doi: 10.3788/lop47.030602

混沌激光通信的保密性能研究进展

赵清春 王云才

(太原理工大学理学院物理系， 山西 太原 030024)

摘要 利用激光器可以产生高维宽带混沌载波，并有望构建混沌激光保密通信信道。结合国内外的研究工作，从密码分析学的角度讨论了混沌激光通信的保密性能，介绍了混沌激光通信保密性能的研究进展，重点分析了目前报道的几种增强混沌激光通信保密性能方案的优缺点，同时提出了其他几种备用措施。

关键词 混沌激光通信；保密性；激光器；密钥

中图分类号 TN918.6 **OCIS** 060.4510 140.1540 **文献标识码** A

Research Progress in Security Analysis of Chaotic Optical Communication

Zhao Qingchun Wang Yuncai

(*Department of Physics, College of Science, Taiyuan University of Technology, Taiyuan, Shanxi* 030024, *China*)

Abstract Wide bandwidth, high dimension chaotic carriers can be generated by lasers. It is hopeful to establish chaotic optical secure communication channel. Combined with the research both at home and abroad, the security performance of chaotic optical communication is demonstrated according to the cryptanalysis. The research progress in security analysis of chaotic optical communication is introduced. The advantages and disadvantages of several currently reported methods of enhancing the security of chaotic optical communication are analyzed in detail. Meanwhile, some other spare measures are proposed.

Key words chaotic optical communication; security; laser; key

1 引 言

光纤通信具有传输频带宽、通信容量大、抗电磁干扰等优点，现已成为目前有线通信的主要方式。波分复用和时分复用技术大大提高了光纤通信的容量和速率，然而信息安全仍然是一个极具挑战性的课题。虽然光波在光纤中传输时很难外泄，但是这不表明信息不被窃听。目前普遍采用的加密技术是公众密钥加密(Public key encryption)[1]。它是一种基于软件的加密方式，成功地解决了密钥的分发问题，由复杂性理论保证了其计算安全性，然而它不是无条件安全的。1994 年，由美国贝尔电报电话公司首席科学家 A. K. Lenstra 组织的 43 个国家的 600 多名专家，利用 1600 台联网的计算机历时 8 个月破译了公众密钥加密算法的 RSA(R. Rivest, A. Shamir, L. Adleman)算法。2005 年，王小云等[2,3]先后破译了用于构造公众密钥的 MD5(Message-digest algorithm 5)系列 Hash 函数及 Hash 函数标准 SHA-1(secure Hash algoritm-1)。目前市面

收稿日期：2009-04-15; **收到修改稿日期**：2009-07-23

基金项目：国家自然科学基金(60777041)资助课题。

作者简介：赵清春(1982—)，男，硕士研究生，主要从事混沌通信保密性能方面的研究。E-mail: zhaoqingchun2000@163.com

导师简介：王云才(1965—)，男，教授，博士生导师，主要从事半导体激光器的非线性动力学特性及其应用等方面的研究。E-mail: wangyc@tyut.edu.cn(通信联系人)

上出现的手机窃听器就是因为 2G 数字移动通信协议中的加密算法被破解。近年来，不断有报道发现 Windows，Unix 等计算机操作系统通信协议中存在安全漏洞，这些均表明公众密钥依然存在着被破译的可能，促使人们寻找更安全的加密技术。

与现行的公众密钥技术相比，混沌通信是一种基于物理层的硬件加密。它依靠结构一致的收发器产生出相同的混沌载波而实现同步，待传输的信息隐藏在发射机产生的混沌载波中，传输至接收机时与本地产生的混沌信号相减即可提取出加密的信息。基于这种混沌同步思想的通信方式最先在电路中得到实现[4]。后来人们逐渐意识到电路产生的混沌载波的带宽一般都比较低，难以高速、大容量地传输信息，因此人们开始关注如何提高电路混沌的带宽或者由其他器件(如激光器)产生出宽带的混沌信号。

激光器在受到扰动(如外光注入、光反馈)时输出会呈现混沌现象，此时的激光称为混沌激光。混沌激光有重要的应用[5]：其自相关函数的 δ 线形可用于激光雷达[6~9]及测量光纤损毁点的光时域反射仪[10,11]，从而提高测距的精度及实现对光纤无盲区高精度损毁点的探测；波形的随机性可用于产生吉比特每秒的高速真随机码[12]；低相干性可用于相干层析和彩虹测量等方面[13,14]。同样的，混沌激光也可用于通信。现已证明，激光器可以产生出关联维数大于 4 (高维混沌)、带宽为几十吉赫兹的混沌载波[15~18]，并且混沌激光通信可以与现行的光通信网络兼容[19,20]，因此它引起了广泛的研究兴趣。然而，人们对混沌激光通信保密性能的关注却比较少。

本文结合国内外的研究工作，分析了各种破译混沌激光通信的方法，重点论述了目前 4 种增强保密性能的方案，并对该领域今后的研究方向做了展望。

2 破译延迟时间

激光器的动力学行为可以由微分方程来描述，例如半导体激光器可以由 Lang-Kobayashi 速率方程来描述。当半导体激光器带有外腔反馈、光电反馈或有外光注入时，输出会呈现混沌状态，而速率方程中会引入延迟时间，此时的方程就是延迟微分方程，表示为

$$y(t,T)=F[x(t),T] \ , \tag{1}$$

式中 $x(t)$为自变量，T 为延迟时间。由此看来，延迟时间是延迟微分方程的一个重要物理量。它是激光器的一个外部参数，是一个理想的附加密钥[21]。破译了延迟时间就可以知道发射机的某些结构，并为破译信息提供参考。

M. W. Lee 等[22]通过实验和数值模拟证明了双反馈比单反馈半导体激光器的保密性好。采用统计分析、功率谱分析和预测误差分析的三种方法分别研究了延迟时间的破译问题。在改变双反馈外腔长度的过程中，整数倍的外腔长度对应的往返延迟时间可以用预测误差分析的办法得到；对于非整数倍的腔长，只有腔的弛豫振荡频率的均值可以从功率谱上得到，而腔的延迟时间却不能得到。J. P. Goedgebuer 等[23,24]提出了波长混沌的概念：当分布布拉格反射激光器在光电反馈的条件下其输出光的波长会呈现混沌现象，而输出光的功率保持不变。这种波长混沌不同于常见的功率混沌（即激光器输出光功率呈现混沌现象，而波长恒定），也可用于保密通信。V. S. Udaltsov 等[25]以波长混沌为例，系统地总结了破译延迟时间的五种主要方法：回归映射、自相关函数、平均互信息技术、极值的时间分布[26]、低维空间中的局部线性拟合[27,28]。前面两种方法只能破译单一的延迟时间，而后面三种方法还能破译双延迟的延迟时间。他们还指出，对双延迟的情况，随着反馈增益系数的增加，破译延迟时间变得困难甚至失败。这同样也表明了双延迟系统的保密性要优于单延迟系统。D. Rontani 等[29]研究发现，在半导体激光器的反馈率设置合适且注入电流设置使激光器的弛豫振荡周期接近延迟时间时，已经无法破译单延迟时间。这说明在参数设置合适时，单延迟时间也可不被破译。

3 破译信息

3.1 实验研究

R. J. Jones 等[30]最先对混沌激光通信的保密性能进行了实验研究。发射机由一个外腔激光器构成。待传输的信息通过电流调制的方式加载到发射机上，即混沌调制。窃听者拥有一个不带外腔的半导体激光器，由光电探测器测量输入和输出自身激光器的信号并相减尝试破译信息。实验发现，虽然窃听者可以通过光电探测器获得信道中传输的信号，但是无法破译其中隐藏的信息。S. Sivaprakasam 等[31]研究了混沌隐藏方式传输信息的保密性。信息由单独的激光器产生并通过分束器注入到发射机激光器；同时，窃听者采用外腔激光器尝试窃取信息。实验结果表明，窃听者都能破译正弦信号及更复杂的波形信息。

通过以上报道可以发现，对基于外腔激光器的混沌通信系统，混沌调制的信息加载方式要比混沌隐藏的保密性好；同时也可见，窃听者装置的结构及参数越与发射机的结构及参数相近，破译信息越容易。

3.2 理论研究

J. B. Geddes 等[32]根据响应函数的理论破译了双环光纤激光器混沌通信中的信息。根据 G. D. Van Wiggeren 等[33,34]提出的混沌通信系统的拓扑结构可得到响应函数，而响应函数中的四个参数可以通过传输信号的自相关和偏自相关函数提取出来。这时混沌载波中隐藏的信息可通过传输信号与响应函数的反卷积得到。这种基于响应函数理论破译信息的前提是通过混沌通信系统的拓扑结构获得响应函数。然而，半导体激光器与光纤激光器产生混沌的机理不同，所以这种破译信息的方式不适用于半导体激光器混沌通信系统。

V. S. Udaltsov等[35]对他们提出的单延迟波长混沌通信系统的保密性进行了研究。首先通过自相关函数和平均互信息技术得到了延迟时间，然后利用3次样条插值得到了描述激光器的微分方程中非线性函数的参数。由得到的这些参数便可以重构出接收机的动力学方程进而得到接收机的输出信号，最后将接收到的信号与接收机的输出信号相减便得到加密的模拟信息。可以看出，这种破译信息的方式只是针对波长混沌通信系统的，它的普适性(即是否可用于破译其他类型的混沌激光通信系统)还有待进一步研究。

S. Ort ń等[36]利用人工神经网络强大的非线性映射能力同样破译了波长混沌通信中的信息。他们设计了一个前向人工神经网络，通过训练集对神经网络中的传递函数赋值，然后根据得到的神经网络与发射机同步破译信息。利用人工神经网络进行信息破译需要训练集，即需要预先知道一部分待加密的信息(明文)。而在实际中事先获取一部分明文是相当困难的，这是利用人工神经网络破译信息的一个局限。

以上 3 种理论破译混沌激光通信中信息的方式是针对某一特定系统或作出假设的前提下进行的。在理论上寻找一种普适的破译信息的方法将是今后的一个研究热点。

4 增强保密性能的方案

在发现混沌激光通信存在保密性的漏洞及被破译的可能性之后，如何提高其保密性迫在眉睫。近两年内，人们提出了副载波调制技术及反馈相位、反馈长度、反馈强度做密钥以增强保密性的方案。

4.1 副载波调制技术

A. Bogris 等[37]将副载波调制技术用于全光混沌通信以增强保密性，其装置如图 1 所示。首先用一个射频信号调制待传输的信息，调制后的信号与偏置电流一起再调制发射机产生混沌输出。信息在接收端经接收机激光器、局部振荡器和低通滤波器后被提取出来。研究发现，当射频载波的频率落在混沌功率谱峰值范围之内时，信息可以很好地被加密及解密。

A. Argyris 等[38]对上面的数值模拟结果进行了实验验证，实验装置如图 2 所示。当副载波的频率设定在混沌载波功率谱峰值处时，传输 1 Gbit/s 的信息，系统的误码率为 10^{-12}，如此低的误码率能够满足现代

通信质量的要求。

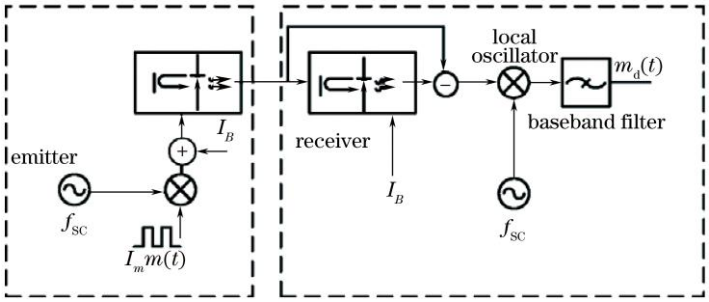

图 1 利用副载波调制技术的混沌发射机及接收机框架

Fig.1 Schematic of the chaotic transmitter and receiver blocks utilizing a subcarrier modulation technique

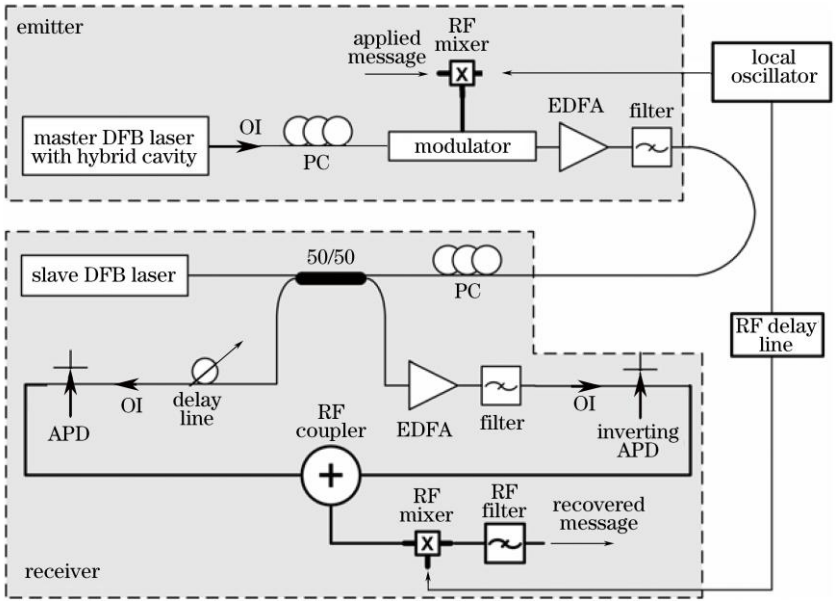

图 2 利用副载波调制技术的混沌光通信系统实验装置图

Fig.2 Experimental setup for a chaotic optical communication system using a subcarrier modulation technique

4.2 反馈相位作密钥

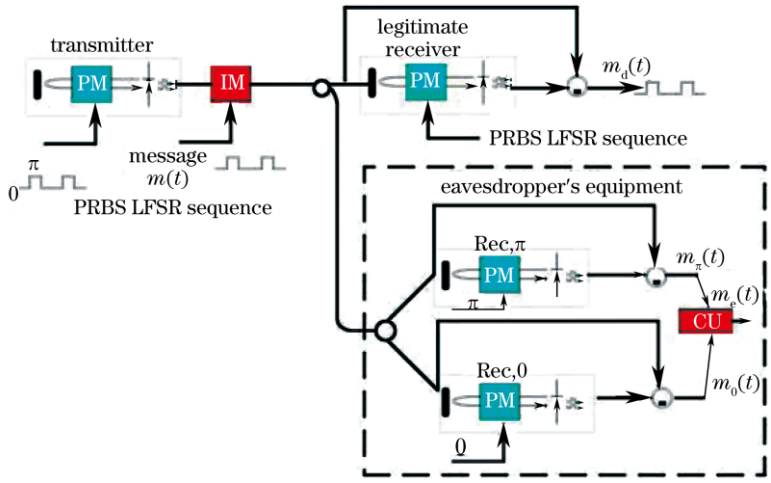

图 3 保密系统及窃听者的接收单元框图

Fig.3 Schematic of the secure system and the eavesdropper's receiving unit

A. Bogris 等[39]提出了将短腔激光器的反馈相位作密钥以增强混沌光通信系统的保密性，其装置如图 3。发射机和接收机的反馈相位在 0 和 π 之间高速变化，窃听者具有与发射机同样参数的激光器但不知道密钥

(即高速改变的反馈相位)。数值模拟结果表明，窃听者激光器无法与发射机同步，因而无法窃听信息。虽然短腔激光器结构紧凑便于集成，然而其反馈相位容易受环境温度等因素的影响不易精确控制。

4.3 反馈长度作密钥

赵清春等[40]提出了将长腔激光器的反馈长度作密钥以增加系统的保密性。图 4 是反馈长度作动态密钥时信息传输及窃听的装置图。发射机由光开关控制选择不同的反馈长度并做高速切换，接收机采用对称的结构提取信息。假定窃听者具有除发射机反馈长度之外的所有参数，通过可变延迟线改变自身激光器的反馈长度并用掺铒光纤放大器(EDFA)增加注入率，尝试破译信息。研究发现：在 EDFA 保证足够强的注入下，窃听者激光器始终能与发射机同步进而破译信息，说明反馈长度作密钥并不能增强混沌光通信的保密性。

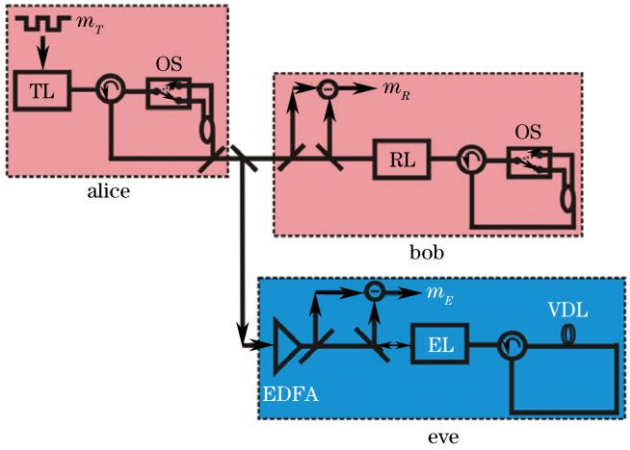

图 4 反馈长度作动态密钥时混沌光通信及信息窃听装置图

Fig.4 Schematic setup for chaotic optical communication and message eavesdropping using the feedback length as a dynamic key

4.4 反馈强度作密钥

郭东明等[41]提出将外腔激光器的反馈强度作密钥以增强混沌光通信的保密性，模型如图 5 所示。发射机和接收机的外腔中插入强度调制器来调制反馈光的强度。结果显示：只有当接收机采用与发射机相同的反馈强度调制时，信息才能很好地恢复。这说明了外腔激光器的反馈强度能在一定程度上增强混沌光通信的保密性能。虽然收发两端在反馈强度同步变化的情况下，系统的误码率降低了，但是受限于普通计算机的运算速度，目前数值模拟中加载信息的码长都不能太长，误码率难以达到 10^{-9} 或更低量级，这也一定程度上限制了数值模拟结果的实用化。

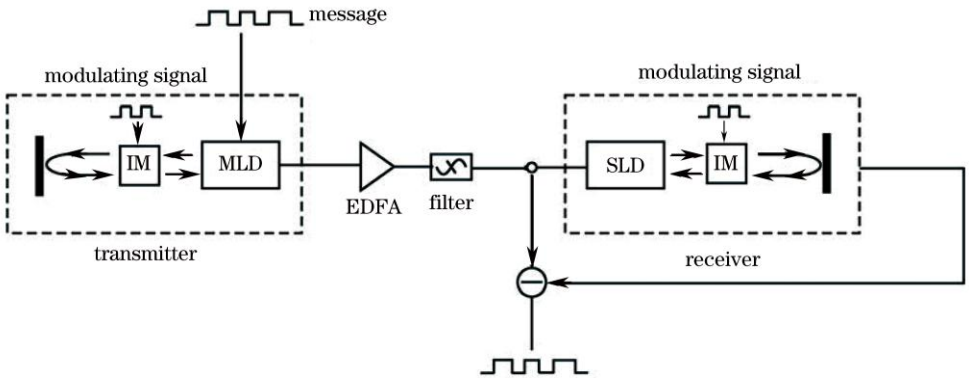

图 5 外腔激光器的反馈强度作密钥时混沌光通信框图

Fig.5 Block diagram for chaos-based optical communication using the feedback strength of external cavity laser as a key

5 总结与展望

混沌激光通信系统产生的载波带宽大、维数高而且能够传输高速的信息，弥补了电路混沌通信系统很

多缺陷，成为一种新颖实用的保密通信方案。然而目前关于混沌激光通信系统保密性能的一些理论及实验研究证明，这种通信方案还一定程度地存在着保密性的漏洞。例如：单延迟不如双延迟系统的保密性好；借助响应函数的理论可以破译光纤激光器混沌通信中的信息等。于是，提出了各种增强保密性能的方案：副载波调制技术；反馈相位、反馈长度、反馈强度作密钥。然而可以当作密钥使用的激光器参数有限，如何增强混沌光通信的保密性将是今后的研究热点。建议使用以下 3 种方法来增强混沌光通信的保密性：

1) 对于延迟时间系统，可以设置系统的延迟时间变量为 3 个甚至更多个，这样可以增强系统的保密性，提高抗破译能力；

2) 将目前成熟的软件加密技术与混沌光通信结合产生出高速保密的实用化系统；

3) 借鉴现有的密钥分发机制(公众密钥或量子密钥)实现混沌光通信中的密钥分发也是亟待解决的问题。

参 考 文 献

1 W. Diffie, M. E. Hellman. New directions in cryptography[J]. *IEEE Trans. Information Theory*, 1976, **22**(6): 644~654

2 X. Wang, X. Lai, D. Feng *et al.*. Cryptanalysis of the Hash functions MD4 and RIPEMD[J]. *Lecture Notes in Computer Science*, 2005, **3494**: 1~18

3 X. Wang, Y. L. Yin, H. Yu. Finding collisions in the full SHA-1[J]. *Lecture Notes in Computer Science*, 2005, **3621**: 17~36

4 L. M. Pecora, T. L. Carroll. Synchronization in chaotic systems[J]. *Phys. Rev. Lett.*, 1990, **64**(8): 821~824

5 Wang Yuncai. Generation and applications of chaotic laser[J]. *Laser & Optoelectronics Progress*, 2009, **46**(4): 13~21
王云才. 混沌激光的产生与应用[J]. 激光与光电子学进展, 2009, **46**(4): 13~21

6 K. Myneni, T. A. Barr, B. R. Reed *et al.*. High-precision ranging using a chaotic laser pulse train[J]. *Appl. Phys. Lett.*, 2001, **78**(11): 1496~1498

7 F. Y. Lin, J. M. Liu. Chaotic lidar[J]. *IEEE J. Sel. Top. Quantum Electron.*, 2004, **10**(5): 991~997

8 B. Wang, Y. Wang, L. Kong *et al.*. Multi-target real-time ranging with chaotic laser radar[J]. *Chin. Opt. Lett.*, 2008, **6**(11): 868~870

9 Gong Tian'an, Wang Yuncai, Kong Lingqin *et al.*. Chaotic lidar for automotive collision warning system[J]. *Chinese J. Lasers*, 2009, **36**(9): 2426~2430
龚天安, 王云才, 孔令琴 等. 面向汽车防撞的混沌激光雷达[J]. 中国激光, 2009, **36**(9): 2426~2430

10 Y. Wang, B. Wang, A. Wang. Chaotic correlation optical time domain reflectometer utilizing laser diode[J]. *IEEE Photon. Technol. Lett.*, 2008, **20**(19): 1636~1638

11 Wang Anbang, Wang Yuncai. Chaos correlation optical time domain reflectometry[J]. *Science in China Series F: Information Sciences*, 2010, **40**(3)
王安帮, 王云才. 混沌激光相关法光时域反射测量技术[J]. 中国科学F辑: 信息科学, 2010, **40**(3)

12 A. Uchida, K. Amano, M. Inoue *et al.*. Fast physical random bit generation with chaotic semiconductor lasers[J]. *Nat. Photon.*, 2008, **2**(12): 728~732

13 M. Peil, I. Fischer, W. Elsäßer *et al.*. Rainbow refractometry with a tailored incoherent semiconductor laser source[J]. *Appl. Phys. Lett.*, 2006, **89**(9): 091106

14 Y. Wang, L. Kong, A. Wang *et al.*. Coherence length tunable semiconductor laser with optical feedback[J]. *Appl. Opt.*, 2009, **48**(5): 969~973

15 D. M. Kane, J. P. Toomey, M. W. Lee *et al.*. Correlation dimension signature of wideband chaos synchronization of semiconductor lasers[J]. *Opt. Lett.*, 2006, **31**(1): 20~22

16 Y. Wang, G. Zhang, A. Wang. Enhancement of chaotic carrier bandwidth in laser diode transmitter utilizing external light injection[J]. *Opt. Commun.*, 2007, **277**(1): 156~160

17 A. Wang, Y. Wang, H. He. Enhancing the bandwidth of the optical chaotic signal generated by a semiconductor laser with optical feedback[J]. *IEEE Photon. Technol. Lett.*, 2008, **20**(19): 1633~1635

18 A. B. Wang, Y. C. Wang, J. F. Wang. Route to broadband chaos in a chaotic laser diode subject to optical injection[J]. *Opt. Lett.*, 2009, **34**(8): 1144~1146

19 T. Matsuura, A. Uchida, S. Yoshimori. Chaotic wavelength division multiplexing for optical communication[J]. *Opt. Lett.*, 2004,

29(23): 2731~2733

20 J. Z. Zhang, A. B. Wang, J. F. Wang *et al.*. Wavelength division multiplexing of chaotic secure and fiber-optic communications[J]. *Opt. Express*, 2009, **17**(8): 6357~6367

21 T. C. Wu, F. Y. Lin. Chaotic communication based on delayed optoelectronic feedback semiconductor laser with two time delays[C]. *SPIE*, 2007, **6783**: 678310

22 M. W. Lee, P. Rees, K. A. Shore *et al*.. Dynamical characterisation of laser diode subject to double optical feedback for chaotic optical communications[J]. *IEE Proc. Optoelectron.*, 2005, **152**(2): 97~102

23 J. P. Goedgebuer, L. Larger, H. Porte. Optical cryptosystem based on synchronization of hyperchaos generated by a delayed feedback tunable laser diode[J]. *Phys. Rev. Lett.*, 1998, **80**(10): 2249~2252

24 L. Larger, J. P. Goedgebuer, F. Delorme. Optical encryption system using hyperchaos generated by an optoelectronic wavelength oscillator[J]. *Phys. Rev. E*, 1998, **57**(6): 6618~6624

25 V. S. Udaltsov, L. Larger, J. P. Goedgebuer *et al.*. Time delay identification in chaotic cryptosystems ruled by delay-differential equations[J]. *J. Opt. Technol.*, 2005, **72**(5): 373~377

26 B. P. Bezruchko, A. S. Karavaev, V. I. Ponomarenko *et al.*. Reconstruction of time-delay systems from chaotic time series[J]. *Phys. Rev. E*, 2001, **64**(5): 056216

27 M. J. Bünner, T. Meyer, A. Kittel *et al.*. Recovery of the time-evolution equation of time-delay systems from time series[J]. *Phys. Rev. E*, 1997, **56**(5): 5083~5089

28 C. Zhou, C. H. Lai. Extracting messages masked by chaotic signals of time-delay systems[J]. *Phys. Rev. E*, 1999, **60**(1): 320~323

29 D. Rontani, A. Locquet, M. Sciamanna *et al*.. Loss of time-delay signature in the chaotic output of a semiconductor laser with optical feedback[J]. *Opt. Lett.*, 2007, **32**(20): 2960~2962

30 R. J. Jones, S. Sivaprakasam, K. A. Shore. Integrity of semiconductor laser chaotic communications to naïve eavesdroppers[J]. *Opt. Lett.*, 2000, **25**(22): 1663~1665

31 S. Sivaprakasam, J. Paul, P. S. Spencer *et al.*. Eavesdropping in all-optical data encryption using chaotic external-cavity diode lasers[C]. *CLEO*, 2001, **1**: Ⅰ-254~255

32 J. B. Geddes, K. M. Short, K. Black. Extraction of signals from chaotic laser data[J]. *Phys. Rev. Lett.*, 1999, **83**(25): 5389~5392

33 G. D. Van Wiggeren, R. Roy. Communication with chaotic lasers[J]. *Science*, 1998, **279**(5354): 1198~1200

34 G. D. Van Wiggeren, R. Roy. Optical communication with chaotic waveforms[J]. *Phys. Rev. Lett.*, 1998, **81**(16): 3547~3550

35 V. S. Udaltsov, J. P. Goedgebuer, L. Larger *et al.*. Cracking chaos-based encryption systems ruled by nonlinear time delay differential equations[J]. *Phys. Lett. A*, 2003, **308**(1): 54~60

36 S. Ortín, L. Pesquera, A. Cofiño *et al.*. Extraction of nonlinear dynamics for laser diodes with feedback in chaotic regime[C]. *SPIE*, 2004, **5452**: 273~282

37 A. Bogris, K. E. Chlouverakis, A. Argyris *et al.*. Subcarrier modulation in all-optical chaotic communication systems[J]. *Opt. Lett.*, 2007, **32**(15): 2134~2136

38 A. Argyris, A. Bogris, I. Giles *et al.*. Subcarrier modulation boosts chaotic optical communication systems to error-free performance[C]. *Opt. Fiber Commun. Conf.* 2009, JWA 45

39 A. Bogris, P. Rizomiliotis, K. E. Chlouverakis *et al.*. Feedback phase in optically generated chaos: A secret key for cryptographic applications[J]. *IEEE J. Quantum Electron.*, 2008, **44**(2): 119~124

40 Q. Zhao, Y. Wang, A. Wang. Eavesdropping in chaotic optical communication using the feedback length of an external-cavity laser as a key[J]. *Appl. Opt.*, 2009, **48**(18): 3515~3520

41 Guo Dongming, Yang Lingzhen, Wang Anbang *et al*.. Modulation of feedback strength to enhance the security of chaos optical communication system[J]. *Acta Physica Sinica*, 2009, **58**(12): 8275~8280

郭东明, 杨玲珍, 王安帮 等. 反馈强度调制增强混沌光通信的保密性[J]. 物理学报, 2009, **58**(12): 8275~8280