文章编号:1001 - 9081(2010)03 - 0680 - 05

TD-ERCS 混沌系统的几个短周期轨道及其稳定性

贾伟尧[1],盛利元[2],陈亚丽[3]
(1. 西南大学 物理科学与技术学院,重庆 400715; 2. 中南大学 物理科学与技术学院,长沙 410083;
3. 漯河职业技术学院 机电工程系,河南 漯河 462002)
(wyjia@swu.edu.cn)

摘 要:基于切延迟的椭圆反射腔系统(TD-ERCS)是一类为混沌加密而设计的混沌系统,虽然其具有全域混沌等优良的加密特性,但 TD-ERCS 包含大量的可能导致弱密钥的短周期轨道,对这些短周期轨道进行功率谱分析与 Lyapunov 计算,发现 $m = 0$ 时周期轨道是稳定的,$m \geq 1$ 时周期轨道是不稳定的,且这种不稳定性不依赖参数 μ 的选取,切延迟操作使得 TD-ERCS 系统从有序走向混沌,表明 TD-ERCS 在混沌加密中不会存在稳定的短周期轨道所导致的弱密钥。

关键词:混沌加密;基于切延迟的椭圆反射腔系统;周期轨道;稳定性
中图分类号: TP309; O192 **文献标志码**:A

Several short periodic trajectories of TD-ERCS and their stabilities

JIA Wei-yao[1], SHENG Li-yuan[2], CHEN Ya-li[3]
(1. *School of Physical Science and Technology, Southwest University, Chongqing* 400715, *China*;
2. *School of Physical Science and Technology, Central South University, Changsha Hunan* 410083, *China*;
3. *Department of Electromechanical Engineering, Luohe Vocational and Technical College, Luohe Henan* 462002, *China*)

Abstract: TD-ERCS is a class of chaotic system designed for chaos encryption. Though it has good encryption properties such as being chaotic in all fields for encryption, Tangent-Delay Ellipse Reflecting Cavity map System (TD-ERCS) is comprises of quite a lot of short cycling trajectories, which may lead to weak keys. Power spectrum analysis and Lyapunov calculation of the periodic trajectories indicated that the periodic trajectories were stable under tangent-delay operation $m = 0$ and instable under tangent-delay operation $m \geq 1$. And the instability was independent of parameter μ, TD-ERCS tended from order to chaos under tangent-delay operation. The results show that TD-ERCS does not have weak keys caused by the stable short-period Trajectories.

Key words: chaotic encryption; Tangent-Delay Ellipse Reflecting Cavity map System (TD-ERCS); periodic trajectory; stability

0 引言

基于切延迟的椭圆反射腔系统(Tangent-Delay Ellipse Reflecting Cavity map System, TD-ERCS)是专门为混沌加密理论构建的一个多维混沌系统,该系统在切延迟操作 $m \geq 1$ 时系统是混沌的[1]1-3。基于 TD-ERCS 构造的并行随机数发生器的随机特性测试和分析进一步展示了该系统在混沌加密理论方面的应用前景[2]。然而,在混沌加密中,若系统存在稳定的周期轨道(特别是短周期)就意味着弱密钥[3],对加密算法的安全性构成严重威胁。在没有切延迟操作时,TD-ERCS 存在周期轨道[4],但 TD-ERCS 却在切延迟操作处于全域混沌状态[1],因此,研究 TD-ERCS 在切延迟作用下的周期轨道及其稳定性是分析 TD-ERCS 系统用于信息加密是否安全的必要环节。

作者已经发现了计算机截断误差使 TD-ERCS 从简单走向复杂的一个重要证据[5]2-3,[6],试图进一步从密码学角度寻找 TD-ERCS 系统是否存在弱密钥的重要证据,进而去证实 TD-ERCS 的安全性。本文从研究切延迟操作的性质入手,从理论上证明了 TD-ERCS 系统在不同切延迟操作下都存在的几个短周期,对这些短周期进行了计算机仿真、功率谱分析和最大 Lyapunov 指数计算,结果表明切延迟操作对周期轨道稳定性以及在系统从有序走向混沌起了关键性作用。

1 切延迟操作

TD-ERCS 的物理模型[1]1-2如图 1 所示。椭圆方程为:

$$x^2 + \frac{y^2}{\mu^2} = 1; \quad |x| \leq 1, |y| \leq 1, 0 < \mu \leq 1 \tag{1}$$

让初始射线 l_0 从初始位置 $M_0(x_0, y_0)$ 射入,l_0 与 M_0 点的切线夹角为 $\alpha(0 < \alpha < \pi)$,入射到椭圆上 $M_1(x_1, y_1)$ 点,经反射成 l_1,l_1 入射到 $M_2(x_2, y_2)$,经反射成 l_2,如此继续,得到一个点序列 $M = \{M_i(x_i, y_i) \mid i = 0,1,2,\cdots\}$ 和一个射线序列 $L = \{l_i \mid i = 0,1,2,\cdots\}$。取点序列 M 中坐标 x_i 序列 $X = \{x_i \mid i = 0,1,2,\cdots\}$ 和反射线 l_i 的斜率 k_i 序列 $K = \{k_i \mid i = 0,1,2,\cdots\}$ 描述 ERCS 的状态,且有迭代方程:

$$x_n = -\frac{2k_{n-1}y_{n-1} + x_{n-1}(\mu^2 - k_{n-1}^2)}{\mu^2 + k_{n-1}^2}; \; n = 1,2,3,\cdots \tag{2}$$

$$k_n = \frac{2k'_n - k_{n-1} + k_{n-1}k'^2_n}{1 + 2k_{n-1}k'_n - k'^2_n}; \; n = 1,2,3,\cdots \tag{3}$$

收稿日期:2009 - 09 - 06;**修回日期**:2009 - 11 - 01。
基金项目:国家自然科学基金资助项目(60672041);西南大学基本科研业务费专项资金资助项目(XDJK2009C029)。
作者简介:贾伟尧(1979 -),男,河南漯河人,讲师,硕士,主要研究方向:混沌安全性研究、混沌保密通信; 盛利元(1956 -),男,湖南益阳人,教授,硕士,主要研究方向:混沌加密理论、信号处理; 陈亚丽(1981 -),女,河南漯河人,助教,硕士,主要研究方向:电气自动化。

$$k'_{n-m} = -\frac{x_{n-m}}{y_{n-m}}\mu^2;\ m = 1,2,\cdots,n \tag{4}$$

其中 k'_n 为 M_n 点处椭圆切线斜率,有 $k'_n = -\frac{x_n}{y_n}\mu^2$,$y_n = k_{n-1}(x_n - x_{n-1}) + y_{n-1}$。在式(3)中,用式(4)中的 k'_{n-m} 替换 k'_n,这种替换称为切延迟操作,m 称为切延迟单位,此时的 ERCS 称为 TD-ERCS。

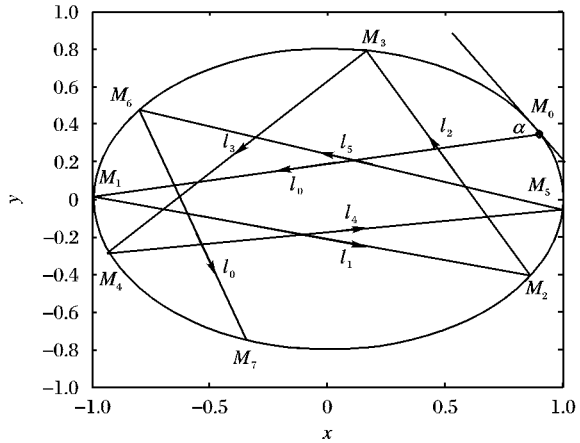

图 1　ERCS 物理模型

在切延迟操作下,相互平行或垂直的切线反射性等价[7]2。在切延迟操作下,研究周期轨道,引入过渡态与正常态概念[7]2。

2　几个短周期轨道

2.1　周期 2 轨道

为表示方便,用点序列 $M = \{M_i(x_i,y_i) \mid i = 0,1,2,\cdots\}$ 来表示周期轨道。

定理 1　$0 < \mu < 1$ 时,对于 $m = 0$,TD-ERCS 仅存在 2 个周期 2 轨道 $\{1,-1\}$ 和 $\{0,0\}$。

证明　$m = 0$,系统没有切延迟。由于椭圆关于中心对称,依照系统图 1 的演化规则及几何性质,周期 2 轨道存在的充要条件是周期点处的法线经过椭圆中心。周期 2 轨道 $\{1,-1\}$ 和 $\{0,0\}$ 分别对应椭圆长轴端点 $(1,0)$、$(-1,0)$ 和短轴端点 $(0,1)$、$(0,-1)$,其法线是 x 轴和 y 轴,故 $\{1,-1\}$ 和 $\{0,0\}$ 是周期 2 轨道。至于其他点,可在椭圆上任取一点 (x_0,y_0),$x_0 \neq 0, y_0 \neq 0$,求得其法线方程为:

$$yx_0 - \frac{1}{\mu^2}xy_0 = x_0y_0\left(1 - \frac{1}{\mu^2}\right) \tag{5}$$

令 $y = 0$,得 $x = x_0(1-\mu^2) \neq 0$,可见 $\mu \neq 1$ 时,法线不经过原点,即 (x_0,y_0) 不是周期 2 的轨道点。　证毕。

定理 2　$0 < \mu < 1$ 时,对于 $m \geqslant 1$,TD-ERCS 存在 2 个周期 2 轨道 $\{1,-1\}$ 和 $\{0,0\}$。

证明　周期 2 轨道 $\{1,-1\}$ 对应椭圆长轴的两端点 $(1,0)$ 和 $(-1,0)$,其切线是反射性等价的。因此,系统的正常态若处在周期轨道点 $(1,0)$ 或 $(-1,0)$ 上,只要前第 m 个点也在周期轨道点 $(1,0)$ 或 $(-1,0)$ 上,则根据切延迟操作规则,系统演化的下一个点也是周期轨道点 $(1,0)$ 或 $(-1,0)$。这样,只要给定初值 x_0 为周期轨道点 $(1,0)$ 或 $(-1,0)$,且采用第一类过渡态或第二类过渡态,则系统过渡态的点就是周期轨道点 $(1,0)$ 和 $(-1,0)$,正常态在 $m \geqslant 1$ 条件下就有周期 2 轨道 $\{1,-1\}$。同样的方法也可证 $\{0,0\}$。　证毕。

2.2　周期 3 轨道

定理 3　$0 < \mu < 1$ 时,对于 $m = 0$,TD-ERCS 至少存在轴对称的周期 3 轨道。

证明　周期 3 轨道是椭圆的内接三角形,依照系统图 1 的演化规则及几何性质,对于 $m = 0$,三角形的角平分线与其顶点处的椭圆法线重合,就是说,周期 3 轨道的必要条件是周期点处的三条法线相交于一点。不失一般性,设三个周期点坐标分别为 (x_1,y_1),(x_2,y_2),(x_3,y_3),套用式(5)得三条法线方程:

$$l_1:\ yx_1 - \frac{1}{\mu^2}xy_1 = x_1y_1\left(1 - \frac{1}{\mu^2}\right)$$

$$l_2:\ yx_2 - \frac{1}{\mu^2}xy_2 = x_2y_2\left(1 - \frac{1}{\mu^2}\right)$$

$$l_3:\ yx_3 - \frac{1}{\mu^2}xy_3 = x_3y_3\left(1 - \frac{1}{\mu^2}\right)$$

由此得 l_1、l_2 和 l_3 交于一点的条件为

$$x_1x_2y_1y_3 + x_1x_3y_2y_3 + x_2x_3y_1y_2 - x_1x_2y_2y_3 - x_1x_3y_1y_2 - x_2x_3y_1y_3 = 0 \tag{6}$$

因此,若 (x_1,y_1) 在 y 轴上,则 $x_1 = 0$,必有 $y_2 = y_3$;若 (x_1,y_1) 在 x 轴上,则 $y_1 = 0$,必有 $x_2 = x_3$。再由对称性知,至少有 4 个周期 3 轨道,它们关于 x 轴或 y 轴对称。　证毕。

已知坐标轴上一个点及对称性,再由入射线与反射线夹角相等条件可求出轴对称周期3轨道点。如关于 y 轴对称的一个周期 3 轨道为 $\left\{0, -\frac{\mu^2}{k_1^2} - 2\frac{\mu}{k_1}, \frac{\mu^2}{k_1^2} + 2\frac{\mu}{k_1}\right\}$,其中 $k_1 = \frac{2k}{1-k^2}$,$k = \pm\sqrt{\frac{2}{\mu^2} - 1 + \frac{2}{\mu^2}\sqrt{1+\mu^4-\mu^2}}$。非轴对称周期 3 轨道的存在性,还没有找到简明证明方法。

定理 4　$0 < \mu < 1$ 时,若 $m = 3m_1, m_1 = 1,2,\cdots$,则 TD-ERCS 存在轴对称的周期 3 轨道。

证明　为了简化表示,设由定理 3 确定的周期 3 轨道为 $\{0,-x,x\}$。类似定理2的证明,给定初值 x_0 为周期3轨道 $\{0,-x,x\}$ 的点,采用第一类过渡态,由于 $m = 3m_1, m_1 = 1,2,\cdots$,故系统过渡态的点都是周期 3 轨道 $\{0,-x,x\}$ 的点,即得到的 m 条初始切线正是周期 3 轨道 $\{0,-x,x\}$ 的点的切线,且相继重复 m_1 次,直到最末一个过渡态轨道点 x_{m-1} 也为周期 3 轨道 $\{0,-x,x\}$ 的点,并导致第一个正常态的轨道点 $x_m = x_0$,再由式(10)知,延迟切线正是 x_0 点的切线,故第二个正常态轨道点 x_{m+1} 仍是 $\{0,-x,x\}$ 的点,且延迟切线也是同一点的切线。如此继续,可知所有正常态轨道点都是 $\{0,-x,x\}$ 上的点。　证毕。

2.3　周期 4 轨道

定理 5　$0 < \mu < 1$,对于 $m = 0$,TD-ERCS 存在非轴对称的周期 4 轨道。

证明　在椭圆上任取一点 $M_1(x_1,y_1)$,若 $M_1(x_1,y_1)$ 是周期4轨道点,则由周期轨道点的性质可以求出其他3个周期点,依次设其为 $M_2(x_2,y_2)$、$M_3(x_3,y_3)$、$M_4(x_4,y_4)$。由对称性知,M_1 与 M_3,M_2 与 M_4 必然关于中心对称,如图2所示,周期4轨道是一个平行四边形。进一步,可通过 M_1、M_2、M_3 和 M_4 分别作椭圆的切线,这四条切线构成椭圆的外切平行四边形,可证它是一个矩形。

设 M_1 为起始点,过 M_2 和 M_3 各做一条法线,设射线在 M_2 处的入射角和反射角分别为 α_2 和 β_2,在 M_3 处的入射角和反射角分别为 α_3 和 β_3,根据系统的演化规则,必须有 $\alpha_2 = \beta_2$,$\alpha_3 = \beta_3$,即 $\alpha_2 + \beta_3 = \beta_2 + \alpha_3$。又由平行四边形性质知 $\alpha_2 + \beta_2 + \alpha_3 + \beta_3 = \pi$,故只能有 $\alpha_2 + \beta_3 = \beta_2 + \alpha_3 = \pi/2$。因此,若周期 4 轨道存在,则其轨道点处的切线必定构成一个矩形。

根据以上几何关系,可得到周期 4 轨道点坐标间关系:

$$x_1 = -x_3,\ y_1 = -y_3,\ x_2 = -x_4,\ y_2 = -y_4 \tag{7}$$

和切线与 M_2 的法线之间的关系:

$$y_1y_2 + x_1x_2\mu^4 = 0 \tag{8}$$

以及 M_2 处入射线与反射线的斜率:

$$k_1 = \frac{y_2 - y_1}{x_2 - x_1},\ k_2 = \frac{y_3 - y_2}{x_3 - x_2} = \frac{y_2 + y_1}{x_2 + x_1} \tag{9}$$

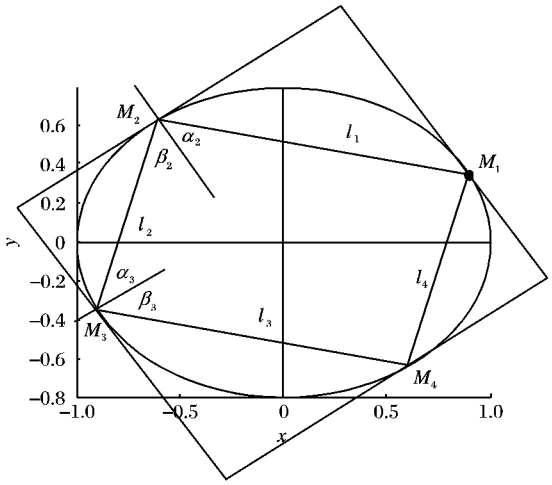

图 2 $0 < \mu < 1$ 的周期 4 轨道

这里已经将式(7)代入。由式(7)可知,只要能证明 $M_2(x_2,y_2)$ 存在,则周期 4 就存在。

$M_2(x_2,y_2)$ 存在的必要条件是 $\alpha_2 = \beta_2$。两边取正切得:

$$\tan\alpha_2 = \frac{k_1 - \frac{1}{\mu^2}\frac{y_2}{x_2}}{1 + k_1\frac{1}{\mu^2}\frac{y_2}{x_2}} = \frac{\frac{1}{\mu^2}\frac{y_2}{x_2} - k_2}{1 + k_2\frac{1}{\mu^2}\frac{y_2}{x_2}} = \tan\beta_2 \tag{10}$$

将式(9)代入式(10),化简后得:

$$x_1^2x_2y_2\mu^2 - x_1y_1x_2^2\mu^4 + x_1y_1y_2^2 - x_2y_2y_1^2\mu^2 + x_2y_2\mu^2(\mu^2 - 1) = 0 \tag{11}$$

将式(11)与椭圆方程 $x_2^2 + \frac{y_2^2}{\mu^2} = 1$ 联立,原则上可解出 x_2 和 y_2,此解过程复杂,且还不能证明 $\alpha_3 = \beta_3$。为此可由式(8)与椭圆方程联立,再利用 4 个周期点的象限关系,解得:

$$x_2 = \frac{-y_1}{\sqrt{y_1^2 + x_1^2\mu^6}},\ y_2 = \frac{x_1\mu^4}{\sqrt{y_1^2 + x_1^2\mu^6}} \tag{12}$$

将此解代入式(11),若使式(11)恒等,则由式(12)给出的 $M_2(x_2,y_2)$ 是周期 4 的轨道点,即非轴对称周期 4 轨道存在。容易验证,式(12)是式(11)的解。再由 $M_1(x_1,y_1)$ 的任意性知,非对称的周期 4 轨道有无穷多个。 证毕。

显然,上面的证明同时也给出了周期 4 轨道点的计算方法。易见,定理5所给的周期4轨道,其中所有轨道点的切线反射性等价,因此,采用证明定理 2 的方法,同样可得下面定理。

定理6 $0 < \mu < 1$ 时,对于 $m \geqslant 1$,TD-ERCS 存在由定理 5 给出的周期 4 轨道。

周期 4 轨道是一种十分特殊的周期轨道,其轨道点在椭圆上连续分布,在任意切延迟操作下都存在,这一性质决定了它是研究轨道稳定性的一个难得的仿真实验素材。

3 周期轨道的稳定性分析

3.1 几个短周期轨道仿真

虽然前面从几何定理出发,导出了 TD-ERCS 系统的周期 2、周期 3 和周期 4 的理论解。由于在切延迟单位 $m = 0$ 与 $m \geqslant 1$ 条件下,TD-ERCS 有相同的短周期轨道,又由于计算机存在截断误差,故可利用计算机仿真检验这些周期轨道的稳定性。仿真实验在 Matlab 6.5 上完成,取双精度实数,截断误差为 2^{-53},直接利用迭代关系式(6)、式(7)及切线延迟式(10)进行仿真,均采用第一类过渡态。

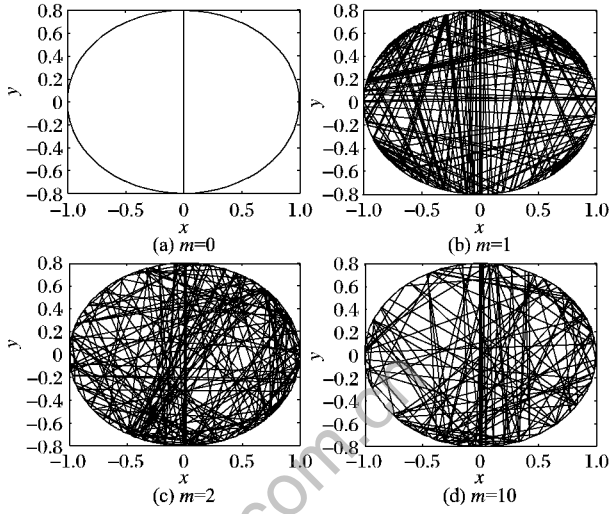

图 3 周期 2 轨道{0,0}仿真

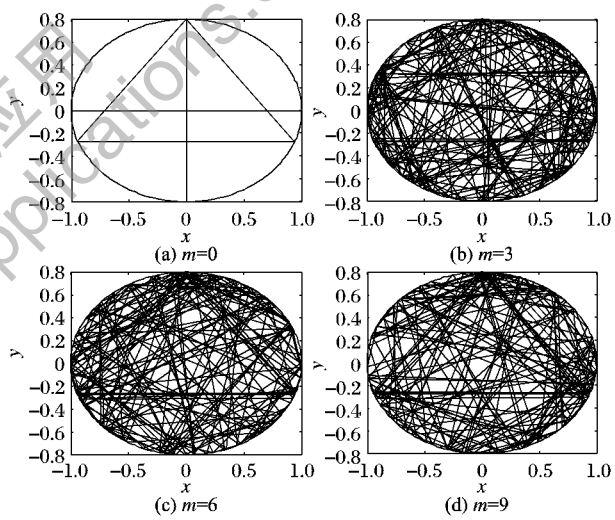

图 4 周期 3 轨道{0, -x,x} 仿真

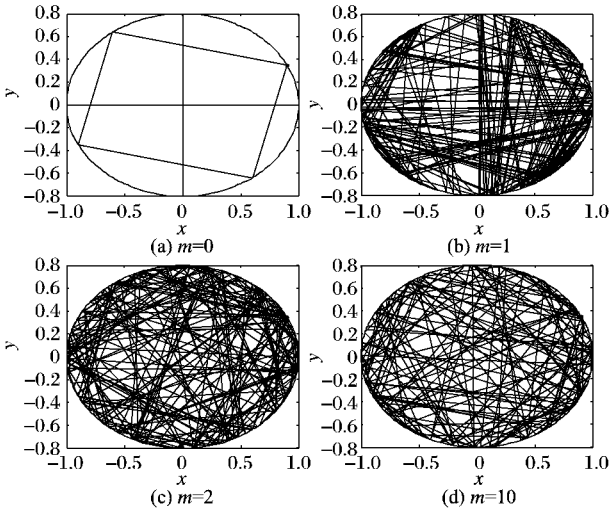

图 5 周期 4 轨道{x_0,x_1, $-x_0$, $-x_1$} 仿真

图 3 为周期 2 轨道{0,0} 的仿真结果($\mu = 0.8$, $x_0 = 0$, $n = 150$)。$m = 0$ 时,{0,0} 是稳定的;$m \geqslant 1$ 时,{0,0} 是不稳定的。图 4 为周期 3 轨道{0,x, $-x$} 的仿真结果($\mu = 0.8$,

$x_0 = 0$, $n = 150$)。$m = 0$ 时,$\{0, x, -x\}$ 是稳定的;$m = 3, 6, 9$ 时,$\{0, x, -x\}$ 是不稳定的。图 5 为周期 4 轨道 $\{x_0, x_1, -x_0, -x_1\}$ 的仿真结果($\mu = 0.8$, $x_0 = 0.9$, $n = 150$)。$m = 0$ 时,$\{x_0, x_1, -x_0, -x_1\}$ 是稳定的;$m \geq 1$ 时,$\{x_0, x_1, -x_0, -x_1\}$ 是不稳定的。图 6 给出了 $m = 0$ 时的周期 2 轨道 $\{1, -1\}$,其中:$\mu = 0.8$, $x_0 = 1$, $n = 250$。仿真结果表明该周期轨道是不稳定的,这是 $m = 0$ 时周期轨道不稳定的唯一例外,它是由计算机截断误差诱导产生的随机振荡行为[5]3。

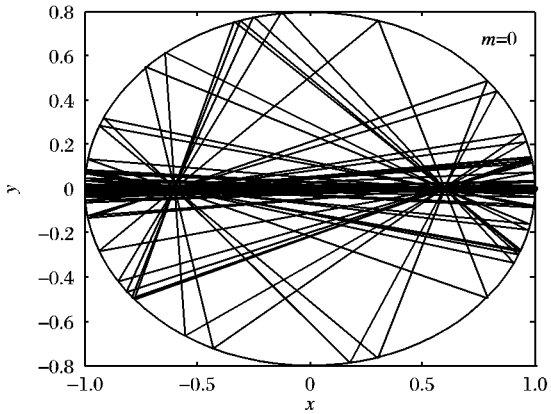

图 6　周期 2 轨道 $\{1, -1\}$ 仿真

以上仿真实验可得出如下基本结论:$m = 0$ 时,除周期 2 轨道 $\{1, -1\}$ 外,TD-ERCS 的短周期轨道是稳定的;$m \geq 1$ 时,TD-ERCS 的短周期轨道是不稳定的。

3.2　周期 4 轨道的功率谱分析

切延迟操作使周期轨道变得不稳定,直接后果将使系统走向混沌。为证明这一推断,对图 5 的周期 4 轨道进行了功率谱分析,实验结果如图 7 所示,其中 $\mu = 0.8$, $x_0 = 0.9$, $n = 1024$。计算中,先行 200 次迭代,再从 $n = 200$ 开始,取 1024 个轨道点计算功率谱。对于 $m = 0$,周期 $T = 4$,故频率为 $f = 1/T = 0.25$,频谱为 δ 函数。对于 $m = 1, 2, 10$,均表现为白噪声性质的频谱,正是系统显现混沌特性的标志,表明 TD-ERCS 在切延迟操作下从有序走向混沌。

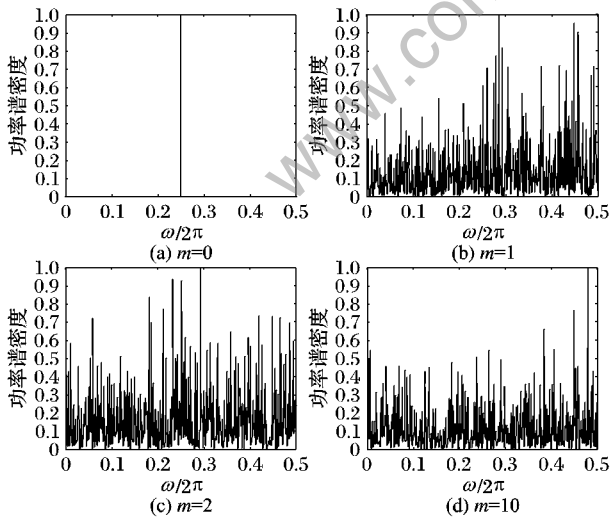

图 7　周期 4 轨道 $\{x_0, x_1, -x_0, -x_1\}$ 功率谱

3.3　周期 4 轨道的最大 Lyapunov 指数计算

最大 Lyapunov 指数大于 0 是混沌的充分必要条件,对具有很强代表性的周期 4 轨道的最大 Lyapunov 指数进行计算,参数 $\mu = 0.8$,初始值 $x_0 = 0.9$,系统在不同切延迟操作下均进行 103 000 次迭代,舍去前 10 000 次过渡态,取 $n = 3000$ 个轨道点,时间序列取轨道点的横坐标,先通过自相关法求时间序列的最佳时间延迟 τ,再通过 G-P 算法对时间序列相空间重构,得到时间序列的最佳嵌入维数 n,最后利用 Wolft 算法计算出最大 Lyapunov 指数[8-11],计算结果如表 1。

表 1　周期 4 轨道 $\mu = 0.8$, $m = 1, 2, 10$ 的最大 Lyapunov 指数

切延迟 m	时间延迟 τ	嵌入维数 n	最大 Lyapunov 指数
1	7	7	0.8624
2	1	5	1.1950
10	5	5	0.7221

由表 1 结果可知,周期 4 轨道在不同切延迟操作下均走向混沌,再次表明周期 4 轨道的不稳定性,按上述方法对周期 4 轨道在参数 $m = 1$、不同参数 μ 时得到的时间序列 x_n 的最大 Lyapunov 指数进行计算,结果如表 2。计算结果表明,这种不稳定与参数 μ 的选取关系不大,也就是说,当 $m \geq 1$ 时,在参数 $\mu(0,1)$ 的大部分范围内周期 4 轨道都是不稳定的,即便是在 0 附近,周期 4 轨道也是准周期的,处于亚稳态。这也进一步说明,TD-ERCS 系统在大的参数空间 $\mu(0.000\,001, 1)$ 内,都具有较强的抗退化能力。

表 2　周期 4 轨道在切延迟 $m = 1$ 时,不同参数 μ 的最大 Lyapunov 指数

参数 μ	时间延迟 τ	嵌入维数 n	最大 Lyapunov 指数
1.000 000	8	9	0.5254
0.990 000	13	5	1.0171
0.010 000	30	7	2.1877
0.000 001	27	3	0.0272

周期 4 轨道在切延迟 $m = 1$、椭圆参数 $\mu = 0.000\,001$、迭代次数 $n = 20000$ 时的时间序列 x_n 的演化进程和功率谱如图 8 所示:图 8(a) 为 x_n 的演化进程;图 8(b) 为演化时间 6000 附近 x_n 的演化进程的局部放大图,图中可以观察到倍周期分叉、自相似结构等准周期行为;图 8(c) 所示的功率谱中虽然只有一个主峰,对功率谱纵轴方向放大 1500 倍后发现,功率谱中还有无穷多个小峰,见图 8(d)。说明系统还有其他倍周期成分,而计算得到的最大 Lyapunov 指数为 0.0272,略大于 0,进一步表明其具备弱混沌特征,说明切延迟操作使周期轨道退化的有效机制几乎适用于整个参数 μ 空间,从而保证了 TD-ERCS 用于混沌加密时具备大的参数空间。同时,参数 μ(椭圆压缩因子) 等于 0.000 001 时,椭圆几乎压缩成一条线,此时的 TD-ERCS 系统在计算机迭代时受计算机误差累积效应影响很大,也许正是由于误差的累积才导致了系统的准周期性,从而出现倍周期分叉等现象,对这一现象的解释和进一步研究,会丰富对 TD-ERCS 这一新生混沌系统的认识和了解,从而加深对混沌的一般认识,特别是可以进一步了解误差与周期轨道之间的内在联系。

4　结语

TD-ERCS 混沌模型与其他混沌模型一样,存在着短周期轨道,用于加密时还存在计算机截断误差,而截断误差往往使长周期的混沌轨道退化为短周期轨道[12-14]。本文研究结果表明,切延迟操作使得 TD-ERCS 系统的短周期轨道演变为长周期的混沌轨道,从而使系统从有序走向混沌,混沌系统没有在计算机截断误差作用下退化,甚至截断误差还会导致混沌的产生[5]3,[6]2-3,从混沌加密理论来看,TD-ERCS 混沌系统不可能存在稳定的短周期导致的弱密钥,具有很强的抗退化能力。这一结论具有密码学上的重要意义,再次显示出 TD-ERCS 混

沌系统在密码学上的应用前景。对同一周期轨道采用不同切延迟操作,得到不同的实验结果,这种对比实验表明切延迟操作对 TD-ERCS 系统的演化起了决定性作用,使得稳定的周期轨道变得不稳定。但从表观上看,如果 $m = 0$ 的周期轨道是稳定的,$m \geq 1$ 时对应的同一周期轨道也应该是稳定的,因为两者的反射介面(即延迟切线)本质上没有发生变化,其他计算内容和截断误差也相同。然而实验结果却截然相反,表明可能还存在一种目前尚不清楚的机制,使得切延迟操作具有破坏系统稳定性的特殊作用。

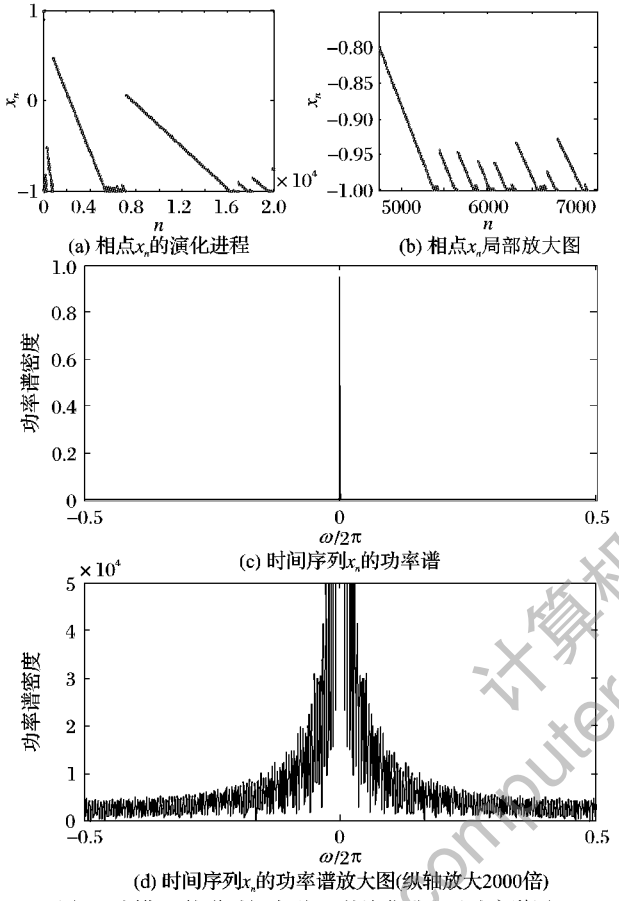

图 8 周期 4 轨道时间序列 x_n 的演化进程及功率谱图

参考文献:

[1] 盛利元,孙克辉,李传兵. 基于切延迟的椭圆反射腔映射系统及其性能研究[J]. 物理学报,2004,53(9):2871 - 2876.

[2] 盛利元,曹利凌,孙克辉,等. 基于 TD-ERCS 混沌系统的伪随机数发生器及其统计特性分析[J]. 物理学报,2005,54(9):4031 - 4037.

[3] LI S J, MOU X Q, CAI Y L, *et al*. On the security of a chaotic encryption scheme: Problems with computerized chaos in finite computing precision [J]. Computer Physics Communications, 2003, 153(1): 52 - 58.

[4] 贾伟尧,盛利元. 无切延迟作用的 TD-ERCS 混沌系统的周期轨道[J]. 西南大学学报:自然科学版,2007,29(11):57 - 60.

[5] 盛利元,贾伟尧. 一个截断误差诱导下的随机数字振荡系统[J]. 物理学报,2005,54(12):5574 - 5580.

[6] 盛利元,贾伟尧,吴舒辞,等. 截断误差诱导阵发混沌与拓展维[J]. 物理学报,2007,56(7):3753 - 3758.

[7] 贾伟尧,盛利元. 切延迟作用下的 TD-ERCS 混沌系统的周期轨道研究[J]. 西南大学学报:自然科学版,2009,31(7):78 - 82.

[8] 吕金虎,陆君安,陈世华. 混沌时间序列分析及其应用[M]. 武汉:武汉大学出版社,2005.

[9] GRASSBERGER P, PROCACCIA I. Characterization of strange attractors [J]. Physical Review Letters, 1983, 50(5): 346 - 349.

[10] ROSENSTEIN M T, COLLINS J J, de LUCA C J. A practical method for calculating largest Lyapunov exponents from small data sets [J]. Physica D, 1993, 65(1/2): 117 - 134.

[11] WOLF A, SWIFT J B, SWINNEY H L, *et al*. Determining Lyapunov exponents from a time series [J]. Physica D, 1985, 16(3): 285 - 317.

[12] BECK C, ROEPSTORFF G. Effects of phase space discretization on the long-time behavior of dynamical systems [J]. Physica D, 1987, 25(1/3): 173 - 180.

[13] BINDER P M. Limit cycles in a quadratic discrete iteration [J]. Physica D, 1992, 57(1/2): 31 - 38.

[14] LEVY Y E. Some remarks about computer studies of dynamical systems [J]. Physics Letters, 1982, 88A: 1 - 3.

(上接第 676 页)

项数分布模糊分类快速排队,进而重复搜索。实验结果表明,此类 H 型 S 盒中未出现重复,因此有如下命题成立。

命题 5 有限域 F_2 上的 8×8 循环矩阵构造的 H 型 S 盒 $S(x) = h(g(f(x)))$ 的个数为 2^{30},其中 $x \in F_2^8$,$S(x) \in F_2^8$,f,h 为仿射变换,$f(x) \triangleq A_1 x + b_1$,$h(x) \triangleq A_2 x + b_2$,矩阵 A_1,A_2 为循环矩阵,b_1,$b_2 \in F_2^8$,g 为有限域 F_2^8 上乘法求逆变换,这里限定 $F_2^8 = F_2[x]/(x^8 + x^4 + x^3 + x + 1)$。

4 结语

本文给出了一类适于硬件实现的 S 盒构造方法,探讨了该类 S 盒的密码学性质及其计数问题,评估了在硬件实现过程中的资源消耗和效率。在不降低密码算法的安全性前提下,与 Rijndeal 算法 S 盒相比,资源消耗相当,特别地,在硬件电路中采用该类 S 盒作为密码算法部件,可动态实现 S 盒内容的更新换代,有效提高密码算法的安全性。

参考文献:

[1] NYBERG K. Differentially uniform mappings for cryptography [C]// Advances in Cryptography - Eurocrypt'93. Berlin: Springer-Verlag, 1994: 55 - 64.

[2] JAKOBSEN T, KNUDSEN L R. Attacks on block ciphers of low algebraic degree [J]. Journal of Cryptology, 2002, 14(1): 197 - 210.

[3] MORIAI S, SHIMOYAMA T, KANEKO T. Interpolation attacks of the block cipher: SNAKE [C]// Proceedings of Fast Software Encryption. Berlin: Springer-Verlag, 1999: 275 - 289.

[4] Nessie Project. Nessie security report [EB/OL]. [2009 - 07 - 20]. http://www.cryptonessie.org.

[5] LIU FEN, JI WEN, HU LEI, *et al*. Analysis of the SMS4 block cipher [C]// Proceedings of the 12th Australasian Conference on Information Security and Privacy, LNCS 4586. Berlin: Springer-Verlag, 2007: 158 - 170.

[6] LIU JING-MEI, WEI BAO-DIAN, CHENG XIANG-GUO, *et al*. An AES S-box to increase complexity and cryptographic analysis [C]// Proceedings of the 19th International Conference on Advanced Information Networking and Applications. Washington, DC: IEEE Computer Society, 2005: 724 - 728.