第 34 卷 第 8 期 计 算 机 工 程 2008 年 4 月
Vol.34 No.8 Computer Engineering April 2008
·博士论文· 文章编号：1000—3428(2008)08—0001—03 文献标识码：A 中图分类号：TP391

基于新复合混沌动力系统的加密算法

佟晓筠[1]，崔明根[2]，杨天龙[1]
(1. 哈尔滨工业大学计算机科学与技术学院，威海 264209；2. 哈尔滨工业大学理学院，威海 264209)

摘 要：提出两个新型混沌映射，并基于 Devaney 定义给出了严格混沌的理论特性证明。利用复合离散混沌系统的特性，提出基于两个新型混沌映射设计的复合离散混沌系统的序列密码算法，该映射产生的具有均匀分布函数量化后可生成具有平衡性质的 0-1 序列。 复合离散混沌系统均匀的不变分布还使密文具有很好的随机特性，由于迭代对初始条件的敏感性和迭代函数选择的随机性，密钥、明文与密文之间形成了复杂而敏感的非线性关系，而且密文和明文的相关度也很小，可以有效地防止密文对密钥和明文信息的泄露。分析表明，该系统具有很高的安全性并扩大了密钥空间。

关键词：混沌；复合非线性动力系统；加密算法

Encryption Algorithm Based on New Composite Chaos Dynamics System

TONG Xiao-jun[1], CUI Ming-gen[2], YANG Tian-long[1]
(1. School of Computer Science and Technology, Harbin Institute of Technology, Weihai 264209;
2. College of Sciences, Harbin Institute of Technology, Weihai 264209)

【Abstract】Chaos defined in general in quantitative characteristics is not a strict definition. In this paper two new chaos functions are proposed and theoretical proof about chaos is finished based on a strict Devaney definition. Using composite chaotic system character, a composite chaos sequences cipher algorithm is designed, the map of which has uniform distribution function, and can produce balance nature series to 0-1 after being quantified. The unchanged probability of composite chaos makes ciphertext have a good random. As the sensitivity to initial condition and random nature to iterative function choice, key and plaintext and ciphertext form complex and sensitive nonlinear relations, and the correlation is very small. The leaking of ciphertext to key and plaintext information can be effectively prevented. Experimental results show that the system has a very high safety and the key space is expanded.

【Key words】chaos; composite nonlinear dynamics system; encryption algorithm

1 概述

最近提出的一些基于离散混沌系统的加密[1]和随机数生成算法[2]，其安全性都不理想[3]。目前大部分混沌加密都采用自然的混沌系统，利用混沌定性化定义产生的混沌系统，它们不能提供具有密码学意义的保密性.。

实际上，在许多混沌密码学方法中已经发现了缺陷，例如MIT的Short利用非线性动力学预测方法破译了美国海军研究所提供的混沌掩盖加密方案[4]，另外，Wheeler也指出Matthews的混沌序列密码，由于具有严重的有限精度效应而不适于实际应用。

本文提出了基于复合离散混沌系统的序列密码体系，建立了一个具有均匀分布的密文的复杂非线性密码变换，通过对复合混沌系统迭代轨迹的选择将变换信息与明文完全融合在一起，从而减少了密文对信息的泄露。还使密文序列具有良好的分布特性，有利于抵御统计分析，保证密码系统具有很高的安全性。

2 新的离散混沌系统

2.1 混沌的定义

大部分研究都是基于 Li-Yorke 和 lyapunov 指数的混沌定义，但利用 lyapunov 定义研究混沌存在缺陷。本文从拓扑动力学角度研究对新混沌方程给出严格定义证明。

混沌(Devaney意义下)[5]：设V是一度量空间，X,Y是V上的任意开子集，一个连续映射$f:V\to V$，若满足下面 3 个条件，则称f在V上是混沌的：

(1)f 具有对初始条件的敏感依赖性。存在$\delta>0$，对任意的 $x\in V$ ，和 x 的任何邻域 N，存在 $y\in N$ 和自然数 $n>0$，有 $d(f^n(x)-f^n(y))>\delta$ 成立。

(2)f 具有拓扑传递性。即对任何一个开集 $X,Y\subset U$ ，存在 $k>0$，使得 $f^k(X)\cap Y\neq\Phi$ 。

(3)f的周期点集T在V中是稠密的。即存在 $x\in V$ ，$\forall\varepsilon>0$，都存在 $y\in T$ 使得不等式 $|y-x|<\varepsilon$ 成立。

2.2 两个特殊的离散混沌系统

首先在[-1,1]上构造两个特殊的非线性离散混沌动力系统，并对其性质进行分析，在[-1,1]上定义函数：

$$f_1(x)=4x^3-3x \quad (1)$$

$$f_2(x)=8x^4-8x^2+1 \quad (2)$$

基金项目：山东省自然科学基金资助重点项目(Z2006G01)
作者简介：佟晓筠(1963－)，女，副教授、博士研究生，主研方向：信息安全，混沌密码学；崔明根，教授、博士生导师；杨天龙，博士研究生
收稿日期：2007-04-25 **E-mail：**tong_xiaojun@163.com

2.2.1 $f_1(x)$ 和 $f_2(x)$ 是混沌迭代系统的证明

(1)证明 $g(\theta)=3\theta$ 是混沌的迭代系统。

1)证明 $g(\theta)=3\theta$ 的初始条件敏感性

θ 定义在 s^1 中。对任意 $\theta_1 \in s^1$，因为 $g^n(\theta_1)=3^n\theta_1$，$g^n(\theta_2)=3^n\theta_2$，设 $\delta=|\theta_1-\theta_2|$，对于 $|g^n(\theta_1)-g^n(\theta_2)|=|3^n(\theta_1-\theta_2)|>\delta$，所以 $g(\theta)$ 对初始条件敏感。

2)证明 $g(\theta)=3\theta$ 是拓扑传递的

因为 s^1 上任意小弧 U 可由 $gk(U)$ 最终扩展以覆盖整个 s^1，所以任意 ε 内包含的区间 $U,\ V\subset[0,2\pi]$，都有 $gk(U)\cap V\neq\varnothing$，$g(\theta)=3\theta$ 是拓扑传递的.

3)证明 $g(\theta)=3\theta$ 周期点在 V 中稠密。

因为 $g^n(\theta)=3^n\theta$，当 $3^n\theta=\theta+2k\pi$ 时，$g^n(\theta)=\theta$ 即 $\theta=\frac{2k\pi}{3^n-1}$，$k$ 为整数，$0\le k\le 3^n$

因为 $\lim\limits_{n\to\infty}\frac{2k\pi}{3^n-1}=0$，所以周期点有极限。对任意 $\varepsilon>0$，必存在整数 m,n 使 $|g^m(\theta)-g^n(\theta)|<\varepsilon$，令 $k=m-n$，$|gk(\theta)-\theta|<\varepsilon$，所以有 $|g2k(\theta)-gk(\theta)|<\varepsilon$，则 θ，$gk(\theta)$，$g2k(\theta),\cdots$ 把圆周等距离分割，则 $g(\theta)=3\theta$ 周期点在 V 中稠密。

根据 Devaney 混沌定义，即证 $g(\theta)=3\theta$ 是混沌的。

(2)下面利用拓扑共轭方法证明 $f_1(x)=4x^3-3x$ 在区间[-1, 1]上是混沌的。

设 $h_1(\theta)=\cos(\theta)$，$h_1:[0,\ 2\pi]\to[-1,1]$是满射，一对一的，且 $h_1(\theta)$ 连续，所以 h_1 是同胚映射。$h_1\circ g(\theta)=\cos(3\theta)=4\cos^3(\theta)-3\cos(\theta)$，$f_1\circ h_1(\theta)=4\cos^3(\theta)-3\cos(\theta)$，所以 $h_1\circ g=f_1\circ h_1$，g 与 f_1 是拓扑共轭的。

根据共轭性质，在 s^1 上开弧 $\hat{U}$ 和 $\hat{V}$，存在 k，使 $gk(\hat{U})\cap\hat{V}\neq\varnothing$，所以有 $f_1^k(\hat{U})\cap\hat{V}\neq\varnothing$，$f_1$ 是拓扑传递的。

$x\in I[-1,1]$ 上的任何邻域 U 升到 s^1 上的 $\hat{U}$ 上，存在 n 使 $g^n(\hat{U})$ 覆盖 s^1，所以 $f_1^n(U)$ 同样覆盖 I。因此存在 U 中的点，它离开 x 至少 $\delta=1$。证明了 $f_1(x)=4x^3-3x$ 是敏感的。g 的周期点稠密性蕴含在 $\hat{U}$ 中的周期点。该点在 U 中显然是 f_1 周期的。因此，证明了 $f_1(x)=4x^3-3x$ 是混沌的。

同理设 $g(\theta)=4\theta$，可证 $f_2(x)=8x^4-8x^2+1$ 是混沌的。

2.2.2 对应的不变分布密度函数

对于混沌方程 $f_1(x)=4x^3-3x$ 和 $f_2(x)=8x^4-8x^2+1$ 可以证明具有不变概率分布密度函数为 $\rho_f(x)=\frac{1}{\pi\sqrt{1-x^2}}$，$x\in[-1,1]$。可见上述两个混沌方程具有很好随机性，可以与序列密码很好的结合，用于加密。

2.3 相关函数和自相关函数

2.3.1 自相关函数证明

自相关函数的定义为 $r(\tau)=\int_{-1}^{1}xf^{\tau}(x)\rho(x)\mathrm{d}x-(\bar{x})^2$。

现假设，采用替换 $x=\cos u$ 之后，混沌方程 $f(x)=8x^4-8x^2+1$ 的迭代可以表示为 $f^n(x)=\cos(4^n u)$，它的自相关函数满足

$$r(\tau)=\begin{cases}0.5 & \tau=0\\ 0 & \tau\neq 0\end{cases} \tag{3}$$

证明 因为 $\rho(x)=\frac{1}{\pi\sqrt{1-x^2}}$，所以 $\bar{x}=\int_{-1}^{1}x\rho(x)\mathrm{d}x=\int_{-1}^{1}\frac{x}{\pi\sqrt{1-x^2}}\mathrm{d}x=0$。

(1)当 $\tau=0$ 时

$$r(0)=\int_{-1}^{1}xf^{0}(x)\rho(x)\mathrm{d}x-(\bar{x})^2=\int_{-1}^{1}x^2\rho(x)\mathrm{d}x-(\bar{x})^2\overset{x=\cos u}{=}$$
$$\int_{\pi}^{0}\cos^2 u\frac{-\sin u}{\pi\sqrt{1-\cos^2 u}}\mathrm{d}u=\frac{1}{\pi}\int_{0}^{\pi}\cos^2 u\mathrm{d}u=$$
$$\frac{1}{\pi}\int_{0}^{\pi}\frac{1+\cos(2u)}{2}\mathrm{d}u=0.5$$

(2)当 $\tau\neq 0$ 时

$$r(\tau)=\int_{-1}^{1}xf^{\tau}(x)\rho(x)\mathrm{d}x-(\bar{x})^2=\int_{-1}^{1}xf^{\tau}(x)\rho(x)\mathrm{d}x\overset{x=\cos u}{=}$$
$$\int_{\pi}^{0}\cos u\cos(4^{\tau}u)\frac{-\sin u}{\pi\sqrt{1-\cos^2 u}}\mathrm{d}u=$$
$$\frac{1}{2\pi}\left[\frac{\sin\left[(4^{\tau}+1)u\right]}{4^{\tau}+1}+\frac{\sin\left[(4^{\tau}-1)u\right]}{4^{\tau}-1}\right]\Bigg|_{0}^{\pi}=0$$

综上即证。用同样的变量替换方法，可证方程 $f(x)=4x^3-3x$ 的迭代表达式是 $f^n(x)\overset{x=\cos u}{=}\cos(3^n u)$。其自相关表达式与式(3)相同。

2.3.2 互相关函数证明

互相关函数的定义为

$$c(\tau)=\int_{-1}^{1}\int_{-1}^{1}x_1f^{\tau}(x_2)\rho(x_1)\rho(x_2)\mathrm{d}x_1\mathrm{d}x_2-(\bar{x})^2=0 \tag{4}$$

证明 因为 $\bar{x}=0$，所以

$$c(\tau)=\int_{-1}^{1}\int_{-1}^{1}x_1f^{\tau}(x_2)\rho(x_1)\rho(x_2)\mathrm{d}x_1\mathrm{d}x_2\overset{\substack{x_1=\cos u\\ x_2=\cos v}}{=}$$
$$\int_{\pi}^{0}\int_{\pi}^{0}\cos u\cos(4^{\tau}v)\frac{-\sin u}{\pi\sqrt{1-\cos^2 u}}\frac{-\sin v}{\pi\sqrt{1-\cos^2 v}}\mathrm{d}u\mathrm{d}v=$$
$$\frac{1}{\pi^2}\int_{0}^{\pi}\cos u\mathrm{d}u\int_{0}^{\pi}\cos(4^{\tau}v)\mathrm{d}v=\frac{1}{\pi^2}\sin u\Big|_{0}^{\pi}\frac{\sin(4^{\tau}v)}{4^{\tau}}\Bigg|_{0}^{\pi}=0$$

因此方程 $f(x)=8x^4-8x^2+1$ 的互相关函数为 0。用同样的变量替换方法，可证 $f(x)=4x^3-3x$ 的迭代表达式是 $f^n(x)\overset{x=\cos u}{=}\cos(3^n u)$。互相关表达式与式(4)相同。

3 复合混沌的伪随机序列发生器的设计与分析

3.1 复合混沌的伪随机序列发生器的设计

假定 $f_1(x_1)$，$f_2(x_2)$，$f_3(x_3)$ 是 3 个不同的一维混沌映射。$f_1(x)=4x^3-3x$，$f_2(x)=8x^4-8x^2+1$，$x_1(0)$，$x_2(0)$，$x_3(0)$是初始状态，$\{x_1(i)\}$，$\{x_2(i)\}$，$\{x_3(i)\}$是其混沌轨道。$f_3(x_3,p_3)$选取一维Logistic方程：$f_3(x_3)=1-2x_3^2$，$x_3\in[-1,1]$，其中，$f_3(x_3)$满足文献[3]的遍历性。

定义复合混沌伪随机序列发生器如下：

$$k(i)=\begin{cases}1 & f_3(x_q(i))>0\wedge f_3(x_q(i))<1\\ \text{no output} & f_3(x_q(i))=0,\ q=1,2\\ 0 & f_3(x_q(i))>-1\wedge f_3(x_q(i))<0\end{cases} \tag{5}$$

3.2 复合混沌系统伪随机序列的性能分析与测试

(1)平衡性是指序列中 0 和 1 的个数应该大致相等。

定理 如果$f_3(x_3)$满足以下 4 条性质，则有 $P\{k(i)=0\}=P\{k(i)=1\}$，即$\{k(i)\}$在{0, 1}具有平衡性。

1)均是定义在 $I=[a,\ b]$上的满射；

2)均在 $I=[a,\ b]$上各态历经（遍历性）；

3)$\{x_3(i)\}$ 当$i\to\infty$时渐进独立；

4)非线性迭代系统$x_3(i+1)=f_3(x_3(i))$具有唯一的不变分布密度函数$\rho(x)$性质。

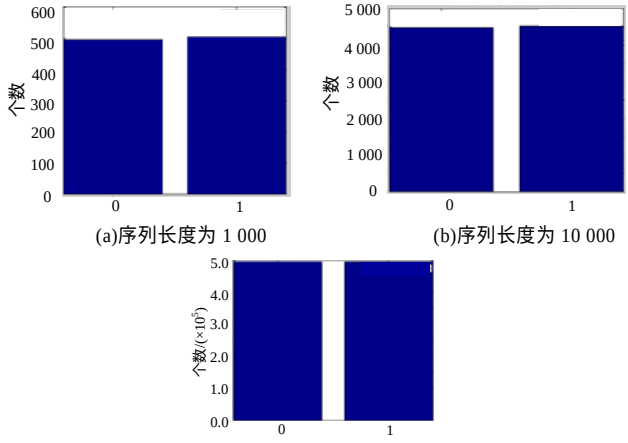
证明 因为$f_3(x_3, p_3)$在$I=[a, b]$上各态历经(遍历性)，且$\{x_3(i)\}$当$i\to\infty$时渐进独立，当$i\to\infty$时有：

$$P\{x_1 > x_2\} = \int_a^b \int_a^x \rho(x)\rho(y)\,\mathrm{d}y\,\mathrm{d}x \tag{6}$$

$$P\{x_1 < x_2\} = \int_a^b \int_a^x \rho(y)\rho(x)\,\mathrm{d}y\,\mathrm{d}x \tag{7}$$

故有 $P\{x_1 > x_2\} = P\{x_1 < x_2\}$，即 $P\{k(i)=0\} = P\{k(i)=1\}$。

对该方案生成序列长度分别为 1 000, 10 000 和 100 000 进行实验，结果如图 1 所示。实验表明，0 和 1 的个数平衡，因此产生的混沌序列满足平衡性。

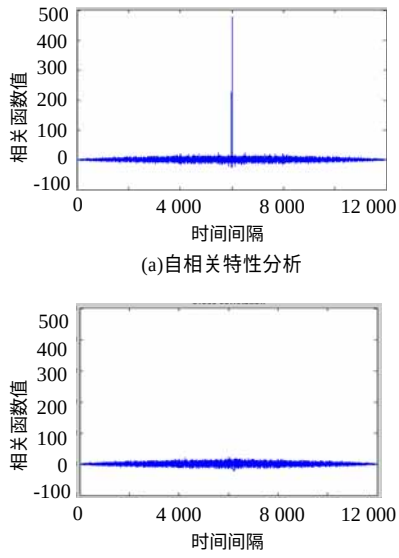


(a)序列长度为 1 000　　(b)序列长度为 10 000

(c)序列长度为 100 000

图 1　各序列长度均匀性分析

(2)自相关和互相关分析。对混沌序列作了自相关和互相关分析，如图 2 所示。由图 2 可知，混沌序列表现出良好的随机特性，自相关函数近似于理想冲击函数$\delta(x)$，具有微小差异初值的混沌系统在多次迭代之后所产生的混沌序列具有近似为 0 的互相关性。所以该序列用来加密具有很强的抗攻击、抗破译能力。



(a)自相关特性分析

(b)互相关特性分析

图 2　自相关与互相关函数分析

4　实验结果

$f_1(x_1)$和$f_2(x_2)$选取设计的新的混沌方程，$f_3(x_3)$选取Logistic映射，假设$\{P_n\}$是明文信息序列；$\{K_n\}$是密钥信息序列，由复合方程迭代产生后进行处理后所得；$\{C_n\}$是密文信息序列。

加密算法设计为

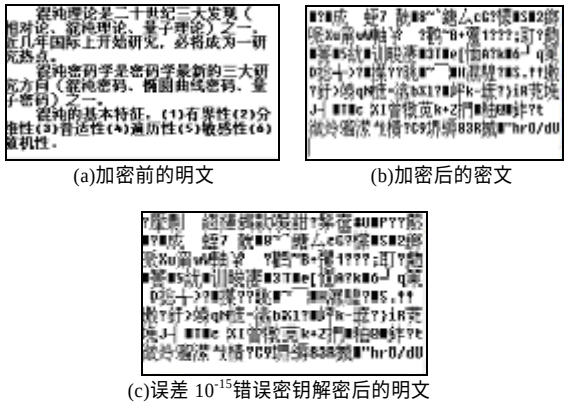
$$\{C_n\}=\{P_n\}\oplus\{K_n\} \tag{8}$$

解密算法设计为

$$\{P_n\}=\{C_n\}\oplus\{K_n\} \tag{9}$$

选取初始密钥x_0=0.234，利用流密码对文本进行加密实验。

(1)对文本文件加密解密。文本文件加密解密结果如图 3 所示，由于混沌系统具有对初始条件的敏感依赖性，因此改变$x_0=0.234\times10^{-15}$，错误密钥解密后如图 3(c)所示。



(a)加密前的明文　　(b)加密后的密文

(c)误差 10^{-15}错误密钥解密后的明文

图 3　文本文件加密解密结果

(2)复合混沌系统流密码的安全性分析。多混沌系统流密码具有更高的安全性。当采用双精度的浮点运算实现时，$x_1(0)$, $x_2(0)$各有 63 bit有效位(因为$x_1(0)$和$x_2(0)$都必须为正数，其符号位恒为 0)，所以穷举攻击的复杂度至少为 2^{126}。这样的复杂度能满足大多数的应用。采用伪随机数发生器产生的二进制序列去掩盖明文，减少了密文和单个混沌轨道之间的关联，增加了相关分析的难度。

5　结束语

本文设计了复合多混沌系统的伪随机数发生器，经过理论和实验的结果证明，该伪随机数发生器产生的随机序列具有良好的密码学性能，产生的密钥序列具有串分布均匀、随机统计特性良好、相邻密钥相关性小、周期长、线性复杂度高、混淆扩散性好等特点，是一个非常理想的伪随机数发生器。实验结果证明，该密码系统的工作密钥空间足够大，足以抵抗穷举密钥攻击、差分分析及统计分析等，安全性高，并且代价低。

参考文献

[1] Kotulski Z, Szczepaski J. Application of Discrete Chaotic Dynamical Systems in Cryptography——DCC Method[J]. International Journal of Bifurcation and Chaos, 1999, 9(6): 1121-1135.

[2] Stojanovski T. Chaos-based Random Number Generators[J]. IEEE Transactions on Circuits System-1: Fundamental Theory and Applications, 2001, 48(3): 281-288.

[3] Jakimoski G, Kocarev L. Chaos and Cryptography: Block Encryption Ciphers Based on Chaotic Maps[J]. IEEE Transactions on Circuits System-1: Fundamental Theory and Applications, 2001, 48(2): 163-169.

[4] Short K M. Stept Toward Unmakring Secture Communications[J]. Int'l J. Bifurcation & Chaos, 1994, 4(4): 959-977.

[5] 卢　侃. 混沌动力学[M]. 上海: 上海翻译出版公司, 1990.