A Survey on Chaos-Based Cryptosystems: Implementations and Applications

Belqassim Bouteghrine, Camel Tanougast, and Said Sadoudi

Abstract Chaos theory is considered as a tool for studying the systems that show divergence and disorder. After having used discrete mathematics to deduce non-convergence situations, these theories are modeled in the form of a dynamic system and are applied in several domains such as electronic, mechanic, network security, etc. In network security domain, the development of new cryptosystems based on chaos is a relatively new area of research and is increasingly relevant. The essence of the theoretical and practical efforts in this field derive from the fact that these cryptosystems are faster than conventional methods, while ensuring performance of security, at least similar. In this paper, we discuss several proposals about chaos-based cryptosystem and pseudo-random number generator (PRNG). Moreover, topology and architecture of the proposed chaos systems are detailed. Finally, in order to show the more suitable system for encryption and secure communication, a synthesis comparison is presented and considered.

Keywords Chaos · Network security · Crypto-systems · Communication · PRNG

1 Introduction

Nowadays, network communication is vulnerable to many threats and cyber-attacks and it becomes more important for network experts to safeguard the network access [1]. Among the available security mechanisms, chaos-based cryptosystems are considered one of the most effective solution that provides the integrity, the authentication and the confidentiality. Recently, the development of new cryptosystems based on chaos is a relatively new area of research and is increasingly relevant.

B. Bouteghrine (✉) · C. Tanougast
LCOMS, Université de Lorraine, 57070 Metz, France
e-mail: belqassim.bouteghrine@univ-lorraine.fr

C. Tanougast
e-mail: Camel.Tanougast@univ-lorraine.fr

S. Sadoudi
Ecole Militaire Polytechnique, Algiers, Algeria

C. H. Skiadas and Y. Dimotikalis (eds.), *14th Chaotic Modeling and Simulation International Conference*, Springer Proceedings in Complexity,
https://doi.org/10.1007/978-3-030-96964-6_6

In [2], an Field-Programmable-Gate-Array (FPGA) implementation of image encryption purpose using two chaotic discrete time systems. The proposed two phases algorithm is executed by using the well known Arnold Cat map and the generalized logistic map, respectively. Authors in [3] initiate a systematic methodology for securing real-time video communication. The proposed chaos-based cryptosystem have been implemented on an FPGA hardware platform via Verilog Hardware Description Language (Verilog HDL). Sreenath and Narayanan [4] presents a Hardware implementation of a Pseudo chaos signal generator using three reconfigurable discrete time systems with a linear feedback shift registers (RLFSR). The proposed technique was implemented using Verilog HDL codes, then analyzed using Xilinx Plan Ahead compiler and Model-sim software. In terms of network security protocols, [5] proposed a novel chaos-based mechanism that includes Pseudo-Random Key-Generator which can be used to secure a socket-based communication. The proposed key-generator, created by solving the Lorenz chaos-system, has the main task of delivering at each opened channel a new 32-bit key that is used for encrypting/decryption the exchanged data.

In this paper, we discuss several proposals about chaos-based cryptosystem and pseudo-random number generator (PRNG). Moreover, topology and architecture of the proposed chaos systems are detailed. Finally, in order to show the more suitable system for encryption and secure communication, a synthesis comparison is presented and considered.

The remainder of this paper is structured as follows. Section 2 describes the classification of the most used chaotic systems. Section 3 shows the hardware implementations of these chaotic systems as well as their purposes. Section 4 concludes this paper.

2 Background and Description of Chaotic Systems

Due to the sensitivity and periodicity properties, chaotic systems have been involved mainly in key generation of the recently proposed cryptography schemes. Regarding their topology and mathematical model, we can classify all existing and newly proposed chaos systems in two main categories: continuous-time systems and discrete-time systems.

2.1 Continuous Time Systems

The continuous-time systems are described by a set of linear differential equation. Moreover, in order to ensure that the dynamical systems to be chaotic, the dimensions of the system's phase space must be at least equal to three (3). In the literature, there are several well known continuous-time systems such as Lorenz [6], Chen [7], Lu [8], etc.

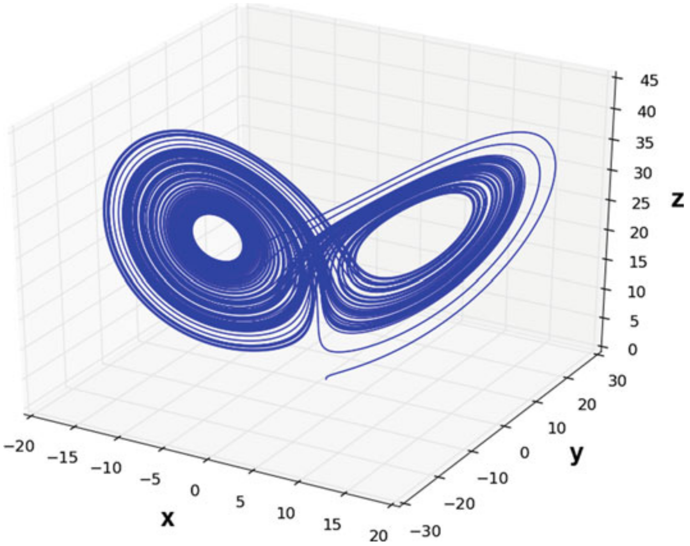

Fig. 1 Trajectory graph of the Lorenz system

Lorenz System The basic form of the Lorenz 3-D system is described by the following set of equation:

$$\dot{x} = a(y - x)$$
$$\dot{y} = y + bx - xz$$
$$\dot{z} = xy - cz$$

where x, y and z are the state variables. a, b and c are the system parameters. The chaotic behaviour (see Fig. 1) appears for a = 10, b = 28 and c = 8/3 with the initial conditions $x_0 = 0$, $y_0 = 5$ and $z_0 = 25$ [8].

Van-der-Pol System The Van-der-Pol oscillator as given in [9], is described in two dimensions as follows:

$$\dot{x} = a(x - (1/3)x^3 - y)$$
$$\dot{y} = (1/a)x$$

where x, y are the state variables, and a is the system controller. The phase portrait of the 2-D system is illustrated in Fig. 2.

Chen System Based on the 3-D Lorenz system, Chen 3-D system is proposed and described by the following set of equations:

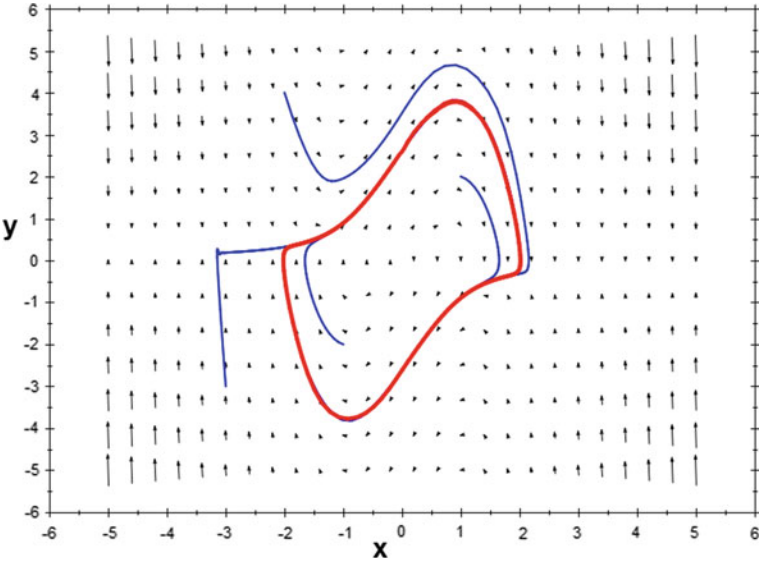

Fig. 2 Phase plan projection of the Van-der-Pol system

$$
\begin{aligned}
\dot{x} &= a(y - x) \\
\dot{y} &= (b - a)x + by - xz \\
\dot{z} &= xy - cz
\end{aligned}
$$

where x, y and z are the state variables. a, b and c are the system parameters. The chaotic behaviour appears for a = 35, b = 28 and c = 8/3 [10], while the phase plan projection is shown in Fig. 3.

Lu System The Lu system is known as the bridge between Lorenz system and Chen system [8]. Thereby, the mathematical model is given as follows:

$$
\begin{aligned}
\dot{x} &= a(y - x) \\
\dot{y} &= by - xz \\
\dot{z} &= xy - cz
\end{aligned}
$$

where x, y and z are the state variables. a, b and c are the system parameters. The trajectory graph of the proposed system is given in Fig. 4.

Linz-Sprott System Trying to simplify the formula of a chaotic system, Linz and Sprott [10] have proposed a new system which is defined as follows:

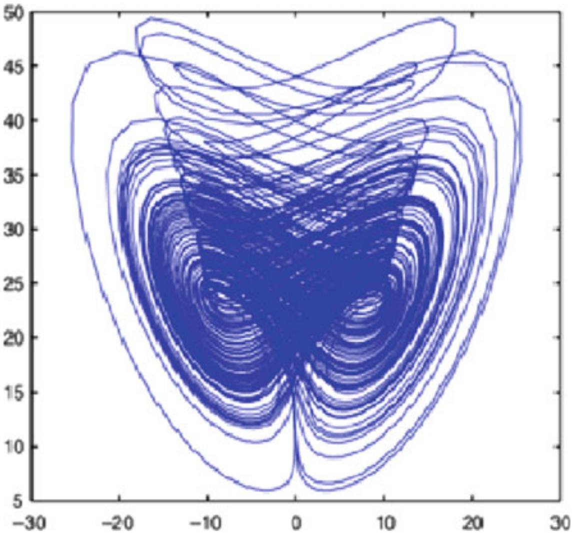

Fig. 3 Phase plan X−Y projection of the 3-D Chen system

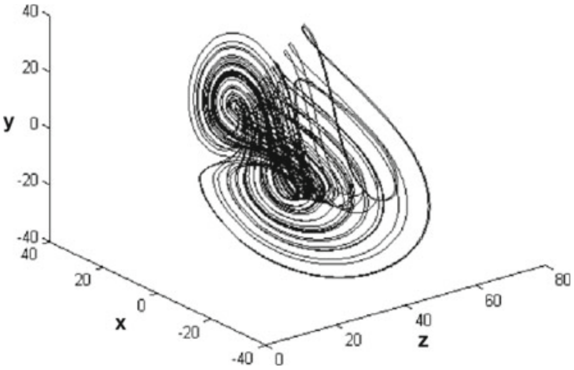

Fig. 4 Trajectory X−Y−Z of the 3-D Lu system

$$
\begin{aligned}
\dot{x} &= y \\
\dot{y} &= z \\
\dot{z} &= -az - y - 1 + |x|
\end{aligned}
$$

where x, y and z are the state variables and a is the system's parameter. As shown in Fig. 5, the chaotic behaviour of the proposed system is achieved for a = 0.6.

Four-Wing memristive hyperchaotic System Looking for higher dimensional chaotic system, authors in [11] have proposed a novel 4-D system which is described as follows:

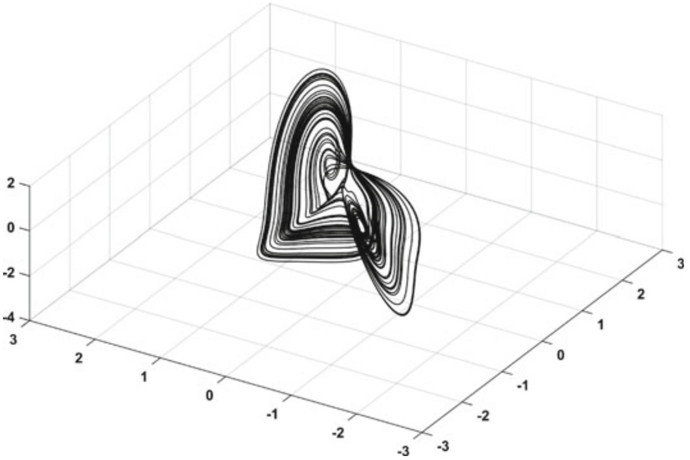

Fig. 5 Trajectory X−Y−Z of the Linz-Sprott system

$$\begin{aligned}\dot{x} &= ax + byz\\ \dot{y} &= cy + dxz - pyW(w) - Q\\ \dot{z} &= ez + fxy + gxw\\ \dot{w} &= -y\\ W(w) &= m + 3nw^2\end{aligned}$$

where x, y, z, w are the state variables. a, b, c, d, e, f, g, m, n, p, Q are the controllers of the proposed system. In order to ensure the chaotic behaviour, the controllers parameters are defined as follows: a = 0.35, b = −10, c = −0.6, d = 0.3, e = −1.6, f = 2, g = 0.1, m = 0.1, n = 0.01, p = 0.2 and Q = 0.01. The trajectory graphs corresponding to the proposed system with the associated parameters, are shown in Fig. 6.

New 3-D Continuous Time System Getting inspired from the Lorenz system [12], with only two (02) controllers, a novel 3-D system is proposed and defined as follows:

$$\begin{aligned}\dot{x} &= y - x - az\\ \dot{y} &= xz - x\\ \dot{z} &= -xy - y + b\end{aligned}$$

where x, y and z are the state variables. a and b are the system parameters. The chaotic behaviour of the proposed system is observed for the values a = 0.5 and b = 1 while the initial conditions are $x_0 = y_0 = z_0 = 0$ (see Fig. 7).

New 4-D Continuous Time System In [13], another new 4-D chaotic system is proposed based on the Rossler system, and defined by the following set of equations:

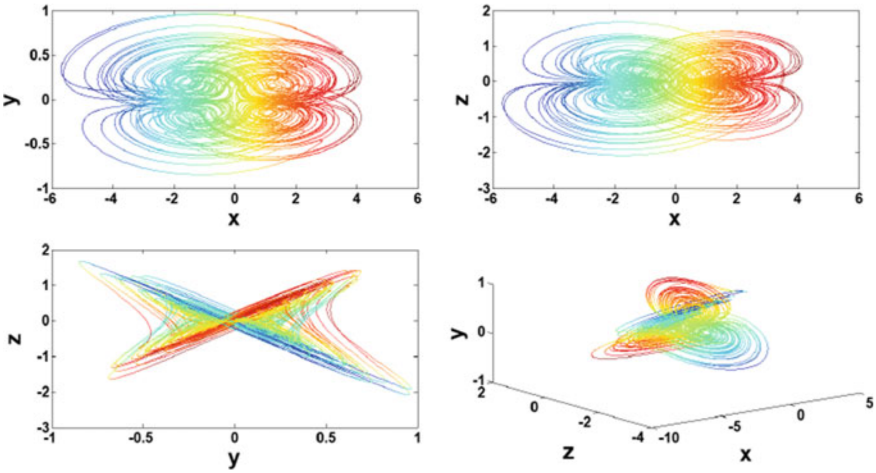

Fig. 6 Trajectory graphs of the proposed 4-Wing system

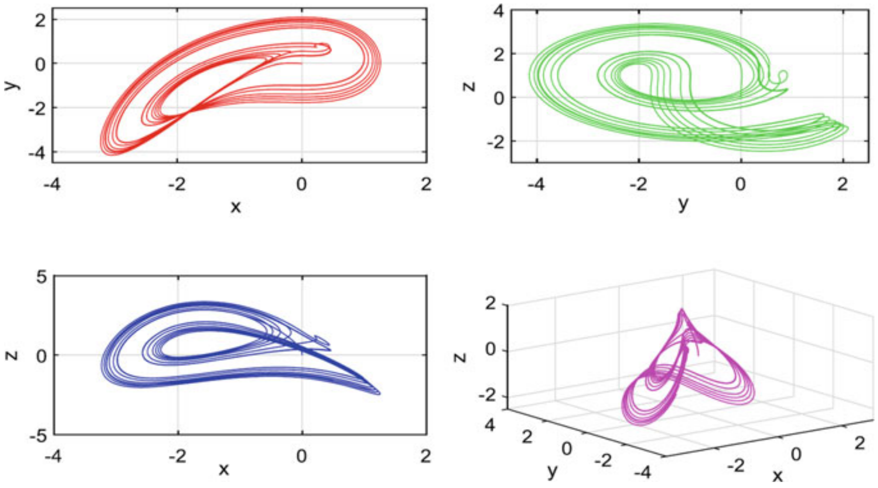

Fig. 7 Phase plan projections of the proposed 3-D system

$$
\begin{aligned}
\dot{x} &= -y - z + dw \\
\dot{y} &= x + ay \\
\dot{z} &= b + z(x - c) - a(y - w) \\
\dot{w} &= az - w
\end{aligned}
$$

where x, y, z and w are the state variables. a, b, c and d are the system parameters. By choosing a = 0.4, b = 0.6, c = 3 and d = 0.8, the chaotic behaviour of the proposed system is showed by phase plan projection (see Fig. 8).

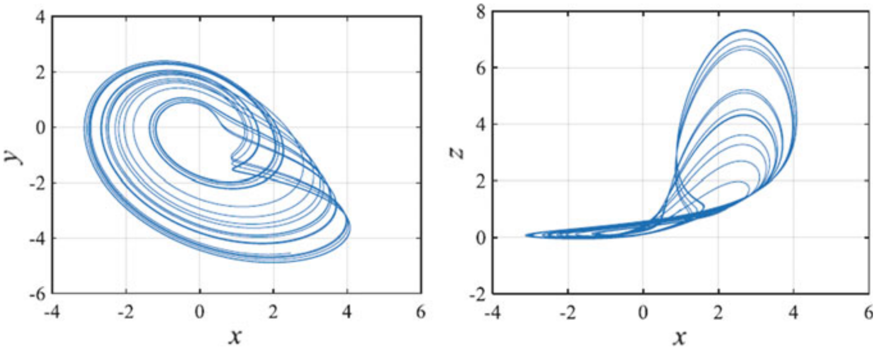

Fig. 8 Phase plan projection of the proposed system

2.2 Discrete Time Systems

The discrete time chaos system is a dynamic system which works in increments and takes the conditions at a given time t to change these conditions at a later time $t + \Delta t$. Hence, unlike the mathematical model of the continuous time systems, discrete time maps are described mathematically by an iterated function. Moreover, the dimension of the system's phase space could be only equal to one (01) to show chaos behaviour.

Logistic Map In the literature, many proposals have used the well known logistic map such as in [14] for PRNG, [2] for image encryption,[15] for chaotic signal generating, etc. The mathematical description of this map is given as follows:

$$x_{i+1} = ax_i(1 - x_i)$$

where x_i is the state variable and a is the system controller.

To ensure the chaotic behaviour (see Figs. 9 and 10) of this system, a should be in the interval [3.57 − 4].

Hénon Map A simple 2-D with quadratic non-linearity, Hénon system was the first map to show strange attractor with a fractal structure [16]. The mathematical description of this map is given as follows:

$$\begin{aligned} x_{i+1} &= a + y_i - x_i^2 \\ y_{i+1} &= bx_i \end{aligned}$$

where x_i and y_i are the state variables and a, b are the system controllers.

The obtained strange attractor of this map, is shown in Fig. 11 while the controllers are a = 1.4 and b = 0.3.

Rene-Lozi Map By introducing the absolute value in the Hénon map, the Rene-Lozi map used in [17] for stream cipher purpose, is described as follows:

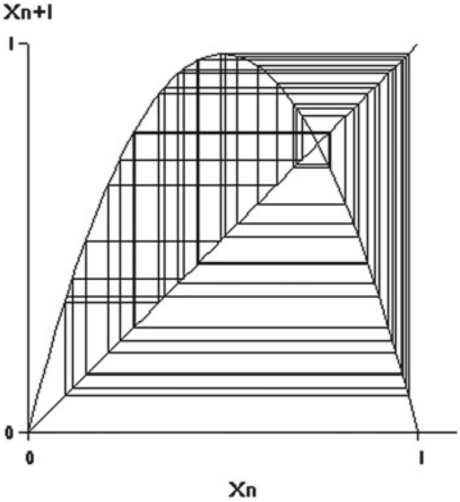

Fig. 9 Trajectory graph of the logistic map

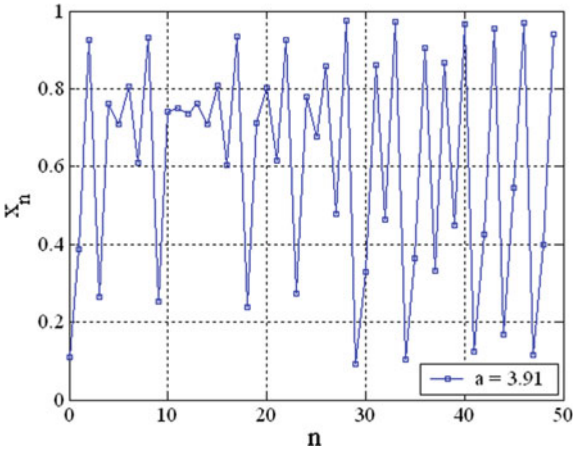

Fig. 10 Signal graph of the logistic map

$$x_{i+1} = 1 + y_i - a|x_i|$$
$$y_{i+1} = bx_i$$

where x_i and y_i are the state variables and a, b are the system controllers.

Similarly to the Hénon map, it has been shown that for a = 1.4 and b = 0.3, chaotic behaviour of this map can appear (see Fig. 12).

Bernoulli Map Unlike all the discrete time maps, Bernoulli map is composed of two piece-wise linear parts which are separated by a discontinue space of points [11] (see Fig. 13).

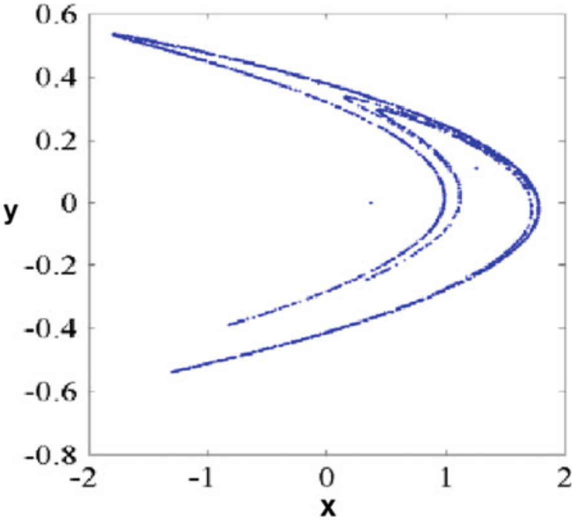

Fig. 11 Trajectory graph of the Hénon map

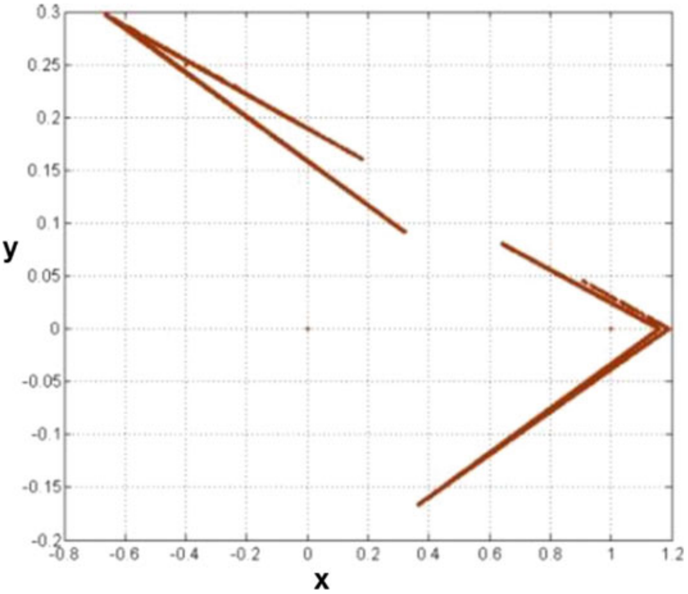

Fig. 12 Trajectory graph of the Rene-Lozi map

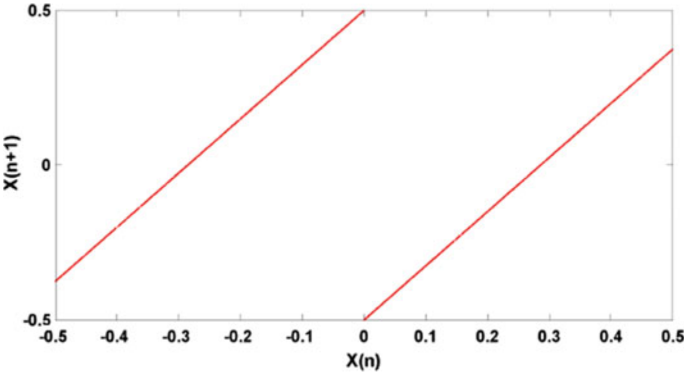

Fig. 13 Trajectory graph of the Bernoulli map

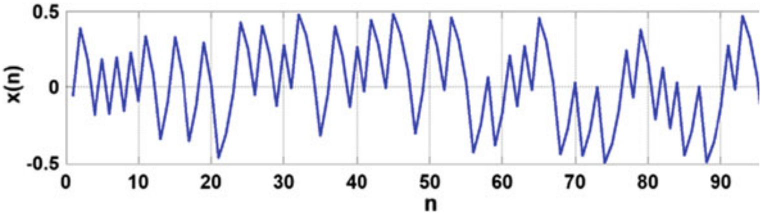

Fig. 14 Signal graph of the Bernoulli map

Mathematically, the Bernoulli map is defined as follows:

$$x_{i+1} = \begin{cases} ax_i + 0.5 & \text{if } x < 0 \\ ax_i - 0.5 & \text{if } x \geq 0, \end{cases}$$

where x_i is the state variable and a is the control parameter.
The chaotic status of this map is ensure for all the values of the parameter a inside the interval $]1.4 - 2]$ (see Fig. 14).

Sine Map The sine map is qualitatively similar to the logistic map, and the superficial similarity has resulted in a much deeper connection.

As indicated by its name, the sine map is defined by a sine function as follows:

$$x_{i+1} = a \sin(\pi x_i), \quad 0 \leq x_i \leq 1, \ a > 0$$

where x_i is the state variable and a is the system parameter. The projection graph which proves the behaviour of this map is shown in Fig. 15.

Tent Map Regarding the slope of its mathematical function, tent map with only one state variable, is considered as a slope of two (02) model. Without any control parameter, the tent map is defined as follows:

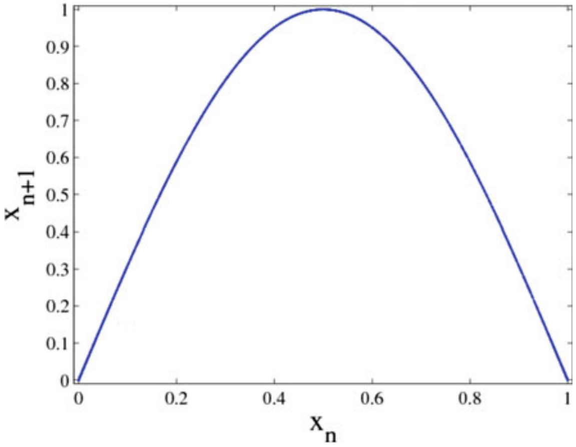

Fig. 15 Trajectory graph of the sine map

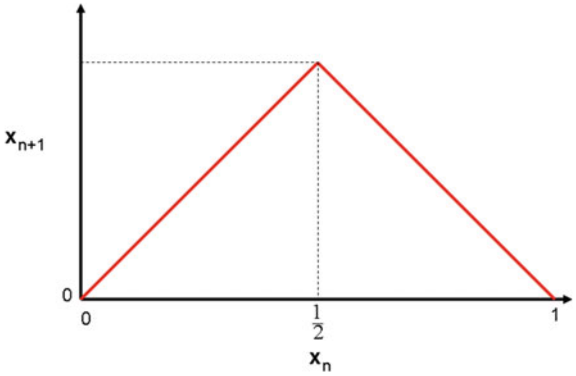

Fig. 16 Trajectory graph of the tent map

$$x_{i+1} = \begin{cases} 2x_i & \text{if } 0 \le x_i < 1/2 \\ 2(1 - x_i) & \text{if } 1/2 \le x_i \le 1 \end{cases}$$

where x_i is the state variable. Moreover, the trajectory graph of the tent map is shown in Fig. 16.

All these systems have been used mainly for either generating random numbers, cipher keys or chaotic signals. They differ from each other in terms of dimension, control parameters and the purpose of use. In Table 1 we summarize all these differences obtained regarding our study.

Table 1 Summary of the chaotic systems: description and purpose of application

System	References	Type	Dimension	Controllers	Purpose
Lorenz	[8]	Continuous	3-D	3	Image encryption
Van-der-Pol	[9]	Continuous	2-D	1	Random number generator
Chen	[10]	Continuous	3-D	3	Chaos signal generator
Lu	[8]	Continuous	3-D	3	Image encryption
Linz-Sprott	[10]	Continuous	3-D	1	Chaos signal generator
4-Wing	[11]	Continuous	4-D	11	Random number generator
New 3-D	[12]	Continuous	3-D	2	Random number generator
New 4-D	[13]	Continuous	4-D	4	Image processing
Logistic	[14]	Discrete	1-D	1	Random bit Generator
Hénon	[16]	Discrete	2-D	2	Encryption
Rene-Lozi	[17]	Discrete	2-D	2	Stream cipher
Bernoulli	[11]	Discrete	1-D	1	Random number generator
Sine	[15]	Discrete	1-D	1	Chaos signal generator
Tent	[18]	Discrete	1-D	0	Chaos signal generator

3 Hardware Implementations and Applications

FPGA-based prototyping is specifically geared toward meeting the design and verification demands created by the complexities of low and constrained resources devices. Moreover, FPGA-based prototyping allows designers to develop and test their systems and provides software developers early access to a fully functioning hardware platform long before silicon is available. In order to be implemented on FPGA, the continuous time systems need to be discredited numerically using some popular methods such as Euler and Runge-Kutta (RK) methods. Euler's method is a straightforward method that estimates the next point based on the rate of change at the current point and it is easy to code [19]. It is called also a single step method. While RK methods are actually a family of schemes derived in a specific style. Higher order accurate RK methods are multi-stage because they involve slope calculations at multiple steps at or between the current and next discrete time values [20]. The next value of the dependent variable is calculated by taking a weighted average of these multiple stages based on a Taylor series approximation of the solution. The weights in this weighted average are derived by solving non-linear algebraic equations which are formed by requiring cancellation of error terms in the Taylor series. Developing higher order RK methods is tedious and difficult without using symbolic tools for computation. The most popular RK method is RK4 since it offers a good balance between order of accuracy and cost of computation. RK4 is the highest order explicit Runge-Kutta method that requires the same number of steps as the order of accuracy (i.e. RK1 = 1 stage, RK2 = 2 stages, RK3 = 3 stages, RK4 = 4 stages, RK5 = 6 stages, . . .). Beyond fourth order the RK methods become relatively more expensive

Table 2 Summary of the FPGA implementations

References	FPGA technology	Resources	Chaos system	Discretization
[12]	Virtex-6	LUTs = 1070 Regs = 1196	New 3-D	Euler
[9]	Virtex-6	LUTs = 22674 Regs = 21,797	Van-der-Pol	RK4
[14]	Virtex-7	LUTs = 510 Regs = 120	Logistic	No need
[17]	Spartan-6	LUTs = 562 Regs = 386	Rene-Lozi	No Need
[11]	ZYNQ-XC7Z020	LUTs = 22,556 Regs = 264,26	Four-wing	RK4
[16]	Virtex-5	LUTs = 1496 Regs = 432	Hénon	No Need
[8]	Virtex-II	LUTs = 2490 Regs = 1316	Lorenz/Lu	RK-4
[22]	Virtex-5	LUTs = 2799 Regs = 1722	Logistic	No Need
[23]	Zynq-7000	LUTs = 856 Regs = 521	Hénon	No Need
[24]	Stratix-IV	LUTs = 49,005 Regs = 611	New 3-D	Euler

to compute. Among all the studied proposals, we have synthesised a brief comparison that includes mainly the used FPGA technology and the consumed resources. Table 2 summarizes the difference between different proposals regarding the chosen system as well as the resource consumption. However, we found that in the single-precision and the double-precision operations, there are more than 10^{-6} differences in less than 100 iterations, and the difference reaches more than one digit after 1000 iterations [21]. This is because the binary has a round-off error, so the binary cannot strictly obey the commutative law or the distribution law in floating-point operations.

4 Conclusion

In this paper, we discuss several proposals about chaos-based cryptosystem and pseudo-random number generator (PRNG). Moreover, topology and architecture of the proposed chaos systems are detailed. Finally, in order to show the more suitable system for encryption and secure communication, a synthesis comparison is presented and considered.

References

1. B. Bouteghrine, M. Rabiai, C. Tanougast, S. Sadoudi, FPGA implementation of Internet key exchange based on chaotic cryptosystem, in *10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)* (Metz, France, 2019), pp. 384–387
2. B. Baruah, M. Saikia, An FPGA implementation of chaos based image encryption and its performance analysis. IJCSN Int. J. Comput. Sci. Netw. **5**, 5 (2016) (Unpaginated)

3. S. Chen, S. Yu, J. Lu, G. Chen, J. He, Design and FPGA-based realization of a chaotic secure video communication system. IEEE Trans. Circuits Syst. Video Technol. **28**(9), 2359–2371 (2017)
4. H. Sreenath, G. Narayanan, FPGA implementation of pseudo chaos-signal generator for secure communication systems, in *2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)* (Bangalore, India, 2018), pp. 804–807
5. B. Bouteghrine, M. Rabiai, C. Tanougast, S. Sadoudi, Hardware implementation of secured socket communication based on chaotic cryptosystem, in *2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)* (Oxford, UK, 2019), pp. 1–4
6. A. Qi, C. Han, G. Wang, Design and FPGA realization of a pseudo random sequence generator based on a switched chaos, in *2010 International Conference on Communications, Circuits and Systems (ICCCAS)* (Chengdu, China, 2010), pp. 417–420
7. J. Lu, X. Wu, X. Han, J. Lu, Adaptive feedback synchronization of a unified chaotic system. Phys. Lett. A **329**(4–5), 327–333 (2004)
8. M.S. Azzaz et al., FPGA implementation of new real-time image encryption based switching chaotic systems, in *IET Irish Signals and Systems Conference (ISSC 2009)*, vol. 56. (Dublin. Ireland, 2009)
9. M. Tuna, A novel secure chaos-based pseudo random number generator based on ANN-based chaotic and ring oscillator: design and its FPGA implementation. Analog Integr. Circ. Sig. Process **105**(2), 167–181 (2020)
10. A. Senouci et al., FPGA based hardware and device-independent implementation of chaotic generators. AEU-Int. J. Electron. Commun. **82**, 211–220 (2017)
11. F. Yu et al., Design and FPGA implementation of a pseudo-random number generator based on a four-wing memristive hyperchaotic system and Bernoulli map. IEEE Access **7**, 181884–181898 (2019)
12. I. Koyuncu et al., Design, FPGA implementation and statistical analysis of chaos-ring based dual entropy core true random number generator. Analog Integr. Circ. Sig. Process. **102**(2), 445–456 (2020)
13. C.H. Yang, Y.S. Chien, FPGA implementation and design of a hybrid Chaos-AES color image encryption algorithm. Symmetry **12**(2), 189 (2020)
14. M. Garcia-Bosque et al., Chaos-based bitwise dynamical pseudorandom number generator on FPGA. IEEE Trans. Instrum. Measur. **68**(1), 291–293 (2018)
15. Z. Hua, B. Zhou, Y. Zhou, Sine-transform-based chaotic system with FPGA implementation. IEEE Trans. Industr. Electron. **65**(3), 2557–2566 (2017)
16. A.M. Atteya, A.H. Madian, A hybrid Chaos-AES encryption algorithm and its implemention based on FPGA, in *IEEE 12th International New Circuits and Systems Conference (NEWCAS)*, vols. 217–220 (Quebec, Canada, 2014)
17. L. Merah et al., FPGA hardware co-simulation of new chaos-based stream cipher based on Lozi map. Int. J. Eng. Technol. **9**(5), 420–425 (2017)
18. Y. Mao, L. Cao and W. Liu, Design and FPGA implementation of a pseudo-random bit sequence generator using spatiotemporal chaos, in *2006 International Conference on Communications, Circuits and Systems* (Guangzi, China, 2006), pp. 2114–2118
19. D.I. Lanlege et al., Comparison of Euler and Range-Kutta methods in solving ordinary differential equations of order two and four. Leonardo J. Sci. **32**, 10–37 (2018)
20. S.C. Palligkinis, G. Papageorgiou, I.T. Famelis, Runge-Kutta methods for fuzzy differential equations. Appl. Math. Comput. **209**, 97–105 (2009)
21. C.H. Yang, H.C. Wu, S.F. Su, Implementation of encryption algorithm and wireless image transmission system on FPGA. IEEE Access **7**, 50513–50523 (2019)
22. P. Dabal, R. Pelka, A chaos-based pseudo-random bit generator implemented in FPGA device, in *14th IEEE International Symposium on Design and Diagnostics of Electronic Circuits and Systems* (Cottbus, Germany, 2011), pp. 151–154

23. R. Hobincu, O. Datcu, FPGA implementation of a chaos based PRNG targetting secret communication, International Symposium on Electronics and Telecommunications (ISETC), Timisoara. Romania **1–4**, 2018 (2018)
24. E. Tlelo-Cuautle et al., FPGA realization of a chaotic communication system applied to image processing. Nonlinear Dyn. **82**(4), 1879–1892 (2015)