International Journal of Theoretical Physics (2019) 58:3871–3898
https://doi.org/10.1007/s10773-019-04254-w

# A Novel Construction Scheme for Nonlinear Component Based on Quantum Map

Faiza Firdousi [1] · Syeda Iram Batool [2,3] · Muhammad Amin [2,3]

Received: 30 March 2019 / Accepted: 19 August 2019 / Published online: 26 August 2019


**Abstract**
In this article, we have deigned a new mechanism for the construction of confusion component which is one of the most important and integral part of any confidential scheme in secure communication. The privacy of digital information is one of the most vital issues of the digitally advanced world. The proposed nonlinear component which is usually termed as substitution box (S-box) is constructed by utilizing quantum map. Moreover, we have performed the robust analysis for our anticipated nonlinear component and compared it with already existing standards.

**Keywords** Quantum map · Nonlinear component · Privacy

## 1 Introduction

Substitution boxes (S-boxes) are the only nonlinear component in any symmetric encryption system. They follow the confusion principle presented by Claude Shannon in 1949. The confusion architecture is very effective in achieving secrecy if used correctly. Therefore, the S-boxes need to be robust and efficient to tackle any sort of differential attack or attacks made on the bases of linear content of S-box. That is why it is vital to keep the nonlinearity in mind when designing an S-box. For over two decades, much research has been dedicated to the use of chaos to generate nonlinear S-boxes. But, mostly the nonlinearity achieved by them has not been so impressive. In order to achieve good nonlinearity, Khan et al. [1] applied a fractional linear transformation along with multiple chaotic systems to obtain an S-box. It is an easy and simple way but the nonlinearity content was not satisfactory enough. Later, in 2015, Ahmed et al. [2] proposed a new technique, in which the input elements of the S-box were generated using piecewise linear chaotic map, then rastor and zigzag pattern scanning is applied to the

✉ Syeda Iram Batool
syedairambatool@gmail.com

[1] Department of Electrical Engineering, Institute of Space Technology, Islamabad, Pakistan

[2] Department of Avionics Engineering, Institute of Space Technology, Islamabad, Pakistan

[3] Cyber and Information Security Lab (CISL), Institute of Space Technology, Islamabad, Pakistan

initial S-box to obtain the final S-box. Özkaynak et al. [3] also presented a new S-box using the fractional order chaotic Chen system. Wang et al. [4] used a new three dimensional continuous chaotic map with infinite equilibrium points to design an S-box, but its nonlinearity was also not good enough. Liu et al. [5] proposed employing spatiotemporal chaos to generate random S-boxes. He used the non-adjacent coupled map lattices and Arnold's cat map to extract the spatiotemporal chaotic behavior of the system. Lambic et al. [6] used existing chaos based S-boxes [7, 8] to derive a new S-box by defining a new composition approach. Similarly, Tian et al. [9] proposed a novel approach to constructing S-boxes. He proposed to use a comparatively new version of the logistic map, named as intertwined logistic map. He combined the intertwined logistic map [10] with the Bacterial foraging algorithm [11] to derive a new S-box. Zaibi et al. [12] proposed an approach to use one dimensional chaotic maps like the one dimensional logistic map and the piecewise linear chaotic map to generate a new S-box. The nonlinearity is not mentioned in the paper. Ahmad et al. [13] proposed to chaotically modify the trajectory of the piecewise linear chaotic map and logistic map to eliminate the gently decreasing peaks to obtain sharp peaks of the modified chaotic map. Then later, the modified map is scanned in a zigzag fashion to obtain better results to generate a random S-box. Belazi et al. [14] proposed to employ the chaotic sine map to derive a new S-box with nonlinearity greater than 105. Recently, Khan et al. [15–20] proposed significant contributions in the construction of confusion component of block ciphers [21, 22]. In more recent works [23–26], many schemes have been proposed for the use of chaos to construct S-boxes, but they all suffer for a nonlinearity of 106 or less. In this paper we have proposed novel unique S-boxes with improved nonlinearity greater than 106. Moreover, chaos based encryption schemes were also proposed in literature due to its close association with cryptographic applications [27–58]. In this article, our primary aim is to explore the quantum logistic map to generate many S-boxes, optimized its parameters to select the best S-box. The selected S-boxes are then tested to check their strength against cryptographic attacks. The tests carried out are nonlinearity test, strict avalanche criteria, bit independence test, differential approximation probability, linear approximation probability, algebraic degree, algebraic immunity, correlation immunity, sum of square indicator, absolute indicator, transparency order, propagation criterion, fixed points, composite algebraic immunity, robustness to differential cryptanalysis, signal to noise ratio-differential power analysis and NIST randomness suit.

The rest of the paper is organized as follows. In section 2, we have discussed basic terms which will be quite helpful to understand the quantum chaos. We have added cryptographic characteristics of nonlinear confusion component in section 3. The idea of utilizing quantum chaotic maps for the construction of nonlinear component is discussed in section 4. The results and discussions of obtained nonlinear component are given in detailed in section 5. Finally, we added conclusion in section 6.

## 2 Basic Preliminaries

In this section some preliminary work related to the quantum logistic map is discussed.

### 2.1 Quantum Logistic Map

In early 1980s and 90s, vast amount of research effort was being put in to study the effect of noise and quantum fluctuations on the classical chaotic systems [48]. The results were mostly

bended towards the favor of quantum chaotic systems as they exhibit regular, non-chaotic behavior when exposed to quantum fluctuations [49]. In 1990, Goggin et al. [50] wrote a paper in which he described the effect of quantum fluctuations on the much studied, famous logistic map. He reached to a conclusion, much different from Elgin's [49], when he applied quantum fluctuations on the Lorenz strange attractor. In Elgin's work, the Lorenz attractor disappeared after applying the quantum fluctuations to the three dimensional chaotic system, and were replaced by stable fixed points. But Goggin discovered that when quantum fluctuations were applied on the logistic map, it followed a period doubling cascade to chaos. The quantum chaotic system he proposed is the quantum logistic map (QLM), which we will study qualitatively in this paper. The equation for the QLM is given below:

$$\begin{aligned} x_{i+1} &= r\left(x_i - |x_i|^2 - r y_i\right), \\ y_{i+1} &= -y_i e^{-2\beta} + 2re^{-\beta}[-x_i(y_i + z_i) + y_i], \\ z_{i+1} &= -z_i e^{-2\beta} + 2re^{-\beta}[-x_i(y_i + z_i) + z_i], \end{aligned} \tag{1}$$

where, $r$ is the same controlling parameter as in the classical logistic map and $\beta$ is the dissipation parameter, i.e. the controlling parameter in the QLM. Moreover, $x_0 \in [0.1, 0.9]$, $y_0 \in [0, 0.2]$,and $z_0 \in [0, 1]$.The range of $r$ most suitable for QLM is [3.68, 3.73], [3.75, 3.82] and [3.88, 3.99]. As $r$ is varied, Eq. (1) shows the same behavior as the classic logistic map. In his paper, Goggin discovered that by increasing $\beta$, Eq. (1) exhibits a period doubling route to the classical logistic map. In what follows, we give a qualitative analysis of the QLM and conclude that it achieves the universal delta, known as the feigenbaum delta. We also note that the QLM follows the converse of Sharkovsky's theorem.

### 2.2 Fixed Point, Periodic Point, Orbit

We would start with the elementary definition of a fixed point. The function $f$ maps a plane onto itself, that is, $f: \mathbb{R} \to \mathbb{R}$. A discrete dynamical system is of the form:

$$x_{n+1} = f(x_n), \tag{2}$$

where, $f^n(x)$ is the $n^{th}$ iteration of Eq. (2). $x_0$ is a fixed point of $f$ if $f(x_0) = x_0$. This means that for any initial condition provided to a discrete dynamical system, if the input is always equal to the output, then the discrete map is mapping on a fixed point. $x_0$ is a periodic point of $f$ if $f^n(x_0) = x_0$. This means that the function is mapping on values with a period $n$. An orbit of $x$ is given by the series: $x, f^1(x)$, $f^2(x)$, …, $f^n(x)$,where $n$ is the total number of iterations made. The iterations computed for the same β, r and initial conditions amount for a single orbit. There is only one value in an orbit of period 1 because all the iterations give a single value, and that is the fixed point.

There are two values in an orbit of period two because all the iterations exhibit two values periodically, which are the period two periodic points, and so on. It takes the first iterations for the discrete map to actually settle down on the actual values. We say that the map is exhibiting a transient effect. So that's why the first iterations are always discarded when plotting the maps for some calculations. The transient effect is shown in Fig. 1, where the plot of the first iterations is transitioning and then settling down on a fixed pattern. Figure 1 gives a look into the periods formed by iterating the QLM and changing the value of the dissipation parameter $\beta$.

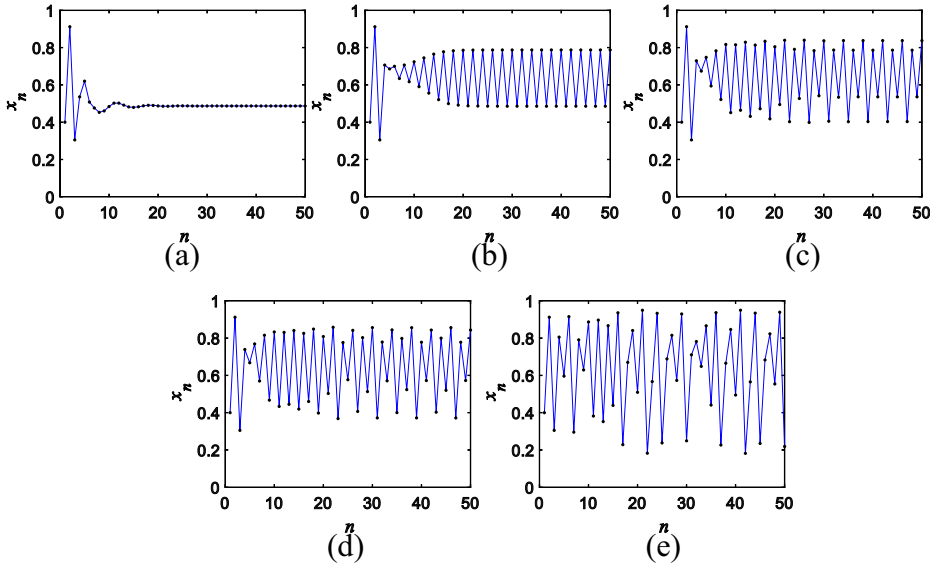


**Fig. 1** Periods 1 to $2^n$, for different values of $\beta$, with $r = 3.8$, $x_0 = 0.4$, $y_0 = 0$, $z_0 = 0$. **a** Period 1 orbit with $\beta$=2.5, (**b**) Period 2 orbit with $\beta$=3, (**c**) Period 4 orbit with $\beta$=3.132, (**d**) Period 8 orbit with $\beta$=3.199, (**e**) $\infty$ period orbit with $\beta = 6$

### 2.3 Period Doubling Route to Chaos

The QLM starts from the orbit of a fixed point (period 1) (Fig. 1a), and as $\beta$ is increased, it settles down on orbits of period 2, then 4, then 8, 16, 32, … $2^n$. This means that the increase in the periods of the preceding orbits follow the pattern in powers of 2. This is denoted by the term period doubling. Figure 1 only shows the period doubling orbits till period 8, because after period 8, the sequence becomes chaotic (Fig. 1e). This means that the sequence of the orbit never repeats. This also states that the period doubling has gone so far that the period of the orbit is no longer recognizable. This phenomenon is termed as the period doubling route to chaos. The sequence of period doublings is known as the period doubling cascade, in which many periods are doubling together simultaneously and, eventually, unrecognizable.

### 2.4 Bifurcations

The term bifurcation means the division of something into two. The bifurcation of any system represents how the system changes with each orbit, with the same initial conditions, but increasing bifurcation parameter. It can depict the asymptotic long term behavior of any dynamic system. The period doubling is also a form of bifurcation where one period is split into two periods, then from them, into four, and so on. The period doubling bifurcation of the discrete dynamical systems is represented by the orbit diagram, or more commonly known as the bifurcation diagram. The bifurcation diagram of QLM is shown in Fig. 2. There are different types of bifurcations in the study of dynamical systems. The most common is the period doubling or pitchfork bifurcation, as opposed to the saddle node bifurcation. The QLM follows the pitchfork bifurcation, as is shown in Fig. 2. As can be seen in the figure, the visible period $2^n$ branches of a bifurcation are called tines, as in the tines of a fork, with the period $2^{n-1}$ acting as the handle of the fork.

Figure 2 is plotted with respect to $x$. Figure 2a shows the period bifurcation of the parameter $r$ with the orbits of $x$ of QLM, known as the $r$-bifurcation, as $r$ is increased to 4. The $r$-bifurcation of QLM is similar to the $r$-bifurcation of the classical map. That means after applying quantum fluctuations on the classical map, the $r$-bifurcation has not been modified. So we need to look at the behavior from the point of view of $\beta$-bifurcation.

### 2.5 $\beta$-Bifurcation of Quantum Logistic Map

In Fig. 2b, $r = 3.8$. The bifurcation diagrams do not include the transient effect, but the later settled down iterations. As $\beta$ is increased from 2.5, the first few orbits experience a stable fixed point till $\beta < 2.842$. These are the stable period one orbits and the fixed point is an attractor. Up till here is the stationary regime or equilibrium point. Beyond $\beta = 2.842$ the period one orbits become unstable and their state is changed from being an attractor to repeller. At this point the period one cycles are bifurcated and give birth to the period two cycles, then as $\beta$ is increased, the process repeats to $2^n$ cycles. For the values, $2.843 < \beta < 3.035$, the $x$ converges to and oscillates between four periodic points and thus a period 4 orbit is born. In the $\beta$-bifurcation diagram periods until $2^4$ are visible (if zoomed in). But beyond that $x$ becomes chaotic and no periods are visible anymore. This sequence of successive (and eventually, simultaneous) pitchfork bifurcations give rise to the infinite cascade of period doublings. Figure 2b shows that, just like the classical map, the QLM also follows the period doubling route to chaos. The unstable cycles are still present but are not shown in the bifurcation diagram. Note that the periods shown for different values of $\beta$ in Fig. 1 also fall in line with the Fig. 2b. A visual comparison of the bifurcation diagram of both the classical and quantized logistic map (Fig. 2) seems that the range of values for which $\beta$ is chaotic is larger than the range of $r$. The $r$ is most chaotic in the range [3.86, 4], while $\beta$ is evenly chaotic in the range $[4.07, \infty)$. Moreover, the $x$ of QLM covers more of the unit interval than in its classical counterpart.

### 2.6 Feigenbaum Delta

The point beyond which the period doublings cannot be further told apart is the point of accumulation, where the period of $x$ has become infinite and this is the start of the chaotic realm. If the value of $\beta$ where the period two starts is denoted by $\beta_2$, and the value where the

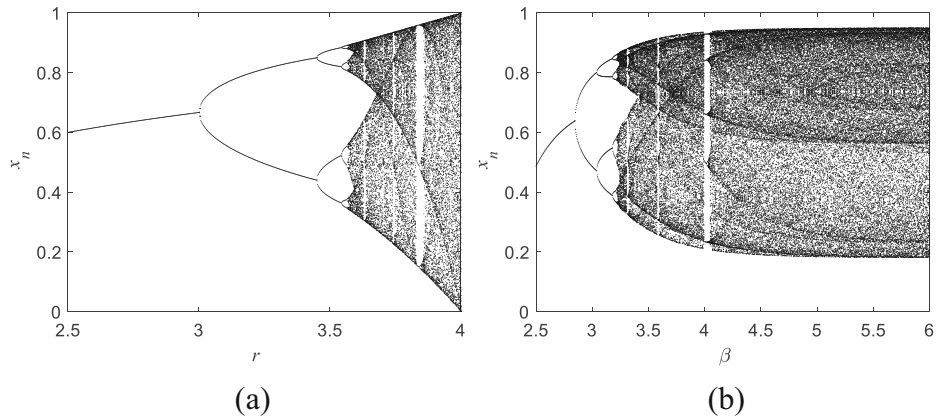


**Fig. 2** Bifurcation diagrams of quantum logistic map: (**a**): $r$-bifurcation, (**b**) $\beta$-bifurcation

period $p$ starts is denoted by $\beta_p$, then the accumulation point in $\beta$-bifurcation diagram is denoted by $\beta_\infty$ (infinite period). The accumulation point or $\beta_\infty$ for QLM is at 3.219, which occurs after the period 16 orbits. Beyond the period 16 orbits the period of $x$ becomes infinite because of the successive period doubling cascades. These continual pitchfork bifurcations don't just happen after some random value of $\beta$. In fact, if the discrete dynamical system under study is universal, then the values of $\beta$ at which the bifurcation will occur can be substantially approximately calculated. This precisely is the notion of the feigenbaum delta. The feigenbaum delta is a universal constant which is fixed for most discrete maps with similar dynamics like the logistic map. This delta approximately gives the points at which the next pitchfork bifurcation will occur and also the point of accumulation. It is calculated by the following ratio:

$$\delta = \lim_{n\to\infty} \frac{\lambda_{n-1}-\lambda_{n-2}}{\lambda_n-\lambda_{n-1}} \approx 4.669, \tag{3}$$

where, $\lambda_n$ is the value of the control parameter at which the $n$th bifurcation takes place. If the value of $\delta$ of the map under study is approximately equal to 4.669 with some admissible error, then the map is said to be universal. The $n \to \infty$ depicts that the period is approaching $\infty$. For the QLM, the $n \to \infty$ occurs at $n = 16$, because after this the period becomes infinite. Table 1 gives the values of $\beta$ at which the bifurcations occur.

We calculate the ratio by using Eq. (3) by considering the $\lambda_3$, $\lambda_4$,and $\lambda_5$. So plugging these notations in Eq. (3) gives the ratio 4.4474 with 4.7% error, which is permissible. This is approximately equal to the universal Feigenbaum delta. So we conclude that the QLM achieves the Feigenbaum delta and therefore it is also universal as its classical map.

### 2.7 Order in Chaos

After the chaotic regime begins at the accumulation point, for the values $\beta > \beta_\infty$, not all intervals of the control parameter are equally chaotic. There are slight ranges of periodic orbits embedded right between the chaotic aperiodic ranges, called windows of periodicity. However slight they may be, they are still present. For the classical map, the largest such window is the famous period three orbit embedded after $r \sim 3.8$. There may be many such similar windows of periodicity right between the aperiodic orbits where the behavior of the dynamical system might become stable again. This phenomenon is called order in chaos. Likewise, in the QLM (Fig. 2b) the most prominent window of stability is the period five orbit which occurs right after $\beta \sim 4$. If we increase the resolution of the plot and zoom into the neighborhood of one of these five stable points in the period five window, more successive period doubling bifurcations can be seen. Each point in the period five orbit is further bifurcated to give $5 \to 2 \times 5 \to 2^2 \times 5 \to 2^n \times 5 \to \beta_{5,\infty}$, where $\beta_{5,\infty}$ is the accumulation point where the period five period

**Table 1** Values of $\beta$ on which the successive bifurcations occur

| Period-$2^n$ ($\lambda_n$)→ | Period-2 ($\lambda_1$) | Period-4 ($\lambda_2$) | Period-8 ($\lambda_3$) | Period-16 ($\lambda_4$) | Period-32 ($\lambda_5$) |
|---|---|---|---|---|---|
| $\beta \quad \to$ | 2.8421 | 3.0376 | 3.1767 | 3.2105 | 3.2181 |

doubling cascade becomes chaotic. This means that each point inside a periodic window has a miniature bifurcation diagram of its own, and thus has infinite many bifurcation points inside it. Figure 3b shows the zoomed in portion of the neighborhood of red circle marked in the $\beta$-bifurcation plot shown in Fig. 3a of QLM. The red circle in Fig. 3b is zoomed in Fig. 3c, while the red circle in Fig. 3c is zoomed in Fig. 3d, and it goes on and on and on. Thus, an infinite pitchfork bifurcation cascade is found inside each of the bifurcations. All the secondary zoomed-in plots have classical logistic map like bifurcations. Figure 3d shows the zoomed in version of a similar bifurcation. It shows that this bifurcation (triple zoomed-in) has a period five orbit. These miniature infinite bifurcations show the existence of a fractal structure of the QLM.

### 2.8 Period 3 Implies Chaos

In discrete dynamical systems there are even periodic orbits in powers of 2, as seen earlier. But there also exist the odd periods greater than 1. As encountered before in Fig. 3a and d, which have visible period five orbits embedded between the chaotic regions. In 1964 a Ukrainian mathematician, Alexander Sharkovsky [4], made a

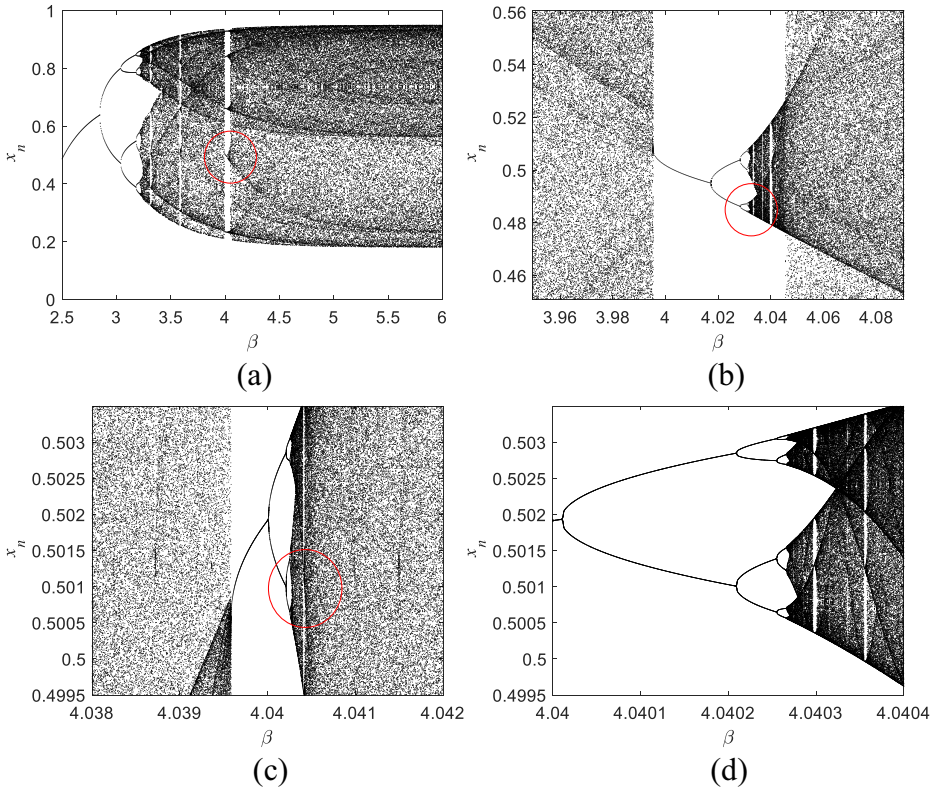


**Fig. 3** Zoomed in versions of the $\beta$-bifurcation of quantum logistic map. **a** un-zoomed plot of bifurcation diagram, (**b**) zoomed in bifurcation diagram of the red circle in (**a**), (**c**) zoomed in bifurcation diagram of the red circle in (**b**), (**d**) zoomed in bifurcation diagram of the red circle in (**c**)

remarkable discovery and proposed the famous Sharkovsky's ordering [51] of natural numbers given in Eq. (4).

$$3 \lhd 5 \lhd 7 \lhd \cdots \tag{4a}$$

$$\lhd 2 \cdot 3 \lhd 2 \cdot 5 \lhd 2 \cdot 7 \lhd \cdots \tag{4b}$$

$$\lhd 2^2 \cdot 3 \lhd 2^2 \cdot 5 \lhd 2^2 \cdot 7 \lhd \cdots \tag{4c}$$

$$\lhd 2^3 \lhd 2^2 \lhd 2 \lhd 1. \tag{4d}$$

Equation (4) is an ordering of natural odd numbers. The notation $o \lhd p$ signifies that $o$ comes before $p$ in the Sharkovsky's ordering. Eq. (4a) is an ordering of odd numbers greater than 1, in an increasing order. Eq. (4b) is an order of odd numbers as multiples of 2. Eq. (4c) gives an ordering of odd numbers as multiples of $2^2$. The ordering eventually extends to ordering of odd numbers greater than 1, as multiples of $2^n$, for all $n$. The last list Eq. (4d) is an ordering of powers of 2 in decreasing order. This is a very important list in the sense that it tells the existence of the period of an orbit based on the existence of a given periodic orbit already present in a map. The Sharkovsky's theorem explains the Sharkovsky's ordering as given in Theorem 1 [51].

**Theorem 1** *(Sharkovsky [51]). Let $f: \mathbb{R} \to \mathbb{R}$ be a continuous map which maps the real line onto itself. If $o \lhd p$ and $f$ has a point of period $o$, then $f$ must have a point of period $p$.*

Theorem 1 states that if a continuous map has an orbit of period $o$ in the Sharkovsky's ordering, then it must have an orbit of period $p$. This implies that if an orbit of period $o$ exists then orbits of all the natural numbers following $o$ in the Sharkovsky's ordering are also present in the map. And thus the famous case of period three orbit, period three implies chaos, comes into action. In his paper [51], Sharkovsky claimed if an orbit of period three is found in a map that means periods of all numbers following $o$ in Sharkovsky's order will also be present in the map, which leads to chaos. Numerous proofs have been given of this famous theorem since [5:8]. Now, suppose that if $o = 7$ then that means that the map $f$ has orbits of all the following periods: 7, 9, 11,13,15, …14,18,22,26,30…28,36,44, 52, 60…56,72,88,104,120…112,144,176,208,240…16, 8, 4, 2, 1. The question arises that if $o = 7$, then would the orbits of periods 3 and 5 exist? The answer is no. This is explained in the converse of Sharkovsky's theorem, presented by Elaydi [52], which states that the converse of Sharkovsky's theorem is not true.

**Theorem 2** *(Elaydi [52]). For any positive integer o there exists a continuous map $f: \mathbb{R} \to \mathbb{R}$, such that $f$ has points of period $o$ but no points of period $n$ for all positive integers $n$ that precede $o$ in the Sharkovsky ordering,* i.e., *$n \lhd o$.*

Theorem 2 is a converse on Sharkovsky's Theorem which states if in a map an orbit of period $o$ exists then the orbits of period $n$ and other orbits of natural numbers that come before $o$ in the Sharkovsky's ordering do not exist in the map. This is precisely the case for the QLM in which a period five orbit exists (which is the

largest periodic window embedded in the chaotic region marked with purple block), but no period three orbit exists in the QLM $\beta$-bifurcation, following the converse of Sharkovsky's theorem. For the QLM we can say that period 5 implies chaos. Because even though period 3 orbit does not exist according to [52], but the orbits of periods following five in the Sharkovsky's ordering still exist in the QLM [51]. Figure 4 shows the $x$, $y$ and $z$ sequences of the QLM for the first 200 iterations, in the chaotic region. This sums up the qualitative analysis of the QLM. In the next section we introduce a native coupling scheme for the QLM to generate our substitution boxes.

### 2.9 Coupling Scheme

The proposed coupling scheme is inspired by the coupled cap lattices (CML) [53], but still is quite different in application from them. Eq. (5) gives the proposed coupling strategy to couple the $x$, $y$ and $z$ sequences of QLM.

$$\begin{aligned} x_{i+1} &= (1-\epsilon)x_i + \epsilon y_i, \\ y_{i+1} &= (1-\epsilon)y_i + \epsilon z_i, \\ z_{i+1} &= (1-\epsilon)z_i + \epsilon x_i, \end{aligned} \tag{5}$$

where, $\epsilon \in [0, 1]$. The following section gives the proposed strategy to construct the desired S-boxes.

## 3 Security Analysis of Substitution Boxes

A good nonlinear component satisfies some of the strong cryptographic properties which includes, bijectivity, nonlinearity, strict avalanche criterion, bit independent criterion, linear and differential approximation probabilities, and also some advanced cryptographic properties like delta uniformity, transparency order, algebraic and correlation immunity, propagation

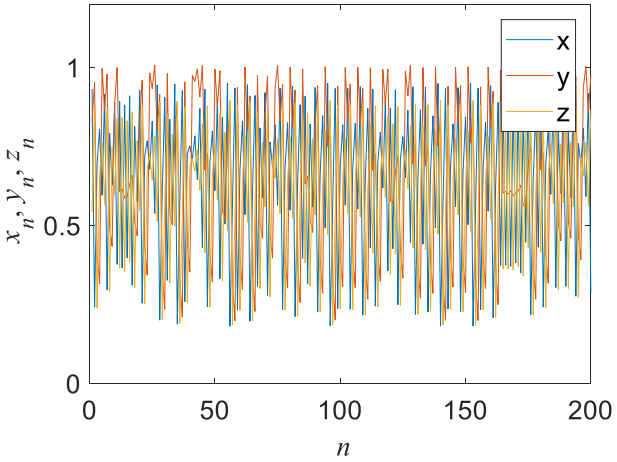


**Fig. 4** Sequences $x$, $y$ and $z$ generated by the quantum logistic map in one plot against the number of iteration $n = 200$, with $r = 3.8$, $\beta$=6, $x_0 = 0.4$, $y_0 = 0.15$, $z_0 = 0.2$

criteria, fixed and opposite fixed points and some others. In this section, we will define these cryptographic characteristics. We have also presented the randomness tests applied on the selected S-boxes in this section.

### 3.1 Bijective Property

A mapping function is said to be bijective if each of the element in one set maps to exactly one element of another set, and all the elements are paired. A bijective mapping is both injective and surjective. A substitution box is a bijective mapping of $m$ binary input bits to $n$ binary output bits where $m = n$. In this paper we are designing an 8 bits input to 8-bit output, square substitution box (8 × 8 S-box). In order for a Boolean function to be bijective, it has to fulfill the bijectivity criteria given by Eq. (6), which means that each output (0–255) should be generated exactly once.

$$wt\left(\sum_{i=1}^{n} a_i f_i\right) = 2^{n-1}, \tag{6}$$

where, $wt(.)$ is the hamming weight and $a_i \in \{0, 1\}$, $(a_1, a_2, a_3, \ldots a_n) \neq (0, 0, 0, \ldots 0)$. Every function $f_i$ needs to be balanced in the sense that there must be equal number of zeros to ones. A bijective S-box is just a permutation of the input vectors.

### 3.2 Nonlinearity

Nonlinearity is defined as the distance between the principal Boolean function and the set of all affine Boolean functions. The distance between the set of all affine functions and the Boolean function under study is measured and then the bits in the truth table are altered to obtain the nearest affine function. The number of changes needed to get the final affine function is the measure of the nonlinearity of the Boolean function. The nonlinearity $N_f$ of a function $f$ is given by Eq. (7).

$$N_f = \min_{l \in L_n} \mathrm{d}_H(f, l), \tag{7}$$

where, $l$ is an affine function that belongs to $L_n$, the set of all affine functions, and $d_H$ is the hamming distance between $f$ and $l$, which is given by $d_H(f, l) = 2^{n-1} - \frac{1}{2}\langle \rho, \mu \rangle$, where $\langle \rho, \mu \rangle = (Number\ of\ cases\ where\ f = l) - (Number\ of\ cases\ where\ f \neq l)$. The nonlinearity is calculated by using the walsh-hadamard transform stated in Eq. (8):

$$N_f = 2^{n-1}\left(1 - 2^{-n} max\left|\hat{F}(w)\right|\right), \tag{8}$$

where, $\hat{F}(w)$ is the Walsh spectrum, which is given by, $\hat{F}(w) = \sum_{x \in GF(2^n)} -1^{f(x) \oplus L_{w(x)}}$ and $L_w(x)$ is a linear function given by: $w_1x_1 \oplus w_1x_1 \ldots \oplus w_nx_n$. Each S-box consists of 8 Boolean functions, hence nonlinearity is calculated for each Boolean function and so the final nonlinearity is obtained by averaging over 8 nonlinearities.

### 3.3 Strict Avalanche Criteria (SAC)

A strict avalanche criterion (SAC) is an S-box analysis test in which a single input bit is changed and the resulting change in the output bits is noted. In order to fulfill the SAC test, with a single input changed bit, the output bits of the entire S-box should change with a probability of half, meaning almost half of the S-box should change. This change in single bit affecting more than half the output bits is called the Avalanche Effect. The SAC is usually calculated with the help of a dependence matrix [54]. To satisfy the SAC, the $m \times n$ elements of an $(n, m)$ S-box and the mean of the dependence matrix should lie round about 0.5. The ideal value is 0.5.

### 3.4 Output Bit Independence Criteria (BIC)

The output bit independence criteria (BIC) is found by toggling an independent bit at the input side and observing the entire change in the output bits and avalanche vectors triggered by that change. In Ref. [54] it is shown that if an S-box satisfies the nonlinearity and SAC criteria then it should also satisfy the BIC. That is, if an S-box consists of 8 Boolean functions $f_1$, $f_2$, $\ldots f_8$, then in order to fulfill BIC the

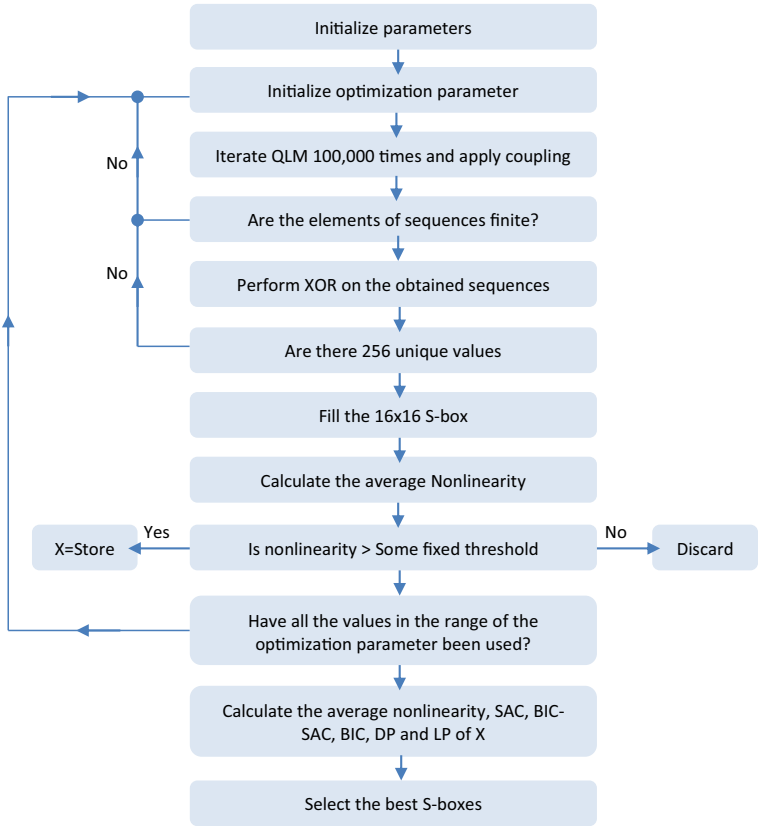


**Fig. 5** Flow chart of the optimization procedure

**Table 2** Acceptable ranges of all the parameters of QLM

| $\beta$ | $r$ | $\epsilon$ | $x_0$ | $y_0$ | $z_0$ |
|---|---|---|---|---|---|
| [6,∞) | [3.6,3.9] | [0,1] | [0,1] | [0,0.2] | [0,1) |

function $f_i \oplus f_j$, where the range of $(i, j)$ is between 1 and 8, and $i$ is not equal to $j$, must fulfill the SAC and nonlinearity criteria. So BIC can also be calculated by finding out the nonlinearity and SAC of $f_i \oplus f_j$.

### 3.5 Equiprobable Input / Output XOR Distribution

Equiprobable input/output XOR distribution or differential approximation probability (DP) is the measure of differential uniformity between input and output bits (input and output must be equiprobable). So that it could be made sure that the input bits are uniformly mapped onto the output bits, a distinct input differential $^{\triangle}x$ should uniquely map to a distinct output differential $^{\triangle}y$. The DP can be measured as in Eq. (9).

$$DP = \max_{^{\triangle}x \neq 0, ^{\triangle}y} \left( \frac{\#\{x \in X | f(x) \oplus f(x + {}^{\triangle}x) = {}^{\triangle}y\}}{2^n} \right), \tag{9}$$

where, $X$ is the set of input values and $n$ is the number of elements in it.

### 3.6 Linear Approximation Probability

The linear approximation probability (LP) is the measure f how much an S-box is robust against a linear attack. It is measure as in Eq. (10).

$$LP = \max_{\psi x, \psi y \neq 0} \left( \frac{\#\{x \in X | x \cdot \psi x = f(x) \cdot \psi x\}}{2^n} \right), \tag{10}$$

where $\psi x$ and $\psi y$ are the input and output masks.

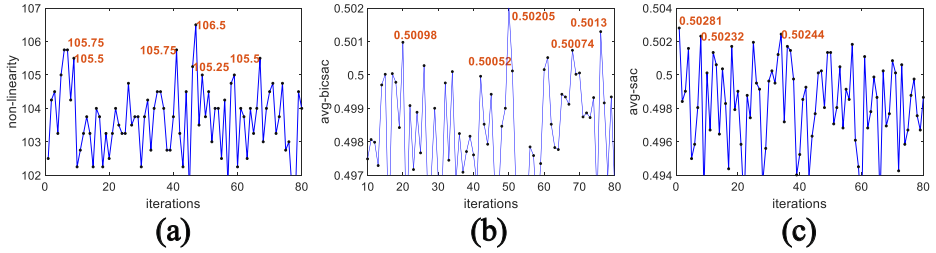


**Fig. 6** Properties of S-boxes generated by optimizing $\beta$, (**a**) nonlinearity, (**b**) average BIC-SAC, (**c**) average SAC with $r = 3.99$, $\epsilon = 0.85$, $x_0 = 0.01$, $y_0 = 0$, $z_0 = 0$, $\beta = 6 : 10$

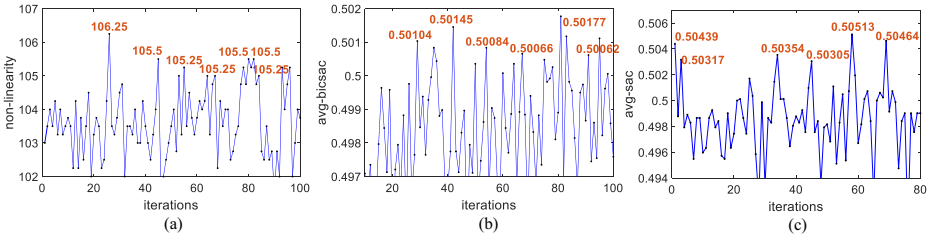


**Fig. 7** Properties of S-boxes generated by optimizing $\epsilon$, (**a**) nonlinearity, (**b**) average BIC-SAC, (**c**) average SAC with $r = 3.99$, $\beta = 6$, $x_0 = 0.01$, $y_0 = 0$, $z_0$=0, $\epsilon$=0:1

### 3.7 Annihilator Immunity

Let $f$ and $g$ be two Boolean functions which map from $\{0,1\}^n \rightarrow \{0,1\}$, then any function $g$ for which the product $f.\ g$ becomes 0 is called the annihilator of $f$ [32]. The algebraic immunity or $AI(f)$ is the lowest degree of all annihilating functions $g$ for which their product becomes 0.

### 3.8 Algebraic Degree

The algebraic degree of an S-box is the maximum numbers terms in its truth table. Eq. (11) gives the algebraic degree of an $(n, m)$ S-box, with $n$ inputs and $m$ outputs.

$$\deg\left(S_{n,m}\right) = \min\left\{\deg\left(L_j\right)\right\}, \left(j = 1, \ldots, 2^{m-1}\right), \tag{11}$$

where, $L_j$ is the set of all linear combinations of the $m$ Boolean functions of the S-box.

### 3.9 Correlation Immunity

To measure the amount of correlation between the linear combinations of input and output bits of an S-box, a measure called correlation immunity is used. Correlation immunity tells how much correlation immune an S-box is. There should be less correlation between the input and output bits of an S-box. An S-box is said to be $m^{th}$ order correlation immune if its constitutient Boolean functions follow Eq. (12).

$$\begin{aligned} 1 \leq wt(w) \leq m, \\ \hat{F}(w) = 0, \end{aligned} \tag{12}$$

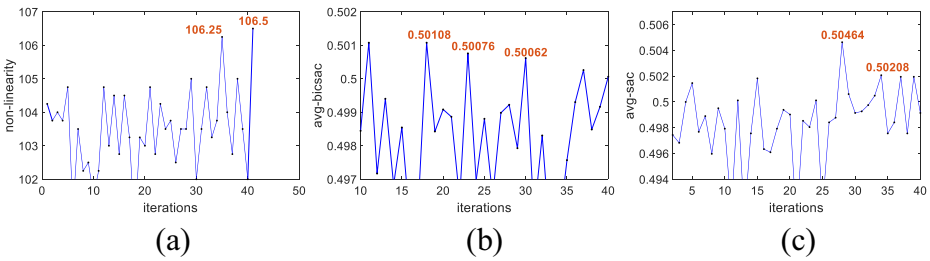


**Fig. 8** Properties of S-boxes generated by optimizing $r$, (**a**) nonlinearity, (**b**) average BIC-SAC, (**c**) average SAC with $\epsilon = 0.85$, $\beta = 8.3$, $x_0 = 0.01$, $y_0 = 0$, $z_0 = 0$, $r = 3 : 3.99$

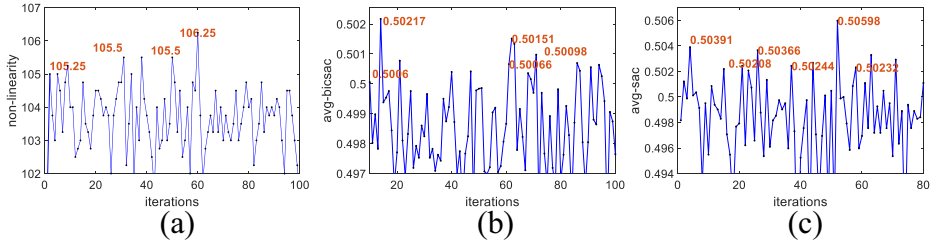


**Fig. 9** Properties of S-boxes generated by optimizing $x$, (**a**) nonlinearity, (**b**) average BIC-SAC, (**c**) average SAC with $r = 3.99$, $\beta = 8.3$, $\epsilon = 0.85$, $y_0 = 0$, $z_0 = 0$, $x_0 = 0.1 : 0.2$

where, $wt(.)$ as the hamming weight of the inputs of an $n$-variable Boolean function and $\hat{F}(w)$ as the walsh-hadamard transform of those inputs.

### 3.10 Sum of Square and Absolute Indicator

The autocorrelation of an $n$ variable Boolean function $f$ defined for all $w \in \mathbb{F}_2^n$ is given by Eq. (13).

$$\Delta_f(w) = \sum_{x \in \mathbb{F}_2^n} -1^{f(x) \oplus f(x \oplus w)}, \tag{13}$$

where, $(x \oplus w) = \{1, \ldots, 2^{n-1}\}$.The absolute indicator of a Boolean function $f$ is the maximum absolute $\Delta_f$ calculated for all $w \in \{1, \ldots, 2^{n-1}\}$, denoted by $AC_f$.Likewise, the absolute indicator of an $(n, m)$-S-box, denoted by $AC_{(n,m)}$. Let the Absolute Indicator of a linear combination of the output Boolean function of an $(n, m)$ S-box be denoted by $AC_{l_i}, \left(i = 1, \ldots, 2^{n-1}\right)$, then $AC_{(n,m)} = max(|AC_{l_i}|)$. The sum of square indicator for $f$, denoted by $\sigma_f$,is given by $\sum_w (\Delta(w))^2$.

### 3.11 Propagation Criteria

Preneel et al. generalized the concept of SAC, so that SAC became one special case in the propagation characteristics of a Boolean function [33]. Let $g \in \mathbb{F}_2^n$,then a Boolean function $f$ is said to satisfy the propagation criterion of degree $k$ ($PC(k)$), such that $1 \leq hw(g) \leq k$,if $f(x) \oplus f(x \oplus g)$ is balanced. A propagation criterion of degree 1, $PC(1)$ implies SAC. Any Boolean function is said to satisfy the propagation criterion if for any $t$ flipped inputs bits, every output vector changes with a probability of half. The SAC is equivalent to $PC(1)$ because when a

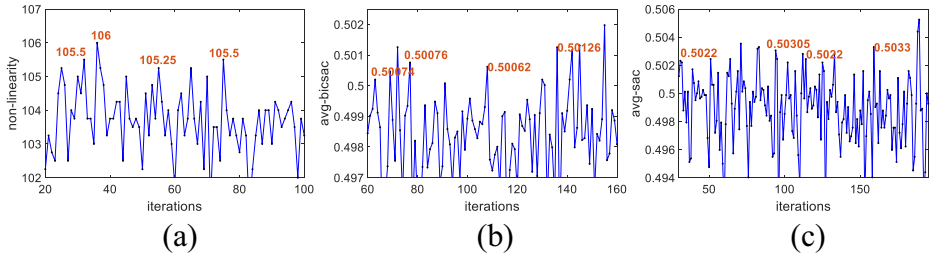


**Fig. 10** Properties of S-boxes generated by optimizing $y$, (**a**) nonlinearity, (**b**) average BIC-SAC, (**c**) average SAC with $r = 3.99$, $\beta = 8.3$, $\epsilon = 0.85$, $x_0 = 0.4$, $z_0 = 0$, $y_0 = 0 : 0.2$

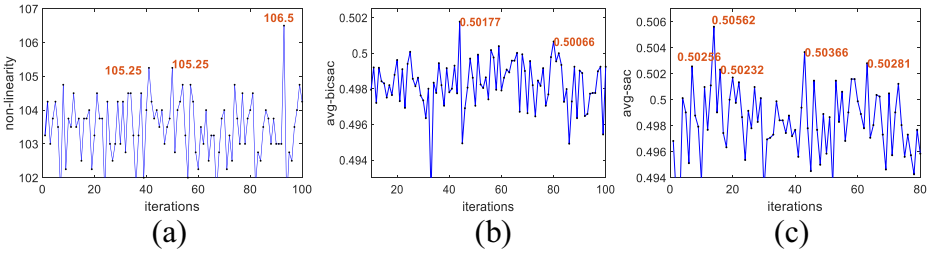


**Fig. 11** Properties of S-boxes generated by optimizing $z$, (**a**) nonlinearity, (**b**) average BIC-SAC, (**c**) average SAC with $r = 3.99$, $\beta = 8.3$, $\epsilon = 0.85$, $x_0 = 0.4$, $y_0 = 0$, $z_0 = 0.1 : 0.2$

Boolean function satisfies SAC it means that when 1 input bit is changed, the output bits change with a probability of half. An $(n, m)$ S-box is said to satisfy $PC(k)$, if all its $L_i$ satisfy the $PC(k)$.

### 3.12 Fixed Points and Opposite Fixed Points

A fixed point of an S-box is an entry in the S-box look up table where the input equals the output [34]. It can be illustrated mathematically by stating that for an $(n, m)$ S-box, $S_{n,m}(a) = a$. An opposite fixed point is a point in an S-box for which the output is the complement of the input, or mathematically, $S_{n,m}(a) = \overline{a}$. It is a good design criterion that there should be a complete absence of fixed and opposite fixed points in a cryptographically secure S-box.

### 3.13 Delta Uniformity

An $(n, m)$ S-box is said to be differentially $\delta$-uniform if for every $v \in \mathbb{F}_2^n$ and $u \in \mathbb{F}_2^m$, the equation $S_{n,m}(x) \oplus S_{n,m}(x \oplus v) = u$ gives $\delta$ solutions [34]. We say that the $\delta$-uniformity (or differential uniformity) of an S-box is $\delta$. In order to be robust against the differential cryptanalysis the $\delta$-uniformity must be low.

**Table 3** Substitution box parameter values: $r = 3.99$, $\beta = 8.3$, $\epsilon = 0.85$, $x_0 = 0.01$, $z_0 = 0$, $y_0 = 0$

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

**Table 4** Substitution box parameter values: $r = 3.99$, $\beta = 8.3$, $\epsilon = 0.85$, $x_0 = 0.01$, $z_0 = 0$, $y_0 = 0$

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

### 3.14 Differential Cryptanalysis

The differential cryptanalysis [35] exploits the high entries in the difference distribution table. Let $L$ denote the largest value in the difference distribution table of an S-box and $R$ denote the number of non-zero entries in the first column of the difference distribution table. The robustness to the differential cryptanalysis is small if $L$ or $R$ are small. Therefore, the robustness to differential cryptanalysis should be as high as possible, between 0 and 1.

### 3.15 Differential Power Analysis

The differential power analysis (DPA) is a type of side channel attack. DPA techniques exploit the varying power characteristics consumed by different types of circuits used to implement the cryptographic algorithms. In this paper we have used the varying signal to noise ratio

**Table 5** Substitution box parameter values: $r = 3.99$, $\beta = 6$, $\epsilon = 0.25$, $x_0 = 0.01$, $z_0 = 0$, $y_0 = 0$

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

**Table 6** Substitution box parameter values: $r = 3.99$, $\beta = 8.3$, $\epsilon = 0.85$, $x_0 = 0.159$, $z_0 = 0$, $y_0 = 0$

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

(SNR) to measure the DPA of the proposed S-boxes. SNR (DPA) with a high value closer to 9.6 is desirable for S-boxes robust against the DPA attacks [36].

## 4 Proposed Substitution Box Construction

The proposed substitution boxes are constructed using the following strategy. There are six control parameters in total given by Eqs. (1)–(2) combined: $r$, $\beta$, $\epsilon$, $x_0$, $y_0$, and $z_0$. The S-boxes are constructed by looping through the Eqs. (1)–(2) to generate unique sequences which are then shaped into $8 \times 8$ S-boxes, then selecting the best S-boxes from them. Starting from the parameter $\beta$, every control parameter is optimized to give the best S-boxes. Figure 5 shows the flow diagram of the proposed procedure.

The following steps describe the proposed procedure. The procedure is divided into three sections for the ease of understanding.

**Table 7** Substitution box parameter values: $r = 3.93$, $\beta = 8.3$, $\epsilon = 0.85$, $x_0 = 0.01$, $z_0 = 0$, $y_0 = 0$

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

**Table 8** SAC and BIC-SAC of S-boxes from step 15

| S-box No | Min. SAC | Max. SAC | Avg. SAC | Min. BIC-SAC | Avg. BIC-SAC |
|---|---|---|---|---|---|
| 1 | 0.421875 | 0.609375 | 0.506836 | 0.46680 | 0.49993 |
| 2 | 0.421875 | 0.593750 | 0.496582 | 0.46484 | 0.49637 |
| 3 | 0.406250 | 0.625000 | 0.494141 | 0.44336 | 0.50056 |
| 4 | 0.406250 | 0.609375 | 0.501465 | 0.47461 | 0.49770 |
| 5 | 0.406250 | 0.625000 | 0.504883 | 0.46680 | 0.50098 |

I. **Parameter selection and values initialization:**

1. Select the parameter for optimization. (e.g. $\beta$)
2. Keeping the limitations on the values of parameters (e.g. $0 < \epsilon < 1$) in mind, select the values for the remaining control parameters and initial conditions.
3. Select a fresh value of the optimization parameter from the range given in Table 2.

II. **Optimization:**

4. Iterate Eq. (1) then Eq. (2), 100,000 times to generate the three random sequences $\overline{X}, \overline{Y}, \overline{Z}$.
5. Multiply the three sequences with 1000,000, take their modulo 256, then floor of the resulting three sequences to obtain *XX*, *YY* and *ZZ*.
6. Check if the sequences *XX*, *YY* and *ZZ* consist of real, finite integers. If the condition turns out true, then proceed to next step. Otherwise go to step 3.
7. Apply the XOR operation between the sequences *XX* and *YY*, and store the resulting sequence in the vector $xor_1$.
8. Apply the XOR operation between the sequences $xor_1$ and *ZZ* and store the new sequence in the vector $xor_2$.
9. Select all the unique values as they first appear (from left to right) in the sequence $xor_2$.
10. Check if there are 256 unique values in the range 0–255. If yes, then proceed to next step, otherwise go to Step 3.
11. Store the 256 unique values in a $16 \times 16$ matrix to obtain the S-box.
12. Calculate and store the average nonlinearity, SAC and BIC-SAC of the constructed S-box.
13. If the average nonlinearity of the obtained S-box is above 106, store the S-box.
14. Repeat steps 3–14 until the desired limit for the optimization parameter (given in Table 2 has reached)

**Table 9** BIC, Nonlinearity, DP and LP of proposed S-boxes

| S-box No | Min. BIC | Avg. BIC | Avg. $N_f$ | Max. DP | Max. Count LP | Max. Value LP |
|---|---|---|---|---|---|---|
| 1 | 96 | 103.21 | 106.5 | 12 | 162 | 0.132 |
| 2 | 98 | 104.35 | 106.25 | 10 | 158 | 0.117 |
| 3 | 96 | 103.35 | 106.25 | 12 | 160 | 0.125 |
| 4 | 92 | 103.50 | 106.25 | 10 | 164 | 0.140 |
| 5 | 92 | 103.42 | 106.50 | 12 | 164 | 0.140 |

**Table 10** Nonlinearity of the final selected S-boxes

| S-box | $N_1$ | $N_2$ | $N_3$ | $N_4$ | $N_5$ | $N_6$ | $N_7$ | $N_8$ | Min $N_f$ | Max $N_f$ | Avg. $N_f$ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 108 | 108 | 106 | 104 | 106 | 108 | 104 | 108 | 104 | 108 | 106.5 |
| 2 | 110 | 106 | 102 | 108 | 106 | 104 | 108 | 106 | 102 | 110 | 106.25 |

III. **S-box evaluation and final selection:**

15. Check if there are two or more similar S-boxes from step 13. If yes, keeping the unique ones, discard all the repeating S-boxes.
16. Evaluate the properties given in section 2, of the remaining S-boxes from step 15.
17. Select the S-boxes with best possible results.

The optimization parameters are $r$, $\beta$, $\epsilon$, $x_0$, $y_0$, and $z_0$. The above mentioned steps are performed on these six parameters one by one. Now suppose if the parameter $r$ is being optimized, then all other parameters will remain constant till the end of the above mentioned procedure. The range of varying the optimization parameters are given in Table 2. It is most suitable to start the above optimization procedure (Step 2) by taking the initial value of the optimization parameter somewhere around the starting range mentioned in Table 2, and end the optimization procedure (Step 10) with the ending range. The nonlinearity is the most important property of any S-box, so the S-boxes are first evaluated according to their nonlinearity. If the nonlinearity is below 106, the S-box is totally rejected (Step 9). As mentioned before, the S-boxes obtained entirely from chaos mostly do not achieve average non-linearity value more than 105. Therefore, our algorithm is designed to check if QLM is capable of achieving greater nonlinearity than 106. If the results favor more nonlinearity, then the QLM might become a suitable candidate to be used as a tool in fast and easy S-box generation for sensitive and secret communications.

The results of parameter optimization are given and discussed in the following section.

## 5 Results and Discussions

We have plotted the graphs of the average nonlinearity, SAC and BIC-SAC of the generated S-boxes obtained in step 12, against the varying optimization parameters, one by one. Figure 6

**Table 11** Dependence matrix of proposed S-box 1

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 0.531 | 0.484 | 0.516 | 0.484 | 0.547 | 0.547 | 0.563 | 0.453 |
| 0.563 | 0.531 | 0.531 | 0.484 | 0.594 | 0.500 | 0.469 | 0.469 |
| 0.500 | 0.469 | 0.469 | 0.500 | 0.484 | 0.438 | 0.484 | 0.516 |
| 0.516 | 0.516 | 0.500 | 0.547 | 0.500 | 0.500 | 0.578 | 0.563 |
| 0.500 | 0.531 | 0.484 | 0.438 | 0.469 | 0.469 | 0.469 | 0.531 |
| 0.438 | 0.516 | 0.516 | 0.469 | 0.531 | 0.469 | 0.469 | 0.563 |
| 0.406 | 0.516 | 0.453 | 0.484 | 0.516 | 0.625 | 0.453 | 0.500 |
| 0.547 | 0.484 | 0.563 | 0.500 | 0.500 | 0.500 | 0.547 | 0.516 |

**Table 12** Dependence matrix of proposed S-box 2

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 0.531 | 0.469 | 0.453 | 0.469 | 0.531 | 0.531 | 0.484 | 0.500 |
| 0.453 | 0.453 | 0.438 | 0.531 | 0.484 | 0.563 | 0.531 | 0.578 |
| 0.469 | 0.484 | 0.531 | 0.500 | 0.484 | 0.453 | 0.531 | 0.484 |
| 0.453 | 0.469 | 0.516 | 0.516 | 0.516 | 0.531 | 0.516 | 0.531 |
| 0.438 | 0.453 | 0.453 | 0.531 | 0.469 | 0.547 | 0.438 | 0.547 |
| 0.563 | 0.594 | 0.531 | 0.516 | 0.500 | 0.500 | 0.547 | 0.453 |
| 0.500 | 0.469 | 0.422 | 0.469 | 0.500 | 0.422 | 0.531 | 0.453 |
| 0.531 | 0.484 | 0.484 | 0.547 | 0.484 | 0.438 | 0.484 | 0.500 |

shows the graphs of nonlinearity, SAC and BIC-SAC against the parameter $\beta$, while in Fig. 7 these evaluation tools are plot against the parameter $\epsilon$, and so on.

These figures show the sensitivity of varying the optimization parameter. As the optimization parameter is increased slightly, there is a drastic change in the nonlinearity, SAC and BIC-SAC values obtained for the next generated S-box. Therefore, these six input parameters can serve as security keys for the generation of any S-box in order to perform secure communication and data encryption. Only the individual with the knowledge of the secret keys will be able to reconstruct the S-box applied to encrypt any data. Furthermore, the QLM has proven itself as a useful tool for robust, easy, secure and fast S-box construction as the values of the security parameters for the chosen S-boxes are quite good, and better than many chaos based S-box generation algorithms [1–6]. In Figs. 6, 7, 8, 9, 10 and 11, nonlinearity values greater than 105 and, SAC and BIC-SAC values greater than 0.5005 are marked in green to make them distinguishable. As can be seen from Figs. 6, 7, 8, 9, 10 and 11a, there are six S-boxes in total that have an average nonlinearity greater than 106. But out of these, two are the same; therefore, we are left with five S-boxes to select from. In the next section, we analyze the remaining 5 S-boxes and perform steps 16 and 17. The resulting 5 S-boxes of Step 15 are given above (Tables 3, 4, 5, 6 and 7). These S-boxes are the result of obtaining all S-boxes of nonlinearity greater than 106 and deleting the duplicate S-boxes. In Step 16, the S-boxes are analyzed to obtain the best possible S-boxes. In steps 16 the 5 remaining S-boxes are analyzed by computing all of their cryptographic security properties and comparing them together and then the S-box with the best properties are selected. Tables 8 and 9 give the summary of all the S-box evaluation tests performed on the 5 S-boxes. $N_f$ represents the final nonlinearity of the given S-box.

It can be seen from Tables 8 and 9, that the best nonlinearity component is that of S-box 1 and 5, but the maximum LP count is also a very important factor when it comes to the differential security of the S-boxes, whose value is best for S-box 1 and 2. The value best for

**Table 13** BIC nonlinearity of proposed S-box 1

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| – | 104 | 102 | 104 | 106 | 98 | 106 | 106 |
| 104 | – | 96 | 104 | 102 | 98 | 104 | 108 |
| 102 | 96 | – | 106 | 104 | 100 | 106 | 108 |
| 104 | 104 | 106 | – | 108 | 106 | 106 | 104 |
| 106 | 102 | 104 | 108 | – | 92 | 104 | 98 |
| 98 | 98 | 100 | 106 | 92 | – | 104 | 108 |
| 106 | 104 | 106 | 106 | 104 | 104 | – | 104 |
| 106 | 108 | 108 | 104 | 98 | 108 | 104 | – |

**Table 14** BIC nonlinearity of proposed S-box 2

| – | 104 | 104 | 106 | 104 | 98 | 104 | 106 |
|---|---|---|---|---|---|---|---|
| 104 | – | 100 | 104 | 104 | 106 | 104 | 106 |
| 104 | 100 | – | 106 | 104 | 108 | 106 | 108 |
| 106 | 104 | 106 | – | 102 | 104 | 106 | 106 |
| 104 | 104 | 104 | 102 | – | 106 | 100 | 108 |
| 98 | 106 | 108 | 104 | 106 | – | 100 | 106 |
| 104 | 104 | 106 | 106 | 100 | 100 | – | 102 |
| 106 | 106 | 108 | 106 | 108 | 106 | 102 | – |

maximum DP is best of S-box 2 and 4, but S-box 4 does not exhibit good LP property. The best value of BIC-nonlinearity is that of S-box 2. Furthermore, it can also be said that there is not much difference between the nonlinearity values 106.5 and 106.25, and more votes are bended towards S-box 2, except for the lower nonlinearity, i.e. 106.25. So, if not considering the low nonlinearity, the best S-box is S-box 2. But we suggest that for those applications in which the value of nonlinearity is of great importance, they should use the S-box 1, while those applications which are sensitive to differential attacks must use the S-box 2. Therefore, we propose two final S-boxes, i.e. S-box1 and S-box 2. The detailed analysis of the two final proposed S-boxes is given in the next section.

## 5.1 Detailed Analysis of the Proposed S-Boxes

The final proposed S-boxes are S-box 1 and 2, given in Tables 3 and 4, respectively. This section details the results and discussion of the proposed S-boxes.

### 5.1.1 Nonlinearity

The nonlinearity of most chaos based good S-boxes is more than 105 on average, with 112 being the highest average nonlinearity achieved till date. The more the nonlinearity, the better is the nonlinear content in the S-box. The optimization of QLM has proven to generate S-boxes of nonlinearity more than 106. Table 10 shows that the minimum nonlinearity of both the proposed S-boxes is no less than 102, while the maximum nonlinearity is 108 and 110 for S-box1 and 2, respectively, while the average of S-box 1 and 2 is 106.5 and 106.25, respectively. It can also be seen from the comparison given in Table 19 that the proposed S-boxes are better than some already proposed S-boxes in literature.

**Table 15** BIC of SAC of Proposed S-box 1

| – | 0.508 | 0.502 | 0.498 | 0.529 | 0.492 | 0.510 | 0.477 |
|---|---|---|---|---|---|---|---|
| 0.508 | – | 0.496 | 0.512 | 0.498 | 0.473 | 0.475 | 0.500 |
| 0.502 | 0.496 | – | 0.535 | 0.496 | 0.500 | 0.506 | 0.498 |
| 0.498 | 0.512 | 0.535 | – | 0.514 | 0.486 | 0.467 | 0.498 |
| 0.529 | 0.498 | 0.496 | 0.514 | – | 0.492 | 0.535 | 0.488 |
| 0.492 | 0.473 | 0.500 | 0.486 | 0.492 | – | 0.506 | 0.510 |
| 0.510 | 0.475 | 0.506 | 0.467 | 0.535 | 0.506 | – | 0.527 |
| 0.477 | 0.500 | 0.498 | 0.498 | 0.488 | 0.510 | 0.527 | – |

**Table 16** BIC of SAC of Proposed S-box 2

| – | 0.492 | 0.494 | 0.523 | 0.508 | 0.500 | 0.504 | 0.516 |
|---|---|---|---|---|---|---|---|
| 0.492 | – | 0.502 | 0.506 | 0.465 | 0.496 | 0.502 | 0.504 |
| 0.494 | 0.502 | – | 0.510 | 0.482 | 0.475 | 0.514 | 0.473 |
| 0.523 | 0.506 | 0.510 | – | 0.486 | 0.479 | 0.482 | 0.498 |
| 0.508 | 0.465 | 0.482 | 0.486 | – | 0.527 | 0.498 | 0.496 |
| 0.500 | 0.496 | 0.475 | 0.479 | 0.527 | – | 0.490 | 0.486 |
| 0.504 | 0.502 | 0.514 | 0.482 | 0.498 | 0.490 | – | 0.490 |
| 0.516 | 0.504 | 0.473 | 0.498 | 0.496 | 0.486 | 0.490 | – |

### 5.1.2 Strict Avalanche Criteria

The ideal value of SAC is 0.5 which can be obtained by averaging over all the elements of the dependence table. The less the difference between the SAC and 0.5, the better is the S-box. Tables 11 and 12 give the dependence tables of the proposed S-boxes. It can be seen from the tables that all the elements of the dependence table are very much near to 0.4 and 0.5. Table 19 gives a summary of the minimum, maximum and average value of SAC for both the proposed S-boxes, obtained from their dependence tables. The minimum value of SAC is 0.42 for both the S-boxes, while the maximum is 0.61 and 0.59, respectively. The average values for both S-boxes are 0.506 and 0.597, which are very much close to 0.5, making the S-boxes fulfill the SAC test.

### 5.1.3 Bit Independence Criteria

As mentioned before, if an S-box fulfills the non-linearity and SAC criteria then it must also fulfill the BIC test. So both our S-boxes do pass the BIC test as their nonlinearity is good and the SAC is near to 0.5. But still for better evaluation we have drawn the BIC-nonlinearity Tables 13 and 14 for both the proposed S-boxes. From the tables it can be seen the minimum value of the BIC nonlinearity of both the S-boxes is 96 and 98, respectively. While the average BIC-nonlinearity is 103.214 and 104.357, respectively, which is acceptable for a good S-box.

**Table 17** Differential approach table for the chosen S-box 1

| 0 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 8 | 6 | 6 | 8 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 6 | 8 | 6 | 6 | 6 | 6 | 8 | 10 | 6 | 6 | 8 | 8 | 10 | 4 | 6 | 8 |
| 10 | 6 | 8 | 8 | 4 | 8 | 6 | 6 | 6 | 8 | 8 | 4 | 6 | 4 | 6 | 6 |
| 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 8 | 6 | 6 | 6 | 6 | 6 |
| 6 | 6 | 10 | 8 | 6 | 6 | 6 | 6 | 6 | 8 | 8 | 6 | 8 | 8 | 8 | 8 |
| 10 | 6 | 8 | 8 | 6 | 6 | 6 | 6 | 8 | 6 | 6 | 6 | 6 | 6 | 6 | 8 |
| 6 | 6 | 6 | 8 | 8 | 8 | 6 | 8 | 6 | 8 | 8 | 6 | 6 | 8 | 12 | 8 |
| 6 | 8 | 6 | 6 | 8 | 8 | 8 | 6 | 8 | 8 | 6 | 6 | 8 | 8 | 6 | 6 |
| 6 | 6 | 10 | 6 | 6 | 8 | 8 | 6 | 8 | 6 | 8 | 6 | 8 | 6 | 6 | 6 |
| 6 | 4 | 8 | 6 | 6 | 6 | 6 | 6 | 6 | 8 | 6 | 8 | 6 | 8 | 6 | 6 |
| 6 | 6 | 8 | 8 | 8 | 6 | 8 | 6 | 8 | 8 | 8 | 8 | 6 | 6 | 6 | 6 |
| 8 | 8 | 6 | 8 | 8 | 6 | 8 | 8 | 6 | 8 | 6 | 6 | 6 | 6 | 6 | 6 |
| 6 | 6 | 6 | 6 | 8 | 8 | 6 | 10 | 8 | 6 | 8 | 6 | 8 | 8 | 8 | 10 |
| 6 | 8 | 6 | 8 | 8 | 6 | 6 | 8 | 6 | 8 | 6 | 6 | 8 | 6 | 6 | 6 |
| 8 | 6 | 8 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 8 | 6 | 6 | 8 | 6 | 6 |
| 6 | 8 | 6 | 6 | 6 | 6 | 6 | 6 | 10 | 6 | 6 | 6 | 6 | 6 | 10 | 6 |

**Table 18** Differential approach table for the chosen S-box 2

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 6 | 6 | 8 | 6 | 6 | 6 | 6 | 6 | 8 | 8 | 8 | 6 | 8 | 6 | 6 |
| 6 | 6 | 6 | 6 | 4 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 8 |
| 8 | 8 | 6 | 6 | 6 | 6 | 6 | 8 | 10 | 8 | 8 | 8 | 6 | 8 | 6 | 8 |
| 8 | 6 | 10 | 8 | 8 | 6 | 6 | 6 | 4 | 6 | 4 | 8 | 6 | 6 | 8 | 6 |
| 6 | 6 | 6 | 6 | 8 | 8 | 6 | 8 | 8 | 8 | 6 | 8 | 6 | 6 | 8 | 6 |
| 6 | 8 | 8 | 6 | 6 | 8 | 6 | 6 | 6 | 8 | 6 | 6 | 6 | 6 | 6 | 8 |
| 6 | 6 | 6 | 6 | 8 | 6 | 8 | 6 | 8 | 8 | 8 | 6 | 8 | 6 | 6 | 6 |
| 8 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 8 | 6 |
| 6 | 6 | 6 | 6 | 6 | 6 | 6 | 8 | 6 | 6 | 8 | 6 | 8 | 8 | 6 | 6 |
| 8 | 6 | 6 | 10 | 8 | 6 | 8 | 6 | 8 | 6 | 6 | 6 | 4 | 8 | 6 | 6 |
| 8 | 8 | 8 | 8 | 6 | 6 | 6 | 8 | 8 | 6 | 6 | 8 | 6 | 8 | 8 | 6 |
| 6 | 8 | 8 | 6 | 8 | 8 | 8 | 6 | 8 | 6 | 8 | 10 | 6 | 6 | 8 | 6 |
| 8 | 6 | 6 | 6 | 6 | 8 | 6 | 6 | 6 | 10 | 6 | 6 | 6 | 6 | 6 | 6 |
| 6 | 8 | 8 | 8 | 8 | 6 | 8 | 6 | 6 | 6 | 6 | 8 | 6 | 6 | 8 | 8 |
| 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 8 | 6 | 6 | 6 | 8 | 8 | 6 |
| 6 | 6 | 6 | 6 | 6 | 8 | 6 | 6 | 8 | 6 | 8 | 6 | 8 | 6 | 6 | 6 |

### 5.1.4 BIC of SAC

The value of BIC-SAC, like SAC, is ideally 0.5. Tables 15 and 16 show the dependence tables for the proposed S-boxes. The lowest entry in the dependence table of both the S-boxes is 0.47 and the average of all the values is 0.45 and 0.5 for S-box1 and 2, respectively. These values show that the proposed S-boxes fulfill the BIC-SAC test.

### 5.1.5 Differential Probability

For an S-box to be secure, the value of DP should be as low as possible. The values for DP for the proposed S-boxes are tabulated in Tables 17 and 18. The maximum value is 12 for both S-box 1 and 10 for S-box 2, which is better than the first S-box. That is why we have recommended using the S-box 2 where there is more danger of differential cryptanalysis attack.

### 5.1.6 Some Advanced Properties

Table 19 gives the summary of the properties of the proposed S-boxes. Table 20 gives the advanced cryptographic properties of some of the recent S-boxes with nonlinearity almost equal to 106. The table.

indicates comparison of the proposed S-boxes and these recently proposed S-boxes with similar nonlinearities. The values of the given cryptographic properties show that our proposed

**Table 19** Summary of proposed S-box analysis

| | Nonlinearity | | | SAC | | | BIC | | | BIC-SAC | | LP | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| S-box | Min. | Max. | Avg. | Min | Max | Avg. | Min. | Avg. | Min. | Avg. | DP | Count | Value |
| 1 | 104 | 108 | 106.5 | 0.421 | 0.609 | 0.506 | 96 | 103.2 | 0.466 | 0.499 | 12 | 162 | 0.132 |
| 2 | 102 | 110 | 106.25 | 0.421 | 0.593 | 0.496 | 98 | 104.4 | 0.464 | 0.496 | 10 | 158 | 0.117 |

**Table 20** Some other cryptographic properties of substitution boxes [38, 39]

| | Proposed substitution boxes | | | | | Some recent modern substitution boxes | | | | | | Standard | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Proposed1 | Proposed2 | Proposed3 | Proposed4 | Proposed5 | Ref. [27] | Ref. [28] | Ref. [29] | Ref. [30] | Ref. [25] | Ref. [31] | AES | APA |
| Nonlinearity | 106 | 106 | 106 | 106 | 106 | 106 | 106 | 106 | 103 | 106 | 103 | 112 | 112 |
| Correlation immunity | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Absolute indicator | 96 | 96 | 88 | 96 | 96 | 112 | 96 | 96 | 96 | 104 | 92 | 32 | 32 |
| Sum of square indicator | 264,832 | 294,016 | 266,368 | 281,728 | 290,560 | 275,584 | 274,816 | 269,056 | 330,496 | 251,776 | 278,272 | 133,120 | 133,120 |
| Algebraic degree | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 8 | 7 | 7 |
| AI*1 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| Transparency order | 7.812 | 7.8 | 7.827 | 7.795 | 7.819 | 7.817 | 7.812 | 7.81 | 7.816 | 7.798 | 7.803 | 7.86 | 7.859 |
| Propagation criteria | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| No. of FP*2 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 0 | 2 | 1 | 0 | 0 |
| No. of opposite FP | 1 | 1 | 1 | 1 | 0 | 1 | 2 | 1 | 0 | 3 | 0 | 0 | 2 |
| Composite AI | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| Robustness to DC*3 | 0.953 | 0.961 | 0.953 | 0.961 | 0.953 | 0.961 | 0.961 | 0.961 | 0.961 | 0.961 | 0.953 | 0.984 | 0.984 |
| SNR (DPA)*4 | 9.212 | 9.312 | 9.594 | 9.577 | 8.671 | 9.766 | 9.015 | 9.612 | 9.278 | 9.543 | 9.303 | 9.6 | 8.91 |

*1 AI is the algebraic immunity. *2 FP stands for fixed points. *3 DC stands for differential cryptanalysis. *4 SNR (DPA) is the signal to noise ratio, differential power analysis

**Table 21** NIST tests of randomness

| | Proposed S-box 1 | | | Proposed S-box 1 | | |
|---|---|---|---|---|---|---|
| | *p*-value | Proportion | Outcome | *p*-value | Proportion | Outcome |
| Block frequency | 0.598714 | 1/1 | Pass | 0.994364 | 1/1 | Pass |
| Cumulative sums | 0.989269 | 2/2 | Pass | 0.999477 | 2/2 | Pass |
| Fast Fourier transform | 0.330390 | 1/1 | Pass | 0.967650 | 1/1 | Pass |
| Frequency | 1.000000 | 1/1 | Pass | 1.000000 | 1/1 | Pass |
| Longest runs | 0.716298 | 1/1 | Pass | 0.767028 | 1/1 | Pass |
| Non-overlapping template | 0.563400 | 144/148 | Pass | 0.566500 | 145/148 | Pass |
| Overlapping template | 0.295708 | 1/1 | Pass | 0.886589 | 1/1 | Pass |
| Rank | 0.481248 | 1/1 | Pass | 0.741908 | 1/1 | Pass |
| Runs | 0.215925 | 1/1 | Pass | 0.859684 | 1/1 | Pass |
| Serial | 0.178011 | 2/2 | Pass | 0.471947 | 2/2 | Pass |

S-boxes possess similar or better properties than the S-boxes of comparisons proposed by some famous researchers.

## 5.2 Randomness Testing

In order to test if the elements of an S-box follow a random order, the NIST statistical test suite is applied on S-boxes. There are in total there are 188 NIST tests in the randomness testing suite, but of out of them a few are not applicable to S-boxes. In total 159 tests are applicable to S-boxes. These 159 tests are summarized under 10 headings in this paper. For the purpose of running the tests the S-boxes are converted to a one dimensional string of 2048 binary bits. This string is then input to perform the randomness testing. The tests applicable to S-boxes are block frequency, cumulative sums, fast Fourier transform, frequency, longest runs, non-overlapping template, overlapping template, rank, runs and serial tests. There is only one sub-test in the block frequency, fast Fourier, frequency, longest runs, overlapping template, rank and runs test. There are two sub-tests in the cumulative sums and serial tests, while the non-overlapping template consists of 148 sub-tests, therefore making 159 randomness tests applied to our S-boxes. The tests are designed in such a way that every test results in a *p*-value. If the found *p*-value is equal to 0 or less than 0.01 it indicates a non-random sequence. If the *p*-value is greater than or equal to 0.01 it indicates a random sequence. And if the *p*-value equals 1, the sequence provided is perfectly random. The results of NIST randomness testing on S-box 1 and 2 are shown in Table 21. To summarize it all, the proposed S-box 1 passed 155 tests

**Table 22** Comparison with other S-boxes

| S-box | Nonlinearity | SAC | BIC | BICSAC | DP | LP |
|---|---|---|---|---|---|---|
| Proposed 1 | 106.5 | 0.506 | 103.2 | 0.499 | 12 | 0.132 |
| Proposed 2 | 106.25 | 0.496 | 104.3 | 0.496 | 10 | 0.117 |
| Skipjack | 105.75 | 0.503 | 104.1 | 0.499 | 12 | 0.109 |
| Ref [1] | 105.25 | 0.498 | 103.7 | 0.498 | 12 | 0.125 |
| Ref [2] | 104.70 | 0.578 | 103.1 | 0.494 | 12 | – |
| Ref [4] | 106.00 | 0.519 | 104.2 | 0.501 | 10 | 0.132 |
| Ref [5] | 104.50 | 0.498 | 104.6 | 0.507 | 12 | 0.125 |
| Ref [24] | 104.00 | 0.4999 | – | – | 06 | 0.109 |
| Ref [25] | 106.00 | 0.529 | 100.0 | – | 10 | 0.071 |

out of 159 while the proposed S-box 2 passed 157 tests out of 159 tests. This concludes that the proposed substitution boxes are random as they pass almost all the NIST randomness tests that are applicable to the S-boxes.

### 5.3 Comparison of the Proposed S-Boxes with Other Common Schemes

A comparison table is given in Table 22. The nonlinearity of the proposed S-boxes is not as good as the AES S-box, but as compared to other chaos based schemes, it gives quite good results. As mentioned earlier, the chaos based schemes do not exhibit nonlinearities much more than 105. Considering this, the QLM exhibits good nonlinearity. The proposed S-box 2 can compete in the BIC-SAC as its value is higher than most chaos based algorithms. The values for DP and LP are also good compared to the rest of the S-boxes mentioned here.

## 6 Conclusion and Future Scope

In this research article, we have utilized quantum logistic chaotic iterative map to design a new mechanism for the confusion component immensely utilized in modern secure block ciphers. The suggested confusion element has robust characteristics which fulfills the requirements of resilient encryption mechanism in real time environment. The offered substitution boxes have a vast amount of possible usage in systems which need fast S-box generation with optimal security features. The projected mechanism can be utilized to generate similar S-boxes dynamically as the generated S-boxes would all possess almost equal characteristics. The optimization procedure can be applied to any chaotic iterative map to generate new S-boxes with resistant cryptographic properties.

**Acknowledgments** Authors are highly thankful to Chancellor Dr. Syed Wilayat Hussain, Institute of Space Technology, Islamabad Pakistan, for providing conducive environment for research and development.

### Compliance with Ethical Standards

**Conflict of Interest** There is no any conflict of interest among the authors regarding the publication of this article.

## References

1. Khan, M., Shah, T., Mahmood, H., Gondal, M.A.: An efficient method for the construction of block cipher with multi-chaotic systems. Nonlinear Dyn. **71**, 493–504 (2013)
2. Ahmad, M., Ahmad, F., Nasim, Z., Bano, Z., Zafar, S.: Designing chaos based strong substitution box. In Contemporary Computing (IC3), 2015 Eighth International Conference on (pp. 97-100). IEEE
3. Özkaynak, F., Çelik, V., Özer, A.B.: A new S-box construction method based on the fractional-order chaotic Chen system. SIViP. **11**(4), 659–664 (2017)
4. Wang, X., Akgul, A., Cavusoglu, U., Pham, V.T., Vo Hoang, D., Nguyen, X.: A chaotic system with infinite equilibria and its S-Box constructing application. Appl. Sci. **8**(11), 2132 (2018)
5. Liu, L., Zhang, Y., Wang, X.: A novel method for constructing the S-box based on spatiotemporal chaotic dynamics. Appl. Sci. **8**(12), 2650 (2018)
6. Lambić, D.: A novel method of S-box design based on chaotic map and composition method. Chaos, Solitons Fractals. **58**, 16–21 (2014)
7. Asim, M., Jeoti, V.: Efficient and simple method for designing chaotic Sboxes. ETRI J. **1**, 170–172 (2008)

8. Chen, G.: A novel heuristic method for obtaining S-boxes. Chaos Solitons Fractals. **36**, 1028–1036 (2008)
9. Tian, Y., Lu, Z.: Chaotic S-box: intertwining logistic map and bacterial foraging optimization. Math. Probl. Eng. **2017**, 1–11 (2017)
10. Sam, I.S., Devaraj, P., Bhuvaneswaran, R.S.: An intertwining chaotic maps based image encryption scheme. Nonlinear Dyn. **69**(4), 1995–2007 (2012)
11. Passino, K.M.: Biomimicry of bacterial foraging for distributed optimization and control. IEEE Control. Syst. Mag. **22**(3), 52–67 (2002)
12. Zaibi, G., Kachouri, A., Peyrard, F., & Fournier-Prunaret, D. (2009, June). On dynamic chaotic s-box. In 2009 Global Information Infrastructure Symposium (pp. 1-5). IEEE
13. Ahmad, M., Chugh, H., Goel, A., Singla, P.: A chaos based method for efficient cryptographic S-box design. In: International Symposium on Security in Computing and Communication, pp. 130–137. Springer, Berlin, Heidelberg (2013)
14. Belazi, A., El-Latif, A.: A simple yet efficient S-box method based on chaotic sine map. Optik. **130**, 1438–1444 (2017)
15. Khan, M., Shah, T.: Construction and applications of chaotic S-boxes in image encryption. Neural Comput. Applic. **27**, 677–685 (2016)
16. Khan, M., Shah, T.: A new implementations of chaotic S-boxes in CAPTCHA. SIViP. **10**, 293–300 (2016)
17. Khan, M., Waseem, H.M.: A novel image encryption scheme based on quantum dynamical spinning and rotations. PLoS ONE. **13**(11), e0206460
18. Khan, M.: A novel image encryption scheme based on multi-parameters chaotic S-boxes. Nonlinear Dyn. **82**, 527–533 (2015)
19. Khan, M.: An image encryption by using Fourier series. J. Vib. Control. **21**, 3450–3455 (2015)
20. Khan, M., Shah, T.: An efficient construction of substitution box with fractional chaotic system. SIViP. **9**, 1335–1338 (2015)
21. Waseem, H.M., Khan, M.: A new approach to digital content privacy using quantum spin and finite-state machine. Appl. Phys. B. **125**, 27 (2019). https://doi.org/10.1007/s00340-019-7142-y
22. Waseem, H.M., Khan, M.: Information confidentiality using quantum spinning, rotation and finite state machine. Int. J. Theor. Phys. **57**(11), 3584–3594 (2018)
23. Silva-García, V.M., Flores-Carapia, R., Rentería-Márquez, C., Luna-Benoso, B., Aldape-Pérez, M.: Substitution box generation using Chaos: an image encryption application. Appl. Math. Comput. **332**, 123–135 (2018)
24. Khan, M.A., Ali, A., Jeoti, V., Manzoor, S.: A chaos-based substitution box (S-box) design with improved differential approximation probability (DP). Iranian Journal of Science and Technology, Transactions of Electrical Engineering. **42**(2), 219–238 (2018)
25. Lambić, D.: S-box design method based on improved one-dimensional discrete chaotic map. Journal of Information and Telecommunication. **2**(2), 181–191 (2018)
26. Özkaynak, F.: An analysis and generation toolbox for chaotic substitution boxes: a case study based on chaotic labyrinth rene thomas system. Iranian Journal of Science and Technology, Transactions of Electrical Engineering https://doi.org/10.1007/s40998-019-00230-6(0123456789()
27. Anees, A., Ahmed, Z.: A technique for designing substitution box based on van der pol oscillator. Wirel. Pers. Commun. **82**(3), 1497–1503 (2015)
28. 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. **87**(2), 1081–1094 (2017)
29. Farah, T., Rhouma, R., Belghith, S.: A novel method for designing S-box based on chaotic map and teaching–learning-based optimization. Nonlinear Dyn. **88**(2), 1059–1074 (2017)
30. ul Islam, F., Liu, G.: Designing S-box based on 4D-4wing hyperchaotic system. 3D Res. **8**(1), 9 (2017)
31. Özkaynak, F., Özer, A.B.: A method for designing strong S-boxes based on chaotic Lorenz system. Phys. Lett. A. **374**(36), 3733–3738 (2010)
32. Braeken, A. (2006). Cryptographic properties of Boolean functions and S-boxes (Doctoral dissertation, phd thesis-2006)
33. Preneel, B., Van Leekwijck, W., Van Linden, L., Govaerts, R., & Vandewalle, J. (1990). Propagation characteristics of Boolean functions. In Workshop on the Theory and Application of of Cryptographic Techniques (pp. 161-173). Springer, Berlin, Heidelberg
34. Kazymyrov, O. (2013). Extended criterion for absence of fixed points, IACR Cryptology EPrint Archive, 2013, p. 576, 2013
35. Seberry, J., Zhang, X. M., & Zheng, Y. (1993). Systematic generation of cryptographically robust S-boxes. In Proceedings of the 1st ACM Conference on Computer and Communications Security (pp. 171-182). ACM
36. Guilley, S., Hoogvorst, P., Pacalet, R.: Differential power analysis model and some results. In: Smart Card Research and Advanced Applications Vi, pp. 127–142. Springer, Boston (2004)

37. Batool, S.I., Waseem, H.M.: A novel image encryption scheme based on Arnold scrambling and Lucas series. Multimed. Tools Appl. (2019). https://doi.org/10.1007/s11042-019-07881-x
38. Khawaja, M.A., Khan, M.: Application based construction and optimization of substitution boxes over 2D mixed chaotic maps. Int. J. Theor. Phys. (2019). https://doi.org/10.1007/s10773-019-04188-3
39. Khawaja, M.A., Khan, M.: A new construction of confusion component of block ciphers. Multimed. Tools Appl. (2019). https://doi.org/10.1007/s11042-019-07866-w
40. Khan, M., Masood, F.: A novel chaotic image encryption technique based on multiple discrete dynamical maps. Multimed. Tools Appl. (2019). https://doi.org/10.1007/s11042-019-07818-4
41. Khan, M., Waseem, H.M.: A novel digital contents privacy scheme based on Kramer's arbitrary spin. Int. J. Theor. Phys. **58**, 2720–2743 (2019)
42. Khan, M., Munir, N.: A novel image encryption technique based on generalized advanced encryption standard based on field of any characteristic. Wirel. Pers. Commun. (2019). https://doi.org/10.1007/s11277-019-06594-6
43. Waseem, H.M., Khan, M., Shah, T.: Image privacy scheme using quantum spinning and rotation. J. Electron. Imaging. **27**(6), 063022 (2018)
44. Younas, I., Khan, M.: A new efficient digital image encryption based on inverse left almost semi group and Lorenz chaotic system. Entropy. **20**(12), 913 (2018)
45. Rafiq, A., Khan, M.: Construction of new S-boxes based on triangle groups and its applications in copyright protection. Multimed. Tools Appl. **78**, 15527–15544 (2019)
46. Munir, N. and Khan, M., 2018. A generalization of algebraic expression for nonlinear component of symmetric key algorithms of any characteristic p. In *2018 International Conference on Applied and Engineering Mathematics (ICAEM)* (pp. 48–52). IEEE
47. Khan, M., Asghar, Z.: A novel construction of substitution box for image encryption applications with Gingerbreadman chaotic map and S8 permutation. Neural Comput. Applic. **29**, 993–999 (2018)
48. Tung, M., Yuan, J.M.: Dissipative quantum dynamics: driven molecular vibrations. Phys. Rev. A. **36**(9), 4463–4473 (1987)
49. Elgin, J.N., Sarkar, S.: Quantum fluctuations and the Lorenz strange attractor. Phys. Rev. Lett. **52**(14), 1215–1217 (1984)
50. Goggin, M.E., Sundaram, B., Milonni, P.W.: Quantum logistic map. Phys. Rev. A. **41**(10), 5705–5708 (1990)
51. Sharkovsky, O.M.: Coexistence of the cycles of a continuous mapping of the line into itself. Ukrainskij matematicheskij zhurnal. **16**(01), 61–71 (1964)
52. Elaydi, S.: On a converse of Sharkovsky's Theorem. Am. Math. Mon. **103**(5), 386–392 (1996)
53. Kaneko, K.: Overview of coupled map lattices. Chaos. **2**(3), 279–282 (1992)
54. Adams, C. M., & Tavares, S. E. (1993). Designing S-boxes for ciphers resistant to differential cryptanalysis. In Proceedings of the 3rd Symposium on State and Progress of Research in Cryptography, Rome, Italy (pp. 181-190)
55. Burns, K., Hasselblatt, B.: The Sharkovsky theorem: a natural direct proof. Am. Math. Mon. **118**(3), 229–244 (2011)
56. Štefan, P.: A theorem of Šarkovskii on the existence of periodic orbits of continuous endomorphisms of the real line. Commun. Math. Phys. **54**(3), 237–248 (1977)
57. Du, B.S.: A simple proof of Sharkovsky's theorem. Am. Math. Mon. **111**(7), 595–599 (2004)
58. Bhatia, N. P., & Egerland, W. O. (1994). New Proof and Extension of Sarkovskii's Theorem (No. ARL-TR-355). Army research lab Aberdeen proving ground MD