \cdot d_H(s_j, s_z^*) \\ s_z^* = min_{s_z} d_H(s_j, s_z) \end{aligned} \tag{13}$$

The global probability P_{imp} of each circuit implementation to be the one implemented by the transmitter is finally calculated as the weighted Euclidean distance (14). The implementation of the real circuit used by the remote transmitter is the one with the highest probability.

$$P_{imp} = \sqrt{\frac{1}{2}([P_{imp}(d_H)]^2 + [P_{imp}(H)]^2)} \tag{14}$$

4 Experimental validation: simulation results

In order to evaluate the proposed universal receptor, an experimental validation supported by simulation tools and scenarios was designed, deployed, and carried out. All experiments were supported by the MATLAB 2022a software suite, due to its proved numerical capabilities. All simulations were performed using a Linux architecture (Ubuntu 22.04 LTS) with the following hardware characteristics: Dell R540 Rack 2U, 96 GB RAM, two processors Intel Xeon Silver 4114 2.2G, HD 2TB SATA 7,2K rpm.

All four circuit implementations were modeled using the corresponding PSPice models, and all electrical signals were obtained using a numerical algorithm such as Runge-Kutta (with order four). The chaotic cryptosystem and its synchronization were also represented numerically. The clear information to be encrypted and transmitted was a plain text sequence. The number of characters correctly received by the receptor was monitored and measured as a dependent variable. The successful transmission rate is finally calculated as the ratio between the number of characters correctly decrypted and received and the total number of characters transmitted.

Two different scenarios were simulated, and their results were compared. In the first scenario, different Chua's circuit implementations were randomly associated in the transmitter and the receptor. In the second scenario, all receptors implemented the proposed universal receptor scheme.

Figure 10 shows the results obtained. As can be seen, when the implementations were randomly associated, the success rate is around 53%. This is coherent with one combination whose operation is smooth (when receptor and transmitter include the same circuit implementation), and some additional successful transmissions, received on a random basis. On the other hand, with the proposed universal receptor, successfully received characters are around 90%. This means an improvement greater than 63%. This allows us to conclude that the proposed solutions enable and enhance the interoperability between different circuit implementations.

5 Conclusions and future works

Typically, mobile devices are considered powerful enough to execute all the modules and services required to support secure and broadband communications, but future scenarios require embedded devices as the primary hardware component. And those embedded devices are resource-constrained. Their limited computing power can only manage minimal communication services, excluding other additional functionalities such as heavy-security mechanisms. Lightweight security and encryption are the most adopted approaches to mitigate this problem, including stream cipher and chaotic cryptosystems. However, while software implementations are fully replicable with no error, hardware components may change their properties and behavior depending on

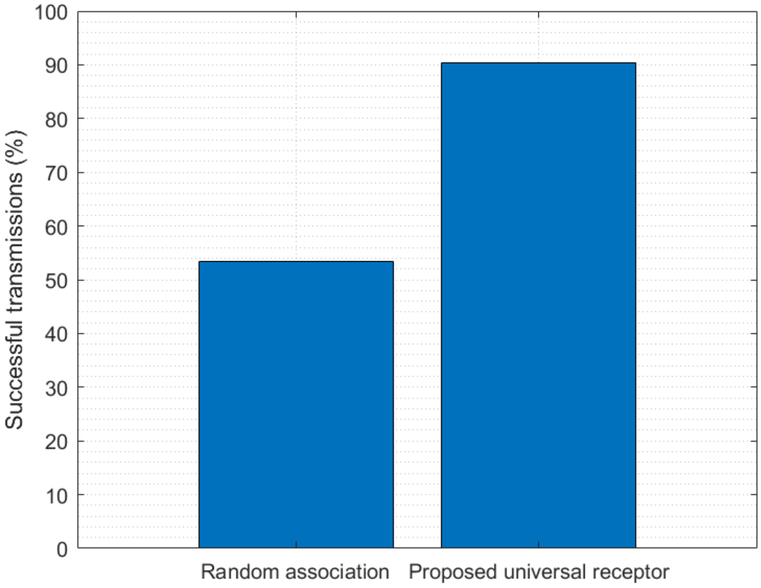

Figure 10: Experimental results

the manufacturing techniques and design. For standard digital circuits these small variations are not relevant, but chaotic cryptosystems are extremely sensitive and the transmitter and the receptor are expected to be totally identical.

In this paper, we address this challenge and propose a universal receptor for chaotic cryptosystems in embedded mobile devices. The described receptor will be able to operate with transmitters based on any of the existing implementation of the Chua's circuit. Using a combination of entropy metrics and binary distances, the receptor is able to identify the circuit implementation in the transmitter and dynamically adapt the receptor to this configuration.

Simulations tools are employed to validate the proposed technology, and results show the interoperability errors reduce more than 63%.

Future works will analyze the performance of the proposed technology in real scenarios and deployment with hardware devices and embedded software and components.

Acknowledgments

This work is supported by the Ministry of Science, Innovation and Universities through the COGNOS project (PID2019-105484RB-I00).

References

[1] Musa Hussain, Syed Muhammad Rizvi Jarchavi, Syeda Iffat Naqvi, Usama Gulzar, Salahuddin Khan, Mohammad Alibakhshikenari, and Isabelle Huynen. Design and fabrication of a printed tri-band antenna for 5g applications operating across ka-, and v-band spectrums. *Electronics 2021, Vol. 10, Page 2674*, 10:2674, 10 2021.

[2] Borja Bordel, Ramón Alcarria, and Tomás Robles. Interferenceless coexistence of 6g networks and scientific instruments in the ka-band. *Expert Systems*, page e13369, 2023.

[3] Borja Bordel, Ramón Alcarria, Diego Sánchez de Rivera, and Álvaro Sánchez. An inter-slice management solution for future virtualization-based 5g systems. *Advances in Intelligent Systems and Computing*, 926:1059–1070, 2020.

[4] Paul Schwenteck, Giang T. Nguyen, Holger Boche, Wolfgang Kellerer, and Frank H. P. Fitzek. 6g perspective of mobile network operators, manufacturers, and verticals. *IEEE Networking Letters*, pages 1–1, 4 2023.

[5] Borja Bordel, Ramón Alcarria, Joaquin Chung, Rajkumar Kettimuthu, Tomás Robles, and Iván Armuelles. Towards fully secure 5g ultra-low latency communications: A cost-security functions analysis. *Computers, Materials & Continua*, 74:855–880, 9 2022.

[6] Borja Bordel, Ramón Alcarria, Joaquin Chung, and Rajkumar Kettimuthu. Predictor-corrector models for lightweight massive machine-type communications in industry 4.0. *Integrated Computer-Aided Engineering*, 30:369–393, 1 2023.

[7] Dakhaz Mustafa Abdullah and Siddeeq Y. Ameen. Enhanced mobile broadband (embb): A review. *Journal of Information Technology and Informatics*, 1:13–19, 4 2021.

[8] Anutusha Dogra, Rakesh Kumar Jha, and Shubha Jain. A survey on beyond 5g network with the advent of 6g: Architecture and emerging technologies. *IEEE Access*, 9:67512–67547, 2021.

[9] Borja Bordel, Ramón Alcarria, Tomás Robles, and Diego Sánchez-De-Rivera. Service management in virtualization-based architectures for 5g systems with network slicing. *Integrated Computer-Aided Engineering*, 27:77–99, 1 2020.

[10] Borja Bordel, Ramon Alcarria, Diego Sanchez De Rivera, Diego Martín, and Tomas Robles. Fast self-configuration in service-oriented smart environments for real-time applications. *Journal of Ambient Intelligence and Smart Environments*, 10:143–167, 2018.

[11] Borja Bordel, Ramón Alcarria, and Tomás Robles. Recognizing human activities in industry 4.0 scenarios through an analysis-modeling- recognition algorithm and context labels. *Integrated Computer-Aided Engineering*, 29:83–103, 1 2022.

[12] Praveen Kumar Reddy Maddikunta, Quoc Viet Pham, Prabadevi B, N. Deepa, Kapal Dev, Thippa Reddy Gadekallu, Rukhsana Ruby, and Madhusanka Liyanage. Industry 5.0: A survey on enabling technologies and potential applications. *Journal of Industrial Information Integration*, 26:100257, 3 2022.

[13] Borja Bordel, Ramón Alcarria, Tomás Robles, and Diego Martín. Cyber–physical systems: Extending pervasive sensing from control theory to the internet of things. *Pervasive and Mobile Computing*, 40:156–184, 9 2017.

[14] Tomás Robles, Borja Bordel, Ramón Alcarria, and Diego Mart{ı́}n de Andrés. Mobile wireless sensor networks: Modeling and analysis of three-dimensional scenarios and neighbor discovery in mobile data collection. *Ad Hoc Sens. Wirel. Networks*, 35:67–104, 2017.

[15] Vishal A. Thakor, Mohammad Abdur Razzaque, and Muhammad R.A. Khandaker. Lightweight cryptography algorithms for resource-constrained iot devices: A review, comparison and research opportunities. *IEEE Access*, 9:28177–28193, 2021.

[16] Borja Bordel, Ramon Alcarria, Tomas Robles, and Alvaro Sanchez-Picot. Stochastic and information theory techniques to reduce large datasets and detect cyberattacks in ambient intelligence environments. *IEEE Access*, 6:34896–34910, 6 2018.

[17] Borja Bordel, Ramón Alcarria, and Tomás Robles. Lightweight encryption for short-range wireless biometric authentication systems in industry 4.0. *Integrated Computer-Aided Engineering*, 29:153–173, 1 2022.

[18] Borja Bordel, Amalia Beatriz Orue, Ramon Alcarria, and Diego Sanchez-De-Rivera. An intra-slice security solution for emerging 5g networks based on pseudo-random number generators. *IEEE Access*, 6:16149–16164, 3 2018.

[19] Borja Bordel, Ramon Alcarria, Tomas Robles, and Marcos Sanchez Iglesias. Data authentication

and anonymization in iot scenarios and future 5g networks using chaotic digital watermarking. *IEEE Access*, 9:22378–22398, 2021.

[20] María Pilar Mareca and Borja Bordel. Improving the complexity of the lorenz dynamics. *Complexity*, 2017, 2017.

[21] Mahmoud Ahmad Al-Khasawneh, Siti Mariyam Shamsuddin, Shafaatunnur Hasan, and Adamu Abu Bakar. An improved chaotic image encryption algorithm. *2018 International Conference on Smart Computing and Electronic Enterprise, ICSCEE 2018*, 11 2018.

[22] Naoki Masuda and Kazuyuki Aihara. Cryptosystems with discretized chaotic maps. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, 49:28–40, 1 2002.

[23] Khunanon Karawanich, Montree Kumngern, Jirat Chimnoy, and Pipat Prommee. A four-scroll chaotic generator based on two nonlinear functions and its telecommunications cryptography application. *AEU - International Journal of Electronics and Communications*, 157:154439, 12 2022.

[24] Pilar Mareca and Borja Bordel. A robust implementation of a chaotic cryptosystem for streaming communications in wireless sensor networks. *Advances in Intelligent Systems and Computing*, 570:95–104, 2017.

[25] Usman Arshad, Syeda Iram Batool, and Muhammad Amin. A novel image encryption scheme based on walsh compressed quantum spinning chaotic lorenz system. *International Journal of Theoretical Physics*, 58:3565–3588, 10 2019.

[26] Walid El-Shafai, Fatma Khallaf, El Sayed M. El-Rabaie, and Fathi E.Abd El-Samie. Robust medical image encryption based on dna-chaos cryptosystem for secure telemedicine and healthcare applications. *Journal of Ambient Intelligence and Humanized Computing*, 12:9007–9035, 10 2021.

[27] Attaullah, Tariq Shah, and Sajjad Shaukat Jamal. An improved chaotic cryptosystem for image encryption and digital watermarking. *Wireless Personal Communications*, 110:1429–1442, 2 2019.

[28] Borja Bordel, Ramón Alcarria, Joaquin Chung, Rajkumar Kettimuthu, and Tomás Robles. Evaluation and modeling of microprocessors' numerical precision impact on 5g enhanced mobile broadband communications. pages 267–279, 2021.

[29] Li Xiong, Liwan Qi, Sufen Teng, Qishan Wang, Lu Wang, and Xinguo Zhang. A simplest lorenz-like chaotic circuit and its applications in secure communication and weak signal detection. *The European Physical Journal Special Topics 2021 230:7*, 230:1933–1944, 6 2021.

[30] Octavio A. Gonzales, Gunhee Han, José Pineda De Gyvez, and Edgar Sânchez-Sinencio. Lorenz-based chaotic cryptosystem: a monolithic implementation. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, 47:1243–1247, 8 2000.

[31] Ravi Monani, Brian Rogers, Amin Rezaei, and Ava Hedayatipour. Implementation of chaotic encryption architecture on fpga for on-chip secure communication. *2022 IEEE Green Energy and Smart Systems, IGESSC 2022*, 2022.

[32] A. Shailaja and Krishnamurthy Gorappa Ningappa. A low area vlsi implementation of extended tiny encryption algorithm using lorenz chaotic system. *International Journal of Information and Computer Security*, 14:3–19, 2021.

[33] Kaya Demir and Salih Ergun. A comparative study on the robustness of chaos-based random number generators. *Proceedings - APCCAS 2019: 2019 IEEE Asia Pacific Conference on Circuits and Systems: Innovative CAS Towards Sustainable Energy and Technology Disruption*, pages 245–248, 11 2019.

[34] Mohamed Salah Azzaz, Rabiai Fellah, Camel Tanougast, and Redouane Kaibou. Design and fpga implementation of trng based on a new multi-wing attractor in lorenz chaotic system. *The European Physical Journal Special Topics 2021 230:18*, 230:3469–3480, 7 2021.

[35] Hammam Orabi, Mohammed Elnawawy, Assim Sagahyroon, Fadi Aloul, Ahmed S. Elwakil, and Ahmed G. Radwan. On the implementation of a rotated chaotic lorenz system on fpga. *Proceedings - APCCAS 2019: 2019 IEEE Asia Pacific Conference on Circuits and Systems: Innovative CAS Towards Sustainable Energy and Technology Disruption*, pages 417–422, 11 2019.

[36] P. D. Kamdem Kuate, Qiang Lai, and Hilaire Fotsin. Dynamics, synchronization and elec-

tronic implementations of a new lorenz-like chaotic system with nonhyperbolic equilibria. *https://doi.org/10.1142/S0218127419501979*, 29, 12 2019.

[37] Mohamed Gafsi, Nessrine Abbassi, Mohammed Ali Hajjaji, Jihene Malek, and Abdellatif Mtibaa. Xilinx zynq fpga for hardware implementation of a chaos-based cryptosystem for real-time image protection. *https://doi.org/10.1142/S0218126621502042*, 30, 4 2021.

[38] Şuayb Çağrı Yener, Reşat Mutlu, and Ertuğrul Karakulak. Implementation of a microcontroller-based chaotic circuit of lorenz equations. *Balkan Journal of Electrical and Computer Engineering*, 8:355–360, 10 2020.

[39] Mohamed Saber and Esam A.A. Hagras. Parallel multi-layer selector s-box based on lorenz chaotic system with fpga implementation. *Indonesian Journal of Electrical Engineering and Computer Science*, 19:784–792, 8 2020.

[40] Rui Wang, Meng-Yang Li, and Hai-Jun Luo. Exponential sine chaotification model for enhancing chaos and its hardware implementation. *Chinese Physics B*, 31:080508, 8 2022.

[41] Iman S. Badr, Ahmed G. Radwan, El Sayed M. EL-Rabaie, Lobna A. Said, Ghada M. El Banby, Walid El-Shafai, and Fathi E. Abd El-Samie. Cancellable face recognition based on fractional-order lorenz chaotic system and haar wavelet fusion. *Digital Signal Processing*, 116:103103, 9 2021.

[42] Yuling Luo, Junxiu Liu, Lvchen Cao, Jinjie Bi, and Senhui Qiu. Hardware implementation of cryptographic hash function based on spatiotemporal chaos. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, 152:395–404, 11 2015.

[43] Merah Lahcene, Chaib Noureddine, Pascal Lorenz, and Ali Pacha Adda. Securing information using a proposed reliable chaos-based stream cipher: with real-time fpga-based wireless connection implementation. *Nonlinear Dynamics*, 111:801–830, 1 2023.

[44] A. Flores-Vergara, E. E. García-Guerrero, E. Inzunza-González, O. R. López-Bonilla, E. Rodríguez-Orozco, J. R. Cárdenas-Valdez, and E. Tlelo-Cuautle. Implementing a chaotic cryptosystem in a 64-bit embedded system by using multiple-precision arithmetic. *Nonlinear Dynamics*, 96:497–516, 4 2019.

[45] Walid El-Shafai, Fatma Khallaf, El Sayed M. El-Rabaie, and Fathi E.Abd El-Samie. Proposed 3d chaos-based medical image cryptosystem for secure cloud-iomt ehealth communication services. *Journal of Ambient Intelligence and Humanized Computing*, pages 1–28, 7 2022.

[46] Abraham Flores-Vergara, Everardo Inzunza-González, Enrique Efren García-Guerrero, Oscar Roberto López-Bonilla, Eduardo Rodríguez-Orozco, Juan Miguel Hernández-Ontiveros, José Ricardo Cárdenas-Valdez, and Esteban Tlelo-Cuautle. Implementing a chaotic cryptosystem by performing parallel computing on embedded systems with multiprocessors. *Entropy 2019, Vol. 21, Page 268*, 21:268, 3 2019.

[47] Ju H. Park. Chaos synchronization between two different chaotic dynamical systems. *Chaos, Solitons & Fractals*, 27:549–554, 1 2006.

[48] Leon O Chua. The genesis of chua's circuit, 1 1992.

[49] Leon O. Chua. Chua's circuit 10 years later. *International Journal of Circuit Theory and Applications*, 22:279–305, 7 1994.

[50] Luigi Fortuna, Mattia Frasca, and Maria Gabriella Xibilia. Chua's circuit implementations: Yesterday, today and tomorrow. *Chua's Circuit Implementations: Yesterday, Today And Tomorrow*, pages 1–224, 1 2009.

[51] Guo Qun Zhong. Implementation of chua's circuit with a cubic nonlinearity. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, 41:934–941, 1994.

[52] Pilar Mareca and Borja Bordel. Robust hardware-supported chaotic cryptosystems for streaming commutations among reduced computing power nodes. *Analog Integrated Circuits and Signal Processing*, 98:11–26, 1 2019.

[53] Louis M. Pecora and Thomas L. Carroll. Synchronization in chaotic systems. *Physical Review Letters*, 64:821, 2 1990.