文章编号 2095-1531(2014)01-0089-09

光学密码术最新进展

DONATI Silvano(唐士文)[1,2*], ANNOVAZZI-LODI Valerio[1], 王 昭[3]
(1. 意大利帕维亚大学 电子、计算机及生物医学工程系,伦巴第大区 帕维亚 27100,意大利;
2. 国立中兴大学 精密工程研究生院,台中 40227,中国台湾;
3. 西安交通大学 机械工程学院,陕西 西安 710049)

摘要:在总结基于耦合半导体激光器光学混沌的产生和同步原理的基础上,讨论了其在光学密码术中的应用,提出了基于混沌载波的数字加密基本方案和改进方案,包括混沌掩膜法(CM)和混沌键控法(CSK)。最后,给出了混沌加密传输技术的一些最新进展,如相位调制(PM)、自由空间光学链路(FSOL)、多激光器和多用户方案等。

关 键 词:光学密码术;混沌;自混合;激光二级管
中图分类号:O436 **文献标识码**:A doi:10.3788/CO.20140701.0089

Recent advances in optical cryptography

DONATI Silvano[1,2*], ANNOVAZZI-LODI Valerio[1], WANG Zhao[3]
(1. *Department of Electrical, Computer and Biomedical Engineering, University of Pavia, Pavia* 27100, *Italy*;
2. *Graduate Institute of Precision Engineering, National Chung Hsing University, Taichung* 40227, *Taiwan, China*;
3. *Institute of Manufacturing Systems and Quality Engineering, Jiao Tong University, Xi'an* 710049, *China*)
* *Corresponding author, E-mail: silvano. donati@ unipv. it*

Abstract: After summarizing the fundamentals of optical chaos generation and synchronization with coupled semiconductor lasers, we consider their application in optical cryptography, and present basic and more advanced schemes of data coding on chaotic carriers, as proposed in the literature, including Chaos masking (CM) and Chaos Shift Keying (CSK). Finally, we outline some recent developments of the chaos secure transmission technique, such as Phase Modulation (PM), Free-Space Optical Link (FSOL), multi-laser and multi-user schemes.

Key words: optical cryptography; chaos; self-mixing; laser diodes

收稿日期:2013-10-11;**修订日期**:2013-12-13

1 引 言

混沌是由数学和物理学科形成[1]的一个交叉性很强的研究方向,目前已在应用科学领域得到广泛研究。混顿最初是在当系统复杂度[2-3](即独立对象数或微分方程数和系统中的非线性)在很大程度上偏离了19世纪的拉格朗日系统的基础水平时发现的一种新现象。由于复杂度的增加,不能进行传统的简化,系统的伪随机或混沌演变表现出了无法预计的完全不同的新现象,这些现象无法用低复杂度的理论来解释,从而开启了一个新的应用研究领域。

Haken[4-5]首先指出描述激光器的麦克斯韦方程组[5-6]与描述空气中对流的洛伦兹方程最终是一致的,即众所周知的混沌。从那时起,激光中三变量的微分方程被称作洛伦兹-哈肯(L-H)方程,不久又由 Arecchi[6]证明该方程为识别稳态或非稳态类激光器的依据。

2 混沌本质

实际上,半导体激光器属于稳定的B类[6],除非在L-H方程里增加了新的项,比如从其他激光器或从一个可去除的反射镜反馈回的外部注入。有了这个项,L-H就变为众所周知的Lang和Kobayashi方程(或当激励从电场中分离时变成Lamb′s方程),当反馈强度足够大时,系统可能进入混沌,这正是我们所期望的工作机制。

实现混沌的方案如图1所示,既可以是双光源形式(可以是互对称或非对称,也可以是单向的),也可以是辅以外部反射体的单光源形式(自耦合或自混合)。自混合在两个完全不同的领域有着截然不同的应用:(1)在弱注入水平(当返回能量仅为出射能量的 $10^{-8}\sim10^{-3}$ 倍)时,激光场的扰动是腔场的频率和振幅的调制(AM和FM),取决于返回的外部振幅和相位,这时该系统可被用于测量仪器中对外部光程(自混合干涉仪[7])测量或用作光学雷达探测弱反馈信号[8-9],即所谓的相干注入探测器[9]。(2)在中/强耦合(10^{-3}到几个 10^{-2} 倍)时,系统进入高水平动态机制并且开始产生周期和多周期震荡和混沌,为通讯和信息技术提供了一种新方法。在光学混沌和其应用方面可以找到大量的文献,而且最近又出现了有关混沌和相关现象的物理原理[10]和应用方面[11]的大量综述,本文都有引出,以供感兴趣的读者查阅。

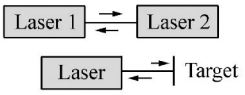


图1 耦合激光器:上,互(对称或非对称)耦合;下,自耦合

Fig. 1 Coupled-lasers: top, mutual (can be symmetrical or asymmetrical) bottom, self-coupling

实验证明,Lang和Kobayashi(L-K)方程[12-13]为混沌新现象的研究提供了一个强有力的工具。利用L-K方程研究双光源单向耦合情况(如图1,上)时,很容易对其到达高动态行为和混沌的过程进行解释,如图2所示。这里用于描述系统演变的参数为激光器1(主)和2(从)中振荡的振幅 $S=E_1E_2^*$ 与耦合强度 K(从激光器1注入到激光

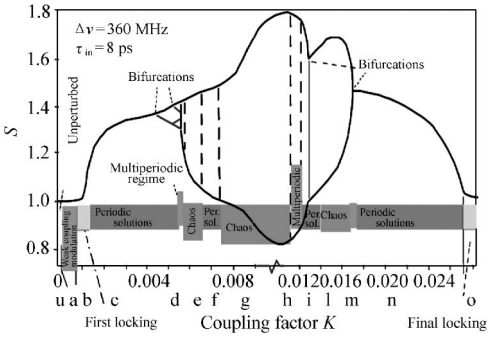


图2 耦合系统的振幅与耦合强度 K 的关系,从无扰机制开始(u区),到周期解机制(c,f,i,n区),多周期(d,h,m)和混沌机制(e,g,l),经过从第一个(b)到最后一个(o区)锁定区

Fig. 2 Beating amplitude of master and slave oscillations of the coupled system, versus the strength of coupling K, starting from the unperturbed regime (region u) and unveiling regimes of periodic solutions (regions c,f,i,n), multiperiodicity (d, h, m) and chaos (e, g, l), passing through first locking (b) to final locking (region o)

器 2 中的比例)[14]。根据以下 3 个指标来识别所处机制:(1)时间序列[或振幅 $S(t)$],(2)频谱 $S(f)$,以及状态图 S vs dS/dt [5,11]。在无扰条件下,时间序列为正弦式,谱为单个峰,状态图是一个圆。接着就是一段窄的弱耦合调制区,再紧接着就是锁定态,这时信号 S 消失了。但是随着 K 的增加,S 重新出现,而且时间序列在每个不同周期有些变形,谱有些次谐波,状态图为双环图,上述现象即所谓的单周期振荡机制。K 更大时,次谐波的数量和振幅增加,状态图有多个环,这是多周期机制。最后,当谐波伴随次谐波、谱大幅扩展、时间序列为随机状时,状态图扩展到所有坐标空间,即进入混沌[11,14]。图 3 给出了多周期解和混沌的图例。

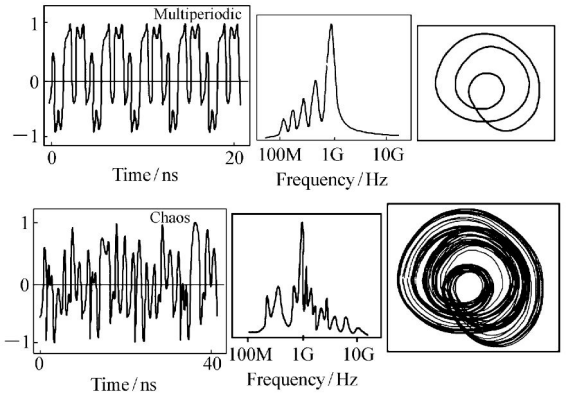


图 3　一个多周期机制(图 2 中 d、h、m 区)和混沌机制(e、g、l)的时间序列(左),频谱(中间)和状态图(右)

Fig. 3　Time series(left), frequency spectrum(center) and state diagram(right) of the beating signal S for the multiperiodic regime(regions d, h, m in Fig. 2) and chaos (e, g, l)

3　混沌的应用

新波形可认为是一类自由响应或某一复杂系统的特征函数,类似于一个反映二阶系统或振荡的自由响应的正弦振荡。与此类似,也可以推测从外部注入到系统中一个混沌信号时,系统将自身调节以跟随注入信号的动态演化,或变为同步。当试图锁定线性二阶振荡器时一般需要一个频率接近于其自由振荡频率的信号,所以应使系统处于自由响应区以便混沌发生器间同步。

在文献[15]中,已经考虑了图 4 所示系统的同步方案,用两个相同的耦合激光系统,系统 1 中包括 LD1 和 LD2,系统 2 中包括 LD3 和 LD4。系统 1 的输出(输出 1)被连接到系统 2 的和节点上,即 LD4 的输入端;另外,LD4 的输出被送到系统 2 的减节点上。这样,当 LD2 和 LD4 的输出不同时,系统 1 对系统 2 施加一个校正使得系统 2 接近系统 1,当二者达到相等时,系统 2 被同步。

利用 L-K 方程对同步方案(图 4)进行建模,发现系统 2 的输出达到稳态解这一过程与起始点无关,对所有自由产生的不同的混沌波形,在小残余误差的几个振荡周期后振幅误差 $(E_2 - E_1)/E_0$ 迅速降为零。

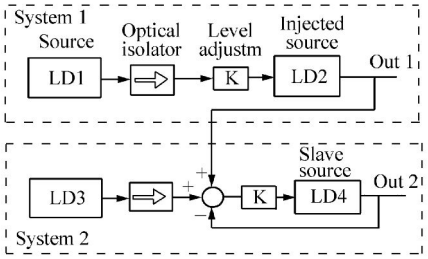


图 4　同步方案:使用两个相同的耦合激光器系统(LD1/LD2 和 LD3/LD4),输出 1 被送到系统 2 中激光器 LD4 的输入和节点上,LD4 的输出被送回相减,所以当输出 2 等于输出 1 时(被同步),校正信号为零

Fig. 4　Scheme of synchronization: two identical coupled-laser systems (LD1/LD2 and LD3/LD4) are used. Out 1 is sent to the sum node at the input of slave laser LD4 of system 2, and the output of LD4 is sent back in subtraction, so that when out 2 is equal to out 1 (is synchronized) no further correction is applied

一个关键问题是对系统参数的敏感性:希望能够容忍对系统标称值较小的偏离,但是这种偏离超过一定的阈值(如 0.5%)时将不能形成同步。对一个实际的系统,误差 $(E_2 - E_1)/E_0$ 是允许参数不匹配的均方根的函数(如图 5,左);去除 E_2 和 E_1 的增益不匹配可得图 5(右)。值得注意的是,激光参数在一个合理的大范围变化时并不影响同步的趋势。为了保证误差比较小则需要参

数不匹配小于 0.2%。一般地,若不匹配大于 0.8%,则误差增大而无法达到同步。混沌同步对系统参数的灵敏性是信号可靠传输的关键,这将在下一节中讨论。

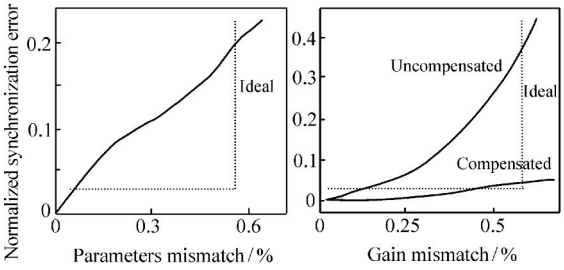


图5 在振幅归一化条件下的同步误差与系统参数(左)及增益(右)不匹配的关系

Fig. 5 Synchronization error versus relative mismatch of system parameters(left) and vs gain mismatch, in uncompensated and amplitude-normalized conditions(right)

4 利用混沌的信息加密

很容易从同步方法想到密码术的第一方案即混沌掩膜(CM):对所产生的混沌加(一个不相关的)载有所要求信息的小信号将不会损害从系统的同步,因为该确定性信号可被忽略,且从接收信号(混沌+信息)中减去同步输出(混沌)信号,便得到了所要的信息[15]。

但是 CM 方案存在缺点:首先加在混沌上的信号波段很窄,用滤波术就可能对信息解密;其次,信息的小振幅(如传输功率的 5%)使得大部分传输功率为混沌所用而不是为信息所用,所以 SNR 很低。问题就变为寻找一种方法能使得信息与混沌功率一样大。

混沌键控法(CSK)可解决上述问题[15]。该方法中,用不同的混沌波形编码数字信息的"0"和"1"位,通过作用到几个参数中的一个(如激光的驱动电流)来控制系统的动态演化过程[16]。所以,每一位利用了整个混沌波形和对应的能量,从而完全利用了可获得的光子和 SNR。

正如图 6 所示,在传输过程中,激光器 LD1 的驱动电流从 J_0 变换到 J_1,编码信息为"0"和"1",最终对编码信息可得到一系列分段的混沌波形。在接收端,两双生系统分别被偏置为 J_0(LD3/LD4)和 J_1(LD5/LD6)。被接收波形的注入与设计位同步,对 LD3/LD4 为"0",对 LD5/LD6 为"1"。

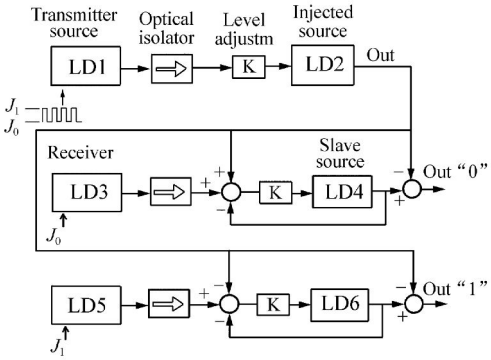


图6 CSK 密码术:二值化的信息"0"和"1"对偏置电流 J_0 和 J_1 进行调制,使激光器 LD1/LD2 产生混沌波形序列。在接收端两双生系统分别被偏置为 J_0(LD3)和 J_1(LD5),而且传输波形的注入使得它们与设计位同步,对 LD3/LD4 为"0",对 LD5/LD6 为"1"

Fig. 6 CSK cryptography: the binary message modulates levels J_0 and J_1 of the bias current, and lasers LD1/LD2 generate a sequence of chaos waveforms, for the "0" and "1" of the message. At the receiver end two twin systems are biased at J_0(LD3) and J_1(LD5) and injection of transmitted waveform makes them synchronize on its designated bit, "0" for system LD3/LD4 and "1" for LD5/LD6

然而无论是 CSK 还是 CM 方案都难以用基本耦合系统单元的双激光器结构实现,系统较复杂。为了构建实际系统,需要简化方案,而利用自混合混沌元(也被称作 DOF—延迟光学反馈)是可行的(如图 7)。

通常全光纤 DOF 结构(如图 8(a))中,激光二极管的光经一透镜会聚到单模光纤上,光纤端面有一倾角(一般为 8~12°)以避免回反光。

光纤末端的反射镜将出射信号光部分反回。通过改变光纤端到反射镜的距离可以调整反馈水平 K,同时 PZT 相位调制器产生相位编码的信息。这样就实现了所谓的长腔系统。

也可以通过集成光学技术实现 DOF 结构(如

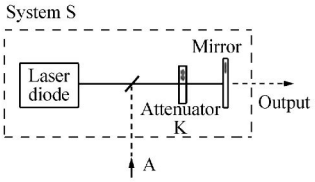


图 7　DOF（延迟光学反馈）混沌发生器：由反射镜形成激光器的自注入耦合机制。分光器注入用于同步的外部信号

Fig. 7　DOF (delayed optical feedback) chaos generator: the laser is subject to a self-injection-coupling regime from the mirror. The beamsplitter injects an external signal for synchronization

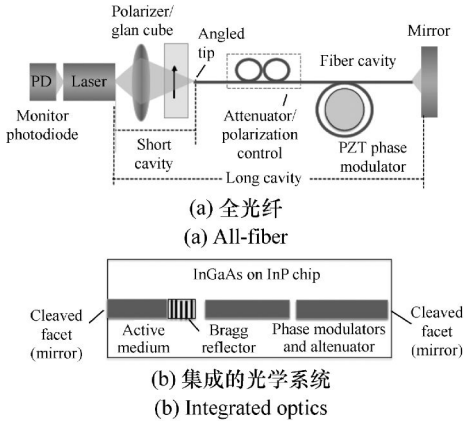


图 8　实现 DOF 方案的技术

Fig. 8　Technologies for implementing the DOF scheme

图 8(b))，在一个单光子集成电路（PCI）中集成主动源（DFB 激光器）、用于振幅/相位调制的主动波导、后反射器（反射镜状的芯片切面）。这一结构提供了更加稳定的短腔系统。

图 9 给出了 FET 欧洲研究合同[17]中用 InP 材料制做的集成电路芯片图。

CM 和 CSK 的实际解决方案已有文献报道。图 10 给出了一个 CSM—PM 系统的例子[18]，采用短腔 DOF，$LiTaO_3$ 相位调制器将信息以相位 $\Delta\psi_{in}$ 加到发射器与接收器的总相位 2 ks 上，s 为从发射器到接收器的光程。因为短腔 DOF 对外腔相位敏感，混沌波形以某种方式被相位 $\Delta\psi_{in}$ 编码。在接收端，相同的 DOF 中的相位调制器电压被设置为零，因而该接收器只对零输入信息或相位 $\Delta\psi_{in}$ 完全同步。随着发射器和接收器相位差的增

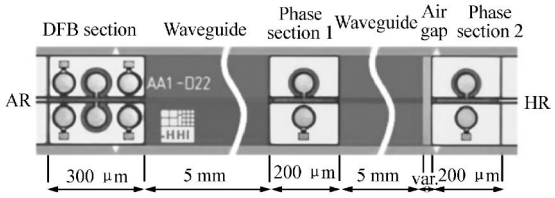


图 9　一个 DOF 短腔 PIC 芯片，由在 InP 基底上的 InGaAs 波导、并集成了一个 DFB 激光器、两个 5 mm 波导和两个相位调制器，实现传输中的相位编码方案（见正文）

Fig. 9　A DOF short-cavity PIC-chip, fabricated by InGaAs waveguides on a InP substrate, and incorporating a DFB laser, two 5-mm waveguides and two phase modulators, to realize a phase-coded scheme of transmission (see text)

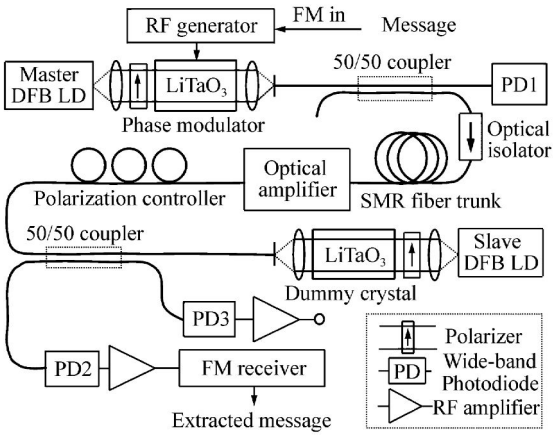


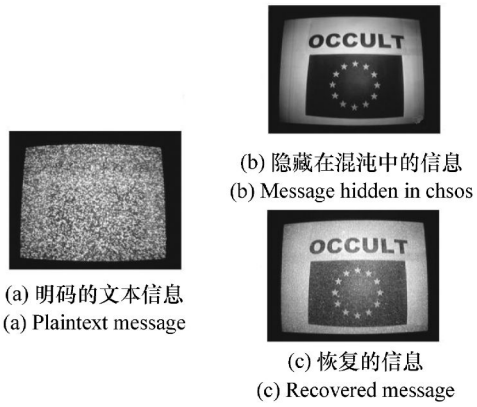
图 10　短腔 DOF—CSK 系统，采用 $LiTaO_3$ 相位调制器将 FM 编码的信息以相位变化量形式作用在腔上，因而也作用在由 DOF 产生的混沌波形上。在 DOF 接收器上，相同的调制器使得只有在零相位时才能完全同步，实现了相位到振幅的转换。光电探测后，FM 解调器对信息解码

Fig. 10　A short-cavity DOF-CSK system, uses a $LiTaO_3$ phase modulator to impress an FM-coded message as a phase variation in the cavity and hence in the chaos waveform generated by the DOF. At the DOF receiver, a dummy modulator allows for full synchronization only for zero phase deviation, acting as a phase-to-amplitude converter. After photodetection, an FM demodulator decodes the message

加,其混沌波形的相关性逐步减小,该过程就是一种相位到振幅的转换。光电探测后再经过 FM 解调,可得到正比于 $\Delta\psi_{in}$ 也即正比于输入的信号。

在所有利用混沌进行安全传输的解决方案中,其安全性是基于对激光参数的同步敏感性。两个用户必须共用一个“双生”激光器对,比如参数非常相近的激光器,它们一般是来自于同一晶片。因此对窃听者来说很难找到与双生对匹配的激光器来与其混沌匹配从而非法解码以获取信息。

利用标准双激光系统、基于混沌的 GHz 范围的数字信号的传输已经在雅典城市网络中得到验证[19],而且还对 RF 信号的模拟传输进行了实验测试(如图 11)[20]。



(a) 明码的文本信息
(a) Plaintext message

(b) 隐藏在混沌中的信息
(b) Message hidden in chsos

(c) 恢复的信息
(c) Recovered message

图 11 视频信号传输实验

Fig. 11 Experiment of transmission of a video signal

未来长距离传输的几种基础模块也已经被提出,如用于 WDM 的混沌波长转换器[21]以及混沌重复器[22]。而且也对如何更加有效地保护信息的编码方法进行了研究[23]。文献[13]还给出了基于电光反馈的另一种方案。

5 最新进展

除了基本的双激光器方案外,一些更先进的方案(如图 12)也被提出,它们对授权用户具有更好的同步质量,这些用户共用匹配的激光对,因此可以更好地防止信息被窃听。因为这些方案是对称的(与基本的双激光有所不同),Tx 和 Rx 都被第三个(混沌)激光器(驱动器 Drv)注入,所以其同步性和安全性都比较好。

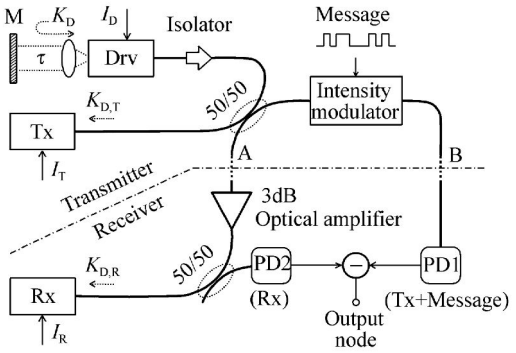


图 12 三激光器 CM 的混沌系统:采用一个普通的源驱动器(Drv)产生混沌并使一对双生激光器(Tx 和 Rx)同步。通过在接收器端采用基本的混沌相减方法而恢复信息

Fig. 12 A three-laser CM crypto-system uses a common source driver (Drv) to route into chaos and synchronise a pair of twin lasers (Tx and Rx). The message is recovered as in the basic scheme by chaos cancellation at the receiver

图 12 是一个实现三激光器方案的 CM 结构[24]。这里,Drv 激光器通过延迟的光学反馈产生混沌,Rx 和 Tx 可能是开环,也可能是通过一个反射镜形成的局部光学弱反馈。Drv 的 RF 功率

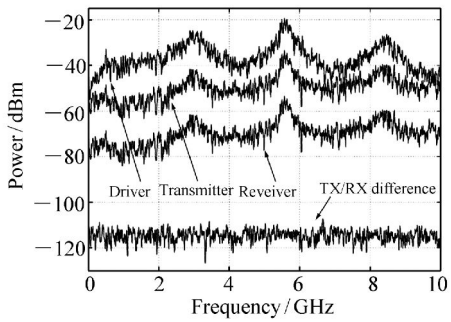


图 13 图 12 方案中 Drv、Tx 和 Rx 的 RF 功率谱。为了便于观察,将 Drv 和 Rx 曲线分别上移和下移 20 dB,给出了差信号

Fig. 13 Numerical RF power spectra for Drv, Tx and Rx in the scheme of Fig. 12. For better visualization, the traces of Drv and Rx have been shifted upwards by 20 dB and downwards by 20 dB, respectively. The difference signal is also shown

谱、Tx 功率谱和 Rx 功率谱以及它们的差如图 13 所示。图 14 模拟了 5Gb/s 信息的传输,给出了明码文本信息、其隐藏在混沌中以及混沌相减后恢复信息的 RF 谱,还给出了恢复信息的眼图。

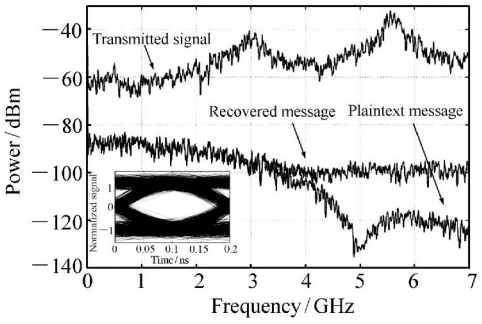


图 14　图 12 方案中使用 CM 传输的 5Gb/s 数字信息的 RF 谱。插图为恢复信息的眼图

Fig. 14　Numerical RF spectra for CM transmission of a 5 Gb/s digital message with the scheme of Fig. 12. The eye diagram of the recovered message is shown in the inset

实验中很难达到如此高水平的去混沌,但是证明了三激光器比双激光器具有的优势。增加一个激光器不算缺点,因为在网络中用户对之间的几个互联可共用同一个 Drv。

三激光器方案经过调整很容易用于自由空间的传播。最近自由空间的光学链路(FSOLs)的安全性已引起人们的关注,特别是对那些快速扩张其通讯基础建设的国家,因为 FSOLs 开放的光路容易导致信息被窃听。

图 15 给出了用于自由空间传播的一个三激光器方案[25],这里的衰减通常比较大,Drv 发出的光学信号在注入到 Rx 和 Tx 前被探测和放大,对 Tx 到 Rx 的注入也同样被探测和放大。一般都是电子放大,与光学放大相比其成本低,在系统中容易实现。

同样的方案也为室内、火车或飞机中的信息安全传输提供了一个可行的结构,许多用户共用同一个传播通道以及 Drv,它们可被安装在诸如天花板的上面。一种对标准结构改进后的方案曾被用于多用户网络中,该网络采用混沌加密。迄今为止的方案实际上都限于共用一双生激光对的两个特定用户间的信息传输。然而大多数情况下

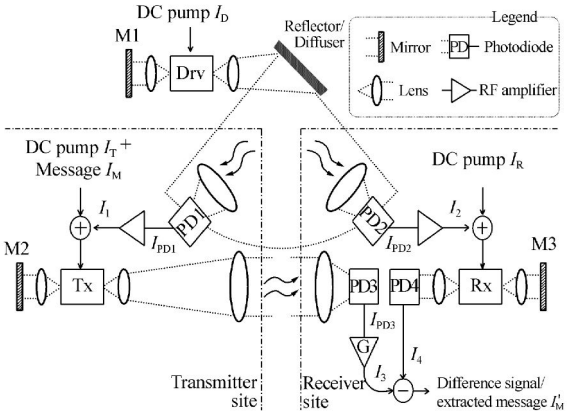


图 15　自由空间进行数据安全传输的结构。由于通道中的高衰减,Drv 的光学出射信号在注入 Rx 和 Tx 之前先被探测并放大,Tx 注入到 Rx 前也一样

Fig. 15　Configuration for secure data transmission in free-space. Due to high channel attenuation, the optical emission of the Drv is photodetected and amplified before injection into Rx and Tx. The same is done for Tx to Rx injection

需要多个用户组成一个网络,且能够以安全的方式自由地进行信息传输。实际中很难在一个晶圆上找到多于 3 或 4 个匹配的器件以保证有效的同步,所以多用户传输需要每一个用户为其另一伙伴持有一个激光器(双生对之一),显然这是不现实的。另一种方案就是增加信息的幅度从而可降低同步的水平,但这种情况下安全性会降低。

最近提出了一种可能的解决方案[26],该方案来源于众所周知的公开键钥技术。利用该技术,使得在一个网络中任意两个注册用户交换数据成为可能。这种可能性可由第三方提供,第三方保证网络的安全性。对每一个注册用户都需要一对双生混沌激光器,一个由第三方持有,另一个由用户自己持有。基本的混沌传输的双激光器(或三激光器)方案即可在用户与第三方之间,也可在两用户之间进行数据安全交换。在第二种情况,第三方将合适的混沌载于 Tx 上,在那里加载数据并被送到 Rx。基于这样一个框架,有几种方案可以考虑,详见文献[26]。

6 结 论

本文基于耦合半导体激光器中光学混沌产生和同步的原理,讨论了其在光学密码术中的应用。提出基于混沌载波的数字加密基本方案和改进方案,详细介绍了 CM 和 CSK。最后,给出了混沌加密传输技术的一些最新进展,如 PM、FSOL、多激光器和多用户方案等。

参考文献:

[1] WIECZOREK S,KRAUSKOPF B,SIMPSON T B,*et al.*. The dynamical complexity of optically injected semiconductor lasers[J]. *Phys. Report*,2005,416:1-128.

[2] MEYERS R. *Encyclopedia of Complexity and System Science*[M]. Berlin:Springer,2009.

[3] TSOUKAS H. Chaos, complexity and organization theory[J]. *Organization*,1998,5:291-313.

[4] HAKEN H. Analogy between higher instabilities in fluids and lasers[J]. *Phys. Lett.*,1975,53(A):77-78.

[5] OHTSUBO K. *Semiconductor Lasers:Stability, Instability and Chaos*[M]. 2nd edition, Springer Series Optical Sciences vol. 111. New York:Springer-Verlag,2009.

[6] ARECCHI F T,PUCCIONI G L,TREDICCE J R. Deterministic chaos in laser with injected signal[J]. *Optics Commun.*, 1984,51:308-314.

[7] DONATI S. Developing self-mixing interferometry for instrumentation and measurements[J]. *Laser and Photonics Review*, 2012,6:393-417.

[8] DONATI S. Responsivity and noise of self-mixing photodetection schemes[J]. *IEEE J. Quantum El*,2011,47:1428-1433.

[9] DONATI S. *Photodetectors*[M]. New York:Prentice Hall,Upper Saddle River,N. J.,2000.

[10] SORIANO M C,GARCIA-OJALVO J,MIRASSO C,*et al.*. Complex photonics:dynamics and applications of delay-coupled semiconductors lasers[J]. *Review Modern Physics*,2013,85:421-470.

[11] DONATI S,HWANG S K. Chaos and high-level dynamics in coupled lasers and their applications[J]. *Prog. Quantum Electronics*,2012,36(2-3):293-341.

[12] LANG R,KOBAYASHI K. External optical feedback effects on semiconductor injection laser properties[J]. *IEEE J. Quant. Electr.*,1980,QE-16:347-355.

[13] DONATI S,MIRASSO C. Optical chaotic cryptography, feature issue of[J]. *IEEE J. Quantum Elect.*,2002,QE-38: 1138-1184.

[14] ANNOVAZZI-LODI V,DONATI S,MANNA M. Chaos and locking in a semiconductor laser due to external injection[J]. *IEEE J. Quantum Electronics*,1994,QE-30:1537-1541.

[15] ANNOVAZZI-LODI V,DONATI S,SCIR A. Synchronization of chaotic injected-laser systems and its application to optical cryptography[J]. *IEEE J. Quant. Electr.*,1996,QE-32:953-959.

[16] ANNOVAZZI-LODI V,DONATI S,SCIR A. Synchronization of chaotic lasers by optical feedback for cryptographic applications[J]. *IEEE J. Quant. Electr.*,1997,QE-33:1449-1454.

[17] SYVRIDIS D,ARGIRIS A,BOGRIS A,*et al.*. Integrated devices for optical chaos generation and communications applications[J]. *IEEE J. Quantum Electron.*,2009,45(11):1421-1428.

[18] ANNOVAZZI-LODI V,BENEDETTI M,MERLO S,*et al.*. Message encryption by phase modulation of a chaotic optical carrier[J]. *IEEE Phot. Techn. Lett.*,2007,19:76-78.

[19] ARGYRIS A,SYVRIDIS D,LARGER L,*et al.*. Chaos-based communication link at high bit rate using commercial fiber-optic link[J]. *Nature Letters*,2005:343-346.

[20] ANNOVAZZI-LODI V,BENEDETTI M,MERLO S,*et al.*. Optical chaos masking of video signals[J]. *IEEE Photonic Technology Letters*,2005,17:1995-1997.

[21] ANNOVAZZI-LODI V,AROMATARIS G,BENEDETTI M,*et al.*. All-optical wavelength conversion of a chaos masked signal[J]. *IEEE Phot. Techn. Lett.*,2007,19:1783-1785.

[22] LEE M W,SHORE K A. Demonstration of a chaotic optical message relay using DFB laser diode[J]. *IEEE Phot. Tech. Lett.*,2006,18:169-171.

[23] URSINI L,SANTAGIUSTINA M,ANNOVAZZI-LODI V. Enhan-cing chaotic communication performances by manchester coding[J]. *IEEE Photonics Technology Letters*,2008,20:401-403.

[24] ANNOVAZZI-LODI V,AROMATARIS G,BENEDETTI M,*et al.*. Private message transmission by common driving of two chaotic lasers[J]. *IEEE J. Quantum Electronics*,2010,46:258-264.

[25] ANNOVAZZI-LODI V,AROMATARIS G,BENEDETTI M,*et al.*. Secure optical transmission on a free space optics data link[J]. *IEEE J. Quantum Electronics*,2008,44:1089-1095.

[26] ANNOVAZZI-LODI V,AROMATARIS G,BENEDETTI M. Multi-user private transmission with chaotic lasers[J]. *IEEE J. Quantum Electronics*,2012,48:1095-1101.

作者简介:

DONATI Silvano(唐士文)(1942—),男,意大利人,博士,教授(chair professor),博士生导师,IEEE 及 OSA 会士,1966 年于意大利米兰大学获博士学位,在电子学(CCD 中的噪音、耦合振荡器)和光电仪器(激光干涉仪、光纤陀螺仪、光纤电流传感器)领域做出了突出贡献,近年来主要从事全光纤无源器件、光电探测器中的噪音、光学混沌和密码术以及光混频等方面的研究。E-mail:silvano. donati@ unipv. it

ANNOVAZZI-LODI Valerio(1955—)男,意大利人,教授,AEIT 及 IEEE 光子学会高级会员,1979 年、1984 年于意大利帕维亚大学分别获学士、硕士学位,主要从事 MEMS、MOEMS、振荡器和激光器中的混沌及其应用等方面的研究。E-mail:valerio. annovazzi@ unipv. it

王　昭(1964—),女,陕西西安人,博士,教授,博士生导师,1986 年于华中科技大学获学士学位,1989 年于中国科学院西安光学与精密机械研究所获硕士学位,1998 年于西安交通大学获博士学位,主要从事光电测量及光学信息处理方面的研究。E-mail:wangzhao@ mail. xjtu. edu. cn