引用本文：王晓虎，蒲涛，郑吉林，等. 数/模转换器对 QNRC 系统性能的影响及解决方案[J]. 光通信技术，2022，46(6)：67-72.

数/模转换器对 QNRC 系统性能的影响及解决方案

王晓虎，蒲 涛*，郑吉林，周 华，李云坤

（中国人民解放军陆军工程大学 通信工程学院，南京，210007）

摘要：高采样速率、高分辨率数/模转换器(DAC)是量子噪声随机加密(QNRC)系统性能提升的核心器件之一，一直制约着QNRC系统技术发展。为了探究不同的DAC采样速率和分辨率对QNRC系统性能的影响，采用VPItransmission Maker Optical System 9.1软件进行系统仿真设计.首先，搭建了介观态功率为-21 dBm、传输距离为1000 km、传输速率为10 Gb/s和密文态数目为2^8-1的基于相移键控的QNRC系统；然后，改变DAC的采样速率、分辨率，对QNRC系统的性能进行对比分析。分析结果表明：当DAC的采样速率、分辨率分别为30 Gb/s、6 bit时，QNRC系统的性价比最佳。

关键词：量子噪声随机加密系统；数/模转换器；相移键控调制

中图分类号：TN918.1　**文献标志码**：A　**文章编号**：1002-5561(2022)06-0067-06

DOI：10.13921/j.cnki.issn1002-5561.2022.06.013　**开放科学(资源服务)标识码(OSID)**：

Influence of digital-to-analog converter on the performance of QNRC system and its solution

WANG Xiaohu, PU Tao*, ZHENG Jilin, ZHOU Hua, LI Yunkun

(Communications Engineering College, Army Engineering University of PLA, Nanjing 210007, China)

Abstract: The high sampling rate and high resolution digital-to-analog converter (DAC) is one of the core components to improve the performance of quantum noise random encryption(QNRC) system, which has been restricting the development of QNRC system technology. In order to explore the effects of different DAC sampling rates and resolutions on the performance of the QNRC system, the VPItransmission Maker Optical System 9.1 software is used for system simulation design. Firstly, a QNRC ststem basded on phase-shift keying modulation with mesoscopic power of -21 dBm, transmission distance of 1000 km, transmission rate of 10 Gb/s and number of ciphertext states of 2^8-1 is built. Then, the sampling rate and resolution of DAC are changed to compare and analyze the performance of QNRC system. The analysis results show that when the DAC sampling rate and resolution are 30 Gb/s and 6 bit respectively, the QNRC system has the best cost-performance ratio.

Key words: quantum noise random encryption system, digital-to-analog converter, phase-shift keying modulation

0 引言

随着现代数字信号处理技术和集成电路工艺水平的快速发展，高速率、高分辨率的数/模转换器(DAC)、模/数转换器(ADC)对光传输系统达到理论性能极限起着至关重要的作用[1]，并且在第五代移动通信技术(5G)通信领域、宽带雷达成像、航空航天和以太光互联等领域亦有着十分重要的意义[2]。

量子噪声随机加密(QNRC)是一种基于量子不可克隆、海森堡不确定性原理，利用量子噪声对介观态伪多进制信号进行加密的一种物理层安全技术[3-4]。QNRC系统在发送端通过密钥流对输入光信号进行伪多进制调制，合法接收端利用事先获得的密钥流进行解密，将接收到的多进制信号解调为二进制信号；而窃听方在无密钥情况下，只能通过对多进制截获信号进行判决，与此同时，光传输信号在介观态下产生的

收稿日期：2022-03-10。

基金项目：国家自然科学基金项目(62071487、61974165)资助。

作者简介：王晓虎(1998—)，男，硕士研究生，江苏淮安人。本科毕业于厦门大学电子科学与技术学院电子信息工程专业，现就读于陆军工程大学通信工程学院电子科学与技术专业，研究方向为光网络抗截获通信、QNRC系统方面。

***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、微波光子学和光传感技术等。

量子噪声还会掩盖相邻的密文态，从而导致窃听方无法通过合法手段获得有效信号[5]。QNRC 系统同时兼具较高安全性及高传输速率的优势，并且能够与现有的光纤通信网络、传输设备兼容，具有广阔的发展前景，引起了国内外专家学者的极大关注。其中，日本玉川大学古泽健团队[6]采用东芝公司和日立公司的芯片，研发的 QNRC 系统技术全球领先。近几年，国内部分高校也陆续开展了相关研究。2019 年，北京邮电大学的张杰团队[7-8]研究了 DAC 性能受限时对 QNRC 系统的性能影响；2020 年，华中科技大学光学与电子信息研究所[9]采用高采样速率、高分辨率的 DAC 实现了传输速率为 100 Gb/s、传输距离为 100 km 和密文态数目为 2^{15} 的基于强度调制的 QNRC 系统。但是，受限于工艺水平及各团队研究成本，一般团队不具备高速率、高分辨率 DAC 的实验条件。因此，寻找一种特定的绕开高速率、高分辨率 DAC 的 QNRC 系统研究方法迫在眉睫。为此，本课题组做了许多工作：2017 年，焦海松等人[10]在 Optic Express 上发表论文，首次对 QNRC 的安全性进行了定量分析；2019 年，陈毓凯等人[11-12]提出了基于正交相移键控-QNRC（QPSK-QNRC）系统的实验方案并与谭业腾设计的 PSK-QNRC 系统性能进行了对比分析；2020 年，李云坤等人[13]提出了基于并联强度键控（ISK）调制的方案，实现了密文态数目为 $2^{10}-1$ 的 ISK-QNRC 实验系统并进行了仿真论证。然而，本课题组当前只是基于理论与工程经验分析如何绕开高速率、高分辨率 DAC 研究 QNRC 系统，并未付诸实践。因此，本文以相移键控-QNRC（PSK-QNRC）系统为基础，通过测试不同的 DAC 采样速率和分辨率对 QNRC 系统性能的影响，得出一种最佳性价比 QNRC 系统方案。

1 PSK-QNRC 原理与系统实现方案

1.1 PSK-QNRC 原理

PSK-QNRC 原理示意图如图 1 所示，图中的 i、z、k 表示基于 PSK 调制时不同相位的密文态信号分布。在 PSK-QNRC 系统中，伪多进制密文信号通过相位调制器调制，输出相干态为 $|\varphi(m)\rangle=\left|\alpha e^{jm\frac{\pi}{M_b}}\right\rangle$。其中，$\frac{m}{M_b}=\frac{V_d}{V_\pi}$，$M_b$ 为存在基态的数目，m 为密文信号（$m=M-1$），M 指“0”、“1”这 2 种基态数目总和（$M=2M_b$），V_π、V_d 和 α 分别为调制器半波电压、驱动电压和相干态幅度。不同的密文态拥有不同的相位，每一对基态的 2 种密文态相位之差为 π，所有密文态对应的相位均匀分布在单位圆上，即其代表的明文数据交替排列，相位噪声可以对相邻密文态进行掩盖。圆周相角（2π）被等分为 M 部分，每个量子模的判别区间相邻信号的相位差为 $\delta_\varphi=2/M=\pi/M_b$[14]。拥有运行子密钥的合法接收方只需要区分 2 个相位相差为 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。当量子噪声（相位不确定度）$\Delta\varphi$ 强度超过 δ_φ，非法窃听方由于不能准确获得噪声掩盖下的相干态 $|\varphi(m)\rangle$，从而无法获得密钥及数据信息，达到保密通信的目的[15-16]。

1.2 PSK-QNRC 系统实现方案

本文根据 PSK-QNRC 原理，采用 VPItransmission Maker Optical System 9.1 软件进行系统仿真设计，搭建了介观态功率为 -21 dBm、传输距离为 1000 km、传输速率为 10 Gb/s 和密文态数目为 2^8-1 的 PSK-QNRC 系统，系统实现方案框图、参数设置分别如图 2、表 1 所示。在 PSK-QNRC 系统中，收发端共享运行子密钥，通过密钥扩展模块生成密钥流，与数据比特加密映射后

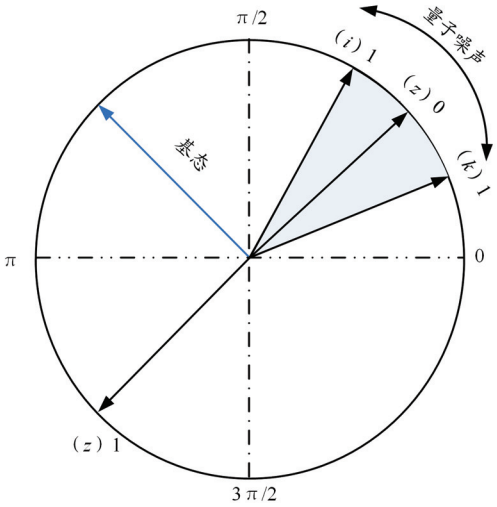


图 1 PSK-QNRC 原理示意图

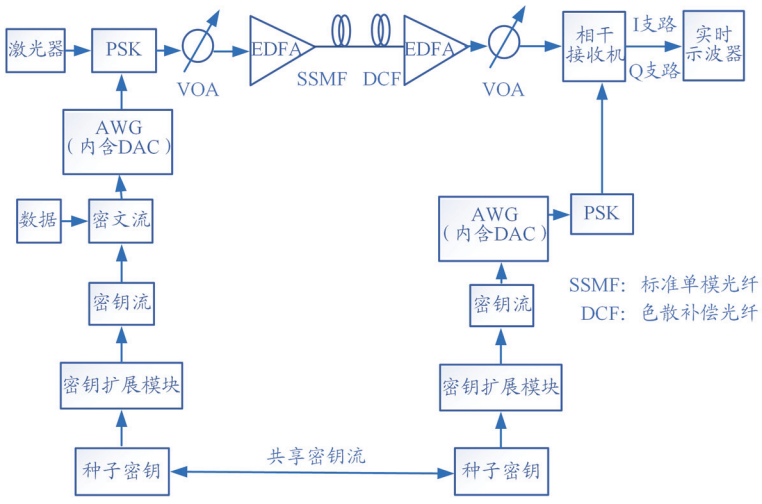
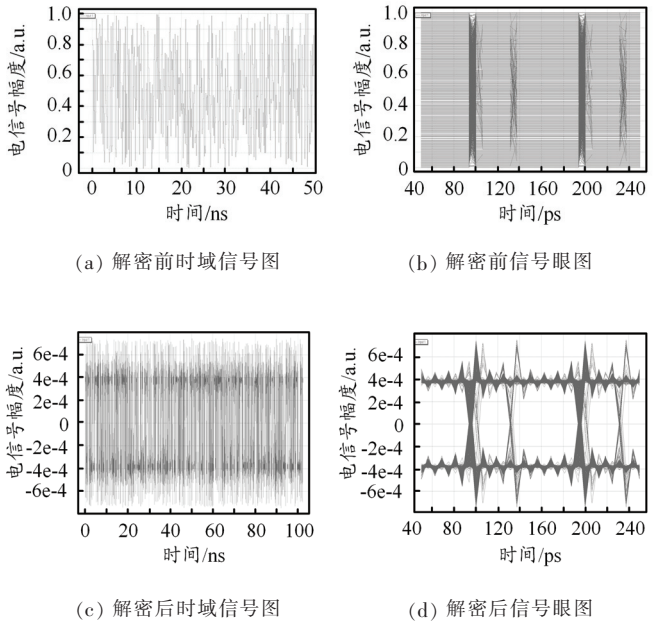


图 2 PSK-QNRC 系统实现方案框图

表 1 仿真参数

参数	值	参数	值
密文比特长度/bit	8	光纤损耗/(dB·km^{-1})	0.2
传输速率/(Gb·s^{-1})	10	标准单模光纤色散斜率/[ps·(nm·km)$^{-1}$]	16
EDFA 增益倍数/dB	20	色散补偿光纤色散斜率/[ps·(nm·km)$^{-1}$]	−80
EDFA 噪声系数/dB	4	标准单模光纤长度/km	833.33
AWG 电流噪声谱密度/(A·Hz$^{-1/2}$)	10e−12	色散补偿光纤长度/km	166.67
光电二极管热噪声/(A·Hz$^{-1/2}$)	10e−12	激光器线宽/Hz	100e5

通过任意波形发生器(AWG)进入 PSK;经过相位调制的光信号通过光衰减器(VOA)调节至介观态,再使用光放大器(EDFA)放大后进行传输。接收端产生一路解密信号,与接收到的加密光信号进行功率和时延匹配后,一起进入相干接收机(由一个 90°混频器与 2 个平衡检测器构成),相干接收机完成对加密信号的解密,解密前后信号时域图及眼图如图 3 所示。从图 3(b)可知,信号在解密前几乎无眼图,引入噪声后信号无法辨别。从图 3(c)、图 3(d)可知,在 DAC 采样速率与分辨率足够高(例如采样速率、分辨率分别为 30 Gb/s、8 bit 时)的情况下,多进制密文信号经过解密后,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。



(a) 解密前时域信号图　(b) 解密前信号眼图

(c) 解密后时域信号图　(d) 解密后信号眼图

图 3 解密前后信号时域图及眼图

2 DAC 发展现状及对 QNRC 系统性能的影响

2.1 DAC 发展现状

QNRC 系统作为一种伪多进制高阶调制系统,在收发端均需要将数字形式的密文信号转换为可用于传输的模拟信号。出于安全性考虑,实验过程中需要 DAC 能提供多种进制的模拟电平,以满足 QNRC 系统的安全性需求。因此,DAC 性能的高低将直接影响到 QNRC 系统的安全性与可靠性。目前,国内外高性能 DAC 发展现状[17-18]如表 2 所示。

表 2 国内外高性能 DAC 发展现状

研究单位	型号	速率	分辨率/bit	工艺尺寸/nm
清华大学	—	400 Mb/s	16	250
复旦大学	—	960 Mb/s	14	65
浙江大学	—	400 Mb/s	12	180
西安电子科技大学	—	120 Mb/s	12	120
东南大学	—	2.5 Gb/s	8	65
ADI 公司	AD9154	2.4 Gb/s	16	65
	AD9173	12.6 Gb/s	16	28
	AD9135	2.8 Gb/s	11	—
TI 公司	DAC39J84	2.8 Gb/s	16	180
Linear 公司	LTC2000	2.5 Gb/s	16	180

本文以传输速率为 10 Gb/s 的 QNRC 系统为例,调节 DAC 的采样速率和分辨率,对 QNRC 系统的性能进行研究。

2.2 DAC 采样速率不足对系统性能影响及最佳方案

当 DAC 分辨率为 10 bit 时,改变 DAC 采样速率,分别测出在 DAC 采样速率为 5 Gb/s、10 Gb/s、20 Gb/s、25 Gb/s、30 Gb/s 和 40 Gb/s 时的误码率曲线图如图 4 所示,对应解密信号的眼图如图 5 所示(接收端光功率为 1.14 dBm)。

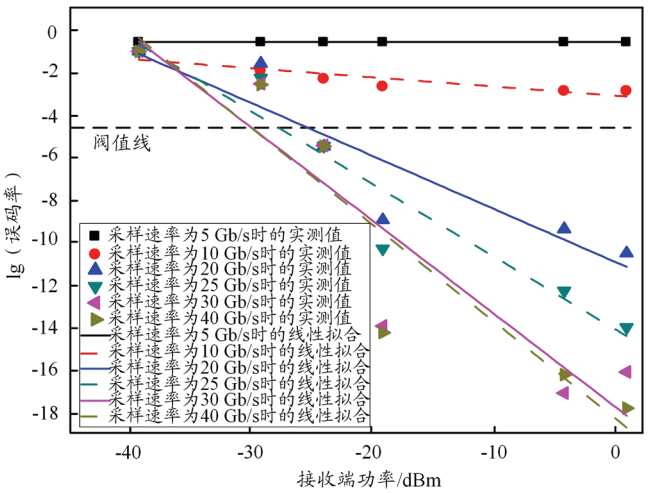
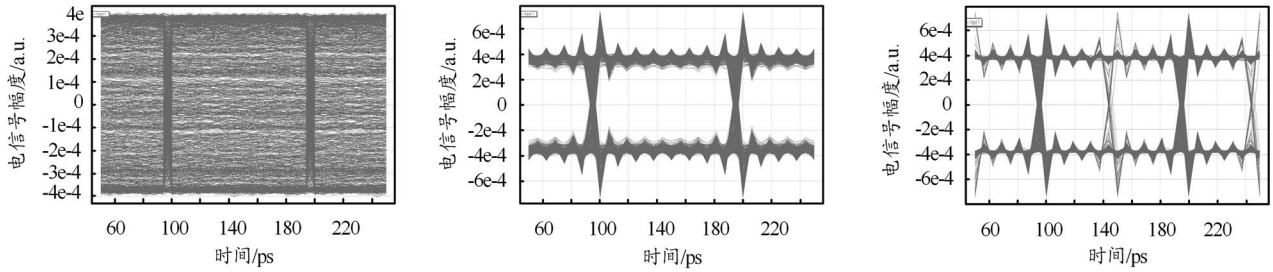


图 4 DAC 不同采样速率下的误码率曲线图



(a) 采样速率为 5 Gb/s　(b) 采样速率为 10 Gb/s　(c) 采样速率为 20 Gb/s

(d) 采样速率为 25 Gb/s　(e) 采样速率为 30 Gb/s　(f) 采样速率为 40 Gb/s

图 5　DAC 不同采样速率时的解密信号眼图

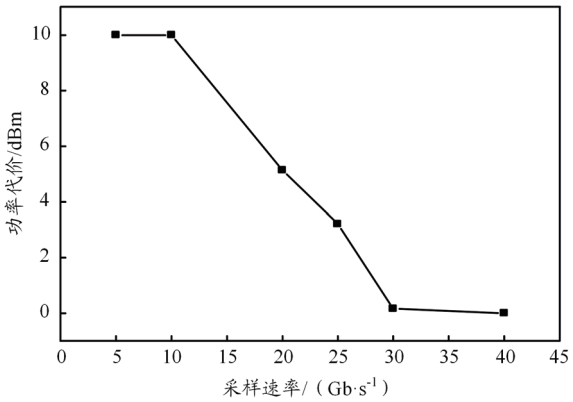


图 6　DAC 不同采样速率时的功率代价图

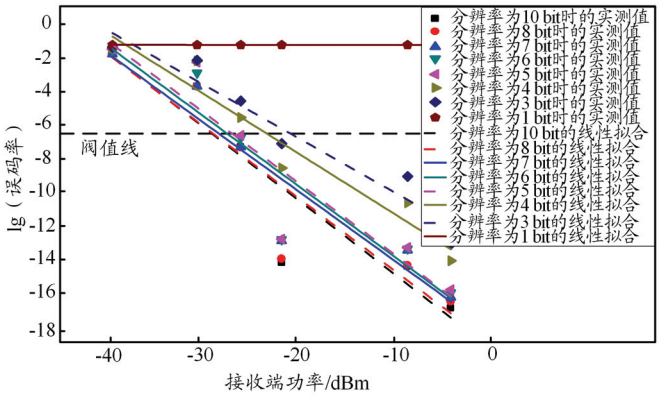


图 7　DAC 不同分辨率时的误码率曲线图

从图 4、图 5 可知,以 40 Gb/s 采样速率 DAC 为基准,当采样速率为 5 Gb/s 和 10 Gb/s 时,由于在有限接收光功率范围内系统性能无法达到阈值,几乎无眼图或者眼图不规范;当采样速率分别为 20 Gb/s、25 Gb/s 和 30 Gb/s 时,DAC 对应的功率代价分别 5.3 dBm、3.21 dBm 和 0.16 dBm,且眼图质量随着采样速率提高而更加清晰可见。功率代价与 DAC 采样速率的关系如图 6 所示。可以看出,当 DAC 采样速率严重不足时,系统付出的功率代价较大;而当采样速率达到奈奎斯特采样定律所要求的 3~5 倍传输速率后,再提升采样速率,系统所能节省的功率代价将显著降低。综合来看,在实验条件需要成本控制的情况下,实现 QNRC 传输系统只需要提供一个 3 倍于系统传输速率的 DAC 采样速率芯片,在采样速率达到 30 Gb/s 后,各眼图之间质量区别不大。因此,实现最佳性价比 QNRC 系统的传输速率为其采样速率的三分之一。

2.3 DAC 分辨率不足对系统性能影响及最佳方案

当 DAC 采样速率为 30 Gb/s 时,改变 DAC 分辨率,分别测出在DAC 分辨率为 1 bit、3 bit、4 bit、5 bit、6 bit、7 bit、8 bit 和 10 bit 时的误码率曲线图如图 7 所示,对应时域信号的眼图如图 8 所示(接收端光功率为 1.14 dBm)。

从图 7、图 8 可知,以 10 bit 分辨率 DAC 为基准,当分辨率为 1 bit 时,由于在有限接收光功率范围内系统性能无法达到阈值,几乎无眼图;当分辨率分别为 3 bit、4 bit、5 bit、6 bit、7 bit 和 8 bit 时,对应的功率代价分别为 9.52 dBm、7.11 dBm、2.04 dBm、1.57 dBm、0.43 dBm 和 0.14 dBm,且眼图质量随着分辨率提高而更加清晰

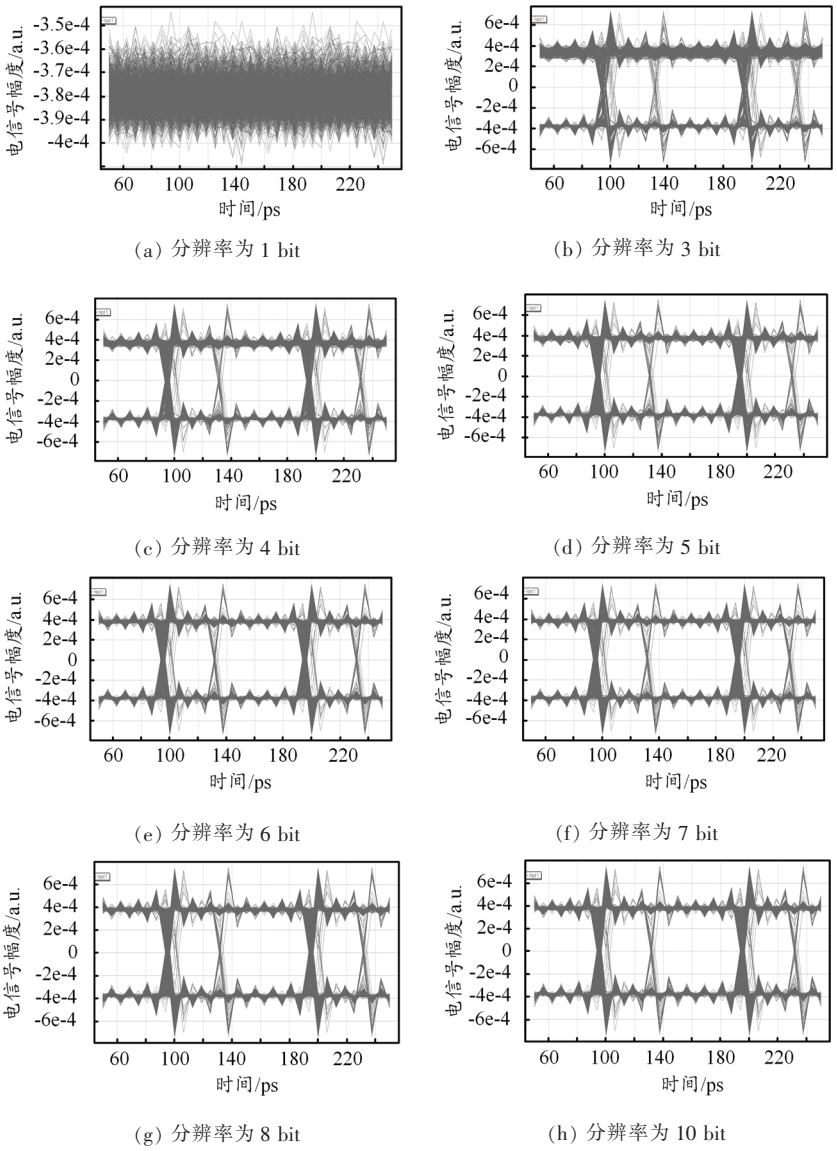


图 8 DAC 不同分辨率时的解密信号眼图

可见；当分辨率达到 6 bit 及以上时，各眼图质量区别不大。功率代价与 DAC 分辨率的关系如图 9 所示。可以看出，由于本实验系统输入密文态数目为 2^8-1（8 bit 密文态），在 DAC 分辨率较低时，系统付出的功率代价较大；当 DAC 分辨率接近于系统密文态输入位数时，再提升 DAC 分辨率所能节省的功率代价将逐渐变小；综合来看，在实验条件需要成本控制的情况下，实现 QNRC 传输系统只需要 DAC 分辨率达到甚至略低于输入最高密文态位数（例如 8 bit 密文态情况下 DAC 分辨率达到 6 bit 便可满足实验需求，此时 DAC 成本最低），此时的 QNRC 系统性价比最佳。

3 最佳性价比实现方案与对比分析

不同 DAC 条件下系统误码率曲线图如图 10 所示。以 10 bit、40 Gb/s 拟合线为基准，可以看出，本文得出的最佳性价比 DAC 方案（采样速率为 30 Gb/s、分辨率为 6 bit）、低位 DAC 方案（采样速率为 20 Gb/s、分辨率为 3 bit）对应的功率代价分别为 1.87 dBm、11 dBm。因此，最佳性价比 DAC 方案在付出较低功率代价的基础上，能够实现低误码率传输，且系统搭建成本大大降低。目前，采样速率为 30 Gb/s、分辨率为 6 bit 的 DAC 已实现国产。

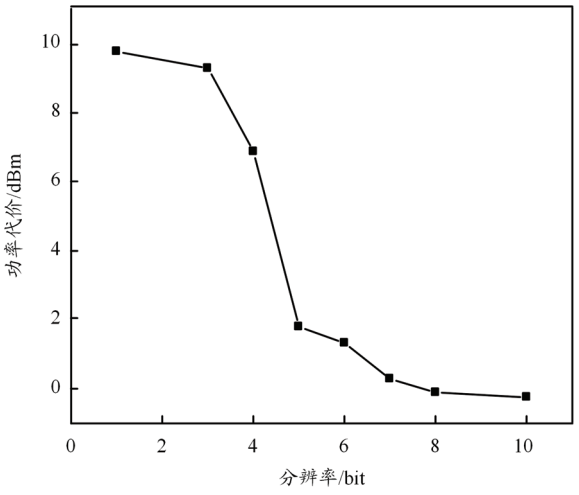


图 9 DAC 不同分辨率时的功率代价图

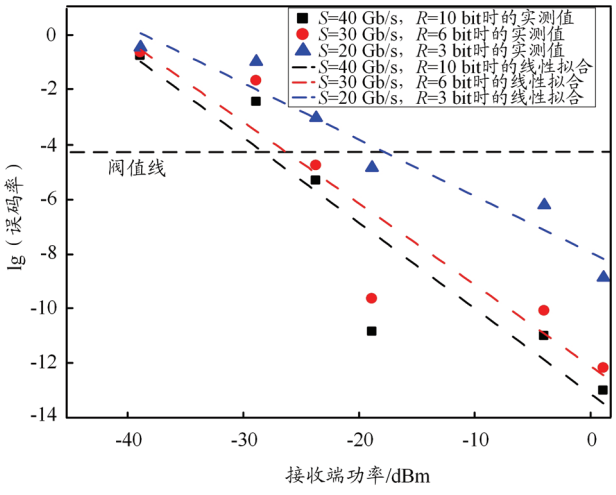


图 10 不同 DAC 条件下系统误码率曲线图
（S 为采样速率，R 为分辨率）

4 结束语

本文为了控制 QNRC 系统成本，以 PSK 调制、传输距离为 1000 km、密文态数目为 2^8-1 和介观态功率为–20 dBm 的 QNRC 系统为研究对象，通过测量、分析和对比不同条件下的 DAC 芯片性能，提出了在保证 QNRC 系统性能前提下能实现的最高性价比方案。该方案不依赖国外的高速率、高分辨率 DAC，能实现同等或相近的系统性能，为开发高性能 QNRC 系统提供了一种新思路。

参考文献：

[1] 刘祥水，曾祥伟，汤郡郡. 某型数模转换器国产化设计方案验证[J]. 中国设备工程，2020(7)：131–132.

[2] 王逸伦. 高精度高速电流舵型数模转换器设计[D]. 杭州：浙江大学，2020.

[3] 何海迅. 高分辨率高速 DA 转换电路的研究与实现[D]. 成都：电子科技大学，2019.

[4] NAIR R, YUEN H P, CORNDORF E, et al. Quantum noise randomized ciphers[J]. Physical Review A, 2006, 74(5): 052309-1–052309-33.

[5] CHEN Y, JIAO H, ZHOU H, et al. Security analysis of QAM quantum-noise randomized cipher system [EB/OL]. [2022–03–10]. https://ieeexplore.ieee.org/document/9141199/references#references.

[6] 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.

[7] 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)：122–134.

[8] YUEN H P. KCQ: a new approach to quantum cryptography I. general principles and key generation [EB/OL]. [2022–03–10]. https://arxiv.org: quant-ph/0311061.

[9] YU Q, Y WANG, 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.

[10] JIAO H S, TAO P, 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.

[11] 陈毓锴，郑吉林，焦海松，等. 正交相移键控 QNRC 系统的安全性研究[J]. 激光与光电子学进展，2020，57(17)：132–140.

[12] 谭业腾. 抗截获通信技术研究及其物理层安全性评估 [D]. 南京：陆军工程大学，2020.

[13] 李云坤，蒲涛，郑吉林，等. 基于并联强度调制的 QNRC 实现方案研究[J].中国激光，2021，48(17)：104–111.

[14] BANWELL T, TOLIVER P, YOUNG J C, et al. High data rate quantum noise protected encryption over long distances[EB/OL]. [2022–03–10]. https://ieeexplore.ieee.org/document/1605716/citations#citations.

[15] TANIZAWA K, FUTAMI F. Digital coherent detection with decryption in PSK Y-00 quantum stream cipher [EB/OL]. [2022–03–10]. https: //doi.org/10.1109/OECC.2018.8730060.

[16] KANTER G S, REILLY D, SMITH N. Practical physical-layer encryption: The marriage of optical noise with traditional cryptography [J]. Communications Magazine IEEE, 2009, 47(11): 74–81.

[17] 李少军. 宽带通信中的超高速数据转换器研究[D]. 西安：西安电子科技大学，2020.

[18] 杨会利. 高可靠高精度 R–2R 型数模转换器的研究[D]. 合肥：安徽大学，2018.