一维鲁棒混沌映射及S盒的设计

韩丹丹[1],闵乐泉[2],赵 耿[3],张丽姣[2],闫世杰[1]
(1.北京科技大学自动化学院,北京 100083; 2.北京科技大学数理学院,北京 100083; 3.北京电子科技学院,北京 100070)

摘 要: 本文利用Li-York混沌判别定理,构造了一类分段线性连续混沌映射.基于此类映射,建立了一个构造一类分段非线性鲁棒混沌映射的判别定理.作为应用,构造了一个由多项式函数和三角函数映射合成的分段非线性鲁棒混沌映射.通过计算该混沌映射的分岔图,验证了映射在参数范围内的混沌性.作为鲁棒混沌的应用,设计了三个基于分段非线性鲁棒混沌映射的伪随机数发生器.在此基础上,利用混沌映射对初始参数的敏感性,提出了批量生成S盒的算法.S盒密码性能的分析结果表明,生成的S盒具有良好的密码学性能,可以较好的抵抗线性与差分攻击,为密码算法的研究发展提供基础与条件.

关键词: Li-York混沌; 鲁棒混沌; 伪随机数发生器; S盒
中图分类号: TP393 **文献标识码:** A **文章编号:** 0372-2112 (2015)09-1770-06
电子学报URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2015.09.014

One-Dimensional Robust Chaotic Map and the Construction of S-Box

HAN Dan-dan[1], MIN Le-quan[2], ZHAO Geng[3], ZHANG Li-jiao[2], YAN Shi-jie[1]
(1. *School of Automation and Electrical Engineering, University of Science and Technology Beijing, Beijing* 100083, *China*;
2. *School of Mathematics and Physics, University of Science and Technology Beijing, Beijing* 100083, *China*;
3. *Beijing Electronic Science and Technology Institute, Beijing* 100070, *China*)

Abstract: Using the judgment theorem of Li-York chaos, this paper generates a class of piecewise linear chaotic maps. Based on the chaotic maps, a constructing theorem of piecewise nonlinear robust chaotic map is proposed. As an application, this theorem is used to construct a piecewise nonlinear robust chaotic map with a polynomial function and a trigonometric function. This study computes the bifurcation diagram of the map. The computed results demonstrate the chaotic robustness features of the map. Three pseudo-random number generators are generated based on the piecewise nonlinear robust chaotic map. On this basis, the generation algorithm of S-boxes is proposed with the property of sensitivity to the initial parameters of the chaotic map. The cryptography performance is tested and the tested results show that generated S-boxes have good cryptographic properties, and can not only better resist the linear and differential attacks, but also provide the foundation and conditions for the research and development of cryptography.

Key words: Li-York chaos; robust chaos; pseudo-random number generator; S-box

1 引言

在当今数字化的信息时代,计算机和网络通信安全问题日益凸显,通信中的保密安全工作成为信息安全研究的热点.在网络通信过程中,信息加密成为保证其安全快而有效的方法之一.随着美国数据加密标准Data Encryption Standard (DES)的出现,S盒作为分组密码系统的非线性元件而被广泛使用,为密码算法提供混乱作用.设计密码性能良好的S盒是设计安全密码算法的核心问题[1,2].

1975年华人学者李天岩和美国数学家J.A.Yorke在美国《数学月刊》上发表"周期三蕴含混沌"论文[3].文中建立了混沌判别定理,该定理为人们研究系统提供了工具,被广泛用于物理学[4]及动力系统的设计分析[5~7]等研究中.1989年,A.Robert和J.Matthews首次提出了一个混沌加密算法,并指出混沌密码算法可能适于替代一次一密系统.自此应用混沌系统构造新型密码算法的方法得到了越来越多的关注.用离散混沌系统[8~10]或连续混沌系统[11,12]来构造S盒是研究的热点问题之一.研究表明利用混沌系统构造S盒是完全可行的.其中,文献[8]通过迭代Logistic和Tent映射得到伪随机序列,然后用取整量化的方法得到S盒.在文献[10]中通

收稿日期:2014-06-26;修回日期:2015-04-30;责任编辑:马兰英
基金项目:国家自然科学基金(No.61074192,No.61170037)

过迭代分段线性离散混沌系统构造 S 盒.文献[11]中采用的是时延迟连续系统,通过求解系统,将其系统输出量转换成 6 位二进制形式,选取其中 3 位用于计算进而得到 S 盒.

基于 Li-York 混沌判别定理,本文构造了一维分段线性连续混沌映射.在此基础上,通过引进新的参数和非线性映射将其扩展为一类分段非线性连续映射,并建立了新的构造混沌映射定理.利用构造的分段非线性连续映射,设计了三个基于混沌的伪随机数发生器.基于混沌映射在参数区间上的鲁棒特性及伪随机数发生器的伪随机性提出了生成 S 盒的算法,并对生成的一系列 S 盒进行性能分析.性能分析的结果表明产生的 S 盒具有良好的密码学性能.

2　一维分段光滑鲁棒混沌映射

2.1　Li-York 混沌判别定理

Li-York 混沌判别定理的表述如下:

定理 1[3]　设 $I\subset R$ 为一闭区间,$f: I\to I$ 为连续映射.若存在点 $a\in I$ 有 $b=f(a)$,$c=f^2(a)$,$d=f^3(a)$,满足:

$$d\leqslant a<b<c \quad 或 \quad d\geqslant a>b>c \tag{1}$$

则 f 是一个(Li-York 意义下的)混沌映射.

基于此定理,我们在闭区间 $I=[m,n]\subset(0,\infty)$ 上设计一类分段线性连续映射,结构如下:

$$f(x)=\begin{cases}k_1x+b_1, & \text{if} \quad x\in[m,a]\\ k_2x+b_2, & \text{if} \quad x\in(a,b]\\ k_3x+b_3, & \text{if} \quad x\in(b,c]\\ k_4x+b_4, & \text{if} \quad x\in(c,n]\end{cases} \tag{2}$$

选取其中的参数 $k_i,b_i(i=1,2,3,4)$ 使得

$$\begin{aligned}&b=f(a),c=f^2(a),d=f^3(a),\\ &0=m<d\leqslant a<b<c<n\end{aligned} \tag{3}$$

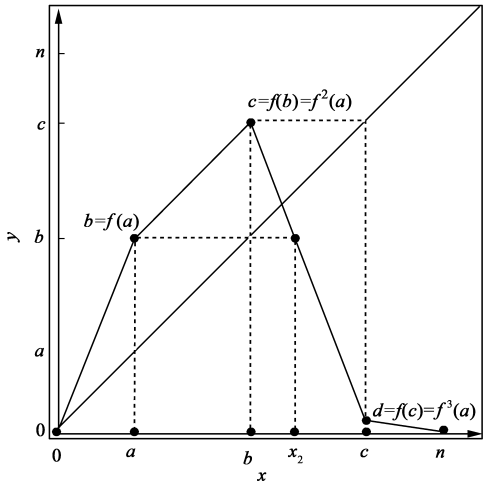


图1　映射的曲线图.虚线为各点位置的映射值连线，细线为对角线$y=x$.其中x_2是$f(x)=b$除a外的另一个解

则由定理 1 知这类分段线性连续映射在 Li-York 意义下是混沌的.这类映射的曲线图如图 1 所示.

2.2　分段光滑鲁棒混沌映射

在本节我们研究分段线性连续映射式(2),借助参数 p 和非线性连续映射 $g: I\to R$ 来构造满足定理 1 条件的鲁棒混沌映射:

$$F(x)=f(x)+pg(x) \tag{4}$$

我们提出一个构造混沌映射的定理如下.

定理 2　设 $f(x)$是由式(2)和式(3)定义的满足定理 1 的分段线性混沌映射,$g: I\to R$ 是任意的非负连续单增的函数,如果 $g(b)>-k_3g(a)$,必存在 $p>0$ 使得 F 在 I 上满足条件:

(1)对 $\forall\, x\in I, m\leqslant(f+pg)(x)\leqslant n$.

(2)取 $a_1=a$,使得

$$\begin{aligned}&b_1=(f+pg)(a),c_1=(f+pg)^2(a),\\ &d_1=(f+pg)^3(a)\end{aligned} \tag{5}$$

满足条件

$$m<d_1\leqslant a<b_1<c_1<n \tag{6}$$

则 F 是 Li-York 意义下的混沌映射.

证明　(*a*)首先证条件(1)成立.

记

$$\begin{aligned}&f_{\max}=\max_{x\in I}f(x)=f(b), \quad f_{\min}=\min_{x\in I}f(x)=f(m),\\ &g_{\max}=\max_{x\in I}g(x), \quad g_{\min}=\min_{x\in I}g(x),\\ &F_{\max}=\max_{x\in I}F(x), \quad F_{\min}=\min_{x\in I}F(x).\end{aligned}$$

则

$$\begin{aligned}F_{\min}&\geqslant f_{\min}+pg_{\min}>m\\ F_{\max}&\leqslant f_{\max}+pg_{\max}\end{aligned}$$

令

$$F_{\max}<n$$

解得

$$f(b)+pg_{\max}\leqslant n$$

则当

$$p\leqslant\frac{n-f(b)}{g_{\max}} \tag{7}$$

时条件(1)成立.

(*b*)求使条件(2)成立的 p.首先由式(3)和 $pg>0$,知

$$b_1=F(a_1)=(f+pg)(a)=b+pg(a)>a=a_1 \tag{8}$$

其次,由 g 的非负单增性和式(3)知

$$\begin{aligned}c_1&=F(b_1)=f(b+pg(a))+pg(b_1)\\ &>f(b+pg(a))+pg(a)\end{aligned}$$

因此由式(8)知只须

$$f(b+pg(a))>b=f(a) \tag{9}$$

则 $c_1>b_1$.

由图 1 和式(2)知 $f(x)=b$ 有 2 个解:

$$x_1=a,\quad x_2=\frac{b-b_3}{k_3}$$

则由图 1 知,只须

$$a<b+pg(a)<\frac{b-b_3}{k_3}<c \tag{10}$$

则 $c_1>b_1$.

不等式(10)左端显然成立,要使右端的不等式成立,只须

$$p<\frac{(b-b_3)/k_3-b}{g(a)} \tag{11}$$

最后求使 $d_1=F(c_1)\leqslant a_1=a$ 的 p.

首先由式(8)和(2),且 $g(b)>-k_3g(a)$ 知

$$\begin{aligned}c_1&=F(b_1)=(f+pg)(b_1)=f(b+pg(a))+pg(b_1)\\&=k_3(b+pg(a))+b_3+pg(b_1)\\&=c+p(k_3g(a)+g(b_1))\\&>c\end{aligned} \tag{12}$$

从而可得

$$\begin{aligned}d_1&=F(c_1)=(f+pg)(c_1)=f(c_1)+pg(c_1)\\&<f(c)+pg_{\max}=d+pg_{\max}\end{aligned}$$

则只须 $d+pg_{\max}<a_1=a$

即

$$p<\frac{a-d}{g_{\max}} \tag{13}$$

可得 $d_1\leqslant a<b_1<c_1$.

综上所述,由式(7)、式(11)及式(13)知,若

$$p\in\left(0,\min\left\{\frac{n-f_b}{g_{\max}},\frac{b-b_3-k_3b}{k_3g(a)},\frac{a-d}{g_{\max}}\right\}\right) \tag{14}$$

则 $F=f+pg$ 是从 I 到 I 上的 Li-York 意义下的混沌映射.

2.3 例子

取映射式(2)的参数为:

$$m=0,f(m)=0,n=10,f(n)=0,a=2,b=5,c=8,d=\frac{1}{10}$$

映射 g 为:

$$g(x)=x^3+2x+\cos(2x)+1$$

则可构造:

$$F(x)=f(x)+p[x^3+2x+\cos(2x)+1] \tag{15}$$

其中 $g(x)$ 在区间 I 上是连续非负映射,且

$$\begin{aligned}g'(x)&=3x^2+2-2\sin(2x)\\g(b)&=5^3+\cos(10)+11>-k_3[2^3+\cos(4)+5]\\&=\frac{79}{30}[2^3+\cos(4)+5]\end{aligned}$$

满足定理 2 条件,则对任意

$$\begin{aligned}0<p&<\min\left\{\frac{2-\frac{1}{10}}{10^3+\cos(20)+21},\frac{5-\frac{127}{6}+5\frac{79}{30}}{-\frac{79}{30}[2^3+\cos(4)+5]}\right\}\\&\approx0.00186\end{aligned} \tag{16}$$

映射 F 是混沌的.

将参数 p 作为鲁棒因子,则映射 F 关于 p 是鲁棒混沌的,分岔图如图 2 所示.

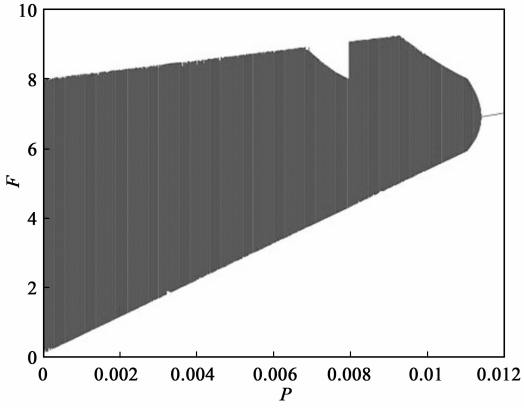


图2 映射F关于参数P的分岔图

3 S 盒的设计算法及分析

3.1 S 盒的设计算法

取映射式(15),其中参数 p 满足式(16)使得映射在区间上是混沌的.S 盒的设计算法如下:

(1)取初始条件 $x_0=5.4$,$p=0.001859$,迭代映射式(15)200 次,迭代后的最终结果作为下面运算的初始值 x_1.

(2)利用参数 p 的混沌鲁棒性,取参数区间为 $(10^{-6},0.0016)$,以 1.6×10^{-6} 为间距取值确定参数 p^i,$i=1,2,\cdots,N$,循环次数 $N=1000$,进行下面的循环,每次循环可产生一个 8×8 的 S 盒.

(3)对于第 i 次循环,先创建一个空的整数序列 S,取初始值 x_1,p^i,$m=6000$,迭代映射式(15)m 次,得到 $x=(x(1),x(2),\cdots,x(6000))$.

(4)选取序列:

$$y_1=x(1:2000),y_2=x(2001:4000),y_3=x(4001:6000)$$

(5)取参数 $k_1=\sqrt{6}$,$L=10^8$,构造序列:

$$s_1=k_1y_1-y_3,\quad s_2=y_1y_3$$

(6)利用伪随机数发生器及 s_1,s_2,y_2 序列,将序列变成[0,255]和[0,1]整数序列:

$$c_1=\mathrm{mod}(\mathrm{round}(\mathrm{abs}(L\frac{s_1-\max(s_1)}{\max(s_1)-\min(s_1)})),256) \tag{17}$$

$$c_3=\mathrm{mod}(\mathrm{round}(\mathrm{abs}(L\frac{s_2-\max(s_2)}{\max(s_2)-\min(s_2)})),256) \tag{18}$$

$$c_2=\mathrm{mod}(\mathrm{round}(\mathrm{abs}(Ly_2)),2) \tag{19}$$

(7)利用 c_2 从 c_1,c_3 中取值得到新的序列:

$$cc=\begin{cases}c_1, & \text{if}\quad c_2=0\\ c_3, & \text{if}\quad c_2=1\end{cases} \tag{20}$$

(8)依次将 cc 中元素放入空序列 S 中,出现与前面元素重复时放弃此次放入,继续放入后面新的元素,即可得到 0 ~ 255 的整数序列 $\overline{S}_i$.

(9)将 $\overline{S}_i$ 中的元素变成 8 位二进制型($x^0, x^1, \cdots, x^7$),利用 Affine 变换对其进行如下运算:

$$\boldsymbol{y} = \boldsymbol{A}x \oplus b$$

然后将其变成十进制 0 ~ 255 的序列,并转成 16 × 16 的表格形式,即得到一个 S 盒 S_i. 完成后转回(3),进行循环得到一批 S 盒.

其中

$$\boldsymbol{A} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}, \boldsymbol{b} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

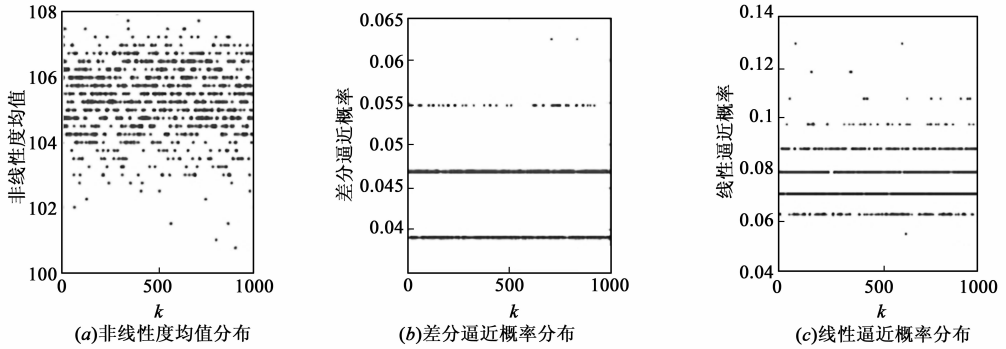
利用此算法,我们得到 1000 个 S 盒,从其抗差分、线性攻击的能力[13]进行分析:非线性度均值最小为 100.75,均在 100 以上;差分逼近概率均在 0.065 以下,最小达到 0.0390625,其中有 385 个 S 盒差分逼近概率达到 0.0390625;线性逼近概率均在 0.13 以下,有 S 盒线性逼近概率达到 0.05493164. 结果说明生成的 S 盒具有较好的密码学性能,且性能稳定,可为分组密码算法提供非线性基础. 其中非线性度的均值分布如图 3(a)所示,差分逼近概率分布如图 3(b)所示,线性逼近概率如图 3(c)所示.

3.2 性能分析

当参数取 $p = 0.0010202$ 时,将得到的 S 盒记为 S_1,如表 1 所示,并对其性能分析.

(1)非线性度[13],差分逼近[14]及线性逼近概率[15]

盒 S_1 的非线性度,差分逼近及线性逼近概率如表 2 所示,其中文献[11,16,17]的分析结果也在表中列出. 从表中看出 S_1 的非线性度均匀稳定,均在 100 以上;差分逼近与线性逼近概率很小,能较好的抵抗差分与线性攻击.



(a)非线性度均值分布　(b)差分逼近概率分布　(c)线性逼近概率分布

图3　性能分析图

表 1　参数 $p = 0.0010202$ 生成的 S 盒 S_1

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

(2)严格雪崩及比特间独立性[13]

盒 S_1 的相关矩阵如表 3 所示,比特间相关矩阵如表 4 所示.分析结果如表 5 所示,其中文献[11,16,17]的两种性能在表中也分别列出,从表中看出 S_1 的比特间相关矩阵均值为 0.5007,非常逼近标准值 0.5,说明该 S 盒布尔函数的异或运算近似满足严格雪崩.

表 2 非线性度,差分逼近及线性逼近概率对比

S 盒	非线性度最小值	非线性度最大值	非线性度均值	差分逼近概率	线性逼近概率
S_1	100	110	105.25	0.0390625	0.054932
文献[11]	103	109	105.10	0.0390625	0.066467
文献[16]	96	108	103.50	0.0390625	0.092835
文献[17]	108	110	108.00	0.0390625	0.079101

表 3 盒 S_1 的相关矩阵

0.561	0.548	0.541	0.503	0.535	0.578	0.483	0.543
0.421	0.505	0.540	0.466	0.577	0.498	0.451	0.491
0.445	0.466	0.462	0.500	0.478	0.436	0.398	0.539
0.522	0.444	0.461	0.554	0.436	0.505	0.462	0.593
0.502	0.504	0.466	0.522	0.455	0.538	0.503	0.452
0.401	0.517	0.483	0.509	0.558	0.524	0.495	0.561
0.532	0.499	0.581	0.530	0.576	0.527	0.550	0.497
0.514	0.391	0.419	0.512	0.505	0.493	0.528	0.468

表 4 盒 S_1 的比特间相关矩阵

0	0.483	0.555	0.480	0.536	0.521	0.514	0.506
0.483	0	0.499	0.494	0.522	0.510	0.505	0.499
0.555	0.499	0	0.496	0.466	0.509	0.492	0.493
0.480	0.494	0.496	0	0.507	0.485	0.493	0.475
0.536	0.522	0.466	0.507	0	0.495	0.513	0.479
0.521	0.510	0.509	0.485	0.495	0	0.499	0.487
0.514	0.505	0.492	0.493	0.513	0.499	0	0.507
0.506	0.499	0.493	0.475	0.479	0.487	0.507	0

表 5 严格雪崩及比特间独立性对比

S 盒	相关矩阵最小值	相关矩阵最大值	比特间相关矩阵均值
S_1	0.3910	0.5930	0.5007
文献[11]	0.4140	0.6093	0.4982
文献[16]	0.3906	0.5859	0.4992
文献[17]	0.4062	0.5781	0.5026

4 结论

在动力学系统的研究中,混沌系统及系统对初始值和参数值的敏感性等特性 为系统的应用研究提供了工具.其中鲁棒特性则保证了系统在参数域中混沌的稳定性.本文在 Li-York 混沌判别定理的基础上提出了一维空间中构造鲁棒混沌的定理.将多项式和三角函数作为非线性部分用于构造分段非线性鲁棒混沌映射.本文提出的三个基于混沌映射的伪随机数发生器通过大数相乘取模的方法将混沌变量转化成 0 ~ 255 的整数变量,进而提出了批量生成 S 盒的算法,并通过分析检测出 S 盒具有较高的非线性度(均值都在 100 之上);近似满足严格雪崩,当改变 1 比特输入时,输出变量发生改变的概率接近于标准值 0.5.并且具有较小的差分及线性逼近概率,能有效的抵抗差分与线性密码分析.

参考文献

[1] Xing J P, Zou X C, Guo X. Ultra-low power S-boxes architecture for AES CLC[J]. The Journal of China Universities of Posts and Telecommuications, 2008, 15(1): 112 – 117.

[2] 冯登国,吴文玲.分组密码的设计与分析[M].北京:清华大学出版社,2000.64 – 110.
Feng D G, WU W L. Design and Analysis of Block Ciphers [M]. Beijing: Tsinghua University Press, 2000. 64 – 100. (in Chinese)

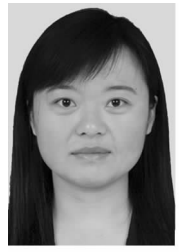
[3] Li T Y, Yorke J A. Period three implies chaos[J]. The American Mathematical Monthly, 1975, 82(10): 985 – 992.

[4] Gavrielides A, Kovanis1 V, Nizette M, Erneux T, Simpson T B. Period three limit-cycles in injected semiconductor lasers [J]. Journal of Optics B: Quantum and Semiclassical Optics, 2002, 4(1): 20 – 26.

[5] 罗佑新.曲柄滑块机构综合的三周期牛顿混沌法研究

[J].哈尔滨工业大学学报,2009,41(3):187 – 189.
Luo Y X. 3-cycle Newton chaos iteration solution method and its application to function synthesis of planar crank-slide mechanism[J]. Journal of Harbin Institue of Technology, 2009, 41(3):187 – 189.(in Chinese)
[6] Lee M. H. Three-cycle problem in the logistic map and Sharkovskii's theorem[J]. Acta Physica Polonica B, 2011, 42(5):1071 – 1080.
[7] Hassene G, Nahla K, Safya B. Period-three route to chaos induced by a cyclic-fold bifurcation in passive dynamic walking of a compass-gait biped robot[J]. Commun Nonlinear Sci Numer Simulat, 2012, 17(1):4356 – 4372.
[8] Wang Y, Wong K W, Li C B, Li Y. A novel method to design S-box based on chaotic map and genetic algorithm[J]. Physics Letters A, 2012, 376(1):827 – 833.
[9] Wang G W, Luo S X, He L, Yin G. A method for design and analysis of S-box based on logistic maps[A]. 2012 2nd International Conference on Computer Science and Network Technology Changchun[C]. Changchun: Northeast Normal University Changchun, 2012. 826 – 829.
[10] Su B Y, Xu G, Zhao G, Liao Y. A method for obtaining chaos-based S-box via a PWLCM[J]. Advanced Materials Research, 2013, 651(1):885 – 890.
[11] Ozkaynak F, Yavuz S. Designing chaotic S-boxes based on time-delay chaotic system[J]. Nonlinear Dyn, 2013, 74(1): 551 – 557.
[12] Khan M, Shah T, Mahmood H, Gondal M A, Hussain I. A novel technique for the construction of strong S-boxes based on chaotic Lorenz systems[J]. Nonlinear Dyn, 2012, 70(1): 2303 – 2311.
[13] Dawson M, Tavares S. Advances in Cryptology: Proceedings of EUROCRYPT'91[M]. Germany: Springer-Verlag, 1991. 5 – 50.
[14] Biham E, Shamir A. Advances in Cryptology-CRYPTO'90[M]. Germany: Springer-Verlag, 1991. 1 – 30.
[15] Matsui M. Advances in Cryptology—EUROCRYPT'93[M]. Germany: Springer Berlin Heidelberg, 1994. 350 – 400.
[16] Asim M, Jeoti V. Efficient and simple method for designing chaotic S-boxes[J]. ETRI Journal, 2008, 30(1):170 – 172.
[17] Wang Y, Lei P. An improved method to obtaining S-box based on chaos and genetic algorithm[J]. The Hong Kong Institution of Engineers Transactions, 2012, 19(4):53 – 58.

作者简介



韩丹丹　女,1989 年出生于山东省济宁市兖州市,北京科技大学自动化学院博士.主要研究方向为复杂混沌动力学系统和通信安全,合作发表期刊论文和会议论文 8 篇.
E-mail:hxu1204@163.com

闵乐泉　男,1951 年出生于北京,现为北京科技大学教授,博士生导师.主要研究方向:混沌系统的广义的同步与安全通信;复杂系统建模;细胞神经网络模板的鲁棒性设计.合作发表期刊论文和会议论文 200 余篇,其中被 SCIE 收录 60 余篇,EI 收录 100 余篇.
E-mail:minlequan@sina.com