Nonlinear Dyn
https://doi.org/10.1007/s11071-024-10138-4

RESEARCH

Characteristics of 3D coupled map lattice and its application in pseudo-random number generator

Zhuo Liu · Yong Wang · Jinyuan Liu · Jun Feng · Leo Yu Zhang

Received: 7 May 2024 / Accepted: 7 August 2024

Abstract Coupled map lattice (CML), as a classical model of the higher-dimensional chaotic system, possesses outstanding chaotic dynamic behavior both at time and space. Compared with one-dimensional CML and two-dimensional CML, three-dimensional (3D) CML has more complicated chaotic behavior, and it is pretty suitable for designing chaos-based cryptographic schemes. In this paper, foremost, theoretical mathematical expressions of Lyapunov exponent (LE) and synchronization stability in the 3D CML model are deeply and comprehensively obtained, which guide the parameters setting to keep the model in the fully chaotic state and avoid synchronization state. Also, other chaotic behaviors such as bifurcation, ergodicity, and probability density distribution are analyzed, and all of those demonstrate the 3D CML model has complex chaotic performance. Furthermore, according to the 3D CML model and theoretical results, a novel pseudo-random number generator (PRNG) has been proposed with safety assurance via the simple interception operation. Finally, large amounts of simulations verify the theoretical results are correct and our proposed PRNG scheme possesses outstanding performance. Finally, the 3D CML model is extended into the ND CML one, LE expression is also derived. Above all, our research can provide some theoretical guidance for using the CML model (i.e. 3D CML and ND CML) as a core component to construct chaos-based cryptographic schemes, and it owns well potential application.

Keywords Higher-dimensional chaotic system · 3D coupled map lattice · Lyapunov exponent · Synchronization stability · Pseudo-random number

Z. Liu
School of Mathematics and Big Data, Guizhou Education University, Guiyang, China

Y. Wang (✉)
College of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chongqing, China
e-mail: wangyong_cqupt@163.com

J. Liu
School of Intelligent Technology and Engineering, Chongqing University of Science and Technology, Chongqing, China

J. Feng
School of Cyber Science and Engineering, Huazhong University of Science and Technology, Wuhan, China

L. Y. Zhang
School of Information and Communication Technology, Griffith University, Gold Coast, Australia

1 Introduction

Chaos, primarily observed in the meteorology, is complex and irregular [23], it possesses some outstanding characteristics, e.g. randomness, extreme sensitivity to initial values and the unpredictable orbit. Since those special properties are essentially similar to those of cryptography [7], chaos has been widely used as a core component for designing chaos-based cryptographic schemes [4,9,21,25–27,30,37]. Besides those application schemes, chaos theory is also an essential

Published online: 29 August 2024

foundation for leading to the growing development of chaos cryptography [2,3,20]. Many researchers have explored chaos theory in the domain of chaos-based cipher [8,11].

The chaotic system used in chaos cryptography is commonly simplified into two categories. One is the simple chaotic system, since having a simple structure, high efficiency and mature theoretical foundation [14], they are prevalent in those chaos-based cryptographic schemes. Another is the higher-dimensional chaotic system, compared with a simple one, it has more complicated chaotic dynamic behavior and unique advantages to be the core component for confusing information in a secure scheme. Among those higher-dimensional chaotic models, coupled map lattice (CML) is one of the most classic model [12], which has those highlights of the parallel structure and high computational efficiency, as well as keeping chaos both at time and space. Based on the above-mentioned highlights, CML has been universally used as a core component to design cryptographic primitives in those sub-fields, such as stream cipher [15,18], Hash function [32,34] and multimedia encryption [31,33]. Combining two-dimensional (2D) CML and partitioned cellular automation, a novel and excellent stream cipher algorithm is proposed in [18]. In [32], a new hash function is designed via an improved CML, which combines floating-point chaotic computations and algebraic operations, as well as local and global couplings, and finally achieves high bit confusion and diffusion. The 2D CML owns good statistical properties, and it is used for constructing the one-way hash function algorithm [34]. The bit-level image encryption scheme is designed based on an enhanced cross CML in [31], which has high effectiveness and safety against the common attacks. A new encryption scheme via the wide-range system mixed CML model is proposed [33], which is effective for securing both grayscale and color images.

Meanwhile, the pseudo-random number generator (PRNG) is commonly considered as a core component of chaos-based cryptography schemes. For enhancing security, the higher-dimensional chaotic system is popularly used to construct amounts of PRNG schemes[16, 31]. However, for the higher-dimensional chaotic system, it is important to obtain a better trade-off between security and efficiency. For instance, in [28], a novel dynamical 4-D chaotic circuit is designed, and then generates PRNG sequences by construction of chaotic circuits with competent S-Box parameters. However, its efficiency needs further improvement. Furthermore, combining three different fractional chaotic systems, a novel structure for the PRNG scheme is proposed as a keystream to encrypt the image. For this scheme, both security and efficiency are weak. During our previous research work [36], the 2D CML model is analyzed and designed for the PRNG scheme, the relation between chaos and the pseudo-random number is established, and our scheme has high security and efficiency. However, it is well acknowledged that in such chaos-based cryptography applications, more complexity underlying a chaotic system indicates much security. Therefore, suppose using the 3D CML model to design the PRNG scheme, and it is coupled by those adjacent six nodes from there dimensional. Under the premise of considering security, the security of 3D CML-based cryptography scheme will be probably improved, this point needs further verification in this paper.

The above-mentioned existing research shows that ensuring the complex dynamic behavior of CML by reasonably configuring its structure and parameters is of great significant and timely to the security schemes. From this perspective, extending 2D CML into 3D CML is a promising approach to obtaining more complicated dynamic behavior. However, to the best of our knowledge, there are only a few scientific theoretical studies on the behavior of 3D CML. From the view of using it for confusing or encrypting information, in this paper, two core metrics: Lyapunov exponent (LE) and synchronization stability are chosen and analyzed, because, from the view of cryptography, LE is usually used to measure the diffusion performance of a chaotic system, synchronization stability is closely related to the complexity of a system. To design security schemes based on 3D CML, we definitely expect this model to be in the asynchronous state, which is the opposite side of synchronization stability.

Motivated by this, the 3D CML model is taken for a case study, its LE and synchronization stability are theoretically derived, which provides important theoretical guidelines for cryptographic application. Bifurcation, ergodicity and probability density distribution (PDD) of the 3D CML model are simulated to show it has outstanding chaotic performance. Based on the above-mentioned theoretical outcome, our PRNG scheme is designed, and experimental simulations illustrate our scheme possesses outstanding performance.

To summarise, among others, the main objectives of our study include:

1. The mathematical expression of LE in the 3D CML model is given theoretically, according to the accurate LE values, it is easy to judge whether the 3D CML model is in a chaotic state or not, as well as providing important theoretical guidelines for ensuring the model in the fully developed chaotic state of cryptographic application.
2. The mathematical formula of synchronization stability in the 3D CML model is derived, according to theoretical results, the parameters are set reasonably to avoid synchronization phenomenon, and it improves the security of the chaos-based cryptographic application.
3. Finally, all experiment simulations of LE and synchronization stability align perfectly with the theoretic formulas, those conclusions greatly enrich and support the development of chaos cryptography. Also, bifurcation, ergodicity and PDD of the 3D CML model are analyzed. Compared with one-dimensional (1D) CML and two-dimensional (2D) CML, 3D CML has more complicated chaotic behavior for designing the chaos-based cryptographic scheme.
4. According to the 3D CML model, based on those theoretical results, a novel PRNG scheme is constructed with safety assurance, and all simulation results verify that our scheme is both secure and efficient.
5. Some important conclusion of LE in the ND CML model is derived, it can provide some theoretical guidance for application of the CML model.

The rest of this paper is written as follows. Section 2 shows some preliminary knowledge. Theoretical analysis of LE and synchronization stability in 3D CML is presented in Sect. 3, meanwhile, bifurcation,ergodicity and PDD of the 3D CML model are simulated in this section. In Sect. 4, our PRNG scheme is proposed via the 3D CML model. Some numerical tests are presented to further verify those theoretical results are correct, and our scheme has excellent performance via extensive simulation analyse in Sect. 5. Furthermore, some important conclusion of the ND CML model is shown in Sect. 6. Finally, the conclusion is drawn in Sect. 7.

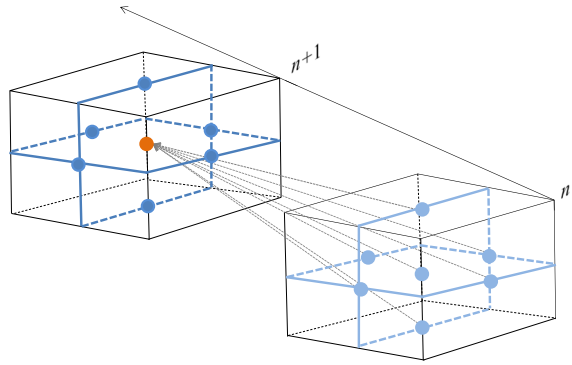


Fig. 1 The 3D CML model

2 Preliminaries

2.1 The 3D CML model

It is well known that the 2D CML model has outstanding chaotic dynamic behavior performance [31], in which, the current node value is decided by those adjacent four nodes. To further enhance the chaotic dynamic behavior, the 2D CML model is extended into a three-dimensional one, as depicted in Fig. 1, the current node value of 3D CML is calculated by those adjacent six nodes, and its mathematical definition is described as

Definition 1 The three-dimensional CML model is defined as

$$x_{n+1}^{s,t,u} = (1-\varepsilon)\mathrm{F}(x_n^{s,t,u}) + \frac{\varepsilon}{6}\left[\mathrm{F}(x_n^{s+1,t,u}) + \mathrm{F}(x_n^{s-1,t,u}) + \mathrm{F}(x_n^{s,t+1,u}) + \mathrm{F}(x_n^{s,t-1,u}) + \mathrm{F}(x_n^{s,t,u-1}) + \mathrm{F}(x_n^{s,t,u+1})\right], \tag{1}$$

where $s = 1, 2, \cdots, R$, $t = 1, 2, \cdots, L$ and $u = 1, 2, \cdots, U$. And R, L and U are the row, column and height indexes of the 3D CML model, respectively.

And its periodic boundary conditions are $x_n^{s+R,t,u} = x_n^{s,t,u}$, $x_n^{s,t+L,u} = x_n^{s,t,u}$ and $x_n^{s,t,u+U} = x_n^{s,t,u}$.

2.2 Lyapunov exponent

LE is significantly important in judging the chaotic behavior of a dynamic system quantitatively. In a system of $x_{n+1} = \mathrm{F}(x_n)$, LE ≥ 0 indicates the system is chaotic, LE < 0 shows the system is regular, which is shown as

$$\mathrm{LE} = \lim_{n\to\infty} \frac{1}{n} \ln \left| \prod_{m=1}^{n} \mathrm{F}'(x_m) \right|. \tag{2}$$

For a higher-dimensional chaotic system, according to the order from large to small, it has multiple LEs shown as $\{\mathrm{LE}_1, \mathrm{LE}_2, \cdots, \mathrm{LE}_n\}$, where LE_1 is the maximum LE (MLE).

2.3 Pseudo-randomness

For a floating number x, it exists the following important theoretical results, and Theorem 1 is decipted and proven in [36].

Theorem 1 *For a random (or pseudo-random) distribution in* $[0, 1]$*, assume that the density function has a bounded first-order derivative.For any sample* $x = 0.w_1w_2\cdots w_{z-1}w_z$ *(*$w_i \in \{0, 1\}$ *and* $i \in [1, z]$*) from this distribution, one has*

$$\lim_{z\to\infty} P(w_z = 0) = \lim_{z\to\infty} P(w_z = 1). \tag{3}$$

According to Theorem 1, it is clear that $z \to +\infty$ indicates $P(w_z = 0) = P(w_z = 1) = \frac{1}{2}$.

3 The performace analyses of the 3D CML model

3.1 Lyapunov exponent analysis

In this section, we mathematically derive the LE expression of the 3D CML model. According to the theoretical formula, the parameters are properly set and its LEs are calculated accurately for evaluating its chaotic performance, which makes sure the model in the most complicated chaotic state and avoids it in the synchronization state. The details of derivation are described in the appendix A.

Proof See the appendix A. □

According to the appendix A, it is easy to obtain the mathematical expression in LE of the 3D CML model, which is shown as

$$\mathrm{LE} = \mathrm{LE_F} + \ln\left|1-\varepsilon + \frac{\varepsilon}{3}\left(\cos\frac{2\pi k}{U} + \cos\frac{2\pi r}{R} + \cos\frac{2\pi l}{L}\right)\right|, \tag{4}$$

In Eq. (4), for $k = 0, 1, \cdots, U-1$, $r = 0, 1, \cdots, R-1$ and $l = 0, 1, \cdots, L-1$, it is evident that we can accurately calculate the LEs of the 3D CML model for different sizes and the coupling parameters. In addition, when $k = 0, r = 0$ and $l = 0$, it is immediate that we can obtain Theorem 2 about MLE of the 3D CML model, which provides the theoretical foundation for engineering application.

Theorem 2 *The maximum Lyapunov exponent (MLE) of the 3D CML model is solely determined by the local chaotic map.*

Proof For Eq. (4), satisfying $k = 0, r = 0$ and $l = 0$, the MLE of the 3D CML model is calculated as

$$\begin{aligned}\mathrm{LE_{MLE}} &= \mathrm{LE_F} + \ln\left|1-\varepsilon + \frac{\varepsilon}{3}(\cos 0 + \cos 0 + \cos 0)\right| \\ &= \mathrm{LE_F}.\end{aligned} \tag{5}$$

□

$\mathrm{LE_{MLE}} = \mathrm{LE_F}$ implied Theorem 2 is correct, it provides theoretical guidelines for 3D CML's application. For different parameters, one can easily calculate LEs, take the Logistic map $x_{n+1} = 4x_n(1-x_n)$ as the local map, according to Theorem 2, it is clear that MLE of 3D CML is $\ln^2$. Furthermore, the Piece-Wise Logistic map (PLM) defined in Eq. (6) is an enhanced version of well-known Logistic map with much larger LE and more complex chaotic characteristics than the Logistic map [35].

$$\begin{aligned}x_{m+1} &= \mathrm{PLM}(x_m) \\ &= \begin{cases} \mu N^2(x_m - \frac{i-1}{N})(\frac{i}{} - x_m), & \frac{i-1}{N} < x_m < \frac{i}{N}, \\ \cdots \\ 1 - N^2\mu(x_m - \frac{i-1}{N})(\frac{i+1}{N} - x_m), & \frac{i}{N} < x_m < \frac{i+1}{N}, \end{cases}\end{aligned} \tag{6}$$

where $x_m \in (0, 1)$ is the state value, $\mu \in (0, 4]$ is the control parameter, and N is the segment number of PLM. For comparison, PLM is selected as the local map, its MLE is 4.574594. When the 3D CML model is used for designing the chaos-based cryptography scheme, PLM is a better choice than the Logistic map. Consequently, for numerous of chaos-based cryptography schemes, Theorem 2 is a theoretical foundation for judging the chaotic dynamic behavior of the 3D CML model. Meanwhile, it is easy to get the following corollaries via Theorem 2.

Corollary 1 *The MLE is independent of the size of the 3D CML model.*

Corollary 2 *In the 3D CML model, increasing LE of the local chaotic map F leads to an increase in the MLE of the model.*

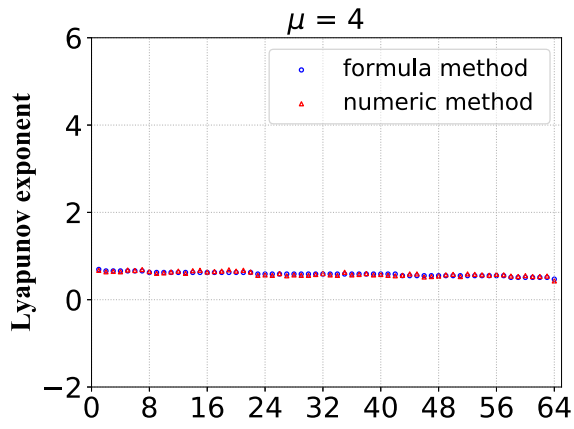
From the view of cryptography, the 3D CML model used in the encryption applications should own good chaotic performance. Corollaries 1 and 2 show that the local chaotic map is all-important for the 3D CML model, which directly determines its chaotic dynamic behavior. The larger the MLE of the local chaotic map is, the more complex the 3D CML model will be. Therefore, when designing those encryption schemes based on the 3D CML model, we should choose the local chaotic map F with a large MLE.

Here, to further verify those theoretical results, we select the classical Logistic map $x_{n+1} = 4x_n(1 - x_n)$ and PLM with $\mu = 4$ and $N = 64$ as the local map, denoted as L-3D CML and PLM-3D CML, respectively. Figure 2 illustrates the LEs of them via the simulation method and formula method. As can be seen from the figure, those simulation LEs and theoretical LEs are almost the same, which fully verifies the theoretical results in LE are correct.

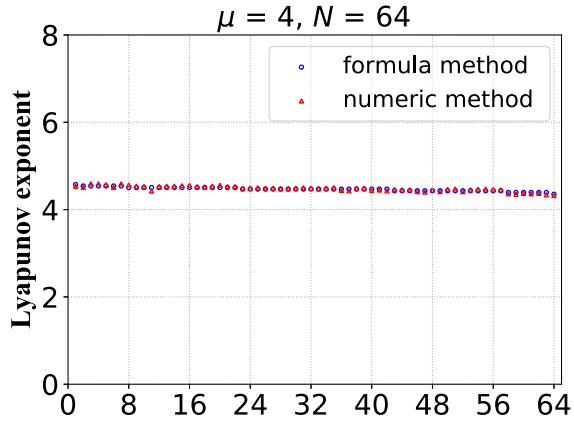
According to theoretical results, it is easy to get the different parameter changes on the chaotic behavior, since we can accurately compute the LE values via Eq. (4). Take PLM with $\mu = 4$, $N = 64$ and Logistic with $\mu = 4$ as the local map for example, for PLM, set $\varepsilon = 0.1, U = R = L = 4$; $\varepsilon = 0.8, U = R = L = 4$; while in Logistics map, make $\varepsilon = 0.1, U = R = L = 6$ and $\varepsilon = 0.8, U = R = L = 6$. Calculate their LE values and show their LE values as following in Fig. 3. According to this figure, it is clear that the local map decides MLE of the 3D CML model, we choose the local map with larger LE. So, PLE is selected for display better chaotic performance. And also ε effect the other LE values, to demonstrate this point theoretically, take the derivative of Eq. (4) with respect to ε,then LE$'$ is expressed as

$$\mathrm{LE}' = \frac{\cos\frac{2\pi k}{U} + \cos\frac{2\pi r}{R} + \cos\frac{2\pi l}{L} - 3}{3 + \varepsilon(\cos\frac{2\pi k}{U} + \cos\frac{2\pi r}{R} + \cos\frac{2\pi l}{L} - 3)}. \tag{7}$$

To select the coupling parameter ε with better chaotic property, we first consider the case that the denominator $3+\varepsilon(\cos\frac{2\pi k}{U}+\cos\frac{2\pi r}{R}+\cos\frac{2\pi l}{L}-3)$ of Eq. (7) is 0. In this case, $k = r = l = 4$ and $\varepsilon = 0.5$, so $\varepsilon = 0.5$ should be avoided. We then investigate the value of LE$'$ by enumerating all the possibilities of k, l and r. It turns out that when $\varepsilon \in (0, 0.5)$, LE$' < 0$ regardless the choices of k, l and r. And depending on specific choices of k, l and r, LE$'$ can be either positive and negative for $\varepsilon \in (0.5, 1)$. That said, the value of LE monotonically decreases for $\varepsilon \in (0, 0.5)$ and fluctuates for $\varepsilon \in (0.5, 1)$ and smaller ε achieves better chaotic property.



(a) LEs of L-3D CML



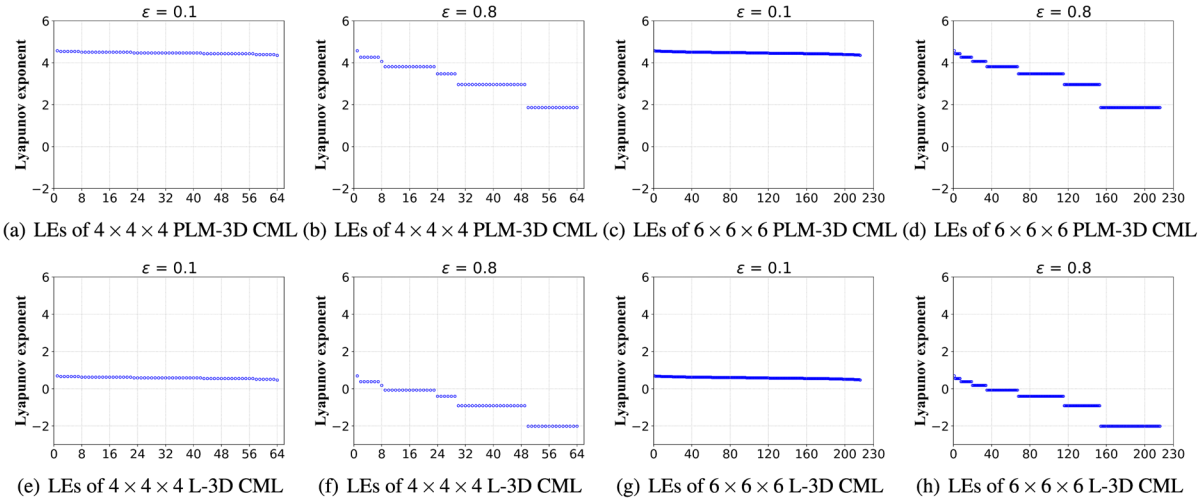
(b) LEs of PLM-3D CML

Fig. 2 LEs of the $4 \times 4 \times 4$ 3D CML model with the Logistic map and PLM

To sum up, the mathematical formula of LE in the 3D CML model is essential for the application research in chaos cryptography, which guides the setting of parameters to remain the 3D CML model keep in a fully chaotic state.

3.2 Synchronization stability analysis

For the higher-dimensional chaotic system, the stability of periodic orbit and synchronization chaos are sub-



(a) LEs of $4 \times 4 \times 4$ PLM-3D CML (b) LEs of $4 \times 4 \times 4$ PLM-3D CML (c) LEs of $6 \times 6 \times 6$ PLM-3D CML (d) LEs of $6 \times 6 \times 6$ PLM-3D CML

(e) LEs of $4 \times 4 \times 4$ L-3D CML (f) LEs of $4 \times 4 \times 4$ L-3D CML (g) LEs of $6 \times 6 \times 6$ L-3D CML (h) LEs of $6 \times 6 \times 6$ L-3D CML

Fig. 3 LE values of the 3D CML model with different parameters

stantially more complicated than the simple chaotic system. From the standpoint of cryptography application, as appropriate parameter tuning is critical for applications based on chaotic systems, the parameter settings should ensure that the chaotic model keeps in a fully developed chaotic state with asynchronous.

In the 3D CML model, the indicator $\{\mathrm{LE}_2, \cdots, \mathrm{LE}_n\}$ should be discussed, with $\mathrm{LE}_2 > 0$ meaning in an asynchronous state and $\mathrm{LE}_2 < 0$ meaning in a synchronous state. Thus, the theoretical investigation of the synchronization stability of the model is presented as follows:

To begin with, let $k = R$, $l = L - 1$ and $r = U$, according to Eq. (4), we can get the second maximum LE value LE_2 as

$$\mathrm{LE}_2 = \mathrm{LE}_\mathrm{F} + \ln \left| 1 - \varepsilon + \frac{\varepsilon}{3} \left(2 + \cos \frac{2\pi (L-1)}{L} \right) \right| \quad (8)$$

Then, set $\mathrm{LE}_2 = 0$, the critical value of L is calculated as

$$L_c = \left\lfloor \frac{2\pi}{\arccos \frac{3e^{-\mathrm{LE}_\mathrm{F}} - 3 + \varepsilon}{\varepsilon}} \right\rfloor. \quad (9)$$

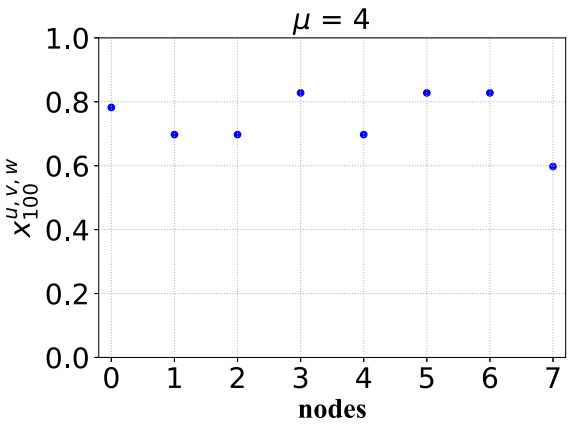
Here, L_c represents the minimum number of nodes that can ensure the system keeps in an asynchronous state, i.e., $L > L_c$ should be used to make $\mathrm{LE}_2 > 0$. According to Eq. (9), one can get the following theorem.

Theorem 3 *In the 3D CML model, the critical value L_c of the synchronization stability is only related to LE_F and ε.*

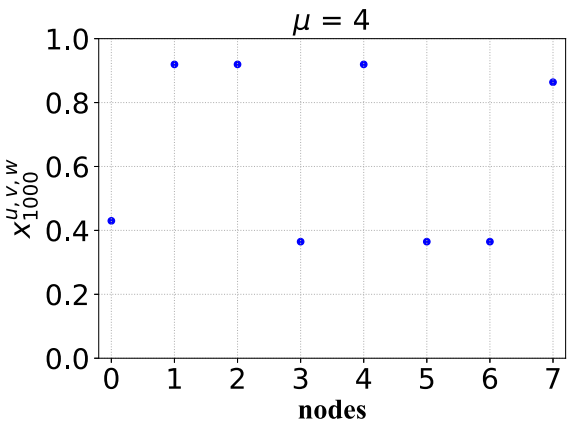
For those chaos-based cryptographic schemes, according to Eq. (9) and Theorem 3, one can choose the suitable parameters and effectively avoid the chaotic iteration values appearing in the synchronous phenomenon in the 3D CML model, and it can guarantee the security of those chaos-based cryptographic schemes theoretically.

Furthermore, take the Logistic map and PLM as the local map to verify the synchronization stability. For the Logistic map, according to Eq. (9), set $\varepsilon = 0.9$, and $L_c = 2$ is obtained. So, initialize the 3D CML model with size $2 \times 2 \times 2$. Then, iterate 3D CML for 100 times and 1000 times denoted as $x_{100}^{u,v,w}$ and $x_{1000}^{u,v,w}$, respectively. we plot them in Fig. 4. From this figure, we can observe the 3D CML model is not in a fully developed chaotic pattern. To make $\mathrm{LE}_2 > 0$, select the $2 \times 2 \times 4$ 3D CML model, other parameters remain unchanged, simulation results are depicted in Fig. 5. As can be seen from the table, no stable synchronous chaos can be observed in the 3D CML model here. At the same time, based on Eq. (9), whatever the parameters are, PLM-3D CML is still in the asynchronous state.

This once again illustrates that PLM-3D CML model's performance is better than L-3D CML model's. With this consideration and to maintain a certain level of coupling effect, we take the empirical value $\varepsilon = 0.1$ for 3D CML instantiated with PLM in the rest of this paper.

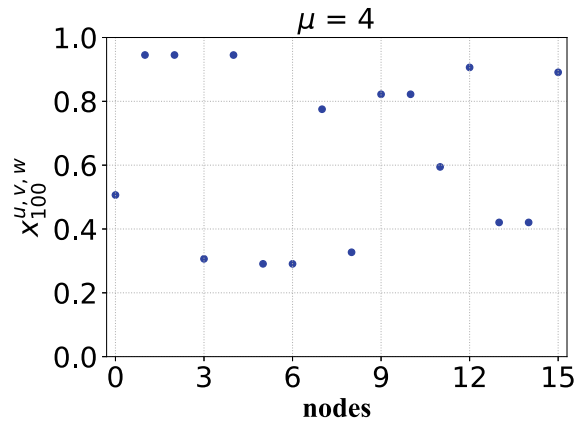


(a) The state values $x_{100}^{u,v,w}$

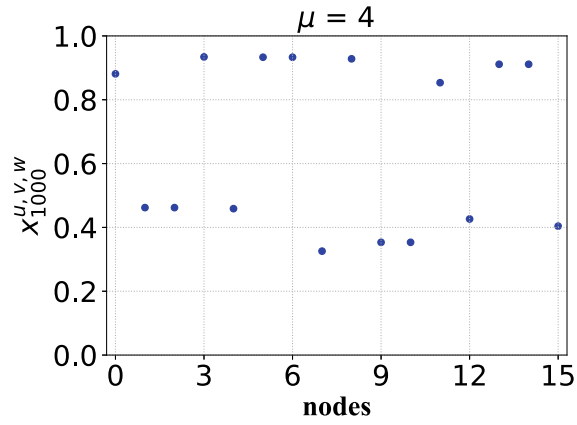


(b) The state values $x_{1000}^{u,v,w}$

Fig. 4 The state values of the $2 \times 2 \times 2$ L-3D CML



(a) The state values $x_{100}^{u,v,w}$



(b) The state values $x_{1000}^{u,v,w}$

Fig. 5 The state values of the $2 \times 2 \times 4$ L-3D CML

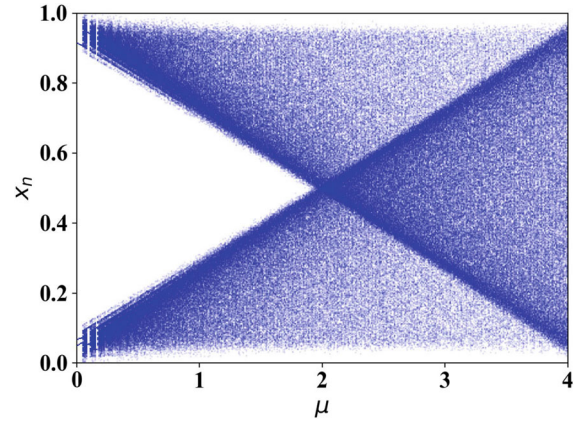


Fig. 6 Bifurcation of the 3D CML model

3.3 Bifurcation analysis

For the dynamic system, bifurcation intuitively displays the sudden change process near the critical point, it is used to effectively observe and analyze the dynamic behavior under different parameters. In the 3D CML model, choose PLM with $\mu = 4$, $N = 64$ as the local map, set $R = L = U = 4$ and $\varepsilon = 0.1$. According to extensive experiments of all 64 nodes in the 3D CML model, it is observed that the bifurcation of all the nodes is basically the same, so, take the first node as an example for analyzing the bifurcation. The results are shown in Fig. 6. From the figure, it can be seen that the change of ε has a significant impact on the bifurcation of the model, with the increasing of ε, bifurcation

becomes more and more sufficient. When $\mu = 4$, LE of PLM is maximum, and bifurcation of the 3D CML is the most comprehensive. Therefore, when $\mu = 4$, chaotic dynamics behavior is the most complex, and cryptography applications have the best performance.

3.4 Ergodicity analysis

Ergodicity is that chaotic motion orbit would pass through the state point in the phase space in the finite time. It is closely related to randomness, the wider ergodicity indicates its randomness is difficult to predict. So, selecting a chaotic system with a wider and more uniform traversal interval is a better choice for designing kinds of chaos-based cryptography systems.

In the 3D CML model, choose PLM with $N = 64$ as the local map, and set $R = L = U = 4$ and $\varepsilon = 0.1$. For different μ with 0.1, 0.5, 1.0,1.5,2.0,3.0, 3.5, and 4.0, respectively, the interval is shown in Fig. 7. According to the figure, it is clear that the traversal interval becomes much wider along the change of μ. When $\mu = 0.1$, the interval lies in $[0, 0.1]$ and $[0.9, 0.1]$, when $\mu = 2$, the interval is $[0, 1]$, and most of values are mainly concentrated in $[0.4, 0.6]$, when $\mu = 4$, the state values of the 3D CML model are uniformly distributed throughout the traversal interval $[0, 1]$. At this point, the chaotic performance of model is best, and the randomness and uniformity of chaotic sequences are also perfect.

3.5 PDD analysis

PDD describes the probability and distribution of the output values of a random variable in a certain region. From the view of cryptography, when using a chaotic system as the core component of designing a cryptographic algorithm, the more uniform PDD of chaotic sequences means stronger security of the algorithm. In this section, choose PLM with $N = 64$ and $\mu = 0.1$ as the local map, and set $R = L = U = 4$ and $\varepsilon = 0.1$. Then, generate the 3D CML model for multiple iterations and count the distribution of chaotic sequences in intervals $[0, 1]$, the details are shown in algorithm 1. The results of algorithm 1 are plotted in Fig. 8, and it is clear that PDD of 3D CML is uneven.

Algorithm 1: PDD of PLM-3D CML

Input: The $4 \times 4 \times 4$ 3D CML model with $\varepsilon = 0.1$.
Output: PDD.
Function `Main`**:**
  Step 1 Run the $4 \times 4 \times 4$ 3D CML for 1000 times and abandon them to eliminate influence of initial values;
  Step 2 Continue to iterate the model for 300000 times and obtian $\{x^i\}_{i=1}^{19200000}$;
  Step 3 Divide $(0, 1)$ into evenly into 1000 intervals.
  for x^i **do**
    Compute frequency of x^i in each interval;
  end
Output the diagram of PDD;
return 0

3.6 Comparative analysis

To verify the 3D CML model has better chaotic performance than 1D CML and 2D CML, we do the following analyses.

Kolmogorov entropy is an important index to depict the chaotic behavior of a dynamic system, it is calculated as Eq. (10). According to Eq. (10), it is clear that the K is the sum of all positive LEs. The larger the value of K is, the more complex the dynamic behavior becomes.

$$K = \lim_{\mathrm{LE}_n > 0} \mathrm{LE}_n. \tag{10}$$

Kolmogorov entropy values of the 64 1D CML, the 8×8 2D CML and the $4 \times 4 \times 4$ 3D CML are calculated as $K_1 = 41.03428$, $K_2 = 41.05647$ and $K_3 = 41.06386$, respectively, it is easy to get

$$K_3 > K_2 > K_1.$$

For the same 64 nodes in different CML models (i.e.1D CML, 2D CML and 3D CML), the 3D CML model owns the highest information loss rate, which indicates the 3D CML model holds the best chaotic performance.

Considering the synchronization stability of 1D CML, 2D CML and 3D CML, selecting the Logistic map $x_{n+1} = 4x_n(1 - x_n)$ as the local map. According to the corresponding equations in [8], $\mathrm{LE_F} = \ln^2$, it is easy to calculate the critical node number L_c, those values of L_c are shown in Table 1. According to this table, it is clear that those three models can appear the synchronization under certain conditions. When $\varepsilon = 0.5, 0.8, 0.9$ and 0.999999999, those three model appear the synchronization state. For instance, L_c of 1D CML, 2D CML and 3D CML are 7, 2 and 2, respectively, in this case, 1D CML and 2D CML appear synchronization state, but 3D CML don't. Consequently,

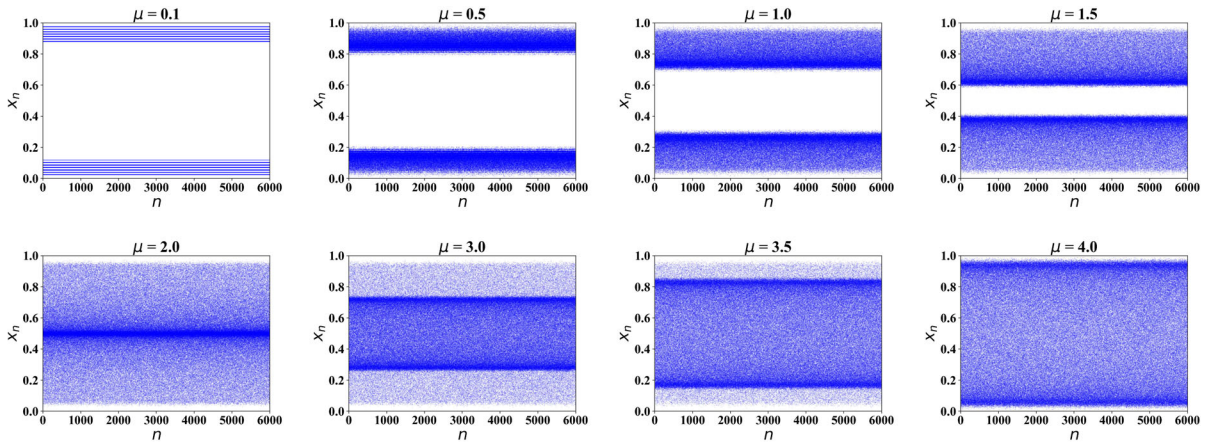


Fig. 7 Ergodicity of the 3D CML model with different parameters μ

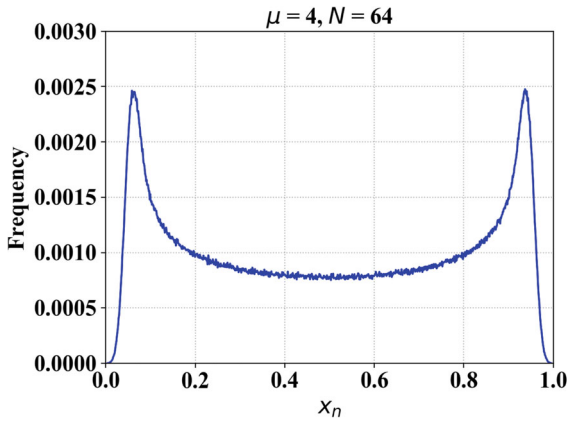


Fig. 8 PDD of the 3D CML model

Table 1 Critical node number of the 3D CML model with synchronization

Parameter ε	L_c of 3D CML	L_c of 2D CML	L_c of 1D CML
0.01	0	0	109
0.1	0	0	42
0.3	0	0	18
0.5	1	1	11
0.8	2	2	7
0.9	2	3	6
0.999999999	2	3	6

1D CML and 2D CML are more likely in the synchronization state for the same parameters. Above all, it demonstrates the 3D CML model has better chaotic performance than others.

4 The proposed PRNG scheme

According to the above-mentioned analysis, the 3D CML model possesses remarkable chaotic performance. So, it is taken as a core component for constructing the PRNG scheme, the details are depicted in algorithm 2 and summarized in the following steps.

Step 1: Set $R = L = U = 4, \varepsilon = 0.1$ in the 3D CML and select PLM with $\mu = 4$, $N = 64$ as the local map. Iterate the model 1000 times and then give up to eliminate the influence of the initial values.

Step 2: Continue to iterate the model and obtain the z floating number for one iteration. For each number x_k,$k \in [1, z]$, it can be transformed into

$$x_k = 0.w_1 w_2 \cdots w_{z-1} w_z,\ w_z \in \{0, 1\}. \tag{11}$$

Step 3: The pseudo-randomness chaotic sequences w with $(z-s+1)$-bit can be intercepted via the following equation.

$$w = w_s w_{s+1} \cdots w_{z-1} w_z. \tag{12}$$

Here, one can select $z = 64$ and $s = 33$, in order to further reducing computational complexity or memory usage, we perform algorithm optimization measure. For each x^i, we do the operation of extracting bits firstly, then, itarate the model, this can effectively reduce memory space. Its pseudocode is shown as in algorithm 3, which is parameterized based on algorithm 2. According to this algorithm, clearly, for one iteration of model, 2048-bit sequences are generated, then, for n times, $2048n$-bit sequences are obtained. The performance analyses of our proposed PRNG scheme are shown in the following section.

Algorithm 2: Our proposed PRNG scheme

Input: Initial conditions and system parameters of the 3D CML model.
Output: Pseudo-random bits.
Function `Main`**:**
  Step 1 Run the 3D CML instances and collect the corresponding orbits $\{x^i\}_{i=0}^{l}$ and update the states;
  while $x^k \in \{x^i\}$ **do**
    $x^k = 0.w_1 w_2 \cdots w_{z-1} w_z$
    $w = w_s w_{s+1} \cdots w_{z-1} w_z$
  end
Go back to **Step 1**
return 0

Algorithm 3: Our proposed PRNG scheme for parameter concretization

Input: The $4 \times 4 \times 4$ PLM-3D CML model with $\varepsilon = 0.1$.
Output: 2048-bits.
Function `Main`**:**
  Step 1 Run the $4 \times 4 \times 4$ PLM-3D CML for 1000 times and abandon them to eliminate the influence of initial values, then, continue to iterate the model once;
  Step 2 To each node value x^i, perform the following operation;
  $x^i = 0.w_1 w_2 \cdots w_{63} w_{64}$
  $w = w_{33} w_{34} \cdots w_{63} w_{64}$
for $i = 0, i++, i < 64$ **do**
  Go back to **Step 2**;
end
return 0

5 Performance analysis of the proposed PRNG

According to the above-mentioned analyses, those theoretical results in LE and synchronization stability provide the critical theoretical foundation for chaos cryptography. To further verify those theoretical results, and also test the performance of the pseudo-random number generator, we have carried out the following experimental simulations.

5.1 The advantage of our scheme

Our proposed PRNG scheme based on the 3D CML model has those following highlights.

1. The 3D CML model, as a higher-dimensional chaotic model, has pretty chaotic dynamic behavior. Considering the 3D CML model as the core component, it can greatly improve the security of our scheme. And also, mathematical expression of LE and synchronization stability are given, it provides important theoretical guidelines for ensuring the model in the fully developed chaotic state of cryptographic application.
2. In our scheme, 32-bit sequences are directly obtained by intercepting the state value, no additional computational operations are required. One iteration of the model can generate 2048-bit, and it can greatly improve the efficiency of our scheme.
3. Our scheme is designed according to Theorm 1, its uniformity is theoretically guaranteed. Meanwhile, one can ensure the 3D CML model possesses best performance theoretically.

5.2 Randomness tests

The statistical test package STS launched by NIST is currently the most authoritative tool for testing the pseudo-random sequences, and it contains 15 items. For each item, there exists P-Value for measuring whether the sequences can pass the random testing successfully. Suppose P- Value $\geq \alpha$, it indicates the testing sequences pass the random testing successfully. Otherwise, it fails the random testing.

In our testing simulation, according to the algorithm 3, for each iteration of our algorithm, 2048-bit random sequences are obtained. For NIST testing, the dataset with 1 000 000 000 bit sequences is required. So, iterate algorithm 3 for 62036 times to have 1 000 000 000 bit sequences, the details are shown in Fig. 9. Moreover,

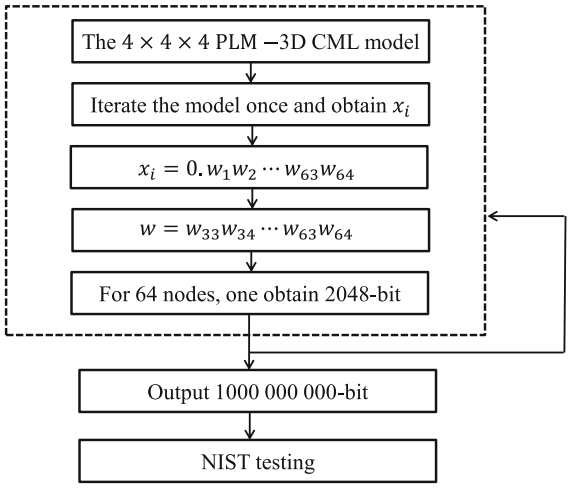


Fig. 9 The diagram of NIST testing in algorithm 3

set $\alpha = 0.01$ and test 1000 pairs with each length of 1000 000 bit, the NIST test results are listed in Table 2. According to Table 2, it is clear that all the *P*-Value are greater than 0.01, the minimum pass rate and the maximum pass rate are 0.9863 and 0.9936, respectively. We can get all the pass rates in an acceptable interval. The testing results of *P*-Value and pass rates show that all the chaotic sequences produced by the 3D CML model possess perfect random characteristics.

TestU01 test is a statistical random testing tool, offering a collection of utilities for the uniform random number generators. We have unitized the 3D CML model to produce the chaotic sequences with length of 2^{20},2^{25} and 2^{30}, respectively. Considering the three indexes of Rabbit test, Alphabit test, and BlockAlphabit test, we test the chaotic sequences and show the testing results in Table 3. According to Table 3, the different chaotic sequences can all pass the TestU01 test successfully. The TestU01 test verifies that the chaotic sequences have excellent randomness.

Above all, the above-mentioned testing of NIST and TestU01 test both prove that the chaotic sequences have outstanding random performance and those sequences are proper for being applied as the core model in the cryptography system.

5.3 Correlation tests

Correlation coefficient is an indicator that measures the degree of linear relationship between two sequences, its interval is $[-1, 1]$. The closer the value is to 0, the independence between these two sequences is much stronger. When it is equal to 0, two sequences are independent. When in the interval $(-0.3, 0.3)$, it demonstrates those two sequences are independent. Correlation coefficient can be calculated as

$$cov(x, y) = E(x - E(x))(y - E(y)), \tag{13}$$

$$r_{xy} = \frac{cov(x, y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{14}$$

where x and y are two sequences with the length of l, $E(x) = \sum_{i=1}^{l} \frac{x_i}{l}$, $D(x) = \sum_{i=1}^{l} \frac{(x_i - E(x))^2}{l}$, x_i and y_j are the i^{th} and j^{th} element of x and y, respectively.

In our test, select PLM with $N = 64$ and $\mu = 4$ as the local map. For the 3D CML model, choose $\varepsilon = 0.1$ and $R = L = U = 4$, according to our proposed PRNG scheme, set 1000 initial value vectors randomly, 1000 different sets of chaotic sequences with 66000-bit are generated, then utilize those 1000 different sets and calculate the correlation coefficient value r_{xy}, the values are shown in the Fig. 10. According to the figure, it can be seen that r_{xy} lies in the interval $(-0.02, 0.02)$, which fully indicates that those chaotic sequences are mutually independent.

5.4 Key space

From a security perspective, key space must be large enough to effectively resist violent attacks. In our proposed scheme, initial all 64 nodes of the 3D CML as $X(0, 0, 0)$, $X(0, 1, 0)$, $\cdots$, $X(3, 3, 3)$, and all those nodes are taken as the secret key. According to the IEEE 754 standard, a 64-bit floating-point precision degree is 10^{-15}, and each node of the $4 \times 4 \times 4$ 3D CML model has 10^{15} key space, 64 nodes totally own $10^{15\times64} = 10^{960}$. Therefore, the time of cracking the key space is calculated as

$$10^{960}/(2^{168} \times 5.9 \times 10^{30}) = 2.7 \times 10^{953} year. \tag{15}$$

The time of cracking the key space 10^{960} is 10^{953} year, it can effectively resist violent attack, and also verifies our proposed algorithm is pretty secure.

5.5 Key sensitivity

Key sensitivity is a considerable indicator for measuring the security of encryption algorithm, it measures the change in output ciphertext through small changes in initial parameters, so, set the following two situations:

Case 1: $\varepsilon = 0.1$, $\mu = 4$, $x_0 = 0.7639248273644901$;
Case 2: $\varepsilon = 0.1$, $\mu = 4$, $x_0 = 0.7639248373644901$.

According to the above-mentioned two cases, two different chaotic sequences are produced to encrypt the same image Airplane, adopt the XOR operation between 8-bit chaotic sequences and image grayscale values. The encrypted images are described as in Figs. 11b, c, differences of those encrypted images are shown in Fig. 11d, its value is 0.9961. Meanwhile, count the histograms of these two encrypted images, the results are depicted in Figs. 11f, g, it is clear that the histogram is uneven. It demonstrates that the 3D CML model possesses strong key sensitivity.

Table 2 NIST 800-22 test results on the chaotic sequences of our proposed PRNG scheme

No.	Test index	Test number /Failure number	Pass rate	*P*-Value	Results
1	Frequency	1000/11	0.9890	0.3669	Success
2	Block Frequency	1000/14	0.9860	0.4410	Success
3	Cumulative Sums(forward)	1000/07	0.9930	0.3804	Success
	Cumulative Sums(reverse)	1000/06	0.9940	0.8832	Success
4	Runs	1000/07	0.9930	0.3736	Success
5	Longest Run	1000/13	0.9870	0.5443	Success
6	Rank	1000/14	0.9860	0.0590	Success
7	Discrete Fourier Transform	1000/16	0.9840	0.0753	Success
8	Nonoverlapping Template*	1000/10	0.9899	0.4796	Success
9	Overlapping Template	1000/08	0.9920	0.7715	Success
10	Universal	1000/13	0.9870	0.8891	Success
11	Approximate Entropy	1000/08	0.9920	0.9724	Success
12	Random Excursions(the sample size=636)				
	(1)	636/12	0.9811	0.4015	Success
	(2)	636/08	0.9874	0.7743	Success
	(3)	636/08	0.9874	0.7681	Success
	(4)	636/04	0.9937	0.7743	Success
	(5)	636/09	0.9858	0.3609	Success
	(6)	636/05	0.9921	0.4506	Success
	(7)	636/05	0.9921	0.5729	Success
	(8)	636/08	0.9874	0.9780	Success
13	Random Excursions Variant(the sample size=636)				
	(1)	636/05	0.9921	0.8572	Success
	(2)	636/10	0.9843	0.2597	Success
	(3)	636/10	0.9843	0.2790	Success
	(4)	636/10	0.9843	0.4777	Success
	(5)	636/10	0.9843	0.1084	Success
	(6)	636/10	0.9843	0.0814	Success
	(7)	636/07	0.9890	0.6619	Success
	(8)	636/08	0.9874	0.2993	Success
	(9)	636/07	0.9890	0.4071	Success
	(10)	636/06	0.9906	0.1943	Success
	(11)	636/05	0.9921	0.9292	Success
	(12)	636/07	0.9890	0.6915	Success
	(13)	636/09	0.9858	0.4329	Success
	(14)	636/03	0.9953	0.4156	Success
	(15)	636/02	0.9969	0.6980	Success
	(16)	636/02	0.9969	0.4747	Success
	(17)	636/05	0.9921	0.8572	Success

Table 2 continued

No.	Test index	Test number /Failure number	Pass rate	*P*-Value	Results
	(18)	636/07	0.9890	0.9970	Success
14	Serial 1	1000/04	0.9960	0.2133	Success
	Serial 2	1000/03	0.9970	0.2066	Success
15	Linear Complexity	1000/11	0.9890	0.1959	Success

5.6 Differential attack analysis

When adversaries perform differential attack on the encryption algorithm, according to minor adjustments of the plaintext, then, compare the difference between the original plaintext ciphertext and the slightly adjusted plaintext ciphertext. In the 3D CML model, make small changes and verify the algorithm's resistance to differential attack. The key parameters are set in the following four cases:

Case 1: $\varepsilon = 0.1, \mu = 4, x_0 = 0.7639248273644901$;
Case 2: $\varepsilon = 0.1, \mu = 4+\Delta t, x_0 = 0.763924827364$-4901;
Case 3: $\varepsilon = 0.1, \mu = 4, x_0 = 0.763924827364490$-$1 + \Delta t$;
Case 4: $\varepsilon = 0.1 + \Delta t, \mu = 4, x_0 = 0.7639248273$6-44901;

where $\Delta t = 2^{-20}$. According to the above-mentioned cases, generate four pairs of chaotic sequence S_1, S_2, S_3, S_4 with 10000000-bit. Then, compute average absolute distance d of sequences (S_1, S_2),(S_1, S_3) and (S_1, S_4) via the following Eq. (16).

$$d = \frac{1}{M}\sum_{i=1}^{M}\left|e_i - e_i^{'}\right|, \tag{16}$$

where e_i and $e_i^{'}$ are the original sequence and the new sequence, respectively. The ideal value of average absolute distance d is 85.333. According to Eq. (16), the results are depicted in the Table 4. From this table, it is clear that all the values are near 85.333, and it fully demonstrates that our proposed scheme owns strong resistance to differential attacks.

5.7 Balanced analysis

We have plotted the number of 1 s with respect to different lengths of our PRNG outputs,shown in Fig. 12. According to this figure, it is easy to see that the bit sequences generated by our scheme have an approximately equal number of 0 s and 1 s, and almost coincide with the ideal line $y = \frac{n}{2}$. This indicates that our PRNG scheme has good balanced performance.

Table 3 TestU01 test results on the chaotic sequences of our proposed PRNG scheme

Length	*Rabbit*	Alphabit	BlockAlphabit
2^{30}	38/38	17/17	17/17
2^{25}	38/38	17/17	17/17
2^{20}	38/38	17/17	17/17

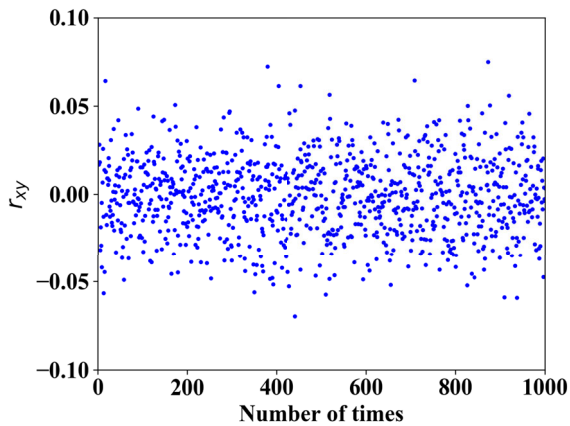


Fig. 10 Correlation coefficient values

5.8 Periodicity analysis

PRNGs are necessarily periodic, which is a serious problem when the generation of random numbers is in question. For that reason, cycles of PRNGs should have great length in order to enable the smooth functioning for a long period of time. Some of the previous chaos-based PRNGs were evaluated on the basis of non-periodicity, but on a relatively small amount of

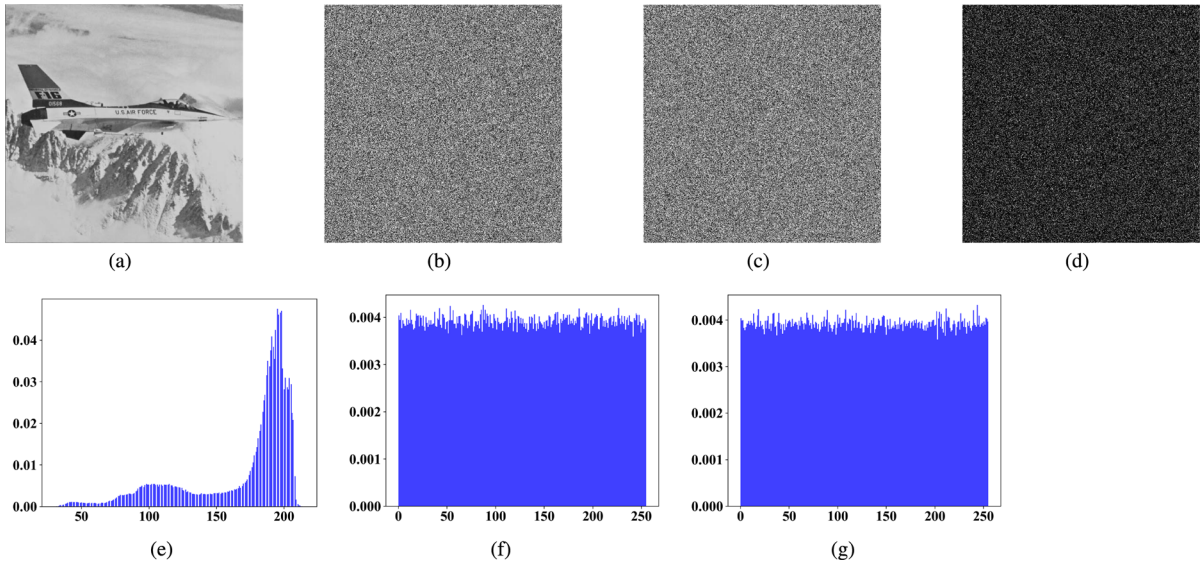


Fig. 11 The results of Airplane and the encrypted Airplane **a** Airplane; **b** The encrytped Airplane with Case 1; **c** The encrytped Airplane with Case 2; **d** The different image of Case 1 and Case 2; **e** The histogram result of Airplane; **f** The histogram result of encrytped Airplane with Case 1; **g** The histogram result of encrytped Airplane with Case 2

data (less than 2^{40} bits). However, none of these PRNGs have estimated cycle length.

Period of sequence in our proposed PRNG scheme is 2^{128}, while the classical period of PRNG scheme is 2^{40}. Consequently, our proposed PRNG scheme has sufficient length.

Table 4 The average absolute of chaotic sequences

The chaotic sequences	d
(S_1, S_2)	85.3122
(S_1, S_3)	85.3426
(S_1, S_4)	85.3401

5.9 Entropy analysis

The entropy is an key indicator for measuring state's uncertainty. If an n-bit number sequence has a good disorder, it will be considerd as a random one. A good PRNG should generate unexpected sequence with high disorder. So, we use Eq. (17) to determine those properties of our PRNG scheme.

$$E_m = \sum_{i=0}^{2^N-1} p(m_i) \log_b \frac{1}{p(m_i)}, \tag{17}$$

where N is the number of bits in each element of the sequence m, $p(m_i)$ is the chance that the element m_i will appear in the sequence, E_m is the entropy value, and b represents the radix value.

To fully verify the entropy value of our PRNG scheme, take the radix $b = 2$ and $b = 8$ for example, according to Eq. (17), we can caculate entropy values of our PRNG scheme, the results are plotted in Figs. 13 and 14. From those figures, we can see the numerical results are very close to the ideal value. It indicates that the generated binary sequences of our PRNG scheme have high complexity.

5.10 Efficiency analysis

To further assess the performance of our proposed PRNG algorithm, it is evaluated through comparing with other chaotic PRNGs [1,10,17,19,36]. The methods in [1] and [19] are more recent heuristic proposals based on enhancing simple chaotic systems and using CML, respectively. By enhancing 1D chaotic systems, the work in [10] is a famous heuristic PRNG design due to its simplicity and thorough experimental evaluation. It is noted that the design in [17] is the only

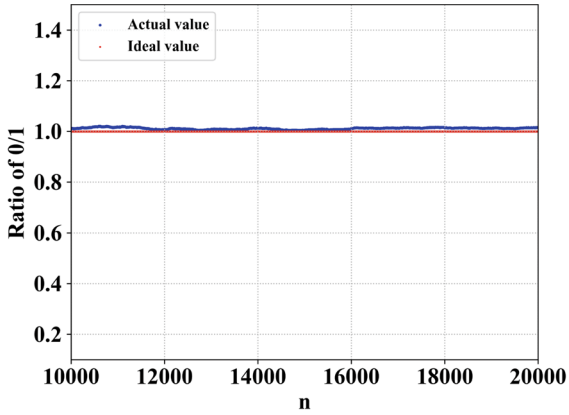


Fig. 12 The ratio of 0/1 in the random sequences generated by our PRNG scheme

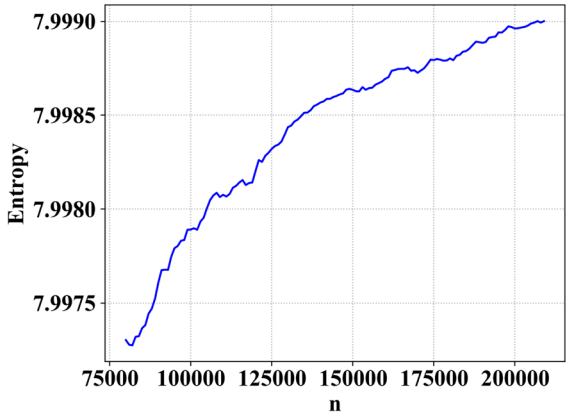


Fig. 13 Entropy values with radix=2

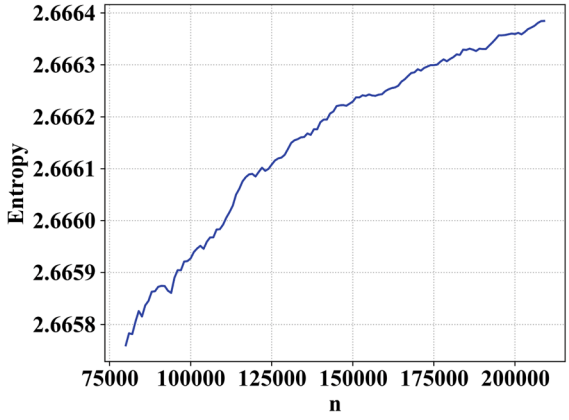


Fig. 14 Entropy values with radix=8

previously known method that provides theoretically guaranteed uniform randomness from chaotic systems. For the 2D CML mode used for PRNG in [36]. For PRNGs in [1,10,17,19,36], the same settings of the original works are used. All the algorithms are then implemented on a Laptop with the Core i7-10710U CPU and 16 G RAM.

Table 5 lists the running speed (averaged from 1, 000 tests) for generating 1 *MByte* binary stream from all these methods. With a running speed of 23.85 *MByte/s*, the proposed method is more efficient than the other theoretical sound RPNGs [17] and [36], and is also more efficient than the heuristic designs [1] (with running speed 0.3338 *MByte/s*), [13] (with running speed 22.84 *MByte/s*), [19] (with running speed 17.24 *MByte/s*) and [35] (with running speed 22.16 *MByte/s*), but inferior to the method in [10] (with running speed 62.50 *MByte/s*). However, looking further at the third and fourth column of Table 5, it is clear that the proposed method provides theoretical randomness guarantee while the method in [10] does not.

To further verify the efficiency of our proposed scheme, other similar classical schemes are used to compare with ours. Basic operations for generating 8-bit are counted and presented in Table 6. According to this table, our scheme requires 27 basic operations. While basic operations of other schemes in [1,6,10,13,17,19,24,35,36] are 27 basic operations, 1628 basic operations, 24.88 basic operations, 13.33 basic operations, 35.13 basic operations, 40 basic operations, 42 basic operations, 18 basic operations, 56 basic operations and 51.50 basic operations, repectively. Therefore, our scheme possesses a significant advantage in efficiency, also with theoretical analysis and experimental analysis to make sure its security.

5.11 Comparison analysis

Some chaos-based PRNGs are currently being proposed in the cryptographic field. Even though those schemes can pass some randomness analysis such as NIST testing, some or no security analysis have been mentioned in those schemes. PRNG is an core component of constructing the cyrptographic scheme, a thorough security analysis should be carried out to show its good performance. So, we perform the cpmparison analysis of our scheme with others in [5,22,29,38,39].

The comparison results are shown in Table 7,this table shows the investigated aspects of several PRNGs. According to this table, it is clear that our proposed scheme has been tested the most. In addition, note that

Table 5 Running speed comparison

Methods	Running speed (MByte/s)	Theoretical analysis	Experimental analysis
Ours	23.85	Yes	Yes
[1]	0.3338	No	Yes
[10]	62.50	No	Yes
[13]	22.84	No	Yes
[17]	21.28	Yes	Yes
[19]	17.24	No	Yes
[35]	22.16	No	Yes
[36]	12.80	Yes	Yes

Table 6 Number of basic operations in schemes for generating 8-bit

Number of operations	Ours	[1]	[6]	[10]	[13]	[17]	[19]	[24]	[35]	[36]
No. of exclusive OR	0	0	24	0	8	0	0	1	0	8
No. of interception	1/4	0	0	2/3	0	0	1	0	0	0
No. of Modulo	0	8	0	8	0	0	0	0	0	0
No. of comparison	0	4	0	1/3	0	32	0	2	8	0
No. of inversion	0	0	0	0	0	0	0	1	0	8
No. of addition/subtraction	15/2	248	3/8	8/3	9	8	14	5	16	59/4
No. of multiplication/division	19	1368	4/8	5/3	18	0	26	7	32	83/4
No. of converting floating-point to char	1/4	0	0	0	1/8	0	1	2	0	0
Total	27	1628	24.88	13.33	35.13	40	42	18	56	51.50

Table 7 Analysis of our PRNGs in comparison to other existing schemes

No.	Item	Ours	[5]	[22]	[29]	[36]	[38]	[39]
1	Chaotic Map	3D CML	Generalized Sprott-A system	Enhanced Logistic map	Skew Tent map	2D CML	Piecewise Cubic map	Lorenz system
2	LE(theory)	✓	×	×	×	✓	✓	×
3	LE(simulation)	✓	✓	✓	✓	✓	✓	✓
4	Synchronization Stability	✓	×	×	×	×	×	×
5	Bifurcation	✓	✓	✓	✓	✓	✓	✓
6	NIST SP800-22	✓	✓	✓	✓	✓	✓	✓
7	TestU01	✓	×	✓	×	✓	✓	×
8	Key Space	✓	✓	✓	✓	✓	✓	✓
9	Key Sensitivity	✓	✓	✓	✓	✓	✓	✓
10	Differential Attack	✓	×	×	×	×	✓	×
11	Correlation Test	✓	✓	✓	✓	×	✓	✓
12	Entropy	✓	✓	✓	✓	×	✓	×
13	Periodicity	✓	×	✓	✓	×	×	×
14	Efficiency	✓	✓	✓	✓	✓	✓	✓
15	Comparison	✓	✓	✓	✓	×	×	×

this linear complexity test is just the frequency subtest of NIST SP800-22, where 1000 binary sequences with length 10^6-bit (produced by our PRNG) have been already tested extensively with results summarized in Table 2.

6 Promotion of the 3D CML model

According to the performance analyses of the 3D CML model in section 3, it is well known as a higher-dimensional chaotic for constructing numerous cryptographic schemes. With the increasing demand for security, and also in order to apply to more application scenarios in the future, the 3D CML model can be extended into the ND CML one, which is shown in definition 2.

Definition 2 The N-dimensional CML model is defined as

$$\begin{aligned} x_{n+1}^{l_1,l_2,\cdots,l_{N-1},l_N} &= (1-\varepsilon)\mathrm{F}(x_n^{l_1,l_2,\cdots,l_{N-1},l_N}) \\ &+ \frac{\varepsilon}{2N}\Big[\mathrm{F}(x_n^{l_1+1,l_2,\cdots,l_{N-1},l_N}) + \mathrm{F}(x_n^{l_1-1,l_2,\cdots,l_{N-1},l_N}) \\ &+\mathrm{F}(x_n^{l_1,l_2+1,\cdots,l_{N-1},l_N}) + \mathrm{F}(x_n^{l_1,l_2-1,\cdots,l_{N-1},l_N}) \\ &+\cdots+\mathrm{F}(x_n^{l_1,l_2,\cdots,l_{N-1}+1,l_N}) + \mathrm{F}(x_n^{l_1,l_2,\cdots,l_{N-1}-1,l_N}) \\ &+\mathrm{F}(x_n^{l_1,l_2,\cdots,l_{N-1},l_N+1}) + \mathrm{F}(x_n^{l_1,l_2,\cdots,l_{N-1},l_N-1})\Big]. \end{aligned} \tag{18}$$

where $l_1 = 1,2,\cdots,L_1$, $l_2 = 1,2,\cdots,L_2$, $\cdots$, $l_{N-1} = 1,2,\cdots,L_{N-1}$ and $l_N = 1,2,\cdots,L_N$ are the indexes of all the nodes, respectively.

According to LE results of the 3D CML model, the significant theoretical results for LE can be conjectured as the following equation.

$$\begin{aligned} \mathrm{LE} =& \mathrm{LE_F} + \ln\Big|1-\varepsilon+\frac{\varepsilon}{N}(\cos\frac{2\pi k_1}{L_1}+\cos\frac{2\pi k_2}{L_2} \\ &+\cdots+\cos\frac{2\pi k_{N-1}}{L_{N-1}}+\cos\frac{2\pi k_N}{L_N})\Big|. \end{aligned} \tag{19}$$

To veridate the conclusion of Eq. (19) is correct, the details are represented as in the following proof.

Proof See the appendix B. □

According to the appendix B, it is clear Eq. (19) is correct, we can get the following important theorem.

Theorem 4 *The maximum Lyapunov exponent (MLE) of the ND CML model is solely determined by the local chaotic map.*

Proof For Eq. (19), satisfying $k_1 = 0, k_2 = 0, \cdots, k_{N-1} = 0, k_N = 0$, the MLE of the ND CML model is calculated as

$$\begin{aligned} \mathrm{LE_{MLE}} &= \mathrm{LE_F} + \ln\Big|1-\varepsilon+\frac{\varepsilon}{N}(\cos 0+\cos 0 \\ &\quad +\cdots+\cos 0+\cos 0|, \\ &= \mathrm{LE_F}. \end{aligned} \tag{20}$$

□

This important conclusion for LE in the ND CML model is obtained according to the process of 3D CML model, the LE values of the ND CML model can be calculated accurately, the model parameters would be set reasonably to keep the model in the fully chaotic state. Furthermore, the dynamic performance of the ND CML model is related to the security of chaotic-based cyrptographic schemes. Therefore, it is greatly beneficial to the application of the ND CML model.

7 Conclusion

The 3D CML model, as a higher-dimensional chaotic system, owns some special chaotic dynamic behavior, as well as more complicated peformance than 1D CML and 2D CML. Its mathematical expression of LE is derived, which is significantly used to set the parameters of 3D CML and ensure the model is in a fully chaotic state. Meanwhile, the synchronization stability expression of the 3D CML is given, this devotes itself to the suitable parameters for avoiding the synchronous state. The LE and synchronization stability analyses in the 3D CML model give new insights, as well as provide a theoretical foundation in cryptographic application. Based on those theoretical results, our PRNG scheme is designed, the simulation demonstrates our scheme possesses outstanding performance. In our scheme, massive bits are produced efficiently, it is suitable for lightwight devices. In fact, in scenarios where security requirements are not too high, the 3D CML model with the local Logistic map is a good choice, since Logistic map is faster than PLM, but the security is lower than PLM's. In the future, the cryptographic application of the 3D CML model with different local map will be the focus area via scenarios with different levels of security, especially, for the chaos-based encryption schemes of massive images. Furthermore, the 3D CML model is extended into a

ND CML one, its LE expression is obtained, it is substantial helpful for theoretical research and application development of the higher-dimensional model.

Author contributions All authors contributed to the study conception and design. Material preparation, data collection and analysis were performed by Zhuo Liu, Yong Wang and Jinyuan Liu. The first draft of the manuscript was written by Zhuo Liu and all authors commented on previous versions of the manuscript. All authors read and approved the final manuscript.

Funding This research is supported by General Program of the National Natural Science Foundation of China (no.62272077), the Science and Technology Foundation Project of Guizhou Province (QianKeHeJiChu-ZK[2022]YiBan329, QianKeHe JiChu-ZK[2022]YiBan331), Reward and subsidy fund proje - ct of Guizhou Education University, Ministry of science and technology of the people's Republic of China and National Natural Science Foundation of China(2023GZJB011), Science Research Foundation Project of Guizhou Normal University (Xiao2023014 and Xiao2024064).

Data Availibility All data generated or analyzed during this study are included in this published article.

Declarations

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

Appendix A

The proof details of theorem 2 in the 3D CML model are shown as

Proof To begin with, the 3D CML model is converted into a one-dimensional CML as Eq. (21)

$$\begin{aligned} x_{n+1}^{(s-1)L+t+(u-1)RL} &= (1-\varepsilon)\mathrm{F}(x_n^{(s-1)L+t+(u-1)RL}) \\ &+ \frac{\varepsilon}{6}\Big[\mathrm{F}(x_n^{sL+t+(u-1)RL} + \mathrm{F}(x_n^{(s-2)L+t+(u-1)RL} \\ &+ \mathrm{F}(x_n^{(s-1)L+t+1+(u-1)RL} + \mathrm{F}(x_n^{(s-1)L+t-1+(u-1)RL} \\ &+ \mathrm{F}(x_n^{(s-1)L+t+(u-2)RL} + \mathrm{F}(x_n^{(s-1)L+t+uRL}\Big]. \end{aligned} \tag{21}$$

and the periodic boundary conditions are rewritten as

$$\begin{aligned} x_n^{(s-1)L+t+(u-1)RL} &= x_n^{(s-1+R)L+t+(u-1)RL}, \\ x_n^{(s-1)L+t+(u-1)RL} &= x_n^{(s-1+R)L+t+L+(u-1)RL}, \\ x_n^{(s-1)L+t+(u-1)RL} &= x_n^{(s-1+R)L+t+L+(u-1+U)RL}. \end{aligned} \tag{22}$$

The 3D CML model can be expressed as an $R \times L \times U$ dimensional column vector

$$\begin{aligned} \mathbf{z}_n = \Big[&x_n^1, x_n^2, \cdots, x_n^L, x_n^{L+1}, \cdots, x_n^{2L}, \cdots, \\ &x_n^{R\times L}, x_n^{R\times L+1}, \cdots, x_n^{R\times L\times U}\Big]. \end{aligned}$$

Assume that all the nodes of the 3D CML model keep the synchronization state among them, so

$$\begin{aligned} x_n^1 = x_n^2 = \cdots = x_n^L = x_n^{L+1} = \cdots = x_n^{2L} \\ = \cdots = x_n^{R\times L} = x_n^{R\times L+1} = \cdots = x_n^{R\times L\times U}. \end{aligned} \tag{23}$$

Then, we can obtain the derivatives of F as

$$\begin{aligned} &\mathrm{F}'(x_n^{(s-1)L+t+(u-1)RL}) = \mathrm{F}'(x_n^{(sL+t+(u-1)RL}) \\ &= \mathrm{F}'(x_n^{(s-2)L+t+(u-1)RL}) = \mathrm{F}'(x_n^{(s-1)L+t+1+(u-1)RL}) \\ &= \mathrm{F}'(x_n^{(s-1)L+t-1+(u-1)RL}) = \mathrm{F}'(x_n^{(s-1)L+t+(u-2)RL}) \\ &= \mathrm{F}'(x_n^{(s-1)L+t+uRL}) = \mathrm{F}'(n). \end{aligned} \tag{24}$$

and the differentials of Eq. (21) are

$$\begin{aligned} &\delta(x_{n+1}^{(s-1)L+t+(u-1)RL}) = \\ &(1-\varepsilon)\mathrm{F}'(x_n^{(s-1)L+t+(u-1)RL})\delta x_n^{(s-1)L+t+(u-1)RL} \\ &+ \frac{\varepsilon}{6}\Big[\mathrm{F}'(x_n^{sL+t+(u-1)RL})\delta x_n^{sL+t+(u-1)RL} \\ &+ \mathrm{F}'(x_n^{(s-2)L+t+(u-1)RL})\delta x_n^{(s-2)L+t+(u-1)RL} \\ &+ \mathrm{F}'(x_n^{(s-1)L+t+1+(u-1)RL})\delta x_n^{(s-1)L+t+1+(u-1)RL} \\ &+ \mathrm{F}'(x_n^{(s-1)L+t-1+(u-1)RL})\delta x_n^{(s-1)L+t-1+(u-1)RL} \\ &+ \mathrm{F}'(x_n^{(s-1)L+t+uRL})\delta x_n^{(s-1)L+t+uRL} \\ &+ \mathrm{F}'(x_n^{(s-1)L+t+(u-2)RL})\delta x_n^{(s-1)L+t+(u-2)RL}\Big]. \end{aligned} \tag{25}$$

Furthermore, based on Eq. (24), Eq. (25) is simplified as

$$\begin{aligned} \delta(x_{n+1}^{(s-1)L+t+(u-1)RL}) &= \mathrm{F}'(n)\Big\{(1-\varepsilon)\delta x_n^{(s-1)L+t+(u-1)RL} \\ &+ \frac{\varepsilon}{6}\Big[\delta x_n^{sL+t+(u-1)RL} + \delta x_n^{(s-2)L+t+(u-1)RL} \\ &+ \delta x_n^{(s-1)L+t+1+(u-1)RL} + \delta x_n^{(s-1)L+t-1+(u-1)RL} \\ &+ \delta x_n^{(s-1)L+t+(u-2)RL} + \delta x_n^{(s-1)L+t+uRL}\Big]\Big\}. \end{aligned} \tag{26}$$

Then, considering the position relation among the nodes of 3D CML, according to Eqs. (24) and (26), we have the Jacobin matrix for $\delta\mathbf{z}_{n+1} = \mathbf{J}_n\mathbf{z}_n$ as

$$\mathbf{J}_n = \mathrm{F}'(x_n)\mathbf{K}, \tag{27}$$

where $\mathbf{K}$ is a $RLU \times RLU$ block circulant matrix defined as

$$\mathbf{K} = \begin{bmatrix} \mathbf{G}_1 & \mathbf{G}_2 & \cdots & \mathbf{G}_U \\ \mathbf{G}_U & \mathbf{G}_1 & \cdots & \mathbf{G}_{U-1} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{G}_2 & \mathbf{G}_3 & \cdots & \mathbf{G}_1 \end{bmatrix},$$

in $\mathbf{K}$, $\mathbf{G}_1, \mathbf{G}_2, \cdots, \mathbf{G}_{U-1}, \mathbf{G}_U$ with $RL \times RL$ are shown as

$$\mathbf{G}_1 = \begin{bmatrix} \mathbf{A}_1 & \mathbf{A}_2 & \cdots & \mathbf{A}_R \\ \mathbf{A}_R & \mathbf{A}_1 & \ddots & \mathbf{A}_{R-1} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{A}_2 & \mathbf{A}_3 & \cdots & \mathbf{A}_1 \end{bmatrix},$$

$$\mathbf{G}_2 = \begin{bmatrix} \mathbf{A}_2 & & \\ & \ddots & \\ & & \mathbf{A}_2 \end{bmatrix}, \mathbf{G}_R = \begin{bmatrix} \mathbf{A}_R & & \\ & \ddots & \\ & & \mathbf{A}_R \end{bmatrix},$$

and

$$\mathbf{G}_3 = \mathbf{G}_4 = \cdots = \mathbf{G}_{R-1} = \mathbf{0},$$

Among them,

$$\mathbf{A}_1 = \begin{bmatrix} 1-\varepsilon & \frac{\varepsilon}{6} & 0 & \cdots & \frac{\varepsilon}{6} \\ \frac{\varepsilon}{6} & 1-\varepsilon & \frac{\varepsilon}{6} & \ddots & 0 \\ 0 & \frac{\varepsilon}{6} & 1-\varepsilon & \ddots & 0 \\ \vdots & \vdots & \ddots & \ddots & \frac{\varepsilon}{6} \\ \frac{\varepsilon}{6} & 0 & \cdots & \frac{\varepsilon}{6} & 1-\varepsilon \end{bmatrix},$$

$$\mathbf{A}_2 = \mathbf{A}_R = \begin{bmatrix} \frac{\varepsilon}{6} & & \\ & \ddots & \\ & & \frac{\varepsilon}{6} \end{bmatrix},$$

and

$$\mathbf{A}_3 = \mathbf{A}_4 = \cdots = \mathbf{A}_{R-1} = \mathbf{0}.$$

Set $\mathbf{G} = \mathbf{J}_1 \times \mathbf{J}_2 \times \cdots \times \mathbf{J}_n = \mathbf{K}^n \prod_{i=1}^{n} \mathrm{F}'(x)$, and the eigenvalue of $\mathbf{K}$ is λ. So, the eigenvalue of $\mathbf{G}$ is $\lambda^n \prod_{i=1}^{n} \mathrm{F}'(x)$ and its norm is $|\lambda|^n \left| \prod_{m=1}^{n} \mathrm{F}'(x_m) \right|$, the LE of 3D CML is formulated as

$$\begin{aligned} \mathrm{LE} &= \lim_{n\to\infty} \frac{1}{n} \ln \left| |\lambda|^n \prod_{m=1}^{n} \mathrm{F}'(x_m) \right| \\ &= \lim_{n\to\infty} \frac{1}{n} \ln \left| \prod_{m=1}^{n} \mathrm{F}'(x_m) \right| + \ln|\lambda|. \end{aligned} \tag{28}$$

Moreover, $\mathbf{K}$ is a block circulant matrix and $\mathbf{G}_3 = \mathbf{G}_4 = \cdots = \mathbf{G}_{U-1} = \mathbf{0}$, its eigenpolynomial are given as

$$\prod_{r=1}^{U} \left| \mathbf{G}_1 + \mathbf{G}_2\omega_k + \mathbf{G}_U\omega_k^{U-1} - \lambda\mathbf{E} \right|, \tag{29}$$

where $k = 0, 1, 2, \cdots, U-1$, $\mathbf{E}$ is an identity matrix and $\omega_k = \cos(\frac{2\pi k}{U}) + i\sin(\frac{2\pi k}{U})$.

Then, let $\mathbf{A} = \mathbf{G}_1 + \mathbf{G}_2\omega_k + \mathbf{G}_U\omega_k^{U-1} - \lambda\mathbf{E}$, and it is represented as

$$\mathbf{A} = \begin{bmatrix} \mathbf{A}_1' & \mathbf{A}_2 & \cdots & \mathbf{A}_R \\ \mathbf{A}_R & \mathbf{A}_1' & \ddots & \mathbf{A}_{R-1} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{A}_2 & \mathbf{A}_3 & \cdots & \mathbf{A}_1' \end{bmatrix},$$

where

$$\mathbf{A}_1' = \begin{bmatrix} P & \frac{\varepsilon}{6} & 0 & \cdots & \frac{\varepsilon}{6} \\ \frac{\varepsilon}{6} & P & \frac{\varepsilon}{6} & \ddots & 0 \\ 0 & \frac{\varepsilon}{6} & P & \ddots & 0 \\ \vdots & \vdots & \ddots & \ddots & \frac{\varepsilon}{6} \\ \frac{\varepsilon}{6} & 0 & 0 & \cdots & P \end{bmatrix}, \mathbf{A}_2 = \mathbf{A}_R = \begin{bmatrix} \frac{\varepsilon}{6} & & \\ & \ddots & \\ & & \frac{\varepsilon}{6} \end{bmatrix},$$

and

$$\mathbf{A}_3 = \mathbf{A}_4 = \cdots = \mathbf{A}_{R-1} = \mathbf{0},$$

where $P = 1 - \varepsilon + \frac{\varepsilon}{6}\omega_k + \mathbf{G}_k\omega_k^{U-1} - \lambda$.

Since $\mathbf{A}$ is a block circulant matrix, its eigen polynomial are shown as

$$\prod_{k=1}^{R}\prod_{r=1}^{U} \left| \mathbf{A}_1' + \mathbf{A}_2\omega_k + \mathbf{A}_U\omega_k^{U-1} + \mathbf{A}_2\omega_r + \mathbf{A}_U\omega_r^{R-1} - \lambda\mathbf{E} \right|, \tag{30}$$

where $\omega_r = \cos(\frac{2\pi r}{R}) + i\sin(\frac{2\pi r}{R})$. According to the above-mentioned analysis, the eigenvalues of $\mathbf{K}$ are obtained as

$$\begin{aligned} \lambda = {} & 1 - \varepsilon + \frac{\varepsilon}{6}\omega_k + \frac{\varepsilon}{6}\omega_k^{U-1} + \frac{\varepsilon}{6}\omega_r + \frac{\varepsilon}{6}\omega_r^{R-1} \\ & + \frac{\varepsilon}{6}\omega_l + \frac{\varepsilon}{6}\omega_l^{L-1}, \end{aligned} \tag{31}$$

where $\omega_l = \cos(\frac{2\pi l}{L}) + i\sin(\frac{2\pi l}{L})$.

Substituting Eq. (31) into Eq. (28), we can get the LEs of 3D CML as

$$\mathrm{LE} = \mathrm{LE}_\mathrm{F} + \ln \left| 1 - \varepsilon + \frac{\varepsilon}{3}(\cos\frac{2\pi k}{U} + \cos\frac{2\pi r}{R} + \cos\frac{2\pi l}{L}) \right|, \tag{32}$$

□

Appendix B

The proof details of theorem 4 in the ND CML model are represented as

Proof To begin with, the ND CML model is transformed into a one-dimensional one as Eq. (33)

$$\begin{aligned}
&x_{n+1}^{(l_1-1)L_2+l_2+\cdots+l_{N-1}+(l_N-1)L_1L_2\cdots L_{N-1}}\\
&=(1-\varepsilon)\mathrm{F}(x_n^{(l_1-1)L_2+l_2+\cdots+l_{N-1}+(l_N-1)L_1L_2\cdots L_{N-1}})\\
&+\frac{\varepsilon}{2N}\Big[\mathrm{F}(x_n^{l_1L_2+l_2+\cdots+l_{N-1}+(l_N-1)L_1L_2\cdots L_{N-1}})\\
&+\mathrm{F}(x_n^{(l_1-2)L_2+l_2+\cdots+l_{N-1}+(l_N-1)L_1L_2\cdots L_{N-1}})\\
&+\mathrm{F}(x_n^{(l_1-1)L_2+l_2-1+\cdots+l_{N-1}+(l_N-1)L_1L_2\cdots L_{N-1}})\\
&+\mathrm{F}(x_n^{(l_1-1)L_2+l_2+1+\cdots+l_{N-1}+(l_N-1)L_1L_2\cdots L_{N-1}})\\
&+\cdots+\mathrm{F}(x_n^{(l_1-1)L_2+l_2+\cdots+l_{N-1}-1+(l_N-1)L_1L_2\cdots L_{N-1}}\\
&+\mathrm{F}(x_n^{(l_1-1)L_2+l_2+\cdots+l_{N-1}+1+(l_N-1)L_1L_2\cdots L_{N-1}})\\
&+\mathrm{F}(x_n^{(l_1-1)L_2+l_2+\cdots+l_{N-1}+l_NL_1L_2\cdots L_{N-1}})\\
&+\mathrm{F}(x_n^{(l_1-1)L_2+l_2+\cdots+l_{N-1}+(l_N-2)L_1L_2\cdots L_{N-1}})\Big].
\end{aligned}\tag{33}$$

and its periodic boundary conditions are changed into

$$\begin{aligned}
&x_n^{(l_1-1)L_2+l_2+\cdots+l_{N-1}+(l_N-1)L_1L_2\cdots L_{N-1}}\\
&=x_n^{(l_1-1+L_1)L_2+l_2+\cdots+l_{N-1}+(l_N-1)L_1L_2\cdots L_{N-1}},\\
&x_n^{(l_1-1)L_2+l_2+\cdots+l_{N-1}+(l_N-1)L_1L_2\cdots L_{N-1}}\\
&=x_n^{(l_1+L_1-1)L_2+l_2+L_2+\cdots+l_{N-1}+(l_N-1)L_1L_2\cdots L_{N-1}},\\
&\cdots\\
&x_n^{(l_1-1)L_2+l_2+\cdots+l_{N-1}+(l_N-1)L_1L_2\cdots L_{N-1}}\\
&=x_n^{(l_1+L_1-1)L_2+l_2+L_2+\cdots+l_{N-1}+L_{N-1}+(l_N-1)L_1L_2\cdots L_{N-1}},\\
&x_n^{(l_1-1)L_2+l_2+\cdots+l_{N-1}+(l_N-1)L_1L_2\cdots L_{N-1}}\\
&=x_n^{(l_1+L_1-1)L_2+l_2+L_2+\cdots+l_{N-1}+L_{N-1}+(l_N+L_N-1)L_1L_2\cdots L_{N-1}}.
\end{aligned}\tag{34}$$

The ND CML model can be shown as a $L_1\times L_2\cdots\times L_{N-1}\times L_N$ dimensional column vector

$$\begin{aligned}
\mathbf{z}_n=\Big[&x_n^1,x_n^2,\cdots,x_n^{L_1},x_n^{L_1+1},\cdots,x_n^{2L_1},\cdots,x_n^{L_1\times L_2},\\
&x_n^{L_1\times L_2+1},\cdots,x_n^{L_1\times L_2\times\cdots\times L_{N-1}\times L_N}\Big].
\end{aligned}$$

Assume that all the nodes of the ND CML model keep the synchronization state among them, so

$$\begin{aligned}
x_n^1&=x_n^2=\cdots=x_n^{L_1}=x_n^{L_1+1}=\cdots=x_n^{2L_1}=\cdots\\
&=x_n^{L_1\times L_2}=x_n^{L_1\times L_2+1}\\
&=\cdots=x_n^{L_1\times L_2\times\cdots\times L_{N-1}\times L_N}.
\end{aligned}\tag{35}$$

Then, we can obtain the derivatives of F as

$$\begin{aligned}
&\mathrm{F}'(x_n^{(l_1-1)L_2+l_2+\cdots+l_{N-1}+(l_N-1)L_1L_2\cdots L_{N-1}})\\
&=\mathrm{F}'(x_n^{l_1L_2+l_2+\cdots+l_{N-1}+(l_N-1)L_1L_2\cdots L_{N-1}})\\
&=\mathrm{F}'(x_n^{(l_1-2)L_2+l_2+\cdots+l_{N-1}+(l_N-1)L_1L_2\cdots L_{N-1}})\\
&=\mathrm{F}'(x_n^{(l_1-1)L_2+l_2-1+\cdots+l_{N-1}+(l_N-1)L_1L_2\cdots L_{N-1}})\\
&=\mathrm{F}'(x_n^{(l_1-1)L_2+l_2+1+\cdots+l_{N-1}+(l_N-1)L_1L_2\cdots L_{N-1}})\\
&=\cdots=\mathrm{F}'(x_n^{(l_1-1)L_2+l_2+\cdots+l_{N-1}-1+(l_N-1)L_1L_2\cdots L_{N-1}})\\
&=\mathrm{F}'(x_n^{(l_1-1)L_2+l_2+\cdots+l_{N-1}+1+(l_N-1)L_1L_2\cdots L_{N-1}})\\
&=\mathrm{F}'(x_n^{(l_1-1)L_2+l_2+\cdots+l_{N-1}+1+l_NL_1L_2\cdots L_{N-1}})\\
&=\mathrm{F}'(x_n^{(l_1-1)L_2+l_2+\cdots+l_{N-1}+1+(l_N-2)L_1L_2\cdots L_{N-1}})\\
&=\mathrm{F}'(n).
\end{aligned}\tag{36}$$

and the differentials of Eq. (33) are

$$\begin{aligned}
&\delta(x_{n+1}^{(l_1-1)L_2+l_2+\cdots+l_{N-1}+(l_N-1)L_1L_2\cdots L_{N-1}})=\\
&(1-\varepsilon)\mathrm{F}'(x_n^{(l_1-1)L_2+l_2+\cdots+l_{N-1}+(l_N-1)L_1L_2\cdots L_{N-1}})\\
&\delta x_n^{(l_1-1)L_2+l_2+\cdots+l_{N-1}+(l_N-1)L_1L_2\cdots L_{N-1}}\\
&+\frac{\varepsilon}{2N}\Big[\mathrm{F}'(x_n^{l_1L_2+l_2+\cdots+l_{N-1}+(l_N-1)L_1L_2\cdots L_{N-1}})\\
&\delta x_n^{l_1L_2+l_2+\cdots+l_{N-1}+(l_N-1)L_1L_2\cdots L_{N-1}}\\
&+\mathrm{F}'(x_n^{(l_1-2)L_2+l_2+\cdots+l_{N-1}+(l_N-1)L_1L_2\cdots L_{N-1}})\\
&\delta x_n^{(l_1-2)L_2+l_2+\cdots+l_{N-1}+(l_N-1)L_1L_2\cdots L_{N-1}}\\
&+\mathrm{F}'(x_n^{(l_1-1)L_2+l_2-1+\cdots+l_{N-1}+(l_N-1)L_1L_2\cdots L_{N-1}})\\
&\delta x_n^{(l_1-1)L_2+l_2-1+\cdots+l_{N-1}+(l_N-1)L_1L_2\cdots L_{N-1}}\\
&+\mathrm{F}'(x_n^{(l_1-1)L_2+l_2+1+\cdots+l_{N-1}+(l_N-1)L_1L_2\cdots L_{N-1}})\\
&\delta x_n^{(l_1-1)L_2+l_2+1+\cdots+l_{N-1}+(l_N-1)L_1L_2\cdots L_{N-1}}\\
&+\cdots+\mathrm{F}'(x_n^{(l_1-1)L_2+l_2+1+\cdots+l_{N-1}-1+(l_N-1)L_1L_2\cdots L_{N-1}})\\
&\delta x_n^{(l_1-1)L_2+l_2+1+\cdots+l_{N-1}-1+(l_N-1)L_1L_2\cdots L_{N-1}}\\
&+\mathrm{F}'(x_n^{(l_1-1)L_2+l_2+1+\cdots+l_{N-1}+1+(l_N-1)L_1L_2\cdots L_{N-1}})\\
&\delta x_n^{(l_1-1)L_2+l_2+1+\cdots+l_{N-1}+1+(l_N-1)L_1L_2\cdots L_{N-1}}\\
&+\mathrm{F}'(x_n^{(l_1-1)L_2+l_2+1+\cdots+l_{N-1}-1+l_NL_1L_2\cdots L_{N-1}})\\
&\delta x_n^{(l_1-1)L_2+l_2+1+\cdots+l_{N-1}-1+l_NL_1L_2\cdots L_{N-1}}\\
&+\mathrm{F}'(x_n^{(l_1-1)L_2+l_2+1+\cdots+l_{N-1}-1+(l_N-2)L_1L_2\cdots L_{N-1}})\\
&\delta x_n^{(l_1-1)L_2+l_2+1+\cdots+l_{N-1}-1+(l_N-2)L_1L_2\cdots L_{N-1}}\Big].
\end{aligned}\tag{37}$$

Furthermore, based on Eq. (36), Eq. (37) is simplified as

$$\begin{aligned}
&\delta(x_{n+1}^{(l_1-1)L_2+l_2+\cdots+l_{N-1}+(l_N-1)L_1L_2\cdots L_{N-1}})\\
&=\mathrm{F}'(n)\Big\{(1-\varepsilon)\delta x_n^{(l_1-1)L_2+l_2+\cdots+l_{N-1}+(l_N-1)L_1L_2\cdots L_{N-1}}\\
&+\frac{\varepsilon}{2N}\Big[\delta x_n^{l_1L_2+l_2+\cdots+l_{N-1}+(l_N-1)L_1L_2\cdots L_{N-1}}\\
&+\delta x_n^{(l_1-2)L_2+l_2+\cdots+l_{N-1}+(l_N-1)L_1L_2\cdots L_{N-1}}\\
&+\delta x_n^{(l_1-1)L_2+l_2-1+\cdots+l_{N-1}+(l_N-1)L_1L_2\cdots L_{N-1}}\\
&+\delta x_n^{(l_1-1)L_2+l_2+1+\cdots+l_{N-1}+(l_N-1)L_1L_2\cdots L_{N-1}}\\
&+\cdots+\delta x_n^{(l_1-1)L_2+l_2+\cdots+l_{N-1}-1+(l_N-1)L_1L_2\cdots L_{N-1}}\\
&+\delta x_n^{(l_1-1)L_2+l_2+\cdots+l_{N-1}+1+(l_N-1)L_1L_2\cdots L_{N-1}}\\
&+\delta x_n^{(l_1-1)L_2+l_2+\cdots+l_{N-1}-1+l_NL_1L_2\cdots L_{N-1}}\\
&+\delta x_n^{(l_1-1)L_2+l_2+\cdots+l_{N-1}+1+(l_N-2)L_1L_2\cdots L_{N-1}}\Big]\Big\}.
\end{aligned}\tag{38}$$

Then, considering the position relation among the nodes of ND CML, according to Eqs. (36) and (38), we have the Jacobin matrix for $\delta\mathbf{z}_{n+1}=\mathbf{J}_n\mathbf{z}_n$ as

$$\mathbf{J}_n=\mathrm{F}'(x_n)\mathbf{K},\tag{39}$$

where $\mathbf{K}$ is a $(L_1L_2\cdots L_{N-1}L_N)\times(L_1L_2\cdots L_{N-1}L_N)$ block circulant matrix defined as

$$\mathbf{K}=\begin{bmatrix}\mathbf{G}_1 & \mathbf{G}_2 & \cdots & \mathbf{G}_{L_{N-1}}\\ \mathbf{G}_{L_{N-1}} & \mathbf{G}_1 & \cdots & \mathbf{G}_{L_{N-1}-1}\\ \vdots & \vdots & \ddots & \vdots\\ \mathbf{G}_2 & \mathbf{G}_3 & \cdots & \mathbf{G}_1\end{bmatrix},$$

in $\mathbf{K}$, $\mathbf{G}_1,\mathbf{G}_2,\cdots,\mathbf{G}_{L_{N-1}},\mathbf{G}_{L_N}$ with $(L_1L_2\cdots L_{N-1})\times(L_1L_2\cdots L_{N-1})$ are shown as

$$\mathbf{G}_1=\begin{bmatrix}\mathbf{A}_1 & \mathbf{A}_2 & \cdots & \mathbf{A}_{L_{N-2}}\\ \mathbf{A}_{L_{N-2}} & \mathbf{A}_1 & \ddots & \mathbf{A}_{L_{N-2}-1}\\ \vdots & \vdots & \ddots & \vdots\\ \mathbf{A}_2 & \mathbf{A}_3 & \cdots & \mathbf{A}_1\end{bmatrix},$$

$$\mathbf{G}_2=\begin{bmatrix}\mathbf{A}_2 & & \\ & \ddots & \\ & & \mathbf{A}_2\end{bmatrix},\ \mathbf{G}_{L_{N-2}}=\begin{bmatrix}\mathbf{A}_{L_{N-2}} & & \\ & \ddots & \\ & & \mathbf{A}_{L_{N-2}}\end{bmatrix},$$

and

$$\mathbf{G}_3=\mathbf{G}_4=\cdots=\mathbf{G}_{L_{N-1}-1}=\mathbf{0},$$

Among them, $\mathbf{A}_1$ with $(L_1L_2\cdots L_{N-2})\times(L_1L_2\cdots L_{N-2})$ are shown as

$$\mathbf{A_1}=\begin{bmatrix}\mathbf{T}_1 & \mathbf{T}_2 & \cdots & \mathbf{T}_{L_{N-3}}\\ \mathbf{T}_{L_{N-3}} & \mathbf{T}_1 & \cdots & \mathbf{T}_{L_{N-3}-1}\\ \vdots & \vdots & \ddots & \vdots\\ \mathbf{T}_2 & \mathbf{T}_3 & \cdots & \mathbf{T}_1\end{bmatrix},$$

in $\mathbf{A}_1$, $\mathbf{T}_1,\mathbf{T}_2,\cdots,\mathbf{T}_{L_{N-1}},\mathbf{T}_{L_N}$ with $(L_1L_2\cdots L_{N-3})\times(L_1L_2\cdots L_{N-3})$ are shown as

$$\mathbf{T}_1=\begin{bmatrix}\mathbf{B}_1 & \mathbf{B}_2 & \cdots & \mathbf{B}_{L_{N-4}}\\ \mathbf{B}_{L_{N-4}} & \mathbf{B}_1 & \ddots & \mathbf{B}_{L_{N-4}-1}\\ \vdots & \vdots & \ddots & \vdots\\ \mathbf{B}_2 & \mathbf{B}_3 & \cdots & \mathbf{B}_1\end{bmatrix},$$

$$\mathbf{T}_2=\begin{bmatrix}\mathbf{B}_2 & & \\ & \ddots & \\ & & \mathbf{B}_2\end{bmatrix},\ \mathbf{T}_{L_{N-4}}=\begin{bmatrix}\mathbf{B}_{L_{N-4}} & & \\ & \ddots & \\ & & \mathbf{B}_{L_{N-4}}\end{bmatrix},$$

and

$$\mathbf{T}_3=\mathbf{T}_4=\cdots=\mathbf{T}_{L_{N-4}-1}=\mathbf{0},$$

Iterate $\mathbf{T_1}$ for N times, the last iteration result is shown as

$$\mathbf{C}_1=\begin{bmatrix}1-\varepsilon & \frac{\varepsilon}{2N} & 0 & \cdots & \frac{\varepsilon}{2N}\\ \frac{\varepsilon}{2N} & 1-\varepsilon & \frac{\varepsilon}{2N} & \ddots & 0\\ 0 & \frac{\varepsilon}{2N} & 1-\varepsilon & \ddots & 0\\ \vdots & \vdots & \ddots & \ddots & \frac{\varepsilon}{2N}\\ \frac{\varepsilon}{2N} & 0 & \cdots & \frac{\varepsilon}{2N} & 1-\varepsilon\end{bmatrix},$$

$$\mathbf{C}_2=\mathbf{C}_{L_1}=\begin{bmatrix}\frac{\varepsilon}{2N} & & \\ & \ddots & \\ & & \frac{\varepsilon}{2N}\end{bmatrix},$$

and

$$\mathbf{C}_3=\mathbf{C}_4=\cdots=\mathbf{C}_{L_1-1}=\mathbf{0}.$$

Set $\mathbf{G}=\mathbf{J}_1\times\mathbf{J}_2\times\cdots\times\mathbf{J}_n=\mathbf{K}^n\prod_{i=1}^{n}\mathrm{F}'(x)$, and the eigenvalue of $\mathbf{K}$ is λ. So, the eigenvalue of $\mathbf{G}$ is $\lambda^n\prod_{i=1}^{n}\mathrm{F}'(x)$ and its norm is $|\lambda|^n\left|\prod_{m=1}^{n}\mathrm{F}'(x_m)\right|$, the LE of 3D CML is formulated as

$$\begin{aligned}\mathrm{LE}&=\lim_{n\to\infty}\frac{1}{n}\ln\left||\lambda|^n\prod_{m=1}^{n}\mathrm{F}'(x_m)\right|\\&=\lim_{n\to\infty}\frac{1}{n}\ln\left|\prod_{m=1}^{n}\mathrm{F}'(x_m)\right|+\ln|\lambda|.\end{aligned}\tag{40}$$

Moreover, $\mathbf{K}$ is a block circulant matrix and $\mathbf{G}_3=\mathbf{G}_4=\cdots=\mathbf{G}_{L_{N-1}-1}=\mathbf{0}$, its eigenpolynomial are given as

$$\prod_{k_{N-1}=1}^{L_{N-1}} \left| \mathbf{G}_1 + \mathbf{G}_2\omega_{k_{N-1}} + \mathbf{G}_{L_{N-1}}\omega_{k_{N-1}}^{L_{N-1}-1} - \lambda\mathbf{E} \right|, \tag{41}$$

where $k_{N-1} = 0, 1, 2, \cdots, L_{N-1}-1$, $\mathbf{E}$ is an identity matrix and $\omega_{k_{N-1}} = \cos(\frac{2\pi k_{N-1}}{L_{N-1}}) + i\sin(\frac{2\pi k_{N-1}}{L_{N-1}})$. Then, let $\mathbf{A} = \mathbf{G}_1 + \mathbf{G}_2\omega_{k_{N-1}} + \mathbf{G}_{L_{N-1}}\omega_{k_{N-1}}^{L_{N-1}-1} - \lambda\mathbf{E}$, and it is represented as

$$\mathbf{A} = \begin{bmatrix} \mathbf{A}_1' & \mathbf{A}_2 & \cdots & \mathbf{A}_{L_{N-2}} \\ \mathbf{A}_{L_{N-2}} & \mathbf{A}_1' & \ddots & \mathbf{A}_{L_{N-2}-1} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{A}_2 & \mathbf{A}_3 & \cdots & \mathbf{A}_1' \end{bmatrix},$$

where

$$\mathbf{A}_1' = \begin{bmatrix} P & \frac{\varepsilon}{2N} & 0 & \cdots & \frac{\varepsilon}{2N} \\ \frac{\varepsilon}{2N} & P & \frac{\varepsilon}{2N} & \ddots & 0 \\ 0 & \frac{\varepsilon}{2N} & P & \ddots & 0 \\ \vdots & \vdots & \ddots & \ddots & \frac{\varepsilon}{2N} \\ \frac{\varepsilon}{2N} & 0 & 0 & \cdots & P \end{bmatrix},$$

$$\mathbf{A}_2 = \mathbf{A}_{L_{N-2}} = \begin{bmatrix} \frac{\varepsilon}{2N} & & \\ & \ddots & \\ & & \frac{\varepsilon}{2N} \end{bmatrix},$$

and

$$\mathbf{A}_3 = \mathbf{A}_4 = \cdots = \mathbf{A}_{L_{N-2}-1} = \mathbf{0},$$

where

$$P = 1 - \varepsilon + \frac{\varepsilon}{2N}\omega_{k_1} + \mathbf{G}_{k_1}\omega_{k_1}^{L_1-1} + \cdots + \frac{\varepsilon}{2N}\omega_{k_{N-2}} + \mathbf{G}_{k_{N-2}}\omega_{k_{N-2}}^{L_{N-2}-1} - \lambda.$$

Since $\mathbf{A}$ is a block circulant matrix, its eigen polynomial are shown as

$$\prod_{k_1=1}^{L_1}\prod_{k_2=1}^{L_2}\cdots\prod_{k_{N-1}=1}^{L_{N-1}} \left| \mathbf{A}_1' + \mathbf{A}_2\omega_{k_1} + \mathbf{A}_{L_1}\omega_{k_1}^{L_1-1} + \mathbf{A}_2\omega_{k_2} + \mathbf{A}_{L_2}\omega_{k_2}^{L_2-1} + \cdots + \mathbf{A}_2\omega_{k_{N-1}} + \mathbf{A}_{L_1}\omega_{k_{N-1}}^{L_{N-1}-1} - \lambda\mathbf{E} \right|, \tag{42}$$

where $\omega_{k_1} = \cos(\frac{2\pi k_1}{L_1}) + i\sin(\frac{2\pi k_1}{L_1}), \cdots, \omega_{k_{N-1}} = \cos(\frac{2\pi k_{N-1}}{L_{N-1}}) + i\sin(\frac{2\pi k_{N-1}}{L_{N-1}})$.

According to the above-mentioned analysis, the eigenvalues of $\mathbf{K}$ are obtained as

$$\lambda = 1 - \varepsilon + \frac{\varepsilon}{2N}\omega_{k_1} + \frac{\varepsilon}{2N}\omega_{k_1}^{L_1-1} + \frac{\varepsilon}{2N}\omega_{k_2} + \frac{\varepsilon}{2N}\omega_{k_2}^{L_2-1} + \cdots + \frac{\varepsilon}{2N}\omega_{k_{N-1}} + \frac{\varepsilon}{2N}\omega_{k_{N-1}}^{L_{N-1}-1} + \frac{\varepsilon}{2N}\omega_{k_N} + \frac{\varepsilon}{2N}\omega_{k_N}^{L_N-1}, \tag{43}$$

where $\omega_{k_N} = \cos(\frac{2\pi k_N}{L_N}) + i\sin(\frac{2\pi k_N}{L_N})$.

Substituting Eq. (43) into Eq. (40), we can get the LEs of ND CML as

$$\mathrm{LE} = \mathrm{LE}_{\mathrm{F}} + \ln\left| 1 - \varepsilon + \frac{\varepsilon}{N}(\cos\frac{2\pi k_1}{L_1} + \cos\frac{2\pi k_2}{L_2} + \cdots + \cos\frac{2\pi k_{N-1}}{L_{N-1}} + \cos\frac{2\pi k_N}{L_N}) \right|. \tag{44}$$

□

References

1. Alawida, M., Samsudin, A., Teh, J.S.: Enhanced digital chaotic maps based on bit reversal with applications in random bit generators. Inf. Sci. **512**, 1155–1169 (2020)
2. Amigo, J., Kocarev, L., Szczepanski, J.: Theory and practice of chaotic cryptography. Phys. Lett. A **366**(3), 211–216 (2007)
3. Ascoli, A., Demirkol, A.S., Tetzlaff, R., Chua, L.: Edge of chaos theory resolves smale paradox. IEEE Trans. Circuits Syst. I-Regul. Pap. **69**(3), 1252–1265 (2022)
4. Cai, X., Xu, W., Lau, F.C., Wang, L.: Joint carrier-code index modulation aided *m*-ary differential chaos shift keying system. IEEE Trans. Veh. Technol. **69**(12), 15486–15499 (2020)
5. Cang, S., Kang, Z., Wang, Z.: Pseudo-random number generator based on a generalized conservative sprott-a system. Nonlinear Dyn. **104**, 827–844 (2021)
6. Chen, S., Ma, S., Qin, Z., Zhu, B., Xiao, Z., Liu, M.: A low complexity and long period digital random sequence generator based on residue number system and permutation polynomial. IEEE Trans. Comput. **71**(11), 3008–3017 (2022)
7. Dachselt, F., Schwarz, W.: Chaos and cryptography. IEEE Trans. Circuits Syst. I-Fundam. Theor. Appl. **48**(12), 1498–1509 (2001)
8. Ding, M., Yang, W.: Stability of synchronous chaos and on-off intermittency in coupled map lattices. Phys. Rev. E **56**(4), 4009 (1997)
9. Hua, Z., Zhou, Y.: One-dimensional nonlinear model for producing chaos. IEEE Trans. Circuits Syst. I-Regul. Pap. **65**(1), 235–246 (2017)
10. Hua, Z.Y., Zhou, Y.C.: Dynamic parameter-control chaotic system. IEEE Trans. Cybern. **46**(12), 3330–3341 (2015)
11. Jost, J., Joy, M.P.: Spectral properties and synchronization in coupled map lattices. Phys. Rev. E **65**(1), 016201 (2001)

12. Kaneko, K.: Coupled map lattice. In: Chaos, Order, and Patterns, pp. 237–247. Springer, Berlin (1991)
13. Krishnamoorthi, S., Jayapaul, P., Dhanaraj, R.K., Rajasekar, V., Balusamy, B., Islam, S.H.: Design of pseudo-random number generator from turbulence padded chaotic map. Nonlinear Dyn. **104**, 1627–1643 (2021)
14. Lai, Q., Kuate, P.D.K., Liu, F., Iu, H.H.C.: An extremely simple chaotic system with infinitely many coexisting attractors. IEEE Trans. Circuits Syst. II Exp. Briefs **67**(6), 1129–1133 (2019)
15. Li, P., Li, Z., Halang, W.A., Chen, G.: A stream cipher based on a spatiotemporal chaotic system. Chaos Solitons Fractals **32**(5), 1867–1876 (2007)
16. Li, S., Liu, Y., Ren, F., Yang, Z.: Design of a high throughput pseudorandom number generator based on discrete hyperchaotic system. IEEE Trans. Circuits Syst. II Exp. Briefs **70**(2), 806–810 (2022)
17. Li, S.J., Mou, X.Q., Cai, Y.L.: Pseudo-random bit generator based on couple chaotic systems and its applications in stream-cipher cryptography. In: Proceedings of international conference on cryptology in India, pp 316–329. Springer (2001)
18. Liu, Z., Wang, Y., Zhao, Y., Zhang, L.Y.: A stream cipher algorithm based on 2d coupled map lattice and partitioned cellular automata. Nonlinear Dyn. **101**(2), 1383–1396 (2020)
19. Lv, X.P., Liao, X.F., Yang, B.: A novel pseudo-random number generator from coupled map lattice with time-varying delay. Nonlinear Dyn. **94**(1), 325–341 (2018)
20. Ma, J., Guo, Y.: Model approach of electromechanical arm interacted with neural circuit, a minireview. Chaos Solitons Fractals **183**, 114925 (2024)
21. Mansouri, A., Wang, X.: A novel one-dimensional chaotic map generator and its application in a new index representation-based image encryption scheme. Inf. Sci. **563**, 91–110 (2021)
22. Murillo-Escobar, M., Cruz-Hernández, C., Cardoza-Avendaño, L., Méndez-Ramírez, R.: A novel pseudorandom number generator based on pseudorandomly enhanced logistic map. Nonlinear Dyn. **87**, 407–425 (2017)
23. Ott, E., Grebogi, C., Yorke, J.A.: Controlling chaos. Phys. Rev. Lett. **64**(11), 1196 (1990)
24. Patidar, V., Sud, K.K., Pareek, N.K.: A pseudo random bit generator based on chaotic logistic map and its statistical testing. Informatica **33**(4), 441 (2009)
25. Sayed, W.S., Roshdy, M., Said, L.A., Radwan, A.G.: Design and FPGA verification of custom-shaped chaotic attractors using rotation, offset boosting and amplitude control. IEEE Trans. Circuits Syst. II Exp. Briefs **68**(11), 3466–3470 (2021)
26. Sun, J., Li, C., Wang, Z., Wang, Y.: A memristive fully connect neural network and application of medical image encryption based on central diffusion algorithm. IEEE Trans. Ind. Inf. **20**(3), 3778–3788 (2023)
27. Teh, J.S., Samsudin, A., Akhavan, A.: Parallel chaotic hash function based on the shuffle-exchange network. Nonlinear Dyn. **81**(3), 1067–1079 (2015)
28. Tsafack, N., Kengne, J., Abd-El-Atty, B., Iliyasu, A.M., Hirota, K., Abd El-Latif, A.A.: Design and implementation of a simple dynamical 4-d chaotic circuit with applications in image encryption. Inf. Sci. **515**, 191–217 (2020)
29. Umar, T., Nadeem, M., Anwer, F.: A new modified skew tent map and its application in pseudo-random number generator. Comput. Stand. Interfaces **89**, 103826 (2024)
30. Wang, C., Song, L.: An image encryption scheme based on chaotic system and compressed sensing for multiple application scenarios. Inf. Sci. **642**, 124 (2023)
31. Wang, M., Wang, X., Zhao, T., Zhang, C., Xia, Z., Yao, N.: Spatiotemporal chaos in improved cross coupled map lattice and its application in a bit-level image encryption scheme. Inf. Sci. **544**, 1–24 (2021)
32. Wang, S., Hu, G.: Coupled map lattice based hash function with collision resistance in single-iteration computation. Inf. Sci. **195**, 266–276 (2012)
33. Wang, X., Liu, P.: A new full chaos coupled mapping lattice and its application in privacy image encryption. IEEE Trans. Circuits Syst. I-Regul. Pap. **69**(3), 1291–1301 (2022)
34. Wang, Y., Liao, X., Xiao, D., Wong, K.W.: One-way hash function construction based on 2d coupled map lattices. Inf. Sci. **178**(5), 1391–1406 (2008)
35. Wang, Y., Liu, Z., Ma, J., He, H.: A pseudorandom number generator based on piecewise logistic map. Nonlinear Dyn. **83**(4), 2373–2391 (2016)
36. Wang, Y., Liu, Z., Zhang, L.Y., Pareschi, F., Setti, G., Chen, G.: From chaos to pseudorandomness: a case study on the 2-d coupled map lattice. IEEE Trans. Cybern. **53**(2), 1324–1334 (2023)
37. Yi, X.: Hash function based on chaotic tent maps. IEEE Trans. Circuits Syst. II Exp. Briefs **52**(6), 354–357 (2005)
38. Zhang, Z., Wang, Y., Zhang, L.Y., Zhu, H.: A novel chaotic map constructed by geometric operations and its application. Nonlinear Dyn. **102**, 2843–2858 (2020)
39. Zhao, Y., Gao, C., Liu, J., Dong, S.: A self-perturbed pseudo-random sequence generator based on hyperchaos. Chaos Solitons Fractals X **4**, 100023 (2019)