光通信物理层安全中量子噪声流加密

马乐[1]，张杰[2*]，王博[2]，雷超[2]，李亚杰[2]，曲倩[1]，肖博[1]，王瑜暄[1]，袁平亮[1]

[1]国家电网甘肃省电力公司信息通信分公司，兰州 甘肃 730000；

[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 作为一种新兴的光通信物理层安全技术，量子噪声流加密结合了数学复杂度和物理复杂度，具有高安全、高速率、长跨距、结构灵活、与现有光纤通信系统高度兼容等优点。详细阐述量子噪声流加密的研究现状和基本原理，在密钥协商方面，对比了量子噪声流加密的 Y-00 协议与量子密钥分发的 BB84 类型协议，概述量子噪声流加密的关键技术方案。介绍了量子噪声流加密的典型应用案例，提出一种统一协商信道和传输信道的内生安全光通信系统，并进行了实验验证。最后分析量子噪声流加密的发展趋势。

关键字 光通信；Y-00 协议；量子噪声流加密；内生安全光通信

中图分类号 TN913.7 **文献标识码** A **doi**：10.3788/LOP57.230603

Quantum Noise Stream Cipher of Optical Communication in Physical Layer Security

Ma Le[1], Zhang Jie[2*], Wang Bo[2], Lei Chao[2], Li Yajie[2], Qu Qian[1], Xiao Bo[1], Wang Yutong[1], Yuan Pingliang[1]

[1]*Information Communication Company, Gansu Electric Power Company, State Grid, Gansu, Lanzhou* 730000, *China*;

[2]*State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*

Abstract As a new security technology in the physical layer of optical communication, quantum noise stream cipher combines mathematical complexity and physical complexity. The quantum noise stream cipher has the advantages of high security, high speed, long span, flexible structure, and high compatibility with the existing optical fiber communication systems. This paper presents the current research status and the basic principle of the quantum noise stream cipher. In the aspect of key negotiation, we compare the Y-00 protocol of quantum noise stream cipher with the BB84-type protocol of quantum key distribution and summarize the quantum noise stream cipher's key technical schemes. Additionally, we introduce a typical application of quantum noise stream cipher and propose an endogenously secure optical communication system with a unified negotiation channel and transmission channel. The experimental verification is demonstrated, and finally, the development trend of a quantum noise stream cipher is analyzed.

Key words optical communications; Y-00 protocol; quantum noise stream cipher; endogenously secure optical communication

OSIC codes 060.2330; 060.4785; 060.5565

1 引 言

随着高清视频、5G 通信的快速发展，各种信息交互量与日俱增，对光传输系统的安全性提出了新挑战。为实现光通信物理层安全，学术界对如何形成高速率、长跨距、低成本、强防护的安全光传输系统开展

收稿日期：2020-03-27；**修回日期**：2020-04-22；**录用日期**：2020-04-27

基金项目：国家电网甘肃省电力公司科技项目(522723180031)、国家自然科学基金(61831003)

* **E-mail**：jie.zhang@bupt.edu.cn

了长期的探索与实践[1]。根据信号处理技术手段的不同，光通信物理层安全技术可以大致分为三大类：电信号处理方案、全光信号处理方案、光电信号处理方案。

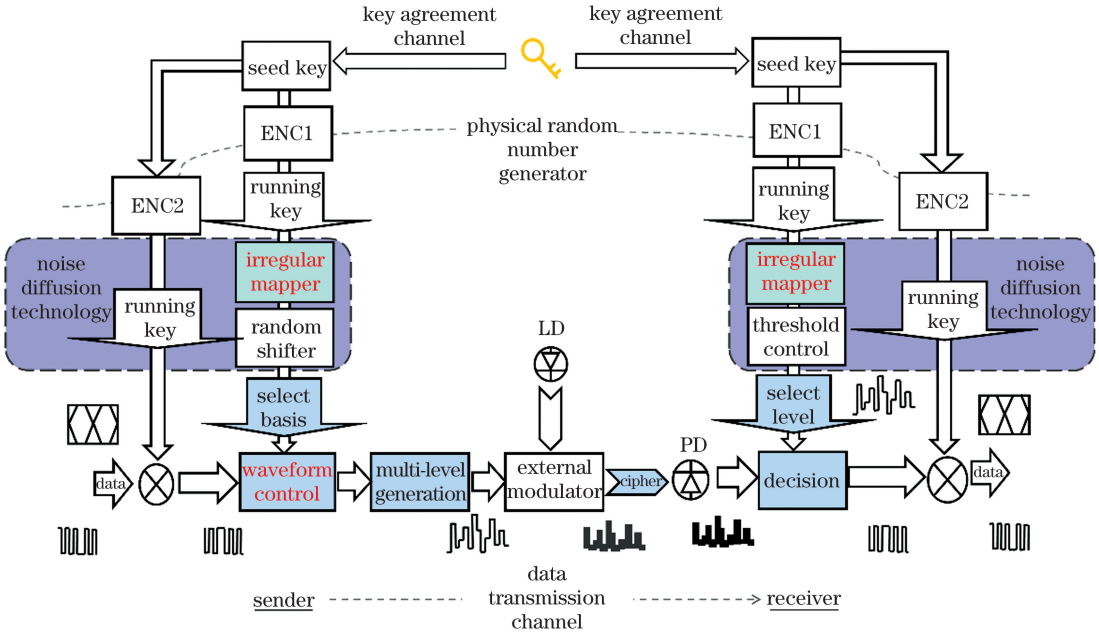
本文主要关注光电信号处理相关的研究，量子噪声流加密(QNSC)是近几年兴起的一种基于数学复杂度(短密钥扩展为长密钥的算法)和物理复杂度(量子测量坍缩原理)的加密技术[1]。该技术有望突破对称加密的香农极限，在物理层安全光通信中具有很大的应用潜力。主要总结 QNSC 用于传输信道和协商信道的基本原理和关键技术，并通过对比介绍了该技术的特征；随后梳理 QNSC 的具体应用场景和存在的问题，探讨了统一传输信道与协商信道的内生安全光通信系统；最后对 QNSC 的发展趋势进行总结。

2 量子噪声流加密

2.1 QNSC 原理

量子噪声流加密也称为量子随机加密、量子流加密、量子迷加密，这里统称为量子噪声流加密(QNSC)。QNSC 的主要协议是 Y-00，该协议由美国西北大学的 Yuen 教授于 2000 年提出[2]。QNSC 属于流加密，其基本原理是香农提出的理论上安全的“一次一密”。但要实现真正意义上的“一次一密”，存在以下需求：密钥和明文等长，且真随机；密钥生成速率与信息传输速率要一致。在高速率通信背景下，这种需求很难满足。现有的解决思路是：首先，通过协商信道分发短的真随机密钥；其次，使用短的真随机密钥来生成长密钥流；最后，使用该长密钥流加密明文生成密文。这就意味着系统的安全性由传输信道和协商信道二者的安全性共同保证。

图 1 是以相位调制为例的 QNSC 技术加解密流程图，主要分为协商信道(上部分)和传输信道(下部分)。具体实现方法如下。



ENC：encryption；LD：laser diode；PD：photoelectric detection

图 1 Y-00 加解密配置图

Fig. 1 Diagram of Y-00 encryption and decryption configuration

1)密钥生成过程。如图 2 所示，使用经过协商信道预先共享的种子密钥 K_s，将经过加密盒(ENC)的 K_s 扩展为运行密钥 K_r，运行密钥通过映射器来选择基(basis)。ENC 和映射器是密钥生成过程的重要组成部分，其中应用最广泛的 ENC 有线性移位寄存器(LFSR)、高级加密标准(AES)及安全散列算法 1(SHA-1)等。在图 1 中，映射器主要采用不规则映射和重叠选择键控组合的噪声扩散技术来选择基，这种噪声扩散的目的是增强密钥的随机性。

2)加密过程。在电域上将二进制数据 X(明文)与基按加密函数生成密文，将激光器输出的信号作为光载波，密文信号经外部调制器加载到光载波上传输。此时，密文信号被调制到光域的介观态上，

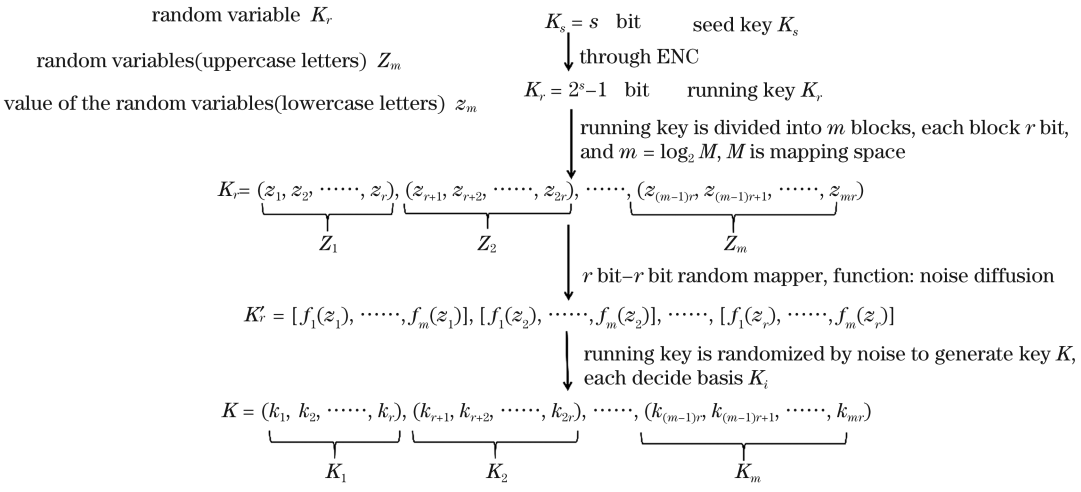


图 2 Y-00 密钥生成过程

Fig. 2 Y-00 key generation process

得到量子模 $|\psi(X, K_i)\rangle = |\psi(u)\rangle$。当信号映射空间 M 足够大或调制阶数足够高时，量子噪声引起的不确定性会大于已调信号之间的不确定性，从而达到量子噪声掩蔽的效果。加密函数为 $u = f(x, K_i) = K_i + [x \oplus \mathrm{Pol}(K_i)] \times 2^{|K_i|}$。其中，$\mathrm{Pol}(K_i)$ 根据 K_i 的奇偶性取值，当 K_i 为奇数时，$\mathrm{Pol}(K_i)=1$，当 K_i 为偶数时，$\mathrm{Pol}(K_i)=0$；$2^{|K_i|}$ 为密钥 K_i 决定的基的最高位；x 为明文；u 为加密得到的密文值。该函数的物理意义是对明文与基的最高位进行异或加密，加密原理如图 3 所示。

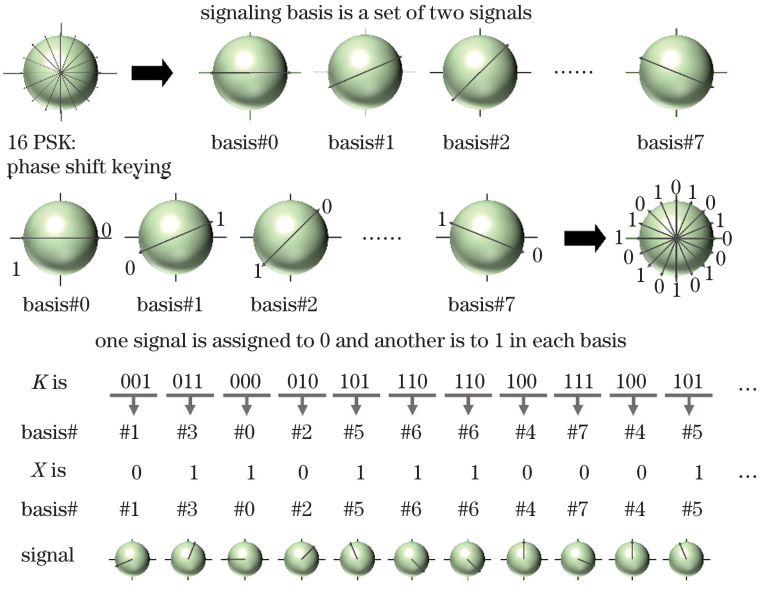


图 3 Y-00 加密过程

Fig. 3 Y-00 encryption process

3)解密过程。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声的影响，而合法的接收者在使用密钥解密后可以将密文检测为低阶调制数据，进而选择合适的判决电平以恢复明文。

QNSC 本质是相干光量子效应，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。量子噪声来自元件的量子效应，不是由设备的缺陷引起的，受测不准关系的支配，无法完全消除。具体来说，每个脉冲产生的光子数(脉冲能量值)不能固定，而是服从参数为$<n>$的泊松分布，其中$<n>$为平均光子数。因此，激光束发出的脉冲序

列也服从泊松分布的统计波动，该波动被称为量子噪声、光学噪声或散粒噪声。所以在图 3 中，Bob 面临测量相角 φ 的固有限制。相角 φ 不再是精确的物理量，而是在一定值附近波动，标准偏差为 $\Delta\varphi=\pm1/\sqrt{n}$，即该噪声与脉冲平均能量的平方根（光子数 n）成反比。

2.2 QNSC 协商与量子密钥分发对比

QNSC 与量子密钥分发（QKD）的对比如表 1 所示[3]，基于 BB84 协议的 QKD 是光纤通信物理层密钥分发的重点。该协议已被证明在理论上可以提供无条件的安全性，但 QKD 存在两方面的不足：一方面，QKD 的传输距离和通信速率都受到技术水平的限制；另一方面，QKD 方案中的单光子态具有敏感性，在光纤损耗下非常脆弱，无法进行光放大。因此，在大规模、长距离组网建设中无法使用这种技术。

QNSC 采用容易产生相干态的光信号作为光源，利用合法接收方和窃听者的非对称测量创造优势，解决了光脉冲中光子个数少的难题，从而突破了量子通信速率低、传输距离短等技术水平限制。QNSC 的主要特点是结构灵活、与现有光纤通信系统高度兼容、支持波分复用和光中继放大、支持多点到多点的拓扑结构、有望突破加密技术的香农极限等。实验表明，QNSC 具有较高的速率和较大的传输距离。

表 1 BB84 类型协议与 Y-00 对比[3]

Table 1 Comparison between BB84-TYPE and Y-00[3]

Comparison content	BB84-TYPE	Y-00
Purpose	Key generation	Currently data encryption (can be used for key generation)
Means of advantage creation	Intrusion-level detection	Asymmetric optimal measurement
Intrusion detection	Precise intrusion-level estimation needed to bound information leak	Not needed but can be implemented to increase security/data rate
Use of pre-shared key	Not required by design (needed for authentication to avoid MIM)	Essential for encryption
Man-in-the-middle (MIM) attack	Prone to	Not prone to (due to the use of pre-shared key)
Mean number of photons	~0.1 (non continuous variable-QKD)	≫1 (10–1000 and above)
Maximum data rate reported	~1 Mbit/s	>10 Gbit/s
Detector technology	Single-photon detector	Conventional photo-detector
Long distance application	Quantum repeater	Conventional optical amplification

3 量子噪声流加密的关键技术

QNSC 的传输方案和协商方案目的不同，但是关键技术基本一致，都是通过光纤传输技术来实现的。如图 4 所示，从技术层面来看，QNSC 主要包括光信号的产生、调制、检测等几方面。

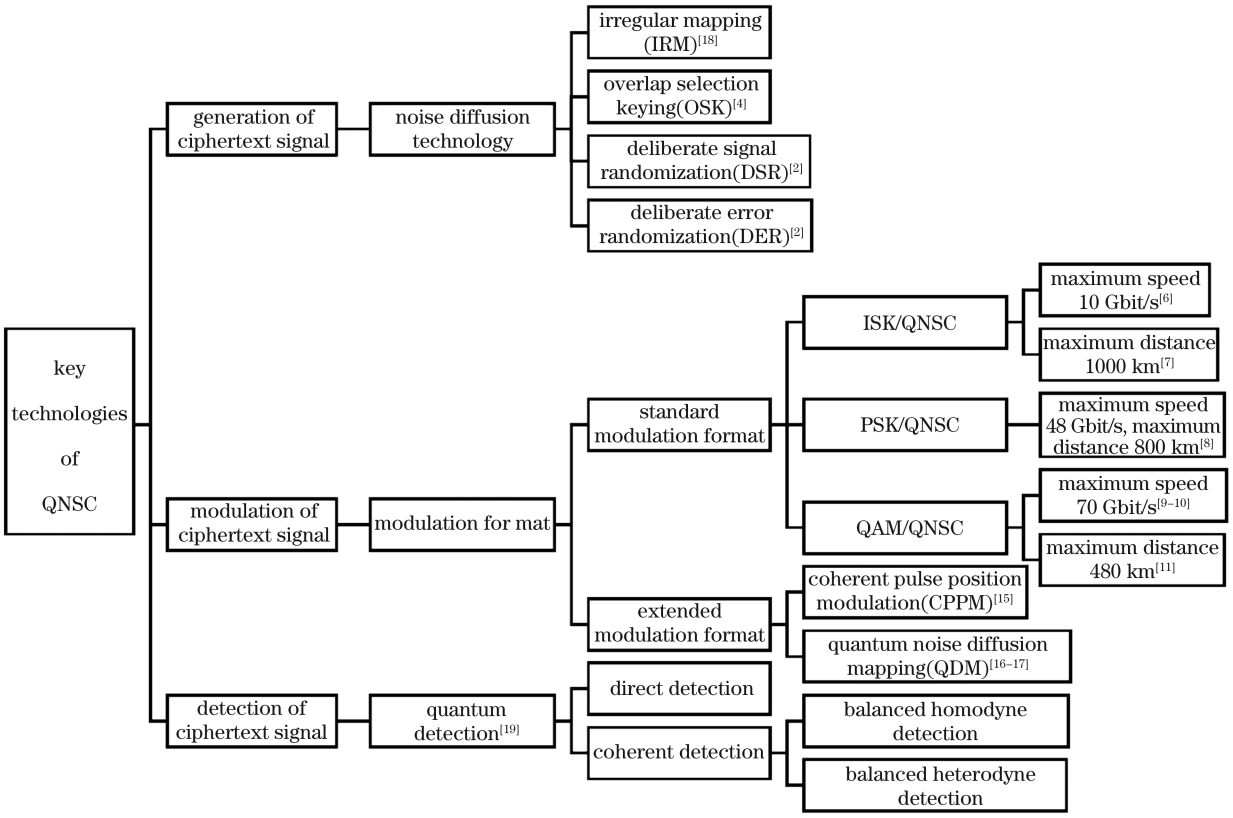
3.1 调制格式

目前，QNSC 中标准调制格式主要有三种，即相位调制（PSK/QNSC）、幅度调制（ISK/QNSC）[4]及正交振幅调制（QAM/QNSC）[5]。

ISK/QNSC 是一种在幅度域上对数据进行加密的物理层加密技术，原理如图 5 所示。目前实验中，单通道最高速率可达 10 Gbit/s，但传输距离为 360 km，密文空间为 64[6]。最长传输距离可达 1000 km，但传输速率为 1.5 Gbit/s[7]。

PSK/QNSC 是一种在相位域上对数据进行加密的物理层加密技术，原理如图 6 所示。2019 年，日本玉川大学基于正交相移键控（QPSK）调制格式，利用从粗到细相位随机化、偏振复用技术实验实现了 48 Gbit/s 的最高传输速率，同时最长传输距离可达 800 km，单跨 100 km，密文空间可达 2^{18}，噪声掩盖数为 338。单通道传输系统的一项重要指标是速率与距离的乘积，考虑到前向纠错码，该实验速率和距离乘积可达 32000 Gbit·s^{-1}·km，这是目前实验成果中最好的传输性能[8]。

QAM/QNSC 是一种在幅度域和相位域上同时对数据进行加密的物理层加密技术，原理如图 6 所示。目前最高传输速率为 70 Gbit/s，使用 4，16，64，



PSK/QNSC: phase shift key/quantum noise stream cipher; ISK/QNSC: intensity shift key/quantum noise stream cipher; QAM/QNSC: quadrature amplitude modulation/quantum noise stream cipher

图 4 QNSC 的关键技术

Fig. 4 Key technique of QNSC

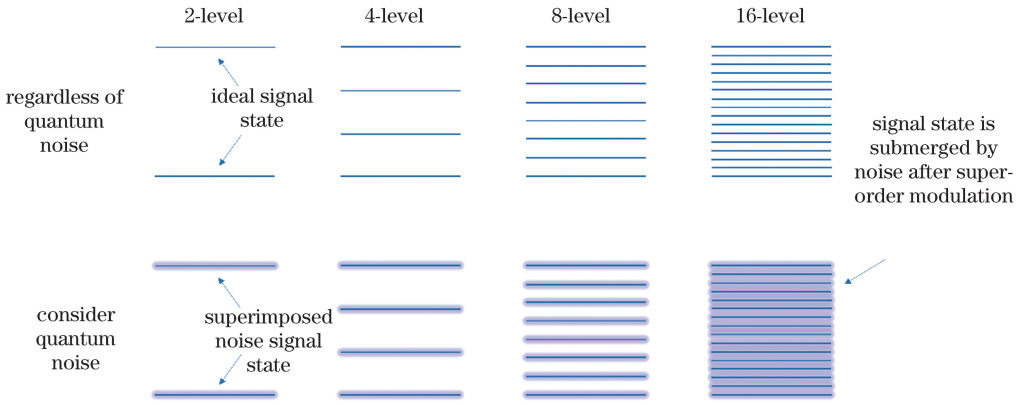


图 5 ISK/QNSC 原理图

Fig. 5 Schematic of ISK/QNSC principle

128QAM 数据实时变换，实时传输距离为单跨 100 km，密文空间达 2^{20}，该实验速率和距离乘积可达 7000 Gbit·s^{-1}·km，且该方法未使用复用技术而是结合连续变量量子密钥分发(CV-QKD)产生种子密钥，密钥生成速率为 600～700 bit/s，传输光子数大约为 10^6 个[9-10]。QAM/QNSC 目前在实验上的最长传输距离为 480 km，但即使利用偏振复用，传输速率也仅为 40 Gbit/s[11]。

针对 PSK/QNSC 和 QAM/QNSC 的安全性能和传输性能，国内外学者对其进行了比较。安全证明最重要的步骤就是计算攻击者最小平均检测错误率和估计攻击者所获得信息量的上界，所以日本玉

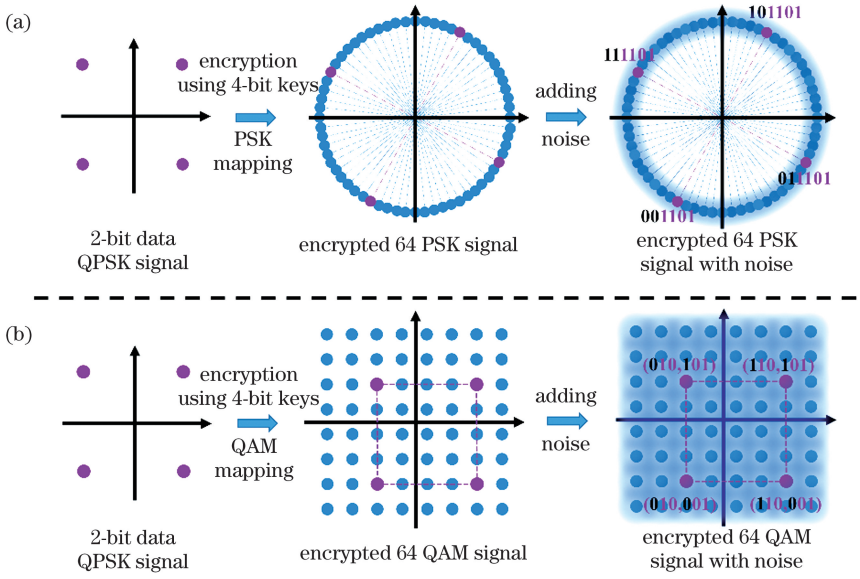


图 6 两种技术的原理图。(a) PSK/QNSC;(b) QAM/QNSC

Fig. 6 Principle schematic of two technologies. (a) PSK/QNSC; (b) QAM/QNSC

川大学将这两个参数作为评价指标比较了 PSK、QAM、三重 PSK、三重 QAM 的安全性能。仿真结果表明,在已知明文攻击和唯密文攻击中,相较于其他调制格式,PSK 具有更好的安全性能[12]。量子噪声对攻击者的影响可以通过量子噪声掩蔽数来评价,日本玉川大学以该参数为指标比较了 ASK、ISK、PSK、QAM 的安全性能,经过严格的数学推导,仿真结果表明,在相同的发射功率和量子状态信号下,ISK 的量子噪声掩蔽数最高[13]。传输性能中最重要的指标就是 Q 因子,北京邮电大学以 Q 因子为指标,在传输距离为 200 km、最佳发射功率为 6 dBm 的背景下,比较了 PSK/QNSC 和 QAM/QNSC 在正交频分复用(OFDM)系统中的传输性能。实验结果显示,PSK-OFDM 的 Q 因子比 QAM-OFDM 的 Q 因子高 1.5 dB,说明 PSK-OFDM 的传输性能优于 QAM-OFDM[14]。

相比于 PSK/QNSC 和 QAM/QNSC,ISK/QNSC 的优势在于系统结构简单、成本低,在超高速光纤链路及具有高功率激光的卫星链路中具有显著的优势。而 PSK/QNSC 通过相位旋转加密,在星座图中的星座点之间欧氏距离更小,更容易被噪声覆盖,故而 PSK/QNSC 的安全性更高。QAM/QNSC 可以实时任意地改变调制数据的多样性,其原理是采用 2^NQAM 数据调制,每个符号可以发送 N bit 信息,因此频谱利用率可以提高 N 倍,从而实现更大的传输容量,但同时随着数据调制阶数的增大,相邻星座点之间欧氏距离明显变小,系统抗干扰能力急剧下降,同步难度增大。除了以上标准调制格式,研究人员还在为 QNSC 寻找其他扩展的调制格式,例如相干脉冲调制(CPPM)[15]、量子噪声扩散映射(QDM)[16-17]等。

3.2 噪声扩散技术

除了专门针对流加密的快速相关攻击,QNSC 还会受到唯密文攻击和已知明文攻击。对于唯密文攻击,攻击者尝试仅通过密文得到明文和密钥。对于已知明文攻击,攻击者尝试通过部分明文和相应的密文来得到密钥。密钥在 QNSC 中起着重要作用,密文信号的编码、调制、传输及检测技术都依赖于密钥的安全性。因此如何获得高效、稳定、可靠的长密钥流已成为一个亟待解决的问题。针对这个问题,目前的解决方法是采用噪声扩散技术(随机化)来保证系统的安全性。

规则映射(RM)是将运行密钥的每个数字按照规则映射到对应的量子模,该规则的表达式为

$$\begin{pmatrix} k_j \\ \alpha_{\mathrm{map}(k_j)} \\ \Pi_{\mathrm{map}(k_j)} \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & \cdots & M \\ \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_M \\ 0 & 1 & 0 & \cdots & 1 \end{pmatrix}, \tag{1}$$

式中:Π 为奇偶校验值,被用来添加到最终的量子模中以混合 0 bit 和 1 bit 值;$\alpha_{\mathrm{map}(k_j)}$ 为映射角度或幅度;明文 $X = x_1, x_2, \cdots, x_n$;运行密钥 $K_r = k_1, k_2, \cdots, k_n$,$k_j \in (1, \cdots, M)$。此时,量子模为

$$\begin{aligned} |\psi(X, K_r)\rangle = & |\alpha_{k_1 + M(x_1 + \Pi_{k_1})}\rangle \\ & |\alpha_{k_2 + M(x_2 + \Pi_{k_2})}\rangle \cdots |\alpha_{k_n + M(x_n + \Pi_{k_n})}\rangle。 \end{aligned} \tag{2}$$

通常不使用规则映射，因为此时检测过程中的量子噪声会影响特定量子模的几个 bit 位，该映射器容易受到快速相关攻击。通常的选择是不规则映射(IRM)[18]，这种不规则映射的特点是可以抵御快速相关攻击，表达式为

$$\begin{pmatrix} k_j \\ \alpha_{\mathrm{map}(k_j)} \\ \Pi_{\mathrm{map}(k_j)} \end{pmatrix} = \begin{pmatrix} 31 & 10 & M & \cdots & 16 \\ \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_M \\ 0 & 1 & 0 & \cdots & 1 \end{pmatrix}。 \tag{3}$$

重叠选择键控(OSK)是一种利用附加的伪随机数发生器对明文比特进行加扰的方法[4]。例如，在时间为 t、伪随机数发生器的输出位为 1 时，明文位 x_t 翻转，否则保持不变。因为明文的每一位都会影响光传输信号的选择，所以这种方法并不是经典的噪声扩散技术。可以看出，采用这种方法的好处是操作简单方便，但是实现成本较高。

故意信号随机化(DSR)通过连续摆动信号参数(例如信号的相位和幅度)来增强量子噪声的掩蔽效果[2]。只要波动幅度低于由系统参数确定的临界值，合法接收机就可以吸收信号波动，从而 DSR 机制只需安装在发射机上。但是这种方法需要高速真随机数发生器作为驱动机制，为了解决这个问题，有学者提出 DSR 的改进版本，采用的方法是使用伪随机数发生器代替真随机数发生器，并将此类型称为键控故意随机化(KDSR)。

故意错误随机化(DER)将精心设计的错误故意插入到传输信号中[2]。这种噪声扩散技术将合法用户和窃听者之间关于密钥的测量差异转换为纠错能力，使得性能差的密码转换为性能好的量子流密码。与其他噪声扩散技术相比，DER 具有复杂的结构，因为它包括了一些其他的噪声扩散技术，例如 DSR 和 OSK。此外，使用这种噪声扩散技术时还需要在接收机上进行一些修改，即为了检测到故意插入的错误，将接收机替换为双阈值信号检测方案，并安装了经典的解码机制以消除检测到的错误。因此，尽管该方案在差错控制码的应用上有良好的效果，但它比其他噪声扩散技术方案更为复杂。

3.3 量子检测技术

量子通信使用量子态作为信息载体。一般而言，粒子只有在微观尺度下才能观测到量子特性。此时信号能量微弱，这就要求接收机具有相当高的接收灵敏度和极低的噪声。因此对于光通信而言，检测是一个难题[19]。在现有光传输通信系统中，常见的检测方式包括直接光子能量检测与相干检测两种。直接检测技术需要较高的研制成本，而且检测器的体积大，对工作环境要求也较高，适用性不强。相干检测方式的检测装置为一对光电二极管，通过差分电路降低检测器噪声和本振光抖动，得到较高的灵敏度。这种检测方式最大的优点是可以在常温条件下工作，且量子效率比直接检测方式要高得多，在 1550 nm 电信光纤通信窗口波长上可以达 50% 以上。相干检测又分为平衡零差检测和平衡外差检测两类。通常，基于 ISK 的 QNSC 接收机使用直接检测，基于 PSK 的 QNSC 接收机需要使用光延迟干涉仪进行一比特差分检测或使用本地振荡器进行相干检测。基于 QAM 的 QNSC 接收机也是使用相干检测。

综上，量子噪声是理论上无法消除的绝对现象。由于此现象完全随机且无法复制，因此它与测量数据不相关。如果这种现象可以将影响扩散到整个信号区域，则不可能完全解密，很难区分正常接收者和窃听者的接收条件。因此，QNSC 的优化无法兼顾安全性能、传输性能、协议鲁棒性、接收机灵敏度。

4 量子噪声流加密的应用

目前，QNSC 的应用领域主要包括千兆以太网[20]、高清电视[21]、无人机系统[22]、光卫星链路[23]、内生安全光通信等。将重点介绍 QNSC 在内生安全光通信系统中的应用。

4.1 内生安全光通信系统

目前 QNSC 系统中直接加密和密钥分发分别由独立的系统来完成，密钥来源于外部，是“通密分离”的附加式安全。针对这一问题，北京邮电大学张杰教授[24]设计了“三区耦合、两路简并”的微元噪声模型，并提出了内生安全光通信系统，结构如图 7 所示。

如图 7 中间部分所示，“三区耦合”是指在微元内生安全模型中，抵入噪声传输带来信号结构的根本性变化，形成了远噪区、近噪区及浸噪区的微元域多噪区信号分布。数据通过微元映射进入远噪区传输，远噪区的高信噪比保证了安全传输性能(第 7 bit～第 N bit)；测量序列通过微元映射进入近噪区进行传输，利用微元近噪区的噪声敏感性，测量信道误码性能以进行数据协商，从而分发密钥(第 3 bit～第 6 bit)；在浸噪区内信号和噪声完全叠加，难以区分，利用浸噪区的这一特点实现噪声对数据信号的随机扰藏(第 0 bit～第 2 bit)。

如图 7 两边所示，在微元内生安全模型中，利用

远噪区实现对数据的安全传输，与此同时，利用近噪区测量和提取信道特征信息以实现安全协商能力。在统一 QNSC 信道下，实现了安全传输和安全协商两类通路功能简并，即“两路简并”，进而可以直接在一根光纤上传输，为满足内生安全要求提供了重要保障。

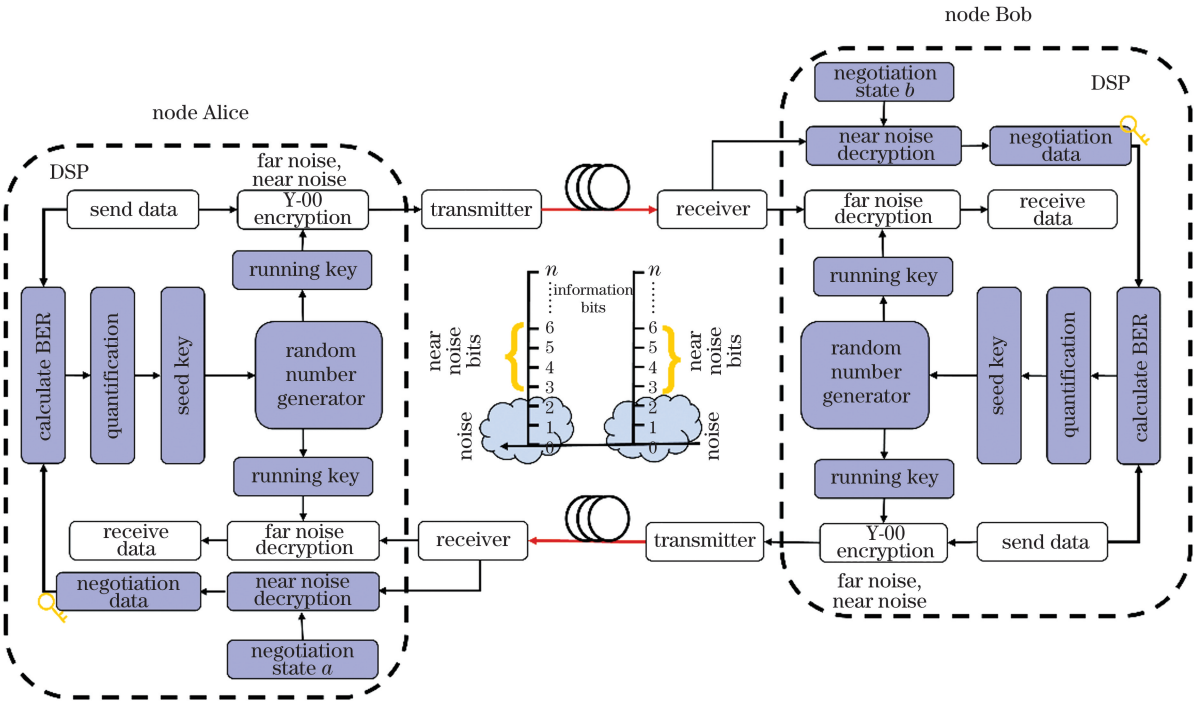


图 7 内生安全光通信系统理论模型

Fig. 7 Theoretical model of endogenously secure optical communication system

4.2 内生安全光通信研究进展

面对网络结构、业务种类、成本效率等多方面的挑战，内生安全光通信能在一定程度上有效提升光安全传输的综合性能，并能够降低成本、增加灵活性、提升效率。内生安全光通信研究进展如图 8 所示。

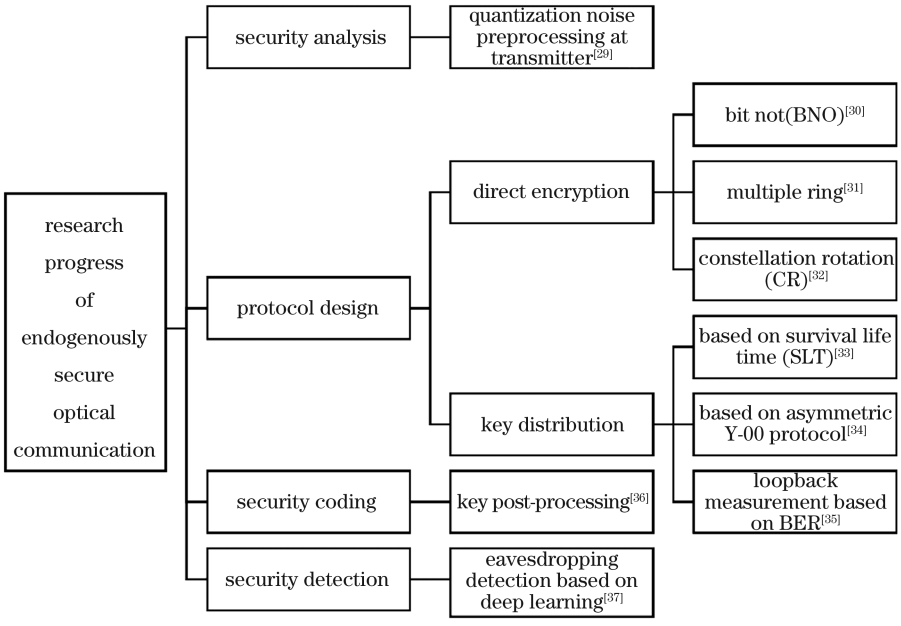


图 8 内生安全光通信研究进展

Fig. 8 Research progress of endogenously secure optical communication

在安全性分析方面，有学者对数模转换器(DAC)比特分辨率引入的量化噪声进行了仔细分析[25]。为了避免光放大器产生的受激辐射噪声，一般攻击者会将窃听点选择在紧接发射端之后。该学者利用具有不同比特分辨率 DAC 的 QAM/QNSC 和 PSK/QNSC，比较了攻击者在发射端和接收端的检测失败率与检测信号星座图大小的关系。实验表明，量化噪声可以保证信号经光发射器发送之后的安全性，而且此时为了降低接收信号的误码率，需要降低受激辐射噪声的发送功率，所以总噪声保持不变，即传输性能保持不变。

在协议设计方面，内生安全光通信设计了“三区耦合、两路简并”的微元噪声模型。主要从两方面来考虑，一方面考虑传输信道的直接加密方案，另一方面考虑协商信道的密钥分发方案。

针对直接加密方案，有学者从密文映射的角度，提出了基于比特非(BNO)的 MQAM 映射、基于多环的 BPSK 映射、基于星座旋转(CR)的 MPSK 和 MQAM 映射[26-28]。此处重点介绍基于 CR 的 MQAM 映射，随着明文比特长度的增加，噪声对比特位置的影响越来越小。针对这一问题，该学者利用 CR 对数据状态进行映射，达到不安全区域熵值增加的目的。这种方法的优点是无需种子密钥就可以扩展噪声对多比特明文的影响，但是并不能平衡噪声对不同比特位的影响，因此使用 CR 映射时，密钥的安全性并没有增加。

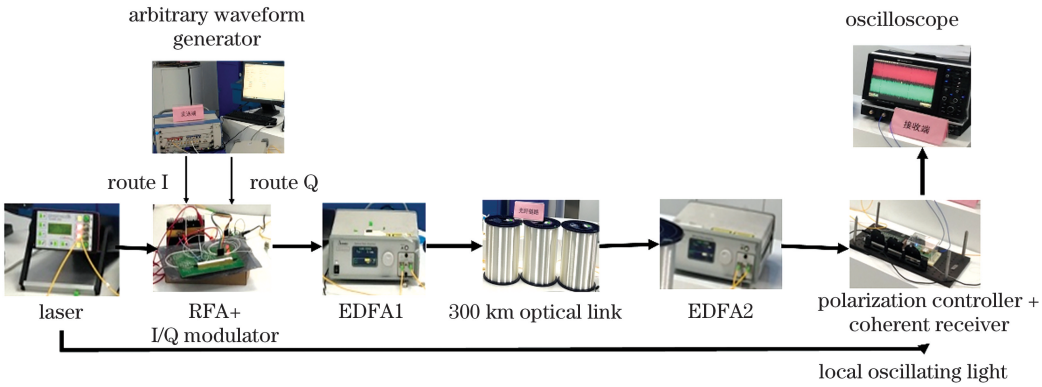
针对密钥分发方案，内生安全光通信主要利用光纤信道的短时相关性和互易性来进行密钥分发，密钥分发方案借助密钥熵、安全性、一致性、随机性、密钥生成率等具体方面来衡量所设计方案的好坏，难点在于无法提取出能够反映信道唯一性、互易性及随机性的密钥序列，以保证攻击者难以准确地识别出该密钥序列。为了解决这一难题，国内几位学者提出了基于生存时间(SLT)、基于单向非对偶任意基变换(ONABT)、基于误码率(BER)环回测量的密钥生成方案[29-31]。这些方案的特点是利用 Y-00 协议、数字信号处理(DSP)、收发两端误码率测量等方法实现长距离(300 km 以上)、高速率(最高 2 Mbit/s)、低成本的经典安全密钥分发，而且这些方案还可以与当前的光传输系统兼容，无需改变节点结构。

在安全编码方面，有学者基于低密度奇偶校验码(LDPC)编码，利用 Cascade 协议进行密钥后处理。实验表明，在 300 km 数字相干光 OFDM 系统中，最终的密钥生成速率可达 352.5 kbit/s，密钥一致性达 100%[32]。该方法省去了不必要的筛选步骤，将保密增强添加到信息协商过程中，大大降低了总体计算量和计算复杂度，提高处理效率，以最小的信息开销达到完全纠正密钥的目的。

在安全检测方面，为提高检测精度和效率，有学者提出一种基于深度学习的窃听检测方案，该方案将眼图、Q 因子、误差向量幅度、光信噪比作为卷积神经网络的训练样本。实验表明，在具有 5%窃光比的 300 km 数字相干光 OFDM 系统中，样本经过 30 次训练后，窃听检测精度可以达 95%[33]。

4.3 内生安全光通信系统实验验证

实验配置如图 9 所示，在长度为 300 km 的标准单模光纤(SSMF)上进行内生安全传输与协商的联合实验。整个系统主要分为两部分：一部分是在近噪区进行密钥协商(双向传输)；另一部分是在远噪区进行安全传输(单向传输)。两部分的过程很相似，在此重点阐述基于误码率进行密钥协商的过程。



RFA: radio frequency amplifier; EDFA: erbium-doped fiber amplifier

图 9 安全传输密钥协商联合系统实物图

Fig. 9 Physical diagram of secure transmission and key negotiation joint system

在发射机处，外腔激光器（ECL）将波长为1550 nm的光束以10 dBm的功率发送到同相/正交（I/Q）调制器。同时，在发射机端的数字信号处理模块中，随机数生成器（PRNG）生成伪随机二进制序列（PRBS）数据。量子噪声流加密后，任意波形发生器（AWG）以10 Gsample/s采样率将I和Q数据转换为电信号，经射频放大器（RFA）放大后，信号被I/Q调制器加载到光载波上。来自I/Q调制器的光信号通过光衰减器（VOA）传输，降低了光功率，从而提高了针对非法接收端Eve的数据安全性。然后，信号由掺铒光纤放大器（EDFA）放大，并通过300 km标准单模光纤传输。接收信号在接收器端由EDFA放大，并由与ECL本振光（OL）结合的相干光接收器检测，然后，通过20 Gsample/s示波器实时捕获检测到的I/Q信号。为了准确地测量BER的波动，实验减小了发射信号的幅度以增加BER值。该实验在两个单独的时隙中测量BER性能，其中一个显示从Alice到Bob的BER性能，另一个则是Bob到Alice。最后，可以使用这两个测量结果获得光纤链路的BER样本，进而通过密钥后处理生成密钥。

首先对传输系统的传输性能进行实验验证，如图10(a)所示，随着传输距离增加，光信号功率不断衰减，为了保证接收机有足够的光功率输入，需要尽量增大发射端EDFA的输出光功率，但这会使其引入过多的自发辐射（ASE）噪声，从而Q因子随之降低。单泵浦EDFA的最大输出功率为13 dBm，双泵浦EDFA最大输出功率为23 dBm。因此发射端采用双泵浦EDFA时可以获得更大的输出光功率。由于单泵浦EDFA噪声系数较小，因此接收端采用单泵浦EDFA以减小噪声。

有必要合理设置EDFA放大功率，使到达接收机的光功率满足解密条件。图10(a)、(b)中以2 dBm为梯度，设置发射端EDFA输出光功率为4 dBm～16 dBm，保持距离300 km，电压450 mV不变。结果表明：随着发射功率的增加，Q因子先增大到峰值后再减小；当输入信号功率为8 dBm时，Q因子达到峰值，并且不再随输入信号功率增加而增加；当功率大于8 dBm时，Q因子逐渐减小。对应地，当输入信号功率为10 dBm时，误码率达到最低值，并且不再随输入信号功率增加而减小；当输入信号功率大于10 dBm时，误码率逐渐增加。这是因为随着EDFA发射功率的增强，光纤非线性效应已成为影响系统性能的主要因素。

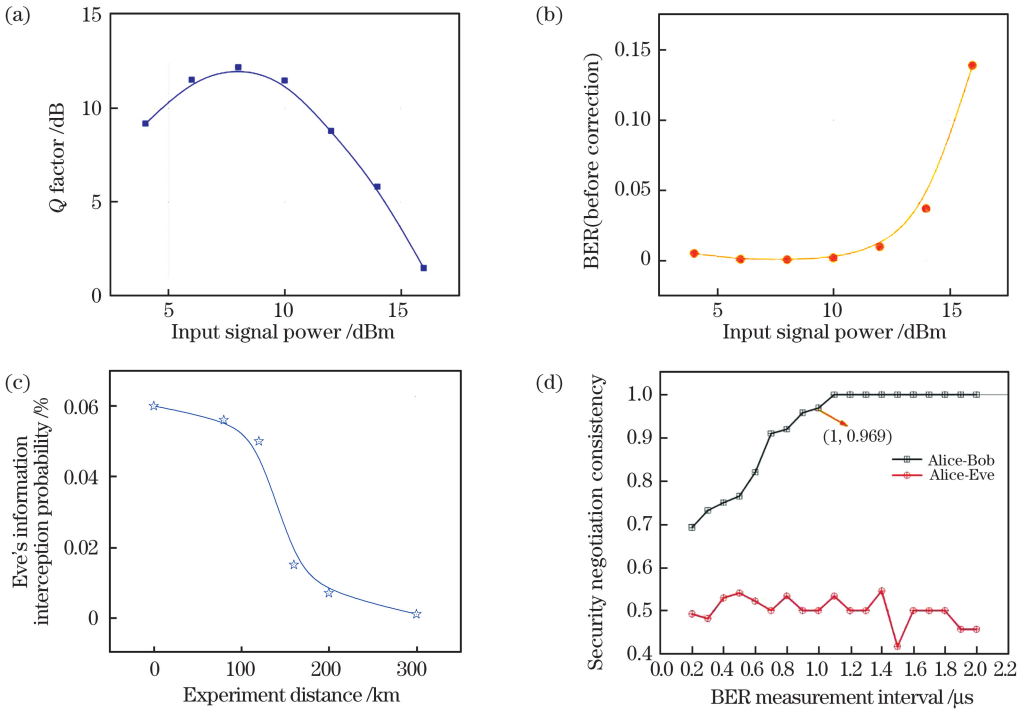


图10 实验结果。(a)输入信号功率对Q因子的影响结果；(b)输入信号功率对误码率的影响结果；(c)信息截获概率与距离的关系；(d)通信方密钥一致性测试结果

Fig. 10 Results of the experiment. (a) Effect of input signal power on Q factor; (b) effect of input signal power on BER; (c) relationship between the probability of information interception and distance; (d) key consistency test results of communication parties

图 10(c)为不同传输条件下系统的安全性能，其中系统的传输速率为 10 Gbit/s，调制格式为 QAM-OFDM，调制方式为相干调制，传输距离分别为 0，80，120，160，200，300 km，非法接收端 Eve 靠近发送端对光纤链路进行窃听，在不同的传输条件下，Eve 的信息截获概率不同。随着传输距离的增加，Eve 的信息截获概率降低，说明光纤引入的非线性使得系统的加密性能增强。

如图 10(d)所示，随着误码测量间隔增加，Alice-Bob 的密钥一致率逐渐增加，接近于 100%，而 Alice-Eve 的密钥一致率一直维持在 50%附近。结果表明，Alice-Bob 和 Alice-Eve 之间的密钥一致率在设置中相差大约 40%～50%。即使 Eve 拥有关于这些系统或特性的信息，也将无法生成与 Alice 和 Bob 相同的密钥，这是因为光纤的非线性分布在光纤的整个长度上。

最后对协商系统的密钥随机性、一致性及安全性进行实验验证。实验中，Alice 和 Bob 生成的一致性种子密钥经过伪随机数发生器生成运行密钥，运行密钥经 NIST SP 800-22 随机性检测标准检测。检测结果如表 2 所示，检测结果概率值小于 0.01 时，则判定序列是非随机的，否则序列是随机的。

表 2 运行密钥随机性检测结果

Table 2 Running key randomness test result

Test item	Pseudo random number generator	Test item	Pseudo random number generator
Frequency	0.735678	Linear complexity	0.292823
Block frequency	0.875266	Sequence	0.903806
Run	0.225167		0.623760
Intra-block longest run	0.665906	Approximate entropy	0.525363
Rank of binary matrix	0.197381	Accumulation	0.540815
Discrete Fourier transform	0.978059		0.847687
Non-overlapping module matching	>0.01117	Random walk	>0.010981
Overlapping module matching	0.196138	Random walk state frequency	>0.152266
General statistics of Maurer	0.948782	Linear complexity	0.292823

5 结 论

调研了 QNSC 的基本原理、关键技术、研究进展及典型应用。在此基础上详细介绍了基于 QNSC 的内生安全光通信系统，包括理论模型、实验验证及性能分析等。然而 QNSC 是一个广阔的研究领域，还有众多问题尚有待解决，例如光通信物理层安全涉及的多种性能评价指标，亟需建立相对完善且实用的物理层安全评价体系。

参 考 文 献

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

[2] Yuen H P. KCQ: a new approach to quantum cryptography I. general principles and key generation [EB/OL]. (2004-07-30)[2020-03-26]. https://arxiv.org/abs/quant-ph/0311061.

[3] Verma P K, El Rifai M, Chan K W C. Multi-photon quantum secure communication [M]. Singapore: Springer, 2019: 90.

[4] Hirota O, Kato K, Shoma M, et al. Quantum key distribution with unconditional security for all optical fiber network[J]. Proceedings of SPIE, 2004, 5161: 320-331.

[5] Kato K, Hirota O. Quantum quadrature amplitude modulation system and its applicability to coherent-state quantum cryptography [J]. Proceedings of SPIE, 2005, 5893: 589303.

[6] Doi Y, Akutsu S, Honda M, et al. 360 km field transmission of 10 Gbit/s stream cipher by quantum noise for optical network [C] //Optical Fiber Communication Conference 2010, March 21-25, San Diego, California. Washington, D.C.: OSA, 2010: OWC4.

[7] Futami F, Tanizawa K, Kato K, et al. 1, 000-km transmission of 1.5-Gb/s Y-00 quantum stream cipher using 4096-level intensity modulation signals [C]//2019 Conference on Lasers and Electro-Optics,

May 5-10, 2019, San Jose, California. Washington, D.C.: OSA, 2019: SW3O.

[8] Tanizawa K, Futami F. Single-channel 48-Gbit/s DP PSK Y-00 quantum stream cipher transmission over 400- and 800-km SSMF[J]. Optics Express, 2019, 27(18): 25357-25363.

[9] Nakazawa M, Yoshida M, Hirooka T, et al. QAM quantum noise stream cipher transmission over 100 km with continuous variable quantum key distribution [J]. IEEE Journal of Quantum Electronics, 2017, 53(4): 1-16.

[10] Nakazawa M, Yoshida M, Hirano T. Secure transmission using QAM quantum noise stream cipher with continuous variable QKD[C]//Optical Fiber Communication Conference 2018, March 11 - 15, 2018, San Diego, California. Washington, D.C.: OSA, 2018: Th3E.2.

[11] 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.

[12] Kato K, Hirota O. Quantum stream cipher: part V. on the optimal modulation scheme and the implementation of deliberate signal randomization [J]. Proceedings of SPIE, 2007, 6710: 67100T.

[13] Kato K. A unified analysis of optical signal modulation formats for quantum enigma cipher[J]. Proceedings of SPIE, 2017, 1040: 104090K.

[14] Yang X K, Zhang J, Li Y J, et al. DFTs-OFDM based quantum noise stream cipher system [J]. Optical Fiber Technology, 2019, 52: 101939.

[15] Sohma M, Hirota O. Masking property of quantum random cipher with phase mask encryption [J]. Quantum Information Processing, 2014, 13(10): 2221-2239.

[16] Hirota O, Kurosawa K. Immunity against correlation attack on quantum stream cipher by Yuen 2000 protocol [J]. Quantum Information Processing, 2007, 6(2): 81-91.

[17] Hirota O. Practical security analysis of a quantum stream cipher by the Yuen 2000 protocol[J]. Physical Review A, 2007, 76(3): 032307.

[18] Shimizu T, Hirota O, Nagasako Y. Running key mapping in a quantum stream cipher by the Yuen 2000 protocol [J]. Physical Review A, 2008, 77(3): 034305.

[19] Lu Y. Research on continuous variable quantum secure communication technology [D]. Shanghai: Shanghai Jiaotong University, 2011: 56.
陆鸢. 连续变量量子保密通信技术研究[D]. 上海: 上海交通大学, 2011: 56.

[20] Futami F, Kato K, Hirota O. A novel transceiver of the Y-00 quantum stream cipher with the randomization technique for optical communication with higher security performance[J]. Proceedings of SPIE, 2016, 9980: 99800O.

[21] Akutsu S, Doi Y, Hosoi T, et al. 192 km relay transmission and HDTV transmission experiments by quantum Yuen-2000 transceiver[J]. AIP Conference Proceedings, 2009, 1110(1): 331.

[22] Futami F, Hirota O. Demonstration of 2.5 Gbit/sec free space optical communication by using Y-00 cipher: toward secure aviation systems [J]. Proceedings of SPIE, 2014, 9202: 92020R.

[23] Hirota O, Ohhata K, Honda M, et al. Experiments of 10 Gbit/sec quantum stream cipher applicable to optical Ethernet and optical satellite link [J]. Proceedings of SPIE, 2009, 7465: 746509.

[24] Zhang J. Technologies and applications of endogenously secure optical communication [J]. Radio Communications Technology, 2019, 45(4): 337-342.
张杰. 内生安全光通信技术及应用[J]. 无线电通信技术, 2019, 45(4): 337-342.

[25] Yang X K, Zhang J, Li Y J, et al. Single-carrier QAM/QNSC and PSK/QNSC transmission systems with bit-resolution limited DACs [J]. Optics Communications, 2019, 445: 29-35.

[26] Wang K, Li Y J, Yang X K, et al. Ciphertext mapping method based on bitwise NOT operation in quantum noise stream cipher [C]//2018 Asia Communications and Photonics Conference (ACP), October 26-29, 2018, Hangzhou, China. New York: IEEE Press, 2018.

[27] Wang K, Zhang J, Li Y J, et al. Multi-bit mapping based on constellation rotation in quantum noise stream cipher[J]. Optics Communications, 2019, 446: 147-155.

[28] Wang K, Li Y J, Zhao Y L, et al. A multi-ring BPSK mapping in quantum noise stream cipher[C]//2019 24th OptoElectronics and Communications Conference (OECC) and 2019 International Conference on Photonics in Switching and Computing (PSC), July 7-11, 2019, Fukuoka, Japan. New York: IEEE Press, 2019.

[29] Lei C, Zhang J, Li Y J, et al. Key distribution based on survival life time with Y-00 protocol in optical

fiber link [C]//2019 24th OptoElectronics and Communications Conference (OECC) and 2019 International Conference on Photonics in Switching and Computing (PSC), July 7-11, 2019, Fukuoka, Japan. New York: IEEE Press, 2019.

[30] Lei C, Zhang J, Li Y J, et al. Long-haul and high-speed key distribution based on one-way non-dual arbitrary basis transformation in optical fiber link [C]//Optical Fiber Communication Conference (OFC) 2020, March 8-12, 2020, San Diego, California. Washington, D.C.: OSA, 2020: W2A.51.

[31] Wang X Q, Zhang J, Li Y J, et al. Secure key distribution system based on optical channel physical features[J]. IEEE Photonics Journal, 2019, 11(6): 1-11.

[32] Tu Z W, Zhang J, Li Y J, et al. Experiment demonstration of physical layer secret key distribution with information reconciliation in digital coherent optical OFDM system [C]//2019 Asia Communications and Photonics Conference (ACP), November 2-5, 2019, Chengdu, Sichuan, China. New York: IEEE Press, 2019.

[33] Liu M, Li Y, Song H, et al. Experimental demonstration of optical fiber eavesdropping detection based on deep learning[C]//2019 Asia Communications and Photonics Conference (ACP), November 2-5, 2019, Chengdu, Sichuan, China. New York: IEEE Press, 2019.