



S-Box Construction Method Based on the Combination of Quantum Chaos and PWLCM Chaotic Map


Jun Peng, Chongqing University of Science and Technology, Chongqing, China

 <https://orcid.org/0000-0001-6800-0064>

Shangzhu Jin, Chongqing University of Science and Technology, Chongqing, China

 <https://orcid.org/0000-0002-6486-4225>

Shaoning Pang, Federation University, Sydney, Australia

 <https://orcid.org/0000-0002-2833-5270>

Du Zhang, Macau University of Science and Technology, Cotai, China

Lixiao Feng, Chongqing University of Science and Technology, Chongqing, China

Zuojin Li, Chongqing University of Science and Technology, Chongqing, China

Yingxu Wang, University of Calgary, Calgary, Canada

ABSTRACT

For a security system built on symmetric-key cryptography algorithms, the substitution box (S-box) plays a crucial role to resist cryptanalysis. This article incorporates quantum chaos and PWLCM chaotic map into a new method of S-box design. The secret key is transformed to generate a sextuple system parameter, which is involved in the generation process of chaotic sequences of two chaotic systems. The output of one chaotic system will disturb the parameters of another chaotic system in order to improve the complexity of encryption sequence. S-box is obtained by XOR operation of the output of two chaotic systems. Over the obtained 500 key-dependent S-boxes, the authors test the S-box cryptographical properties on bijection, nonlinearity, SAC, BIC, differential approximation probability, respectively. Performance comparison of proposed S-box with those chaos-based one in the literature has been made. The results show that the cryptographic characteristics of proposed S-box has met the design objectives and can be applied to data encryption, user authentication and system access control.

KEYWORDS

Cryptography, Information Security, PWLCM Chaotic Map, Quantum Chaos, Substitution Box

INTRODUCTION

In the context of world digitalization, massive data are being generated every day from mobile computing and IoT devices. For data management, the security requirements have become increasingly

DOI: 10.4018/IJCI.20211001.0a24

This article published as an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

important to all kinds of data. For a modern cryptosystem with symmetric-key cryptographic algorithm, Substitution-box (S-box) is a non-linear component that performs permutation calculation, and its performance directly determines the quality of the cryptographic algorithm.

As we know, chaos has good cryptographic characteristics and has been widely used in the design of information security systems. The literature of the field contains numerous studies with chaos based cryptosystem. Wang et al (Wang, Wong, & Liao et al., 2011), Kadir et al (Kadir, Hamdulla, & Guo, 2014), Yavuz et al (Yavuz, Yazici, & Kasapbaşı et al., 2016), Murillo-Escobar et al (Murillo-Escobar, Cruz-Hernández, & Cardoza-Avenidaño et al., 2017), and Wang et al (Wang, Çavuşoğlu, & Kacar et al., 2019) proposed a new chaotic encryption system or PRNG (pseudorandom number generator) in their studies.

Tang and Liao et al proposed a new approach to obtain cryptographically strong dynamic S-boxes based on iterating discretized chaotic map (Tang, Liao, & Chen, 2005). Fatih and Ahmet proposed a methodology to design cryptographically S-Boxes based on continuous-time chaotic Lorenz system (Fatih, & Ahmet, 2010), the results show that proposed cryptosystem using the designed S-Boxes is very suitable for secure communication. Subsequently, Fatih et al also studied an S-box design algorithm based on time-delay chaotic systems. Compared with other algorithms in literature, the proposed algorithm is considered to be more useful according to the criteria such as simple and efficient implementation (Özkaynak, & Yavuz, 2013). Wang and Wong et al represented a method to design S-box based on chaos and genetic algorithm by making full use of the traits of chaotic map and evolution process (Wang, Wong, & Li et al., 2012), and the one of highlights is that the problem of constructing S-box is transformed to a Traveling Salesman Problem. Khan et al studied a construction method for designing S-box by using chaotic boolean functions and applied the obtained S-box to encrypt image (Khan, Shah, & Batool, 2016). The measurable analyses performed on the proposed framework show improvement in encryption quality and safety against numerous brute-force and statistical attacks, as well as the differential and linear cryptanalysis. Furthermore, Çavuşoğlu et al represented a novel approach for strong S-box generation algorithm design by utilizing a random number generator (RNG) produced by a chaotic scaled Zhongyang system (Çavuşoğlu, Zengin, & Pehlivan, 2017). Performance tests show the proposed S-box is stronger and more effective. In addition, by using a new three dimensional chaotic systems without equilibrium to construct S-boxes (Wang, Çavuşoğlu, & Kacar et al., 2019), and the experiment results indicate that S-box based encryption algorithm can be used safely in image encryption operations.

Recently, quantum chaos has attracted much attention for cryptosystem design due to its excellent cryptographic properties (Ahmed, Abd El-Latifab, & Li et al., 2013; Akhshani, Akhavan, & Mobaraki et al., 2014; Seyedzadeh, Norouzi, & Mosavi et al., 2018; Singh, Kumar, & Shaw et al., 2018; Lambić, 2018; Arshad, Batool, & Amin, 2019; Dhall, Sharma, & Gupta, 2019). In this paper, we presented a novel construction method for designing cryptographically strong S-box based on the combination of quantum chaos and PWLCM chaotic mapping. One of the main motivations is that we want to achieve a more sophisticated random sequence to generate strong S-box, which is expected to have better security performance and can be applied to data encryption, user authentication and system access control et al.

The rest of the paper is organized as follows. In Section II, the method for designing S-boxes is presented in detail including the introduction of the quantum chaotic system employed. Then in Section III, the experiments and several cryptographic properties including bijection, nonlinearity, strict avalanche criterion, output bit independence criterion, differential approximation probability are analyzed, followed by performance comparison of proposed S-box with those chaos-based one in the literatures. Finally, conclusion is drawn in Section IV.

THE PROPOSED S-BOX DESIGN

Quantum Chaotic System

By coupling a kicked quantum system to a bath of harmonic oscillators, dissipative quantum logistic map was constructed by Goggin et al (Goggin, Sundaram, & Milonni, 1990). In order to study the effects of quantum correlations the authors write $a = \langle a \rangle + \delta a$, where δa represents a quantum fluctuation about $\langle a \rangle$ (Goggin, Sundaram, & Milonni, 1990). This quantum chaotic map is given as follows.

$$\begin{cases} x_{n+1} = r(x_n - |x_n|^2) - ry_n \\ y_{n+1} = -y_n e^{-2\beta} + e^{-\beta} r [(2 - x_n - x_n^*)y_n - x_n z_n^* - x_n^* z_n] \\ z_{n+1} = -z_n e^{-2\beta} + e^{-\beta} r [2(1 - x_n^*)z_n - 2x_n y_n - x_n] \end{cases} \quad (1)$$

where $x = \langle a \rangle$, $y = \langle \delta a^\dagger \delta a \rangle$, $z = \langle \delta a \delta a \rangle$, r is adjustable parameter, β is dissipation parameter, and x_n, y_n, z_n represent the state value, and in general, they are complex numbers. x_n^* and z_n^* are the complex conjugation of x_n and z_n , respectively. In what follows this map is iterated with x_0, y_0 , and z_0 real, so that x_n, y_n , and z_n are real for all n . When $r \in (3.74, 4)$, $\beta \geq 3.5$, $x \in (0, 1)$, $y \in (0, 0.2461)$, $z \in (0, 0.2461)$, this quantum system is chaotic (Goggin, Sundaram, & Milonni, 1990). Equation (1) reduce to the classical one-dimensional Logistic map when the quantum corrections y_n and $z_n \rightarrow 0$. The Figure 1 is the Quantum chaotic sequence of x_n with the following parameters: $x_0 = 0.5$, $y_0 = 0.02$, $z_0 = 0.02$, $r = 3.9$, $\beta = 4.0$.

PWLCM Chaotic System

The Studies by Li and Chen et al show that PWLCM has many excellent dynamic properties (Li, Chen, & Mou, 2005), including ergodicity, random-like behavior, large positive Lyapunov exponent, uniform invariant density function and exponential decay autocorrelation function. These properties are very useful for encryption applications using PWLCM. The PWLCM is described as follows:

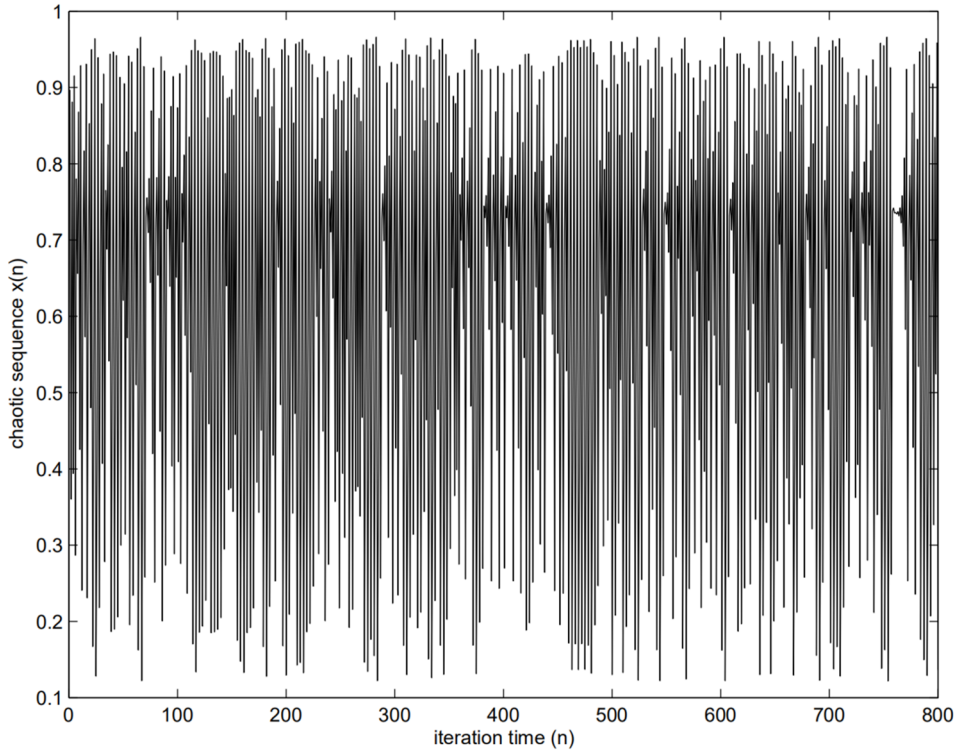
$$x_{n+1} = f_\mu(x_n) = \begin{cases} x_n \cdot \frac{1}{\mu}, & \text{if } x_n \in [0, \mu) \\ (x_n - \mu) \cdot \frac{1}{0.5 - \mu}, & \text{if } x_n \in [\mu, 0.5] \\ f_\mu(1 - x_n), & \text{if } x_n \in (0.5, 1) \end{cases} \quad (2)$$

where $x_n \in (0, 1)$, μ is a control parameter. When $\mu \in (0, 0.5)$ this map is in chaotic state. The Figure 2 is the PWLCM chaotic sequence of x_n when $x_0 = 0.1$ and $\mu = 0.352$.

8 × 8 S-Boxes Construction Algorithm

In this section, we study the construction algorithm of S-boxes with 8 × 8 size in detail. The schema of constructing algorithm is shown in Figure 3, where C_1 and C_2 represent quantum chaotic system and

Figure 1. Quantum Chaotic Sequence.



PWLCM chaotic system, respectively. The input is the secret key and the output is the corresponding S-Box generated by this algorithm. The process of generating 8×8 S-Box is described below. Let S_{out} represents the output S-Box of the algorithm. Randomly select a 64-bits key $K = K_1 K_2 \dots K_8$, then calculate the following six parameters t_i ($1 \leq i \leq 6$), and let $n = 1, S_{out} = \emptyset$.

$$t_1 = (K_7 + K_8) \bmod 8 \quad (3)$$

$$t_2 = (K_5 + K_6) \bmod 8 \quad (4)$$

$$t_3 = (K_3 + K_4) \bmod 8 \quad (5)$$

$$t_4 = (K_1 + K_2) \bmod 8 \quad (6)$$

$$t_5 = (K_1 \times K_2 + K_3 \times K_4) \bmod 8 \quad (7)$$

Figure 2. PWLCM Chaotic Sequence.

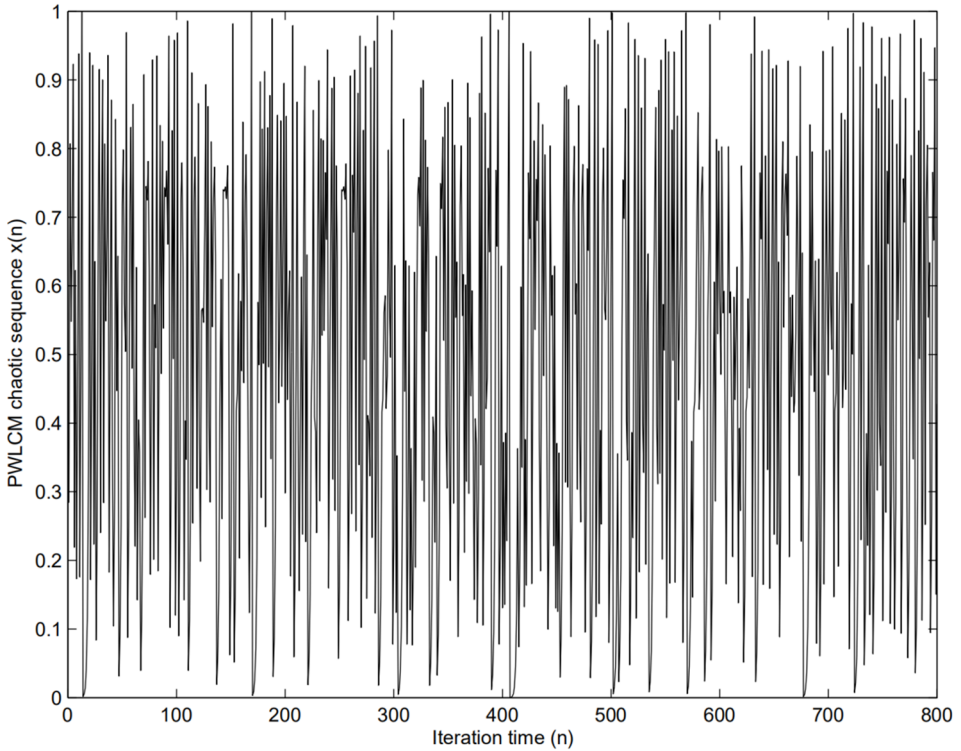
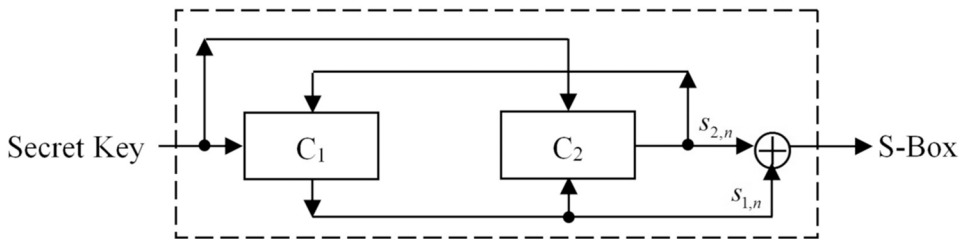


Figure 3. Schema of Constructing Algorithm



$$t_6 = (K_5 \times K_6 + K_7 \times K_8) \bmod 8 \quad (8)$$

Step 2: Calculate the output of the first stage chaotic system C_1 . In order to obtain the output, first we need to set the following initial value and parameters of C_1 .

(a) If $n = 1$, let

$$x_0 = \frac{K_1^{\ll t_1} \oplus K_2^{\ll t_2} + K_3^{\ll t_3} \oplus K_4^{\ll t_4}}{512} \quad (9)$$

$$y_0 = 0.02 \times \frac{K_5^{\ll t_5} \oplus K_6^{\ll t_6}}{256} \quad (10)$$

$$z_0 = 0.02 \times \frac{K_7^{\ll t_7} \oplus K_8^{\ll t_8}}{256} \quad (11)$$

$$\beta = 3.5 + 0.5 \times \frac{K_1^{\ll t_4} \oplus K_4^{\ll t_1} + K_2^{\ll t_3} \oplus K_3^{\ll t_2}}{512} \quad (12)$$

$$N_1 = 50 + [(K_1 + K_5)^{\ll t_2} \oplus (K_3 + K_7)^{\ll t_4}] \text{ mod } 128 \quad (13)$$

where $W^{\ll t}$ means cyclic left-shift by t bits of W .

(b) If $n > 1$, use the output $S_{2,n-1}$ of the second stage chaotic system C_2 to disturb the parameters as follows.

$$x_0 \leftarrow x_0 \times (S_{2,n-1} / 256) \quad (14)$$

$$y_0 \leftarrow y_0 \times (S_{2,n-1} / 256) \quad (15)$$

$$z_0 \leftarrow z_0 \times (S_{2,n-1} / 256) \quad (16)$$

$$N_1 \leftarrow 50 + (N_1 \times S_{2,n-1}) \text{ mod } 128 \quad (17)$$

Remark 1: If $S_{2,n-1} = 0$, in this case, we let $x_0 = 0.5$, $y_0 = 0.01$, and $z_0 = 0.01$.

Step 3: Calculate the output of the second stage chaotic system C_2 . In order to obtain the output, first we need to set the following initial value and parameters of C_2 .

(a) If $n = 1$, let

$$x_0 = \frac{K_1^{\ll t_2} \oplus K_3^{\ll t_4} + K_2^{\ll t_3} \oplus K_4^{\ll t_1}}{512} \quad (18)$$

$$N_2 = 50 + [(K_5 + K_6)^{\llcorner t_6} \oplus (K_7 + K_8)^{\llcorner t_5}] \bmod 128 \quad (19)$$

$$\mu = \frac{K_1 \oplus K_2 \oplus K_3 \oplus K_4 \oplus K_5 \oplus K_6 \oplus K_7 \oplus K_8}{512} \quad (20)$$

(b) If $n > 1$, use the output $S_{1,n-1}$ of the first stage chaotic system C_1 to disturb the parameters as follows.

$$x_0 \leftarrow x_0 \times (S_{1,n-1} / 256) \quad (21)$$

$$N_2 \leftarrow 50 + (N_2 \times S_{1,n-1}) \bmod 128 \quad (22)$$

Remark 2: If $S_{1,n-1} = 0$, in this case, we let $x_0 = 0.5$. Obtain the S-Box.

(a) Let $\hat{s}_{out,n} = s_{1,n} \oplus s_{2,n}$;

(b) If $\#S_{out} < 256$ and $\hat{s}_{out,n} \notin S_{out}$, then $S_{out} \leftarrow S_{out} \cup \hat{s}_{out,n}$;

(c) If $\#S_{out} = 256$ then stop the algorithm. The designed S-Box, i.e. S_{out} , is obtained. Otherwise, let $n = n + 1$, goto **Step 2** to continue the algorithm.

S-BOX TESTING AND CRYPTOGRAPHIC PROPERTIES ANALYSIS

In this section, we obtained 500 key-dependent S-boxes with 500 different keys. Table 1 gives an example 8×8 S-box with the dependent key as “8dwU9VCF”. Consider a “good” S-box must comply with some cryptographic properties (Adams, & Tavares, 1990), we use the below properties as the evaluation criteria for our S-box testing.

Bijection Property

For an S-box, the following method is presented to check the bijective property (Jakimoski, & Kocarev, 2001). The boolean function $f(x) = (f_1, f_2, \dots, f_n)$ is bijective if it satisfies the following condition:

$$wt(a_1 f_1 \oplus a_2 f_2 \oplus \dots \oplus a_n f_n) = 2^{n-1} \quad (23)$$

where the $a_i \in \{0, 1\}$, $(a_1, a_2, \dots, a_n) \neq (0, 0, \dots, 0)$ and $wt(\cdot)$ is the Hamming weight. The above condition for the boolean function $f(x)$ to be bijective guarantees that any linear combination of f_i has Hamming weight 2^{n-1} ($i = 1, 2, \dots, n$). Bijection property ensures that all possible 2^n n -bit

input vectors map to distinct output vectors. According to the Step 4 of the construction method in Section II, we found that all the obtained S-boxes satisfy bijection property.

Remark 3: The usage of S-box is explained as follows: if we assume that the input of S-box is a byte u , which can be expressed as xy in hexadecimal, we use x to select rows and y to select columns to find the output of S-box. For example, an input integer $(138)_{10}$ or $(8A)_{16}$, from Table 1 we can see the corresponding output would be $(131)_{10}$.

Nonlinearity Property

Nonlinearity criteria for boolean functions are classified in view of their suitability for cryptographic design (Meier, & Staffelbach, 1990). In general, nonlinearity of the boolean function $f(x)$ can be represented by the Walsh spectrum:

$$N_f = 2^{n-1}(1 - 2^{-n} \max_{\omega \in GF(2^n)} |S_{\langle f \rangle}(\omega)|) \quad (24)$$

The Walsh spectrum of $f(x)$ is defined by

$$S_{\langle f \rangle}(\omega) = \sum_{x \in GF(2^n)} (-1)^{f(x) \oplus x \cdot \omega} \quad (25)$$

where $\omega \in GF(2^n)$ and $x \cdot \omega$ denotes the dot-product of x and ω over $GF(2)$, and where the sum is evaluated over the reals. Nonlinearity property ensures that S-box is not a linear mapping from input vectors to output vectors.

For the S-box in Table 1, the nonlinearity value is 108. Furthermore, the maximum, minimum and average nonlinearity of 500 S-boxes are 108, 90 and 103.4560, respectively (see Figure 4). Especially, 92.20% of the S-boxes whose nonlinearity are among [100, 108], and only 0.80% are among [90, 95], showing that most of the S-boxes have a high nonlinearity property.

Strict Avalanche Criterion (SAC)

An S-box is said to satisfy the SAC if, whenever a single input bit is complemented, each of the output bits should change with a probability of one half. The dependence matrix is constructed to ascertain whether a given S-box satisfies the strict avalanche criterion (Webster, & Tavares, 1986). If the S-box satisfies SAC, then the average value of the dependent matrix is close to 0.5, that is to say, the value of each element in the dependent matrix must be close to half.

The dependence matrix of the S-box in Table 1 is listed in Table 2 by using the method in (Webster, & Tavares, 1986), and minimum, maximum and mean value is 0.3906, 0.6094, and 0.5037, respectively.

Furthermore, we found that all the mean values of the dependence matrix of 500 S-boxes are located within [0.4890, 0.5239] (see Figure 5), which are close to 0.5, and the average of standard deviation is 0.0113 (see Figure 6), showing that all S-boxes have excellent SAC performance.

Output Bit Independence Criterion (BIC)

Another ideal feature of S-boxes is that they should satisfy the output bit independence criterion (BIC). This means that all pairs of avalanche variables must be independent of the avalanche

Table 1. 8×8 S-box generated by proposed algorithm

-	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00	178	245	85	248	137	148	49	25	171	26	4	211	240	160	133	170
01	224	116	98	216	204	73	200	42	48	65	0	62	35	253	99	20
02	38	134	144	34	236	250	184	15	233	54	181	237	104	254	136	203
03	212	228	70	146	63	44	177	112	52	169	6	174	87	37	17	143
04	95	167	156	159	32	162	76	33	19	60	14	22	239	109	100	66
05	5	246	18	50	101	128	229	8	202	196	223	88	182	153	115	47
06	221	255	90	118	231	9	127	220	195	64	111	97	117	206	232	59
07	145	198	67	121	93	3	230	71	192	179	210	84	83	89	61	39
08	123	214	242	86	225	205	78	30	58	21	131	106	193	140	215	149
09	138	154	235	163	113	119	226	151	24	218	27	94	185	209	187	114
0A	36	152	53	126	75	142	135	79	227	10	249	219	244	81	150	190
0B	194	207	164	45	175	172	186	91	125	217	1	12	168	199	82	13
0C	238	72	51	41	122	166	208	105	68	129	107	213	252	183	158	80
0D	92	157	222	69	40	120	55	124	31	130	108	173	43	7	189	176
0E	188	110	74	139	2	56	141	132	16	234	155	180	197	201	165	161
0F	191	28	96	29	251	147	77	103	102	243	247	241	57	46	11	23

Figure 4. The nonlinearity of 500 S-boxes.

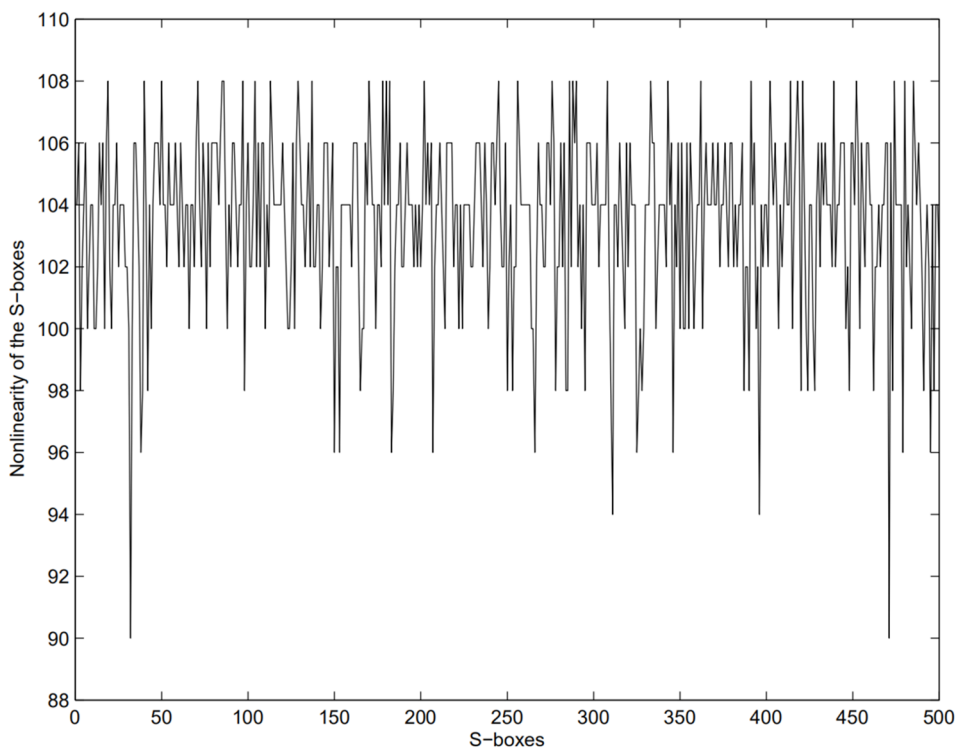


Table 2. The dependence matrix of the S-box in Table 1

0.5469	0.4531	0.5625	0.4688	0.4688	0.4844	0.3906	0.5313
0.5000	0.5156	0.4531	0.4219	0.4375	0.5625	0.5781	0.5313
0.4844	0.6094	0.4844	0.4531	0.5469	0.5469	0.4531	0.4688
0.4688	0.5313	0.4688	0.4063	0.5156	0.5625	0.5469	0.6094
0.4688	0.5156	0.4375	0.5156	0.5000	0.5000	0.5313	0.4688
0.5000	0.5625	0.5313	0.5000	0.5000	0.5000	0.4063	0.5000
0.4688	0.5000	0.5156	0.5000	0.5469	0.5313	0.4844	0.5000
0.5625	0.5313	0.5000	0.5000	0.4844	0.5313	0.5156	0.5625

vector set generated by the inverse of a single plaintext bit (Fatih, & Ahmet, 2010). Assume the boolean functions in the 8×8 S-box are f_1, f_2, \dots, f_8 . If $F_i = f_j \oplus f_k$ is highly non-linear and very close to the SAC-fulfilling function. It can ensure that each pair of output bits has a correlation as close to zero as possible when any input bit is inverted. If f_j and f_k satisfy BIC, $F_i = f_j \oplus f_k$ ($j \neq k, 1 \leq j, k \leq 8$) should also satisfy nonlinearity and SAC.

Figure 5. The mean values of dependence matrix of 500 S-boxes.

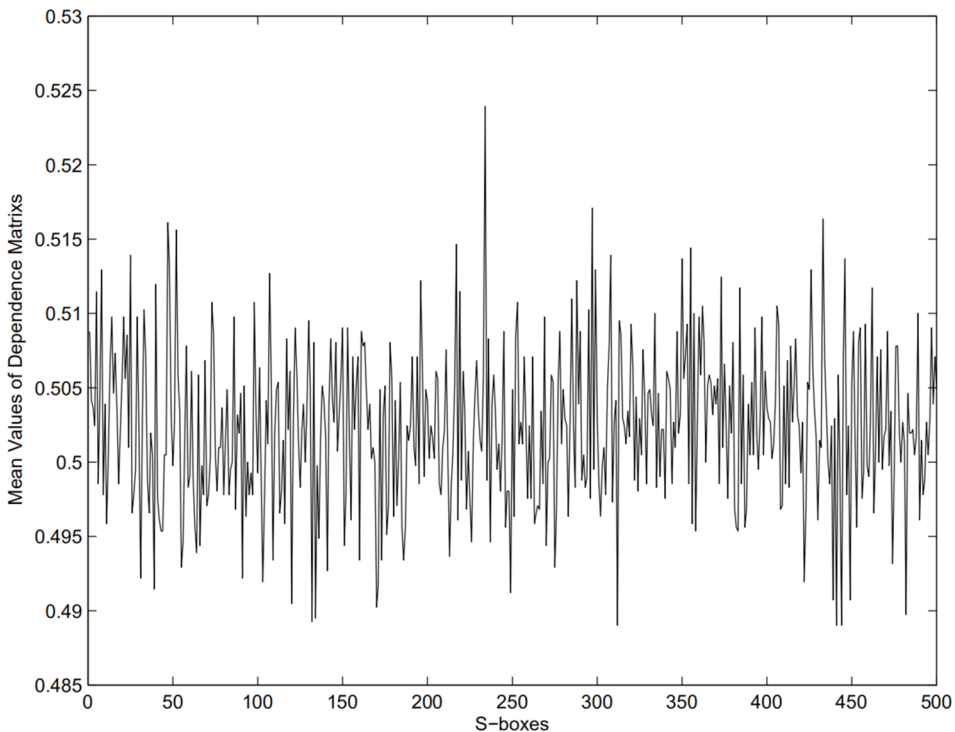
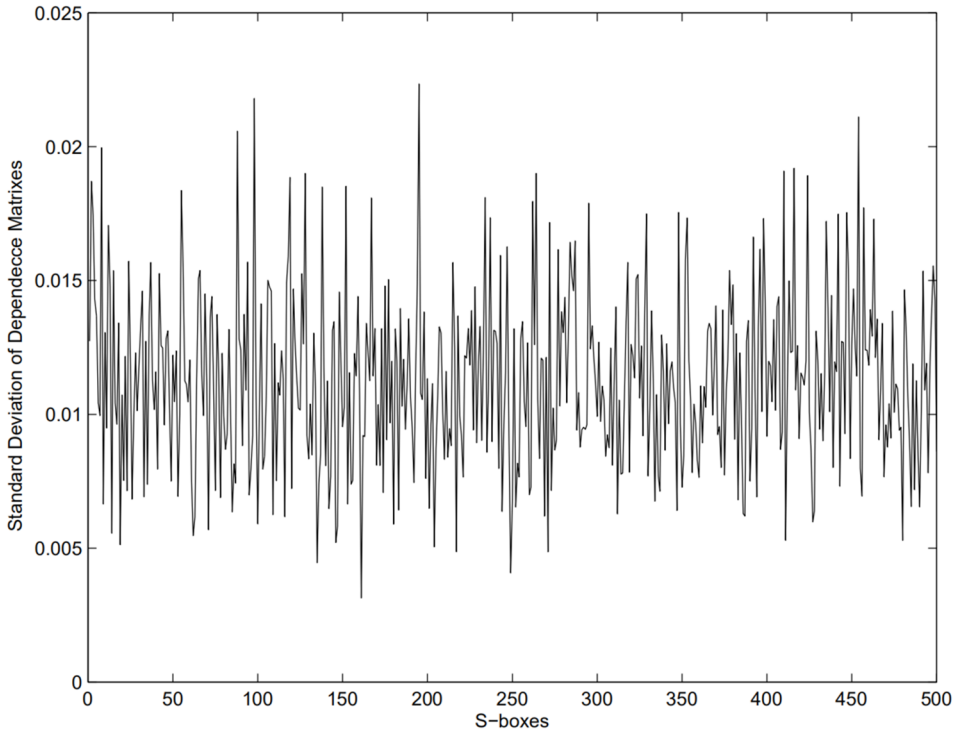


Figure 6. The standard deviation of dependence matrix of 500 S-boxes.



The computational nonlinearities of S-boxes are shown in Figure 4. The nonlinearities average value of $f_j \oplus f_k$ is more than 100, and the mean value of $f_j \oplus f_k$ dependence matrix is close to 0.5, which indicates that all S-boxes basically meet the BIC performance requirements.

Differential Approximation Probability

For an S-box, it should ideally have differential uniformity to resist the differential cryptanalysis, which means that an input differential Δx should uniquely map to an output differential Δy , thereby ensuring a uniform mapping probability for each x . The differential approximation probability is a measure for differential uniformity and is defined as (Biham, & Shamir, 1991):

$$DP_f = \max_{\Delta x \neq 0, \Delta y} \left(\frac{\#\{x \in X \mid f(x) \oplus f(x \oplus \Delta x) = \Delta y\}}{2^n} \right) \quad (26)$$

where X is the set of all possible input values, and 2^n is the number of its elements. In fact, DP_f means the maximum probability of output differential Δy corresponding to the input differential Δx . The smaller the value of DP_f , the better the performance against differential cryptanalysis.

For the S-box in Table 1, the frequency of the most probable output differential Δy corresponding to the input differential Δx is shown in Table 3 and Figure 7. The maximum frequency is only 10, i.e. $DP_f = 0.03906$.

Table 3. Differential approximation probability (DP) matrix

--	4	8	10	6	6	8	6	6	6	6	6	10	10	6	8
8	6	6	6	8	6	10	10	6	6	6	8	10	8	8	8
6	8	6	6	6	6	8	6	8	8	8	6	6	8	8	6
6	8	8	6	6	6	8	6	6	6	6	6	6	6	6	6
8	6	6	8	6	8	6	8	6	6	6	6	6	6	6	6
8	6	8	6	8	6	6	8	6	6	8	6	8	6	8	8
8	6	6	8	6	4	6	6	6	6	6	8	6	6	8	8
6	8	6	6	8	10	10	8	6	8	6	6	10	10	8	6
8	6	8	8	6	8	8	6	6	6	6	10	6	8	6	4
8	6	6	6	8	8	4	8	6	6	6	8	6	6	8	6
8	6	6	8	6	6	6	6	6	6	6	8	6	8	8	6
6	8	8	6	8	6	8	6	6	6	6	6	6	8	8	6
8	8	8	8	8	6	6	6	8	8	6	8	8	6	10	6
6	6	8	8	4	8	8	6	6	8	6	8	6	6	6	6
8	10	6	6	6	6	6	6	6	6	8	8	6	10	6	8
8	6	10	6	8	6	8	6	8	6	6	8	10	8	6	6

We randomly selected 100 out of 500 S-boxes and calculated the DP_f value corresponding to each S-box. The results are shown in Table 4. From result we found that 93% of the DP_f have a

Figure 7. The frequency of the most probable output differential Δy corresponding to the input differential Δx .

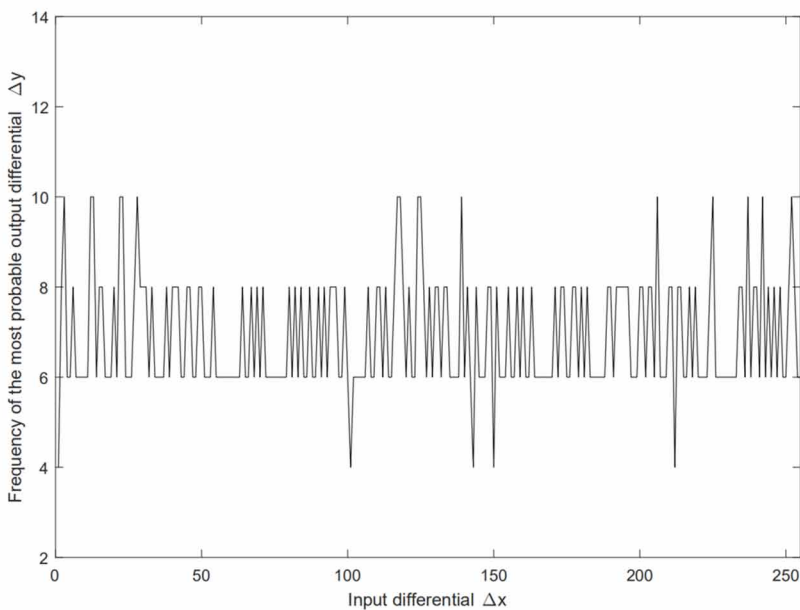


Table 4. The differential approximation probability

Frequency	10	12	14	16
DP_f	0.03906	0.04688	0.05469	0.06250
Numbers	43	50	6	1

Table 5. Correlation coefficient between S-boxes when using small different secret keys

No. of S-box	1	2	3	4	5	6	7	8
Correlation coefficient	-0.0579	-0.0689	0.0961	0.0115	-0.0646	-0.0138	-0.0433	-0.0681

value less than 0.05, implying that most of these S-boxes have good ability of resisting differential cryptanalysis to some extent.

Correlation Coefficients

The correlation coefficients between S-boxes are calculated using two different keys and can be used to investigate the sensitivity of S-boxes to keys. Suppose we let *key1* is “8dwU9VCf” and only one character in the secret key is changed at a time. For example, add one to the character value to be changed, and then we get eight new keys slightly different from the secret key *key1*. These eight keys will generate eight different S-boxes. The correlation coefficient between each new S-box and the original S-box generated by *key1* is calculated, and the results are shown in Table 5. The smaller correlation coefficient indicates that the proposed algorithm is sensitive to the secret key.

The Performance Comparison

In this part, we compare the performance of the S-box generated by the proposed algorithm with those chaos-based S-boxes in the literatures. The comparison mainly focuses on three properties, i.e., nonlinearity, dependence matrix, and differential approximation probability (DP). The results are listed in Table 6.

From results we found that the proposed S-box has the largest nonlinearity, which is equivalent to that in (Wang, Wong, & Li et al., 2012). From the perspective of dependence matrix, the average value of our S-box is closer to 0.5, slightly inferior to the one investigated in (Tang, Liao, & Chen, 2005).

Table 6. The performance comparison of chaos-based S-box

S-box	Nonlinearity	Dependence matrix			DP
		Average	Min	Max	
Tang 2005	103	0.4966	0.3984	0.5703	10 (3.906%)
Fatih 2010	104	0.5049	0.4219	0.5938	10 (3.906%)
Wang 2012	108	0.5068	0.4063	0.5781	10 (3.906%)
Özkaynak 2013	107	0.5061	0.4141	0.6094	10 (3.906%)
Khan 2016	102	0.4812	0.1250	0.6250	16 (6.250%)
Çavuşoğlu 2017	104	0.5039	0.4219	0.5938	10 (3.906%)
Wang 2019 (S-box3)	106	0.4917	0.3594	0.5781	10 (3.906%)
Proposed S-box	108	0.5037	0.3906	0.6094	10 (3.906%)

In the aspect of differential approximation probability, except for S-box generated in (Khan, Shah, & Batool, 2016), all of them have the same performance. Based on the above comparison results, the S-box proposed in this paper has better security performance. It should be noted that the algorithm in this paper can generate a large number of S-boxes by using different secret keys. In practice, we'd better select those S-boxes with excellent performance in order to meet the requirements of high security.

CONCLUSION

In designing S-boxes with good cryptographical properties, this paper presents a constructive method that applies quantum chaos and PWLCM chaotic mapping. The numerical analysis results of the obtained S-boxes show that the cryptographic properties of “good” S-boxes, such as bijection, nonlinearity, SAC, BIC and differential approximation probability, are approximately satisfied. Finally, the sensitivity of S-box to key is studied. By changing the key slightly, we can generate completely different S-boxes, which shows that the sensitivity of S-boxes to the key is well satisfied. By comparing the performance of proposed S-box with those chaos-based S-boxes in the literatures, it shows that the proposed S-box has better security performance. The S-box studied in this paper can be generated quickly, and is very suitable for constructing a cryptosystem with good performance, which satisfies the security requirements of mobile computing and other application scenarios.

ACKNOWLEDGMENT

The presented work is partially funded by the National Science and Technology Major Project (No. 2016ZX05060), the National Natural Science Foundation of China (No. 61873043), the Science and Technology Research Program of Chongqing Municipal Education Commission (No. KJ1713329), the Natural Science Foundation of Chongqing (No. cstc2019jcyjmsxmX0355 and No. cstc2018jcyjAX0048), the Scientific Research Fund of Chongqing University of Science and Technology (No. ckzg201914), and Chongqing Key Project of Technological Innovation and Application Demonstration (No. cstc2018jszx-cydzX0162).

REFERENCES

- Abd El-Latif, A. A., Li, L., Wang, N., Han, Q., & Niu, X. M. (2013). A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces. *Signal Processing*, 93(11), 2986–3000. doi:10.1016/j.sigpro.2013.03.031
- Adams, C., & Tavares, S. (1990). The structured design of cryptographically good S-Boxes. *Journal of Cryptology*, 3(1), 27–41. doi:10.1007/BF00203967
- Akhshani, A., Akhavan, A., Mobaraki, A., Lim, S. C., & Hassan, Z. (2014). Pseudo random number generator based on quantum chaotic map. *Communications in Nonlinear Science and Numerical Simulation*, 19(1), 101–111. doi:10.1016/j.cnsns.2013.06.017
- Arshad, U., Batool, S. I., & Amin, M. (2019). A novel image encryption scheme based on walsh compressed quantum spinning chaotic Lorenz system. *International Journal of Theoretical Physics*, 58(10), 3565–3588. doi:10.1007/s10773-019-04221-5
- Biham, E., & Shamir, A. (1991). Differential cryptanalysis of DES-like cryptosystems. *Advances in Cryptology - CRYPTO'90. LNCS*, 537, 2–21.
- Çavuşoğlu, Ü., Zengin, A., Pehlivan, I., & Kaçar, S. (2017). A novel approach for strong S-Box generation algorithm design based on chaotic scaled Zhongtang system. *Nonlinear Dynamics*, 87(2), 1081–1094. doi:10.1007/s11071-016-3099-0
- Dhall, S., Sharma, R., & Gupta, S. (2019). A multi-level steganography mechanism using quantum chaos encryption. *Multimedia Tools and Applications*. Advance online publication. doi:10.1007/s11042-019-08223-7
- Fatih, Ö., & Ahmet, B. Ö. (2010). A method for designing strong S-Boxes based on chaotic Lorenz system. *Physics Letters. [Part A]*, 374(36), 3733–3738. doi:10.1016/j.physleta.2010.07.019
- Goggin, M. E., Sundaram, B., & Milonni, P. W. (1990). Quantum Logistic map. *Physical Review A*, 41(10), 5705–5708. doi:10.1103/PhysRevA.41.5705 PMID:9902961
- Jakimoski, G., & Kocarev, L. (2001). Chaos and cryptography: Block encryption ciphers based on chaotic maps. *IEEE Transactions on Circuits and Systems*, 48(2), 163–169. doi:10.1109/81.904880
- Kadir, A., Hamdulla, A., & Guo, W. Q. (2014). Color image encryption using skew tent map and hyper chaotic system of 6th-order CNN. *Optik (Stuttgart)*, 125(5), 1671–1675. doi:10.1016/j.ijleo.2013.09.040
- Khan, M., Shah, T., & Batool, S. T. (2016). Construction of S-box based on chaotic Boolean functions and its application in image encryption. *Neural Computing & Applications*, 27(3), 677–685. doi:10.1007/s00521-015-1887-y
- Lambić, D. (2018). Security analysis and improvement of the pseudo-random number generator based on quantum chaotic map. *Nonlinear Dynamics*, 94(2), 1117–1126. doi:10.1007/s11071-018-4412-x
- Li, S. J., Chen, G. R., & Mou, X. Q. (2005). On the dynamical degradation of digital piecewise linear chaotic maps. *International Journal of Bifurcation and Chaos in Applied Sciences and Engineering*, 15(10), 3119–3151. doi:10.1142/S0218127405014052
- Meier, W., & Staffelbach, O. (1990). Nonlinearity criteria for cryptographic functions. *Advances in Cryptology - EUROCRYPT'89. LNCS*, 434, 549–562.
- Murillo-Escobar, M. A., Cruz-Hernández, C., Cardoza-Avenidaño, L., & Méndez-Ramírez, R. (2017). A novel pseudorandom number generator based on pseudorandomly enhanced logistic map. *Nonlinear Dynamics*, 87(1), 407–425. doi:10.1007/s11071-016-3051-3
- Özkaynak, F., & Yavuz, S. (2013). Designing chaotic S-boxes based on time-delay chaotic system. *Nonlinear Dynamics*, 74(3), 551–557. doi:10.1007/s11071-013-0987-4
- Seyedzadeh, S. M., Norouzi, B., Mosavi, M. R., & Mirzakuchaki, S. (2015). A novel color image encryption algorithm based on spatial permutation and quantum chaotic map. *Nonlinear Dynamics*, 18(1-2), 511–529. doi:10.1007/s11071-015-2008-2

Singh, R. K., Kumar, B., Shaw, D. K., & Khan, D. A. (2018). Level by level image compression-encryption algorithm based on quantum chaos map. *Journal of King Saud University - Computer and Information Sciences*, 10.1016/j.jksuci.2018.05.012

Tang, G. P., Liao, X. F., & Chen, Y. (2005). A novel method for designing S-boxes based on chaotic maps. *Chaos, Solitons, and Fractals*, 23(2), 413–419. doi:10.1016/j.chaos.2004.04.023

Wang, X., Çavuşoğlu, Ü., Kacar, S., Akgul, A., Pham, V. T., Jafari, S., Alsaadi, F. E., & Nguyen, X. Q. (2019). S-Box based image encryption application using a chaotic system without equilibrium. *Applied Sciences (Basel, Switzerland)*, 9(4), 781–798. doi:10.3390/app9040781

Wang, Y., Wong, K. W., Li, C. B., & Li, Y. (2012). A novel method to design S-box based on chaotic map and genetic algorithm. *Physics Letters. [Part A]*, 376(6), 827–833. doi:10.1016/j.physleta.2012.01.009

Wang, Y., Wong, K. W., Liao, X. F., & Chen, G. R. (2011). A new chaos-based fast image encryption algorithm. *Applied Soft Computing*, 11(1), 514–522. doi:10.1016/j.asoc.2009.12.011

Webster, A. F., & Tavares, S. E. (1986). On the design of S-boxes. *Advances in Cryptology: Proceedings of CRYPTO'85*, 523-534.

Yavuz, E., Yazici, R., Kasapbaşı, M. C., & Yamaç, E. (2016). A chaos-based image encryption algorithm with simple logical functions. *Computers & Electrical Engineering*, 54, 471–483. doi:10.1016/j.compeleceng.2015.11.008

*Jun Peng (PhD) was born in Chongqing, China in July 1970. He received a Ph.D. in Computer Software and Theory from Chongqing University in 2003, a MA in computer system architecture from Chongqing University in 2000, and a BSc in Applied Mathematics from the Northeast University in 1992. From 1992 to present he works at Chongqing University of Science and Technology, where he is currently a Professor in School of Intelligent Technology and Engineering, and Dean of School of Electrical and Information Engineering (2011-2018). He was a visiting scholar in the Laboratory of Cryptography and Information Security at Tsukuba University, Japan in 2004, and Department of Computer Science at California State University, Sacramento in 2007, respectively. He has authored or coauthored over 100 peer reviewed journal or conference papers. He has served as the program committee member or session co-chair for over 20 international conferences such as SEKE'08, SEKE'10, ICCI'09, ICCI'10, ICCI*CC'11-19, ICTAI'10, ICOACS'16, ACSS'18. His current research interests are on cryptography, chaos and network security, image processing and big data analysis.*

Shangzhu Jin received the BSc degree in computer science from Beijing Technology and Business University, China in 1999, and the MSc degree in control theory and control engineering from Yanshan University, China, in 2005, and the PhD degree from Aberystwyth University, UK, in 2015. He is currently an associate professor at the School of Intelligent Technology and Engineering, Chongqing University of Science and Technology. His research interests include fuzzy systems, approximate reasoning, and network security. His paper, entitled "Backward Fuzzy Interpolation and Extrapolation with Multiple Multi-antecedent Rules" has won the best student paper award at the 21th IEEE International Conference on Fuzzy Systems.

Shaoning Pang is an Associate Professor of Cybersecurity at the School of Science, Engineering and Information Technology, Federation University Australia. Before joining FedUni, he was a full Professor of Data Analytic and the Director of Center for Computational Intelligence for Cybersecurity (CICS) with the Unitec Institute of Technology New Zealand. His main research areas are cognitive cybersecurity Intelligence, cyber resilience, applied data analytics for digital health and smart environment. Dr. Pang was a Global Judge for the 2018 AI Summit London and a lead guest editor of the Sensors journal MDPI. Also, he is an associate editor of the Computational Intelligence journal Wiley-Blackwell, a Senior Member of IEEE, the current Vice President of Asia Pacific Neural Network Society (APNNS) and the Event Editor of Neural Networks journal Elsevier. He has served Chair, Co-chair and Committee Member/Track Chair of a number of international conferences, including as the founding chair of International Cybersecurity Data Mining Competition (www.csmining.org).

Du Zhang is Professor and Dean of the Faculty of Information Technology, Macau University of Science and Technology, Macau, China. He received his Ph.D. and M.S. degrees, both in computer science, from the University of Illinois and Nanjing University, China, respectively. Previously he was a Professor and Chair of the Computer Science Department at California State University, Sacramento. He has research affiliations with numerous universities in the USA, UK, France, Hong Kong, China, Czech Republic, and Mexico. Professor Zhang's current research interests include machine learning (STEP perpetual learning), knowledge-based systems, big data analytics, and software engineering. He has over 200 publications in these and other areas. He has served in various roles on numerous international conferences, and is editor or editorial board member for several journals in the areas of artificial intelligence, software engineering and knowledge engineering, big data, and applied mathematics. Professor Zhang is a senior member of both the IEEE and ACM, a board member of the Society of Information Reuse and Integration, and a member of Upsilon Pi Epsilon and Phi Beta Delta.

Lixiao Feng received a master degree (Electrical Engineering) from Chongqing University in 2010. His research interests focus on signal process and programming.

Zuojin Li is a Professor at the College of Electrical Engineering, Chongqing University of Science and Technology in China. He received his PhD from the Chongqing University in China. His research interests cover machine vision, image processing, pattern recognition, intelligence system, multi-sensor data fusion.

*Yingxu Wang (PhD) is professor of cognitive informatics, brain science, software science, and denotational mathematics. He is the founding President of International Institute of Cognitive Informatics and Cognitive Computing (ICIC). He is Fellow of ICIC, Fellow of BCS, Fellow of WIF (UK), a P.Eng. of Canada, and a Senior Member of IEEE and ACM. He has been visiting professor (on sabbatical appointment) at Oxford University (1995 | 2018-22), Stanford University (2008 | 2016), UC Berkeley (2008), and MIT (2012), respectively. He has been a full professor since 1994. He is the founder and steering committee chair of the annual IEEE International Conference on Cognitive Informatics and Cognitive Computing (ICCI*CC) since 2002. He is founding Editor-in-Chiefs of International Journal of Cognitive Informatics & Natural Intelligence; International Journal of Software Science & Computational Intelligence; Journal of Advanced Mathematics & Applications; and Journal of Mathematical & Computational Methods, as well as Associate Editors of IEEE Trans. on SMC - Systems and IEEE SMC Magazine. He has served as chair or co-chair of 30 IEEE or other int'l conferences and a member of IEEE Selection Committee for Senior Members in 2011. Dr. Wang's publications have been cited for 8,800+ times according to Google Scholar. According to Research Gate statistics, his research profile has reached top 2.5% worldwide with 243,000+ referral access. He is the recipient of dozens international awards on academic leadership, outstanding contributions, best papers, and teaching in the last three decades.*