DOI: 10.24996/ijs.2023.64.9.37

ISSN: 0067-2904

Novel Dynamic S-Box Based on Password Key and Circle Map

Ala'a Talib Khudhair[1], Ekhlas Khalaf Gbashi[2], Abeer Tariq Maolood[2]
[1] *Department of Computer Science, Al-Turath University College, Baghdad, Iraq*
[2] *Department of Computer Science, University of Technology, Baghdad, Iraq*

Received: 21/12/2021 Accepted: 10/11/2022 Published: 30/9/2023

Abstract

Many cryptosystems and security techniques use substitution boxes to ensure the data's secure communication. A new technique is presented for generating a robust S-box to fulfill security requirements. The AES algorithm represents a block cipher cryptographic algorithm. It was selected by the National Institute of Science and Technology as the optimal cryptographic algorithm in 2011. Through the study of the properties of original S-BOX, this algorithm has been subjected to a number of attacks (linear, differential, statistical, and interpolation), and original S-BOX has been static, which makes the attack strong and shows a weakness in the algorithm. It is necessary to make this algorithm more efficient and powerful through the improvement of the dynamic generation of the steps for the protection of textual data security. This paper proposes a dynamic S-Box based on the user's password key (8 chars), shifting, and a 1D circle map. The results in this work indicated that the suggested approach presents a secure S-BOX, which is considered to have 255 differences identified when 1 bit of the key is changed; therefore, about 99% of the S-Box has been changed. Also, an inverse table of S-Box (16*16) is generated via the S-Box output created from the above-mentioned suggestions for returning the values regarding the union of the column and the row for all the S-Box generated values. We examine the quality of our S-Box through various well-known performance parameters. All of the analysis yields very encouraging results, certifying that the generated S-box meets all criteria that are required for reliable and secure encryption. Just a few milliseconds are needed to implement it.

Keywords: substitution boxes**,** password key, 1D Circle map, encryption.

طريقة صندوق أس جديدة بالاعتماد على كلمة المرور وخريطة الدائرة

الاء طالب خضير [1] ، اخلاص خلف كباشي[2]، عبير طارق مولود[2]
[1] قسم علوم الحاسوب، كلية التراث الجامعة، بغداد، العراق
[2] قسم علوم الحاسوب، الجامعة التكنولوجية، بغداد، العراق

الخلاصة

تستعمل العديد من أنظمة التشفير وتقنيات الأمان المربعات البديلة لضمان الاتصال الآمن للبيانات. للوفاء بمتطلبات الأمان ، نقدم تقنية جديدة لإنشاء صندوق S قوي. تعد خوارزمية AES إحدى خوارزميات تشفير الكتلة .تم اختياره كأفضل خوارزمية تشفير من قبل المعهد الوطني للعلوم والتكنولوجيا في عام 2011. من خلال دراسة خصائص S-BOX الأصلية ، تعرضت الخوارزمية لعدة هجمات (تفاضلية ، خطية ، استيفاء وهجوم

*Email: alaa.talib@turath.edu.iq

إحصائي) والأصلية كان S–BOX ثابتًا وهذه نقطة قوة للهجوم وضعف في الخوارزمية .لذلك من الضروري جعل الخوارزمية أكثر قوة وكفاءة من خلال تحسين التوليد الديناميكي لحماية أمن البيانات النصية. في هذا البحث ، اقترح S–Box الديناميكي بناءً على مفتاح كلمة المرور (8 أحرف) الذي يتم ادخاله من قبل المستخدم، و shifting وخريطة الدائرة 1D.أشارت النتائج في هذا العمل إلى أن النهج المقترح يقدم S–BOX آمنًا ، تم تغيير حوالي 99٪ من قيم الS–Box عند تغيير بت واحد من المفتاح ، يتم إنشاء جدول عكسي لـ S–Box (16 * 16)عبر إخراج S–Box الذي تم إنشاؤه من الاقتراحات المذكورة أعلاه لإرجاع القيم المتعلقة باتحاد العمود والصف لجميع قيم S–Box التي تم إنشاؤها . نقوم بفحص جودة S–Box من خلال العديد من معايير الأداء المعروفة. نحصل على نتائج مشجعة للغاية من جميع التحليلات التي تشهد أن S–box الذي تم إنشاؤه يفي بجميع المعايير اللازمة ليكون موثوقًا به للتشفير الآمن. فقط ملي ثانية ، هو الوقت اللازم لتنفيذه.

1. Introduction

Many parties use cryptography systems to communicate securely. A block cipher helps to accomplish information privacy, which is one of the objectives of cryptography. Text information has a massive impact on all aspects, both in public and in personal life. Because of the increases in the utilization of intrusive programs in the past few years, there is a necessity for improving the algorithms, due to the fact that the majority of modern encryption algorithms have been exposed to consecutive attacks [1]. It is one of the most widely utilized tools for ensuring the security of information. Many block ciphers rely on permutation and substitution or the Feistel structure [2]. The circle map has the ability to show these behaviors as mode and phase locking, sub-harmonics, and period doubling [3]. With regard to the field of cryptography and all of the symmetric cryptographic algorithms, the S-Box is considered a nonlinear unit regarding the encryption algorithms, typically because of the associations between the cipher and the key, which is referred to as “confusion.” The key purpose of this study is to use chaos theory for the generation of the random S-BOX and password keys for updating all of the values in the state to the generated S-BOX [4].

1.2 Literature Survey

1- In 2011, Jolfaei and Mirghadri [5]: The chaos is utilized for expanding confusion and diffusion in images due to the fact that it is sensitive to initial conditions. Barker's maps have been utilized for designing dynamic maps of permutations and S-boxes. The suggested algorithm has been measured via a series of tests, which include visual tests, randomization testing, graph analyses, coding quality, information interruptions, and correlation analyses. Results have been quite good for ten rounds and a 128-bit data block.

2- In 2015, Abulgader, Ismail, idbeaa, and Zainal [6]: have suggested an approach for overcoming the weaknesses in the S-BOX and improving AES performance through the replacement of the Mix phase with a chaotic system, the process of the XOR, for the reduction of the high computational costs of the Mix column, and the generation of the S-box based upon the chaotic system. Results have shown that the suggested approach was successful in generating an efficiently encrypted image that has very low coefficients of correlation between neighboring pixels and provides high operation speed.

3- In 2015 (Abulgader et al.) [7], an approach for overcoming S-BOX drawbacks and improving AES performance was proposed by replacing the Mix phase with a chaotic system in which the XOR process resulted in the reduction of high calculations in the Mix column and the generation of the S-box based on the chaotic system. Results have shown that the suggested approach enabled the generation of an efficiently encrypted image with very low coefficients of correlation between adjacent pixels and provided high operation speed.

4- In 2016, Alabaichi [8] concentrated on the encryption of colored images using 3D Chebyshev maps to generate secret keys for image diffusion and 2D Arnold Cat maps to generate S-box using the XOR function with old S-box. The suggested algorithm has been tested with the use of the UACI, NPCR, and information entropy. Results have shown that the algorithm has the ability to resist different kinds of attacks.

5. A study by Kamel and Farhan (2017) [9]: created a new block cipher as a moving structure based on two of the proposed algorithms. The first algorithm utilized complementary DNA functions (shift and two S-box layers). In the second algorithm, it included the degree of shift and addition of the DNA. In engine implementation, it resulted in the generation of a secret key using a chaotic generator agreed upon by sender and receiver, and text was encrypted using multiple measurements and the NIST's five statistical analyses, where the benefits of all tests outweighed their low efficiency.

2. Circle map

Circle maps can be defined as mapping examples showing various significant factors in complex dynamical behavior. They have the ability to show these behaviors as mode and phase locking, sub-harmonics, quasi periodicity, and period doubling, along with routes to chaos through recurrent disruption to quasi periodicity or period doubling. In particular, it is adequate for studying and generating sustained undamped sounds when the possible iterations' space is confined by the map to functions regarding such nature through constructions [10].

2.1 Iterated Maps from Circle to Itself

The most generalized circle map type is:

$$y_{n+1} = \phi(y_n) \quad (1)$$

The mapping from bounded intervals to identical bounded intervals is represented by Φ. Commonly, the unit interval is taken and indicated as Φ: [0; 1)   [0; 1), that otherwise might be considered to be periodically-closed. Also, it is done through taking quotient regarding real numbers via integers, and repeat the real's in interval [0; 1), then indicated Φ: R/Z   R/Z (Milnor's 2006, p161). Topologically, one can also say that Φ maps points on circle back onto circle. In the case of wanting to model an excellent sinusoidal oscillator that has been perturbed via a certain coupled nonlinear function, which becomes:

$$y_{n+1} = \left(y_n + \Omega - \frac{\mathrm{k}}{2\pi} f(y_n)\right) mod\ 1 \quad (2)$$

In which, Ω represents a constant which is considered as a fixed angular progress with regard to a sinusoidal oscillator, while k represents the strength of the coupling that is related to the nonlinear perturbation f (.). Y0 represents the starting phase. The option of f (.) is extremely flexible, whereas discontinuous functions' examples are identified in smooth cases and literature as the smooth cases. The canonical theoretical example has been represented by the standard circle map: [11]

$$y_{n+1} = \left(y_n + \Omega - \frac{\mathrm{k}}{2\pi} sin(2\pi y_n)\right) mod\ 1 \quad (3)$$

For studying the long term behavior regarding the iterated map Φ(.), one might consider the winding number

$$W = \lim_{n\to\infty} \frac{y_n - y_0}{n} \quad (4)$$

Which measures average angle that is added in long-term. In the case when such an added angle that has been notated over a [0; 1) interval represents a rational value p/q with p; q Ɛ N, after that following q iterations, one will have some recurrence; thus, this map will be periodical. In addition, the irrational winding values have been referred to as "quasi-periodic," which of course is the frequency that is associated with an unperturbed oscillator and assessed as ΦΩ = ΩS where S represents the rate of sampling, or time interval between 2 of the time steps for ΩƐ [0; 0.50]. In the case when Ω is greater than 0:5, one can get aliasing, and the effective frequency will be reduced once more, with the opposite sign of the phase, as shown in Figure 1. [12]

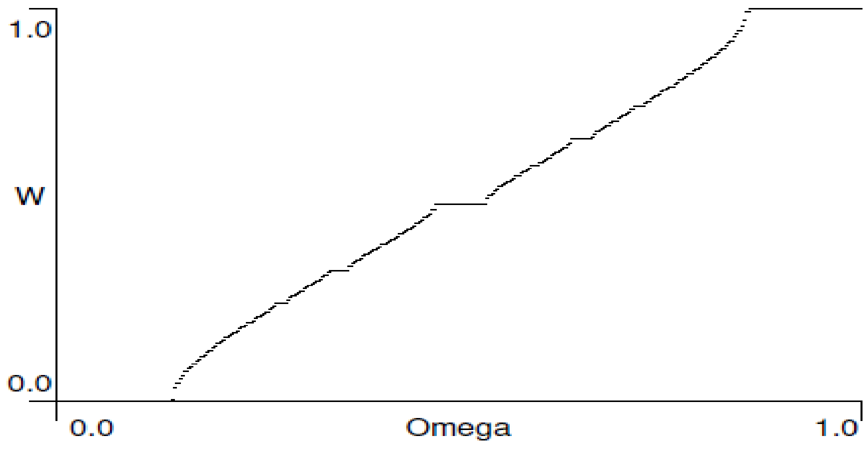
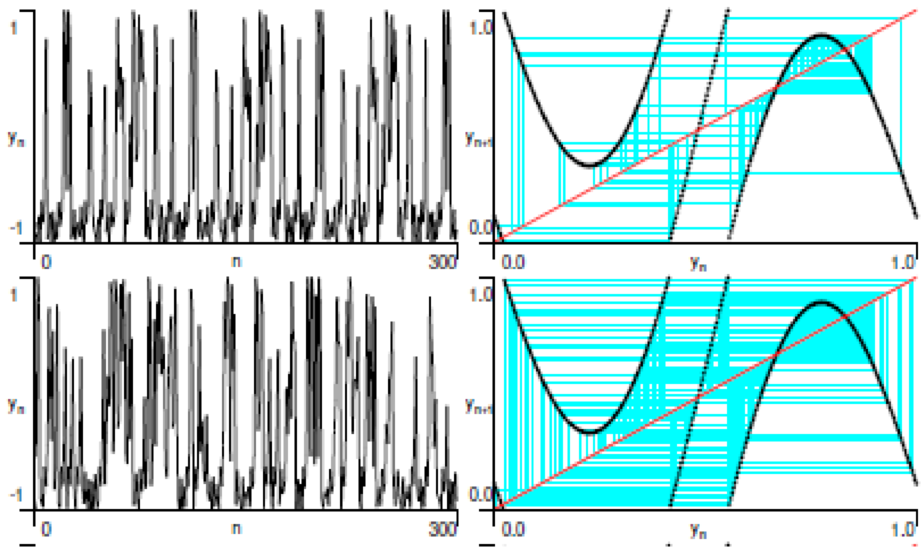


Figure 1: Devil's staircase rendered numerically for the standard circle map.

2.2 Relation to the Other Maps

Some of the maps that have been mentioned in the literature include circle maps. For instance, Di Scipio had considered the term that he had referred to as "sine map" (Di Scipio 1999): [13]

$$y_{n+1} = (sin(2\pi y_n)\,) \tag{5}$$



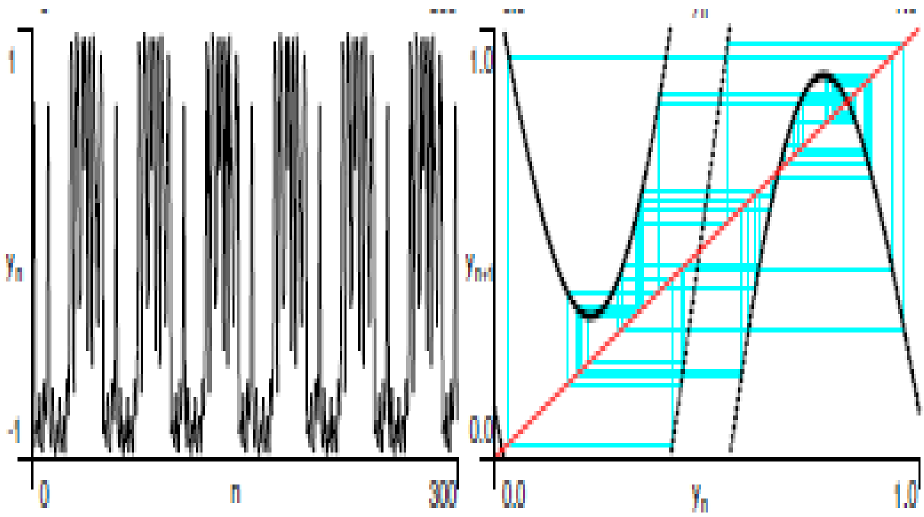


Figure 2: Sensitivity to the start position of the iteration *yo* at *k* =6*:*4, Ω = 0*:*11, 2 orbits (top and bottom) are stable, 1 (center) is chaotic. All of the orbits are nonsingular.

where r represents the constant of scaling and can be defined as a reduced standard circle map form (3) with linear oscillator frequency Ω that has been removed and linear self-increment disregarded. Manzoli et al. have considered the variations of the standard map (Katok & Hasselblatt 1995; Libchaber & Glazier 1988) as shown in Figure 2: [14]

$$y_{n+1} = \left(y_i + \Omega - \frac{\mathrm{k}}{2\pi} sin(2\pi y_i) + \in x_i\right) \quad (6)$$

$$x_{n+1} = \left(\in x_i - \frac{\mathrm{k}}{2\pi} sin(2\pi y_i)\right) \quad (7)$$

3. Proposed Dynamic S-Box

The phases to generate an INV S-Box and a new S-Box might be indicated as follows:

3.1 S-Box Generation

Because of the encryption algorithm's repeated exposure attacks, there is a requirement to reinforce the algorithms to be steadfast against all attacks [15]. The algorithm is going to be enhanced via a dynamic S-Box as follows:

Step 1: Enter the password key (8 characters) and expand it to 64 characters by converting the ASCII code for each character in the password key to binary and then generating a random number using the circle map. The method of generating random numbers is that the user must select the number of rounds (number of i) through the generation of a circle map. Suppose the user selects the number of rounds as "22." Now cut 8 numbers after the comma. In this case, a new word was generated, which will be the new password key, and the same operation as in step 1 was repeated until 64 characters were generated. The circle map equation is utilized for generating the random numbers:

$$\theta_{n+1} = \theta_n + \Omega - k/2\pi * \sin(2\pi\theta_n) \quad (8)\ [16]$$

where θ value lies between 0 and 1. It has 2 parameters, which are, coupling strength K and driving phase Ω. As model for the phase-locked loops, Ω could be interpreted as driving frequency. For K = 0 and Ω irrational [17].

Step 2: Generating 512 numbers from the password key (64 char), which is converted to binary (512 bit), taking the first 16 bits from 512 bits and converting them into integers, shifting the 16 bits to the left 15 times for another 15 integer numbers, and so on until the last 16 bits. Note: If the number of shifts = 9, then the number of shifts = 0.

Step 3: Remove duplicate numbers and fill it with the remaining numbers between [0, 255]. Then generate a 2D matrix containing 256 random numbers.

Step 4: Apply the IP (Initial Permutation) of the DES algorithm [18].

3.2 INV S-Box Generation

The inverse table S-box has been invoked by returning row and column values for every number.

3.3 Example of S-box Generation

1. The first step is to perform a 1D circle map, where θ = 0.5, Ω = 0.33, k = 0.8 and π = 3.14. The result has been listed in Table 1.

Table 1: result of 1D Circle Map

Number of i (rounds)	Result
Where i=1	0.827999627936893
Where i=2	2.26771418897304
Where i=3	1.34851071264342
Where i=4	0.652401024432296
Where i=5	2.00804338335345
Where i=6	2.28261924407415
Where i=7	1.38108050060487
Where i=8	0.853479870990219
Where i=9	2.18528509236707
Where i=10	1.36517931970788
…..	……

2. Expansion password key. Suppose the initial password key is "**computer**". The result of expansion is shown in Table 2.

Table 2: result of expansion password key

Password key	No. of round	Random NO. from circle map	New password key
computer	3	34851071	lِmƒ؛t9ت
lِmƒ؛t9ت	10	36517931	چغkءu:Yœ
چغkءu:Yœ	15	31617665	±ي-àêèeن
±ي-àêèeن	17	74806329	cق-à«Yr
cق-à«Yr	25	16261409	±{kƒصرY9
±{kƒصرY9	28	32386514	6قmƒWژ¬“
6قmƒWژ¬“	29	52659266	±·µ«£²N

Final result is (computer lِmƒ؛tچغ 9تkءu:Yœ±ي-êèeن cق-à«Yr±{kƒصرY96قmƒWژ¬“±·µ«£²N)

3. Convert final result to binary (512 bits), take first 16 bits "0110001101101111"
0110001101101111 = 25455 mod 256 = 111
1100011011011110 = 50910 mod 256 = 222
1000110110111101 = 36285 mod 256 = 189
0001101101111011 = 7035 mod 256 = 123
0011011011110110 = 14070 mod 256 = 246
0110110111101100 = 28140 mod 256 = 236
1101101111011000 = 56280 mod 256 = 216
1011011110110001 = 47025 mod 256 = 177
0110111101100011 = 28515 mod 256 = 99
1101111011000110 = 57030 mod 256 = 198
1011110110001101 = 48525 mod 256 = 141
0111101100011011 = 31515 mod 256 = 27
1111011000110110 = 63030 mod 256 = 54
1110110001101101 = 60525 mod 256 = 109
1101100011011011 = 55515 mod 256 = 219
1011000110110111 = 45495 mod 256 = 183
The same operation for the second 16 bits and so on until the last 16 bits. The resulted 2D matrix contains 256 random numbers.

4. Remove duplicate numbers and fill it with the remaining numbers between [0,255] as shown in Table 3.

Table 3: Generate 16 Numbers from 16 Bits by Shift and Rotates after remove duplicate

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

5. Divide the s-box into four parts, each with 64 values, and apply the DES algorithm's IP (initial permutation) to each part [19]. The result is shown in Table 4.

Table 4: Update Values by IP of DES algorithm

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

6. The final result of the S-box is shown in Table 5, and the S-Box Inverse has been shown in Table 6 after converting the values in Table 4 to HEX.

Table 5: Dynamic S-Box

D9	4C	57	47	D7	E0	C6	DE	66	32	BA	1D	5C	83	1B	7B
9B	CA	E4	75	74	0D	6D	EC	67	2B	93	D5	D1	B5	B7	B1
B9	26	AB	A3	6B	70	63	6F	B3	99	5D	8E	AE	C1	8D	BD
CD	65	72	3A	B8	06	36	F6	6C	95	C9	EA	E8	DA	DB	D8
C7	38	AF	76	1C	73	4B	9E	1E	C5	BC	82	DC	CE	2E	B6
15	2C	F0	0B	E3	E5	A7	60	AD	CC	A9	2D	DD	28	9D	D2
33	53	5A	BB	51	39	A5	CF	8F	E2	5E	ED	6E	E7	97	3D
0A	8B	78	05	71	9C	D3	B0	56	59	D4	16	37	94	4E	E9
22	12	07	24	EE	3B	79	C8	2A	14	09	A8	17	AC	F3	23
34	1A	0E	01	27	92	98	8C	3C	20	10	03	EB	96	F7	CB
21	11	04	D6	B2	EF	2F	5B	29	13	08	49	62	6A	F2	91
30	18	0C	00	64	58	E6	46	35	1F	0F	02	F1	25	31	19
F9	C3	A4	89	7F	61	4A	3F	FB	D0	AA	90	81	69	4F	41
FD	E1	BE	9F	85	7A	52	43	FF	F5	C0	A1	87	7D	55	45
F8	C2	A2	88	7E	5F	48	3E	FA	C4	A6	8A	80	68	4D	40
FC	DF	B4	9A	84	77	50	42	FE	F4	BF	A0	86	7C	54	44

Table 6: Dynamic S-Box Inverse

B3	93	BB	9B	A2	73	35	82	AA	8A	70	53	B2	15	92	BA
9A	A1	81	A9	89	50	7B	8C	B1	BF	91	0E	44	0B	48	B9
99	A0	80	8F	83	BD	21	94	5D	A8	88	19	51	5B	4E	A6
B0	BE	09	60	90	B8	36	7C	41	65	33	85	98	6F	E7	C7
EF	CF	F7	D7	FF	DF	B7	03	E6	AB	C6	46	01	EE	7E	CE
F6	64	D6	61	FE	DE	78	02	B5	79	62	A7	0C	2A	6A	E5
57	C5	AC	26	B4	31	08	18	ED	CD	AD	24	38	16	6C	27
25	74	32	45	14	13	43	F5	72	86	D5	0F	FD	DD	E4	C4
EC	CC	4B	0D	F4	D4	FC	DC	E3	C3	EB	71	97	2E	2B	68
CB	AF	95	1A	7D	39	9D	6E	96	29	F3	10	75	5E	47	D3
FB	DB	E2	23	C2	66	EA	56	8B	5A	CA	22	8D	58	2C	42
77	1F	A4	28	F2	1D	4F	1E	34	20	0A	63	4A	2F	D2	FA
DA	2D	E1	C1	E9	49	06	40	87	3A	11	9F	59	30	4D	67
C9	1C	5F	76	7A	1B	A3	04	3F	00	3D	3E	4C	5C	07	F1
05	D1	69	54	12	55	B6	6D	3C	7F	3B	9C	17	6B	84	A5
52	BC	AE	8E	F9	D9	37	9E	E0	C0	E8	C8	F0	D0	F8	D8

4. Experimental Results

The proposed new S-BOX is going to be put to the test against many standard statistical parameters.

4.1 Avalanche Criteria (AC)

Changing the input amount will totally impact the amount of output when the avalanche value ranges from [0, 1], and assessed from equation:

$$\text{Avalanche Effect} = \frac{No.\ of\ Flipped\ bits\ in\ (o/p) cipher\ text}{No.\ of\ All\ bits\ in (o/p) cipher\ text} \quad (9)[20]$$

Note the signification differences between the outputs of Tables 5 and 6 when changing just one character in the password key until the difference reaches 99% using the equation.
Avalanche effect= 254/256 = 0.99

4.2 Complexity

Through the generated results, one can identify the S-Box complexity, in which the expansion phase regarding the password key is extremely complex since it is going to depend on equation (8) of the circle map. For instance, when changing just one character in the password key and using the same value parameters, the S-BOX results in a different percentage of 99%, as shown in Tables 7 and 8.

Table 7: Dynamic S-Box when password key is "Bomputer"

B9	**93**	**D5**	**D1**	**DA**	**E0**	**84**	**DE**	**EC**	**99**	**57**	**47**	**6B**	**83**	**13**	**7A**
B2	65	BA	1D	AE	0D	4D	E8	92	95	E4	75	B8	36	37	A1
2B	C9	EA	74	6D	70	42	6F	F6	4C	AB	A3	B5	C1	09	BD
D9	32	5D	8E	D7	06	26	F4	64	CA	72	3A	5C	1B	9B	D0
C5	78	05	1C	73	4B	B6	48	2C	D4	16	C2	CE	2E	D8	23
B3	53	5A	3B	E5	A7	60	1E	CC	71	5E	ED	28	9D	D2	7B
E2	BC	82	51	39	A5	DB	24	8B	F0	0B	61	E7	97	6C	91
59	A9	2D	27	9C	D3	B0	8F	66	38	AF	76	94	4E	E9	3D
14	03	D6	17	6A	46	0F	67	1A	07	DC	C4	58	19	15	69
20	0C	A8	12	63	2F	AD	90	29	10	01	E3	25	F2	B7	43
11	02	EB	96	85	C8	87	33	18	04	6E	F1	AC	8C	0A	B4
1F	08	86	89	B1	CB	56	A4	22	0E	00	49	C7	79	5B	21
F9	E1	BF	9E	7F	55	41	30	FB	EE	C3	A0	81	62	45	34
FD	F3	CD	A6	8A	77	4F	3C	FF	F7	DD	BB	98	7D	52	3F
F8	DF	BE	9A	7E	54	40	2A	FA	E6	C0	9F	80	5F	44	31
FC	EF	C6	A2	88	68	4A	35	FE	F5	CF	AA	8D	7C	50	3E

Table 8: Dynamic S-Box Inverse when password key is "Bomputer"

BA	**9A**	**A1**	**81**	**A9**	**42**	**35**	**89**	**B1**	**2E**	**AE**	**6A**	**91**	**15**	**B9**	**86**
99	A0	93	0E	80	8E	4A	83	A8	8D	88	3D	43	13	57	B0
90	BF	B8	4F	67	9C	36	73	5C	98	E7	20	48	72	4D	95
C7	EF	31	A7	CF	F7	1D	1E	79	64	3B	53	D7	7F	FF	DF
E6	C6	26	9F	EE	CE	85	0B	47	BB	F6	45	29	16	7D	D6
FE	63	DE	51	E5	C5	B6	0A	8C	70	52	BE	3C	32	5A	ED
56	6B	CD	94	38	11	78	87	F5	8F	84	0C	6E	24	AA	27
25	59	3A	44	23	1B	7B	D5	41	BD	0F	5F	FD	DD	E4	C4
EC	CC	62	0D	06	A4	B2	A6	F4	B3	D4	68	AD	FC	33	77
97	6F	18	01	7C	19	A3	6D	DC	09	E3	3E	74	5D	C3	EB
CB	1F	F3	2B	B7	65	D3	55	92	71	FB	2A	AC	96	14	7A
76	B4	10	50	AF	2C	46	9E	1C	00	12	DB	61	2F	E2	C2
EA	2D	4B	CA	8B	40	F2	BC	A5	21	39	B5	58	D2	4C	FA
3F	03	5E	75	49	02	82	34	4E	30	04	66	8A	DA	07	E1
05	C1	60	9B	1A	54	E9	6C	17	7E	22	A2	08	5B	C9	F1
69	AB	9D	D1	37	F9	28	D9	E0	C0	E8	C8	F0	D0	F8	D8

4.3 Time

For implementation, the time is small and requires only a few milliseconds, as listed in Table 9.

Table 9: Results of execution time

Password key	S-BOX Execution time
computer	0.103 millisecond
Bomputer	0.105 millisecond

4.4 Non-linearity

S :{0,1}x →{0,1}y has been defined as least value of non-linearity of all of the non-zero linear combinations of x Boolean functions fi : {0,1}→{0,1}, i= x-1,…,1,0. The non-linearity of the S-box has to be high in order for it to resist the linear cryptanalysis.

4.5 comparisons with previous work

s-box	Nonlinearity			SAC	BIC-NL	BIC-SAC	DU	LP	time
	Min	Max	Avg.						
Proposed s-box	100	110	106.75	0.5002	104	0.4988	30	0.125	0.103
Previous work [9]	104	108	105.75	0.4927	98	0.5052	10	0.1328	0.115

5. Conclusions

In this work, S-Box was developed on the basis of a password key, a circle map, and shifting. The results of this study show that changing 1 byte in the password key without changing the circle map parameters will change the password expansion process, which affects S-Box output. This refers to S-Box generation complexity. The major point is that a dynamic S-Box isn't static, yet it is based on the input, indicating that the security was generated during the generation. Using IP in this proposal contributed to increased randomness, which led to an increase in diffusion and confusion.

References:

[1] A. A. Abd El-Latif, B. Abd-El-Atty, and S. E. Venegas-Andraca, "A novel image steganography technique based on quantum substitution boxes," *Optics & Laser Technology*, vol. 116, pp. 92-102, 2019.

[2] F. Özkaynak, "On the effect of chaotic system in performance characteristics of chaos based s- box designs," *Physica A: Statistical Mechanics and its Applications*, vol. 550, 2020.

[3] D. Lambić, "A novel method of S-box design based on chaotic map and composition method," *Chaos, Solitons & Fractals*, vol. 58, pp. 16-21, 2014/01/01, 2014.

[4] A. Belazi, A. A. Abd El-Latif, A.-V. Diaconu, R. Rhouma, and S. Belghith, "Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms," *Optics and Lasers in Engineering*, vol. 88, pp. 37-50, 2017.

[5] Alireza Jolfaei, Abdolrasoul Mirghadri, "Image Encryption Using Chaos and Block Cipher," *Computer and Information Science*, vol. 4, no. 1, pp. 172-185, 2011.

[6] Ali Abdulgader. Mahamod Ismail, Nasharuddin Zainal, Tarik Idbeaa, "Enhancement of AES Algorithm based on Chaotic Maps and Shift Operation for Image Encryption," *Journal of Theoretical and Applied Information Technology*, vol. 71, no. 1, pp. 1817-3195, 10th January 2015.

[7] Ashwaq Mahmood Alabaichi, "Color Image Encryption using 3D Chaotic Map with AES key Dependent S-Box," *IJCSNS International Journal of Computer Science and Network Security*, vol. 16, no. 10, 2016.

[8] Abdulgader, Ismail, Zainal and Idbeaa, "Enhancement of AES Algorithm Based on Chaotic Map and Shift Operation for Image Encryption," *Journal of Theoretical and Applied Information Technology*, vol. 71, no. 1, 10th January 2015.

[9] Kamel Sh. H. And Farhan A. K., "Proposal Dynamic Block Cipher Structure Depend on Secret Map," *Department Computer Sciences, University of Technology*, 2017.

[10] Q. Lu, C. Zhu, and X. Deng, "An Efficient Image Encryption Scheme Based on the LSS Chaotic Map and Single S-Box," *IEEE Access*, vol. 8, pp. 25664-25678, 2020.

[11] D. Lambić, "A novel method of S-box design based on discrete chaotic map," Nonlinear Dynamics, vol. 87, no.4, pp. 2407-2413, 2017/03/01, 2017.

[12] A. Belazi and A. A. A. El-Latif, "A simple yet efficient S-box method based on chaotic sine map," *Optik*, vol.130, pp. 1438-1444, 2017.

[13] A. Belazi, M. Khan, A. A. A. El-Latif, and S. Belghith, "Efficient cryptosystem approaches: S-boxes and permutation–substitution-based encryption," *Nonlinear Dynamics*, vol. 87, no. 1, pp. 337-361, 2017/01/01 2017.

[14] M. Khan and Z. Asghar, "A novel construction of substitution box for image encryption applications with Gingerbreadman chaotic map and S8 permutation," *Neural Computing and Applications*, vol. 29, no. 4, pp. 993-999, 2016.

[15] A. H. Zahid and M. J. Arshad, "An Innovative Design of Substitution-Boxes Using Cubic Polynomial Mapping," *Symmetry*, vol. 11, no. 3, Art. no. 437, 2019.

[16] X. Wang, A. Akgul, U. Cavusoglu, V.-T. Pham, D. Vo Hoang, and X. Nguyen, "A Chaotic System with Infinite Equilibria and Its S-Box Constructing Application, "*Applied Sciences,* vol. 8, no. 11, 2018.

[17] L. Liu, Y. Zhang, and X. Wang, "A Novel Method for Constructing the S-Box Based on Spatiotemporal Chaotic Dynamics," *Applied Sciences*, vol. 8, no. 12, 2018.

[18] E. Al Solami, M. Ahmad, C. Volos, M. Doja, and M. Beg, "A New Hyperchaotic System-Based Design for Efficient Bijective Substitution-Boxes," *Entropy,* vol. 20, no. 7, 2018.

[19] A. Razaq et al., "A Novel Method for Generation of Strong Substitution-Boxes Based on Coset Graphs and Symmetric Groups," *IEEE Access,* vol. 8, pp. 75473-75490, 2020.

[20] S. S. Jamal, A. Anees, M. Ahmad, M. F. Khan, and I. Hussain, "Construction of Cryptographic S-Boxes Based on Mobius Transformation and Chaotic Tent-Sine System," *IEEE Access*, vol. 7, pp. 173273-173285, 2019.