一种基于 Feistel 网络的反馈式分组混沌密码的研究*)

彭 军[1] 张 伟[2] 杨治明[1] 廖晓峰[3]
(重庆科技学院电子信息工程学院 重庆 400050)[1]
(重庆教育学院计算机与现代教育技术系 重庆 400067)[2]
(重庆大学计算机科学与工程学院 重庆 400044)[3]

摘 要 近年来,将混沌理论应用到信息安全已成为研究的一个热点。本文基于 Feistel 网络,提出了一种新颖的反馈式分组混沌密码算法。在该算法中,当前加密分组输出将影响下一明文分组要运行的轮数,而每一轮使用的 S-盒的序号与加密密钥有关,轮数及 S-盒的序号均由混沌映射动态生成。由于混沌的固有特性,使得加密系统变得更加复杂,更加难以分析和预测。实验结果表明,本算法具有优良的密码学特性,对明文和密钥以及混沌系统参数的细微变动都非常敏感,产生的密文随机性很好。对本算法的安全性进行了分析,结果表明它具有很高的抗穷举攻击的能力。

关键词 Feistel 网络,分组密码,混沌映射

Research on a Feedback Block Chaotic Cipher Algorithm Based on Feistel Network

PENG Jun[1] ZHANG Wei[2] YANG Zhi-Ming[1] LIAO Xiao-Feng[3]
(College of Electronic Information Engineering, Chongqing University of Science and Technology, Chongqing 400050)[1]
(Department of Computer and Modern Education Technology, Chongqing Education College, Chongqing 400067)[2]
(Department of Computer Science and Engineering, Chongqing University, Chongqing 400044)[3]

Abstract In recent years, the application research of information security using chaos theory has become an area of active research. In this paper, we propose a novel feedback block chaotic cipher algorithm based on Feistel network. The output cipher text of current plaintext block affects the number of round that will be used in the next plaintext block and the no of S-box used by each round function is related to the secret key. The value of rounds and the sequence number of S-box are all generated dynamically by chaotic map. 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 excellent cryptographic properties, i. e., the algorithm is very sensitive with respect to the small change of plaintext, secret key and the parameters of chaotic system, and the randomicity of ciphertext is very ideal. At last, the security of the algorithm is studied, and the result indicates that the algorithm proposed in this paper possesses higher capability of resisting the brute-force attack.

Keywords Feistel network, Block cipher, Chaotic map

1 引言

由非线性系统产生的混沌信号,对系统初值和参数极其敏感。由于具有高度的不可预测性和类随机、宽频谱等特性,使得混沌密码学成为信息安全领域的一个研究热点并取得了诸多研究成果[1~6]。英国数学家 Matthews[1] 最早提出了混沌序列密码的概念,他研究了 Logistic 混沌映射作为序列密钥流生成器问题。Habutsu 等[2] 则基于分段线性 Tent 混沌映射提出了一种混沌加密系统。随后 Biham[3] 指出,使用选择密文攻击可容易地对该系统解密,并且已知明文攻击的复杂度为 2^{38}。L. Kocarev 等[4] 提出了一种基于 Logistic 混沌映射的分组加密算法,讨论了混沌具有密码学所要求的如扩散、混乱等特性。此外,K. W. Wong[5] 提出了一种快速混沌加密方案,通过动态更新查询表来实现加解密,而 K. Murali[6] 则基于密码学使用常规同步方法去同步一个级联的异构混沌系统,以实现信息的加密传输。可以肯定,这些研究成果对后续的混沌密码学研究工作起到了一定的指导作用。

Feistel 网络被广泛地用于分组密码的设计,典型的有 DES、Lucifer、FEAL、LOKI、GOST 和 Blowfish 等,其基本思想为[7]:取一个长度为 n 的分组,将它分成长度为 $n/2$ 的左右两个部分,设为 L 和 R。定义一个迭代型的分组密码算法,其第 i 轮的输出为

$$L_i=R_{i-1},R_i=L_{i-1}\oplus F(R_{i-1},K_{i,\mathrm{sub}})$$

其中 $K_{i,\mathrm{sub}}$ 是第 i 轮使用的子密钥,F 可以是任意的轮函数。只要 F 能在每一轮中重新构造,Feistel 网络的结构特点就能保证该密码的可逆性,哪怕 F 是不可拟的。这是因为:

$$R_i\oplus F(L,K_{i,\mathrm{sub}})=(L_{i-1}\oplus F(R_{i-1},K_{i,\mathrm{sub}}))\oplus F(R_{i-1},K_{i,\mathrm{sub}})=L_{i-1}$$

*)基金项目:国家自然科学基金(60271019)、教育部博士点专项基金(20020611007)、重庆市科委应用基础研究项目基金(7370)。彭 军 副教授、博士,研究方向为网络安全、混沌密码学;张 伟 副教授、博士,研究方向为网络安全、混沌保密通信;杨治明 讲师、硕士,研究方向为网络安全;廖晓峰 教授、博士后、博士生导师,研究方向为神经网络、混沌保密通信、信号处理。

因此，该网络可同时用于加密和解密，特别适合硬件实现。

本文将利用Logistic混沌映射，基于Feistel网络，提出一种新颖的反馈式分组混沌密码算法(以下简称FBCCA)，并对该算法进行密码学分析实验。

本文提出的分组密码，其分组加密的每一轮采用Feistel网络结构。与DES或HOST等算法不同的是，每个分组运行的轮数不是固定为16或32，而是根据前一分组的加密输出动态确定，因此我们称之为反馈式分组密码。同时，子密钥的选取也是动态的，它与加密密钥和本轮的输入有关，通过一个混沌映射的多次迭代而确定。将混沌引入到子密钥的选取中，增加了系统的随机性、复杂性和鲁棒性。

2 混沌映射的选取

关于如何选取满足密码学特性要求的混沌映射，是一个需要解决的关键问题。L. Kocarev等在文[4]中给出了这方面的一些指导性建议。选取的混沌映射应至少具有如下三个特性：混合特性(Mixing property)、鲁棒混沌(Robust chaos)和具有大的参数集(Large parameter set)。具体请参见文[4]。

本文为便于阐述和理解，仍采用文[4]中的Logistic混沌映射，定义如下：

$$L(y)=ay(1-y) \tag{1}$$

其中参数$a=4$(满映射情形)，$y\in[0,1]$。由于式(1)不是结构稳定的，因此用下式替换y：

$$y=(\tilde{y}+p)\bmod 1 \tag{2}$$

其中$\tilde{y}\in[0,1]$，$p\in R$为参数。这样，对所有的参数p，Logistic映射都是鲁棒混沌的[4]，可以被用来设计加密算法。在本文算法中，Logistic映射将被用于确定每轮使用的子密钥以及每个明文分组需要迭代的轮数。

3 分组加密算法

设明文$P=P_1P_2\cdots P_m$，对应密文$C=C_1C_2\cdots C_m$，其中m为分组的个数。密钥$K=K_1K_2\cdots K_n$，本文取$n=8$，即密钥长度为64位。

根据密钥K，按下式生成两个与混沌映射迭代有关的数值X_s和N_s[8]：

$$X_s=(K_1\oplus K_2\oplus\cdots\oplus K_n)/256 \tag{3}$$

$$N_s=(K_1+K_2+\cdots K_n)\bmod 256 \tag{4}$$

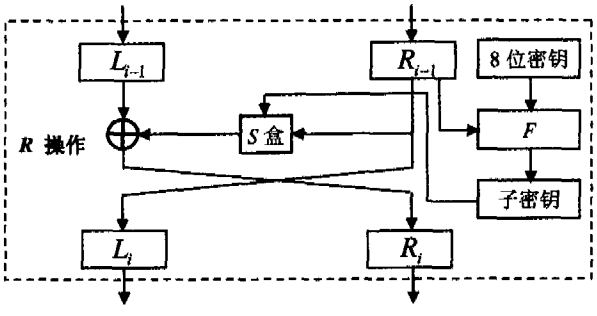

图1 一轮FBCCA算法(简称R操作)

图1是一轮FBCCA分组密码算法(以下简称R操作)。图中L_{i-1}和R_{i-1}分别为前一轮输出分组$C_{i-1}=\{L_{i-1},R_{i-1}\}$的左半部分和右半部分(各16字节)。函数$F$用于生成本轮使用的子密钥$K_{sub}$，以确定要使用的S-盒的序号。

函数F描述如下：

(1) 计算混沌映射式(1)的迭代初值：$X=(X_s+R_{i-1}/256^2)\bmod 1$

(2) 计算混沌映射式(1)的迭代次数：$N=floor(N_s+X\cdot 256)$

(3) 对混沌映射式(1)，用初值X迭代N次，得到最终迭代值X_N

(4) 计算子密钥：$K_{sub}=(floor(R_{i-1}+X_N\cdot 8))\bmod 8)+1$

该描述中，函数$floor(\ )$表示取下整数，子密钥K_{sub}就是S-盒对应的序号。在FBCCA算法中，直接选用了GOST算法提供的S-盒(具体参见文[9])。GOST算法一共有8个S-盒，每一个S-盒都是数0～15的一个置换。例如，S-盒1定义如下：

4,10,9,2,13,8,0,14,6,11,1,12,7,15,5,3

于是当S-盒的输入为0时，则输出为4；如果输入为7，则输出为12。依此类推。

下面给出FBCCA分组密码算法的加密过程。

(1) 设第k个明文分组为P_k，并对其进行R_k轮R操作。若$k=1$，则$R_k=32$；若$k>1$，则按以下步骤确定：

a. 设$\tilde{L}_{k-1}$，$\tilde{R}_{k-1}$分别表示第$k-1$个分组加密输出的左半部分和右半部分(各2个字节)，而$\tilde{L}_{k-1,h}$和$\tilde{L}_{k-1,l}$分别为$\tilde{L}_{k-1}$的高8位字节和低8位字节，$\tilde{R}_{k-1,h}$和$\tilde{R}_{k-1,l}$分别为$\tilde{R}_{k-1}$的高8位字节和低8位字节。

b. 计算$\tilde{T}_{k-1}=(\tilde{L}_{k-1}\oplus\tilde{R}_{k-1})/(256\cdot 256)$

$\tilde{X}_s=\tilde{T}_{k-1}\bmod 1$

$\tilde{N}_s=\tilde{L}_{k-1,h}\oplus\tilde{L}_{k-1,l}\oplus\tilde{L}_{k-1,h}\oplus\tilde{R}_{k-1,l}$

$\tilde{X}_N=L(\tilde{X}_s,\tilde{N}_s)$

其中$L(\tilde{X}_s,\tilde{N}_s)$表示对混沌映射式(1)使用初值$\tilde{X}_s$迭代$\tilde{N}_s$次得到的迭代值。

c. 计算$R_k=16+floor(\tilde{X}_N\cdot 16)$

(2) 执行步骤(1)后，得到加密分组C_k。

(3) 对后续明文分组重复步骤(1)，直至明文分组结束。

FBCCA分组密码算法的解密过程与加密过程类似，可以使用相同的R操作，只是在使用时略有不同。例如，要对第k个明文分组P_k进行加密时，此时R操作的输入是该分组的左右两部分，即$\{\tilde{L}_k,\tilde{R}_k\}$。经过相应轮次的R操作后，输出加密分组$C_k=\{\tilde{L}_k,\tilde{R}_k\}$。解密时，则先按加密过程中的相同算法确定本密文分组使用的轮次R_k，然后对密文分组的右左两部分即$\{\tilde{R}_k,\tilde{L}_k\}$进行$R_k$轮次的R操作，其输出分组为$\{\bar{R}_k,\bar{L}_k\}$，并将其重新组合成明文$P_k=\{\bar{L}_k,\bar{R}_k\}$。

4 实验结果

我们知道，一个好的密码系统应该对密钥是敏感的，而且对明文也应该是敏感的。从本算法的设计角度来看，这两种敏感特性是能够得到满足的。传统的如DES或GOST等分组密码，其对明文的敏感性体现为一个明文分组的变化只影响到其对应的密文分组。而本文提出的FBCCA分组密码算法，一个明文分组的变化不但影响到对应的密文分组，而且影响到其后续的密文分组，这是因为后续明文分组在加密时使用了前面的密文分组，也就是说加密算法中加入了反馈信息。这点是本算法的一个很大的特点。

以下是实验时使用的数据：混沌映射选用式(1)，其中参数$p=0.367$；明文msg1='A Chaotic Block Encryption Algorithm'，密钥key1='Wh8t * ga/'。为了检测算法对密钥

和明文的敏感性，对明文和密钥只改变 1 位，即明文 msg2＝'B Chaotic Block Encryption Algorithm'，密钥 key1＝'Wh8t * gb/'。实验结果如图 2 所示，图中正方形实线为明文，上三角形虚线为使用 msg1 和 key1 时的密文。图 2(a)中圆点实线为使用 msg2 和 key1 时的密文，图 2(b)中圆点实线为使用 msg1 和 key2 时的密文。我们注意到，msg1 与 msg2 只有第一个字符不同，key1 与 key2 也只有一个字符不同。但从图中看出，密文与明文是截然不同的，这表明算法对明文和密钥都十分敏感。

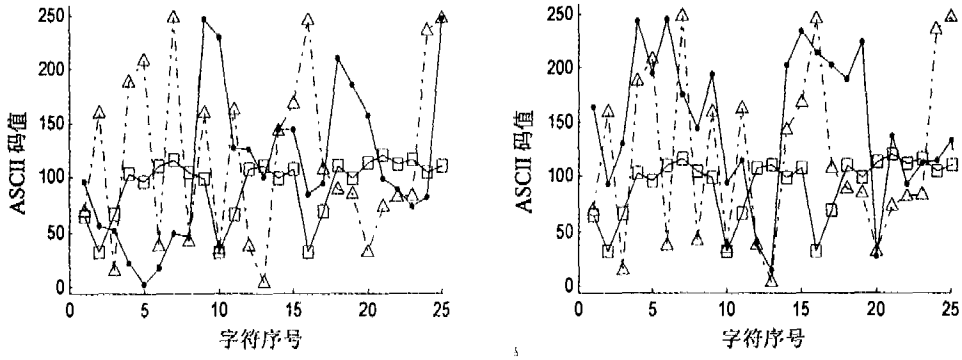

图 2　(a)明文 msg1 及其密文，以及明文 msg2 密文(使用相同的密钥 key1)；(b)明文 msg1 及使用密钥 key1 和 key2 时的密文

好的密码算法还应使明文映射成一个看似随机的密文，这样密文将隐藏明文的统计信息。为此，我们还设计了如下两组明文：

msg3＝'BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB'

msg4＝'ABBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB'

仍采用上述的实验方法，得到结果如图 3 所示。结果表明，明文 msg3 和 msg4 都有十分明显的统计分布规律，但其对应的密文没有任何对攻击者"有用"的统计信息，同时也看出本算法对这种类型的明文也具有非常好的敏感性(包括对密钥的敏感性)。

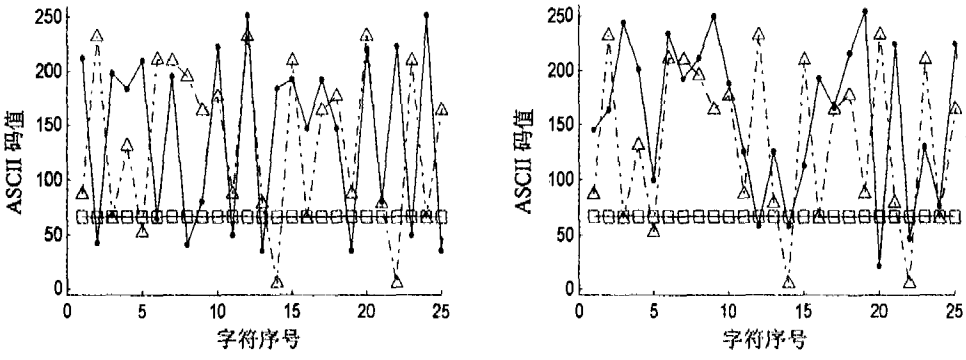

图 3　(a)明文 msg3 及其密文，以及明文 msg4 的密文(使用相同的密钥 key1)；(b)明文 msg3 以及使用密钥 key1 和 key2 时的密文

5　安全性分析

在 FBCCA 算法中，密钥的长度为 64 位。如果公开混沌系统及其参数(包括参数 p)，则穷举法攻击的成功概率为 2^{-64}。由于密钥和混沌系统对算法的贡献最终体现在确定每轮使用的 S-盒的序号以及每个分组执行的轮数，因此攻击者可不对密钥进行攻击，而是猜测每个分组使用的 S-盒的序号，那么其成功的概率更小。分析如下：按照加密算法，第一个分组执行了 32 轮的 R 操作，每次 R 操作有 8 种选择 S-盒的可能(假设公开 S-盒的细节)，破解第一个分组的概率为 $(2^{-3})^{32}=2^{-96}$，其破解的结果就是攻击者获得了第一个分组 32 轮 R 操作使用的子密钥，它是 S-盒序号的一个组合排列。但该子密钥是根据密钥和混沌系统以及明文动态产生的，而非固定不变，破解的结果对攻击者而言"毫无意义"。对后续分组的破解，其结果更是没有多少价值，原因在于除了子密钥是动态的外，连每个分组执行的轮次也是动态的(范围为 16～31)。这种破解结果将不会给攻击者提供任何"有用的模式"。

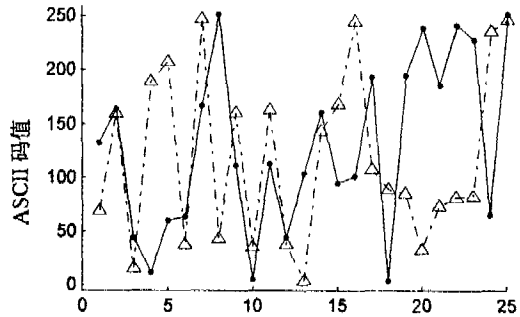

图 4　明文 msg1 的加密密文

上三角形虚线对应混沌系统参数 $p=0.367$，圆点实线对应混沌系统参数 $p=0.366$。两种情况均使用相同的加密密钥 key1。

因此比较而言，攻击密钥的难度相对小得多。但是，如果不公开混沌系统及其参数，则难度将大幅提高。由混沌系统的特性知道，混沌序列对系统参数和初值极端敏感，它们的微小变化都将产生截然不同的混沌序列，且序列之间有非常好

(下转第 77 页)

统耦合度，提高了系统重用性。

操作系统中，Windows 系统就是典型事件/消息驱动。其 GUI 完全靠消息驱动实现，一些重要机制亦然，如定时器、异步 I/O 读写以及内核不可抢占级别下与用户空间的通讯。消息机制大大提高了系统扩展性。

事件驱动方式能明显降低耦合度，提高扩展性。本框架因应用需求必须充分解耦，支持高扩展性。MVC 模式虽然给出方案，但不能完全满足本文需求，例如其核心模式——观察者模式中，观察者到模型是强耦合关系。通过基于消息的事件驱动，我们获得了更大的灵活性。

结论 分层事件驱动风格对不同的系统需求进行了支持，包括交互式应用，响应的实时性，系统可扩展性。在实际应用中，我们将不同的入侵分析系统，响应系统和日志系统通过该风格的框架集成到系统中。特别是事件驱动方式在分层构架中提供的足够的实时性，使得系统在速度和扩展性的选择方面获得了良好的灵活性。

参 考 文 献

1 Shaw M, Garlan D. Software architecture perspectives on emerging discipline. Prentice Hall, 1996

2 韩宏，卢显良. 插件式网络安全集成防护框架. 计算机科学，2005，32(4)

3 Gamma E, Helm R. Design Patterns Elements of Reusable Object-Oriented Software. Addison Wesley Longman, 1995

4 Krasner G E, Pope S T. A cookbook for using the Model-View-Controller user interface paradigm in smalltalk-80. Journal of Object-Oriented Programming, SIGS Publications, New York, NY, USA, 1988

5 Coutaz J. PAC, an Object Oriented Model for Dialog Design, Human-Computer Interaction. In: INTERACT'87 proceedings, 1987

6 Kruchten P B. The 4+1 View Model of Architecture. IEEE Software, Nov. 1995

7 Fowler A. A Swing Architecture Overview: The Inside Story on JFC Component Design. http://java.sun.com/products/jfc/tsc/articles/architecture/

8 Buschmann F, Meunier R. Pattern-Oriented Software Architecture Volum1: A System of Patterns. John Wiley & Sons, Inc. 1996

9 Reiss S P. Connecting tools using message passing in the Field Environment. IEEE Software, July 1990

(上接第 74 页)

的相关性能。这也是混沌序列能被广泛地应用到信息加密领域的一个重要原因。此处我们给出一个对比实验以示说明。仍然使用明文 msg1 和密钥 key1，混沌系统参数 $p=0.367$ 和 $p=0.366$(相差 10^{-3})，实验结果如图 4 所示。实验结果表明，参数 p 对密文的影响是很显著的。这说明如果将混沌系统参数作为密钥的一部分，将增大系统的安全性，提高抗破译的能力。设参数 p 的精度为 2^{-16}，则加密算法被攻破的概率为 $2^{-64}\cdot 2^{-16}=2^{-80}$。

结论 本文基于 Feistel 网络提出了一种新颖的反馈式分组混沌密码算法，并对算法进行了详细描述。与 DES 或 HOST 等算法不同的是，每个分组执行的轮数是根据前一分组的输出动态确定的，并且每一轮使用的 S-盒的序号也是由混沌映射动态产生的。将混沌引入到加密算法中来，由于混沌的固有特性，使得加密系统变得更加复杂，更加难以分析和预测，其抗攻击的能力大幅提高。实验结果也显示出本算法具有优良密码学特性，对明文和密钥以及混沌系统参数等非常敏感。此外，还对算法的安全性进行了分析，对于使用穷举法对系统进行攻击，我们认为其难度是相当大的。

文中的算法对更长的加密密钥以及其他混沌映射仍然适用。本文是我们在混沌分组密码研究工作的一个阶段性成果，后续的工作将对算法在抵抗差分密码分析和线性密码分析等方面做深入的研究，结果将另文报道。

参 考 文 献

1 Matthews R. On the derivation of a chaotic encryption algorithm. Cryptologia, 1989, XIII (1): 29～42

2 Habutsu T, Nishio Y, Sasase I, et al. A secret cryptosystem by iterating a chaotic map. In: 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. In: 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 (4～5): 199～206

5 Wong K W. A fast chaotic cryptographic scheme with dynamic look-up table. Phys Lett A, 2002, 298(4): 238～242

6 Murali K. Heterogeneous chaotic systems based cryptography. Phys Lett A, 2000, 272: 184～192

7 Schneier B. 应用密码学—协议、算法与 C 源程序. 吴世忠，祝世雄，张文政，等译. 北京：机械工业出版社，2000

8 Pareek N K, Patidar V, Sud K K. Discrete chaotic cryptography using external key. Phys Lett A, 2003, 309(1～2): 75～82

9 GOST R 34.11-94, Gosudarstvennyi Standard of Russian Federation. Information technology. Cryptographic Data Security. Hashing function. Government Committee of the Russia for Standards, 1994