基于多层密钥的混沌映射保密通信系统

包浩明,朱义胜
(大连海事大学信息科学技术学院,辽宁大连 116026)

摘 要: 针对低维映射安全性的弱点,提出一种混沌遮掩保密通信的改进方案.该方案利用分层的两级密钥管理体制,将加密用的混沌序列改为动态参数,在提高密文安全性能的同时,不降低加密速度和传输速度.论证表明,低维映射仍有很好的应用潜力.

关键词: 混沌映射; 密钥; 攻击; 保密通信
中图分类号: TN918 文献标识码: A 文章编号: 0372-2112 (2009) 06-1222-04

A Chaotic Mapping Secure Communication System Based on Hierarchical Key

BAO Hao-ming, ZHU Yi-sheng
(*Information science technology college, Dalian Maritime Univ, Dalian, Liaoning* 116026, *China*)

Abstract: A improved secure communication method based on chaotic masking is proposed to overcome weakness of low dimensional chaotic map. In the scheme the chaotic time series with dynamic parameters for encryption based on hierarchical two-level key management is designed. The performance of the encryption speed and transmission speed is not lowered while the security of ciphertext is obtained. The results showed that low dimensional chaotic map has great potential of secure communication.

Key words: chaotic map; key; attack; secure communication

1 引言

近年来混沌理论的应用逐渐成为信息与控制领域中的热点问题之一.利用混沌动力学的类随机特性进行保密通信已经开展了许多研究工作,迄今为止已经提出并发展了多种保密通信方式:混沌遮掩、混沌调制、混沌开关、混沌编码等.

自Oppenheim等人提出混沌遮掩保密通信方式后,针对这一方式研究设计的具体系统越来越多,多数混沌遮掩保密通信方式都是建立在Lorenz系统族等连续混沌动力学系统基础之上[1,2].为了拓展系统模式的类型且更适用于多媒体数字通信,以离散混沌映射为基础的保密通信系统应用逐渐增多[3~8],它和传统密码学的结合更加紧密.

和连续混沌系统类似,离散混沌系统迭代轨迹对初始条件有强烈的敏感性,具有良好的类随机特性.但是,低维离散混沌映射构成的保密通信系统也同样存在着安全性能不是非常完美的问题,人们曾经提出的若干系统容易被神经网络拟合、重构预测等方法实施攻击[9].

为了提高离散混沌映射保密通信系统的安全性,本文提出了一种基于动态参数映射的改进方案,该方法明显提高了安全性能,能抵御多种攻击方法.

2 一些混沌保密通信系统的安全性弱点

一类离散映射混沌遮掩保密通信系统[7],其加密方式可表述为如下Logistic映射:

$$x_{n+1}=[\mu x_n(1-x_n)+ks_n]\bmod \quad (1)$$

其中,$x_{n+1}, x_n\in\mathbf{R}$, $n\in\mathbf{Z}$, $3.58<\mu<4$, $k<0.02$, $n=0, 1, 2\cdots$.上式是一维可微映射,x_n和s_n分别为系统状态和外输入,k为嵌入系数,μ为常系数,模运算可使系统状态有界.虽然该映射包含了模运算和外加输入项,但计算表明,只要系数μ满足一定条件,它在Li-Yorke意义下是混沌的,有一个正的Lyapunov指数.

此类系统构造简单,加解密速度快,和更早的映射加密方式相比,在安全性上有一定改进,但也存在固有的弱点.

理论上认为,连续域上的混沌映射,其周期点测度为零.但将这个混沌映射数字化之后,情形就不一样了[10].混沌映射保密通信系统是基于数字电路系统或软件实现的,由于受到有限精度的影响,混沌动力学

收稿日期: 2007-07-30; 修回日期: 2009-01-20
基金项目: 国家自然科学基金资助项目(No. 60671061)

特征难以保持, 映射迭代退化为有限状态机, 此时的迭代轨道最终都会进入一个有限的周期中去, 混沌系统特有的非周期性和遍历性均被破坏. 这种数字化的混沌映射严格地讲不再是混沌的, 它的周期性对保密通信的安全性来说是不利的.

尽管式(1)中将明文信号也嵌入了动力学体系中并施以模运算, 可以确认这种嵌入运算对减少混沌退化、抵御攻击有着积极的外扰动作用, 但其作用比较有限, 在超快计算机下系统被搜索攻击的危险性仍然存在.

虽然 Logistic 混沌轨道表现出复杂的随机特征, 但它的状态是经过方程演化迭代而来的, 必然有内在确定约束, 再加上低维映射形式简单, 只有一个正 Lyapunov 指数. 在这种情况下, 很容易受到攻击, 尤其是在选择/已知明文攻击下更加脆弱. 式(1)表述的映射保密系统的安全性很大程度上决定于明文的迭代嵌入, 选择明文攻击时敌方可能得到前后相邻的两个 s_n 归零的状态值 x_m, x_{m+1}, 根据 Kerckhoff 准则, 安全性不应依赖于密码体制构造, 因而 $\frac{x_{m+1}}{x_m(1-x_m)}$ 可被轻易获取. 由此还可推知, 该加密方案不能用于有语音间歇期的话音实时保密通信系统中. 即使在唯密文攻击下, 只要能截获连续性大数据量密文, 通过基于相空间的重构预测等方法仍有可能攻破系统.

3　一种基于多层密钥的混沌映射保密通信系统的设计

为了解决上述安全性上的问题, 我们结合现代保密通信系统的设计原则, 从原有系统的弱点出发, 将映射的固定参数改为动态参数, 在此基础上设计了改进的Logistic 映射混沌保密通信系统如图 1 所示, 该系统不仅继承了原系统结构简单、加密成本低、加密速度快等优点, 同时在抵御多种形式的攻击上有明显优势.

该系统分为发送端加密部分和接收端解密两大部分. 发送端加密部分按照“多层密钥”的思想分为两层(图 2), 直接加密明文 s_n 的底层 Logistic 映射, 其初值和参数(x_0, μ)作为工作密钥是动态变化的, 受上层管理与保护. 上层 Logistic 映射的初值和参数(y_0, λ)作为主密钥, 控制并自动生成底层工作密钥. 若整体算法选择得当, 底层工作密钥更新速度快, 随机性好, 可以趋近 Shannon 理论中“一次一密”的完善加密要求. 上层主密钥相对于攻击方来说是间接的, 因而也有良好的安全性. 接收端解密部分同理.

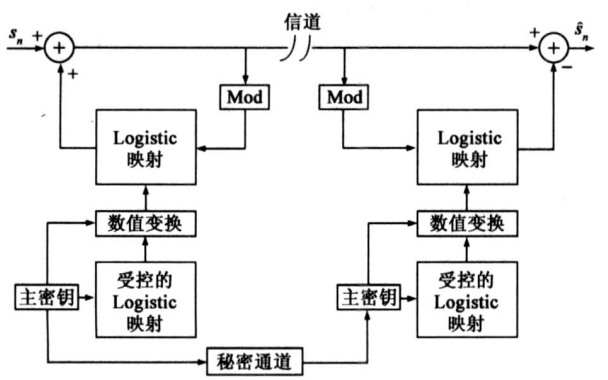

图1　改进的Logistic映射混沌保密通信系统

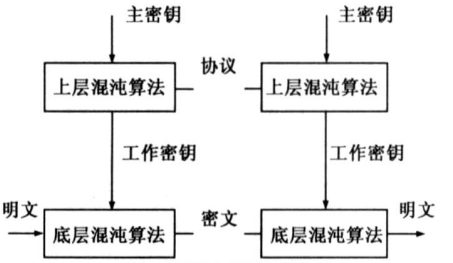

图2　两层密钥管理体系

本系统各部分分述如下:

(1)上层混沌算法采用受控的 Logistic 映射

$$y_{n+1} = \lambda y_n(1-y_n) + u_n \qquad (2)$$

式中

$$u_n = (\sigma y_n) \bmod (\varepsilon) \qquad (3)$$

u_n 为状态反馈输入, σ, ε为两个正系数, 3.59< λ< 4, 7< σ< 14, 0< ε< 1- 0.25λ. 在一定条件下式(2)所表示系统, 其 Lyapunov 指数明显提高[10]. 这样, 可以增大主密钥空间, 改善密钥强度. 由于系数 σ能引起混沌行为的变化, 在系统中可以将主密钥由(y_0, λ)改设为(y_0, λ, σ).

(2)上层对底层的控制需要通过数值变换来实现. 底层工作密钥之一是 Logistic 映射的系数 μ^*, 在上层控制规律作用下是动态的,

$$\mu^* = \frac{0.41[y_n - 0.0625\lambda^2(4-\lambda)]}{0.25\lambda - 0.0625\lambda^2(4-\lambda)} + 3.59 \qquad (4)$$

映射的伸长与折叠作用导致迭代区间为(0.0625 λ²(4-λ), 0.25λ), 故有上式. 另一个工作密钥是底层映射的初值, 它在变化的情况下已经失去了原始含义, 可直接将上层的控制作用定为对状态值的控制, 通过仿真估算, 其最佳值设为

$$x_n^* = |0.65 \cdot (x_n - 0.9y_n)|, \bmod(0.25\mu^*) \qquad (5)$$

其中, x_n^* 是受控的状态. 每个时钟到来时状态值 x_n 在上层映射作用下有一个“随机跃迁”. 为充分利用底层映射, 每隔 N 个时钟周期才开启一次上层对 μ 的控制, N 不宜过大, 否则会削弱整个系统的安全性(见图 3).

(3)底层混沌算法采用 Logistic 映射对明文进行遮掩加密, 加密方式可以表示

$$x_{n+1} = [\mu^* x_n^* (1-x_n^*) + ks_n]; \bmod(0.25\mu^*) \qquad (6)$$

式中, μ^*, x_n^* 分别由(4)、(5)得到, s_n 为采样的明文信

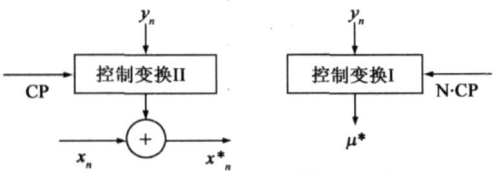

图3 上层对底层的控制变换

号. 加密过程见图 1, 映射每迭代一次加密一个明文采样数据, 明文序列 s_n 也被嵌入迭代之中. 系统采用算术加运算进行遮掩加密, 因此明文只能是小功率信号.

(4) 传送到信道的信号为

$$e_n = \mu^* x^*_n (1 - x^*_n) + ks_n \qquad (7)$$

解密部分和加密部分结构相同, 在底层也含有一个等效延时器, 由于明文信号参与映射迭代, 所以接收到的信号同前一次信号迭代后的数值相减, 才可恢复所传输的明文信号. 详细分析从略.

本系统可用软件实现, 也可用高精度的逻辑器件构成. 既可用于数字信道加密, 也可用于网络协议加密.

4 系统安全性能的分析

数字混沌映射的短周期效应对保密通信系统的安全性来说是非常不利的, 如何克服这种不利因素并获得所希望的理想结果, 目前尚没有严格的理论工具指导这方面的计算. 本文方案能明显提高系统的非周期特性, 对此只能进行简略的半定量分析. 在最简单的情况下, 仅仅考虑对 μ^* 的控制作用, 当底层映射 x_n 到达周期循环状态时, 只有上层映射 y_n 也达到周期循环状态, 整个系统才能开始重复循环. 系统周期的数量级为 $T_{Xn} \cdot T_{Yn}$, 其中 T_{Xn}, T_{Yn} 分别为两个映射的独立周期.

目前对混沌保密通信系统的攻击方法主要还是基于混沌本身动力学特征的, 如相空间重构预测、回归映象等. 采用单层固定密钥的方案, 对加密体制构造的改进最终都反映为奇怪吸引子空间图象更复杂一些, 但密文序列仍然按照特定规律完整演化形成混沌轨道. 本文提出的基于多层密钥的动态参数加密方案, 就信道中传输的密文序列而言, 随着底层工作密钥的随机性变化, 并没有固定的自映射迭代规律. 其特点可用图 4 来简要说明. 在上层混沌映射的作用下, 密文序列的状态值不再属于某一固定映射迭代轨道, 而是在一族映射的各个轨道间不断跃迁, 跃迁是受上层混沌算法控制的随机跃迁, 攻击者截获密文序列后很难察觉并掌握这种跃迁规律. 换言之, 密文序列可以看成在无数个 Logistic 映射及其无数个轨道上随机取值组合而成, 它的相邻状态值关联性极小, 很难通过预测重构估计出主密钥.

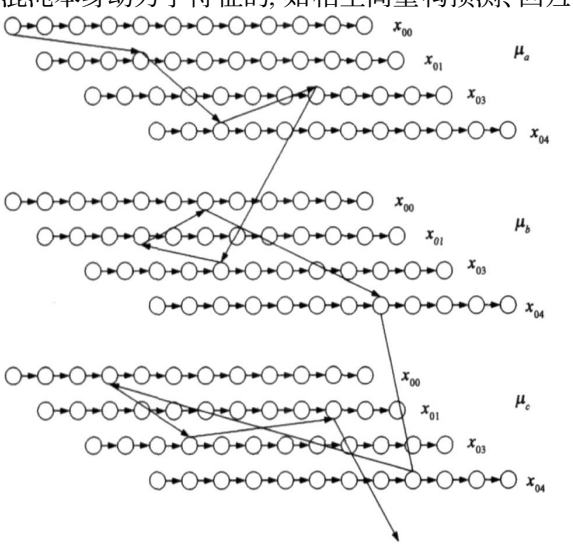

图4 密文序列状态值的轨道跃迁

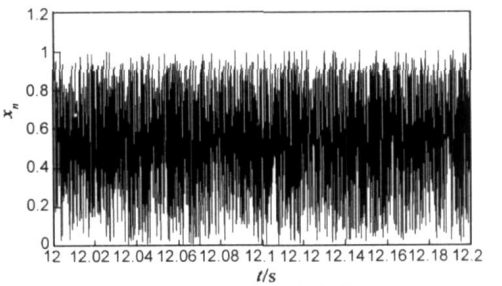

图5 密文序列时域波形

对本文方案进行仿真, 系统设定如下: 系统采样时间为 $T = 0.0001$s; 上层混沌算法中, $\lambda = 3.73$, $\sigma = 10$, $\varepsilon = 0.05$, $y_0 = 0.5$; 数值变换环节中, $N = 3$; 底层混沌算法中, $s_n = 1 + 0.5\sin(0.0002\pi n)$, $k = 0.005$. 由图 5 的信道密文序列时域波形可见, 直观遮掩效果良好. 图 6、7 分别为上层映射和底层映射的相图; 图 8 为一般 Logistic 映射本身的相图, 图 9 为式 (1) 表示的单层密钥加密方式的相图, 图 8、9 中, 初值 $x_0 = 0.2$, 系数 $\mu = 4$, 其余同上. 图 6 和图 8 对照可看出, 上层映射相比于未受控的 Logistic 映射混沌行为显著增强, 有益于各层密钥的保护. 图 7 和图 9 对照可发现, 底层映射密文序列的相图中点分布十分混乱, 对攻击者所用的各种预测手段来说截获这样的序列值没有价值.

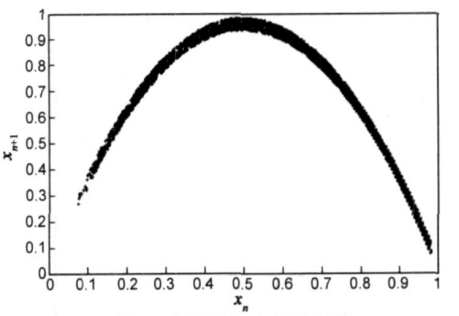

图6 上层混沌映射的相图

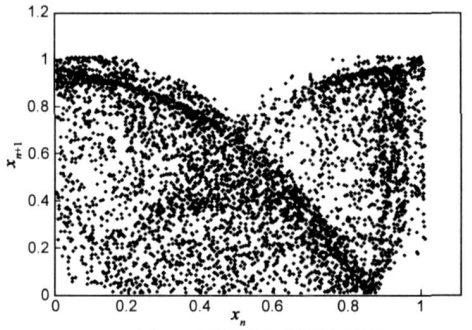

图7　底层混沌映射的相图

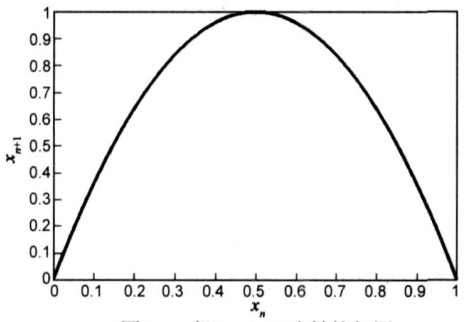

图8　一般Logistic映射的相图

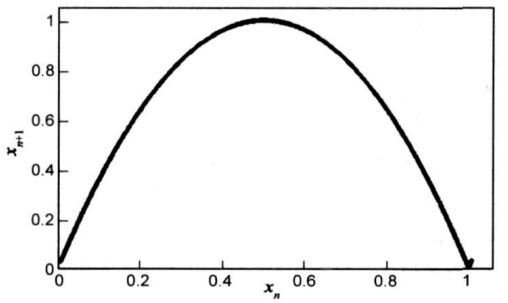

图9　单层密钥加密方式的相图

5　结语

在多层密钥的管理体制下, 基于动态参数的思想建立混沌映射保密通信系统, 可使密文序列具有相当高的安全性, 这可以使低维混沌映射在通信安全领域中也能有广泛的应用. 方案中虽以 Logistic 映射为基础构成系统, 但也适用于其他映射类型.

本文提出的系统方案在注重安全性的同时, 针对每个明文数据仍然保持一次加密运算, 没有采用高次数反复迭代来增强复杂性, 因此加解密速度很快, 加密成本较低, 符合保密技术的实用化要求.

参考文献:

[1] Cuomo K M, Oppenheim A V, Strogatz S H. Synchronization of Lorenz-based chaotic circuits with application to communications[J]. IEEE Trans CASⅡ 1993, 40(10): 626– 632.

[2] Liao T, Huang N. An observer-based approach for chaotic synchronization with applications to secure communications[J]. IEEE Trans Circuits Systs I, 1996, 46(9): 1144– 1150.

[3] Kocarev L. Chaos-based cryptography: A brief overview[J]. IEEE Trans CAS I, 2001, 1(3): 6– 21.

[4] Kocarev L. Jakimoski G. Pseudorandom bits generated by chaotic maps[J]. IEEE Trans CAS I, 2003, 50(1): 123– 126.

[5] Huang F, Guan Z H. Cryptosystem using chaotic keys[J]. Chaos, Solitons and Fractals, 2005, 23(3): 851– 855.

[6] Pareek N K, Patidar V and Sud K K. Image encryption using chaotic logistic map[J]. Image and Vision Computing , 2006, 9(1): 926– 934.

[7] 吴敏, 丘水生. 一个混沌保密通信方案的改进. 通信技术, 2003, (1): 103– 105.
Min W, Shui-sheng Q. Improvement of a chaos-based secure communication scheme[J]. CommunicationsTechnology. 2003, (1): 103– 105. (in Chinese)

[8] 陈帅, 钟先信. 基于离散数字混沌序列的图像加密. 电子与信息学报, 2007, 4(4): 898– 900.
Shuai C, Xian-xin Z. Image encryption through discrete digital chaotic sequence[J]. Journal of Electronics & Information Technology, 2007, 4(4): 898– 900. (in Chinese)

[9] Short K M. Steps toward unmasking secure communication[J]. Int J Bifurc Chaos, 1994, 4(4): 959– 977.

[10] 陈关荣, 汪小帆. 动力系统的混沌化——理论、方法与应用[M]. 上海: 上海交通大学出版社, 2006.

作者简介:

包浩明　男, 1967 年生于呼和浩特市, 大连海事大学在读博士生. 主要研究方向为保密通信与信号处理.

朱义胜　男, 1945 年生, 大连海事大学教授, 博士生导师. 主要研究方向为电路理论、宽带匹配和数字信号处理.

E-mail: yszhu@dlmu.edu.cn