一种利用外键控制的密文反馈混沌分组密码算法研究*)

陈 军[1] 张为群[2] 何春筱[3] 韦鹏程[1] 张 伟[1]

(重庆教育学院计算机与现代教育技术系 重庆 400067)[1]

(西南大学计算机与信息科学学院 重庆 400715)[2] (重庆邮电学院应用技术2分院 重庆 600066)[3]

摘 要 近年来,基于混沌理论的保密通信和数据保密得到广泛、深入的研究,提出了许多基于混沌理论的混沌加密算法,但这些算法缺乏可靠的安全性和鲁棒性。本文提出一种利用外键控制的密文反馈混沌分组密码算法,其最大的优点是系统的密钥由128位的外部键生成,混沌系统的系统参数、初始条件和迭代的次数随着密文反馈动态生成。这样,密码系统的随机性、复杂性得到了极大的提高。同时理论和实验表明,该算法具有较高的安全性和鲁棒性,能够抵抗差分和线性密码分析。

关键词 混沌加密,分组密码,Logistic映射

Study on a Novel Feedback Chaotic Block Cipher Algorithm Using External Key

CHEN Jun[1] ZHANG Wei-Qun[2] HE Chun-Xiao[3] WEI Peng-Cheng[1] ZHANG Wei[1]

(Department of Computer & Modern Education Tecnology, Chongqing Education College, Chongqing 400067)[1]

(School of Computer & Information, Southwest China University, Chongqing 400715)[2]

(The Second Division of Application Technology Department, Chonqing University of Post and Telecommunication, Chongqing 400066)[3]

Abstract In recent years, a growing number of based on chaos have been proposed, many of them fundamentally flawed by a lack of robustness and security. In this paper, we propose a novel feedback discrete chaotic block cryptosystem using external key. In this chaotic block cryptosystem, the system parameter or initial condition of the chaotic map are generated by an external 128-bit secret, and the ciphertext block of current plaintext block is fed back to generate the next round of the system parameter, the initial condition and number of iterations. In addition, the nature features of chaos make the cryptosystem more complex and more difficult to be analyzed or predicted. Simulation results show that the proposed algorithm has high security and robustness, can against the differential and linear attacks and with high security.

Keywords Chaotic encryption, Block cipher, Logistic map

1 引言

混沌(Chaos)是一种复杂的非线性动力学行为,混沌系统所具有的对初值敏感性,混沌轨道的伪随机性、遍历性和不可预测等自然特性,可以提供数量众多、非相关、伪随机而又确定可再生的混沌序列,使其在保密通信和密码学领域的应用越来越广泛,研究越来越深入,取得了大量的成果[1~5]。纵观这些研究成果,混沌的应用主要有四个方面:一是运用混沌同步进行混沌保密通信;二是运用一维或高维混沌所产生的伪随机序列与待加密的明文进行异或运算以产生密文,这是混沌应用于序列密码算法的典型方法;三是将混沌映射作为加密变换的轮函数,将混沌迭代与明文信息相结合以产生密文;四是混沌映射与分组密码中非常经典的Feistel结构相结合,以获得具有非常好的扩散和扰乱效果。

在已有的混沌系统中,都是以系统的确定的混沌参数和初值条件作为秘密密钥,其迭代的次数是固定的,然而这样的混沌系统在文[6~9]中已经被证明为不安全。为了克服以上的弱点,本文在详细分析Logistic映射的基础上,提出一种基于外键控制的密文反馈模式的混沌分组密码算法,该算法的最大特点是系统的密钥是由128位的外部键生成,混沌系统的系统参数、初始条件和迭代次数由密文反馈动态生成。这样,密码系统的随机性、复杂性得到了极大的提高,可以有效地抵抗针对系统参数和初始条件的攻击。

2 混沌系统

混沌现象是在非线性动力系统中出现的确定性的、类似随机的过程,这种过程既非周期又不收敛,并且对初始值有极其敏感的依赖性。

一类非常简单却被广泛研究的动力系统是Logistic映射,其定义如下:

$$X_{k+1}=\lambda X_k(1-X_k) \tag{1}$$

其中,$0\leqslant\lambda\leqslant4$称为分枝参数,$X_k\in(0,1)$。混沌动力系统的研究工作指出,当$3.5699456\cdots<\lambda<4$Logistic映射工作于混沌态。也就是说,由初始条件X_0在Logistic映射的作用下所产生的序列$\{X_k,k=0,1,2,3,\cdots\}$是非周期的、不收敛的,并对初始值非常敏感。

文[10]证明了系统式(1)所产生的混沌序列的概率分布密度函数PDF(Probability Density Function)为:

$$\rho(x)=\begin{cases}\dfrac{1}{\pi\sqrt{1-x^2}}, & -1<x<1\\ 0, & \text{否则}\end{cases} \tag{2}$$

$\rho(x)$是不依赖于初始值,所以式(2)表达的混沌系统具有普遍

*)重庆市科委自然科学基金资助项目(No. CSTC,2005BB2286),重庆市教委资助项目(No. kj051501)。陈 军 讲师,硕士研究生。张为群 教授。何春筱 讲师。韦鹏程 讲师,博士研究生。张伟 副教授,博士,在站博士后。

性。

通过 $\rho(x)$，我们可以很容易地计算得到 Logistic 映射所产生的混沌序列的一些很有意义的统计特性。x 的时间平均即混沌序列轨迹点的均值为：

$$\bar{x}=\lim_{N\to\infty}\frac{1}{N}\sum_{i=0}^{N=i}x_i=\int_{-1}^{1}x\rho(x)\mathrm{d}x=0 \tag{3}$$

对于相关函数，独立选取两个初始值 x_0 和 y_0，则序列的互相关函数为：

$$c(l)=\lim_{N\to\infty}\frac{1}{N}\sum_{i=0}^{N-1}(x_i-\bar{x})y_{(i+l)}-\bar{y})=\int_0^1\int_0^1\rho(x,y)(x-\bar{x})(\tau^l(y)-(\bar{y}))\mathrm{d}x\mathrm{d}y=0 \tag{4}$$

注意联合 PDF：$\rho(x,y)=\rho(x)\times\rho(y)$。而序列的自相关函数 ACF(Auto-Correlation Functions)则等于 delta 函数 $\delta(1)$。这正是我们所需要的。

通过以上分析知，尽管混沌动力系统具有确定性，但其形式简单，对初始条件值敏感，具备白噪声的统计特性等，因而可以应用于保密通信和密码学领域等许多应用领域。

3 算法描述

基于 128 位外键控制密钥的密文反馈模式分组密码算法加密过程如图 1 所示。

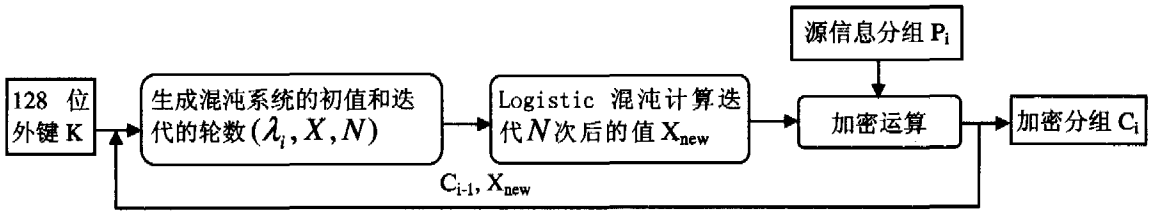

图 1 加密过程

(a) 选取 128 位外键(K)作为整个加密系统的密钥，把 K 划分成 8 位的 16 个分组：

$$K=K_1K_2K_3\cdots K_{16} \tag{5}$$

(b)把明文划和密文分成 8 位的分组组合：

$$P=P_1P_2\cdots P_3 \tag{6}$$

$$C=C_1C_2\cdots C_3 \tag{7}$$

(c)根据式(8)和(9)分别计算 X_s、N_s，X_s 和 N_s 它们作为计算 Logistic 混沌系统的初始条件和迭代轮数的种子。

$$X_s=\frac{K_1\oplus K_2\oplus\cdots\oplus K_{16}}{256} \tag{8}$$

$$N_s=(K_1+K_2+\cdots+K_{16})\bmod 256 \tag{9}$$

(d)根据式(10)和(11)计算 Logistic 混沌系统的初始条件 X 和迭代次数 N。

$$X=(X_s+\frac{K_r}{256})\bmod 1 \tag{10}$$

$$N=N_S+K_r \tag{11}$$

其中 $K_r(1\leqslant K\leqslant 16)$ 是密钥 $K=K_1K_2K_3\cdots K_{16}$ 的子密钥，r 由随机函数 Rand()随机生成。

(e)根据线性映射(12)和(13)计算 Logistic 混沌系统的参数 λ_i。

$$\lambda_i=((a*y_i+c)\bmod m)/200+3.57 \tag{12}$$

$$y_i=(a*y_{i-1}+c)\bmod m \tag{13}$$

上式中，$a=16$，$c=7$，$m=81$，$y_i=0$。

(f)用 λ_i 和 X 作为 Logistic 混沌系统的参数和初始条件，迭代 N 次后得到 X_{new}，然后根据式(14)和(15)进行加密/解密。

$$C_i=(P_i+\lfloor X_{new}*256\rfloor)\bmod 256 \tag{14}$$

$$P_i=(C_i+256-\lfloor X_{new}*256\rfloor)\bmod 256 \tag{15}$$

(g)为了加密下一个明文分组，把 X_{new} 和 C_{i-1} 作为 Logistic 混沌系统的初始条件 X_s 和迭代轮数 N_s 的种子，然后重复步骤(d)～(f)，知道所有明文被加密。

4 模拟仿真及分析

4.1 密钥空间

本文提出算法的密钥长度为 128 位，可以知道系统具有足够大的密钥空间为 $2^{128}=10^{38.5}$，这样可以有效地抵抗穷举攻击。同时加密系统的初始条件 X，系统参数 λ_i 和迭代次数 N 是由反馈密文 C_{i-1} 和 X_{new} 动态生成，所以密码分析者必须知道本轮加密的初始条件 X，系统参数 λ_i 和迭代次数 N，因而可以有效地抵抗针对混沌系统 λ 和初始条件 N 的攻击。

4.2 密文分布分析

密文分布是一个密码系统最重要的特性之一，它将直接影响到密码系统的安全。一个分布不均匀密文，往往是密码分析者进行唯密文攻击的首选人口[11]。为更清晰地描述这一特性，我们对如下两个明文分别进行加密实验：

明文 1：Dear sir, We'd like to invite you to come back to our site today (www. cqec. net. cn) to finish your registration and check out all that has to offer. Therefore, we have included you password and your username for you reference. Your password : abcd123 your username: tracy123.

明文 2：明文 2：BBBBBBBBBBLLLLLLLLLLVVVVVV-VVVV。

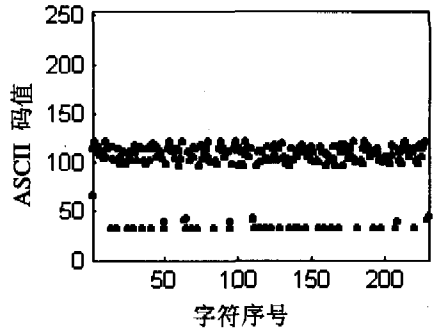

图 2 明文 1

由于通过基于外键控制的密文反馈模式的分组密码算法加密得到的密文含有不可打印的 ASCII 字符，因此为了形象地展示密文与明文之间的区别，我们使用二维图形来表达。从明文和密文的图形来看，明文的码值比较集中，而密文的码值却非常分散。图 2 和图 3 分别为加密前后字符的 ASCII 分布图，可以看出加密前字符分布比较集中，其码值主要分布在一个较小的范围内。但通过加密后，情况则大不相同，字符分

布很均匀。也就是说，通过扩散、扰乱等作用后，密文中不包含明文的任何信息(包括明文的统计概率信息)。这正是我们想要达到的加密效果。图 4 和图 5 为明文 2 的实验结果。

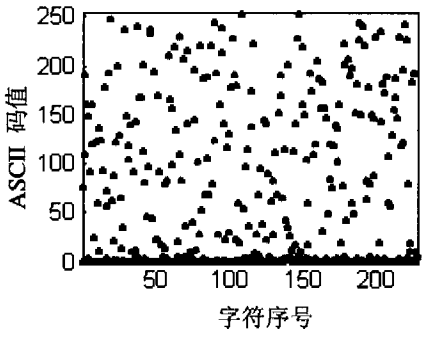

图 3　密文 1

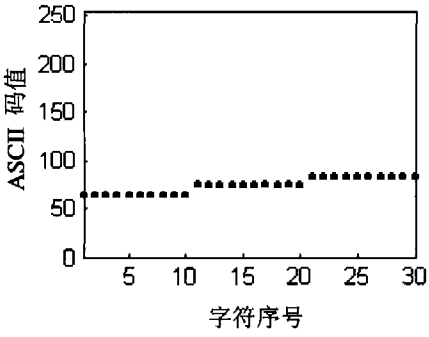

图 4　明文 2

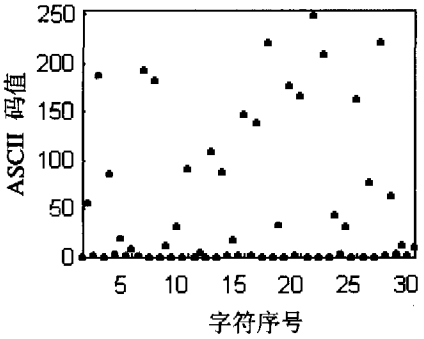

图 5　密文 2

4.3　扰乱与扩散性能分析

扰乱与扩散是设计分组密码的两条基本指导原则[11]。扩散是将每一位明文的影响尽可能地作用到较多的输出密文位中去，同时，还要尽量使得每一位密钥的影响也尽可能迅速地扩展到较多的密文位中去。其目的是有效隐藏明文的统计特性，这也就是混沌系统的初始条件敏感依赖性。扰乱，是指密文和明文之间的统计特性的关系尽可能的复杂化，这也就是混沌映射通过迭代，将初始域扩散到整个相空间。通过扰乱和扩散，可以有效地抵抗统计和抗差分攻击。

在传统分组密码算法中，其置乱都是基于预先编排好置换盒(如 DES 的 P 盒)，它只是重新编排了明文分组排序而已，对加密过程中所要求的扰乱和扩散特性的贡献非常小，以至于在差分和线性密码分析中都将其效果忽略不计[12]。而在本文所提算法中，混沌系统的初始条件 X 和系统的参数 λ 决定明文分组置乱效果，而迭代的次数 N、初始条件 X 和系统的参数 λ 基于密文反馈动态更新的，即混沌系统的初始值和控制参数是紧密相关的，所以这种置乱是敏感地依赖于密钥且随机的，大大增加了密码系统的扰乱与扩散特性。

4.4　密文对密钥的敏感依赖

基于外键控制的密文反馈模式的混沌分组加密系统对密钥是非常敏感的。使用微小差异的密钥就会产生截然不同的加密密文，或从密文中恢复出错误的明文，而这一点正是密码学所要求的。图 6 和图 7 分别是加密密钥作微小的改动，从密文恢复出的明文的实验的结果。

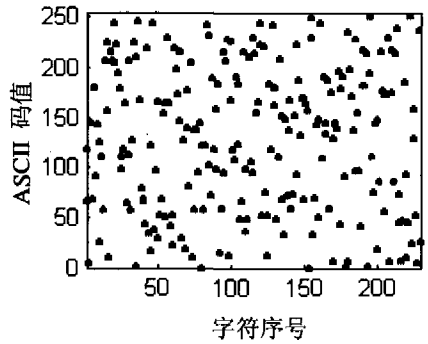

图 6　参数微小失配时恢复出的明文 1

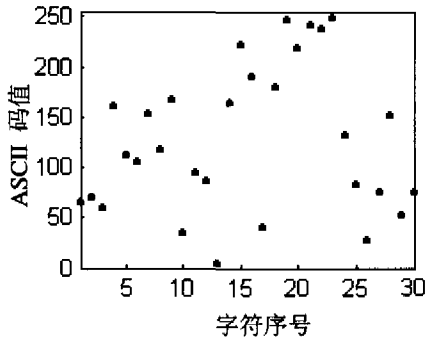

图 7　参数微小失配时恢复出的明文 2

结论　本文分析了 Logistic 映射的混沌特性和密码学特性，并根据这些特点，设计出一种新颖的基于外键控制的密文反馈模式的混沌分组密码算法，该算法的最大特点是系统的秘密密钥由 128 位的外部键生成，混沌系统的系统参数、初始条件和迭代的次数随着密文反馈动态生成。同时，混沌系统的本质特性使得算法的复杂度极大地提高，从而更难以分析和预测。实验结果和理论分析表明，它具有较强的抵抗差分密码分析和线性密码分析的能力有及较高的安全性。

参 考 文 献

1　Matthews R. On the derivation of a chaotic encryption algorithm. Cryptologia, XIII (1), 1989. 29～42
2　Habutsu T, Nishio Y, Sasase I, et al. A secret cryptosystem by iterating a chaotic map. Advance in cryptology-EUROCRYPT'91, LNCS 547, Springer-Verlag, Berlin, 1991. 127～140
3　Biham E. Cryptanalysis of the chaotic-map cryptosystem suggested as EUROCRYPT'91. Advance in cryptology - EUROCRYPT'91, LNCS 547, Springer-Verlag, Berlin, 1991. 532～534
4　Kocarev L, Jakimoski G. Logistic map as a block encryption algorithm. Phys. Lett. A, 2001, 289: 199～206
5　Wong K W. A fast chaotic cryptographic scheme with dynamic look-up table. Phys. Lett. A, 2002, 298: 238～242
6　Alvarez G, Montoya F, Romera M, et al. Phys. Lett. A 276, 2000, 191
7　Alvarez G, Montoya F, Romera M, et al. Phys. Lett. A 311, 2003, 172
8　Alvarez G, Montoya F, Romera M, et al. Phys. Lett. A 306, 2003, 200
9　Alvarez G, Montoya F, Romera M, et al. Keystream cryptanalysis of a chaotic cryptographic method. Comput. Phys. Commun., 2003
10　王光瑞，陈光旨. 非线性常微分方程的混沌运动. 南宁：广西科学技术出版社，1995
11　Schneier B 著. 吴世忠，祝世雄，张文政，等译. 应用密码学，机械工业出版社，2001
12　Pareek N K, Patidar V, Sud K K. Phys. Lett. A 309, 2003, 75