第 56 卷 第 1 期 2007 年 1 月
1000-3290/2007/56(01)/0078-06

物 理 学 报
ACTA PHYSICA SINICA

Vol.56,No.1,January,2007

TD-ERCS 混沌系统的差分分析*

盛利元[1)†] 闻 姜[1)] 曹莉凌[1)] 肖燕予[2)]

1)(中南大学物理科学与技术学院,长沙 410083)

2)(湖南大学数学与计量经济学院,长沙 410082)

(2006 年 4 月 7 日收到;2006 年 5 月 21 日收到修改稿)

基于差分分析基本原理和混沌系统“迭代”与分组密码“轮”的对应关系,提出了迭代差分分布和差分失效指数的概念,用于评估混沌系统抗差分分析的能力.将混沌系统置于“裸”状态,直接分析混沌系统的迭代差分分布,从而测出差分失效指数.研究混沌系统的安全性,差分失效指数是一个普适的可测的重要的系统特征指数.对 TD-ERCS 和 Logistic 混沌系统的测试结果表明,在 90% 的参数变化范围内,TD-ERCS 的差分失效指数等于 2(理论上的最小值),相比之下,Logistic 的差分失效指数等于 55.推知,TD-ERCS 是一种能自动免疫差分分析的混沌系统.

关键词:混沌的安全性,差分分析,TD-ERCS,Logistic

PACC:0545

1. 引 言

近 10 多年来,混沌数字加密理论成为新的研究热点.常见采用低维混沌系统(也是自然系统)如 Logistic,tent,PL1D 等等设计流密码、分组密码和 Hash 函数[1—5],但就混沌系统自身来说,多少存在某些安全缺陷.在混沌密码分析文献中,所有的安全性分析都是针对密码算法的.不断修正算法缺陷将使一个简单混沌加密算法会变得十分复杂,而安全性仍然很难得到根本性改善.混沌系统是构造混沌加密算法的“核”,若“核”不安全,很难想象由它构成的加密算法是安全的.对初始条件的敏感性只是混沌系统用于信息加密的必要条件而不是充分条件,混沌系统的安全性是混沌加密算法安全性的基础,这是目前混沌数字加密理论研究的盲区,应该引起注意和重视.要想找到一种安全的混沌加密算法,首先要在传统密码分析的基础上建立起混沌的安全性理论,在此理论指导下寻找或构造安全混沌.盛利元等[6]基于混沌安全性条件构造了一类新的混沌系统:基于切延迟的椭圆反射腔映射系统(TD-ERCS).本文试图对这一新的混沌系统进行差分分析.差分密码分析是由 Biham 和 Shamir[7] 提出的迄今已知的攻击分组密码的最好方法之一,Kocarev[8] 把差分分析与线性分析作为评估混沌安全性的首选指标.本文不涉及具体的密码算法,仅根据 TD-ERCS 迭代与分组密码轮的对应关系,直接分析 TD-ERCS 迭代对输出差分和输入差分的特征分布的影响,从而提出了一个可评估混沌系统抗差分分析能力的可测量指数——差分失效指数.

2. TD-ERCS 混沌系统的迭代关系

文献[9]提出了一个基于 TD-ERCS 的伪随机数发生器的算法,这里仅给出该算法的相关计算式.给定压缩系数 $\mu\in(0,1]$,切延迟 $m\in Z^+$,及初始值 $|x_0|\in[0,1]$ 和 $\alpha\in(0,\pi)$,计算其他初值:

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

$$k_0' = -\frac{k_0}{y_0}\mu^2, \tag{2}$$

$$k_0 = \frac{\tan\alpha + k_0'}{1 - k_0'\tan\alpha}. \tag{3}$$

然后由下面的迭代关系计算 TD-ERCS 的状态参量 (x_n,k_n),即

$$x_n = -\frac{2k_{n-1}y_{n-1} + x_{n-1}(\mu^2 - k_{n-1}^2)}{\mu^2 + k_{n-1}^2}, \tag{4}$$

* 国家自然科学基金(批准号:60672041)资助的课题.

† E-mail:itpo@mail.csu.edu.cn

$$k_n = \frac{2k'_{n-m} - k_{n-1} + k_{n-1}k'^2_{n-m}}{1 + 2k_{n-1}k'_{n-m} - k'^2_{n-m}}, \tag{5}$$

$|x_n| \in [0,1]$，$|k_n| \in [0,\infty)$，$n = 1,2,3,\cdots$，其中

$$k'_{n-m} = \begin{cases} -\dfrac{x_{n-1}}{y_{n-1}}\mu^2, n < m, \\ -\dfrac{x_{n-m}}{y_{n-m}}\mu^2, n \geqslant m, \end{cases} \tag{6}$$

$$y_n = k_{n-1}(x_n - x_{n-1}) + y_{n-1}, \tag{7}$$

这里，(x_n, y_n)为椭圆

$$x^2 + \frac{y^2}{\mu^2} = 1 \tag{8}$$

上的点，k_n 是通过该点的射线的斜率，k'_n 是该点的切线的斜率；(x_0, k_0)为 TD-ERCS 的初态，α 是初始射线与点(x_0, y_0)的切线的夹角；$n < m$ 的状态称为过渡状态，$n \geqslant m$ 的状态称为正常状态；当 $m \geqslant 1$ 时，系统有切线延迟操作，系统是混沌的；当 $m = 2,4,5,6,\cdots$时，系统可获得两个相互独立的状态序列 $\{x_i\}$和 $\{k_i\}$，它们是相互独立的；分别由下面两式变换成均匀分布的伪随机序列：

$$\theta_i = \frac{\arccos(x_i)}{\pi}, \tag{9}$$

$$\beta_i = 0.5 + \frac{\arctan(k_i)}{\pi}, \tag{10}$$

$\theta_i \in [0,1]$，$\beta_i \in [0,1)$，$i = 0,1,2,3,\cdots$.

$\{\theta_i\}$和 $\{\beta_i\}$具有稳定的均匀分布，与初始条件和系统参数无关，称为 TD-ERCS 的归一化相点，对应的相空间用 Λ 表示.

3. TD-ERCS 与分组密码的对应关系

混沌系统的主要特征与密码算法的主要特征具有一一对应的关系是混沌系统可用于信息加密的原因之一. Kocarev[8] 给出了一个不完善的对比图(图 1).图中，对应密码算法的安全性与特性，混沌系统一栏用‘?’表示，我们认为它对应混沌系统的安全性条件及其相关性质.图中还缺少分组密码的混乱特征和子密钥特征，是否意味着目前常见的混沌系统缺少对应特征？仔细分析，发现 TD-ERCS 存在这两种对应特征.椭圆上点(x_n, y_n)的切线斜率即(6)式可对应子密钥，它与 μ 有关，与点(x_n, y_n)的坐标有关，也与 m 间接有关，是一个在迭代过程产生的类随机变量，仅使用一次. Alvarez[10] 指出，混沌系统的各态遍历性对应混乱，但要求混沌系统有稳定不变的分布. TD-ERCS 具有这样一种优良性质.将这三个对应关系列于图 2，并与图 1 综合，构成了 TD-ERCS 与分组密码的对应关系.因此，可以在不涉及具体加密算法条件下，直接对 TD-ERCS 进行差分分析，由此判断 TD-ERCS 抵抗差分分析的能力.这种不针对具体加密算法，而只涉及混沌系统自身安全性的分析称为混沌系统的‘裸’状态分析，这种安全性分析方法更有利于分析和比较各种混沌系统的安全性，直接发现混沌系统自身存在安全漏洞，最终有利于混沌加密算法设计.

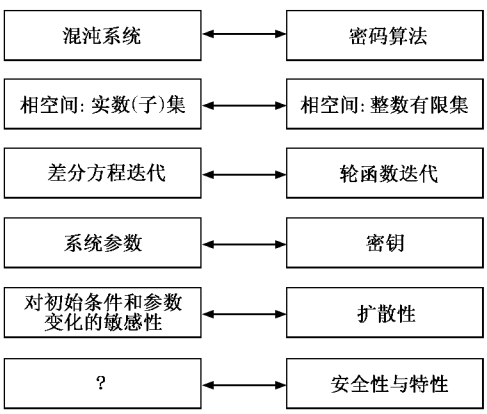

图 1　混沌系统与密码算法的对应关系

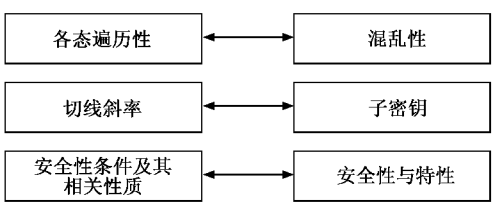

图 2　TD-ERCS 与密码算法的补充对应关系

4. 混沌系统的差分分析模型

差分分析是利用高概率特征通过分析明文对的差值对密文对的差值的影响来恢复某些密钥比特的方法，它的有效性前提条件是对应轮函数输出差分的输入差分存在高概率分布特征. Boesgaard[11] 推荐差模差分(subtraction modulus difference)和异或差分(XOR difference)为最好的差分定义，但它们仅适合整型数据环境.为了适应实型数据环境，可将差模差分推广为实型的距离差分.

定义 1　给定系统两个输入 $x_1, x_2 \in [0,1]$及对应输出 $y_1, y_2 \in [0,1]$，距离差分定义为

$$\Delta x = |x_1 - x_2| \text{ 和 } \Delta y = |y_1 - y_2|. \quad (11)$$

根据差分分析的基本原理,若对应输出差分 Δy 的输入差分 Δx 有一个高概率分布特征,则与此系统相关的密码算法在差分分析下就可能不安全.分别用随机变量 ξ 和 η 表示输入差分和输出差分,混沌系统差分分析的核心内容就是要测定条件分布 $P(\xi<\Delta x|\eta=\Delta y)$.对于混沌映射系统而言,由于对应给定输出的输入不是唯一的,故不能直接测出 $P(\xi<\Delta x|\eta=\Delta y)$,但如下定理提供了间接方法.

定理 设 ξ,η 为 $[0,1]$ 区间上的随机变量,且服从相同的概率分布,即概率密度 $p_\xi(x)=p_\eta(x)$,则 $P(\eta<x|\xi=y)=P(\xi<x|\eta=y)$,其中 $x,y\in[0,1]$.

证明 利用条件概率性质,有

$$\begin{aligned}
&P(\xi<x|\eta=y)\\
&=\int_0^x p_\xi(z|\eta=y)\mathrm{d}z\\
&=\int_0^x \frac{p(z\cap y)}{p_\eta(y)}\mathrm{d}z\\
&=\frac{1}{p_\eta(y)}\int_0^x p(z\cap y)\mathrm{d}z,\\
&P(\eta<x|\xi=y)\\
&=\int_0^x p_\eta(z|\xi=y)\mathrm{d}z\\
&=\int_0^x \frac{p(z\cap y)}{p_\xi(y)}\mathrm{d}z\\
&=\frac{1}{p_\xi(y)}\int_0^x p(z\cap y)\mathrm{d}z,
\end{aligned}$$

因有 $p_\xi(y)=p_\eta(y)$,定理得证.

该定理表明,在同一区间上服从同一分布的两个随机变量,互为条件的概率分布相同.对于混沌的迭代关系而言,它的一个输出同时又是下一次迭代的输入,故有理由认为迭代关系的输入差分 ξ 和输出差分 η 是一对性质完全相同的随机变量,故可以通过测试 $P(\eta<\Delta x|\xi=\Delta y)$ 求 $P(\xi<\Delta x|\eta=\Delta y)$.

对于混沌的迭代关系,输入差分 $\xi=\Delta x$ 和输出差分 $\eta=\Delta y$ 两者是相关的,输出差分将随迭代以指数规律增加,其相关性也将迅速减弱.为了表述这种规律,引入迭代差分分布的概念.

定义 2 设 ξ 和 η 分别为输入差分和输出差分的随机变量,给定输入差分 $\xi=\Delta x$,则经过 n 次迭代后的输出差分 η 的分布称为迭代 n 次差分分布,用 $P^n(\eta<\Delta y|\xi=\Delta x)$ 表示,简称迭代差分分布(iterative differential distribution,IDD).

迭代差分分布的变化从一个侧面可能反映了混沌系统的某种特质.

定义 3 若存在一个正整数 N,使得 $n\geqslant N$ 时,$P^n(\eta<\Delta y|\xi=\Delta x)=P(\eta<\Delta y)$,$n<N-1$ 时,$P^n(\eta<\Delta y|\xi=\Delta x)\neq P(\eta<\Delta y)$,则称 N 为混沌系统的差分失效指数(differential-invalid exponent, DIE),此时的概率分布记为 $P^N(\eta<\Delta y|\xi=\Delta x)$,即

$$P^N(\eta<\Delta y|\xi=\Delta x)=P(\eta<\Delta y). \quad (12)$$

差分失效指数的数理意义是,经过 N 次迭代,输入差分 ξ 与输出差分 η 成为相互独立的随机变量,在一定程度上反映了系统的混乱性强度.N 越小,系统的混乱性强度越高,系统抗差分分析的能力越强,因而是评估混沌系统安全性的一个重要指数,也可以作为评估混沌系统混乱度的一个可测的客观指数.

对给定的混沌系统,N 可能与初始条件、系统参数和输入差分等有关,其平均差分失效指数用 $\bar{N}$ 表示,是一个定值,有待进一步研究具体的计算方法和测定方法.

对于 TD-ERCS,由于具有稳定的均匀分布,易得其输入差分 ξ 或输出差分 η 的分布

$$P(\xi<x)=P(\eta<x)=2x-x^2, x\in[0,1], \quad (13)$$

对应概率密度为

$$p_\xi(x)=p_\eta(x)=2-2x, x\in[0,1]. \quad (14)$$

这样,针对 TD-ERCS 的差分分析的主要任务是研究差分失效指数 N,使得

$$\begin{aligned}
P^N(\eta<\Delta y|\xi=\Delta x)&=P(\eta<\Delta y)\\
&=2\Delta y-(\Delta y)^2, \quad (15)
\end{aligned}$$

或概率密度

$$p_\eta^N(\Delta y|\xi=\Delta x)=p_\eta^N(\Delta y)=2-2\Delta y, \quad (16)$$

并测定相应的 $\bar{N}$.

5. 测试及结果分析

将归一化相空间 Λ 均衡地分成 1000×1000 个方格,取每个方格的中心点为初始状态点开始迭代,共有 1000000 个样本点.给定系统参数 (μ,m) 和输入差分 Δx_0,经 n 次迭代后得输出差分 Δx_n,统计这 1000000 个 Δx_n 的分布,得概率密度曲线.根据切延迟定义,N 次迭代中至少应包含一次正常态的迭代,因此对于切延迟 m 的系统,有 $N\geqslant m$.测试和作图在 Matlab6.5 上完成,部分数据通过 SPSS 统计软件的 χ^2 检验.

表 1　部分参数点上 TD-ERCS 的差分失效指数

m	μ										$\frac{N-m+1}{N}$
	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1	
1	2/2	2/2	2/2	2/2	2/2	2/2	2/2	2/2	2/2	2/2	2/2
2	1/2*	1/2	1/2	1/2	1/2	1/2	1/2	1/2	1/2	1/2	1/2
3	1/3	1/3	1/3	1/3	1/3	1/3	1/3	1/3	1/3	1/3	1/3
4	1/4 *	1/4	1/4	1/4	1/4	1/4	1/4	1/4	1/4	1/4	1/4
5	1/5	1/5	1/5	1/5	1/5	1/5	1/5	1/5	1/5	1/5	1/5
6	1/6	1/6	1/6	1/6	1/6	1/6	1/6	1/6	1/6	1/6	1/6
7	1/7	1/7	1/7	1/7	1/7	1/7	1/7	1/7	1/7	1/7	1/7
8	1/8	1/8	1/8	1/8	1/8	1/8	1/8	1/8	1/8	1/8	1/8
9	1/9	1/9	1/9	1/9	1/9	1/9	1/9	1/9	1/9	1/9	1/9
10	1/10	1/10	1/10	1/10	1/10	1/10	1/10	1/10	1/10	1/10	1/10
						.....					

表 1 给出了 TD-ERCS 在部分参数点(μ, m)上获得的差分失效指数. 表中取 $\Delta x_0 = 10^{-8}$，分别测量不同参数(μ, m)下的 N，然后对 μ 求 N 的平均值(假定 μ 具有均匀分布). 表中分数意义为 $\frac{N-m+1}{N}$，其中分子表示正常态迭代次数. 由表中数据可知，当 $m = 1$ 时，$N = 2$，即系统只需迭代 2 次就使差分分析失效；当 $m \geqslant 1$ 时，均有 $N = m$，即正常态只需迭代 1 次就使差分分析失效，由于过渡态定义为 $m = 1$ 的状态，因此，在这些点上，无论切延迟 m 取值多大，实际的差分失效指数与 $m = 1$ 的差分失效指数相同(标有‘ * ’的数据是指系统在迭代次数 $n > m$ 时输出差分分布存在偏离(16)式的现象). 这一重要结论表明，在由表 1 所给定的系统参数范围内，TD-ERCS 的差分失效指数仅为 2，是理论上的最小值，与系统参数无关. 其结果显然远优于像 DES 这类分组加密算法. 由于 $N = 2$ 是理论上的最小值，故 TD-ERCS 是一种自动免疫差分分析的混沌系统.

对于 TD-ERCS，差分失效指数与系统参数的关系几乎只在 $\mu < 0.1$ 时才逐渐表现出来. 图 3 给出了一个代表性的实例，取 $m = 5$，$\Delta x_0 = 10^{-10}$ 及 $n = 5$，分别测定对应 $\mu = 0.05$，$\mu = 0.003$，$\mu = 0.001$ 的迭代差分分布. 实验表明，对应 $\mu = 0.05$ 的迭代差分分布已经与理论分布符合，也就是说，在 $\mu \geqslant 0.05$ 的参数范围内，TD-ERCS 是差分免疫的.

差分失效指数是一种具有普适意义的指数. 为了说明这一特征，测试了 Logistic 混沌系统的差分失效指数. Logistic 混沌系统取形式 $f = 1 - \mu x^2$，$-1 \leqslant x \leqslant 1$，当 $\mu = 2$ 时是混沌的，且 x 的分布与 TD-ERCS 的 x 分布相同，采用(9)式转化为归一化的均匀分布，与 TD-ERCS 混沌系统具有可比性. 在归一化初值空间[0,1]上均匀取 20000 个初值开始迭代，得 20000 个样本点，取输入差分 $\Delta x_0 = 10^{-10}$，对输出差分 Δx_n 统计，测得 $N = 55$. 实验表明，Logistic 混沌系统的差分失效指数存在，TD-ERCS 的抗差分分析能力远优于 Logistic 系统.

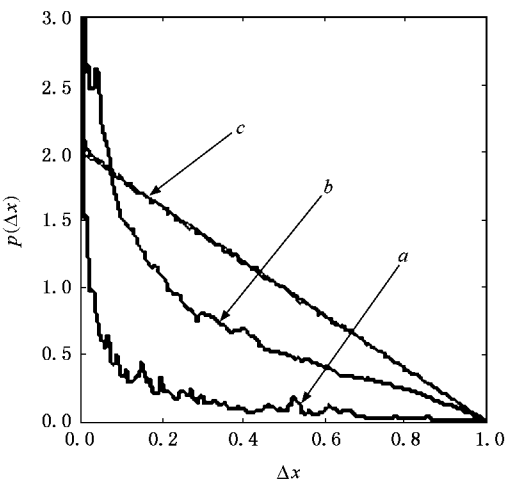

图 3　不同系统参数下 TD-ERCS 的迭代差分分布(曲线 a，$\mu = 0.001$；b，$\mu = 0.003$；c，$\mu = 0.05$)

差分失效指数与输入差分 Δx 的关系也是一个值得重点关注的性质. 测试了 TD-ERCS 和 Logistic 这两个混沌系统的 N 随输入差分 Δx 变化的特性，发现两系统的 N 均与 Δx 无关，其原因目前还不清楚.

迭代差分分布随迭代变化的趋势可用图 4 定性

说明.因 TD-ERCS 具有最小的差分失效指数,难找合适点说明这一特性,故用 Logistic 混沌系统为例.图中分别对应 $n=51$,$n=53$ 和 $n=55$ 的 3 条迭代差分分布曲线,具有随迭代逐渐逼近一个稳定分布曲线的趋势,逼近速度较缓.

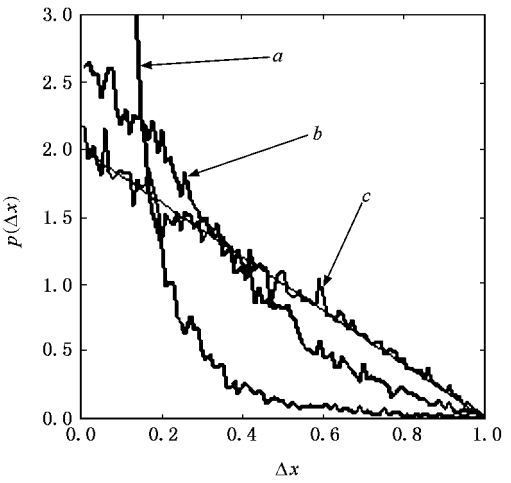

图 4 Logistic 迭代差分分布随迭代的变化(曲线 a,$n=51$;b,$n=53$;c,$n=55$)

6. 结 论

混沌系统是混沌数字加密算法的'核',研究混沌数字加密算法的安全性,首先必需研究混沌系统的安全性,只有确认混沌系统是安全的,才能保证构造的加密算法是安全的.

基于差分密码分析原理提出的混沌系统'裸'状态差分分析方法适合混沌的差分分析,通过测定差分失效指数评估混沌系统抗差分分析的能力,也能作为评估混沌系统混乱度的一个客观指数.

用'裸'状态差分分析方法分析 TD-ERCS 混沌系统的抗差分分析能力,发现 TD-ERCS 具有极强的抗差分分析能力,远优于分组密码算法,也远优于 Logistic 混沌系统,是一种能自动免疫差分分析的混沌系统,为构造安全的混沌数字加密算法提供了新的理论依据.

[1] Baptista M S 1998 *Phys. Lett.* A **240** 50

[2] Kocarev L, Jakimoski G 2001 *Phys. Lett.* A **289** 199

[3] Stojanoski T Kovarev L 2001 *IEEE Trans. CAS-I* **48** 281
Stojanoski T Kovarev L 2001 *IEEE Trans. CAS-I* **48** 382

[4] Palacios A, Juarez H 2002 *Phys. Lett.* A **303** 345

[5] Wang X M, Zhang J S, Zhang W F 2003 *Acta Phys. Sin.* **52** 2737 (in Chinese) [王小敏、张家树、张文芳 2003 物理学报 **52** 2737]

[6] Sheng L Y, Sun K H, Li C B 2004 *Acta Phys. Sin.* **53** 2871 (in Chinese) [盛利元、孙克辉、李传兵 2004 物理学报 **53** 2871]

[7] Biham E, Shamir A 1991 *Journal of Cryptology* **4** 3

[8] Kocarev L 2001 *IEEE Circuits and System Magazine* **1** 6

[9] Sheng L Y, Cao L L, Sun K H, Wen J 2005 *Acta Phys. Sin.* **54** 4031 (in Chinese) [盛利元、曹莉凌、孙克辉、闻 姜 2005 物理学报 **54** 4031]

[10] Alvarez G, Li S J 2006 http://www.hooklee.com/Papers/IJBC2006b.pdf

[11] Boesgaard M, Vesterager M, Christensen T, Zenner E 2005 http://th.informatik.uni-mannheim.de/people/zenner/pub/rabbit-skew.pdf

Differential cryptanalysis of TD-ERCS chaos *

Sheng Li-Yuan[1)†] Wen Jiang[1)] Cao Li-Ling[1)] Xiao Yan-Yu[2)]

1)(*School of Physics and Technology*, *Central South University*, *Changsha* 410083, *China*)

2)(*Mathematics and Metrics Economy College*, *Hunan University*, *Changsha* 410082, *China*)

(Received 7 April 2006; revised manuscript received 21 May 2006)

Abstract

Based on the fundamental principle of differential cryptanalysis and corresponding relation between the iteration of chaotic system and the round of block cipher, two important concepts, namely the iterative differential distribution (IDD) and the differential-invalid exponent (DIE) are proposed, which are used in evaluating chaotic system's power of conteracting the differential cryptanalysis. IDD is defined as the distribution of output differential vs. a given input differential at a varied iterative number, and DIE is defined as the minimal iterative number at which both output differential and input differential are independent of each other. By putting chaotic system into the "naked" state and directly analyzing the IDD, the DIE of chaotic system can be gotten. DIE is a universal, measurable and important characteristic exponent of chaos in studying security of chaos. The tests on both TD-ERCS and Logistic systems indicate that in the parameter region of 90%, DIE of DT-ERCS is equal to 2, which is the minimal DIE in theory. In comparison, DIE of Logistic chaotic system equals 55, hence TD-ERCS is a chaotic system with the power of active immunity to differential cryptanalysis.

Keywords: security of chaos, differential cryptanalysis, TD-ERCS, Logistic

PACC: 0545

* Project supported by the National Natural Science Foundation of China (Grant No. 60672041).

† E-mail: itpo@mail.csu.edu.cn