S-盒的 Lyapunov 指数研究*

臧鸿雁[1)†] 范修斌[2)] 闵乐泉[1)] 韩丹丹[1)]

1) (北京科技大学数理学院, 北京 100083)

2) (中国科学院软件研究所, 北京 100190)

(2012 年 4 月 10 日收到; 2012 年 4 月 30 日收到修改稿)

在密码算法的设计中, S-盒有着信息混淆的重要功能. 传统的 S-盒的密码学指标一般包括线性偏差、差分特征、代数免疫度、不动点个数、雪崩效应等. 2006 年, Kocarev 给出了有限集合上的离散混沌理论. 本文借鉴该理论, 在汉明距离的基础上给出了 S-盒的 Lyapunov 指数的定义, 利用该定义计算了几个密码算法中的 S-盒的 Lyapunov 指数值, 并进行了比较. 证明了在欧氏距离上定义的 Lyapunov 指数最大的映射, 按本文提出的 S-盒的 Lyapunov 指数的定义其 Lyapunov 指数为 0; 讨论了 S-盒的 Lyapunov 指数与 S-盒的雪崩效应之间的关系, 该关系实际上是混沌理论中的蝴蝶效应与密码学中的雪崩效应之间的关系. 本文提出的 S-盒的 Lyapunov 指数的定义可视为对传统的 S-盒的密码学指标的补充.

关键词: 有限集合, 离散混沌理论, S-盒, Lyapunov 指数

PACS: 05.45.Vx, 05.45.Gg

1 引 言

根据 Shannon 理论, 密码算法特别是对称密码算法主要是基于信息的扩散和混淆实现的. 扩散技术一般基于线性变换, 混淆技术一般基于非线性变换, 例如大家熟悉的 S-盒. S-盒在很多密码算法中得到了重要应用, 例如 Advanced Encryption Standard (AES) 密码算法、商用密码算法 (SMS4)、ZUC 算法 (数学家祖冲之名字的缩写) 等. 传统的 S-盒的密码学指标一般包括线性偏差、差分特征、代数免疫度、不动点个数、雪崩效应等 [1,2]. 那么还有没有其他的密码学指标呢? 本文基于混沌理论, 尝试给出 S-盒的一个新的密码学指标.

混沌是一种非线性动力学现象, 是确定性系统产生的内在随机性. 混沌理论在 20 世纪 80 年代和 90 年代蓬勃发展 [3−6]. 近年来, 有关混沌理论及其应用的研究得到了越来越多学者的关注 [7−11]. 非周期性是混沌系统的关键特性, 混沌系统行为对初值具有高度敏感性. 基于混沌系统的良好的 “混淆” 和 “扩散” 信息属性 [12], 人们提出了一些基于混沌映射的密码系统 [11,13].

动态系统的研究大部分都是在计算机的帮助下实现的, 所有轨道在计算机上显示都是周期性的 [14]. 非周期性也只存在于连续系统当中. 在 2006 年, Kocarev 等 [7,8] 提出了有限集合上的离散混沌的概念, 并给出有限集合上的离散混沌的理论基础, 扩展了混沌系统的研究内容.

本文中, 我们借鉴 Kocarev 等 [7,8] 给出的有限集合上的离散混沌理论, 在汉明距离的基础上, 给出了 S-盒的 Lyapunov 指数的定义; 并通过实例说明了我们给出的 S-盒的 Lyapunov 指数是具有实际意义的. 本文研究了 S-盒的 Lyapunov 指数与雪崩效应之间的关系, 这个关系实际上是混沌理论中的蝴蝶效应与密码学中的雪崩效应之间的关系.

本文具体计算了 SMS4 的 S-盒 [15]、AES 的 S-盒 [16] 以及基于混沌映射所生成的 S-盒 [17] 的 Lya-

* 国家自然科学基金 (批准号: 61074192, 60833008) 资助的课题.

† E-mail: zhylixiang@sina.com

punov 指数, 并进行了比较和分析.

2 有限集合上的离散 Lyapunov 指数

2.1 一维混沌系统 Lyapunov 指数

混沌运动的基本特点是运动对初始条件极为敏感, 即所谓的蝴蝶效应, 两个靠近的初值所产生的轨道, 会随时间推移按指数方式分离, Lyapunov 指数就是定量描述这一现象的参数.

定义 1[9] 一维映射 $x_{n+1}=f(x_n)$ 的 Lyapunov 指数定义为 $\lambda(x_0)=\lim\limits_{T\to\infty}\dfrac{1}{T}\sum\limits_{k=0}^{T-1}\ln|f'(x_k)|$.

Lyapunov 指数的定义是对连续系统上的映射给出的, 对于有限集合上的 Lyapunov 指数的定义和研究具有实际意义. 我们利用计算机模拟混沌系统时, 计算精度有限, 这样导致了连续系统上的混沌映射转换为有限集合上的混沌映射.

在 2006 年, Kocarev 等 [7] 提出了有限集合上的离散混沌的概念, 定义了其 Lyapunov 指数.

2.2 有限集合上的离散 Lyapunov 指数

记 $\mathbb{N}$ 是自然数集合, 记 $S=\{0,1,\cdots,M-1\}$, 其中 $M\in\mathbb{N}$, 考虑一个双射 $F:S\to S$, 则 F 的所有轨迹都是周期性的, 记 α 为初值为 $a_0\in S$ 的 F 的一段最小周期为 T 的轨迹, 即 $\alpha=\{a_0,a_1=F(a_0),\cdots,a_{T-1}=F(a_{T-2}),a_0=F(a_{T-1})\}$, 其中 $a_0,a_1,\cdots,a_{T-1}$ 两两不等. 令 $U_i=\{i-1,i+1\}$, $i=1,2,\cdots,M-2$, 令 $U_0=\{1\}$, $U_{M-1}=\{M-2\}$. U_i 称为点 i 所有的相邻点.

定义 2[7] 对任意 $i\in S$, 任给 $c_i\in U_i$, 双射 F 的离散 Lyapunov 指数定义为

$$\lambda_F=\frac{1}{M}\sum_{i=0}^{M-1}\ln d\left[F(c_i),F(i)\right]. \tag{1}$$

其中 $d(x,y)$ 是点 x 和 y 之间的欧氏距离.

我们可以在 (1) 式中随便选择点 i 和它的邻点 c_i. 一共存在着至多 2^{M-2} 个 Lyapunov 指数. 通常情况下, 所有的离散 Lyapunov 指数值相差很小 [7]. 如果 U_i 中不仅一个元素, 定义点 i 的邻点是 $c_i=i+1$. 又 $d(x,y)=|x-y|$, 则 (1) 式变为

$$\lambda_F=\frac{1}{M}\sum_{k=0}^{M-1}\ln|F(\alpha_k+1)-F(\alpha_k)|. \tag{2}$$

若定义点 i 的相邻点是 $c_i=i+1$, 又 $d(x,y)=|x-y|$, Kocarev 等给出了双射 F 的轨道 α 的离散 Lyapunov 指数定义和双射 F 的所有轨道加权平均离散 Lyapunov 指数定义.

定义 3[7] 记 α 为初值为 $a_0\in S$ 的 F 的一段最小周期为 T 的轨迹, 定义映射 F 的周期轨道 α 的 Lyapunov 指数为

$$\lambda_{(F,\alpha)}=\frac{1}{M}\sum_{k=0}^{T-1}\ln|F(\alpha_k+1)-F(\alpha_k)|.$$

定义 4[7] 设双射 F 的所有轨道为 $\{\alpha_j,j\in I\}$, I 是一个有限集, α_j 的最小周期为 T_j, 初值为 a_{j0}, 即每个轨道为 $\left\{a_{j0},a_{j1},\cdots,a_{j(T_j-1)}\right\}$, 则所有轨道加权平均离散 Lyapunov 指数定义为

$$\tilde{\lambda}_F=\sum_{j\in I}\frac{T_j}{M}\lambda_{(F,\alpha)}. \tag{3}$$

容易证明, (3) 式中的加权平均离散 Lyapunov 指数和 (2) 式中的离散 Lyapunov 指数定义等价.

定理 1 $\lambda_F=\tilde{\lambda}_F$

证明

$$\begin{aligned}\tilde{\lambda}_F&=\sum_{j\in I}\frac{T_j}{M}\lambda_{(F,\alpha)}\\&=\sum_{j\in I}\frac{T_j}{M}\left(\frac{1}{T_j}\sum_{k=0}^{T_j-1}\ln|F(a_{jk}+1)-F(a_{jk})|\right)\\&=\frac{1}{M}\sum_{k=0}^{M-1}\ln|F(a_{jk}+1)-F(a_{jk})|\\&=\lambda_F,\end{aligned}$$

定理得证.

2.3 有限集合上的离散 Lyapunov 指数最大的一个映射

下面给出在欧氏空间上按 (2) 式的定义, Lyapunov 指数最大的一个双射 [18].

令 $M=2m$ 为偶数. 定义 $F_{\max}$ 为

$$F_{\max}(x)=\begin{cases}m+k & x=2k,k=0,1,\cdots,m-1\\ k & x=2k+1,k=0,1,\cdots,m-1\end{cases}, \tag{4}$$

在上式中取 $m=2^{n-1}$.

定理 2[18] (4) 式所示映射的离散 Lyapunov 指数等于

$$\lambda_{F\max}=\frac{m+1}{2m}\ln m+\frac{m-1}{2m}\ln(m+1).$$

对于集合 S 的任意双射 F, $\lambda_F \leqslant \lambda_{F\max}$[18].

下面, 我们将有限集合上的 Lyapunov 指数定义推广到密码学中的 S-盒的研究中.

3 密码学中 S-盒的 Lyapunov 指数

3.1 S-盒的 Lyapunov 指数定义

在密码算法的设计中, 特别是对称密码的算法设计中, S-盒有着信息混淆的重要功能, 例如在 AES, SMS4, ZUC 等算法中, 都用到了 S-盒. 一般情况下, S-盒是一个双射 $F: F_2^n \to F_2^n$, 其中 $F_2^n = \underbrace{F_2 \times F_2 \times \cdots \times F_2}_{n个}$, F_2 为仅包含元素 0 和 1 的二元域. 对 S-盒的研究内容一般包括 S-盒的设计准则、构造方法、密码学性质等 [19]. 下面给出 S-盒的一个新的密码学指标 —-Lyapunov 指数.

将有限集合上的 Lyapunov 指数定义中的距离改为汉明距离, 并给出如下关于 S-盒的 Lyapunov 指数新定义.

对 S-盒的双射 F, 令 $\alpha = \{a_0, a_1 = F(a_0), \cdots, a_{T-1} = F(a_{T-2}).\ a_0 = F(a_{T-1})\}$ 为一个最小周期为 T 的轨迹. 其中, 对 $\forall i, j \in \{0, 1, \cdots T-1\}$, 当 $i \neq j$ 时, $a_i \neq a_j$.

定义 5 双射 F 的周期为 T 的轨道 α 对于自变量变化 Δ 的 Lyapunov 指数为

$$\lambda_{(F,\alpha,\Delta)} = \frac{1}{T}\sum_{k=0}^{T-1} \log_2 \frac{H(F(a_k \oplus \Delta), F(a_k))}{W(\Delta)}, \tag{5}$$

其中, H 为汉明距离, 即 F_2^n 中的两个向量中元素不同的个数; W 为汉明重量, 即 F_2^n 中的向量中元素 "1" 的个数, $W(\Delta) \neq 0$; "$\oplus$" 为 F_2^n 上的向量的模 2 加运算.

注记: 如果取 $W(\Delta) = 1$, 则定义 5 变为如下形式:

$$\lambda_{(F,\alpha,\Delta)} = \frac{1}{T}\sum_{k=0}^{T-1} \log_2 (H(F(a_k \oplus \Delta), F(a_k))). \tag{6}$$

以下关于 Lyapunov 指数的计算中均取 $W(\Delta) = 1$.

下面给出双射 F 的对于自变量变化 Δ 的所有轨道加权平均离散 Lyapunov 指数定义.

定义 6 设双射 F 的所有轨道为 $\{\alpha_j, j \in I\}$, I 是一个有限集, α_j 的最小周期为 T_j, 初值为 a_{j0}, 即每个轨道为 $\{a_{j0}, a_{j1}, \cdots, a_{j(T_j-1)}\}$, 则双射 F 的对于自变量变化 Δ 的所有轨道加权平均离散 Lyapunov 指数定义为

$$\tilde{\lambda}_{1(F,\Delta)} = \sum_{j\in I} \frac{T_j}{M}\lambda_{(F,\alpha,\Delta)}. \tag{7}$$

也可以按所有轨道的最小值给出 Lyapunov 指数定义.

定义 7 双射 F 的对于自变量变化 Δ 的 Lyapunov 指数定义为 (5) 式对长度为 T_j 的周期轨道的最小值:

$$\tilde{\lambda}_{2(F,\Delta)} = \min_{T_j} \lambda_{(F,\alpha,\Delta)}. \tag{8}$$

根据 (2) 式, 也可以给出关于双射 F 的对于自变量变化 Δ 的与周期轨道无关的 Lyapunov 指数定义.

定义 8 双射 F 的对于自变量变化 Δ 的 Lyapunov 指数定义为

$$\lambda_{(F,\Delta)} = \frac{1}{M}\sum_{i\in F_2^n} \log_2 \frac{H(F(i \oplus \Delta), F(i))}{W(\Delta)}, \tag{9}$$

其中 $M = 2^n$.

定理 3 定义 6 与定义 8 等价, 即 $\tilde{\lambda}_{1(F,\Delta)} = \lambda_{(F,\Delta)}$.

证明 由 (7) 式和 (9) 式有

$$\begin{aligned}
&\tilde{\lambda}_{1(F,\Delta)} \\
&= \sum_j \frac{T_j}{M}\lambda_{(F,\alpha,\Delta)} \\
&= \sum_j \frac{T_j}{M}\left(\frac{1}{T_j}\sum_{k=0}^{T_j-1} \log_2 \frac{H(F(\alpha_k \oplus \Delta), F(\alpha_k))}{W(\Delta)}\right) \\
&= \frac{1}{M}\sum_{i\in F_2^n} \log_2 \frac{H(F(i \oplus \Delta), F(i))}{W(\Delta)} \\
&= \lambda_{(F,\Delta)},
\end{aligned}$$

定理得证.

最后, 给出双射 F 的 Lyapunov 指数定义.

定义 9 对双射 F 的 Lyapunov 指数定义为

$$\lambda_F = \min_{\Delta} \lambda_{(F,\Delta)}. \tag{10}$$

对双射 F, F 的离散 Lyapunov 指数能够刻画该双射中当自变量改变 1 个 bit 时, 其函数值位数的变化情况.

定理 4 按照定义 8 和定义 9, (4) 式所示双射 $F_{\max}$ 的 Lyapunov 指数为 0.

证明 只要证明对 $\forall x \in F_2^n, \forall \Delta$, 若 $W(\Delta) = 1$, 均有 $H(F(i \oplus \Delta),\ F(i)) = 1$ 即可.

一个整数的二进制展开形式为 $x=\sum_{i=0}^{n-1}x_i2^i$, 记

$$x=(x_{n-1},x_{n-2},x_{n-3},\cdots,x_1,x_0),$$

其中 x_i 为布尔变元, $x_i\in F_2=\{0,1\}$.

1) 当 $\Delta=(0,0,0,\cdots,1)$ 时

(1) 当 $x=2k$ 时, 其中 $k=0,1,2,\cdots,m-1$, 有 $x_0=0$, 即

$$x=(x_{n-1},x_{n-2},x_{n-3},\cdots,x_1,0),$$

此时

$$k=(0,x_{n-1},x_{n-2},x_{n-3},\cdots,x_1),$$

则

$$\begin{aligned}F_{\max}(x)&=m+k=2^{n-1}+k\\&=(1,x_{n-1},x_{n-2},x_{n-3},\cdots,x_1),\\x\oplus\Delta&=(x_{n-1},x_{n-2},x_{n-3},\cdots,x_1,1);\end{aligned}$$

此时

$$\begin{aligned}&k=(0,x_{n-1},x_{n-2},x_{n-3},\cdots,x_1),\\&F_{\max}(x\oplus\Delta)=k\\&=(0,x_{n-1},x_{n-2},x_{n-3},\cdots,x_1),\end{aligned}$$

则

$$\begin{aligned}&H\left(F_{\max}(x\oplus\Delta),F_{\max}(x)\right)\\&=W\left(F_{\max}(x\oplus\Delta)\oplus F_{\max}(x)\right)\\&=W\left((0,x_{n-1},x_{n-2},x_{n-3},\cdots,x_1)\right.\\&\quad\left.\oplus(1,x_{n-1},x_{n-2},x_{n-3},\cdots,x_1)\right)\\&=W\left((1,0,0,\cdots,0,\cdots,0)\right)=1.\end{aligned}$$

(2) 当 $x=2k+1$ 时, $k=0,1,2,\cdots,m-1$, 有 $x_0=1$, 即

$$x=(x_{n-1},x_{n-2},x_{n-3},\cdots,x_1,1),$$

此时

$$k=(0,x_{n-1},x_{n-2},x_{n-3},\cdots,x_1),$$

则

$$\begin{aligned}F_{\max}(x)&=k\\&=(0,x_{n-1},x_{n-2},x_{n-3},\cdots,x_1),\\x\oplus\Delta&=(x_{n-1},x_{n-2},x_{n-3},\cdots,x_1,0);\end{aligned}$$

此时

$$k=(0,x_{n-1},x_{n-2},x_{n-3},\cdots,x_1),$$

$$\begin{aligned}F_{\max}(x\oplus\Delta)&=m+k=2^{n-1}+k\\&=(1,x_{n-1},x_{n-2},x_{n-3},\cdots,x_1),\end{aligned}$$

则

$$\begin{aligned}&H\left(F_{\max}(x\oplus\Delta),F_{\max}(x)\right)\\&=W\left(F_{\max}(x\oplus\Delta)\oplus F_{\max}(x)\right)\\&=W\left((1,x_{n-1},x_{n-2},x_{n-3},\cdots,x_1)\right.\\&\quad\left.\oplus(0,x_{n-1},x_{n-2},x_{n-3},\cdots,x_1)\right)\\&=W\left((1,0,0,\cdots,0,\cdots,0)\right)=1.\end{aligned}$$

2) 当 $\Delta\neq(0,0,0,\cdots,0,1)$, 且满足 $W(\Delta)=1$ 时

(1) 当 $x=2k$ 时, $k=0,1,2,\cdots,m-1$, 有 $x_0=0$, 即

$$x=(x_{n-1},x_{n-2},x_{n-3},\cdots,x_1,0),$$

此时

$$k=(0,x_{n-1},x_{n-2},x_{n-3},\cdots,x_1),$$

则

$$\begin{aligned}F_{\max}(x)&=m+k=2^{n-1}+k\\&=(1,x_{n-1},x_{n-2},x_{n-3},\cdots,x_1);\end{aligned}$$

此时 $x\oplus\Delta$ 即为 $x=(x_{n-1},x_{n-2},x_{n-3},\cdots,x_1,0)$ 中不包括最后一位的某一位的取非运算, 不妨设 $x\oplus\Delta$ 为 x 中的 x_i 取非运算, 其他元素不变, x_i 取非运算记为 $\bar{x}_i$, 即

$$\bar{x}_i=\begin{cases}0 & x_i=1\\1 & x_i=0\end{cases},$$

则

$$x\oplus\Delta_i=(x_{n-1},x_{n-2},x_{n-3},\cdots,\bar{x}_i,\cdots,x_1,0);$$

此时

$$\begin{aligned}&k=(0,x_{n-1},x_{n-2},x_{n-3},\cdots,\bar{x}_i,\cdots,x_1),\\&F_{\max}(x\oplus\Delta_i)\\&=(1,x_{n-1},x_{n-2},x_{n-3},\cdots,\bar{x}_i,\cdots,x_1),\end{aligned}$$

则

$$\begin{aligned}&H\left(F_{\max}(x\oplus\Delta_i),F_{\max}(x)\right)\\&=W\left(F_{\max}(x\oplus\Delta_i)\oplus F_{\max}(x)\right)\\&=W\left((1,x_{n-1},x_{n-2},x_{n-3},\cdots\bar{x}_i,\cdots,x_1)\right.\\&\quad\left.\oplus(1,x_{n-1},x_{n-2},x_{n-3},\cdots,x_i,\cdots,x_1)\right)\\&=W\left((0,0,0,\cdots1,\cdots,0)\right)=1.\end{aligned}$$

(2) 当 $x = 2k+1$ 时, $k = 0,1,2,\cdots,m-1$, 有 $x_0 = 1$, 即

$$x = (x_{n-1}, x_{n-2}, x_{n-3}, \cdots, x_1, 1),$$

此时

$$k = (0, x_{n-1}, x_{n-2}, x_{n-3}, \cdots, x_1),$$

则

$$F_{\max}(x) = k = (0, x_{n-1}, x_{n-2}, x_{n-3}, \cdots, x_1);$$

此时 $x \oplus \Delta$ 即为 $x = (x_{n-1}, x_{n-2}, x_{n-3}, \cdots, x_1, 1)$ 中不包括最后一位的某一位的取非运算, 不妨设 $x \oplus \Delta$ 为 x 中的 x_i 取非运算, 其他元素不变, x_i 取非运算记为 $\bar{x}_i$, 则

$$x \oplus \Delta_i = (x_{n-1}, x_{n-2}, x_{n-3}, \cdots, \bar{x}_i, \cdots, x_1, 1),$$

此时

$$\begin{aligned} k &= (0, x_{n-1}, x_{n-2}, x_{n-3}, \cdots, \\ &\quad \bar{x}_i \cdots, x_1), \\ F_{\max}(x \oplus \Delta_i) &= (0, x_{n-1}, x_{n-2}, x_{n-3}, \cdots, \\ &\quad \bar{x}_i, \cdots, x_1), \end{aligned}$$

则

$$\begin{aligned} &H\left(F_{\max}(x \oplus \Delta_i), F_{\max}(x)\right) \\ &= W\left(F_{\max}(x \oplus \Delta_i) \oplus F_{\max}(x)\right) \\ &= W\left((0, x_{n-1}, x_{n-2}, x_{n-3}, \cdots, \bar{x}_i, \cdots, x_1)\right. \\ &\quad \left.\oplus(0, x_{n-1}, x_{n-2}, x_{n-3}, \cdots, x_i, \cdots, x_1)\right) \\ &= W\left((0,0,0,\cdots,1,\cdots,0)\right) = 1. \end{aligned}$$

定理得证.

按照文献 [7] 定义的 Lyapunov 指数, 该双射的 Lyapunov 指数为最大. 但是上述双射作为密码学中的 S-盒使用, 它的密码学性质显然是很差的. 按照我们给出的定义 8 和定义 9, 该双射的 Lyapunov 指数为 0, 由此可见我们新定义的 Lyapunov 指数是有实际意义的.

3.2 S-盒雪崩效应与 S-盒的 Lyapunov 指数之间的关系

下面, 对 S-盒雪崩效应与 S-盒的 Lyapunov 指数之间的关系进行讨论.

定义 10[19] 对于 S-盒的双射 $F(x) = (f_1(x), f_2(x), \cdots, f_n(x))$: $F_2^n \to F_2^n$ 满足雪崩效应, 是指改变输入的一个 bit, 大约有一半输出 bit 改变. 即输出大约有 $\frac{n}{2}$bit 改变.

由定义 10 可知, 该定义并不是一个严格的量化定义. 下面, 给出其量化定义, 给出 ε-雪崩效应定义.

定义 11 ε-雪崩效应: 对于 S-盒的双射

$$F(x) = (f_1(x), f_2(x), \cdots, f_n(x)) : F_2^n \to F_2^n,$$

若

$$\sup_{w(\Delta)=1, x \in F_2^n} \left| H\left(F(x \oplus \Delta), F(x)\right) - \frac{n}{2} \right| = \varepsilon,$$

则称 S-盒满足 ε-雪崩效应.

S-盒的 Lyapunov 指数与 ε-雪崩效应之间的关系满足如下定理.

定理 5 对 $\forall \Delta, W(\Delta) = 1$, 满足

$$\frac{n}{2} - \varepsilon \leqslant 2^{\lambda_{(F,\Delta)}} \leqslant \frac{n}{2} + \varepsilon.$$

证明 对 $\forall x \in F_2^n$, $\left| H\left(F(x \oplus \Delta), F(x)\right) - \frac{n}{2} \right| \leqslant \varepsilon$, 即有

$$\frac{n}{2} - \varepsilon \leqslant H\left(F(x \oplus \Delta), F(x)\right) \leqslant \frac{n}{2} + \varepsilon,$$

则有

$$\begin{aligned} \lambda_{(F,\Delta)} &= \frac{1}{2^n} \sum_{i \in F_2^n} \log_2 \frac{H\left(F\left(i \oplus \Delta\right), F\left(i\right)\right)}{W\left(\Delta\right)} \\ &\leqslant \frac{1}{2^n} \sum_{i \in F_2^n} \log_2 \frac{(n/2 + \varepsilon)}{1} \\ &= \frac{1}{2^n} \log_2 \left(\frac{n}{2} + \varepsilon\right) 2^n \\ &= \log_2 \left(\frac{n}{2} + \varepsilon\right). \\ \lambda_{(F,\Delta)} &= \frac{1}{2^n} \sum_{i \in F_2^n} \log_2 \frac{H\left(F\left(i \oplus \Delta\right), F\left(i\right)\right)}{W\left(\Delta\right)} \\ &\geqslant \frac{1}{2^n} \sum_{i \in F_2^n} \log_2 \frac{(n/2 - \varepsilon)}{1} \\ &= \frac{1}{2^n} \log_2 \left(\frac{n}{2} - \varepsilon\right) 2^n \\ &= \log_2 \left(\frac{n}{2} - \varepsilon\right), \end{aligned}$$

即

$$\log_2 \left(\frac{n}{2} - \varepsilon\right) \leqslant \lambda_{(F,\Delta)} \leqslant \log_2 \left(\frac{n}{2} + \varepsilon\right).$$

从而有

$$\frac{n}{2} - \varepsilon \leqslant 2^{\lambda_{(F,\Delta)}} \leqslant \frac{n}{2} + \varepsilon.$$

定理得证.

该定理给出了 S-盒的 Lyapunov 指数与雪崩效应之间的关系, 实际上这是混沌学中的蝴蝶效应与密码学中的雪崩效应之间的关系.

4 三个 8×8 S-盒的 Lyapunov 指数

基于以上 S-盒的设计准则, 人们提出了许多构造 S-盒的方法, 这些 S-盒对进一步设计密码算法提供了非线性资源. 本文分别针对三种不同算法生成的 S-盒, 按照本文提出的 Lyapunov 指数的定义计算了其 Lyapunov 指数.

按 (7) 式和 (10) 式计算的 Lyapunov 指数值记为 λ_1, 按 (8) 式和 (10) 式计算的 Lyapunov 指数值记为 λ_2, 对 SMS4 算法生成的 S-盒 [15] (SMS4-S-盒), AES 算法生成的 S-盒 [16](AES-S-盒) 以及基于混沌映射所生成的 S-盒 [17] (混沌 S-盒) 计算的 Lyapunov 指数值见表 1.

表 1 三种算法生成的 S-盒的 Lyapunov 指数

S-盒	λ_1	λ_2
SMS4-S-盒	1.8519	0.7925
AES-S-盒	1.8432	1.1073
混沌 S-盒	1.8564	0.5000

较大的 Lyapunov 指数意味着自变量改变 1 bit 引起的函数值的变化较大, 从表 1 的结果看, 按照不同周期轨道的加权平均来计算 Lyapunov 指数, 混沌系统生成的 S-盒的 Lyapunov 指数较大, 但是按照不同周期轨道的最小值来计算 Lyapunov 指数, 混沌系统生成的 S-盒的 Lyapunov 指数却较小, 这表明混沌系统所生成的 S-盒对某些周期较小的轨道 Lyapunov 指数很小.

5 结 论

本文借鉴有限集合上的离散混沌理论, 在汉明距离的基础上, 给出了 S-盒的 Lyapunov 指数的定义, 通过实例说明了 S-盒的 Lyapunov 指数具有实际意义.

关于映射 F 的对于自变量变化 Δ 的 Lyapunov 指数, 本文提出了两种定义方式, 见 (7) 式和 (8) 式, 对 SMS4 算法生成的 S-盒 (SMS4-S-盒), AES 算法生成的 S-盒 (AES-S-盒) 以及基于混沌映射所生成的 S-盒 (混沌 S-盒) 分别计算了其 Lyapunov 指数值. 按照不同周期轨道的加权平均来计算 Lyapunov 指数, 混沌系统生成的 S-盒的 Lyapunov 指数较大, 但是按照不同周期轨道的最小值来计算 Lyapunov 指数, 混沌系统生成的 S-盒的 Lyapunov 指数却较小, 这表明混沌系统所生成的 S-盒对某些周期较小的轨道 Lyapunov 指数很小. 对于 (4) 式所示的双射, 在文献 [7] 中其 Lyapunov 指数最大, 按本文提出的 Lyapunov 指数的定义计算该双射的 Lyapunov 指数为 0, 从密码学的角度看, 该双射也并非一个好的双射.

S-盒的 Lyapunov 指数是对传统的 S-盒的密码学指标的补充. 本文给出了 S-盒的 Lyapunov 指数与雪崩效应之间的关系, 这个关系实际上是蝴蝶效应与雪崩效应之间的关系.

[1] Biham E, Shamir A 1991 *J. Cryptology* **4** 3

[2] Mitsuru M 1998 *in Advances in Cryptology*: *EUROCRYPT'93* (Berlin: Springer-Veriag) p386

[3] Hitzl D L, Zele F 1985 *Physica* D **14** 305

[4] Pecora L M, Carroll T L 1990 *Phys. Rev. Lett*. **648** 821

[5] Wu C W, Chua L O 1993 *Int. J. Bifurcat. Chaos* **3** 1619

[6] Yang T, Chua L O 1996 *Int. J. Bifurcat. Chaos* **6** 2653

[7] Kocarev L, Szczepanski J, Amigo J M, Tomovski I 2006 *IEEE Trans. Circuits Syst*. I: *Regular Papers* **53** 1300

[8] Amigo J M, Kocarev L, Szczepanski J 2007 *Phys. Lett.* A **366** 211

[9] Chen G R, Wang X F 2006 *Chaotic Theory, Method and Application of Dynamic System* (Shanghai: Shanghai Jiaotong University Press) p88 (in Chinese) [陈关荣, 汪小帆 2006 动力系统的混沌化 —- 理论、方法与应用 (上海: 上海交通大学出版社) 第 88 页]

[10] Zhou X Y 2011 *Acta Phys. Sin*. **60** 100503 (in Chinese) [周小勇 2011 物理学报 **60** 100503]

[11] Cao G H, Hu K, Tong W 2011 *Acta Phys. Sin*. **60** 110508 (in Chinese) [曹光辉, 胡凯, 佟维 2011 物理学报 **60** 110508]

[12] Fridrich J 1998 *Int. J. Bifurcat. Chaos* **8** 1259

[13] Wang J, Jiang G P 2011 *Acta Phys. Sin*. **60** 060503 (in Chinese) [王静, 蒋国平 2011 物理学报 **60** 060503]

[14] Chirikov B V, Vivaldi F 1999 *Physica* D **129** 223

[15] Lü S W, Fan X B, Wang Z S 2008 *Complete Mapping and Application in Cryptography* (Hefei: University of Science and Technoloqy of China Press) p244 (in Chinese) [吕述望, 范修斌, 王昭顺 2008 完全映射及其密码学应用 (合肥: 中国科技大学出版社) 第 244 页]

[16] Kazlauskas K, Kazlauskas J 2009 *Informatica* **20** 23

[17] Tang G P, Liao X F, Chen Y 2005 *Chaos Soliton. Fract.* **23** 413

[18] Amigó J M, Kocarev L, Szczepanski J 2007 *IEEE Trans. Circuits Syst.* II: *Express Briefs* **54** 882

[19] Webster A F, Tavares S E 1986 *in Advances in Cryptology*: *Proceedings of CRYPTO'85* (Berlin: Springer-Verlag) p523

Research of Lyapunov exponent of S-boxes*

Zang Hong-Yan[1)†] Fan Xiu-Bin[2)] Min Le-Quan[1)] Han Dan-Dan[1)]

1) (*Mathematics and Physics School, University of Science and Technology Beijing, Beijing* 100083, *China*)

2) (*Institute of Software, Chinese Academy of Sciences, Beijing* 100190, *China*)

(Received 10 April 2012; revised manuscript received 30 April 2012)

Abstract

In the design of cryptographic algorithms, S-boxes provide the cryptosystems with the information confusion function. The traditional cryptography indexes of the S-boxes generally include linear deviation, differential characteristics, algebraic immunity, fixed point number, snowslide effect, and so on. In 2006, Kocarev et al. (Kocarev L, Szczepanski J, Amigo J M and Tomovski I 2006 IEEE Transactions on Circuits and Systems-I: regular papers **53** 6 1300) set up a discrete chaos theory based on the finite set. In light of the theory in this paper, we introduce the definition of the Lyapunov exponent with Hamming distance, calculate and compare the Lyapunov exponent values of the S-boxes in several cryptographic algorithms. In this paper we prove that a map defined on the Euclidean distance has a maximal Lyapunov exponent value of 0. In this paper it is shown that the relationship between the Lyapunov exponent and the snowslide effect of the S-box is the relationship between the butterfly effect in chaos theory and the snowslide effect in cryptography. The definition of the Lyapunov exponent of the proposed S-boxes may be complementary to the traditional cryptography indexes of the S-box.

Keywords: finite set, discrete chaos theory, S-boxes, Lyapunov exponent

PACS: 05.45.Vx, 05.45.Gg

* Project supported by the National Natural Science Foundation of China (Grant Nos. 61074192, 60833008).

† E-mail: zhylixiang@sina.com