

文章编号: 0253-2239(2006)06-0812-6

## 偏振态移位键控光混沌通信系统的保密性\*

方 捻<sup>1</sup> 王陆唐<sup>1</sup> 郭淑琴<sup>2</sup> 黄肇明<sup>1</sup>

(<sup>1</sup> 上海大学通信与信息工程学院, 上海 200072)  
(<sup>2</sup> 浙江工业大学信息工程学院, 杭州 310014)

**摘要:** 为了评判偏振态移位键控(PolSK)光混沌通信系统的保密性强弱, 先要验证它的混沌特性, 因此对该系统的信号进行了分析。利用三种方法判定该信号是否具有混沌特性: 在三维相空间观察奇异吸引子; 分别从最大李氏(Lyapunov)指数满足的方程出发以及 wolf 法计算其最大李氏指数; 并计算其自功率谱密度函数。结果明显观察到奇异吸引子, 算得最大李氏指数分别为 0.0364 和 0.0106, 都大于零, 自功率谱为噪声背景、宽峰的连续谱; 从而判定该系统传输的信号确实是混沌信号。另一方面, 用最小伪邻点算法计算该系统信号的嵌入维数, 结果达到 6 维, 说明该系统具有中高维度混沌特性; 结合系统的抗攻击性分析, 得出结论: 相比于一般的混沌掩盖方案, 该系统具有较强的保密性和安全性。

**关键词:** 光通信; 保密性; 奇异吸引子; 最大李氏指数; wolf 法; 最小伪邻点法; 偏振态移位键控; 光纤环形激光器

中图分类号: TN929 文献标识码: A

## Security of Polarization-Shift Keying Chaos Optical Communication System

Fang Nian<sup>1</sup> Wang Lutang<sup>1</sup> Guo Shuqin<sup>2</sup> Huang Zhaoming<sup>1</sup>

(<sup>1</sup> School of Communication and Information Engineering, Shanghai University, Shanghai 200072)  
(<sup>2</sup> College of Information & Engineering, Zhejiang University of Technology, Hangzhou 310014)

**Abstract:** For judging the security of the chaos optical communication system employing the polarization-shift keying (PolSK) modulation technology, its chaos characteristic needs to be verified above all. So analysis is done for the signal of this system. Three methods are used to judge the signal maintaining chaos characteristics or not: watching the strange attractor in three-dimensional phase space, computing the largest Lyapunov exponent by the equation it meets and wolf method, and computing self-power spectrum density function. As a result, the strange attractor is clearly watched, the largest Lyapunov component is positive 0.0364 and 0.0106, respectively, and the self-power spectrum is wide and continuous with the noise background. Therefore, the judgment of chaos for the signal transmitted in the system is presented. On the other hand, the minimal embodied dimension of the signal is given by the false nearest neighbours (FNN) method and it reaches 6, which shows the higher dimension chaos characteristics of the system. Adding the analysis of the ability of anti-attack for the system, it is concluded that the system owns higher security than the normal chaos masking schemes.

**Key words:** optical communication; security; strange attractor; the largest Lyapunov exponent; wolf method; false nearest neighbours method; polarization-shift keying modulation; fiber ring laser

### 1 引 言

在光混沌传输系统参量调制方式中, 光学系统可利用的参量有: 光波的强度, 波长(频率)、相位以及偏振态等。目前许多研究工作都集中在光强度<sup>[1]</sup>、波长

(频率)<sup>[2]</sup>和相位<sup>[3]</sup>等参量的调制方面, 而在偏振态调制方面的研究较少。根据 Rajarshi Roy 等学者的研究成果<sup>[4]</sup>, 在一个由掺铒光纤放大器(EDFA)所组成的光纤环形激光器混沌系统中, 光波具有高速、高维

\* 国家自然科学基金(60577042)和上海市重点学科(T102)资助课题。

作者简介: 方 捻(1972~), 女, 回族, 河南西华人, 上海大学通信与信息工程学院副教授, 主要从事全光网关键器件及混沌保密光通信等方面的研究。E-mail: nfang@staff.shu.edu.cn

收稿日期: 2005-05-27; 收到修改稿日期: 2005-12-02

数(多态)的偏振态变化,因此利用混沌系统的偏振态调制可以实现高保密性、高码率的信息传输。

王陆唐等已报道了采用偏振技术实现光混沌通信的研究结果<sup>[5,6]</sup>。主要采用光混沌系统的偏振态移位键控(Polarization shift keying, PolSK)调制技术实现信息的保密通信。偏振态移位键控调制技术是将数字码调制到光束所指定的偏振态上。当偏振态移位键控调制技术应用到混沌系统中时,光束偏振态——数字码态的对应关系处于一个动态过程,即处于一个随机不断改变的过程,没有一个偏振状态固定地代表数字码中某一状态。本文着重对其保密性进行分析。

## 2 实验系统及工作原理

偏振态移位键控光混沌保密通信实验系统结构如图 1 所示。整个实验系统包括一个作为混沌信号发射系统的基于半导体光放大器(SOA)的光纤环形激光器,一条 5 km 长的标准单模光纤作为信号传输链路,以及一个带有时延结构的开环混沌接收系统。

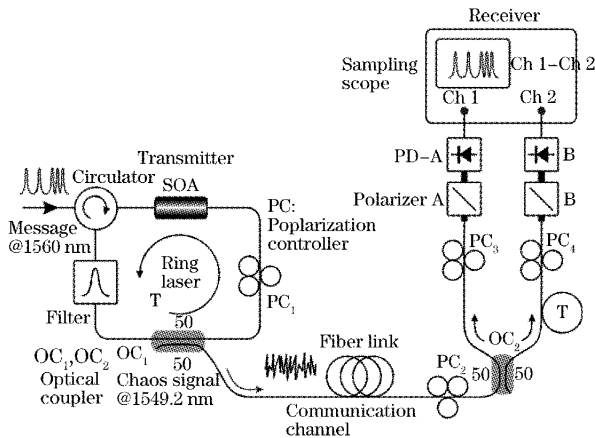


图 1 偏振态移位键控光混沌保密通信实验系统结构图  
Fig. 1 Setup of the experimental system of PolSK chaos secure optical communication

在发射系统中,主要器件为半导体光放大器,这里采用的是 OptoSpeed 公司的半导体光放大器模块(SOA1550MRI-XI 1500)。由于光纤内部存在着双折射效应且随机分布,因此造成光纤环中传播的光束在不同的部位具有不同的偏振态,且随着循环次数的不同在不断变化。另一方面由于半导体光放大器工作状态变化,以及外界一些因素变化,如温度、震动等对光纤的影响都会导致光束偏振态随时间发生改变。因此,光纤环状激光器在光束偏振态

方面是一个混沌动力学系统,其输出的光信号是一种偏振混沌信号。在光纤环中传播的光束通过半导体光放大器时,得到放大最终形成激光输出,其工作波长由光滤波器的中心波长决定。光环行器用于信号光的输入,同时起到光隔离作用,限制光束在环中的传播方向。混沌光信号通过光纤耦合器  $OC_1$  输出。输入信号光只能通过半导体光放大器一次,其传播方向与混沌信号光束的方向相反。输入信号光为一组码率为 630 Mb/s, 27-bit 伪随机归零码循环序列,平均光功率强度为 2.1 dBm。当输入信号为“0”码时,对光纤环形激光器基本没有影响,而当输入信号为“1”码时,光功率的变化导致半导体光放大器的增益发生改变,并进一步导致半导体光放大器有源介质的折射率发生改变,从而导致混沌光束的相位发生改变。因此,通过半导体光放大器的交叉相位调制(XPM)效应,输入信号光能控制混沌信号光束的相位变化以改变其偏振状态,也就把输入信号的信息动态地调制到了混沌光束的偏振态上。光纤环中的偏振控制器  $PC_1$  采用 General Photonics Corporation 公司的光纤挤压器(PLC-001),用于设置光纤环的初始等效双折射,这是取得收发系统同步的关键参量之一<sup>[6]</sup>。

在接收端,为了能达到调整传输光偏振状态的目的,使用了一个偏振控制器  $PC_2$ 。由传输链路输入的混沌信号光通过光耦合器  $OC_2$  均分为两路接收。支路 A 直接接收传播过来的混沌信号,支路 B 通过适当的时延之后再接收。两个光电探测器的输出分别连接示波器的两个输入信道。在示波器内完成两信道信号的强度相减以恢复出所传递的信息。这里采用的是安捷伦数字采样示波器(Angelent Corporation's Infiniium, 1.5 GHz bandwidth and 8 GHz sampling rate)。

## 3 混沌信号的判定

混沌运动是系统的一种非线性性质,但并不是所有的非线性都是混沌的,因此非线性只是产生混沌的必要而非充分条件<sup>[7]</sup>,首先必须对在本系统中传输的光信号是否为混沌信号进行判断。

首先要对实验信号进行相空间重构<sup>[8]</sup>。相空间重构其实是将系统相空间向重构空间投影,若重构维数选得太小,系统相空间轨迹向低维空间投影,将产生许多虚假交叉(即虚假邻点),随着重构维数的增大,虚假邻点数减少,当取足够大的重构维数时,重构相空间就认为不存在虚邻点了,称此时的重构

为嵌入<sup>[9]</sup>。通常称适合(即认为不存在虚邻点)的重构维为嵌入维。

延迟坐标法是由时间序列构造多维的状态空间

矢量,对于一个  $N$  点的时间序列  $x(t_0 + n\Delta t)$ ,  $n=0, 1, \dots, N-1$ , 应用 Takens 定理, 相应的重构轨迹为<sup>[10]</sup>

$$Y(n) = [x(t_0) \quad x(t_0 + \Delta t) \quad \dots \quad x[t_0 + (k-1)\Delta t]] = \begin{bmatrix} x(t_0) & x(t_0 + \Delta t) & \dots & x[t_0 + (k-1)\Delta t] \\ x(t_0 + J\Delta t) & x(t_0 + \Delta t + J\Delta t) & \dots & x[t_0 + (k-1)\Delta t + J\Delta t] \\ \dots & \dots & \dots & \dots \\ x[t_0 + (m-1)J\Delta t] & x[t_0 + \Delta t + (m-1)J\Delta t] & \dots & x[t_0 + (N-1)\Delta t] \end{bmatrix}, \quad (1)$$

其中  $x(t)$  是嵌入空间的状态矢量,  $J$  是重构延时,  $m$  是嵌入维数,  $\Delta t$  是采样间隔,  $k = N - (m-1)J$ ,  $\tau = J\Delta t$  表示延时参量。

下面利用三种方法综合判定。

### 3.1 直接观测法

根据动力学系统的数值运算结果, 画出相空间中相轨迹随时间的变化图以及状态变量随时间的历程图。通过对比、分析等来确定混沌现象。在相空间中, 周期运动对应于封闭曲线, 混沌运动对应于一定区域内随机分布的永不封闭的轨迹<sup>[7]</sup> (奇异吸引

子), 而随机运动对应的轨迹则杂乱无章, 不存在吸引子。

我们选取数据长度为 402 的实验信号, 经过相空间重构运算, 得到本实验系统传输的信号在相空间中相轨迹随时间的变化图, 同时给出一个相应数据长度的随机噪声信号的相轨迹图作对比, 如图 2 所示。从图 2(a) 可看出, 在本系统中传输的光信号确实存在吸引子, 应属于混沌信号。而图 2(b) 中随机噪声信号的相轨迹随时间的变化看不出任何规律, 也不存在吸引子。

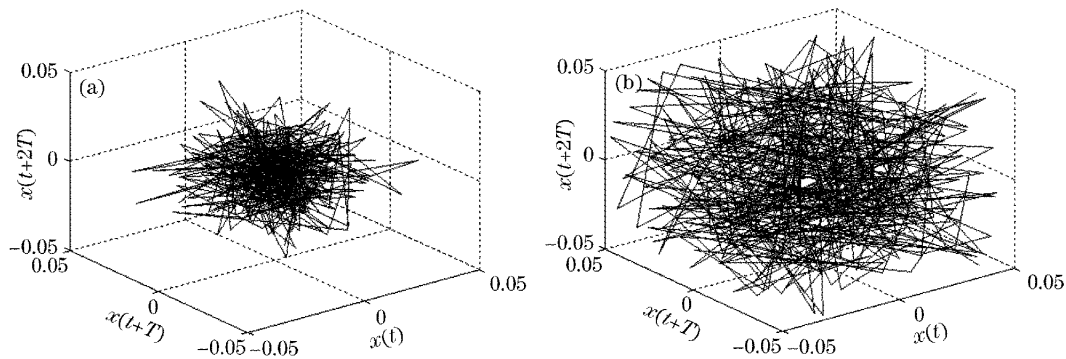


图 2 本实验系统的信号(a)与随机噪声信号(b)的相轨迹

Fig. 2 Phase tracks of signal transmitted in the experimental system (a) and random noise signal (b)

### 3.2 李氏指数分析法

李雅普诺夫 (Lyapunov) 指数  $\sigma$  是用来衡量动力学系统相邻轨迹平均发散率的一个物理量, 是诊断系统是否进入混沌的主要参量<sup>[2]</sup>, 反映了系统中的微小扰动随时间变化所表现出来的发散或者收敛特性。因此, 可以应用李氏指数对系统的混沌状态进行识别。

负的李氏指数意味着局部收敛的平均速度, 而正的李氏指数则意味着局部发散的平速度。正的和负的李氏指数可以在同一个耗散系统中并存, 这种耗散系统就是混沌系统。

对实际问题而言, 由于系统都是有界的, 所以只

要发现其中李氏指数大于零, 就可判定系统是混沌的<sup>[11]</sup>, 所以最大李氏指数的计算有着重要意义。

首先从最大李氏指数满足的方程出发计算本实验系统信号的最大李氏指数。

最大李氏指数  $\sigma$  满足以下方程<sup>[8]</sup>:

$$d(t) = C \exp(\sigma t), \quad (2)$$

(2) 式中  $d(t)$  为  $t$  时刻的平均扩散度,  $C$  为归一化常量。重构的相空间中的某一点  $x_i$ , 设与之最近的点  $x'_i$ , 记  $d_i(0) = \min_{x'_i} \|x_i - x'_i\|$ , 为相邻最近两点的距离。经过  $k\tau$  时间后, 由 (2) 式得到

$$d_i(k) = \|x_{i+k} - x'_{i+k}\| = C_i \exp[\sigma(k\tau)], \quad (3)$$

上式两边同时取对数, 得到

$$\ln d_i(k) = \ln C_i + \sigma(k\tau), \quad (4)$$

(4) 式表示斜率为  $\sigma$  的近似平行的直线, 用最小二乘法拟合得到直线

$$y(k) = \frac{1}{\tau} \langle \ln d_i(k) \rangle, \quad (5)$$

式中  $\langle \ln d_i(k) \rangle$  表示对所有的  $i$  的平均, 直线的斜率即为所需的最大李氏指数。

选取数据长度为 256, 按照上述方法计算实验系统传输的信号的最大李氏指数为 0.0364。

为了确保计算与判断的准确性, 对同样的实验信号还用 Wolf 方法<sup>[12]</sup> 进行了计算。

在重构空间取初始点  $Y(t_0)$ , 设其与最近邻点  $Y_0(t_0)$  的距离为  $L_0$ , 追踪这两点的时间演化, 直到  $t_1$  时刻, 其间距超过某规定值  $\epsilon > 0, L' = |Y(t_1) - Y_0(t_1)| > \epsilon$ . 保留  $Y(t_1)$ , 并在  $Y(t_1)$  邻近另找一个点  $Y_1(t_1)$ , 使得  $L_1 = |Y(t_1) - Y_1(t_1)| < \epsilon$ , 并且与之夹角尽可能小, 继续上述过程, 直至  $Y(t)$  到达时间序列的终点, 这时追踪演化过程总的迭代次数为  $M$ , 则最大李氏指数为

$$\sigma = \frac{1}{t_M - t_0} \sum_{i=0}^M \ln \left( \frac{L'_i}{L_i} \right), \quad (6)$$

利用 Wolf 方法, 计算的最大李氏指数为 0.0106。

两种方法计算的结果都大于零。因此, 可以判定该信号为混沌信号, 实验系统是一个非线性动力学系统。

### 3.3 自功率谱密度分析法

为了表示混沌信号的频域特性, 可以通过求其自相关函数  $R_{xx}(\tau)$  的傅里叶变换, 根据所得的自功率谱密度函数  $S_{xx}(f)$  来分析混沌的频域特性:

$$S_{xx}(f) = \int_{-\infty}^{\infty} R_{xx}(\tau) \exp(-j2\pi f\tau) d\tau,$$

$$R_{xx}(\tau) = \int_{-\infty}^{\infty} S_{xx}(f) \exp(-j2\pi f\tau) df.$$

对于周期运动, 功率谱只在基频及其倍频处出现尖峰, 准周期对应的功率谱在几个不可约的基频以及它们叠加所在频率处出现尖峰。发生倍周期分岔时, 功率谱中将出现分频及其倍频, 在这些频率点上功率谱图也都具有尖峰; 混沌运动的特征是在功率谱中出现噪声背景、宽峰的连续谱, 其中包含有与周期运动相对应的尖峰。根据这些特点, 很容易识别运动的特征是周期的、准周期的、随机的或者混沌的<sup>[7]</sup>。

取 225 个数据点, 计算其自相关函数的傅里叶变换得到实验信号的自功率频谱(如图 3 所示)。显

然满足混沌的特征。

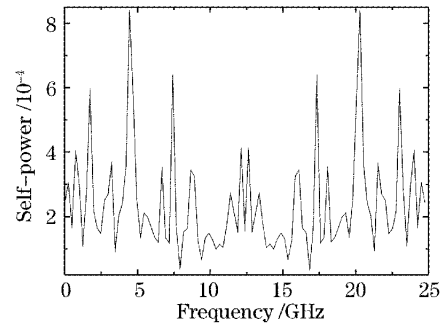


图 3 本实验系统信号的自功率谱

Fig. 3 Self-power spectrum of the signal of the experimental system

综合以上三个判据, 本实验系统中所传输的信号确实属于光混沌信号。说明本实验系统是一个光混沌通信系统。

## 4 系统保密性分析

确定实验系统的信号是混沌信号后, 才可以考虑它作为一个混沌系统具有的通信保密性能。

根据 Rajarshi Roy 等学者的研究, 被传送的混沌光波的维数对混沌通信的保密性很重要。维数越高, 保密性就越强<sup>[13]</sup>。因此, 计算了实验系统信号的嵌入维数, 并进行了抗攻击性能分析。

### 4.1 最小嵌入维数计算

采用最小伪邻点算法(FNN)计算本系统混沌光信号的最小嵌入维数。

时间序列  $X(n)$  是非线性动力系统多维状态变量在一维空间的投影, 维数嵌入的目的就是将该投影展开到原来系统的多维状态空间。给定一组时间序列, 如何求出它的最小嵌入维数  $d$ , 从数学角度讲, 最小嵌入维数  $d$  和任何  $m > d$  的维数, 都可以将吸引子展开到一个新的高维空间。但是, 从应用的角度讲, 最小嵌入维数将意味着最小的计算工作量, 同时减小了截断误差和仪器测量误差所带来的噪声干扰的影响。选择最小嵌入维数  $d$  也等于计算吸引子的不变量, 因为这些不变量表征了吸引子的几何特性。

最小伪邻算法<sup>[10]</sup> 是计算最小嵌入维数的一种有效方法, 它的基本原理是, 当维数从  $m$  变到  $m+1$  时, 判断轨迹  $Y(n)$  上的某一点是真邻点还是假邻点。如果是真邻点, 则表明  $m > d$ , 如果是假邻点, 则  $m < d$ 。假邻点的产生是因为在较小的嵌入空间 ( $m < d$ ) 观察轨迹的结果。当在一个较大的空间内

( $m \geq d$ ) 观察时, 轨迹上的所有点都变成了真邻点。

经过计算, 选取 499 个数据点时本系统信号的最小嵌入维数达到 6 维, 属于中高维度, 保密性较强。如图 4 所示, 横坐标表示最小嵌入维数, 纵坐标表示假邻点数的百分比。

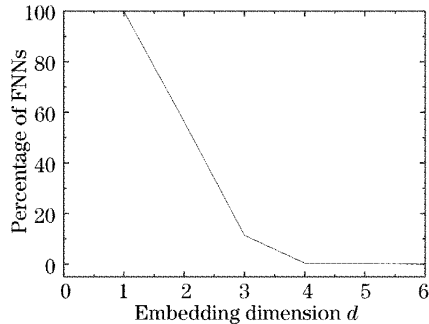


图 4 用最小伪邻点算法计算本系统传输信号的最小嵌入维数

Fig. 4 The minimal embodied dimension of the signal of the experimental system by FNN method

## 4.2 抗攻击性分析

本混沌保密通信系统中传播的激光其偏振态呈现混沌性, 而非强度混沌。没有信号输入时, 收发两端混沌系统处于同步状态, 减法器输出为零。当输入信号为“0”码时, 此刻, 相当于没有输入信号状态, 收发混沌系统仍同步, 减法器输出还是零; 而当输入信号为“1”码时, 输入信号与混沌信号在半导体光放大器中发生交叉相位调制效应, 发送端混沌信号的偏振态由于信号相位受到调制而改变, 收发两端的偏振态混沌信号不再同步, 减法器输出不为零。如果整个系统一直处于非同步状态, 找不到一个判别标准, 也就无法从混沌信号中获取所传输的信息。如果不知道系统的初始状态参量(光纤环的周期以及偏振状态), 不可能实现系统同步, 也无法获取所传输的信息。

另一方面, 对混沌保密通信信号的破译算法已有多种, 但基本上都是针对混沌掩盖方案提出。如回归映射法、相空间重构法、非线性预测法等。而本系统利用的是混沌的偏振态键控调制技术实现保密通信, 通过对系统是否处于同步以及非同步状态的判别, 来从混沌信号中获取所传递的信息。因此, 在接收端, 无论是接收支路 A 的光信号还是支路 B 的光信号, 都无法从中提取出所需要的信息, 因为它们都是一组连续变化、无规律的混沌信号。同样, 单凭直接从传输信道上窃取的一段光混沌信号, 用现有的破译算法也恢复不出原始信息。即使用相空间重

构法重构出混沌的吸引子, 再生出混沌信号, 也无法用直接接收的混沌信号减去再生的混沌信号(对混沌掩盖方式)或除以再生的混沌信号(对混沌强度调制方式)来窃取所传递的信息, 因为本系统的特色就在于利用混沌的偏振态键控的数字调制技术, 并且“0”码与“1”码的判别与系统同步或非同步的状态相对应, 而系统是处于同步状态还是非同步状态一定要通过两路接收信号比较才能得出。

本偏振态移位键控光混沌通信系统的特点还在于光束偏振态——数字码态的对应关系处于一个动态过程, 即处于一个随机不断改变的过程, 没有一个偏振状态固定地代表数字码中某一状态。因此, 即使从信道上提取部分光信号, 用偏振片(检偏器)分析出光的偏振方向以确定偏振, 得到的是随机变化的信号, 仍然无法恢复出原始信息, 因为“0”码与“1”码并不固定地对应光的某一偏振, 而是与系统同步或非同步的状态相对应。

所以, 无论是硬件方面的攻击, 还是软件方面的破译, 偏振态移位键控光混沌通信系统都具有较强的免疫力。

## 5 结 论

对采用偏振态移位键控调制技术和混沌光学系统相结合的混沌光传输实验系统的保密性做了分析。首先对实验系统信号进行混沌性判别, 利用三种判据综合判定实验系统中传输的信号确实是混沌信号。然后利用最小伪邻点算法计算了该混沌信号的最小嵌入维数, 证实该实验系统属于中高维度混沌系统, 保密性较强。通过分析正确接收本系统混沌信号必须的参量和方法, 以及现有的破译算法的局限性, 从硬件与软件两方面分析了系统的抗攻击性能, 最后得出结论, 偏振态移位键控光混沌通信系统具有良好的保密性能。

## 参 考 文 献

- 1 Yan Senlin. High rate chaos secure communication system of multiple quantum well lasers [J]. *Acta Optica Sinica*, 2005, 25(2): 179~185 (in Chinese)  
颜森林. 高速多量子阱激光器混沌保密通信系统研究[J]. *光学学报*, 2005, 25(2): 179~185
- 2 Yan Senlin, He Longqing, Wu Haiyong *et al.*. Studies on method of phase shift controlling chaos for dual ring erbium doped fiber lasers [J]. *Chin. J. Lasers*, 2005, 32(5): 642~646 (in Chinese)  
颜森林, 何龙庆, 吴海勇等. 双环掺铒光纤激光器混沌相移控制方法研究[J]. *中国激光*, 2005, 32(5): 642~646
- 3 Senlin Yan. All-optical chaotic MQW laser repeater for long-haul chaotic communications [J]. *Chin. Opt. Lett.*, 2005, 3(5):

- 283~286
- 4 Gregory D. van Wingeren, Rajarshi Roy. High-speed fiber-optic polarization analyzer; measurements of the polarization dynamics of an erbium-doped fiber ring laser[J]. *Opt. Commun.*, 1999, **164**(3): 107~120
  - 5 Lutang Wang, Zhaoming Huang. Optical chaos communication with a dynamical SOA-based fiber ring laser[C]. *Proc. SPIE*, 2003, **5281**: 619~627
  - 6 Lutang Wang, Weijia Wu, Nian Fang *et al.*. Experimental study on chaotic optical communication with PolSK modulation technology[C]. *Proc. SPIE*, 2005, **6021**: 190~196
  - 7 Yang Xiuli. A study on polarization-shift keying technology and optic chaos communication system [D]. Shanghai: Shanghai University, 2005. 6,7,9  
杨秀丽. 偏振移位键控技术和光混沌保密通信系统的研究[D]. 上海: 上海大学, 2005. 6,7,9
  - 8 Li Guohui, Zhou Shiping, Xu Deming. Computing the largest Lyapunov exponent form time series[J]. *J. Applied Sciences*, 2003, **21**(2): 127~131 (in Chinese)  
李国辉, 周世平, 徐得名. 时间序列最大 Lyapunov 指数的计算[J]. *应用科学学报*, 2003, **21**(2): 127~131
  - 9 Lin Jiayu, Wang Yueke, Huang Zhiping *et al.*. A new voice activity detection method based on chaos theory[J]. *J. China Institute of Communications*, 2001, **22**(2): 123~128 (in Chinese)  
林嘉宇, 王跃科, 黄芝平等. 一种新的基于混沌的语音、噪声判别方法[J]. *通信学报*, 2001, **22**(2): 123~128
  - 10 Li Yaan, Xu Demin. State space reconstruction of nonlinear dynamic system[J]. *Ship Engineering*, 2000, **22**(5): 47~50 (in Chinese)  
李亚安, 徐德民. 非线性动力系统的状态空间重构[J]. *船舶工程*, 2000, **22**(5): 47~50
  - 11 Wen Quan, Zhang Yongchuan, Cheng Shijie. Identify determinacy from chaotic time series [J]. *International J. Hydroelectric Energy*, 2001, **19**(3): 72~75 (in Chinese)  
温权, 张勇传, 程时杰. 辨识混沌时间序列中的确定性[J]. *水电能源科学*, 2001, **19**(3): 72~75
  - 12 Lü Jinhu, Lu Junan, Chen Shihua. *The Analysis of Chaotic Time Series and Its Application* [M]. Wuhan: Wuhan University Press, 2002 (in Chinese)  
吕金虎, 陆君安, 陈士华. 混沌时间序列分析及其应用[M]. 武汉: 武汉大学出版社, 2002
  - 13 Gregory D. van Wingeren, Rajarshi Roy. Chaotic communication using time-delayed optical system[J]. *Int. J. Bifurcation and Chaos*, 1999, **9**(11): 2129~2156