applied sciences

Article

A Chaotic System with Infinite Equilibria and Its S-Box Constructing Application

Xiong Wang [1], Akif Akgul [2], Unal Cavusoglu [3], Viet-Thanh Pham [4,*] and Duy Vo Hoang [4] and Xuan Quynh Nguyen [5]

[1] Institute for Advanced Study, Shenzhen University, Shenzhen 518060, China; wangxiong8686@szu.edu.cn
[2] Department of Electrical and Electronics Engineering, Faculty of Technology, Sakarya University of Applied Sciences, 54187 Serdivan, Turkey; aakgul@sakarya.edu.tr
[3] Department of Computer Engineering, Faculty of Computer and Information Sciences, Sakarya University, 54187 Serdivan, Turkey; unalc@sakarya.edu.tr
[4] Modeling Evolutionary Algorithms Simulation and Artificial Intelligence, Faculty of Electrical & Electronics Engineering, Ton Duc Thang University, Ho Chi Minh City, Vietnam; vohoangduy@tdt.edu.vn
[5] National Council for Science and Technology Policy, Hanoi, Vietnam; Quynhnx@hactech.edu.vn
* Correspondence: phamvietthanh@tdt.edu.vn

Received: 3 October 2018; Accepted: 31 October 2018; Published: 2 November 2018

Abstract: Systems with many equilibrium points have attracted considerable interest recently. A chaotic system with a line equilibrium has been studied in this work. The system has infinite equilibria and exhibits coexisting chaotic attractors. The system with an infinite number of equilibria has been realized by an electronic circuit, which confirms the feasibility of the system. Based on such a system, we have developed a new S-Box generation algorithm. With the developed algorithm, two new S-Boxes are produced. Performance tests of S-Boxes are performed. The tests have shown that proposed S-Boxes have good performance results.

Keywords: chaos; equilibrium; Lyapunov exponent; bifurcation diagram; circuit; S-Box

1. Introduction

Systems with chaotic behaviour have been discovered and studied for many years [1–4]. In general, there are countable equilibrium points in conventional chaotic systems [5]. By applying a systematic examination, Sprott found 18 simple chaotic flows with one or two equilibrium points [6]. The well-known Lorenz system has one saddle and two unstable saddle-foci [1]. Similarly, other typical chaotic systems with three equilibrium points are Chen system [7], Lü system [8], Yang systems [9,10] and so on [11]. Dynamical analysis and electronic circuit design of a chaotic system with four equilibrium points were reported in [12]. Dadras and Momeni proposed a chaotic system with five equilibrium points [13]. Furthermore, a method to construct chaotic systems with any preassigned number of equilibria was presented by Wang and Chen [14].

Recently, researchers have shown an increased interest in chaotic systems with an infinite number of equilibrium points such as systems with a line equilibrium [15], systems with circular equilibrium [16], or systems with square equilibrium [17], etc. It is noted that memristor-based systems often have a line of equilibrium points [18]. It is interesting that Chen et al. have found nine discrete chaotic systems with one-line equilibria and applied them for image encryption [19]. Chaotic systems with infinite equilibria and their applications should be further investigated.

It is now well established from a variety of studies that chaos is useful for designing S-Box, which is the vital nonlinear confusion part in encryption algorithms [20–23]. Nonlinear chaotic algorithm for designing substitution-boxes was presented [24]. S-Box generation algorithms were designed with chaotic maps [20,25], the Lorenz system [21,26], or the chaotic scaled Zhongtang system [27]. Ozkaynak and Yavuz developed S-boxes using a time-delay chaotic system [28]. In addition, a new eight-term chaotic system with two equilibrium points was introduced and employed in a novel S-Box [23]. Creating S-Box structures based on chaotic systems with infinite equilibria is an attractive topic. Previous research has established that S-Box is the only nonlinear part using in block encryption algorithms. S-Box is considered as the most fundamental structure of block encryption algorithms [29–32]. As a result, a well-designed S-Box structure makes the encryption resistant against various attacks. The application of S-Boxes in cryptography is reported for wireless sensor network [33], image encryption scheme [34], color image watermarking [35], and copyright protection [36].

The aim of this work is to study a chaotic system with an infinite number of equilibrium points and its S-Box generating application. In Section 2, we introduce the system and its dynamics. Circuit implementation of the system is presented and experiential results are reported in Section 3. In Section 4, a new S-Box generation algorithm is proposed. Finally, Section 5 concludes our work.

2. Chaotic System with a Line Equilibrium

In this work, we consider the seven-term autonomous system in the following form:

$$\begin{cases} \dot{x} = y, \\ \dot{y} = -ax - by + yz, \\ \dot{z} = -cxy - x^2 + y^2, \end{cases} \tag{1}$$

in which x, y, z are state variables. In system (1), a, b, c are three positive parameters ($a, b, c > 0$). It is easy to verify that system (1) is invariant under the coordinate transformation:

$$(x, y, z) \to (-x, -y, z). \tag{2}$$

We can find the equilibrium of system (1) by solving:

$$y = 0, \tag{3}$$

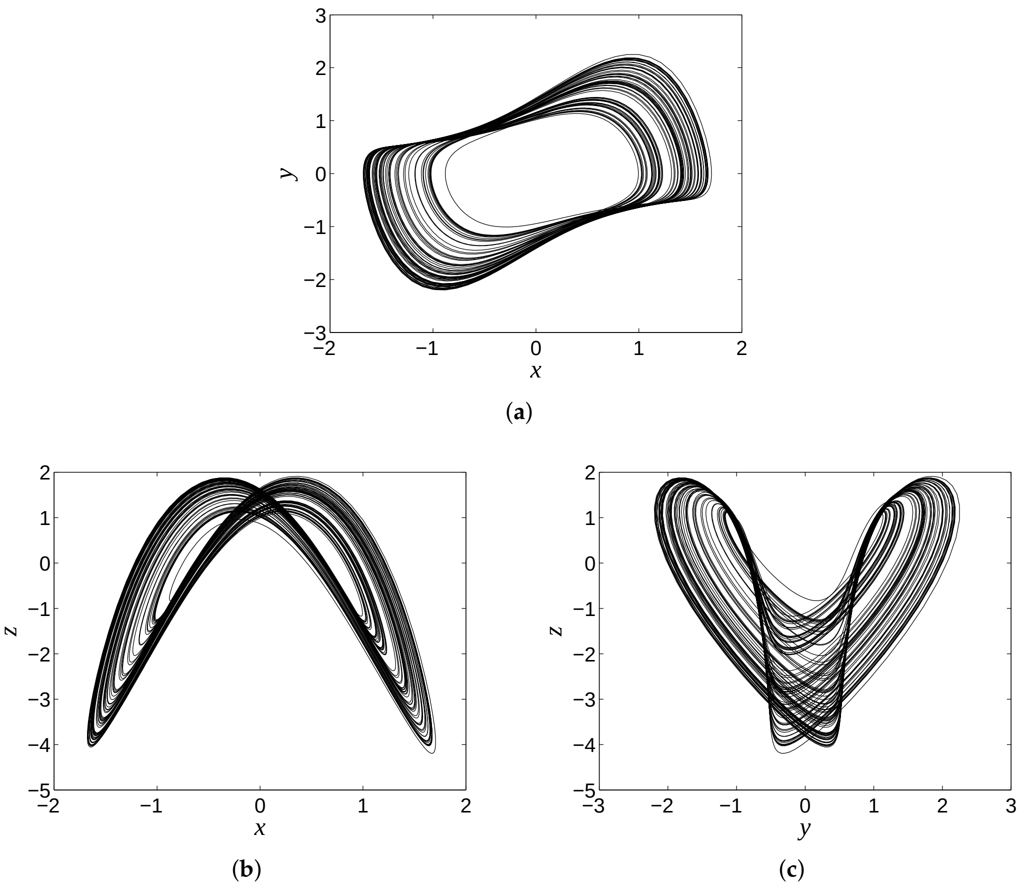
$$-ax - by + yz = 0, \tag{4}$$

$$-cxy - x^2 + y^2 = 0. \tag{5}$$

Therefore, it is easy to see that system (1) has a line equilibrium:

$$E(0, 0, z). \tag{6}$$

Interestingly, system (1) exhibits chaotic behavior for $a = 1.5$, $b = 0.5$, and $c = 5$ (see Figure 1). Calculated Lyapunov exponents and corresponding Kaplan–Yorke dimension of the system with infinite equilibria are $\mathrm{L}_1 = 0.1406$, $\mathrm{L}_2 = 0$, $\mathrm{L}_3 = -1.3768$, and $\mathrm{D}_{KY} = 2.1021$. In our simulations, we have used the well-known Runge–Kutta 4th-order method [37] and Lyapunov exponents have been obtained by applying the Wolf's method [38].



(**a**)

(**b**) (**c**)

Figure 1. Phase portraits of the system with infinite equilibria in (**a**) $x - y$ plane; (**b**) $x - z$ plane; and (**c**) $y - z$ plane for $a = 1.5$, $b = 0.5$, $c = 5$, and initial conditions $(x(0), y(0), z(0)) = (0.5, 1, 0.5)$.

We have changed the value of the parameter c to discover the dynamics of system (1). Other parameters are kept as $a = 1.5$, $b = 0.5$ while the initial conditions are $(x(0), y(0), z(0)) = (0.5, 1, 0.5)$. The bifurcation diagram and corresponding maximum Lyapunov exponents of system (1) are displayed in Figures 2 and 3. As can be seen in Figures 2 and 3, there are windows of periodic dynamics and chaos. For $c > 5.65$, the system with infinite equilibria only displays limit cycles as illustrated in Figure 4.

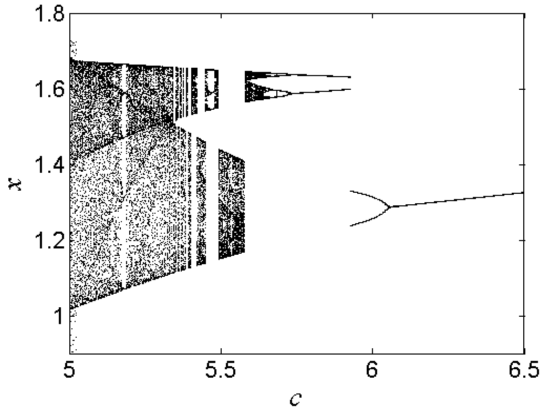


Figure 2. Bifurcation diagram of system with infinite equilibria (1) for $a = 1.5$, $b = 0.5$ and $c \in [5, 6.5]$.

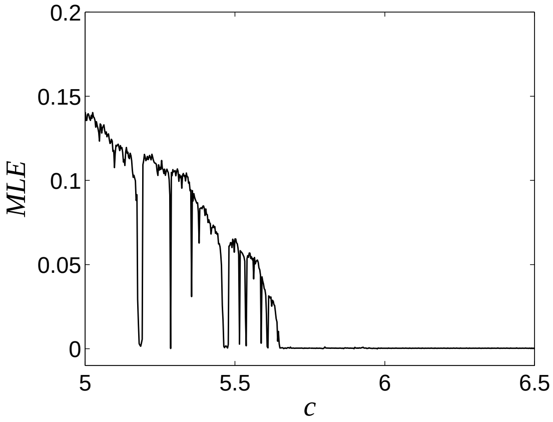
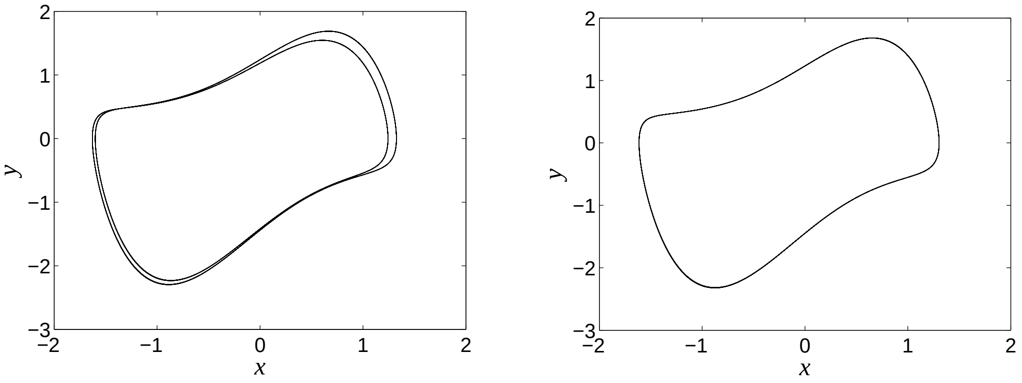


Figure 3. Maximum Lyapunov exponents of system with infinite equilibria (1) when changing the parameter c from 5 to 6.5.

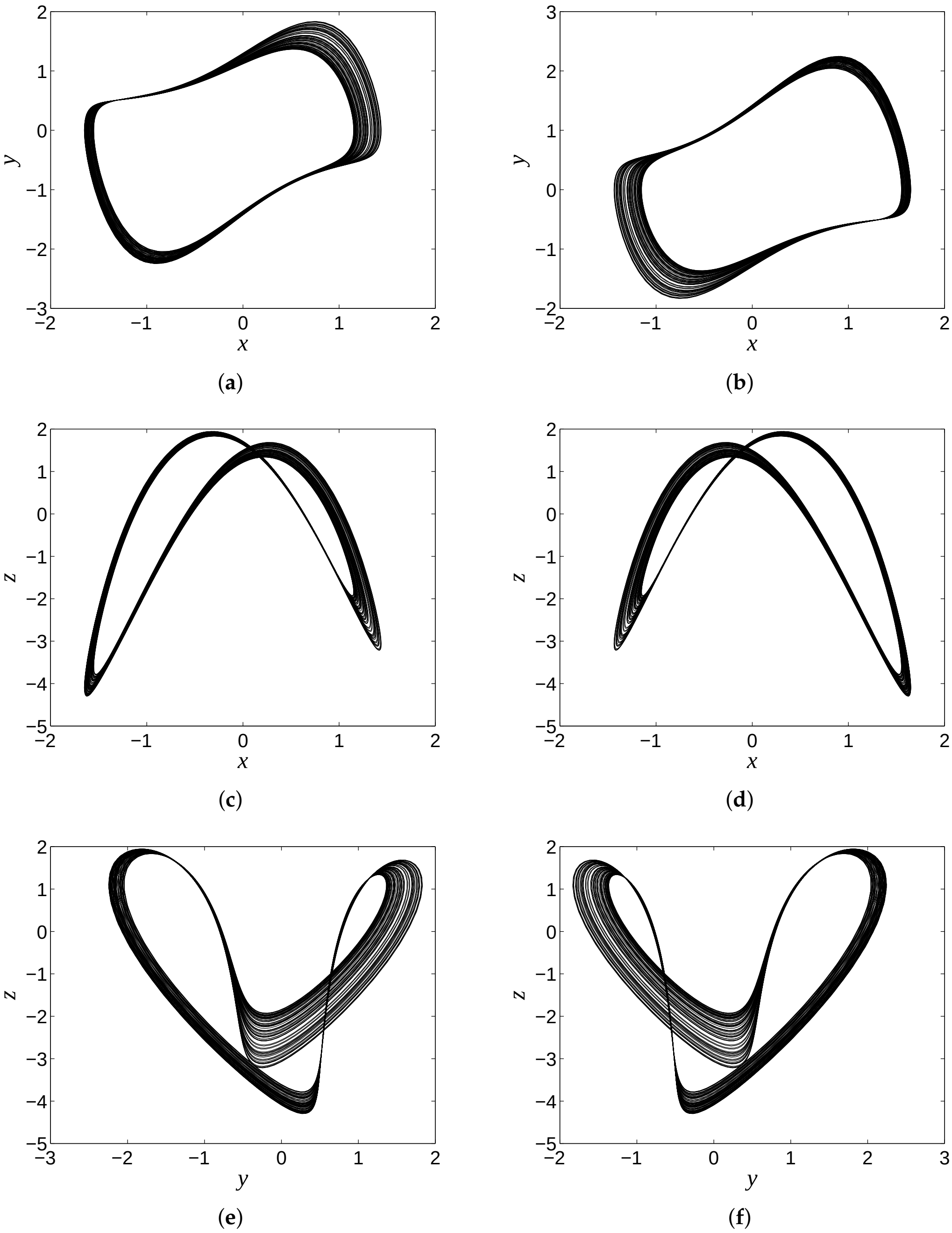


(**a**)

(**b**)

Figure 4. Limit cycles of the system with infinite equilibria for $a = 1.5$, $b = 0.5$, and initial conditions $(x(0), y(0), z(0)) = (0.5, 1, 0.5)$: (**a**) $c = 5.95$, and (**b**) $c = 6.25$.

Previous research has established that multistability is a desirable property of the nonlinear system [39–42]. Coexistence of multiple attractors has been found in diffirent chaotic systems [43–45]. Interestingly, when changing the value of the parameter c, we have observed the presence of coexisting attractors in system with infinite equilibria (1). For example, coexistence of chaotic attractors is illustrated in Figure 5 for $a = 1.5$, $b = 0.5$, $c = 5.5$, and initial conditions $(x(0), y(0), z(0)) = (\pm 0.5, \pm 1, 0.5)$.



(**a**) (**b**)

(**c**) (**d**)

(**e**) (**f**)

Figure 5. Coexisting attractors of the system with infinite equilibria in: $x - y$ plane (**a**,**b**), $x - z$ plane (**c**,**d**), and $y - z$ plane (**e**,**f**) for $a = 1.5$, $b = 0.5$, $c = 5.5$, and initial conditions $(x(0), y(0), z(0)) = (\pm 0.5, \pm 1, 0.5)$.

3. Circuit Realization of the Chaotic System

In this section, we present briefly the electronic realization of the chaotic system with infinite equilibria. The schematic of the circuit is designed with common electronic component as shown in Figure 6. The circuit includes nine resistors, three capacitors, four operational amplifiers and four multipliers. It is noted that the circuit is based on operational amplifiers [46,47], which are configured as integrator amplifiers and an inverting amplifier. The circuit is powered by +15 V and −15 V. In order to realize the system for parameters $a = 1.5$, $b = 0.5$, and $c = 5$, we have selected $R_1 = 400$ kΩ, $R_2 = 266$ kΩ, $R_3 = 800$ kΩ, $R_4 = R_8 = R_9 = 40$ kΩ, $R_5 = R_6 = 100$ kΩ, $R_7 = 8$ kΩ and $C_1 = C_2 = C_3 = 1$ nF. As denoted in Figure 6, the voltages over three capacitors are X, Y, and Z, which correspond to three state variables x, y and z.

The chaotic system with infinite equilibria was implemented on an electronic card as illustrated in Figure 7. The oscilloscope phase portrait results are shown in Figure 8. The agreement of the theoretical results (Figure 1) and obtained experimental results (Figure 8) verifies the feasibility of the system with infinite equilibria.

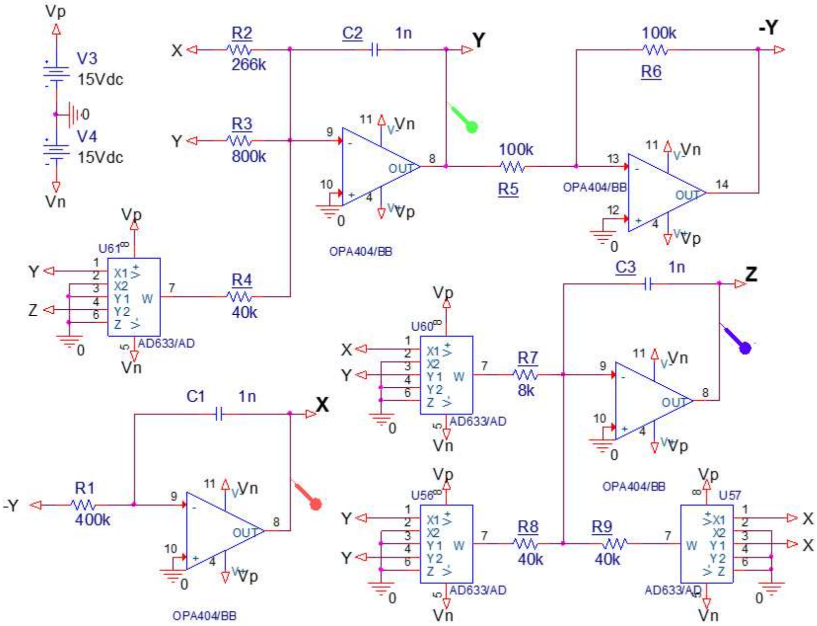
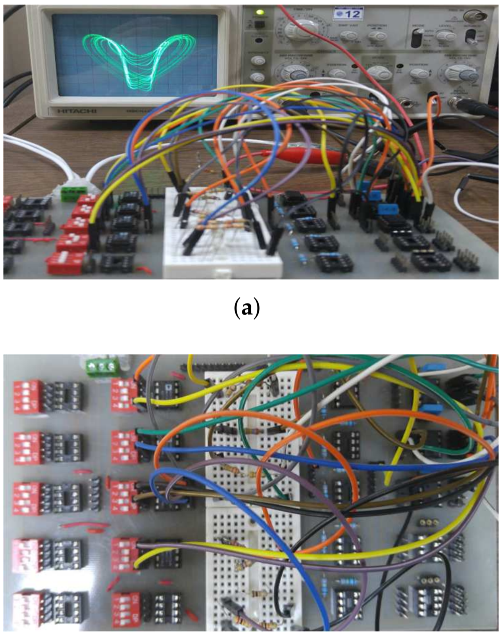
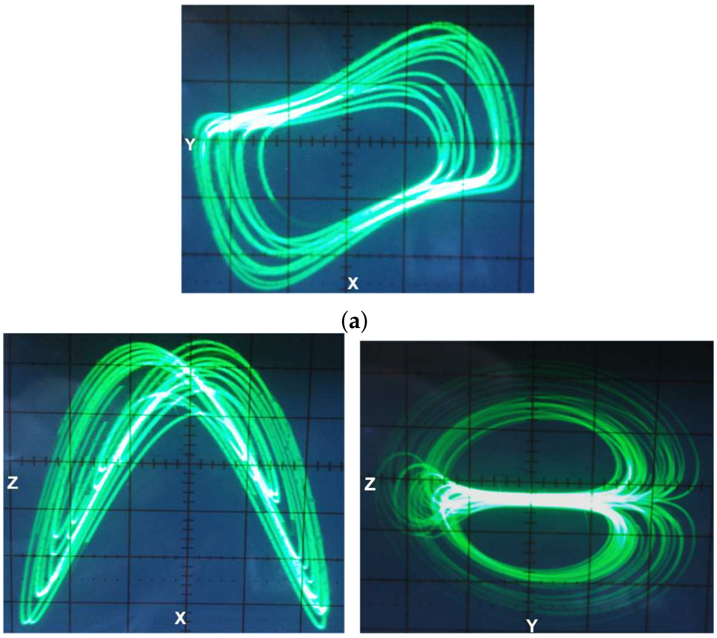


Figure 6. The circuit schematic of the chaotic system with infinite equilibria, which is designed by using common electronic components.


(**a**)

(**b**)

Figure 7. The implemented circuit of the chaotic system with infinite equilibria: (**a**) the measurement of the circuit by using the oscilloscope, (**b**) the electronic card.



(**a**)

(**b**) (**c**)

Figure 8. Measured phase portraits of the real circuit in (**a**) $X - Y$ plane, (**b**) $X - Z$ plane, and (**c**) $Y - Z$ plane.

4. S-Box Generation Algorithm and Its Performance Analysis

Chaotic systems are widely used in cryptographic studies because of their high randomness, rich dynamical properties and high sensitivity to initial conditions [48–55]. S-Box is one of the most main structures used in block cipher algorithms [56]. S-Box structures with strong cryptographic features make cryptography very resistant to attack. In the literature, there are studies using different methods for S-Box production [21,23,24,26,27,57]. S-Box structures are one of the most important components used in encryption algorithms. S-Box operations provide confusion as a nonlinear component in encryption algorithms and thus a powerful S-Box structure with good performance values is very important for strong encryption. The sub-byte operation is performed by using S-Box. In this study, high random number generation capabilities of the chaotic system are used in the design of S-Box algorithm. In this way, S-Boxes are produced with higher performance characteristics. The advantage of the proposed method provided is that the S-Box structures are obtained with less processing load. Numerous S-Boxes can be produced using different initial values and parameters. As a result of performance tests, it is shown that S-Boxes with high performance characteristics will be used in cryptographic operations for secure communication. S-Box structures are used in different applications for secure communication systems, such as personal area communication, wireless sensor network and medical device connectivity. The S-Box can be used as a component or key expansion operations in encryption algorithms. In addition, S-Box structures are frequently used in text, image, video encryption and embedded system applications.

In this section, a new S-Box generation algorithm is presented with a light processing load using the introduced chaotic system with infinite equilibria. Performance tests are performed on the S-Boxes generated by the S-Box algorithm. The performance evaluation of the generated S-Boxes is made by comparing with the reported S-Boxes in the literature. Algorithm 1 shows the pseudo code of the S-Box generation algorithm.

Following the entry of the initial conditions and system parameters of the chaotic system in the S-Box generation algorithm, the appropriate sampling step is determined and the chaotic system is solved by the RK-4 numerical analysis method. The float values are obtained by solving the chaotic system. Until the 256 unique values required for the S-Box are generated, the system continues to generate values. By applying rem and fix operations on the float numbers obtained from the chaotic system, the value in the first three digits of the generated float value is obtained after the comma. The obtained values are maintained in the 0–255 range by applying *mod* 256 operation. The values (first three digits after the comma) obtained from the x and z phases are subjected to *bitxor* processing to obtain a new decimal value (*decnum*). If the new decimal value is already generated in the S-Box, this value is discarded. If it is not in the S-Box, it is added to the S-Box. In this way, a unique 256 value generation is provided in the range of 0–255. The generated 256-element S-Box is converted into 16 × 16 matrix and S-Box performance tests are applied. In the pseudo code in Algorithm 1, the generation is given to be performed over the x and z phases. In practice, however, the generation of S-Box is carried out using different surpluses and tests are carried out. Two S-Boxes with good test results are proposed and performance test results are given in our work.

Algorithm 1 S-Box generator algorithm pseudo code

```
1:  Start
2:  i = 1; sbox = [];
3:  Entering system parameters → $(a = 1.5, b = 0.5, c = 5)$
4:  Entering initial condition → $(x_0 = 0.5, y_0 = 1, z_0 = 0.5)$
5:  Determination of the appropriate value of Δh(0.05)
6:  Solving the chaotic system using RK-4 algorithm and obtaining time series
7:  **while** (i < 257) **do**
8:      $x = mod(fix(rem(ys(1), 1) * 10^3), 256);$
9:      $z = mod(fix(rem(ys(3), 1) * 10^3), 256);$
10:     $decnum = bitxor(x, z)$
11:     **if** (Is there decnum in S-Box = yes) **then**
12:         Go step 7.
13:     **else** {Is there decnum in S-Box = no}
14:         sbox[i] ← decnum
15:         i++;
16:     **end if**
17: **end while**
18: sbox ← reshape(sbox,16,16)
19: Implementation of S-Box Performance Tests
20: Ready to use 16*16 chaos based S-Box
21: End
```

Tables 1 and 2 show S-Boxes generated by the S-Box algorithm. The S-Box 1 presented in Table 1 is generated using the y and z phases of the chaotic system. The production of S-Box 2 presented in Table 2, x and z phases are preferred. Analysis of Nonlinearity, Strict avalanche criterion (SAC), Output bits independence criterion (BIC), Differential Approximation Probability (DP) and Linear Approximation Probability (LP) analyses are performed on the proposed S-Boxes. The performance test results are summarized in Table 3. In addition to the proposed S-Box performance results, the results of some S-Box studies in the literature are also given in Table 3.

Nonlinearity [58] is one of the most important criteria within the S-Box evaluation criteria. It is found that the nonlinearity values of the proposed S-Box 1 are 106, 104, 104, 104, 106, 108, 110 and 108 while the nonlinearity values of the proposed S-Box 2 are 108, 106, 106, 106, 106, 106, 108, and 108. As can be seen from Table 3, the proposed S-Box 1 nonlinearity max, min, avg values are 110, 104 and 106, respectively. The nonlinearity max, min and avg values are 108, 106 and 106, respectively. The AES S-Box nonlinearity value has the best value in the literature. Other studies in the literature are attempting to produce S-Boxes with equal or better nonlinearity values. When the performance test results in Table 3 are compared, it is seen that proposed S-Boxes have the best max, avg and min values after the AES S-Box.

One of the tests used in the performance evaluation of S-Boxes is the independence of output bits method developed by Webster and Tavares [59]. In this method, S-Box is evaluated on two criteria. The BIC-SAC value refers to the relationship between the independence of the output bits and the Strict avalanche criterion. BIC-Nonlinearity examines the relation between the independence of output bits and nonlinearity. BIC-SAC and BIC-Nonlinearity values of the proposed S-Boxes in Table 3 are given. When these values and the values of the S-Boxes in the literature are examined, it is seen that the proposed S-Boxes have a good BIC-SAC value and have a BIC-Nonlinearity value lower than the AES BIC-Nonlinearity value but better than the other studies in the literature.

Table 1. The proposed S-Box 1.

21	77	79	5	165	241	6	12	102	144	168	192	250	11	49	195
206	252	101	249	94	98	108	3	29	219	64	172	119	46	65	126
142	13	178	90	236	17	132	55	137	200	162	143	85	0	140	243
141	222	234	23	4	193	148	247	155	58	44	122	92	158	50	82
182	36	204	128	20	254	89	60	1	242	106	181	110	80	93	56
133	91	199	183	248	42	138	226	48	7	166	244	120	146	107	188
41	33	57	116	87	218	170	197	220	53	111	210	246	184	39	156
61	185	202	18	201	164	117	123	47	190	203	24	171	253	157	169
14	72	112	27	51	186	95	177	212	43	66	115	229	35	233	124
153	232	180	54	104	215	69	129	78	81	163	84	209	75	38	31
176	149	88	231	139	96	240	151	239	22	37	59	174	161	154	71
205	230	225	73	34	16	237	223	109	245	191	74	9	113	211	134
52	114	125	130	99	68	238	224	70	159	62	76	136	235	179	28
187	217	25	118	127	67	150	10	86	97	160	32	173	167	100	194
207	255	228	45	214	40	198	216	145	131	251	63	19	213	227	121
147	8	152	196	135	83	30	208	189	175	26	103	2	105	221	15

Table 2. The proposed S-Box 2.

205	187	157	107	37	195	184	145	185	21	130	124	179	245	127	19
32	87	198	101	192	221	230	213	186	25	140	136	247	39	9	78
223	235	222	167	16	220	73	11	80	163	243	225	14	108	202	88
215	147	59	242	97	214	188	91	119	36	233	234	67	224	20	219
81	46	229	174	134	63	146	23	74	105	95	106	44	138	102	208
61	173	8	103	0	150	197	27	51	47	241	57	131	111	182	249
110	210	104	69	28	169	118	191	5	209	52	48	199	55	64	77
17	116	253	168	113	6	181	13	236	82	149	133	75	109	252	246
159	54	84	72	139	160	164	170	100	62	10	2	1	172	141	177
175	24	231	201	123	94	121	49	176	151	68	115	35	156	42	60
31	137	165	248	120	154	40	206	161	86	228	189	34	144	171	142
240	132	180	255	238	129	200	53	71	212	155	83	226	50	7	29
90	126	4	207	58	89	183	158	18	148	128	96	244	227	153	203
93	3	38	218	196	99	162	143	250	135	217	15	232	66	166	204
194	254	178	43	56	41	152	251	117	33	45	92	193	76	190	85
65	70	26	125	22	98	12	114	112	211	122	30	216	79	239	237

Strict avalanche criteria (SAC) is a performance criterion developed by Webster and Tavares [59]. In this test, when only one of the input bits changes, the probability of each half of the output bits changing is calculated. The optimum value for this test is 0.5. The min, max and avg SAC values of the proposed S-Boxes in Table 3 are shown. It has been determined that the SAC values of the proposed S-Boxes and presented in the literature are close to the optimum value and satisfy the SAC criterion.

Differential Approximation Probability (DP) developed by Biham and Shamir [60] investigates the exclusive or (XOR) distribution between the input and output bits of the S-Box. The approximation of the distribution between input and output bits indicates that the S-Box is strong against differential cryptanalysis. DP values of the proposed S-Boxes and some S-Boxes in the literature are given in Table 3. According to these values, the AES S-Box DP value has the best value. The DP value of the proposed S-Boxes seems to be better than most studies in the literature.

Linear Approximation Probability (LP) [61] is another criterion used to measure the linear cryptanalysis resistance of the S-Box. When the LP values in Table 3 are examined, the LP value of the proposed S-Box 1 and S-Box 2 is found as 0.132. It is seen that the LP value of the proposed

S-Boxes has a good value in the literature studies after the AES and Skipjack [62] algorithm S-Boxes. As a result, when all the performance test results in Table 3 are evaluated, it has been found that S-Boxes generated by the developed S-Box algorithm produce better results in many criteria compared to the literature. According to the test results, it has been shown that the proposed S-Boxes can be used for cryptographic application.

Table 3. The comparison table of S-Box.

S-Box	Nonlinearity			BIC-SAC	BIC-Nonlinearity	SAC			DP	LP
	Min	Avg	Max			Min	Avg	Max		
Proposed S-Box 1	104	106	110	0.5014	104.214	0.4375	0.5197	0.625	10	0.132
Proposed S-Box 2	106	106	108	0.5023	104.5	0.4218	0.5061	0.6406	10	0.132
[21]	95	102	107	0.5011	100.28	0.3906	0.5034	0.6250	12	0.136
[57]	98	104	108	0.5048	102.857	0.2812	0.4953	0.6093	12	0.140
[24]	102	104	108	0.5021	104.071	0.3906	0.5056	0.5937	12	0.125
[26]	100	103	106	0.5009	103.714	0.4218	0.5048	0.5937	10	0.125
[23]	104	106	108	0.49763	103.857	0.3906	0.5063	0.5937	12	0.164
[62]	104	105.7	108	0.4994	104.1	0.3986	0.5032	0.5938	12	0.109
[56]	112	112	112	0.5046	112	0.4531	0.5048	0.5625	4	0.062

5. Conclusions

A chaotic system with an infinite number of equilibrium points has been investigated in this work. Dynamics of the system have been discovered by using numerical simulations and circuital experiments. The system with infinite equilibrium displays attractive behaviour such as chaos and multistability. By using such a system, we have presented a new S-Box algorithm and proposed two S-Boxes. Different tests have been implemented to confirm the good performance of two S-Boxes, which are appropriate to cryptographic applications. The comparison of the proposed S-Boxes with some studies in the literature is presented. As a result of the comparison in the literature, it has been shown that the proposed S-Boxes have the best max, min and avg nonlinearity values after the AES algorithm and have good values in other criteria. We will apply such S-Boxes to develop a secure communication system for medical devices in our future works. In addition, constructing the fuzzy controller to stabilize the chaotic behavior of the system will be studied.

Author Contributions: Conceptualization, X.W.; Formal Analysis, X.W.; Investigation, A.A. and U.C.; Methodology, A.A. and V.-T.P.; Project Administration, X.Q.N.; Software, U.C. and V.-T.P.; Supervision, D.V.H.; Writing—Original Draft, D.V.K.; Writing—Review and Editing, X.Q.N.

Funding: The author Xiong Wang was supported by the National Natural Science Foundation of China (No. 61601306) and Shenzhen Overseas High Level Talent Peacock Project Fund (No. 20150215145C). Akif Akgul was supported by Sakarya University Scientific Research Projects Unit under Grants 2016-09-00-008, 2016-50-01-026.

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

References

1. Lorenz, E.N. Deterministic nonperiodic flow. *J. Atmos. Sci.* **1963**, *20*, 130–141. [CrossRef]
2. Rössler, O.E. An equation for continuous chaos. *Phys. Lett. A* **1976**, *57*, 397–398. [CrossRef]
3. Strogatz, S. *Nonlinear Dynamics and Chaos: With Applications to Physics, Biology, Chemistry, and Engineering*; Perseus Books: Cambridge, CA, USA, 1994.
4. Chen, G.; Yu, X. *Chaos Control: Theory and Applications*; Springer: Berlin/Heidelberg, Germany, 2003.
5. Sprott, J.C. *Elegant Chaos Algebraically Simple Chaotic Flows*; World Scientific: Singapore, 2010.
6. Sprott, J. Some simple chaotic flows. *Phys. Rev. E* **1994**, *50*, R647–R650. [CrossRef]
7. Chen, G.; Ueta, T. Yet another chaotic attractor. *Int. J. Bifurc. Chaos* **1999**, *9*, 1465–1466. [CrossRef]
8. Lü, J.H.; Chen, G.R. A new chaotic attractor coined. *Int. J. Bifurc. Chaos* **2002**, *12*, 659–661. [CrossRef]
9. Yang, Q.; Chen, G.; Zhou, T.S. A unified Lorenz-type system and its canonical form. *Int. J. Bifurc. Chaos* **2006**, *16*, 2855–2871. [CrossRef]

10. Yang, Q.; Chen, G.; Huang, K. Chaotic attractors of the conjugate Lorenz-type system. *Int. J. Bifurc. Chaos* **2007**, *17*, 3929–3949. [CrossRef]
11. Abooee, A.; Yaghini-Bonabi, H.A.; Jahed-Motlagh, M.R. Analysis and circuitry realization of a novel three-dimensional chaotic system. *Commun. Nonlinear Sci. Numer. Simul.* **2013**, *18*, 1235–1245. [CrossRef]
12. Cicek, S.; Ferikoglu, A.; Pehlivan, I. A new 3D chaotic system: Dynamical analysis, electronic circuit design, active control synchronization and chaotic masking communication application. *Optik* **2016**, *127*, 4024–4030. [CrossRef]
13. Dadras, S.; Momeni, H.R. A novel three-dimensional autonomous chaotic system generating two, three and four-scroll attractors. *Phys. Lett. A* **2009**, *60*, 3637–3642. [CrossRef]
14. Wang, X.; Chen, G. Constructing a chaotic system with any number of equilibria. *Nonlinear Dyn.* **2013**, *71*, 429–436. [CrossRef]
15. Jafari, S.; Sprott, J.C. Simple chaotic flows with a line equilibrium. *Chaos Solit. Fract.* **2013**, *57*, 79–84. [CrossRef]
16. Gotthans, T.; Petržela, J. New class of chaotic systems with circular equilibrium. *Nonlinear Dyns.* **2015**, *73*, 429–436. [CrossRef]
17. Gotthans, T.; Sprott, J.C.; Petržela, J. Simple chaotic flow with circle and square equilibrium. *Int. J. Bifurc. Chaos* **2016**, *26*, 1650137. [CrossRef]
18. El-Sayed, A.M.A.; Elsaid, A.; Nour, H.M.; Elsonbaty, A. Dynamical behavior, chaos control and synchronization of a memristor-based ADVP circuit. *Commun. Nonlinear Sci. Numer. Simul.* **2013**, *18*, 148–170. [CrossRef]
19. Chen, E.; Min, L.; Chen, G. Discrete chaotic systems with one-line equilibria and their application to image encryption. *Int. J. Bifurc. Chaos* **2017**, *27*, 1750046. [CrossRef]
20. Tang, G.; Liao, X.; Chen, Y. A method for designing dynamical S-boxes based on discretized chaotic map. *Chaos Solit. Fract.* **2005**, *23*, 1901–1909. [CrossRef]
21. Khan, M.; Shah, T.; Mahmood, H.; Gondal, M.A.; Hussain, I. A novel technique for the construction of strong S-boxes based on chaotic Lorenz systems. *Nonlinear Dyn.* **2012**, *70*, 2303–2311. [CrossRef]
22. Liu, H.; Kadir, A.; Niu, Y. Chaos-based color image block encryption scheme using S-box. *AEÜ Int. J. Electron. Commun.* **2014**, *68*, 676–686. [CrossRef]
23. Çavuşoğlu, Ü.; Kaçar, S.; Pehlivan, I.; Zengin, A. Secure image encryption algorithm design using a novel chaos based S-Box. *Chaos Solit. Fract.* **2017**, *95*, 92–101. [CrossRef]
24. Hussain, I.; Shah, T.; Gondal, M.A. A novel approach for designing substitution-boxes based on nonlinear chaotic algorithm. *Nonlinear Dyn.* **2012**, *70*, 1791–1794. [CrossRef]
25. Tang, G.; Liao, X.; Chen, Y. A novel method for designing S-boxes based on chaotic maps. *Chaos Solit. Fract.* **2005**, *23*, 413–419. [CrossRef]
26. Özkaynak, F.; Özer, A.B. A method for designing strong S-Boxes based on chaotic Lorenz system. *Phys. Lett. A* **2010**, *374*, 3733–3738. [CrossRef]
27. Çavuşoğlu, Ü.; Zengin, A.; Pehlivan, I.; Kaçar, S. A novel approach for strong S-Box generation algorithm design based on chaotic scaled Zhongtang system. *Nonlinear Dyn.* **2017**, *87*, 1081–1094. [CrossRef]
28. Ozkaynak, F.; Yavuz, S. Designing chaotic S-boxes based on time-delay chaotic system. *Nonlinear Dyn.* **2013**, *74*, 551–557. [CrossRef]
29. Katz, J.; Lindell, Y. *Introduction to Modern Cryptography*, 2nd ed.; CRC Press: Boca Raton, FL, USA, 2014.
30. Ferguson, N.; Schneier, B.; Kohno, T. *Cryptography Engineering: Design Principles and Practical Applications*, 1st ed.; Wiley: Hoboken, NJ, USA, 2011.
31. Stallings, W. *Cryptography and Network Security: Principles and Practice*, 7th ed.; Pearson: London, UK, 2016.
32. Schneier, B. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 20th ed.; Wiley: Hoboken, NJ, USA, 2017.
33. Zaibi, G.; Peyrard, F.; Kachouri, A.; Fournier-Prunaret, D.; Samet, M. Efficient and secure chaotic S-Box for wireless sensor network. *Secur. Commun. Netw.* **2014**, *7*, 279–292. [CrossRef]
34. Khan, M.; Shah, T. An efficient chaotic image encryption scheme. *Neural. Comput. Appl.* **2015**, *26*, 1137–1148. [CrossRef]
35. Batool, S.; Shah, T.; Khan, M. A color image watermarking scheme based on affine transformation and S_4 permutation. *Neural. Comput. Appl.* **2014**, *25*, 2037–2045. [CrossRef]
36. Khan, M.; Shah, T. A copyright protection using watermarking scheme based on nonlinear permutation and its quality metrics. *Neural. Comput. Appl.* **2015**, *26*, 845–855. [CrossRef]

37. Press, W.H.; Teukolsky, S.A.; Vetterling, W.T.; Flannery, B.P. *Numerical Recipes: The Art of Scientific Computing*, 3rd ed.; Cambridge University Press: Cambridge, UK, 2007.
38. Wolf, A.; Swift, J.B.; Swinney, H.L.; Vastano, J.A. Determining Lyapunov exponents from a time series. *Phys. D* **1985**, *16*, 285–317. [CrossRef]
39. Ngonghala, C.; Feudel, U.; Showalter, K. Extreme multistability in a chemical model system. *Phys. Rev. E* **2011**, *83*, 056206. [CrossRef] [PubMed]
40. Pisarchik, A.N.; Feudel, U. Control of multistability. *Phys. Rep.* **2014**, *540*, 167–218. [CrossRef]
41. Hens, C.; Dana, S.K.; Feudel, U. Extreme multistability: Attractors manipulation and robustness. *Chaos* **2015**, *25*, 053112. [CrossRef] [PubMed]
42. Lai, Q.; Hu, B.; Guan, Z.H.; Li, T.; Zheng, D.F.; Wu, Y.H. Multistability and bifurcation in a delayed neural network. *Neurocomputing* **2016**, *127*, 785–792. [CrossRef]
43. Guan, Z.H.; Lai, Q.; Chi, M.; Cheng, X.M.; Liu, F. Analysis of a new three-dimensional system with multiple chaotic attractors. *Nonlinear Dyn.* **2014**, *75*, 331–343. [CrossRef]
44. Kengne, J.; Njitacke, Z.T.; Fotsin, H.B. Dynamical analysis of a simple autonomous jerk system with multiple attractors. *Nonlinear Dyn.* **2016**, *83*, 751–766. [CrossRef]
45. Kengne, J.; Njitacke, Z.T.; Negou, A.N.; Tsostop, M.F.; Fotsin, H.B. Coexistence of multiple attractors and crisis route to chaos in a novel chaotic jerk circuit. *Int. J. Bifurc. Chaos* **2016**, *26*, 1650081. [CrossRef]
46. Fortuna, L.; Frasca, M.; Xibilia, M.G. *Chua's Circuit Implementation: Yesterday, Today and Tomorrow*; World Scientific: Singapore, 2009.
47. Wei, Z.C.; Pehlivan, I. Chaos, coexisting attractors, and circuit design of the generalized Sprott C system with only two stable equilibria. *Optoelectron. Adv. Mater. Rapid Commun.* **2012**, *6*, 742–745.
48. Amigo, J.; Kocarev, L.; Szczepanski, J. Theory and practice of chaotic cryptography. *Phys. Lett. A* **2007**, *366*, 211–216. [CrossRef]
49. Jakimoski, G.; Kocarev, L. Chaos and cryptography: Block encryption ciphers based on chaotic maps. *IEEE Trans. Circuits Syst. I Fund. Theory Appl.* **2001**, *48*, 163–169. [CrossRef]
50. Wang, Y.; Wong, K.W.; Liao, X.; Chen, G. A new chaos-based fast image encryption algorithm. *Appl. Soft Comput.* **2011**, *11*, 514–522. [CrossRef]
51. Hua, Z.; Zhou, Y. Image encryption using 2D Logistic-adjusted-Sine map. *Inf. Sci.* **2016**, *339*, 237–253. [CrossRef]
52. Wu, X.; Wang, D.; Kurths, J.; Kan, H. A novel lossless color image encryption scheme using 2D DWT and 6D hyperchaotic system. *Inf. Sci.* **2016**, *349*, 137–153. [CrossRef]
53. Wang, X.; Zhang, W.; Guo, W.; Zhang, J. Secure chaotic system with application to chaotic ciphers. *Inf. Sci.* **2013**, *221*, 555–570. [CrossRef]
54. Bakhache, B.; Ghazal, J.M.; El Assad, S. Improvement of the security of zigbee by a new chaotic algorithm. *IEEE Syst. J.* **2014**, *8*, 1024–1033. [CrossRef]
55. Çavuşoğlu, Ü.; Akgül, A.; Kaçar, S.; Pehlivan, I.; Zengin, A. A novel chaos-based encryption algorithm over TCP data packet for secure communication. *Secur. Commun. Netw.* **2016**, *9*, 1285–1296. [CrossRef]
56. Gladman, B. A specification for Rijndael, the AES algorithm. *at fp.gladman.plus.com/cryptography_technology/rijndael/aes.spec* **2001**, *311*, 18–19.
57. Khan, M.; Shah, T.; Gondal, M.A. An efficient technique for the construction of substitution box with chaotic partial differential equation. *Nonlinear Dyn.* **2013**, *73*, 1795–1801. [CrossRef]
58. Adams, C.; Tavares, S. The structured design of cryptographically good S-boxes. *J. Cryptol.* **1990**, *3*, 27–41. [CrossRef]
59. Webster, A.; Tavares, S.E. On the design of S-boxes. In *Conference on the Theory and Application of Cryptographic Techniques*; Springer: Berlin/Heidelberg, Germany, 1985; pp. 523–534.
60. Biham, E.; Shamir, A. Differential cryptanalysis of DES-like cryptosystems. In *Advances in Cryptology-CRYPTO*; Springer: Berlin/Heidelberg, Germany, 1991; Volume 90, pp. 2–21.
61. Matsui, M. Linear cryptanalysis method for DES cipher. In *Workshop on the Theory and Application of of Cryptographic Techniques*; Springer: Berlin/Heidelberg, Germany, 1993; pp. 386–397.
62. Brickell, E.F.; Denning, D.E.; Kent, S.T.; Maher, D.P.; Tuchman, W. SKIPJACK review: Interim report. In *Building in Big Brother*; Springer: New York, NY, USA, 1995; pp. 119–130.