引用本文：张旭，张杰，李亚杰，等. 基于量子噪声流加密的光纤物理层安全传输技术[J]. 光通信技术，2020，44(4)：18-22.

基于量子噪声流加密的光纤物理层安全传输技术

张 旭[1]，张 杰[2*]，李亚杰[2]，张会彬[2]，雷 超[2]，涂志伟[2]

（1.国网甘肃省电力公司 信息通信公司，兰州 730050；2.北京邮电大学 信息光子学与光通信国家重点实验室，北京 100876）

摘要：针对通信窃听问题，以“内生安全光通信理论与技术研究”项目为研究背景，从信息层面、载波层面和调制后的信号层面，介绍了光纤物理层安全传输的现有技术发展。提出了一种基于量子噪声流加密的光纤物理层安全传输技术，将离散傅里叶变换扩展的正交频分复用(DFTs-OFDM)引入基于正交幅度调制(QAM)的量子噪声流加密传输系统，在保证高频谱利用率的同时，有效抵御非合作方的窃听。研究结果表明：该传输技术实现了 10 Gb/s 的传输速率、无中继传输距离达 300 km 的光纤传输，且 Q 因子超过 9，信息截获概率低于 0.001%。

关键词：物理层安全传输；量子噪声流加密；正交频分复用

中图分类号：TN929.11　**文献标识码**：A　**文章编号**：1002-5561(2020)04-0018-05

DOI：10.13921/j.cnki.issn1002-5561.2020.04.004　**开放科学(资源服务)标识码(OSID)**：

Fiber physical layer secure transmission technology based on quantum noise stream cipher

ZHANG Xu[1], ZHANG Jie[2*], LI Yajie[2], ZHANG Huibin[2], LEI Chao[2], TU Zhiwei[2]

(1. State Grid Gansu Electric Power Company Information Communication Company, Lanzhou 730050, China; 2. State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China)

Abstract: Aiming at the problem of communication eavesdropping, based on the research project of "research on self-secured optical communications theories and technologies", the existing technology development of fiber physical layer security transmission is introduced at the information level, carrier level and modulated signal level. This paper proposes a fiber physical layer secure transmission technology based on quantum noise stream cipher. The orthogonal frequency division multiplexing based on DFT-spread(DFTs-OFDM) is introduced into the quantum noise stream cipher transmission system based on quadrature amplitude modulation (QAM), which can effectively resist the eavesdropping of non-partners while ensuring high spectrum utilization. The research results show that the optical transmission rate of 10 Gb/s has no relay transmission distance of 300 km, and the Q factor exceeds 9, and the information interception probability is less than 0.001%.

Key words: physical layer secure transmission; quantum noise stream cipher; orthogonal frequency division multiplexing

0 引言

信息技术飞速发展，光纤以其传输频带宽、抗干扰性高和信号衰减小的特点，已成为全世界通信的主要传输媒介。光纤通信发展迅速，但是光缆传输距离长、线路环境复杂，现有光通信无法抵御线路或节点窃听攻击。非合作方可以利用光纤通信网络中的光放大器、光交叉连接设备以及传输链路等网络单元，通过将光信号分解出光纤，非法提取正常的传输信号的信息。该方法隐蔽性强，不易被发现。目前，利用物理层安全方案实现通信系统安全性，成为新的研究热点，受到了国内外的广泛重视。物理层安全光通信是以抵御线路或节点窃听攻击为目的，以增强抗截获信息防护能力为手段的新体制光通信技术。当前针对物理层安全光通信的基础研究可以分为 2 类：一类是量子密钥分发理论；另一类是物理层安全理论。以量子密钥分发为代表的新型网络信息安全技术仍有待完善，目前存在诸多制约因素。量子密钥分发要求使用

收稿日期：2019-08-04。

基金项目：国家自然科学基金重点项目(61831003)资助。

作者简介：张旭(1984—)，男，甘肃天水人，长期从事电力系统通信和信息化工作，熟悉通信传输网、信息系统开发、大数据分析和人工智能等方面的技术，作为主要负责人承担 erp、营销信息化和大容量骨干通信网运营监测等开发应用工作。

*** 通信作者**：张杰(E-mail: jie.zhang@bupt.edu.cn)。

单光子或弱信号进行传输，以至于它对噪声及信号损伤非常敏感。长距离传输所需的光放大器会不可避免地引入噪声，因此量子密钥分发与现有长距离传输系统不兼容。本文重点研究噪声加密安全光通信技术，提出一种基于量子噪声流加密的光纤物理层安全传输技术。

1 光纤物理层安全传输现有技术综述

光纤物理层安全通信技术是在光网络物理层上进行安全处理，旨在通过通信手段以保证传输信息和传输过程的安全，防止非合作方对信号进行恶意拦截。为了应对光网络物理层安全问题，国内外均投入了大量的人力、物力进行相关光通信物理层安全技术的研究。光网络物理特性的多样性决定了其安全技术也具有方式多、方法多和技术路线多的特点，目前光网络物理层安全技术整体研究情况如图 1 所示。

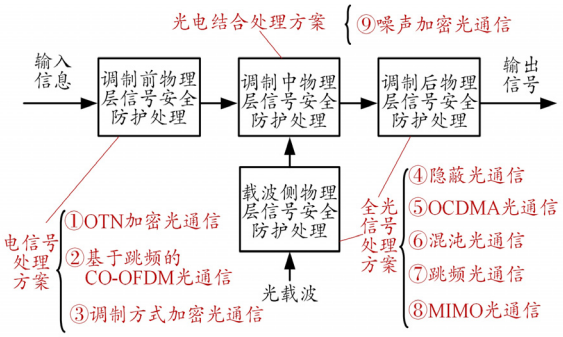

图 1 光网络物理层安全技术概述图

物理层防护主要围绕信号物理层变换过程展开。从信息层面、载波层面以及调制后的信号层面分为调制前、调制中、调制后和载波侧物理层信号安全防护处理。在实现手段上分为电信号处理方案、全光信号处理方案和光电结合处理方案。

◆电信号处理方案是在电域完成安全处理，强调变换的复杂性和多样性，提高信息抗分析能力。具体包含光传送网（OTN）加密光通信、相干光正交频分复用（CO-OFDM）加密光通信和调制方式加密光通信。

◆全光信号处理方案主要是对调制后的全光信号以及载波侧的光源信号进行处理，通过全光处理，可以实现信号在光域背景下难以分析识别。具体包括隐蔽（Steganography）光通信[1]、光码分复用（OCDMA）通信、混沌光通信[2]、跳频光通信（时间–波长变换）[3]和多入多出（MIMO）光通信。该方案的突出特点是信号光被隐藏，难以在线路上进行识别和判决。

◆光电结合处理方案强调光噪声的影响，传统光通信方式主要考虑光噪声对系统通信性能的影响，为了保证良好的传输效率，一般通过各种技术尽量减小光噪声的影响。而光电结合方案则充分利用光噪声解决安全传输问题，与全光信号处理方案相比，具有更好的系统兼容性。目前，除了 OTN 加密光通信和光电结合处理方案之外，其它各种光通信物理层安全技术均处于理论研究阶段，并无实际产品进行商用，而 OTN 加密光通信基本是上层加密技术的延伸。

2 基于量子噪声流加密的光纤物理层安全传输技术

2.1 量子噪声流加密原理概述

量子噪声流加密是将二进制信号转换为非常密集的高维信号集，利用光的相位和幅度波动来执行加密。与典型的高维信号不同，扩展的星座集不用于提高频谱效率，而是用于提高安全性。多路复用值中只有一位用于发送信息，而其它值则是抵御窃听者（Eve）的伪信息[4]。量子噪声扩散使相邻电平（强度和相位）之间充分重叠，明文得以隐藏，数据信号隐藏在 Eve 接收器中的量子相位噪声或幅度噪声中[2]。这在所使用的密码学算法之上增加了真正的随机噪声分量，使得密码破译更加困难。而合法用户通过预共享密钥，在高信噪比条件下还原信息[5]。另外，量子噪声流加密可以与传统的波分复用通信系统共存，并且可以长距离传播[6]。

基于 QAM 的量子噪声流加密原理如图 2 所示。合法通信双方使用的密钥（状态基）是绝对安全的[7]。调制器发出 2×5 路信号，分成正交等长的 I 路和 Q 路，其中每路进行的是 2^5 进制幅度调制，光的幅度变为密集多值，前 4 位数据就是状态基。加密映射规则

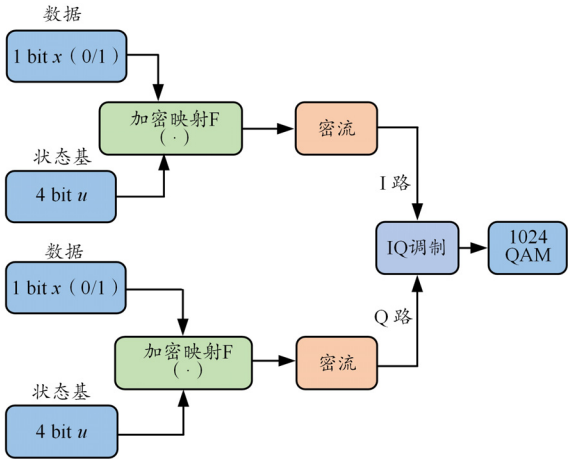

图 2 基于 QAM 的量子噪声流加密原理示意图

如式(1)所示,其中 x 是数据,u 是状态基,当 u 是偶数时,$Pol(u)=0$;当 u 是奇数时,$Pol(u)=1$。

$$F(x,u)=u+[x\oplus Pol(u)]\times 2^{|u|} \tag{1}$$

加密的带噪声的 1024QAM 信号星座图如图 3 所示,发送数据 $(1,Q)_{data}=(1,1)$,状态基 $(1,Q)_{base}=(0100,0010)$,产生的加密信号是 $(1,Q)=(10100,10010)$。在每个时隙中,QPSK 星座随不同的状态基移动。加密的模拟信号十进制范围是 $0\sim 2^{m+l}-1$,其中 m 是数据长度,在图 3 中 $m=1$;l 是状态基长度,$l=4$。由于光束的电场有正有负,所以此时的信号范围是 $-2^{m+l}+1\sim 2^{m+l}-1$。在合法接收端,使用反向的加密规则解密信号,对于 I 路信号的判决门限是 $2^l/2=2^{l-1}$,光束中的判决门限是 $2^l-(2^{m+l}-1)$,图 3 中的判决门限是 8,光束中的判决门限是 −15。归一化后,I 路在二进制的结果为 01000,这个电平用来判决信号计算误比特率。对于知道密钥也就是状态基的合法接收端来说,属于同一状态基的 2 个信号之间的信号距离足够大,因此合法接收端可以基本无误检测信号;而 Eve 不知道状态基,必须在噪声存在的情况下区分 1024(甚至更高阶)QAM 信号,因此无法得到正确信号。因此,本文可以通过增加信号的数量来提高 Eve 解密的难度,而合法接收端利用密钥信息区分状态基。换句话说,该加密技术通过合法接收方和窃听者之间的信噪比(SNR)的巨大差异来建立安全性。

2.2 量子噪声流加密的光纤物理层安全传输系统

基于量子噪声流加密的长跨距无中继光纤物理层安全传输系统的结构框图如图 4 所示。在发送端,以一个中心波长为 1550 nm 的外腔激光器作为光源。原始数据由数字信号处理(DSP)模块生成,经随机信号发生器转化为电信号,然后由 I/Q 调制器加载到光载波上。经掺铒光纤放大器(EDFA)功率放大后,光信号通过300 km超低损单模光纤在无中继放大器的情况下传输至接收端。到达接收端后,信号先由 EDFA放大,再和同源激光器发出的本振光通过相干接收机作用,解调出I/Q 路信号。然后通过示波器采集得到数据、接收端 DSP 模块恢复出原始信号。图 5 为存在 Eve 窃听的系统模型框图。本文采用 50%分光器模拟 Eve 窃取光信号,通过相同的方法处理所得光信号,区别在于 Eve 没有生成状态基的密钥,它只能通过猜测解出原始信号。

图 6 为 DSP 模块在发送端和接收端的处理流程图。在发送端,首先将二进制伪随机序列数据映射成正交相移键控(QPSK)格式,接着将 QPSK 信号转换为经过加密处理的 QAM 格式(其中,将 1 位 QPSK 数据与多位状态基分别在 I/Q 路组合生成加密 QAM 信号)。然后,采用 DFTs-OFDM 技术实现 2 个波段携带有效载荷[8],通过离散傅里叶变换(DFT)展开,将整个有效载荷分成两部分。每部分采用 256-DFT,将两部

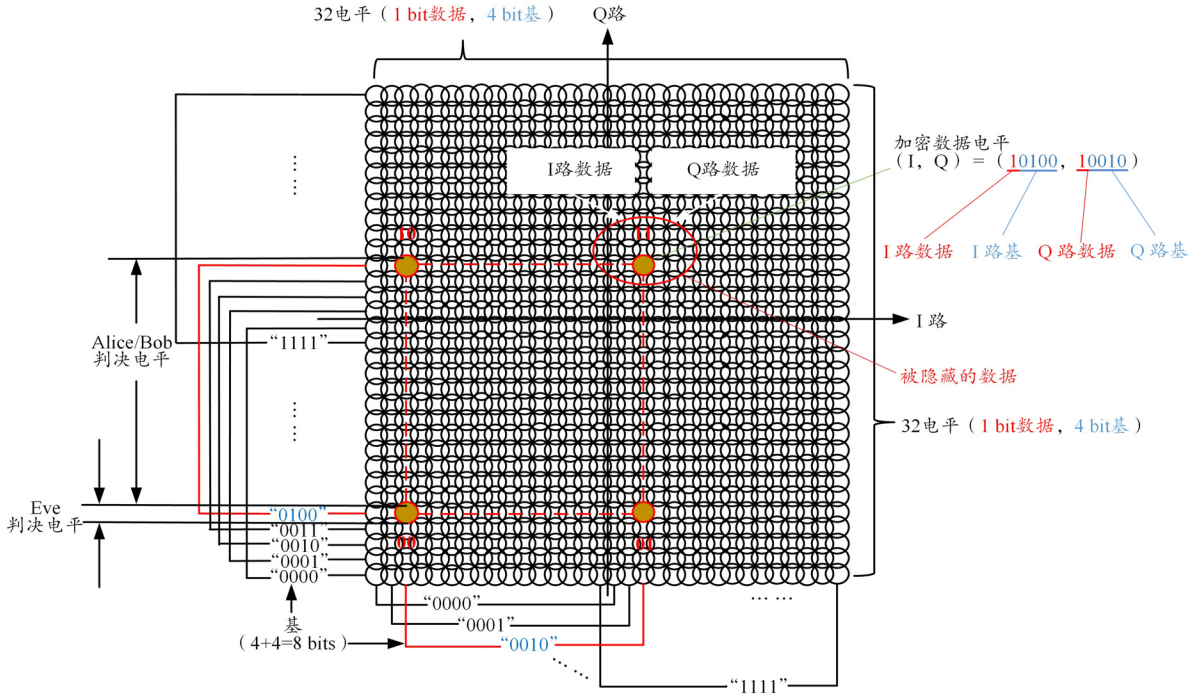

图 3 加密的带噪声的 1024QAM 信号星座图

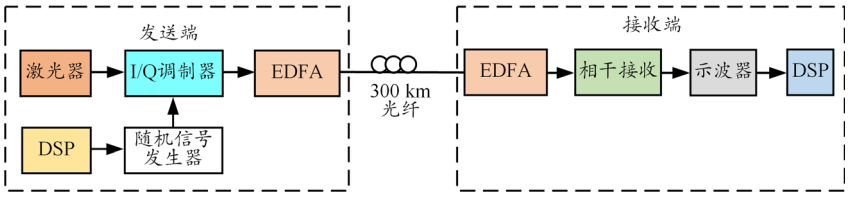

图 4 基于量子噪声流加密的长跨距无中继光纤安全传输系统结构框图

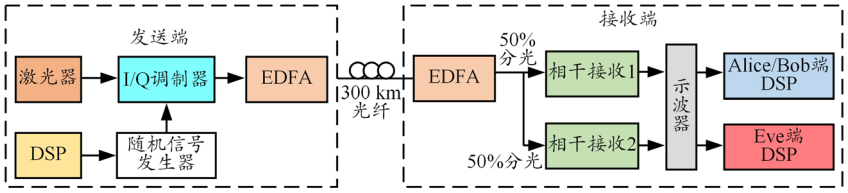

图 5 窃听分析系统框图

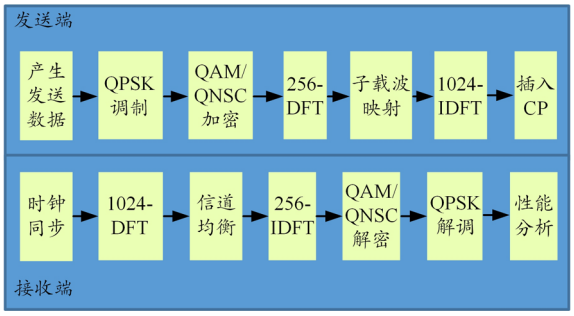

图 6 收发端数字信号处理技术

分插入发射机带宽中心;在高频率部分填充 0,用 1024 点离散逆傅里叶变换(IDFT)将频域信号转换为时域信号。最后,插入循环前缀(CP),其本质是一个数据符号后面的一段数据复制到该符号的前面形成的循环结构,这样可以保证有时延的 OFDM 信号在 DFT 积分周期内总是具有整数倍周期。在接收端,经过时钟同步后,先由 1024–DFT 将时域信号转到频域信号处理。因为经过了 300 km 光纤信道的传输,所以先通过均衡技术最大程度地消除信道带来的影响,然后以发送端相反顺序处理,解出 QPSK 信号,再进行性能分析。

2.3 实验验证

基于量子噪声流加密的光纤物理层安全传输系统实物图如图 7 所示,系统实验使用的主要仪器参数如表 1 所示。

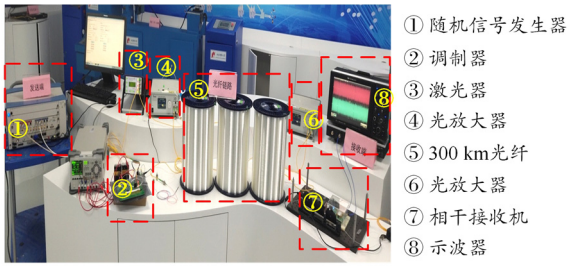

图 7 基于量子流噪声加密的光纤物理层安全传输系统实物图

表 1 主要实验仪器参数设置

器件	参数
激光器波长	1550 nm
激光器输出功率	10 dBm
AWG 输出速率	10 Gb/s
AWG 输出电压	600 mV
发送/接收端 EDFA 输出功率	10 dBm/0.5 dBm
示波器采样速率	40 GS/s

系统传输性能主要通过误码率(BER)来衡量。但 BER 实际变化范围很小,很难判断系统性能的优劣。在此引入 Q 因子,定义为:

$$Q=20\times\lg10[\sqrt{2}\times\mathrm{erfcinv}(2\times BER)] \tag{2}$$

Q 因子在 BER 小范围变化时变化明显,起到放大镜的作用。Q 因子与距离的关系图如图 8 所示,随着距离增加,Q 因子慢慢下降。这是因为距离越长所需激光器输入功率也就越大。而激光器输入信号功率过大时,系统受非线性影响加深,使得 Q 因子也即传输性能下降。在 300 km 时,Q 因子能达到 9 以上。BER 随距离变化情况如图 9 所示,当传输距离在 0~300 km 范围内增加时,BER 呈指数上升。在低密度奇偶校验码(LDPC)纠错码的作用下,合法通信方在 300 km 以内依旧能保证 BER 为 0。

为了进一步说明该传输系统的安全性,本文分析了 Eve 的窃听攻击,通过截获状态基错误率和信息截获概率来表征安全性能。基错误率也就是 Eve 猜测状态基错误的概率,该指标越高说明 Alice 和 Bob 加密用的密钥越安全。信息截获概率 P 定义如式(3)所示,其含义为 Eve 所获得数据的 BER 与 1/2 的差的绝对

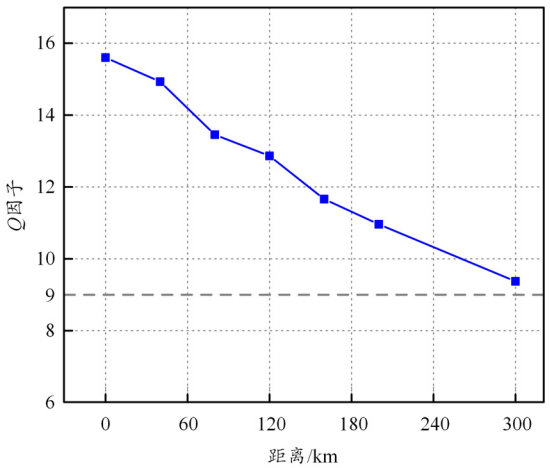

图 8 Q 因子与距离的关系图

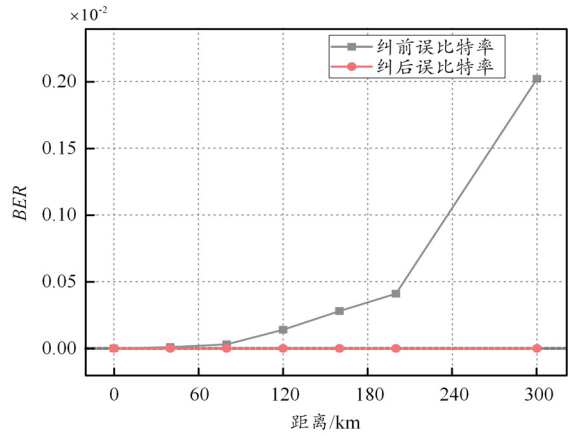

图 9 *BER* 随距离变化图

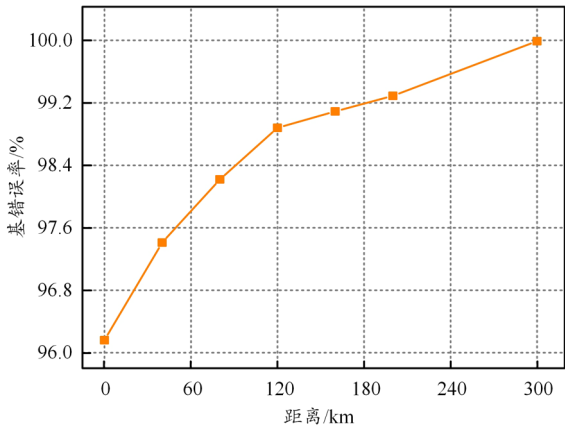

图 10 基错误率和距离的关系

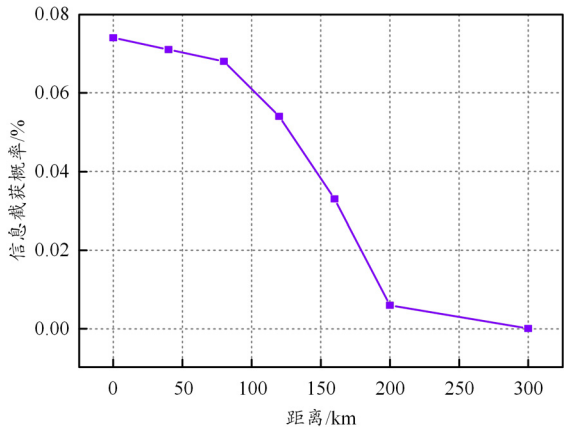

图 11 信息截获概率和距离的关系

值,因为靠猜测 0/1,也有 50%的正确率,所以减去 1/2 才是 Eve 真正截获得到信息的概率。

$$P=|BER-1/2| \quad (3)$$

Eve 模拟合法接收端截获 Alice 和 Bob 的传输数据,基错误率和距离的关系如图 10 所示,随着传输距离的增加,Eve 的基错误率越来越高, 距离为 300 km 时,已接近 100%。说明了 Eve 基本不可能获得状态基的信息,也就是密钥基是安全的。信息截获概率和距离的关系如图 11 所示,随着传输距离的增加,非合作方的信息截获概率不断降低,Eve 获取信息错误率增加。当传输距离为 300 km 时,非合作方 Eve 信息截获概率为 0.001%,很难获取正确的信息。

3 结束语

光纤通信发展迅速,但是光缆传输距离长、线路环境复杂, 现有光通信无法抵御线路或节点窃听攻击,一些不法分子利用微小的漏洞来窃取信息。本文提出的将 DFTs-OFDM 技术引入基于量子噪声流加密的 QAM 系统,避免了额外使用导频信号,提高了频谱利用率,更便于实施信道均衡;本文同时就安全传输性能进行了不同距离的实验分析。实验结果表明:在 300 km 时,*Q* 因子仍高于 9,纠错后 BER 为 0,验证了该实验系统良好的传输性能。同时,通过分析一个光纤窃听攻击的场景,测得 Eve 基错误率接近 100%,信息截获概率小于 0.001%,能够有效抵御非法节点窃听攻击。

参考文献:

[1] MA P Y, WU B, SHASTRI B J, et al. Steganographic communication via spread optical noise: A link-level eavesdropping resilient system [J]. Journal of Lightwave Technology, 2018, 36(23): 5344–5357.

[2] ZHANG Jie. Enhanced complexity of optical chaos in a laser diode with phase-conjugate feedback [J]. Optics letters, 2016, 41(20): 4637–4640.

[3] SUTIVONG A, NAGUIB A F, GORE D, et al. Separating pilot signatures in a frequency hopping OFDM system by selecting pilot symbols at least hop away from an edge of a hop region: USA Patent 7768979[P]. 2010–08–03.

[4] YOSHIDA M, HIROOKA T, KASAI K, et al. Single-channel 40-Gbit/s digital coherent QAM quantum noise stream cipher transmission over 480 km[J]. Optics Express, 2016, 24(1): 652–661.

[5] FUTAMI F, GRIPP J, TANIZAWA K, et al. Y-00 quantum stream cipher overlay in a coherent 256-Gbit/s polarization multiplexed 16-QAM WDM system [J]. Optics Express, 2017, 25(26): 33338–33349.

[6] FUTAMI F, HIROTA O. 40 Gbit/s (4×10 Gbit/s)Y-00 protocol for secure optical communication and its transmission over 120 km [C]// Optical Fiber Communication Conference and Exposition (OFC/NFOEC), March 4–8, 2012, Los Angeles, United States. New York: OSA, 2012: 1–3.

[7] NAIR R, YUEN H P, CORNDORF E, et al. Quantum-noise randomized ciphers[J]. Physical Review A, 2006, 74(5): 052309-1– 052309-14.

[8] CHEN X, LI A, GAO G, et al. Experimental demonstration of improved fiber nonlinearity tolerance for unique-word DFT-spread OFDM systems[J]. Optics Express, 2011, 19(27): 26198–26207.