第 34 卷 第 23 期 计 算 机 工 程 2008 年 12 月
Vol.34 No.23 Computer Engineering December 2008
·安全技术· 文章编号：1000—3428(2008)23—0173—03 文献标识码：A 中图分类号：TP301

基于混沌反控制的流密码算法设计

李昌刚[1]，张 昕[2]
(1. 浙江万里学院电子信息学院，宁波 315100；2. 浙江万里学院基础学院，宁波 315100)

摘 要：应用混沌反控制思想产生超混沌，根据超混沌系统的伪随机特性进行流密码设计。通过对离散线性时不变系统施加非线性状态反馈控制构造一个超混沌发生系统。证明了反馈增益矩阵的存在性，给出选择增益矩阵及系数矩阵元素的约束关系，在此基础上设计基于三维超混沌系统的流密码算法。仿真结果表明该算法具有良好的统计特性。

关键词：混沌反控制；超混沌系统；流密码；阈值处理

Design of Stream Cipher Algorithm Based on Chaos Anti-control

LI Chang-gang[1], ZHANG Xin[2]
(1. Faculty of Electronic & Information, Zhejiang Wanli University, Ningbo 315100;
2. Junior College, Zhejiang Wanli University, Ningbo 315100)

【Abstract】This paper uses chaos anti-control idea to generate a hyper-chaotic system, and uses the pseudo-random feature of hyper-chaotic system to design a stream cipher. The nonlinear state feedback is added to a Discrete Linear Time Invariant(DLTI) system and the hyper-chaotic system is constructed. The existence of feedback gain matrix is proved and the constraint condition between and coefficient matrix is given. A stream cipher algorithm based on a 3D hyper-chaotic system is designed. Simulation results indicate that the stream cipher has favorable statistic characteristics.

【Key words】 chaos anti-control; hyper-chaotic system; stream cipher; threshold handling

1 概述

混沌现象是非线性动态系统中出现的确定性的伪随机过程。混沌系统的非周期性、整体上稳定而在局部上具有的扩张性，以及对初始条件及系统参数异常敏感的特性都显示了混沌系统具有优良的随机性特征。近年来，一些学者尝试采用混沌系统作为伪随机序列发生器，进而应用于流密码的设计中[1]。

混沌反控制思想是由文献[2]提出的，它不像传统应用中设法消除系统中存在的混沌现象，而是有意识地产生混沌。研究表明[3]，超混沌系统由于系统的吸引子在相平面多个方向上扩散、压缩及折叠，因此比混沌系统更加复杂，其输出更难以预测，也就更适合密码学方面的应用。

2 超混沌系统的产生

先考虑三阶离散线性时不变(Digital Luminance Transient Improvement, DLTI)系统[3]：

$$\boldsymbol{x}(n+1)=\boldsymbol{A}\boldsymbol{x}(n)+\boldsymbol{B}\boldsymbol{u}(n) \tag{1}$$

其中，状态变量 $\boldsymbol{x}\in\Re^3$；$\boldsymbol{A}=\begin{bmatrix}a_{11}&0&0\\0&a_{22}&a_{23}\\0&a_{32}&a_{33}\end{bmatrix}$ 是实系数矩阵，并假定其稳定，其谱半径 $\rho(\boldsymbol{A})=\max\limits_{1\le i\le 3}|\lambda_i(\boldsymbol{A})|<1$；系数矩阵 $\boldsymbol{B}=\begin{bmatrix}0&0\\1&0\\0&1\end{bmatrix}$。为了使系统(式(1))是超混沌的，设计了输入函数 $\boldsymbol{u}(n)$，它是系统状态 $\boldsymbol{x}(n)$ 的分段线性函数，即

$$\boldsymbol{u}(n)=\begin{bmatrix}f(\boldsymbol{K}\boldsymbol{x}(n))\\f(\boldsymbol{K}\boldsymbol{x}(n))\end{bmatrix}$$

其中，$\boldsymbol{K}=\begin{bmatrix}0&k_1&k_2\\0&k_3&k_4\end{bmatrix}\in\Re^{2\times 3}$；$f(\cdot)$ 为分段线性可微函数 $f:\Re\to\Re$，其定义如下：

$$f(y)=(-1)^{m+1}(y-2m) \tag{2}$$

其中，$2m-1\le y\le 2m+1$，$m=0,\pm1,\pm2,\cdots$。

由式(1)、式(2)得式(1)的 Jacobian 为

$$\boldsymbol{J}=\frac{\partial\boldsymbol{x}(n+1)}{\partial\boldsymbol{x}(n)}=\frac{\partial}{\partial\boldsymbol{x}(n)}(\boldsymbol{A}\boldsymbol{x}(n)+\boldsymbol{B}\boldsymbol{u}(n))=$$
$$\frac{\partial}{\partial\boldsymbol{x}(n)}(\boldsymbol{A}\boldsymbol{x}(n)+\boldsymbol{B}f(\boldsymbol{K}\boldsymbol{x}(n)))=\boldsymbol{A}+\boldsymbol{B}\frac{\partial f(\boldsymbol{K}\boldsymbol{x}(n)}{\partial\boldsymbol{x}(n)}\boldsymbol{K}= \tag{3}$$
$$\begin{cases}\boldsymbol{A}+\boldsymbol{B}\boldsymbol{K} & \boldsymbol{K}\boldsymbol{x}(n)\in(4n+2,4n+4]\\ \boldsymbol{A}-\boldsymbol{B}\boldsymbol{K} & \boldsymbol{K}\boldsymbol{x}(n)\in(4n,4n+2]\end{cases}$$

其中，$n=0,\pm1,\pm2,\cdots$。

令 $\boldsymbol{P}_n=(\boldsymbol{A}+\boldsymbol{B}\boldsymbol{K})^{n_1}(\boldsymbol{A}-\boldsymbol{B}\boldsymbol{K})^{n_2}$，其中，$n_1+n_2=n$。如果矩阵 $\boldsymbol{A}+\boldsymbol{B}\boldsymbol{K}$ 有 2 个特征值 α_1，α_2 (另一特征值为 a_{11})，且 $\alpha_1\ne\alpha_2$；矩阵 $\boldsymbol{A}-\boldsymbol{B}\boldsymbol{K}$ 有 2 个特征值 β_1，β_2 (另一特征值也为 a_{11})，且 $\beta_1\ne\beta_2$；$\alpha_1,\alpha_2,\beta_1,\beta_2$ 全都位于单位圆之外，矩阵 $\boldsymbol{A}+\boldsymbol{B}\boldsymbol{K}$ 与 $\boldsymbol{A}-\boldsymbol{B}\boldsymbol{K}$ 是可交换的，即

$$(\boldsymbol{A}+\boldsymbol{B}\boldsymbol{K})(\boldsymbol{A}-\boldsymbol{B}\boldsymbol{K})=(\boldsymbol{A}-\boldsymbol{B}\boldsymbol{K})(\boldsymbol{A}+\boldsymbol{B}\boldsymbol{K})$$

或 $\boldsymbol{A}\boldsymbol{B}\boldsymbol{K}=\boldsymbol{B}\boldsymbol{K}\boldsymbol{A}$，那么矩阵 $\boldsymbol{A}+\boldsymbol{B}\boldsymbol{K}$ 与 $\boldsymbol{A}-\boldsymbol{B}\boldsymbol{K}$ 有相同的特征向量系。此时式(1)的 2 个 Lyapunov 指数可以表示为

$$\lambda_{1,2}=\lim_{n\to\infty}\frac{1}{n}\ln|\det\left(\boldsymbol{T}\begin{bmatrix}\alpha_1&0\\0&\alpha_2\end{bmatrix}^{n_1}\boldsymbol{T}^{-1}\boldsymbol{T}\begin{bmatrix}\beta_1&0\\0&\beta_2\end{bmatrix}^{n_2}\boldsymbol{T}^{-1}\right)| \tag{4}$$

其中，矩阵 $\boldsymbol{T}$ 即由矩阵 $\boldsymbol{A}+\boldsymbol{B}\boldsymbol{K}$ 与 $\boldsymbol{A}-\boldsymbol{B}\boldsymbol{K}$ 的公共特征向量所组成的可逆矩阵，那么

基金项目：国家自然科学基金资助项目(60464001)
作者简介：李昌刚(1972－)，男，副教授、博士，主研方向：混沌动力学系统与控制，密码技术，汽车电子技术；张 昕，讲师、硕士
收稿日期：2008-01-20 **E-mail：**lcg_allan@163.com

$$\lambda_1=\lim_{n\to\infty}\frac{n_1}{n}\ln|\alpha_1|+\lim_{n\to\infty}\frac{n_2}{n}\ln|\beta_1|$$

$$\lambda_2=\lim_{n\to\infty}\frac{n_1}{n}\ln|\alpha_2|+\lim_{n\to\infty}\frac{n_2}{n}\ln|\beta_2|$$

若 n_1, n_2 与 n 同阶，则有 $\lambda_1>0$, $\lambda_2>0$，此时式(1)是超混沌的。

为了满足条件 $\boldsymbol{ABK}=\boldsymbol{BKA}$，这 2 个矩阵的元素必须对应相等。因为

$$\boldsymbol{ABK}=\begin{bmatrix}0 & 0 & 0\\ 0 & k_1a_{22}+k_3a_{23} & k_2a_{22}+k_4a_{23}\\ 0 & k_1a_{32}+k_3a_{33} & k_2a_{32}+k_4a_{33}\end{bmatrix}$$

$$\boldsymbol{BKA}=\begin{bmatrix}0 & 0 & 0\\ 0 & k_1a_{22}+k_2a_{32} & k_1a_{23}+k_2a_{33}\\ 0 & k_3a_{22}+k_4a_{32} & k_3a_{23}+k_4a_{33}\end{bmatrix}$$

所以要求

$$\begin{cases}k_1a_{22}+k_3a_{23}=k_1a_{22}+k_2a_{32}\\ k_2a_{22}+k_4a_{23}=k_1a_{23}+k_2a_{33}\\ k_1a_{32}+k_3a_{33}=k_3a_{22}+k_4a_{32}\\ k_2a_{32}+k_4a_{33}=k_3a_{23}+k_4a_{33}\end{cases}$$

成立。解该式得

$$\begin{aligned}&a_{23}=a_{32}\\ &k_2=k_3\\ &k_4=\frac{1}{a_{23}}(k_1a_{23}+k_2a_{33}-k_2a_{22})\\ &a_{23}\neq 0\end{aligned}\tag{5}$$

因此，只要矩阵元素的选择满足式(5)，就一定存在 $\boldsymbol{ABK}=\boldsymbol{BKA}$，并且此时系统是超混沌的。

对于各矩阵元素的选择可先由圆盘定理估计出范围再进行选择，具体估计如下：

由于矩阵 $\boldsymbol{A}$ 是稳定的，因此有 $|a_{11}|<1$，且 $a_{11}\in\Re$。而

$$|\alpha-a_{22}|\le|a_{23}|$$

$$|\alpha-a_{33}|\le|a_{23}|$$

则有

$$\min\{a_{22},a_{33}\}-|a_{23}|\le\alpha\le\max\{a_{22},a_{33}\}+|a_{23}|$$

因此，当

$$\max\{a_{22},a_{33}\}+|a_{23}|<1$$

$$\min\{a_{22},a_{33}\}-|a_{23}|>-1$$

时，$|\alpha|<1$ 成立。

同理，

$$|\beta-(a_{22}+k_1)|\le|a_{23}+k_2|$$

$$|\beta-(a_{33}+k_1+\frac{a_{33}-a_{22}}{a_{23}}k_2)|\le|a_{23}+k_2|$$

则有

$$\max\{(a_{22}+k_1)+|a_{23}+k_2|,(a_{33}+k_1+\frac{a_{33}-a_{22}}{a_{23}}k_2)+|a_{23}+k_2|\}<-1$$

或者

$$\min\{(a_{22}+k_1)-|a_{23}+k_2|,(a_{33}+k_1+\frac{a_{33}-a_{22}}{a_{23}}k_2)-|a_{23}+k_2|\}>1$$

时，有 2 个 $|\beta_i|>1$，$i=1,2$ 成立。

$$|\gamma-(a_{22}-k_1)|\le|a_{23}-k_2|$$

$$|\gamma-(a_{33}+k_1+\frac{a_{33}-a_{22}}{a_{23}}k_2)|\le|a_{23}-k_2|$$

则当

$$\max\{(a_{22}-k_1)+|a_{23}-k_2|,(a_{33}-k_1-\frac{a_{33}-a_{22}}{a_{23}}k_2)+|a_{23}-k_2|\}<-1$$

或者

$$\min\{(a_{22}-k_1)-|a_{23}-k_2|,(a_{33}-k_1-\frac{a_{33}-a_{22}}{a_{23}}k_2)-|a_{23}-k_2|\}>1$$

时，有 2 个 $|\gamma_i|>1$, $i=1,2$ 成立。

因此，参数选择时应参考以上各式的条件，例如，选择参数矩阵：

$$\boldsymbol{A}_1=\begin{bmatrix}0.6 & 0 & 0\\ 0 & 0.5 & 0.1\\ 0 & 0.1 & 0.8\end{bmatrix}$$

$$\boldsymbol{B}=\begin{bmatrix}0 & 0\\ 1 & 0\\ 0 & 1\end{bmatrix}$$

$$\boldsymbol{K}_1=\begin{bmatrix}0 & -2 & 1.2\\ 0 & 1.2 & 1.6\end{bmatrix}$$

$$\boldsymbol{A}_2=\begin{bmatrix}-0.5 & 0 & 0\\ 0 & 0.4 & 0.1\\ 0 & 0.1 & 0.7\end{bmatrix}$$

$$\boldsymbol{K}_2=\begin{bmatrix}0 & -3 & 1.5\\ 0 & 1.5 & 1.5\end{bmatrix}$$

计算矩阵 $\boldsymbol{A}_1$ ($\boldsymbol{A}_2$)的特征值分别为 0.6, 0.469 7, 0.830 3 (-0.5, 0.369 7, 0.730 3)；矩阵 $\boldsymbol{A}_1+\boldsymbol{BK}_1$ ($\boldsymbol{A}_2+\boldsymbol{BK}_2$)的特征值分别为 0.6, -1.893 6, 2.793 6(-0.5, -3.084 4, 2.684 4)；矩阵 $\boldsymbol{A}_1-\boldsymbol{BK}_1$ ($\boldsymbol{A}_2-\boldsymbol{BK}_2$)的特征值分别为 0.6, 2.833 1, -1.133 1 (-0.5, 3.823 9, -1.223 9)；即矩阵 $\boldsymbol{A}_1$ ($\boldsymbol{A}_2$)是稳定的，而矩阵 $\boldsymbol{A}_1+\boldsymbol{BK}_1$ ($\boldsymbol{A}_2+\boldsymbol{BK}_2$)及 $\boldsymbol{A}_1-\boldsymbol{BK}_1$ ($\boldsymbol{A}_2-\boldsymbol{BK}_2$)分别有 2 个特征值在单位圆之外，且满足 $\boldsymbol{A}_1+\boldsymbol{BK}_1$ ($\boldsymbol{A}_2+\boldsymbol{BK}_2$)与 $\boldsymbol{A}_1-\boldsymbol{BK}_1$ ($\boldsymbol{A}_2-\boldsymbol{BK}_2$)可交换的条件，因此，系统

$$\boldsymbol{x}(n+1)=\boldsymbol{A}_1\boldsymbol{x}(n)+\boldsymbol{B}\boldsymbol{u}_1(n)\ (\ \boldsymbol{x}(n+1)=\boldsymbol{A}_2\boldsymbol{x}(n)+\boldsymbol{B}\boldsymbol{u}_2(n)\ )$$

是超混沌的。

3 流密码算法设计

考虑 2 个类似于式(1)的超混沌系统：

(1) $\boldsymbol{x}(n+1)=\boldsymbol{A}_1\boldsymbol{x}(n)+\boldsymbol{B}\boldsymbol{u}_1(n)$

(2) $\boldsymbol{y}(n+1)=\boldsymbol{A}_2\boldsymbol{y}(n)+\boldsymbol{B}\boldsymbol{u}_2(n)$

且 $\boldsymbol{A}_1$, $\boldsymbol{A}_2$, $\boldsymbol{B}$, $\boldsymbol{K}_1=\begin{bmatrix}0 & k_{11} & k_{12}\\ 0 & k_{13} & k_{14}\end{bmatrix}$, $\boldsymbol{K}_2=\begin{bmatrix}0 & k_{21} & k_{22}\\ 0 & k_{23} & k_{24}\end{bmatrix}$(注：这些参数值可作为密钥使用)的参数选择同第 2 节的例子。其中，

$$\boldsymbol{u}_1(n)=\begin{bmatrix}f(k_{11}x_2(n)+k_{12}x_3(n))\\ f(k_{13}x_2(n)+k_{14}x_3(n))\end{bmatrix}$$

$$\boldsymbol{u}_2(n)=\begin{bmatrix}f(k_{21}x_2(n)+k_{22}x_3(n))\\ f(k_{23}x_2(n)+k_{24}x_3(n))\end{bmatrix}$$

则流密码序列的产生如图 1 所示，其中，Σ 为求和运算符；Z^{-1} 为单位延时算子；$cipher_i$, $i=1,2,3,4$ 为系统输出的流密码序列；σ 为阈值函数，其定义为

$$\sigma(x)=\begin{cases}0 & x\le c\\ 1 & x>c\end{cases}$$

阈值 c 的选择使得概率 $P\{x\le c\}=P\{x>c\}=0.5$。根据状态 $\boldsymbol{x}(n)$ ($\boldsymbol{y}(n)$)的混沌特性以及 $f(\boldsymbol{K}_1\boldsymbol{x}(n))$ ($f(\boldsymbol{K}_1\boldsymbol{y}(n))$)的分段线性及对称性，当迭代次数足够大时，$f(\boldsymbol{K}_1\boldsymbol{x}(n))$ ($f(\boldsymbol{K}_1\boldsymbol{y}(n))$)遍历 $[-1,+1]$ 区间上的所有点。因此，当迭代次数很大时，选

择阈值 $c=0$。

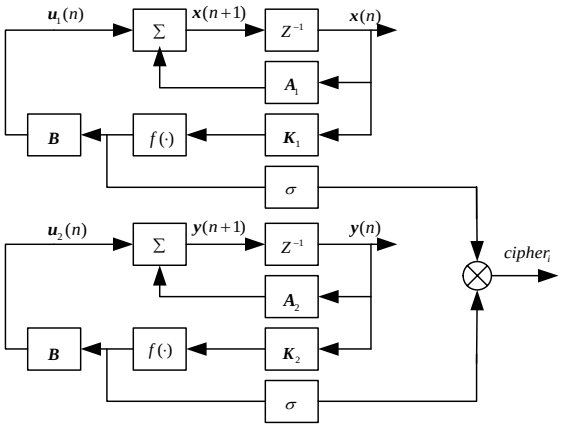

图 1　流密码发生序列设计框图

4　系统分析及数值仿真

下面以系统(1)、系统(2)为例进行数值仿真，矩阵参数的选择同第 3 节。随机抽取 $f_i(x)$, $i=1,2,3,4$ 的输出，仿真结果如图 2、图 3 所示。

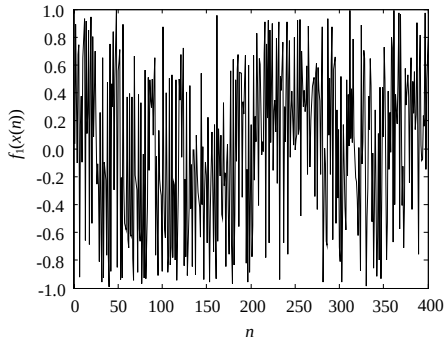

图 2　$f_1(x)$的输出序列

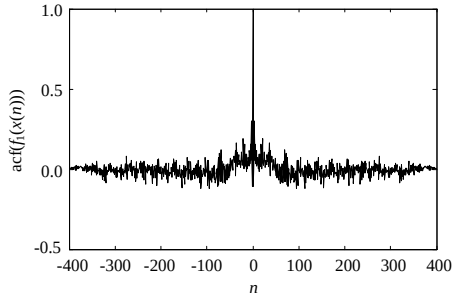

图 3　$f_1(x)$的自相关函数

图 2 表示 $f_1(x)=f(k_{11}x_2(n)+k_{12}x_3(n))$ 的输出，即系统

$$\boldsymbol{x}(n+1)=\boldsymbol{A}_1\boldsymbol{x}(n)+\boldsymbol{B}\boldsymbol{u}_1(n)$$

的状态输出经过函数 $f(\cdot)$ 映射后的一个输出，迭代初值选为：$x_1(0)=0.1$，$x_2(0)=0.2$，$x_3(0)=0.3$；可见，$f_1(x)$ 的输出是不规则的伪随机序列，自相关函数如图 3 所示，近似于白噪声信号的自相关函数，具有良好的随机特性。

图 4 给出了

$$f_2(x)=f(k_{13}x_2(n)+k_{14}x_3(n))$$

与

$$f_3(x)=f(k_{21}y_2(n)+k_{22}y_3(n))$$

之间的互相关函数。迭代初值选取：$y_1(0)=0.2$，$y_2(0)=0.3$，$y_3(0)=0.4$。可见，函数 $f_2(x)$ 与 $f_3(x)$ 之间的互相关很小，这表明由 $f_2(x)$ 不能有效地预测 $f_3(x)$，反之亦然。

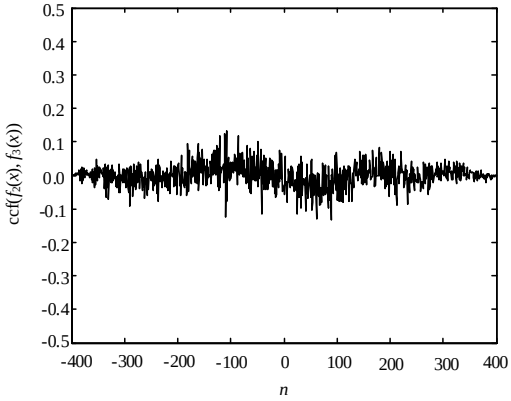

图 4　$f_2(x)$与$f_3(x)$之间的互相关函数

现有的流密码产生方法主要有：线性反馈移位寄存器法，线性同余法，二次同余法，三次同余法，密码编码法，非线性反馈移位寄存器法等。其中，同余法已经被成功破译[4]；密码编码法实现速度较慢[5]；NLFSR法还没有可靠的数学理论基础。与现有的流密码产生方法相比，本文的伪随机序列发生器类似于一次一密系统[6]。因为发送方可随机配置矩阵$\boldsymbol{A}$及矩阵$\boldsymbol{K}$，也可以任意地选择每个系统的迭代初值，且在实数域范围内进行，所以保证了系统输出不同的流密码序列。(注：矩阵$\boldsymbol{A}$及$\boldsymbol{K}$的元素值以及系统的迭代初值均可作为密钥使用)。整个系统由 2 个结构相似的子系统组成，每个子系统的分段线性反馈函数的输出经阈值化后再经XOR操作，相当于 2 个超混沌系统之间的相互扰动，增加了预测的困难性。

5　结束语

本文构造了一个离散超混沌系统。通过在特殊的线性时不变系统加入分段线性状态反馈，使得所形成的闭环系统为超混沌系统，并将各子系统的分段线性函数的输出经阈值化后再进行异或操作而产生的 0-1 序列作为流密码序列。系统最大可同时输出 4 路流密码序列。这种流密码应用超混沌序列之间的相互扰动，更利于密码应用，仿真结果表明系统具有良好的抗预测攻击及统计特性。

参考文献

[1] Lee Weibin, Chen Tungher. A Public Verifiable Copy Protection Technique for Still Images[J]. Journal of System and Software, 2002, 62(3): 195-204.

[2] Wang Xiaofan, Chen Guanrong. On Feedback Anticontrol of Discrete-time Chaos[J]. International Journal of Bifurcation and Chaos, 1999, 9(7): 1435-1441.

[3] Wang Xiaofen, Chen Guanrong. Chaotifying A Stable LTI System by Tiny Feedback Control[J]. IEEE Trans. on Circuits System, 2000, 47(3): 410-415.

[4] Reeds J A. Solution of Challenge Cipher[J]. Cryptologia, 1979, 3(2): 83-95.

[5] American Bankers Association. ANSI X9.17-1985 American National Standard for Financial Institution Key Management (Wholesale)[S]. 1985.

[6] Schneier B. 应用密码学——协议、算法与 C 源程序[M]. 2 版. 吴世忠, 祝世雄, 张文政, 等, 译. 北京: 机械工业出版社, 1996.