Chaos-Based Dynamical Parameter Estimation for Physical Layer Authentication in Wireless IoT Networks

electronics

Article

Chaos-Based Dynamical Parameter Estimation for Physical Layer Authentication in Wireless IoT Networks

Ruslans Babajans [1], Darja Cirjulina [1], Sergejs Tjukovs [1], Sara Becchi [2], Jacopo Secco [2], Dmytro Vovchuk[1], Deniss Kolosovs [1] and Dmitrijs Pikulins [1,*]

[1] Institute of Photonics, Electronics and Telecommunications, Riga Technical University, LV-1048 Riga, Latvia; ruslans.babajans@rtu.lv (R.B.); darja.cirjulina@rtu.lv (D.C.); sergejs.tjukovs@rtu.lv (S.T.); dmytro.vovchuk@rtu.lv (D.V.); deniss.kolosovs@rtu.lv (D.K.)
[2] Department of Electronics and Telecommunications, Politecnico di Torino, 10123 Turin, Italy; sara.becchi@polito.it (S.B.); jacopo.secco@polito.it (J.S.)
* Correspondence: dmitrijs.pikulins@rtu.lv

Abstract

The proliferation of Internet of Things (IoT) devices and services creates not only significant benefits but also new security threats. Classical information encryption techniques are not suitable for resource-constrained edge modules, thereby generating the demand for lightweight and efficient data protection algorithms. This work presents a novel dynamical parameter estimation scheme for chaotic oscillators, applied to physical-layer authentication (PLA). The proposed approach relies on the receiver's capability to estimate a selected parameter of the transmitter's oscillator determined by circuit configuration from the received chaotic signal using a locally synchronized oscillator, thereby enabling secure authentication based on a hardware-encoded identifier. The scheme is intended to complement a chaos-based wireless sensor network (WSN) architecture, where sensor nodes (SNs) implement analog chaotic oscillators, and the gateway operates discrete-time models. The Vilnius chaotic oscillator was chosen to validate the proposed PLA scheme. A rigorous bifurcation analysis of analytical, SPICE and discrete oscillator models was first conducted to identify parameter regions that preserve chaotic dynamics, establishing correspondence between models to guarantee the feasibility of parameter estimation across implementations. The digital realization of the parameter estimator demonstrated accurate and stable operation, with a small and nearly constant estimation relative error not exceeding 1.01%. Key performance metrics were analyzed, including estimation time, precision, and noise robustness. A tradeoff between estimation speed and accuracy was identified, particularly under noisy channel conditions. Finally, the influence of the receiver's native oscillator parameter on distinguishable transmitter parameter ranges was demonstrated, highlighting the configurability and security potential of the proposed system against unauthorized transmissions.

Keywords: physical-layer authentication; chaotic oscillator; nonlinear dynamical systems; IoT

Academic Editors: Dianwei Qian and Shiwen Tong

Received: 9 January 2026
Revised: 6 February 2026
Accepted: 9 February 2026
Published: 10 February 2026

1. Introduction

Wireless communications have become an integral component of modern intelligent systems, including buildings, industrial automation, healthcare, transportation, and smart cities. It enables the acquisition and transmission of data from distributed sensors, which are often deployed in environments with limited infrastructure support, while the wireless

transmission medium offers significant advantages—such as flexible deployment of Internet of Things (IoT) nodes and reduced dependence on wired power and data connections—it also introduces fundamental security vulnerabilities [1,2]. In particular, radio frequency (RF) transmissions are by nature broadcast and can be received by any device within range. In applications involving critical infrastructure or healthcare, where sensitive information is transmitted, this exposure significantly increases the risk of malicious attacks [3]. Ensuring a high level of security typically relies on advanced cryptographic algorithms, which impose substantial computational and energy overhead. However, wireless sensor nodes deployed at the network edge are generally cost- and energy-constrained, as large numbers of such devices are often required for adequate coverage [4]. As a result, active research has focused on enhancing the security of resource-constrained wireless communication systems by applying chaos theory to novel cryptographic and authentication techniques.

The chaos phenomenon is observed in nonlinear dynamical systems and is characterized by the strong dependence on initial conditions, sensitivity to parameter variations, and non-repetitive signals [5]. In the fields of electronics and telecommunications, chaos occurs in relatively simple analog oscillators and systems of differential equations describing them [6], discrete maps [7], switching DC-DC converters [8–10], phase-locked loops [11], systems with memristors [12,13], semiconductor lasers and optoelectronic oscillators [14]. Chaos theory is widely integrated across engineering areas such as communications, computing, random number generation, robotic motion, distributed sensing, and information encryption [15]. As IoT edge devices are mostly resource-constrained, lightweight cryptography has emerged to reduce computational complexity, memory usage, and power consumption [16]. Chaotic maps are broadly adopted in lightweight cryptography algorithms to minimize computational overhead and achieve superior performance [17–23].

Another way of to improve security in simple devices is to integrate hardware features and environmental conditions to generate cryptographic primitives. A notable technology for low-power IoT devices is the Physical Unclonable Function (PUF), which leverages inherent, uncontrollable variations in the semiconductor manufacturing process to create a unique fingerprint for each device with minimal hardware overhead. PUF can provide Physical-Layer Authentication (PLA) for IoT without relying on traditional cryptographic methods or requiring secret keys to be stored in memory [24].

It is also possible to utilize the imperfections in components of a transmitter circuit to create a Radio Frequency Fingerprint, which can be used for PLA [25]. The physical properties of a wireless communication channel are used as a source of randomness suitable for key generation. Measurements of channel characteristics, such as received signal strength (RSS), channel impulse response (CIR), channel state information (CSI), and channel frequency response (CFR), provide sufficient information for channel-based authentication schemes [26]. Following the acquisition of channel measurements, the raw data undergoes quantization into bitstreams, which are then synchronized via information reconciliation and refined through privacy amplification to produce a consistent, high-entropy cryptographic key. This integrated process ensures that any discrepancies caused by environmental noise are corrected and that potential information leakage is eliminated [27].

In summary, PLA schemes exploit random hardware and media features to generate unique and unpredictable device fingerprints. However, since chaotic systems generate signals with low autocorrelation and spread-spectrum characteristics while remaining fully deterministic, they can be implemented as an alternative physical-layer authentication approach.

Chaos-based authentication is an area of intensive remains an active area of research, and with various several promising techniques are being proposed in the scientific literature. In [28], the Asymmetric Cubic Logistic Map is used in a challenge-response

authentication scheme [29] to ensure secure, efficient, and attack-resistant authentication in telehealth environments. To further improve the security of Wireless Sensor Networks (WSNs), authors in [30] combine the Chebyshev chaotic map cryptographic mechanism with physical unclonable functions. The same combination of chaotic map and PUF is presented in [31] to design a lightweight authentication protocol for underwater acoustic networks. Chaotic maps are used because of their lower computational overhead than Elliptic Curve Cryptography (ECC), but some proposed authentication and key agreement (AKA) protocols suffer from distinct vulnerabilities [32]. Discrete chaotic maps are usually typically implemented in microcontrollers or field-programmable gate arrays (FPGAs); however, it is also possible to use analog chaotic oscillators can also be employed in a digital communication system, such as quadrature chaos shift keying (QCSK) proposed in [33], where the generated chaotic waveforms are used as carriers.

Additionally, it has been demonstrated that an analog chaotic oscillator can be synchronized with its mathematical model implemented on an FPGA [34], thus enabling coherent communication between a cost-optimized IoT device equipped with a simple analog oscillator and a more advanced gateway capable of storing a collection of digital models of chaotic oscillators. An experimental study of synchronization between analog and digital chaotic oscillators revealed model features that could potentially be incorporated into a PLA scheme for resource-constrained IoT devices. Analysis of the normalized differential equations of analog chaotic oscillators reveals that specific dimensionless parameters can be estimated from the state variables. These dimensionless quantities are expressed in terms of oscillator's circuit components, such as resistance, capacitance, and inductance, and can be selected according to the corresponding bifurcation diagrams. As in the case with PUFs, a unique device identifier can be coded in the hardware during the production process. Moreover, designs with tunable components can facilitate even more sophisticated authentication protocols.

This paper makes the following key contributions:

- A novel chaotic oscillator parameter estimator-based PLA scheme is proposed using Vilnius chaotic oscillator, and preliminary results are presented that identifying key performance metrics of the estimator are presented.
- Bifurcation diagrams of different models of the Vilnius chaotic oscillator are presented, showing the corresponding changes in dynamical regimes as the parameter a is varied. This analysis establishes suitable parameter a ranges that ensure chaotic operation and is a prerequisite for implementing the proposed authentication scheme.

The structure of the article is organized as follows: in Section 2, the concept of a parameter estimator-based hardware authentication technique is presented, also showing its integration in a generalized chaotic communication system. Section 3 presents the Vilnius chaotic oscillator circuit and its discrete mathematical model, designed for implementation in an FPGA. In Section 4, the results of the bifurcation analysis are presented for the three models of the Vilnius chaotic oscillator: the analytical model, the SPICE model, and the discrete-time model. The dimensionless parameter a, determined by the real circuit components, is chosen as a bifurcation argument, revealing a nonhomogeneous structure with chaotic regions and periodic windows. Section 5 describes the digital design of the proposed chaotic oscillator parameter estimator and presents its performance assessment. The article concludes with a discussion of the obtained results in Section 6.

2. Chaos Oscillator Parameter Estimator-Based Hardware Authentication Scheme

The current section presents the concept of the chaos-based PLA scheme for WSN. The star-topology chaos-based WSN originally proposed in [35] is presented in Figure 1.

The key design element of the presented system is the use of analog chaotic oscillator circuits in each individual Sensor Node (SN) together with the discrete models of chaotic oscillators implemented in Gateway (GW) for chaos-based wireless data transfer. Chaotic oscillators are simple, low-power analog circuits that would be a cost-effective solution for an individual SN. On the GW, a single FPGA chip can host discrete models of multiple oscillators, thus making it possible to transfer information between the SNs and GW using chaotic waveforms. The previous work [36] demonstrated that it is possible to establish synchronization between analog chaotic oscillators and their discrete models hosted on an FPGA.

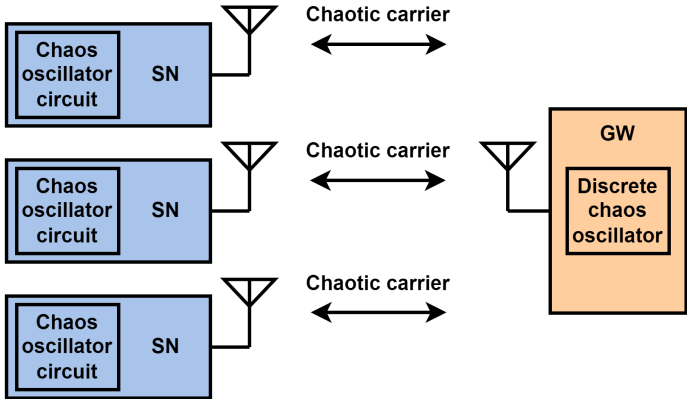

Figure 1. Star-topology WSN based on application of analog and discrete chaos oscillators.

In order to understand the proposed PLA scheme, it is important to outline the key design elements of the chaos-based data transfer scheme shown in Figure 2, which represents a generalized architecture based on earlier studies [37,38]. The transmitter hosts the drive chaos oscillator with state variables x_m, y_m and z_m. The state variable y_m is used to establish chaotic synchronization using the Pecora–Carroll approach [39]. The binary information signal $b(t)$ is transferred by applying a chaos shift keying (CSK) technique. The figure shows that the transmitted information is encoded by applying phase shift keying (PSK) to the chaotic state variable x_m, as in [38]. The transmitter then applies modulation to transfer the information-carrying and synchronization signals to the receiver through the wireless channel. Alternatively, the chaos-based data transmission system in [37] transfers the binary information signal $b(t)$ by CSK using x_m and z_m, yet the core elements of the system are similar.

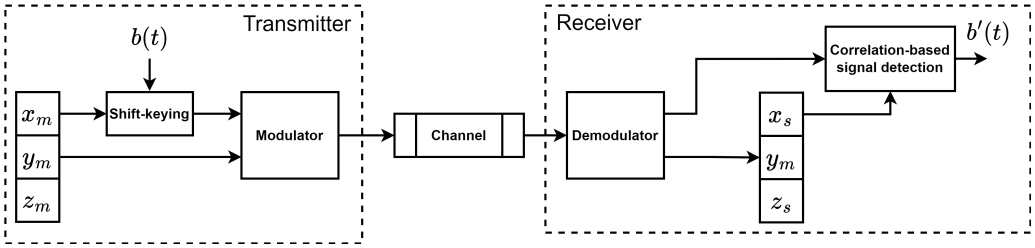

Figure 2. Generalized chaos-based data transfer scheme.

The receiver hosts the response chaotic oscillator with state variables x_s, y_s and z_s. The demodulator outputs the received y_m and information-carrying x_m. By Pecora–Carroll synchronization, the y_m replaces the y_s of the receiver's oscillator, thus establishing synchronization. When synchronized, x_s and x_m, as well as z_s and z_m signals match. The detection of the received binary information signal $b'(t)$ is done by calculating Pearson's correlation coefficient using x_s and the received information-carrying x_m. In the context of chaos-based WSN, the transmitter's chaotic oscillator is implemented as a circuit on printed

circuit board (PCB), and the receiver's chaotic oscillator is implemented as a discrete model on a FPGA.

The key enabling factor for such data transfer is the ability of chaotic oscillators to synchronize. The use of chaotic carriers alone enhances the security aspect on the hardware level, yet chaotic synchronization alone is not enough to fully secure the data transfer. The receiver can easily synchronize and receive data from another, possibly unauthorized transmitter with a similar oscillator. This leads to a necessity to supplement the previously proposed chaos-based data transfer schemes with the mechanism for distinguishing between different transmitters.

Chaotic synchronization is highly robust, data transmission requires two synchronized chaotic oscillator signals, and the oscillator dynamics are governed by parameterized equations directly related to the chaotic waveforms. Therefore, the proposed authentication scheme relies on estimating at least one parameter of the transmitter's chaos oscillator at the receiver. The detailed outline of the proposed authentication scheme is presented in Figure 3.

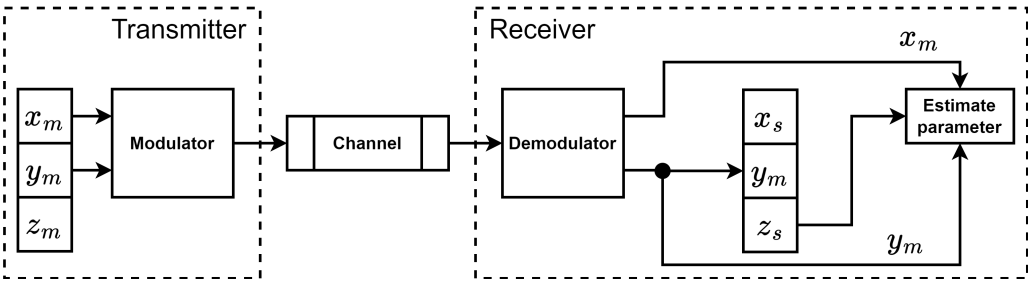

Figure 3. Proposed chaos-based authentication scheme.

The figure demonstrates the transmitter sending the x_m and y_m signals to the receiver. Like in the data transfer case, the y_m is used for Pecora–Carroll synchronization. In the receiver, the received x_m and y_m as well as the signal from the local chaos oscillator z_s are passed to the block that estimates one of the parameters of the transmitter's chaotic oscillator. The use of chaotic synchronization allows to use z_s that is in phase with z_m, thus there is no need to transmit all three chaotic signals in order to estimate the transmitter's oscillator parameter. This system can supplement the existing proposed modulation schemes in Figure 2, enabling the identification of the transmitter's chaotic oscillator based on a selected control parameter. This estimation can be performed prior to the message transfer. Because the signals used in the estimation are transmitted over a public channel, the parameter must be dynamically adjusted according to a pre-agreed pattern, thereby preventing the data from being received from an unauthorized transmitter with a similar architecture.

The parameter estimation mechanism exploits the stable synchronization regime: once the state synchronization error is driven to zero by Pecora–Carroll synchronization, this enables the convergence of the estimator to a stable value. Although the present approach does not employ adaptive laws for synchronization as in adaptive synchronization schemes, its robustness relies on a similar feedback-driven error correction principle in the estimator itself. In this sense, the presented estimator shares conceptual similarities with adaptive synchronization [13,40].

The following sections further elaborate on the implementation and performance evaluation of the oscillator parameter estimator in the case of the Vilnius chaotic oscillator.

3. Vilnius Chaotic Oscillator

The Vilnius chaotic oscillator [41] is a simple, robust nonlinear circuit widely used in studies of chaotic dynamics due to its ease of implementation and reliable operation. This oscillator was selected for the present work because its straightforward structure and stable performance enable good agreement between simulations and experimental measurements. The chosen chaotic oscillator can generate signals at different frequency ranges by adjusting the nominal values of its reactive elements. This frequency scalability is particularly relevant for chaos-based communication systems, where the selection of carrier frequency must align with the channel bandwidth and system requirements.

3.1. Circuit and Mathematical Model

The Vilnius chaotic oscillator, shown in Figure 4, is implemented using an operational amplifier, an RLC resonant circuit placed in the positive-feedback path, an additional capacitor, and a diode. This configuration enables the generation of chaotic oscillations with a minimal component count.

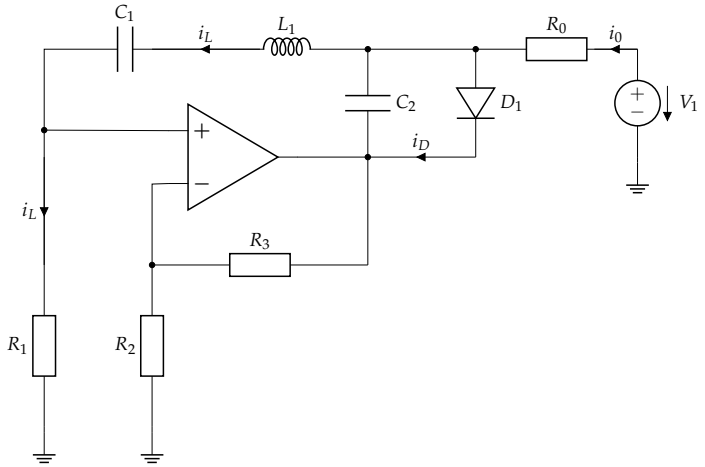

Figure 4. Schematic of the Vilnius chaotic oscillator [41], where $V_1 = 5\,\text{V}$, $R_1 = 1\,\text{k}\Omega$, $R_2 = 9.1\,\text{k}\Omega$, $R_3 = 6.2\,\text{k}\Omega$, $R_4 = 18\,\text{k}\Omega$, $L_1 = 1\,\text{mH}$, $C_1 = 1\,\text{nF}$, $C_2 = 150\,\text{pF}$, as D_1 1N4148 was used, as operational amplifier TL082 was used.

The oscillator dynamics can be described by three state variables: the voltage across the capacitor C_1 (v_{C1}), the current through the inductor L_1 (i_L), and the voltage across the capacitor C_2 (v_{C2}). Applying Kirchhoff's voltage and current laws yields the following differential equations:

$$\begin{cases} C_1 \dfrac{\mathrm{d}v_{C1}}{\mathrm{d}t} = i_L \\ C_2 \dfrac{\mathrm{d}v_{C2}}{\mathrm{d}t} = i_0 + i_L - i_D \\ L_1 \dfrac{\mathrm{d}i_L}{\mathrm{d}t} = (k-1) \cdot R_1 \cdot i_L - v_{C_1} - v_{C_2} \end{cases} \tag{1}$$

where i_D is the diode current, i_0 is the current through the resistor R_0, and k denotes the closed-loop gain of the operational amplifier:

$$k = 1 + \frac{R_3}{R_2}. \tag{2}$$

The nonlinear behavior of the oscillator arises from the diode's current–voltage characteristic, expressed as:

$$i_D = i_S \cdot \left(e^{\frac{v_D}{v_T}} - 1 \right), \tag{3}$$

with $v_D = v_{C2}$, i_S representing the diode saturation current (approximately 2×10^{-14} A for a 1N4148 diode), and v_T the thermal voltage (approximately 25.8 mV at 298 K).

The combination of the diode's exponential nonlinearity and the feedback network produces chaotic oscillations. The system exhibits a classical period-doubling route to chaos, as confirmed through bifurcation analysis and the presence of positive Lyapunov exponents, which verify chaotic behavior for certain parameter values.

3.2. Discrete Implementation of the Oscillator

Beyond the physical formulation given above, the Vilnius oscillator is also conveniently described through a set of dimensionless parameters introduced in the original work by Tamaševičius et al. [41] compiled in (4), resulting in the normalized differential equations in (5).

$$\begin{array}{ccc} x = \frac{v_{C_1}}{V_T}, & y = \frac{\rho \cdot i_L}{V_T}, & z = \frac{v_{C_2}}{V_T}, \\ V_T = \frac{k_B T}{e}, & \rho = \sqrt{\frac{L}{C_1}}, & \varepsilon = \frac{C_2}{C_1}, \\ a = (k-1)\frac{R_1}{\rho}, & b = \frac{\rho \cdot i_0}{V_T}, & c = \frac{\rho \cdot i_S}{V_T}, \\ \theta = \frac{t}{\tau}, & \tau = \sqrt{L \cdot C_1}. & \end{array} \tag{4}$$

$$\begin{cases} \frac{dx}{d\theta} = y \\ \frac{dy}{d\theta} = a \cdot y - x - z \\ \varepsilon \cdot \frac{dz}{d\theta} = b + y + c(\exp(z) - 1) \end{cases} \tag{5}$$

In our previous work [36], we obtained the discrete-time solution of the system using Euler–Cromer numerical integration. The discrete system is expressed by the difference equations in (6), where $\Delta\theta$ is the integration time step.

$$\begin{cases} \underbrace{x[n+1]}_{\text{Next value}} = \underbrace{x[n]}_{\text{Current value}} + \underbrace{y[n]}_{\text{Derivative}} \cdot \underbrace{\Delta\theta}_{\text{Time step}} \\ \underbrace{y[n+1]}_{\text{Next value}} = \underbrace{y[n]}_{\text{Current value}} + \underbrace{(a \cdot y[n] - x[n] - z[n])}_{\text{Derivative}} \cdot \underbrace{\Delta\theta}_{\text{Time step}} \\ \underbrace{z[n+1]}_{\text{Next value}} = \underbrace{z[n]}_{\text{Current value}} + \underbrace{\left(\frac{b}{\varepsilon} + \frac{1}{\varepsilon} \cdot y[n] - \frac{c}{\varepsilon} \cdot (\exp(z[n]) - 1) \right)}_{\text{Derivative}} \cdot \underbrace{\Delta\theta}_{\text{Time step}} \end{cases} \tag{6}$$

The resulting system shows that the next value of the state variable equals the current value plus the derivative multiplied by the time step. This form is then transferred to a digital circuit, as demonstrated in Figure 5. The system is based on registers that update the state variables on each rising edge of the clock cycle. The stored values $x[n]$, $y[n]$, and $z[n]$, as well as the constants, are passed to the "Calculate derivatives" pipeline that calculates the "Derivative" part from (6) for each state variable with equal delays. The nonlinearity in the pipeline is approximated via read-only memory (ROM) with a 12-bit address space lookup table (LUT). The calculated derivatives dx, dy and dz are then multiplied by the time step $\Delta\theta$ and added to the respective $x[n]$, $y[n]$ and $z[n]$ signals, thus acquiring the next values $x[n+1]$, $y[n+1]$ and $z[n+1]$. The system was designed for fixed-point arithmetic,

allocating 8 bits to the integer and 14 bits to the fractional part of the output chaotic signals. The following digital design of the oscillator was previously implemented in an FPGA and verified in [36].

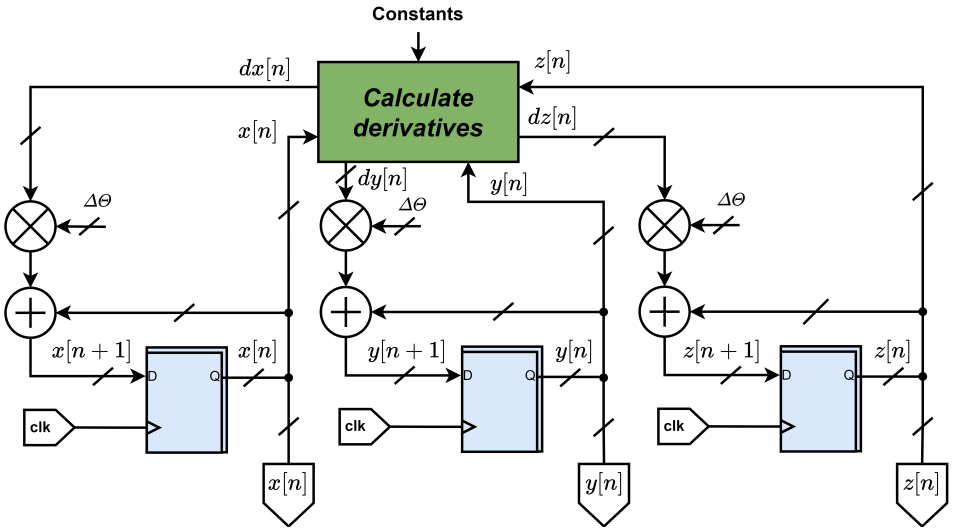

Figure 5. Full digital design of chaotic oscillator system equations.

4. Bifurcation Analysis of the Vilnius Oscillator

Bifurcation analysis is a fundamental tool for examining how qualitative changes in system dynamics arise as a function of a control parameter. In nonlinear oscillators, variations in governing parameters force the system to transition from steady-state or periodic oscillations to complex aperiodic motion through a sequence of bifurcations. These transitions are typically characterized through brute-force bifurcation diagrams, which visualize the asymptotic behavior of a selected state variable as the control parameter is swept over a predefined range. For chaotic communication and authentication systems, such analysis is essential, as the presence, robustness, and stability of chaotic modes determine the feasibility and reliability of the proposed methodology.

In this section, bifurcation analysis is carried out for three representations of the Vilnius chaotic oscillator: the continuous-time mathematical model, the LTspice circuit-level implementation, and the digital discrete-time model used for FPGA realization. Each of these models inherently introduces different levels of abstraction, non-ideality, and numerical effects. Therefore, comparing their bifurcation characteristics is necessary to ensure consistent dynamic behavior across the analytical, simulation, and hardware domains.

The obtained bifurcation diagrams are analyzed to identify regions of periodicity, onset of chaos, and the presence of periodic windows embedded within chaotic regimes. Particular emphasis is placed on the behavior of the system with respect to the control parameter a, selected as the parameter for authentication in chaos-based data transfer using Vilnius chaotic oscillators.

The final objective of this analysis is to determine practical parameter intervals of a where chaos is simultaneously sustained in the LTspice (i.e., analog hardware-equivalent) model and in the digital implementation suitable for FPGA deployment. These identified operating regions form the basis for reliable parameter estimation, ensuring that the proposed authentication mechanism operates in a stable chaotic regime in both analogue sensor nodes and digital gateways, thus enabling consistent and secure system performance.

4.1. Numerical Calculations

The first bifurcation diagram, based on the system of differential Equation (1), illustrates the primary dynamical changes and operating modes of the oscillator as the parameter a is varied. The obtained bifurcation diagrams are presented in Figure 6.

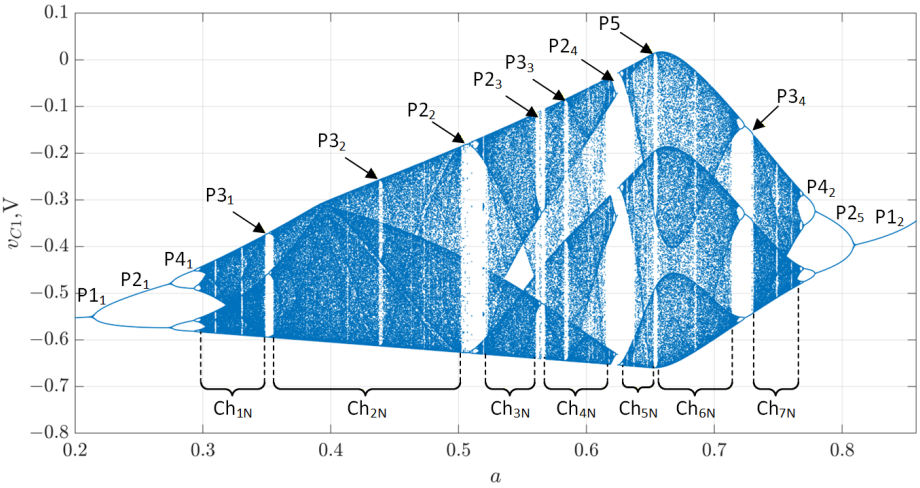

Figure 6. The bifurcation diagram obtained from the differential Equation (1).

The operation begins in a period-1 (P1) regime and evolves into chaotic dynamics through a classical period-doubling cascade as the control parameter a increases. As the system continues to grow, it exhibits broad chaotic regions, indicating a strongly aperiodic response. These chaotic domains are interrupted by low-periodicity windows, where the oscillator temporarily returns to regular behavior. In the examined interval, the most prominent of these windows correspond to P3, P2, and P5 regimes, appearing as clearly distinguishable periodic branches embedded within the chaotic band.

For higher values of a, the onset of a transition back toward periodicity is observed. The inverse period-doubling sequence results in the degeneration of chaotic motion into lower-order periodic oscillations. Eventually, the system returns to a stable P1 regime, demonstrating that chaos in the analog Vilnius oscillator is confined within a finite and well-defined parameter interval. The obtained bifurcation diagram confirms the presence of a robust chaotic operating region suitable for the proposed methodology, depicted as ChxN, while also clearly identifying parameter ranges where the system becomes periodic and therefore inappropriate for authentication purposes.

4.2. Simulation Study

LTspice evaluates the circuit's behavior under more realistic conditions by incorporating the non-idealities present in commercially available components. The operational amplifier and diode are represented using detailed SPICE-level models that include nonlinear transfer characteristics, finite bandwidth, parasitic capacitances, and temperature dependence, providing a substantially more realistic representation of their behavior than idealized models. In contrast, the passive components and supply sources are modeled using their nominal values and therefore remain close to ideal. Consequently, the LTspice simulation provides a partially realistic approximation of the oscillator, capturing the dominant nonlinearities of the active elements while retaining simplified representations of the linear components, and serves as an essential intermediate evaluation stage before hardware prototyping.

All component values and operating parameters were selected to match those defined in Section 3. The only parameter varied during the simulation was the dimensionless control

parameter a, which was introduced previously. To adjust a, resistor R_1 was recalculated according to its analytical relation with the resonant impedance. This choice was made because R_1 is simple to modify experimentally and provides direct control of a. The parameter a was swept from 0.2 to 1.2, and the corresponding R_1 values were determined using MATLAB *2023b*.

To further examine how parameter a affects the system behavior, bifurcation diagrams were generated by launching LTspice simulations directly from MATLAB. This automated framework swept R_1 over the interval $R_1 \in [294, 1761]\,\Omega$ corresponding to $a \in [0.2, 1.2]$. A Poincaré-section-based bifurcation diagram was created for each simulation by recording the variables v_{C1}, v_{C2}, and i_{L1} after the transient process and selecting v_{C2} and i_{L1} as the sectioning variables. In third-order systems such as the Vilnius oscillator, several transverse sectioning planes are possible, and different choices may highlight different features of the dynamics. Because the bifurcation diagrams in the original study plot v_{C1} as the observable, both v_{C2} and i_{L1} provide valid sectioning variables from which the corresponding points of v_{C1} can be extracted. Evaluating both options ensures methodological consistency and allows reconstruction of bifurcation structures that are directly comparable to those reported in earlier work. Representative results are shown in Figure 7.

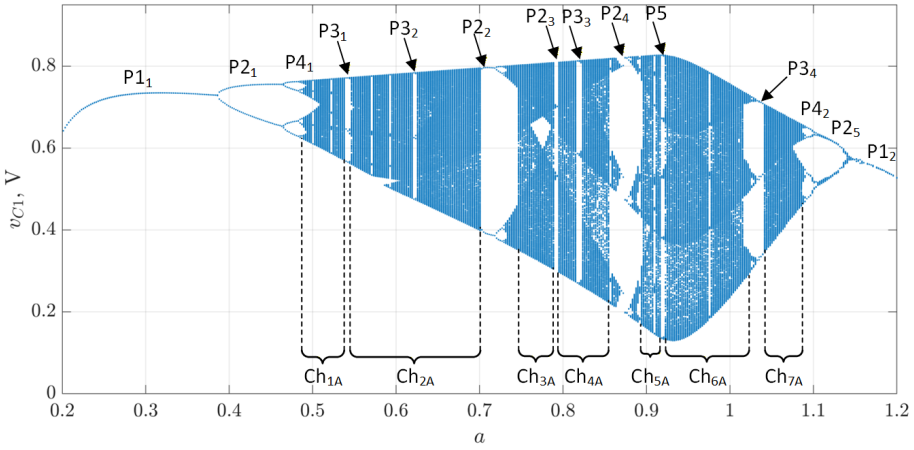

Figure 7. Bifurcation diagram of the Vilnius oscillator obtained from LTspice simulations, sweeping $a \in [0.2, 1.2]$.

As shown in the figure, varying the parameter a results in clear qualitative transitions in the system dynamics. For small values of a, the oscillator exhibits a stable periodic orbit. Increasing a leads to a period-doubling sequence, followed by the beginning of broadband chaos. The diagrams also reveal periodic windows embedded within the chaotic region and significant variation in attractor width as a increases. These features are consistent with the known behavior of the Vilnius oscillator and confirm that LTspice captures its characteristic nonlinear transitions.

Comparing Figures 6 and 7, we observe that both diagrams demonstrate qualitatively consistent nonlinear behavior. This confirms that the physical circuit preserves the main dynamical characteristics predicted by the mathematical model. In both cases, the system starts in a stable P1 regime at lower values of a, then enters a sequence of period-doubling bifurcations, followed by the development of broad chaotic regions. As in the numerical model, the LTspice oscillator exhibits multiple periodic windows embedded within the chaotic band. The positions of the main periodic windows are in very good correspondence between the two models, indicating that the control parameter a plays a similar dynamical role in both domains.

Although the LTspice and numerical bifurcation diagrams exhibit the same qualitative behavior, the LTspice diagram is systematically shifted toward higher values of the control parameter a. This is expected, as LTspice simulates the real circuit with finite-bandwidth operational amplifier dynamics, diode threshold effects, parasitic elements, and DC bias shifts, whereas the numerical model assumes ideal components and exact normalization. These nonidealities effectively reduce the actual dynamical gain, meaning that larger nominal values of a are required to reach the same bifurcation states. Thus, the shift reflects realistic circuit physics rather than a disagreement between the two models.

The results confirm that chaotic behavior in the Vilnius oscillator is not only a theoretical prediction but also a physically realizable property of the circuit. The LTspice simulations demonstrate that the oscillator maintains robust and sustained chaotic dynamics over a sufficiently broad parameter range. This validates that the chaotic domains observed in the numerical model persist in the practical implementation, confirming that the Vilnius oscillator is suitable for the proposed authentication methodology.

4.3. Discrete-Time Model

Figure 8 presents the bifurcation diagram of the discrete-time model from (6) Like. The overall structure of the diagram remains consistent with the previously discussed results: the system transitions from periodic behavior to period-doubling cascades, developing wide chaotic regions with embedded periodic windows. As expected, the discrete-time bifurcation profile is closer to the numerical model than to the LTspice simulation, since it is derived directly from the normalized mathematical formulation. Nevertheless, noticeable differences remain due to digitization effects inherent in the discrete implementation. These include finite fixed-point precision, limited dynamic range, quantization of state variables, and LUT-based approximation of the nonlinear exponential term. Together, these factors distort the parameter thresholds and modify the widths and positions of chaotic and periodic regions, leading to the observed deviations.

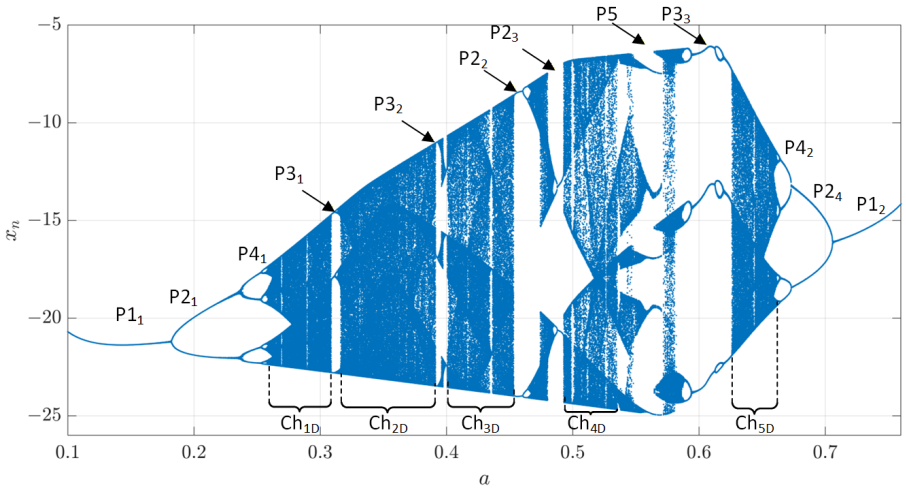

Figure 8. The bifurcation diagrams obtained from the discrete-time model.

As demonstrated in Section 4, the primary objective is to establish correspondence between the parameter ranges of a in which chaotic oscillations arise in both the analog and discrete-time models, ensuring the feasibility of the proposed authentication methodology. It has been found that the required horizontal alignment and extension of the chaotic regions in the discrete model can be achieved by adjusting only two parameters: the supply-related term V_1 and the effective dynamic scaling factor ϵ. By carefully tuning these values, it becomes possible to shift the onset of chaos and reshape the bifurcation structure so that it more closely matches the LTspice implementation. The resulting bifurcation

diagram, obtained for $V_1 = 2$ and $\epsilon = 0.125$, is presented in Figure 9, demonstrating a significantly improved correspondence between the analog and digital domains. This allows further selection of the regions of a, where the proposed methodology could be efficiently applied.

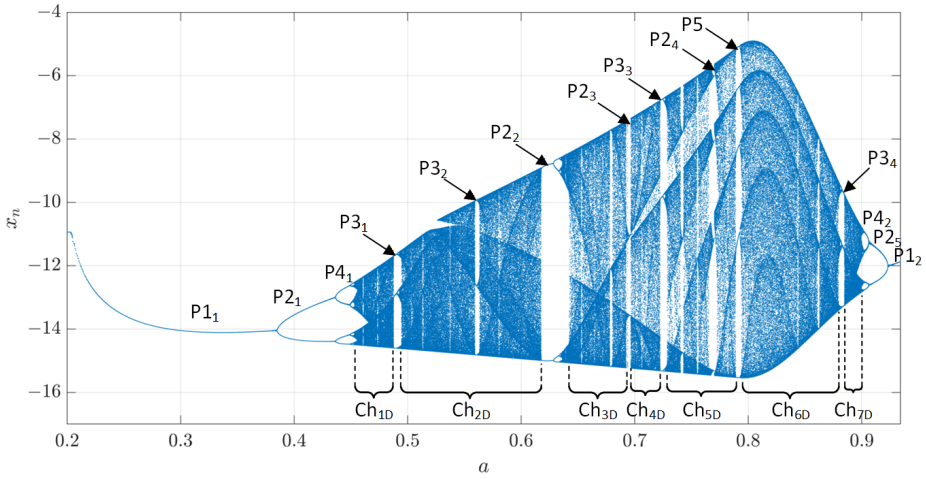

Figure 9. The bifurcation diagrams obtained from the adjusted discrete-time model $V_b = 2$, $\epsilon = 0.125$.

5. Vilnius Chaotic Oscillator Parameter Estimator

The current section presents the digital design of the parameter estimator of the Vilnius chaotic oscillator, followed by a performance evaluation of the estimator. The first step of designing the parameter estimator is to select the parameter of the chaotic oscillator that will be estimated based on the difference equations. By observing the system (6), the most convenient parameter for estimation is a from the second term of the difference equations:

$$y[n+1] = y[n] + (a \cdot y[n] - x[n] - z[n]) \cdot \Delta\theta \tag{7}$$

From this equation, the parameter a can be expressed as:

$$a_{estimated}[n] = \frac{\frac{y[n+1]-y[n]}{\Delta\theta} + x[n] + z[n]}{y[n]} \tag{8}$$

The convenience is that the equation contains only one parameter and that the signal relations are linear, unlike other terms of the system (6). Relating to the analog circuit, the parameter a is defined as:

$$a = (k-1)\frac{R_1}{\rho}, \qquad \rho = \sqrt{\frac{L_1}{C_1}}, \tag{9}$$

where k is the closed-loop gain of the operational amplifier, and R_1 is the series resistor in the resonant loop. The variable ρ represents the characteristic impedance of the L_1C_1 resonant circuit.

The parameter a directly influences the effective damping of the resonant subsystem and therefore governs the qualitative behavior of the oscillator. In the circuit, this parameter can be adjusted either via the gain k or the resistor R_1. As demonstrated in earlier studies [41], varying a yields transitions between periodic oscillations, period-doubling cascades, and fully developed chaos. In Section 4, bifurcation diagrams plotted as a function of a are presented to enable direct comparison with the original experimental and numerical results. The current section further focuses on the digital implementation of the a parameter estimator based on (8).

5.1. Digital Implementation of the Parameter Estimator

The digital design of the a parameter estimator is divided into two components: first, we acquire the numerator from (8):

$$s[n] = \frac{y[n+1] - y[n]}{\Delta\theta} + x[n] + y[n], \tag{10}$$

second, we acquire the estimated value $a[n]$ from the expression:

$$a_{estimated}[n] = \frac{s[n]}{y[n]}. \tag{11}$$

The digital implementation of the first component is presented in Figure 10. The digital design is a pipeline set to work in Fixed-point arithmetic. The $s[n]$ is acquired by inputting the $x[n]$, $z[n]$, $\frac{y[n]}{\Delta\theta}$ and performing the required operations as described in (10). Because the time step is a multiple of two, the $\frac{y[n]}{\Delta\theta}$ division can be done with bit shifting. The acquisition of the $s[n]$ takes 4 registers, resulting in a 4 clock cycle delay. As shown in (11), the second component requires $s[n]$ and $y[n]$ in the same phase, so a digital delay line for delaying the $y[n]$ for 4 clock cycles is added, giving the $y_{delayed}[n]$ output signal.

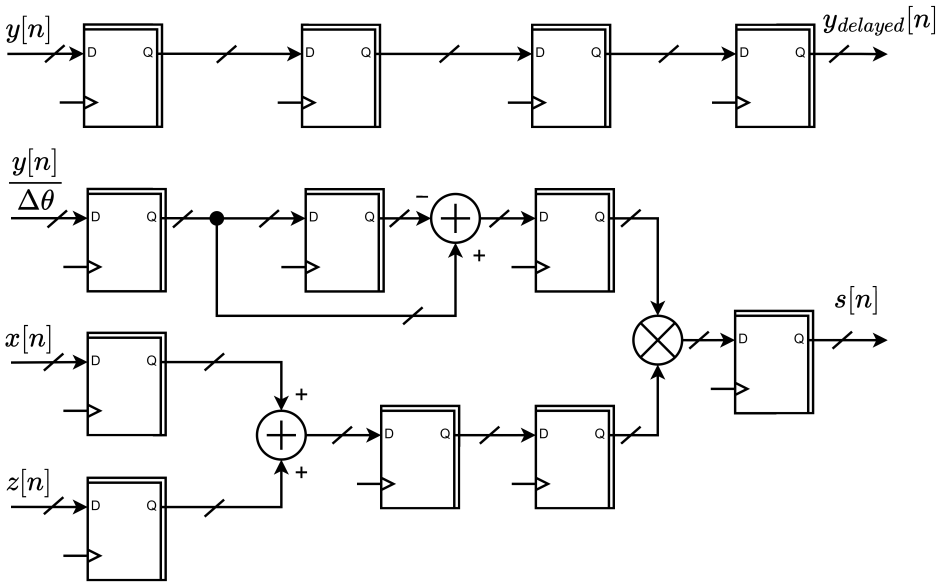

Figure 10. Pipeline design for acquiring the numerator par of the a parameter estimator.

The digital implementation for the second component is not as straightforward because division of the two signals in the digital system cannot be done in a single clock cycle and requires an algorithm. The solution to acquire $a_{estimated}[n]$ is through the adaptive filter least mean squares (LMS) (Wiener filter with minimum mean squared error (MMSE)). Equation (11) with the $y_{delayed}[n]$ can be expressed as:

$$a_{estimated}[n] \cdot y_{delayed}[n] = s[n] \tag{12}$$

Defining the cost function as a squared error, the following is obtained:

$$\mathcal{J}[n] = \mathbb{E}\left[\left(s[n] - a_{estimated}[n] y_{delayed}[n]\right)^2\right] \tag{13}$$

Next, the equation is differentiated with respect to $a_{estimated}[n]$:

$$\frac{d\mathcal{J}[n]}{da_{estimated}[n]} = -2 \cdot y_{delayed}[n] \cdot \Big(s[n] - a_{estimated}[n] \cdot y_{delayed}[n]\Big) \tag{14}$$

Thus, $a_{estimated}[n]$ can be assessed using the stochastic gradient as:

$$a_{estimated}[n+1] = a_{estimated}[n] - \mu \frac{d\mathcal{J}[n]}{da_{estimated}[n]} \tag{15}$$

The final equation for the digital implementation is acquired by applying (14) in (15):

$$a_{estimated}[n+1] = a_{estimated}[n] + 2\mu \cdot y_{delayed}[n] \cdot \Big(s[n] - a_{estimated}[n] \cdot y_{delayed}[n]\Big) \tag{16}$$

The constant μ is the step size (also known as the convergence speed). This constant depicts how fast the algorithm converges to the Wiener MMSE solution. This constant needs to be selected accordingly, as setting μ too low results in slow convergence, while setting it too high produces output oscillations. A sufficient condition for mean-square stability is:

$$0 < \mu < \frac{2}{\mathbb{E}[y[n]^2]} \tag{17}$$

Figure 11 presents the digital implementation of the LMS adaptive filter (16). The first two registers are the output registers of the numerator calculation pipeline, so they output the $s[n]$ and $y_{delayed}[n]$ for the LMS adaptive filter. The filter is a pipeline that performs the mathematical operations defined in (16) with additional delays to ensure that the operations are performed on the correct signal samples. A critical design aspect is the aforementioned convergence speed μ and multiplication with 2μ. In the system, 2μ is set to 1×10^{-5}. The system is implemented in fixed-point arithmetic, so the 2μ constant is floored, making it a multiple of two and allowing multiplication to be replaced with bit-shifting. Because the 2μ is a very small constant, the output $a_{estimated}[n]$ requires 20 fractional bits. The expected integer range is from $0 < a_{estimated}[n] < 2$, so devoting 2 integer bits would be enough, yet the system has 4 integer bits for some headroom.

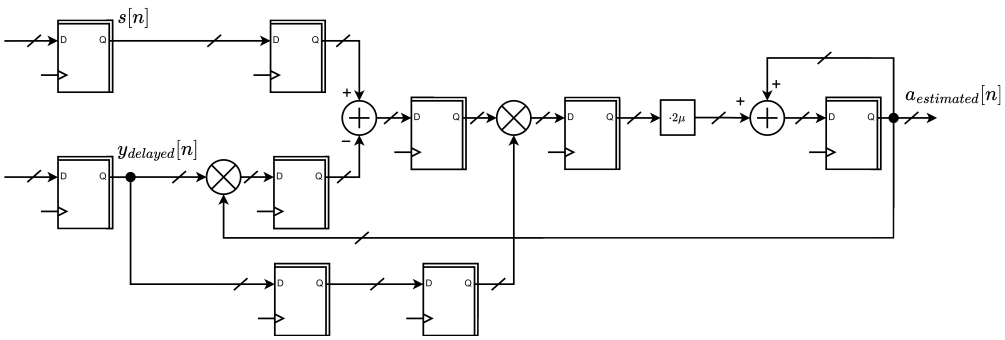

Figure 11. The digital implementation of the LMS adaptive filter for parameter a estimation.

The FPGA resource utilization of the presented estimator's design together with the resource utilization of the Vilnius chaos oscillator are presented in Table 1. The design was compiled for a Altera (Intel) Cyclone 5CSXFC6D6F31C6 chip. To provide vendor-independent comparison, Intel adaptive logic modules (ALMs) are converted to equivalent LUTs assuming 1 ALM $\approx$ 2 four-input LUTs, following the Cyclone V ALM architecture.

Table 1. FPGA resource utilization of the estimator together with Vilnius chaos oscillator.

Resource	Utilization	Available	Utilization, %
LUT	614	83,820	0.7
BRAM	90,122	5,662,720	1.6
FF	550	166,000	0.33
DSP	6	112	5.36

5.2. Performance Evaluation

This subsection is devoted to studying the performance of the designed parameter estimator for the Vilnius chaotic oscillator. The first test of the estimator is demonstrated in Figure 12. The block diagram in Figure 12a shows that the signals $x[n]$, $y[n]$, and $z[n]$ of the discrete oscillator are passed to the estimator. The parameter a of the oscillator is set to 0.47 and is kept constant. The output of the estimator is presented in Figure 12b. The initial value of $a_{estimated}[n]$ was set to 0, and it is seen that the $a_{estimated}[n]$ is rapidly approaching the stable value with insignificant ripples, reaching it after 4×10^4 clock cycles. The diagram also displays the true value of the a parameter, overlaying it as the level with a dashed line. The estimator's output $a_{estimated}[n]$ level equals 0.485, which does not match exactly the transmitter's a parameter. This is because the LMS does not converge to the true physical parameter but to the best linear MMSE estimator of $s[n]$ from $y_{delayed}[n]$.

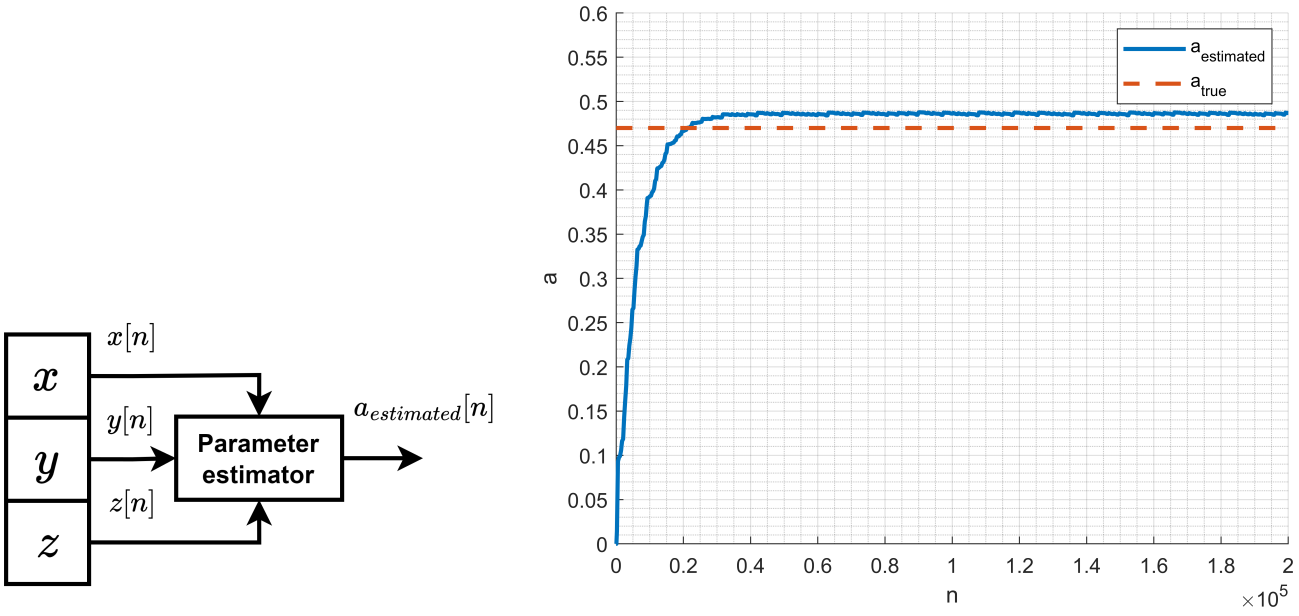

Figure 12. Experimental setup for verifying the a parameter estimator (**a**) and the output of the a parameter estimator (**b**).

The second test evaluates the estimator's performance when it is tasked with estimating the parameter a of the transmitter with the receiver's oscillator synchronized to the transmitter's oscillator. The block diagram of the verification setup is presented in Figure 13a. The transmitter sends the $x_m[n]$ and $y_m[n]$ signals to the receiver, where $y_m[n]$ is used to achieve chaotic synchronization using the Pecora–Carroll approach. The synchronization signal is applied after 5×10^4 clock cycles. The received $x_m[n]$ and $y_m[n]$ as well as the signal $z_s[n]$ from the receiver's chaos oscillator are passed to estimate the transmitter's a parameter. This setup exactly reflects the proposed authentication scheme presented in

Figure 3. In the receiver's oscillator, a is fixed at 0.47, while the transmitter's oscillator is switched to 0.6, 0.5, and 0.3, after every 2×10^5 clock cycles following synchronization.

Figure 13b shows the $a_{estimated}[n]$ output signal of the estimator. In the first 5×10^4 clock cycles, the receiver's and transmitter's chaos oscillators are asynchronous, so $a_{estimated}[n]$ does not output a stable level, which is expected. After the synchronization signal is applied, the $a_{estimated}[n]$ reaches a stable level equal to 0.61, then after 2×10^5 clock cycles, $a_{estimated}[n]$ level switches to 0.51, and after another 2×10^5 clock cycles, $a_{estimated}[n]$ level switches to 0.31. When synchronized, the estimator tracks the a parameter of the transmitter's chaos oscillator, which is also displayed on the graph. The reached $a_{estimated}[n]$ levels exhibit minor ripples and approximately 4×10^4 cycles of transition time, like in Figure 12b.

In the current configuration the 4×10^4 cycles of convergence time at 50 MHz FPGA system clock yields an estimated time of 800 µs. Chaos-based data systems can operate at 60 kb/s, comparable to low-bitrate long-range IoT that operates in 0.3–300 kb/s range, which the developed chaos-based data transfer paired with PLA targets. The estimator, in its current form, has very little overhead given the low bitrate and can be further adjusted and used for the PLA.

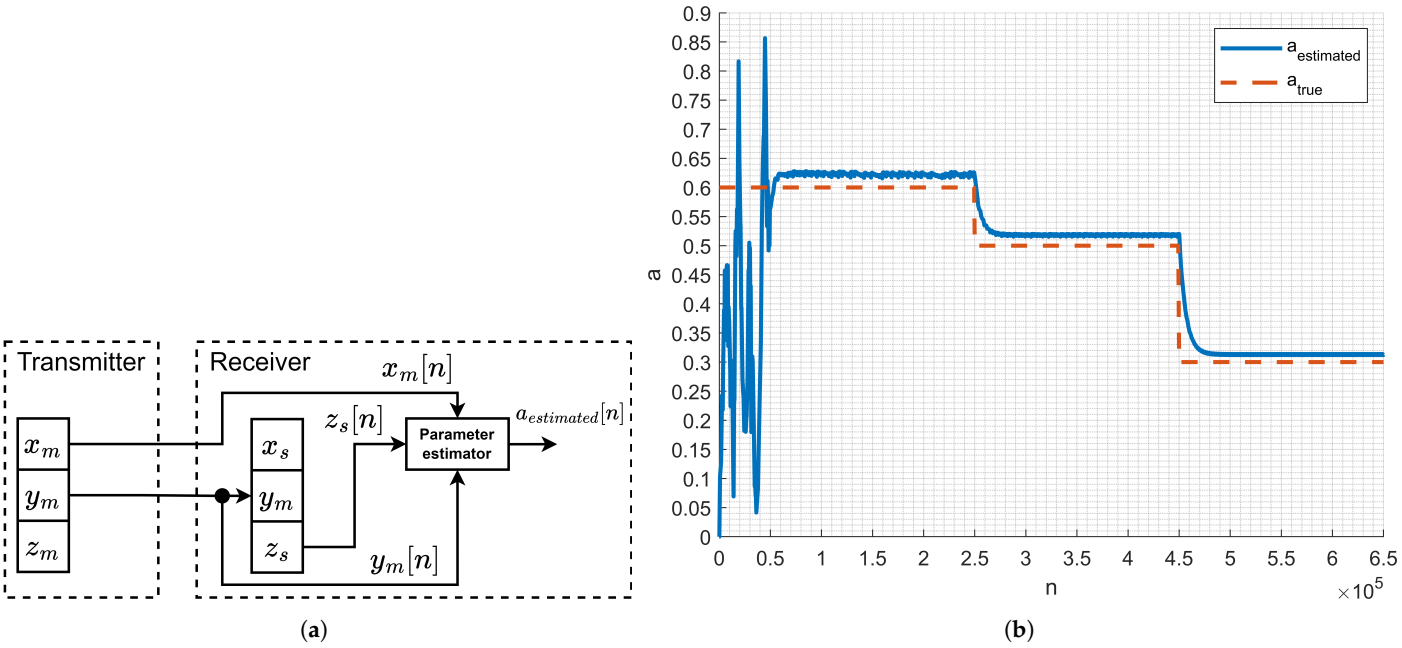

Figure 13. Experimental setup for verifying the a parameter estimator in synchronous mode (**a**) and the output of the a parameter estimator (**b**).

Overall, although the estimator does not produce the exact values of the transmitter's a, it outputs levels that are clearly distinguishable and close to the original values. Furthermore, the difference between actual and estimated a appears to be constant. Another observation made in the results in Figure 13b is that the ripples on the estimated level in the case of transmitter's a equal 0.6 are more than in the case of the other a values. This raises the question of what distinguishable a levels can be reliably used for authentication.

The next study examines how the estimated average value and minimum–maximum range of $a_{estimated}$ vary based on the transmitter's a. For the study, the transmitter's a is varied from 0.2 to 0.7 in increments of 0.01. The two cases of receiver's a are taken—in the first case receiver's a equals 0.47, like in Figure 13; in the second case receiver's a equals 0.6.

The results of the study are presented in Figure 14. The results in the case of receiver's a equals 0.47 in Figure 14 demonstrate a very small minimum–maximum range when transmitter's a increases from 0.2 to 0.52, making them well distinguishable. The $a_{estimated}$

minimum–maximum range then increases, reaching its peak at 0.61 and then decreases. Within this a value range, the minimum–maximum ranges of the neighboring $a_{estimated}$ values overlap, meaning that they are indistinguishable when used for authentication. Every third a value must be used instead.

Alternatively, if the receiver's a is set to 0.6, the $a_{estimated}$ minimum–maximum ranges are different across the transmitter's a value range. For the transmitter's a range 0.2 to 0.52, the minimum–maximum ranges increase, resulting in a slight overlap, so every second $a_{estimated}$ is distinguishable. The range above 0.52 has decreased minimum–maximum ranges, also making every second $a_{estimated}$ distinguishable instead of every third, as in the case when the receiver's a was set to 0.47.

The results present several key points. First, it is possible to select a set of distinguishable parameter a values to use in the authentication. Second, the minimum–maximum range of the estimator's output depends on the receiver's parameter a, making this a crucial and controllable parameter when selecting the a values used for authentication. Finally, the difference between the estimated and true values of a is the same across the entire parameter range, as seen by overlaying the true values with a dashed line. The maximum relative error of the average a in Figure 14 does not exceed 6 % if the linear shift is not compensated. By compensating the estimated average 0.017 shift, the relative error then does not exceed 1.01 %. This highlights the necessity for calibration.

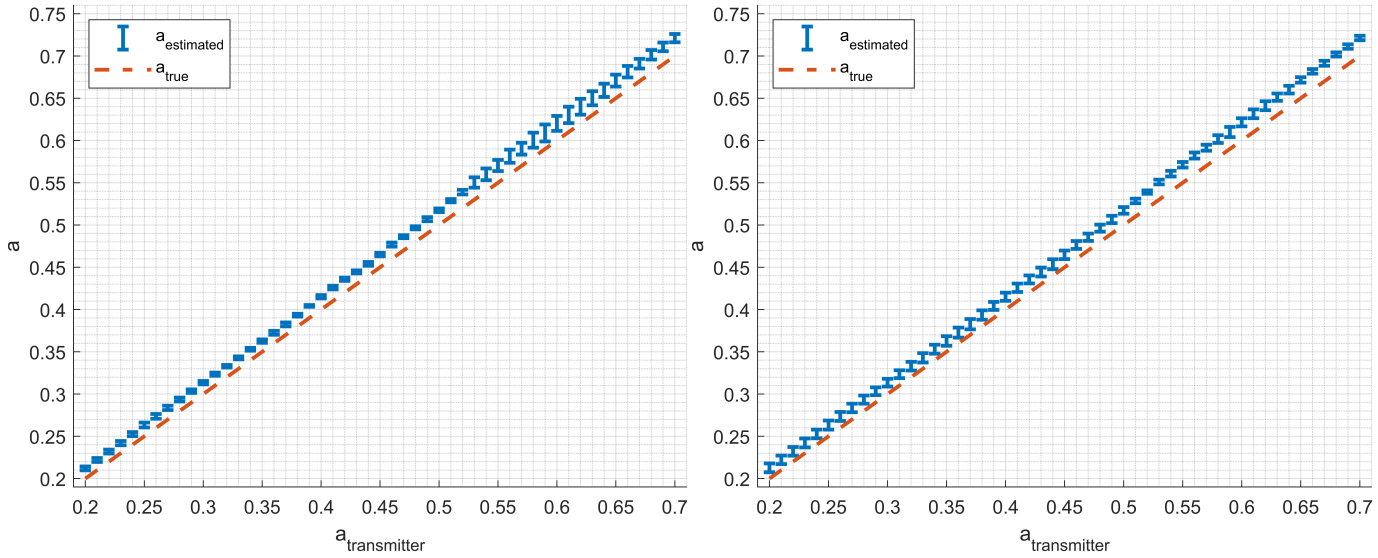

Figure 14. The output of the a parameter estimator average and minimum–maximum range for different transmitter a values in the case of receiver's $a = 0.47$ (**a**) and in the case of receiver's $a = 0.6$ (**b**).

The next study aims to investigate how additive noise affects the performance of the estimator. The setup for this evaluation is demonstrated in Figure 15a. The notable modification is the inclusion of band-limited additive white Gaussian noise (B.L.AWGN), which is added to the transmitter oscillator's signals $x_m[n]$ and $y_m[n]$. The added noise signals are in-band with the related chaotic signals, representing the worst-case scenario, as the out-of-band noise can be filtered, thus improving the signal-to-noise ratio (SNR). Since the parameter estimation system is designed to operate with synchronous receiver's and transmitter's chaotic oscillators, this noise will impact both the synchronization of the oscillators and the estimation quality. The transmitter's and receiver's a are both set to 0.47, and the noise signal's SNR is varied from 18 to 50 dB.

The results of this study are presented in Figure 15b. The first set of results was obtained for the convergence speed 2μ set to 1×10^{-5}, which is the same as in previous studies. The results present the $a_{estimated}$ average value and minimum–maximum range across the SNR range, demonstrating that the minimum–maximum range noticeably increases as the SNR decreases. This behavior is expected and indicates that the noise will affect the ability to distinguish the levels of the parameter. Improving the noise performance of the estimator is possible by decreasing the convergence speed, i.e, increasing the window of the adaptive filter. The second set of results was acquired for the convergence speed 2μ set to 3×10^{-6} and demonstrates a noticeably lower $a_{estimated}$ minimum–maximum range for the same SNR levels.

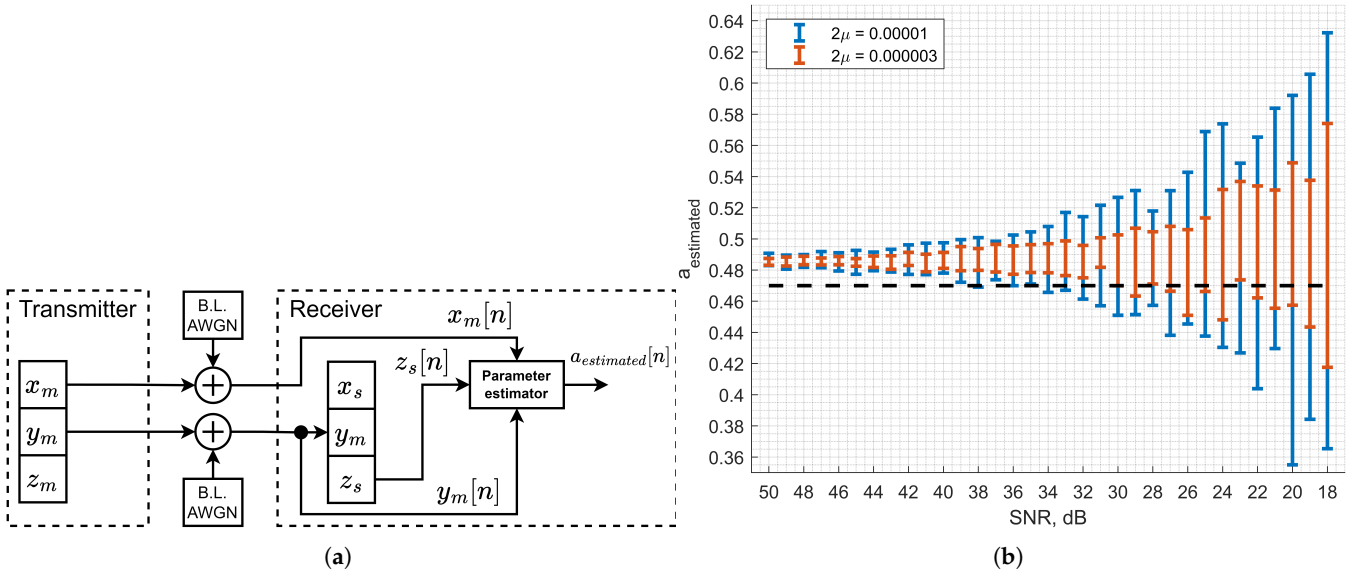

Figure 15. Experimental setup for verifying the a parameter estimator in B.L.AWGN channel (**a**) and the output of the a parameter estimator (**b**).

6. Discussion

The present work introduced a novel scheme based on chaotic oscillator parameter estimation for PLA. The core idea is that one of the transmitter oscillator parameters can be estimated at the receiver by using the received chaotic signals together with a locally synchronized chaotic oscillator. The possibility to set and estimate the parameter of the chaos oscillator provides a powerful authentication mechanism that can be integrated into chaos-based data transfer systems. This PLA scheme is designed to supplement the proposed chaos-based WSN, where sensor nodes utilize analog chaotic oscillators, and the GW hosts discrete models of the oscillators.

The first part of this study performed a bifurcation analysis of the selected parameter to identify the regions that produce chaotic behavior, as maintaining chaos is essential when defining the parameter range used for authentication. Another goal of this part is to adjust the discrete-time model of the oscillator to establish correspondence between the parameter ranges in which chaotic oscillations arise in both the analog and discrete-time models, thus ensuring the feasibility of the proposed authentication methodology. The second part of the work involved the digital implementation of the Vilnius chaotic oscillator parameter estimator and the identification of key metrics of its operation. The designed system proved to work as intended – the difference between the true and estimated parameters is small and is constant over the considered parameter range, meaning that it can be easily compensated.

The performance evaluation of the designed estimator highlighted the aspects that must be carefully adjusted for further successful deployment. The first metric is the

time required to estimate the parameter, which is governed by the convergence speed. The time of estimation can be reduced, resulting in increased output fluctuations, which directly affect the possibility of distinguishing the discrete set of parameter ranges used in the authentication scheme – the time vs. precision tradeoff. The noise immunity study highlighted that the output fluctuations increase with the increase in noise level, so the convergence speed must be adapted for the channel state as well. For the existing chaos-based data transfer system, the channel state can be estimated using the existing solution, as information signal detection in the proposed chaos-based data transfer schemes is performed with Pearson's correlation coefficient, which evaluates the similarity between the local and received chaotic signals. This metric was also used to assess the quality of synchronization in noisy channels, and thus can supplement the parameter estimation system to adjust for the channel state. The second metric is the ability to distinguish the discrete set of parameter ranges based on the native parameter of the receiver's oscillator. The work demonstrated that the native parameter of the receiver's oscillator directly affects which parameter values of the transmitter can be distinguished. This makes the system highly configurable, as it is possible to set the native parameter of the receiver's oscillator, adjust the convergence speed for satisfactory parameter estimation precision, and thus determine the parameter range of the transmitter that can be used for authentication. On top of that, several configurations are possible, resulting in a highly parameterized system that mitigates unauthorized data transmission with a similar architecture.

This leads to future steps to implementing the full authentication system based on the designed estimator. The first step is to perform a hardware implementation of the system, which will include the analog oscillator, the discrete oscillator paired with the designed estimator on an FPGA. This step will highlight how to fine-tune the estimator for optimal use considering the hardware realities. Because the developed chaos-based communication system is developed for low-bitrate IoT and has data rate about 60 kb/s, the current configuration of the estimator introduces a small latency, estimated to be 800 µs for 50 MHz system clock frequency. The latency can be increased, providing a more stable estimation. The presented results demonstrate an effective key space of approximately 5 bits at the hardware-metric level, which is insufficient for standalone authentication. However, this key space can be significantly increased by extending the estimation window and through aggregation across multiple authentication instances. Once the hardware layer is finalized, future work will focus on integrating this metric into a higher-layer authentication protocol, including mechanisms for reference enrollment, key derivation, and secure challenge–response handling.

While the present authentication framework is demonstrated using single-scroll chaotic oscillators, an interesting direction for future research is its extension to more complex chaotic systems, such as multiscroll attractors. Multiscroll dynamics are known to exhibit increased phase-space complexity and a larger number of coexisting scrolls, which could further enhance the uniqueness and entropy of hardware fingerprints. Incorporating such attractors into the proposed synchronization-based authentication scheme may therefore improve resistance to cloning and modeling attacks

Author Contributions: Conceptualization, D.V.; data curation, J.S., D.V. and D.K.; formal analysis, S.T., J.S., D.V. and D.K.; funding acquisition, D.P.; investigation, R.B., D.C. and S.B.; methodology, R.B., D.C. and J.S.; project administration, D.P.; resources, J.S.; software, R.B., S.T., S.B. and D.K.; supervision, D.P.; validation, D.C., S.B. and D.V.; visualization, S.T., S.B., D.V. and D.K.; writing—original draft, R.B., D.C., S.T. and D.P.; writing—review and editing, J.S., D.K. and D.P. All authors have read and agreed to the published version of the manuscript.

Funding: Supported by research and development grant No. RTU-PA-2024/1-0064 under the EU RRF project No. 5.2.1.1.i.0/2/24/I/CFLA/003.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data are contained within the article.

Acknowledgments: This research was performed at Riga Technical University, Space Electronics and Signal Processing Laboratory—SpacESPro Lab.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

AKA	authentication and key agreement
ALM	adaptive logic module
B.L.AWGN	band-limited additive white Gaussian noise
BRAM	Block RAM
CFR	channel frequency response
CIR	channel impulse response
CSI	channel state information
CSK	chaos shift keying
DSP	digital signal processing
ECC	Elliptic Curve Cryptography
FF	flip-flop
FPGA	field-programmable gate array
GW	Gateway
IoT	Internet of Things
LMS	least mean squares
LUT	lookupTable
MMSE	minimum mean squared error
PCB	printed circuit board
PLA	Physical-Layer Authentication
PSK	phase shift keying
PUF	Physical Unclonable Function
QCSK	quadrature chaos shift keying
RF	radio frequency
ROM	read-only memory
RSS	received signal strength
SN	Sensor Node
SNR	signal-to-noise ratio
WSN	Wireless Sensor Network

Nomenclature

$\frac{\mathrm{d}x}{\mathrm{d}t}$	the derivative of x with respect to t
ϵ	normalized parameter of the differential equation
$\mathbb{E}$	error
$\mathcal{J}$	cost function
μ	step size
ρ	oscillator's contour characteristic impedance
τ	oscillator's time constant
θ	normalized time
a	normalized parameter of the differential equation
$a_{estimated}$	estimated parameter a value
a_{true}	true parameter a value
b	normalized parameter of the differential equation
C	capacitor

c	normalized parameter of the differential equation
$ChxN$	chaotic operating region
e	electron charge
i_0	current of the resistor R_0
i_D	diode current
i_L	inductor i_{L_1} current
i_S	saturation current of the diode
k	gain of the operational amplifier
k_B	Bolzman's constant
L	inductor
n	sample
P	period regime of the oscillator
R	resistor
s_n	acquired signal of the pipeline
t	time
v_{C1}	capacitor C_1 voltage
v_{C2}	capacitor C_2 voltage
v_D	voltage across the diode
v_{R1}	resistance R_1 voltage
v_{RL}	resistance R_L voltage
V_T	the thermal voltage of the diode
x	normalized voltage v_{C_1}
y	normalized current i_{L_1}
$y_{delayed}$	delayed y signal
z	normalized voltage v_{C_2}

References

1. Ullah, S.; Radzi, R.Z.; Yazdani, T.M.; Alshehri, A.; Khan, I. Types of Lightweight Cryptographies in Current Developments for Resource Constrained Machine Type Communication Devices: Challenges and Opportunities. *IEEE Access* **2022**, *10*, 35589–35604. [CrossRef]
2. Silva, C.; Tenório, N.; Bernardino, J. Lightweight Encryption Algorithms for IoT. *Computers* **2025**, *14*, 505. [CrossRef]
3. Sarker, K.U. A systematic review on lightweight security algorithms for a sustainable IoT infrastructure. *Discov. Internet Things* **2025**, *5*, 47. [CrossRef]
4. Migwi, D.; Romaniuk, R.S. Lightweight and Scalable Security for Wireless IoT Systems: Challenges and Research Directions. *Int. J. Electron. Telecommun.* **2025**, *71*, 1–8. [CrossRef]
5. Demirkol, A.S.; Sahin, M.E.; Karakaya, B.; Ulutas, H.; Ascoli, A.; Tetzlaff, R. Real time hybrid medical image encryption algorithm combining memristor-based chaos with DNA coding. *Chaos Solitons Fractals* **2024**, *183*, 114923. [CrossRef]
6. Petrzela, J. Chaos in Analog Electronic Circuits: Comprehensive Review, Solved Problems, Open Topics and Small Example. *Mathematics* **2022**, *10*, 4108. [CrossRef]
7. Hu, X.K.; Yang, J.; Song, Z.; Zhou, P. A discrete Lorenz-like map and its pseudo-Hamiltonian energy. *Phys. Scr.* **2025**, *100*, 075232. [CrossRef]
8. Wang, L.; Wang, C.; Zhang, H.; Ma, P.; Zhang, S. Estimation-Correction Modeling and Chaos Control of Fractional-Order Memristor Load Buck-Boost Converter. *Complex Syst. Model. Simul.* **2024**, *4*, 67–81. [CrossRef]
9. Benadero, L.; Aroudi, A.E.; Martínez-Salamero, L.; Tse, C.K. Period Doubling Route to Chaos in Open Loop Boost Converters under Constant Power Loading and Discontinuous Conduction Mode Conditions. In *Proceedings of the 2020 IEEE International Symposium on Circuits and Systems (ISCAS), Seville, Spain, 12–14 October 2020*; IEEE: Piscataway, NJ, USA, 2020; pp. 1–5. [CrossRef]
10. Cristiano, R.; Henao, M.M.; Pagano, D.J.; Ponce, E. Chaos Through Sliding Bifurcations in a DC–DC Boost Power Converter. *Int. J. Bifurc. Chaos* **2024**, *34*, 2430033. [CrossRef]
11. Piqueira, J.R.C. Hopf bifurcation and chaos in a third-order phase-locked loop. *Commun. Nonlinear Sci. Numer. Simul.* **2017**, *42*, 178–186. [CrossRef]
12. Duan, Z.; Chen, J.; He, S.; Yu, X.; Wang, Q.; Zhang, X.; Xiong, P. A Fully Integrated Memristive Chaotic Circuit Based on Memristor Emulator with Voltage-Controlled Oscillator. *Micromachines* **2025**, *16*, 246. [CrossRef]
13. Yu, F.; Kong, X.; Yao, W.; Zhang, J.; Cai, S.; Lin, H.; Jin, J. Dynamics analysis, synchronization and FPGA implementation of multiscroll Hopfield neural networks with non-polynomial memristor. *Chaos Solitons Fractals* **2024**, *179*, 114440. [CrossRef]

14. Chen, W.; Mao, X.; Wang, J.; Zhang, R.; Wang, L.; Jia, Z.; Li, P.; Wang, A.; Wang, Y. Optical Chaos Generation and Applications. *Adv. Photonics Res.* **2025**, *6*, 2500055. [CrossRef]
15. Grassi, G. Chaos in the Real World: Recent Applications to Communications, Computing, Distributed Sensing, Robotic Motion, Bio-Impedance Modelling and Encryption Systems. *Symmetry* **2021**, *13*, 2151. [CrossRef]
16. Gușiță, B.; Anton, A.A.; Stângaciu, C.S.; Stănescu, D.; Găină, L.I.; Micea, M.V. Securing IoT edge: A survey on lightweight cryptography, anonymous routing and communication protocol enhancements. *Int. J. Inf. Secur.* **2025**, *24*, 149. [CrossRef]
17. Bonny, T.; Al Nassan, W. NeuroChaosCrypt: Revolutionizing Chaotic-Based Cryptosystem With Artificial Neural Networks—A Comparison With Traditional Cryptosystems. *IEEE Access* **2024**, *12*, 62030–62046. [CrossRef]
18. Zhang, C.; Zhang, S.; Liang, K.; Chen, Z. Double Image Encryption Algorithm Based on Parallel Compressed Sensing and Chaotic System. *IEEE Access* **2024**, *12*, 54745–54757. [CrossRef]
19. Thukral, M.K. SCLLCM: A Robust One Dimesional Chaotic Map for Image Encryption Application. In *Proceedings of the 2024 Asia Pacific Conference on Innovation in Technology (APCIT), MYSORE, India, 26–27 July 2024*; IEEE: Piscataway, NJ, USA, 2024; pp. 1–5. [CrossRef]
20. Moysis, L.; Kafetzis, I.; Volos, C.; Tutueva, A.V.; Butusov, D. Application of a Hyperbolic Tangent Chaotic Map to Random Bit Generation and Image Encryption. In *Proceedings of the 2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus), St. Petersburg, Moscow, Russia, 26–29 January 2021*; IEEE: Piscataway, NJ, USA, 2021; pp. 559–565. [CrossRef]
21. Abdelli, A.; El Hadj Youssef, W.; Khriji, L.; Machhout, M. Enhanced lightweight encryption algorithm based on chaotic systems. *Phys. Scr.* **2024**, *99*, 106006. [CrossRef]
22. Aljaedi, A.; Alharbi, A.R.; Aljuhni, A.; Alghuson, M.K.; Alassmi, S.; Shafique, A. A lightweight encryption algorithm for resource-constrained IoT devices using quantum and chaotic techniques with metaheuristic optimization. *Sci. Rep.* **2025**, *15*, 14050. [CrossRef] [PubMed]
23. Feng, W.; Tang, Z.; Zhao, X.; Qin, Z.; Chen, Y.; Cai, B.; Zhu, Z.; Wen, H.; Ye, C. State-Dependent Variable Fractional-Order Hyperchaotic Dynamics in a Coupled Quadratic Map: A Novel System for High-Performance Image Protection. *Fractal Fract.* **2025**, *9*, 792. [CrossRef]
24. Al-Meer, A.; Al-Kuwari, S. Physical Unclonable Functions (PUF) for IoT Devices. *ACM Comput. Surv.* **2023**, *55*, 314:1–314:31. [CrossRef]
25. Peng, L.; Hu, A.; Zhang, J.; Jiang, Y.; Yu, J.; Yan, Y. Design of a Hybrid RF Fingerprint Extraction and Device Classification Scheme. *IEEE Internet Things J.* **2019**, *6*, 349–360. [CrossRef]
26. Alhoraibi, L.; Alghazzawi, D.; Alhebshi, R.; Rabie, O.B.J. Physical Layer Authentication in Wireless Networks-Based Machine Learning Approaches. *Sensors* **2023**, *23*, 1814. [CrossRef] [PubMed]
27. Osorio, D.P.M.; Olivo, E.E.B.; Alves, H.; Latva-Aho, M. Safeguarding MTC at the Physical Layer: Potentials and Challenges. *IEEE Access* **2020**, *8*, 101437–101447. [CrossRef]
28. Nofal, M.; Elmanfaloty, R.A. Chaos-Based Dynamic Authentication for Secure Telehealth in Smart Cities. *Modelling* **2025**, *6*, 25. [CrossRef]
29. Kushwaha, P.; Sonkar, H.; Altaf, F.; Maity, S. A Brief Survey of Challenge–Response Authentication Mechanisms. In *Proceedings of the ICT Analysis and Applications*; Fong, S., Dey, N., Joshi, A., Eds.; Springer: Singapore, 2021; pp. 573–581. [CrossRef]
30. Wang, L.; Han, C. Multi-factor authentication and key agreement scheme based on PUF and Chebyshev chaotic map for wireless sensor networks. *Sci. Rep.* **2025**, *16*, 3311. [CrossRef]
31. Xie, Q.; Yao, Y. PUF and Chaotic Map-Based Authentication Protocol for Underwater Acoustic Networks. *Appl. Sci.* **2024**, *14*, 5400. [CrossRef]
32. Zahednejad, B.; Gao, C.Z. Mitigating server Key Compromise Impersonation: A secure and efficient authentication and key agreement protocol for IoT devices using chaotic maps. *J. Inf. Secur. Appl.* **2025**, *92*, 104083. [CrossRef]
33. Cirjulina, D.; Babajans, R.; Capligins, F.; Kolosovs, D.; Litvinenko, A. Experimental Study on Colpitts Chaotic Oscillator-Based Communication System Application for the Internet of Things. *Appl. Sci.* **2024**, *14*, 1180. [CrossRef]
34. Babajans, R.; Kolosovs, D.; Cirjulina, D.; Tjukovs, S.; Bogdanovs, N.; Pikulins, D. Noise Performance Study of FPGA-based and Analog Chaos Oscillator Synchronization. In *Proceedings of the 2025 IEEE 12th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE), Vilnius, Lithuania, 15–17 May 2025*; IEEE: Piscataway, NJ, USA, 2025; pp. 1–5. [CrossRef]
35. Babajans, R.; Cirjulina, D.; Capligins, F.; Kolosovs, D.; Litvinenko, A. Synchronization of Analog-Discrete Chaotic Systems for Wireless Sensor Network Design. *Appl. Sci.* **2024**, *14*, 915. [CrossRef]
36. Babajans, R.; Cirjulina, D.; Kolosovs, D. Field-Programmable Gate Array-Based Chaos Oscillator Implementation for Analog–Discrete and Discrete–Analog Chaotic Synchronization Applications. *Entropy* **2025**, *27*, 334. [CrossRef] [PubMed]
37. Cirjulina, D.; Babajans, R.; Kolosovs, D. Design Particularities of Quadrature Chaos Shift Keying Communication System with Enhanced Noise Immunity for IoT Applications. *Entropy* **2025**, *27*, 296. [CrossRef] [PubMed]

38. Babajans, R.; Cirjulina, D.; Grizans, J.; Aboltins, A.; Pikulins, D.; Zeltins, M.; Litvinenko, A. Impact of the Chaotic Synchronization's Stability on the Performance of QCPSK Communication System. *Electronics* **2021**, *10*, 640. [CrossRef]
39. Pecora, L.M.; Carroll, T.L. Synchronization in chaotic systems. *Phys. Rev. Lett.* **1990**, *64*, 821–824. [CrossRef] [PubMed]
40. Karimov, A.; Tutueva, A.; Karimov, T.; Druzhina, O.; Butusov, D. Adaptive Generalized Synchronization between Circuit and Computer Implementations of the Rössler System. *Appl. Sci.* **2020**, *11*, 81. [CrossRef]
41. Tamaševičius, A.; Mykolaitis, G.; Pyragas, V.; Pyragas, K. A simple chaotic oscillator for educational purposes. *Eur. J. Phys.* **2004**, *26*, 61. [CrossRef]