# 一种基于离散混沌系统的S-Box候选算法设计*

丁文霞[1],王 浩[2]
(1. 国防科技大学 电子科学与工程学院,湖南 长沙 410073;
2. 中南大学 信息科学与工程学院,湖南 长沙 410083)

**摘 要**:S-Box是现行分组密码中唯一的非线性部件,主要提供了分组密码算法中必需的混淆作用,其密码强度决定了整个分组密码的安全强度。为进一步提高S-Box的强度,结合离散混沌系统的内在随机性、有界性、非周期性及对初始条件和参数极度敏感等特点,提出一种采用多混沌映射和交叉映射生成S-Box的生成算法。实验分析表明,该算法生成的样本密钥敏感性强,随机性好,既能较好地满足S-Box设计所要求的各项准则和特性,安全性高,同时又能降低计算复杂度,提高计算速度,且易于生成和扩展,因而是一种性能良好的S-Box候选算法。

**关键词**:应用密码学;混沌;S-Box;严格雪崩准则;输出比特间独立性
**中图分类号**:TP391.41 **文献标志码**:A **文章编号**:1001-2486(2013)01-0083-06

# Design of S-Boxes based on discrete chaos system

*DING Wenxia*[1], *WANG Hao*[2]
(1. College of Electronic Science and Engineering, National University of Defense Technology, Changsha 410073, China;
2. School of Information Science and Engineering, Central South University, Changsha 410083, China)

**Abstract**: S-box is the only nonlinear components of block cipher algorithm which can provide confounding effect. Its password strength determinates the security strength of the whole cipher algorithms. An S-Box generation algorithm based on the discrete chaos system which uses multi-chaos maps and cross-generation method to generate S-Boxes was proposed. Good characteristics such as bounded, aperiodic and extremely sensitive to initial conditions and parameters of discrete chaos system were combined in the algorithm. Experimental analysis shows that the samples generated by our algorithm have strong key sensitivity and good randomness, thus can satisfy both the high security criteria and features required by the S-Box design. It improves the performance by reducing the computational complexity and has good scalability and low implementation cost. Therefore, the proposed method can serve as a promising choice for designing S-Boxes.

**Key words**: applied cryptography; chaos; Substitution Box (S-Box); Strict Avalanche Criterion (SAC); Output Bits Independence Criterion (BIC)

混沌现象是在非线性动力系统中出现的确定性的、类似随机的过程,这种过程既非周期又不收敛,并且对初始值有极其敏感的依赖性。目前,混沌理论在很多领域尤其是应用密码学领域引起了极大关注。

由于S-Box可以为密码系统提供Shannon所描述的混乱作用,因此它目前在分组密码算法中得到了广泛的应用[1-5]。S-Box最初出现在Lucifer算法中,后来由于DES作为密码标准使用而广为流传,进而大量出现在Rijndael, Mars和Twofish等AES候选算法中。目前S-Box设计标准已日趋成熟并得到广泛认可[1-5]。

本文结合混沌动力学系统的特点,提出了一种基于离散混沌系统的S-Box生成算法,该算法采用多混沌映射和交叉映射的方法,既能较好地满足S-Box设计所要求的各项准则和特性,安全性高,同时又能降低计算复杂度,速度快,且样本丰富,因而是一种性能良好的S-Box候选算法。

## 1 S-Box的概念及其设计标准

通俗地说,一个S-Box是一个简单的代替,即将$n$-位输入映射到$m$-位输出。一个$n$-位输入到$m$-位输出的S-Box称为$n \times m$位的S-Box。Bruce Schneier等人认为,S-Box应尽可能大、随机、非线性、非退化且与密钥相关[1],如果没有密钥的控制,则只是一般的替代,而不是S-Box,根据Kerckhoff假设,其作用只能是简单置乱。因此,S-Box实质上可以假定为密钥控制下的非线性映

* **收稿日期**:2012-08-18
**基金项目**:国家自然科学基金资助项目(60902092)
**作者简介**:丁文霞(1973—),女,湖南湘潭人,副教授,博士,硕士生导师,E-mail:dwx2004@sina.com

射,由于解密的需要,还需满足双射的特性。从密码分析的角度看,S-Box 不能被看作黑盒。因此无论采用什么方法设计的 S-Box,都必须首先给出如何准确全面地度量 S-Box 的密码强度的标准。当前,人们在分析 S-Box 的设计和运算方面已做了大量的研究工作,提出了很多有关 S-Box 设计的准则和好的 S-Box 所应该具有的特性,现归纳如下[1-5]:

(1)双射:通常要求 S-Box 是可逆的,尤其在 SP 网络中所使用的 S-Box 必须是双射。当 $m=n$ 时,文献[1,3]给出了满足双射的充分必要条件为:

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

其中,$a_i \in \{0,1\}$,任取$(a_1,a_2,\cdots,a_n) \neq (0,0,\cdots,0)$,$wt(\,)$ 表示汉明重量。如果上式成立,则可以说每个 $f_i$ 是 0/1 平衡的,且 $f$ 是双射的。

(2) 非线性度:一般来说,非线性度对布尔函数的线性结构有制约关系,非线性度越大,算法抗线性攻击的能力越强。非线性是好的 S-Box 所必须具备的重要性能,其 walsh 谱定义为:

$$N_f = 2^{n-1}\left(1 - 2^{-n} \max_{\omega \in GF(2^n)} |S_{<f>}(\omega)|\right) \tag{2}$$

而 $f(x)$ 的 walsh 谱为:

$$s_{<f>}(\omega) = \sum_{x \in GF(2^n)} (-1)^{f(x) \oplus x \cdot \omega} \tag{3}$$

其中,$\omega \in GF(2^n)$,$x \cdot \omega = x_1 \cdot \omega_1 \oplus \cdots \oplus x_n \cdot \omega_n$ 表示 $x$ 与 $\omega$ 的点积。

(3) 差分均匀性:差分均匀性是针对差分密码分析而引入的,用来度量一个密码函数抗击差分密码分析的能力,即对每个输入差分 $\Delta x$ 应能唯一映射到输出差分 $\Delta y$,从而确保每个 $x$ 的均匀映射概率。在实际计算中,可采用差分逼近概率 $DP_f$ 来表示输入输出的异或分布情况:

$$DP_f = \max_{\Delta x \neq 0, \Delta y}\left(\frac{|\{x \in X | f(x) \oplus f(x \oplus \Delta x) = \Delta y\}|}{2^n}\right) \tag{4}$$

其中,$X$ 表示所有可能输入的集合,$2^n$ 是该集合的元素个数。$DP_f$ 所表示的是给定一个输入差分 $\Delta x$,输出为 $\Delta y$ 的最大可能性。

(4) 严格雪崩准则(SAC):$S(x) = (f_1(x),\cdots,f_m(x)): F_2^n \to F_2^m$ 满足严格雪崩准则,是指改变输入的 1 个比特,每个输出比特改变的概率为 0.5。文献[1]给出了用来验证给定的密码变换 $f$ 是否满足 SAC 的相关构造矩阵。在实际分析中一般会用到表征严格雪崩效应的下列指标:

$$asac = \frac{1}{k}\sum_{i=1}^{k}\sum_{x \in F_2^k}[f(x) \oplus f(x+e_i)] \tag{5}$$

$$\min sac = \min_i \sum_{x \in F_2^k}[f(x) \oplus f(x+e_i)] \tag{6}$$

$$\max sac = \max_i \sum_{x \in F_2^k}[f(x) \oplus f(x+e_i)] \tag{7}$$

其中 $f(x)$ 为布尔函数,而 $e_i$ 与 $x$ 为 $GL(2)$ 上的 $k$ 维向量,$e_i$ 表示第 $i$ 分量为 1 而其余分量为 0 的向量。

(5) 输出比特间独立性(BIC):这是任何密码变换都希望具有的第二个特性。一种由 C. Adams 和 S. Tavares 给出的测量输出比特独立的方法[11]是:对于给定的布尔函数 $f_j$,$f_k(j \neq k)$ 是某 S-Box 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效应,则它们可以确保当一个输入比特取反时,每个输出比特对的相关系数接近于 0。于是,可以通过验证 S-Box 的任意两个输出比特间 $f_j \oplus f_k$ 是否满足严格雪崩效应,来证明该 S-Box 是否满足输出比特间独立准则。

## 2 一种基于离散混沌系统的S-Box候选算法设计

多年来,人们总结出一些构造 S-Box 的方法,如随机选择、选择和测试、人为构造以及用数学方法构造等[1],目前,基于混沌映射的 S-Box 设计方法得到了广泛的研究[6-10],如 Jakimoski 在文献[6]中提出了一种基于混沌映射构造 S-Box 的方法,该方法主要是通过以下四个步骤由离散混沌系统来获得一个离散化的一一映射:

(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 1 个数字,如果一个点在区间 $i$,令其度量为 $i$。

(2) 从每个区间随机选择一个初始点,决定它在混沌映射 $N$ 次迭代后的像。

(3) 找出唯一像对应初始点的集合 $S$,选择 $S$ 中包含 256 个元素的子集 $A$ 和相应的像集 $B$。

(4) 标上新的度量 0,1,…,255(对 $A$ 中的元素按原来度量的大小),对 $B$ 施行同样的操作。如果 $A$ 中初始点的新标号为 $i$,它的像的标号为 $j$,则 $f(i) = j$,从而映射是一一映射。

很明显,该算法像空间的初始划分数量要比 256 更大,才能保证第四步真正找到一个双射,而

如果只是通过这四步来构造 S-Box,其性能还不够好,因为这与混沌映射的密度函数有密切关系。一般而言,离散化后的混沌系统所产生的混沌序列并不能满足密码系统所需要的自相关与互相关特性。因而文献[2,6 - 10]针对该算法提出了一些改进思路,如张林华在文献[2]中采用一维 Logistic 混沌映射,提出一种以每次 8 比特的方式扫描混沌二值序列,不重复地取出其中256个0 ~ 255 的伪随机整数序列来生成 S-Box:$g:M\to M$,$M=\{0,1,\cdots,255\}$ 的新的 S-Box 候选方案,该方案与 G. Jakmoski 算法相比,计算复杂度有所降低,但由于采用单一混沌映射,因而其性能依然会受混沌映射的密度函数(如 Logistic 映射的"return map"现象[12])及周期性(易产生平凡密钥及拟平凡密钥[12])的影响。

本文在综合分析以上算法的基础上,设计了一种基于混沌伪随机排序整数序列的 8 × 8(即 $n=8$)S-Box 候选算法,算法主要原理及实现步骤如下:

(1)采用两个不同的混沌映射(如一维 Logistic 映射和 $z$ 映射)由相同的初值 $x0$ 相互迭代产生一组实值序列(长度 > 512),一维 Logistic 映射和 $z$ 映射定义如下:

Logistic 映射方程定义为:

$$x_{n+1}=rx_n(1-x_n),0\leqslant r\leqslant 4,x_n\in(0,1) \tag{8}$$

其中,$r$ 为分支参数,当 $0\leqslant r\leqslant 3.569\,945\,972$ 时,该动力系统因从稳定状态到分叉而产生倍周期,当 $3.569\,945\,972<r\leqslant 4$ 时,该动力系统进入混沌状态。

$z$ 映射定义式为:

$$x_{n+1}=\sin^2(z\arcsin\sqrt{x_n}) \tag{9}$$

此处 $z$ 为整型参数,当 $z>1$ 时,系统混沌。由该式可以看出,此映射与一维 Logistic 映射具有完全一样的混沌吸引域和值域,但结构却完全不同,因此二者既可以很方便地相互迭代,又可以很好地克服单一混沌映射受密度函数及周期性影响的缺陷。

(2)从(1)生成的实值序列中取出前 256 个不重复的实数值,将其按降序排列得排序表 $P1$,再从后续实值序列中继续取出 256 个不重复的实数值排序生成排序表 $P2$,即可得两个值域为[1,256]的整数序列;

(3)按式 $SB(i)=P1(P2(i))-1,(i=1,2,\cdots,256)$ 进行交叉映射,生成一维 S-Box,将其变为二维表的形式,即构成一个完整的 S-Box。

## 3　算法性能分析

下面,以 $x_0=0.564879$ 时产生的 S-Box 样本 - 1(参见表1)和另外50个S-Box为例,对本算法产生的 S-Box 的一些主要性能作以下分析(令 $f_1$,$f_2,\cdots,f_8$ 表示 S-Box 高位到低位的 8 个布尔函数):

(1)由表1和式(1)可知S-Box样本 - 1具有双射特性,式(1)计算出的值为 128,与理想值相同,因而输出函数的比特平衡性很好,其他 S-Boxes 具有相同的特性;

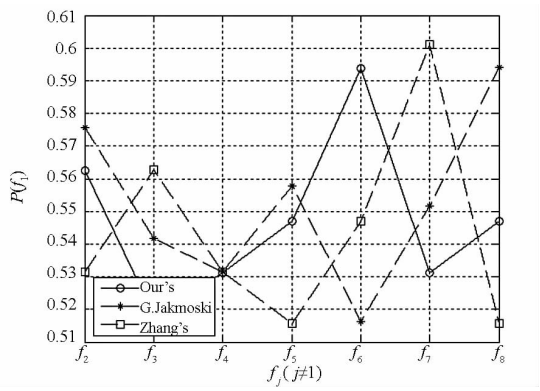
(2)S-Box样本 - 1布尔函数的非线性度分别为103,104,106,105,105,104,108,103,表明本算法具有非常好的非线性,能够较好地抵御线性攻击;

(3)S-Box样本 - 1雪崩效应测试结果见表2,表1计算的平均值为 0.5048,可知本算法平均值非常接近理想值0.5;

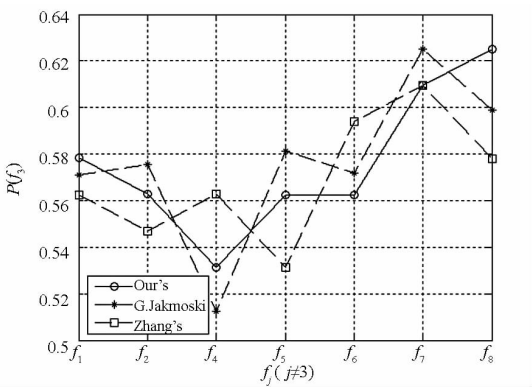
(4)S-Box样本 - 1输出比特独立性测试最大概率表见表3;由表3知样本 - 1输入各比特取反时,$f_i\oplus f_j$ 输出取反的最大概率平均值非常接近理想值0.5,因而 S-Box 样本的输出比特独立性很好;

(5)采用计算差分逼近概率的方法进行检验,根据式(4)进行计算,本算法构造的 S-Box 的输入输出差分分布最大值只有 12,最小值为 6,这说明其差分分布较好;

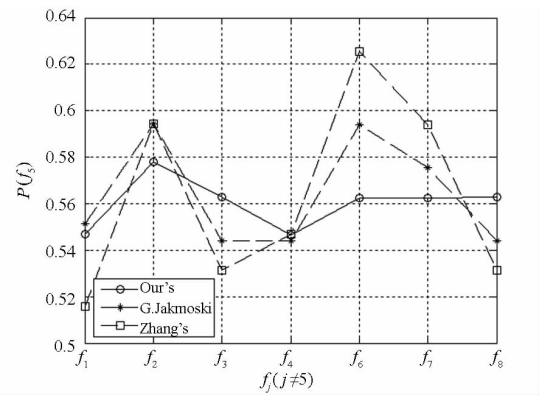
(6)为进一步说明本 S-Box 候选算法的可行性,本文将此算法产生的 50 个样本的输出比特独立性测试最大概率和平均雪崩效应测试部分结果与文献[6]中 G. Jakimoski 提出的基于混沌映射构造 S-Box 的方法及张林华在文献[2]中提出的类似 S-Box 候选算法样本分别进行了相应的对比,结果分别如图1、图2所示(后两种算法的混沌映射均采用一维 Logistic 映射,50 个样本平均)。表4则给出了三算法50个S-Box样本在同等计算环境下平均生成时间的对比结果。由图1、图2和表4可知,本算法的平均雪崩效应和输出比特独立性比上述两种算法速度更快。



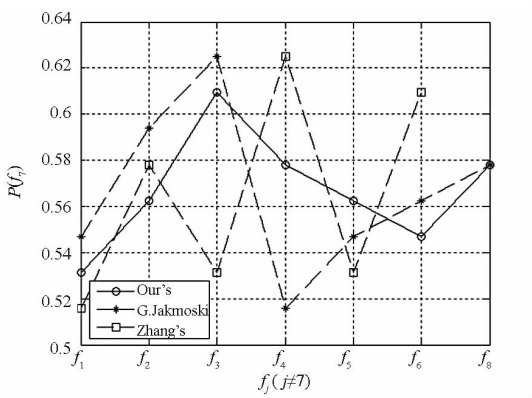

(a) $f_1$




(b) $f_3$



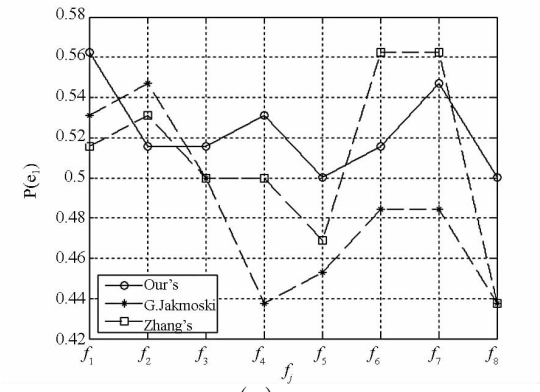

(c) $f_5$



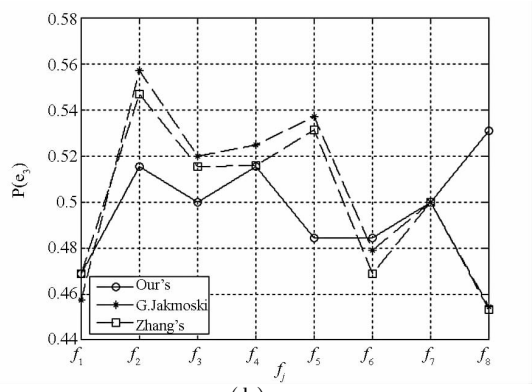

(d) $f_7$

图 1　样本输出比特独立性测试最大概率(以 $f_i(i = 1,3,5,7)$ 为例) 对比

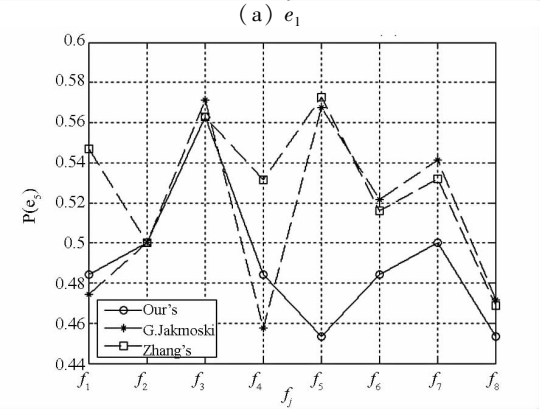
Fig. 1　Comparison of the BIC of three algorithms(e. g. $f_i(i = 1,3,5,7)$)



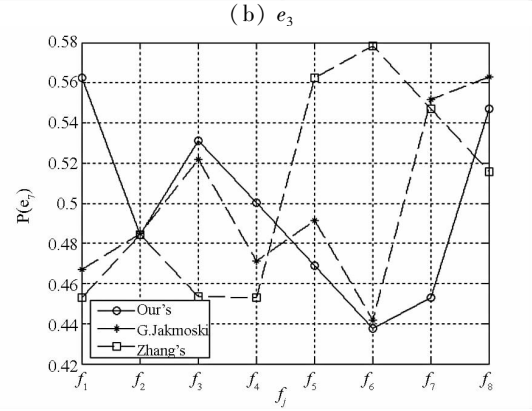

(a) $e_1$




(b) $e_3$




(c) $e_5$




(d) $e_7$

图 2　样本雪崩效应测试结果对比(以 $e_i(i = 1,3,5,7)$ 为例)

Fig. 2　Comparison of the SAC of three algorithms(e. g. $e_i(i = 1,3,5,7)$)

表 1　S-Box 样本 - 1

Tab. 1　S-Box sample-1 generated by our algorithm

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

表 2　样本 - 1 输入各比特取反时,输出取反的概率

Tab. 2　Test results of the SAC of Sample - 1

| $e_i$ | $f_1$ | $f_2$ | $f_3$ | $f_4$ | $f_5$ | $f_6$ | $f_7$ | $f_8$ |
|---|---|---|---|---|---|---|---|---|
| 00000001 | 0. 562500 | 0. 515625 | 0. 515625 | 0. 531250 | 0. 500000 | 0. 515625 | 0. 546875 | 0. 500000 |
| 00000010 | 0. 484375 | 0. 546875 | 0. 531250 | 0. 375000 | 0. 437500 | 0. 562500 | 0. 515625 | 0. 515625 |
| 00000100 | 0. 468750 | 0. 515625 | 0. 500000 | 0. 515625 | 0. 484375 | 0. 484375 | 0. 500000 | 0. 531250 |
| 00001000 | 0. 515625 | 0. 453125 | 0. 453125 | 0. 484375 | 0. 500000 | 0. 484375 | 0. 500000 | 0. 484375 |
| 00010000 | 0. 484375 | 0. 500000 | 0. 562500 | 0. 484375 | 0. 453125 | 0. 484375 | 0. 468750 | 0. 531250 |
| 00100000 | 0. 468750 | 0. 562500 | 0. 531250 | 0. 531250 | 0. 500000 | 0. 484375 | 0. 500000 | 0. 453125 |
| 01000000 | 0. 562500 | 0. 484375 | 0. 531250 | 0. 500000 | 0. 468750 | 0. 437500 | 0. 453125 | 0. 546875 |
| 10000000 | 0. 531250 | 0. 437500 | 0. 531250 | 0. 500000 | 0. 500000 | 0. 500000 | 0. 515625 | 0. 531250 |

表 3　样本 - 1 输入各比特取反时,$f_i \oplus f_j$ 输出取反的最大概率

Tab. 3　The dependent matrix of $f_i \oplus f_j$

| $e_i$ | $f_1$ | $f_2$ | $f_3$ | $f_4$ | $f_5$ | $f_6$ | $f_7$ | $f_8$ |
|---|---|---|---|---|---|---|---|---|
| $f_1$ | 0. 000000 | 0. 562500 | 0. 578125 | 0. 531250 | 0. 546875 | 0. 593750 | 0. 531250 | 0. 546875 |
| $f_2$ | 0. 562500 | 0. 000000 | 0. 562500 | 0. 609375 | 0. 578125 | 0. 593750 | 0. 562500 | 0. 562500 |
| $f_3$ | 0. 578125 | 0. 562500 | 0. 000000 | 0. 531250 | 0. 562500 | 0. 562500 | 0. 609375 | 0. 625000 |
| $f_4$ | 0. 531250 | 0. 609375 | 0. 531250 | 0. 000000 | 0. 546875 | 0. 578125 | 0. 578125 | 0. 515625 |
| $f_5$ | 0. 546875 | 0. 578125 | 0. 562500 | 0. 546875 | 0. 000000 | 0. 562500 | 0. 562500 | 0. 562500 |
| $f_5$ | 0. 593750 | 0. 593750 | 0. 562500 | 0. 578125 | 0. 562500 | 0. 000000 | 0. 546875 | 0. 562500 |
| $f_6$ | 0. 531250 | 0. 562500 | 0. 609375 | 0. 578125 | 0. 562500 | 0. 546875 | 0. 000000 | 0. 578125 |
| $f_7$ | 0. 546875 | 0. 562500 | 0. 625000 | 0. 515625 | 0. 562500 | 0. 562500 | 0. 578125 | 0. 000000 |

表 4　三算法 50 个 S-Box 样本平均生成时间对比(8 ×8 大小)

Tab. 4　50 8 ×8 samples average generation time of three algorithms (s)

| | Jakmoski 算法 | 张林华算法 | 本算法 |
|---|---|---|---|
| 算法样本生成平均时间(s) | 0. 4359 | 0. 023 | 0. 016 |

## 4 结束语

本文提出了一种基于离散混沌系统的 S-Box 生成算法,仿真分析结果表明,本文所提算法的计算复杂度较 Jakmoski 等算法低,速度快,而多混沌映射和交叉映射方法的采用又很好地克服了 Jakmoski 算法和张林华算法中单一混沌映射的性能缺陷,因而安全性高,较好地满足了 S-Box 设计所要求的各项准则和特性。同时,本算法密钥敏感性强,样本的随机性好,既容易生成,又易于扩展,因而是一种性能良好的 S-Box 候选产生算法。

## 参考文献(References)


[1] Schneier B. 应用密码学 - 协议/算法和 C 源代码[M]. 北京:机械工业出版社, 2000.
Schneier B. Applied cryptography-protocol / algorithm and C source code[M]. Beijing: Machinery Industry Press, 2000. (in Chinese)

[2] 张林华. 基于混沌的密码技术应用研究[D]. 重庆大学,2006.
ZHJANG Linhua. The cryptography application research based on chaos[D]. PhD thesis, Chongqing University, 2006. (in Chinese)

[3] Ghada Z, Kachouri A, Peyrard F, et al. On Dynamic chaotic S-Box [C]//Information Infrastructure Symposium, 2009 (GIIS'09. Global):1 - 5.

[4] Wang Y, Yang L, Li M, et al. A method for designing S-Box based on chaotic neural network[C]//2010 Sixth International Conference on Natural Computation (ICNC 2010): 1033 - 1037.

[5] Xu G, Zhao G. The design of dynamical S-Boxes based on discrete chaos map system[C]//Communications, Circuits and Systems, 2009 (ICCCAS 2009): 876 - 880.

[6] Goce J, Ljupco K. Chaos and cryptography. Block encryption ciphers based on chaotic maps[J]. IEEE Tarns. Circuits and Systems-I, 2001,48(2): 163 - 169.

[7] Goce J, Ljupco K. Differenytial and linear probabilities of a block-encryption cipher [J]. IEEE Trans. Circuits and Systems-I, 2003, 50(1): 121 - 123.

[8] Tang G P, Liao X F, et al. A novel method for designing S-Boxes based on chaotic maps [J]. Chaos, Solutions and Fractals, 2005,23:413 - 419.

[9] Tang G P, Liao X F. A method designing dynamic-boxes based on discretized chaotic maps[J]. Chaos, Solutions and Fractals, 2005,23: 1901 - 1909.

[10] Szczepanksi J, Amigo J M, Michalek T, et al. Cryptographically secure substitutions based on the approximation of mixing Maps [J]. IEEE Trans. (CAS-I),2005, 52(2):443 - 453.

[11] Adams C M, Tavares S E. The structured design of cryptographically good S-Boxes[J]. Journal of Cryptology, 1990,3(1):27 - 41.

[12] 丁文霞. 基于混沌理论的多媒体信息安全算法研究[D]. 国防科技大学,2009.
DING Wenxia. The researches of multimedia information security algorithms based on chaotic theory[D]. National University of Defense Technology, 2009. (in Chinese)