引用本文：陈毓锴，蒲涛，李云坤，等. 量子噪声随机加密技术研究[J]. 光通信技术，2022，46(6)：61-66.

量子噪声随机加密技术研究

陈毓锴[1,2]，蒲 涛[2*]，李云坤[2,3]，赵 勇[1]，林克凌[1]，杨 明[1]，徐逸帆[1,2]，李 晋[2]

（1. 中国人民解放军 61623 部队，北京 100840；
2.中国人民解放军陆军工程大学 通信工程学院，南京 210007； 3. 中国人民解放军 31106 部队，南京 210016）

摘要：针对光网络安全防护问题，从物理层安全性评估、实验验证 2 个层面深入研究量子噪声随机加密（QNRC）物理层抗截获传输技术。首先，介绍了国内外 QNRC 的发展现状，凝练了一套物理层安全性评估通用方法。然后，提出一种基于光域解密的强度移位键控－量子噪声随机加密（ISK-QNRC）实验方案，针对该方案中高分辨率、高采样速率的数／模转换器制造工艺问题，提出一种并联 ISK-QNRC 方案并进行了验证，结果表明该方案信息传输安全、有效。最后，分析了 QNRC 技术的典型应用场景及发展趋势。

关键词：光网络安全防护；量子噪声随机加密；安全性评估方法；并联强度调制；应用场景

中图分类号：TN918　**文献标志码**：A　**文章编号**：1002-5561(2022)06-0061-06

DOI：10.13921/j.cnki.issn1002-5561.2022.06.012　**开放科学（资源服务）标识码（OSID）**：

Research on quantum-noise random cipher technology

CHEN Yukai[1,2], PU Tao[2*], LI Yunkun[2,3], ZHAO Yong[1], LIN Keling[1], YANG Ming[1], XU Yifan[1,2], LI Jin[2]

（1. Troop 61623 of PLA, Beijing 100840, China; 2. Communications Engineering College,
Army Engineering University of PLA, Nanjing 210007, China; 3. Troop 31106 of PLA, Nanjing 210016, China）

Abstract: Aiming at the problem of optical network security protection, the anti-interception transmission technology of quantum noise random encryption （QNRC） physical layer is deeply studied from two aspects of physical layer security evaluation and experimental verification. Firstly, the development status of QNRC at home and abroad is introduced, and a set of general methods for physical layer security evaluation is summarized. Then, An experimental scheme of intensity shift keying quantum noise random encryption （ISK-QNRC) based on optical domain decryption is proposed. Aiming at the manufacturing process problems of high resolution and high sampling rate digital to analog converters in the scheme, a parallel ISK-QNRC scheme is proposed and verified. The results show that the scheme is safe and effective in information transmission. Finally, the typical application scenarios and development trends of QNRC technology are analyzed.

Key words: optical network security protection, quantum-noise random cipher, security assessment method, parallel intensity modulation, application scenarios

0 引言

近年来，随着物联网、大数据和云计算等技术的兴起，信息安全形势日益复杂。经“十二五”、“十三五”光缆建设，我国已建成纵横全国、连通全球的光传输网。光传输网作为全局性、支撑性和基础性网络，拥有海量信道资源，承载着大量业务，其安全直接关系到国防、政务和金融的安全，在国家“网络强国”的战略背景下，如何提高光传输网及其承载的互联信息安全至关重要且亟待解决。随着各类光纤信道窃听手段的不断成熟，光传输网面临着巨大的信息安全挑战，因此光通信物理层抗截获技术应运而生。目前，主流的光通信物理层抗截获技术有量子噪声随机加密（QNRC）[1]、量子保密通信[2]、混沌光通信[3]、光码分多址[4]和光隐匿通信[5]等，其中，QNRC 技术凭借其在安全性、传输速率及与现有光传输网的兼容性等方面的优势，

收稿日期：2022-01-17。

基金项目：国家自然科学基金项目(62071487、61901480、61974165)资助。

作者简介：陈毓锴(1996—)，男，福建漳州人，硕士，助理工程师，硕士期间对 QNRC 理论安全性及传输技术进行了系列研究，熟悉光物理层安全、大数据挖掘和人工智能等方面的技术，主要研究方向为光纤传输与网络安全。

*** 通信作者**：蒲涛(1974—)，男，博士，教授，博士生导师，主要研究方向为光物理层安全、微波光子学、光传感技术等。

在许多抗截获技术中脱颖而出，具有广阔的应用场景。QNRC 技术是一种结合了经典流密码思想和量子力学原理的光物理层信息抗截获传输技术，在调制过程中借助量子噪声随机对信号的幅度或相位进行加密，保证了光纤信道的不可破译性。

本文在研究 QNRC 技术的基础上，凝练一套物理层安全性评估通用方法，并以评估结果作为系统实验参数配置的依据，对 QNRC 系统性能进行研究。

1 国内外发展现状

QNRC 最早是在美国空军研究项目支持下，由美国西北大学提出的一种安全传输方案，QNRC 以其优越的性能表现受到国内外学者的广泛关注。日本的玉川大学和东北大学凭借其国内良好的芯片制造工艺，取得了目前最好的 QNRC 传输性能：当传输速率分别为 40 Gb/s、10 Tb/s 时，传输距离分别为 800 km、160 km[6-7]。同时，玉川大学的 IWAKOSHI T[8]用量子多重假设方法检验 QNRC 在无限已知明文攻击下的猜测概率，为 QNRC 的安全性评估提供了一种新的思路。

近年来，国内北京邮电大学、陆军工程大学和华中科技大学在 QNRC 理论和实验两方面均取得了长足的进展。理论方面，2017 年，陆军工程大学焦海松等人[9]首次对 QNRC 系统中数据安全性和密钥安全性进行分析，提出以保密容量为评价指标来评估 QNRC 的安全性能，对后续 QNRC 的安全性评估具有指导意义。实验方面，北京邮电大学张杰教授团队[10]首次将基于离散傅里叶变换扩展的正交频分复用（DFTs-OFDM）系统与 QNRC 系统结合起来，兼顾了 DFTs-OFDM 系统优异的传输性能和 QNRC 系统的高安全性，最终实现了距离为 200 km、速率为 10 Gb/s 的无中继、无误码传输。华中科技大学 YU Q 等人[11]采用双驱动马赫-曾德尔调制器进行了单边带调制，消除色散引起的功率衰落，并提出了一种基于递推最小二乘法正则化稀疏算法，平衡了算法复杂度、传输性能和安全性能，最终实现了速率为 100 Gb/s、距离为 100 km 的数据安全传输。但相比于国外，国内仍需建立相对完善的物理层安全评价体系，亟需提高芯片的技术水平，改善设计方式。

2 物理层安全性评估通用方法

目前，关于 QNRC 系统的安全性评价指标主要有唯一解距离、量子噪声掩盖的量子状态数和窃听者检测失败概率等。YUEN H P 团队[12]利用密码学理论中的唯一解距离（窃听者进行密钥唯一确定所需要的最小的密文长度）作为评判 QNRC 系统安全性的标准，当密文长度超过唯一解距离，密码系统可破。唯一解距离与密码系统的安全性呈正相关。OHHATA K 小组[13]利用量子噪声掩盖的量子状态数对 QNRC 加密系统进行定量评估，发现即使窃听者使用量子外差接收机，QNRC 系统也可以提供很好的噪声掩盖效应。YOSHIDA M 等人[14]使用窃听者检测失败概率来评估系统安全性，窃听者检测失败概率越高，系统安全性越强。上述安全性指标主要是从窃听者的角度对 QNRC 系统安全性进行评估。而 Y-00 协议是 QNRC 的基本协议，该协议保证了 QNRC 系统中合法通信双方相对窃听者的信道优势。基于此信道优势，可构建 Wyner 窃听信道模型，从信息论的角度来评估 QNRC 系统的安全性。针对不同调制格式的 QNRC 系统，本文基于窃听信道模型，凝练了一套物理层安全性评估通用方法，具体操作如下：

①构建窃听信道模型。在窃听信道模型中，保密容量作为物理层安全性评价指标，预设了系统安全传输速率的上限。当合法信道拥有相对于窃听信道的信道优势且传输速率小于系统安全传输速率时，通过合理设计编解码方案，可实现安全、可靠的通信。由于 QNRC 系统中传输的信号同时承载着密钥及数据信息，在系统物理层安全性评估过程中可分别构建密钥和数据的窃听信道模型，分析密钥及数据的安全性，并根据密钥和数据传输速率的相关性，同时考虑二者的安全限制，进而分析整个系统的安全性。

②计算密文符号转移概率。QNRC 系统常见的调制方式有相位调制、强度调制和正交振幅调制 3 种类型，三者的加密机制及信号结构均不同。在不同调制格式的 QNRC 系统中，要得到安全性指标保密容量或安全速率，首先应根据加密机制及信号结构确定窃听者及合法接收者的判决区域，结合量子外差接收机的条件概率密度函数，求得窃听者及合法接收者的密文符号转移概率。

③获取保密容量。根据构建的密钥窃听信道模型，基于窃听者的密文符号转移概率，可计算密钥转移概率，进而由合法用户及窃听者获取密钥的互信息量差得到密钥保密容量。

④获得系统最大可达安全速率。考虑密钥和数据的保密容量对 QNRC 系统的安全性限制后，得出 QNRC 系统能够达到的最大安全速率。在该速率下，从互信息评价角度来看，数据及密钥均是安全的。

3 实验验证

在对 QNRC 系统物理层安全性定量评估后，可将其评估结果作为系统实验参数配置的依据。本文提出了基于光域解密的强度移位键控-量子噪声随机加密（ISK-QNRC）实验方案和并联 ISK-QNRC 实验方案，直接在光域对 QNRC 系统进行性能研究。

3.1 基于光域解密的 ISK-QNRC 实验

图 1 为基于光域解密的 ISK-QNRC 实验结构图，该结构对电路实现部分做了最大的简化。分布式反馈激光器（DFB）产生的载波信号经过强度调制后，生成对应的密文光信号。任意波形发生器（AWG）可将密文符号转换为对应的多进制信号，并将其作为马赫-曾德尔强度调制器（MZM）的调制信号。为了保证量子噪声掩盖相邻的量子态，密文信号功率被可调光衰减器（VOA_1）衰减至介观态水平，并采用光功率计进行功率监测。传输信道主要由 100.8 km 的标准单模光纤（SSMF）、相应的色散补偿光纤（DCF）和掺铒光纤放大器（EDFA）组成。AWG 另一通道将收发双方共享的运行密钥流转换为多进制信号，作为接收端的调制信号。本振采用可调谐激光器（TLD），产生的光信号经强度调制后，可作为密文的解密信号。该解密信号与密文信号必须功率匹配、时延匹配，在实验中分别采用 VOA_3、可调光延时线（OTDL）进行调节。随后，解密信号及密文信号经平衡探测器（BPD）进行光电检测、平衡相减，再经时钟数据恢复（CDR）后，由误码仪测量系统误码率，实时示波器测量眼图。

图 2 为传输 100.8 km 后 ISK-QNRC 密文信号及解密信号的测试眼图。图 2(a)、图 2(c)分别为调制进制数 M=1024 和 M=4 情况下 Y-00 密文信号的测试眼图，可以看出，Y-00 密文信号的眼图未张开，这直观地表明了 ISK-QNRC 系统的安全性；此外，M=1024 时的眼图比 M=4 时的眼图更为混淆，其原因为密文信号为密集多进制调制信号，且信号掩盖在噪声中，进制数越大，噪声的防护效应越强，系统的安全性能随之增加。图 2(b)、图 2(d)为 M=1024 和 M=4 情况下解密信号的测试眼图，二者的眼图均清晰可见。这表明合法接收方可以将噪声掩盖下的多进制密文信号检测为二进制信息，进而恢复出数据。此外，相比较而言，当 M=4 时的解密信号更为清晰，这表明随着进制数的增加，系统的传输性能随之劣化，但仍在通信可接受范围内。

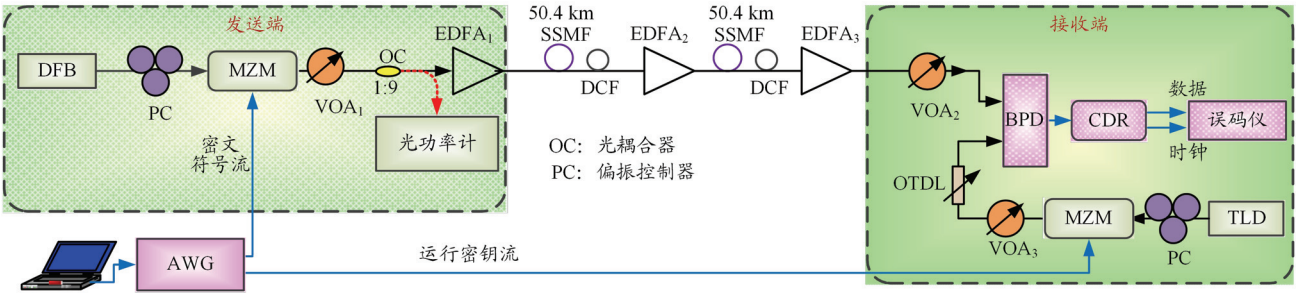
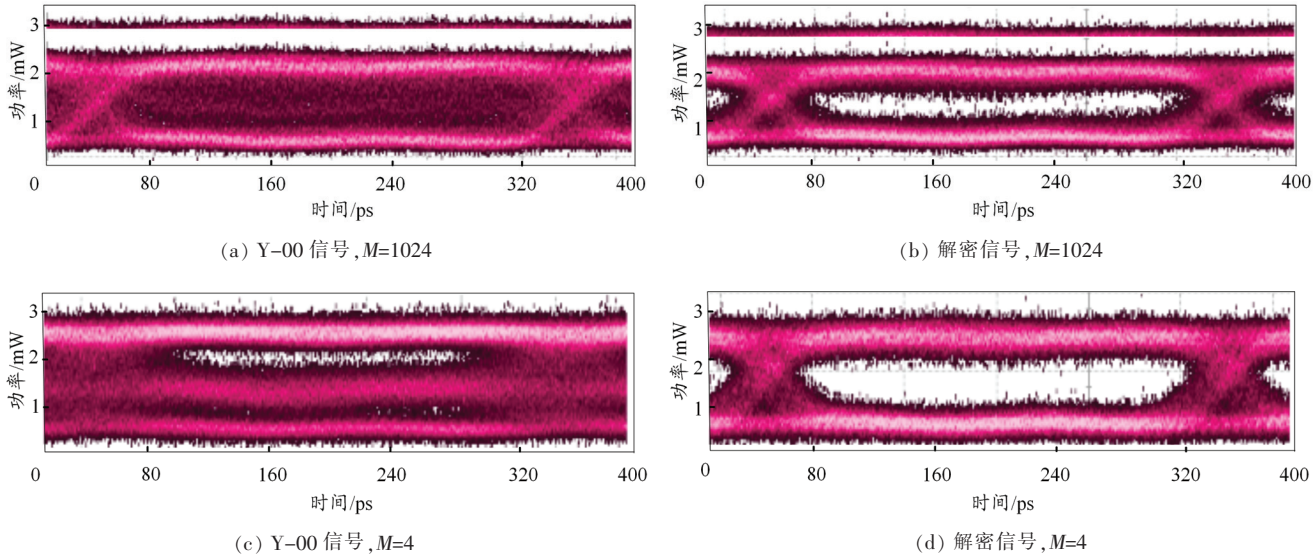


图 1 基于光域解密的 ISK-QNRC 实验结构图



(a) Y-00 信号，M=1024　　(b) 解密信号，M=1024

(c) Y-00 信号，M=4　　(d) 解密信号，M=4

图 2 ISK-QNRC 100.8 km 传输测试眼图

因此,QNRC 技术可以很好地兼顾通信过程中高速、长距离传输和高安全性的优点。

3.2 并联 ISK-QNRC 实验

QNRC 采用高阶多进制调制加密方案,发射机、接收机中均需制备密集多进制的信号,且该信号进制数与系统的安全性密切相关。在高速光纤传输系统中,研制多进制调制的发射机、接收机依赖于高分辨率、高采样速率的数/模转换器(DAC)。DAC 是 QNRC 发射机/接收机的关键部件,制约着 QNRC 的进一步发展应用。短期内要开发高性能的 DAC 芯片难度较大,急需找到新的方法来避开 DAC 制造工艺的限制问题[15]。针对基于光域解密的 ISK-QNRC 实验方案中高速率、高分辨率 DAC 限制问题,本文提出了一种并联 ISK-QNRC 解决方案,用以提高密集多进制信号的进制数水平,并采用 VPItransmission Maker Optical System 仿真软件进行可行性验证,搭建的仿真系统框图如图 3 所示。

在发送端,运行密钥流与传输数据加密映射为密文,AWG 分别将密文的前 l 比特及后 n 比特转化为对应的多进制信号,用以调制 MZM_1 和 MZM_2,并生成 2 路光路信号。接着,利用 VOA_1 将第二路光信号衰减至原功率水平的 $1/2^l$,并与第一路光信号进行耦合。MZM_1、MZM_2 采用相同的设备型号,在二进制信号电压驱动情况下,最大功率与最小功率的功率差为 ΔP,其中 MZM_1 与 MZM_2 的功率差分别为

$$\begin{aligned}\Delta P_{AM1}&=\Delta P(1-1/2^l)\\ \Delta P_{AM2}&=\Delta P(1-1/2^n)\end{aligned}\tag{1}$$

而耦合后的 2 路光信号的功率差为

$$\Delta P_{AM}=\frac{\Delta P}{2}(1-1/2^{l+n})\tag{2}$$

由式(2)可知,利用 2 路信号分别调制 MZM_1、MZM_2,并将调制后的光路信号进行精准调节,则耦合后的光信号可实现调制水平的叠加,进而实现更高进制的调制。

传输信道基本模块主要由 100.8 km 的 SSMF、相应的 DCF 和中继 EDFA 组成。

在接收端,AWG 分别将密钥的前 l 比特及后 $(n-1)$ 比特转化为多进制信号,并加载至 MZM_3、MZM_4 上。同样地,将第二路光信号功率衰减至原先的 $1/2^l$,并将 2 路光信号进行耦合,经 BPD 进行光电检测,并与携载着密文信息的传输信号进行一一比对相减,得到对应的二进制信号。对该二进制信号进行时钟数据恢复,并观察眼图与波形图。上述方案本质上是将 2 个低分辨率的 DAC 结合在一起,提供更高的分辨率,具有结构简单、易于实现和对高速电路需求少等优点。

并联 ISK-QNRC 系统信号解密前后眼图如图 4 所示。可以看出,经并联强度调制后,传输的密文信号为多进制信号,并且掩盖于噪声中,窃听者得到的只能是混淆的眼图,无法准确获得密文信息,更加难以从密文信息中恢复出数据信息。而合法接收方由于已知密钥,只需判决低阶明文信息,因此经长距离传输后,得到的解密信号眼图仍然清晰可辨,可以得到准确的明文信息。上述结果表明了并联 ISK-QNRC 方案中信息传输的安全性及有效性。

4 典型应用场景及发展趋势

4.1 典型应用场景

目前,日本日立信息通信工程有限公司[16]使用 QNRC 设备沿着东京站至池袋站商业线路进行了距离为 192 km、速率为 2.5 Gb/s 的数据保密传输;日本量子信息技术研究所[17]在对 QNRC 设备测试过程中,不仅对千兆以太网业务进行加密防护,而且实现了信道路由的动态路径变化和数据的远程备份。

随着技术研究的不断深入,QNRC 设备将广泛应用于数据中心联网、视频安防监控、安全多点访问、高清电视电话会议和无线激光通信等领域。其中,典型应用场景为:在互为主备的 2 个数据中心进行数据倒

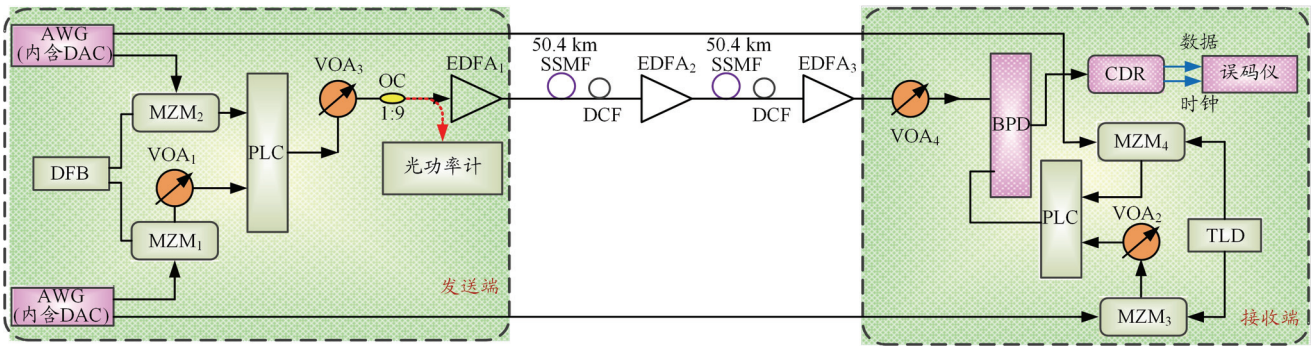
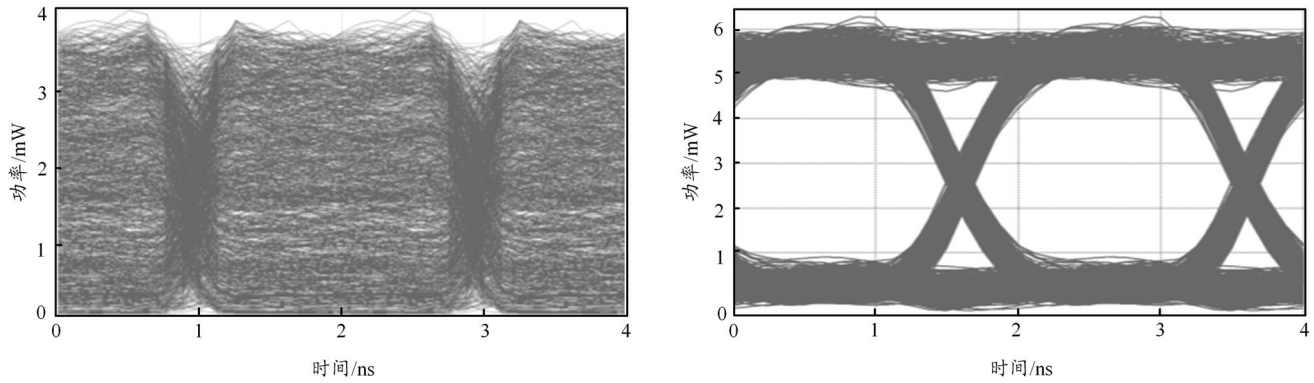


图 3 并联 ISK-QNRC 系统仿真框图



(a) 密文信号眼图　　(b) 解密信号眼图

图 4　并联 ISK-QNRC 系统信号解密前后眼图

换时(如图 5 所示),对服务器的数据进行线路侧加密保护;在金融干线、专线的线路侧两端传输站对大颗粒业务进行加密传输;将 QNRC 设备做成单独的模块,集成于无线激光器中,可应用于空空对话、空地对话等场景。

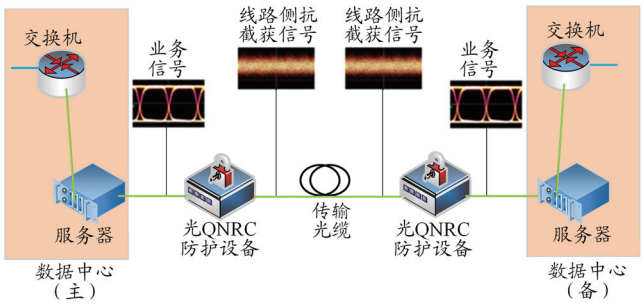


图 5　数据中心联网应用场景

4.2 发展趋势

QNRC 技术虽可与现有光网络兼容,但距离大规模应用还有一定距离。在应用需求上,我国目前三大运营商的公网或专网传输层使用的设备大多为分组传送网(PTN)设备或者光传送网(OTN)设备。QNRC 安全防护设备在实际应用测试中,应测试是否可以对 OTN 系统信号进行全方位业务防护。同时,应重点关注在实际复杂环境中,QNRC 安全防护设备的极限安全传输距离及其与 OTN 设备相连光接口的接口速率、光功率等指标。针对不同应用场景,应考虑成本及工艺限制,研制不同类型的防护设备,如跨省骨干网可研制高速率、长距离的安全传输设备,本地接入网则研制成本较低、灵活性强的安全接入设备。

为满足 QNRC 技术的应用需求,必须不断优化其安全和传输性能。对于安全性能,Y-00 协议在噪声掩盖效应不够强时,面临被窃听者快速相关攻击的威胁,存在安全漏洞。一方面,可对 Y-00 协议进行改进,引进混沌映射和神经网络等技术,使该协议只能正向映射,无法逆向映射,进一步增强协议的安全性。另一方面,在整个通信过程中,可寻找更多、更强的可用噪声,进一步增强噪声掩盖效应。对于传输性能,在接收端可利用数字相干技术来提高频谱利用率和补偿色散传输损伤,进一步增强传输性能。

5 结束语

光传输网是我国信息化基础设施的重要组成部分,光缆链路布设在公共环境中,很容易受到安全威胁,光网络安全防护问题亟待解决,迫切需要使用以 QNRC 为代表的光物理层抗截获传输技术。本文凝练了一套物理层安全性评估通用方法,提出了一种新的 ISK-QNRC 实验结构和并联 ISK-QNRC 方案,实验验证了 ISK-QNRC 系统信息传输的安全性。

参考文献:

[1] 陈毓锴,蒲涛,郑吉林,等. 相位调制量子噪声随机加密系统的仿真验证[J]. 光学学报, 2020,40(16):24-29.

[2] PATEL K A, DYNES J F, MARINI M, et al. Quantum key distribution for 10 Gb/s dense wavelength division multiplexing networks [J]. Applied Physics Letters, 2014, 104(5): 175-179.

[3] 义理林, 柯俊翔. 混沌保密光通信研究进展 [J]. 通信学报,2020,41(3):168-181.

[4] WANG X, GAO Z, WANG X, et al. Bit-by-bit optical code scrambling technique for secure optical communication [J]. Optical Express, 2011, 19(4): 3503-3512.

[5] ZHU H, WANG R, PU T, et al. Experimental demonstration of optical stealth transmission over wavelength-division multiplexing network[J]. Applied Optics, 2016, 55(23): 6394-6398.

[6] TANIZAWA K, FUTAMI F. Single-channel 48-Gbit/s DP PSK Y-00 quantum stream cipher transmission over 400-km and 800-km SSMF [J].

Optics express, 2019, 27(18): 25357–25363.
[7] YOSHIDA M, KAN T, KASAI K, et al. 10 Tbit/s QAM quantum noise stream cipher coherent transmission over 160 km [J]. Journal of Lightwave Technology, 2020, 39(4): 1056–1063.
[8] IWAKOSHI T. Guessing probability under unlimited known-plaintext attack on secret keys for Y00 quantum stream cipher by quantum multiple hypotheses testing [J]. Optical engineering, 2018, 57 (12): 126103-1 – 126103-7.
[9] JIAO H, PU T, ZHENG J, et al. Physical-layer security analysis of a quantum-noise randomized cipher based on the wire-tap channel model[J]. Optics Express, 2017, 25(10): 10947–10960.
[10] YANG X, ZHANG J, LI Y, et al. DFTs-OFDM based quantum noise stream cipher system [J]. Optical Fiber Technology, 2019, 52 (11): 101939-1–101939-7.
[11] YU Q, WANG Y, LI D, et al. Secure 100 Gb/s IMDD transmission over 100 km SSMF enabled by quantum noise stream cipher and sparse RLS-volterra equalizer[J]. IEEE Access, 2020, 8: 63585–63594.
[12] NAIR R, YUEN H P. Comment on: Exposed-key weakness of $\alpha\eta$[J]. Physics Letters A, 2008, 372(47): 7091–7096.
[13] OHHATA K, HIROTA O, HONDA M, et al. 10-Gb/s optical transceiver using the Yuen 2000 encryption protocol [J]. Journal of lightwave technology, 2010, 28(18): 2714–2723.
[14] 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.
[15] TANIZAWA K, FUTAMI F. Digital coherent PSK Y-00 quantum stream cipher with 2^{17} randomized phase levels[J]. Optics Express, 2019, 27 (2): 1071–1079.
[16] AKUTSU S, DOI Y, HOSOI T, et al. 192 km relay transmission and HDTV transmission experiments by quantum Yuen-2000 transceiver [C] //American Institute of Physics. Proceedings of American Institute of Physics, Quantum Communication, Measurement and Computing&The Ninth International Conference. New York: American Institute of Physics, 2009: 331–334.
[17] FUTAMI F, KUROSU T, TANIZAWA K, et al. Dynamic routing of Y-00 quantum stream cipher in field-deployed dynamic optical path network [C]//Optical Fiber Communication Conference 2018 (OFC2018), March 3–7, 2018, Santiago, America. New York: Optical Society of America, 2018: Tu2G. 5-1–Tu2G. 5-7.