A Quantum Dynamical Map in the Creation of Optimized Chaotic S-Boxes

Nafiseh Hematpour, Sodeif Ahadpour, and Sohrab Behnia

Abstract The substitution boxes are an open challenge due to not meeting the theoretical criteria of a good S-box. Recently, the use of chaos in the design of efficient S-boxes was proposed. In this article, after introducing a new quantum system, we examine its effect on the formation of chaotic S-boxes. We compare the proposed quantum chaotic map with previous results. Also, in the previous work, the PSO algorithm was improved with the help of the classical map and then used in the optimization of chaotic S-boxes. We are using and improving the performance of PSO in generating the S-box, by the introduced quantum chaotic map. Then, by changing the type of optimization, we examine its effects. For the first time, the harmony search algorithm is improved by the said quantum map, and then we use it to optimize the produced chaotic S-box. By examining the performance of generated S-boxes by common attacks such as nonlinearity, BIC, SAC, LP, and DP. The results for the improved harmony search algorithm is better.

Keywords Quantum dynamical map · Substitution box (S-box) · Harmony search algorithm · Particle swarm optimization (PSO) · Nonlinearity

1 Introduction

Many researchers in recent decades, to achieve higher security, have combined the two fields of chaos and cryptography under the heading of chaotic-based cryptography [1–4]. Due to their many applications, quantum dots are one of the favorite topics of researchers. So far, quantum dots have been used in solar cells [5], diodes

N. Hematpour (✉) · S. Ahadpour
University of Mohaghegh Ardabili, Ardabil, Iran
e-mail: n_hematpour@uma.ac.ir

S. Ahadpour
e-mail: ahadpour@uma.ac.ir

S. Behnia
Department of Physics, Urmia University of Technology, Urmia, Iran
e-mail: s.behnia@sci.uut.ac.ir

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_16

[6], medical imaging [7], and quantum computing [8]. When quantum dots are paired with other quantum dots or external fields, They have a long periodicity, making them suitable for use in cryptography. The National Institute of Standards and Technology (NIST) proposed the Data Encryption Standard (DES) for the encryption and decryption process in 1977 [9], which was replaced by the AES symmetric-key algorithm in 2001 [10]. S-box, which performs confusion, has been widely employed in traditional cryptographic standards such as DES and AES. Making efficient boxes is a major issue for security experts. Recently, some S-box algorithms based on the chaotic map have been proposed [11–14]. Then optimization algorithms are used to improve the performance of chaotic S-boxes [11, 15, 16]. All optimizers require a fitness function, which [11] shown to use nonlinearity fitness for better results. In this reference, classical maps are proposed to improve the performance of the PSO algorithm. Considering the theoretical criteria of a good S-box, there is a need to form new S-boxes.

In this work, a quantum map is replaced by a classical map. Also, the harmony search algorithm is replaced with the PSO algorithm to investigate the effect of the type of optimization.

The paper continues as follows: In Sect. 2, preliminary is proposed that includes the introduction of quantum dots and the study of their behavior. In Sect. 3, S-box criteria are presented. Sections 4 includes the algorithm for creating improved PSO and optimized S-box. Improved HS and optimized S-box is offered in Sect. 5. Section 6 provides an analysis of the performance of the S-boxes. Finally, a conclusion is proposed.

2 Preliminary

We introduce a generalized Dicke model presenting a new quantum chaotic map. It also investigates the chaos of this created system.

2.1 The Maps of Generalized Dicke Model

The dynamical system governed by a generalized Dicke Hamiltonian form is constructed as follows:

$$H = a^{\dagger}a + \omega_A J_z + \frac{\gamma}{\sqrt{N}}(a^{\dagger} + a)(J_- + J_+) + \frac{\gamma}{\sqrt{N}}V(J_-, J_+)$$
$$\Sigma_n \delta(t - nT). \tag{1}$$

In fact, we consider delta function added to Dicke Hamiltonian. where, a and $a^{\dagger}$ are respectively bosonic annihilation and creation operators. The parameter $\hbar\tilde{\omega}_A$ denotes the energy separation of N two-level atoms [17]. We assume that $\hbar = 1, \omega_A =$

$\tilde{\omega}_A/\tilde{\omega}_f \geq 0$, and $\tilde{\omega}_f$ is the field of frequency. $\gamma = \tilde{\gamma}/\tilde{\omega}_f$ is the coupling parameter. Furthermore, J_z and $J_\pm$ are the atomic relative population operator and the atomic transition operator, respectively [18]. In [12], we introduced a chaotic mapping based on this Hamiltonian.

$$< J_{+(n+1)} >= \alpha \left(< J_{+(n)} > - < J_{-(n)} J_{+(n)} > \right). \tag{2}$$

According to previous studies for quantum systems [19], here in the same way map with quantum corrections for a system of coupled quantum dots is extracted. To appear the effect of the quantum correlations using $J_+ =< J_+ > +\delta J_+$ and $J_- =< J_- > +\delta J_-$, we have:

$$\begin{aligned} < J_{+(n+1)} > = r \left(< J_{+(n)} > - < J_{-(n)} >< J_{+(n)} > \right) \\ - r < \delta J_- \delta J_+ > . \end{aligned} \tag{3}$$

Taking time derivation of $(\delta J_+ \delta J_-)$ implies

$$\frac{d}{dt}(\delta J_+ \delta J_-) = \delta \dot{J}_+ \delta J_- + \delta J_+ \delta \dot{J}_-. \tag{4}$$

Next, by applying $< \delta J_+(nT)\delta J_-(nT) >= y_n$, $< \delta J_+ \delta J_+ >= z_n$, $< J_+(nT) >= x_n$, we obtain (see Appendix 1):

$$\begin{cases} X_{n+1} = r(x_n - x_n^2) - r y_n \\ Y_{n+1} = -y_n + r e^{-\beta}((1 - x_n + e^{2\beta} - x_n e^{2\beta}) y_n - z_n x_n - e^{2\beta} z_n x_n) \\ Z_{n+1} = -z_n e^{2\beta} + r e^{\beta}(2z_n - 2x_n z_n - x_n y_n - y_n x_n) \end{cases} . \tag{5}$$

Equation (5) gives the lowest-order quantum corrections. For convenience, we consider that $\beta = i w_A T$ [20]. The sensitivity of the map to its initial values are shown in Fig. 1. We plotted Fig. 1 for constant parameter $r = 9$, $b = 0.5$, $y_0 = 0.435$ and $z_0 = 0.777$ as well as variable initial condition $x_0 = 0.423$ and $x_0 = 0.424$. Lyapunov exponent curve are seen in Fig. 2.

3 S-Box Criteria

An $n * m$ S-box is a nonlinear mapping $S : V_n \rightarrow V_m$, where V_n and V_m represent the vector spaces of n, m elements from $GF(2)$. Important tests to check the performance of S-box are nonlinearity (NL), strict avalanche criterion (SAC), bit independence criterion (BIC), linear approximation probability (LP), and differential approximation probability (DP).

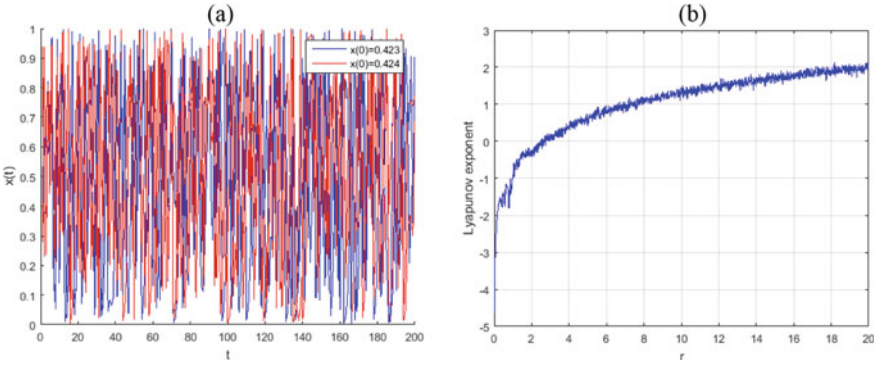

Fig. 1 **a** The sensitivity of the chaotic map to initial values the maps of generalized Dicke model for $x_0 = 0.423$ and $x_0 = 0.424$ where the control parameter $r = 9$, $b = 0.5$, $y_0 = 0.435$ and $z_0 = 0.777$. **b** The variation of the Lyapunov exponent the maps of generalized Dicke model in term of parameters r

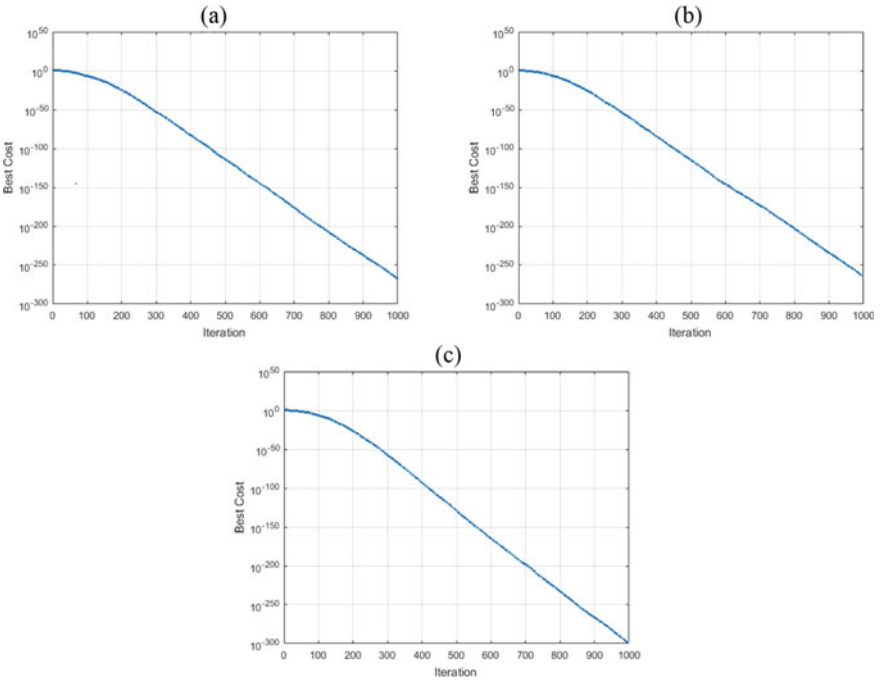

Fig. 2 The variation of the cost function (sphere) for **a** PSO algorithm with unifrnd and rand functions **b** improved PSO algorithm with quantum maps **c** improved PSO algorithm with quantum maps and hierarchy of rational-order chaotic maps

3.1 Nonlinearity

The nonlinearity value is calculated from the following equation:

$$N = 2^{n-1} - \frac{1}{2} \max_{a \in B^n} \left| \sum_{x \in B^n} (-1)^{f(x)+a \cdot x} \right|$$

where $B = \{0, 1\}$, $f : B^n \rightarrow B$, $a \in B^n$ and $a \cdot x$ is the dot product between a and x (see [21] for example). Since the affine functions are weak in terms of cryptography, the similarity of the Boolean function variable of S-box is measured with the affine variable.

3.2 Strict Avalanche Criterion (SAC)

Webster and Tavares introduced SAC. If one bit in the input of Boolean function changed, half of the output bits should be changed [22]. The value of SAC = 0.5 is necessary for passing this test.

3.3 Bit Independence Criterion (BIC)

BIC, which calculate the independence of the avalanche vectors sets, is a desirable feature for any encryption transformation for S-box analysis (Webster and Tavares defined this test in [22]). If one changes the inverse of input single bits, these sets are created [23].

3.4 Linear Approximation Probability (LP)

LP [24] is:

$$LP = \max_{a,b \neq 0} \left| \frac{\#\{x | x \cdot a = f(x) \cdot b\}}{2^n} - 0.5 \right|$$

where a, b are the input and output masks, and the set x contains all the possible inputs, and 2^n is the number of its elements. The maximum value of imbalance in the event between input and output bits is called LP. Low LP is necessary for resistance against linear attacks.

3.5 *Differential Approximation Probability (DP)*

DP is:

$$DP = \max_{\Delta_x \neq 0, \Delta_y} (\#x \in X, f_x \oplus f(x + \Delta_x) = \Delta_y / 2^n)$$

where X shows the set of all possible input values, and 2^n is the number of its elements. DP which calculate XOR the distribution between input and output bits of S-Box is introduced by Biham and Shamir [25]. The closer distribution between the input and output bits is necessary for resistance against differential attacks.

4 Improved PSO and Optimized S-Box

In PSO, the swarm consists of particles, each one representing a potential solution in the optimization problem. These particles have position and velocity. The PSO algorithm uses the unified function for the initial population and the rand function to update the speed and position. In this paper, we use a quantum map for the initial population. Instead of the rand function, once we use the quantum map and for the second time, the classical hierarchy of rational-order chaotic maps (the best result of [11]) (see Fig. 1). As can be seen, the best results are obtained for improved PSO with quantum maps and the hierarchy of rational-order chaotic maps (see Fig. 2). Now we use this optimization algorithm to get the best S-box based on the highest nonlinear value (see Appendix 2). The best S-box is seen in Table 2 (Table 1). The highest obtained nonlinearity value is 106.

5 Improved HS and Optimized S-Box

Zong Woo Geem et al. in 2001 developed Harmony search which is a music-based metaheuristic algorithm [26]. It used to solve many optimization problems such as function optimization, engineering optimization [27], water distribution networks [28]. To enhance the global convergence and to prevent to stick on a local solution, different HS methods based on chaotic maps have been proposed [29]. The improved HS (see Fig. 3) steps and its application for optimizing the designed chaotic S-box are discussed. The steps of the algorithm are as follows:

Step 1 Enter improved HS parameters (number of decision variables, decision variables matrix size, Maximum number of iterations, Harmony Memory size, number of new Harmonies, Harmony Memory consideration rate, Pitch Adjustment rate, Fret width(Band width), Fret width Damp ratio) and $r = 5.5$, $\beta = 0.5$ for (5).

Table 1 New S-box for the map of (5)

99	206	2	73	228	88	191	176	6	101	211	98	231	153	62	207
164	179	49	195	108	31	141	8	185	57	27	249	91	128	209	154
252	201	138	205	247	76	60	165	14	55	5	56	12	238	139	240
149	125	192	54	188	183	39	229	193	117	180	13	233	146	30	150
214	97	106	82	35	109	131	230	173	152	127	182	41	25	47	236
92	196	160	122	242	111	34	220	212	81	175	170	77	118	132	4
26	145	119	168	15	187	63	136	7	148	181	123	17	221	241	53
254	250	255	67	1	239	93	103	46	226	157	90	167	51	184	105
72	219	140	133	194	203	59	115	232	70	246	243	199	112	142	224
19	42	213	186	177	66	94	68	129	79	21	256	234	80	172	223
171	58	74	156	126	38	16	33	48	178	78	52	114	143	104	23
200	32	251	151	216	237	65	89	28	190	75	202	83	159	69	245
20	96	45	225	9	50	174	113	137	95	198	44	162	244	18	87
210	130	102	61	107	85	215	147	248	43	71	29	64	24	121	100
116	134	22	155	124	135	217	235	189	163	11	253	144	3	84	218
204	110	86	208	158	10	197	161	120	222	37	169	40	36	227	166

Table 2 New optimized S-box for the map of (5) with improved PSO algorithm

185	241	245	54	115	154	198	63	190	228	29	94	177	213	186	240
192	191	28	200	208	193	194	238	34	244	188	132	254	164	107	2
151	239	125	128	171	231	181	96	220	71	21	204	43	101	39	95
256	33	41	218	127	141	137	230	207	201	44	4	102	124	70	10
248	153	212	13	158	119	69	1	143	167	14	3	195	121	206	6
81	17	152	82	111	210	109	113	199	27	140	211	131	148	233	112
48	221	92	253	187	57	243	60	217	78	234	130	116	173	216	120
31	227	246	179	83	7	162	196	232	23	182	47	45	126	72	91
90	76	62	215	30	169	88	222	99	172	176	237	136	189	139	100
197	235	64	156	229	77	87	142	157	98	166	105	51	183	61	59
106	38	68	67	144	155	202	247	40	123	104	174	147	122	163	117
79	36	255	22	37	236	20	74	32	138	223	165	35	86	97	226
58	19	110	209	108	114	103	118	25	9	50	5	160	12	129	252
65	24	149	16	249	52	224	184	55	66	178	225	219	150	242	93
11	53	49	84	175	146	205	15	26	56	89	18	250	159	180	8
170	214	42	133	46	161	75	145	134	85	203	80	251	73	168	135

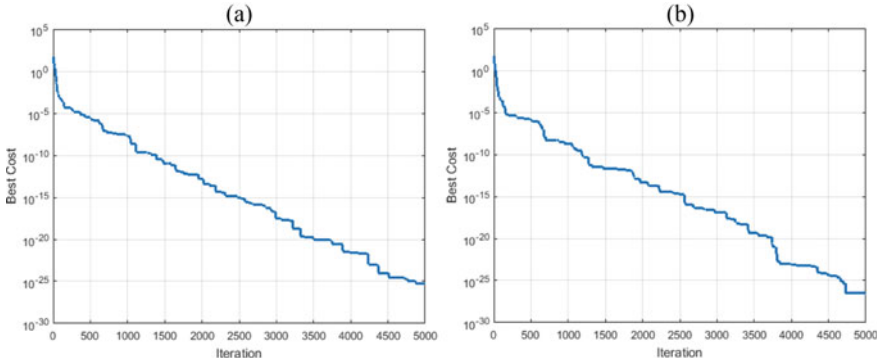

Fig. 3 The variation of the cost function (sphere) for **a** HS algorithm with unifrnd **b** improved HS algorithm with quantum maps

Step 2 Initialize Harmony Memory using liana function(liana function produce random number between 100 and 120 by using (5)).

Step 3 Creation of S-box based on quantum map (5):

1. Enter $r = 5.5, \beta = 0.5$ for (5) (consider Fig. 1).
2. Pass the transition state by repeating the map (5).
3. We create empty $16 * 16$ box.
4. Repeat the map (5) and select $x(f)$.
5. The S-box numbers are obtained:

$$S(i) = x(f) * 10^5 \bmod 256$$

6. The process continues from 4 and select different $S(i)$.

Step 4 Calculation of nonlinearity for all Harmony Memory positions.

Step 5 Sort Harmony Memory from MAX to MIN.

Step 6 Update Best solution ever found.

Step 7 Create new Harmony position using liana function.

Step 8 Pitch Adjustment using nafis function(nafis function produce random number between -1 and 1 by using (5)).

Step 9 If Nonlinearity(new position) > best solution save S-box.

Step 10 Merge Harmony memory and new Harmonies.

Step 11 Sort Harmony Memory from MAX to MIN.

Step 12 Update Best solution ever found.

Step 13 Save Best Nonlinearity.

Step 14 If iteration finished, print Best Nonlinearity.

Optimized S-box creation algorithm using improved HS algorithm with quantum maps is presented in Fig. 4. The created S-box are seen in Table 3. Figure 5 shows

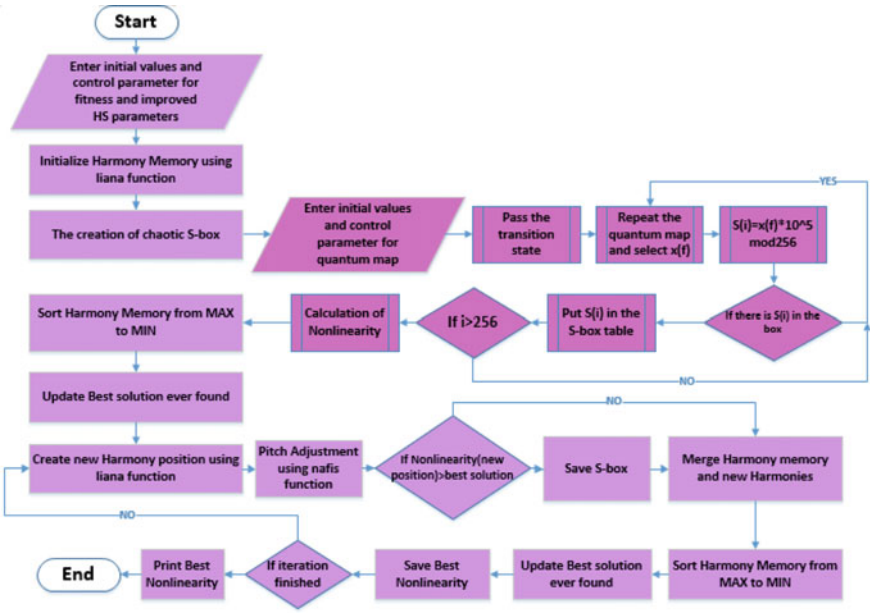

Fig. 4 Optimized S-box creation algorithm using improved HS algorithm with quantum maps

best nonlinearity of optimized S-box with nonlinearity fitness function for improved PSO algorithm with quantum maps and hierarchy of rational-order chaotic maps and improved HS algorithm with quantum maps.

6 Security Analysis

The security of any encryption is measured by its key(the keyspace size more than 2^{100} [30, 31]). We prob the keyspace of a quantum map to create the S-box. The order of complexity for decoding is:

$$T(r, \beta, x_0, y_0, z_0) = \theta(r \times \beta \times x_0 \times y_0 \times z_0)$$

If the computer's analysis power is 10^{16} decimal, the accuracy for each variable is 10^{-16}. The number of these parameters for the quantum map in (5), is 5. So the keyspace for each is $10^{80}(2^{265})$. These spaces could resist all types of brute-force attacks.

Table 4 represent nonlinearity, SAC, BIC, LP and DP results for new S-boxes and compares with the other results.

Table 3 New optimized S-box for the map of (5) with improved HS algorithm

206	4	51	105	57	121	73	247	36	152	101	109	18	134	119	173
25	222	43	122	78	242	30	110	83	114	12	65	23	185	58	138
141	96	1	64	209	135	116	126	156	226	212	84	237	238	160	128
47	255	103	253	40	67	98	229	153	225	14	8	66	29	99	217
21	155	146	219	37	246	181	227	108	17	171	220	7	52	256	94
89	130	211	20	77	133	82	190	24	10	50	44	62	120	136	234
224	208	80	3	163	251	245	195	148	143	203	235	113	72	216	117
144	115	16	142	162	111	70	193	191	38	177	174	213	165	194	86
145	42	34	45	202	204	22	158	139	31	157	75	92	180	241	198
11	188	61	26	151	132	197	39	233	207	97	170	184	68	214	104
149	182	35	49	112	189	60	140	107	239	56	100	199	150	87	186
250	231	196	187	33	19	168	161	46	183	249	76	221	2	93	95
9	201	240	91	13	90	192	236	223	125	28	5	147	131	244	129
230	41	71	210	254	167	69	200	27	205	48	54	228	85	172	218
166	176	248	55	159	106	88	102	15	243	59	164	6	53	124	179
81	178	252	169	154	32	123	118	63	74	79	232	137	175	127	215

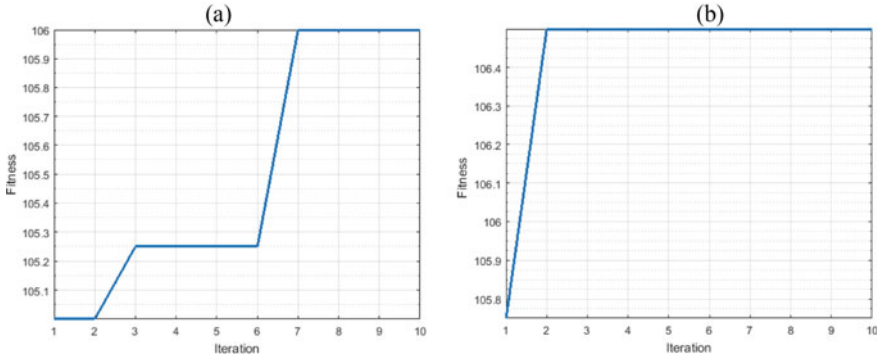

Fig. 5 Best nonlinearity of optimized S-box for **a** improved PSO algorithm with quantum maps and hierarchy of rational-order chaotic maps **b** improved HS algorithm with quantum maps

7 Conclusion

We are using the introduced quantum map based on quantum dots to generate chaotic S-boxes. The proposed map results, improving in performance of introduced PSO and HS optimization algorithms. In comparing the with classic ones, it is effectively acting on generation the S-box. The obtained results show the importance of optimization algorithms in generating the S-box. The Harmony search algorithm for the known sphere function has a weaker answer than the PSO algorithm. In optimizing chaotic S-boxes, the use of Harmony search algorithms produces better results. The introduced

Table 4 Nonlinearity, SAC, BIC, LP, and DP results for new S-boxes and compare with the other results

	Nonlinearity	SAC	BIC-nonlinearity	BIC-SAC	LP	DP
New S-box	105.5	0.512939	103.714		0.140625	10
New optimized S-box with PSO	106	0.499512	103.5	0.500837	0.132813	10
New optimized S-box with HS	106.5	0.501465	104.071	0.498047	0.132813	10
[11]	106.5	0.503662	102.857	0.499512	0.140625	10
[12]	105.25	0.495605	104.571	0.504325	0.140625	12
[13]	104.2	0.4931	103.3	0.4988	0.1563	12
[14]	106	0.52881	100	–	–	10
[10]	112	0.5048	112	–	–	4

S-boxes can be used in all image encryption, steganography, watermarking, and quantum digital signatures to increase security.

Appendix 1

In this appendix we derive Eq. (5). By inserting expressions $J_+ =< J_+ > +\delta J_+$ and $J_- =< J_- > +\delta J_-$ into force equation ([12]) we get

$$\begin{aligned} f(J_+, J_-) &= - < J_+ > -\delta J_+ \\ &+ e^{-iw_A T} r(< J_+ > +\delta J_+ - < J_- >< J_+ > -\delta J_- \delta J_+ \\ &- < J_- > \delta J_+ - \delta J_- < J_+ >). \end{aligned} \tag{6}$$

By considering $\dot{J}_+ = \delta \dot{J}_+$, $\dot{J}_- = \delta \dot{J}_-$, and due to

$$\delta \dot{J}_- = \delta \dot{J}_+^{\dagger}, \tag{7}$$

we use [12] for obtaining:

$$\begin{aligned} \frac{d}{dt}(\delta J_+ \delta J_-) &= [i w_A (< J_+ > +\delta J_+) - i \frac{\gamma}{\sqrt{N}} a^{\dagger}(0) e^{it} (\delta J_+ \\ &\delta J_- - \delta J_- \delta J_+) - i \frac{\gamma}{\sqrt{N}} a(0) e^{-it} (\delta J_+ \delta J_- - \delta J_- \delta J_+) \\ &+ [- < J_+ > -\delta J_+ + e^{i w_A T} r(< J_+ > +\delta J_+ - < J_- >< J_+ > \\ &- \delta J_- \delta J_+ - < J_- > \delta J_+ - \delta J_- < J_+ >)] \, \Sigma_n \delta(t - nT)] \delta J_- \end{aligned}$$

$$+\delta J_+(-iw_A(<J_->+\delta J_-)+i\frac{\gamma}{\sqrt{N}}a(0)e^{-it}[\delta J_-\delta J_+$$
$$-\delta J_+\delta J_-]+i\frac{\gamma}{\sqrt{N}}a^\dagger(0)e^{it}[\delta J_-\delta J_+-\delta J_+\delta J_-]+[-<J_->$$
$$-\delta J_-+e^{iw_AT}r(<J_->+\delta J_--<J_+><J_->-\delta J_+$$
$$\delta J_--<J_+>\delta J_--\delta J_+<J_->)]\ \Sigma_n\delta(t-nT)]\,. \tag{8}$$

By integrating Eq. (8), from nT to $(n+1)T$, and take the expectation value, by taking into account $<\delta J_-(nT)>=<\delta J_+(nT)>=0$, $<a^\dagger(0)>=<a(0)>=0$ we obtain:

$$<\delta J_+((n+1)T)\delta J_-((n+1)T)>=-<\delta J_+(nT)\delta J_-(nT)$$
$$>+re^{-iw_AT}<\delta J_+(nT)\delta J_-(nT)>-re^{-iw_AT}<J_->$$
$$<\delta J_+(nT)\delta J_-(nT)>-re^{-iw_AT}r<\delta J_-(nT)\delta J_-(nT)>$$
$$<J_+>+re^{iw_AT}<\delta J_+(nT)\delta J_-(nT)>-re^{iw_AT}$$
$$<\delta J_+(nT)\delta J_-(nT)><J_+>-re^{iw_AT}<\delta J_+(nT)$$
$$\delta J_+(nT)><J_->\,. \tag{9}$$

The calculation of $<\delta J_+\delta J_+>$ goes as follows:

$$\frac{d}{dt}(\delta J_+\delta J_+)=\delta\dot{J}_+\delta J_++\delta J_+\delta\dot{J}_+. \tag{10}$$

We end up with:

$$\frac{d}{dt}(\delta J_+\delta J_+)=[iw_A(<J_+>+\delta J_+)-i\frac{\gamma}{\sqrt{N}}a^\dagger(0)e^{it}[\delta J_+$$
$$\delta J_--\delta J_-\delta J_+]-i\frac{\gamma}{\sqrt{N}}a(0)e^{-it}[\delta J_+\delta J_--\delta J_-\delta J_+]$$
$$+[-<J_+>-\delta J_++e^{-iw_AT}r(<J_+>+\delta J_+-<J_->$$
$$-\delta J_-\delta J_+-<J_->\delta J_+-\delta J_-<J_+>)]\times\Sigma_n\delta(t-nT)]$$
$$\delta J_++\delta J_+[iw_A(<J_+>+\delta J_+)-i\frac{\gamma}{\sqrt{N}}a^\dagger(0)e^{it}[\delta J_+\delta J_-$$
$$-\delta J_-\delta J_+]-i\frac{\gamma}{\sqrt{N}}a(0)e^{-it}[\delta J_+\delta J_--\delta J_-\delta J_+]+[-<J_+>$$
$$-\delta J_++e^{-iw_AT}r(<J_+>+\delta J_+-<J_->$$
$$-<J_->\delta J_+-\delta J_-<J_+>)]\Sigma_n\delta(t-nT)]. \tag{11}$$

By integrating form Eq. (11), from nT to $(n+1)T$, and by assuming $<\delta J_-(nT)>=<\delta J_+(nT)>=0$, $<a^\dagger(0)>=<a(0)>=0$ we obtain:

$$
\begin{aligned}
&< \delta J_+((n+1)T)\delta J_+((n+1)T) > e^{-2i\omega_A(n+1)T} - < \delta J_+(nT) \\
&\delta J_+(nT) > e^{-2i\omega_A nT} = e^{-2i\omega_A nT}(- < \delta J_+(nT)\delta J_+(nT) > \\
&+ e^{-i\omega_A T} r(< \delta J_+(nT)\delta J_+(nT) > - < J_-(nT) > \\
&< \delta J_+(nT)\delta J_+(nT) > - < J_+(nT) >< \delta J_-(nT)\delta J_+(nT) >)) \\
&+ e^{2i\omega_A nT}(- < \delta J_+(nT)\delta J_+(nT) > + e^{-i\omega_A T} r(\\
&< \delta J_+(nT)\delta J_+(nT) > - < J_-(nT) >< \delta J_+(nT)\delta J_+(nT) > \\
&- \delta J_+(nT)\delta J_-(nT) >< J_+(nT) >)).
\end{aligned} \tag{12}
$$

Appendix 2

This appendix describes the improved PSO steps and its application for optimizing the designed chaotic S-box. The steps of the algorithm are as follows:

Step 1 Enter improved PSO parameters (number of decision variables, size of decision variables matrix, Maximum number of iterations, population size, inertia weight, inertia weight damping ratio, personal learning coefficient, global learning coefficient) and $a_1 = 2.61, a_2 = 3.168$ for the Hierarchy of rational order chaotic maps [11].

Step 2 Initial population production using chaotic map (5).

Step 3 Creation of S-box based on quantum map (5):

1. Enter $r = 5.5, \beta = 0.5$ for (5) (consider Fig. 1).
2. Pass the transition state by repeating the map (5).
3. We create empty $16 * 16$ box.
4. Repeat the map (5) and select $x(f)$.
5. The S-box numbers are obtained:

$$S(i) = x(f) * 10^5 \bmod 256$$

6. The process continues from 4 and select different $S(i)$.

Step 4 Calculate nonlinearity of all primary particles and search personal and global best for this population.

Step 5 Update the speed and position (consider jth dimension at iteration t of each particle i):

$$
\begin{aligned}
V_{i,j}(t+1) = {} & wV_{i,j}(t) + (c1)(r1)(BestX_{i,j}(t) - X_{i,j}(t)) \\
& + (c2)(r2)(GlobalBest(t) - X_{i,j}(t))
\end{aligned} \tag{13}
$$

$$X_{i,j}(t+1) = X_{i,j}(t) + V_{i,j}(t+1) \tag{14}$$

where $V_{i,j}(t)$ is a velocity of particle i at iteration t; $X_{i,j}(t)$ it is a position of i particle at iteration t; r1 and r2 are two random number between (0, 1) provided by the Hierarchy of rational order chaotic maps [11]; $BestX_{i,j}(t)$ is the local best particle i in all swarm and $GlobalBest(t)$ is the leader of the swarm or global best position of all population.

Step 6 Local and global search and save the best nonlinearity and related S-box.

References

1. S. Behnia, A. Akhshani, S. Ahadpour, A. Akhavan, H. Mahmodi, Cryptography based on chaotic random maps with position dependent weighting probabilities. Chaos, Solitons and Fractals **40**, 362–369 (2009)
2. S. Behnia, S. Ahadpour, P. Ayubi, Design and implementation of coupled chaotic maps in watermarking. Applied Soft Computing **21**, 481–490 (2014)
3. S. Behnia, M. Yahyavi, R. Habibpourbisafar, Watermarking based on discrete wavelet transform and q-deformed chaotic map. Chaos, Solitons and Fractals **104**, 6–17 (2017)
4. N. Hematpour, S. Ahadpour, S. Behnia, Digital signature: Quantum chaos approach and bell states, Chapter 9 Springer Science and Business Media LLC, 2019
5. T. K. Das, S. P Ilaiyaraja C, Whispering gallery mode enabled efficiency enhancement: Defect and size controlled cdse quantum dot sensitized whisperonic solar cells, *Scientific Reports*, 8, 9709, 2018
6. Q. Li, X.Wang, Z. Zhang, H. Chen, Y. Huang, C. Hou, J.Wang, R. Zhang, J. Ning, Z. J Min C, Development of modulation p-doped 1310 nm inas/gaas quantum dot laser materials and ultrashort cavity fabry-perot and distributed-feedback laser diodes, *ACS Photonics*, 5, 1084-1093, 2018
7. K. J. McHugh, L. Jin, A. M. Behrens, S. Jayawardena, W. Tang, M. Gao, J. R Langer A, Biocompatible semiconductor quantum dots as cancer imaging agents, *Advanced Materials*, 30, 1706356, 2018
8. M. Wilson, Silicon-based quantum dots have a path to scalable quantum computings. Physics Today **71**, 17–20 (2018)
9. National Institute of Standards and Technology, FIPS PUB 46-3: Data Encryption Standard (DES), super-sedes FIPS, 46-2, 1999
10. Advanced encryption standard (aes), Federal Information Processing Standards Publication 197 Std
11. N. Hematpour, and S. Ahadpour, Execution examination of chaotic S-box dependent on improved PSO algorithm, *Neural Computing and Applications*, 1-23, 2020
12. N. Hematpour, S. Ahadpour, and S. Behnia, Presence of dynamics of quantum dots in the digital signature using DNA alphabet and chaotic S-box, *Multimedia Tools and Applications*, 1-23, 2020
13. F. Ozkaynak, S. Yavuz, Designing chaotic S-boxes based on time-delay chaotic system. Nonlinear Dynamics **74**, 551–557 (2013)
14. D. Lambic, A new discrete-space chaotic map based on the multiplication of integer numbers and its application in s-box design, *Nonlinear Dynamics*, 1-13, 2020
15. H.A. Ahmed, M.F. Zolkipli, M. Ahmad, A novel efficient substitution-box design based on firefly algorithm and discrete chaotic map. Neural Computing and Applications **31**, 7201–7210 (2019)
16. T. Farah, R. Rhouma, S. Belghith, A novel method for designing S-box based on chaotic map and Teaching-Learning-Based Optimization. Nonlinear Dynamics **88**, 1059–1074 (2017)
17. C. Emary, T. Brandes, Chaos and phase transitions in quantum dots coupled to bosons. Physical review E **67**, 0662031–06620322 (2003)

18. J.G. Hirsch, O. Castaños, R.L. Pena, E.N. Achar, Mean field description of the Dicke Model. Found. Probab. Phys. 6 AIP Conf. Proc. **1424**, 144–148 (2012)
19. M.E. Goggin, B. Sundaram, P.W. Milonni, Quantum logistic map. Physical review A **41**, 5705 (1990)
20. S. Ahadpour, N. Hematpour, *Quantum chaos in quantum dots coupled to bosons*, arXiv:1207.5590v1, 2012
21. T. Cusick, P. Stanica, *Cryptographic boolean functions and applications* (Elsevier, Amsterdam, 2017)
22. A. Webster, S. Tavares, *On the design of s-boxes*, in: Conference on the theory and application of cryptographic techniques, Springer, 523-34, 1985
23. H. Zhang, T. Ma, G. Huang, Z. Wang, Robust global exponential syn- chronization of uncertain chaotic delayed neural networks via dual-stage impulsive control, IEEE Trans. Syst. Man. Part B Cybern **40**, 831–844 (2009)
24. M. Matsui, *Linear cryptanalysis method for des cipher, Workshop on the theory and application of cryptographic techniques*, Springer, Berlin, Heidelberg, 386-397, 1993
25. E. Biham, A. Shamir, Differential cryptanalysis of des like cryptosystems. J. Cryptol. **4**, 3–72 (1991)
26. Z.W. Geem, J.H. Kim, G.V. Loganathan, A new heuristic optimization algorithm: Harmony search. Simulation **76**, 60–68 (2001)
27. K.S. Lee, Z.W. Geem, A new meta-heuristic algorithm for continuous engineering optimization: harmony search theory and practice. Comput. Methods Appl. Mech. Engrg. **194**, 3902–3933 (2005)
28. Z.W. Geem, Optimal cost design of water distribution networks using harmony search. Engineering Optimization **38**, 259–280 (2006)
29. B. Alatas, Chaotic harmony search algorithms. Applied Mathematics and Computation **216**, 2687–2699 (2010)
30. B. Schneier, *Applied cryptography: Protocols, algorithms, and source code* in c, John Wiley and Sons, 2007
31. M. Mollaeefar, A. Sharif, M. Nazari, A novel encryption scheme for colored image based on high level chaotic maps. Multimedia Tools and Applications **76**, 607–629 (2017)