文章编号：1000-8608(2012)05-0730-06

一种基于复合混沌动力系统的序列密码算法

王丽燕[1]， 李永华[1]， 贾思齐[2]， 刚家泰*[1]

（1.大连大学 信息工程学院，辽宁 大连 116622；
2.大连理工大学 软件学院，辽宁 大连 116620）

摘要： 基于二维Logistic映射和分段线性混沌映射，提出了一种新的序列密码算法.该算法用二维Logistic映射的输出作为分段线性映射的分段参数P.再用带有参数P的分段线性混沌映射构造加密算法.对算法进行了仿真实验和安全性分析，并对由二维Logistic映射和分段线性混沌映射产生的序列的随机性、初值敏感性等性质进行了研究.安全性分析表明，该算法加密效果良好，密钥、明文与密文之间关系均十分敏感，而且密文和明文的相关度也很小，可以有效地抵御统计分析，防止密文对密钥和明文信息的泄露.

关键词： Logistic混沌映射；分段线性混沌映射；复合混沌动力系统；序列密码
中图分类号： TN918 **文献标志码：** A

0 引 言

随着网络技术的发展和信息交换的日益频繁，信息安全技术的研究变得越来越重要，作为新的密码技术，混沌密码技术已引起国内外学者浓厚的兴趣和广泛的研究.混沌作为一种特有的非线性现象，具有良好的伪随机特性、轨道的不可预测性、对初始状态及结构参数的极端敏感性等一系列优良特性，这些特性都与密码学中的混乱和扩散相吻合.

混沌密码作为一类新型的密码技术，在数据加密、图像加密和电子商务安全等领域得到了广泛研究[1-4].周红等提出了一种基于分段线性映射产生具有均匀不变密度和自相关函数呈δ形态的动力系统，并利用多次迭代混沌映射来获得非线性前馈型流密码[5,6].为了进一步提高安全性，桑涛等将用于加密的分段线性动力系统改进为“逐段二次方根”混沌映射，设计反馈序列密码[7].王相生等用一个特殊的混沌动力系统，通过随机改变混沌映射的参数来提高混沌的复杂性，并以此代替密钥生成器，产生密钥流[8,9].尽管已经提出了许多混沌加密方法，但有些加密方法已受到质疑并已形成攻击方案.比如，Short破译了美国海军研究所提供的混沌掩盖加密方法[10].Wheeler等在文献[11]中说明文献[1]中给出的混沌序列密码由于存在严重的有限精度效应问题而不适于实际应用.金晨辉等在文献[12]中指出了文献[5,7]中密码算法的弱点，并给出了相应的优化分割攻击方案.文献[13,14]都进一步指出了用单一的混沌动力系统进行迭代的加密算法的弱点，并给出了相应的攻击方案.为了解决用单一混沌系统实现的密码算法不够安全的问题，许多学者提出了各种加密方案，李红达等提出了基于复合离散混沌动力系统的序列密码算法，算法以迭代初始点作为密钥，以粗粒化的迭代轨迹作为密文[15,16]，用传统加密和混沌加密级联[17]、高维混沌系统或多混沌系统[18]实现密码算法等.本文则将二维Logistic映射和分段线性混沌映射复合，用二维Logistic映射的输出作为分段线性混沌映射的分段参数P，再用带有参数P的分段线性混沌映射构造加密算法，给出加密和解密算法，并进行仿真实验和安全性分析.

1 混沌动力系统

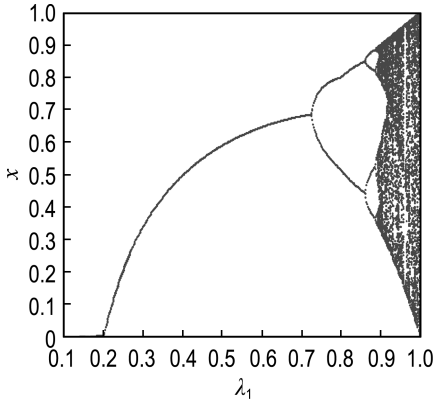
1.1 二维Logistic映射

二维Logistic映射定义为

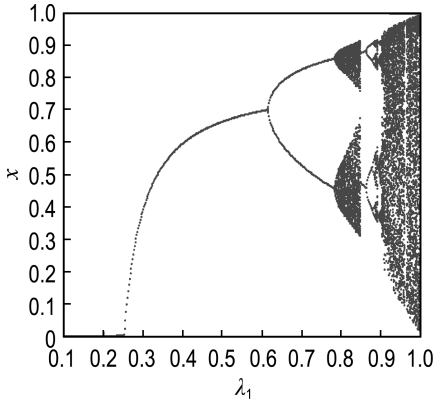
收稿日期： 2011-08-13； **修回日期：** 2012-07-03.
基金项目： 国家自然科学基金资助项目(71072161).
作者简介： 王丽燕(1963-)，女，大连理工大学2004届博士，教授；刚家泰*(1960-)，男，副教授，E-mail：gjt1960@126.com.

$$\begin{cases} x_{n+1} = u\lambda_1 x_n(1-x_n)+\lambda y_n \\ y_{n+1} = u\lambda_2 y_n(1-y_n)+\lambda x_n \end{cases} \quad (1)$$

其中 u、λ_1、λ_2、λ 为控制参数，通常取 $u=4$. 二维 Logistic 映射的行为是非常复杂的[19]，图 1 给出了两组不同控制参数情形下的分岔图.



(a) $\lambda_2=1-\lambda_1$，$\lambda=0.3$



(b) $\lambda_2=\lambda_1$，$\lambda=1-\lambda_1$

图 1　二维 Logistic 映射分岔图

Fig. 1　Branch chart of 2-D Logistic mapping

当 $\lambda_1=0.8$，$\lambda_2=0.2$，$\lambda=0.3$ 时，利用奇异值分解求其 Lyapunov 指数，求得其中一个 Lyapunov 指数为 0.044 8>0，说明这时系统处于混沌状态.

1.2　一维分段线性混沌映射

一维分段线性混沌映射定义为

$$X(t+1)=F_P(X(t))=\begin{cases} \dfrac{X(t)}{P};\ 0\leqslant X(t)<P \\ \dfrac{X(t)-P}{0.5-P};\ P\leqslant X(t)<0.5 \\ \dfrac{1-X(t)-P}{0.5-P};\ 0.5\leqslant X(t)<1-P \\ \dfrac{1-X(t)}{P};\ 1-P\leqslant X(t)\leqslant 1 \end{cases} \quad (2)$$

其中 $X\in[0,1]$，$P\in(0,0.5)$. 当 $P=0.247$ 时，该一维分段线性混沌映射的图像如图 2 所示.

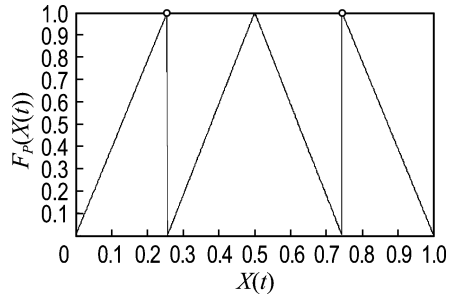


图 2　分段线性混沌映射

Fig. 2　Piecewise linear chaotic map

根据文献[20]，该迭代系统是混沌的，其输出序列$\{X(t)\}$在[0,1]上遍历，具有良好的自相关性且呈 δ 形态. 由 Frobenius-Perron 算子[21] 有

$$\begin{aligned} P_r(f^*(x)) = {} & Pf^*(xP)+(0.5-P)f^*(P+ \\ & x(0.5-P))+(0.5-P)\times \\ & f^*(0.5+(1-x)(0.5-P))+ \\ & Pf^*(1-xP) \end{aligned}$$

易得 $P_r(1)=1$，说明系统的不变分布密度函数为 $f^*(x)=1$. 从而系统在[0,1]上是均匀分布的.

2　加密方案

加密方案如图 3 所示.

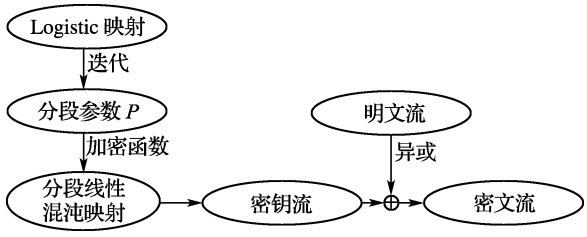


图 3　加密算法框图

Fig. 3　Encryption algorithm block diagram

设明文长度为 h，对二维 Logistic 映射：$\begin{cases} x_{n+1} = u\lambda_1 x_n(1-x_n)+\lambda y_n \\ y_{n+1} = u\lambda_2 y_n(1-y_n)+\lambda x_n \end{cases}$，选取 $u=4$，$\lambda=0.3$，$\lambda_1=0.8$，$\lambda_2=0.2$，给定初始值$(x_0 \quad y_0)$，迭代得 $y_i\in[0,1](i=1,2,\cdots,2h)$，由于分段线性混沌映射的参数 $P\in(0,0.5)$，可简单地取 $P_i=y_i/2$，且 $P_i\in(0,0.05)$. 显然，P_i 为一个混沌序列. 具体的加密和解密算法如下.

步骤 1 将明文由十进制转换为十六位二进制，如果明文是文字，将明文字符的 ASCII 码转化为十六位二进制. 得到二进制明文序列$\{a_1, a_2, \cdots, a_h\}$($a_i$ 只能取 0 或者 1，$i = 1,2,\cdots,h$).

步骤 2 选取 Logistic 映射的初始值$(x_0 \quad y_0)$，迭代得 $y_i \in [0,1]$($i = 1,2,\cdots,2h$)，并将 $P_i = y_i/2$($P_i \in (0,0.05)$)代入分段线性混沌映射(2)进行迭代得到混沌序列$\{x_i\}$($i = 1,2,\cdots,2h$).

步骤 3 由离散化算子 $T_j(x_i) = [10^j x_{i+h}] \bmod 2$ 计算得到 $k_i = T_j(x_{i+h})$，$i = 1,2,\cdots,h$. 其中$(x_0 \quad y_0)$和 j 均为密钥.

步骤 4 得到的二进制序列$\{k_1, k_2, \cdots, k_h\}$与明文二进制序列$\{a_1, a_2, \cdots, a_h\}$进行异或运算就得到加密二进制序列.

解密算法与加密算法类似，先进行步骤 2 和 3，然后和二进制密文序列作异或运算就可以把密文还原成明文，得到解密的效果.

3 算法仿真

为了更明确说明加密算法运算过程，对加密算法进行性能分析，下面给出一个例子，对一段文字进行加密.

例 1 明文：混沌密码学原理及其应用

首先将明文字符转换成 ASCII 码，然后转化为十六位二进制，其明文序列的二进制序列表示为

101110111110110011100011111001111100001111011100110000101110101111010001101001111101010010101101110000000111011011011110010110000011000110111001001101001110100110111010011110000011

对于二维 Logistic 映射有

①若取$(x_0 \quad y_0)$=(0.432 323 0 0.452 680 0)，j=8，得到对应的密文为

壘 廕鋻 〈潾 & ；

②若取$(x_0 \quad y_0) = (0.432\ 323\ 0 + 10^{-16}\ 0.452\ 680\ 0)$，$j$=8，得到的密文为

兗 S⊙ㄣT 鸆↟@諵谾 舋 ~ ；

③若取$(x_0 \quad y_0) = (0.432\ 323\ 0 + 2 \times 10^{-16}\ 0.452\ 680\ 0)$，$j$=8，得到的密文为

垚*e 箏鈡礴 b 涼铊 ；

④若取$(x_0 \quad y_0) = (0.324\ 252\ 7 + 10^{-16}\ 0.452\ 680\ 0)$，$j$=8，得到的密文为

J} 刀→ ㄙ捯 5¶{親；

⑤若取$(x_0 \quad y_0) = (0.324\ 252\ 7 - 10^{-16}\ 0.452\ 680\ 0)$，$j$=8，得到的密文为

h ⊦字 XI钭拣郧歜 c!!；

⑥若取$(x_0 \quad y_0)$ = (0. 324 252 7 0.452 680 0)，j=7，得到的密文为

n⊥⊦ 孳 l i t.

用 0、1 序列的图形化表示如图 4 所示，k 为 0 与 1 出现次数的比值. 从仿真结果来看，初始值的微小变化将会引起密文的巨大变化.

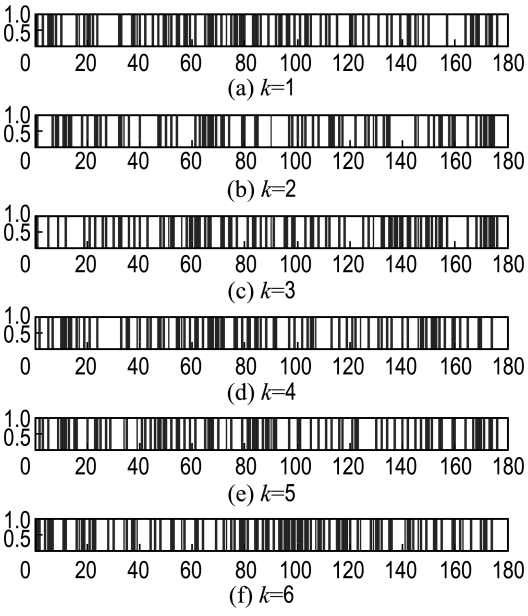


图 4 不同初始值的密文

Fig. 4 Ciphers under different initial values

例 2 对文本“混沌一词从字面上理解就是杂乱无章，混乱无序之意，但是由于混沌系统的奇异性和复杂性到目前为止尚未被人们彻底了解，因此至今混沌还没有给出一个比较统一的定义”，用密钥$(x_0 \quad y_0)$=(0.432 323 0 0.452 680 0)，j=8，进行加密得到密文：

“鐿 →C_⊦趍枨樻 U|)M 祫蟠Φ 熩

q0 啢佃投鴻藐薧{6 蜇)┻┐ 詣+0w 剄

n 傖 ┌2 冀 b(:↕?J>b$傯 U 欈 p*聊詨}

哈$ 唬→唊┻I✲靇#睃伤劗 g x=k┼至

g禗 Pr 婝 b←r 皍”.

用正确的密钥可以精确地恢复得到明文. 但若改变密钥，比如将密钥变成 $(x_0\quad y_0)=(0.4323230+10^{-16}\quad 0.4526800)$，$j=8$，则解密得到：

“n6L 攷 g 坲　混 c　祁钚惇 CK　]　’
交☼W 調 T 韙鵹 8 磨玐杕 5←疋&*　f
鍊¶婁弘檻 3¶赸智 AU　岐泐→盗 H=’V 巳
鬏緒纅 i0 骗:　隶　wkg 晟騱/劅　蚫 1
瀐=乛　4•3 梶郥 p 厦|”.

由此可见密钥的微小变化导致不能得到正确的明文，说明密钥与密文之间关系十分敏感.

4　安全性分析

4.1　敏感性分析

取明文为 10^5 位全为 0 的二进制序列，取密钥 $(x_0\quad y_0)=(0.4323230\quad 0.4526800)$，$j=8$，加密得到密文为 C. 试验表明，当初始值 x_0 变为 $x_0=0.4323230+10^{-16}$ 和 $x_0=0.4323230+2\times10^{-16}$，而 y_0 与 j 不变时，新生成的密文和原密文 C 相比，分别有 50.05% 和 50.02% 位发生了变化.

如果选取一系列全为 0 的二进制序列为明文，其长度 L 由 1 位增加到 10 000 位，选取 10 个不同初始值 $x_0=0.4323230+10^{-16}i$ $(i=0,1,\cdots,9)$，y_0 与 j 不变，得到改变的比特位数 (b_c) 与长度 L 的关系如图 5 所示. 图 6 是 $j=2,4,6,8,10$，$(x_0\quad y_0)=(0.4323230\quad 0.4526800)$ 时得到改变的比特位数与长度 L 的关系图. 可以看出初始值发生微小变化，都会使变化后的密文与原密文相比有接近 50% 的比特位数发生变化. 这就说明密钥与密文具有很强的敏感性.

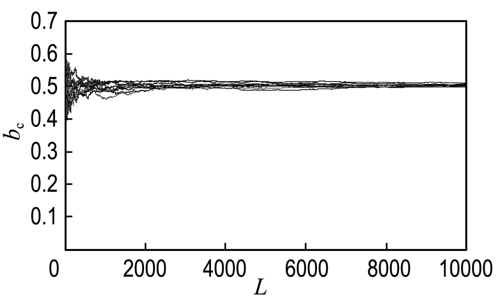


图 5　不同初始值条件下比特位数变化比

Fig. 5　The changed bit ratio under different initial values

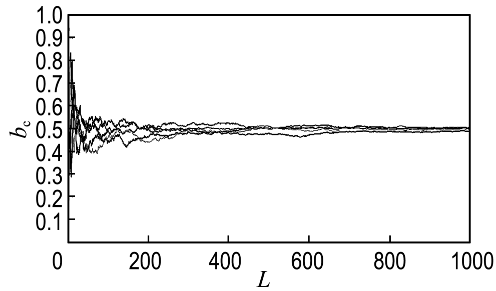


图 6　不同密钥条件下比特位数变化比

Fig. 6　The changed bit ratio under different key

4.2　统计性分析

取一系列全为 0 的二进制序列为明文，其长度 L 由 1 位增加到 10 000 位，取密钥 $(x_0\quad y_0)=(0.4323230\quad 0.4526800)$，$j=8$，生成的密文中 1 的位数与长度 L 之比 p 如图 7 所示.

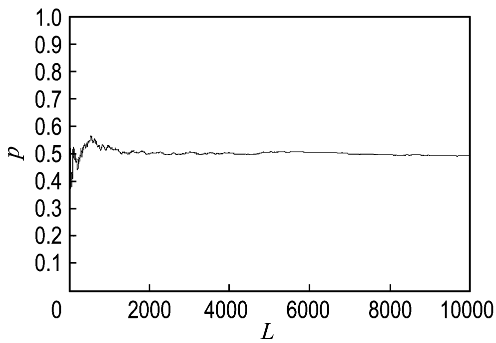


图 7　改变的比特位数与长度 L 之比

Fig. 7　The ratio of changed bit number to the length L

由图 7 可以看出，在加密时明文序列的每个比特位数都以 0.5 的概率发生改变或保持不变，也就是说，与明文相比，密文序列中大约有一半的比特位数发生改变，这使密文与明文的相关度很小，而且随着长度的增加还趋于 0. 同时还可以保证生成的密文序列中 0 与 1 的个数几乎相等，这说明本算法产生均匀分布的密文，可以有效抵抗统计攻击.

4.3　密钥空间分析

在本文中选择的密钥是二维 Logistic 映射和分段线性混沌映射的迭代初始值 x_0 和 y_0 以及离散化算子参数 j，且二维 Logistic 映射的参数 λ、λ_1、λ_2、u 也是可以随机选取的，所以同样可以选取作为密钥. 仅以计算精度为 10^{-4} 估算本算法的密钥空间，密钥空间就大于 10^{30}. 实际上，目前计算

机系统的计算精度远大于 10^{-4}，这样相应的密钥空间会更大.因此本文算法拥有足够大的密钥空间，可以抵抗穷举攻击.

5 结 论

本文利用二维 Logistic 映射与分段线性映射的参数空间和相空间较大的特点，以及混沌序列的遍历性与复杂性，用二维 Logistic 映射的输出作为分段线性映射的分段参数 P，分段线性映射的输出与明文异或后得到密文.本算法克服了单一迭代型混沌密码的参数和初态的低位比特对前若干输出信号的影响不大的信息漏洞，使整个加密过程十分复杂，提高了密文的不可预测性，可以抵御分辨率攻击法和分割攻击法.计算机模拟实验结果表明，本算法产生均匀分布的密文，密钥与密文具有很强的敏感性，密钥空间很大且明文与密文的相关度很小，提高了抗已知明文/密文攻击的能力，可以有效地抵御统计分析，是一个良好的加密算法.

参考文献：

[1] Matthewn H. On the derivation of a 'chaotic' encryption algorithm [J]. **Cryptologia**, 1989, **13**(1): 29-42.

[2] Mitchell D W. Nonliner key generators [J]. **Cryptologia**, 1990, **14**(4):350-354.

[3] Feldmann U, Hasler M, Schwarz W. Communication by chaotic signals: the inverse system approach [J]. **International Journal of Circuit Theory and Applications**, 1996, **24**(5):551-579.

[4] Frey D R. Chaotic digital encoding: an approach to secure communication [J]. **IEEE Transactions on Circuits and Systems II**, 1993, **40**(10):660-666.

[5] 周 红，罗 杰，凌燮亭. 混沌非线性反馈密码序列的理论设计和有限精度实现[J]. 电子学报，1997，**25**(10):57-60.
ZHOU Hong, LUO Jie, LING Xie-ting. Generating nonlinear feedback stream ciphers via chaotic systems [J]. **Acta Electronica Sinica**, 1997, **25**(10):57-60. (in Chinese)

[6] 周 红，俞 军，凌燮亭. 混沌前馈型流密码的设计[J]. 电子学报，1998，**26**(1):98-101.
ZHOU Hong, YU Jun, LING Xie-ting. Design of chaotic feed forward stream cipher [J]. **Acta Electronica Sinica**, 1998, **26**(1):98-101. (in Chinese)

[7] 桑 涛，王汝笠，严义埙. 一类新型混沌反馈密码序列的理论设计[J]. 电子学报，1997，**27**(7):47-50.
SANG Tao, WANG Ru-li, YAN Yi-xun. The theoretical design for a class of new chaotic feedback stream ciphers [J]. **Acta Electronica Sinica**, 1997, **27**(7):47-50. (in Chinese)

[8] 王相生，王小港，甘骏人. 基于可变参数混沌的序列密码的设计[J]. 计算机工程，2001，**27**(9):103-104.
WANG Xiang-sheng, WANG Xiao-gang, GAN Jun-ren. A chaotic sequence encryption method [J]. **Computer Engineering**, 2001, **27**(9): 103-104. (in Chinese)

[9] 王相生，甘骏人. 一种基于混沌的序列密码生成方法[J]. 计算机学报，2002，**25**(4):351-356.
WANG Xiang-sheng, GAN Jun-ren. A chaotic sequence encryption method [J]. **Chinese Journal of Computers**, 2002, **25**(4):351-356. (in Chinese)

[10] Short K M. Steps toward unmasking secure communications [J]. **International Journal of Bifurcation and Chaos**, 1994, **4**(4):959-977.

[11] Wheeler D D, Matthews R A J. Supercomputer investigations of a chaotic encryption algorithm [J]. **Cryptologia**, 1991, **15**(2):140-152.

[12] 金晨辉，高海英. 对两个基于混沌的序列密码算法的分析[J]. 电子学报，2004，**32**(7):1066-1070.
JIN Chen-hui, GAO Hai-ying. Analysis of two stream ciphers based on chaos [J]. **Acta Electronica Sinica**, 2004, **32**(7):1066-1070. (in Chinese)

[13] 张 斌，金晨辉. 对迭代型混沌密码的逆推压缩攻击[J]. 电子学报，2010，**38**(1):129-140.
ZHANG Bin, JIN Chen-hui. Inversion and compression attacks to iterative chaotic ciphers [J]. **Acta Electronica Sinica**, 2010, **38**(1):129-140. (in Chinese)

[14] 汪海明，李 明，金晨辉. 对 XW 混沌密码算法的分割攻击[J]. 计算机应用研究，2010，**27**(7):2625-2628.
WANG Hai-ming, LI Ming, JIN Chen-hui. Divide-and-conquer attack on XW chaotic cipher [J]. **Application Research of Computers**, 2010, **27**(7):

2625-2628. (in Chinese)

[15] 李红达,冯登国. 复合离散混沌动力系统与序列密码体系[J]. 电子学报, 2003, **31**(8):1209-1212.
LI Hong-da, FENG Deng-guo. Composite nonlinear discrete chaotic dynamical systems and stream cipher systems [J]. **Acta Electronica Sinica**, 2003, **31**(8): 1209-1212. (in Chinese)

[16] 李红达,冯登国. 基于复合离散混沌动力系统的序列密码算法 [J]. 软件学报, 2003, **14**(5):991-998.
LI Hong-da, FENG Deng-guo. Stream cipher algorithms based on composite nonlinear discrete chaotic dynamical systems [J]. **Journal of Software**, 2003, **14**(5):991-998. (in Chinese)

[17] 丘水生,陈艳峰,吴　敏, 等. 一种新的混沌加密系统方案原理[J]. 电路与系统学报, 2006, **11**(1):98-103.
QIU Shui-sheng, CHEN Yan-feng, WU Min, *et al*. A novel scheme of chaotic encryption system [J]. **Journal of Circuits and Systems**, 2006, **11**(1): 98-103. (in Chinese)

[18] 刘金梅,丘水生,向　菲,等. 基于多混沌映射的信息加密算法[J]. 华南理工大学学报(自然科学版), 2007, **35**(5): 1-5.
LIU Jin-mei, QIU Shui-sheng, XIANG Fei, *et al*. Information encryption algorithm based on multiple chaotic mappings [J]. **Journal of South China University of Technology (Natural Science Edition)**, 2007, **35**(5): 1-5. (in Chinese)

[19] 刘尚懿,王丽君. 一种基于二维 Logistic 映射的图像加密算法[J]. 鞍山科技大学学报, 2006, **29**(4): 365-370.
LIU Shang-yi, WANG Li-jun. Image encryption algorithm based on Coupled Logistic chaotic map [J]. **Journal of Anshan University of Science and Technology**, 2006, **29**(4):365-370.

[20] XIAO Di, LIAO Xiao-feng, DENG Shao-jiang. One-way hash function construction based on the chaotic map with changeable-parameter [J]. **Chaos, Solitons & Fractals**, 2005, **24**(1):65-71.

[21] Lasota A, Mackey M. **Probabilistic Properties of Deterministic Systems** [M]. Cambridge: Cambridge University Press, 1985:32-76.

A stream cipher algorithm based on composite chaotic dynamical systems

WANG Li-yan[1], LI Yong-hua[1], JIA Si-qi[2], GANG Jia-tai[*1]

(1. College of Information Engineering, Dalian University, Dalian 116622, China;
2. School of Software Technology, Dalian University of Technology, Dalian 116620, China)

Abstract: A new stream cipher algorithm is designed based on 2-D Logistic map and piecewise linear chaotic map, which uses the output of 2-D Logistic map as the piecewise parameter P of piecewise linear chaotic map. The encryption algorithm is constructed by piecewise linear chaotic map with P. The simulation experiments and security analyses are conducted for this algorithm, and the random properties and the sensitivity to initial value of stream generated by these two maps are studied. The analytical results of security indicate that this algorithm is effective in encryption, the key, plaintext and cipher text form complex and sensitive nonlinear relations, and the correlation between plaintext and cipher text is very small, which makes the algorithm effectively defend statistic analysis. The leaking of key and plaintext information from cipher text can also be effectively prevented.

Key words: Logistic chaotic map; piecewise linear chaotic map; composite chaotic dynamical system; stream cipher