Nonlinear Dyn (2021) 103:1151–1166
https://doi.org/10.1007/s11071-020-06098-0

ORIGINAL PAPER

2D mixed pseudo-random coupling PS map lattice and its application in S-box generation

Peizhao Zhou · Junxiao Du · Kai Zhou · Shengfei Wei

Received: 13 August 2020 / Accepted: 16 November 2020 / Published online: 6 January 2021

Abstract In this paper, firstly, we investigate a new 1D PWLCM-Sin (PS) map which derived from PWLCM and Sin map by modulo operation. Due to the stronger parameter space, bigger Lyapunov exponents and better ergodicity than simple 1D map, the PS map is more suitable for local map of spatiotemporal dynamics. Secondly, with the novel 2D pseudo-random mixed coupling method we present a spatiotemporal chaos which used PS map as local map $f(x)$. This spatiotemporal chaos named 2D Mixed pseudo-random Coupling PS Map Lattice (2DMCPML). The experimental results of bifurcation diagrams, Kolmogorov–Sinai entropy density and spatiotemporal chaotic diagrams showed that 2DMCPML has advantages of larger parameter space, more complex chaotic behavior and more ergodic output sequence than CML. Therefore, 2DMCPML is more suitable in cryptography than CML. Subsequently, we proposed a chaos-based random S-box design algorithm employed the spatial chaotic character of 2DMCPML to generate a large number of S-boxes. The cryptographic performance indicated that generated S-boxes can resist cryptanalysis attack well. Finally, four criteria bounds are set. The numbers of S-boxes satisfying these bounds generated by 2DMCPML and several 1D chaotic maps is calculated, respectively. The result showed that spatiotemporal chaos can generate more S-boxes with high cryptographic quality than low-dimensional chaos. This new discovery is significant to the development of some cryptographic researches such as dynamic S-box algorithm.

Keywords Spatiotemporal chaos · Low-dimensional chaos · S-box · Cryptography

P. Zhou · J. Du · K. Zhou · S. Wei (✉)
School of Physics, Northeast Normal University, Changchun 130024, China
e-mail: weisf116@nenu.edu.cn

P. Zhou
e-mail: zhoupz1996@163.com

1 Introduction

Substitution box (S-box) is important nonlinear module in the design architecture of block ciphers which is used to confuse the relationship between cipher-text and secret key. In mathematical perspective, S-box can be regard as vectorial Boolean functions. S-box structures are generally based on mathematical structures and random methods. It is necessary to design a large number of robust S-boxes. The security of block ciphers is directly related to its S-boxes while the data encryption standard (DES) is the best example. There are 8 S-boxes in DES algorithm. Matsui pointed out that some S-boxes of DES have weak nonlinear characteristics, and proposed the linear cryptanalysis which trying to obtain the linear approximation of these S-boxes. Based on this method, Matsui

successfully break the full 16-round of DES cipher with 2^{47} known-plaintexts [1]. Afterward, differential attack to DES-like cipher is presented by Biham and Shamir [2]. The appearance of linear cryptanalysis and differential cryptanalysis require S-box contain good nonlinearity and differential uniformity. As a result, advanced encryption standard (AES) has been developed to replace DES [3]. Inversion mapping are used in AES S-boxes design which ensure constructed S-boxes have abilities to resist both linear and differential attacks. In terms of comprehensive performance, AES S-box structure is the best S-box structure that can be designed on GF (2^8). Particularly, differential probability and BIC-nonlinearity of AES S-box are the best in existing S-box structures, and the nonlinearity is almost best. Due to these excellent cryptography characteristics, AES S-box structure has stood the test in commercial practice for many years. However, the algebraic cryptanalysis [4] and side-channel cryptanalysis [5] researches developed recently showed that S-box base on algebraic structure remained weakness. The security of AES may also be challenged. For that reason, many researchers are working on new methods as an alternative to algebraic structures. Lately, many random methods are proposed to design S-box and chaotic systems are usually chosen to be randomness sources of these methods. Açikkapi et al. implemented side-channel attacks to AES algorithm before and after replacing the standard AES S-box to a best or worst chaotic S-box which presented in the last decade, found that the chaos-based random S-box have better performance than AES S-box in side-channel attacks resisting [6]. Therefore, chaotic S-box may be a good alternative choice to AES S-box structures especially in side-channel attacks prevention.

In the early days, discrete-time chaos was first used in S-box construction [7]. Since then, S-box design by different discrete chaos was proposed [8–13].After Özkaynak and Özer proposed a method base on Lorenz system [14], S-box construction methods based on continuous-time chaotic systems began to appear [15–17]. Some chaotic systems with more complex dynamic behaviors were used to S-box design to improve cryptography performance. Various S-box structures were presented based on time delay [18], fractional [19–21] and hyperchaotic systems [22, 23]. In order to obtain S-box structures with best performance criterion, researchers have combined chaotic systems with optimization algorithm [24–28]. Many approaches combined chaotic systems with mathematical structures which play a more important role than chaos were proposed [29–35].

Moreover, a universal method based on modulo operation to generate S-boxes for all chaotic maps was proposed in [36], in addition to suggest the standard of chaos-based S-box structure with best cryptographic properties. In order to analyze the role of chaotic system used in the S-box design process on S-box performance criteria, Özkaynak in [37] showed that strong S-box structures can be designed by the S-box design approach with modulo operation used in [36], using entropy source that do not display chaotic behavior. Which indicate that modulo operation play a more important role than entropy source in this case. Lately, the effects of pre and post some implements on design criteria were analyzed in [38, 39]. In [40], not only a successful design work be done, but also the effect of fixed point and reverse fixed point on cryptanalysis process was considered.

It has been proved that high-dimensional chaotic system has some advantages than low-dimensional chaotic map system, such as larger parameter range, more complex behavior and longer period [41]. For that reason, high-dimensional chaotic system is considered to be better choice in many cryptographic studies like image encryption and PRNG. On the other hand, there are few researches about the high-dimensional chaotic system, especially spatiotemporal chaotic system, in random S-box design. Therefore, it is necessary to investigate the performance of high-dimensional chaotic system in S-box generation compared with low-dimensional chaotic system. In this paper, spatiotemporal chaos was taken as a representation of high-dimensional chaotic system to investigate the above issue.

The coupled map lattice (CML) is a classical spatiotemporal chaos has been deeply studied and widely applied [42–45] in cryptography. Its adjacent couplings can describe by the following equation:

$$X_{n+1}(i) = (1-\varepsilon)f[X_n(i)] + \frac{\varepsilon}{2}\{f[X_n(i-1)] + f[X_n(i+1)]\}; \quad (1)$$

where $i = 1, 2, \ldots, L$ is the lattice index, n is the time index, $0 < \varepsilon < 1$ is the coupling coefficient, $f(X_n) = \omega X_n(1 - X_n)$, $(3.569946 \leq \omega \leq 4)$ is logistic map. The periodic boundary condition $X_n(0) = X_n$

(L) has been used in this system. But due to the periodic windows of CML, parameter u should be carefully selected. In recent years, many spatiotemporal chaos based on new coupling methods have been proposed to avoid the high correlation effect between adjacent lattices. Chen et al. investigated a novel spatiotemporal chaos which connections are rewired randomly with varying probability P and rewiring period T [46]. But the spatial connection pattern of this spatial random coupling method cannot be reproduced in same parameters, which limited its application in cryptography. Another direction is nonlinear coupling method. In [47], a novel dynamics base on nonlinear coupling method named Arnold coupled logistic map lattice (ACLML) was presented. Subsequently, a mixed linear–nonlinear coupled map lattices (MLNCML) was suggested in [48]. The nonlinear coupling method replaced the adjacent coupling with non-adjacent coupling, but the system base on it still retained property that one lattice is limited by another two fixed lattices in every iteration.

In other to avoid above disadvantages, we investigated a new spatiotemporal system with pseudo-random coupling strategy that we called 2DMCPML. The three coupling lattices selected by a novel 2D pseudo-random mixed coupling method, when two of them are neighbor lattices, and the last one decided by the pseudo-random sequence value of local lattice. The used of 2D pseudo-random mixed coupling method has following advantages: (1) make the dynamics behavior of local map more complex. (2) Accelerate the whole system into full spatial chaos. (3) Increase the number of coupling parameters. (4) Reduce the correlation effects of adjacent lattices, since every iterations are effected by a different lattice in random position. The local maps of many spatiotemporal chaos are classical Logistic map. The simple 1D map like Logistic map and Sin map has been proved that contain many disadvantages: blank windows, weak parameter space, low orbit complexity and uneven distribution of output chaotic sequence. Therefore, we designed a new 1D chaotic map named PS map to replace simple 1D map for local map. The PS map is constructed by PWLCM and Sin map base on nonlinear combination structure in [49]. Numerical simulation of PS map showed that it is more suitable for local map of spatiotemporal chaos than simple 1D map. Subsequently, we analyzed the dynamic properties of 2DMCPML. The experimental results of bifurcation diagrams, Kolmogorov–Sinai entropy density and spatiotemporal chaotic diagrams showed that 2DMCPML has advantages of larger parameter space, more complex chaotic behavior and more ergodic output sequence than CML. These new features ensure 2DMCPML more suitable in cryptography than CML. Moreover, the evolution of spatiotemporal chaotic diagrams from CML to 2DMCLML and then to 2DMCPML demonstrated the enhancement of chaotic behaviors which PS map and 2D mixed coupling method provided.

The purpose of our work is not only to present a new spatiotemporal system but also to investigate the availability of 2DMCPML in the generation of random S-box and the advantages of spatiotemporal system to low-dimensional chaos in S-box generation. Thus, we employed the spatial chaotic character of 2DMCPML to construct 1000 random S-boxes. The cryptographic performance of constructed S-boxes are tested. An example S-box with good cryptographic performance was selected to compare with the some representative S-box structures. Finally, four criteria bounds were set in this paper. The number of S-boxes satisfying these bounds generated by 2DMCPML and several 1D chaotic maps is calculated, respectively. The result showed that spatiotemporal chaos can generate more S-boxes with high cryptographic quality than low-dimensional chaos. This discovery may have important effect to the development of some cryptographic researches such as dynamic S-box algorithm.

The rest paper is organized in following way. In Sect. 2, the 1D PS map is presented. The 2D Mixed pseudo-random Coupling PS Map Lattices is proposed in Sect. 3. In Sect. 4, the details of S-box construction method based on 2DMCPML is given. The cryptographic performance of S-boxes constructed by 2DMCPML are analyzed in Sect. 5. In Sect. 6, the example S-box of our work is compared with some representative S-box structures, in addition, the advantage of spatiotemporal chaos to low-dimensional chaos in S-boxes generation is investigated. At last, a conclusion is drawn in Sect. 7.

2 The 1D PS map

Since the chaotic behavior of spatiotemporal chaos is mainly determined by local map, the local map should

be selected carefully. Combining PWLCM map and Sin map, a new 1D PS map was proposed for the local map of 2DMCPML in this section.

The 1D PWLCM is a generalized form of tent map. It can describe by following function:

$$X_{n+1} = F_p(X_n) = \begin{cases} X_n/p, & 0 \le X_n < p, \\ (X_n/p)/(0.5-p), & p \le X_n < 0.5, \\ F_p(1-X_n), & 0.5 \le X_n \le 1; \end{cases} \quad (2)$$

where the parameter p should be selected from (0,0.5), and the status value X_n is in the range of [0,1]. The PWLCM is chaotic when $p \in (0,0.5)$.

The Sin map is a well-known 1D chaos. It is widely used in study of cryptography. The Sin chaotic function is

$$X_{n+1} = \mu \sin(\pi X_n)/4; \quad (3)$$

where the parameter μ is in the interval (0,4], and the status value X_n is in the interval [0,1]. Sin map has chaotic behaviors, when $\mu \in [3.569946, 4]$.

The simple 1D map like PWLCM, Logistic and Sin map share some common disadvantages: blank windows, weak parameter space, low orbit complexity and uneven output sequences distribution. These problems limit their application in cryptography. Base on a modulo operation [49], we obtain the PWLCM-Sin map. The parameters of both seed maps are unified for convenience. The mathematical expression of PS map is

$$X_{n+1} = F_\omega(X_n) = \begin{cases} ((4-\omega)\sin(\pi X_n)/4 + 8X_n/\omega) \bmod 1, & 0 \le X_n < 0.125\omega, \\ ((4-\omega)\sin(\pi X_n)/4 + (X_n - 0.125\omega)/(0.5 - 0.125\omega)) \bmod 1, & 0.125\omega \le X_n < 0.5, \\ F_\omega(1-X_n), & 0.5 \le X_n \le 1; \end{cases} \quad (4)$$

where the parameter ω is in the interval (0,4), the status value X_n also interval in [0,1]. The PS map has a more complex structure than a simple 1D map, which indicates that it may has more complex chaotic orbits. In order to get the quantified performance of PS map, Lyapunov exponent, bifurcation and distribution of output sequences are tested. Figure 1a shows that the Lyapunov exponents of PS system are positive in whole parameter space and significantly bigger than simple 1D map. Therefore, PS map has more complex orbits and chaotic sequences than simple 1D map. The bifurcation diagram of PS map is shown in Fig. 1b. It is clear that no blank windows and short-period phenomenon in appear the bifurcation which indicated PS map has a much larger available parameter space than simple 1D map. Figure 1c shows the relatively uniform output distribution of PS map. Above new features ensure PS map is suitable for cryptography.

3 The proposed 2DMCPML system

Extending the spatial dimension to two-dimension, mixing the pseudo-random coupling component with adjacent coupling component, using PS map as local map, we proposed a novel spatiotemporal chaotic model 2DMCPML. It can describe by the following equation:

$$X_{n+1}(i,j) = (1-\varepsilon) f[X_n(i,j)] + \frac{\varepsilon}{2}(1-\sigma) \{f[X_n(i+1,j)] + f[X_n(i,j-1)]\} + \varepsilon\sigma f[X_n(a,b)]; \quad (5)$$

where i, j, a, b are lattice indexes, n is time index. ε and σ are coupling coefficients in the range of [0,1]. $X_n(i, j)$ is the state of local map in lattice (i, j) and the local dynamics $f(X)$ define as PS map. The periodic boundary conditions $X_n(i + L, j) = X_n(i, j)$ and $X_n(i, j + L) = X_n(i, j)$ are used in 2DMCPML.

The coupling relationship in Eq. (5) is portrayed in Fig. 2. For any lattice (i, j), the state $X_{n+1}(i, j)$ is influenced by following elements: (1) itself $X_n(i, j)$, (2) adjacent lattice from two directions $X_n(i + 1, j)$ and $X_n(i, j - 1)$, (3) non-adjacent lattice with random position $X_n(a, b)$. Here, the value of a and b decided by the $X_n(i, j)$ state value. Combining the first and second place in the decimal part of $X_n(i, j)$ to get a two-digit

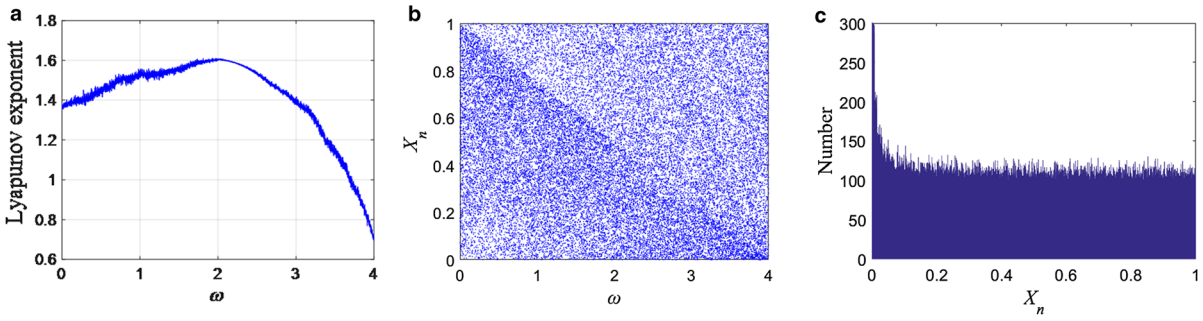

Fig. 1 The simulation of PS map. **a** Lyapunov exponents, **b** bifurcation diagram, **c** output distribution

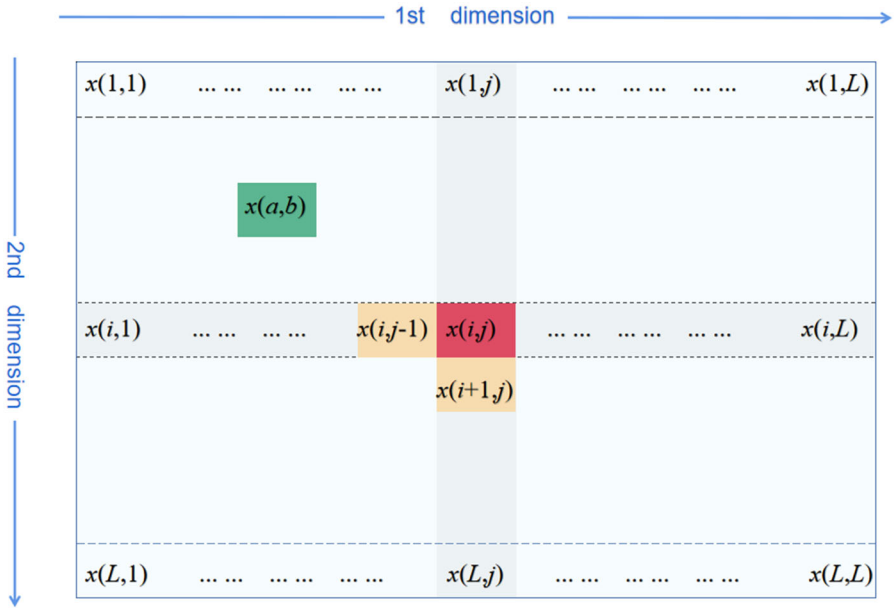

Fig. 2 The coupling relationship of 2DMCPML

number, mod this number with L then plus 1, one can get a. Similarly, combining the third and fourth place in the decimal part of $X_n(i, j)$ to get another two-digit number, mod this number with L then plus 1, one can get b. For example, if $X_n(i, j) = 0.40967142$ and $L = 16$, the two-digit number is 40 and 96, respectively, so $a = (40 \bmod 16) + 1 = 9$ and $b = (96 \bmod 16) + 1 = 1$.

For practicality and comparison purpose, CML assign $L = 256$, 2DMCPML assign $L = 16$. Here considered the spatiotemporal system under relatively weak coupling condition. The Bifurcation diagrams of CML and 2DMCPML with fixed ε are drawn in Fig. 3 to demonstrate the chaotic behavior in time dimension. Figure 3a–c indicate the bifurcations of CML with $\varepsilon = 0.1$, 0.3 and 0.5, respectively, when $\omega \in [3, 4]$. Obviously, CML keeps some characters occur in Logistic map like forking behavior, blank Window and short periods which limits its application in cryptography.

The bifurcation diagrams of 2DMCPML with $\varepsilon = 0.1$, 0.3 and 0.5 where $\sigma = 0.5$ are shown in Fig. 3d–f, respectively. There are no forking behavior and blank window in these figures which is a new feature. Meanwhile the state values of 2DMCPML are distributed almost in entire space of [0,1]. The explanation of the difference in bifurcation is that the new PS map has better chaotic dynamics than logistic map and the 2D pseudo-random mixed coupling increases the instability of potential periodic orbits. CML systems are generally considered more suitable for cryptographic applications than ordinary

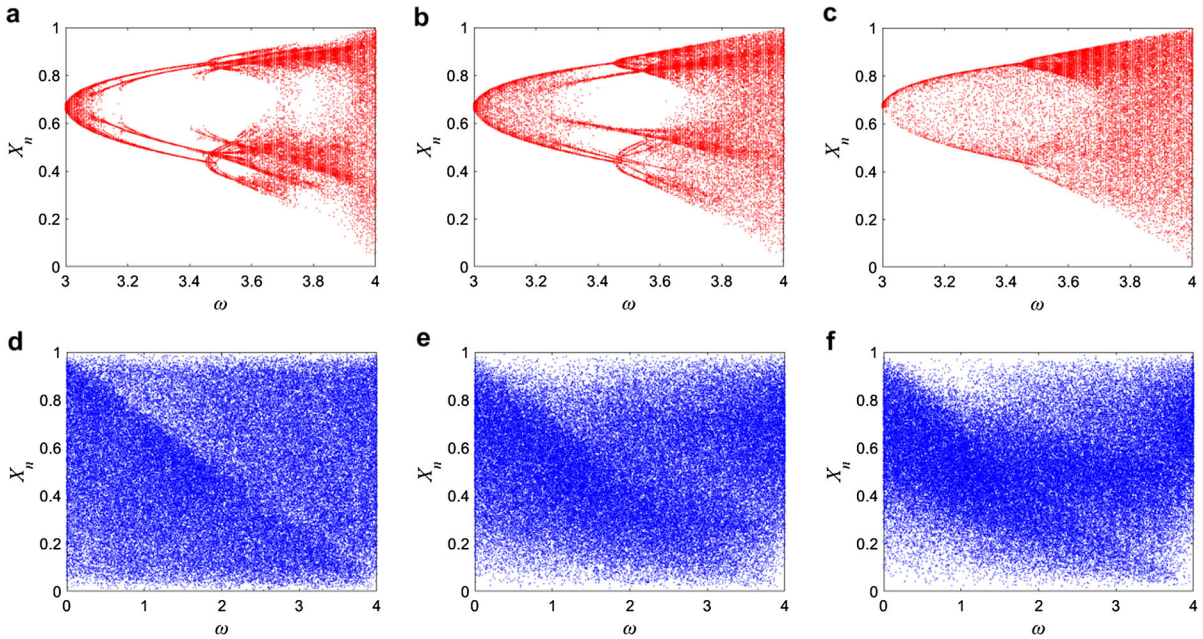

Fig. 3 The bifurcation diagrams of spatiotemporal chaos. **a** CML with $\varepsilon = 0.1$, **b** CML with $\varepsilon = 0.3$, **c** CML with $\varepsilon = 0.5$, **d** 2DMCPML with $\varepsilon = 0.1$, **e** 2DMCPML with $\varepsilon = 0.3$, **f** 2DMCPML with $\varepsilon = 0.5$

low-dimensional maps for its less blank window. Similarly, 2DMCPML is more suitable for cryptographic applications than CML.

Lyapunov exponent measure the divergence of nearby orbits and provide a qualitative view to dynamic behavior of system. Generally, the larger Lyapunov exponent is, the more complex chaotic dynamical behavior is. The proposed spatiotemporal chaos 2DMCLML can be considered as L^2 dimensions dynamics. Kolmogorov–Sinai (KS) entropy density is usually used to measure the chaotic property of multi-dimensions dynamics which is the average of all positive Lyapunov exponents [50].

The KS entropy density for different ε and ω of 2DMCLML and CML systems are shown in Fig. 4a, b, respectively. It is apparent that the KS entropy densities of CML are within [0, 0.5] in Fig. 4a while KS entropy densities of 2DMCPML are mostly higher than 0.5 in Fig. 4b. The proposed 2DMCPML have higher KS entropy densities than CML in almost entire parameter space. This characteristic indicates that 2DMCPML contains more intensive and extensive chaotic behaviors.

In order to analyze global chaotic properties of proposed system, the spatiotemporal chaotic diagrams with fixed local parameter and coupling strength is investigated. All spatiotemporal systems here consist of 256 lattices and iterate 500 times. Figure 5a illustrates the spatiotemporal chaotic diagrams of CML with $\omega = 3.9$, $\varepsilon = 0.1$. As iteration progress, state values tend to converge slightly. The state values distribution is in small range and uneven.

The spatiotemporal chaotic diagrams of 2D Mixed pseudo-random Coupling Logistic Map Lattices (2DMCLML) with $\omega = 3.9$, $\varepsilon = 0.1$ and $\sigma = 0.5$ is drawn in Fig. 5b. Comparing Fig. 5a with Fig. 5b, it is clear that 2DMCLML have lager scope and more uniform distribution of state values. Bearing in mind that 2DMCLML and CML use a same local dynamics Logistic map, the only explanation of this difference is that the 2D Mixed pseudo-random Coupling method indeed benefit system chaotic property. Therefore, 2D Mixed pseudo-random Coupling method is more suitable in cryptography than adjacent coupling method.

Figure 5c shows the spatiotemporal chaotic diagrams of 2DMCPML with $\omega = 3.9$, $\varepsilon = 0.1$ and $\sigma = 0.5$. Comparing Fig. 5b, c, one can found that the 2DMCPML have lager range and more uniform distribution of state values than 2DMCLML after replacing the local Logistic map with PS map. This

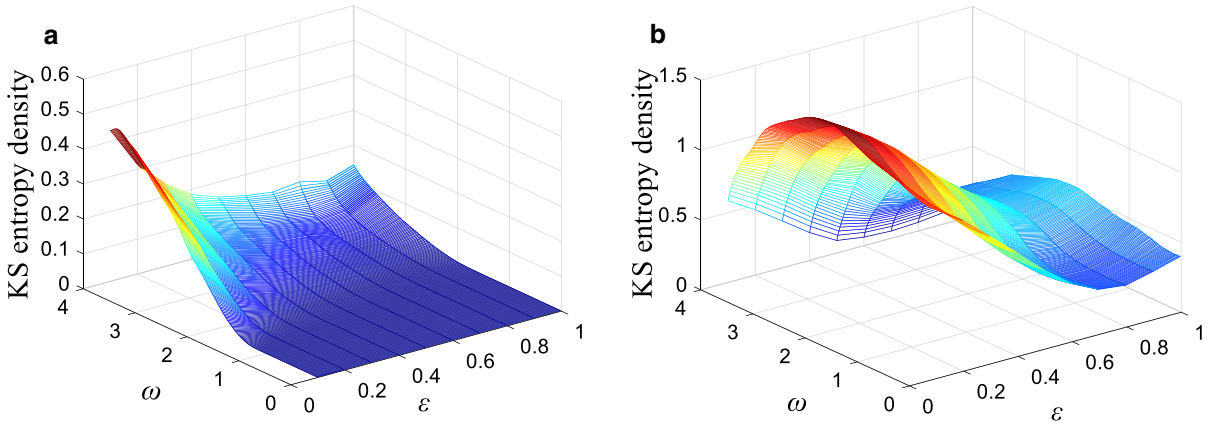

Fig. 4 The KS entropy density for different ε and ω of spatiotemporal chaos. **a** CML, **b** 2DMCLML

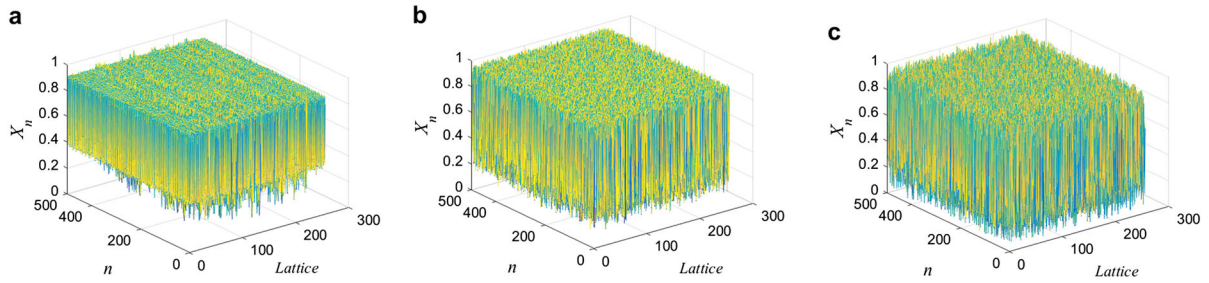

Fig. 5 The spatiotemporal chaotic diagrams of spatiotemporal chaos. **a** CML with $\omega = 3.9$, $\varepsilon = 0.1$, **b** 2DMCLML with $\omega = 3.9$, $\varepsilon = 0.1$ and $\sigma = 0.5$, **c** 2DMCPML with $\omega = 3.9$, $\varepsilon = 0.1$ and $\sigma = 0.5$

new feature suggested again that PS map is a better choice for local map than Logistic map.

Above analysis indicated that 2DMCPML has advantages of large parameter space, more complex chaotic behavior and more ergodic output sequence than most chaotic system in terms of practical usability. According to the IEEE floating point standard, the computational precision of 64-bit double precision number is about 10^{16} [51]. In case of ω, ε and σ are chosen to be key, the key space of 2DMCPML is close to $4 \times 10^{48} \approx 2^{161}$which is a great number.

4 S-box construction method based on 2DMCPML

In this section, random S-box generation method using spatial chaotic property of 2DMCPML is provided which can construct robust S-box without significantly increase computation. In order to obtain $n \times n$ S-box, the size of 2DMCPML is set to $L = 2^{n/2}$. Here take $n = 8$ for example. The detailed algorithm is described as follows:

Step 1: Determine the coupling parameters ε and σ, as well as the local map parameter ω. Set the initial values for all lattices of 2DMCPML that the initial values are not all the same.

Step 2: Iterate the spatiotemporal system 2DMCPML for k times to go into chaotic, where $k > 200$.

Step 3: Define a one-dimensional empty sequence with 256 elements: $S = [S(0), S(1),\ldots S(255)]$. Save the lattices state value of 2DMCPML into S, row by row, starting from the first row, like this: $S = [S(0) = X(1,1),\ldots, S(15) = X(1,16),\ldots, S(240) = X(16,1), \ldots, S(255) = X(16,16)]$.

Step 4: Reorder all elements in S by ascending order of their values. The element with larger index put on the left, if values of two elements are equal. Translate the index of S to a 8×8 table, i.e.,

obtains an S-box. Afterward, iterate 2DMCPML one time to prepare for constructing next S-box.

Repeat the Steps 3–4, one can generate S-boxes as many as desired.

There are total $256! \approx 2^{1684}$ different bijective S-boxes on GF (2^8). The number of different bijective S-boxes indicated that there is a great space for exploration in the research of constructing 8×8 S-box. The proposed method used lots of long period orbits of spatiotemporal chaos to generate large numbers of S-boxes.

5 S-box performance analyze

Generating 1000 8×8 S-boxes by the method of last section with $\varepsilon = 0.1$, $\sigma = 0.5$, and $\omega = 2.1$. Five basic requirements are used to evaluate the performance of the constructed S-boxes. Including bijective property, nonlinearity, strict avalanche criterion (SAC), outputs bit independence criterion (BIC) and equiprobable input/output XOR distribution. These criteria are widely used to assess S-box.

A Boolean function f_i is bijective if it satisfies the following equation:

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

where $a_i \in \{0,1\}$, $(a_1, a_2, \ldots, a_n) \neq (0, 0, \ldots, 0)$ and wt() is the hamming weight. The proposed method in last section guarantees each element in the S-box are unique number between 0 and 255, so that each Boolean function satisfies Eq. (6), and all constructed S-boxes are bijective.

The nonlinearity measures the hamming distance between N-bit Boolean function and N-bit affine function [52]. If the nonlinearity of Boolean function is low, its linear approximation is easy to obtain and the S-box cryptographic performance is weak. For the convenience of calculation, the nonlinearity value of n-bit Boolean function $f(x)$ is usually represented by the following formula:

$$N_f = 2^{n-1}\left(1 - 2^{-n} \max_{\omega \in \mathrm{GF}(2^n)} \left|S_{(f)}(\omega)\right|\right); \tag{7}$$

where $S_{(f)}(w)$ is the Walsh spectrum of $f(x)$, it can describe by the following equation:

$$S_{(f)}(\omega) = \sum_{x \in \mathrm{GF}(2^n)} (-1)^{f(x) \oplus x \cdot \omega}; \tag{8}$$

where $\omega \in \mathrm{GF}(2^n)$, and $x \cdot w$ denotes the dot product of x with w.

Here, we measure the nonlinearity property of S-box structure by the average nonlinearity values of N-bit Boolean function. Although, in recent study [53], the author claimed that this measurement was incorrect because it consider the average nonlinearity of N-bit Boolean function only, ignoring the rest of the linear combinations of N-bit Boolean function in the process. He suggested that the nonlinearity property should be measured as the minimum nonlinearity value of all linear combinations of N-bit Boolean function. However, whether the rest of linear combinations of N-bit Boolean function (such as $f_1 \oplus f_3 \oplus f_4 \oplus f_6$) can be used in linear cryptanalysis is a question without certain answer at present. Thus, the measurement here is still correct.

Figure 6 shows the average nonlinearity values of S-boxes constructed by 2DMCPML. The lower bound of average nonlinearity values is 100, S-box with very poor nonlinearity property did not appear. The best and mean values of average nonlinearity are 107 and 103.54, respectively. Therefore, constructed S-boxes have good nonlinear properties.

Webster and Tavares proposed strict avalanche criterion (SAC) combining completeness and the avalanche effect [54]. An S-box satisfies the strict avalanche criterion, which means each output bit will change with a probability of 0.5, if changing one bit of the input. Constructing dependence matrix is usually used to verify SAC, and the optimum value is 0.5. The average value of dependence matrix and average offset of dependence matrix elements from 0.5 are both ordinarily used to measure SAC.

Figure 7 shows the average values of dependence matrix of S-boxes constructed by 2DMCPML. Constructed S-boxes have close property to SAC since all values are within the interval [0.485, 0.52].

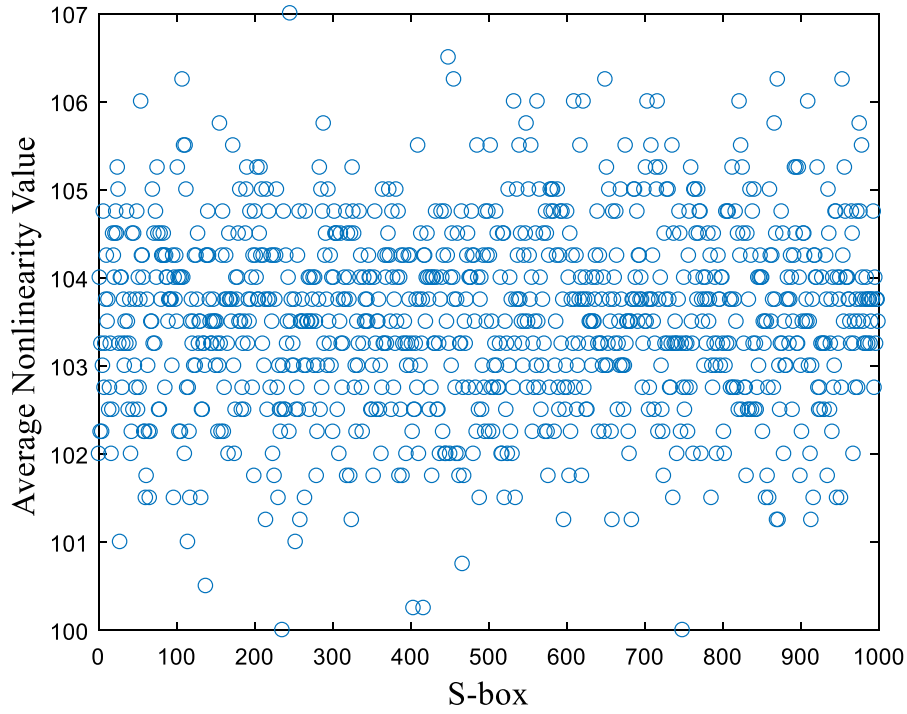

Fig. 6 Average nonlinearity values of S-boxes constructed by 2DMCPML

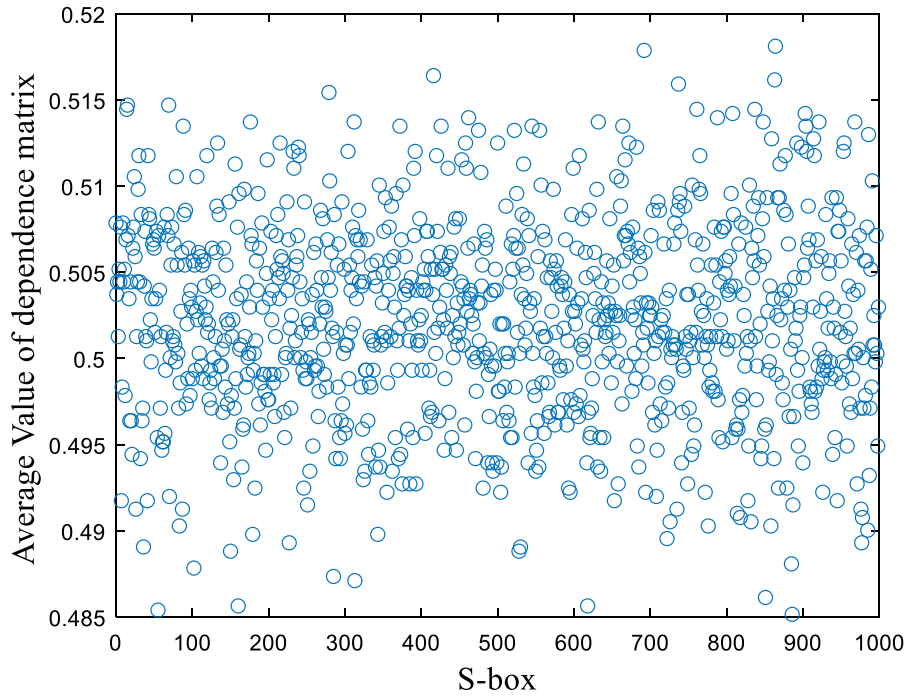

Fig. 7 Average values of dependence matrix of S-boxes constructed by 2DMCPML

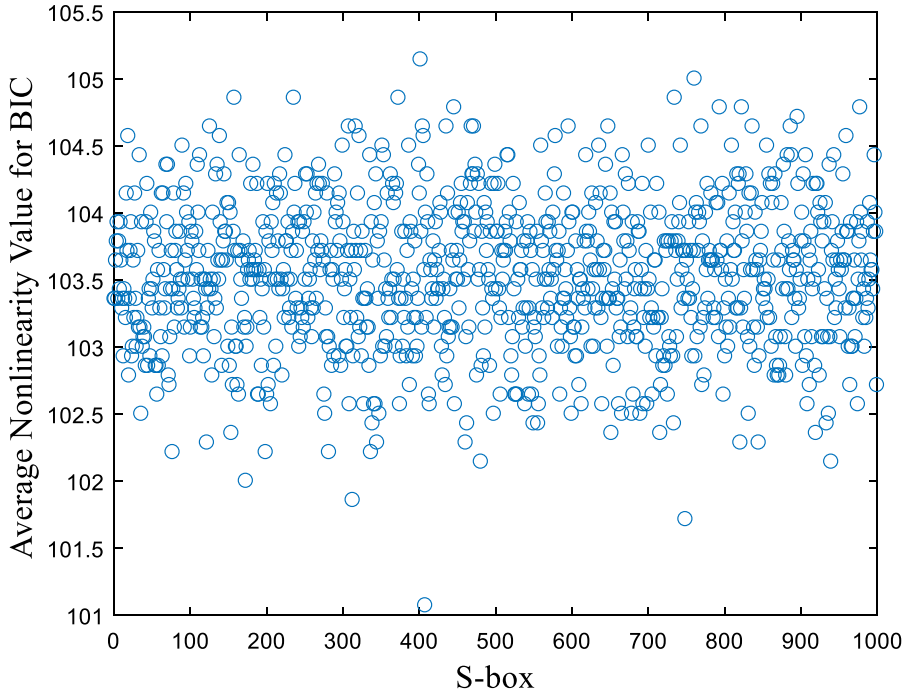

Fig. 8 Average nonlinearity values for BIC of s-boxes constructed by 2DMCPML

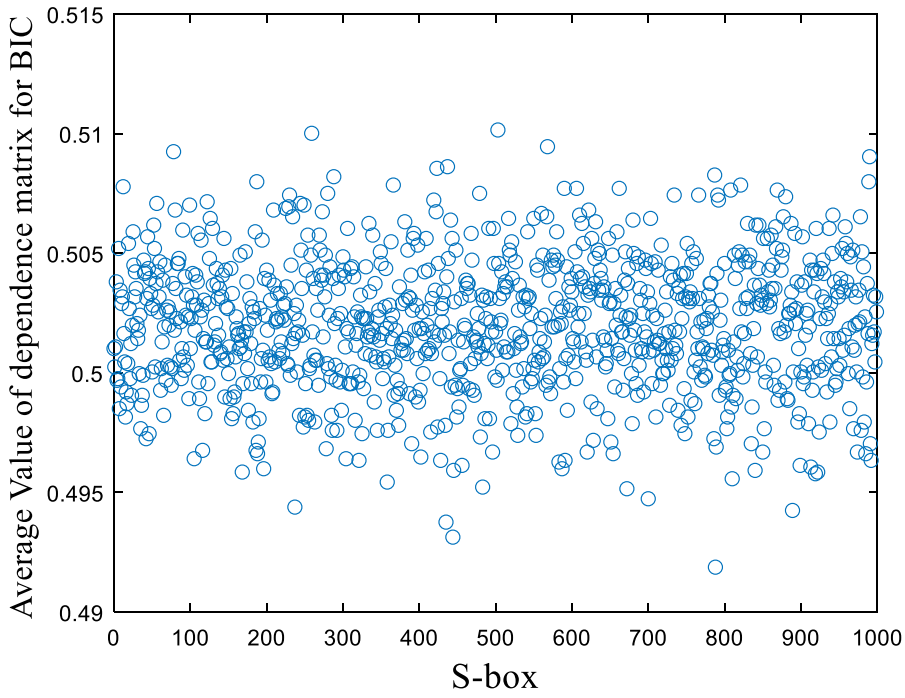

Fig. 9 Average values of dependence matrix for BIC of s-boxes constructed by 2DMCPML

The outputs bit independence criterion (BIC) is another essential analysis criterion for the design of S-box. In this paper, the measurement proposed by Adams and Tavares is used to test the BIC of S-box which analyzes the effect of the two previous criteria on the output bits [55]. The 8 Boolean functions of 8 × 8 S-box are denoted as $f_1, f_2, \ldots, f_8$. If $f_v \oplus f_w$ has high nonlinearity property and is quite close to SAC

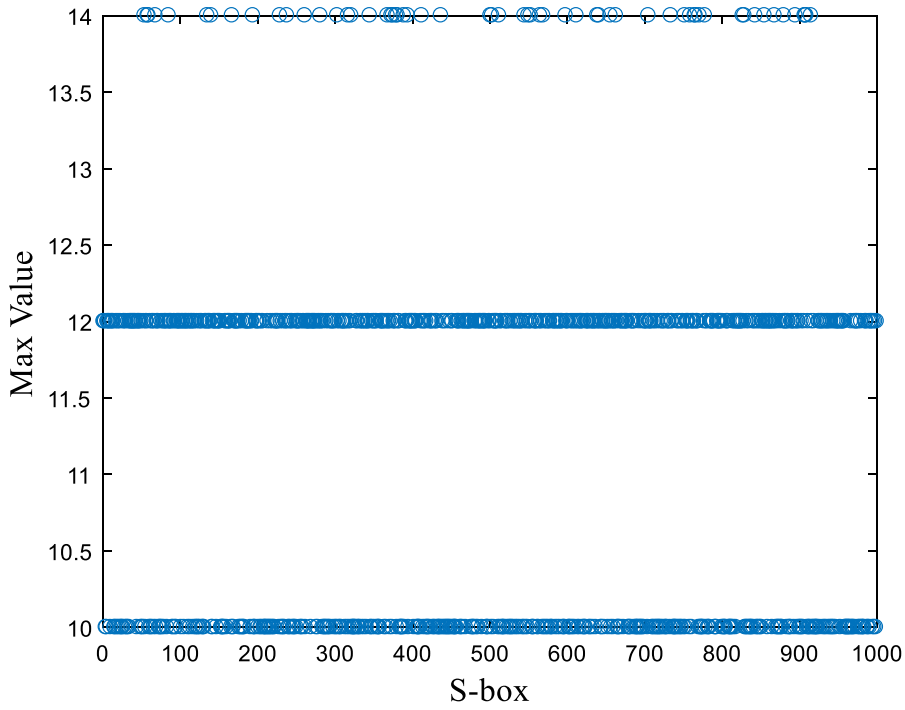

Fig. 10 Max values of equiprobable input/output XOR distribution table of S-boxes constructed by 2DMCPML

for any v and w ($v, w \in \{1, 2, \ldots, 8\}$, and $v \neq w$), we can believe that every pair of output bits have a very small correlation and the S-box has a good BIC property.

The average values of nonlinearity and dependence matrix of $f_v \oplus f_w$ are shown in Figs. 8 and 9, respectively. In terms of nonlinearity, the Average nonlinearity values for BIC is greater than 101. In terms of SAC, the Average values of dependence matrix for BIC is very close to 0.5. Therefore, constructed S-boxes have good BIC property.

The last measurement is equiprobable input/output XOR distribution which also known as maximum expected differential probability (MEDP) [2]. It is directly related to differential cryptanalysis. The maximum value in the input/output XOR distribution table should be as small as possible. Differential probability for a given function f can be calculated by:

$$\mathrm{DP}_f = \max_{\Delta x \neq 0, \Delta y} (\#\{x \in X | f(x) \oplus f(x \oplus \Delta x) = \Delta y\}); \tag{9}$$

where X is the set of all possible input values.

Figure 10 displays the max values of equiprobable input/output XOR distribution table of S-boxes constructed by 2DMCPML. The max values mostly concentrate in 10 and 12; meanwhile all max values are not greater than 14. This result indicated that constructed s-boxes can resist differential attacks well.

Above simulation results shows that the 1000 S-boxes generated by 2DMCPML have good overall cryptography performance and without very weak S-box. This is a good property to dynamic S-box algorithms. Moreover, the chaotic system 2DMCPML of proposed method has a big parameter space. These properties ensure the proposed method well suited for dynamic S-box algorithms.

6 Performance comparison

6.1 Example S-box comparison

An example S-box with good cryptographic performance of S-boxes generated by proposed method is selected and shown in Table 1. The nonlinearities of eight output bits of example S-box are 110, 104, 106, 106, 106, 108, 108, 108 and the average value is 107. The dependence matrix, nonlinearity of $f_v \oplus f_w$ and equiprobable input/output XOR distribution of example S-box are shown in Tables 2, 3 and 4, respectively.

The example S-box is compared with some representative S-box structures in Table 5. The results

Table 1 The example of S-box constructed by proposed method

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

Table 2 The dependence matrix of example S-box

0.453125	0.5	0.46875	0.5	0.515625	0.484375	0.5	0.5
0.4375	0.5	0.546875	0.53125	0.4375	0.5	0.515625	0.5
0.53125	0.546875	0.53125	0.46875	0.59375	0.5	0.484375	0.53125
0.53125	0.453125	0.578125	0.46875	0.453125	0.421875	0.484375	0.515625
0.453125	0.484375	0.546875	0.53125	0.515625	0.484375	0.484375	0.53125
0.546875	0.56250	0.515625	0.53125	0.421875	0.453125	0.453125	0.421875
0.46875	0.46875	0.515625	0.546875	0.484375	0.46875	0.5	0.546875
0.515625	0.515625	0.484375	0.53125	0.453125	0.484375	0.546875	0.5

Table 3 The nonlinearity for $f_v \oplus f_w$ of example S-box

–	106	104	100	102	102	106	108
106	–	106	100	102	102	104	102
104	106	–	104	104	102	108	106
100	100	104	–	102	104	102	102
102	102	104	102	–	104	104	100
102	102	102	104	104	–	100	106
106	104	108	102	104	100	–	100
108	102	106	102	100	106	100	–

showed that cryptographic performance of example S-box is stronger than most chaos-based random S-boxes but weaker than some S-box structures use mathematical structure or optimization algorithms.

6.2 Different chaos comparison

Four criteria bounds are set as following way. (1) Bound 1: NL $\geq$ 104, (2) Bound 2: NL $\geq$ 104 && |SAC-0.5| $\leq$ 0.005, (3) Bound 3: NL $\geq$ 104 && |SAC-0.5| $\leq$ 0.005 && |BIC_SAC| $\leq$ 0.005, (4) Bound 4: NL $\geq$ 104 && |SAC-0.5| $\leq$ 0.005 && |BIC_SAC| $\leq$ 0.005 && DP $\leq$ 10. Where NL is the average nonlinearity value of S-box, SAC is the average value of dependence matrix of S-box, BIC_SAC is the average value of dependence matrix of S-box output pair $f_v \oplus f_w$ and *DP* is the max values of equiprobable input/output XOR distribution table of S-box.

For comparison purpose, we use the output chaotic sequence of three different one-dimensional chaos: Logistic map, Sin map and PS map to generate 1000 8×8 random S-boxes, respectively. The numbers of S-boxes satisfying above four bounds generated by 2DMCPML and three different 1D chaos is calculated. The result is shown in Table 6. It is clear that the numbers of S-boxes satisfying the four bounds generated by 2DMCPML are all more than three 1D chaotic maps which mean the spatiotemporal chaos

Table 4 Equiprobable input/output XOR distribution table of example S-box

8	6	6	10	10	6	8	8	6	6	6	8	6	6	6	8
6	8	8	8	6	6	6	6	8	8	8	6	6	4	6	6
6	6	6	6	6	8	6	4	6	8	6	8	6	6	6	8
8	6	6	6	8	8	8	6	6	6	6	6	4	8	6	6
10	6	8	8	8	6	6	8	6	10	6	8	8	6	8	6
4	6	6	8	6	6	6	8	6	6	8	6	6	6	6	8
8	6	8	6	6	6	8	8	4	8	6	6	6	6	6	6
6	6	6	8	8	6	6	6	6	8	8	8	6	6	8	8
6	8	6	8	8	6	6	6	6	10	8	10	6	6	6	6
6	8	6	8	8	6	6	6	6	8	6	6	4	6	6	6
6	6	8	8	6	6	6	6	8	6	6	8	8	6	8	6
8	6	6	6	6	6	6	6	8	6	6	6	8	6	6	8
8	8	6	6	6	6	6	6	6	6	8	6	6	6	6	6
6	6	8	8	8	8	8	8	6	6	6	6	8	8	8	6
6	6	6	6	6	8	6	8	6	6	6	10	6	8	6	8
8	6	6	6	8	8	10	8	6	8	8	8	6	6	8	–

Table 5 Comparison of example S-box and different S-box structures

S-box	Nonlinearity			Max.XOR	SAC		Min. BIC-nonlinearity	BIC-SAC
	Avg	Min	Max		Avg	Offset		
Proposed	107	104	110	10	0.4993	0.0310	100	0.5050
AES	112	112	112	4	0.5049	0.0264	112	0.4984
Chaos-based random method								
Ref. [10]	106.7	106	108	10	0.5034	0.0244	100	0.4951
Ref. [20]	104.7	100	108	10	0.4982	0.0380	96	0.4942
Ref. [8]	109.2	108	112	8	0.5012	0.0295	104	0.5056
Ref. [11]	106.5	106	108	10	0.5010	0.0288	100	0.5045
Ref. [12]	106.2	104	110	10	0.5029	0.0332	96	0.5070
S-box 1 [37]	105.2	102	108	10	0.5037	0.0364	94	0.4994
S-box 1 [36]	106.7	106	108	10	0.4941	0.0327	98	0.4957
Ref. [42]	105.2	104	108	10	0.5056	0.0291	98	0.4954
Ref. [13]	105	98	108	10	0.5061	0.0398	94	0.5038
Chaos-assisted optimization method								
Ref. [25]	110.2	110	112	10	0.5000	0.0283	104	0.5052
Ref. [26]	103.2	98	106	12	0.4995	0.0400	100	0.5037
Ref. [27]	107.5	106	108	10	0.4943	0.0369	98	0.4982
S-box 1 [28]	109.5	106	112	8	0.5068	0.0347	102	0.5045
Chaos-assisted mathematical structure method								
Ref. [30]	105.5	100	110	32	0.5022	0.0310	102	0.4990
S-box 5 [34]	112	112	112	4	0.5049	0.0264	112	0.5046
Ref. [35]	114	112	116	12	0.4978	0.0227	98	0.4979
Scheme 1 [38]	112	112	112	4	0.5051	0.0266	112	0.5044

Table 6 The numbers of S-boxes satisfying one of four bounds generated by 2DMCPML and different 1D chaos

	Bound 1	Bound 2	Bound 3	Bound 4
Sin	334	269	151	40
Logistic	346	274	154	42
PS	355	292	163	50
2DMCPML	399	337	195	81

can indeed generate more S-boxes with strong cryptographic feature. This new discovery is significant to the development of some cryptographic researches such as dynamic S-box algorithm.

7 Conclusion

In this paper, firstly, we design a new 1D PS map which derived from PWLCM and Sin map by modulo operation. Experimental results show that PS map overcomes many shortcomings such as blank windows, weak parameter space and bad ergodicity which widely occur in simple 1D map. Since the chaotic behavior of spatiotemporal chaos is mainly determined by its local map, the PS map is more suitable for local map of spatiotemporal dynamics. Secondly, with the novel 2D pseudo-random mixed coupling method we present a spatiotemporal chaos used PS map as local map $f(x)$. The experimental results of bifurcation diagrams, Kolmogorov–Sinai entropy density and spatiotemporal chaotic diagrams showed that 2DMCPML has advantages of larger parameter space, more complex chaotic behavior and more ergodic output sequence than CML. Moreover, the evolutions of spatiotemporal chaotic diagrams from CML to 2DMCLML and then to 2DMCPML demonstrate the enhancement of chaotic behaviors which PS map and 2D mixed coupling method provided. Above new features ensure 2DMCPML more suitable in cryptography than CML. Subsequently, we employed the spatial chaotic character of 2DMCPML to generate a large number of S-boxes. The cryptographic performance indicated that generated S-boxes can resist cryptanalysis attack well. Finally, four criteria bounds are set. The numbers of S-boxes satisfying these bounds generated by 2DMCPML and three 1D chaotic maps is calculated, respectively. The result showed that spatiotemporal chaos can indeed generate more S-boxes with strong cryptographic features than low-dimensional chaos. This new discovery is significant to the development of some cryptographic researches such as dynamic S-box algorithm.

In terms of practical usability, the advantages and disadvantages of proposed method can be summarized as follow.

(1) Considering chaos-based random S-box has better performance in side-channel attacks resisting [6], S-box constructed by proposed method can be used as masks to prevent side-channel attacks of symmetric cryptography.
(2) The proposed method is well suited for dynamic S-box algorithms due to big parameter space and good overall S-box cryptography performance. Such as, the parameter space of proposed method is about 2^{161}, much greater than dynamic AES S-box algorithms such as [56], which has 256 different dynamic AES S-boxes.
(3) The large parameter space, more complex chaotic behavior and more ergodic output sequence of the entropy source 2DMCPML ensure it can well apply not only in S-box construction, but also in other cryptography like image encryption [48] and pseudo-random number generator [57].
(4) The comprehensive performance of example S-box is stronger than most chaos-based S-boxes but weaker than some S-box structures used mathematical structure or optimization algorithms, which means that example S-box is weaker than some S-box structures used mathematical structure or optimization algorithms in linear cryptanalysis or differential cryptanalysis resisting.

Funding This study was funded by the National Natural Science Foundation of Jilin Province (CN) (Grant Number: 20170101040JC).

Compliance with ethical standards

Conflict of interest The authors declare that they have no conflict of interest.

References

1. Matsui, M.: Linear cryptanalysis method for DES Cipher. In: Helleseth, T. (eds.) Advances in Cryptology—EUROCRYPT'93. Lecture Notes in Computer Science, pp. 386–397. Springer, Heidelberg (1994)

2. Biham, E., Shamir, A.: Differential cryptanalysis of DES-like cryptosystems. J. Cryptol. **4**, 3–72 (1991)
3. Daemen, J., Rijmen, V.: AES proposal: Rijndael. In: First Advanced Encryption Conference, California (1998)
4. Bard, G.V.: Algebraic Cryptanalysis. Springer, Boston (2009)
5. Guo, S., Zhao, X., Zhang, F., Wang, T., Shi, Z.J., Standaert, F., Ma, C.: Exploiting the incomplete diffusion feature: a specialized analytical side-channel attack against the AES and its application to microcontroller implementations. IEEE Trans. Inf. Forensics Secur. **9**, 999–1014 (2014)
6. Acikkapi, M.S., Ozkaynak, F., Ozer, A.B.: Side-channel analysis of chaos-based substitution box structures. IEEE Access **7**, 79030–79043 (2009)
7. Jakimoski, G., Kocarev, L.: Chaos and cryptography: block encryption ciphers based on chaotic maps. IEEE Trans. Circ. Syst. **I**(48), 163–169 (2001)
8. Lambić, D.: A novel method of S-box design based on chaotic map and composition method. Chaos, Solitons Fractals **58**, 16–21 (2014)
9. Belazi, A., Khan, M., El-Latif, A.A.A., Belghith, S.: Efficient cryptosystem approaches: S-boxes and permutation-substitution-based encryption. Nonlinear Dyn. **87**, 337–361 (2016)
10. Lambić, D.: A novel method of S-box design based on discrete chaotic map. Nonlinear Dyn. **87**, 2407–2413 (2017)
11. Lambić, D.: A new discrete-space chaotic map based on the multiplication of integer numbers and its application in S-box design. Nonlinear Dyn. **100**, 699–711 (2020)
12. Lu, Q., Zhu, C., Deng, X.: An efficient image encryption scheme based on the LSS chaotic map and single S-box. IEEE Access **8**, 25664–25678 (2020)
13. Özkaynak, F.: An analysis and generation toolbox for chaotic substitution boxes: a case study based on chaotic Labyrinth Rene Thomas system. Iran. J. Sci. Technol. Trans. Electr. Eng. **44**, 89–98 (2020)
14. Özkaynak, F., Özer, A.B.: A method for designing strong S-Boxes based on chaotic Lorenz system. Phys. Lett. A **374**, 3733–3738 (2010)
15. Khan, M., Shah, T., Mahmood, H., Gondal, M., Hussain, I.: A novel technique for the construction of strong S-boxes based on chaotic Lorenz systems. Nonlinear Dyn. **70**, 2303–2311 (2012)
16. Khan, M., Shah, T.: A construction of novel chaos base nonlinear component of block cipher. Nonlinear Dyn. **76**, 377–382 (2013)
17. Çavuşoğlu, Ü., Zengin, A., Pehlivan, I., Kaçar, S.: A novel approach for strong S-Box generation algorithm design based on chaotic scaled Zhongtang system. Nonlinear Dyn. **87**, 1081–1094 (2016)
18. Özkaynak, F., Yavuz, S.: Designing chaotic S-boxes based on time-delay chaotic system. Nonlinear Dyn. **74**, 551–557 (2013)
19. Khan, M., Shah, T.: An efficient construction of substitution box with fractional chaotic system. SIViP **9**, 1335–1338 (2013)
20. Özkaynak, F., Çelik, V., Özer, A.B.: A new S-box construction method based on the fractional-order chaotic Chen system. SIViP **11**, 659–664 (2016)
21. Belazi, A., Abd El-Latif, A.A., Diaconu, A., Rhouma, R., Belghith, S.: Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms. Opt. Lasers Eng. **88**, 37–50 (2017)
22. Liu, G., Yang, W., Liu, W., Dai, Y.: Designing S-boxes based on 3-D four-wing autonomous chaotic system. Nonlinear Dyn. **82**, 1867–1877 (2015)
23. Islam, F., Liu, G.: Designing S-box based on 4D-4Wing hyperchaotic system. 3D Res. (2017). https://doi.org/10.1007/s13319-017-0119-x
24. Chen, G.: A novel heuristic method for obtaining S-boxes. Chaos, Solitons Fractals **36**, 1028–1036 (2008)
25. Alzaidi, A.A., Ahmad, M., Doja, M.N., Solami, E.A., Beg, M.M.S.: A new 1D chaotic map and β-hill climbing for generating substitution-boxes. IEEE Access (2018). https://doi.org/10.1109/access.2018.2871557
26. Tanyildizi, E., Özkaynak, F.: A new chaotic S-box generation method using parameter optimization of one dimensional chaotic maps. IEEE Access **7**, 117829–117838 (2019)
27. Ahmed, H.A., Zolkipli, M.F., Ahmad, M.: A novel efficient substitution-box design based on firefly algorithm and discrete chaotic map. Neural Comput. Appl. **31**, 7201–7210 (2019)
28. Ahmad, M., Khaja, I.A., Baz, A., Alhakami, H., Alhakami, W.: Particle swarm optimization based highly nonlinear substitution-boxes generation for security applications. IEEE Access **8**, 116132–116147 (2020)
29. Hussain, I., Shah, T., Gondal, M.: A novel approach for designing substitution-boxes based on nonlinear chaotic algorithm. Nonlinear Dyn. **70**, 1791–1794 (2012)
30. Hussain, I., Shah, T., Mahmood, H., Gondal, M.A.: A projective general linear group based algorithm for the construction of substitution box for block ciphers. Neural Comput. Appl. **22**, 1085–1093 (2012)
31. Hussain, I., Shah, T., Gondal, M., Mahmood, H.: An efficient approach for the construction of LFT S-boxes using chaotic logistic map. Nonlinear Dyn. **71**, 133–140 (2012)
32. Hussain, I., Shah, T., Gondal, M.: Efficient method for designing chaotic S-boxes based on generalized Baker's map and TDERC chaotic sequence. Nonlinear Dyn. **74**, 271–275 (2013)
33. Khan, M., Shah, T., Batool, S.: A new implementation of chaotic S-boxes in CAPTCHA. SIViP **10**, 293–300 (2016)
34. Jamal, S.S., Anees, A., Ahmad, M., Khan, M.F., Hussain, I.: Construction of cryptographic s-boxes based on Mobius transformation and chaotic tent-sine system. IEEE Access **7**, 173273–173285 (2019)
35. Ahmad, M., Al-Solami, E., Alghamdi, A.M., Yousaf, M.A.: Objective S-boxes method using improved chaotic map-based heuristic search and algebraic group structures. IEEE Access **8**, 110397–110411 (2020)
36. Özkaynak, F.: Construction of robust substitution boxes based on chaotic systems. Neural Comput. Appl. **31**, 3317–3326 (2019)
37. Özkaynak, F.: On the effect of chaotic system in performance characteristics of chaos based s-box designs. Phys. A (2020). https://doi.org/10.1016/j.physa.2019.124072
38. Yousaf, A., Alolaiyan, H., Ahmad, M., Dilbar, M., Razaq, A.: Comparison of pre and post-action of a finite Abelian group over certain nonlinear schemes. IEEE Access **8**, 39781–39792 (2020)

39. Artuğer, F., Özkaynak, F.: A novel method for performance improvement of chaos-based substitution boxes. Symmetry (2020). https://doi.org/10.3390/sym12040571
40. Liu, H., Kadir, A., Xu, C.: Cryptanalysis and constructing S-Box based on chaotic map and backtracking. Appl. Math. Comput. (2020). https://doi.org/10.1016/j.amc.2020.125153
41. Wang, S.H., Liu, W.R., Lu, H.P., Kuang, J.Y., Hu, G.: Periodicity of chaotic trajectories in realizations of finite computer precisions and its implication in chaos communications. Int. J. Mod. Phys. B **18**(17n19), 2617–2622 (2004)
42. Yuan, H., Luo, L., Wang, Y.: An S-box construction algorithm based on spatiotemporal chaos. Inte. Conf. Commun. Mobile Comput. **1**(2010), 61–65 (2010)
43. Pisarchik, A.N., Flores-Carmona, N.J., Carpio-Valadez, M.: Encryption and decryption of images with chaotic map lattices. Chaos Interdiscip. J. Nonlinear Sci. **16**, 033118 (2006)
44. Wang, S., Hu, G.: Coupled map lattice based hash function with collision resistance in single-iteration computation. Inf. Sci. **195**, 266–276 (2012)
45. Lü, L., Li, Y., Sun, A.: Parameter identification and chaos synchronization for uncertain coupled map lattices. Nonlinear Dyn. **73**, 2111–2117 (2013)
46. Chen, Y., Xiao, J., Wu, Y., Li, L., Yang, Y.: Optimal windows of rewiring period in randomly coupled chaotic maps. Phys. Lett. A **374**(31–32), 3185–3189 (2010)
47. Zhang, Y.-Q., Wang, X.-Y.: Spatiotemporal chaos in Arnold coupled logistic map lattice. Nonlinear Anal.: Modell. Control. **18**, 526–541 (2013)
48. Zhang, Y.-Q., Wang, X.-Y.: A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice. Inf. Sci. **273**, 329–351 (2014)
49. Zhou, Y., Bao, L., Chen, C.L.P.: A new 1D chaotic system for image encryption. Sig. Process. **97**, 172–182 (2014)
50. Shibata, H.: KS entropy and mean Lyapunov exponent for coupled map lattices. Phys. A **292**, 182–192 (2001)
51. IEEE Standard for Floating-Point Arithmetic. IEEE Std 754-2008. (2008). https://doi.org/10.1109/IEEESTD.2008.4610935
52. Cusick, T., Stanica, P.: Cryptographic Boolean Functions and Applications. Elsevier, Amsterdam (2009)
53. Dimitrov, M.M.: On the design of chaos-based S-boxes. IEEE Access **8**, 117173–117181 (2020)
54. Webster, A., Tavares, S.: On the design of S-boxes. In: Advances in Cryptology: Proceedings of CRYPTO'85. Lecture Notes in Computer Science, pp. 523–534 (1986)
55. Dawson, M.H., Tavares, S.E.: An expanded set of design criteria for substitution boxes and their use in strengthening DES-like cryptosystems. IEEE Pac. Rim Conf. Commun., Comput. Sig. Process. Conf. Proc. **1**, 191–195 (1991)
56. Malik, M.S.M., Ali, A., Khan, M.A., Ehatisham-ul-Haq, M., Mehmood, S.N., Rehman, M., Ahmad, W.: Generation of highly nonlinear and dynamic AES substitution-boxes (S-boxes) using chaos-based rotational matrices. IEEE Access **8**, 35682–35695 (2020)
57. Munir, F.A., Zia, M., Mahmood, H.: Designing multi-dimensional logistic map with fixed-point finite precision. Nonlinear Dyn. (2019). https://doi.org/10.1007/s11071-019-05112-4