Designing a random S-box with the mixed spatiotemporal chaos

Liyan Liu
City Institute, Dalian University of Technology, Dalian, China
E-mail: liuliyan81@sina.com

Abstract. A random S-box is designed by using the mixed linear-nonlinear spatiotemporal chaotic system. Firstly, a chaotic sequence produced by the mixed chaotic system is used to generate the elements of the S-box randomly. Then the elements of the S-box are permuted by using the mixed chaotic system. Owing to the high dimensional feature of the mixed chaotic system, the generated S-box has a strong randomness property. Finally, we analyse six properties of the designed S-box, such as bijective property, nonlinearity, strict avalanche criterion, outputs bit independence criterion, input/output XOR distribution and linear approximation probability. The experimental results indicate that the designed S-box by using the mixed chaotic system has better performance.

1. Introduction
Block ciphers play an important role in the field of information security. Because substitution box (S-box) can provide necessary confusion to ensure the security of block cipher, it is the unique nonlinear component of some block ciphers, such as Advanced Encryption Standard (AES), Data Encryption Standard (DES) and International Data Encryption Algorithm (IDEA).

The chaotic theory has been used in the S-box widely [1-6] in recent years. Chaotic sine map was employed to construct S-boxes in [1]. Khan et al. [2] designed S-boxes with Lorenz and Rössler chaotic systems. Tent map was used to obtain a dynamic S-box in [3]. Chebyshev map and 3D Baker map were utilized to generate S-boxes in [4]. Logistic and Baker chaotic maps were employed to construct S-boxes in [5]. A new chaotic S-box was designed by using of logistic map in [6]. However, the above designed S-boxes are based on low dimensional systems. Under finite precision computation in the modern computers, the dynamical behaviors of the low dimensional chaotic system may degrade. This degradation can lead periodic trajectories, so that the randomness of chaotic sequences is affected. Two spatiotemporal chaotic systems with high dimensional characteristics [7-8] have been used to construct S-boxes. The mixed linear-nonlinear coupled map lattices (MLNCML) system [9] is also a spatiotemporal chaos system. Because of its high dimensional feature, it can not only resist the degradation of finite precision computation but also produce many chaotic sequences. Therefore, the MLNCML system is also suitable to construct S-boxes.

In this paper, we design a new S-box with the MLNCML system. The random sequences generated by the MLNCML system are employed to generate and permute the elements of the S-box. The results of performance analysis show that the designed S-box is effective. And the designed S-box in this paper has better performance than the other S-boxes.
2. Preliminaries

2.1. MLNCML system
The MLNCML system [9] is expressed as:

\[ x_{t+1}(i) = (1 - \varepsilon) f(x_t(i)) + (1 - \gamma) \frac{\varepsilon}{2} \left( f(x_t(i + 1)) + f(x_t(i - 1)) \right) + \gamma \varepsilon \left( f(x_t(a)) + f(x_t(c)) \right), \]

where \( i, a \) and \( c \) are the lattices \( 1 \leq i \leq N \), \( N \) is the number of all the lattices, \( t \) is the time parameter \( (t = 1, 2, 3, \ldots) \), \( \gamma \) is the coupling parameter \( (0 \leq \gamma \leq 1) \), \( f(x) = \mu x(1 - x) \) and \( \mu \in [0, 4] \), \( \varepsilon \) is the coupling parameter \( (0 \leq \varepsilon \leq 1) \). The MLNCML system is a mixed linear-nonlinear spatiotemporal chaotic system.

2.2. Bijective property
If the linear sum of the Boolean function \( f_i(1 \leq i \leq n) \) of the designed \( n \times n \) S-box was \( 2^{n-1} \), \( f \) was a bijection [10]. The expression is \( \sum_{i=1}^{n} a_i f_i = 2^{n-1} \) \((w() \) is the Hamming weight, \( a_i \in \{0,1\} \) and \( (a_1, a_2, \ldots, a_n) \neq (0, 0, \ldots, 0) \).

2.3. The equiprobable input/output XOR distribution
In [11], differential cryptanalysis for an S-box was proposed by using the imbalances in the input/output XOR distribution table. The XOR value of each output and that of each input must have the same probability. Any S-box should have differential uniformity. Using the differential approximation probability (DP), we can determine the differential uniformity of the proposed S-box. The DP is defined as:

\[ DP_f = \max_{\Delta x \neq 0, \Delta y} \left( \frac{\#\{x \in X | f(x) \oplus f(x \oplus \Delta x) = \Delta y \}}{2^n} \right), \]

where \( 2^n \) is the number of its elements and \( X \) is the series of all possible input values.

2.4. Linear approximation probability
The maximum value of the imbalance of an event is expressed as the linear approximation probability (LP) is. In [12], LP is expressed as:

\[ LP_f = \max_{\alpha_1, \alpha_2 \neq 0} \left( \frac{\#\{x \in X | x \cdot \alpha_1 = f(x) \cdot \alpha_2 \} - 1}{2^n} \right), \]

Where \( 2^n \) is the number of its elements, \( \alpha_1 \) and \( \alpha_2 \) are input and output masks respectively and \( X \) is the series of all possible input values. The parity of the input bits chosen by the mask \( \alpha_1 \) equals to the parity of the output bits chosen by the mask \( \alpha_2 \).

2.5. Nonlinearity
In [13], the nonlinearity \( N_f \) of a Boolean function \( f(x) \) was computed by:

\[ N_f = 2^{n-1} - \frac{1}{2} \max_{\omega \in GF(2)^n} \left| F(\omega) \right|, \]

where \( F(\omega) \) denotes the Walsh Spectrum [14], \( x \cdot \omega \) is the dot-product over \( GF(2) \).
2.6. Strict avalanche criterion
Webster and Tavares firstly introduced the strict avalanche criterion (SAC) in [15]. If the SAC is satisfied, all of the output bits change with a probability of a half when a single input bit is complemented. The dependence matrix is always used to describe the SAC of an S-box. If each element of the dependence matrix is close to the optimum value 0.5, the S-box approximately satisfies the SAC.

2.7. Output bits independence criterion
The output bits independence criterion (BIC) is also presented in [15]. For a certain series of avalanche vectors generated by complementing a single plaintext bit, all the avalanche variables should be pair-wise independent.

Suppose \( f_1, f_2, \ldots, f_n \) are the Boolean functions in an S-box. If the S-box satisfies BIC, \( f_j \oplus f_k (j \neq k, 1 \leq j, k \leq n) \) should satisfy the avalanche criterion and be highly nonlinear.

3. Designing the S-box with the MLNCML chaotic system
An S-box is designed by using the MLNCML chaotic system in this section. Given the initial values of the MLNCML system parameters, the obtained S-box is unique. The following is the detailed construction procedures of the proposed S-box.

\( \text{Step 1.} \) Obtain \( N = 100 \) chaotic sequences by iterating the Equation (1) 2000 times.

\( \text{Step 2.} \) Choose the tenth of the 100 sequences, and compute each elements of the sequence by using the Equation (6).

\[ y(i) = \text{mod} \left( \text{mod} \left( x_{10} (99 + i) \times 10^{14} \right), 1000 \right), 256 \right) \]

\( \text{Step 3.} \) Choose 256 different elements from the sequence \( y \) in order and construct a new sequence \( z \).

\( \text{Step 4.} \) Reconvert \( z \) to a matrix \( A(16 \times 16) \).

\( \text{Step 5.} \) Exchanging the values of \( A(j, k) \) and \( A(m, n) \), where \( j \) is the row number of the matrix \( A \), \( k \) is the column number of the matrix \( A \), and \( j, k \in [1, 16] \), \( m \) and \( n \) are computed by using the Equation (7), the relation of \( j, k, b, d \) satisfies Arnold cat map.

\[ \begin{align*}
  m &= \text{mod} \left( \lfloor x_{10} (A((j-1) \times 16 + k) \times 10^{14}) \rfloor + (200 + (j - 1) \times 16 + k) \times 10^{14} \right), 16 \\
  n &= \text{mod} \left( \lfloor x_{10} (b \times 10^{14}) \rfloor + 1 \right), 16
\end{align*} \]

\( A \) is the obtained S-box, as shown in Table 1.

Table 1. The obtained S-box.

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

We use six criteria [1, 4-8] to analyze the performance of the proposed S-box, which are bijective property, input/output XOR distribution, linear approximation probability (LP) nonlinearity, strict avalanche criterion (SAC) and outputs Bit Independence Criterion (BIC).

4.1. Bijective property

The bijectivity value of the proposed S-box is 128. Therefore, the proposed S-box satisfies the bijective property.

4.2. The equiprobable input/output XOR distribution

In Figure 1 and Table 2, the maximum differential approximation probabilities of different S-boxes are compared. We can note that the maximum differential approximation probability of the proposed S-box is consistent with that of other S-boxes. Therefore, the proposed S-box satisfies DP property.

4.3. Linear approximation probability

In Figure 2 and Table 2, the linear approximation probabilities of different S-boxes are compared. We can find that the proposed S-box is equal or greater than other S-boxes [4-5, 8] for the value of LP. So, the proposed S-box has a good LP performance.
4.4. Nonlinearity
We analyze the nonlinearity of the proposed S-box, and the results are shown in Figure 3 and Table 2. We can see that the average value of nonlinearity for the proposed S-box is 104. The result accords with the results of other S-boxes. Hence, the proposed S-box has good nonlinearity.

4.5. Strict avalanche criterion
In Figure 4 and Table 2, SAC for different S-boxes are compared. We can find that the SAC property of the proposed S-box is consistent with that of other S-boxes. In the proposed S-box, the elements of its dependence matrix are between 0.4063 and 0.6250, as shown in Table 3, and the average value is 0.4988, which very verges on the ideal value 0.5. It proves that the proposed S-box has good SAC performance.

4.6. Output bits independence criterion
The mean value of BIC-nonlinearity is 103.57 and the mean value of BIC-SAC is 0.4986 in the proposed S-box. These indicate that the proposed S-box has good BIC performance. In Figures 5 and 6 and Table 2, BIC performances for different S-boxes are compared. We can see that the proposed S-box has the similar BIC performance with other S-boxes.
Table 2. S-boxes characteristic comparison.

| S-boxes  | DP | LP | Nonlinearity | SAC | BIC |
|----------|----|----|--------------|-----|-----|
|          | MaxDP | MaxLP | Max | Avg. | Max | Avg. | BIC-Nonlinearity | BIC-SAC |
| Proposed | 10/0.0391 | 0.1328 | 108 | 100 | 104 | 0.6250 | 0.4988 | 103.57 | 0.4986 |
| Reference [4] | 14/0.0547 | 0.1328 | 106 | 100 | 103 | 0.6094 | 0.4219 | 0.5000 | 103.14 | 0.5024 |
| Reference [5] | 10/0.0391 | 0.1328 | 109 | 103 | 104.88 | 0.5703 | 0.3984 | 0.4966 | 102.96 | 0.5044 |
| Reference [6] | -0.0390 | 0.1406 | 110 | 106 | 107.5 | 0.6094 | 0.3750 | 0.5093 | 103.07 | 0.5025 |
| Reference [7] | 12/0.0469 | 0.1406 | 108 | 102 | 104.25 | 0.6250 | 0.4219 | 0.5083 | 103.07 | 0.5008 |
| Reference [8] | 12/0.0469 | 0.1250 | 108 | 102 | 104.5 | 0.6406 | 0.4219 | 0.4980 | 104.64 | 0.5075 |

5. Conclusions
This paper designs a random S-box with the MLNCML chaotic system. We use a chaotic sequence generated by the MLNCML system to form the elements of the initial S-box, and then employ all of the chaotic sequences generated by the MLNCML system to shuffle the elements of the S-box. A large number of chaotic sequences and permutation operation greatly improve the randomness property of the designed S-box. The performance analysis results indicate that the designed S-box in this paper is effective and has equal or better performance than other S-boxes.

Table 3. Dependence matrix.

| Dependence matrix |
|-------------------|
| 0.4531 0.5781 0.4375 0.4688 0.5313 0.4688 0.4688 0.5000 |
| 0.5000 0.5313 0.4531 0.5156 0.5625 0.4688 0.5000 0.4375 |
| 0.4688 0.5000 0.5000 0.5000 0.4688 0.4844 0.5000 0.5156 |
| 0.5625 0.4844 0.5781 0.4844 0.4688 0.4688 0.5313 0.5469 |
| 0.5156 0.4844 0.5781 0.5313 0.4063 0.5156 0.5000 0.4844 |
| 0.5000 0.4688 0.5156 0.4531 0.4844 0.4844 0.4688 0.5313 |
| 0.5313 0.5313 0.5313 0.5000 0.5000 0.5156 0.4375 0.4063 |
| 0.5313 0.6250 0.5625 0.4375 0.5000 0.5156 0.4063 0.5313 |

References
[1] Belazi A and El-Latif A A A 2016 A simple yet efficient S-box method based chaotic sine map Optik - International Journal for Light and Electron Optics S0030402616314887
[2] Khan M, Shah T, Mahmood H and Gondal M A 2013 An efficient method for the construction of block cipher with multi-chaotic systems Nonlinear Dyn. 71 489-92
[3] Wang Y, Wong K W, Liao X F and Xiang T 2009 A block cipher with dynamic S-boxes based on tent map Commun. Nonlinear Sci. Numer. Simul. 14 3089-99
[4] Chen G, Chen Y and Liao X F 2007 An extended method for obtaining S-boxes based on 3-dimensional chaotic baker maps Chaos Solitons Fractals 31 571-9
[5] Tang G, Liao X F and Chen Y 2005 A novel method for designing S-boxes based on chaotic maps Chaos Solitons Fractals 23 413-9
[6] Tian Y and Lu Z M 2017 Intertwining logistic map and bacterial foraging optimization Mathematical Problems in Engineering
[7] Liu L Y and Lei Z Y 2019 An approach for constructing the S-box using the CML system Journal of Physics: Conference Series
[8] Liu L Y, Zhang Y Q and Wang X Y 2018 A novel method for constructing the S-box based on spatiotemporal chaotic dynamics Applied Sciences 8 2650
[9] Kaneko K 1993 Theory and application of coupled map lattices (New York: John Wiley and Sons)
[10] Adams C and Tavares S 1989 Good S-boxes are easy to find International Cryptology Conference on Advances in Cryptology
[11] Biham E and Shamir A 1991 Differential cryptanalysis of DES-like cryptosystems J. Cryptol. 4
3-72

[12] Matsui M 1994 Linear cryptanalysis method of DES cipher *Advances in Cryptology: Proceeding of the Eurocrypt ’93* (Lecture Notes in Computer Science vol 765) pp 386-397

[13] Cusick T W and Stǎnicǎ P 2009 *Cryptographic Boolean Functions and Applications* 209-27

[14] Meier W and Staffelbach O 1989 Nonlinearity criteria for cryptographic functions *Workshop on the Theory and Application of of Cryptographic Techniques* (Berlin, Heidelberg: Springer)

[15] Webster A F and Tavares S 1986 On the design of S-boxes *Advances in Cryptology: Proceedings of CRYPTO_85* (Lecture Notes in Computer Science) pp 523-534