文章编号:1000-582X(2009)10-1226-05

切延迟椭圆反射腔映射系统的 S-盒构造

张林华[1],邓绍江[2]
(1.重庆师范大学 数学与计算机科学学院,重庆 400047;2.重庆大学 计算机学院,重庆 400030)

摘 要:利用切延迟椭圆反射腔映射系统良好的混沌特性,构造了一类新的 S-盒,详细分析了其包括双射、非线性度、严格雪崩、输出比特独立性、差分逼近概率和线性逼近概率等密码学特性,并对 Kocarev 等最近提出用离散混沌判定 S-盒强度进行了讨论。理论分析和测试结果表明构造方法容易实现且效率较高,构造的 S-盒较用其它混沌系统构造的 S-盒具有更好的密码学特性,可用于已有的密码方案的进一步改进。

关键词:混沌;切延迟椭圆反射腔映射系统;S-盒;密码分析
中图分类号:TP309.7 文献标志码:A

Construction of substitution boxes based on tangent-delay ellipse reflecting cavity-mapping system

ZHANG Lin-hua[1], *DENG Shao-jiang*[2]
(1. College of Mathematics & Computer Science, Chongqing Normal University, Chongqing 400047, P. R. China;
2. College of Computer Science, Chongqing University, Chongqing 400030, P. R. China)

Abstract: Based on the good chaotic properties of tangent-delay ellipse reflecting cavity-mapping system (TD-ERCS), a kind of novel substitution boxes were constructed. The cryptographic properties, such as bijection, nonlinearity, strict avalanche, independence of output bits, the differential approximation probability and the nonlinear approximation probability of the S-box are analyzed. The investigation method for the strength of the S-box with the discrete chaotic system proposed by Kocarev is discussed. Theoretical analysis and backtesting results show that the method is efficient and easy to put into practice, while the constructed S-boxes show better cryptographic properties than the S-boxes based on other chaotic system, which can be used to improve the existing encryption scheme.

Key words: Chaos; TD-ERCS; S-box; cryptanalysis

目前,在设计密码算法中考虑 S-盒的应用已取得相当多的成果。如在 AES 中采用 8×8 S-盒,在 GOST 中采用一层随机 4×4 S-盒,在 DES 中采用 8 个 6×4 静态 S-盒以及在 IDEA 中采用的用模乘运算设计的 16×16S-盒。

可是,在密码设计过程中至今还没有关于 S-盒设计的数学意义上的精确理论。设计 S-盒主要有两种方法:一种基于数学理论和统计结果,它的抗分析能力可以得到一定程度的证明;另一种基于设计者的直觉和经验,它的安全性有待进一步观察和验证。

收稿日期:2009-05-10
基金项目:国家自然科学基金资助项目(60873201);重庆市自然科学基金资助项目(CSTC2009BB2389,CSTSC2007BB2411);重庆市教委基金资助项目(KJ080805);重庆师范大学资助项目(07XLB036)
作者简介:张林华(1966-),男,重庆师范大学副教授,博士,主要从事编码密码学、图像取证和计算机代数方向的研究,(Tel)023-65123179;(E-mail)linzhang@cqu.edu.cn。

Pieprzyk 和 Finkelstein 于 1988 年提出了设计 $n\times n$S-盒的方法，可是它的逆 S-盒几乎是线性的，显然它的混淆特性不能保证。1989 年，Adams 和 Tavares 给出了另一种 $n\times n$ S-盒的设计方法，但它以穷举搜索为基础，使得 n 的值增大时该方法实现变得十分困难。出现差分分析方法以后，Detombe 和 Tavares 从抗差分攻击出发，利用 5 个变量的 Near－bent 布尔函数构造了 5×5 S-盒，而该方法只实用于输入比特是奇数的情形。此后，国内学者在 S-盒性能的改进方面也取得一定的成果[1-3]。一个显著的特点是，这方面大部分工作的研究重点放在布尔函数的性质上，特别是多输出函数的性质以及正形置换对分组密码设计的性能加强方面[4-5]。

利用混沌映射的性质，Jakimoski 和 Kocarev 用 4 个步骤构造 S-盒，它包括选择混沌映射、映射离散化、选择密钥和密码分析，最后表明 S-盒具有良好的密码学性质[6]。

Szczepanski 和 Amigó 提出了一种设计 S-盒的新方法，探讨了通过混合映射周期变换设计安全 S-盒的可能性，提出的逼近理论并通过实验得到了印证[7-8]。文献[9]给出了用离散分段线性映射构造 S-盒的方法。结合 Kohda 随机序列构造方法和 Baker 映射构造了一类 S-盒，可参见文献[10-11]。

1　基于混沌映射的 S-盒构造方法

目前利用混沌映射可操作性强的构造方法有两种：一种是采用伪随机序列截位构成一一映射的方法[2,11]，另一种就是 Jakimoski 提出的方法。采用混沌映射的多次迭代得到区间映射[8]，构造 8×8 的 S-盒的过程可以表述为

1)将相空间分成 $n+1$ 等份，分别对相应区间标号 0，1，…，n，每个区间对应一个数字，如果一个点落在区间 i，称它的度量为 i。

2)从每个区间随机选择一个初始点，决定它在混沌映射 N 次迭代后的象。

3)找出唯一象对应的初始点集合 S，选择 S 中包含 256 个元素的子集 A 和相应的象集 B。

4)对 A 和 B 中的元素按原来度量的大小标上的新的度量 0，…，255。如果 A 中初始点的新标号为 i，它的象的标号为 j，则 $f(i)=j$，从而映射是 1-1 映射。

研究采用第二种方法并结合以下的 TD-ERCS 进行了实验和性能分析。

2　基于切延迟椭圆反射腔映射系统

TD-ERCS 是专门为混沌加密理论而设计的混沌系统，其不存在由短周期引起的弱密钥、具有自动免疫差分分析能力和较优的系统复杂度，通过实验仿真已经证明在构造 Hash 函数、设计伪随机数发生器等具有安全性方面的优势。该模型的定义及工作原理参见文献[12]，以下仅给出和算法及实验有关的变量说明和公式。

给定 TD-ERCS 系统参数 $\mu\in(0,1]$，初值 $x_0\in[-1,1]$和 $\alpha\in(0,\pi)$，切延迟 m，TD-ERCS 依据椭圆方程

$$x^2+\frac{y^2}{\mu^2}=1,$$

通过迭代关系

$$x_n=-\frac{2k_{n-1}y_{n-1}+x_{n-1}(\mu^2-k_{n-1}^2)}{\mu^2+k_{n-1}^2},$$

$$k_n=\frac{2k'_{n-m}-k_{n-1}+k_{n-1}k_{n-m}^2}{1+2k_{n-1}k_{n-m}'-k_{n-1}^2},$$

将产生 2 个独立的实值序列

$$x_{m+0},x_{m+1},x_{m+2},\cdots,$$

$$k_{m+0},k_{m+1},k_{m+2},\cdots,$$

其中

$$k'_{n-m}=\begin{cases}-\dfrac{x_{n-1}}{y_{n-1}}\mu^2 & n<m;\\ -\dfrac{x_{n-m}}{y_{n-m}}\mu^2 & n\geqslant m,\end{cases}$$

$$y_n=k_{n-1}(x_n-x_{n-1})+y_{n-1},$$

$$y_0=\mu\sqrt{1-x_0^2},$$

$$k'_0=-\frac{x_0}{y_0}\mu^2,$$

$$k_0=\frac{\tan\alpha+k'_0}{1-k'_0\tan\alpha},$$

(μ,x_0,α,m)称为 TD-ERCS 的种子参数。

3　实验结果和性能分析

把初始区间$[-1,1]$分为 $n+1=1\ 000$ 个小区间，取迭代的次数 $N=1\ 000$，切延迟 $m=2$。由于 TD-ERCS 的一致遍历分布，得到唯一像点的概率可由下式计算

$$p(n)=\sum_{i=1}^{n}\frac{1}{n+1}\left(\frac{n}{n+1}\right)^n\to 1/\mathrm{e},$$

理论上区间划分数应该满足

$$n\geqslant 256\ \mathrm{e}=695.88,$$

按照上述方法分别对 Logistic 映射当参数值为 4 时(此时遍历)和 TD－ERCS 做了对照实验，发现在上述条件下前者能得到均值 322 阶的一一映射而后者能够得到均值 355 阶的一一映射。实验的角度验证了后者的遍历性、初始值和参数选择的自由度明显优于前者。下面对最后得到的置换的性能做一个比较全面的分析，由于步骤(2)中迭代的初始值选择是随机的，因此取出其中一个即可，数据如表 1-4 所示。

表 1 基于 TD－ERCS 的 S-盒

H	L(L：低位 8 dB，H：高位 8 dB)															
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	9B	45	9E	BE	F6	04	0C	D5	8B	47	14	C5	6E	F1	06	B0
1	68	B5	C2	FD	C0	82	21	8A	1C	F2	12	E1	E7	AD	23	A3
2	73	24	69	25	1D	86	6B	81	D9	1A	1B	0F	94	27	5F	C9
3	09	D4	67	A9	A2	CE	0E	B3	58	92	56	59	51	98	EC	DE
4	4C	30	77	B4	CB	F9	D2	BD	2D	3C	07	29	54	AE	D8	46
5	2C	E8	BC	C6	FA	26	2A	B8	90	42	00	63	7E	37	85	D7
6	34	50	6C	8F	70	E2	93	A5	0A	2E	DA	F8	32	36	55	18
7	16	75	52	B7	57	2B	DD	4A	44	E3	F5	53	38	DC	39	02
8	AA	CD	6F	41	20	EF	9D	D3	FF	7F	84	61	97	FC	2F	EA
9	B2	01	64	96	40	19	BF	ED	11	3B	0B	5D	E5	5A	17	03
A	F3	4F	C3	22	5E	3A	9C	F0	60	78	C7	7C	B6	DB	AC	A8
B	48	A4	6A	C4	08	87	62	15	3D	80	4B	1E	C8	CC	E4	8E
C	74	66	91	A1	3E	F4	88	AB	5B	CF	DF	43	95	65	E0	C1
D	4D	9F	8C	79	B9	A7	A0	05	7B	1F	EB	71	D0	49	76	BA
E	10	13	F7	EE	E6	83	7A	8D	5C	4E	9A	33	72	FE	35	BB
F	D6	99	3F	D1	0D	A6	7D	6D	AF	CA	FB	31	89	B1	28	E9

表 2 8 个布尔函数输出比特变动概率

单位向量	S-盒从高位到低位的 8 个布尔函数							
	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8
00000001	0.468 8	0.531 3	0.531 3	0.546 9	0.468 8	0.531 3	0.484 4	0.437 5
00000010	0.546 9	0.468 8	0.484 8	0.453 1	0.531 3	0.484 4	0.578 1	0.437 5
00000100	0.500 0	0.453 1	0.546 9	0.531 3	0.578 1	0.562 5	0.484 4	0.453 1
00001000	0.515 6	0.453 1	0.406 3	0.468 8	0.437 5	0.562 5	0.546 9	0.453 1
00010000	0.437 5	0.546 9	0.531 3	0.484 4	0.468 8	0.500 0	0.531 3	0.531 3
00100000	0.406 3	0.515 6	0.515 6	0.468 8	0.453 1	0.453 1	0.546 9	0.515 6
01000000	0.468 8	0.578 1	0.468 8	0.546 9	0.500 0	0.500 0	0.500 0	0.515 6
10000000	0.468 8	0.515 6	0.515 6	0.453 1	0.468 8	0.562 5	0.500 0	0.453 1

表 3 输入 1 dB 变化时，$f_i \oplus f_j$ 输出比特变化的最大概率

布尔函数	S-盒从高位到低位的 8 个布尔函数							
	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8
f_2	0	0.546 9	0.531 25	0.515 6	0.546 88	0.546 88	0.562 5	0.562 5
f_3	0.546 9	0	0.609 38	0.546 9	0.515 63	0.609 38	0.578 1	0.531 3
f_4	0.531 3	0.609 4	0	0.531 3	0.562 50	0.562 50	0.562 5	0.546 9
f_5	0.515 6	0.546 9	0.531 25	0	0.562 50	0.531 25	0.578 1	0.593 8
f_6	0.546 9	0.515 6	0.562 50	0.562 5	0	0.562 50	0.609 4	0.531 3
f_7	0.546 9	0.609 4	0.562 50	0.531 3	0.562 50	0	0.531 3	0.546 9
f_8	0.562 5	0.578 1	0.562 50	0.578 1	0.609 38	0.531 25	0	0.578 1
	0.562 5	0.531 3	0.546 88	0.593 8	0.531 25	0.546 88	0.578 1	0

表 4 通过混沌映射得到的 S-盒性能比较

作者	Order	D_f	L_f	Nonlinearity of box i							
				1	2	3	4	5	6	7	8
Jakimoski	4340	.0469	.0625	104	106	104	108	100	98	98	106
Zhang	51480	.0391	.0706	100	104	102	104	102	102	108	106
Chen	13272	.0391	.0791	102	102	104	104	104	104	106	106

1)置换的阶。把置换 f 分解成圈的乘积，有 f 的阶=[156,12,18,33,20,9,8]= 514 80。

2)非线性度。布尔函数 $f(x)$的非线性度可按下式计算

$$N_f = 2^n(1 - \max_{\omega \in GF(2)^n} | S_f(\omega) |),$$

其中 $f(x)$的 Wash 谱定义为

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

所得 S-盒的非线性度为 100，104，102，104，102，102，108，106。

3)差分逼近概率(DP_f)。线性空间 F_2^8 的变换 $f(x)$的差分逼近概率定义为

$$DP_f = \max_{\Delta x, \Delta y \neq 0} \{\frac{\sharp\{x \mid f(x) \oplus f(x + \Delta x) = \Delta y\}}{256},$$

所得 S-盒的差分逼近概率为 0.039 1。

4)线性逼近概率(LP_f)。线性分析通过比特间“线性表示”揭示出给定 S-盒的弱点。定义

$$NS(\alpha,\beta) = \sharp\{x \mid \bigoplus_{i=0}^{7} \alpha[i].x[i] = \bigoplus_{i=0}^{7} \beta[i].f(x)[i]\},$$

其中 $\alpha,\beta,x \in M,\alpha \neq 0,\beta \neq 0$。由堆积引理，可定义

$$LP_f = \max_{\alpha,\beta \neq 0} (\frac{NS(\alpha,\beta) - 128}{128})^2,$$

所得 S-盒的线性逼近概率为 0.0706。

5)严格雪崩准则(SAC)。令 $f_1, f_2, \ldots, f_8$ 为 S-盒高位到低位的 8 个布尔函数，它要求每一个函数当输入变动 1 dB 时 8 个输出 dB 以 0.5 的概率变动。分析结果见参见表 2。

6)输出比特独立性(BIC)。它是指当单一输入比特变化时，输出比特应该相互独立。实验结果见表 3。

7)离散 Lyapunov 指数(DL_f)[13]。由于混沌是在实域上定义的，而计算机仿真都是在有限状态下完成的，因此 Kocarev 引入离散混沌的概念并取得大量理论性的结果，反过来促进了对 S-盒的研究。对集合 $S=\{0,1,\cdots,M-1\}$上的置换可定义离散 Lyapunov 指数如下

$$DL_f = \frac{1}{M}\sum_{i=0}^{M-1} \ln | f(c_i) - f(i) |,$$

其中 c_i 当 $i=M-1$ 时为 $M-2$，否则定义其值为 $i+1$。Jakimoski 和 Amigo 用它给出了用它判定“强的加密映射”的标准[14] $\ln m - (1 + \ln 2) + \ln(\pi m)/m \leqslant DL_f \leqslant \ln m + 1/m$ 其中 m 等于置换阶的 1/2 . 通过计算得 $3.2057 \leqslant DL_f = 3.981\ 2 \leqslant 4.859\ 8$，

故导出的置换是“强”的加密映射。

在对最近得到的 S-盒做过全面的实验，验证了各文献已有结果，对一些错误的地方进行了纠正，并补充了对其轨道和阶的计算结果。在此基础上对通过混沌映射得到的 S-盒的特性进行了比较。因为 S-盒密码特性之间的关系和比较一直是一个值得研究的难题[15]，如实验表明 AES 的 S-盒线性逼近概率和差分逼近概率都为 0.0156，阶数为 277182 和全是 112 的非线性度都是非常好的指标，但它却具有明显的仿射关系。所以只对近来得到的可比性强的结果进行了比较。首先，Amigó 方法可操作性不强且没有具体的算例，其差分逼近概率和线性逼近概率也不够好，因此主要对上节提到的两种方法得到的结果进行比较，由于 SAC 和 BIC 性能相近且不易比较，列出其它可比较的的性质见表 4。其中文献[10]中用的是第二种方法，并且对文献[9]的结果进行了改进。文献[6]中 Jakimoski 和研究用的是第一种方法且没有做进一步置乱，方法简单明了且实现速度快。从表中不难得出：文中得到的置换阶数有明显的优势，特别是较文献[6]中结果。由此说明 TD-ERCS 混沌特性用于构造 S-盒远优于 Logistic 映射。用于图像隐藏或置乱效果更好。

特别值得一提的是，反复对比实验证明，文献[6]中 S-盒的非线性度原来为 98，100，100，104，104，106，106，108 是错误的。从 S-盒的非线性度看，文中的 S-盒比较文献[8]更加均匀，平均值也更高。

4　结　语

得到了基于 TD-ERCS 的 S－盒，并对利用混沌映射构造 S-盒的方法进行了比较系统的研究和大量的对比实验。通过与最新结果比较，它的综合性能较好，可以用于图像的置乱以及改进已有的混沌密码方案。如何把混沌映射、布尔函数以及置换群结合研究将成为未来的一个重要研究方向。

参考文献：

[1] 陈华，冯登国，吴文玲. 一种改善双射S-盒密码特性的有效算法[J]. 计算机研究与发展，2004，41(8)：1410-1413.
CHEN HUA，FENG DENG-GUO，WU WEN-LIN. An effective algorithm for improving cryptographic properties of bijective S-boxes[J].
Journal of Computer Research and Development，2004，41(8)：1410-1413.

[2] 刘晓晨，冯登国. 满足若干密码学性质的S-盒的构造[J]. 软件学报，2000，11(10)：1299-1302.
LIU XIAO-CHEN ，FENG DENG-GUO. Construct ion of S-Boxes with some cryptographic properties[J]. Journal of Software，2000，11(10)：1299-1302.

[3] 温巧燕，钮心忻，杨义先. 现代密码学中的布尔函数[M]. 北京：科学出版社，2000.

[4] JOHANSON T. A construction of resilient functions with high nonlinearity[J]. IEEE Trans Information Theory，2003，49：494-501.

[5] CHAND K，SARKAR P. Improved construction of nonlinear resilient S-Boxes [J]. IEEE Trans Information Theory，2005，51：339-348.

[6] JAKIMOSKI G，KOCAREV L. Chaos and cryptography：block encryption ciphers[J]. IEEE Trans Circuits Syst-I，2001，48：163-170.

[7] SZCZEPANSKI J，AMIGó J，Michalek T，Kacarev L. Cryptographically secure substitutions based on the Approximation of mixing Maps[J]. IEEE Trans CAS-I，2005，52：443-453.

[8] AMIGó J，SZCZEPANSKI J，KACAREV L. A chaos-based approach to the design of cryptographically secure substitutions[J]. Physics Letters A，2005，343：55-60.

[9] TANG G P，LIAO X F. A method for designing dynamical S-boxes based on discretized chaotic map[J]. Chaos，Solitons and Fractals，2005，23：1901-1909.

[10] CHEN G. A novel heuristic method for obtaining S-boxes[J]. Chaos，Solitons and Fractals，2008，36(4)：1028-1036.

[11] KOHDA T，TSUNEDA A. Statistics of chaotic binary sequences[J]. IEEE Trans Information Theory，1997，43：104-112.

[12] 盛利元，孔克辉，李传兵. 基于切延迟的椭圆反射腔离散混沌系统及其性能研究[J]. 物理学报，2004，53(9)：2871-2876.
SHENG LI-YUAN，KONG KE HUI，LI CHUAN-BIN. Study of a discrete chaotic system ba sed on tangent- delay for elliptic reflecting cavity and it s properties[J]. Acta Physica Sinica，2004，53(9)：2871-2876.

[13] KOCAREV L，SZCZEPANSKI J，AMIGO J M，et al. Discrete chaos - I：Theory[J]. IEEE Trans Circuit and Systems I，2006，53 (6)：1300-1309.

[14] JAKIMOSKI G，SUBBALAKSHMI K P. Discrete lyapunov exponent and differential cryptanalysis[J]. IEEE Trans Circuit and Systems I，2007，54(6)：499-501.

[15] 冯登国，宁鹏. S-盒的非线性准则之间的关系[J]. 通信学报，1998，19(4)：72-76.
FENG DGNG-GUO，NING PENG. The relationship among nonlinear criteria of S-box[J]. Journal of China Institute of Communications，1998，19(4)：72-76.

（编辑 侯 湘）