第 50 卷 第 6 期/2023 年 3 月/中国激光 研究论文

中国激光

光纤保密通信中的全光同步方案设计与实现

曹东东[1,2*]，王明明[1,2]，李将[2]，张卫涛[1,2]，冉焘[1,2]，孙红哲[1,2]，杨振乾[1,2]

[1]航天器在轨故障诊断与维修重点实验室，陕西 西安 710043；

[2]中国西安卫星测控中心，陕西 西安 710043

摘要 光纤保密通信是解决电域加解密“速率瓶颈”和光网络潜在安全威胁的一种有效途径，而实现光纤保密通信的前提是完成密码同步。为保证光纤保密通信系统成功解密，本课题组设计了一种新的全光同步方案，推导出了光纤信道传播时延差的计算公式，详细阐述了全光同步实现过程。采用OptiSystem软件分别在10 Gbit/s和40 Gbit/s加解密速率下进行了全光同步仿真实验，测试分析了密码同步状态对解密输出性能的影响，解密输出数据均与原始明文数据完全相同，而且都保持了较好的输出性能。研究结果表明，所提全光同步方案切实可行，既适用于10 Gbit/s信道速率，也适用于40 Gbit/s信道速率，既适用于常规光纤链路，也适用于经过色散补偿的光纤链路，可以有效解决光纤保密通信中的全光密码同步问题，对光纤保密通信系统的研制开发具有一定的参考价值。

关键词 光通信；光纤保密通信；全光同步；时延校正；波分复用；色散；光纤传播时延差

中图分类号 TN913.7 **文献标志码** A **DOI**：10.3788/CJL220680

1 引 言

近年来，随着光纤攻击与攻击检测技术的不断成熟，各类光纤窃听设备层出不穷，光纤原本所“特有”的物理安全被打破，光网络随时面临安全威胁[1-3]。研究人员提出可以在光网络中采用全光加解密技术进行光纤保密通信，这样既可以解决基于电信号处理的加解密技术的“速率瓶颈”，又可以实现在光域对光信号进行加解密处理[4-7]。然而，目前所报道的全光加解密方案大多是针对光信号进行简单的异或和解异或验证，很少考虑处于异地的加解密双方之间的密码同步问题。在实际应用中，发送端（即加密端）加密所得密文数据要通过光网络传送到相距100 km甚至更长距离处的接收端（即解密端），密文数据在传输过程中会发生一定的传播时延，而且不同距离、不同环境光纤链路对不同波长信号引入的传播时延各不相同，接收端难以确定密文数据的起始位置，导致加解密过程无法同步进行，最终导致误码率增大甚至解密失败。因此，在接收端如何精准确定密文数据序列的起始位置，保证密文数据序列与解密密钥序列的起始位置完全对齐，实现密码同步，是决定光纤保密通信成功的关键。

目前，关于光同步方案的研究工作主要是量子密钥分发（QKD）系统中的远程同步问题[8-11]。在QKD系统中，主要的同步方案有三种：1）使用电缆传送同步电信号[8]；2）采用独立光纤传送量子密钥[9-10]；3）将量子信道和经典信道进行波分复用（WDM）[11]。其中：第一种同步方案通常用于实验系统；第二种方案可以有效传送量子密钥，但经典信道和量子信道通过不同的光纤承载，需要消耗额外的光纤资源，工程建设成本高，无法进行大规模应用；第三种方案可以有效利用现有光网络，不会增加光纤成本，但是量子密钥的光脉冲通常含有的光子数极少，光功率极其微弱，光纤信道串扰对量子密钥造成的影响极大，同时光纤损耗使得接收端对量子密钥的探测效率下降，进而导致误码率增大，限制了传输距离。以上三种同步方案均具有一定的局限性，且主要应用于量子密钥分发系统。在现有的文献资料中，几乎没有关于光网络物理层全光异或加解密系统密码同步方案的研究报道。

为切实解决光网络物理层保密通信中的全光同步问题，受上述第三种方案的启发，本课题组立足现有WDM系统设计了一种新的全光同步方案。在该方案中，密文数据和同步信号进行WDM后均通过光纤经典信道进行传送。本文推导出了光纤信道传播时延差的解析表达式，并通过时延校正来实现光纤保密通信中的密码同步功能。此外，本文对同步实现过程及色散受限距离等进行了详细的理论分析，并通过光通信系统设计软件OptiSystem搭建了全光加解密系统仿真模型，分别在10 Gbit/s和40 Gbit/s比特速率下进行了全光同步仿真验证。

2 基本原理

2.1 同步方案设计

图1所示为本文设计的全光同步方案的原理图，

收稿日期：2022-03-21；**修回日期**：2022-04-24；**录用日期**：2022-05-10；**网络首发日期**：2022-05-20

通信作者：*cdd99992020@163.com

通过在WDM系统中建立密码同步状态来实现光纤保密通信中的全光加解密功能。其中，加密器和解密器采用相同的全光异或结构[4-5]。在发送端，利用合波器将波长较短的密文信号和波长较长且具有特殊码组的同步信号耦合到同一根光纤中，通过光纤经典信道进行传送。在接收端，通过分波器解复用出两路信号，通过同步控制单元对同步信号进行判决检测，并驱动控制光密钥流产生器K2生成解密密钥，解密密钥与同步信号步调一致。长波长的同步信号滞后于短波长的密文信号，导致解密密钥滞后于密文信号，因此需要通过时延控制单元对密文信号进行相应的延时校正，以便使密文数据序列起始位置与解密密钥序列起始位置对齐，从而实现两路信号之间的全光同步功能。

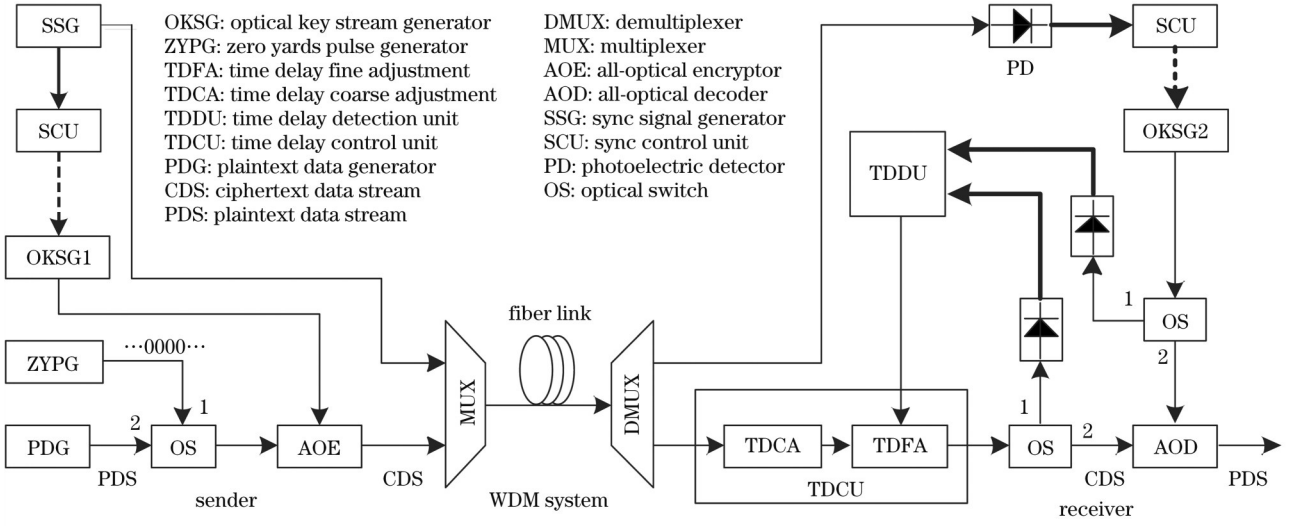

图1　全光同步方案原理图

Fig. 1　Principle diagram of all-optical synchronization scheme

在光纤保密通信中，实现密码同步的关键是计算两路信号之间的时延差，并进行精确的时延校正。时延差来源主要包括光纤信道引起的传播时延差以及系统各模块光电器件引起的处理时延差。其中：传播时延差由光纤色散引起，是时延差的主要来源，可以通过光纤信道传播时延差公式进行计算得到，然后在接收端通过时延控制单元进行延时处理（时延粗调）；相比之下，处理时延差非常小，而且会随着设备性能的变化而变化，难以精确计算，只能通过时延检测单元进行判决检测，然后利用时延控制单元作进一步延时处理（时延精调）。通过时延粗调和时延精调两次时延校正，即可实现光纤保密通信中的全光同步功能。

2.2　时延粗调

时延粗调主要是对光纤信道传播引起的时延差进行校正。设置同步信号发生器输出的同步信号处于长波长λ_{long}，加密所得密文信号处于短波长λ_{short}。在光纤链路中，由于色散的存在，不同频率的光信号以不同的速率在光纤中传播，传播相同距离所需时间不同，即不同光信号的传播时延不同，因此同步信号与密文信号之间产生了时延差。设光纤工作波长λ_0窗口范围的色散系数为D（单位为$ps\cdot nm^{-1}\cdot km^{-1}$），即单位波长间隔（1 nm）的两个频率成分在光纤中传播1 km产生的时延差，则同步信号和密文信号通过长度为L的WDM系统时，由光纤色散引起的时延差可以表示为

$$\Delta t_D = DL(\lambda_{long}-\lambda_{short})。\tag{1}$$

除此之外，即使光纤工作在零色散波长窗口，不同频率的光信号经过一定距离传播后仍然会产生时延差，这主要是由光纤的二阶色散（即色散斜率）在光纤信道中产生的残余色散不断累积引起的。设光纤工作波长λ_0窗口范围的色散斜率系数为S（单位为$ps\cdot nm^{-2}\cdot km^{-1}$），则由光纤色散斜率引起的传播时延差可以表示为

$$\Delta t_S = S\frac{(\lambda_{long}-\lambda_0)+(\lambda_{short}-\lambda_0)}{2}(\lambda_{long}-\lambda_{short})L = S\left(\frac{\lambda_{long}+\lambda_{short}}{2}-\lambda_0\right)(\lambda_{long}-\lambda_{short})L。\tag{2}$$

因此，光纤信道向同步信号和密文信号引入的传播时延差可以表示为

$$\Delta t_{Fiber} = \Delta t_D + \Delta t_S = D(\lambda_{long}-\lambda_{short})L + S\left(\frac{\lambda_{long}+\lambda_{short}}{2}-\lambda_0\right)(\lambda_{long}-\lambda_{short})L = \left[D+S\left(\frac{\lambda_{long}+\lambda_{short}}{2}-\lambda_0\right)\right](\lambda_{long}-\lambda_{short})L。\tag{3}$$

从光纤信道传播时延差的计算公式可以看出，在光纤其他参数一定的情况下，时延差 $\Delta t_{\mathrm{Fiber}}$ 的取值只与光纤长度有关。对于光纤长度为 L 的 WDM 系统，在接收端，首先解复用出两路光信号，然后通过同步控制单元对同步信号进行逐位判决检测，在没有检测到同步码组之前，光密钥流产生器 K2 不输出解密密钥，系统通过时延控制单元对密文信号延时 $\Delta t_{\mathrm{Fiber}}$（时延粗调）。

在实际应用中，全光异或门、光密钥流产生器以及同步控制单元等设备对信号进行处理时都存在一定的时延，且同步信号和密文信号经过的光路并不完全相同，导致时延粗调后的密文信号与解密密钥之间仍然存在一定时延差，因此还必须通过时延精调对密文信号作进一步的延时处理，才能使密文信号的起始位置与解密密钥的起始位置完全对齐。

2.3　时延精调

时延精调是对光纤保密通信中各模块光电器件引起的处理时延差进行校正。本文选择 13 位巴克码序列作为同步码组，其对应的二进制序列为“1111100110101”。如图 1 所示，在系统没有达到严格的密码同步之前，所有光开关连接端口 1。此时，在发送端，同步信号发生器生成比特速率为 1 Gbit/s 且具有 13 位特殊码组“1111100110100”（序列中最后一位“0”代表系统正在进行时延校正）的同步信号（图中用细实线代表光信号）并将其送入 WDM 系统。与此同时，同步信号发生器生成具有相同比特速率和码组的电信号（用粗实线代表电信号）并将其送入同步控制单元，当同步控制单元检测到“1111100110100”时，驱动控制（用粗虚线代表驱动控制过程）光密钥流产生器 K1 生成“1”码脉冲［如图 2(a)所示］，“1”码脉冲与“0”码脉冲发生器从光开关端口 1 输入的全“0”码脉冲［如图 2(b)所示］一起被送入全光加密器进行全光异或处理，输出序列仍然是“1”码脉冲，“1”码脉冲也被送入 WDM 系统，光纤链路对两路光信号进行传送。在接收端，利用同步控制单元对信号进行逐位判决检测，当同步控制单元检测到“1111100110100”时，驱动控制光密钥流产生器 K2 生成“1”码脉冲，“1”码脉冲经光电转换后被送入时延检测单元；与此同时，对经过时延粗调的“1”码脉冲也进行光电转换，然后也送入时延检测单元，通过时延检测单元对两路“1”码脉冲的脉冲上升沿进行判决检测，计算出两路“1”码脉冲上升沿之间的时延差，并驱动控制时延控制单元进行相应的时延校正（时延精调），从而实现严格的密码同步。

此时，系统中所有的光开关接通端口 2，保持光路畅通，使原始明文数据信号发生器生成的待加密明文光包数据流进入全光异或加解密系统。同步信号发生器生成的 13 位巴克码序列“1111100110101”（序列中的最后一位“1”代表系统已经达到严格的密码同步）作为同步码组，驱动控制光密钥流产生器 K1 和 K2 生成正式的光密钥流信号，将它们分别作为加密密钥和解密密钥对通信线路中的光包数据流进行全光异或加密和解密处理。

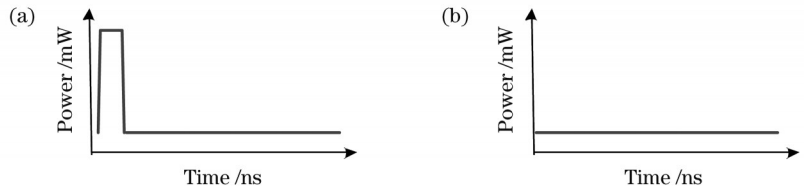

图 2　脉冲信号示意图。(a)“1”码；(b)“0”码

Fig. 2　Schematic of impulse signal. (a) Code 1; (b) code 0

2.4　色散受限距离

色散和损耗是限制光纤通信的两个主要因素。光纤放大器的出现很好地解决了光纤损耗对通信系统的影响，但是光纤色散引起的码间串扰仍然会限制光纤的传输距离和传输速率。色散不仅会导致不同频率成分在传播过程中发生不同的延时，还会导致光脉冲展宽，限制无色散补偿情况下光纤可实现的最大传输距离[12-13]。通常，色散对通信系统传输容量的影响可以用色散受限距离来表示，即

$$L_{\max}=\frac{10^5}{DB^2},\tag{4}$$

式中：$L_{\max}$ 表示在没有进行色散补偿的情况下，理论上光场由于色散受限所能达到的最大传输距离；B 为光脉冲的比特速率；D 为光纤色散系数。可以看出，色散受限距离主要与光纤色散系数、信道比特速率有关，且与信道比特速率的平方成反比。

3　仿真实验

3.1　主要参数设置

利用 OptiSystem 仿真软件搭建全光异或加解密系统模型，通过在收发双方之间接入长距离光纤链路进行全光同步仿真实验。

在仿真模型中，同步信号发生器、“0”码脉冲发生器、明文数据发生器以及光密钥流产生器 K1 和 K2 等各类信号发生模块的结构相同，均由比特序列发生器、归零（RZ）码脉冲生成器、连续波激光器以及马赫-曾德尔电光调制器组成，生成的各路光信号均是通过电光调制方式得到的归零码光脉冲，脉冲消光比均为 30 dB，占空比均为 0.5。明文数据发生器生成待加密的原始明文数据信号码流，对应数据为 128 位周期性循环的伪随机序列“11011001001110000010011011001110110100101……”，比特速率分为 10 Gbit/s 和 40 Gbit/s 两种。光

密钥流产生器K1和K2分别位于加密端和解密端(实际应用中,通过在加密端和解密端本地分别生成密钥流来解决密钥传输过程中可能存在的窃听、篡改等安全问题),均生成128位周期性循环的“10010110111001100011010111000000111011100……”伪随机光密钥流,其比特速率与明文数据信号相对应,异或加密所得密文数据的脉冲序列为“0100111111011110000100110000111000111110……”。将同步信号发生器输出的13位巴克码序列“1111100110101”作为同步码组,为了降低相关模块的复杂度,同步码组的比特速率固定为1 Gbit/s。

全光加密器和解密器的结构相同,均为基于SOA-MZI的全光异或门[4-5]。异或门由一个X型光耦合器、三个Y型光耦合器、两个半导体光放大器(SOA)以及一个高斯滤波器组成。在加解密过程中,X型耦合器将连续探测光波分解为两路光信号,中间两个Y型耦合器分别将两路连续探测信号与脉冲信号(密钥或数据)进行合波,并分别注入在上下两臂对称放置的SOA中。在SOA中,密钥脉冲和数据脉冲(明文或密文)分别调制上下两路连续探测信号发生非线性相位偏移,将自身携带的脉冲信息通过交叉相位调制转换到探测信号上,使两路探测信号产生一定的相位差,最后通过第三个Y型耦合器进行合波干涉,将相位差值转换为“0”“1”脉冲的强度变化,从而实现密钥脉冲与数据脉冲的加解密功能。

WDM系统对同步信号和加密所得密文数据进行耦合传输,光纤链路可选择常规G.652光纤或G.655非零色散位移光纤,不同光纤链路可传输的密文信号速率有所不同。与G.652光纤相比,G.655光纤具有非常优异的色散特性,它在1550 nm波长窗口的色散值较低,且同时具有正负两种色散系数,其色散系数绝对值通常在1.0~6.0 ps·nm^{-1}·km^{-1}范围内变化,不仅适用于10 Gbit/s和40 Gbit/s的光纤通信系统,也适用于新一代100 Gbit/s的光网络。同时,目前不断涌现出的光纤制造工艺也提高了G.655光纤的生产效率,降低了工程成本[14-18]。因此,用光纤链路参数模拟实际应用中的G.655光纤。G.655光纤的主要参数设置如表1所示。

表1 G.655光纤的主要参数设置

Table 1 Main parameter setting of G.655 fiber

Parameter	Value
Reference wavelength /nm	1550
Fiber loss /(dB·km^{-1})	0.2
Dispersion coefficient /(ps·nm^{-1}·km^{-1})	±4.12
Dispersion slope /(ps·nm^{-2}·km^{-1})	0.0828
Mode field area /μm^2	85
Nonlinear refractivity coefficient n_2/(m^2·W^{-1})	2.6×10^{-20}

目前,在G.655光纤应用中,WDM系统的单波长信道速率通常有10 Gbit/s和40 Gbit/s两种。在没有进行色散补偿的情况下,对于10 Gbit/s的信道速率,理论上色散受限的最大传输距离约为240 km,当比特速率增加到40 Gbit/s时,色散受限的最大传输距离只能达到约15 km。在仿真实验中,由于全光异或门的处理过程会导致输出信号质量下降,因此在没有进行色散补偿的情况下,最大光纤传输距离通常达不到理论值。以下基于G.655光纤分别在10 Gbit/s、40 Gbit/s以及光纤链路经过色散补偿的40 Gbit/s加解密速率下进行全光同步仿真实验,不同情况下的光纤长度设置为全光异或加解密系统实现正确解密时所能达到的最大光纤长度。为避免光纤中由强光场注入所引起的非线性影响,并尽可能简化仿真实验模型,将同步信号入纤光功率调整为与加密所得密文信号相同的光功率,保持两路信号入纤光功率均为7 dBm。同步信号和密文信号的信道波长分别设置为1553 nm和1551 nm。

3.2 10 Gbit/s仿真实验

对于10 Gbit/s的信道速率,经过多次仿真实验发现,在保证成功解密的情况下,WDM系统中G.655光纤链路的最大长度可以达到约160 km。利用光纤信道传播时延差公式计算同步信号和密文数据传播160 km所产生的时延差为

$$\Delta t_{\mathrm{Fiber}}=\Delta t_{\mathrm{D}}+\Delta t_{\mathrm{S}}=\left[D+S\left(\frac{\lambda_{\mathrm{long}}+\lambda_{\mathrm{short}}}{2}-\lambda_0\right)\right]\left(\lambda_{\mathrm{long}}-\lambda_{\mathrm{short}}\right)L\approx 1371\ \mathrm{ps}。\tag{5}$$

通过时延控制模块对密文信号进行相应的延时处理,使密文信号与解密密钥起始位置相互对齐,从而实现密码同步。调整密文信号和解密密钥的光功率大小保持基本一致,然后对密钥和密文进行全光异或运算(解密)即可恢复出原始明文信号。

仿真实验过程中各信号的时域波形分别如图3~8所示。图3为波分复用前同步信号“1111100110101”和密文数据“0100111111011110000100110000111000111110……”的时域波形图。图4为解复用出的同步信号和密文数据的时域波形图,可以看出,经过光纤链路传输后,两路信号都发生了延时,并且彼此之间产生了时延差。图5为解密密钥的时域波形图,它发生了与同步信号完全相同的延时。图6为经过时延校正和功率调整后的密文数据的时域波形图,可以看出,最终的密文数据(图6)与解密密钥(图5)的起始位置相互对齐,实现了全光同步。由图7可以看出,解密恢复出的明文数据序列与加密前的原始明文数据序列完全相同,均为“1101100100111000001001101100111011010

010……”，解密成功。图 8(a)、(b)、(c)分别对应波分复用前的密文信号[图 3(b)]、解复用后的密文信号[图 4(b)]以及解密恢复出的明文数据信号[图 7(a)]，可以看出，由于光纤链路的影响，密文数据经光纤信道传播后眼图质量下降，进一步导致解密输出性能下降。图 8(c)所示的信号眼图显示解密恢复出的明文数据信号的 Q 值为 7.12，对应的误码率约为 5.77×10^{-13}。

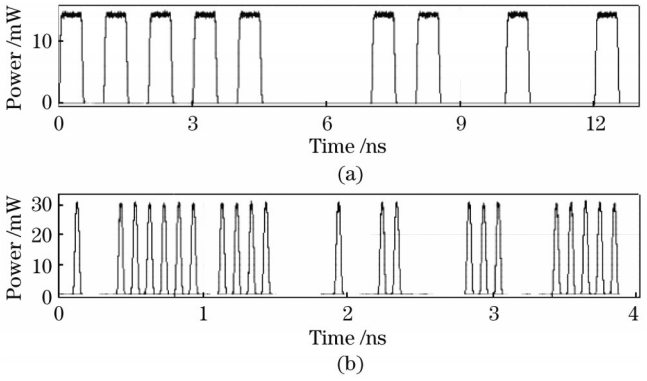

图 3 波分复用前信号的时域波形图。(a)同步信号；(b)密文信号

Fig. 3 Time domain waveform of signals before WDM. (a) Synchronous signal; (b) ciphertext signal

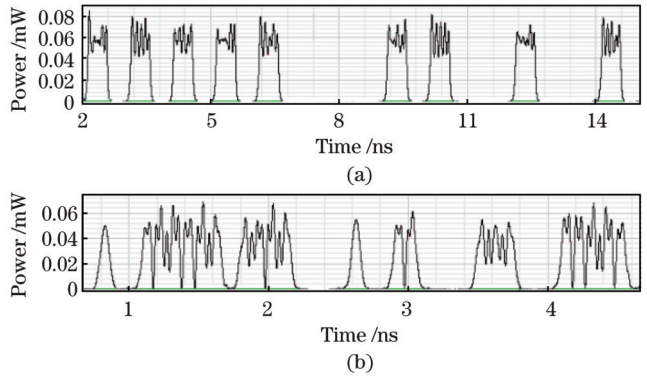

图 4 解复用出的信号的时域波形图。(a)同步信号；(b)密文信号

Fig. 4 Demultiplexed time domain waveform of signals. (a) Synchronous signal; (b) ciphertext signal

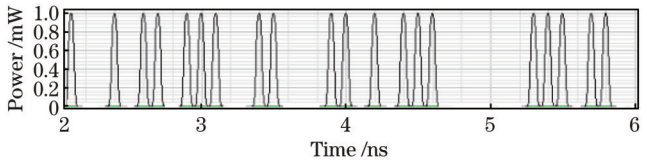

图 5 解密密钥信号的时域波形图

Fig. 5 Time domain waveform of decryption key signal

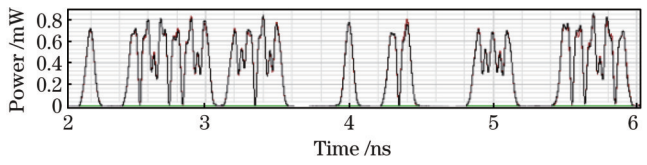

图 6 经过时延校正和功率调整后的密文信号的时域波形图

Fig. 6 Time domain waveform of ciphertext signal after time delay and power adjusting

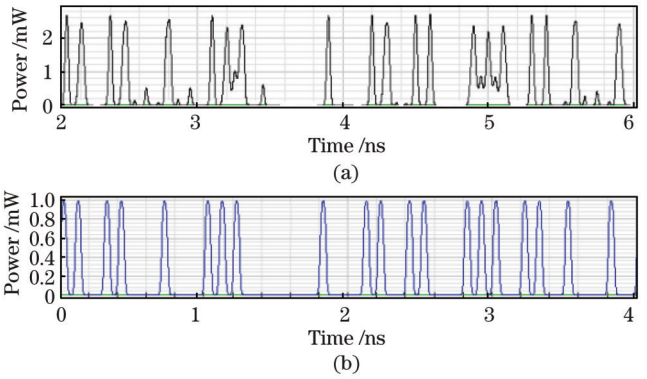

图 7 明文信号的时域波形图。(a)解密恢复出的明文信号；(b)加密前的原始明文信号

Fig. 7 Time domain waveform of plaintext signal. (a) Recovered plaintext signal after decrypting; (b) original plaintext signal before encrypting

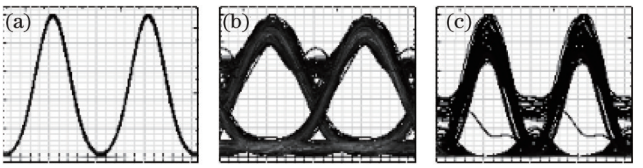

图 8 信号眼图。(a)波分复用前的密文信号；(b)解复用后的密文信号；(c)解密恢复出的明文信号

Fig. 8 Signal eye patterns. (a) Ciphertext signal before WDM; (b) demultiplexed ciphertext signal; (c) recovered plaintext signal after decrypting

3.3 40 Gbit/s 仿真实验

对于 40 Gbit/s 的信道速率，在保证成功解密的情况下，WDM 系统中 G.655 光纤链路的最大长度只能达到约 9 km。利用光纤信道传播时延差公式计算得到同步信号和密文数据传播 9 km 产生的时延差为

$$\Delta t_{\mathrm{Fiber}}=\Delta t_{\mathrm{D}}+\Delta t_{\mathrm{S}}=\left[D+S\left(\frac{\lambda_{\mathrm{long}}+\lambda_{\mathrm{short}}}{2}-\lambda_{0}\right)\right]\left(\lambda_{\mathrm{long}}-\lambda_{\mathrm{short}}\right)L\approx 77\ \mathrm{ps}^{\circ} \tag{6}$$

因此，对密文数据信号进行相应的延时处理，即可实现密码同步，最终解密恢复出原始明文数据。仿真实验中各信号的时域波形分别如图 9～14 所示，波分复用前同步信号的时域波形与图 3(a)中的同步信号相同，各波形图表示的内容与 10 Gbit/s 仿真实验中对应的波形图含义相同。实验结果表明，密文数据经光纤信道传播后信号质量下降，导致解密输出性能下降，而且随着加解密信号速率增大，系统所能达到的最大传输距离减小，但是只要满足密码同步要求，系统依然可以成功解密。

为了验证密码同步对加解密系统的影响，在 40 Gbit/s 仿真实验中(对应的比特周期为 25 ps)，对密码同步状态与解密所得明文信号性能之间的关系开展进一步测试。在接收端，设密文数据序列的起始位置

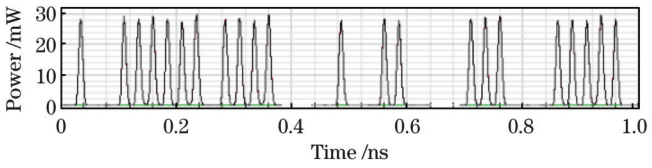

图 9 波分复用前密文信号的时域波形图

Fig. 9 Time domain waveform of ciphertext signal before WDM

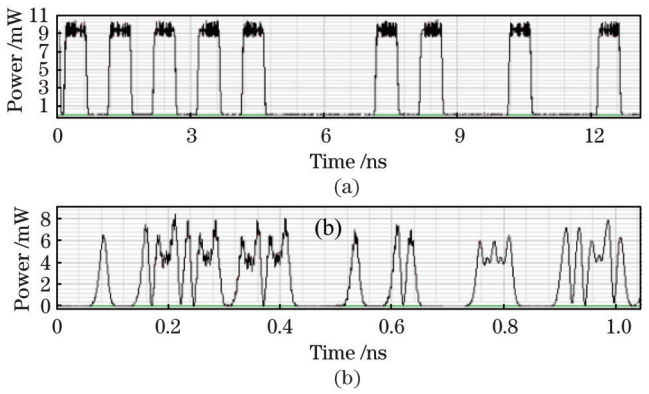

图 10 解复用出的信号的时域波形图。(a)同步信号;(b)密文信号

Fig. 10 Demultiplexed time domain waveform of signals. (a) Synchronous signal; (b) ciphertext signal

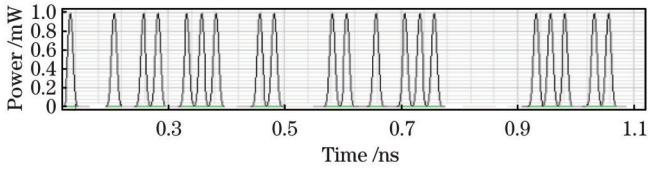

图 11 解密密钥信号的时域波形图

Fig. 11 Time domain waveform of decryption key signal

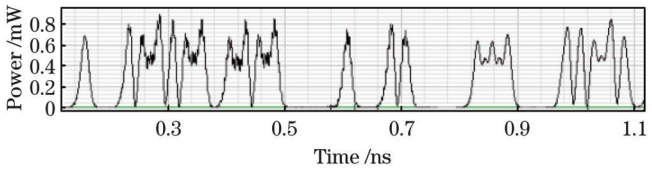

图 12 经过时延校正和功率调整后的密文信号的时域波形图

Fig. 12 Time domain waveform of ciphertext signal after time delay correction and power adjusting

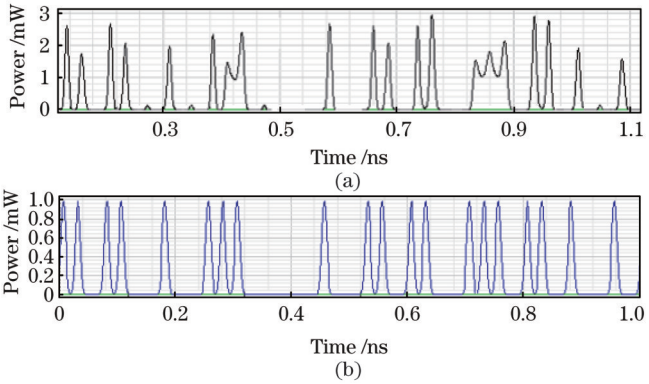

图 13 明文信号的时域波形图。(a)解密恢复出的明文信号;(b)加密前的原始明文信号

Fig. 13 Time domain waveform of plaintext signal. (a) Recovered plaintext signal after decrypting; (b) original plaintext signal before encrypting

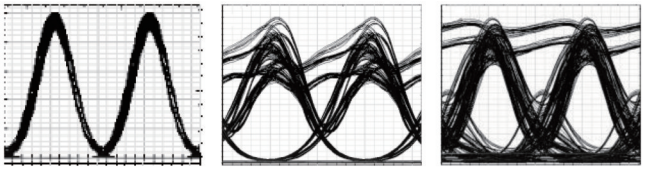

图 14 信号眼图。(a)波分复用前的密文信号;(b)解复用后的密文信号;(c)解密恢复出的明文信号

Fig. 14 Signal eye patterns. (a) Ciphertext signal before WDM; (b) demultiplexed ciphertext signal; (c) recovered plaintext signal after decrypting

为 T_c,解密密钥序列的起始位置为 T_k,用 $T=T_c-T_k$ 表示两路信号之间的密码同步状态。表 2 所示为解密所得明文信号误码率(BER)及 Q 值随 T 的变化情况,图 15 为不同 T 对应的信号眼图。可以看出:当 $T=0$ 时,密文数据与解密密钥起始位置完全对齐,达到了严格的密码同步,此时解密所得明文信号的误码率最小(1.85×10^{-13}),Q 值最大(7.29),信号眼图质量最高[如图 15(e)所示],信号性能最好;随着 T 的绝对值增大,密文数据与解密密钥起始位置的错位程度逐渐加剧,导致解密所得明文信号的误码率增大,Q 值减小,信号眼图质量下降,解密输出信号性能变差。

表 2 密码同步状态对解密恢复出的明文信号的影响

Table 2 Influence of password synchronization state on recovered plaintext signal after decrypting

T /ps	BER	Q factor	T /ps	BER	Q factor	T /ps	BER	Q factor
−12	1	0	−3	9.94×10^{-12}	6.69	6	6.54×10^{-7}	4.83
−11	2.54×10^{-2}	1.88	−2	7.92×10^{-13}	7.05	7	4.58×10^{-6}	4.42
−10	1.39×10^{-2}	2.13	−1	2.59×10^{-13}	7.17	8	5.70×10^{-4}	3.22
−9	7.01×10^{-3}	2.41	0	1.85×10^{-13}	7.29	9	1.76×10^{-3}	2.87
−8	2.63×10^{-3}	2.73	1	5.92×10^{-13}	7.10	10	4.56×10^{-3}	2.54
−7	1.30×10^{-4}	3.62	2	1.29×10^{-12}	6.86	11	3.12×10^{-2}	1.76
−6	1.62×10^{-5}	4.12	3	2.63×10^{-11}	6.54	12	1	0
−5	7.13×10^{-7}	4.81	4	3.07×10^{-10}	6.10			
−4	1.36×10^{-9}	5.92	5	9.13×10^{-8}	5.21			

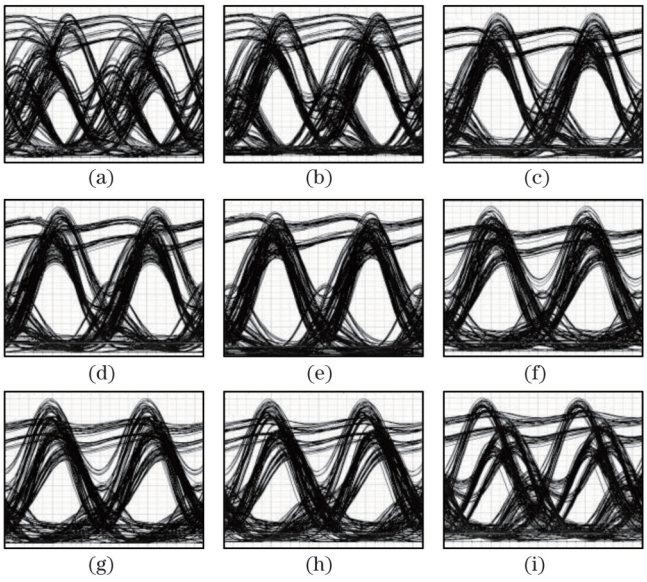

图 15 解密恢复出的明文信号眼图。(a) $T=-7$ ps;(b) $T=-4$ ps;(c) $T=-2$ ps;(d) $T=-1$ ps;(e) $T=0$ ps;(f) $T=1$ ps;(g) $T=2$ ps;(h) $T=4$ ps;(i) $T=7$ ps

Fig. 15 Signal eye pattern of recovered plaintext signal after decrypting. (a) $T=-7$ ps; (b) $T=-4$ ps; (c) $T=-2$ ps; (d) $T=-1$ ps; (e) $T=0$ ps; (f) $T=1$ ps; (g) $T=2$ ps; (h) $T=4$ ps; (i) $T=7$ ps

3.4 光纤链路经过色散补偿的 40 Gbit/s 仿真实验

在上述仿真实验中,对于 40 Gbit/s 的数据速率,加解密系统的最大传输距离只能达到 9 km。为了保证高速率信号的长距离传输,必须通过色散管理技术对光纤信道进行适当的色散补偿[19-22]。在实际应用中,色散补偿无法使通信干线中的总色散值完全为零,因为色散斜率的存在总会引入一定的残余色散。

在仿真实验中,将两段长度均为 80 km、色散系数互为相反数且绝对值相等(4.12 ps·nm^{-1}·km^{-1} 和 -4.12 ps·nm^{-1}·km^{-1})的 G.655 光纤链路接入 WDM 系统,对信道进行色散补偿。利用光纤信道传播时延差公式计算得到同步信号和密文数据传播 80 km+80 km 所产生的时延差为

$$\Delta t_{\mathrm{Fiber}}=\Delta t_{\mathrm{D}}+\Delta t_{\mathrm{S}}-\Delta t_{\mathrm{D}}+\Delta t_{\mathrm{S}}=2\Delta t_{\mathrm{S}}=2S\left(\frac{\lambda_{\mathrm{long}}+\lambda_{\mathrm{short}}}{2}-\lambda_0\right)\left(\lambda_{\mathrm{long}}-\lambda_{\mathrm{short}}\right)L\approx 53\ \mathrm{ps}。\quad(7)$$

对密文数据信号进行相应的延时处理,即可实现密码同步,最终解密恢复出原始明文数据。仿真实验中各信号的时域波形分别如图 16~20 所示,波分复用前同步信号的时域波形与图 3(a)中同步信号的时域波形相同,波分复用前密文数据信号的时域波形与图 9 中密文信号的时域波形相同,原始明文数据信号的时域波形与图 13(b)中明文信号的时域波形相同,各波形图表示的内容与 10 Gbit/s 和 40 Gbit/s 仿真实验中对应波形图的含义相同。实验结果表明,对于经过色散补偿的光纤链路,采用本文提出的全光同步方案依然可以实现密码同步,而且通过色散补偿可以大幅提高 40 Gbit/s 加解密系统的传输距离。从图 20 所示的信号眼图可以看出,解复用后的密文信号和解密恢复出的明文信号的眼图质量依然较好,其中,明文数据信号的 Q 值为 7.33,对应的误码率约为 7.63×10^{-14}。

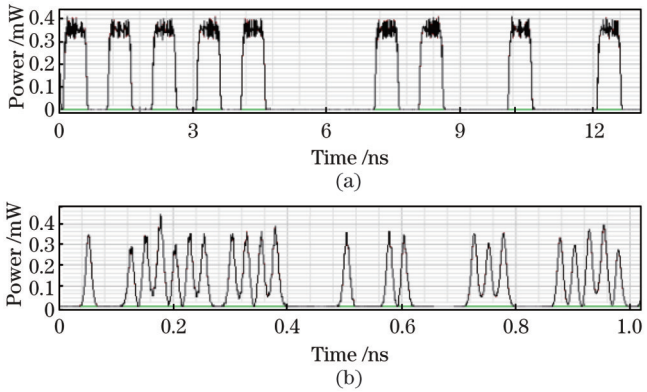

图 16 解复用出的信号的时域波形图。(a)同步信号;(b)密文信号

Fig. 16 Demultiplexed time domain waveform of signals. (a) Synchronous signal; (b) ciphertext signal

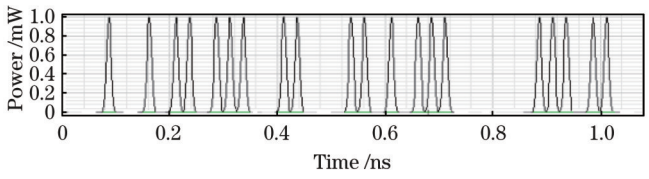

图 17 解密密钥信号的时域波形图

Fig. 17 Time domain waveform of decryption key signal

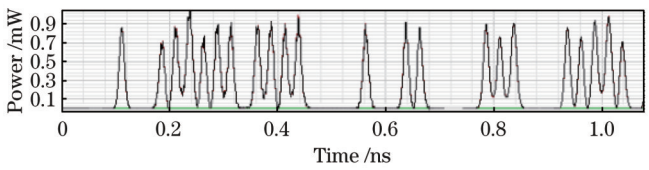

图 18 经过时延校正和功率调整后的密文信号的时域波形图

Fig. 18 Time domain waveform of ciphertext signal after time delay correction and power adjusting

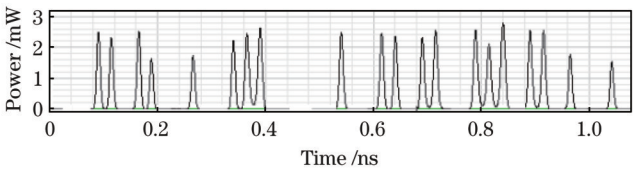

图 19 解密恢复出的明文信号的时域波形图

Fig. 19 Time domain waveform of recovered plaintext signal after decrypting

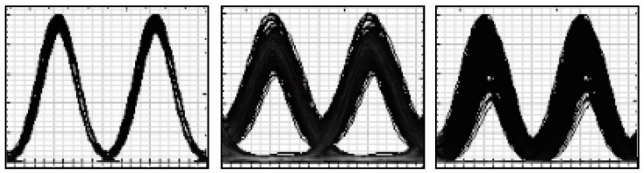

图 20 信号眼图。(a)波分复用前的密文信号;(b)解复用后的密文信号;(c)解密恢复出的明文信号

Fig. 20 Signal eye patterns. (a) Ciphertext signal before WDM; (b) demultiplexed ciphertext signal; (c) recovered plaintext signal after decrypting

4 结 论

在光纤保密通信中,决定系统成功运行的关键是密码同步,只有严格控制加解密两端采用相同的光密钥对光包数据流进行同步操作,保证全光密码同步,才能实现正确解密,恢复出原始明文。通过仿真实验,本文分别在 10 Gbit/s 和 40 Gbit/s 数据速率以及光纤链路经过色散补偿的 40 Gbit/s 数据速率下进行了全光密码同步验证,解密恢复出的明文信号均保持了较好的输出性能。研究结果表明,本文提出的全光同步方案切实可行,可直接应用于 WDM 系统,基本达到了低误码、高速率、长距离、大容量的光纤保密通信要求,对解决光纤通信网目前所面临的“速率瓶颈”和物理层潜在安全威胁具有重要意义,对光纤保密通信系统的研制开发及工程应用具有积极的推进作用。

因实验环境、人力资源以及本课题组成员精力有限,仅在 OptiSystem 平台上对全光密码同步功能进行了仿真验证,未对现有 WDM 系统链路环境与解密输出结果之间的关联性进行更多探究,而且未在实际的光网络环境下对实际数据进行测试验证。下一步研究工作拟考虑搭建全光同步方案原型系统,并在实际的光网络环境中进行实战测试,为光纤保密通信系统的开发应用积累数据和经验。

参 考 文 献

[1] 朱强, 马迎辉. 光网络攻击检测的光纤传感器[J]. 激光杂志, 2017, 38(8): 36-39.
Zhu Q, Ma Y H. Optical fiber sensor for optical network attack detection[J]. Laser Journal, 2017, 38(8): 36-39.

[2] 陈艳辉, 王金东, 杜聪, 等. 光纤偏振编码量子密钥分发系统荧光边信道攻击与防御[J]. 物理学报, 2019, 68(13): 130301.
Chen Y H, Wang J D, Du C, et al. Eavesdropping and countermeasures for backflash side channel in fiber polarization-coded quantum key distribution[J]. Acta Physica Sinica, 2019, 68(13): 130301.

[3] 陈孝莲, 秦奕, 张杰, 等. 基于机器学习的光纤窃听检测方法[J]. 电信科学, 2020, 36(11): 61-67.
Chen X L, Qin Y, Zhang J, et al. Optical fiber eavesdropping detection method based on machine learning[J]. Telecommunications Science, 2020, 36(11): 61-67.

[4] 曹东东, 朱峰, 邓大鹏. 基于SOA-MZI全光异或门的流密码技术研究[J]. 光通信技术, 2012, 36(11): 34-37.
Cao D D, Zhu F, Deng D P. The research of stream cipher technology based on SOA-MZI all-optical XOR gates[J]. Optical Communication Technology, 2012, 36(11): 34-37.

[5] 曹东东, 邓大鹏, 朱峰, 等. 光通信网物理层全光异或加解密技术研究[J]. 光通信研究, 2013(1): 8-10, 23.
Cao D D, Deng D P, Zhu F, et al. Research on all-optical XOR encryption and decryption technology for physical layer of optical communication networks[J]. Study on Optical Communications, 2013(1): 8-10, 23.

[6] 王祥青. 光网络物理层安全认证及加密技术研究[D]. 北京: 北京邮电大学, 2021: 1-16.
Wang X Q. Research on physical layer security authentication and encryption technology of optical network[D]. Beijing: Beijing University of Posts and Telecommunications, 2021: 1-16.

[7] 周立. 光纤保密通信系统的设计、实现及性能分析[D]. 南京: 南京邮电大学, 2021: 64-68.
Zhou L. Design, implementation and performance analysis of optical fiber secure communication system[D]. Nanjing: Nanjing University of Posts and Telecommunications, 2021: 64-68.

[8] 张兵, 唐志列, 梁瑞生, 等. 四态偏振编码解码QKD系统的实验研究[J]. 量子电子学报, 2008, 25(6): 712-718.
Zhang B, Tang Z L, Liang R S, et al. Experiment research of quantum key distribution with four polarization states coding and decoding[J]. Chinese Journal of Quantum Electronics, 2008, 25(6): 712-718.

[9] Mo X F, Zhu B, Han Z F, et al. Faraday-Michelson system for quantum cryptography[J]. Optics Letters, 2005, 30(19): 2632-2634.

[10] 申泽源, 房坚, 何广强, 等. 连续变量量子密钥分发系统中同步方案及实验实现[J]. 中国激光, 2013, 40(3): 0305004.
Shen Z Y, Fang J, He G Q, et al. Synchronous scheme and experimental realization in continuous variable quantum key distribution system[J]. Chinese Journal of Lasers, 2013, 40(3): 0305004.

[11] 刘友明, 汪超, 黄端, 等. 高速连续变量量子密钥分发系统同步技术研究[J]. 光学学报, 2015, 35(1): 0106006.
Liu Y M, Wang C, Huang D, et al. Study of synchronous technology in high-speed continuous variable quantum key distribution system[J]. Acta Optica Sinica, 2015, 35(1): 0106006.

[12] 阙凌薇, 印新达. 光通信系统中色散容限的分析[J]. 光通信研究, 2008(6): 14-16, 36.
Que L W, Yin X D. Analysis of dispersion tolerance in optical communication systems[J]. Study on Optical Communications, 2008(6): 14-16, 36.

[13] 杨韬, 郑波. 40G WDM传输系统传输受限及解决方法研究[J]. 计算机与数字工程, 2011, 39(12): 41-43, 130.
Yang T, Zheng B. Restricted transmission and solutions for 40G WDM systems[J]. Computer & Digital Engineering, 2011, 39(12): 41-43, 130.

[14] 吴金东, 李庆国, 吴雯雯, 等. 非零色散位移光纤的制造新工艺研究[J]. 光学学报, 2011, 31(8): 0806008.
Wu J D, Li Q G, Wu W W, et al. Study of novel fabrication process for non-zero dispersion-shifted fibers[J]. Acta Optica Sinica, 2011, 31(8): 0806008.

[15] 曾辉, 卓辉. 超高速通信系统中非零色散位移光纤多孤子传输影响[J]. 光电子技术, 2015, 35(1): 23-28.
Zeng H, Zhuo H. The transmission effects of multi-solitons in non-zero dispersion shifted fiber super high speed communication system[J]. Optoelectronic Technology, 2015, 35(1): 23-28.

[16] 马志军, 江博凡, 许琦, 等. 金属纳米晶复合光纤的制造和应用[J]. 激光与光电子学进展, 2019, 56(17): 170610.
Ma Z J, Jiang B F, Xu Q, et al. Fabrication and applications of metal nanocrystals hybridized optical fibers[J]. Laser & Optoelectronics Progress, 2019, 56(17): 170610.

[17] 刘益春. 超高非线性二维材料复合光纤制造取得新进展[J]. 物理化学学报, 2022, 38(8): 2012028.
Liu Y C. New progress in the manufacture of ultrahigh nonlinear two-dimensional material hybrid fiber[J]. Acta Physico-Chimica

Sinica, 2022, 38(8): 2012028.
[18] 朱龙洋, 郑宏军, 黎昕, 等. 色散平坦光纤中的高速率PM-16QAM信号传输研究[J]. 红外与激光工程, 2018, 47(9): 0922003.
Zhu L Y, Zheng H J, Li X, et al. Research on high bitrate PM-16QAM signal transmission over dispersion flattened fiber[J]. Infrared and Laser Engineering, 2018, 47(9): 0922003.
[19] 刘玉红, 刘宁亮, 陈建军. 基于Gires-Tournois标准具的色散补偿优化设计[J]. 中国激光, 2017, 44(6): 0606003.
Liu Y H, Liu N L, Chen J J. Optimized design for dispersion compensation based on Gires-Tournois etalon[J]. Chinese Journal of Lasers, 2017, 44(6): 0606003.
[20] 曹文华. 准线性光纤传输系统中几种色散补偿方案的性能比较[J]. 光学学报, 2018, 38(4): 0406002.
Cao W H. Performance comparison of different chromatic dispersion compensation schemes in quasi-linear fiber-optic transmission system[J]. Acta Optica Sinica, 2018, 38(4): 0406002.
[21] 李伟, 王道, 胡必龙, 等. 光学参量啁啾反转脉冲放大系统色散补偿方案[J]. 中国激光, 2020, 47(6): 0601008.
Li W, Wang X, Hu B L, et al. Dispersion-compensation scheme of optical parameter chirp reversal pulse amplification system[J]. Chinese Journal of Lasers, 2020, 47(6): 0601008.
[22] 孙伟义, 黄家鹏, 陈丽明, 等. 10 W量级高功率中红外超快光纤激光系统中色散管理的仿真设计[J]. 中国激光, 2022, 49(1): 0101012.
Sun W Y, Huang J P, Chen L M, et al. Design of a 10 W level dispersion-managed high-power ultrafast mid-infrared fiber laser system[J]. Chinese Journal of Lasers, 2022, 49(1): 0101012.

Design and Implementation of All-Optical Synchronization Scheme in Optical-Fiber Secure Communication

Cao Dongdong[1,2*], Wang Mingming[1,2], Li Jiang[2], Zhang Weitao[1,2], Ran Tao[1,2], Sun Hongzhe[1,2], Yang Zhenqian[1,2]

[1]*Key Laboratory for Fault Diagnosis and Maintenance of Spacecraft in Orbit, Xi'an* 710043, *Shaanxi, China*;
[2]*Xi'an Satellite Control Center, Xi'an* 710043, *Shaanxi, China*

Abstract

Objective In recent years, owing to the advancements in attacks and attack detection technology for optical fiber, various types of optical-fiber eavesdropping devices have emerged; the original "unique" physical security of optical fiber has been broken, and the optical network constantly encounters security threats. In this study, the use of all-optical encryption and decryption technology in optical networks for optical-fiber secure communication is proposed; it can solve the "rate bottleneck" problem of encryption and decryption technology based on electrical signal processing and can encrypt and decrypt the optical signal in the optical domain. Optical-fiber secure communication can be inferred to be an effective method for solving the "rate bottleneck" problem of encryption and decryption in the electric domain and mitigating the potential security threats in optical networks. However, most of the all-optical encryption and decryption schemes reported thus far are simple XOR verifications for optical signals and rarely consider the cipher synchronization problem between the encryption and decryption parties in different places. In practical applications, the ciphertext data encrypted at the sender's end must be transmitted to the receiver 100 km or more away through the optical network, and a certain propagation time delay occurs in the transmission process. Determining the starting position of the ciphertext data is difficult for the receiver; this makes synchronization between the processes of encryption and decryption impossible, leading to an increase in the error rate and decryption failure. Thus, the key to realizing optical-fiber secure communication is cipher synchronization. To effectively solve the cipher synchronization problem in optical-fiber secure communication, an all-optical synchronization scheme is designed in this study to precisely determine the starting position of the ciphertext data sequence and adjust the starting position of ciphertext data and decryption key; this can achieve cipher synchronization, which will help the receiver to successfully decrypt.

Methods In this study, we design an all-optical synchronization scheme based on the existing wavelength division multiplexing (WDM) system, which transmits ciphertext data and synchronization signals through a classical optical fiber channel after applying WDM. The formula for the propagation time delay difference in the optical fiber channel is deduced, and the function of cipher synchronization in optical-fiber secure communication is achieved by employing time delay correction. To prove the feasibility of the all-optical synchronization scheme, a simulation model of the all-optical encryption and decryption system is built on an OptiSystem platform, and the all-optical synchronization scheme is simulated and verified at 10 Gbit/s and 40 Gbit/s. The output data after decryption are identical to the original plaintext data, and both indicate good output performance. To verify the influence of cipher synchronization on the encryption and decryption system, the correlation between the cipher synchronization state and the performance of the plaintext signal decrypted is tested and analyzed in a 40 Gbit/s simulation experiment. To solve the problem of the maximum transmission distance of the 40 Gbit/s data rate being limited, the all-optical synchronization scheme at 40 Gbit/s for long-distance optical fiber links based on dispersion compensation is simulated and verified.

Results and Discussions The simulation results show that the maximum length of the G.655 optical fiber link in the WDM system can reach approximately 160 km for a 10 Gbit/s channel rate with successful decryption, the Q factor of the recovered plaintext

data signal after decryption is 7.12, and the corresponding bit error rate is approximately 5.77×10^{-13}. The maximum length of the G.655 optical fiber link in the WDM system can only reach approximately 9 km for the 40 Gbit/s channel rate with successful decryption, the bit error rate of the recovered plaintext data signal after decryption is 1.85×10^{-13}, and the Q factor is 7.29. With the increasing misplacement of the ciphertext data and decryption key, the bit error rate of the recovered plaintext data signal after decryption increases, the corresponding Q factor decreases, the quality of the signal eye pattern degrades, and the performance of the output signal after decryption deteriorates. The maximum length of the G.655 optical fiber link based on the dispersion compensation in the WDM system can reach 80 km+80 km for the 40 Gbit/s channel rate with successful decryption, the Q factor of the recovered plaintext data signal after decryption is 7.33, and the corresponding bit error rate is approximately 7.63×10^{-14}.

Conclusions The results show that the proposed all-optical synchronization scheme is feasible and can be directly applied to WDM systems. The scheme is suitable for both 10 Gbit/s and 40 Gbit/s channel rates, for both conventional fiber links and fiber links based on dispersion compensation; it can effectively solve the problem of all-optical cipher synchronization in optical-fiber secure communication and meet the requirements of a low bit error rate, high speed, long distance, and large capacity. Solving the "rate bottleneck" problem and mitigating the potential security threats to the physical layer in the optical-fiber communication network are crucial for promoting the development and application of the optical-fiber secure communication system.

Key words optical communications; optical fiber secure communication; all-optical synchronization; time delay correction; wavelength-division multiplexing; dispersion; propagation time delay difference of optical fiber channel