An approach for constructing the S-box using the CML system

Liyan Liu¹ and Zhiyi Lei
City Institute, Dalian University of Technology, Dalian, China

¹E-mail: liuliyan81@sina.com

Abstract. We propose an approach for constructing S-box by using the CML chaotic system. The chaotic sequences produced by the CML chaotic system are used to permute and diffuse the elements of the S-box randomly. The obtained S-box has a strong randomness property due to the high dimensional feature of the CML chaotic system. We analyze bijective property, nonlinearity, strict avalanche criterion, outputs bit independence criterion, input/output XOR distribution and linear approximation probability of the constructed S-box. The experimental results show that the proposed approach for constructing S-box is effective.

1. Introduction
Substitution box (S-box) is an important nonlinear component for the security of cryptographic systems. It has been widely used in many block cryptosystems, such as Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA) and Advanced Encryption Standard (AES). In recent years, the chaotic theory has been widely applied for the S-box. However, the chaotic systems used for designing S-boxes are low dimensional systems. Moreover, the number of chaotic sequences used for designing S-boxes is one or a few. For the low dimensional chaotic system, the dynamical behaviors may degrade under finite precision computation in the modern computers. This degradation can lead periodic trajectories that affect the randomness of chaotic sequences. The coupled map lattices (CML) system [1] is a spatiotemporal chaotic system. It can not only produce many chaotic sequences but also resist the degradation of finite precision computation due to its high dimensional feature. Moreover, the CML system has been employed in the secure encryption schemes [2-4].

In this paper, we present an efficient S-box construction method by using the CML chaotic system. The CML system which is a high dimensional chaotic system can produce many good random sequences and efficiently alleviate dynamical degradation. These random sequences are used to permute and diffuse the elements of the S-box. The analysis results of Six criteria show that the proposed approach is effective. Compared with the former approaches, the simulation and experimental results indicate that the proposed approach has better performance.

2. Related work
The chaos theory has been employed to construct S-boxes broadly [5-26]. Secure S-boxes were generated by using exponential and logistic chaotic maps in [5]. Lorenz system was used to develop S-boxes in [6, 7]. An efficient method for constructing S-boxes is proposed by the use of chaotic sine map in [8]. Wang et al. [9] designed a dynamic S-box construction method using Tent map. 3D four-wing autonomous chaotic system was used to design S-boxes in [10]. An extended method for
constructing S-boxes is presented using a Chebyshev map and a 3D Baker map in [11]. 8*8 S-boxes were obtained by the use of Logistic and Baker chaotic maps in [12]. New S-boxes were synthesized by using Lorenz and Rössler chaotic systems in [13]. A new method of generating S-box was developed by the use of chaotic tent map and composition method in [14]. S-boxes were constructed by the use of the logistic-sine map in [15]. A nonlinear chaotic algorithm was used to construct an efficient S-box in [16]. An S-box was constructed using a chaotic system without equilibrium in [17]. The results of performance tests show that the produced S-boxes have good cryptographic performance. A new S-box construction method based on fractional-order chaotic Chen system was presented in [18]. This method provides a stronger S-box design. A new chaotic S-box based on the intertwining logistic map and bacterial foraging optimization was designed in [22]. The proposed S-box can effectively resist multiple types of cryptanalysis attacks. However, the above chaotic systems used for designing S-box are low dimensional systems. Moreover, the number of chaotic sequences used for designing S-boxes is less than that of the CML system.

3. Preliminaries

3.1. CML system

The CML system [1] is defined as follows:

$$x_{r+1}(i) = (1 - \varepsilon)f[x_i(i)] + \frac{\varepsilon}{2} \{f[x_i(i + 1)] + f[x_i(i - 1)]\}$$

where $t$ is the time parameter ($t = 1, 2, 3, K$), $i$ is the lattice ($1 \leq i \leq N$), $N$ is the number of all the lattices, $\varepsilon$ is the coupling parameter ($0 \leq \varepsilon \leq 1$), $f(x) = \mu x(1 - x)$ and $\mu \in [0, 4]$. The CML system coupled in adjacent lattices is a spatiotemporal chaotic system. When varying the value of $\mu$ in the logistic map continuously, most of these dynamical systems have chaotic features.

3.2. Bijective property

Adams and Tavares [27] pointed out that if the linear sum of the Boolean function $f_i (1 \leq i \leq n)$ of each component of the designed $n \times n$ S-box was $2^n - 1$, $f$ was then a bijection. The expression is represented as $w(\sum_{i=1}^{n} a_i f_i) = 2^n - 1$, where $w(g)$ is the Hamming weight, $a_i \in \{0, 1\}$ and $(a_1, a_2, K, a_n) \neq (0, 0, K, 0)$.

3.3. Nonlinearity

The nonlinearity $N_f$ of a Boolean function $f(x)$ [28] can be represented as:

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

where $F(\omega)$ denotes the Walsh Spectrum [29] of defined as:

$$F(\omega) = \sum_{x \in GF(2)^n} (-1)^{f(x) + x \cdot \omega},$$

where $\omega \in GF(2)^n$ and $x \cdot \omega$ is the dot-product over $GF(2)$.

3.4. Strict avalanche criterion

The strict avalanche criterion (SAC) was firstly introduced by Webster and Tavares [30]. It means that all of the output bits change with a probability of a half when a single input bit is complemented if the SAC is satisfied. The dependence matrix is always used to describe the SAC of an S-box. In fact, if each of its elements is close to the optimum value 0.5, the S-box approximately satisfies the SAC.
3.5. Output bits independence criterion
Webster and Tavares [30] also presented the output bits independence criterion (BIC). It means that all the avalanche variables should be pair-wise independent for a certain series of avalanche vectors produced by complementing a single plaintext bit.

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

3.6. The equiprobable input/output XOR distribution
Differential cryptanalysis for an S-box using the imbalances in the input/output XOR distribution table was proposed in [31]. The XOR value of each output must have the same probability with that of each input. Each S-box should have differential uniformity. The differential uniformity of the proposed S-box can be determined by using the differential approximation probability (DP) calculated as:

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

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

3.7. Linear approximation probability
The linear approximation probability (LP) is the highest value of the imbalance of an event. The parity of the input bits chosen by the mask \( \alpha_i \) is equal to the parity of the output bits chosen by the mask \( \alpha_j \). Based on Matsui’s original definition [32], LP is defined as:

\[
LP = \max_{\alpha_i, \alpha_j} \left( \frac{\# \{ x \in X | x \cdot \alpha_i = f(x) \cdot \alpha_j \} }{2^n} - \frac{1}{2} \right),
\]

where \( \alpha_i \) and \( \alpha_j \) are respectively input and output masks, \( X \) is the series of all possible input values and \( 2^n \) is the number of its elements.

4. The proposed S-box construction approach
In this section, an S-box construction method based on the CML chaotic system is proposed. When the values of the CML system parameters are given, the chaotic sequences generated by the CML system are fixed. Thus, the constructed S-box is stable. The detailed construction procedures of the S-box are given below.

\textit{Step1}. Constructing a linear sequence \( \mathcal{U}(1 \times 256) \) by using the 256 integers between 0 and 255.

\textit{Step2}. Reconvert \( \mathcal{U}(1 \times 256) \) to a matrix \( \mathcal{B}(16 \times 16) \).

\textit{Step3}. Obtaining \( N = 100 \) chaotic sequences by iterating the equation (1) 2000 times.

\textit{Step4}. Obtaining the values of \( b \) and \( d \) by:

\[
\begin{align*}
   b &= \text{mod}(x_{300(l-1)+16r}, \text{mod}(B((l-1) \times 16 + r), N) + 1) \times 10^{14} \times 16) + 1, \\
   d &= \text{mod}(x_{(u) \times 10^{14}}, 16) + 1,
\end{align*}
\]

where \( l \) denotes the row number of the matrix \( B \), \( r \) denotes the column number of the matrix \( B \), \( l, r \in [1,16] \), and the relations of \( l, r, u, v \) are calculated by Arnold cat map

\[
\begin{bmatrix}
   u \\
   v
\end{bmatrix} = \begin{bmatrix}
   1 & p \\
   q & pq + 1
\end{bmatrix} \begin{bmatrix}
   l
\end{bmatrix} \mod(N),
\]

where \( p \) and \( q \) are the parameters of Arnold cat map.

\textit{Step5}. Swapping the values of \( B(l, r) \) and \( \mathcal{B}(b, d) \) by using the equation (6). \( B \) is the final S-box. The constructed S-box is shown in Table 1.
Table 1. The constructed S-box.

|   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|
| 164 | 235 | 130 | 220 | 214 | 159 | 152 |
| 51  | 117 | 73  | 210 | 77  | 47  | 132 |
| 187 | 144 | 112 | 36  | 104 | 223 | 101 |
| 166 | 208 | 32  | 59  | 229 | 189 | 124 |
| 212 | 135 | 146 | 1   | 25  | 241 | 71  |
| 232 | 183 | 97  | 70  | 119 | 44  | 89  |
| 55  | 46  | 92  | 88  | 155 | 27  | 215 |
| 196 | 60  | 95  | 35  | 111 | 195 | 75  |
| 94  | 252 | 206 | 91  | 247 | 83  | 244 |
| 99  | 38  | 216 | 168 | 140 | 3   | 100 |
| 84  | 98  | 116 | 125 | 199 | 129 | 253 |
| 234 | 161 | 102 | 202 | 230 | 139 | 5   |
| 12  | 204 | 49  | 160 | 67  | 18  | 143 |
| 7   | 41  | 93  | 63  | 182 | 226 | 240 |
| 243 | 20  | 90  | 137 | 248 | 28  | 246 |
| 50  | 176 | 207 | 33  | 219 | 201 | 110 |

5. Performance analysis
Adams and Tavares [27] presented that “good” s-boxes have four properties, which are bijection, nonlinearity, strict avalanche and independence of output bits. Six criteria are used to analyze the performance of the obtained S-boxed [6, 8, 11, 12, 15, 17-22], which are bijective property, nonlinearity, strict avalanche criterion (SAC), outputs Bit Independence Criterion (BIC), input/output XOR distribution and linear approximation probability (LP).

5.1. Bijective property
In the proposed S-box, the obtained bijectivity value was equal to 128. Therefore, the proposed S-box satisfies the bijective property.

5.2. Nonlinearity
The results of nonlinearity analysis are shown in Table 2. It can be noted that the mean value of nonlinearity for the proposed S-box is 104.25, which is consistent with the results obtained by other S-boxes.

5.3. Strict avalanche criterion
The values in the dependence matrix of our S-box are between 0.6250 and 0.4219, and the mean value is 0.5083, which is very close to the ideal value 0.5. This indicates that the S-box presented in this paper has good SAC performance. A comparison of SAC for different S-boxes is listed in Table 2. It can be found that the SAC property of the proposed S-box accords with that of other S-boxes.

5.4. Output bits independence criterion
In order to check the BIC of our S-box, we compute the SAC and the nonlinearity of \( f_j \oplus f_k (j \neq k, 1 \leq j,k \leq n) \). The average values of BIC-nonlinearity and BIC-SAC of our S-box are respectively 103.07 and 0.5008, which shows that the proposed S-box satisfies the BIC performance. A comparison of BIC performance for different S-boxes is listed in Table 2. It can be found that the BIC performance of the proposed S-box is consistent with that of other S-boxes.

5.5. The equiprobable input/output XOR distribution
A comparison of the maximum differential approximation probabilities for different S-boxes is shown in Table 2. It can be noted that the maximum differential approximation probability of our S-box is...
consistent with that of other S-boxes. Therefore, the S-box presented in this paper satisfies DP property.

5.6. Linear approximation probability
The LP analysis of different S-boxes is listed in Table 2. It can be found that the proposed S-box is higher than other S-boxes [5, 6, 11, 12, 16] for the value of LP. But, the value of LP in the proposed S-box is equal to that in [22]. Therefore, the proposed S-box has an acceptable LP performance.

| S-boxes        | Nonlinearity | SAC   | BIC   | LP   | MaxDP | MaxLP |
|----------------|--------------|-------|-------|------|-------|-------|
| Proposed       | 108          | 102   | 104.25| 0.6250| 0.4219| 0.5083| 103.07| 0.5008| 12/0.0469| 0.1406 |
| Ref. [5]       | 108          | 100   | 103.25| 0.5938| 0.3750| 0.5059| 104.29| 0.5031| 12/0.0469| 0.1250 |
| Ref. [6]       | 106          | 100   | 103.25| 0.5938| 0.4219| 0.5049| 103.71| 0.5010| 10/0.0391| 0.1328 |
| Ref. [11]      | 106          | 100   | 103   | 0.6094| 0.4219| 0.5000| 103.14| 0.5024| 14/0.0547| 0.1328 |
| Ref. [12]      | 109          | 103   | 104.88| 0.5703| 0.3984| 0.4966| 102.96| 0.5044| 10/0.0391| 0.1328 |
| Ref. [16]      | 108          | 102   | 104.75| 0.5938| 0.3906| 0.5056| 104.07| 0.5022| 12/0.0469| 0.1250 |
| Ref. [17]      | 110          | 104   | 106   | 0.5781| 0.4018| 0.4946| 103.857| 0.4988| 10/-      | -     |
| Ref. [18]      | 108          | 100   | 104.7  | 0.5781| 0.4218| 0.4982| 103.1  | 0.4942| 10/-      | -     |
| Ref. [22]      | 110          | 106   | 107.5  | 0.6094| 0.3750| 0.5093| 103.07| 0.5025| -0/0.0390| 0.1406 |

6. Conclusions
This paper presents an S-box construction approach based on the CML spatiotemporal chaotic system. \(N=100\) chaotic sequences generated by the CML system are employed to construct the S-box, which increases the safety performance of the constructed S-box. Moreover, the high dimensional feature of the CML system can not only resists the degradation of finite precision computation, but also increases the strength of the constructed S-box. In the proposed S-box construction approach, all of the chaotic sequences generated by the CML system are used to shuffle the elements of the obtained S-box, which greatly improves the randomness property of the constructed S-box. The results of performance analysis show that the proposed S-box construction approach is effective and the CML spatiotemporal chaotic system is very suitable for constructing S-box.

References
[1] Kaneko K 1993 Theory and application of coupled map lattices (New York: John Wiley and Sons)
[2] Pisarchik A N, Flores-Carmona N J and Carpio-Valadez M 2006 Encryption and decryption of images with chaotic map lattices Chaos 16 033118
[3] Wang X Y and Bao X M 2013 A novel block cryptosystem based on the coupled chaotic map lattice Nonlinear Dyn. 72 707-15
[4] Wang X and Teng L 2011 An image blocks encryption algorithm based on spatiotemporal chaos Nonlinear Dyn. 67 365-71
[5] Jakimoski G and Kocarev L 2001 Chaos and cryptography: block encryption ciphers IEEE Trans. Circuits Syst. I 48 163-9
[6] Özkaynak F and Özer A B 2010 A method for designing strong S-boxes based on chaotic Lorenz system Phys. Lett. A 374 3733-8
[7] Khan M, Shah T, Mahmood H, Gondal M A and Hussain I 2012 A novel technique for the construction of strong S-boxes based on chaotic Lorenz systems Nonlinear Dyn. 70 2303-11
[8] 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
[9] Wang Y, Wong KW, 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
[10] Liu G, Yang W, Liu W and Dai Y 2015 Designing S-boxes based on 3-D four-wing autonomous chaotic system Nonlinear Dyn. 82 1867-77
[11] 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
[12] 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
[13] 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
[14] Dragan L 2014 A novel method of S-box design based on chaotic map and composition method Chaos Solitons Fractals 58 16-21
[15] Belazi A, Khan M, Abd El-Latif A A and Belghith S 2016 Efficient cryptosystem approaches: S-boxes and permutation substitution-based encryption Nonlinear Dyn. 87 1-25
[16] Hussain I, Shah T and Gondal M A 2012 A novel approach for designing substitution-boxes based on nonlinear chaotic algorithm Nonlinear Dyn. 70 1791-4
[17] Wang X, Ünal Çavuşoğlu, Sezgin Kacar, Akif Akgul, Viet-Thanh Pham, Sajad Jafari, Fawaz E Alsaadi and Xuan Quynh Nguyen 2019 S-box based image encryption application using a chaotic system without equilibrium Appl. Sci. 9 781
[18] Fatih Özkaynak, Vedat Çelik, and Ahmet Bedri Özer 2016 A new s-box construction method based on the fractional-order chaotic Chen system Signal Image & Video Processing 11 659-64
[19] Dragan Lambić 2018 S-box design method based on improved one-dimensional discrete chaotic map Journal of Information and Telecommunication 2 181-91
[20] Wang Y, Lei P and Wong K W 2015 A method for constructing bijective s-box with high nonlinearity based on chaos and optimization International Journal of Bifurcation and Chaos 25 1550127
[21] Ahmad M and Chopra A 2017 Chaotic dynamic s-boxes based substitution approach for digital images
[22] Tian Y and Lu Z M 2017 Chaotic s-box: intertwining logistic map and bacterial foraging optimization Mathematical Problems in Engineering
[23] Peng J, El-Latif A A A, Belazi A and Kotulski Z 2017 Efficient chaotic nonlinear component for secure cryptosystems 2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN) IEEE
[24] Guesmi R, Farah M A B, Kachouri A and Samet M 2015 Chaos-based designing of a highly nonlinear S-box using Boolean functions IEEE International Multi-conference on Systems IEEE
[25] Tian Y and Lu Z 2017 Novel permutation-diffusion image encryption algorithm with chaotic dynamic s-box and DNA sequence operation AIP Advances 7 085008
[26] Harmouch Youssef and Kouch Rachid El 2018 Brownian techniques for constructing high-strong cryptographic s-boxes ACM International Conference Proceeding Series p 19-26
[27] Adams C and Tavares S 1989 Good s-boxes are easy to find International Cryptology Conference on Advances in Cryptology
[28] Cusick T W and Stănică P 2009 Cryptographic Boolean Functions and Applications 209-27
[29] Meier W and Staffelbach O 1989 Nonlinearity criteria for cryptographic functions Workshop on the Theory and Application of of Cryptographic Techniques (Berlin, Heidelberg: Springer)
[30] 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
[31] Biham E and Shamir A 1991 Differential cryptanalysis of DES-like cryptosystems J. Cryptol. 4 3-72
[32] 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