参数可变的多混沌映射加密系统

钟黔川[1,2]，朱清新[1]，张平莉[2]

(1. 电子科技大学计算机科学与工程学院 成都 610054; 2. 西昌学院 四川 西昌 615013)

【摘要】利用混沌映射具有对初值和系统参数的敏感性以及轨道的不确定性，提出一种基于多个一维混沌映射的加密算法。该加密算法使用线性同余随机数发生器产生混沌映射的系统参数和3个一维混沌映射的使用顺序，同时通过输出反馈方式动态改变混沌映射初值、迭代次数以及线性同余随机数发生器参数。实验结果和安全性分析表明，该算法密钥空间大，具有对明文和密钥的敏感性，能有效抵抗选择明文等穷举攻击和统计分析攻击。

关 键 词 分组密码; 混沌加密系统; 混沌映射; 输出反馈

中图分类号 TP309 **文献标识码** A doi: 10. 3969/j. issn. 1001-0548. 2009. 02. 28

Multiple Chaotic Maps Encryption System

ZHONG Qian-chuan[1,2], ZHU Qing-xin[1], and ZHANG Ping-li[2]

(1. School of Computer Science and Engineering, University of Electronic Science and Technology of China Chengdu 610054;
2. Xichang College Xichang Sichuan 615013)

Abstract A new cryptosystem based on multiple one-dimensional chaotic maps is proposed by utilizing the properties of chaotic map such as sensitivity to initial conditions and system parameters, and orbit uncertainty. The system parameters of chaotic maps and the using order of three one-dimensional maps are generated by using linear congruent generators. The initial value and iterative number of chaotic map and linear congruence generator (LCG) parameters are dynamically changed by output feedback. Simulation results and security analyses show that the proposed cryptosystem has large key space and high sensitivity to key and plaintext, and can resist the brute attack and statistical attack.

Key words block cipher; chaotic encryption system; chaotic map; output feedback

在过去的许多年里，文献[1-4]提出了一些基于一维混沌映射的加密系统，也有一些混沌加密系统被成功攻击[6-10]，它的安全性已成为专家学者关注的一个热点。由于混沌映射具有对初值和系统参数的敏感性以及轨道的不确定性，这些特性和分组密码的特点是相吻合的。混沌密码系统一般使用混沌映射的初值、系统参数、迭代次数作为密钥进行加密/解密，本文算法试图使混沌映射每一步迭代都最大限度地保证上述3个参数的最大取值空间，并且利用输出反馈来动态改变这些参数，有力地保障了算法的安全性。

1 混沌加密算法

算法的描述：

(1) 在算法中，128位的密钥被分成多个8 bit为单位的块，每块称作会话密钥，进一步将密钥划分成32 bit为单位的子密钥 $K_{\mu i}, i=1,2,\text{L},4$ 和64 bit为单位的子密钥 $K_i, i=1,2$，它们都是以十六进制来表示的，其划分情况为：

$$K = k_1 k_2 k_3 k_4 \text{L}\ k_{16} = K_{\mu 1} K_{\mu 2} K_{\mu 3} K_{\mu 4} = K_1 K_2 \quad (1)$$

(2) 在加密/解密过程中明文/密文被分成多个8 bit为单位的块，其划分情况分别为：

$$P = P_1 P_2 P_3 P_4 \text{L}\ P_n \quad (2)$$

$$C = C_1 C_2 C_3 C_4 \text{L}\ C_n \quad (3)$$

(3) 在加密/解密过程中选取3个一维混沌映射来进行加密/解密，它们分别是：Logistic映射、帐篷映射、正弦映射，如表1所示。表中第1列为混沌映射名称，第2列是3个混沌映射的编号，第3列是3个混沌映射对应的迭代表达式，第4列是混沌映射系统参数取值范围，该范围表示相应混沌映射处于混沌状态。

(4) 开始时由会话密钥和子密钥构造的初始值分别为：

$$X_b = |(K_1 + K_2)/2^{52} \bmod 1| \quad (4)$$

收稿日期：2007 – 12 – 05；修回日期：2008 – 06 – 25
基金项目：国家自然科学基金(60671033)；国家教育部博士点基金(2006061405)
作者简介：钟黔川(1970 –)，男，博士，主要从事信息安全、混沌密码、数字水印技术等方面的研究.

$$N_b=(k_1k_2+k_3k_4+k_5k_6+k_7k_8+k_9k_{10}+k_{11}k_{12}+k_{13}k_{14}+k_{15}k_{16})\bmod 2^{16} \quad (5)$$

随机数由线性同余随机数发生器(LCG)产生：

$$Y_i=(K_{\mu3}Y_{i-1}+K_{\mu4})\bmod(2^{31}-1) \quad (6)$$

式中　$Y_0=\lfloor X_b\times 2^{31}\rfloor$。由$Y_i$产生的混沌映射号$M$、使用会话密钥的顺序号$j$分别为：

$$M=Y_i \bmod 3 \quad (7)$$

$$j=(Y_i \bmod 16)+1 \quad (8)$$

表1　混沌映射编号、表达式、系统参数取值范围

混沌映射	M	迭代表达式	系统参数
Logistic映射	0	$X_{n+1}=\mu X_n(1-X_n)$	3.57≤μ≤4.0
Tent映射	1	$X_{n+1}=\begin{cases}\mu X_n & X_n\leqslant 0.5\\ \mu(1-X_n) & X_n>0.5\end{cases}$	1.4≤μ≤2.0
Sine映射	2	$X_{n+1}=\mu\sin(X_n)$	0.87≤μ≤1.0

(5) 混沌映射的迭代次数N和初值X分别为：

$$N=N_b+k_i \quad (9)$$

$$X=(X_b+(k_j/2^8))\bmod 1 \quad (10)$$

根据混沌映射号M的不同取值选择不同的混沌映射系统参数μ_i产生式：

$$\begin{cases}\mu_i=(((K_{\mu1}Y_i+K_{\mu2})\bmod 2^{52})/2^{52})\times 0.43+3.57 & M=0\\ \mu_i=(((K_{\mu1}Y_i+K_{\mu2})\bmod 2^{52})/2^{52})\times 0.6+1.4 & M=1\\ \mu_i=(((K_{\mu1}Y_i+K_{\mu2})\bmod 2^{52})/2^{52})\times 0.13+0.87 & M=2\end{cases} \quad (11)$$

(6) 明文/密文每一块被加密/解密，用初值X和系统参数μ_i使混沌映射迭代N次。新值$X(X')$被用于构造明文/密文以及作为下一步迭代输出反馈的一部分，如下列等式所示：

$$K'_{\mu3}=P_i+\lfloor X'(2^{31}-1)\rfloor \quad (12)$$

$$T=P_i+\lfloor X'\times(2^{52}-269)\rfloor \quad (13)$$

$$X'_b=(T/2^{52})\bmod 1 \quad (14)$$

$$K'_{\mu4}=T \bmod(2^{31}-1) \quad (15)$$

$$N'_b=(P_i+X'\times 10^3)\bmod 509 \quad (16)$$

$$C_i=K'_{\mu3} \bmod 256 \quad (17)$$

$$P_i=(C_i+256-(\lfloor X'(2^{31}-1)\rfloor \bmod 256))\bmod 256 \quad (18)$$

对于加密/解密下一块明文/密文，上一次的N'_b和X'_b分别代替式(9)、式(10)中的N_b和X_b，$K'_{\mu3}$和$K'_{\mu4}$分别更新式(6)中的随机发生器参数$K_{\mu3}$和$K_{\mu4}$。

加密/解密过程基本相同，唯一不同之处在于加密过程用的是式(17)，解密过程用的是式(18)。解密过程先用式(18)求P_i，再用式(12)~式(16)求$K'_{\mu3}$、T、X'_b、$K'_{\mu4}$、N'_b。

在文献[11]中已论证了随机数发生器中乘法器和模的取值问题，由于在式(6)中乘法器是由密钥分离而来，可以不考虑它的取值问题。在式(6)中模取$2^{31}-1$，这是根据文献[11]的建议来取的值，因为它是一个奇素数，产生的随机数具有比较大的周期。由于双精度占64位，其中第1位是符号位，依次是指数位，占11位，剩余的52位是尾数，因此取2^{52}作为式(4)、式(11)的模是恰当的，充分保证了系统参数μ_i的密钥取值空间，又不会引入小数的不确定位。

2　实验及结果分析

采用以下试验环境：CPU是Intel Celeron处理器，主频为450 MHz；内存为196 MB；操作系统为Windows 2000；使用VC++编程实现本文的算法。

表2　实验过程中各参数列表

映射号M	明文字符	迭代初值X	系统参数λ_i	迭代次数N	迭代后的值X_{new}	明文P_i	密文C_i
0	c	0.133 403 297 840 231 970 0	3.683 713 007 864 660 500 0	53 601	0.394 756 240 339 066 140 0	99	189
0	h	0.633 037 490 339 064 530 0	3.871 761 393 019 213 400 0	160	0.708 277 388 238 566 560 0	104	196
2	a	0.352 808 638 238 547 360 0	0.950 761 432 193 328 870 0	269	0.567 398 850 620 930 100 0	97	234
1	o	0.708 023 850 620 917 770 0	1.703 204 690 709 347 900 0	133	0.315 985 471 868 431 180 0	111	176
1	t	0.019 110 471 868 436 951 0	1.557 561 908 008 875 600 0	291	0.669 446 086 867 080 850 0	116	64
1	i	0.372 571 086 867 066 640 0	1.813 862 702 424 441 400 0	296	0.417 392 040 562 097 170 0	105	158
0	c	0.710 360 790 562 095 450 0	3.859 613 384 402 577 300 0	180	0.944 324 050 746 886 520 0	99	171

表2为使用密钥“12B4A54432FF4B7C4A923D274C172437”对明文“chaotic”进行加密的过程。

整数类型用signed _int64，小数类型用long double，如果小数类型采用single将使密码空间降低1倍左

右。算法设计的目的是使3个混沌映射的系统参数、初值和迭代后的值均平均约有 2^{52} 个取值。

2.1 统计分析

图1表示本文算法加密42 kB明文后的密文分布，密文也是42 kB，扩展密钥用的是“12B4A54432FF 4B7C4A923D274C172437”。很明显，图2中明文大多是一些高频字符，经过加密后密文分布却是平坦的。统计分析经常被用来进行密码分析和破译，好的密码系统不管明文是如何分布的，密文分布应该是均匀的[5]。从图1的密文分布完全能说明本文的算法能有效防止密码分析者利用统计分析的方法来击破整个加密系统。

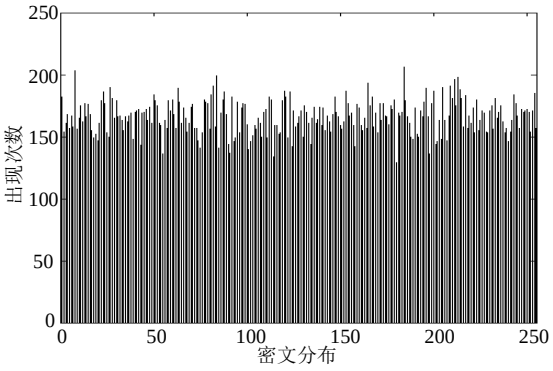

图1 密文ASCII码分布

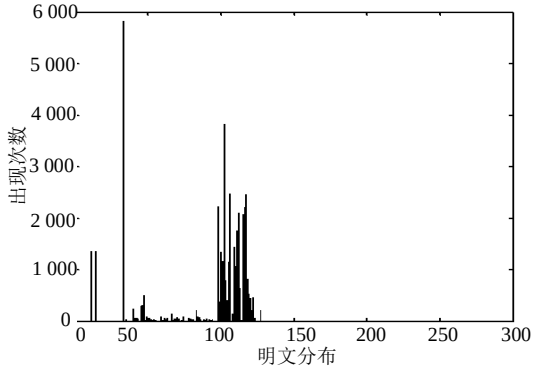

图2 明文ASCII码分布

2.2 敏感性测试

好的加密系统，其函数必须是复杂的，并且一个小的变化必然导致结果发生很大的变化[5]。图3所示为对明文“chaoticcryptosystemblockcipher”用仅差一位的密钥加密后所得的结果，使用的密钥分别是“ 12B4A54432FF4B7C4A923D274C172437 ”和“11B4A 54432FF4B7C4A923D274C172437”。图中横轴表示序号，纵轴表示对应的ASCII码值，实线连接的点表示明文ASCII分布，点连接的“*”表示使用“12B4A54432FF4B7C4A923D274C172437”作为密钥加密后密文ASCII分布，虚线连接的“+”表示使用“11B4A54432FF4B7C4A923D274C172437”为密钥加密后密文ASCII分布。从图中不难看出，虽然密钥仅相差一位，但加密后所得的密文却完全不同，这也说明本文所设计的密码系统对密钥具有敏感性。

图4是用图3明文变化一个字符，将其最前面字符‘c’变为‘a’，密钥仍然使用“12B4A54432FF4B7C4A923D274C172437”加密后所得的结果。图中横轴表示序号，纵轴表示对应的ASCII码值，用实线连接的点表示明文ASCII分布，用点连接的“*”表示使用明文“chaoticcryptosystemblockcipher”加密后密文ASCII分布，用虚线连接的“+”表示明文“ahaoticcry ptosystemblockcipher”加密后密文ASCII分布。比较图4的密文分布，可以看出两者完全不同，很明显对明文是敏感的。

本文的算法表现出的对密钥和明文的敏感性和文献[5]的好密码系统相吻合。

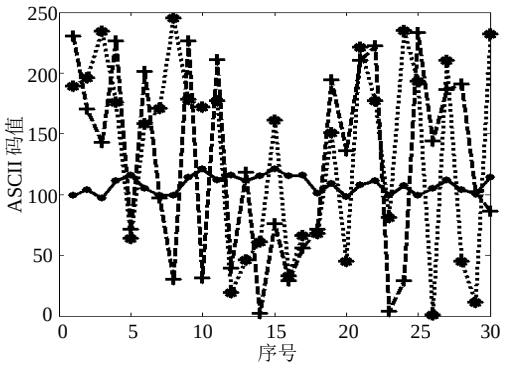

图3 利用仅差一位的密钥进行加密的结果

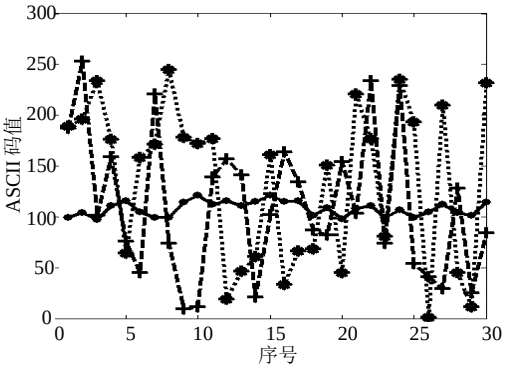

图4 对仅差一个字符的明文进行加密的结果

2.3 抵抗各种攻击分析

比较典型的穷举攻击方法有：唯密文攻击(ciphertext only attack)、已知明文攻击(known plaintext attack)、选择明文攻击(chosen plaintext attack)、选择密文攻击(chosen ciphertext attack)。很显然如果密码系统能够抵抗选择明文攻击，则足以抵抗其他各种攻击。根据Kerchoff’s准则，假定密码分析者知晓除密钥以外的所有事情。在本文的算法中，通过输出反馈的方式，后面输出的密文都与前

面加密的明文相关，密码分析者不可能得到与明文无关的密钥流。加上使用的3个混沌映射的系统参数、初值和迭代后的值均平均约有 2^{52} 个取值，迭代次数取值空间平均约为 2^9，因此每一步迭代的密钥空间约为 $3\times 2^{2\times 52+9}\approx 2^{115}$，密钥空间非常大。在目前的计算条件下，密码分析者通过选择一些明文和相应密文来穷举子密钥是非常困难的，而在算法中整个密钥空间为 2^{128}，通过密钥的扩散，其加密强度要远大于 2^{128}，要想恢复出整个密钥更是难上加难。

3 结 论

本文算法采用 128 bit 密钥，动态选取不同的一维混沌映射，通过线性同余随机数发生器动态改变系统参数，通过输出反馈动态改变混沌映射初值、迭代次数、动态改变线性同余随机数发生器的参数。这大大增强了算法对明文和密钥的敏感性，增加了抵抗各种已知攻击的能力。

参 考 文 献

[1] BAPTISTA M S. Cryptography with chaos[J]. Phys Lett A, 1998, 240: 50-54.
[2] WONG W K, LEE L P, WONG K W. A modified chaotic cryptographic method[J]. Comput Phys Commun, 2000, 138: 234-236.
[3] WONG K W. A fast chaotic cryptography scheme with dynamic look-up table[J]. Phys Lett A, 2002, 298: 238-242.
[4] WONG K W, HO S W, YUNG C K. A chaotic cryptography scheme for generating short ciphertext[J]. Phys Lett A, 2003, 310: 67-73.
[5] SHANNON C E. Communication theory of security system[J]. Bell System Technical Journal, 1949, 28: 656-715.
[6] ÁLVAREZ G, MONTOYA F, ROMERA M, et al. Cryptanalyzing an improved security modulated chaotic encryption scheme using ciphertext absolute value[J]. Chaos, Solitons and Fractals, 2005, 23: 1749-1756.
[7] CHEN Yong, LIAO Xiao-feng. Cryptanalysis on a modified Baptista-type cryptosystem with chaotic masking algorithm[J]. Phys Lett A, 2005, 342: 389-396.
[8] ÁLVAREZ G, MONTOYA F, ROMERA M, et al. Cryptanalysis of dynamic look-up table based chaotic cryptosystems[J]. Phys Let A, 2004, 326: 211-218.
[9] ÁLVAREZ G, MONTOYA F, ROMERA M, et al. Cryptanalysis of an ergodic chaotic cipher[J]. Phys Lett A, 2003, 311: 172-179.
[10] ÁLVAREZ G, MONTOYA F, ROMERA M, et al. Cryptanalysis of a discrete chaotic cryptosystem using external key[J]. Phys Lett A, 2003, 319: 334-339.
[11] TANG Hui-chin. An analysis of linear congruential random number generators when multiplier restrictions exist[J]. European Journal of Operational Research, 2007, 182: 820-828.

编 辑 漆 蓉

·我校科研成果专利介绍·

电子功能陶瓷技术——温度敏感陶瓷、压敏陶瓷

电子功能陶瓷具有压力敏感、气味敏感、热敏、电、磁、声、光等功能互相转换的特性。敏感陶瓷对温度、声音、压力、颜色和光线等的变化非常灵敏，能将其转变成电流或电压的变化并显示出来。广泛应用于自动检测、自动控制等领域。

压敏陶瓷是对电压变化敏感的非线性电阻陶瓷。目前压敏陶瓷主要有4大类—— SiC、TiO_2、$SrtiO_3$和ZnO。但应用广、性能好的当属氧化锌压敏陶瓷，由于ZnO压敏陶瓷呈现较好的压敏特性，在电力系统、电子线路、家用电器等各种装置中都有广泛的应用，尤其在高性能浪涌吸收、过压保护、超导性能和无间隙避雷器方面的应用最为突出。