

一种新型的双向长距离光纤混沌保密通信系统性能研究*

刘宇然 吴正茂 吴加贵 李萍 夏光琼†

(西南大学物理科学与技术学院, 重庆 400715)

(2011 年 5 月 17 日收到; 2011 年 5 月 24 日收到修改稿)

基于两个在驱动混沌信号注入下的响应半导体激光器之间的混沌同步, 提出了一种新型的可实现信息双向、长距离保密传输的系统, 并建立了相应的理论模型. 利用该理论模型, 研究了系统的双向传输性能、安全性能以及系统性能随传输距离的变化. 结果表明: 两个响应激光器在受到发自同一驱动混沌激光器的混沌光注入下, 其混沌输出虽然与注入混沌信号相差很大, 但两个响应激光器的混沌输出却能够实现非常好的无时间延迟的等时同步; 对窃听者可能获取信息的各个途径进行了考察, 结果显示该系统具有很好的安全性; 采用普通单模光纤作为传输信道, 信息经过 50 km 传输后, 解调信息 Q 因子可达到 6 以上; 采用色散位移光纤, 信息经过 200 km 的传输, 解调信息 Q 因子还可达 6 以上.

关键词: 半导体激光器, 混沌同步, 双向通信, 光纤

PACS: 42.55.Px, 05.45.Vx

1 引言

随着信息社会的高度发展, 信息的安全越来越受到人们的重视. 由于混沌具有对初值敏感、类噪声性、遍历性、难以长期预测等特性, 可用于开发出基于物理层面的信息保密传输技术. 1990 年, Pecora 和 Carroll 提出混沌同步让混沌应用于信息保密传输成为可能^[1]. 其中, 基于半导体激光器 (semiconductor laser, SL) 的激光混沌系统, 因具有宽带宽、高度复杂性、与现有光纤通信系统之间良好的兼容性等优势^[2-6], 非常适合用于高速长距离保密通信. 2005 年, Argyris 等人基于 SL 的激光混沌在雅典城的商用光纤网络中实现了 1 Gbit/s、传输距离 120 km 的单向保密通信^[2], 很好地验证这种技术的可行性. 然而, 仅仅能实现信息的单向传输是不够的, 信息的双向、直至多向传输是保密通信发展的必然.

2006 年, Klein 等人提出了基于公共信道的双向保密通信思路^[7]. 据此人们提出了多种基于 SLs

的双向激光混沌保密通信方案^[8-11]. 如 Vicente 等人提出在简单互耦 SLs 系统之间插入半透半反镜的方案^[8]; Zhang 等人提出采用极不对称互注入 SLs 系统的方案^[9]; Deng 等人提出了采用光电互耦 SLs 系统的方案^[10]. 这些方案都是基于两个直接互耦半导体激光器之间的混沌同步实现信息的双向保密传输, 并且在研究过程中没有考虑光纤信道对信息传输的影响. 最近, Uchida 等人提出了一种实现非线性振子间混沌同步的新方案^[12]. 在该方案中, 一个子系统输出的复杂噪声或者混沌信号, 注入到另外两个相似但独立的非线性振子中. 在合适条件下, 两个非线性振子将输出一对波形变化一致的信号. 依据这种思路, Yamamoto 等人采用 SL 实现了几米距离的激光混沌同步^[13]. 与传统的同步系统不同, 这里的两个 SL 之间是没有直接互耦的. 考虑到实际的应用, 能实现几十公里的双向光纤保密通信系统将更具应用前景, 而目前关于这种光纤长距离双向混沌通信系统性能的研究还非常缺乏.

* 国家自然科学基金 (批准号: 60978003, 61078003, 61178011, 11004161), 重庆市自然科学基金 (批准号: 2010BB9125) 和西南大学中央高校基本科研业务费专项资金 (批准号: XDJK2009B010, XDJK2010C021) 资助的课题.

† E-mail: gqxia@swu.edu.cn

在本文中,我们提出了一种新型双向长距离光纤混沌保密通信系统方案.该方案具有良好的可扩展性,可将系统延展到长距离情况.同时对该方案的双向通信性能、信息安全性以及光纤信道长度等对系统性能的影响进行了系统的研究.

2 系统结构

双向长距离光纤混沌保密通信系统示意图如图 1 所示.通过控制带外腔延时反馈的驱动半导体激光器 (DL) 的工作参数,使 DL 得到复杂的激光混沌输出.从 DL 输出的混沌信号通过光纤耦合器 (FC₃) 分成相等的两部分,其中一部分经光纤分支 F₁ 注入到响应激光器 1 (RL₁) 中,另一部分经光纤分支 F₂ 注入响应激光器 2 (RL₂) 中.当两个响应激光器具有相同的内部参数,且从 DL 输出的混沌信号所经历的两个光纤支路的性能参数一致时,RL₁ 和 RL₂ 接收到来自于 DL 的混沌信号将完全一致,从而系统具有良好的对称性.在合适的驱动作用下,两个激光器 RL₁ 和 RL₂ 之间可以实现相互间延时为零的等时混沌同步^[15].在系统中,只要能保持两个激光器 RL₁ 和 RL₂ 之间良好的对称性,且维持从 DL 来的足够大的注入水平,即便两个支路的光纤长度延展到几十、上百公里,两个激光器 RL₁ 和 RL₂ 之间也可以实现很好的等时混

沌同步.

在 RL₁ 和 RL₂ 实现了很好的等时混沌同步后,可在 RL₁ 和 RL₂ 之间实现信息的双向保密传输.关于信息的保密加载与解调,传统的激光混沌保密通信系统是将信息和混沌载波混合后一起注入到接收激光器中,然后利用混沌滤波效应解调出信息.但是这种方法在大多情况下(除附加混沌调制方式以外)都会破坏发射激光器和接收激光器之间的对称性,从而难以得到优质的信息解调效果.在本文中,我们将采用一种新颖的信息加载和解调方式.首先如图 1 所示,考察从 RL₁ 到 RL₂ 的加载信息 1 (message₁) 的传输过程. RL₁ 的激光混沌输出经耦合器 FC₁ 后被分成两部分,其中一部分作为信息 1 的混沌载波.信息 1 通过混沌调制 (chaotic modulation, CM) 方式与混沌载波混合在一起,经光纤链路 F₃ 传输到 RL₂ 的前端,再通过光环形器 (OC₂)、光放大器后注入到光电探测器 (PD₃) 中.同时, RL₂ 输出的混沌信号经光耦合器 (FC₂) 被分成两部分,其中一部分通过光纤延迟线 (DF₂)、光放大器后注入到光电探测器 (PD₄) 中.通过对 PD₃ 的输出电信号和 PD₄ 的输出电信号做“减”操作,并经过必要的滤波处理,即可解调出除外从 RL₁ 端传输来的信息 1. 相似地,从 RL₂ 传输到 RL₁ 的信息 2 (message₂),经历相同的过程也可以得到有效解调.

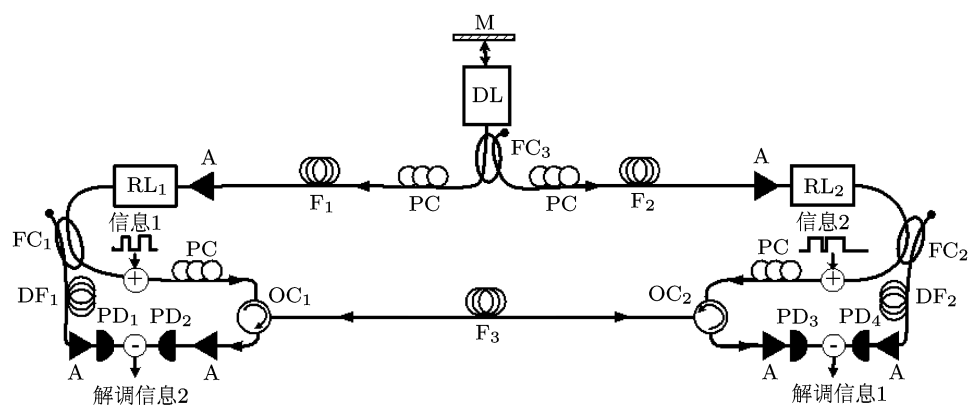


图 1 双向长距离光纤混沌保密通信系统示意图 (DL 为驱动激光器; M 为反射镜; RL 为响应激光器; F 为传输光纤; DF 为延迟光纤; FC 为 50/50 光纤耦合器; PC 为光偏振控制器; OC 为光环形器; A 为光纤放大器; PD 为光电探测器)

3 理论模型

对于系统中所包含的三个激光器的动力学行为,可采用如下包含外腔反馈或外光注入的 Lang-

Kobayashi 速率方程组来描述^[3]:

$$\begin{aligned} \frac{dE_D(t)}{dt} = & \frac{1}{2}(1+i\epsilon)[G_D - \frac{1}{\tau_p}]E_D(t) \\ & + \frac{k_D}{\tau_{in}}E_D(t - \tau_D)\exp(-i\omega\tau_D) \end{aligned}$$

$$\begin{aligned}
& + \sqrt{2\chi N_D(t)} \xi_D(t), \\
\frac{dE_{R1,2}(t)}{dt} = & \frac{1}{2}(1 + i\varepsilon)[G_{R1,2} - \frac{1}{\tau_p}]E_{R1,2}(t) \\
& + \frac{k_{1,2}}{\tau_{in}}E_D(t - \tau_{inj1,2})\exp(-i\omega\tau_{inj1,2}) \\
& + \sqrt{2\chi N_{R1,2}(t)}\xi_{R1,2}(t), \quad (1) \\
\frac{dN_{D,R1,2}(t)}{dt} = & \frac{I}{q} - \frac{N_{D,R1,2}(t)}{\tau_n} - G_{D,R1,2} |E_{D,R1,2}(t)|^2.
\end{aligned}$$

式中, 下标 D 和 R 分别表示 DL 和 RL, 1 和 2 分别对应不同 RL 的编号. E 为激光器的慢变场振幅, N 为载流子数, N_0 为透明载流子数, ε 为线宽增强因子, $G = g(N(t) - N_0)/(1 + \rho|E(t)|^2)$ (g 为微分增益系数, ρ 为饱和增益系数), τ_p 为光子寿命, τ_n 为载流子寿命, k_D 为 DL 的外腔反馈系数, $k_{1,2}$ 为 DL

对 RL_1 和 RL_2 的注入系数, τ_{in} 为光子在激光器内腔中的往返时间, τ_D 为 DL 的外腔反馈时间, $\tau_{inj1,2}$ 为 DL 对 RL_1 和 RL_2 的注入时间, ω 为角频率, χ 为自发辐射率, I 为偏置电流, q 为单位电荷, ξ 表征高斯白噪声.

混沌信号在长距离光纤中的演化可以由非线性薛定谔方程来描述^[4,14,15]:

$$i \frac{\partial E(z, T)}{\partial z} = -\frac{i}{2}\alpha E - \gamma |E|^2 E + \frac{1}{2}\beta_2 \frac{\partial^2 E}{\partial T^2}, \quad (2)$$

式中, $E(z, t)$ 表示激光场的慢变振幅, z 为传输的距离, α 为光纤损耗常数, γ 表征非线性效应, β_2 为光纤的二阶色散常数, T 是以信号脉冲群速度 V_g 运动的参照系中的时间变量 ($T = t - z/V_g$).

另外, 两个混沌信号 (信号 i 和信号 j) 之间的同步性可以用关联函数 $C(t)$ 来描述, 公式如下:

$$C_{i,j}(\Delta t) = \frac{\langle [P_i(t) - \langle P_i(t) \rangle][P_j(t + \Delta t) - \langle P_j(t) \rangle] \rangle}{\langle [P_i(t) - \langle P_i(t) \rangle]^2 \rangle^{1/2} \langle [P_j(t + \Delta t) - \langle P_j(t) \rangle]^2 \rangle^{1/2}}, \quad (3)$$

式中, $\langle \rangle$ 表示时间平均, Δt 表示关联函数的时移, P 表示输出场强度. $|C|$ 的取值范围为 0 和 1 之间, $|C|$ 越接近 1 表明两个混沌信号同步性越好.

对于系统通信的质量, 可以采用 Q 因子来评估. Q 因子的定义为

$$Q = \frac{\langle P_1 \rangle - \langle P_0 \rangle}{\sigma_1 + \sigma_0}, \quad (4)$$

式中, $\langle \rangle$ 表示时间平均, P_1 和 P_0 分别表示比特“1”和比特“0”的能量, σ_1 和 σ_0 分别表示比特“1”和比特“0”的能量的标准差. Q 因子越高表示通信质量越好.

另外, 对于信号在光纤中的长距离传输, 信号能量会随着传输距离的增加而不断损耗. 而通过引入光放大器可以较好补偿这些由长距离光纤传输而导致的能量损耗. 因此, 在本文的数值模拟中, 为了计算的方便, 暂时忽略了光纤的损耗.

4 结果与讨论

在数值计算中, 相关参数取值为 $\varepsilon = 3$, $\tau_p = 2$ ps, $\tau_n = 2$ ns, $\tau_D = 5$ ns, $k_D = 2.5 \times 10^{-2}$, $k_{1,2} = 4 \times 10^{-2}$, $\tau_{in} = 1$ ps, $\chi = 1.1 \times 10^3$ s⁻¹, $I = 29$ mA, $\omega = 1.219 \times 10^{15}$ rad/s, $q = 1.602 \times 10^{-19}$ C, $g = 1.5 \times 10^{-8}$ ps⁻¹, $\rho = 1 \times 10^{-7}$, $N_0 = 1.5 \times 10^8$.

在本系统中, 为了方便计算, DL 对 RL_1 和 RL_2 的注入延时设为相等 $\tau_{inj1} = \tau_{inj2} = \tau_{inj}$.

4.1 不考虑光纤信道的影响

首先, 设定 DL 对 RL_1 和 RL_2 的注入延时 $\tau_{inj} = 3$ ns, 不考虑光纤传输的影响. 图 2 给出了此时任意两个激光器输出的时间序列及其相对应的关联函数图. 从图 2 中可以看出, DL 和 RL_1 (RL_2) 输出的时间序列存在较大的差异, 相应的关联函数在延时 $\Delta t = 3$ ns 处取得的最大值 $C_{max} = 0.77$, 而两个响应激光器 RL_1 和 RL_2 输出的时间序列完全相同, 关联函数在 $\Delta t = 0$ ns 处达到 1, 说明 RL_1 和 RL_2 实现了完全的等时同步 (IS). 基于 RL_1 和 RL_2 的等时同步, 可以实现两者之间的双向混沌保密通信.

图 3 给出了信息在 RL_1 和 RL_2 输出的混沌载波中的隐藏效果以及在接收端的解调效果. 其中信息对混沌载波的调制深度为 2%, 调制速率为 1 Gbit/s. 从图 3 (a2, b2) 中可以看出, 信息能很好地隐藏在混沌载波中. 图 3 (a3, b3) 是对图 3 (a2, b2) 中混沌载波做“减”操作, 并经过四阶巴特沃斯低通滤波器滤波处理后的解调信息波形图. 图 3 (a4, b4) 进一步给出了这些解调信息对应的眼图. 可以看出, 信息在两个接收端都得到很好地解调, 实现了高质量的双向通信.

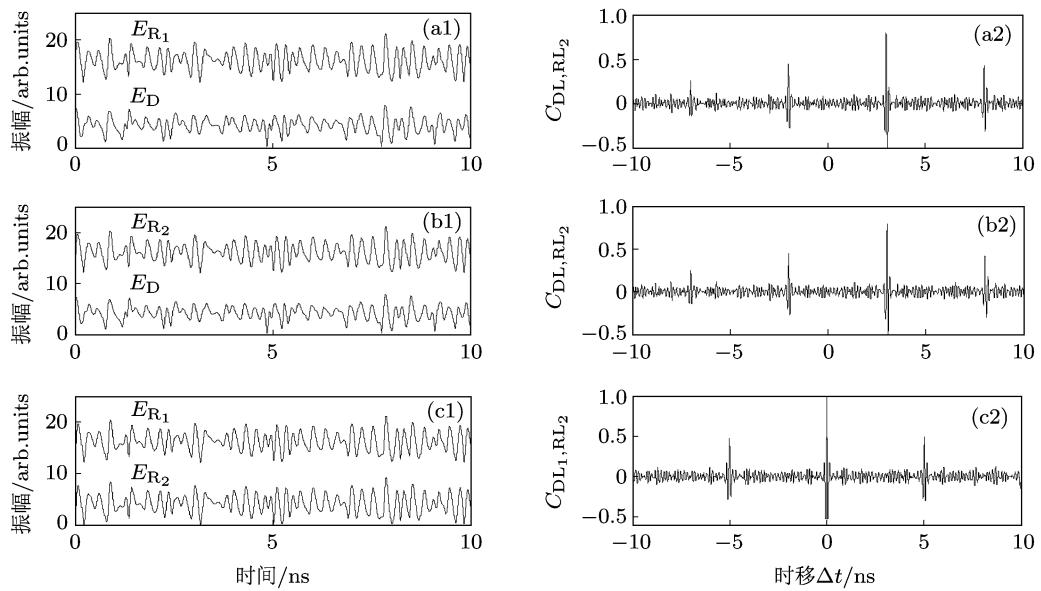


图2 DL,RL1,RL2 三个激光器中任意两个激光器输出的混沌时间序列对比 (a1—c1) 以及它们之间的相关函数图随时延的变化 (a2—c2)

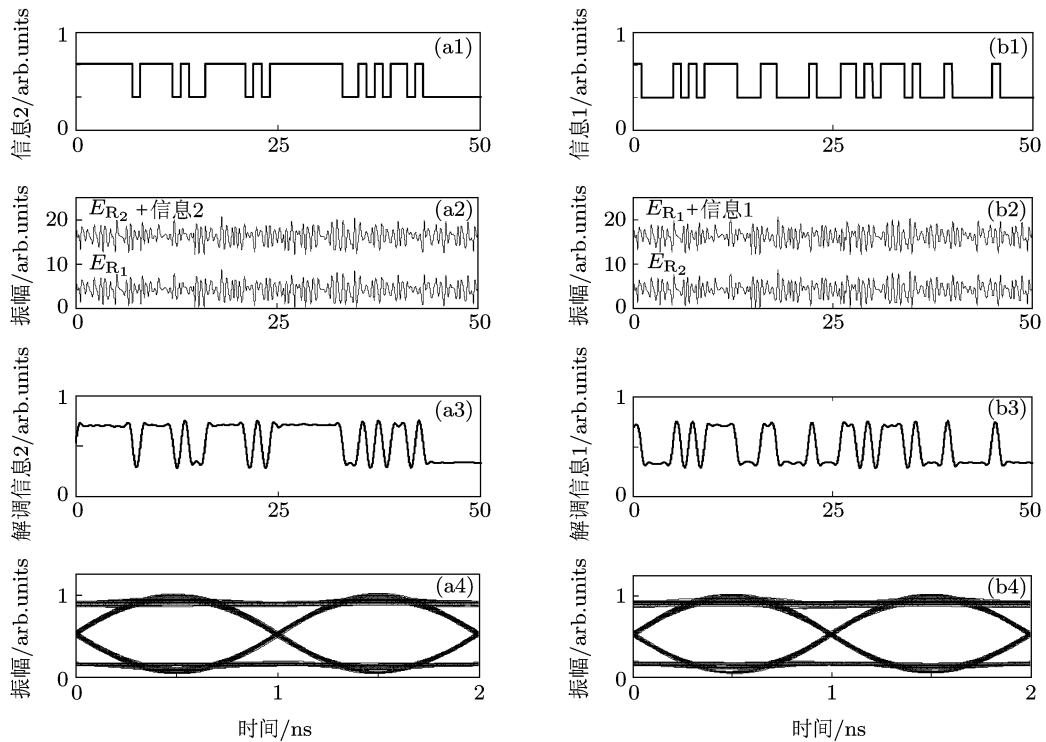


图3 信息的双向加载与解调 (a1,b1) 为加载的伪随机比特序列;(a2,b2) 为信号接收端接收到的信号 (上图) 以及接收端激光器输出的混沌信号 (下图);(a3,b3) 为解调后的比特序列;(a4,b4) 为解调信息的眼图

接下来我们将考察系统的安全性能. 根据图 3 (a1,a2), 信息很好地隐藏在混沌载波中, 窃密者不能直接从载波中获得所隐藏的信息, 这与传统单向混沌通信类似. 虽然直接从混沌载波中不能窃取到传输的信息, 但窃密者是否还有其他的途径获得传输信息呢? 仔细分析如图 1 所示的系统构架, 考察窃

密者所有可能采取的途径: 途径一, 窃密者可能通过截取 F_3 光纤链路中沿两个相反方向传输的信号然后通过延时对比来窃密. 图 4 (a1,a2) 给出了窃密者此时解调出的信息. 此时, 窃听者获取的信息是双向传输比特信息之间的差值, 并不能获得信息本身; 途径二, 窃密者可能通过截取 F_1 光纤链路和 F_3

光纤链路中传输信号进行窃密. 图 4 (b1,b2) 给出了此种途径解调出的信息以及相应的眼图. 此时信息的时间序列变化混乱, 对应眼图完全闭合, 因此信息不能被解调, 这是因为 DL 与 RL_1 之间较差的同步效果 (如图 2(a2)) 所致. 途径三, 窃密者可能通过

截取 F_2 光纤链路和 F_3 光纤链路中传输信号进行窃密, 情况与途径二类似, 信息仍将不能被解调. 总之, 无论截取一路或者多路信号, 窃密者都不能解调出信息, 从而确保了信息双向传输的安全性.

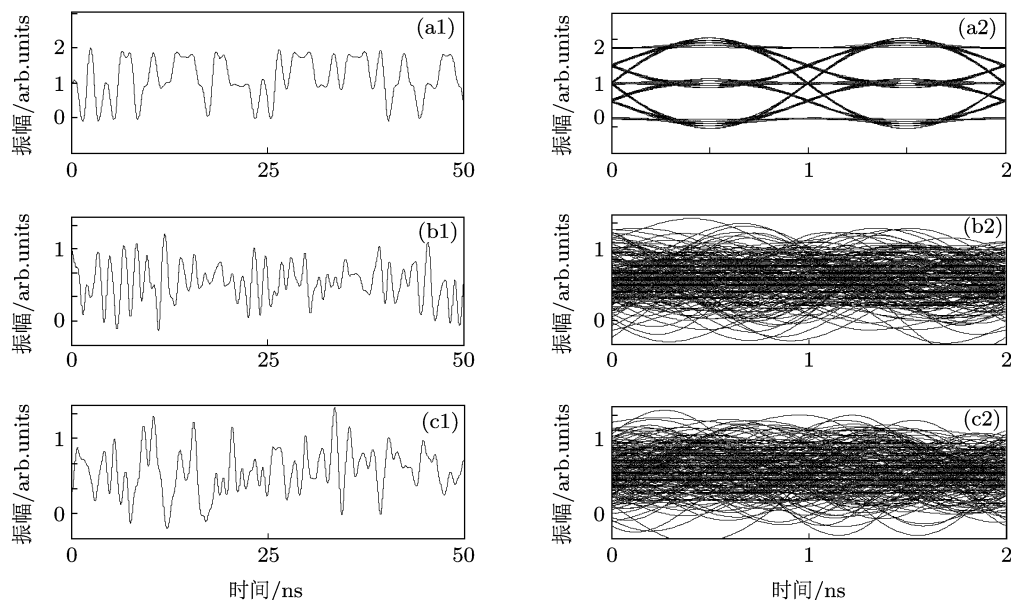


图 4 窃密者获得的信息 (左图) 及对应眼图 (右图) (a1,a2) 为截取信道 F_3 中沿两个相反方向传输信号所获得信息;(b1,b2) 为截取信道 F_1 和 F_3 的传输信号所获得信息;(c1,c2) 为截取信道 F_1 和 F_3 的传输信号所获得信息

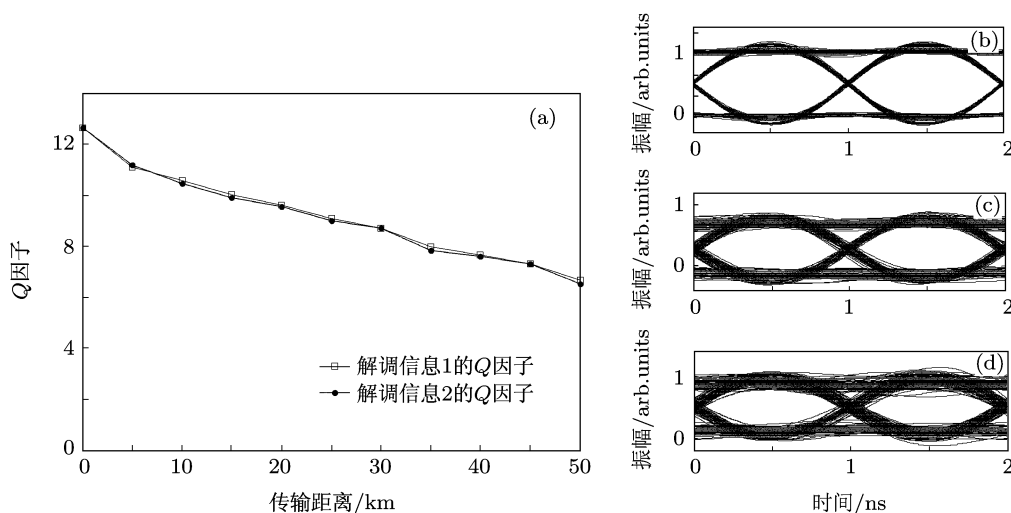


图 5 信息在普通单模光纤中的双向传输解调效果 (a) 为解调信息的 Q 因子随传输距离的变化曲线; (b—d) 分别对应 (a) 中信息传输 10 km, 30 km, 50 km 的眼图

4.2 光纤信道长度对通信性能的影响

首先讨论采用普通单模光纤作为传输信道时的情形. 当传输信道为普通的单模光纤时, 光纤的非线性效应和群速度色散会使信号在传输过程中发生变形, 从而影响信息的解调质量 [4,15].

图 5 给出了采用普通单模光纤经过不同传输距离后的信息解调效果, 其种光纤的参数设定为 $\gamma=1.5 \times 10^{-3} \text{ W}^{-1} \cdot \text{m}^{-1}$, $\beta_2=-20 \text{ ps}^2/\text{km}$. 从图 5(a) 可以看出, 随着传输距离的增加, 信息的解调质量呈下降趋势. 然而经过 50km 的传输, 两个相反方向解调信息的 Q 因子仍可保持在 6 以上 (对应误码

率估计低于 10^{-9}), 表明信息可得到很好的解调. 之所以能实现信息长距离的传输, 这主要得益于系统的良好对称性. 如图 1 所示, 由于两个响应激光器同时受到来自同一驱动混沌激光器、经过同样长度且性能参数一致的两根长距离光纤的传输后的混沌载波信号的注入, 因此两个响应激光器的混沌输出是等时同步的. 从 RL_1 端发射出的混沌载波信号与传输信息一起经 F_3 光纤链路传输到达 RL_2 前端, 与从 RL_2 输出的经光纤延迟线延迟后的混沌信号做“减”操作, 从而解调出传输信息. 因此, 在这个过程中, 传输信息没有注入到接收激光器中, 发射激光器与接收激光器的输出总保持很好的同步效果, 此时真正影响信息解调效果的是光纤色

散对传输信息的影响, 从而此时的混沌保密的通信距离可以提升到与一般光纤通信的通信距离相比拟的水平.

如果采用色散位移光纤作为传输信道, 系统的通信性能将得到进一步的提高. 对于色散位移光纤, 其参数为 $\gamma=1.5 \times 10^{-3} \text{W}^{-1} \cdot \text{m}^{-1}$, $\beta_2=-0.1 \text{ps}^2/\text{km}$. 图 6 给出了相应解调信息 Q 因子以及眼图随传输距离的变化关系. 可以看出, 信息 Q 因子随着传输距离的增加而逐渐下降. 但与普通光纤相比, Q 因子下降得明显更缓. 在传输距离 50 km 处, 两个方向的解调信息 Q 因子达到 11 左右. 而当传输距离达到 200 km 时, 解调信息的 Q 因子仍然大于 6, 表明了解调信息的高质量.

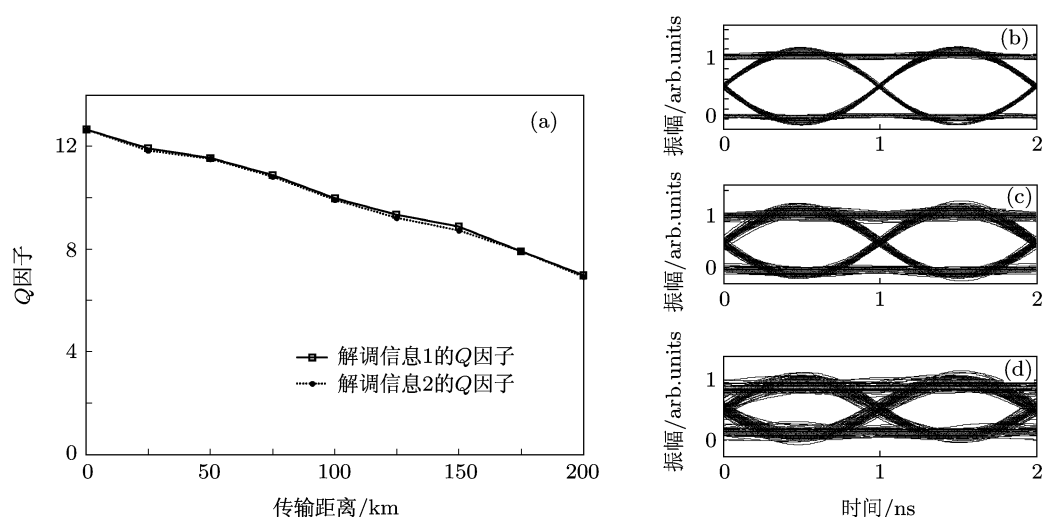


图 6 信息在色散位移光纤中的双向传输解调效果 (a) 为解调信息的 Q 因子随传输距离的变化曲线; (b—d) 分别对应 (a) 中信息传输 50 km, 100 km, 150 km 的眼图

5 结论

本文基于半导体激光器的混沌同步和光纤信道, 构建了一个可实现双向长距离保密通信的系统, 并对其双向通信方式、保密性能以及长距离光纤对通信性能的影响进行了分析. 结果表明: 系统可以实现两个被长距离光纤连接的半导体激光器之间的混沌同步, 且具有良好的延展性, 可适合于长距离通信. 信息可以在公共传输信道中实现双

向通信, 且具有很好抗窃密性能. 由于系统具有良好对称性, 采用普通单模光纤, 系统可以实现速率为 1Gbit/s 传输距离达 50km 的长距离双向通信. 而如果进一步采用色散位移光纤之后, 速率为 1Gbit/s 的信息的双向传输距离可达 200km 以上, 具有显著的长距离通信能力. 期望本文结果能为发展可实用的高速长距离双向保密通信技术提供有益的参考和借鉴.

- [1] Pecora L M, Carroll T L 1990 *Phys. Rev. Lett.* **64** 821
- [2] Argyris A, Syvridis D, Larger L, Annovazzi-Lodi V, Colet P, Fischer I, Garcia-Ojalvo J, Mirasso C R, Pesquera L, Shore K A 2005 *Nature* **438** 343
- [3] Lang R, Kobayashi K 1980 *IEEE J. Quantum Electron.* **QE-16** 347
- [4] Yan S L, Chi Z Y, Chen W J 2004 *Sci. Chin. E. Inf. Sci.* **34** 467 (in Chinese) [颜森林, 迟泽英, 陈文建 2004 中国科学 E 辑 信息科学 **34** 467]
- [5] Liu H J, Feng J C 2009 *Acta Phys. Sin.* **58** 1484 (in Chinese) [刘慧杰, 冯久超 2009 物理学报 **58** 1484]
- [6] Liu J, Wu Z M, Xia G Q 2009 *Opt. Express* **17** 12619
- [7] Klein E, Gross N, Kopelowitz E, Rosenbluh M, Khaykovich L, Kinzel W, Kanter I 2006 *Phys. Rev. E* **74** 046201
- [8] Vicente R, Mirasso C R 2007 *Opt. Lett.* **32** 403
- [9] Zhang W L, Pan W, Luo B, Zou X H, Wang M Y, Zhou Z 2008 *Opt. Lett.* **33** 237
- [10] Deng T, Xia G Q, Cao L P, Chen J G, Lin X D, Wu Z M 2009 *Opt. Commun.* **282** 2243
- [11] Cao L P, Xia G Q, Deng T, Lin X D, Wu Z M 2010 *Acta Phys. Sin.* **59** 5541 (in Chinese) [操良平, 夏光琼, 邓涛, 林晓东, 吴正茂 2010 物理学报 **59** 5541]
- [12] Uchida A, McAllister R, Roy R 2004 *Phys. Rev. Lett.* **93** 244102
- [13] Yamamoto T, Oowada I, Yip H, Uchida A, Yoshimori S, Yoshimura K, Muramatsu J, Goto S, Davis P 2007 *Opt. Express* **15** 3974
- [14] Agrawal G P 2001 *Nonlinear fiber optics* (3rd ed) (California: Academic Press) p49
- [15] Kanakidis D, Bogris A, Argyris A, Syvridis D 2004 *J. Lightwave Technol.* **22** 2256

A new type of bidirectional long distance optical fiber chaotic secure communication system*

Liu Yu-Ran Wu Zheng-Mao Wu Jia-Gui Li Ping Xia Guang-Qiong[†]

(School of Physical Science and Technology, Southwest University, Chongqing 400715, China)

(Received 17 May 2011; revised manuscript received 24 May 2011)

Abstract

Based on the chaotic synchronization of two response semiconductor lasers (RLs) under the injection from a common chaotic signal of a drive laser (DL), a new type of secure communication system, which allows bidirectional and long-distance information transmissions, is proposed. A corresponding theoretical model is established to study the bidirectional transmission performance, security performance and the system performance under different transmission distances. The results show that when two RLs receive chaotic light injected from a DL, the chaotic outputs of two RLs achieve a fairly good isochronal synchronization without any time delay, while there is a big difference between the signals of RLs and the signal of DL; the system owns high security level after having analyzed the various ways from which eavesdropper may obtain message; if the ordinary single mode optical fiber is used as a transmission channel, the Q factor of decoded message can reach more than 6 after a propagation over 50km; if the dispersion-shifted fiber is employed, the Q factor of decoded message can still reach more than 6 after a propagation over 200km.

Keywords: semiconductor laser, chaotic synchronization, bidirectional communication, optical fiber

PACS: 42.55.Px, 05.45.Vx

* Project supported by the National Natural Science Foundation of China (Grant Nos. 60978003, 61078003, 61178011 and 11004161), the Natural Science Foundation of Chongqing City, China (Grant No. 2010BB9125), and the Fundamental Research Funds for the Central Universities (Grant Nos. XDJK2009B010 and XDJK2010C021).

[†] E-mail: gqxia@swu.edu.cn