基于非线性耦合混沌系统的 S 盒构造算法

黄慧芳 [1]
HUANG Huifang

摘 要 提出了一个新的时空混沌系统，并将其设计于构造 S 盒的算法中。系统改进了耦合映射格子模型，即 CML 模型的耦合方式，参照斐波那契数列规律进行非线性耦合。非线性耦合系统的分岔图显示其周期窗口比 CML 系统更小，具有更大的密钥空间，适用于加密算法构造中。将其设计于 S 盒生成算法中，并对生成的 S 盒进行加密指标检测与对比，实验结果表明，由新算法可以批量生成满足构造准则的 S 盒，并可以从中挑选出性能指标优秀的 S 盒应用于分组密码的设计中。

关键词 时空混沌；非线性耦合；斐波那契数列；S 盒

doi：10.3969/j.issn.1672-9528.2024.07.013

0 引言

在自然界中，非线性运动广泛存在，时空混沌系统代表了其中的一个分支。自从耦合格子模型 CML 被提出 [1]，相邻耦合方式便进入人们的眼帘。Sinha[2] 提出随机耦合格子映射时空混沌系统，开启了空间非相邻耦合时空混沌系统的研究。随机耦合的时空混沌系统产生的混沌序列不具有重现性，无法用相同的参数再次恢复之前的混沌序列，因此无法应用到密码学领域。除了随机耦合达成非相邻耦合外，非线性混沌映射提出了空间相邻与非线性混合耦合时空混沌系统，与上述随机耦合时空系统相比具有确定性。该系统的遍历性比 CML 系统强，比 ACLML 系统具有更多的参数空间，因此能够应用到密码学领域。

Matthews[3] 提出用一维混沌映射进行一次一密的加密，此后，很多一维混沌由于自身的伪随机性、遍历性和初值敏感性，纷纷被应用到密码学领域，如 Logistic 映射、Arnold 猫映射和 Baker 映射。但低维混沌也存在不足，如 Logistic 映射的密钥空间小和分岔图存在周期窗口。为了克服这些不足，基于高维混沌映射的加密算法应运而生。时空混沌系统在加密系统中具有两大优点。第一，低维混沌系统轨道在有限计算机精度条件下将变得周期化，而时空混沌系统的轨道周期明显更长，因此实际情况下的周期化问题得到缓解。第二，时空混沌系统是高维系统，因此其多个正 Lyapunov 指数能保证混沌序列的高随机性和复杂的动力学行为。因而从时空混沌系统出发，研究新的混沌系统，克服在密码学领域使用较为普遍的 CML 系统的弱点，找到具有参数范围广、空间层面混沌行为强、周期窗口小等特点的系统具有重要的意义。

分组密码是密码算法的一个分支，在当代信息安全发展中起着重要作用。S 盒是许多分组密码算法中的非线性部件，是增强密码非线性特性，进而提高安全性的关键所在。混沌 S 盒指的是将混沌系统设计到 S 盒的生成算法中，对 S 盒进行研究和改进，在混沌加密领域较为热门。被用来设计 S 盒的混沌系统可以是低维的，如 Logistic 混沌系统 [4]、Baker 混沌映射 [5]、Lorenz 混沌映射 [6]、混沌正弦映射 [7]，也有分数阶混沌映射 [8-9] 及时空混沌系统 [10-11]。

本文在空间相邻耦合映像格子模型的基础上，提出了一种新的耦合模型，比前者具有更复杂的动力学行为。将其应用于 S 盒生成算法中，利用混沌系统的初值和参数敏感性，便可以动态生成批量 S 盒。通过对筛选出的一个 S 盒进行性能测试和比较，结果表明本文生成的 S 盒密码学性能良好，适合应用于分组密码中。

1 非线性耦合时空混沌系统模型

为了代替 CML 系统中的空间相邻耦合，提出了基于斐波那契数列的非线性耦合方式，得到了新的时空混沌系统，系统描述为：

$$x_{n+1}(i)=(1-\varepsilon)f[x_n(i)]+\frac{\varepsilon}{2}\{f[x_n(k)+f[x_n(j)]\} \quad (1)$$

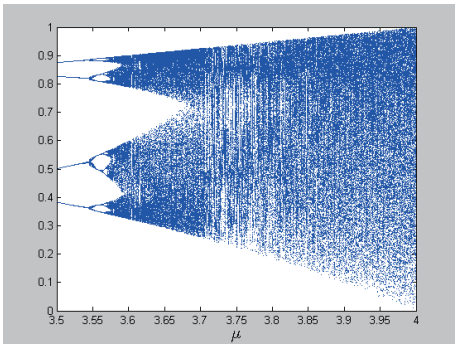
$$f(x)=\mu x(1-x),\mu\in(0,4] \quad (2)$$

式中：$i,j,k\,(1\le i,j,k\le L)$ 表示空间格点，L 表示进行耦合的系统数量，$\varepsilon(0\le\varepsilon\le1)$是耦合系数，$n(n=1,2,3,\cdots)$是时间序列，式（2）是一维 Logistic 映射。空间格点 *i, j, k* 由 *a, b* 两个数列和式（3）、式（4）决定：

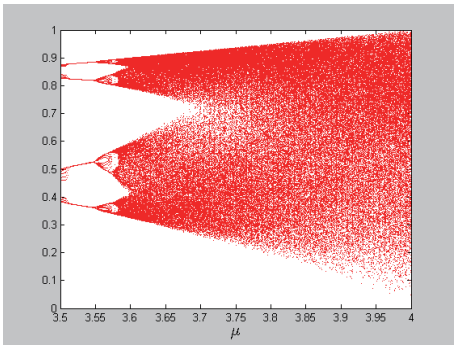
1. 厦门大学嘉庚学院 福建漳州 363105

$$a=[1,2,3,5,8,13,\cdots]$$
$$b=[1,2,4,7,12,20,\cdots]$$
$$j=a(i)\bmod L \quad (3)$$
$$k=b(i)\bmod L \quad (4)$$

新系统与 CML 系统在公式上的区别在于耦合系统 j,k 的选择是由非线性序列决定的。为了统一，新系统采用与 CML 系统一样的格点数 $L=100$，下面对两个系统的分岔图，时空行为图和 Kolmogorov-Sinai 熵广度进行比较分析。图 1（a）是 CML 系统的分岔图，图 1（b）是新型非线性耦合系统的分岔图。



（a）CML 系统

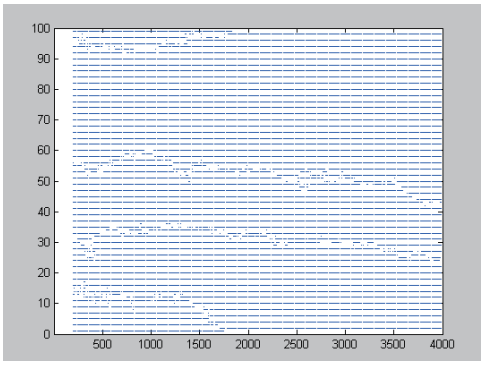


（b）斐波那契非线性耦合系统

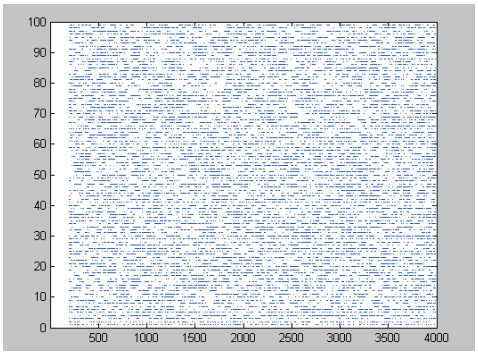
图 1 分岔图

经过图 1 的比较，发现新系统的周期窗口与 CML 系统相比更小。两个分岔图都有从四周期到八周期的分岔过程，当在八周期之后，CML 系统还有到十六周期的分岔，而新型非线性耦合系统不存在十六周期分岔。这说明非线性耦合增强了周期轨道的不稳定性，降低了倍周期分岔的次数，意味着非线性耦合系统若应用于密码学，其密钥空间将比 CML 系统更大。

图 2（a）是 CML 系统在 μ=3.925 时的时空行为图，图 2（b）是新型非线性耦合系统在 μ=3.925 时的时空行为图。通过图 2 的比较，表明新系统更快进入完全湍流模式，而相同参数下，CML 系统还处于缺陷混沌扩散模式。事实上，非线性耦合增强了混沌扩散效应，使其不容易出现混沌缺陷模式 [12]，这也进一步说明非线性耦合系统更适合密码学应用。



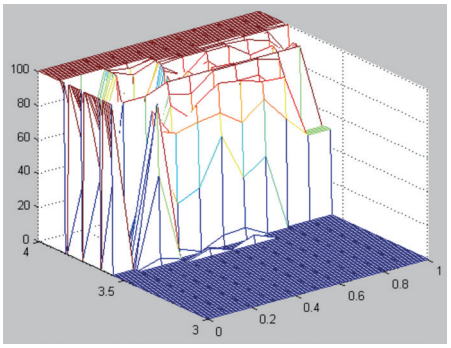
（a）CML 系统



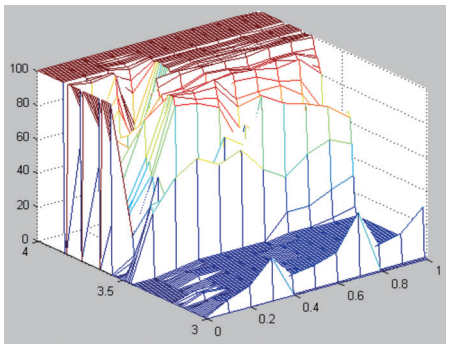
（b）斐波那契非线性耦合系统

图 2 时空行为图

图 3（a）是 CML 系统 Kolmogorov-Sinai 熵广度与参数之间的关系图，图 3（b）是新型非线性耦合系统的 Kolmogorov-Sinai 熵广度与参数之间的关系图。



（a）CML 系统



（b）斐波那契非线性耦合系统

图 3 Kolmogorov-Sinai 熵广度

Kolmogorov-Sinai 熵广度的物理意义是处于混沌状态的格点数的百分比，表示了 L 维空间层面的混沌的普遍性。通过图 3 的比较可以看出，非线性耦合系统出现 100% 空间格点的混沌行为的参数范围比 CML 系统来得多。利用这个特性，新系统更适合在密码学中，将参数作为密钥进行加密算法的设计。

2 S 盒生成算法

本文通过式（1）中的非线性耦合系统产生的混沌序列来动态生成一组 8×8 的 S 盒，具体操作步骤如下。

（1）给定一个初值 $c(1)$ 和 Logistic 映射的参数 μ，迭代 Logistic 映射生成一组耦合系统的初值序列 $cs(1)$，长度为 L。

（2）利用非线性耦合混沌系统迭代初值，迭代 N 次，得到大小为 $L\times N$ 的混沌序列矩阵。

（3）从混沌序列矩阵中的每一行中，依次间隔 i 个值截取长度为 256 的序列，每行截取 6 个序列，总共截取 $6\times L$ 个序列。

（4）对每个长度为 256 的混沌序列进行排序，元素的位置序号便是一组乱序的 0～255 的序列，即可记作 S 盒序列。

（5）检测得到的 $6\times L$ 个 S 盒序列的差分逼近概率（DP）和线性逼近概率（LP），从中筛选 DP、LP，指标值较优秀的保存下来。表 1 为选取的其中一个 S 盒。

3 S 盒性能指标检测

本文对表 1 中的 S 盒的双射特性、非线性度、严格雪崩准则、输出比特间独立性、差分均匀性等指标依次进行分析，并且与近五年内发表的文献 [13-15] 中构造的混沌 S 盒进行对比，比较结果如表 2 所示。

表 1 S 盒

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

表 2 S 盒的性能指标对比

S 盒	非线性度			SAC	Δ_1	BIC-SAC	Δ_2
	Max	Min	Ave				
本文 S 盒	112	102	105.75	0.498 5	0.001 5	0.500 1	0.000 1
文献 [13]	108	102	104.25	0.508 3	0.008 3	0.500 8	0.000 8
文献 [14]	108	104	106.00	0.504 9	0.004 8	0.498 4	0.001 6
文献 [15]	—	—	106.25	0.503 7	0.003 7	0.494 2	0.005 8

首先在双射特性检测中，如式（5）所示的 S 盒满足双射的充要条件为：各分量布尔函数 $f_i(x)$ 的线性运算之和为 2^{n-1}。

$$S(x)=[f_1(x),....,f_m(x)]:F_2^n\rightarrow F_2^m \tag{5}$$

表 1 中 S 盒 8 个分量布尔函数的线性运算之和都为 128，充分满足双射特性。

S 盒是一个多输出函数，式（5）所示 S 盒函数的非线性度定义为：

$$N_s=\min_{\substack{l\in L_n\\ 0\neq u\in F_2^m}} d_H(u\cdot S(x),l(x)) \tag{6}$$

非线性度的值越大意味着抵抗线性攻击的能力越强，本文构造的 S 盒非线性度最大值为 112，最小值为 102，8 个非线性度的均值为 105.75，意味着抵抗线性逼近攻击的能力较强。

严格雪崩准则（strict avalanche criterion，SAC）描述的是当输入序列的发生 1 比特改变时，每个输出比特发生改变的概率，其理论值为 0.5。本文构造出的 S 盒的相关矩阵如表 3 所示，均值为 0.498 5，与理论值相差 0.001 5，将该差值记作 Δ_1，并与其他文献中的 S 盒进行对比，如表 2 所示，可见本文 S 盒具有很好的 SAC 性能。

输出比特间独立性（bits independence criteria，BIC）检测的是 S 盒任意两个输出比特 $f_j\oplus f_k$ 是否满足严格雪崩效应，其理论值也是 0.5。检测本文 S 盒的输出比特间独立性，得到的相关矩阵如表 4 所示，均值为 0.500 1，十分接近 0.5，将差值记为 Δ_2，与其他文献中的 S 盒作对比，由表 2 的对比结果可见，本文 S 盒的输出比特间独立性优于其他方案构造的 S 盒。

差分逼近概率（differential probability，DP）定义式为：

$$\mathrm{DP}=\max_{\Delta x\neq 0,\Delta y}\left(\frac{\#\{x\in X\,|\,f(x)\oplus f(x\oplus\Delta x)=\Delta y\}}{2^n}\right) \tag{7}$$

式中：X 表示所有可能输入的集合；2^n 是该集合的元素个数。差分逼近概率可以用来衡量 S 盒抵抗查分密码攻击的能力，其值越小，抵抗攻击能力越强。

线性逼近概率（linear probability，LP）定义为：

$$LP = \max_{\alpha,\beta\neq 0} P(\alpha,\beta) \tag{8}$$

$$P(\alpha,\beta) = (2p-1)^2 \tag{9}$$

$$p = \frac{\#\{\xi \in Z_2^n : \xi \circ \alpha = F(\xi) \circ \beta\}}{2^n} \tag{10}$$

式中：$\xi \circ \alpha = \xi_1\alpha_1 \oplus \xi_2\alpha_2 \oplus \cdots \oplus \xi_n\alpha_n$。LP 值用来衡量 S 盒关于线性密码攻击的抵抗能力，其值越小，说明抵抗能力越强。本文提出的 S 盒构造方法可以批量生成 DP、LP 指标值较小的 S 盒。对表 1 中 S 盒进行指标检测，并与现有文献中的 S 盒的 DP、LP 值进行比较，比较结果如表 3 ～ 5 所示。

表 3 S 盒的相关矩阵

0.481	0.495	0.513	0.484	0.472	0.567	0.437	0.463
0.578	0.461	0.510	0.516	0.555	0.511	0.572	0.530
0.542	0.518	0.512	0.492	0.376	0.504	0.488	0.550
0.401	0.494	0.468	0.567	0.545	0.537	0.467	0.482
0.556	0.560	0.542	0.443	0.608	0.535	0.486	0.400
0.475	0.459	0.490	0.488	0.458	0.500	0.498	0.417
0.543	0.454	0.450	0.481	0.577	0.522	0.446	0.407
0.577	0.465	0.445	0.466	0.489	0.513	0.497	0.566

表 4 输出比特间独立性

0	0.502	0.745	0.490	0.499	0.508	0.394	0.379
0.502	0	0.491	0.488	0.497	0.493	0.624	0.352
0.745	0.491	0	0.748	0.488	0.731	0.646	0.632
0.490	0.488	0.748	0	0.239	0.286	0.645	0.382
0.499	0.497	0.488	0.239	0	0.251	0.874	0.383
0.508	0.493	0.731	0.286	0.251	0	0.612	0.134
0.394	0.624	0.646	0.645	0.874	0.612	0	0.490
0.379	0.352	0.632	0.382	0.383	0.134	0.490	0

表 5 DP、LP 指标值对比

S 盒	DP 值	LP 值
本文提出的 S 盒	0.039 1	0.062 5
文献 [13] 提出的 S 盒	0.046 9	0.140 6
文献 [16] 提出的 S 盒	0.039 1	0.109 4

4 结论

本文基于斐波那契数列规律设计非线性耦合时空混沌系统，并行了分岔图和时空行为的数值仿真，对比相邻耦合的 CML 系统，新系统的动力学复杂性有了进一步的提高，密钥空间更大。将其应用于动态 S 盒的算法构造中，并检测了所生成 S 盒的差分逼近概率、线性逼近概率、非线性度和严格雪崩准则等指标。通过比较分析，本文生成的 S 盒性能良好，适于在分组密码设计中进行应用。

参考文献：

[1]KANEKO K.Pattern dynamics in spatiotemporal chaos:pattern selection,diffusion of defect and pattern competition intermettency[J].Physica D:nonlinear phenomena,1989,34(1-2):1-41.

[2]SINHA S.Random coupling of chaotic maps leads to spatiotemporal synchronization[J].Physical review,e.statistical physics, plasmas, fluids, and related interdisciplinary topics, 2002, 66(1):6209-6210.

[3]MATTHEWS R.On the derivation of a chaotic encryption algorithm[J].Cryptologia,1989(13):29-42.

[4] 黄慧芳 , 臧鸿雁 . 基于混沌系统的 S 盒生成算法的研究 [J] 计算机应用研究 ,2016,33(6):1802-1805.

[5]TANG G, LIAO X, CHEN Y.A novel method for designing S-boxes based on chaotic maps [J].Chaos,solitons and fractals, 2005, 23(2):413-419.

[6] ÖZKAYNAK F, ÖZER A B.A method for designing strong S-Boxes based on chaotic Lorenz system[J].Physics letters A, 2010, 374(36): 3733-3738.

[7] 郝俊灵 . 一维正弦混沌系统及 S 盒设计 [J]. 莆田学院学报 , 2021, 28(2):46-49.

[8]MAJID K, TARIQ S.An efficient construction of substitution box with fractional chaotic system[J].Signal,image and video processing,2015,9(6):1335-1338.

[9]ZHANG Y, HAO J, WANG X.An efficient image encryption scheme based on S-Boxes and fractional-order differential logistic map[J].IEEE access,2020,8:54175-54188.

[10] 赵耿 , 马英杰 , 陈磊 , 等 . 基于扰动时空混沌系统的动态 S 盒设计 [J]. 电子学报 ,2022,50(8):2037-2042.

[11]WANG X, YANG J.A novel image encryption scheme of dynamic S-boxes and random blocks based on spatiotemporal chaotic system[J].Optik,2020,217:164884.

[12]ZHANG Y, WANG X.Spatiotemporal chaos in arnold coupled logistic map lattice [J].Nonlinear analysis:modeling and control,2013,18(4):526-541.

[13]LIU L, LEI Z.An approach for constructing the S-box using the CML system[J].Journal of physics:conference series, 2019, 1303(1):012090.

[14] 赵耿 , 侯艳丽 , 马英杰 , 等 . 一种基于交叉耦合映像格子的 S 盒构造算法 [J]. 计算机应用与软件 ,2022,39(10):329-335.

[15]AHMED A A E, BASSEM A, SALVADOR E V, et al.A novel image steganography technique based on quantum substitution boxes[J].Optics&laser technology,2019,116:92-102.

[16] 韩妍妍 , 何彦茹 , 刘培鹤 , 等 . 一种基于混沌系统的 ZUC 动态 S 盒构造及应用方案 [J]. 计算机研究与发展 , 2020, 57(10):2147-2157.

【作者简介】

黄慧芳（1991—），女，福建泉州人，硕士，讲师，研究方向：信息安全与密码学。

（收稿日期：2024-04-25）