中国激光

一种基于级联调制的高位多进制量子噪声随机加密系统方案研究

王晓虎[1]，蒲涛[1]，郑吉林[1*]，周华[1]，李云坤[2]，刘娟[3]，戴伟[4]

[1]陆军工程大学通信工程学院，江苏 南京 210001；
[2]中国人民解放军31106部队，江苏 南京 210016；
[3]陆军工程大学教研保障中心，江苏 南京 210007；
[4]东部战区总医院卫勤部，江苏 南京 210016

摘要 为避免数模转换器(DAC)在高速率、高分辨率方面的性能限制对量子噪声随机加密系统(QNRC)的影响，同时也为了降低系统的成本，本文提出了一种采用低位DAC级联调制、光域解密、直接检测的灵活多进制解密系统方案，并利用商用仿真软件VPI Transmission Maker Optical System 9.1 (VPI9.1)对所提方案的可行性进行验证，得到了介观相干态功率为－20 dBm、传输距离为100 km、传输速率为10 Gb/s、密文态数目最高可达216－1的QNRC系统的仿真结果。结果表明：低位DAC级联的方式不仅可以大大提高密文态数目，确保最优的系统传输性能，还可以灵活适配多进制传输系统。此外，所提系统方案避免了数模转换器在高速率、高分辨率方面对QNRC系统的影响，同时还显著降低了高位传输系统的成本，为实现QNRC系统的国产化提供了一种解决方案。

关键词 光通信；量子噪声随机加密；低位数模转换器；多进制传输系统

中图分类号 TN918.1 **文献标志码** A **DOI**：10.3788/CJL220863

1 引 言

光纤通信网络凭借其大带宽、长距离的优势，成为现代高速通信传输网络的核心骨干网。目前，光纤通信网络信息的物理层安全问题日益凸显。量子噪声随机加密(QNRC)技术是近年来兴起的一种保密通信技术，该技术同时兼具高安全性和高传输速率，并且可与现有的光纤通信网络和传输设备兼容，具有广阔的发展前景[1-2]。QNRC系统是一种基于量子不可克隆原理和海森堡不确定性原理，利用量子噪声掩盖相邻密文态，对介观相干态伪多进制信号进行加密的光网络抗截获通信系统。该系统于发送端利用共享密钥流对传输信号进行伪多进制调制，接收方使用合法密钥进行解调，从而达到保密通信的目的[3-5]。量子密钥分发(QKD)技术是量子保密技术中的关键技术。量子密钥分发以量子态作为密钥信息的载体，根据密钥分发协议(BB84、B92和E91等)为合法通信双方提供无条件安全的密钥[6-7]，其结合“一次一密”(OTP)加密[8-9]能够实现无条件安全的信息传递。最新研究显示，双场QKD的传输距离超过了830 km，为远距离QNRC提供了重要支撑[10]。

日本玉川大学的Tanizawa团队[11]在QNRC系统领域的研究上领跑全球。该团队于2019年在具有高分辨率、高传输速率任意波形发生器(AWG)的基础上，采用6 bit粗调＋10 bit精调的模式，成功实现了传输速率为20 Gb/s、传输距离为400 km、密文态数目为$2^{17}-1$的QNRC系统。2020年，日本玉川大学的Futami等[12]采用精度为11 bit的数模转换器(DAC)产生多进制模拟信号，利用重叠选择键控(OSK)的方式将明文和经伪随机数生成器(PRNG)产生的运行子密钥将密文信号进行随机性增强，实现了传输速率为1.5 Gb/s、传输距离为1000 km、密文态数目为2048(2^{11})的ISK-QNRC。近几年，国内部分高校也陆续开展了相关研究，如：2019年，北京邮电大学的张杰团队[13]在*Optics Communications*上发表论文，探讨了DAC限制条件下量化噪声与量子噪声对QNRC系统性能的影响；2020年，华中科技大学光学与电子信息研究所实现了传输速率为100 Gb/s、传输距离为100 km、密文态数目为2^{15}的基于强度调制的QNRC系统[14]；2017年，原解放军理工大学的焦海松等[15]对QNRC的安全性进行了定量分析；2020年，陆军工程大学的陈毓凯等[16]提出了基于QPSK-QNRC系统的实验方案，

收稿日期：2022-05-16；**修回日期**：2022-06-21；**录用日期**：2022-06-30；**网络首发日期**：2022-07-10
基金项目：国家自然科学基金(61974165，62071487)
通信作者：*zhengjilinjs@126.com

并将该系统与谭业腾[17]设计的PSK-QNRC系统的性能进行了对比分析。受限于技术及成本控制，基于高速率、高分辨率的DAC实现QNRC系统在实际工程上很难实现。高速率、高分辨率的DAC及模数转换器（ADC）对QNRC系统传输性能的优劣起着至关重要的作用。大容量、高安全性的QNRC系统需要高速率、高位数的伪多进制波形，而该伪多进制波形也需要高速率、高分辨率的DAC。高速率、高分辨率DAC对QNRC系统性能的限制，使得现有QNRC系统的性能仍有很大的提升空间。

综上，迫切需要找到一种特定的手段，绕开高速率、高分辨率DAC的限制，为未来QNRC系统的实用化提供可能。在粗调＋精调思路的启发下，陆军工程大学的谭业腾等[18]提出了多级级联的PSK-QNRC系统，并对该系统进行了详细全面的仿真分析与可行性验证。陆军工程大学的李云坤等[19]基于并联强度调制的方案实现了密文态数目为$2^{10}-1$的ISK-QNRC实验系统，并对其进行了仿真论证；该方案利用粗调＋精调的模式，成功绕开了高速率、高分辨率DAC，实现了1000 km的低误码传输。然而，粗调＋精调模式仍然采用的是高位AWG，其价格昂贵且难以采购。传统的级联PSK-QNRC系统在密文态数目为$2^{12}-1$或更高位传输时，由于相位变化量极小，对相位调制器驱动电压的控制需精确至微伏甚至是纳伏，难以实现，故其在实际工程应用中存在一定的位数极限。

为有效绕开高分辨率、高速率DAC，同时突破传统级联PSK-QNRC系统的位数极限，本课题组基于国内现有的DAC器件水平，同时充分考虑了成本控制，基于VPI Transmission Maker Optical System 9.1（VPI9.1）进行新型QNRC系统的仿真设计。在收发端各利用4个4 bit分辨率的DAC与各DAC相对应的相位调制器通过独立调制的方式调制信息，在时延匹配后进行级联，实现了介观相干态功率为－20 dBm、传输距离为100 km、最高密文态数目为$2^{16}-1$的基于级联调制的高位量子噪声随机加密系统。本方案可以有效突破传统PSK-QNRC系统的传输位数极限，灵活适配多进制传输系统，且绕开了国外高位、高速率DAC技术的垄断，所需元器件参数均立足于国产可替代化水平，降低了工程实现成本。另外，本方案还可以适配现有的多进制传输系统，适配多进制传输系统对于QNRC来说具有重要的现实意义。国内外多项研究结果表明，多进制传输系统在通信传输方面具有更强的系统可靠性，在通信对抗方面具有更好的抗截获能力[20-21]。本文主要内容如下：首先简单阐释了Yuen2000（Y-00）协议对PSK-QNRC的加密原理，接着利用商业仿真软件VPI9.1对所提ADC级联调制方案以及多进制传输解密进行可行性验证，最后在仿真结果的支持下研究了接收光功率、解密进制数等因素对系统传输性能的影响。

2　基本原理

2.1　PSK Y-00协议加密原理

QNRC技术是一种利用介观相干态不可避免且不可克隆的量子噪声对密文信号进行掩盖的物理层安全技术，Y-00协议是QNRC系统的基本加密协议。Y-00协议加密流程的基本思路如图1所示，收发端（Alice和Bob）共享一个无条件安全的种子密钥K，其可能来源于QKD系统。双方利用密钥生成模块（ENC）将种子密钥序列K扩展为运行密钥序列，将运行密钥序列以若干比特作为一个子密钥符号u，逐比特地加密明文数据x，加密映射公式[22]为

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

式中：Pol(•)为奇偶性函数，奇数取1，偶数取0；$|u|$为子密钥长度，即$2^{|u|}$为基态的数目，且相邻的密文符号承载不同的明文数据x。利用所得的密文符号对衰减至介观相干态的相位参量进行调制，得到密文量子态$\Psi(m)$，密文量子态进入信道传输；合法接收方（Bob）通过运行子密钥，基于映射关系将原有的密集多进制

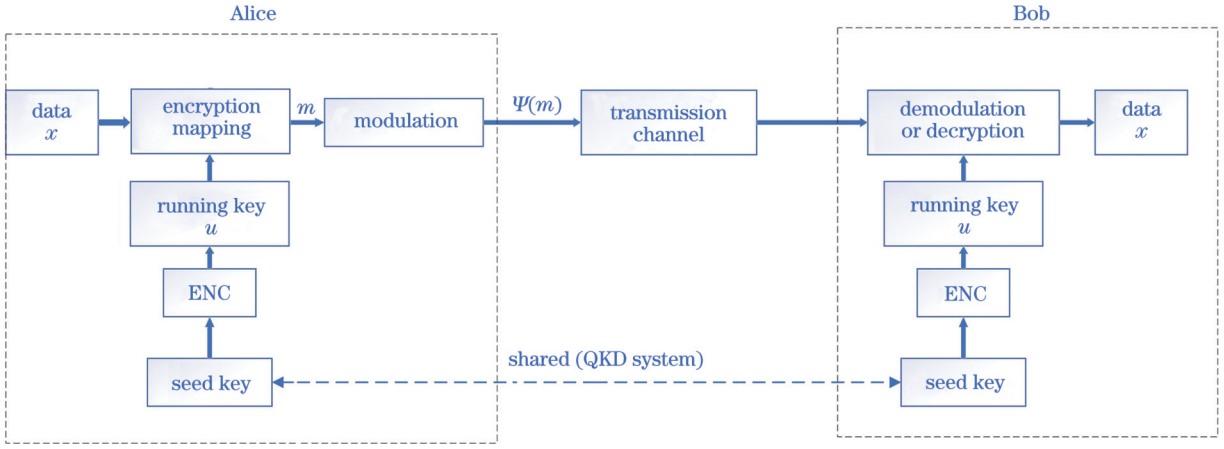

图1　Y-00协议加密流程框图

Fig. 1　Diagram of Y-00 protocol encryption process

密文量子态解调为原传输密文，再经过进一步解密得到原有的明文数据x[12]。

在PSK-QNRC系统中，伪多进制密文信号通过相位调制器进行调制，输出端相干态为$\left|\Psi(m)\right\rangle=\alpha\exp\left(\mathrm{j}m\pi M_{\mathrm{b}}\right)$，$m=0\sim M-1$（$\alpha$为相干态幅度，$M_{\mathrm{b}}$为基态数目，$M=2M_{\mathrm{b}}$），$m/M_{\mathrm{b}}=V_{\mathrm{d}}/V_{\pi}$，$V_{\pi}$为调制器的半波电压，$V_{\mathrm{d}}$为驱动电压。在PSK-QNRC系统中，不同的密文态具有不同的相位，每一对基态的两种密文态的相位之差为π，因此接收端即合法接收方通过正确地运行子密钥可以找到对应的基态，从而将密文态伪多进制恢复成二进制信号。如图2所示，所有密文态对应的相位均匀分布在单位圆上，它们代表的明文交替排列，相位噪声可以对相邻密文态进行掩盖，拥有运行子密钥的合法接收方只需要区分两个相位差为π的密文量子态，就可以根据映射关系获得准确的明文信号，而非法窃听方无法获得准确的量子态，从而无法获得密钥及数据信息[23]。

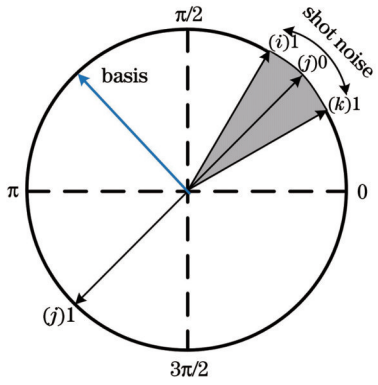

图2　PSK-QNRC示意图

Fig. 2　Schematic of PSK-QNRC

2.2　级联调制的高位QNRC传输方案

如图3所示，Alice于发送端将12位运行子密钥与n（若$n<4$，只需在其前端置$(4-n)$位0即可）位明文信号进行逐比特加密映射，其中第一个4 bit DAC用于调制第一个相位调制器（PM1），第二个4 bit DAC用于调制第二个相位调制器（PM2），以此类推。4个相位调制器（PM）之间使用100 ps延时线相连，对应光信号的相位改变量分别为π、π/2、π/4、π/8，利用光衰减器将调制好的级联信号衰减至介观相干态（功率为−20 dBm）后进入传输链路。接收端同理，PM5对应输入比特位置“0”，承载了运行子密钥解密信息的光信号作为相干解调的参考光（LO），经光纤传输和色散补偿的密文信号作为相干解调的信号光（SIG），两路光信号进行时延匹配后同时进入相干接收机解密。相干接收机的输出是同相（I）支路和正交（Q）支路，I、Q支路的电信号进入实时示波器，实时示波器对I、Q支路的电信号作相位估计，根据相位估计的结果即可进行误码率估算。

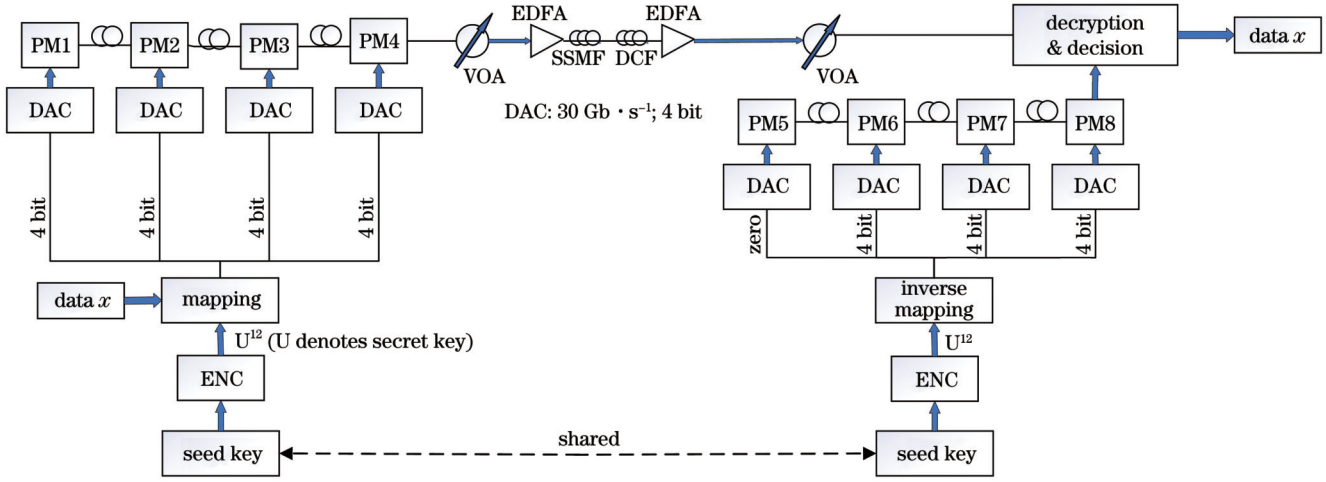

图3　级联调制的高位PSK-QNRC实现方案框图（VOA：可调光衰减器；EDFA：掺铒光纤放大器；SSMF：标准单模光纤；DCF：色散补偿光纤；PM：相位调制器）

Fig. 3　Diagram of high-order digit cascaded PSK-QNRC realization scheme (VOA: variable optical attenuator; EDFA: erbium-doped fiber amplifier; SSMF: standard single mode fiber; DCF: dispersion compensation fiber; PM: phase modulator)

接下来，对该方案Y-00密文信号的相位调制与解调过程进行进一步说明：以（1+12）二进制明文系统方案为例，在发送端，利用4个串联的相位调制器产生M进制的Y-00密文信号，各相位调制器可以产生的相移量为

$$\varphi_{\mathrm{PM}i}=\frac{2^{i}\pi}{M},\ i=1,2,3,4。\tag{2}$$

因此，光载波经过4个串联的相位调制器后产生的总相移量为

$$\varphi=y_1\varphi_{\mathrm{PM1}}+y_2\varphi_{\mathrm{PM2}}+y_3\varphi_{\mathrm{PM3}}+y_4\varphi_{\mathrm{PM4}},\tag{3}$$

式中：y_1、y_2、y_3、y_4分别为4个相位调制器的调制信号，$y_1,y_2,y_3,y_4\in[0,1]$。同理，在接收端采用4个相位调制器进行串联，对M进制的Y-00密文信号进行解密。各相位调制器产生的相移量为

$$\varphi_{\mathrm{PM}j}=\frac{2^{j}\pi}{M},\ j=1,2,3,4。\tag{4}$$

PM5输入的信号置“0”，即$z_1=0$，因此，解密信号经过4个串联相位调制器后产生的相移总量为

$$\varphi'=0\cdot\varphi'_{\mathrm{PM5}}+z_2\varphi'_{\mathrm{PM6}}+z_3\varphi'_{\mathrm{PM7}}+z_4\varphi'_{\mathrm{PM8}},\tag{5}$$

式中：z_1、z_2、z_3、z_4分别为4个相位调制器的调制信号，$z_1,z_2,z_3,z_4\in[0,1]$。假设合法发送方(Alice)发送的密文信号为m或$m+M_{\mathrm{b}}$，信号的基态为m，则发送端相位调制器的总相移量为$\frac{2m\pi}{M}$或$\frac{2(m+M_{\mathrm{b}})\pi}{M}$。接收端相位调制器的总相移量为$\frac{2m\pi}{M}$，经过光域解密和相干解调后，光载波的相位将恢复为0或π，故而发送端的多进制密文信号经过解密后将恢复为二进制信号。

本文采用的实验方案是从物理端对原本的QNRC系统进行改造，收发端各利用4个低位DAC进行级联，并未改变其传输明文及密钥的本质。量子噪声(相位不确定度)取决于介观相干态信号的功率水平，其数学表达式为

$$\Delta\varphi=\pm\frac{1}{2\sqrt{\bar{N}}}=\pm\frac{1}{2|\alpha|},\tag{6}$$

式中：$\sqrt{\bar{N}}$为量子态的平均光子数；$|\alpha|$为量子态的幅度。相邻量子态的相位差取决于基态的数目，其数学表达式为

$$\delta\varphi=\frac{2\pi}{M}=\frac{\pi}{M_{\mathrm{b}}}。\tag{7}$$

因此，量子噪声掩盖的密文量子态数目(NMS)为

$$N_s=\frac{\Delta\varphi}{\delta\varphi}=\frac{M_{\mathrm{b}}}{\pi|\alpha|}=\frac{M_{\mathrm{b}}}{\pi}\sqrt{\frac{Rhv_0}{P_0}},\tag{8}$$

式中：R、h、v_0、P_0分别为传输速率、普朗克常数、光信号频率、介观态平均光功率。当NMS大于1时，系统具备安全性[24]。在物理本质上，只有当量子不确定度大于相邻相位差时，即$\Delta\varphi>\delta\varphi$时，QNRC才有可能保证安全[25]。

如图4所示，本课题组依照表1所示参数设置搭建了基于级联相位调制的高位PSK-QNRC系统仿真平台。为保证解密为多进制信号时信号眼图清晰可辨，提升传输性能，此系统应当选取窄线宽激光器。在发送端，16 bit密文信号分为4×4 bit后进入对应的分辨率为4 bit、传输速率为30 Gb/s的DAC，各DAC之间利用100 ps延时线进行连接，级联后用光衰减器将信号衰减至介观相干态，利用光放大器将介观信号放大，同时引入噪声，以增强安全性。在接收端，采用同样的方式将运行子密钥加载到调制器上，两路光信号进入相干接收机进行解密，并与原本的传输信号进行误码率比对分析。

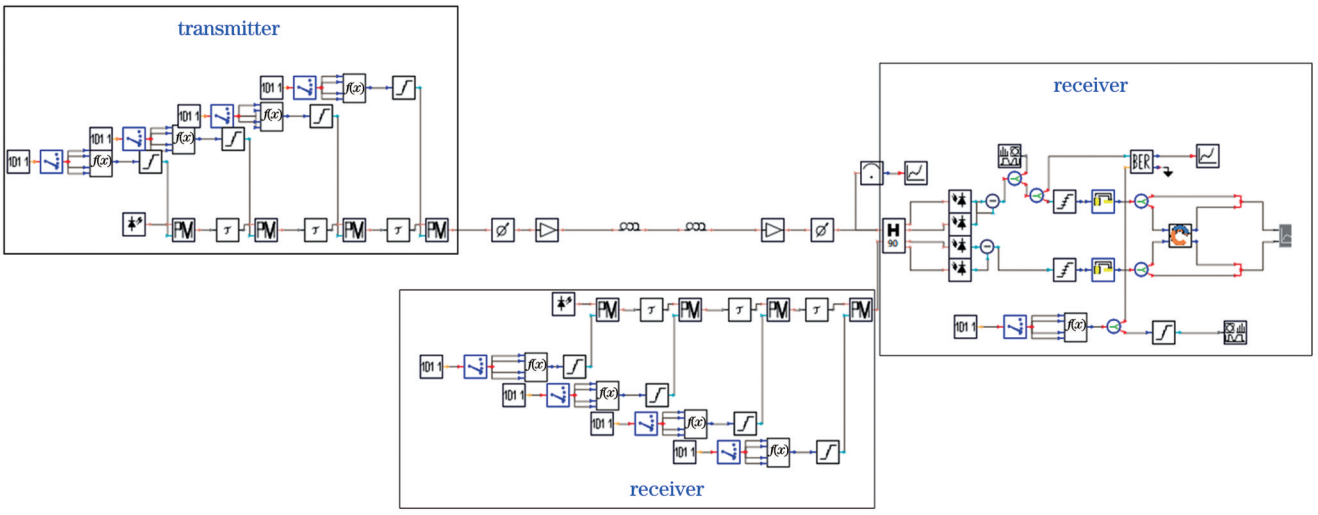

图4　级联高位PSK-QNRC系统仿真框图

Fig. 4　Simulation high-order digit diagram of cascaded PSK-QNRC system

表1　参数设置

Table 1　Configuration of parameters

Parameter	Value	Parameter	Value
Length of ciphertext /bit	4+4+4+4	Attenuation /(dB·km^{-1})	0.2
Bit rate /(Gb·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
Attenuation /dBm	20	Length of DCF /km	16.67
Resolution of DAC	4	DAC sampling rate /(Gb·s^{-1})	30
Delay time of delay signal /ps	100	Linewidth of laser /Hz	10^3

最终得到了各进制解密后信号的眼图和波形图，如图 5 所示。图 5(a)和图 5(b)分别展示了未经解密的引入噪声后的 Y-00 加密信号的眼图和波形图，信号无法判决；图 5(c)展示了在接收光功率为 −10 dBm 条件下传输二进制信号时的解密波形图，图 5(d)展示了其对应的眼图。可以发现，密文信号经过长距离传输并解密之后，信号重新恢复为二进制信号，眼图清晰可辨。合法的接收方能够准确获得明文信息，而非法的窃听方不能从加密信号中准确地获得信息。

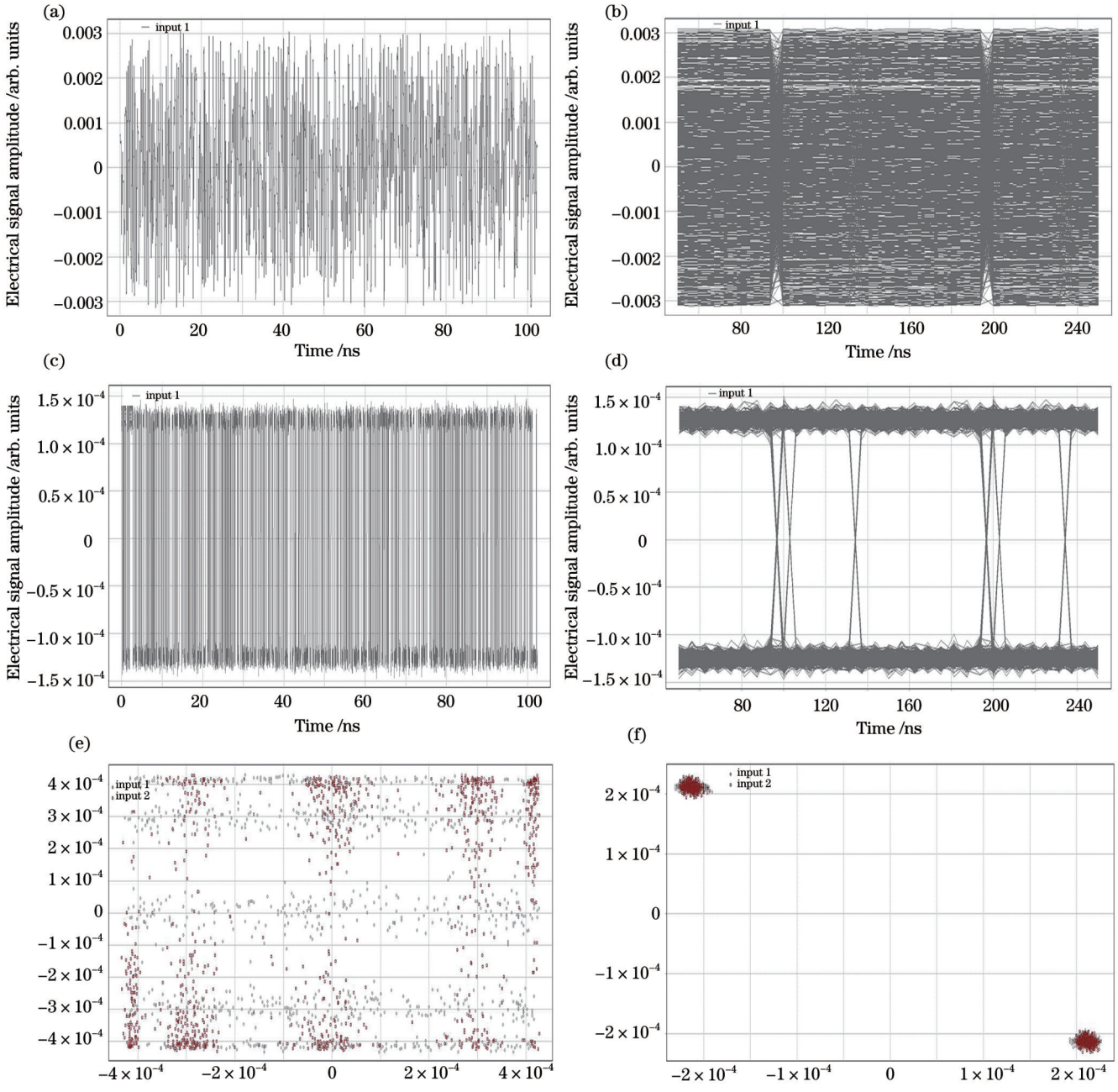

图 5 二进制方案下的仿真图。(a)解密前的波形图；(b)解密前的眼图；(c)解密后的波形图；(d)解密后的眼图；(e)解密前的星座图；(f)解密后的星座图

Fig. 5 Simulation diagrams under binary scheme. (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; (e) constellation diagram before decryption; (f) constellation diagram after decryption

3 分析与讨论

3.1 二进制明文下方案性能的对比

在 $2^{16}-1$ 密文态下，本方案以及采用 16 bit 高速率高分辨率 DAC 的方案(以下简称“原方案”)的误码率(B_{er})随接收光功率变化的曲线如图 6 所示。固定介观相干态功率为 −20 dBm，传输距离为 100 km，传输速率为 10 Gb/s。由误码率曲线可以看出，随着接收光功率增加，光信噪比增大，系统的误码率降低。以公认的无误码传输的误码率 10^{-9} 为基准，本方案实现无误码

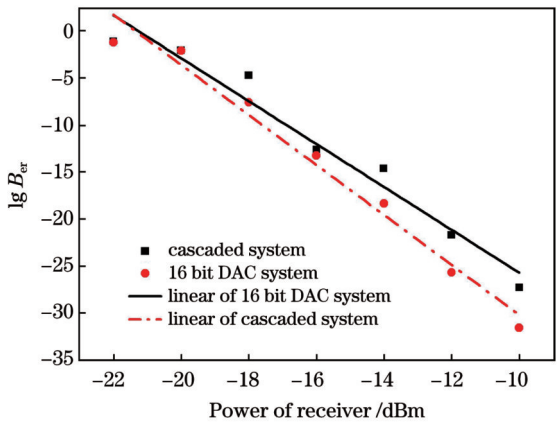

图 6 传输性能对比

Fig. 6 Transmission performance comparison

传输相比原方案需要付出的功率代价为 0.84 dBm。换而言之，在不使用昂贵的高速率高分辨率 DAC 的条件下，采用本方案仅需付出 0.84 dBm 的功率代价即可实现无误码传输。本方案采用的 30 Gb/s 传输速率、4 bit 分辨率的 DAC 在国内已经实现了技术突破，早在 2018 年，中国科学院微电子研究所就已经成功研制出了采样速率为 30 Gb/s、分辨率为 6 bit 的 DAC[26]。本方案可以在保证系统传输性能的前提下，绕开高速率高分辨率 DAC 对 QNRC 系统高位传输系统性能的限制，节约了大量工程铺设成本。

3.2 各进制解密系统下的安全性评估

一般情况下，NMS 被认为是 QNRC 系统安全性的一个典型指标，NMS 越大，量子噪声能够掩盖的量子态的数目也就越多，系统的安全性水平也就越高。本方案采用 4 个 DAC 级联生成对应二进制方案为 13 bit、四进制方案为 14 bit、八进制方案为 15 bit、十六进制方案为 16 bit 的伪多进制信号，故 $M_{b1}=2048$，$M_{b2}=4096$，$M_{b3}=8192$，$M_{b4}=16384$。NMS 指标与系统介观相干态功率之间的关系如图 7 所示。

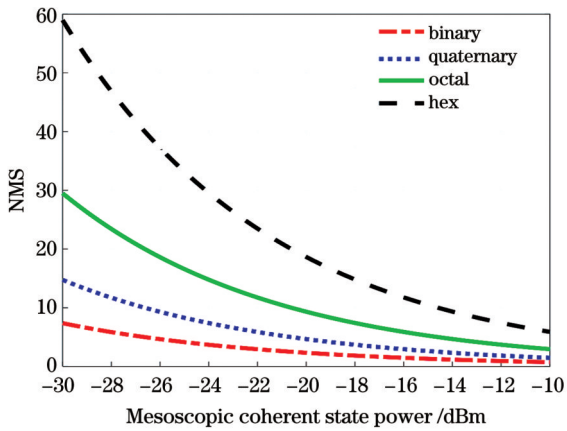

图 7 各方案下 NMS 指标与系统介观相干态功率之间的关系

Fig. 7 Relationship between NMS (number of quantum state) index and system mesoscopic coherent state power under each scheme

N_σ 是一个与介观态平均光功率相关的指标，介观态平均光功率越小，N_σ 越大。传输过程中需要加入 EDFA 来补偿链路中的功率损耗，EDFA 会产生自发辐射（ASE）噪声，而介观态平均光功率越小，接收机接收到的光信号的信噪比就会越低，系统的传输性能也就越差。因此，找到一个合适的介观态平均光功率是平衡安全性和合法用户传输性能的关键。由图 7 可得本方案取介观态平均光功率 $P_0=-20$ dBm 时，二进制、四进制、八进制、十六进制方案解密下的 NMS 值分别为 2.33、4.66、9.33、18.66，可以满足系统在各进制解密下的安全性要求。

3.3 多进制解密系统下方案的性能

本方案的第二个优势在于可以灵活适配多进制传输系统，且无须改变系统自身的结构，仅需将首个 DAC（对应相位调制器的相位改变量为 π）输入的四位信号的前端置对应个数的 0 即可（如二进制系统输入 000X，四进制系统输入 00XX）。对比方案固定密钥为 12 位，传输速率为 10 Gb/s，介观态平均光功率为 −20 dBm，传输距离为 100 km，接收端光功率为 −10 dBm。图 8 展示了四进制方案下的仿真图。由解密后的波形图、眼图、星座图可以看到，解密后的信号重新恢复为对应的各进制信号，眼图清晰可见，合法接收方根据解密信号进行处理后可获得对应的各进制原始明文信号，而非法接收端不能从加密信号中获取明文信息。

由于放大器产生了越来越多的 ASE 噪声，再加上激光器线宽的限制、超长距离色散补偿、多进制解密电平干扰、系统判决电平等诸多因素的影响，本方案在传输距离为 100 km 时对多进制信号的解密性能较为一般，后续计划采用色散补偿算法、离线数字信号处理（DSP）等方法进行改进。

目前仅对该方案下的解密多进制系统的可行性进行验证。图 9 展示了 10 km 传输距离下该方案对应各进制传输的系统误码率曲线图。由测量结果可知，本方案解密多进制信号时，适配各进制系统的性能差距较大。二进制传输系统仍然是首选。适配二进制传输系统时，该方案在接收端光功率大于 −12.74 dBm 时可以实现无误码传输；在适配四进制传输系统时，接收端光功率在大于 −10.12 dBm 时可以实现无误码传输；在适配八进制与十六进制系统时，接收端光功率均需大于 −10 dBm。在码元速率（传码率）相同的条件下，多进制传输系统可以提高信息速率（传信率），增大系统的频带利用率。在信息速率相同的条件下，多进制传输系统还可以降低码元速率，提高传输的可靠性。未来若能将 QNRC 系统适配于多进制扩频通信传输系统，还可以大大增强传输系统的抗干扰能力与保密性。

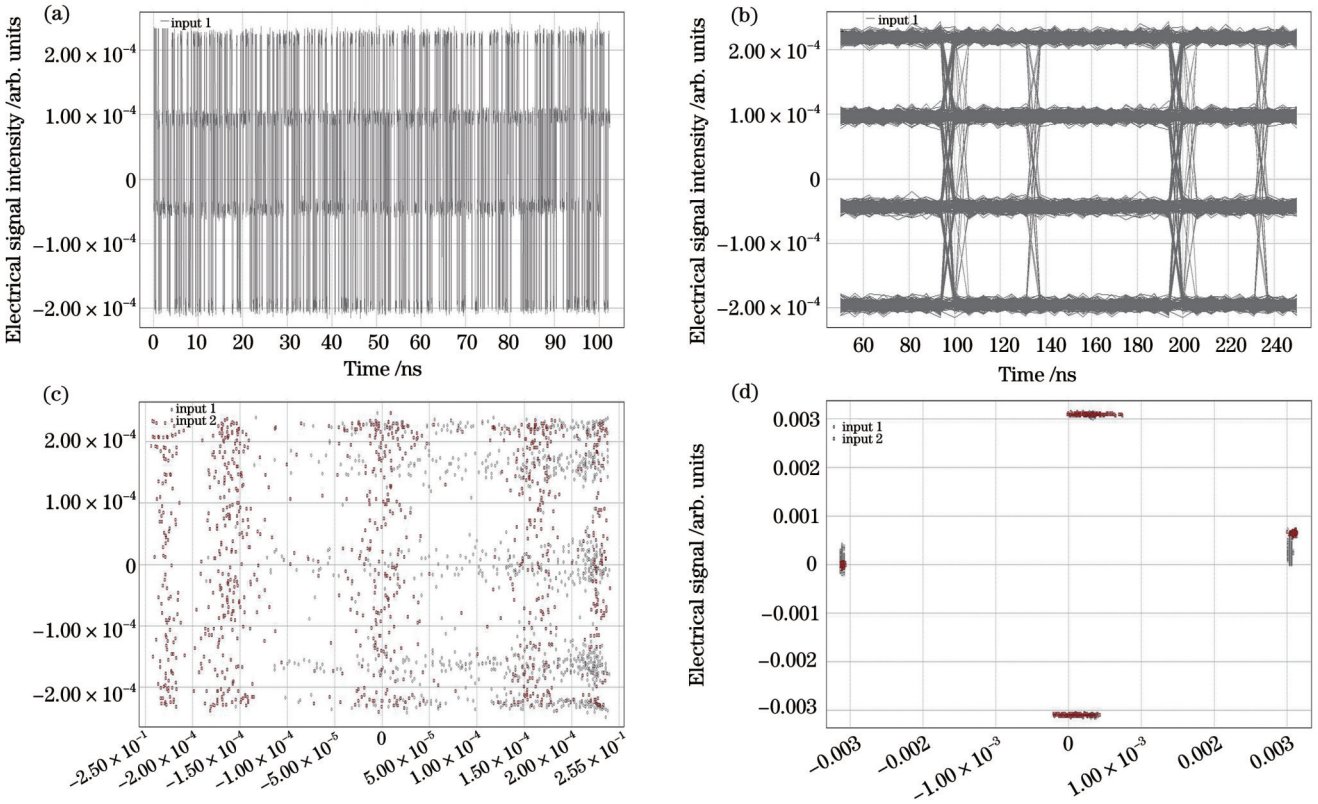

图 8　四进制方案下的仿真图。(a)解密后的波形图;(b)解密后的眼图;(c)解密前的星座图;(d)解密后的星座图

Fig. 8　Simulation diagrams under quaternary scheme. (a) Waveform of signal after decryption; (b) eye diagram of signal after decryption; (c) constellation diagram of signal before decryption; (d) constellation diagram of signal after decryption

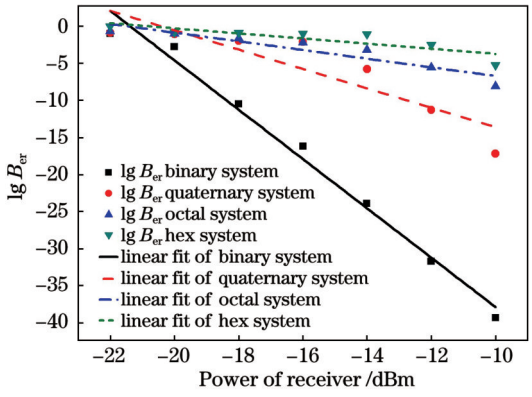

图 9　各方案的传输性能对比

Fig. 9　Transmission performance comparison of each scheme

4　结　　论

以解决高速率、高分辨率 DAC 对 QNRC 系统性能的限制为出发点,采用低位 DAC 级联调制的方案来设计高位 QNRC 传输系统,降低了成本代价,突破了级联 PSK-QNRC 实际传输位数的极限,同时该方法还可以适配多进制传输系统。将所提方案与传统的利用 16 bit 高速率、高分辨率 DAC 的方案进行传输性能对比分析,计算功率代价,验证了本方案的可行性。此外,将本方案适配至多进制传输系统,对各多进制传输下的系统性能进行比较分析,阐释了未来 QNRC 系统适配多进制传输系统的可行性。本方案所用的分辨率为 4 bit、传输速率为 30 Gb/s 的 DAC 在国内已实现量产,为绕开国外高速率高分辨率 DAC,实现国产可替代化,降低工程成本提供了一种可行方案。另外,本文传输最高密文态位数绝不仅仅限于 16 位,如实际传输需要,可在收发端末尾继续进行级联,或采用更高位数的 DAC 级联,都可以提升本方案的密文态传输位数。

参　考　文　献

[1] Kitayama K I, Sasaki M, Araki S, et al. Security in photonic networks: threats and security enhancement[J]. Journal of Lightwave Technology, 2011, 29(21): 3210-3222.

[2] Fok M P, Wang Z X, Deng Y H, et al. Optical layer security in fiber-optic networks[J]. IEEE Transactions on Information Forensics and Security, 2011, 6(3): 725-736.

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

[4] 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.
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.

[5] Yuen H P. KCQ: a new approach to quantum cryptography I. General principles and key generation[EB/OL]. (2003-11-10)[2022-02-10]. https://arxiv.org/abs/quant-ph/0311061.

[6] Lo H K, Chau H F. Unconditional security of quantum key distribution over arbitrarily long distances[J]. Science, 1999, 283(5410): 2050-2056.

[7] Scarani V, Bechmann-Pasquinucci H, Cerf N J, et al. The security of practical quantum key distribution[J]. Reviews of Modern Physics, 2009, 81(3): 1301-1350.

[8] Surhone L M, Tennoe M T, Henssonow S F. One-time pad[M].

Mauritius: Betascript Publishing, 2013.
[9] Bienfang J C, Mink A, Hershman B J, et al. Quantum generated one-time-pad encryption with 1.25 Gbps clock synchronization[C]// OFC/NFOEC Technical Digest. Optical Fiber Communication Conference, March 6-11, 2005, Anaheim, CA, USA. New York: IEEE Press, 2005.
[10] Wang S, Yin Z Q, He D Y, et al. Twin-field quantum key distribution over 830-km fibre[J]. Nature Photonics, 2022, 16(2): 154-161.
[11] 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.
[12] 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.
[13] 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.
[14] 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.
[15] Jiao H S, Pu T, Zheng J L, 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.
[16] 陈毓锴, 郑吉林, 焦海松, 等. 正交相移键控量子噪声随机加密系统的安全性研究[J]. 激光与光电子学进展, 2020, 57(17): 170609.
Chen Y K, Zheng J L, Jiao H S, et al. Analysis on security of quadrature phase shift keying quantum-noise randomized cipher system[J]. Laser & Optoelectronics Progress, 2020, 57(17): 170609.
[17] 谭业腾. 抗截获通信技术研究及其物理层安全性评估[D]. 南京: 中国人民解放军陆军工程大学, 2020.
Tan Y T. Research on anti-interception communication technology and evaluation of the physical-layer security[D]. Nanjing: Army Engineering University of PLA, 2020.
[18] Tan Y T, Pu T, Zheng J L, et al. A novel realization of PSK quantum-noise randomized cipher system based on series structure of multiple phase modulators[C]//2020 International Conference on Wireless Communications and Signal Processing (WCSP), October 21-23, 2020, Nanjing, China. New York: IEEE Press, 2020: 316-320.
[19] 李云坤, 蒲涛, 郑吉林, 等. 基于并联强度调制的量子噪声随机加密实现方案研究[J]. 中国激光, 2021, 48(17): 1706002.
Li Y K, Pu T, Zheng J L, et al. Realization scheme of quantum noise randomized cypher based on parallel intensity modulation[J]. Chinese Journal of Lasers, 2021, 48(17): 1706002.
[20] 崔永, 刘旭光, 王俊花, 等. 多进制扩频传输系统性能分析[C]// 第七届全国信号和智能信息处理与应用学术会议会刊. 北京: 中国高科技产业化研究会, 2013: 192-195.
Cui Y, Liu X G, Wang J H, et al. Performance analysis of multi-ary spread spectrum transmission system[C]//Proceedings of the Seventh National Conference on Signal and Intelligent Information Processing and Application. Beijing: China High-Tech Industrialization Association, 2013: 192-195.
[21] 黄丽. 高速光通信中多进制调制格式传输性能研究[D]. 聊城: 聊城大学, 2014.
Huang L. Transmission performance research of multi-band modulation format in high-speed optical communication[D]. Liaocheng: Liaocheng University, 2014.
[22] Tanizawa K, Futami K. 2^{14} intensity-level 10-Gbaud Y-00 quantum stream cipher enabled by coarse-to-fine modulation[J]. IEEE Photonics Technology Letters, 2018, 30(22): 1987-1990.
[23] Banwell T, Toliver P, Young J C, et al. High data rate quantum noise protected encryption over long distances[EB/OL]. [2022-02-10]. https://ieeexplore.ieee.org/document/1605716/citations#citations.
[24] Barbosa G A, Corndorf E, Kumar P, et al. Secure communication using mesoscopic coherent states[J]. Physical Review Letters, 2003, 90(22): 227901.
[25] 焦海松. 基于量子噪声随机加密的介观态抗截获通信研究及其物理层安全性评估[D]. 南京: 中国人民解放军陆军工程大学, 2018.
Jiao H S. Research on mesoscopic state anti-interception communication based on quantum noise random encryption and its physical layer security evaluation[D]. Nanjing: Army Engineering University of PLA, 2018.
[26] 中国科学院微电子研究所. 微电子所成功研制 30 Gsps 超高速数据转换器[EB/OL]. (2016-05-09)[2022-02-01]. https://www.cas.cn/syky/201605/t20160509_4555994.shtml.
Institute of Microelectronics of the Chinese Academy of Sciences. Institute of microelectronics successfully developed 30 Gsps ultra high speed data converter[EB/OL]. (2016-05-09) [2022-02-01]. https://www.cas.cn/syky/201605/t20160509_4555994.shtml.

High-Bit Multi-Ary Quantum Noise Random Encryption System Based on Cascade Modulation

Wang Xiaohu[1], Pu Tao[1], Zheng Jilin[1*], Zhou Hua[1], Li Yunkun[1], Liu Juan[2], Dai Wei[3]

[1]*College of Communication Engineering, Army Engineering University of PLA, Nanjing* 210001, *Jiangsu, China*;
[2]*PLA of* 31106, *Nanjing* 210016, *Jiangsu, China*;
[3]*Teaching and Research Support Center, Army Engineering University of PLA, Nanjing* 210007, *Jiangsu, China*;
[4]*Department of Health Services, General Hospital of Eastern Theater Command, Nanjing* 210016, *Jiangsu, China*

Abstract

Objective A large-capacity, high-security quantum noise random cryption (QNRC) system requires high-speed, high-resolution pseudo-multi-ary signal waveforms. However, the generation of pseudo-multi-ary signal waveforms requires a high-speed, high-resolution digital-analog converter/analog-to-digital converter (DAC/ADC). Therefore, a high-speed, high-resolution DAC/ADC plays a crucial role in the performance of QNRC systems. However, owing to the performance limitations of the current high-speed, high-resolution DAC/ADC, the performance of the QNRC system is limited. Our suggested approach is motivated by the need to utilize a new method based on low speed and low resolution to avoid the usage of high-speed, high-resolution DAC in the QNRC system, hence eliminating the performance constraint of QNRC systems owing to the DAC bottleneck. Therefore, the potential of

QNRC systems can be fully evaluated while also lowering the system cost.

Methods In this study, a flexible multi-ary PSK-QNRC system based on a low-speed, low-resolution DAC combined with cascaded phase modulators is proposed. The proposed system is optical domain decryption based on coherent detection, which is simple and easy to implement. At the transmitter of the system, the encryption mapping of a 12 bit running sub-key with an n bit plaintext signal is performed on a bit-by-bit basis (if $n<4$, we only need to place $(4-n)$ digits with "0" in front of them), where the first group of four-bit-DAC is used to modulate the first phase modulator, the second group of four-bit-DAC is used to modulate the second phase modulator, and so on. Four phase modulators are used in our experimental system, which are connected by 100 ps delay lines. The cascaded modulated signal output is attenuated to a mesoscopic coherent state, which has a power of −20 dBm, by an optical attenuator and then sent to the transmission link of the PSK-QNRC system. At the receiver end, the optical signal carrying the decryption information of the running sub-key is used as the reference light (LO, local oscillator) for coherent demodulation, and the ciphertext signal transmitted through a span of the optical fiber with dispersion compensation is used as the signal light (SIG) for coherent demodulation. These two optical signals are then simultaneously sent to the coherent receiver for decryption after time-delay matching. The output signals from the coherent receiver include an in-phase branch (I) signal and a quadrature branch (Q) signal. The I and Q branch signals are then sent to a real-time oscilloscope, where signal phase estimation is performed. Finally, bit error rate estimation is performed based on the results of the signal phase estimation. Through theoretical and experimental analyses of the PSK-QNRC encryption system, the feasibility of the proposed scheme for a large-capacity, long-distance quantum-noise random-encryption transmission system is verified.

Results and Discussions To evaluate the proposed scheme, we established an experimental optical PSK-QNRC system (Fig. 3) and a corresponding computer simulation system based on VPI9.1 software (Fig. 4). All the parameter configurations are listed in Table 1. Taking the transmission of the binary plaintext signal (1+12) as an example, the simulation results are shown in Fig. 5. After the ciphertext signal is transmitted and decrypted over a long distance, the signal is restored to a binary signal, and a clear eye diagram is obtained. A legitimate receiver can accurately obtain the plaintext information, whereas an illegal eavesdropper cannot obtain the transmitted signals from the encrypted signal. We discussed and analyzed the performance of the proposed scheme and compared it with a traditional scheme using high-speed and high-resolution ADC/DAC under binary plaintext. Additionally, we analyzed the security performance of the proposed system under binary and multi-ary decryption. The system transmission performance of the proposed scheme is analyzed under a multi-ary decryption setting and compared with the traditional scheme. Figure 6 shows the power penalty comparison curve between this scheme and the 16 bit high-speed, high-resolution DAC scheme under a binary plaintext setting. The results show that the proposed system can retain the performance of the traditional scheme while avoiding the performance limits of the high-speed QNRC transmission system imposed by the DAC resolution limits and can significantly reduce the system cost. Figure 7 shows the evaluation results of the system's security performance. It can be clearly observed that the NMS (number of quantum state) values under the binary decryption and multi-ary decryption schemes (where 4-ary, 6-ary, and 8-ary are considered) are 2.33, 4.66, 9.33, and 18.66, respectively, which can meet the security performance requirements of the system in both binary and multi-ary decryption settings. Figure 8 shows the time-domain waveforms, eye diagrams, and constellation diagrams of the decrypted signals when the plaintext is quaternary. It can be observed that after decryption, both the binary and multi-ary signals are successfully recovered, and the eye diagram is clearly visible. A legitimate receiver can obtain the corresponding original plaintext signal under each condition after signal decryption; however, an illegal receiver cannot obtain the original plaintext information from the encrypted signals. Figure 9 depicts the system bit error rate curve of the proposed scheme with a 10 km signal transmission under multi-ary settings. The results confirm the feasibility of the proposed scheme for multi-ary decryption system applications.

Conclusions To solve the performance limitation of high-speed and high-resolution DAC on the performance of the QNRC system, this study proposed a scheme for designing a high-bit QNRC transmission system based on a low-speed, low-resolution DAC combined with cascaded phase modulators. The proposed scheme not only overcomes the transmission performance constraint imposed by the DAC bottleneck in cascaded PSK-QNRC systems but also significantly reduces the system cost. Moreover, the proposed scheme can be adapted for multi-ary transmission applications.

First, the proposed scheme was discussed, analyzed, and compared with the traditional 16 bit high-speed scheme with a high-resolution DAC in terms of the power penalty. Subsequently, the feasibility of the proposed scheme was verified. Second, this study applied this scheme to a multi-ary transmission setting and conducted a comparative analysis of the system's performance under various multi-ary transmission conditions. The feasibility of the future QNRC system adapting to a multi-ary transmission system was verified. Third, the domestication of DAC with a 4 bit resolution and 30 Gb/s transmission rate used in the proposed system has already been realized, which can bypass the dependence on the imported high-speed, high-resolution DACs, thus providing a feasible solution for realizing domestic QNRC systems with low system costs. Notably, the system proposed in this study is scalable because the maximum number of ciphertext states in the transmission is not limited to 16 bit. When necessary, it can be upgraded by cascading more low-speed DACs at the end of the transceiver or a few higher-resolution DACs to increase the transmitted ciphertext state of the QNRC system.

Key words optical communications; quantum noise random encryption; low-bit digital-to-analog converter; multi-ary transmission system