第 26 卷第 7 期 电子与信息学报 Vol.26No.7
2004 年 7 月 Journal of Electronics & Information Technology July 2004

提高混沌同步保密通信安全性的设计方案研究 [1]

翁贻方 翁莉娟 张 蕾*

(北京工商大学信息工程学院 北京 100037)
*(山东胜利职业学院电子工程系 山东 257097)

摘 要: 在分析几种典型的混沌同步保密通信方案及针对混沌同步保密通信的分析破译方法的基础上，研究了一个新的基于 Lorenz 方程的主动－被动同步保密通信方案，其特点是具有动态密钥，从而对上述攻击方法具有抗破译能力．计算机仿真实验和安全性测试分析结果均表明，该方案的同步效果好、安全性高，达到用基于相空间重构、基于混沌同步的分析方法难以破译的效果．

关键词: 混沌，保密通信，同步，破译，安全性
中图分类号: TN918.8 **文献标识码**: A **文章编号**: 1009-5896(2004)07-1057-07

Research on Chaotic Synchronized Secure Communication Schemes to Improve Security

Weng Yi-fang Weng Li-juan Zhang Lei*

(*Institute of Info. Eng., Beijing Technology and Business Univ., Beijing* 100037, *China*)

(*Dept. of Electrical Eng., Shandong Shenli Vocational College, Shandong* 257097, *China*)

Abstract The security of several typical chaotic synchronized secure communication schemes , as well as the respective unmasking methods are studied to find the way to improve the security. A new secure communication scheme based on active-passive decomposition using parameters perturbation technique, which makes it has a kind of dynamic secrete key, is analyzed in this paper. The dynamic secrete key contributes to the capacity against the unmasking methods. Computer simulation and security test results demonstrate that the scheme is high in security and good in synchronization properties , and that it is safe to the attack of the unmasking methods mentioned in this paper.

Key words Chaos, Secure communication, Synchronization, Unmasking, Security

1 引言

混沌同步保密通信作为一种新的信息安全传输、安全存储技术正在成为信息安全领域的一个研究热点． 20 世纪 90 年代以来，混沌同步保密通信的研究取得了丰硕的成果，已经开始从理论研究、实验研究向实际应用发展．正像密码学和密码分析学是伴随发展的一样，在混沌同步保密通信的研究不断深入的同时，针对它的分析破译方法相继出现，使混沌同步保密通信的发展和应用面临挑战．

本文从研究混沌同步保密通信的安全性出发，比较不同方案的安全性．根据分析破译方法的特点，研究提高抗破译能力的途径，使所设计的混沌同步保密通信方案的安全性满足实际应用的要求．

2 混沌同步保密通信的安全性

混沌系统的特点是对参数和初始状态的敏感性、状态的不可预估、状态的似噪声特性、自

[1] 2002-11-21 收到， 2003-10-28 改回
北京市自然科学基金 (4002004) 、北京市教育委员会科技发展计划 (00KJ048) 资助课题

同步等. 利用混沌系统的上述特点可以实现混沌同步保密通信. 发送端和接收端分别用两个结构相同的混沌系统产生混沌信号. 采用某种同步方法, 可使发送和接收端保持同步, 这种自同步特性可实现实时通信而不必外加同步信号. 目前有多种混沌同步方法 [1,2], 用于保密通信的主要有驱动-响应同步、主动-被动同步、单向耦合同步、外部噪声驱动同步等. 前 2 种同步方法的实质是用发送端的混沌信号驱动接收端的混沌系统, 这相当于一种强迫作用, 不断地把包含发送端混沌系统当前状态的信息输入到接收端混沌系统中, 迫使后者的状态和前者在时间上同步.

在混沌同步保密通信系统中, 信道上传输的是混沌信号. 利用混沌信号的似噪声特性, 对信息信号进行调制, 常见的如混沌掩盖 (又称小信号调制), 是将信息信号调制到混沌信号上. 由于接收系统与发送系统同步, 容易得到解调信号, 解调精度与同步误差有关.

混沌同步保密通信系统的安全性与混沌系统对参数和初始状态的敏感性直接有关, 敏感性高的系统, 使破译者难以猜试出混沌系统的参数和初始状态, 从而达到保密的目的. 对于混沌掩盖的保密通信方案, 混沌变量的随机性、调制信号与被调制信号的功率之比都是决定的因素.

本文用参数或初始状态小数点后的位数表示敏感程度. 以 Lorenz 系统为例, 在非同步方式下, 系统对参数、初始状态小数点后第 14 位敏感, 即两个同构的 Lorenz 系统中的某个参数或初始状态在小数点后 14 位有 $\pm 1 \times 10^{-14}$ 的差异时, 经过一个瞬态过程, 两个系统的对应状态将发生分离. 但是, 工作在同步方式下 (以主动-被动同步方法 [1] 为例), 差异达到小数点前一位, 即 ± 1 时, 两个系统的状态才发生分离. 可见, 工作在某种同步方式下的混沌系统对参数、初始状态变得不敏感. 因此, 在一般的混沌同步保密通信系统中, 实际上依赖于参数或初始状态敏感性的安全性容易被穷举攻击破译.

2.1 混沌同步保密通信的破译方法

混沌同步保密通信的安全性除了因参数敏感性下降容易受到穷举攻击外, 专门针对这种保密通信的破译方法的出现使它的安全性受到更大的威胁. 这类破译方法根据混沌动力学系统的特点, 并应用信号处理技术, 采用信号提取、滤波、参数估计、状态预测等方法, 以下是较有代表性的 3 种.

2.1.1 基于相空间重构的攻击方法[3,4] 根据混沌系统的确定性的特点, 因为小能量的加性噪声不改变相空间的基本几何结构, 从信道上截获一定数量的加密信号, 用这些信号进行高维时延相空间重构, 应用信号处理技术, 进行建模、预测 (或得到) 混沌状态, 从而恢复被加密信号. 这种方法可有效破译混沌掩盖的保密通信. 此外, 混沌掩盖的保密通信还可用噪声削减技术破译, 因为叠加在混沌信号上的信息信号的能量和混沌信号相比较小, 所以可把信息信号视为混沌信号的噪声, 去掉噪声就得到混沌信号. 类似地还可用奇异值分解 (SVD) 技术降噪、总体最小二乘法 (TLS) 技术等达到相同的目的.

2.1.2 基于回归映射 (return map) 的分析方法[5,6] 它是专门针对一类混沌参数调制同步保密通信方案的, 其依据是由混沌信号流构成的回归映射曲线规则.

2.1.3 基于混沌同步的分析方法[7] 它的依据是两个存在耦合关系的同构混沌系统即使在参数存在差异的情况下也会产生广义同步现象 (generalized synchronization). 广义同步是指在同构系统存在参数偏差的情况下, 同步误差维持在一定的范围之内而不发散, 并且参数偏差与平均同步误差间具有平滑的关系曲线. 假设攻击者已截获一定数量的混沌信号序列, 并已知混沌系统的结构, 但不知道系统参数. 攻击者可以构造一个与原系统同构的混沌系统, 并用得到的混沌序列来驱动这个同构系统, 使之达到广义同步. 然后根据误差函数的极小值用逐步逼近的方法来估计混沌系统的参数. 对于混沌掩盖保密通信, 用这一方法估计得到的混沌系统参数较为精确.

2.2 现有混沌同步保密通信方案的安全性分析

驱动-响应同步和单向耦合同步保密通信方案均采用小信号调制 (混沌掩盖) 的方法, 要求信息信号的能量小于混沌信号的能量, 为保证解调精度, 一般是 1/10 或更小. 针对这一特点,

用基于相空间重构的攻击方法、基于混沌同步的分析方法、噪声削减技术破译都是有效的，因此安全性差.

参数调制同步保密通信方案容易用基于回归映射的方法、基于混沌同步的方法破译，安全性不能满足实际要求.

主动 -被动同步解调 (Active-passive decomposition) 保密通信方案对经过处理的信息信号进行调制，与驱动 -响应同步混沌掩盖保密通信方案不同的是： (1) 这种方案不是依靠信息信号和混沌信号能量的比值来保证解密精度，而是用一个混沌信号同时驱动发送和接收端的混沌系统，使其具有高的同步精度，从而保证解调精度； (2) 可灵活地设计信息信号和混沌信号的调制函数，将经过调制的信息信号与混沌信号叠加，而不是直接进行混沌掩盖. 因此，即使用基于相空间重构的攻击方法或噪声削减技术得到被调制的信号，也不是原始的被加密信号. 这就增加了破译的难度. 可见这一方法的安全性好于驱动 - 响应同步混沌掩盖保密通信，但也极易受到基于混沌同步的分析方法的攻击，只是由于信息信号和混沌信号相比有较大能量，用基于混沌同步的分析方法估计参数的精确度较低.

外部噪声驱动同步保密通信方案通过混合多个混沌系统的混沌变量产生的信号更接近随机噪声，用其同时驱动发送和接收端系统使两者达到同步. 由于系统受到外部噪声的摄动，混沌系统的状态偏离原来的轨迹，使基于相空间重构、基于混沌同步的分析方法失效，或难以得到好的破译效果，安全性好. 但是要实现自同步，发送和接收端只能用一个噪声源，需在信道上同时传输被加密信号和噪声信号，使方案的实现受到限制.

以上分析表明，混沌掩盖的信号调制方式是不安全的，参数调制同步可用基于回归映射的分析破译，外部噪声驱动同步方案可实现性受到限制，主动 -被动同步保密通信具有较好的安全性和可实现性，可以此为基础设计出安全系数高的混沌同步保密通信方案.

3 具有动态密钥的主动 -被动同步保密通信方案研究

本文研究了一个新的基于 Lorenz 方程的、具有动态密钥的主动 -被动同步保密通信方案 [8,9] 的安全性. 该方案的设计思想是在使保密通信具有高的同步精度的前提下，针对攻击技术的特点，提出对策. 具体是： (1) 提取和放大混沌变量中对参数和初始状态敏感的信息段，一般取混沌变量在小数点后若干位的数据，获得一个新的、随机性和敏感性均优良的变量，用该变量对信息信号进行调制，已取得提高保密通信系统对参数敏感性的效果； (2) 用对参数敏感的变量对混沌系统的参数进行干扰，使其在基础值附近随机摄动 (参数的基础值是指使系统处于混沌状态的值)，从而破坏基于混沌同步的分析方法需截获一定数量的混沌信号序列的条件.

以 Lorenz 系统为例 [8,9]，用经处理的微小混沌变量 x_e 对系统的 3 个参数 α, γ, ρ 进行反馈微扰. 发送端混沌系统的方程为

$$\begin{aligned} \dot{x}_1 &= \alpha_p x_1 + s(t) \\ \dot{x}_2 &= -x_1 x_3 + \gamma_p x_1 - x_2 \\ \dot{x}_3 &= x_1 x_2 - \rho_p x_3 \end{aligned} \tag{1}$$

其中 $s(t) = 10x_2 + m(t)x_e$ 为信道上传输的信号； $\alpha_p = \alpha + k_1 x_e$, $\gamma_p = \gamma + k_1 x_e$, $\rho_p = \rho + k_1 x_e$ 是通过变量反馈实现参数微扰的算式； $x_e = k_2 x_1 - \mathrm{fix}(k_2 x_1)$ 是从变量 x_1 中提取小数点某位以后的信息 (其中 $\mathrm{fix}(\cdot)$ 表示取整运算)，同时用作对信息信号 $m(t)$ 的调制，和对系统参数的反馈微扰； k_1, k_2 分别是微扰系数和放大系数，分别取 $k_1 = 1.5$, $k_2 = 80$. 接收端混沌系统的方程为

$$\begin{aligned} \dot{y}_1 &= \alpha_{rp} y_1 + s(t) \\ \dot{y}_2 &= -y_1 y_3 + \gamma_{rp} y_1 - y_2 \\ \dot{y}_3 &= y_1 y_2 - \rho_{rp} y_3 \end{aligned} \tag{2}$$

其中 $\alpha_{rp}=\alpha+k_1y_e$， $\gamma_{rp}=\gamma+k_1y_e$， $\rho_{rp}=\rho+k_1y_e$ ，变量 y_e 的提取处理方法和发送端相同，即 $y_e=k_2y_1-\mathrm{fix}(k_2y_1)$.

接收端的解密信号为

$$m_r(t)=[s(t)-10y_2]/y_e \tag{3}$$

此方案的结构可用图 1 示意. 如果接收端系统和发送端同步，则有 $y_e=x_e$ ，能保证参数反馈微扰的作用相同，此时解密得到的恢复信号 $m_r(t)$ 与 $m(t)$ 相等.

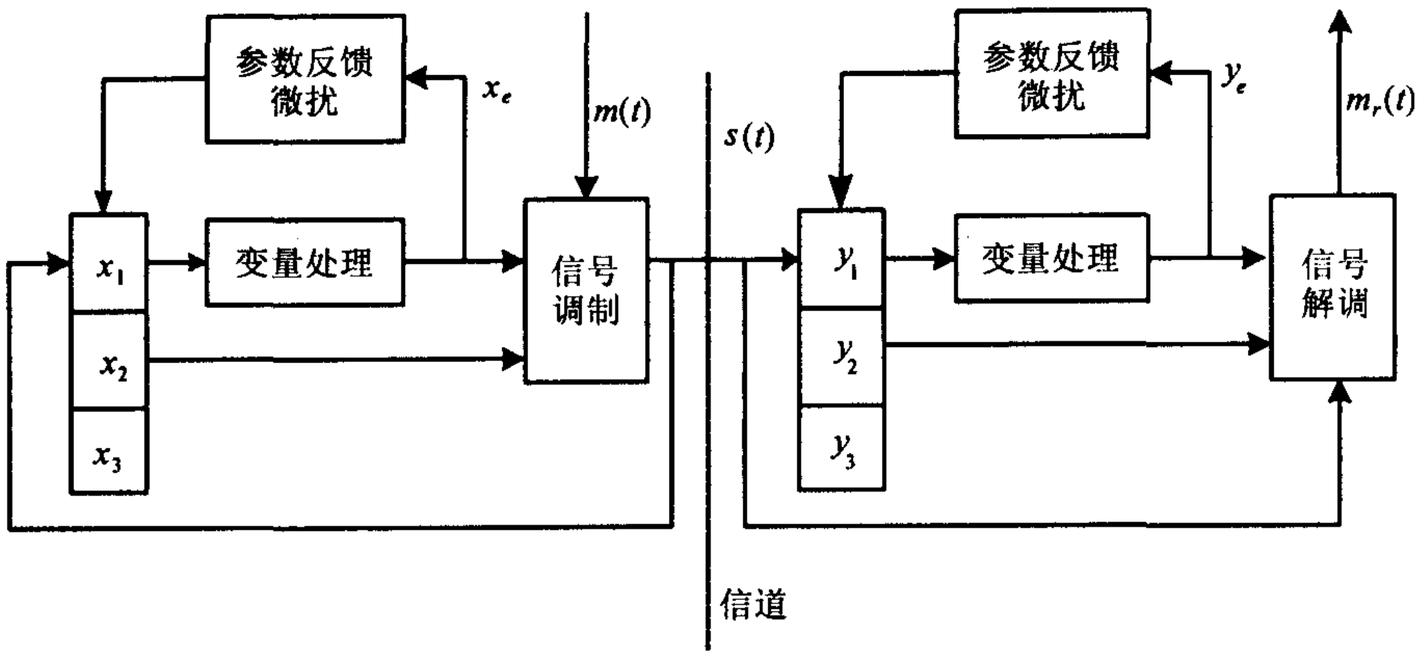


图 1 具有动态密钥的保密通信方案结构示意

3.1 具有动态密钥的混沌同步保密通信系统的同步性分析

混沌同步的定义：考虑 n 维自治动力学系统：

$$\dot{\boldsymbol{x}}(t)=f(\boldsymbol{x}),\qquad \boldsymbol{x}(t_o)=\boldsymbol{x}^o \tag{4}$$

式中 $\boldsymbol{x}$ 为 n 维状态变量 $\boldsymbol{x}=[x_1,x_2,x_3,\cdots,x_n]$； $f(\boldsymbol{x})$ 为 n 维向量函数，各元素 $f_1(x),f_2(x),\cdots,f_n(x)$ 是 $\boldsymbol{x}$ 的有界的、连续可微的单值函数； t_o 是起始时刻； $\boldsymbol{x}^o$ 是状态向量 $\boldsymbol{x}$ 的初始状态.

将式 (4) 称为驱动系统，它的同构系统式 (5) 称为响应系统：

$$\dot{\boldsymbol{y}}(t)=f(\boldsymbol{y}),\qquad \boldsymbol{y}(t_o)=\boldsymbol{y}^o \tag{5}$$

式中 $\boldsymbol{y}$ 为 n 维状态变量 $\boldsymbol{y}=[y_1,y_2,y_3,\cdots,y_n]$； $\boldsymbol{y}^o$ 是状态向量 $\boldsymbol{y}$ 的初始状态.

状态向量 $\boldsymbol{x},\boldsymbol{y}\in R^n$. 令 $\boldsymbol{x}(t)=\psi(t;t_o,\boldsymbol{x}^o)$ 和 $\boldsymbol{y}(t)=\psi(t;t_o,\boldsymbol{y}^o)$ 分别是驱动系统和响应系统的解，并满足 Lipschitz 条件. 当存在一个 R^n 的子集 $D(t_o)$ 时，使得状态向量的初始值 $\boldsymbol{x}^o$, $\boldsymbol{y}^o\in D(t_o)$ ，当 $t\to\infty$ 时，若存在

$$e(t)\equiv\|x(t)-y(t)\|\to 0,\quad t>t_o \tag{6}$$

则称响应系统式 (5) 与驱动系统式 (4) 达到同步. 式中 $\|x(t)-y(t)\|=[(x_1-y_1)^2+(x_2-y_2)^2+\cdots+(x_n-y_n)^2]^{\frac{1}{2}}$ ，是欧几里德范数.

若 $D(t_o)\subset R^n$ ，称为全局同步；若是 R^n 的一个子集，称为局部同步， $D(t_o)$ 为同步区域.

用李雅普诺夫稳定性分析方法说明具有动态密钥的 Lorenz 保密通信系统是稳定同步的．建立发送系统式 (1) 和接收系统式 (2) 的状态误差系统 ($e(t) = x(t) - y(t)$)，得到误差的状态方程

$$\left.\begin{aligned} \dot{e}_1 &= \alpha_p e_1 \\ \dot{e}_2 &= -x_1 e_3 - e_2 \\ \dot{e}_3 &= x_1 e_2 - \rho_p e_3 \end{aligned}\right\} \tag{7}$$

从式 (7) 可见，当 $t \to \infty$ 时，因为 $\alpha_p > 0$，因此有 $e_1 \to 0$．对于由 e_2 和 e_3 构成的二维系统，设李雅普诺夫函数为 $V = e_2^2 + e_3^2$，可求得其导数为

$$\dot{V} = -2(e_2^2 + \rho_p e_3^2) < 0$$

其中 $\rho_p > 0$，根据李雅普诺夫稳定判据可判定系统式 (7) 是大范围渐近稳定的．由于误差系统式 (7) 在 $e = 0$ 处有一个稳定的平衡状态，因此，系统式 (1) 和式 (2) 存在一个稳定的同步态 $x = y$．

发送端系统和接收端系统达到同步后，必有 $x_e = y_e$，两个系统处于相同的参数微扰过程，于是具有动态密钥的保密通信系统是同步的．

3.2 具有动态密钥的混沌同步保密通信的计算机仿真

在 MATLAB 的 SIMULINK 仿真环境下，对图 2 所示双周期信号进行保密通信计算机仿真实验，有很好的同步效果，接收端解密得到的恢复信号 $m_r(t)$ 和 $m(t)$ 相同，当同步的瞬态过程结束后，$m_r(t)$ 和 $m(t)$ 的误差曲线是一条为零的直线．当发送和接收端混沌系统的初始状态不同时，经过 4.5s 的同步时间，同步误差达到零．但当发送和接收端混沌系统的参数不匹配时，两者不能达到同步．接收端的恢复信号与被加密信号存在较大误差，如图 3 所示．此时对参数 α_p 的敏感性达到小数点后 10 位．这一结果达到本方案的设计初衷，高的参数敏感性有利于抵御穷举攻击．

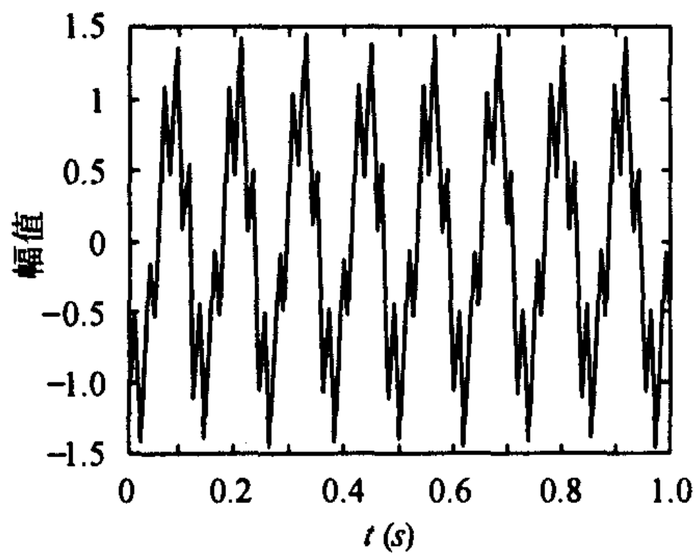


图 2　被加密信号波形

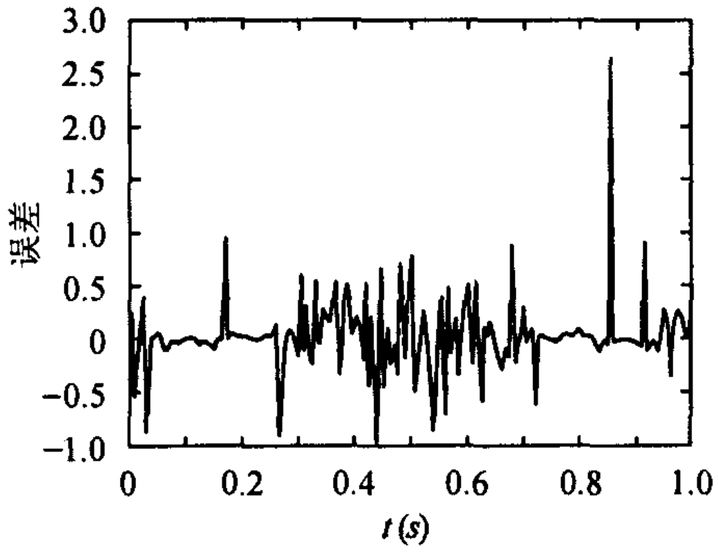
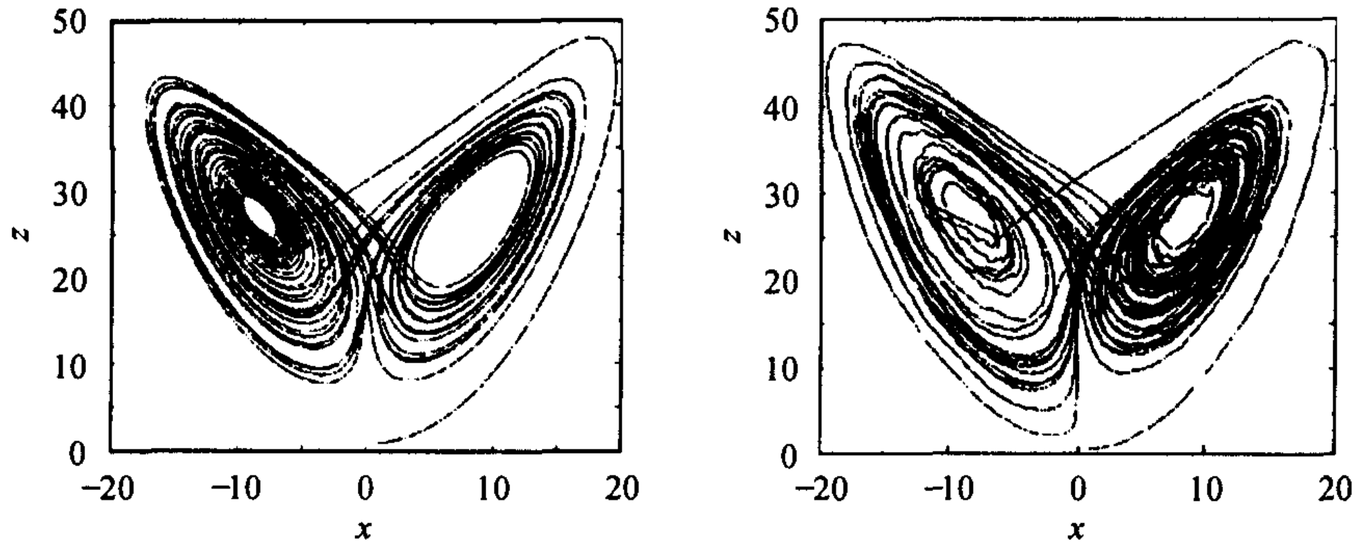


图 3　$m_r(t)$ 和 $m(t)$ 之间的误差

3.3 安全性分析

发送端和接收端系统在相同的初始状态和参数下，加入参数反馈微扰前、后 Lorenz 系统的奇异吸引子如图 4 所示 ($k_1 = 6$)．由图可见，加入参数反馈微扰后，系统的状态偏离了原来的轨迹．



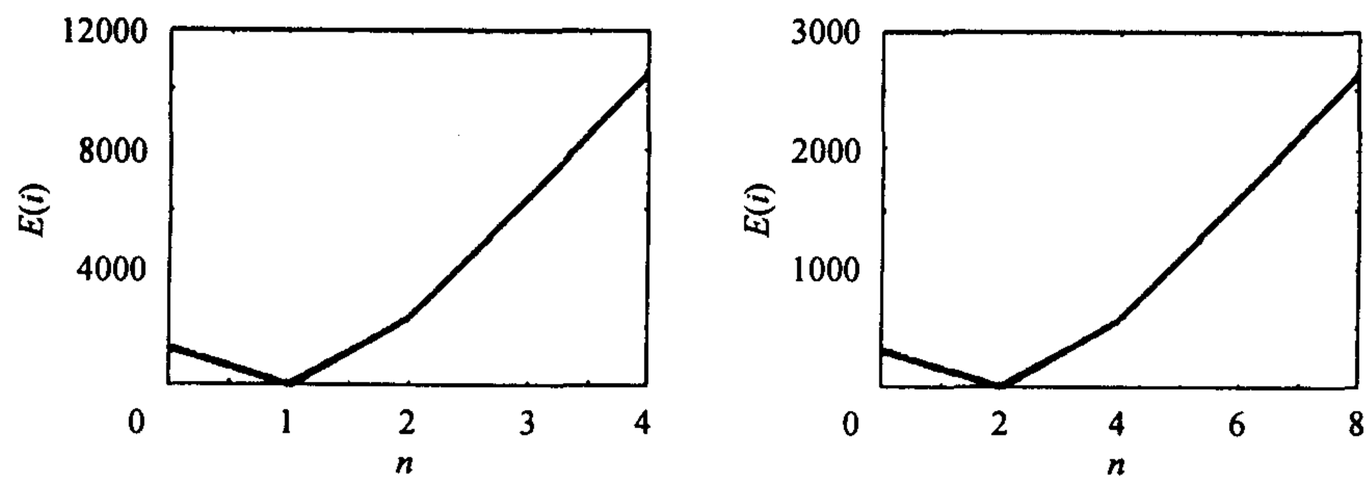
(a) 加入参数反馈微扰前　　(b) 加入参数反馈微扰后

图 4　Lorenz 系统的奇异吸引子

本文 2.2 节的分析表明，主动−被动同步的方案使基于相空间重构的分析无效，故现重点分析本文方案能否被基于混沌同步的参数估计方法破译的问题.

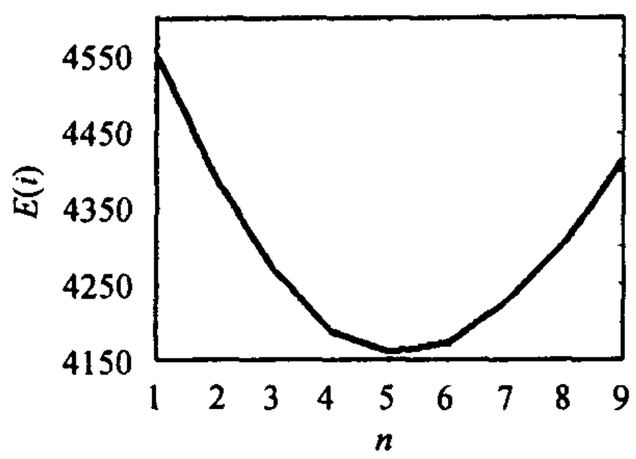
假设破译者已知系统结构和基本参数 $\alpha = 10, \gamma = 28, \rho = 8/3$ ，并且已经用噪声衰减方法提取到 x_2 的近似值 x_{2a} . 现在用 x_{2a} 驱动破译者构建的接收系统，根据这一系统的累计误差的极小值，确定所估计位上的值. 误差定义为 $e(nT) = |x_{2a} - x'_{2a}|$ ，其中 x'_{2a} 是破译者构建的接收系统的对应变量. 令累计误差 $E(i) = \sum_{n=0}^{N} e(nT), n = 0, 1, \cdots, 9$. 将 n 取 $0 \sim 9$ 不同值时的 $E(i)$ 计算出来，其中使 $E(i)$ 取得极小值的 n 值就是所估计位上的值. 设 Lorenz 系统的实际参数为 $\alpha = 10.123456, \quad \gamma = 28, \quad \rho = 8/3$. 从小数点第一位开始逐位估计，取 $N = 30000$, 未加参数反馈微扰时，用上述方法估计到了准确的 α 值. 其中小数点后第一、第二位的累计误差曲线分别如图 5(a) 和图 5(b) 所示，横坐标表示估计值 n ，纵坐标表示 $E(i)$ ，曲线极小值所对应的横坐标的值是估计结果，即 α 的小数点后第一、第二位的估计值分别为 1 和 2 .

进行参数反馈微扰后， α 中小数点后第二位和第六位的估计曲线分别如图 6(a) 和图 6(b) 所示，可见，第二位的估计值是 5 ，与实际值 2 相差较大，而按照图 6(b) 的曲线则无法确定第六位的值. 其他位的估计结果均可归结为上述两种情况. 可见参数反馈微扰的方法是有效的，破坏了参数估计的条件，参数始终处于变动中，且变动的规律难以寻找，使得截获的信息不是相同参数下混沌状态的时间序列，没有足够多的信息可用来估计参数，因此基于混沌同步的分析方法无法准确估计系统的参数. 而本方案又是对参数敏感的，以上两点使安全性得到保证.



(a) 小数点后第一位的估计曲线　　(b) 小数点后第二位的估计曲线

图 5　未加参数反馈微扰的 α 估计曲线



(a) 小数点后第二位的估计曲线　　(b) 小数点后第六位的估计曲线

图 6　加参数反馈微扰的 α 估计曲线

4 结束语

本文分析了几种典型的混沌同步保密通信方案，与针对混沌同步保密通信的分析破译方法，在此基础上研究了基于 Lorenz 方程的、具有动态密钥的主动-被动同步保密通信方案的抗破译能力．计算机仿真实验和安全性分析测试结果均表明，本方案的同步误差为零、安全性高，达到用基于相空间重构、基于混沌同步的分析方法难以破译的效果．

本方案较适合数字实现方式．实际应用需考虑抗干扰等问题．

参　考　文　献

[1] 方锦清．非线性系统中混沌控制方法、同步原理及其应用前景 [J]．物理学进展，1996, 16(2): 137–201.

[2] 翁贻方，Pei Yu．混沌同步原理及其在保密通信中的应用 [J]．北京轻工业学院学报，2000, 18(1): 47–56.

[3] Short K M. Step toward unmasking secure communications[J]. *Int. J. Bifur. Chaos*, 1994, 4(4): 959–977.

[4] Short K M. Unmasking a modulated chaotic communications scheme[J]. *Int. J. Bifur. Chaos*, 1996, 6(2): 367–375.

[5] Perez G. Extracting messages masked by chaos [J]. *Physical Review Letters*, 1995, 74(11): 1970–1973.

[6] Carroll T L, Pecora L M. Cascading synchronized chaotic systems[J]. *Physical Review D,*, 1993, 67(1): 126–140.

[7] Parlitz U, Junge L, Kocarev L. Synchronization-based parameter estimation from time series[J]. *Physical Review E*, 1996, 54(6): 6253–6259.

[8] 翁贻方，鞠磊．高安全性混沌同步保密通信方案设计 [J]．通信学报，2003, 24(2): 44–50.

[9] 翁贻方，鞠磊．变参数混沌同步保密通信方案设计 [J]．信息与控制，2003, 32(2): 128–131.

翁贻方：　女，1954 年生，教授，主要研究方向是混沌同步保密通信、智能控制理论及应用．

翁莉娟：　女，1956 年生，副教授，主要研究方向是非线性理论及混沌，运筹学及应用．

张　蕾：　女，1973 年生，助教，研究方向为数据通信．