

混沌保密光通信研究进展

义理林, 柯俊翔

(上海交通大学区域光纤通信网与新型光通信系统国家重点实验室, 上海 200240)

摘要: 针对混沌保密光通信的关键技术和最新的研究进展, 首先介绍了基于不同非线性器件的混沌生成方法; 然后重点研究了混沌光通信的研究前沿, 包括如何提高安全性、如何提升混沌保密光通信的传输容量和距离; 最后讨论了混沌保密光通信的局限性和潜力, 并对混沌保密光通信的关键技术和研究进展进行了总结。

关键词: 混沌; 安全; 光通信; 时延消除

中图分类号: TP913.7

文献标识码: A

doi: 10.11959/j.issn.1000-436x.2020008

Research progress of chaotic secure optical communication

YI Lilin, KE Junxiang

State Key Lab of Advanced Optical Communication Systems and Networks, Shanghai Jiaotong University, Shanghai 200240, China

Abstract: For the key technologies and latest research progress on chaotic secure optical communication, chaos generation methods based on different nonlinear components were introduced firstly. Then the research progress of chaotic optical communication was discussed, including how to improve the security level, and how to increase the transmission capacity and distance of chaotic optical communication. At last, the limitations and potentials of chaotic optical communication were discussed, the key technologies and research progress of chaotic secure optical communication were summarized.

Key words: chaos, security, optical communication, time delay concealment

1 引言

光纤通信已经成为网络信息的重要物理载体和骨干基础设施, 超过 90% 的网络流量都是通过光纤传输和传送的。然而在海底和陆地光缆以及用户接入光纤等场景中, 网络信息都存在被窃听的风险。因此非常有必要对光纤中的高速光信号进行加密传输。

混沌保密通信是一种基于物理层的硬件加密。它主要基于混沌信号所具有的遍历性、非周期、连续宽带频谱、类噪声等特性, 将传输信号隐藏在混沌信号中, 或者通过符号动力学分析赋予不同的信息序列以不同的混沌波形, 在接收端利用混沌同步特性或者混沌波形的特征解调出所传输的信息。激光混沌系统具有高带宽和低衰减, 且动力学系统比

较复杂, 系统对参数具有极高的敏感性, 具有更高的保密性能, 非常适合高速远程保密通信。不同于混沌保密通信, 量子保密通信是一种密钥分发的技术, 其通过分发的密钥实现保密通信^[1]。混沌光通信作为一种物理安全技术, 有可能成为光纤网络的物理层安全屏障。

激光器由 Maiman^[2]于 1960 年发明, 混沌的概念由 Lorenz^[3]于 1963 年提出。然而, 混沌和激光长期独立发展。直到 1975 年, Haken^[4]首先建立了混沌与激光之间的联系。之后, 研究者们相继开展了许多关于混沌激光动力学特性观测的实验, 并且提出了许多激光器模型, 用来解释相应的实验结果。1990 年, Pecora 等^[5]首次提出了混沌控制和混沌同步, 这大大拓宽了混沌的应用, 例如混沌光通信、

收稿日期: 2019-08-28; 修回日期: 2019-11-22

基金项目: 国家自然科学基金资助项目 (No.61575122)

Foundation Item: The National Natural Science Foundation of China (No.61575122)

随机数产生和安全密钥分配等。混沌系统对初始条件非常敏感，使它们难以预测，具有在数据传输中提供高级别隐私的潜力。因此，混沌光通信在实现物理层信息安全方面引起了很多关注，并且已经通过许多混沌光通信实验得到证明。混沌的产生技术可以基于不同光学元器件的非线性进行分类，包括基于半导体激光器非线性的全光反馈和光电反馈、基于马赫-曾德尔调制器非线性的电光反馈。其中，由于光电元器件的高带宽，电光反馈更可能用于高速混沌光通信系统。

2005年，研究人员在希腊城域网的商业光网络上首次进行了混沌保密光通信的现场实验，其中解密后的传输速率达到千兆比特每秒，并且相应的误码率低于 10^{-7} ，光纤传输的距离超过120 km，说明了混沌保密光通信系统在长距离、高速安全光通信系统中的可行性^[6]。自此，研究人员一直致力于提高混沌保密光通信的传输速率、同步质量和安全性能。2010年，研究人员实现了10 Gbit/s的正交相移键控(QPSK, quadrature phase-shift keying)信号的传输，传输距离超过100 km^[7]，并且使用相位调制器产生的相位混沌来增强其安全性。然而，他们发现大多数混沌光通信方案并不像预期的那样安全^[8-10]。许多统计学方法如自相关函数、互信息和极值统计可用于获得反馈时延特征，这是混沌系统中的关键安全密钥^[8-10]。一旦窃听器获得时延特征，就可以估计出其他所有硬件参数。因此，完全隐藏时延特征对于增强混沌保密光通信的安全性是至关重要的。目前，人们已经提出许多方法来隐藏时延特征。例如，选择激光弛豫频率附近的反馈时延可用于隐藏时延^[11]，但代价是降低了混沌复杂度。因此，需要研究有效的时延隐藏方法。另一方面，增加混沌系统的复杂性是提高安全性的另一种方法。在解决安全问题之后，提升混沌光通信的传输容量和距离对于实际应用变得更加重要。

2 混沌的产生

混沌的产生可以根据源自不同器件的非线性动力学特性来进行分类，包括半导体激光器、马赫-曾德尔调制器、马赫-曾德尔干涉仪和可调色散补偿器。

2.1 半导体激光器

图1显示了从半导体激光器的非线性动力学中产生混沌的3种方法，包括全光反馈、光注入和光电反馈^[12]。全光反馈是产生混沌的最基本配置，如

图1(a)所示，来自激光器的光被外部镜子反射回激光腔，这扰乱了载体和光子之间的相互作用并在半导体激光器中引起混沌。图1(b)显示了通过光注入产生混沌，其中来自一个激光器的光被注入其他激光器中，光学隔离器用于单向注入。当2个激光器的频率失谐并且注入强度很小时，可以观察到混沌。图1(c)显示了通过光电反馈产生混沌，其中光电探测器检测从激光器发出的光，由放大器放大的光电流被反馈到注入电流，扰乱了载流子密度并产生混沌。

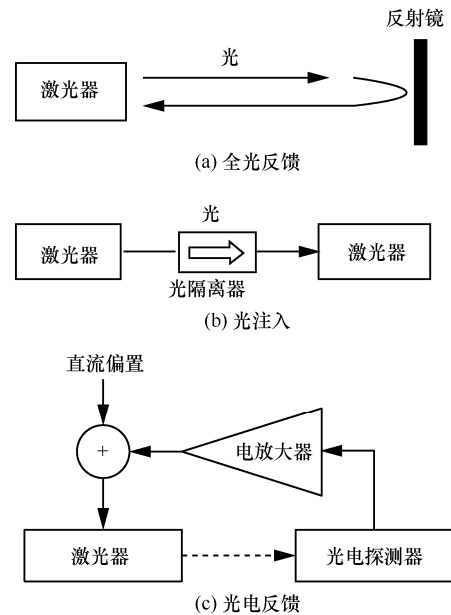


图1 基于半导体激光器非线性的混沌产生方案

2.2 马赫-曾德尔调制器

2002年，Goedgebauer等^[13]提出了一种新的混沌系统，该混沌系统基于马赫-曾德尔(MZM, Mach-Zehnder modulator)调制器的非线性。如图2所示，混沌发射器由2个激光器组成，其中一个激光器的输出由闭合的电光反馈时延环调制，其非线性元件是高速马赫-曾德尔铌酸锂调制器，该调制器具有低的半波电压。光电探测器用于将光信号转换成电信号，电信号被放大后再反馈给调制器。只要转换的电信号幅度大于半波电压的两倍或三倍，就可以获得足够的非线性，进而产生混沌。另一个激光器的输出用来调制被加密的信号，并且它的输出通过光耦合器与混沌信号混合，从而实现对信号的掩盖。另外，被加密的信号参与混沌生成过程，扰乱了混沌动力学特性，从而进一步增加了混沌的复杂性。该方法能够支持10 Gbit/s的混沌光通信，主要受益于商用马赫-曾德尔调制器的高带宽^[14]。

3.1 混沌光通信安全性增强

3.1.1 隐藏时延特征

研究人员发现，许多方法如自相关函数、互信息和极值统计可用于获得时延特征^[10]，此外，功率谱分析方法也可用于获取时延特征^[9]。时延特征是一个关键参数，根据时延可以很容易地估计其他硬件参数。因此，时延特征泄露的可能性成为混沌光通信中的严重问题。为了提高混沌光通信的安全性，隐藏时延特征是必不可少的。由于全光和电光反馈混沌系统中的时延特征隐藏方法不同，因此本文分别介绍基于2种不同装置的时延隐藏方法。

1) 全光反馈混沌系统中的时延特征消除

对于全光反馈的混沌系统，人们已经提出了各种方法来隐藏时延特征。例如，如果人们选择接近于激光器的弛豫振荡周期的时延，并且让激光器处于中等反馈，则可以隐藏时延特征^[11]。图6表示不同反馈强度的自相关函数和互信息，垂直虚线表示时延特征。结果表明，当反馈强度较低，并且反馈

时延和弛豫振荡时间接近时，可以隐藏时延特征。但是，相关研究表明，通过检测光学相位的自相关特性也可用于获得时延特征^[19]。

为了能够在相位上隐藏时延特征，研究人员提出了一种新的方案，如图7所示，在该方案中，由于双向半导体环形激光器中反向传播模式之间的交叉反馈，强度和相位上的时延特征可以消除^[20]。

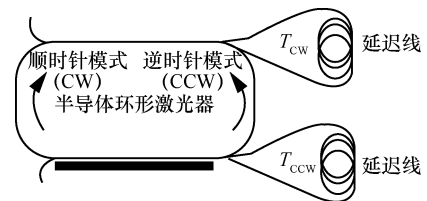


图7 交叉反馈的半导体环形激光器方案

双外腔反馈也是一种削弱时延标签的结构，其结构如图8所示，2个反射镜形成双外腔反馈，通过调节2个腔反馈强度和腔长，最终可有效削弱时延标签^[21]，并且该结构相对简单。

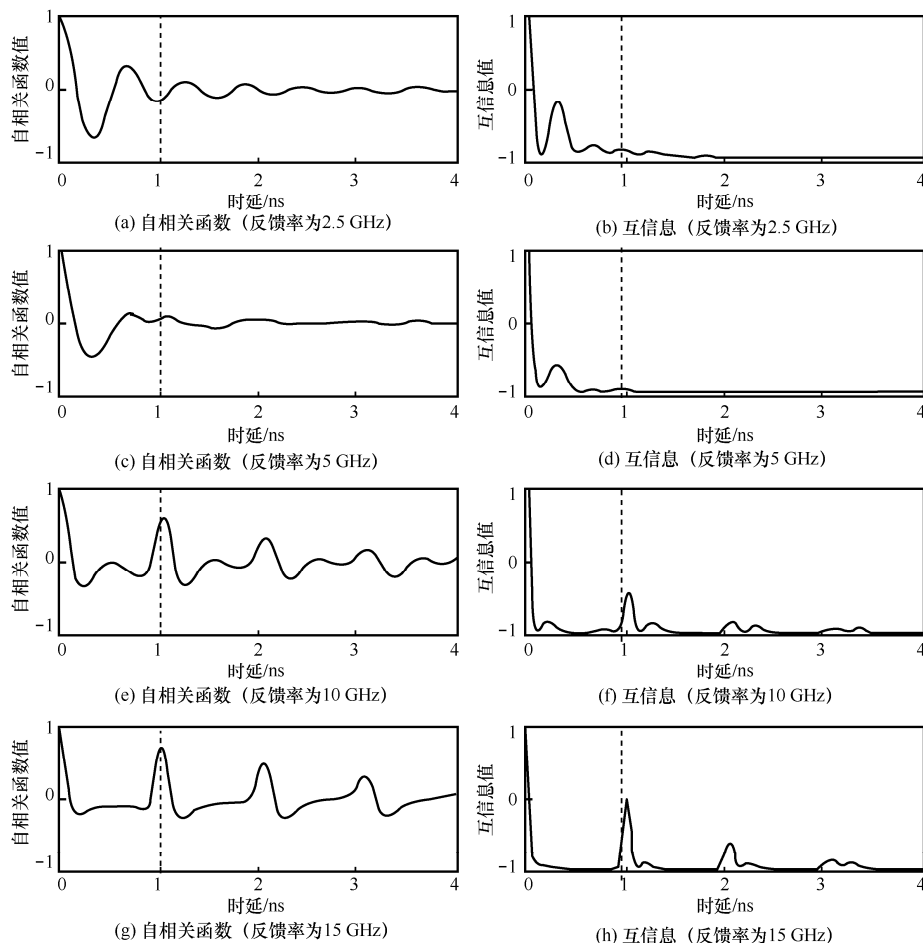


图6 不同反馈强度的自相关函数和互信息

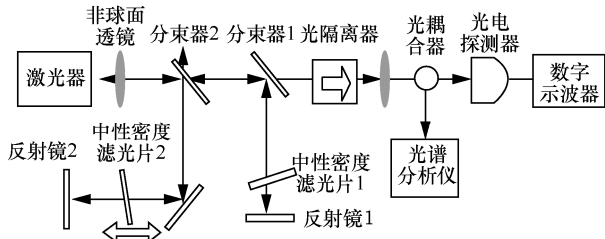


图 8 基于双外腔反馈的时延隐藏方案

非相干反馈也可以实现削弱时延特征的作用，其结构如图 9 所示，通过法拉第旋转器，实现非相干的光反馈，最终实现时延特征削弱^[22]。

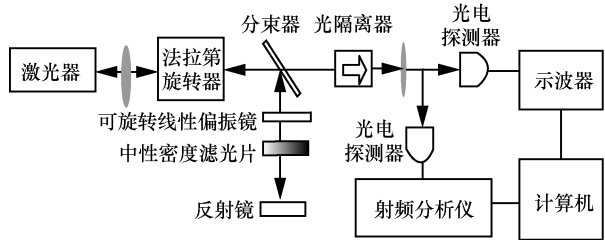


图 9 基于非相干反馈的时延隐藏方案

分布式反馈也能够实现时延特征的削弱。在传统基于激光器光反馈产生混沌的基础上，将腔内的反射镜改成光纤布拉格光栅，可以实现时延特征的削弱。由于光纤布拉格光栅对不同光频率成分具有不同的群时延，使时间周期被破坏，导致时延特征消失。光纤布拉格光栅的结构如图 10 所示，但是该方案对混沌同步要求较高，需要参数一致的光纤布拉格光栅^[23]。此外，啁啾的光纤布拉格光栅也可以用于时延隐藏^[24]，同时该方案还可以增加密钥空间^[25]。

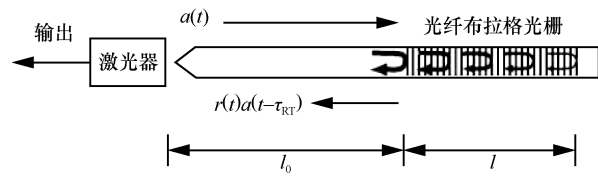


图 10 基于分布式反馈的时延隐藏方案

图 11 给出了一种新的隐藏时延特征的方案，其中在全光反馈环路中引入了商用可调色散补偿器^[26]。由于色散补偿器的存在，混沌载波的不同频率分量经历不同的时延，因此时间周期被破坏并且时延特征消失。结果表明，当色散值足够大时，对于时间序列和功率谱分析方法，时延特征可以被完全隐藏，如图 12 所示。这种方法在电光反馈混沌系统中也是可行的。

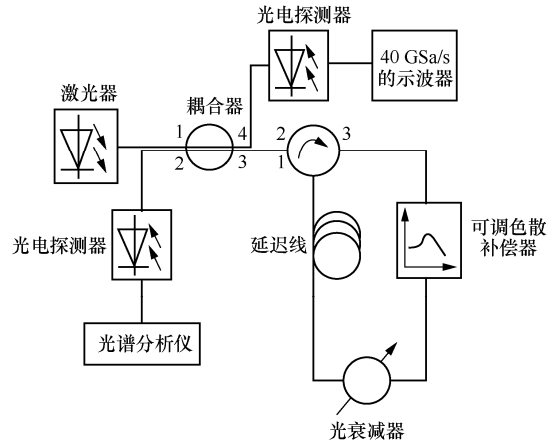
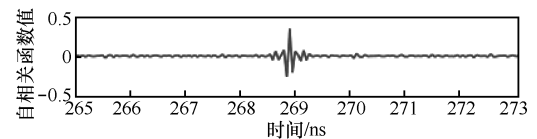
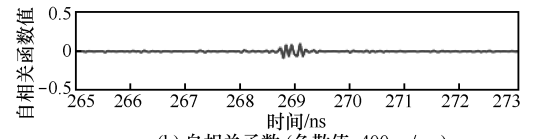


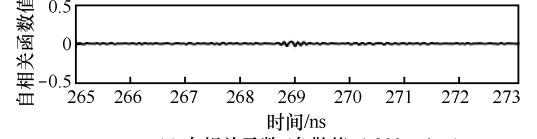
图 11 基于可调色散补偿模块的时延隐藏方案



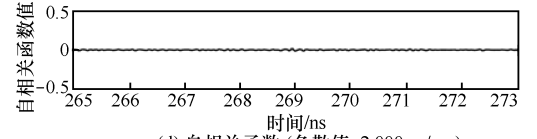
(a) 自相关函数 (色散值=0 ps/nm)



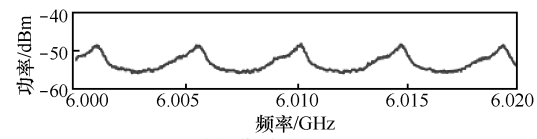
(b) 自相关函数 (色散值=400 ps/nm)



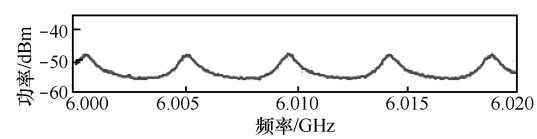
(c) 自相关函数 (色散值=1 200 ps/nm)



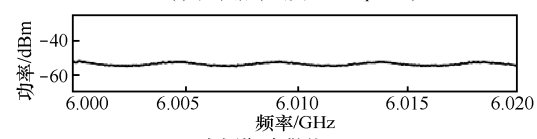
(d) 自相关函数 (色散值=2 000 ps/nm)



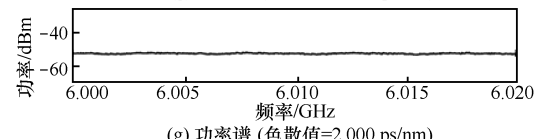
(e) 功率谱 (色散值=0 ps/nm)



(f) 功率谱 (色散值=400 ps/nm)



(g) 功率谱 (色散值=1 200 ps/nm)



(h) 功率谱 (色散值=2 000 ps/nm)

图 12 不同色散值下自相关函数和功率谱

2) 电光反馈混沌系统中的时延特征消除

对于电光反馈系统，为了隐藏电光反馈混沌系统的时延特征，研究人员通过组合全光反馈和电光反馈方案提出了一种新的方案，如图 13 所示，其中全光的强度混沌和电光的相位系统是级联的^[27]。然而，由于整个传输过程的相位是全光和电光系统的线性叠加，依然可以使用相位的自相关特性来获得其时延特征^[19]。

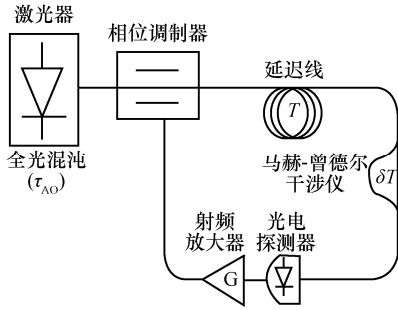


图 13 基于级联全光混沌系统和电光相位混沌系统的时延消除方案

另外，研究人员提出一种方案来彻底隐藏电光混沌系统中的时延特征，如图 14 所示^[28]。在该方案中，数字密钥被引入相位混沌电光时延系统，其包含 2 个时延链路，并且每个链路具有 2 个电光相位调制器（PM, phase modulator）。在每个链路中，第一相位调制器由外部信号驱动，该外部信号分别是信息和数字密钥；第二个相位调制器由另一链路的输出驱动。在该方案中，马赫-曾德尔干涉仪以非线性方式将相位变化转换为强度变化，光电探测器用于检测强度变化，然后将

信号放大后通过驱动相位调制器以产生相位混沌。当数字密钥的比特率高于引入密钥的链路的差分时延阈值时，可以发生时延隐藏^[28]。

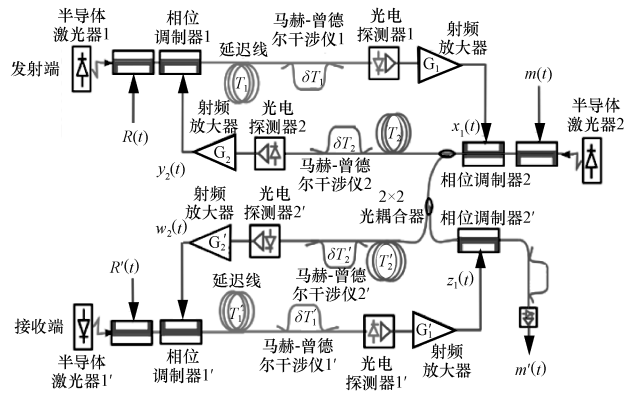


图 14 带有数字密钥的相位混沌串行发生装置的时延消除方案

基于图 15 的装置，研究人员进一步提出了具有 2 个并行时延回路的优化系统^[29]。在发射端和接收端中并联有 2 个非线性时延差分处理环路。只有一个回路的输出传输到接收端，而另一个回路保持在反馈环的内部。该装置可以在没有外部数字密钥的情况下隐藏内部时延，这与参考文献^[28]中的装置不同。实际上，当环路并联耦合并且每个环路具有不同的差分时延时，内部环路的动力学特性与发送信号不相关，因此该系统本质上隐藏了内部时延^[26]。

图 16 给出了利用可调色散补偿模块来实现时延隐藏^[30]，在发射端和接收端的环内都加入可调色散补偿模块，也称为频率相关群时延模块，通过对

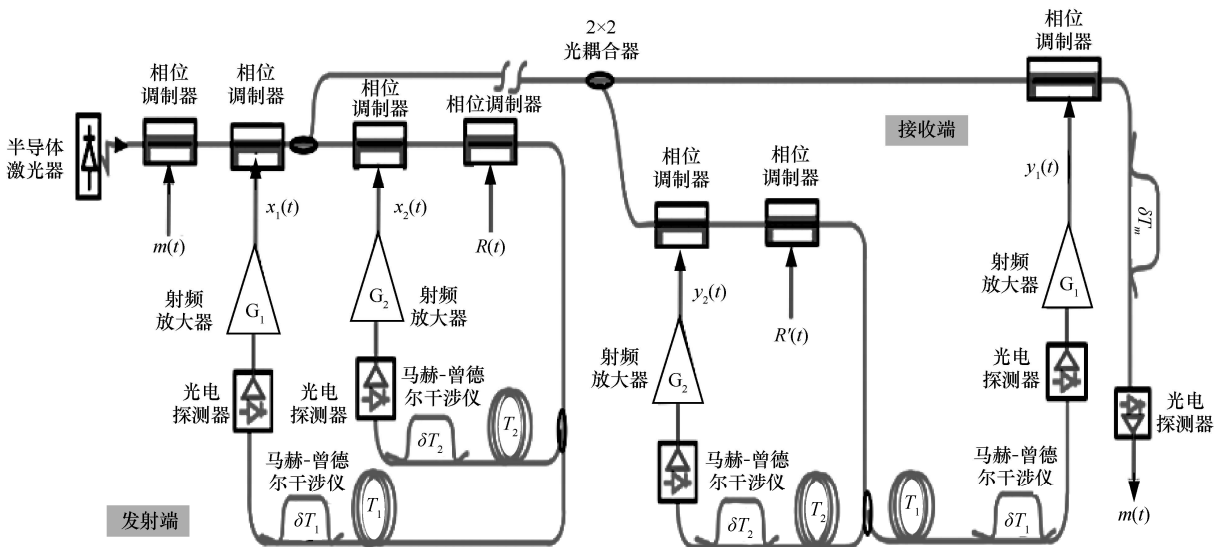


图 15 带有数字密钥的相位混沌并行发生装置的时延消除方案

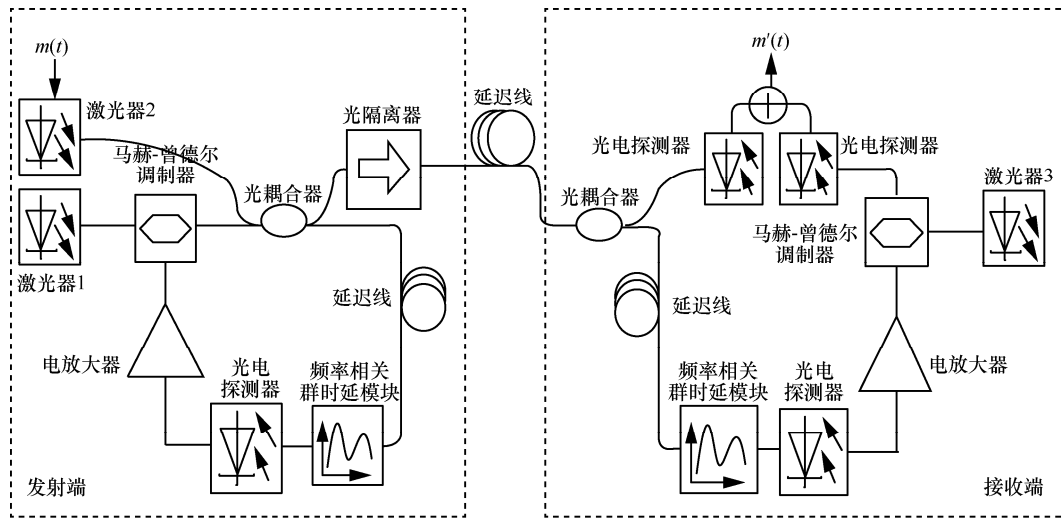


图 16 基于可调色散补偿模块的时延消除方案

混沌载波的不同频率分量产生不同的时延，使时间周期被破坏并且时延特征消失。图 17 展示了时延消除结果。从图 17 可以看出，对于不同的色散曲线，混沌的时延特征在时域的自相关函数和频谱分析上都可以消除。

电光反馈混沌系统中的大多数时延特征的隐藏方法采用了组合混沌装置，并且通过时域处理实现了时延特征的隐藏。只有图 16 给出的可调色散补偿模块方案，其时延特征隐藏是通过频域处理实

现的。该方法的主要优点在于不增加系统复杂度，只要在原有光电反馈混沌收发结构中引入可调色散补偿模块即可，易于实验实现。

3.1.2 增加混沌复杂度

为了进一步增强混沌保密光通信的安全性，除时延隐藏外，增加混沌复杂度是另一种行之有效的方法。通过使用双重掩盖^[31]、曼彻斯特编码^[32]、变化的增益^[33]，结合全光反馈和电光反馈这 2 种方案^[27]，可以在一定程度上增加混沌负责度并提高安全性。

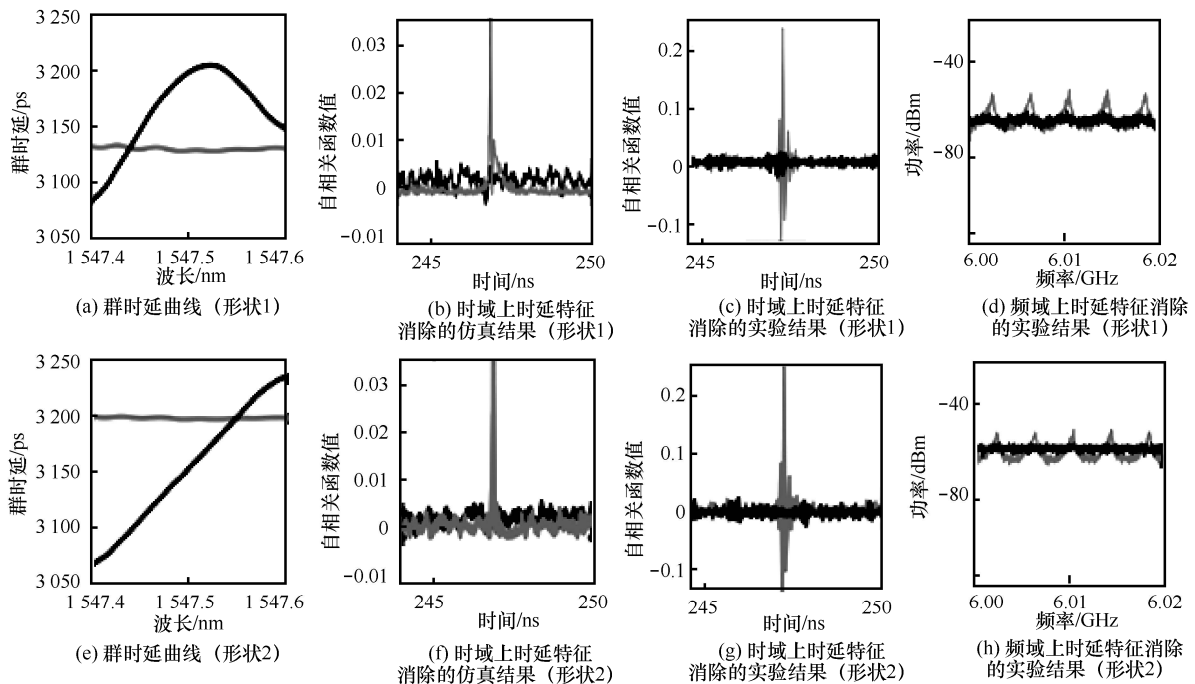


图 17 不同色散曲线下时延消除的结果

例如,在图14和图15的配置中,数字密钥是增加复杂性的一种方式,因此时延特征的隐藏和数字密钥选择性的组合在混沌光通信中提供了较大的安全性增强^[28-29]。另外,图15的配置中的内部时延也会增加混沌复杂^[29]。此外,图3装置中的正交相移键控电光调制器也是一种增加混沌复杂度的方法,因为非线性源于集成的四波光学干涉仪,涉及2个独立的电光调制器的输入^[15]。总之,混沌复杂度的提高伴随着混沌生成装置复杂性的提高,同时也增加了混沌同步的难度。因此,寻找增加混沌复杂度而不使混沌系统装置复杂化从而导致混沌同步难度增加的方法是非常重要的。

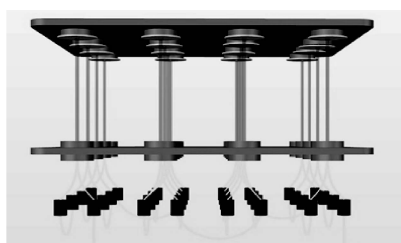
图16所示的方案可以大大增加混沌的复杂度,并且不使混沌系统装置复杂化。在实验中,本文将具有精确温度控制系统的多个G-T腔级联,设计了一个频率相关群时延光模块。每个G-T腔的硬件参数都尽可能相同,并可通过工艺控制确保参数相同,腔长可通过温度独立控制。G-T腔数越多,可组合产生的时频曲线越复杂,状态数越多,能提供的密钥空间数越大,同时匹配难度也越大。综合考虑密钥空间与复杂度,本文采用16个G-T腔组成频率相关群时延模块光模块,其中每个G-T腔的温度控制系统精度达到了 0.001°C 。图18(a)是16腔频率相关群时延模块的3D结构,理论上激光在腔内无损传输,每个G-T腔的群时延曲线存在周期性尖峰,代表着在这些频率处光波干涉相长,相邻峰值位置之间的频率间隔被称为自由谱范围。自由频谱范围由腔长决定,本文使用的G-T腔自由频谱范围为100 GHz,半波带宽约1 GHz。单个G-T腔的群时延曲线如图18(b)所示。通过控制腔温度,腔长会根据所用半导体的热延展性变化,从而改变群时延曲线的自由频谱范围,导致群时延曲线峰值位置的中心频率偏移。频率相关群时延模块的群时延曲线

是所有G-T腔群时延的线性叠加,如图18(c)所示,不同颜色的线条表示不同的温度设置。通过高精度调节每个G-T腔的温度可改变频率相关群时延模块曲线的形状,分析每个G-T腔温度改变带来的同步系数劣化,可量化评估频率相关群时延模块引入的数字密钥。

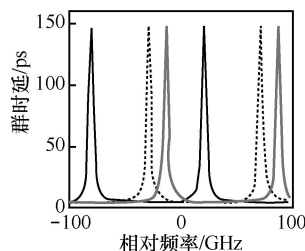
为了更直观地表示同步误差对信号性能的影响,本文采用误码率的劣化来表示混沌同步性能的劣化。由于除G-T腔外的所有其他参数均保持匹配,因此误码率的劣化仅来自混沌同步性能的劣化。图19(a)展示了单个G-T腔中心频率偏移对于解密后信号误码率的影响。从图19(a)可以看出,当单个G-T腔中心频率偏移200 MHz时,解密信号误码率(BER, bit error rate)劣化为 1×10^{-2} ,可认为无法正确解密,对应于图中的同步误差劣化0.2。此外还可得出G-T腔时延峰值频率对应混沌频谱中心位置时,对频率失配更敏感。

图19(b)展示了16个G-T腔级联组成的群时延模块中每个腔中心频率偏移对于解密后信号误码率的影响。当多个腔级联时,时频曲线变得非常复杂,因此解密信号性能对频率失配的敏感度要远高于单个G-T腔情况。即使对于时延峰值对准混沌频谱边缘的G-T腔,频率失配10 MHz也会导致解密信号误码率劣化到 1×10^{-2} ,无法正常解密。而对应时延峰值对准混沌频谱中心的G-T腔而言,频率失配容忍度仅为4 MHz。

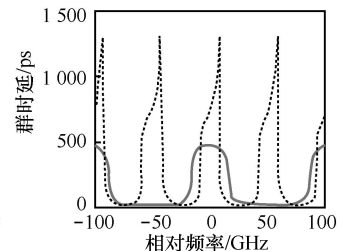
实际使用中需要综合考虑合法用户的解密难度和对安全性的要求等级,设计具有所需温度特性的G-T腔,现有的热敏电阻可探测 0.001°C 的温度变化,从而实现调谐精度为 0.001°C 的精确温度控制。若使用石英作为G-T腔体材料,其温度系数为 $670 \text{ MHz}/^{\circ}\text{C}$,对应0.67 MHz的频率调谐精度。以10 MHz为刻度进行调谐,对应温度调谐刻度为



(a) 16个级联的温控G-T腔构成的频率相关群时延模块



(b) 单个G-T腔的群时延曲线



(c) 16个G-T腔叠加而成的整个FDGD的群时延曲线

图18 群时延模块和群时延曲线

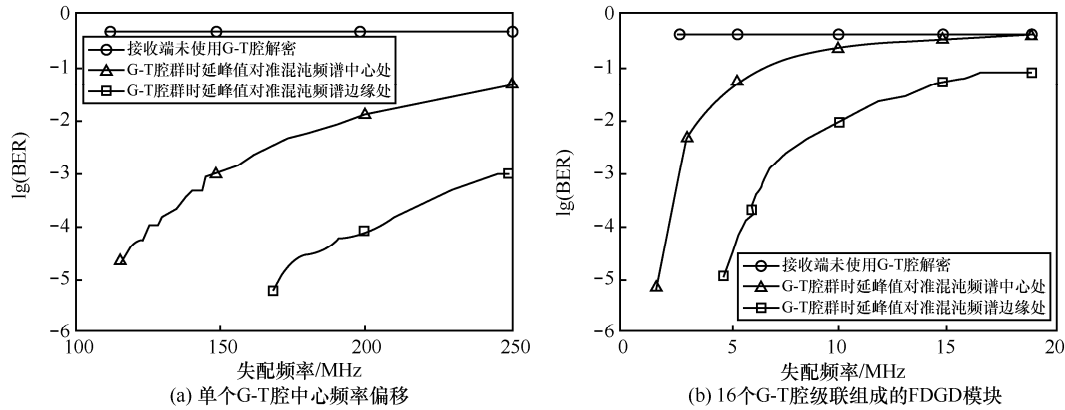


图 19 频率偏移对于解密信号性能的影响

0.015°C, 在温度调谐精度范围之内。例如混沌载波频谱宽度为 10 GHz, 每个 G-T 腔提供的密钥空间为 $10^3 \left(\frac{10 \text{ GHz}}{10 \text{ MHz}} \right)$, 对应的温度调谐范围为 15°C。由于每个 G-T 腔的温度均独立控制, 16 个 G-T 即可将系统的密钥空间增加至 10^{48} 。该方案可以有效提升混沌密钥空间, 大大增强混沌光通信系统的安全性。同时由于设计的群时延模块具有批量可生产性和重复性, 因此是现实混沌光通信系统中增强系统安全性方案中较理想的选择。

3.2 混沌光通信系统演示

自 20 世纪 90 年代早期实现了混沌同步^[5], 混沌光通信已经成为在物理层提供信息安全的热门方向^[6-7,33-55]。大多数方案都是基于半导体激光器的非线性动力学特性, 然而这种方法的传输速率被半导体激光器的弛豫振荡频率限制在 2.5 Gbit/s^[7,42]。相比之下, 基于电光反馈的混沌光通信系统可以支持高比特率, 这主要受益于调制器的大带宽。目前, 基于电光相位混沌系统已经实现了 10 Gbit/s 的数据传输^[16]。除传输速度外, 传输距离也是评估混沌光通信系统性能的关键参数。混沌信号对色散非常敏感, 因此在大多数实验演示中传输距离限制在 100 km 左右。接下来, 本文将介绍混沌光通信的系统研究进展。

1998 年, Vanwiggeren 等^[33]演示了使用基于掺铱光纤环形激光器的混沌系统进行 10 MHz 信息传输。2001 年, Tang 等^[35]通过混沌脉冲半导体激光器的同步实现了 2.5 Gbit/s 信息的加密和解密。2002 年, Kusumoto 等^[36]在基于具有光学反馈的半导体激光器的非线性系统中的混沌同步实现了 1.5 GHz 正弦波信号的传输。2004 年, Gastaud 等^[37]在基

于调制器的混沌光通信系统中, 将比特率提高到 3 Gbit/s, 并且在混沌同步之后实现了 7×10^{-9} 的误码率。由于该方案的混沌光学载波带宽能够超过 20 GHz, 因此预计能够支持几十 Gbit/s 的信号加密。2005 年, Annovazzi-Lodi 等^[38]通过光纤链路实现了 2.4 GHz 标准电视信号加密传输, 这是混沌保密光通信在真实场景下的首次演示。2010 年, Argyris 等^[39]使用单片光子集成电路作为混沌发生器实现 2.5 Gbit/s 的数据传输。在这个方案中, 只有授权的对应设备能够同步和再现相同的混沌载波, 速率可以达到 2.5 Gbit/s, 误码率低于 10×10^{-12} 。根据 2009 年提出的电光相位混沌的方案^[16], 2010 年在法国贝桑松市部署的超过 20 km 的全光纤环网上进行 10 Gbit/s 信号加密传输的现场演示^[7], 这是混沌保密光通信现场演示的速率记录。

以往的混沌光通信系统研究中, 加载的信号均采用二进制强度调制或相位调制, 如 NRZ-OOK (non-return-to-zero on-off-keying) 或 DPSK (differential phase shift keying) 信号, 频谱效率非常低。图 20 通过双二进制调制码型压缩信号的带宽, 来提升混沌保密通信的速率^[54]。该装置是基于传统的电光反馈混沌装置, 由于发射端的系统带宽约为 10 GHz, 而加入的信号为 30 Gbit/s 的非归零信号, 系统的滤波作用使信号变成了带宽为 10 GHz, 速率为 30 Gbit/s 的双二进制信号, 因此, 被加密的信号能够被 10 GHz 带宽的混沌信号完全掩盖, 最终实现对 30 Gbit/s 的双二进制信号加密传输, 并通过色散补偿技术对光纤传输过程中的色散进行补偿。传输过程采用了色散补偿光纤和可调色散补偿器做色散补偿, 图 21(a)~图 21(d)分别为原始电信号的眼图、经电光调制器调制解调后的眼图、加密后的眼图

和解密后的眼图。图 21(e)~图 21(g)分别是图 21(a)~图 21(c)对应的频谱图。从频谱图可以看出,原本带宽为 30 GHz 的非归零信号,经调制解调后,由于系统的滤波效应,变成带宽为 10 GHz 的双二进制信号。该实验演示了 30 Gbit/s 信号 100 km 混沌保密光传输,是截至目前混沌光通信系统的最高速率纪录。

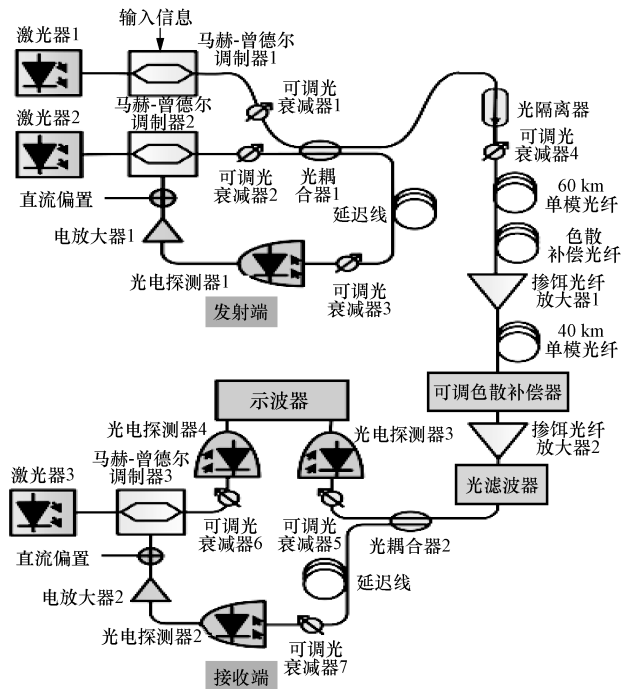


图 20 30 Gbit/s 双二进制信号的混沌加密传输

近年来,随着数字信号处理技术的快速发展,为了能够提升混沌同步的相似度,降低混沌同步难度,本文提出了利用数字信号处理技术来提升混沌的相似度。众所周知,混沌保密光通信中最关键的技术是混沌同步技术,混沌同步的相似度低,意味着接收端无法完全消除发射端加入的混沌掩盖信号,这部分无法被完全消除的混沌信号将作为噪声加入被加密的信号中,使发射端的信噪比严重下降,无法实现解密。然而,实际情况中,由于发射端和接收端的物理器件难以做到精确匹配,本文提出了通过前向均衡器、volterra 滤波器和神经网络对由于物理器件参数失配导致的不同步的混沌信号进行补偿^[55],装置如图 22 所示。在训练阶段,需要通过光电探测器 5 探测未与被加密信号混合的混沌信号,并将该混沌信号作为目标值,对接收端的滤波器参数进行训练,从而提升发射端和接收端混沌同步的同步系数。同步系数的仿真和实验结果

如图 23 所示。从图 23 可以看出,在经过数字信号处理后,同步系数获得了很大的提升。

从研究进展来看,随着激光器、调制器、光电探测器和电子放大器等电光元件的带宽增加,以及先进的光信号处理和数字信号处理技术的发展,有可能实现具有更高速率和更长传输距离的混沌光通信系统。

4 讨论

混沌保密光通信从提出至今已经 20 多年,技术进步飞速,也曾在希腊和法国的商用光纤网进行过现网测试,但始终无法进行规模化应用,其根本原因在于高安全性和实现难度是一对根本矛盾。例如基于激光器全光反馈的结构具有较高的安全性,但要实现多对节点的匹配非常困难,需要从多个激光芯片去寻找配对,成本过高。基于外调制器的光电光反馈匹配相对容易,但由于匹配参数较少,导致容易被破解,安全性不高。如何破解这对矛盾,实现高安全性、低复杂度,从而可规模化应用的混沌光通信系统,是混沌光通信需要解决的根本问题。

截至目前,混沌光通信系统的最高实现记录是速率 30 Gbit/s,传输距离不超过 100 km,与现有光通信系统的速率和传输距离水平有较大的差距。混沌光通信系统速率不高主要受限于宽带混沌信号难以产生,高阶调制信号抗噪声能力差等因素。传输距离不长主要受限于混沌信号对非线性性和色散非常敏感,长距离光纤传输难以同步等因素。现有的混沌传输技术还处于低速二进制直接检测的阶段,对高速多进制信号调制、相干检测、数字信号处理等技术还未有研究。基于这些技术是否可以提高传输速率和距离,同时系统在相干检测窃听下安全性是否会减弱等问题都需要深入研究。

混沌通信基于收发节点参数进行高度匹配,由于匹配难度很高,很难实现大于 2 个节点的完全匹配,因此现有的混沌光通信系统主要应用于点到点通信系统。而系统要形成网络,必须实现多节点互通。要解决此问题,必须实现多节点参数完全匹配。与此相矛盾的是,多节点参数匹配将导致窃听者容易复制硬件设备从而减低破解难度。因此未来需要破解多节点同步和安全性降低这对矛盾,才能实现混沌系统多节点组网。

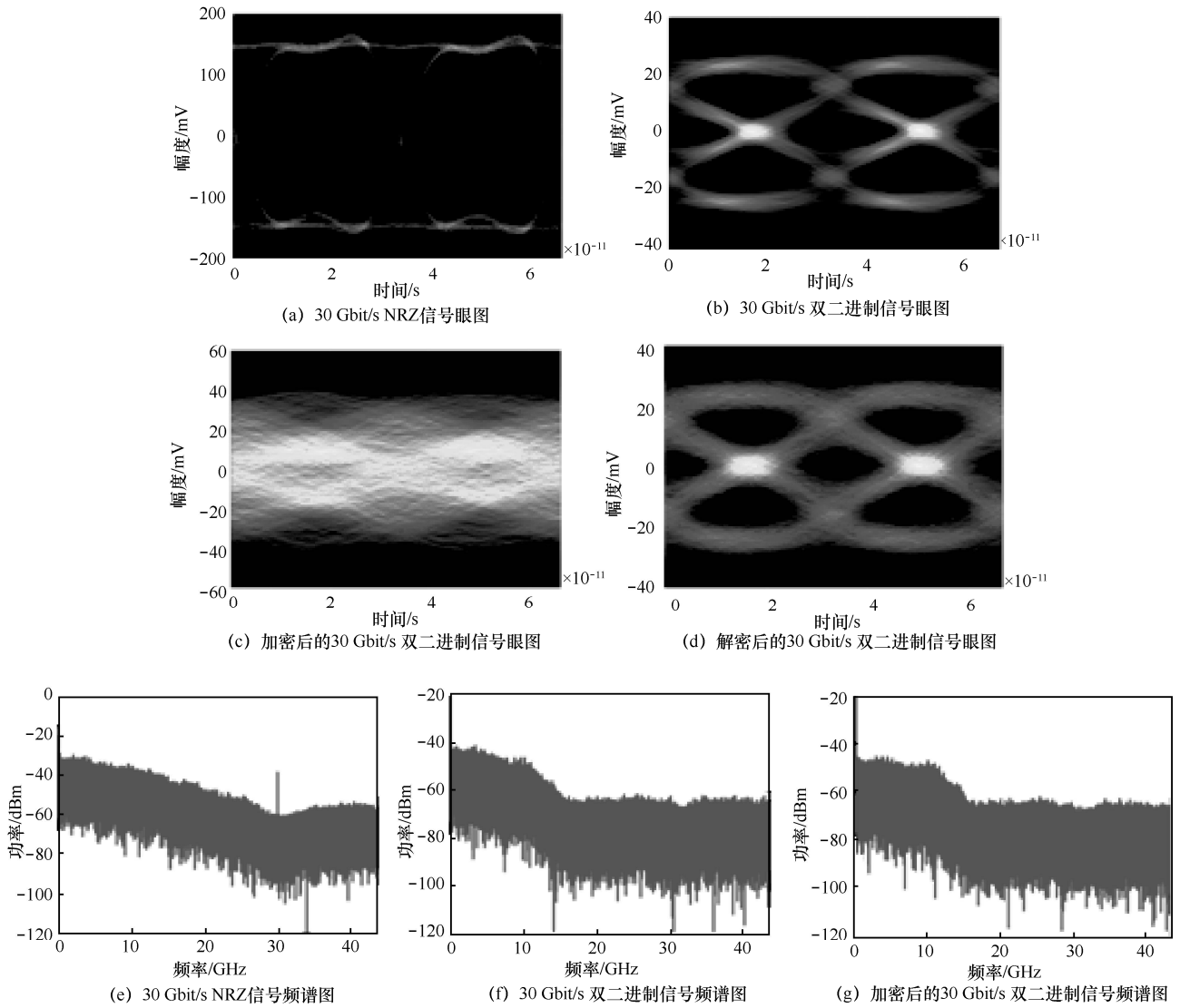


图 21 30 Gbit/s 信号加密解密实验结果

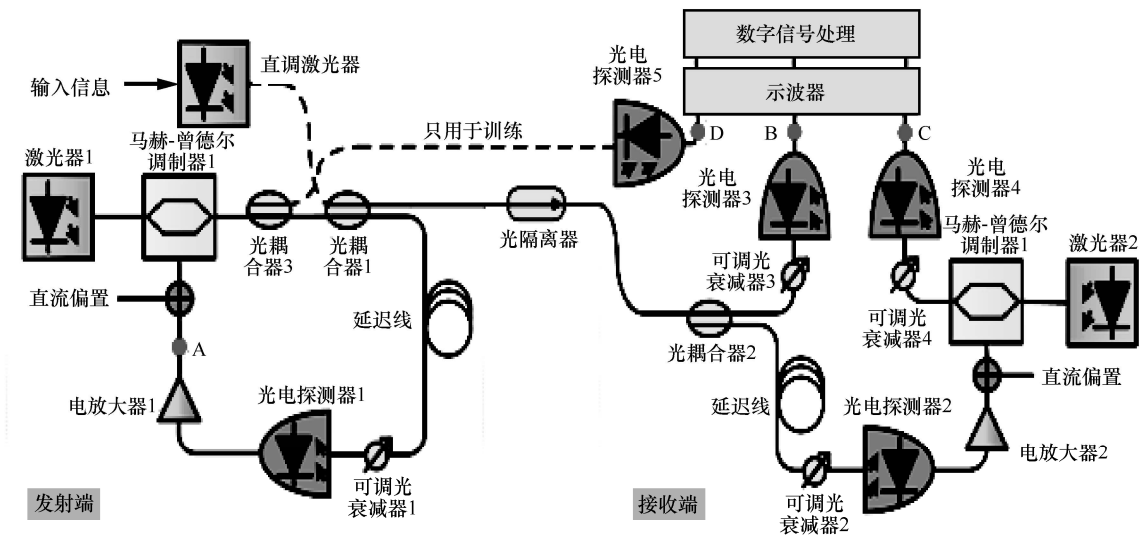


图 22 基于神经网络的混沌同步误差补偿装置

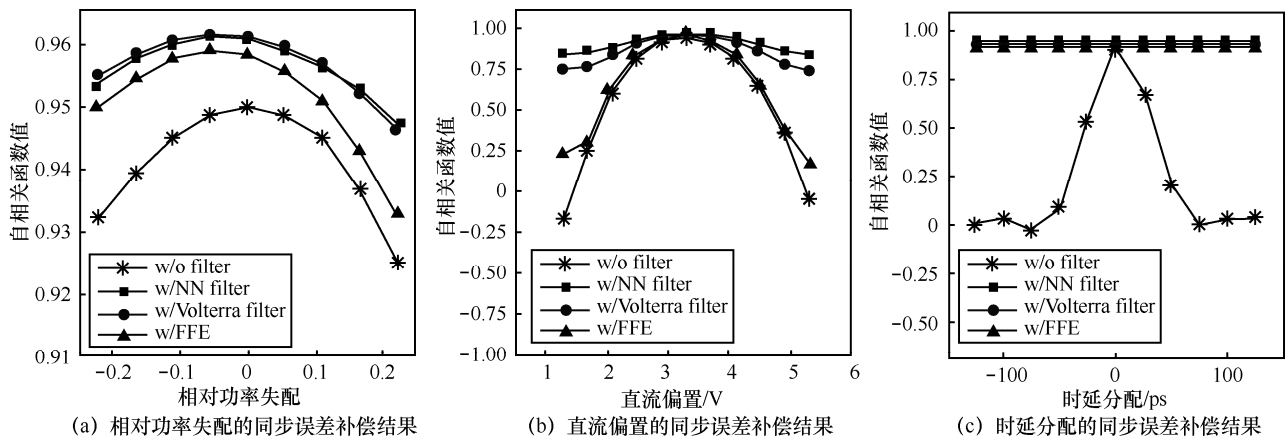


图23 混沌同步误差补偿的实验结果

5 结束语

本文首先根据不同的非线性器件对混沌的产生进行分类, 基于激光器非线性来产生混沌包括全光反馈、光注入和光电反馈3种方式, 由于全光反馈的装置相对简单, 并容易产生混沌, 因此, 基于激光器非线性并通过全光反馈来产生混沌的方法获得了广泛的研究。另外, 相比于基于激光器非线性产生混沌的结构, 基于调制器非线性产生混沌的结构更加容易产生大带宽的混沌信号, 并且相对容易实现混沌同步, 因此适用于混沌保密通信, 并且目前通过该方式实现的混沌保密通信的最高速率可达30 Gbit/s。而相位混沌可以通过相位调制器和马赫-曾德尔干涉仪来产生, 由于相位调制不存在强度的变化, 能够降低传输过程中的非线性, 因此, 通过该方案产生的混沌能够在10 Gbit/s的速率下, 实现100 km的光纤加密传输, 并实现了现场演示。此外, 本文提出了一种通过可调色散补偿器来产生混沌的方式, 可以大大地增加混沌复杂度。本文还介绍了混沌保密光通信的最新研究进展, 包括安全性增强的方案, 其中包括各种时延隐藏的方案以及增加混沌复杂性的方案。另外, 本文还介绍了混沌保密通信系统的研究进展, 速率从最初的几Mbit/s提升到目前最高的30 Gbit/s, 传输距离最大为100 km。随着数字信号处理技术的快速发展和器件带宽的提升, 混沌保密通信的传输速率和传输距离将会得到进一步的提升。最后本文对混沌光通信的困难和未来需要进行的突破进行了讨论, 混沌光通信的进一步发展需要突破高安全性与低复杂度的矛

盾, 需要采用相干检测、数字信号处理技术提升容量和传输距离, 需要破解多节点同步和安全性降低这对矛盾来实现混沌多节点组网。最终实现混沌光通信系统与现有高速光通信系统的完全兼容, 实现为高速光通信系统物理层安全保驾护航的目标。

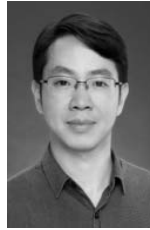
参考文献:

- [1] ZHANG Q, XU F, CHEN Y A, et al, Large scale quantum key distribution: challenges and solutions[J]. Optics Express, 2018, 26(18): 24260-24273.
- [2] MAIMAN T H. Optical and microwave-optical experiments in ruby[J]. Physical Review Letters, 1960, 4(11): 564.
- [3] LORENZ E N. Deterministic nonperiodic flow[J]. Journal of the Atmospheric Sciences, 1963, 20(2): 130-141.
- [4] HAKEN H. Analogy between higher instabilities in fluids and lasers[J]. Physics Letters A, 1975, 53(1): 77-78.
- [5] PECORA L M, CARROLL T L. Synchronization in chaotic systems[J]. Physical Review Letters, 1990, 64(8): 821.
- [6] ARGYRIS A, SYVRIDIS D, LARGER L, et al. Chaos-based communications at high bit rates using commercial fibre-optic links[J]. Nature, 2005, 438(7066): 343-346.
- [7] LAVROV R, JACQUOT M, LARGER L. Nonlocal nonlinear electro-optic phase dynamics demonstrating 10 Gbit/s chaos communications[J]. IEEE Journal of Quantum Electronics, 2010, 46(10): 1430-1435.
- [8] ORTIN S, PESQUERA L, GUTIERREZ J M, et al. Nonlinear dynamics reconstruction with neural networks of chaotic time-delay communication systems[C]//AIP Conference Proceedings. [S.n.:s.l.], 2007: 887.
- [9] WU Y, WANG Y C, LI P, et al. Can fixed time delay signature be concealed in chaotic semiconductor laser with optical feedback[J]. IEEE Journal of Quantum Electronics, 2012, 48(11): 1371-1379.
- [10] RONTANI D, LOCQUET A, SCIAMANNA M, et al. Time-delay identification in a chaotic semiconductor laser with optical feedback: a dynamical point of view[J]. IEEE Journal of Quantum Electronics,

- 2009, 45(7): 879-1891.
- [11] RONTANI D, LOCQUET A, SCIAMANNA M, et al. Loss of time-delay signature in the chaotic output of a semiconductor laser with optical feedback[J]. *Optics Letters*, 2007, 32(20): 2960-2962.
- [12] UCHIDA A. *Optical communication with chaotic lasers*[M]. Weinheim: Wiley-VCH Verlag GmbH, 2012.
- [13] GOEDGEBUER J P, LEVY P, LARGER L, et al. Optical communication with synchronized hyperchaos generated electrooptically[J]. *IEEE Journal of Quantum Electronics*, 2002, 38(9): 1178-1183.
- [14] NGUIMDO R M, *Chaos and synchronization in opto-electronic devices with delayed feedback*[D]. Illes Balears: Universitat de les Illes Balears, 2011.
- [15] NOURINE M, CHEMBO Y K, LARGER L. Wideband chaos generation using a delayed oscillator and a two-dimensional nonlinearity induced by a quadrature phase-shift-keying electro-optic modulator[J]. *Optics Letters*, 2011, 36(15): 2833-2835.
- [16] LAVROV R, PEIL M, JACQUOT M, et al. Electro-optic delay oscillator with nonlocal nonlinearity: optical phase dynamics, chaos, and synchronization[J]. *Physical Review E*, 2009, 80(2): 026207.
- [17] YI L L, KE J X, XIA G Q, et al. Phase chaos generation and security enhancement by introducing fine-controllable dispersion[J]. *Journal of Optics*, 2018, 20(2): 24004.
- [18] ORTÍN S, GUTIERREZ J M, PESQUERA L, et al. Nonlinear dynamics extraction for time-delay systems using modular neural networks synchronization and prediction[J]. *Physica A: Statistical Mechanics and its Applications*, 2005, 351(1): 133-141.
- [19] NGUIMDO R M, SORIANO M C, COLET P. Role of the phase in the identification of delay time in semiconductor lasers with optical feedback[J]. *Optics Letters*, 2011, 36(22): 4332-4334.
- [20] NGUIMDO R M, VERSCHAFFELT G, DANCKAERT J, et al. Loss of time-delay signature in chaotic semiconductor ring lasers[J]. *Optics Letters*, 2012, 37(13): 2541-2543.
- [21] WU J G, XIA G Q, WU Z M. Suppression of time delay signatures of chaotic output in a semiconductor laser with double optical feedback[J]. *Optics Express*, 2009, 17: 20124-20133.
- [22] WU J G, XIA G Q, CAO L P, et al. Experimental investigations on the external cavity time signature in chaotic output of an incoherent optical feedback external cavity semiconductor laser[J]. *Optics Communications*, 2009, 282: 3153-3156.
- [23] LI S S, LIU Q, CHAN S C. Distributed feedbacks for time-delay signature suppression of chaos generated from a semiconductor laser[J]. *IEEE Photonics Journal*, 2012, 4(5):1930-1935.
- [24] WANG D M, WANG L S, ZHAO T, et al. Time delay signature elimination of chaos in a semiconductor laser by dispersive feedback from a chirped FBG[J]. *Optics Express*, 2017, 25(10): 10911.
- [25] WANG D M, WANG L S, GUO Y Y, et al. Key space enhancement of optical chaos secure communication: chirped FBG feedback semiconductor laser[J]. *Optics Express*, 2019, 27(3): 3065.
- [26] KE J X, YI L L, HOU T T, et al. Time delay concealment in feedback chaotic systems with dispersion in loop[J]. *IEEE Photonics Journal*, 2017, 9(2): 1-8.
- [27] HIZANIDIS J, DELIGIANNIDIS S, BOGRIS A, et al. Enhancement of chaos encryption potential by combining all-optical and electrooptical chaos generators[J]. *IEEE Journal of Quantum Electronics*, 2010, 46(11): 1642-1649.
- [28] NGUIMDO R M, COLET P, LARGER L, et al. Digital key for chaos communication performing time delay concealment[J]. *Physical Review Letters*, 2011, 107(3): 034103.
- [29] NGUIMDO R M, COLET P. Electro-optic phase chaos systems with an internal variable and a digital key[J]. *Optics Express*, 2012, 20(23): 25333-25344.
- [30] HOU T T, YI L L, YANG X L, et al. Maximizing the security of chaotic optical communications[J]. *Optics Express*, 2016, 24(20): 23439-23449.
- [31] AROMATARIS G, ANNOVAZZI-LODI V. Enhancing privacy of chaotic communications by double masking[J]. *IEEE Journal of Quantum Electronics*, 2013, 49(11): 955-959.
- [32] URSINI L, SANTAGIUSTINA M, ANNOVAZZI-LODI V. Enhancing chaotic communication performances by Manchester coding[J]. *IEEE Photonics Technology Letters*, 2008, 20(6): 401-403.
- [33] VANWIGGEREN G D, ROY R. Communication with chaotic lasers[J]. *Science*, 1998, 279(5354): 1198-1200.
- [34] LI M, ZHANG X, HONG Y, et al. Confidentiality-enhanced chaotic optical communication system with variable RF amplifier gain[J]. *Optics Express*, 2019, 27(18): 25953-25963.
- [35] TANG S, LIU J M. Message encoding-decoding at 2.5 Gbit/s through synchronization of chaotic pulsing semiconductor lasers[J]. *Optics Letters*, 2001, 26(23): 1843-1845.
- [36] KUSUMOTO K, OHTSUBO J. 1.5-GHz message transmission based on synchronization of chaos in semiconductor lasers[J]. *Optics Letters*, 2002, 27(12): 989-991.
- [37] GASTAUD N, POINSOT S, LARGER L, et al. Electro-optical chaos for multi-10 Gbit/s optical transmissions[J]. *Electronics Letters*, 2004, 40(14): 898-899.
- [38] ANNOVAZZI-LODI V, BENEDETTI M, MERLO S, et al. Optical chaos masking of video signals[J]. *IEEE Photonics Technology Letters*, 2005, 17(9): 1995-1997.
- [39] ARGYRIS A, GRIVAS E, HAMACHER M, et al. Chaos-on-a-chip secures data transmission in optical fiber links[J]. *Optics Express*, 2010, 18(5): 5188-5198.
- [40] ANISHCHENKO V S, VADIVASOVA T E, POSTNOV D E, et al. Synchronization of chaos[J]. *International Journal of Bifurcation and Chaos*, 1992, 2(3): 633-644.
- [41] COLET P, ROY R. Digital communication with synchronized chaotic lasers[J]. *Optics Letters*, 1994, 19(24): 2056-2058.
- [42] LARGER L, GOEDGEBUER J, UDALTSOV V. Ikeda-based nonlinear delayed dynamics for application to secure optical transmission systems using chaos[J]. *Comptes Rendus Physique*, 2004, 5(6): 669-681.
- [43] ANNOVAZZI-LODI V, DONATI S, SCIRE A. Synchronization of chaotic lasers by optical feedback for cryptographic applications[J]. *IEEE Journal of Quantum Electronics*, 1997, 33(9): 1449-1454.
- [44] GOEDGEBUER J P, LARGER L, PORTE H. Optical cryptosystem based on synchronization of hyperchaos generated by a delayed feedback tunable laser diode[J]. *Physical Review Letters*, 1998, 80(10): 2249-2252.

- [45] MIRASSO C R, COLET P, GARCIA-FERNANDEZ P. Synchronization of chaotic semiconductor lasers: application to encoded communications[J]. IEEE Photonics Technology Letters, 1996, 8(2): 299-301.
- [46] FISCHER I, YUN L, DAVIS P. Synchronization of chaotic semiconductor laser dynamics on subnanosecond time scales and its potential for chaos communication[J]. Physical Review A (Atomic, Molecular, and Optical Physics), 2000, 62(1): 1-4.
- [47] SIVAPRAKASAM S, SHORE K A. Message encoding and decoding using chaotic external-cavity diode lasers[J]. IEEE Journal of Quantum Electronics, 2000, 36(1): 35-39.
- [48] ABARBANEL H, KENNEL M, ILLING L, et al. Synchronization and communication using semiconductor lasers with optoelectronic feedback[J]. IEEE Journal of Quantum Electronics, 2001, 37(10): 1301-1311.
- [49] ARGYRIS A, HAMACHER M, CHLOUVERAKIS K, et al. Photonic integrated device for chaos applications in communications[J]. Physical Review Letters, 2008, 100(19): 194101.
- [50] ARGYRIS A, GRIVAS E, HAMACHER M, et al. Chaos-on-a-chip secures data transmission in optical fiber links[J]. Optics Express, 2010, 18(5): 5188-5198.
- [51] NGUIMDO R M, LAVROV R, COLET P, et al. Effect of fiber dispersion on broadband chaos communications implemented by electro-optic nonlinear delay phase dynamics[J]. Journal of Lightwave Technology, 2010, 28(18): 2688-2696.
- [52] AI J Z, WANG L L, WANG J. Secure communications of CAP-4 and OOK signals over MMF based on electro-optic chaos[J]. Optics Letters, 2017, 42(18): 3662-3665.
- [53] ODEN J, LAVROV R, CHEMBO Y K, et al. Multi-Gbit/s optical phase chaos communications using a time-delayed optoelectronic oscillator with a three-wave interferometer nonlinearity[J]. Chaos, 2017, 27(11): 114311.
- [54] KE J X, YI L L, XIA G Q, et al. Chaotic optical communications over 100-km fiber transmission at 30-Gbit/s bit rate[J]. Optics Letters, 2018, 43(6): 1323-1326.
- [55] KE J X, YI L L, HU W S. Chaos synchronization error compensation by neural network[J]. IEEE Photonics Technology Letters, 2019, 31(13): 1104-1107.

[作者简介]



义理林 (1981-)，男，四川广安人，博士，上海交通大学教授、博士生导师，主要研究方向为智能光纤通信、智能光信号处理。



柯俊翔 (1991-)，男，福建永安人，上海交通大学博士生，主要研究方向为混沌保密光通信系统。

优青人物介绍

义理林，上海交通大学教授，博士生导师，区域光纤通信网与新型光通信系统国家重点实验室副主任，国家优秀青年科学基金获得者（2013），教育部青年长江学者（2017）。主要从事智能光信息处理方面的研究，致力于解决高精度光脉冲识别、高性能光时域均衡、高分辨率光频域调控的核心挑战。提出超窄脉冲精确识别方法及偏振态智能调控算法，实现锁模状态可精确调控的智能锁模光纤激光器，成果入选 2019 年度全球光学进展（“Optics in 2019”）和中国光学十大进展。提出多通道线性光均衡技术以及神经网络非线性均衡方法，基于低带宽光电器件实现智能均衡光接入，为烽火通信开发业界首款 100G PON 准产品级平台，技术应用于光迅科技 100GE 产品。提出光纤非线性增益谱数字化精确调控方法，实现高精度智能编程光滤波，获得公开报道的性能最好的矩形光滤波。发表 SCI 论文 90 余篇，其中邀请论文 7 篇，SCI 他引 700 余次。3 次在光通信两大旗舰会议 OFC、ECOC 进行邀请报告，3 次在 OFC、ECOC 组织 workshop。