计算机科学
COMPUTER SCIENCE

基于抗退化混沌系统和初等元胞自动机的动态S盒设计

赵耿, 高世蕊, 马英杰, 董有恒

引用本文

赵耿, 高世蕊, 马英杰, 董有恒. 基于抗退化混沌系统和初等元胞自动机的动态S盒设计[J]. 计算机科学, 2023, 50(11): 333-339.

ZHAO Geng, GAO Shirui, MA Yingjie, DONG Youheng. Design of Dynamic S-box Based on Anti-degradation Chaotic System and Elementary Cellular Automata [J]. Computer Science, 2023, 50(11): 333-339.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.220900026

基于抗退化混沌系统和初等元胞自动机的动态S盒设计

赵　耿[1,2]　高世蕊[1]　马英杰[1]　董有恒[2]
1 北京电子科技学院网络空间安全系　北京 100071
2 北京邮电大学网络空间安全学院　北京 100089
(zhaogeng@besti.edu.cn)

摘　要　S盒是多数分组密码算法的基本非线性模块,可以满足分组密码算法的混淆、扩散要求。为了提高混沌S盒的安全性,文中利用抗退化混沌系统生成S盒元素,基于初等元胞自动机生成S盒检索表的方式来生成S盒。抗退化混沌系统可以避免发生Skew Tent系统进入不动点的情况,消除低精度下系统进入短周期的现象。因为初等元胞自动机的迭代规则为二元域上的运算,且满足时空上的离散性,所以,将初等元胞自动机运用到混沌分组密码中时,不用考虑动力学退化的问题。当初等元胞自动机的迭代规则为全局混沌规则时,只要元胞个数足够,就可以保证输出的伪随机性。利用初等元胞自动机生成S盒的检索表,在保证S盒设计的混淆原则的同时还可以简化S盒的生成步骤。最后对所设计的S盒进行安全性分析对比,实验结果表明,所提方法生成的S盒具有良好的安全性,满足分组密码的混淆、扩散原则,可用于混沌分组密码算法设计中。

关键词:S盒;抗退化;混沌;初等元胞自动机;Lorenz系统;Skew Tent系统
中图法分类号　TP309.7

Design of Dynamic S-box Based on Anti-degradation Chaotic System and Elementary Cellular Automata

ZHAO Geng[1,2],GAO Shirui[1],MA Yingjie[1] and DONG Youheng[2]
1 Department of Cyber Space Security,Beijing Electronic Science and Technology Institute,Beijing 100071,China
2 School of Cyberspace Security,Beijing University of Posts and Telecommunications,Beijing 100089,China

Abstract　S-box is the basic non-linear module of most block cipher algorithms,which can meet the obfuscation and proliferation requirements of block cipher algorithms. In order to improve the safety of chaotic S-boxes,this paper uses an anti-degenerative chaotic system to generate S-box elements,and generates an S-box based on elementary cellular automata to generate S-box retrieval table. The anti-degradation chaotic system can avoid the situation that the Skew Tent system enters the fixed point and eliminate the phenomenon of the system entering a short period of time at low precision. Because the elementary cellular automata is an operation on the binary domain and satisfies the discreteness in time and space,the elementary cellular automata is applied to the chaotic block cipher without considering the problem of dynamics degradation. In the case of global chaos rules,if the number of cells is enough,the pseudorandom of the output can be guaranteed. The use of elementary cellular automata to generate a search table for the S-box can not only ensure the confusion principle of S-box design,but also simplify the steps of S-box generation. Finally,the security analysis and comparison of the designed S-box shows that the S-box generated by the proposed method has good security,satisfies the principle of confusion and diffusion of block ciphers,and can be used in the design of chaotic block cipher algorithms.

Keywords　S-box,Anti-degradation,Chaos,Elementary cellular automata,Lorenz system,Skew Tent system

1　引言

S盒是多数分组密码算法中的唯一非线性部件,在分组密码算法中起着混乱和扩散的作用。S盒的设计方法主要有以下几种:随机生成S盒,如果是动态生成S盒,需要花费很长时间;通过一些性能好的S盒进行改造生成新的S盒,比如Serpent算法[1]所用的S盒就是基于DES中S盒的要求构造的;使用某个特定的密码结构构造S盒,比如CRYPTON v0.5[2]中使用的S盒就是利用3轮Feistel结构来构造的;利用数学函数构造,包括指数函数、对数函数、幂函数、混沌映射

到稿日期:2022-09-05　返修日期:2022-12-15
基金项目:北京高校"高精尖"学科建设项目(3201017);国家自然科学基金(61772047)
This work was supported by the Sharp Subject Project Construction in Colleges and Universities in Beijing(3201017) and National Natural Science Foundation of China(61772047).
通信作者:高世蕊(gao_sr2022@163.com)

等，例如 SAFER 系列算法[3-4]、AES 算法[5]等；基于几乎完全非线性置换设计，比如 MISTY 算法[6]中使用的 S 盒；此外还有基于人工智能遗传算法设计[7]、基于电路结构设计等。

本文使用的方法是利用数学函数构造，即利用抗退化混沌系统以及初等元胞自动机生成动态 S 盒。

混沌系统具有伪随机性、遍历性、初始条件敏感性、长期不可预测性等特点，符合密码设计的安全性要求。本文利用 Lorenz 系统和 Skew Tent 系统生成有限精度下的抗退化混沌系统，改善了 Skew Tent 混沌系统的退化现象。

元胞自动机(Cellular Automata，CA)是由 Neumann 等[8]于 1948 年提出的一种时间和空间上都离散的动力系统，用来模拟生命系统的自我复制现象[9]，通过不同的迭代规则可以产生较为复杂的变换，组合后能实现混淆和扩散[10]。CA 主要由元胞、元胞空间、元胞邻居、迭代规则和边界条件组成[11]。

初等元胞自动机(Elementary Cellular Automata，ECA)是一种简单的一维元胞自动机[12]，其输入输出均为二元域上的计算，不存在普通混沌系统二次量化的过程，因而保证了初等元胞自动机良好的动力学性能。在选择好迭代规则的情况下，还可以保证生成序列的长周期性和伪随机性。

本文利用抗退化混沌系统生成的混沌序列生成 S 盒的元素值 S_0；将混沌序列量化后的值作为初等元胞自动机的输入，初等元胞自动机经过 N 次迭代产生 S 盒的检索表 S_1，利用 S_1 检索元素表 S_0 生成最后的 S 盒。通过改变混沌系统的初值，可以生成不同的 S 盒。

本文第 2 章介绍抗退化混沌系统；第 3 章介绍初等元胞自动机；第 4 章描述本文 S 盒的构造方法；第 5 章对 S 盒的安全性进行分析对比。

2 抗退化混沌系统

2.1 混沌系统

本文使用的抗退化混沌系统是 Lorenz 系统和 Skew Tent 系统经过扰动生成的。

2.1.1 Lorenz 系统

Lorenz 混沌系统[13]起源于气象研究，是美国气象学家 Lorenz 在研究大气对流模型时提炼的三维方程，计算式如式(1)所示：

$$\begin{cases}\dfrac{\mathrm{d}y}{\mathrm{d}t}=\delta(y-x)\\ \dfrac{\mathrm{d}y}{\mathrm{d}t}=\gamma x-y-xz\\ \dfrac{\mathrm{d}z}{\mathrm{d}t}=xy-\beta z\end{cases}\tag{1}$$

其中，δ,β,γ 为系统参数。

利用简单 Euler 算法将 Lorenz 系统离散化，离散后公式如式(2)所示：

$$\begin{cases}x_{n+1}=T\times\delta\times(y_n-x_n)+x_n\\ y_{n+1}=T\times(\gamma\times x_n-y_n-x_n\times z_n)+y_n\\ z_{n+1}=T\times(x_n\times y_n-\beta\times z_n)+z_n\end{cases}\tag{2}$$

其中 x_n,y_n,z_n 表示当前状态；x_{n+1},y_{n+1},z_{n+1} 表示下一时刻状态；T 表示采样时间间隔，$T=0.002$。

2.1.2 Skew Tent 系统

Skew Tent 系统是离散混沌映射系统，为单峰映射，公式如式(3)所示：

$$x_{n+1}=\begin{cases}\dfrac{x_n}{q}, & 0<x_n\leqslant q\\ \dfrac{1-x_n}{1-q}, & q<x_n<1\end{cases}\tag{3}$$

其中，q 为系统参数，$q\in(0,1)$，$x_n\in[0,1]$。

根据文献[14]，由 Skew Tent 系统的 Lyapunov 指数可知，当 Skew Tent 映射的参数处于区间 $[0.2,0.8]$ 时，系统具有良好的混沌性。

2.1.3 抗退化混沌系统

将 Lorenz 系统作为扰动源，将 Skew Tent 系统作为扰动对象，将离散后的 Lorenz 输出转到 Skew Tent 系统的活动区间，即(0,1)区间。

将 Lorenz 系统离散后的一个输出序列作为 Skew Tent 的参数。方法如下：选取输出序列中分布均匀的一部分作为种子源产生 Skew Tent 的参数 q，并将 q 控制在 $[0.2,0.8]$。将 Lorenz 系统的其余两项输出序列作为 Skew Tent 系统的输出扰动。

生成新的抗退化混沌系统如式(4)所示：

$$k=chaotic(T,k_0,t,d)\tag{4}$$

其中，k 是生成的混沌序列，T 为采样间隔，k_0 是混沌系统的初值，t 为迭代次数，d 为计算精度。

因改进后的 Skew Tent 系统 q 值是不断变换的，故系统不会陷入不动点。

2.2 性能分析

对改进后的混沌系统进行轨迹图、初值敏感性以及回归映射的对比分析。

2.2.1 轨迹图对比

Skew Tent 系统经过一定的迭代后，会出现周期现象，图 1 和图 2 分别给出了 Skew Tent 系统和改进后系统在计算精度为 4 时的轨迹图。

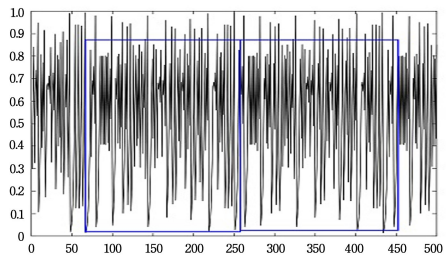


图 1 Skew Tent 轨迹图(电子版为彩图)

Fig. 1 Skew Tent trajectory

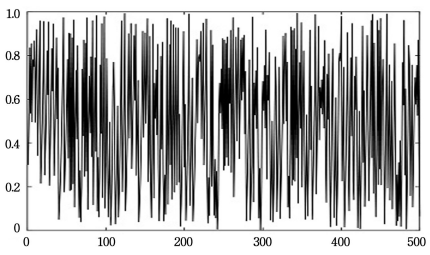


图 2 改进系统轨迹图

Fig. 2 Improved system trajectory

如图 1 中的蓝色线框所示，一个线框的宽度就是 Skew Tent 系统生成序列的一个周期长度，而改进后系统在迭代 500 次后并未出现周期现象，证明该扰动方法提高了系统的抗退化性。

2.2.2　初值敏感性

图 3 给出了抗退化混沌系统在初值分别为 0.3 和 0.300 000 000 1 时前 100 个序列值的轨迹对比图。从图中可以看出抗退化混沌系统在迭代 30 次左右时轨迹不再重合，开始出现大的区别，说明系统具有良好的初值敏感性。

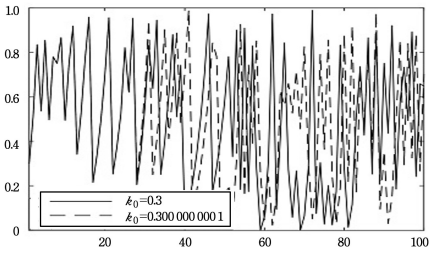
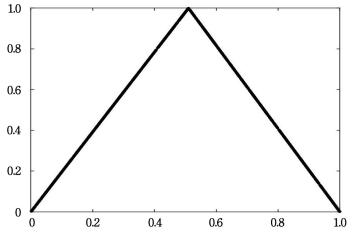


图 3　初值敏感性测试图

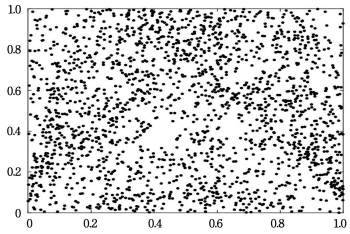
Fig. 3　Chart of initial value sensitive line test

2.2.3　回归映射

回归映射形状的复杂度可以间接反映系统的复杂程度。图 4 给出了原始 Skew Tent 映射以及本文系统的回归映射，其中原始 Skew Tent 映射的参数为 $q=0.51$，各系统的初值为 $k_0=0.3$，计算精度为 5，迭代为 1 000 次。



(a)Skew Tent



(b)Our scheme

图 4　各系统的回归映射图

Fig. 4　Regression map of each system

从图 4 中可以看到原始系统的回归映射是一个明显的三角形，本方案改进后的回归映射较为均匀地分布在整个平面，突破了原始的三角形，说明改进后的系统有更好的伪随机性。

3　初等元胞自动机

初等元胞自动机(ECA)是一种简单的一维元胞自动机[12]，元胞状态有两种，用{0，1}表示，元胞半径为 1，元胞邻居就是其左右两元胞。边界条件一般是周期的，表达式如式(5)所示：

$$\begin{cases} i+1=1, i=L \\ i-1=L, i=1 \end{cases} \tag{5}$$

其中，L 表示 ECA 中元胞的个数，i 表示元胞索引。

在 ECA 中，一个元胞的当前状态由其本身和两个邻居的前次状态共同决定，表达式如式(6)所示：

$$s_{t+1}(i+1)=f_r(s_t(i-1),s_t(i),s_t(i+1)) \tag{6}$$

其中，t 表示时间维度，i 表示空间维度，$s_t(i)$表示第 i 个元胞在 t 时刻的状态值，f 为布尔函数，r 指 ECA 的迭代规则。图 5 给出了 ECA 为循环边界条件时的迭代过程。

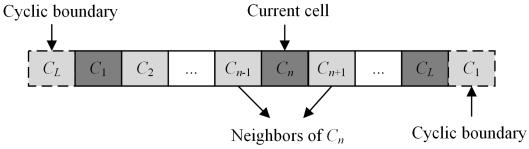


图 5　ECA 为循环边界条件时的迭代过程

Fig. 5　Iterative process when ECA is cyclic boundary condition

本文选用的 ECA 符合循环边界条件，即最后一个元胞与第一个元胞互为邻居，彼此参与对方下一状态的生成过程。

ECA 的迭代规则可以根据迭代结果的性质分为 5 类[15-16]：无效规则、固定点规则、周期规则、全局混沌规则和局部混沌规则。

根据式(6)可知 ECA 的布尔函数 f 是一个二元域上的映射，输入是 3 个状态值，输出为一个状态值，对应到二进制位，就是输入三位二进制数，输出一位。8 种输入，对应到输出是{0，1}两种状态，总共有 2^8 种情况。

当 $r=225$ 时，布尔函数 f 的输入输出如表 1 所列。

表 1　布尔函数 f 的输入输出

Table 1　Input and output of Boolean function f

The iteration results	Binary number							
$s_t(i-1)$	1	1	1	1	0	0	0	0
$s_t(i)$	1	1	0	0	1	1	0	0
$s_t(i+1)$	1	0	1	0	1	0	1	0
$s_{t+1}(i)$	1	1	1	0	0	0	0	1

因为 ECA 的布尔函数存在多种输入对应同一个输出的情况，所以 f 不可逆，是非线性函数，但在 ECA 的初值和迭代规则确定的情况下，可以复现出正确结果。在输入和迭代规则未知的情况下，利用数学方法分析极为困难，这一特性适用于 S 盒的构造，可以增大数学分析的难度。

4　S 盒构造方法

本文的 S 盒构造是利用混沌系统和初等元胞自动机结合生成，具体构造方法如下：

第 1 步　初始化混沌系统：随机产生一个(0，1)之间的小数，作为系统初值 k_0，给定 $T=0.002$，给定计算精度 d 和迭代次数 t。

第 2 步　利用截取位数法对第 1 步产生的混沌序列 k 进行处理：截取 k 中元素的小数点后第 3，4，5 位构成一组新的由 3 位十进制数组成的序列 k_1；再对 k_1 进行隔 2 取值，形成一组新的序列 k_2，舍弃前 200 个后再选取 256 个元素组成新的数组 K_1。

第 3 步　对第二步产生的 K_1 进行升序排列，并将 K_1 的索引同时跟随排列并存入一个新的数组 S_0 中，S_0 中存储的是值域为[1，256]的 256 个整数，对 S_0 中的元素整体进行

“−1”操作将元素值域降为[0,255]。

第 4 步 初始化 ECA:给定 ECA 的元胞个数 L,迭代规则 $r=225$,给长为 L 的 ECA 赋初始状态。大量实验表明,在全局混沌的迭代规则下,都可生成良好的 S 盒,在此以全局混沌规则 225 为例。

对第一步产生的混沌序列 k 进行量化处理,将序列中的数据转为 8 位无符号整数,如式(7)所示:

$$K_n=UINT8(floor(k_n*(2^8))) \tag{7}$$

其中,n 为序列 k 和 K 的第 n 个元素。对序列 K 中的元素取相同的比特位 $bitKi$,构成长度为 n 的 0,1 序列 $bitk$;舍弃 $bitk$ 的前 200 位,取 L 位即 $bitk(201:201+L)$作为 ECA 的初始状态序列。

第 5 步 将 ECA 循环 N 次,存储在 $N\times L$ 的二维数组 $A_{N\times L}$ 中,选取数组 $A_{N\times L}$ 的中间 9 列构成新的数组 $A_{1_{N\times 9}}$,将数组 $A_{1_{N\times 9}}$ 的每行 0,1 值看作 9 位的二进制数,并转为十进制数,形成新的数组 $A_{2_{N\times 1}}$,如式(8)所示:

$$A_{2_{N\times 1}}=\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{19} \\ a_{21} & a_{22} & \cdots & a_{29} \\ \vdots & \vdots & \ddots & \vdots \\ a_{N1} & a_{N2} & \cdots & a_{N9} \end{bmatrix}\times\begin{bmatrix} 256 \\ 128 \\ \vdots \\ 1 \end{bmatrix} \tag{8}$$

$A_{2_{N\times 1}}$ 中的元素值域范围是[0,511],对数组 $A_{2_{N\times 1}}$ 中的元素进行 mod 257 运算构成 $A_{3_{N\times 1}}$,$A_{3_{N\times 1}}$ 中的元素值域为[0,256]。

第 6 步 初始化一个空数组 $s_{1_{1\times N}}$,对数组 $A_{3_{N\times 1}}$ 进行检索,将非零值以及数组 $s_{1_{1\times N}}$ 中没有的值存入 $s_{1_{1\times N}}$,具体过程如图 6 所示,执行完以下循环后,提取 $s_{1_{1\times N}}$ 的非零值构成 S_1。

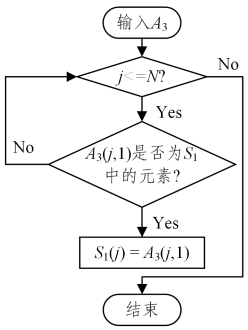


图 6 $S_{1_{1\times N}}$ 形成过程

Fig. 6 $S_{1_{1\times N}}$ formation process

第 7 步 将 S_1 作为索引表,最终 S 盒的形成方式如式(9)所示,最后将 S 数组由 1×256 换为 16×16。

$$S=S_0(S_1(m)),m=1,2,3,\cdots,256 \tag{9}$$

第 8 步 从第一步开始,重新赋予系统初值 k_0,进行 M 次循环,可以产生 M 个 S 盒。

为了保证 ECA 具有长周期性和伪随机性,我们将 L 设置为 200,则第 5 步的中间 9 列是数组 $A_{N\times L}$ 的第 96～104 列。为了保证第 6 步中的 S_1 中元素是 1～256 的一一映射,将迭代次数 N 值设置为 10000。

5 S 盒安全性分析

S 盒是多数分组密码的唯一非线性部件,因此需要对 S 盒的安全性进行分析。

5.1 批量 S 盒安全性分析

改变系统初值 k_0,进行 $M=500$ 次循环,生成 500 个 S 盒,对生成的 S 盒进行批量分析,生成的分析图如图 7－图 11 所示。从图 7 可知,500 个 S 盒中有一半的差分均匀性值为 10;从图 8 可知 500 个 S 盒的非线性度的均值都在 100 以上;由图 9 可知,500 个 S 盒的相关矩阵的平均值分布大部分处于[0.495,0.505]之间,与 0.5 的差值范围是[−0.005,+0.005],说明满足 S 盒的严格雪崩准则要求;由图 10 可知,500 个 S 盒的输出比特间的平均非线性度大部分分布在 102 以上;由图 11 可知,500 个 S 盒的输出比特间相关矩阵的平均值都集中在 0.5 左右,大部分与 0.5 的差值范围在[−0.005,+0.010]区间内。

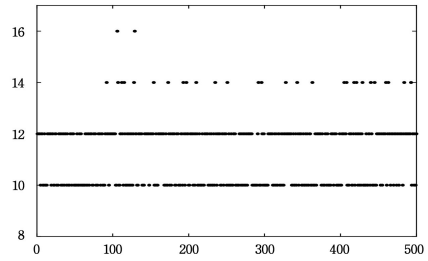


图 7 S 盒最大差分分布图

Fig. 7 Diagram of S-box maximum difference distribution

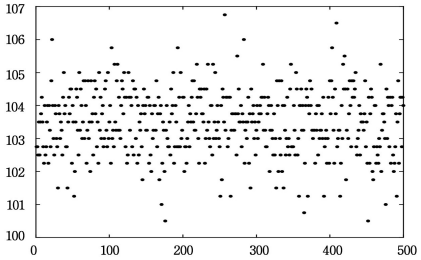


图 8 平均非线性度分布图

Fig. 8 Diagram of average nonlinearity distribution

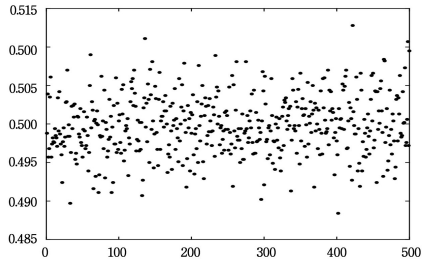


图 9 相关矩阵的平均值分布图

Fig. 9 Average value distribution of correlation matrix

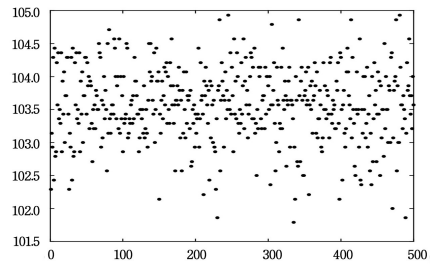


图 10 输出比特间的平均非线性度分布图

Fig. 10 Average nonlinearity distribution between output bits

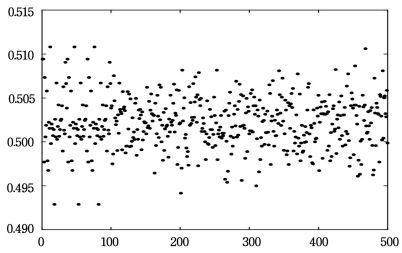


图 11　输出比特间的相关矩阵的平均值分布图

Fig. 11　Average value distribution of correlation matrix between output bits

5.2　S 盒单盒安全性分析对比

从所得到的 S 盒中筛选出如图 12 所示的 S 盒数据，进行性能分析对比。

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

图 12　单个 S 盒示例

Fig. 12　Example of single S-box

5.2.1　双射特性

在分组密码算法，尤其是在代替-置换型分组密码中的 S 盒要求必须是双射的。文献[17]给出了验证 S 盒双射的方法：S 盒满足双射的充分必要条件是各分量布尔函数 f_i 的线性运算之和为 2^{n-1}，如式(10)所示：

$$wt\left(\sum_{i=1}^{n} a_i f_i\right)=2^{n-1} \tag{10}$$

其中，$a_i\in\{0,1\}$，$(a_1,a_2,\cdots,a_n)\neq(0,0,\cdots,0)$；$wt()$表示汉明权重。如果式(10)成立，则 f 是 0，1 平衡的，且是双射的。

在本文中，S 盒是一个有着 256 位元素的检索表，所以 $n=8$。根据式(10)可知，满足双射性的标准为 128，本文 S 盒所有分量的布尔函数之和均为 $2^{8-1}=128$，因此该 S 盒是双射的。

5.2.2　非线性度

非线性度(Nonlinearity)是衡量一个 S 盒抵抗线性攻击的重要指标，一个 S 盒的非线性度越高，其抵抗线性攻击的能力越强。令 $f:F_2^n\to F_2^m$ 是一个 n 元布尔函数，则 $f(x)$的非线性度[18]如式(11)所示：

$$N_f=\min_{l\in L_n} d_H(f,l) \tag{11}$$

其中，L_n 表示全部 n 元线性和仿射函数集合，$d_H(f,l)$表示 f 和 l 的汉明距离。

但在实际应用中，计算 S 盒的非线性度一般使用的是 Walsh-Hadamard 变换，利用 Walsh 谱表示 $f(x)$的非线性度，具体表达式如式(12)所示：

$$S_{(f)}(\omega)=\sum_{\omega\in GF(2^n)}(-1)^{f(x)\oplus x\cdot\omega} \tag{12}$$

其中，$x\cdot\omega$ 表示 x 与 ω 的点积 。本文构造 S 盒的非线性度最大值为 108，最小值为 104，平均值为 106。表 2 列出了 S 盒的非线性度对比，从表中结果可以看出，本文所构造的 S 盒有较强的抵抗线性攻击的能力。

表 2　S 盒非线性度

Table 2　S-box nonlinearity

S-box	Nonlinearity								Mean value
Our scheme	106	106	104	106	106	108	106	106	106.00
Ref.[18]	106	106	104	106	106	104	106	104	105.25
Ref.[19]	106	108	102	106	106	106	108	106	106.00
Ref.[20]	108	104	102	108	98	104	108	108	105.00
Ref.[21]	104	106	106	106	108	106	104	104	105.50

5.2.3　差分均匀度

差分均匀度(Differential Uniformity)[22]是判断 S 盒在密码算法中抗差分能力强弱的重要指标。

文献[23]中指出，S 盒的差分均匀性指当满足式(13)时，称 $S(x)$是差分均匀的 。S 盒的差分均匀性越小越好。

$$\delta_S=\frac{1}{2^n}\max_{\alpha\in F_2^n\setminus\{0\}}\ \max_{\beta\in F_2^m}\#\{x\mid S(x\oplus\alpha)-S(x)=\beta\} \tag{13}$$

在实际应用中，一般使用差分逼近概率 DP_f[24]表示输入输出的异或情况，如式(14)所示：

$$DP_f=\max_{\Delta x\neq 0\ \Delta y}\left(\frac{\#\{x\in X\mid f(x)\oplus f(x\oplus\Delta x)=\Delta y\}}{2^n}\right) \tag{14}$$

其中，x 为所有可能输入的集合；2^n 是集合的元素个数，DP_f 表示给定一个输入差分 Δx，输出为 Δy 的最大可能性。

表 3 列出了 S 盒最大差分值的对比结果，从表中可以看出，各个 S 盒的最大差分值都可以达到 10，说明各个 S 盒都有较好的抗差分能力。

表 3　最大差分值对比

Table 3　Comparison of maximum difference values

S-box	Differential maximum	Differential Approximation probability
Our scheme	10	0.0390625
Ref.[18]	10	0.0390625
Ref.[19]	10	0.0390625
Ref.[20]	10	0.0390625
Ref.[21]	10	0.0390625

5.2.4　严格雪崩准则

严格雪崩准则(Strict Avalanche Criterion，SAC)是由 Webster 和 Tavare 提出的[25]，用来衡量 S 盒的输入改变量和输出改变量之间的随机性，也是 S 盒设计的重要指标之一。

定义 $S=(f_1,\cdots,f_m):F_2^n\to F_2^m$ 满足雪崩效应，指改变输入的 1 比特，大约有一半的输出比特会改变。在实际使用时，S 盒的严格雪崩准则按照矩阵方式来计算[26]，矩阵中的理想值为 0.5，如果矩阵中的值与理想值都接近，则认为这个 S 盒满足严格雪崩准则。

表 4 列出了 S 盒的相关矩阵平均值对比，从中可以看出，本文构造 S 盒的相关矩阵平均值与 0.5 相差 0.0014，图 13 是各个 S 盒相关矩阵平均值与 0.5 的差值分析图。从图中可以看出本文方法构造的差值高于文献[19]，低于其余 3 种方法，说明本文改进的 S 盒可以较好地满足严格雪崩准则。

表 4 S 盒的相关矩阵平均值对比

Table 4 Comparison of mean values of correlation matrices for S-boxes

S-box	Mean value
Our scheme	0.5014
Ref.[18]	0.4981
Ref.[19]	0.4993
Ref.[20]	0.5034
Ref.[21]	0.5065

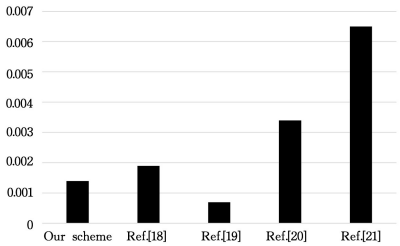


图 13 各 S 盒相关矩阵平均值与 0.5 的差值

Fig. 13 Difference between the mean of each S-box correlation matrix and 0.5

5.2.5 输出比特间独立性

输出间比特间独立性是由 Webster 和 Tavare 首次提出的标准[25]。

文献[27]指出，对于其中任意两个布尔函数 f_j，f_k（$j \neq k$），f_j，f_k 是 S 盒的两个输出比特，如果 $f_j \oplus f_k$ 高度非线性且尽可能地满足严格雪崩准则，则可以保证在输入一比特位改变后，输出的比特间相关性接近于 0。

通过验证 S 盒的任意两个输出比特间的异或是否满足严格雪崩准则来证明 S 盒是否满足输出比特间独立性。

表 5 和表 6 列出了 S 盒的输出比特间-平均非线性度、输出比特间-相关矩阵的平均值。图 14 和图 15 分别是各 S 盒的输出比特间-平均非线性度对比图以及 S 盒的输出比特间相关矩阵平均值与 0.5 的差值分析图。从图 14 中可以看出本文构造的 S 盒 BIC-nonlinearity 平均值高于其余 4 种 S 盒，从表 6 中可以看出本文构造的 S 盒的 BIC-SAC 平均值与 0.5 仅相差 0.00007，从图 15 中可以看出本文构造的 S 盒的输出比特间相关矩阵的平均值远小于其余 4 个 S 盒。综上可以得出本文方案构造的 S 盒的输出比特间独立性更强。

表 5 S 盒输出比特间平均非线性度

Table 5 S-box BIC-nonlinearities

S-box	BIC-Nonlinearity
Our scheme	103.79
Ref.[18]	103.28
Ref.[19]	102.57
Ref.[20]	102.50
Ref.[21]	103.57

表 6 S 盒 BIC-SAC 值对比

Table 6 Comparison of S-box BIC-SAC values

S-box	BIC-SAC
Our scheme	0.50007
Ref.[18]	0.50490
Ref.[19]	0.49990
Ref.[20]	0.49720
Ref.[21]	0.50310

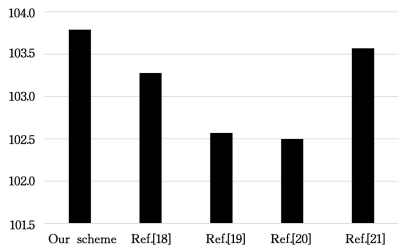


图 14 S 盒输出比特间平均非线性度对比

Fig. 14 Comparison of S-box BIC-nonlinearities

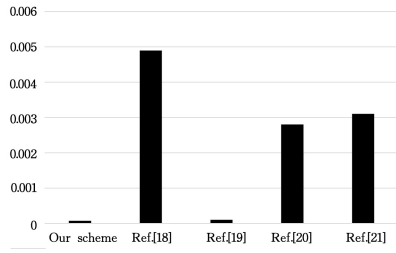


图 15 各 S 盒输出比特间相关矩阵的平均值与 0.5 的差值

Fig. 15 Difference between the BIC-SAC value of each S-box and 0.5

5.2.6 代数次数

代数次数（Algebraic Degree，AD）用来衡量 S 盒抵抗高阶差分密码分析的能力，表 7 列出了各个 S 盒的代数次数。

表 7 各 S 盒的代数次数

Table 7 Algebraic degrees of each S-box

S-box	AD
Our scheme	7
Ref.[18]	7
Ref.[19]	7
Ref.[20]	8
Ref.[21]	8

从表 7 中可以看出本文构造的 S 盒代数次数与文献[18]、文献[19]均为 7，虽略少于文献[20]和文献[21]，但是可以有效抵抗高阶差分密码分析。

结束语 本文首先提出了一种基于 Lorenz 和 Skew Tent 的抗退化混沌系统，避免了 Skew Tent 系统出现不动点的情况，提高了混沌系统的抗退化能力。

本文提出了一种利用混沌序列生成 S 盒的元素表、利用 ECA 生成 S 盒的检索表的 S 盒构成方式。通过对产生的 S 盒进行安全系分析对比，发现其具有良好的密码学性能。而 ECA 具有时空上的离散性，运用到密码体制中不会出现动力学退化的现象，当初等元胞自动机的迭代规则为全局混沌规则时，只要元胞个数足够，就可以保证输出的伪随机性。利用 ECA 生成 S 盒的检索表，一方面可以保证 S 盒的混淆原则，另一方面因 ECA 布尔函数具有不可逆性，所以大大提高了数学分析难度。Skew Tent 系统的输入在(0,1)之间，除 0.5 外均可选，而 ECA 的迭代速度极快，可以满足 S 盒批量生成的效果，适用于一次一密分组密码算法设计。

而传统的 AES 算法 S 盒是根据有限域的 $GF(2^8)$ 多项式运算生成的固定不变的 S 盒，即加密过程中 S 盒不发生变化。本文方法可以批量生成 S 盒，同时，通过对批量 S 盒进行

分析，发现该方法可以达到分组密码的加解密要求，实现在分组密码的加密过程中变换 S 盒，继而实现一次一密的加密方式，这样可以令攻击方只能进行穷举攻击，而穷举攻击所花费的时间使得攻击是没有必要的。综上，说明本文设计的 S 盒具有不错的应用潜力。

参 考 文 献

[1] LI L, ZHANG H G. Serpent—a candidate for Advanced Encryption Standard AES[J]. Information Security and Communications Privacy, 2000(1): 68-72.

[2] HE Y. Attack on reduced-round CRYPTION cipher[D]. Jinan: Shandong University, 2006.

[3] KNUDSEN L. A Key-schedule Weakness in SAFER K-64[J]. Lecture Notes in Computer Science, 1995, 963(1): 274-286.

[4] HU Y P, XIAO G Z, ZHANG Y Q. Modification of SAFER+[J]. Journal of Xidian University, 2000(6): 730-735.

[5] SU X D, CUI J S, ZHANG H G. One of the candidates of advanced encryption standard AES——Rijndael[J]. Information Security and Communications, 2000(1): 62-67, 78.

[6] MASTUI M. New Block Encryption Algorithm MISTY[C]// FSE 97. Berlin: Springer Verlag, 1997: 54-68.

[7] ZHU D, TONG X J, ZHANG M, et al. A New S-Box Generation Method and Advanced Design Based on Combined Chaotic System[J]. Symmetry, 2020, 12(12): 2087-2087.

[8] NEUMANN J, BURKS A W. Theory of self-reproducing automata[M]. Urbana: University of Illinois Press, 1966.

[9] LANGTON C G. Self-reproduction in cellular automata [J]. Physica D: Nonlinear Phenomena, 1984, 10(1/2): 135-144.

[10] JOSHI P, MUKHOPADHYAY D, ROYCHOWDHURY D. Design and Analysis of a Robust and Efficient Block Cipher using Cellular Automata[J]. Cryptology and Information Security Series, 2005, 2005: 396-396.

[11] DONG Y H, ZHAO G, MA Y J. Two-dimensional pseudo-random coupled map lattices system based on partitioned elementary cellular automata and its dynamic properties[J]. Journal on Communications, 2022, 43(1): 71-82.

[12] NASKAR P K, BHATTACHARYYA S, NANDY D, et al. A robust image encryption scheme using chaotic tent map and cellular automata[J]. Nonlinear Dynamics, 2020, 100(3): 2877-2898.

[13] 刘桂芬，赵文强. 加法噪声驱动的随机 Lorenz 系统吸引子及其上半连续性[J]. 重庆工商大学学报(自然科学版)，2022，39(1)：78-84.

[14] CAO L C, LUO Y L, QIU S H, et al. A perturbation method to the tent map based on Lyapunov exponent and its application [J]. Chinese Physics B, 2015, 24(10): 82-89.

[15] WOLFRAM S. Cellular automata as models of complexity[J]. Nature, 1984, 311(5985): 419-424.

[16] LI W, PACKARD N. The structure of the elementary cellular automata rule space[J]. Complex Systems, 2000, 4(3): 281-297.

[17] JAKIMOSKI G, KOCAREV L. Chaos and cryptography: block encryption ciphers based on chaotic maps[J]. IEEE Transactions on Circuits and Systems I Regular Papers, 2001, 48(2): 163-169.

[18] HAN Y Y, HE Y R, LIU P H, et al. A Dynamic S-Box Construction and Application Scheme of ZUC Based on Chaotic System[J]. Journal of Computer Research and Development, 2020, 57(10): 2147-2157.

[19] ZHAO G, ZHANG S M, MA Y J, et al. Design and analysis of dynamic S-box based on anti-degradation chaotic system[J]. Journal of Computer Applications, 2022. 42(10): 3069-3073.

[20] ÖZKAYNAK F. An Analysis and Generation Toolbox for Chaotic Substitution Boxes: A Case Study Based on Chaotic Labyrinth Rene Thomas System[J]. Iranian Journal of Science and Technology, Transactions of Electrical Engineering, 2020, 44(1): 89-98.

[21] YAN W H, DING Q. A Novel S-Box Dynamic Design Based on Nonlinear-Transform of 1D Chaotic Maps[J]. Electronics, 2021, 10(11): 1313.

[22] ADAMS C, TAVARES S. The structured design of cryptographically good s-boxes[J]. Journal of Cryptology, 1990, 3(1): 27-41.

[23] BIHAM E, SHAMIR A. Differential Cryptanalysis of DES-like Cryptosystems[J]. Journal of Cryptology, 1991, 4(1): 63-72.

[24] HALE J K, VERDYNLUNEL S M. Introduction to Functional Differential Equations[M]. New York: Springer-Verlag, 1993.

[25] WEBSTER A F, TAVARES S E. On the Design of S-Boxes[J]. Lecture Notes in Computer Science, 1986, 218(1): 523-534.

[26] SONY L Y, GONG X Q, HE X F, et al. Multi-stage malicious click detection on large scale Web advertising data[C]// Proceedings of Very Large Data Bases. New York: ACM, 2013: 67-72.

[27] LIU Q, FANG J Q, ZHAO G, et al. Research on Chaotic Encryption System based on FPGA technology[J]. Acta Physica Sinica, 2012, 61(13): 78-83.

ZHAO Geng, born in 1964, Ph. D, professor, Ph. D supervisor, is a senior member of China Computer Federation. His main research interests include chaotic secure communication and information security.

GAO Shirui, born in 1998, postgraduate. Her main research interest is chaos block cipher.

（责任编辑：何杨）