一种改进的多级混沌加密系统

An Improved Multistage Chaotic Encryption System

彭 军[1,2] 张 伟[1,3] 廖晓峰[1] 吴中福[1]

(重庆大学计算机学院 重庆400044)[1] (重庆工业高等专科学校计算机系 重庆400050)[2]

(重庆教育学院计算机与现代教育技术系 重庆400067)[3]

Abstract Recently, two essential defects and other weaknesses of the chaotic encryption system in [6] have been given in [8] and an improved encryption scheme is proposed to obtain higher security [8]. Their improved scheme is immune to the four cryptanalytic attacks employed by [7]. Taking into account conventional cryptography theory, we present an improved multistage chaotic encrption system based on similar thought. Computer simulation illustrate that the system proposed in this paper has some characters such as higher security as well as imoplementation fast, etc.

Keywords Chaos, Chaotic cryptosystem, Encryption

1 引言

由于混沌信号具有高度的类随机特性和不可预测性，因此近年来混沌理论及其在保密通信、信息安全中的应用研究日益得到人们的广泛重视。

我们知道通信中的同步是至关重要的。而关于混沌系统的同步，早在90年代初，L. M. Pecora 和 T. L. Carroll[1]就在《物理学评论通信》(Physical Review Letters)上发表了题为"混沌系统中的同步"的研究报告，报道了他们在混沌同步方面所取得的具有里程碑意义的贡献。在这之后很多混沌保密通信方案几乎都是基于同步而获得的[2~4]。文[2]采用同步混沌系统研究了一种新的混沌掩盖通信方案，它分为同步和信息传递两个阶段，同步阶段负责系统的同步，而传递阶段则只负责传递信息。文[3]研究了关于在驱动-响应混沌系统中通过只传递一个标量信号来实现自适应同步问题。文[4]提出了一种基于密码学的异构混沌系统，使用传统的同步方案实现了数字信号的保密通信。

最近还出现了不使用混沌同步的加密系统[5,6]。在文[5]中，作者将明文中的每个字符都编码成 Logisitic 方程的迭代次数，并且加密变换所用的种子数可以大到65536，远大于传统加密算法(通常少于30)。而文[6]则提出了一种新的基于混沌系统迭代的对称加密方案，该方案简单、易实现，有创意。但随后不久，文[7]就指出了该方案的几个弱点并用四种密码分析方法对其进行了成功攻击。紧接着 Li Shujun 等在文[8]中分析了方案[6]容易遭受这四种攻击的原因，并给出了提高安全性的改进方案。

本文在文[8]的基础上，提出了一种改进的多级混沌加密系统。通过在系统中加入两级混沌，并引入传统密码学中的置换器，以进一步提高系统的抗攻击能力。

2 改进的多级混沌加密系统

系统模型见图1所示。

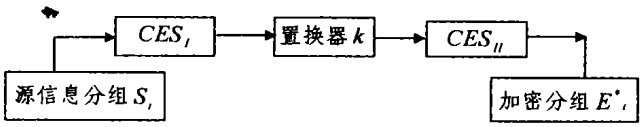


图1 多级混沌加密系统模型

系统描述如下：

1)设待加密信息为 S，按8-位为单位对其进行分组，得到 $S_1S_2\cdots S_i\cdots$。

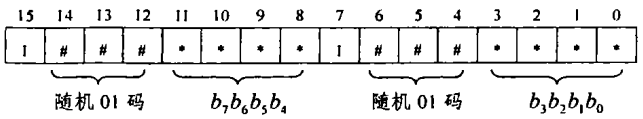
2)将分组 S_i 输入到第 I 级混沌加密系统 CES_I：(C_I, P_I, $x_{0.I}$, U_I, D, EA_I)，其中 C_I 为第 I 级混沌源，P_I 和 $x_{0.I}$ 分别为混沌系统参数和迭代初值，U_I 为某一阈值，用以产生混沌伪随机二进制序列，D 为混沌序列的取值间隔，EA_I 为加密算法，此处为异或操作。本级系统的输出为 E_i，其长度与 S_i 相同。

3)用置换器 k 对 E_i 进行置换操作，结果为 E'_i。

4)将 E'_i 输入到第 II 级混沌加密系统 CES_{II}：(C_{II}, P_{II}, $x_{0.II}$, U_{II}, EA_{II}, T_{max})，前面5个参数解释同上，最后一个参数 T_{max} 为允许的最大迭代次数。加密算法 EA_{II} 描述如下：

思想基本与文[8]类似，这里我们作了部分修改。对于 E'_1，系统从初值 $x_{0.II}$ 开始迭代，并根据阈值 U_{II} 产生二进制串 C_1，在给定的迭代次数 T_{max} ($T_{max}\leqslant 2^{15}-1$，即 $T_{max}\leqslant 32767$)之内，在 C_1 中搜索与 E'_1 匹配(即 E'_1 出现在 C_1 中)的开始位置。如果找到了，则记下从初值到达该位置的迭代次数 n_1，同时将 E'_1 编码为(n_1)，用16位双字节表示。我们称编码的第15位为标志位，则标志位肯定是0，因为 $n_1\leqslant T_{max}\leqslant 2^{15}-1$；如果没有找到，则按如下方式对 E'_1 进行编码：

记 $E'_1=b_7b_6\cdots b_2b_1b_0$，将 E'_1 按如下方式扩充成16位双字节：



其中第4、5、6、12、13、14位用随机01码填充，第7、15位均填充

*)重庆市科技计划项目。彭 军 博士研究生，主要研究方向为网络安全，混沌保密通信。张 伟 博士研究生，主要研究方向为数据挖掘，人工智能。廖晓峰 教授，博士后，主要研究方向为神经网络，混沌理论。吴中福 教授，博士生导师，主要研究方向为远程教育，网络通信。

标志1，将 E_i' 的高四位填入扩充码的第8～11位，E_i' 的低四位填入扩充码的第0～3位。

对后续的 $E_i'(i\geq 2)$ 按同样方式编码，只不过混沌系统将上次得到的迭代点作为本次初值继续迭代，而不再是从 $x_{0.II}$ 开始。

本级系统的输出为 E_i^*，其长度为16。

5）将 E_i^* 进行组合，得到最后的加密信息 $E=E_1^*E_2^*\cdots E_i^*\cdots$。

该多级混沌加密系统的密钥为：$Key=(P_I,x_{0.I},U_I,D,k,P_{II},x_{0.II},U_{II},T_{max})$，其中 k 为置换器的组号。

注意到本文提出的加密系统是一个对称的加密系统，即解密时按加密的逆过程进行操作，就可以将加密信息还原为原始信息。

3 系统实现

要实现上节中的多级混沌加密系统模型，必须确定两个混沌系统以及置换器的结构。首先我们考察两个混沌系统。

为了以示说明，混沌系统选取较简单的情形。第I级混沌系统采用文[8]中的分段线性混沌映射，第II级混沌系统为Logistic映射。它们相应的迭代方程为(1)式和(2)式。

$$x_{n+1}=\begin{cases} x_n/p & ,x_n\in[0,p), \\ (1-x_n)/(1-p) & ,x_n\in[p,1] \end{cases} \quad 0\leq x_n\leq 1,n\in Z \tag{1}$$

$$x_{n+1}=f(x_n)=1-ux_n^2,-1\leq x_n\leq 1,n\in Z \tag{2}$$

图2至图5给出了这两个混沌系统相应的分岔图、状态曲线和李亚普诺夫(Lyapunov)指数曲线。我们知道当李亚普诺夫指数大于零时，系统是混沌的。因此从李亚普诺夫指数曲线我们可以得到系统处于混沌态时的参数范围如下：当$0<p<1$时系统I是混沌的，当$1.41<u\leq 2$时系统II是混沌的。其次，置换器的构造如表1所示。

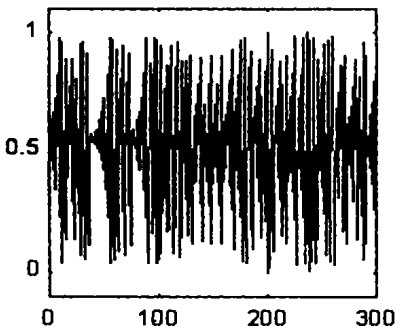


图2 系统I - 状态演化曲线

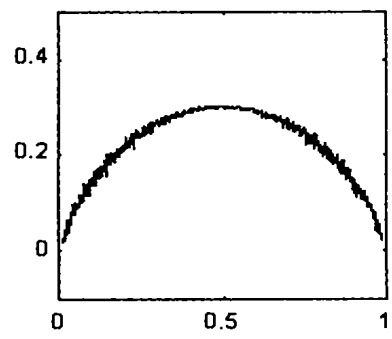


图3 系统I-李亚普诺夫指数曲线

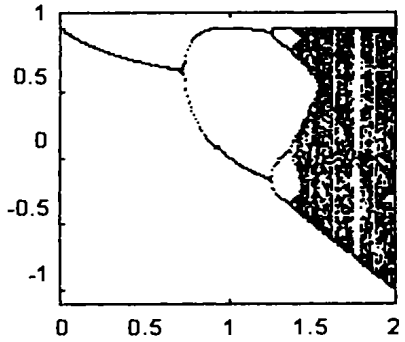


图4 系统II-分岔图

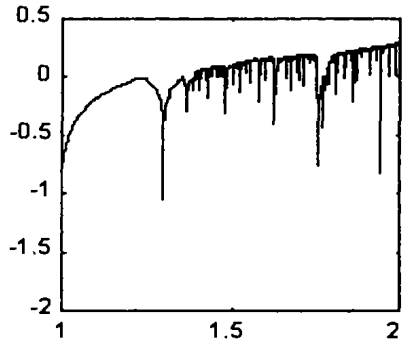


图5 系统II-李亚谱诺夫指数曲线

表1 置换器的构造

组号	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8
(1)	8	4	6	1	3	7	2	5
(2)	5	6	8	2	4	1	7	3
(3)	6	8	1	7	5	4	3	2
(4)	4	7	2	5	1	3	8	6
(5)	7	3	5	6	8	2	4	1

置换器共有5组，并且它们相同列对应的数字都不相同，目的是增大系统的安全性。加密时随机选用一组，并作为密钥组成之一。现举例说明置换器的用法：例如：第(1)组置换将信息的第8位换到第1位的位置，把第4位换到第2位的位置，把第6位换到第3位的位置，依次类推。

解密时可根据置换器的构造，计算出相应的逆置换器。设 $x_i\rightarrow i$，表示将第 x_i 位换到第 i 位的位置，则逆置换相应为 $i\rightarrow x_i$。如第(1)组的逆置换器为：4 7 5 2 8 3 6 1。

4 计算机仿真实验

我们对如下两个明文分别进行加密实验：

明文1采用文[6]中给出的明文：Cryptologyist the science of overt secret writing (cryptography), of its authorized decryption (cryptanalysis), and of the rules which are in turn intended to make that unauthorized decryption more difficult (encryption security).

明文2：A A A A A A A A A A K K K K K K K K K U U U U U U U U U U

系统 CES_I 参数为 $P=0.4,x_{0.I}=0.3,U_I=0.5,D=5$；系统 CES_{II} 参数为 $u=2.0,x_{0.II}=0.3,U_{II}=0,T_{max}=2000$。其中参数U的取值原则是使混沌二进制序列中的0和1的出现次数符合等概率分布，即

$P\{C_i=0\}=P\{C_i=1\}=1/2$

由于通过多级混沌加密系统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，我们使用图6至图9形式的二维图形来表达。

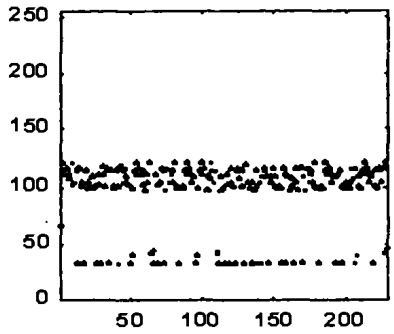


图6 明文1

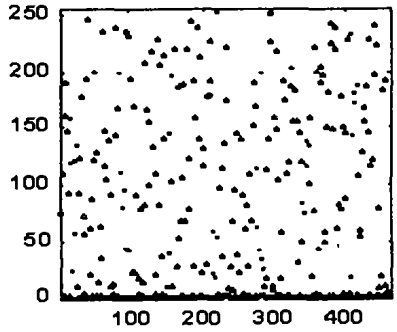


图7 密文1

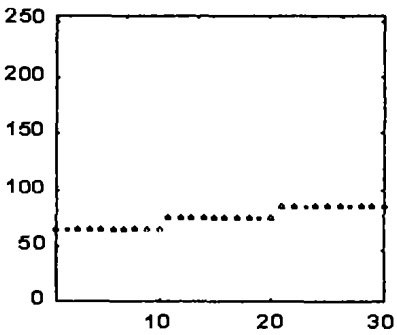


图8 明文2

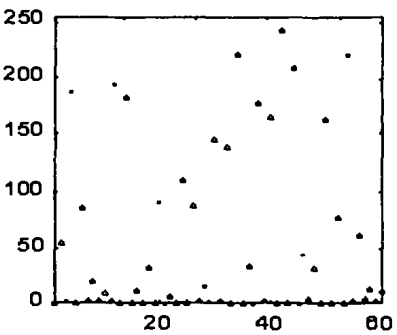


图9 密文2

其中横轴代表信息中字符出现的序号(由于加密时将一个8bit明文编码成一个16bit的密文，因此密文的横轴范围是明文的2倍)，纵轴代表对应字符的ASCII码值(范围0～255)。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。这正是我们想要达到的加密效果。

为了测试系统的可靠性，我们对密钥参数进行微小的扰动。比如$x_{0.1}=0.3+10^{-5}$，其他参数不变，则从密文1和密文2恢复出的原文如图10和图11所示。结果表明系统对参数非常敏感，微小的参数失配都将导致解密的失败，这就更进一步增强了系统的安全性和抗攻击的能力。

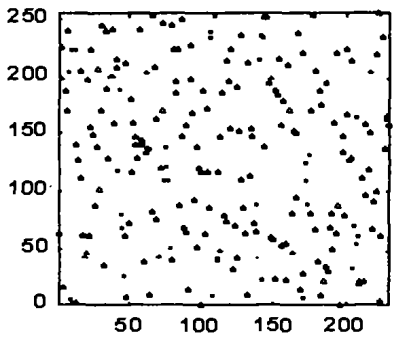


图10 参数微小失配时恢复出的明文1

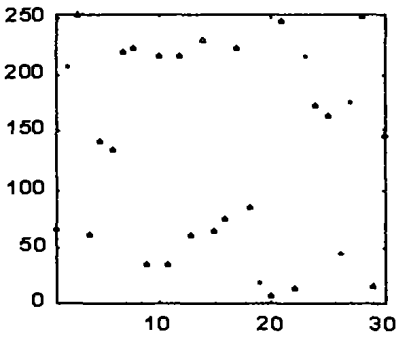


图11 参数微小失配时恢复出的明文2

讨论 香农提出了密码学中用于指导密码设计的两个基本原则[9]：扩散(diffusion)和混乱(confusion)。扩散是将明文冗余度分散到密文中使之分散开来，以便隐藏明文的统计结构；混乱用于掩盖明文和密文之间的关系。

为了改进文[8]中的系统，我们使用了两级混沌，并引入密码学中的置换技术。在第I级加密系统中用混沌序列与原文进行异或，以及第II级加密系统中使用的加密算法，都可以看作是一定意义上的混乱，而在两级加密系统之间引入简单的置换器，则实现了扩散。

由于在C_1中搜索E_i'的过程比较耗时，因此从工程的角度出发，我们将E_i'的长度固定为8比特，以加快加密速度。另外如果串E_i'的匹配搜索失败，则按照一定方式直接将E_i'扩充成16比特，并对无意义的位用随机01码进行填充，以进一步提升密码的伪装程度。

从加密模型推算，密文的长度是明文的2倍，虽然数据量增大了，但是从加密速度和密文的安全性两个方面看，都优于文[6,8]中的算法。如果要减少数据量，可采用数据压缩技术，在加密前对明文进行压缩，或者加密之后对密文进行压缩。如果加密对象是图像数据，则加密前可使用满足一定图像质量的有损压缩，但是对加密后的密文必须使用无损压缩。如可先使用Huffman编码以有效地减少密文的信息熵，再进行游程

(下转第145页)

MAC 类别集合就可以了，而不用去修改每个具有此 MAC 类别集合的文件、目录；如果系统已经不支持低级的安全敏感级别，只需将处于系统不支持的低安全级的文件、目录或进程的安全敏感级别映射成系统当前最低的安全级别即可，而无需一一修改。MAC 核心数据的初始化过程如图4-1所示。

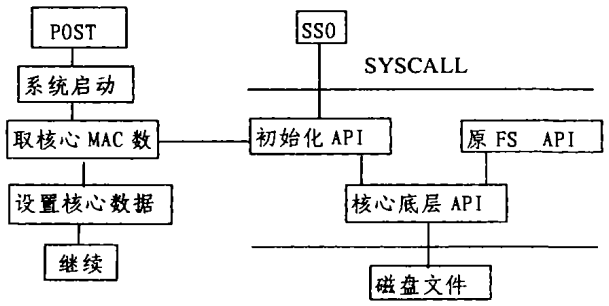


图4-1 MAC 核心数据初始化

结束语 Bell&LaPadula 模型只考虑了系统的机密性，而没有考虑数据完整性和有效性的保护。例如，如果没有自主访问控制，最低安全级别的主体可以删除其类别集合的所有数据，因此，MAC 机制一般不单独使用。另外，MAC 还不足以充分保证系统的安全性，信息泄露有可能通过间接路径（如隐蔽通道）发生。

对 LINUX 系统的安全增强，国内外已有的研究工作尚不尽人意，它们或者是兼容性不太好，或者是系统开销过大。我们的系统充分体现了与已有系统应用的兼容性，安全管理的易用性，以及系统运行的高效性，下表以系统调用 OPEN 为例，示出了 MAC 开销。目前，我们的系统已经通过了 B1安全级的初测试。进一步的工作将研究计算机网络上的多级安全策略，与基本操作系统一起构成适合于网络应用的完善的安全操作系统产品。

连续访问次数(次)	100	1000	10000
无 MAC(us)	314	2969	29676
有 MAC(us)	344	3250	32489
相对百分比(%)	109.51	109.45	109.48

环境：CPU PIII 800；Kernel linux-2.4.4

参 考 文 献

1 刘文清，刘海峰，卿斯汉. 基于 Linux 开发安全操作系统的研究. 计算机科学，2001，28 (2)

2 张志文，周明天. 用内核 ACL 增强 LINUX 的安全性. 计算机科学，2002(1)

3 Rusling D A . The Linux Kernel. January 1998

4 IEEE Draft P1003.1e. IEEE Standard Department，1997

5 Remy Card . Linux File Systems. Brueselles Oct. 1994

6 Louis-Dominique Dubeau. Ext2 file system. 1994

7 陈爱民，于康友，管海明. 计算机的安全与保密. 电子工业出版社，1992

8 Bach M J. The design of Unix Operating System. Prentice-Hall，Inc. 1986

9 Trusted Computer System Evaluation Criteria. Department of Defence U.S.A. 1985. DoD 5200.28-STD

10 Secure Computer System: Unified Exposition and Multics Interpretation. The Mitre Corporation . March 1976

11 Bell D E，LaPadula L J . Secure Computer Systems: Mathematical Foundations: [MITRE Technical Report 2547]. Volume I . March 1973

12 Bell D E . Secure computer system: A refinement of the mathematical model. Hanscom AFB. BEDford. MA. REP: [ESD-TR-73-278]. vol. 3ESD/AFSC，1973

13 Padula L J L，Bell D E. Secure Computer Systems: Mathematical Foundations and Model. M74-244，The MITRE Corporation，BEDFORD，Massachussetts，Oct. 1972

14 Mclean J . The Specification and Modelings of Computer Security. Naval Research Laboratory Washingten，D.C. 20375

15 Osborn S. Mandatory Access Control and Role-Based Access Control. Department of Computer Science The University of Western Ontario London，Ontario，Canada NCA-587

（上接第139页）

长度编码(Run length code)等。之所以要使用无损压缩，原因在于从有误差的密文很难正确地恢复出原文。

另外，为了使加密系统更加难以破译，还可以采用超混沌系统或有时延的混沌系统来生成随机序列，由于它们有多个正的李亚普诺夫指数，导致序列更加难以预测。

总之，混沌理论用于信息加密是一个很有应用前景的研究领域，如何将传统的加密算法、思想与混沌理论相结合，仍然是目前主要的研究方向，如混沌密码体制、混沌数字水印等。如文[10]对混沌映射作为流加密算法进行了较为深入的研究，具有一定的指导作用。

参 考 文 献

1 Pecora L M，Carroll T L. Synchronization in chaotic systems. Phys. Rev. Lett，1990，64(2)：821～824

2 Morgül Ö，Feki M. A chaotic masking scheme by using synchronized chaotic systems. Phys. Lett，1999，A 251 (3)：169～176

3 Liao T-L，Tsai S-H. Adaptive synchronization of chaotic systems and its application to secure communications. Chaos，Solitons & Fractals，2000，11 (9)：1387～1396

4 Murali K. Heterogeneous chaotic systems based cryptography. Phys. Lett，2000，A 272 (3)：184～192

5 Baptista M S. Cryptography with chaos. Phys. Lett，1998，A 240 (1-2)：50～54

6 Alvarez E，et al. New approach to chaotic encryption. Phys. Lett，1999，A 263 (4-6)：373～375

7 Alvarez G，et al. Cryptanalysis of a chaotic encryption system. Phys. Lett，2000，A 276 (1-4)：191～196

8 Li Shujun，Mou Xuanqin，Cai Yuanlong. Improving security of a chaotic encryption approach. Phys. Lett，2001，A 290 (3-4)：127～133

9 Schneier B. [美] 著，吴世忠，祝世雄，张文政等译. 应用密码学——协议、算法与 C 源程序. 机械工业出版社，2000

10 Kocarev L，Jakimoski G. Logistic map as a block encryption algorithm. Phys. Lett，2001，A 289 (4-5)：199～206