第 48 卷 第 17 期/2021 年 9 月/中国激光 研究论文

中国激光

基于并联强度调制的量子噪声随机加密实现方案研究

李云坤**，蒲涛，郑吉林*，谭业腾，陈毓锴

陆军工程大学通信工程学院，江苏 南京 210001

摘要 为解决高速、高分辨率数模转换器(DAC)给量子噪声随机加密(QNRC)研究带来的限制问题，提出一种采用并联强度调制、光域解密、直接检测的方案，利用 VPI 系统对此进行验证与分析讨论，并实现了介观态功率为 −20 dBm、传输距离为 500 km、传输速率为 10 Gbit/s、密文态数目为 $2^{10}-1$ 的 ISK-QNRC 系统。研究结果表明，通过调制器并联的方式，可以有效增大 QNRC 密文态数目。该方案的误码性能对于接收功率以及密文信号与解密信号的功率差比较敏感，在固定接收功率的情况下，做好密文信号与解密信号的功率匹配对于降低误码率十分重要。

关键词 光通信；量子噪声随机加密；强度调制；调制器并联

中图分类号 TN918.1 **文献标志码** A **doi**：10.3788/CJL202148.1706002

1 引 言

光纤通信作为当前承载主要数据传输业务的骨干网络，其传输速率和误码率(BER)两大通信性能指标在近几十年得到了巨大的提升，但随着商业竞争和国防信息领域的斗争加剧，以及各类光纤通信窃听手段逐渐暴露在人们的视野，光纤通信的安全性成为与以传输速率为主要指标的有效性、以误码率为主要指标的可靠性同等重要的第三项指标。自 1975 年 Wyner[1] 提出“Wyner 窃听信道(WTC)模型”之后，人们利用物理层安全加密方法，依靠某种物理现象实现了合法接收方对非法窃听方的信道优势，该方法优于以往依靠数据复杂度的加密方法。比较典型的物理层安全加密方法有光隐藏通信(OSC)[2-3]，OSC 通过密钥将信号隐藏在宿主信道中，能够确保只有拥有密钥的合法接收方才可完整地恢复出加密信号，而窃听者则无法察觉出宿主信道的加密信号。但该技术一方面传输速度受限，另一方面与现有的商用网络设备兼容性一般，因此在大容量、长距离光通信应用要求下，还需要寻求更优解。

量子噪声随机加密(QNRC)[4-6] 是一种基于量子不可克隆原理和海森堡不确定性，利用介观态量子效应掩盖相邻密文态实现加密的物理层安全技术。QNRC 本质上是利用密钥流对光信号进行伪多进制调制，合法接收方可以使用密钥将原信号解调为二进制信号，而窃听方只能对多进制信号进行判决。对处于介观态的光信号而言，量子噪声会掩盖相邻的多进制符号，导致窃听方在判决时产生相对合法接收方更高的疑义度和误码率。QNRC 兼具高的安全性和传输速率，且能够与现有的商用网络技术和设备兼容[7]，具有较广的应用前景。日本玉川大学凭借其尖端的电子制造工艺，在 QNRC 的研究上取得了较快的进展[8-9]；近几年国内部分高校也陆续开展了相关研究，理论方面在安全性评估上给出了定量分析[10-12]，实验方面实现了 100 Gbit/s 的强度调制方案[13]。作为衡量该技术安全性的重要指标，噪声掩盖态数目(NMS)有赖于两大基本参数，即噪声强度以及密文态数目。无限制地提升噪声强度将会降低接收到的光信噪比(OSNR)，在噪声一定的情况下，密文态数目成为限制 NMS 的重要指标。按照常规的实现方案，提升密文态数目需要有高速率、高分辨率的数模转换器(DAC)。受限于工艺水平和成本控制，没有相关研究基础的团队获得高速率、高分辨率的 DAC 难度较大，为绕开高速率、高分辨率的 DAC 限制，寻求某种设备或者器件、结构来帮助提供伪多进制调制的信号源是一种

收稿日期：2020-12-28；**修回日期**：2021-02-15；**录用日期**：2021-03-09

基金项目：国家自然科学基金(61974165，61901480)

通信作者：*zhengjilinjs@126.com；**dxEnglish201@163.com

重要且有效的研究方案[14]。

本文基于并联强度调制(ISK)的方案实现了密文态数目为 $2^{10}-1$ 的 ISK-QNRC,利用仿真软件对此进行了验证和讨论分析。该方案采用一个 4 bit 任意波形发生器(AWG)信号源和一个 6 bit AWG 信号源,以“粗调+精调”的方式调制信息,调整功率后使其进入光耦合器实现 $2^{10}-1$ 并联强度调制,具有结构简单、易于实现、密文态数目较高的特点。首先,结合介观态量子效应阐述了 Y-00 协议对 ISK-QNRC 的加密原理;然后,利用商业仿真软件 VPItransmission Maker Optical System (VPI)对本文提出的并联强度调制方案进行了可行性验证;最后,在仿真验证的基础之上对结果进行分析讨论,研究了传输距离、介观态功率、接收功率等物理参数对于传输性能的影响。

2 基本原理

2.1 ISK Y-00 协议加密原理

如图 1 所示,合法的收发双方(Alice 和 Bob)预先在已知绝对安全的信道上共享长度为 S 比特的二进制种子密钥 K^S,再经过相同结构和设置的密钥扩展模块(ENC)将种子密钥扩展为运行密钥序列 U^N,然后将 N 比特的运行密钥序列均匀地划分为长度为 l 的二进制运行子密钥序列 u_i,用于选择编解码基态,即 $U^N=\mathrm{ENC}(K^S)=\{u_1,u_2,\cdots,u_n\}$,此时将有 $M_b=2^l-1$ 种基态可选。在发送方,Alice 利用运行子密钥对需要传输的数据进行逐比特加密,具体的加密公式为[15]

$$m=f(x,u)=u+[x\oplus \mathrm{Pol}(u)]\cdot 2^{|u|},\tag{1}$$

式中,m 表示加密后的密文,x 表示明文,函数 $\mathrm{Pol}(\cdot)$ 表示取运行子密钥的奇偶性,$|u|$ 表示运行子密钥的长度,$\oplus$ 表示异或运算,u 为运行子密钥。由于运行子密钥为二进制序列,奇偶性取决于最低位比特,经加密后的密文长度为 $l+1$,其最高位比特可以看作为明文和运行子密钥最低位比特的异或,由此可以推知密文态具有 $M=2^{l+1}-1$ 种可能性。

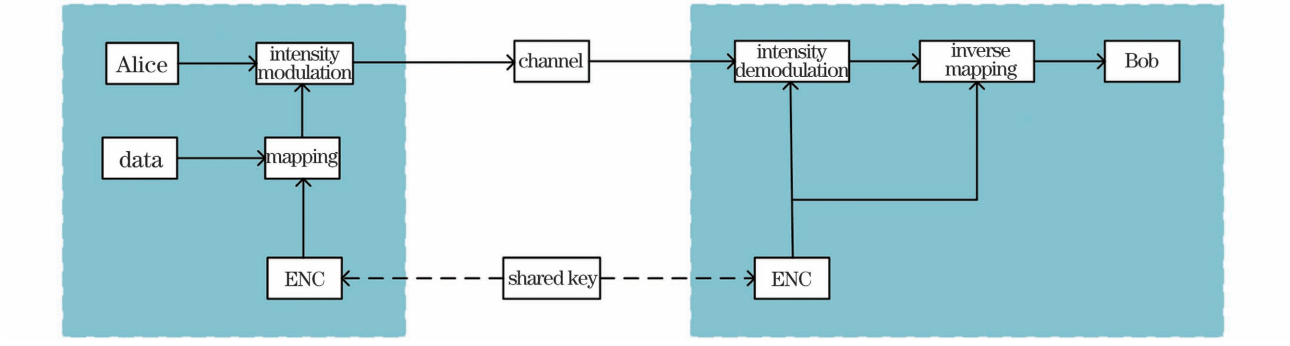

图 1 ISK Y-00 协议加密流程框图

Fig. 1 Diagram of ISK Y-00 protocol encryption process

对处于介观态的 ISK-QNRC 密文而言,其可以表示为

$$|\alpha(m)\rangle=\left|\sqrt{m}\,\frac{\alpha_M}{\sqrt{M}}\exp(\mathrm{i}\theta)\right\rangle,m=1,2,\cdots,M,\tag{2}$$

其中,α_M 是信号光最大时的幅度,θ 是未调制的相位。如图 2 所示[16],量子噪声的存在使得非法与合法的接收方在检测的时候都将受到量子态 $|\psi(x,u)\rangle=|\psi(m)\rangle$ 不确定性的影响。对合法接收方 Bob 而言,其拥有的运行子密钥可以将多进制的密文态转化为二进制纯态,即只需要判定 $\{|\psi(0,u)\rangle,|\psi(1,u)\rangle\}$ 就能正确获得明文信息;但是对于非法窃听方 Eve 而言,由于没有运行子密钥对接收信号进行解密,不得不在量子噪声的范围内对可能存在的密文态进行猜测,从而产生对明文信息的疑义度。

结合上述加密公式和编码规则,详细的明文密文之间的映射关系如图 3 所示,一个运行子密钥代表一组密文态“m”和“$m+M_b$”,这一组密文态分别代表不同的“0”或者“1”,相邻的密文态所对应的明文信息是交错排列的,即“m”代表“0”,那么“$m+1$”代表“1”。图 3 中 P_i 代表密文态的光信号强度,从第一个密文态到最后一个密文态对应的信号强度是从小到大等间隔排列的,即归一化后第一个密文态的信号强度是 $1/M$,第二个密文态的信号强度是 $2/M$,以此类推,最后一个密文态的信号强度是 1。每一个运行子密钥对应一组密文态,这组密文态的信号强度取平均值之后即为该运行子密钥对应的判决门限。

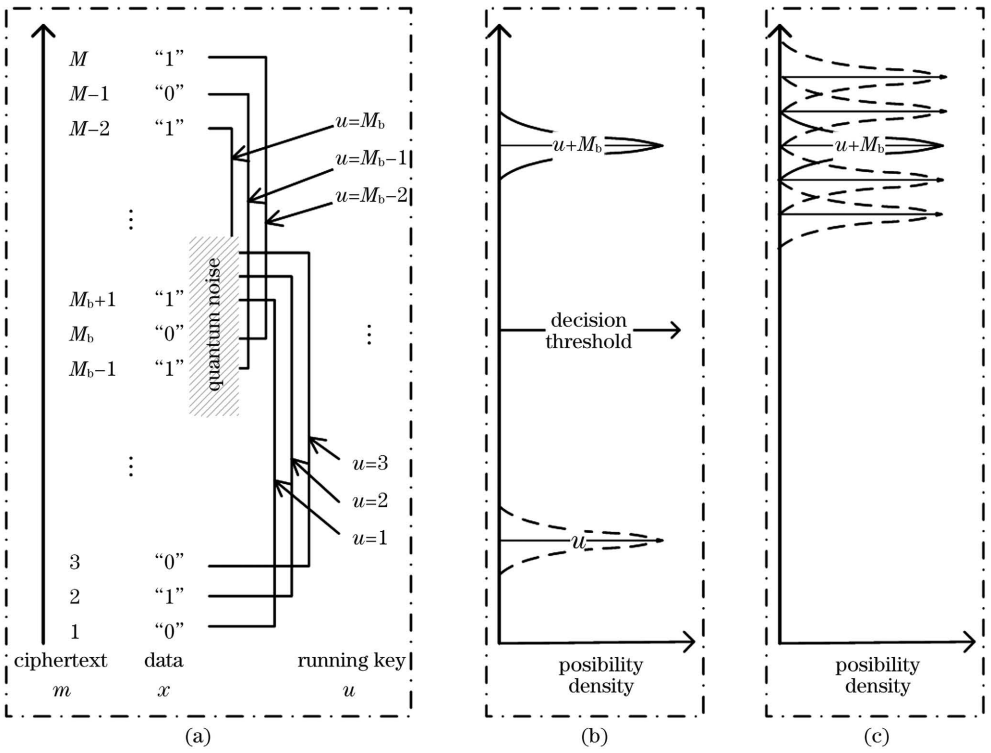

图 2　ISK Y-00 加密原理。(a)Y-00 协议编码规则；(b)Bob；(c)Eve

Fig. 2　Encryption principle of ISK Y-00. (a) Y-00 protocol encoding rule; (b) Bob; (c) Eve

plaintext	running key				
	basis 1	basis 2	basis 3	…	basis M_b
0	P_1	P_{2+M_b}	P_3	…	P_{M_b}
1	P_{1+M_b}	P_2	P_{3+M_b}	…	P_M

(a)

basis	basis 1	basis 2	basis 3	…	basis M_b
threshold	$(P_1+P_{1+M_b})/2$	$(P_2+P_{2+M_b})/2$	$(P_3+P_{3+M_b})/2$		$(P_{M_b}+P_M)/2$

(b)

图 3　ISK Y-00 协议映射关系。(a)明文与密文的映射关系；(b)基态与判决门限的映射关系

Fig. 3　Mapping relationship of ISK Y-00. (a) Mapping relationship between plaintext and ciphertext; (b) mapping relationship between basis and threshold

需要明确的是，在大容量通信背景下，尽管可以做到让种子密钥 K^S 足够长，密钥扩展模块的扩充倍数足够大，保证运行密钥序列 U^N 在某一段时间内一定能够安全地加密所需传输的明文，但种子密钥 K^S 需要周期性更新，这有利于整个系统抵抗窃听方以某种途径获取部分明密文对应关系的已知明文攻击。

2.2　并联 ISK-QNRC 方案

在图 4 所示的并联 ISK-QNRC 实现方案中，发送端运行子密钥与数据比特加密映射之后，前 l 比特用于调制第一个强度调制器，后 n 比特用于调制第二个强度调制器，用光衰减器调节信号强度，使输出光功率为原来的 $1/2^l$，再将两路光信号合路送入链路传输。接收端同理产生一个解密信号，与链路传来的光信号作功率匹配。最后，两路光信号进入光检测器，与输出的电信号进行比对，得到二进制的明文。

假设两个强度调制器性能参数相同，则当驱动电压为二进制信号时，调制器输出的最大光功率 P_{max} 和最小光功率 P_{min} 也相同，其功率差为 ΔP。将加密映射之后的密文信号分为前后两部分，如图 4 分别为 l bit 和 n bit，此时在多进制信号驱动下，两个调制器输出的最大功率和最小功率之差为

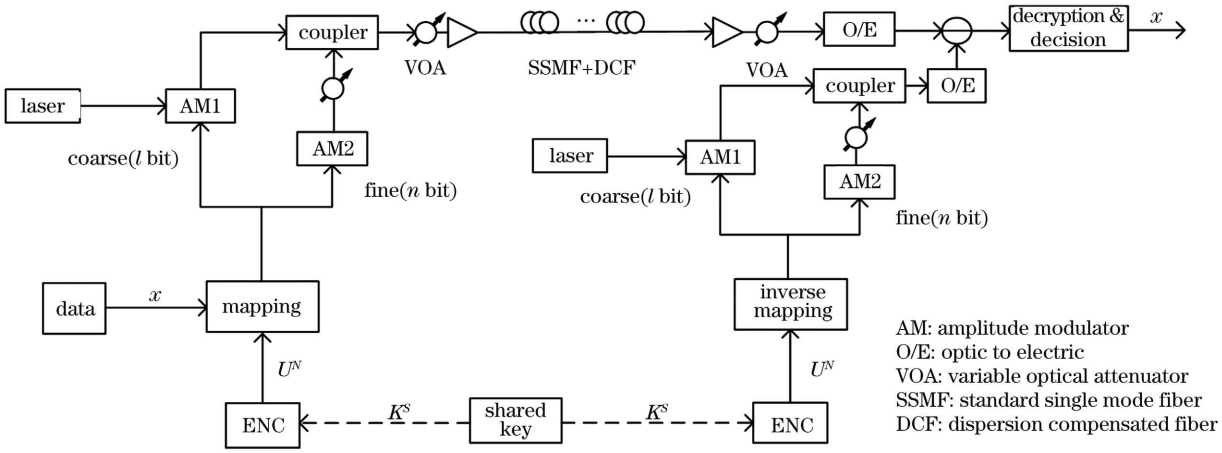

图 4　ISK-QNRC 实现方案框图

Fig. 4　Diagram of ISK-QNRC realization scheme

$$\Delta P_{\mathrm{AM1}}=\Delta P\left(1-1/2^{l}\right), \tag{3}$$

$$\Delta P_{\mathrm{AM2}}=\Delta P\left(1-1/2^{n}\right)。 \tag{4}$$

将强度调制器 AM2 输出的功率衰减为原来的 $1/2^{l}$ 后，再将两路光信号耦合，则输出最大功率和最小功率之差为

$$\Delta P_{\mathrm{AM}}=\frac{\Delta P}{2}\left(1-1/2^{l+n}\right), \tag{5}$$

其中括号外的 1/2 是耦合系数。(5)式说明用 l bit 和 n bit 分别调制两个强度调制器，再将两路光信号精确调节后耦合，从而实现 $2^{l+n}-1$ 强度等级的 ISK-QNRC 系统是可行的。如图 5 所示，依照表 1 的参数设置搭建了基于并联强度调制的 ISK-QNRC 系统仿真平台。为避免两路光信号耦合时发生相干，影响最终结果，此系统应当选取线宽稍宽的激光器。在发送端，将 10 bit 的密文信号分为 4 bit 和 6 bit 并利用 AWG 将其转化为多电平信号驱动调制器，再将 6 bit 那一路的光信号衰减为原来的 1/16，耦合后用光衰减器将信号衰减至介观态，利用光放大器(EDFA)将介观信号放大，同时引入噪声，以增强安全性。在接收端，用同样的方式将运行子密钥加载到调制器上，两路光信号经光电转换后比对得到二进制电信号，再经波形整形后送入误码仪。

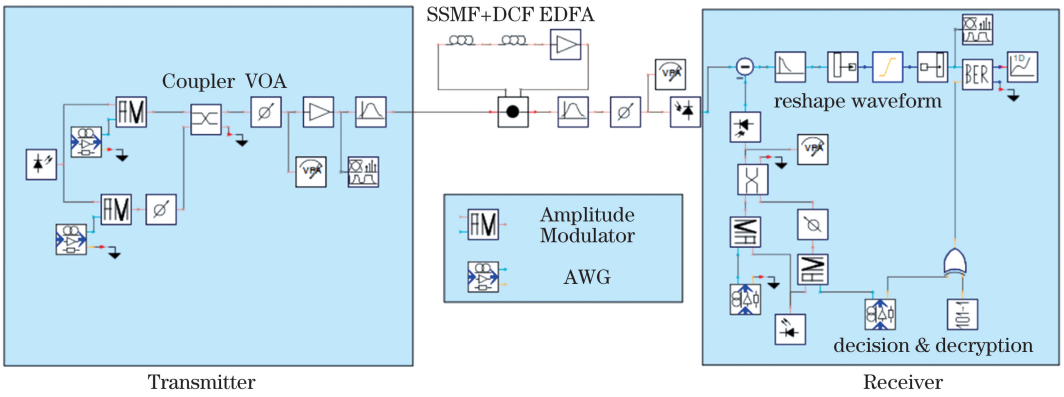

图 5　并联 ISK-QNRC 系统仿真框图

Fig. 5　Simulation diagram of parallel ISK-QNRC system

表 1　参数设置

Table 1　Configuration of parameters

Parameter	Value	Parameter	Value
Length of ciphertext /bit	4+6	Attenuation /(dB·km^{-1})	0.2
Bit rate /(Gbit·s^{-1})	10	Dispersion of SSMF /(ps·nm^{-1}·km^{-1})	16
Gain of EDFA /dB	20	Dispersion of DCF /(ps·nm^{-1}·km^{-1})	−80
Noise figure of EDFA /dB	4	Length of SSMF /km	83.33
Current noise spectral density of AWG /(10^{-12} A·Hz$^{-0.5}$)	10	Length of SSMF /km	16.67
Thermal noise of photodiode /(10^{-12} A·Hz$^{-0.5}$)	10	Linewidth of laser /GHz	1

最终可得经级联调制、引入噪声后 Y-00 加密信号的眼图、波形图如图 6(a)和图 6(b)所示，解密后信号的眼图、波形图如图 6(c)和图 6(d)所示。由此可知，引入噪声之后信号无法辨别，以此实现加密的目的；在经过解密之后，信号重新恢复为二进制信号，眼图清晰可辨，合法接收方能够准确地获得明文信息，而非法的窃听方不能从加密信号中准确地获得信息。

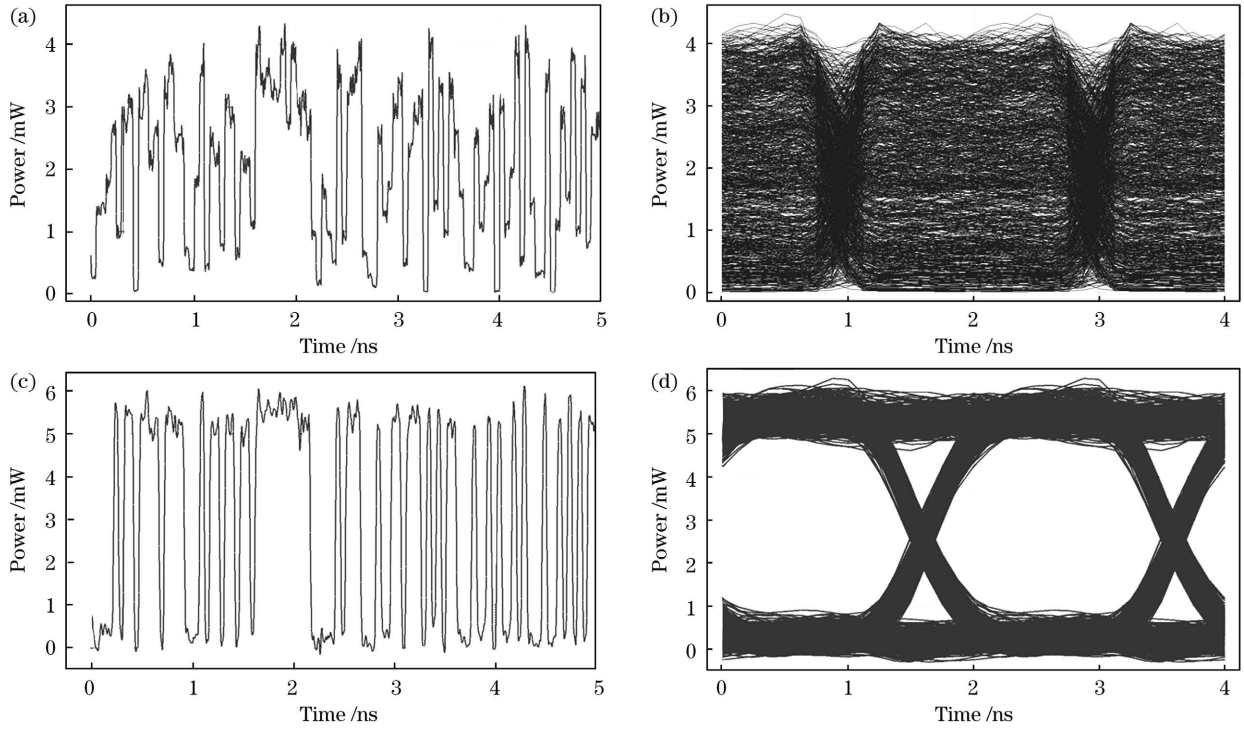

图 6　解密前后波形图和眼图。(a)解密前波形图；(b)解密前眼图；(c)解密后波形图；(d)解密后眼图

Fig. 6　Waveforms and eye diagrams of signal before and after decryption. (a) Waveform of signal before decryption; (b) eye diagram of signal before decryption; (c) waveform of signal after decryption; (d) eye diagram of signal after decryption

3　分析与讨论

图 7 描述了不同接收功率 P_r 在某一固定距离[背靠背(B2B，即 0 km)，500 km，1000 km]、固定介观态功率(−20 dBm)情况下的误码率变化曲线，可知随着接收光功率增加，光信噪比增大，系统的误码率变低。在接收光功率相同时，传输距离越小，误码率越小。误码率为 10^{-10} 时，B2B 与 500 km 传输时的功率代价大约为 1 dBm，500 km 与 1000 km 传输时的功率代价大约为 1.35 dBm。但值得注意的是，此并联 ISK-QNRC 方案采用的是两路调制信号比对获得二进制信号的方式，因此精确匹配两路信号的光功率十分重要，在同样的设置下，尽管光功率变化非常小，但不同的功率差对应的误码率可能会相差一个量级。

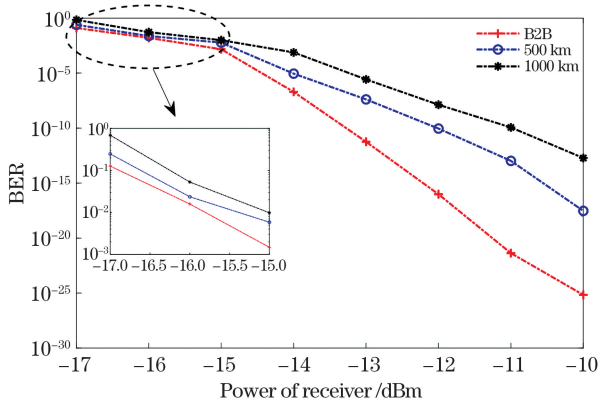

图 7　误码率与接收功率的关系

Fig. 7　BER versus received power

对于 QNRC 系统来说，若介观态功率 P_{so} 太大，则量子噪声掩盖相邻密文态的能力就会减弱，若介观态功率太小，对于合法接收方的接收信噪比又会降低，最终导致误码性能降低。为了在保证保密性的同时拥有更好的传输性能，需要寻找一个合适的介观态功率。图 8 描述了固定距离(B2B，500 km)、固定接收功率(−10 dBm，−15 dBm)下，误码率和介观态功率之间的关系。由此可知，在传输距离都为 500 km时，接收功率大时误码性能好，

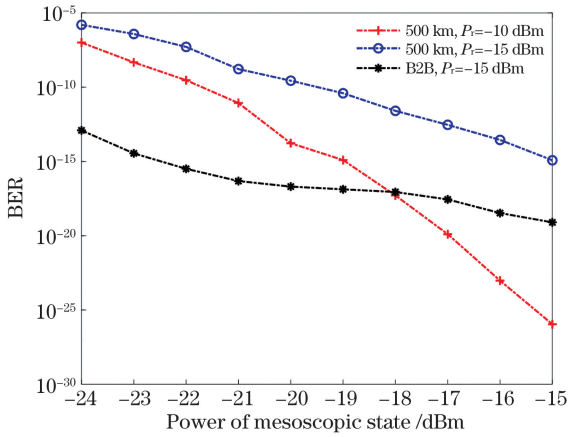

图 8 误码率与介观态功率的关系

Fig. 8 BER versus power of mesoscopic state

在接收功率都为−15 dBm 时，传输距离小时误码性能好。在介观态功率大于−18 dBm 时，尽管传输距离远，但接收功率为−10 dBm 的信号相比于 B2B 信号的误码率更低，此时接收功率对于提高误码性能的作用占据主导地位；相反，在介观态功率小于−18 dBm 时，传输距离对于提高误码性能的作用占据主导地位。由于该方案误码率对两路功率之间的差值敏感，两条曲线的交点不一定准确地位于−18 dBm，但总体的趋势应当是一样的。

衡量光通信系统有效性的重要指标是带宽距离积，在固定的传输速率下，研究传输距离对于探究带宽距离积是必要的。图 9 描述了在固定介观态功率（−15 dBm、−20 dBm）、固定接收功率（−10 dBm、−15 dBm）情况下，传输距离与误码率之间的关系。可以发现，不论介观态功率和接收功率如何，在固定条件下误码性能都是随着传输距离增加而劣化的，其原因是随着传输距离增加，为了补偿光纤带来的损耗，使用放大器的过程中产生了越来越多的放大自发辐射（ASE）噪声，使得接收端信噪比降低，误码性能劣化。此外，不难发现，介观态功率变化相对接收功率变化对整体误码性能变化的影响小，这也验证了该方案对接收功率变化比较敏感的特点。

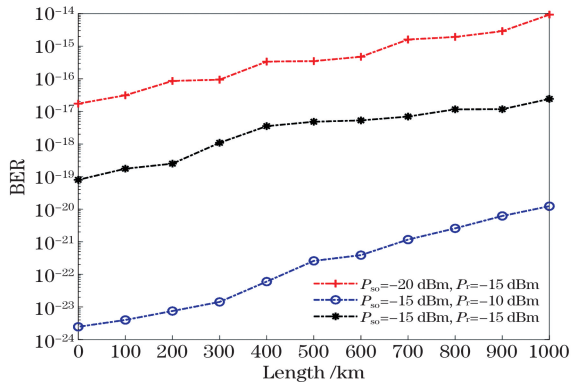

图 9 误码率与传输距离的变化关系

Fig. 9 BER versus length

4 结 论

以绕开高速率、高分辨率 DAC 限制为出发点，采用并联强度调制、光域解密、直接检测的方法实现了并联 ISK-QNRC 方案，并对该方案中介观态功率、传输距离、传输速率这三个重要的物理参数变化带来的误码性能进行了讨论分析，以此得出了将有效性、可靠性、安全性三个性能指标统一的结果（介观态功率为−20 dBm、传输距离为 500 km、传输速率为 10 Gbit/s、密文态数目为 $2^{10}-1$、无误码传输）。此外，本文发现该方案对于接收端功率变化以及密文信号与解密信号的功率差比较敏感，在实际操作中这一点将可能影响整个系统的误码性能，但这种影响可以通过接收端密文信号与解密信号的功率精确匹配来消除。

参 考 文 献

[1] Wyner A D. The wire-tap channel[J]. Bell System Technical Journal, 1975, 54(8): 1355-1387.

[2] Zhu H T, Wang R, Pu T, et al. Optical steganography of code-shift-keying OCDMA signal based on incoherent light source[J]. IEEE Photonics Journal, 2015, 7(3): 1-7.

[3] Yu L C, Lu L, Zhu Y, et al. Simulation on covert communication system based on coherent OCDMA technology[J]. Acta Optica Sinica, 2009, 29(2): 316-322.
余罗陈, 卢麟, 朱勇, 等. 基于相干光码分多址技术的隐藏通信系统仿真[J]. 光学学报, 2009, 29(2): 316-322.

[4] Nair R, Yuen H P, Corndorf E, et al. Quantum-noise randomized ciphers[J]. Physical Review A, 2006, 74(5): 052309.

[5] Ma L, Zhang J, Wang B, et al. Quantum noise stream cipher of optical communication in physical layer security[J]. Laser & Optoelectronics Progress, 2020, 57(23): 230603.
马乐, 张杰, 王博, 等. 光通信物理层安全中量子噪声流加密[J]. 激光与光电子学进展, 2020, 57(23): 230603.

[6] Yuen H P. KCQ: a new approach to quantum cryptography I. General principles and key generation [EB/OL]. (2003-11-10)[2020-12-20]. https://arxiv.org/abs/quant-ph/0311061.

[7] Corndorf E, Liang C, Kanter G S, et al. Quantum-noise randomized data encryption for wavelength-division-multiplexed fiber-optic networks [J]. Physical Review A, 2005, 71(6): 062326.

[8] 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, 2021, 39(4): 1056-1063.

[9] Tanizawa K, Futami F. Digital coherent 20-Gbit/s DP-PSK Y-00 quantum stream cipher transmission over 800-km SSMF [C] // Optical Fiber Communication Conference (OFC) 2019, March 3-7, 2019, San Diego, California. Washington, D. C.: OSA, 2019: Th1J.7.

[10] Tan Y T, Pu T, Zhou H, et al. Performance analysis of physical-layer security in ISK quantum-noise randomized cipher based on wiretap channel[J]. Optics Communications, 2020, 461: 125151.

[11] Chen Y K, Jiao H S, Zhou H, et al. Security analysis of QAM quantum-noise randomized cipher system [J]. IEEE Photonics Journal, 2020, 12(4): 1-14.

[12] Chen Y K, Pu T, Zheng J L, et al. Simulation verification of phase-shift keying quantum-noise randomized cipher system [J]. Acta Optica Sinica, 2020, 40(16): 1606001.
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): 1606001.

[13] 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.

[14] 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.

[15] Hirota O, Sohma M, Fuse M, et al. Quantum stream cipher by the Yuen 2000 protocol: design and experiment by an intensity-modulation scheme [J]. Physical Review A, 2005, 72(2): 022335.

[16] Futami F, Tanizawa K, Kato K. Y-00 quantum-noise randomized stream cipher using intensity modulation signals for physical layer security of optical communications [J]. Journal of Lightwave Technology, 2020, 38(10): 2774-2781.

Realization Scheme of Quantum Noise Randomized Cypher Based on Parallel Intensity Modulation

Li Yunkun**, Pu Tao, Zheng Jilin*, Tan Yeteng, Chen Yukai

College of Communication Engineering, Army Engineering University of PLA, Nanjing, Jiangsu 210001, *China*

Abstract

Objective To address the limitation imposed by a high-speed, high-resolution digital-to-analog converter (DAC) on the quantum noise randomized cypher (QNRC) research, a novel scheme using the structure of paralleled intensity modulators is proposed, increasing the number of ciphertext states considerably.

Methods A detailed explanation of the intensity shift keying (ISK)-QNRC encryption principle demonstrates that an ISK-QNRC with paralleled modulators is feasible. In this study, we established a system which employs optical domain decryption and direct detection. On the receiver's side, a running key is modulated on a local oscillator as the decryption signal. After matching the power of the decryption signal and ciphertext signal, which is from the sender's side, these two signal can be converted into a binary electrical signal via a balanced photonics detector. The plaintext is obtained after XOR for the binary electrical signal with the least significant bit of the running key.

Results and Discussions We establish an optical communication system (Fig. 5) and configure it properly (Table. 1) using professional simulation software VPItransmission Maker Optical System 9.1. Simulation results (Fig. 6) show that the ISK-QNRC system with the mesoscopic power of -20 dBm, a transmission distance of 500 km, the bit rate of 10 Gbit/s, and the number of ciphertext states of $2^{10}-1$ can be realized, while a plaintext cannot be obtained using the wire-tapper without the running key. We discuss the effect of the received power, mesoscopic power, and transmission length on the error performance. As is shown in Fig. 7, the bit error rate (BER) decreases as the received power increases at a specific transmission length (B2B, 500 km, 1000 km) and a specific mesoscopic power (-20 dBm). In addition, when the BER is 10^{-10}, the power penalty for 500 km is

approximately 1 dBm compared with B2B and that for 1000 km is approximately 1.35 dBm compared with 500 km. Fig. 8 describes the relationship between the BER and the mesoscopic power at a specific transmission length (B2B, 500 km) and a specific received power (−10 dBm, −15 dBm). When the transmission length is 500 km, the error performance improves with increasing received power, and when the received power is −15 dBm, the error performance improves with decreasing transmission length. Although the transmission length is longer when the mesoscopic power is greater than −18 dBm, the received power of the −10-dBm signal has a lower BER than that of B2B signal. Here, the received power plays a dominant role in improving the error performance. By contrast, when the mesoscopic power is less than −18 dBm, the transmission length plays a dominant role in improving the error performance. Fig. 9 describes the relationship between the transmission length and BER at specific mesoscopic power (−15 dBm, −20 dBm) and specific received power (−10 dBm, −15 dBm). It is well known that the BER always increases as the transmission length increases because a longer distance means more amplified spontaneous emission noise caused by erbium-doped fiber amplifier. By setting different variable optical attenuator parameters at the receiver's side, we find that the BER is sensitive to the power difference between ciphertext and decryption signals.

Conclusions This study aims to overcome the limitation of high-speed and high-resolution DACs. Therefore, we propose the parallel intensity modulation, optical domain decryption, and direct detection methods to realize the parallel ISK-QNRC scheme. The effect of changes in three important physical parameters (received power, mesoscopic power, and transmission length) on error performance is discussed and analyzed, and the results of three performance indicators of effectiveness, reliability, and security are obtained (mesoscopic power of −20 dBm; transmission length of 500 km; bit rate of 10 Gbit/s; number of ciphertext states of $2^{10}-1$, BER of 10^{-10}). In addition, we observe that the error performance of this scheme is sensitive to the power difference between the ciphertext and decryption signals. In an actual operation, this may affect the error performance of the entire system, but this effect can be eliminated by precisely matching the power of the two signals.

Key words optical communications; quantum noise random cypher; intensity modulation; paralleled modulators

OCIS codes 060.4785; 110.3055; 060.5565; 270.5568