相位调制量子噪声随机加密系统的仿真验证

陈毓锴, 蒲涛, 郑吉林*, 焦海松, 李云坤
陆军工程大学通信工程学院, 江苏 南京 210007

摘要 量子噪声随机加密(QNRC)是一种结合了量子力学原理和经典流密码思想的信息抗截获通信方法。为了对相位调制(PSK)QNRC 系统的特性进行仿真验证,利用 VPI 仿真软件搭建了一套基于商用组件的仿真系统。基于任意波形发生器生成密文电信号及密钥电信号,并在接收端利用相位调制器及差分相移键控(DPSK)接收机从多进制密文信号中恢复二进制信号,最终实现了密文进制数为 256,数据传输速率为 2.5 Gbit/s,传输距离为 500 km 的无误码传输。与强度调制(ISK)方案相比,PSK 方案避免了解调时收、发双方功率必须匹配的问题。进制数的增加不会劣化 PSK 方案的传输性能,有助于提高系统安全性,PSK 方案具有潜在的安全性优势。

关键词 光通信; 抗截获通信; 量子噪声随机加密; 差分相移键控解调; Y-00 协议
中图分类号 TN918.1 **文献标志码** A **doi**: 10.3788/AOS202040.1606001

Simulation Verification of Phase-Shift Keying Quantum-Noise Randomized Cipher System

Chen Yukai, Pu Tao, Zheng Jilin*, Jiao Haisong, Li Yunkun
College of Communications Engineering, Army Engineering University, Nanjing, Jiangsu 210007, *China*

Abstract Quantum-noise randomized cipher (QNRC) is an information anti-interception communication method that combines the principles of quantum mechanics with classical stream cipher. In this study, the characteristics of a phase-shift keying (PSK) QNRC system are simulated and verified through a simulation system based on commercial components using VPI simulation software. In particular, the ciphertext electrical signals and the key electrical signals are generated based on an arbitrary waveform generator. At the receiving end, the binary signal is recovered from the multilevel ciphertext signal using a phase modulator and a differential phase-shift keying (DPSK) receiver. Finally, error-free communication is achieved at a data transmission rate and transmission distance of 2.5 Gbit/s and 500 km, respectively, in which the mechanism of the ciphertext is 256. This PSK scheme overcomes the problem of the intensity-shift keying (ISK) scheme, in which the powers of the transmitter and receiver must be matched during demodulation. The increase of mechanisms does not degrade the transmission performance of the PSK scheme and will help improve system security. Thus, the PSK scheme has potential security advantages.

Key words optical communications; anti-interception communication; quantum-noise random cipher; differential phase shift keying demodulation; Y-00 protocol
OCIS codes 060.4510; 060.5060; 060.4785; 060.5565

1 引 言

由于越来越多的机密和个人数据通过光纤网络传输,光纤通信的安全变得尤为重要[1-2]。量子密钥分发(QKD)能够为通信双方提供无条件安全的密钥[3],其结合“一次一密”可实现理想的量子保密通信。然而,低 QKD 速率无法满足高速光纤通信系统进行“一次一密”的数据加密要求[4]。量子噪声随机加密(QNRC)是一种可替代量子保密通信的抗截获通信技术,可用于现有的光纤通信系统中,并且能够实现高速、长距离的光纤安全通信[5]。Y-00 协议[6]是 QNRC 的基本协议,其基于密钥流将明文信息变换为多进制密文信号。当传输光功率达到介观尺度时,量子噪声特性令光子的位置不确定度大于

收稿日期: 2020-04-07; **修回日期**: 2020-04-30; **录用日期**: 2020-05-06
基金项目: 国家自然科学基金(61974165,61901480)
* **E-mail**: zhengjilinjs@126.com

多进制密文星座图中相邻符号的欧氏距离，只有拥有密钥的合法接收用户才能从多进制密文信息中提取二进制信息，而不知道密钥信息的窃听者需要区分被噪声掩盖的多进制密文信号。

迄今为止，已被报导的使用 Y-00 协议的 QNRC 有相位调制(PSK)[7-8]、强度调制(ISK)[9-10]、偏振调制[11]及正交振幅调制(QAM)[12-13]。上述方案的关键都在于设计 Y-00 收发机的复杂电路和芯片，均为非通用部件。针对此问题，文献[14]基于标准的商用器件，使用任意波形发生器(AWG)生成密文电信号和接收端密钥电信号，将作为一种快速的光比较器的平衡光电探测器用于从多进制密文信号中恢复二进制信号，从而搭建了一套 ISK-QNRC 实验系统。

而对于 PSK-QNRC 系统，文献[15]对其进行了理论安全性评估，但并没有进行仿真验证。因此，本文搭建一套 PSK-QNRC 仿真验证系统，采用差分相移键控(DPSK)解调方式对其特性进行仿真验证与研究。与 ISK-QNRC 类似，实验结构完全采用标准的商用器件。具体地，使用 AWG 生成密文电信号和接收端密钥电信号，并利用相位调制器和 DPSK 接收机从多进制密文信号中恢复出二进制信号。基于该实验结构，在 VPI 仿真平台上对系统进行仿真，实现了传输速率为 2.5 Gbit/s，传输距离为 500 km 的无误码传输。最后，对系统的安全性和可靠性进行评估，并与 ISK 方案进行对比，发现 PSK 方案更具有优势。

2　实验方案与原理

2.1　Y-00 协议加密原理

在 Y-00 协议中，明文为二进制数据 x，密钥为 M_b 进制的 u，生成的 $2M_b$ 进制密文 m 为

$$m=f(x,u)=u+[x\oplus \mathrm{Pol}(u)]\cdot M_b,\quad (1)$$

式中：当密钥 u 为奇数时，$\mathrm{Pol}(u)=1$，当 u 为偶数时，$\mathrm{Pol}(u)=0$。密文 m 用来调制相干态激光的相位，并通过光衰减器将信号光功率衰减至介观态水平，得到相应的量子态为

$$|\varphi(m)\rangle=|\alpha\exp^{\mathrm{i}\theta(m)}\rangle=|\alpha\exp^{\mathrm{i}m\frac{\pi}{M_b}}\rangle,\quad m=0,1,\cdots,2M_b-1,\quad (2)$$

式中：α 为量子态幅度。图 1 为 $|\varphi(m)\rangle$ 的信号矢量图，其中 $\theta(m)$ 为信号的相位，同一直径上两星座点距离最远，且密钥相同，明文比特相反。而相邻 m 承载不同的明文 x 比特。合法用户利用已知的密钥可以将多进制的量子态解调至二进制，即只需区分 $|\varphi(m)\rangle$ 和 $|\varphi(m+M_b)\rangle$。而窃听者不知道密钥，仍需区分多进制信息，由于量子噪声的真随机性，当量子噪声大于相邻量子态间隔时，窃听者获得的信息就会存在混淆。

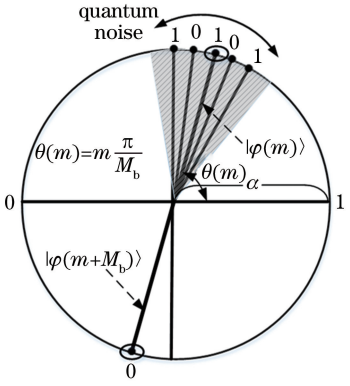

图 1　PSK-QNRC 加密编码信号矢量图

Fig. 1　PSK-QNRC encrypted coded signal vector image

2.2　实验装置

图 2 为所提 PSK-QNRC 方案的仿真系统结构图，图 3 为 Y-00 协议总体方案。假设发送方(Alice)和合法接收方(Bob)通过扩展共享的种子密钥来生成相同的运行密钥流，种子密钥可通过量子密钥分发得到，是绝对安全的[3]。明文数据流为伪随机二进制序列(PRBS)。根据 Y-00 协议，二进制明文比特流与 M_b 进制的运行密钥流离线生成 M ($=2M_b$)进制的密文符号流。

密文符号通过 AWG 生成对应的多进制信号，作为发送端的调制信号，并通过相位调制器将其调制至连续波(CW)激光器产生的光载波的相位上。CW 激光器的中心频率为 193.1 THz，AWG 的符号速率为 2.5 Gsymbol/s，则相应的数据通信速率为 2.5 Gbit/s。为了让相邻量子态被量子噪声掩盖，利用可调光衰减器($\mathrm{VOA_1}$)将相位调制器输出的信号功率衰减至介观态功率水平 P_{S0}，并采用光功率计(OPM)对功率进行监测。为适应长距离光纤传输，在进入传输信道之前，通过光放大器($\mathrm{EDFA_1}$)将介观信号提升到经典信号电平。

传输信道基本模块为 50 km 长的标准单模光纤(SSMF)、相应 50 km 长的色散补偿光纤(DCF)及用来补偿光纤损耗的中继功率放大器(EDFA)。循环(loop)模块用来控制传输基本模块的个数，若 loop 的次数为 0，代表进行背靠背(B2B)传输；若 loop 的次数为 5，则代表进行 500 km 的光纤传输。

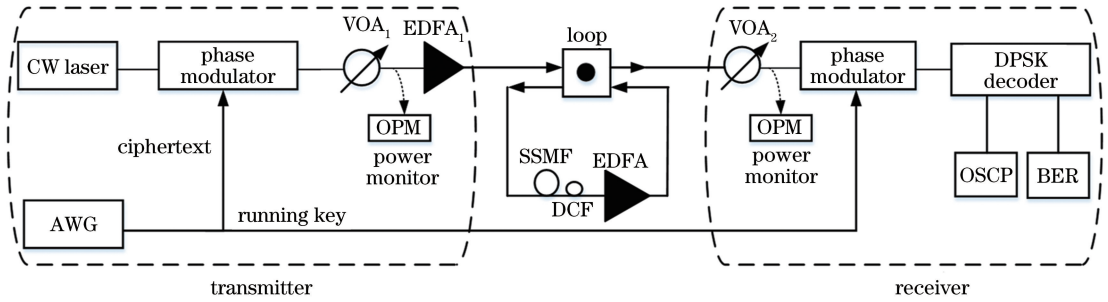

图 2　PSK-QNRC 方案的实验结构

Fig. 2　Experimental structure of PSK-QNRC scheme

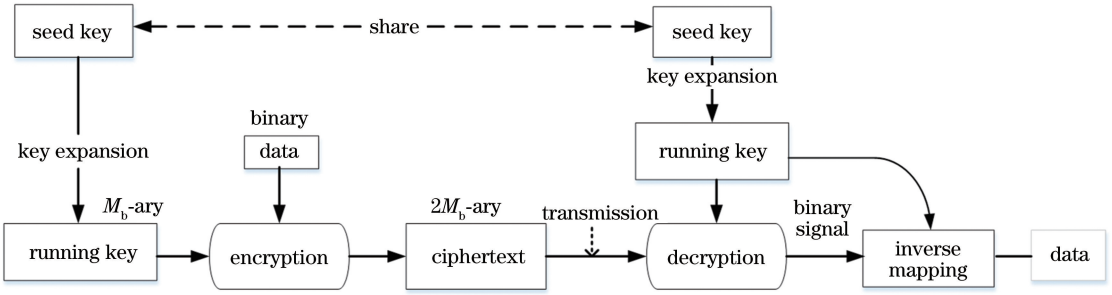

图 3　Y-00 加密协议总体方案

Fig. 3　Overall schematic of Y-00 encryption protocol

接收端在进行解调之前利用光衰减器(VOA$_2$)对接收光功率进行控制。随后传输的 Y-00 加密信号进入相位调制器进行解调,其调制信号同样是来自 AWG 的运行密钥信号,其与密文信号相匹配且二者的符号速率相同。事实上,运行密钥信号与接收到的加密光信号在时间上必须是同步的,但在仿真中,已经自动进行了同步,故不再进行过多讨论。在 ISK-QNRC 方案[14]中发送端与接收端功率必须匹配,才能使密文信号与运行密钥调制的光信号平衡相减,而每次改变接收光功率时都得重新进行功率匹配。

与 ISK-QNRC 方案相比,所提方案避免了收、发双方解调时功率必须匹配的问题。经过相位调制器后,收、发双方共享密钥,故 $m-u=0$ or M_b,则解调后信号携带的相位信息为 $\theta_m=(m-u)\pi/M_b=0$ or π。随后,信号进入 DPSK 接收机,接收机的内部结构如图 4 所示。马赫-曾德尔延迟干涉仪(MZI)有两个作用,一是将信号分为两路,并将其中一路延迟一个比特周期;另外一个作用是将相位信息转换为幅度信息。信号通过干涉仪后,分别进入光电检测器(PD),从而光信号转换为了电信号。之后,两路电信号通过减法器相减,并通过滤波器进行滤波。至此,经过 DPSK 接收机后,多进制密文信号恢复成二进制信号。示波器(OSCP)可用来观察眼图,误码仪用来测试系统误码率(BER)。

3　实验结果与讨论

对系统的传输性能和安全性能进行研究。假设

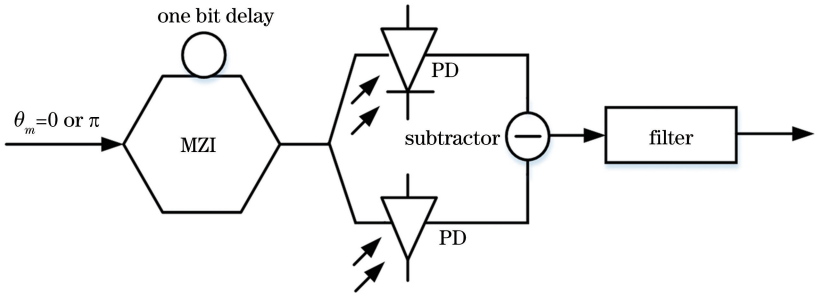

图 4　DPSK 接收机内部结构图

Fig. 4　Internal structure diagram of DPSK receiver

窃听者进行直接测量攻击，即窃听者采用与合法接收方相同的实验装置，只是没有共享的密钥，背靠背地在接收端进行直接测量。通过观察窃听者的眼图，根据眼图的混淆情况来判断系统的安全性；根据合法用户的眼图好坏及测试误码率的大小来衡量传输性能。

3.1　测试眼图

基于 VPI 仿真软件搭建的 PSK-QNRC 实验系统，分别得到了在 B2B 传输实验中使用匹配密钥与非匹配密钥的测试眼图，如图 5 所示，数据传输速率为 $R=2.5$ Gbit/s，介观相干态功率为 $P_{S0}=-40$ dBm，$EDFA_1$ 的放大倍数为 $G_0=30$ dB。图 5 第一行为使用非匹配的密钥所测量得到的眼图，其可以视为强大的窃听者所能测量得到的结果，即能获得完全的量子态，窃听距离为 0 km。可以发现，随着进制数的增加，眼图变差。当 $M=256$ 时眼图完全没有张开，这直观表明了此时 QNRC 系统的安全性，这是因为 QNRC 的安全性特别依赖于量子噪声掩盖的量子态数目 N_δ^{shot}。PSK-QNRC 系统中量子噪声掩盖的量子态数目为

$$N_\delta^{\text{shot}}=\frac{\Delta\varphi}{\delta\varphi}=\frac{M_b}{\pi|\alpha|},\tag{3}$$

式中：$\Delta\varphi$ 为量子相位噪声，即介观状态下相位的不确定度；$\delta\varphi$ 为相邻量子态的相位差。量子态幅度 $|\alpha|$ 可表示为

$$|\alpha|=\sqrt{\frac{P_{S0}}{h\nu R}},\tag{4}$$

式中：h 为普朗克常数；ν 为激光器的中心频率。根据(3)、(4)式，计算出当进制数 $M=8$ 时量子噪声掩盖的量子态数目为 $N_\delta^{\text{shot}}\approx0.072$，而当 $M=256$ 时掩盖的量子态数目为 $N_\delta^{\text{shot}}\approx2.3044$。可见进制数越高，量子噪声掩盖的量子态数目 N_δ^{shot} 越多，系统越安全。事实上，由于系统中还存在着其他噪声，比如放大器的自发辐射(ASE)噪声，则实际噪声掩盖的量子态数目要更多。文献[15]根据理论分析，得出在 ASE 噪声的作用下，量子噪声掩盖的量子态数目 N_δ^{shot} 不必达到 1 就能保证数据传输的安全。因此，当进制数 $M=256$ 时，达到了数据传输的安全性要求，眼图完全没有张开；当进制数 $M=8$ 时，未达到数据传输的安全性要求，眼图虽然存在混淆，但仍有可能被窃听者窃取到信息，这与理论分析结果相符合。图 5 第二行分别为 B2B 情况下 $M=8$ 及 $M=256$ 时，合法用户利用已知密钥解调得到的二进制信号，可以看到，二者眼图都很清晰，表明收、发双方有较好的通信。

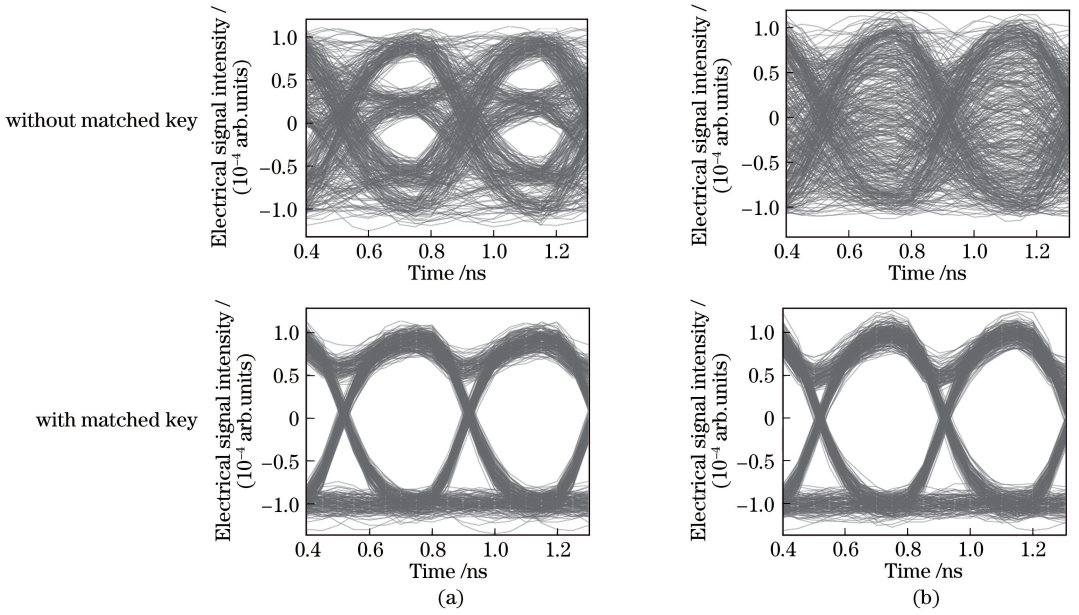

图 5　不同进制数下 B2B 测试的眼图。(a) $M=8$；(b) $M=256$

Fig. 5　Eye diagrams measured by B2B under different mechanisms. (a) $M=8$; (b) $M=256$

图 6 为传输 500 km 后合法用户的测试眼图，参数的设置均与 B2B 传输一致。可以发现，传输 500 km 的眼图与 B2B 测试眼图相比，稍劣化，但仍很清晰，表明所提方案可实现高速、长距离的光纤安全传输。而对比图 6(a)、(b)，二者均很清晰，不存在明显的劣化，可合理推断进制数的增加在提高 PSK-QNRC 系统安全性的同时，不会劣化传输性能。

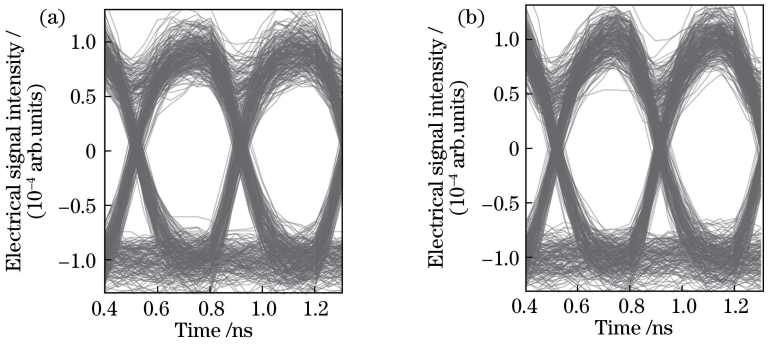

图 6　不同进制数下 500 km 光纤传输测试眼图。(a) $M=8$;(b) $M=256$

Fig. 6　Eye diagrams measured after 500-km fiber transmission under different mechanisms. (a) $M=8$; (b) $M=256$

3.2　测试误码率曲线

文献[15]指出在 PSK-QNRC 系统中发送端使用内部光放大器(EDFA$_1$)是必需的。对此,分别在使用 EDFA$_1$ 与不使用 EDFA$_1$ 情况下,研究介观功率对传输误码率的影响,如图 7 所示。其为 B2B 传输,密文进制数为 $M=256$,光放大器 EDFA$_1$ 的放大倍数为 $G_0=30$ dB。可以发现,随着介观功率的增加,误码率逐渐下降至 10^{-9} 以下,当误码率低于 10^{-9} 时,系统为无误码传输。两条曲线的对比结果表明,误码率同样为 10^{-9},使用 EDFA$_1$ 可使介观功率 P_{S0} 降低约 21.8 dB。而根据(4)式可知,介观功率越低,量子态幅度 $|\alpha|$ 越小,从而量子相位噪声 $\Delta\varphi=1/|\alpha|$ 越强,其可掩盖的量子态数目 $N_{\delta}^{\mathrm{shot}}$ 也就越多,系统也就越安全。同时,光放大器引入了放大自发辐射噪声,给窃听者的窃听带来更多的不确定性。

故在收、发双方同样达到无误码传输的情况下,发送端采用光放大器有利于提高系统的安全性,这也表明在 PSK-QNRC 系统中发送端使用内部光放大器 EDFA$_1$ 是必需的。

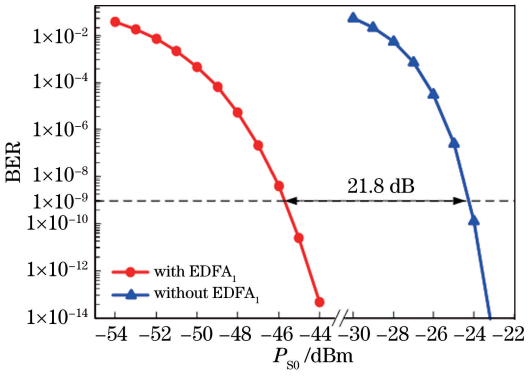

图 7　BER 随 P_{S0} 的变化

Fig. 7　BER versus P_{S0}

图 8 研究了 B2B 情况下误码率随进制数的变化关系,其中 P_{recv} 为接收光功率。数据传输速率为 $R=2.5$ Gbit/s,介观相干态功率为 $P_{S0}=-40$ dBm,光放大器 EDFA$_1$ 的放大倍数为 $G_0=30$ dB。由图 8 可看出,与 ISK 方案不同,PSK 方案中密文符号的进制数对系统的传输性能影响不大,这与图 6 结果一致。这是因为 PSK 方案中合法用户可以利用已知的密钥消除进制数的影响,同时进制数不会对量子相位噪声 $\Delta\varphi$ 产生影响,所以误码率与进制数是无关的。而 ISK 方案中误码率与进制数会有一定的相关性,进制数的增加将劣化系统的传输性能[14]。

因此,得出结论:由于进制数的增加可以提高系统的安全性,且不会劣化 PSK-QNRC 系统的传输性能,因此 PSK 方案较 ISK 方案更具有潜在的安全性优势。

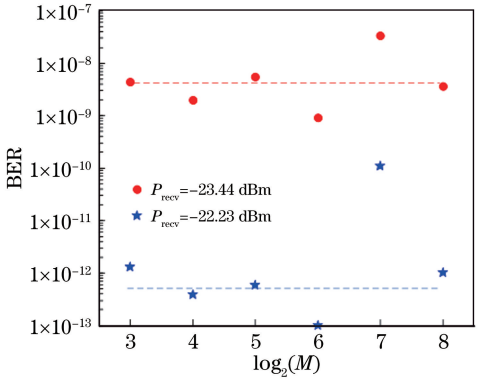

图 8　BER 随 M 的变化

Fig. 8　BER versus M

图 9 研究在 B2B、300 km 及 500 km 光放大链路的传输情况下合法用户的误码率随接收光功率 P_{recv} 的变化关系。数据传输速率为 $R=2.5$ Gbit/s,介观相干态功率为 $P_{S0}=-40$ dBm,光放大器 EDFA$_1$ 的放大倍数为 $G_0=30$ dB,进制数 $M=256$。根据(3)、(4)式计算得到量子噪声掩盖的量子态数

目为 $N_{\delta}^{\mathrm{shot}} \approx 2.3044$，达到了系统安全性要求。由图 9 可看出，随着接收光功率 P_{recv} 的不断增大，误码率逐渐减小。同时，无论是 B2B 还是长距离传输，都可以实现无误码传输，B2B 与 300 km 传输的功率代价为 7.33 dB，300 km 与 500 km 传输的功率代价为 2.52 dB。

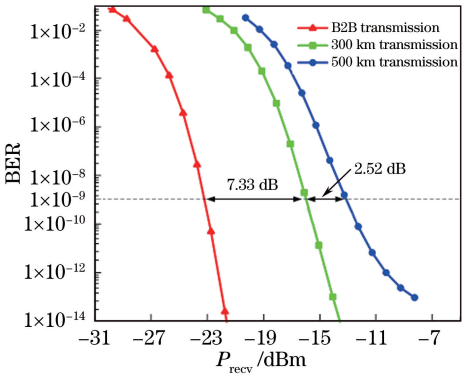

图 9　BER 随 P_{recv} 的变化

Fig. 9　BER versus P_{recv}

4　结　　论

基于任意波形发生器生成密文电信号和接收端密钥电信号，并利用相位调制器及 DPSK 接收机从多进制密文信号中恢复二进制信号，最终实现了密文进制数为 256，数据传输速率为 2.5 Gbit/s，传输距离为 500 km 的无误码传输。该实现结构采用标准的商用器件，不依靠高速复杂的数模转换器芯片。与 ISK 方案相比，所提方案避免了收、发双方解调时功率必须匹配的问题。同时对系统的安全性和可靠性进行评估，结果发现，发送端采用光放大器有利于提高系统的安全性能。与 ISK 方案不同，进制数的增加对 PSK-QNRC 系统的传输性能影响不大，同时有助于提高系统安全性。因此，随着安全性要求的不断提高，PSK 方案具有更好的应用价值。

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] 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.

[4] Tan Y T, Pu T, Zheng J L, et al. Anti-interception communication system based on optical encoding/decoding technology[J]. Acta Optica Sinica, 2020, 40(9): 0906001.
谭业腾, 蒲涛, 郑吉林, 等. 基于光编/解码技术的抗截获通信系统研究[J]. 光学学报, 2020, 40(9): 0906001.

[5] Barbosa G A, Corndorf E, Kumar P, et al. Secure communication using mesoscopic coherent states[J]. Physical Review Letters, 2003, 90(22): 227901.

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

[7] 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.

[8] Kanter G S, Reilly D, Smith N. Practical physical-layer encryption: the marriage of optical noise with traditional cryptography[J]. IEEE Communications Magazine, 2009, 47(11): 74-81.

[9] Futami F. Experimental demonstrations of Y-00 cipher for high capacity and secure optical fiber communications [J]. Quantum Information Processing, 2014, 13(10): 2277-2291.

[10] Futami F, Hirota O. Masking of 4096-level intensity modulation signals by noises for secure communication employing Y-00 cipher protocol[C]// 37th European Conference and Exposition on Optical Communications, September 18-22, 2011, Geneva, Switzerland. Washington, D C: OSA, 2011: Tu.6.C.4.

[11] Corndorf E, Barbosa G, Liang C, et al. High-speed data encryption over 25 km of fiber by two-mode coherent-state quantum cryptography [J]. Optics Letters, 2003, 28(21): 2040-2042.

[12] Nakazawa M, Yoshida M, Hirooka T, et al. QAM quantum stream cipher using digital coherent optical transmission[J]. Optics Express, 2014, 22(4): 4098-4107.

[13] 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.

[14] Jiao H S, Pu T, Shi L, et al. A novel realization of quantum stream cipher with key-modulated local light [J]. Optical Fiber Technology, 2019, 53: 102007.

[15] Jiao H S, Pu T, Xiang P, et al. Physical-layer security analysis of PSK quantum-noise randomized cipher in optically amplified links [J]. Quantum Information Processing, 2017, 16(8): 189.