International Journal of Future Generation Communication and Networking
Vol. 9, No. 12 (2016), pp. 97-106
http://dx.doi.org/10.14257/ijfgcn.2016.9.12.09

The Design of S-box Based on Cascaded Integer Chaos Applied to Wireless Sensor Network

[1,2]Juan Wang, [2]Yan Lu and [1]Qun Ding

[1] Electronic Engineering Institute
Heilongjiang University
Harbin, China, 150001
[2]Electronic and information Engineering Institute
Heilongjiang University of Science and Technology
Harbin, China, 150022
76115347@qq.com, qunding@aliyun.com

Abstract

In the block cryptogram algorithm of wireless sensor network, the emphasis is how to design a secure and efficient S-box. A design method of S-box is proposed based on dynamic iteration of the cascaded integer chaos, which is obtained by the cascade and integer quantization of one-dimensional discrete chaotic map logistic and tent. the S-box not only conform to the application requirements of node operation and computational efficiency, but also compensate the degradation of dynamic characteristics of the single-level integer chaos. The performance tests of S-box were carried out, including nonlinearity degree, differential uniformity, strict avalanche criterion, out-put bit independence criterion and bijective property. In contrast to the existing classical S-box based on chaotic map, the results indicate that the S-box has more excellent cryptographic properties, and it can be used as a candidate nonlinear component in the design of block cryptogram algorithm for wireless sensor network.

***Keywords**: wireless sensor network; block cryptogram; S-box; cascaded integer chaos*

1. Introduction

Wireless sensor network is a multi-hops self-organizing network, which is composed of numerous and budget micro sensor nodes in the monitoring area, and communicate through the way of wireless. Wireless sensor network has characteristics of low power consumption, low cost, distributed structure and self-organization, it has been widely applied in military, industry and many other fields [1]. According to the features of wireless communication and network deployment, the attacker can easily obtain confidential or sensitive information, through the way of transmission between nodes, addition of forged illegal nodes and wiretap, *etc*. Therefore, the information security is extremely important for wireless sensor network [2]. the nodes of wireless sensor network have a variety of restrictions of unfavorable factors, such as low operation ability, small storage capacity and finite energy and so on. Due to the characteristics of high complexity, strong performance and low efficiency, the existing cryptogram algorithms of wireless net is not suitable for direct application in the wireless sensor network. The block cryptogram has many advantages such as fast processing, easy standardization and simple implementation, and it has gradually become the focus research in encryption technology of wireless sensor network [3].

As a unique and indispensable nonlinear component, the S-box provides the necessary confusion effect for the block cryptogram to guarantee its security [4]. For any change in the input, the output of ideal S-box should produce the corresponding random change,

ISSN: 2233-7857 IJFGCN

which is almost impossible to approximate by a linear function [5]. Due to the nonlinear property, excellent cryptology and high efficiency, using chaos to design S-box has achieved a lot of research results. The design of S-box based on one-dimensional discrete chaotic logistic map was firstly proposed in Literature [7], The design of S-box based on two-dimensional discrete chaotic baker map was proposed in Literature [8], The design of S-box based on three-dimensional continuous chaotic Lorenz system was proposed in Literature [9].

There are several deficiencies in the existing classical S-box based on chaotic map. For example, the S-box based on low dimensional chaotic map is easy to be deciphered, and the security is not enough; while the S-box based on high dimensional chaotic system is too complex, and the encryption speed is slow. According to the application requirements of security and efficiency in wireless sensor network, a design method of S-box is proposed based on dynamic iteration of the cascaded integer chaos, which is obtained by the cascade and integer quantization of one-dimensional discrete chaotic map logistic and tent. The results of cryptographic test show that the S-box has excellent cryptographic property and computational efficiency, it can not only meet the encryption requirements of wireless sensor network, but also conform to the low configuration requirements of Wireless sensor network node.

2. The Cascaded Integer Chaotic Map

When the chaotic maps were applied to wireless sensor network, the characteristics of sensor nodes must be considered, including the storage capacity, operational capability, limited computing precision and it is difficult to directly process the floating point operations. Due to the amplitude of chaotic map is continuous, it is not suiTable for direct application in wireless sensor network. As a result, it is necessary to carry out the integer quantization. Literature [10] have study and found that one-dimensional discrete chaotic map would appear the degradation of dynamic characteristics after integer quantization, and its effect on cryptographic security cannot be ignored. consequently, a new cascaded integer chaotic map has been proposed in this paper.

As shown in Figure 1, The first iteration output of logistic map is input as the initial value into the tent map, and the first iteration output of tent map is input into the logistic map for the next iteration. Such cycled process can produce the cascaded chaotic sequence. Owing to each iterative result of the cascaded chaotic map is determined by two chaotic maps, which make the iterative method is more complex.

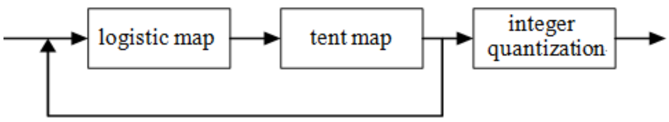


Figure 1. Model of the Cascaded Integer Chaos

The difference iterative equation of logistic chaotic map is given to be,

$$x_{n+1} = \mu_1 x_n (1 - x_n) \qquad \mu_1 \in (0,4] \quad x_n \in (0,1] \tag{1}$$

In the literature [11], the improved equation of tent chaotic mapping is given to be,

$$x_{n+1} = 1 - |1 - \mu_2 x_n| \qquad \mu_2 \in [0,2] \quad x_n \in (0,1] \tag{2}$$

Substituting x_n in Equation (2) to be x_{n+1} in Equation (1), the equation of the cascaded chaotic map is given to be,

$$x_{n+1} = 1 - \left|1 - \mu_1 \mu_2 x_n (1 - x_n)\right| \qquad x_n \in (0,1] \quad \mu_1 \in (0,4] \qquad \mu_2 \in (0,2] \tag{3}$$

According to the method of literature [12], the cascaded chaotic sequences can be integer quantized to be,

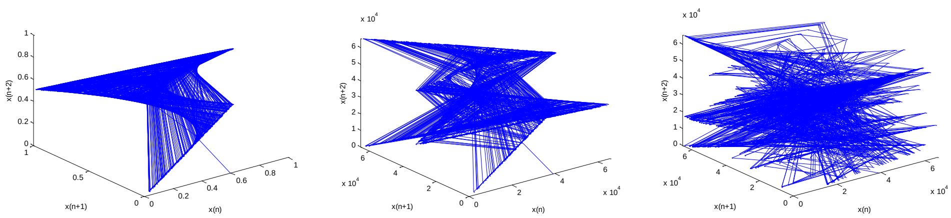
$$t_{n+1}=\begin{cases}4t_n & 0\le t_n<a/4\\ 4t_n-a & a/4\le t_n<a/2\\ 3a-4t_n & a/2\le t_n<3a/4\\ 4a-4t_n & 3a/4\le t_n\le a\end{cases} \quad (4)$$

In Equation (4), $t_n=x_n$, $a=2^{n-1}$,converts t_{n+1} into an integer ,then the integer cascaded chaotic map is given to be,

$$T_{n+1}=\begin{cases}\lfloor 4T_n\rfloor & 0\le T_n<1/4a\\ \lfloor 4T_n-a\rfloor & 1/4a\le T_n<1/2a\\ \lfloor 3a-4T_n\rfloor & 1/2a\le T_n<3/4a\\ \lfloor 4a-4T_n\rfloor & 3/4a\le T_n<a\end{cases} \quad (5)$$

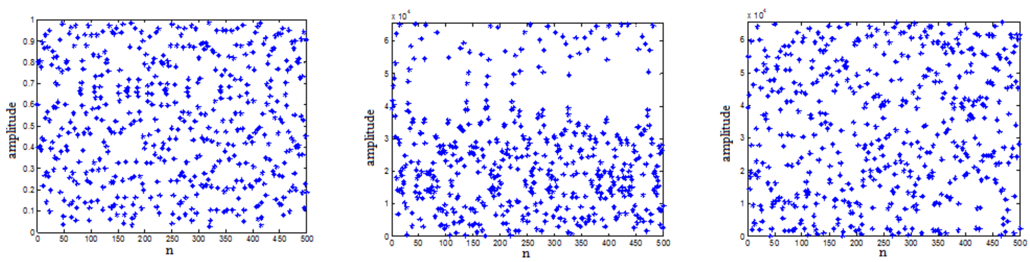
In Equation (5), the word length of processor is assumed to be $nbits$, and $T_{n+1}\in[0,2^n-1]$. For example, if the word length of processor is assumed to be 8 bits, that is $a=2^7$,and $T_{n+1}\in$ [0, 255],which just corresponds to the unsigned integer range of 8bits representation . $4T_n$ means the left shift two bits of T_n, this means that the cascaded integer chaos only need to do addition, subtraction, shift and other simple operations. as a result, the cascaded integer chaos not only suiTable for the node operation of wireless sensor network, but also can reduce the computing capability of processor and the resource costs of hardware.

As shown in Figure 2-4, on the basis of the comparison and analysis of attractor, ergodicity and initial value sensitivity, we found that the cascaded integer chaos has more excellent chaotic characteristics and statistical randomness. It follows that the cascaded integer chaos can effectively compensate the degradation of dynamic characteristics of the single-level integer chaos, and further improve the security of the block cryptogram algorithm of wireless sensor network.



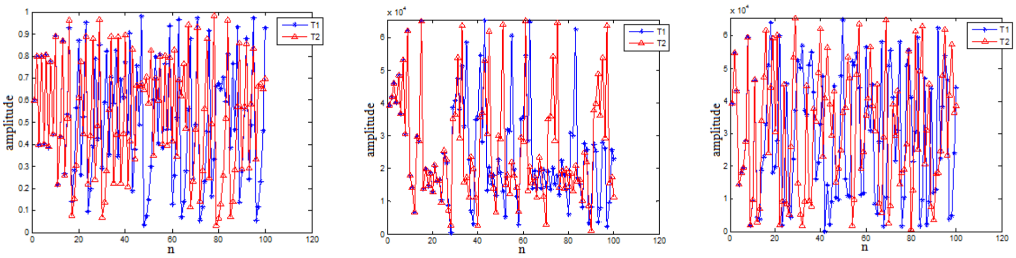
(a) tent (b) integer tent (c) cascaded integer tent

Figure 2. Attractor of different Chaotic Maps



(a) tent (b) integer tent (c) cascaded integer tent

Figure 3. Ergodicity of different Chaotic Maps



(a) tent (b) integer tent (c) cascaded integer tent

Figure 4. Initial Value Sensitivity of different Chaotic Maps

3. Design Method of S-box

In view of the limitation of computation, storage and energy in wireless sensor network, this paper propose a design method of S-box based on the cascaded integer chaos. The generation algorithm of S-box is composed of 2 stages: diffusion operation (step 1- step 2) and substitution operation (step 3- step 5). The concrete steps are as follows:

(1) Set the initial conditions of the cascaded integer chaotic map. the system parameter and the initial value of logistic chaotic map were set to be μ_1 =3.6 and $x_0 = 0.76$, and the system parameter of tent chaotic map is set to be μ_2 =1.987.

(2) According to step 1, the system trajectory would be obtained through the dynamic iteration of the cascaded integer chaotic map.

(3) The iterative interval of the cascaded integer chaos is divided into 256 equal intervals, which are represented as D_i （i =0, 1, …255） and D_i can be understood as [i / 256, (i +1) /256).

(4) To determine whether the iterative output $\mathrm{T_n}$ of the cascaded integer chaotic map exists in the interval D_i . If the value of $\mathrm{T_n}$ exists in the interval D_i （i =0, 1, …255） ,then save $\mathrm{T_n}$ as Y_n and continue to iterate . If the value of $\mathrm{T_n}$ doesn't exist in the interval D_i （i =0, 1, …255） or have already been traversed, then do not save $\mathrm{T_n}$ and continue to iterate, until $\mathrm{T_n}$ traverse all of 256 intervals .

(5) As shown in Table 1, Y_n is arranged line-by-line and converted into the Table of 16 x 16, that is 8×8 S-box.

Table 1. 8×8 S-box

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	F5	D8	EB	AA	9A	B9	6	F6	C2	CA	8C	8A	C3	40	77	5A
1	38	C6	10	0B	20	4E	75	23	2F	81	9B	3	F2	A2	70	4B
2	F0	7A	24	86	CB	1	5F	D4	C8	48	7F	1A	2B	15	AF	BC
3	DA	FC	D7	3F	13	61	F9	AC	A6	27	72	8B	A8	B1	87	73
4	CD	4F	E4	DB	A0	E6	D9	9	18	3E	64	63	11	6B	33	42
5	97	B3	F4	E2	19	AE	7D	B4	45	92	C5	7E	85	83	6C	9F
6	62	2	34	EC	B2	59	A9	BF	0E	ED	39	4D	41	0F	58	89
7	82	65	FA	16	66	99	3B	5B	8E	B5	A7	B6	B0	2D	29	84
8	46	80	7B	0C	7C	21	E5	AB	32	5C	C9	56	5	8F	14	6E

9	C7	4A	37	88	51	EA	DD	0A	FF	94	50	A1	6F	4C	55	1C
A	EE	BD	F1	3C	AD	0D	98	49	54	2A	D2	17	69	90	A3	6A
B	1D	F7	CC	E3	7	8D	60	47	96	D6	0	B7	76	67	71	31
C	C1	3D	93	DE	79	F8	22	EF	26	53	4	FD	5D	CF	44	95
D	F3	E0	78	DC	57	43	D1	1E	FE	25	D5	A5	91	35	A4	2C
E	30	DF	8	C0	9E	D0	E7	C4	CE	1F	B8	12	2E	BA	68	74
F	FB	E1	52	5E	1B	E8	BE	28	E9	36	3A	9C	BB	9D	D3	6D

When the input data is 8 bits, the first 4 bits determine the row of S-box, and the rear 4 bits determine the column of S-box. For example, when the input data is 01000000, the value of the first 4 bits is 4, and the value of the rear 4 bits is 0. Due to the rows and columns of S-box are starting from 0, the corresponding output is determined by the fourth row and zeroth column of S-box. As a result, the value of output data is CD, which can be converted to 11001101.

4. Mathematic Representation of S-box

S box is a multi-input and multi-output nonlinear combination function, also known as the logic function or Boolean function. n-ary Boolean function is a map from F_2^n to F_2, and generally recorded as $f(x): F_2^n \to F_2$ [13].Boolean function is closely related to the cryptographic properties such as nonlinearity degree, strict avalanche criterion, *etc*. Therefore, it is very important to study the mathematic representation of Boolean functions.

4.1. Truth Table Representation

Both domain and range of Boolean function are finite set, so it can be represented by the list method. Corresponding to all possible values of the independent variables, the values of n-ary Boolean function $f(x)$ can be unique determined. If each group of independent variables $(x_{n-1},\cdots,x_1,x_0)$ and their corresponding function values are all listed in the Table, which is called the truth Table of Boolean function. It can be seen from Table 1 when the input is 00H $(x_7x_6x_5x_4x_3x_2x_1x_0 = 00000000)$, the output is F5H $(y_7y_6y_5y_4y_3y_2y_1y_0 = 11110101)$.When the input traverse from 00H to FFH, the eight outputs of S-box can obtain their respective truth Tables.

4.2. Walsh Spectral Representation

Walsh spectrum is another common representation of Boolean function, so the Walsh spectrum is also an important tool to study S-box [14].

Suppose n-ary Boolean function $f(x): F_2^n \to F_2$, $x=(x_{n-1},\cdots,x_1,x_0)$, $w=(w_{n-1},\cdots,w_1,w_0)$, $x \in F_2^n$, $w \in F_2^n$, the dot product of w and x is given to be

$$w \cdot x = \sum_{i=0}^{n-1} w_i x_i \tag{6}$$

In Equation (6), $w \cdot x \in F_2$.

The first order Walsh linear spectrum and the first order Walsh cyclic spectrum of $f(x)$ are given to be[15],

$$S_f(w) = 2^{-n} \sum_{x \in F_2^n} (-1)^{w \cdot x} f(x) \tag{7}$$

$$S_{(f)}(w) = 2^{-n} \sum_{x \in F_2^n} (-1)^{f(x) \oplus w \cdot x} \tag{8}$$

5. Performance Test of S-box

For wireless sensor network, the cryptographic properties of S-box are very critical to the security strength of block cipher. The performance tests were carried out to determine the strength of the cryptographic properties of S-box, including nonlinearity, differential uniformity, strict avalanche criterion, out-put bit independence criterion and bijective property.

5.1. Nonlinearity Degree

Nonlinearity degree is an index used to measure the strength of the cryptosystem to resist the linear attack. The greater the nonlinearity degree of the S box, the stronger the ability to resist the linear cryptanalysis. For the convenience of calculation, the nonlinear degree of $f(x)$ expressed by the Walsh cyclic spectrum is given to be[16]

$$N_f = 2^{n-1}(1 - 2^{-n} \max_{w \in F_2^n} \left| S_{\langle f \rangle}(w) \right|) \tag{9}$$

As shown in Table 2 (a), the S-box has 8 Boolean functions, All the nonlinearity degrees of them are more than 100; As shown in Table 2 (b), the average nonlinearity degree of S-box is 105. It can be seen that the nonlinear property of S-box is high enough to resist the attack of the best linear approximation.

Table 2. Performance Test of Nonlinearity Degree

Table (a). Nonlinearity Degree of S-box

nonlinearity degree	N_1	N_2	N_3		N_4	N_5	N_6	N_7	N_8
S-box in this paper	106	106	108		108	102	104	104	102

Table (b). Comparison of Average Nonlinearity Degree

S-box	S-box in this paper	S-box in literature [17]	S-box in literature [18]	S-box in literature [19]
average nonlinearity degree	105	102	98	103

5.2. Differential Uniformity

The differential cryptanalysis is one of the most effective attack on block cryptogram. If the input / output XOR distribution of S-box is equiprobable, the S- box can effectively resist differential attack [16]. The smaller the maximum value of input/output XOR distribution of S-box, the stronger the ability to resist differential attack.

The input / output XOR distribution of $f(x)$ expressed by the differential approximation probability is given to be

$$DP_f = \max_{\Delta x \neq 0, \Delta y} \left(\frac{\# \{ x \in X \mid f(x) \oplus f(x \oplus \Delta x) = \Delta y \}}{2^n} \right) \quad (10)$$

In Equation (11), DP_f represents the maximum probability when the input difference is Δx and the output difference is Δy. X represents a set of all possible inputs of x, 2^n is the number of all elements in the set X. The smaller the value of differential approximation probability of S-box, the stronger the ability to resist differential attack [13].

As shown in Table 3 (a), the maximum value of input /output difference of S-box is only 10. Correspondingly, the differential approximation probability is merely 3.91%. As shown in Table 3 (b), the maximum value of input /output difference of S-box is equal to the literature [21] and less than other literatures, it shows that the S- box has stronger ability to resist differential attack.

Table 3. Performance Test of Differential Uniformity

Table (a). Input/output XOR Distribution of S-box

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

Table (b). Comparison of Input/output XOR Distribution

S-box	S-box in this paper	S-box in literature [19]	S-box in literature [20]	S-box in literature [21]
maximum value of input /output difference	10	12	12	10

5.3. Strict Avalanche Criterion (SAC)

The strict avalanche criterion refers to that half of the output is going to change when one input bit is changed. In literature [20] , the correlation matrix has been proposed to determine whether the S-box meets the strict avalanche criteria. If the value of each element of correlation matrix is close to 0.5, then the S-box meets the strict avalanche criterion.

The correlation matrix of S-box is shown in Table 4 (a), the average value of all elements is 0.5012, which is very close to the theoretical value; As shown in Table 4 (b), the correlation matrix of the S box is better than that of the existing classical S box, it indicates that the S-box would well meet the strict avalanche criterion.

Table 4. Performance Test of Strict Avalanche Criterion

Table (a). Correlation Matrix of S-box

	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8
00000001	0.5000	0.4688	0.4063	0.5625	0.5156	0.5000	0.5313	0.6094
00000010	0.5156	0.5469	0.5000	0.5156	0.4531	0.5625	0.4844	0.4063
00000100	0.4844	0.4688	0.5313	0.5625	0.5781	0.5156	0.5469	0.4531
00001000	0.4688	0.4844	0.5781	0.5000	0.5156	0.5000	0.5156	0.5469
00010000	0.5156	0.5469	0.4844	0.4844	0.4844	0.4844	0.5156	0.5313
00100000	0.4688	0.4531	0.4844	0.5156	0.4844	0.4531	0.4688	0.4844
01000000	0.5313	0.3906	0.4063	0.5000	0.4844	0.5469	0.5156	0.5469
10000000	0.4688	0.4531	0.4844	0.4375	0.5625	0.5781	0.5000	0.4844

Table (b). Comparison of Strict Avalanche Criterion

S-box	S-box in this paper	S-box in literature [19]	S-box in literature [20]	S-box in literature [21]
strict avalanche criterion	0.5012	0.5056	0.4954	0.5061

5.4. Output Bits Independence Criterion(BIC)

The output bits' independence criterion is one of the essential analysis elements in the design of S box. the method proposed by C. Adams and S. Tavares is used to measure the output bits independence criterion of S-box . Any two Boolean functions of S-box are represented by f_i and f_j , If the S-box meets the BIC- nonlinearity degree, then $f_i \oplus f_j$ would meet the property of nonlinearity degree; If the S-box meets the BIC-SAC, then $f_i \oplus f_j$ would meet the property of strict avalanche criterion [21].

As shown in Table 5 (a), the value of nonlinear degree of $f_i \oplus f_j$ is large, which shows that it can meet the nonlinear property; As shown in Table 5 (b), each element of the correlation matrix of $f_i \oplus f_j$ is close to 0.5, which shows that it can meet the strict avalanche criterion. it is concluded that the S-box has excellent output bits' independence criterion. As a result, we can draw a conclusion that the S-box has excellent output bits' independence criterion.

Table 5. Performance Test of Output Bits Independence Criterion

Table (a). BIC- Nonlinearity Degree of S-box

-	106	104	102	98	92	102	102
106	-	100	98	102	104	106	102
104	100	-	104	108	102	100	108
102	98	104	-	100	106	106	102
98	102	108	100	-	104	106	104
92	104	102	106	104	-	104	108
102	106	100	106	106	104	-	98
102	102	108	102	104	108	98	-

Table (b). BIC- SAC of S-box

-	0.5156	0.4883	0.4805	0.4785	0.4746	0.4844	0.5215
0.5156	-	0.4883	0.5137	0.5059	0.4902	0.4844	0.5078
0.4883	0.4883	-	0.4980	0.5078	0.5332	0.5176	0.5215
0.4805	0.5137	0.4980	-	0.5234	0.4883	0.5215	0.5078
0.4785	0.5059	0.5078	0.5234	-	0.5254	0.4805	0.5371
0.4746	0.4902	0.5332	0.4883	0.5254	-	0.4961	0.5137
0.4844	0.4844	0.5176	0.5215	0.4805	0.4961	-	0.4746
0.5215	0.5078	0.5215	0.5078	0.5371	0.5137	0.4746	-

5.5. Bijective Property

In general, the S-box is a reversible map. When the S-box is applied to the structure of substitution-scrambling, it must be bijective [22]. In the literature [7], the test method of bijective property is put forward, that is, the S box needs to meet the equation is given to be

$$\omega t(\sum_{i=1}^{n} a_i f_i) = 2^{n-1} \tag{12}$$

In Equation (12), hamming weight and Boolean function are represented by $\omega t(\ )$ and f_i respectively, $a_i \in \{0,1\}$ and $(a_1, a_2, \cdots, a_n) \neq (0, 0, \cdots, 0)$ .The sufficient and necessary condition for the S-box to meet the bijective property is that the sum of the linear operation of f_i is 2^{n-1}.

Through the observation, it can be found that all the data of S-box are just right between 0-255, and the sum of the linear operation of f_i is 128, it can be proved that S-box can meet the bijective property.

6. Conclusion

Wireless sensor network provides a brand-new way of information acquisition, but its large-scale application is also facing a series of technical challenges. How to achieve the security of communication and information in wireless sensor network has become increasingly urgent, it is necessary to take into account balance from the aspects of energy consumption, cost, security, *etc*. The design of S-box is realized through converting the system trajectory generated by dynamic iteration of the cascaded integer chaotic map into a pseudo random sequence. Through test and analysis, it can be concluded that the S-box has achieved better performance in terms of memory overhead, operation efficiency and security strength, and it is more suitable for application in the design of Wireless Sensor Network block cryptogram.

Acknowledgements

This work is supported by the National Natural Science Foundation of China (no.61471158) and doctor fund item of ministry of education (no.20132301110004).

References

[1] Z. Qian and Y. Wang, "Review of Wireless Sensor Network for EPC System Network", Journal of Electronics and Information, no. 01, **(2013)**, pp. 215-227.
[2] W. J. Huo and Z. L. Liu, "Secure Encryption Embedded Processor Design for Wireless Sensor Network Application", vol. 17, no. 1, **(2011)**, pp. 75-79.
[3] Y. He and S. Tian, "Block Encryption Algorithm Based on Chaotic S-box for Wireless Sensor Network", Journal of Computer Application, no. 4, **(2013)**, pp. 1081- 1084.
[4] X. Gu and W. Ding, "An S-Box Construction Algorithm Based on Chaotic Lorenz System", Journal of Chongqing University of Technology (Natural Science), no. 3, **(2013)**, pp. 97- 103.
[5] L. Xu, "Research on Security for Wireless Sensor Network Based on Chaos", Harbin Institute of Technology, **(2013)**.
[6] W. Yang and G. Liu, "Design of S-Boxes Based on Spatiotemporal Chaotic Systems of Cross Coupled Map Lattices", JOURNAL OF APPLIED SCIENCES-Electronics and Information Engineering, no. 4, **(2015)**, pp. 438- 448.
[7] Y. Ming-Ji, F. Xi-Ji and Y. Shu-Chun, "Encryption Algorithm Based on 3D Chaotic Mapping in HSV Space", JOURNAL OF HARBIN UNIVERSITY OF SCIENCE AND TECHNOLOGY 2015, vol. 20, pp. 103-106
[8] G. Tang, X. Liao and Y. Chen, "A Novel Method for Designing S-boxes Based on Chaotic Maps", Chaos, Solitons & Fractals, vol. 23, no. 2, **(2005)**, pp. 413-419.
[9] M. Khan, T. Shah, H. Mahmood, M. A. Gondal and I. Hussain, "A Novel Technique for the Construction of Strong S-boxes Based on Chaotic Lorenz Systems, Nonlinear Dynamics, vol. 70, no. 3, **(2012)**, pp. 2303-2311.
[10] C. Xing, "Research and Application of Chaos Encryption Based on WSN", Harbin Institute of Technology, **(2014)**.
[11] H. Wang, B. Song, Q. Liu, J. Pan and Q. Ding, "FPGA Design and Applicable Analysis of Discrete Chaotic Maps", International Journal of Bufication and Chaos, vol. 24, no. 4, **(2014)**, pp. 1-15.
[12] X. Tong, K. Zuo and Z. Wang, "A New Block Encryption Algorithm Based on Mixed Chaos for Wireless Sensor Network", Journal of Physics, no. 03, **(2012)**, 030502-1-11.
[13] M. Zheng, "Block Cipher Based on Integer Chaotic Map for the Wireless Sensor Networks", South China University of Technology, **(2013)**.
[14] L. Xin-Tao, G. Hua-Qiang and K. Shou-Qiang, "A New Five-dimensional Chaotic System and Its Circuit Implementation", JOURNAL OF HARBIN UNIVERSITY OF SCIENCE AND TECHNOLOGY, vol. 20, **(2015)**, pp. 101-113.
[15] H. Cai, "Cryptographic Properties of Boolean Function and Its Application in the AES Cryptanalysis", University of Electronic Science and Technology of China, **(2008)**.
[16] X. Yin and X. Yuan, "On Construction Algorithm of Strong S-boxes Based on Linear Transformation Coupling Chaotic System", Computer Application and Software, no. 8, **(2015)**, pp. 304- 307.
[17] I. Hussain, T. Shah and M. A. Gondal, "A Novel Approach for Designing Substitution-Boxes Based on Nonlinear Chaotic Algorithm", Nonlinear Dynamics, vol. 70, no. 3, **(2012)**, pp. 1791-1794.
[18] M. Khan, T. Shah and M. A. Gondal, "An Efficient Technique for the Construction of Substitution Box with Chaotic Partial Differential Equation", Nonlinear Dynamics, vol. 73, no. 3, **(2013)**, pp. 1795-1801.
[19] F. Ozkaynak and S. Yavuz, "Designing Chaotic S-boxes Based on Time-delay Chaotic System", Nonlinear Dynamics, vol. 74, no. 3, **(2013)**, pp. 551-557.
[20] A. F. Webster adn S. E. Tavares, "On the Design of S-boxes", Advances in Cryptology-CRYPTO'85 Proceedings, Berlin Heidelberg：Springer, **(1986)**, pp.523-534.
[21] C. Adams and S. Tavares, "Good S-boxes Are Easy to Find", Advances in Cryptology-CRYPTO'89 Proceedings. New York: Springer, **(1990)**, p. 612-615.
[22] M. Fan and F. Yang, "A Method to Construct Dynamic S-box Based on Chaotic Map in Block Cipher", Wireless Radio Engineering, vol. 46, no. 3, **(2016)**, pp. 33-36,40.

