引用本文：刘川，黄在朝，刘世栋，等. 基于 LDPC 码的相干光通信 QNSC 系统方案[J]. 光通信技术，2021，45(2)：24-27.

基于 LDPC 码的相干光通信 QNSC 系统方案

刘 川[1,2]，黄在朝[1,2]，刘世栋[1,2]，李俊佳[3]，雷 超[3]，张 杰[3*]

（1.全球能源互联网研究院有限公司，北京 102209；2.国家电网有限公司 电力通信网络技术实验室，北京 102209；
3.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：针对光网络物理层安全通信问题，提出了基于低密度奇偶校验（LDPC）码的相干通信量子噪声流加密（QNSC）系统方案，将码率为 9/10 的 LDPC 码和离散傅里叶变换正交频分复用（DFT-OFDM）技术应用在系统方案中，最后对该方案进行了实验验证。实验结果表明：经过传输跨距为 40 km、80 km、120 km 和 160 km 的标准单模光纤后，LDPC 码有效地降低了系统误码率，改善了系统通信的安全性，同时不会对系统的基本性能造成影响。

关键词：安全通信；量子噪声流加密；误码率；低密度奇偶校验；传输性能

中图分类号：TN929.11　**文献标志码**：A　**文章编号**：1002-5561(2021)02-0024-04

DOI：10.13921/j.cnki.issn1002-5561.2021.02.006　**开放科学（资源服务）标识码（OSID）**：

Coherent optical communication QNSC system scheme based on LDPC code

LIU Chuan[1,2], HUANG Zaichao[1,2], LIU Shidong[1,2], LI Junjia[3], LEI Chao[3], ZHANG Jie[3*]

(1. Global Energy Interconnection Research Institute co., Ltd., Beijing 102209, China; 2. Electric Power Communication Network Technology Laboratory, State Grid Corporation of China, Beijing 102209, China; 3. State Key Laboratory of Information Photonics and Optical Communication, Beijing University of Posts and Telecommunications, Beijing 100876, China)

Abstract: Aiming at the problem of secure communication in physical layer of optical network, a coherent communication quantum noise stream encryption (QNSC) system scheme based on low density parity check (LDPC) code is proposed. The LDPC code with a bit rate of 9/10 and discrete Fourier transform orthogonal frequency division multiplexing (DFT-OFDM) technology are applied in the system scheme. Finally, the scheme is verified by experiments. The experimental results show that after transmitting the standard single-mode fiber with the span of 40 km, 80 km, 120 km and 160 km, The LDPC code effectively reduces the bit error rate of the system, improves the communication security of the system, and does not affect the basic performance of the system.

Key words: secure communication; quantum noise stream encryption; bit error rate; low density parity check; transmission performance

0 引言

光网络物理层安全的关键在于保障数据在传输过程中不被截获，本质是利用外部协商所得的密钥对传输信号进行加密处理。其中，利用量子噪声流加密（QNSC）进行信息安全传输的方案成为主流研究方向之一，它采用了一种通过测量具有相干态的信号而被量子噪声随机化的流加密协议[1]。此加密方法对传输性能影响小，并且充分利用了模数/数模的量化空间，对噪声实现了最大限度的遮掩[2]。近年来，QNSC 系统被广泛地应用在强度调制（IM）[3]、相位调制（PM）[4]和正交幅度调制（QAM）[5-6]的光通信系统中以增强信息传输在物理层的安全性；同时，低密度奇偶校验（LDPC）码具有逼近香农极限的优良性能，而且其译码的复杂度相对较低，结构也相对灵活，能降低数据在长距离传输后的误码率。因此，出现了 LDPC 码和各种高阶调

收稿日期：2020-06-10。

基金项目：国家电网有限公司科技项目(5100-201940006A-0-0-00)资助。

作者简介：刘川（1986—），男，硕士，高级工程师，主要研究方向是电力主动性通信网络技术、软件定义网络技术、多业务接入与控制技术和通信安全技术等。曾获“重庆市科技进步二等奖”、“河南省科技进步三等奖”、“中国电力创新奖二等奖”、“中国通信学会科技进步三等奖”等省部级和地市级科技奖励共 9 项。

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

制相结合的光纤通信系统方案[7-9]。本文以 LDPC 码编码技术为基础，将离散傅里叶变换正交频分复用(DFT-OFDM)引入 QNSC 系统中，提出一种基于 LDPC 码的相干光通信 QNSC 系统方案。

1 LDPC 码编码技术与 Y-00 协议

1.1 LDPC 码编码技术

LDPC 码有长码和短码 2 种码长，其中长码为标准码，纠错性能相对更好，码长 n=64800 bit，共有 11 种码速率；短码的码长 n=16200 bit，共有 10 种码速率。因此，DVB-S2 标准中 LDPC 码可以满足不同通信特征系统的不同要求。LDPC 码的编码过程在其标准中可以看作是前面 k 个信息位，之后再加 $n-k$ 个由一定编码规则得到的校验位。

目前，主要有 2 种关于 LDPC 码的译码算法：一种是基于硬判决的译码算法，优点是在译码的过程中对于存储量的需求较低，可以节约运算所需要的大量内存，并且运算量较低，但其性能较差；另一种则是基于软判决的译码算法，其相对拥有更优的性能，因此得到了越来越广泛的研究。

1.2 Y-00 协议

QNSC 是近几年兴起的一种基于数学复杂度（短密钥扩展为长密钥的算法）和物理复杂度（量子测量坍缩原理）的加密技术，其本质为相干光量子效应的应用，安全性原理是通过固有的量子噪声来最大程度地掩蔽信号空间。QNSC 的主要协议是 Y-00 协议，该协议由 H.P.Yuen 教授于 2000 年提出[10]。基于 Y-00 协议的噪声加密安全光通信方案示意图如图 1 所示。

Y-00 协议的基本思路是在物理层使用 Y-00 协议，采用密集的 M-ary 键控（多级调制），通过把信号电平隐藏在量子噪声中，使窃听者无法正确识别电平。这种类型的密码提供了比数学密码更高的安全级别，且不需要额外的带宽。目前，典型的噪声加密方案及其特征如下：

◆基于相位调制的噪声加密方法。将信号映射到相位空间，可充分利用信号的相位空间状态，实现信号的相位空间隐藏，其特点是加密方法对传输性能影响小。

◆基于幅度调制的噪声加密方法。将信号映射到幅度空间，可充分利用信号的幅度空间状态，实现信号的幅度空间隐藏，其特点是充分利用模数/数模量化空间。

◆基于幅度/相位调制的噪声加密方法。将信号映射到幅度/相位空间，可充分利用信号的相位空间状态，实现信号的多维空间隐藏，其特点是实现大限度的噪声遮掩。

QNSC 本质是相干光量子效应的应用，其安全性原理是通过固有的量子噪声来最大程度地掩蔽信号空间。解密过程中，没有密钥的窃听者使用光电检测器对高阶信号进行测量时会不可避免地受到量子噪

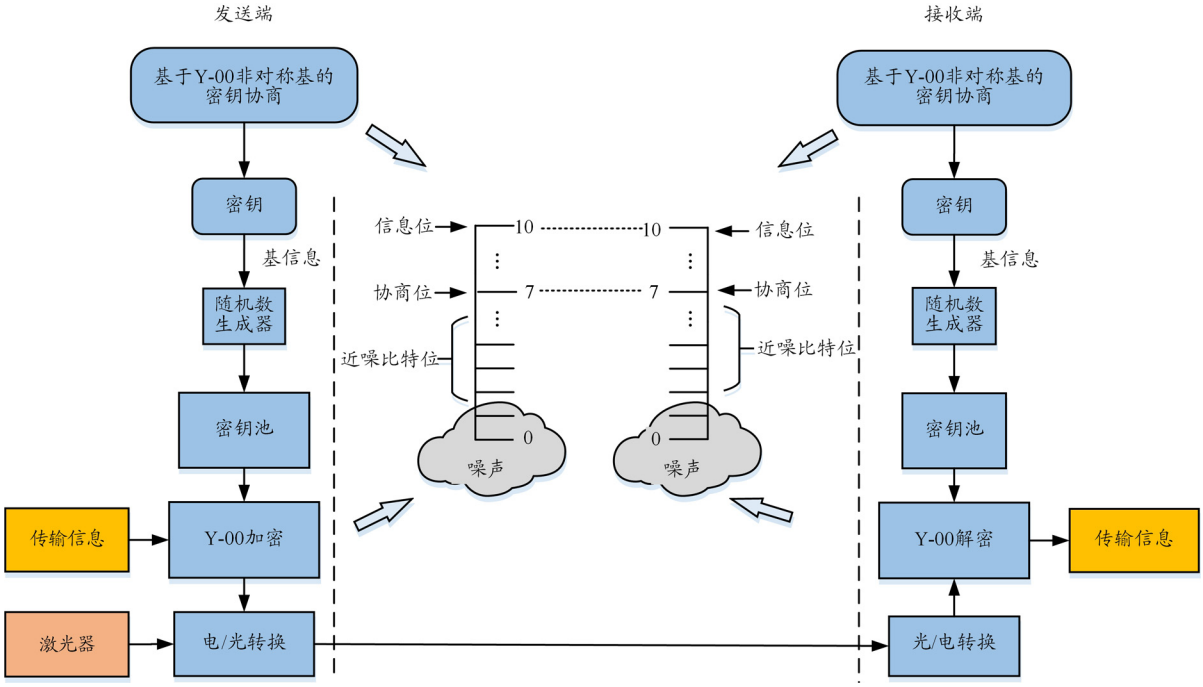

图 1 基于 Y-00 协议的噪声加密安全光通信方案示意图

声的影响，而合法的接收者可以在使用密钥解密后将密文检测变为低阶调制数据，进而选择合适的判决电平以恢复明文。

2 实验方案描述

基于 LDPC 码相干光通信 QNSC 系统方案框图如图 2 所示。在发送端，首先利用 LDPC 码将二进制伪随机序列数据进行编码，然后进行星座映射为 QAM 信号，插入导频，并进行串/并变换，随后进行离散傅里叶逆变换（IDFT）、并/串变换、插入前缀以及数/模变换。在接收端，进行与发送端相反的操作以恢复发送信息。首先进行模/数变换，去除前缀，然后进行串/并变换、离散傅里叶变换（DFT）、并/串变换和信道均衡，最后对信号进行星座解映射、信道 LDPC 码解码，恢复出原始信号。其中，DFT 采用 256 点，IDFT 采用 1024 点。此外，在 DFT 展开后，发送信号高频部分数据为全零，最大程度地消除信道带来的影响。

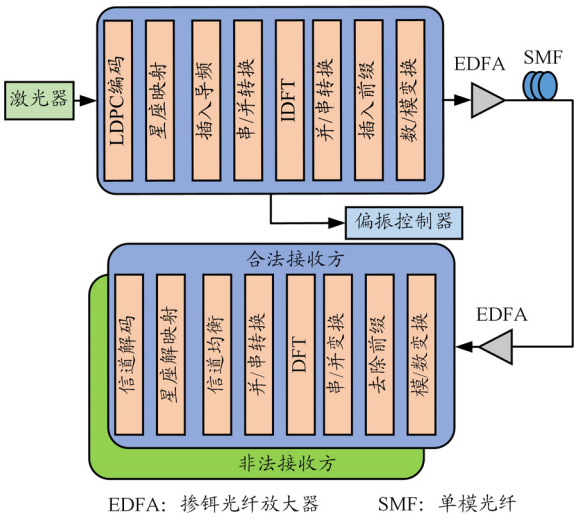

图 2 基于 LDPC 码相干光通信 QNSC 系统方案框图

3 实验结果分析

在光网络单元点到点传输情况下，接收端包括合法接收端和非法接收端，非法接收端的设置是为了评估系统的安全性。其中，任意信号发生器（AWG）设置发送速率为 10 Gb/s，激光器和本振光的波长设置为 1550.01 nm，发送端掺铒光纤放大器（EDFA）输出功率为 10 dBm，传输链路采用 SMF，验证距离分别为 40 km、80 km、120 km 和 160 km。接收端 EDFA 输出功率为 0 dBm，示波器采样速率为 40 GSa/s。发送端数字信号处理单元和接收端数字信号处理单元均采用 Matlab 离线数字信号处理（DSP）。其中，LDPC 码使用 9/10 码率，编码长为 64800 bit，IDFT/DFT 总大小为 1024，加密发送 1024×1024 QAM 信号。系统运行使用 Matlab 离线生成随机数作为发送数据、加密状态基。

为了验证 LDPC 码对于高阶 QAM 的 DFT-OFDM 的 QNSC 系统性能影响，本文实验性地分析了 LDPC 码结合 QNSC 与单纯的 QNSC 系统在不同传输距离情况下传输误码率对比情况，结果如图 3 所示。可以看出，LDPC 码（码率为 9/10）引入 QNSC 系统后，有效改善了 QNSC 系统的传输误码率特性。

另外，在考虑引入 LDPC 码改善高阶 QAM 的 DFT-OFDM+QNSC 系统误码性能的同时，还需要考虑 QNSC 系统的安全性是否受到影响。因此，本文对合法接收端与非法接收端在不同传输距离情况下误码率情况做了对比分析，结果如图 4 所示。可以看出，不同传输距离情况下，非法接收端的误码率一直保持在 0.5 左右，而合法接收端的误码率一直为 0。这表明 LDPC 码的引入对 QNSC 系统的安全性无影响。

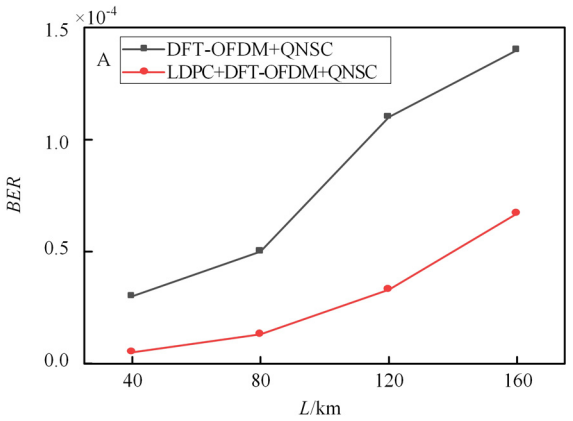

图 3 不同传输距离情况下传输误码率对比图

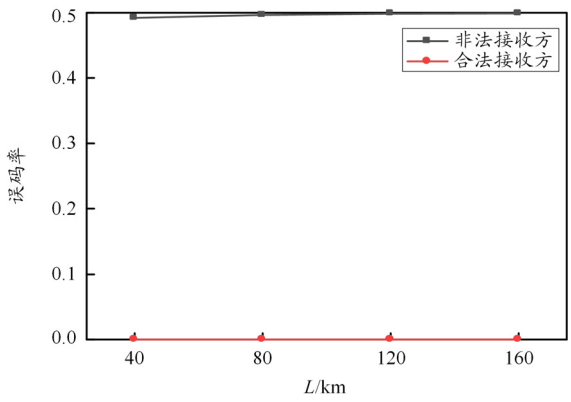

图 4 合法接收端与非法接收端在不同传输距离情况下误码率对比图

4 结束语

本文提出了一种将 LDPC 码应用于相干光通信

QNSC 系统中的方案，对高阶 QAM 信号进行 DFT-OFDM 后，分别在 40 km、80 km、120 km 和 160 km 的 SMF 进行了实验验证。实验结果表明：LDPC 码(9/10)引入 QNSC 系统后有效改善了 QNSC 系统的传输误码率特性，同时系统引入 LDPC 码不改变传输系统的安全性。

参考文献：

[1] HIROTA O. Practical security analysis of a quantum stream cipher by the Yuen 2000 protocol, 2007, 76(3): 103–105.

[2] YOSHIDA M, KAN T, KASAI K, et al. 10 Tbit/s QAM quantum noise stream cipher coherent transmission over 160 km [C]//2020 Optical Fiber Communication Conference (OFC), March 8–12, 2020, San Diego, USA. Piscataway: IEEE, 2020, T3D.2-1–T3D.2-8.

[3] TANIZAWA K, FUTAMI F. 2^{14} (=16384) Level intensity modulation at 10 Gbaud for Y-00 quantum stream cipher [C]//Conference on Lasers and Electro-Optics, May 13–18, 2018, San Jose, USA. San Jose: OSA. 2018. DOI: 10.1364/CLEO_AT.2018.JTu2A.57.

[4] TANIZAWA K, FUTAMI F. Single-channel 48-Gbit/s DP PSK Y-00 quantum stream cipher transmission over 400 km and 800 km SSMF, 2019, 27(25): 357–363.

[5] WANG Kai, ZHANG Jie, LI Yajie, et al. Multi-bit mapping based on constellation rotation in quantum noise stream cipher [J]. Optics Communications, 2019, 44(6): 147–155.

[6] 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.

[7] 赵太飞，屈瑶，许杉，等. 紫外光通信中副载波强度调制的低密度奇偶校验码研究[J]. 激光与光电子学进展，2018，55(12)：161–168.

[8] WANG L, WANG L, NI Y, CHEN X, et al. Design of Irregular QC-LDPC code based multi-level coded modulation scheme for high speed optical communication systems[J]. 中国通信，2019，6(5)：106–120.

[9] LEI Chao, ZHANG Jie, LI Yajie, et al. Long-haul and high-speed key distribution based on one-way non-dual arbitrary basis transformation in optical fiber link [C]//2020 Optical Fiber Communications Conference and Exhibition (OFC), March 8–12, 2020, San Diego, USA. Piscataway: IEEE, 2020: 1–3.

[10] YANG Xiaokun, ZHANG Jie, LI Yajie, et al. Single-carrier QAM/QNSC and PSK/QNSC transmission systems with bit-resolution limited DACs[J]. Optics Communications, 2019, 44 (5): 29–35.

[11] 何文雪，张文博，李超，等. 高速相干光通信系统中水印辅助的低密度奇偶校验方案[J]. 光电子·激光，2015，26(6)：1100–1105.

[12] YUEN H P. KCQ: a new approach to quantum cryptography I. General principles and key generation[J]. Physics, 2003, 12(3): 12–15.