基于波长-模式双复用的量子保密通信系统

罗均文，李云霞，蒙 文，石 磊，魏家华，薛 阳
空军工程大学信息与导航学院，陕西 西安 710077

摘要 提出并设计了一种基于波长-模式双复用的量子保密通信系统，介绍了波长-模式双复用的基本原理，使用 Optisystem 搭建了系统模型并进行了 10 次发送实验，获取并分析了信号的时域波形和频谱图，验证了传输过程中信号波长和线偏振模式的稳定性，实现了系统中基于双不等臂马赫-曾德尔干涉仪方案的量子密钥分发过程，获得了经典光信号的误比特率、眼图以及品质因数。结果表明，此量子保密通信系统能够融合两种复用方式的优势，扩大信道容量，提高信号间的隔离度和正交性，有效减小非线性效应和信号间串扰，较好地保护量子-经典信号同传过程中的量子信号，证明了该量子保密通信系统有效可行。

关键词 量子光学；量子通信；波分复用；模式复用；少模光纤；相位编码
中图分类号 O431.1；O431.2 **文献标识码** A
doi：10.3788/AOS201737.0927001

Quantum Private Communication System Based on Wavelength-Mode Division Co-Multiplexing

Luo Junwen, Li Yunxia, Meng Wen, Shi Lei, Wei Jiahua, Xue Yang
Information and Navigation College, Air Force Engineering University, Xi'an, Shaanxi 710077, *China*

Abstract A quantum private communication system based on the wavelength-mode division co-multiplexing is put forward and designed. The basic principle of wavelength-mode division co-multiplexing is introduced. The transmission experiment is performed for 10 times with the system model built by Optisystem. The time domain waveform and spectra of signals are obtained and analyzed. Stabilities of wavelength and linear polarization mode of signals in the transmission are tested. The quantum key distribution based on the scheme of double unbalanced Mach-Zehnder interferometers is realized in the system. The error bit rate, eye diagram and quality factor of classical optical data are obtained. The results show that this quantum private communication system converges the advantages of two multiplexing forms. The channel capacity is broadened, and the isolation and the orthogonality between signals are enhanced. In addition, the nonlinear effects and the crosstalk between signals are reduced efficiently, and the quantum signal is well maintained in the coexisting transmission process of quantum-classical signals. The proposed quantum private communication system is confirmed to be effective and applicable.

Key words quantum optics; quantum communication; wavelength division multiplexing; mode division multiplexing; few-mode fiber; phase encoding
OCIS codes 270.5565; 270.5568; 270.5585

1 引 言

自 1984 年 Bennett 和 Brassard 提出量子密钥分发(QKD)概念以来[1]，BB84 等大量 QKD 协议被提出[2-3]，且其安全性得到了充分的证明[4]，基于 QKD 协议的量子保密通信得到了广泛关注和深入研究。

为有效降低大量敷设光纤带来的高昂成本，并充分提高现有暗光纤的利用率，目前的量子保密通信系统基本采用量子-经典信号同传的方案，通过波分复用(WDM)使量子信号与经典光信号在同一光纤中传输[5-6]。量子信号为单光子信号，在传输时容易受单模光纤(SMF)非线性效应的影响，且 WDM 的隔离度有

收稿日期：2017-05-05；**收到修改稿日期**：2017-05-10
基金项目：国家自然科学基金(61601497)
作者简介：罗均文(1992—)，男，硕士研究生，主要从事光纤通信和量子通信方面的研究。E-mail：khd65482@163.com
导师简介：李云霞(1966—)，女，硕士，教授，主要从事光纤通信和量子通信方面的研究。E-mail：yunxial@sohu.com

限，经典光信号和量子信号间存在串扰，这对量子信号的传输质量造成了极大损伤。同时，随着大数据时代的到来，经典光信号业务量急剧增加，SMF 的传输容量无法满足下一代光网络的要求[7]。近年来，基于少模光纤模式复用(MDM)的传输方案被认为是解决带宽危机的理想选择[8]。少模光纤的结构特点使得其相比 SMF 具有更低的非线性损伤，模式相互正交也减少了信道间串扰。将其运用在量子保密通信中，对量子弱信号的传输将十分有利。目前，MDM 系统的复杂度较高[9]，量子保密通信必须依靠同传方案实现与经典光网络的融合，因此，如何在较低复杂度的前提下扩大光纤传输容量并减少量子信号所受非线性损伤和信道串扰成为亟待解决的问题。

本文提出了基于波长-模式双复用的量子保密通信方案，QKD 采用相位编码的 BB84 协议，以波长区分信号，降低了复用和解复用所带来的系统复杂度，而线偏振模的正交性又大大减少了信号串扰，且两者均可使得传输容量倍增；使用软件 Optisystem 搭建了系统模型，并在 50 km 少模光纤中进行了仿真传输实验，对实验结果进行了分析，证明了方案的可行性和优越性。

2　基本原理

WDM 是指使用不同波长的光信号携带不同的信息，并将其耦合到同一光纤中进行传输，在接收端解复用得到信息的过程[10]。MDM 是指将不同的信息加载在具有不同线偏振模的光信号上，且光信号在少模光纤中传输，在接收端解复用得到信息的过程[11]。在本文所提出的基于波长-模式双复用的量子保密通信方案中，量子信号和经典光信号不仅具有不同的波长，并且为了增加信号间的隔离度，减少信号串扰，两种信号同时还具有不同的线偏振模。量子信号采用 LP_{01} 模，经典信号采用 LP_{11} 模，依靠线偏振模之间良好的正交性实现信号的高质量传输，其原理如图 1 所示。

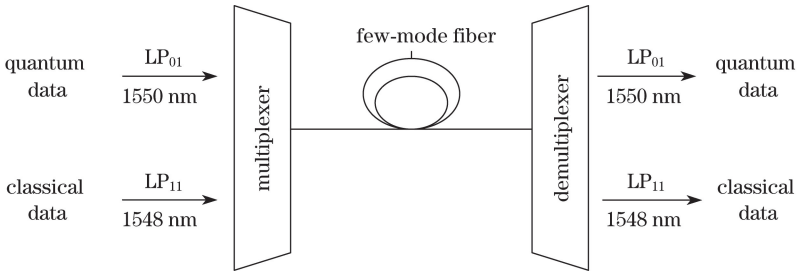

图 1　基于波长-模式双复用的量子保密通信原理图

Fig. 1　Principle diagram of quantum private communication based on wavelength-mode division co-multiplexing

波长-模式双复用的方法不仅融合了 WDM 和 MDM 的扩容优点，同时也弥补了两种方案的不足，利用波长区分可以降低复用和解复用器件的复杂度，利用模式区分可以弥补 WDM 有限隔离度带来的串扰等不足。

为了减小传输过程中双折射效应及偏振模色散的影响，增加量子保密通信系统的稳定性，QKD 的实现采用的是相位编码方案中的双不等臂马赫-曾德尔(M-Z)干涉仪方案[12]，其原理如图 2 所示。

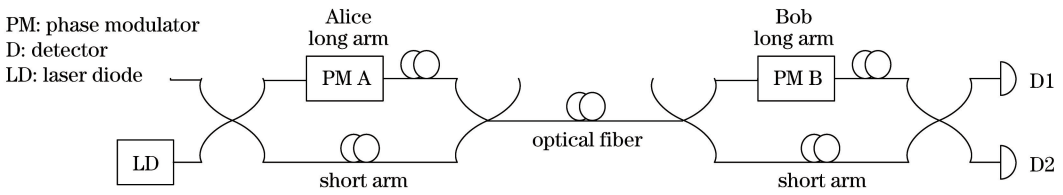

图 2　基于双不等臂 M-Z 干涉仪方案的 QKD 原理图

Fig. 2　Principle diagram of QKD based on double unbalanced M-Z interferometers

根据 QKD 的双不等臂 M-Z 干涉仪方案，Alice 将四种不同相位分为两组编码基，分别为 P_1：[0，π]和 P_2：[π/2，3π/2]，并根据 0 或 π/2 对应比特 0，π 或 3π/2 对应比特 1 的规则，随机地从两个基中选择相位进行编码；而 Bob 则从 0 和 π/2 中随机选择一个相位进行匹配，其中 0 只能正确解出 Alice 编码中所用的

P_1基，π/2 只能正确解出 Alice 编码中所用的 P_2基。在两个 M-Z 干涉仪长短臂差值相等的情况下，可以直接通过 Alice 和 Bob 所用相位的差值 $\Delta\varphi$来判断量子密钥：$\Delta\varphi$为 0 时，则密钥为 0；$\Delta\varphi$为 π 时，则密钥为 1；$\Delta\varphi$为 π/2 或 3π/2 时，则对基失败，无法协商密钥。

3　系统模型设计

为验证基于波长-模式双复用的量子保密通信系统的性能，设计了系统模型，利用 Optisystem 搭建了系统的仿真模型并进行了相应的参数设置。数据速率设置为 10 Gbit/s，模拟传输实验次数为 10。

根据双不等臂 M-Z 干涉仪方案原理，搭建 QKD 的发射端和接收端仿真模型如图 3(a)、(b)所示。为了最大限度保证量子弱信号的传输质量，选用衰减最小的 1550 nm 波长的光脉冲，线偏振模式选择基模 LP_{01}模。发射端中设置有效功率为－14 dBm(峰值功率为 10 dBm)，再使用 20 dB 衰减器将功率衰减至单光子级别，不等臂 M-Z 干涉仪由两个 3 dB 耦合器、一个移相器以及两个延时器组成。在每次传输实验中，移相器模拟 Alice 从四个相位中随机选择一个相位对信号进行编码，两个延时器分别用来模拟干涉仪的长臂和短臂，且其延时相差一个脉冲周期。在接收端中搭建与发射端组成相同的不等臂 M-Z 干涉仪，其中移相器模拟 Bob 每次从两个相位中随机选择一个用作解码的基。同时，在接收端中使用模式观测器观测所接收的线偏振模，使用两个光时域波形观测器观察两个输出端的光脉冲的波形，判断干涉状态，并由此得到密钥。光频谱分析仪则用来观测频谱，分析非线性噪声的影响。

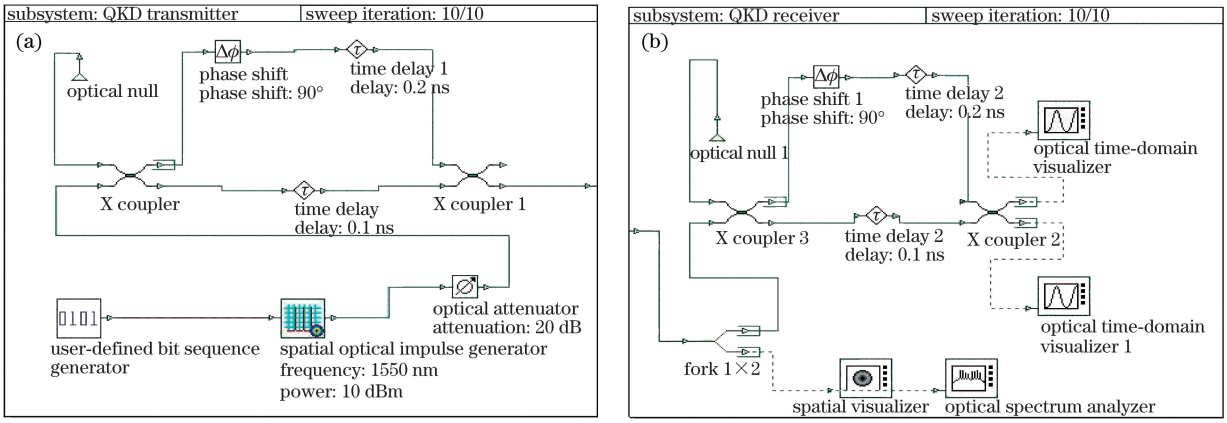

图 3　QKD 的(a)发送端和(b)接收端仿真模型

Fig. 3　Simulation models of (a) transmitter and (b) receiver of QKD

系统中所搭建的经典光信号的发射端和接收端分别如图 4(a)、(b)所示，其中 NRZ 表示不归零码，BER 表示误比特率。为了降低经典光信号对量子弱信号的影响，应该在保证误码率低于 10^{-12}的前提下，尽量减小经典光信号的功率。经典光信号功率设置为－14 dBm[6]，其波长为 1548 nm，线偏振模式为 LP_{11}模。在接收端使用模式观测器观测所接收的线偏振模，使用光接收机及误比特率分析仪得到信号的 BER、品质因数 Q 以及眼图。使用光时域波形观测器观察波形，并使用光频谱分析仪观测频谱，分析非线性噪声的影响。系统的整体结构如图 5 所示。

为了保证少模光纤只支持 LP_{01}和 LP_{11}两种模式，需要对少模光纤的结构参数进行设置。光纤支持模式的数目可以从归一化截止频率 V 看出，V 的定义式为

$$V=\frac{2\pi a}{\lambda}\sqrt{n_{\mathrm{core}}^2-n_{\mathrm{clad}}^2}, \tag{1}$$

式中a为纤芯半径，n_{core}为纤芯折射率，n_{clad}为包层折射率，λ为波长。当 $2.405\leqslant V\leqslant 3.832$ 时，光纤只稳定支持 LP_{01}和 LP_{11}两种模式[13]。当 $n_{\mathrm{core}}=1.462$，$n_{\mathrm{clad}}=1.460$，$a=12\ \mu\mathrm{m}$，λ 分别为 1550 nm 和 1548 nm 时，V 的值分别为 3.719 和 3.723。少模光纤长度设置为 50 km，且每隔 10 km 使用透镜进行一次聚焦，防止线偏振模在传输过程中发散。

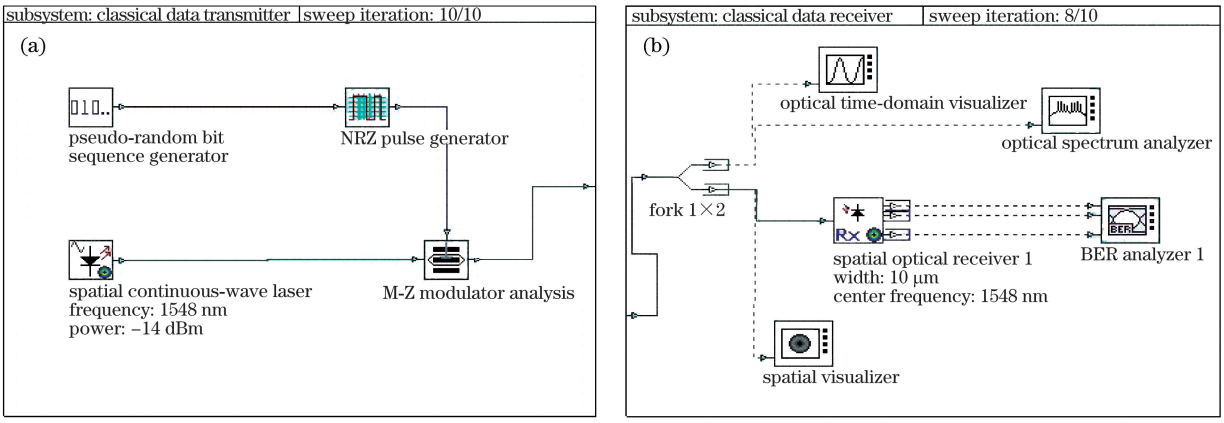

图 4　经典光信号的(a)发送端和(b)接收端仿真模型

Fig. 4　Simulation models of (a) transmitter and (b) receiver of classical data

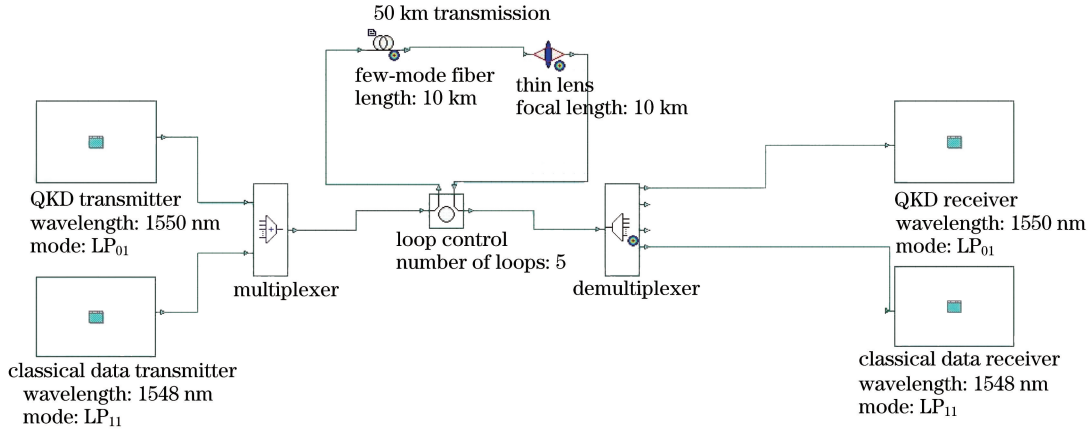

图 5　基于波长-模式双复用的量子保密通信系统结构图

Fig. 5　Structural diagram of quantum private communication system based on wavelength-mode division co-multiplexing

4　分析与讨论

模型搭建完成后，进行仿真实验并对模拟结果进行分析。光频谱分析仪所得量子信号和经典光信号频谱分别如图 6(a)、(b)所示。可以看出，无论是波长为 1550 nm 的量子信号，还是波长为 1548 nm 的经典光信号，除了信号传输后的衰减，没有明显的噪声，说明方案能较好地抑制非线性噪声。所得量子信号和经典光信号模式的模场能量分布如图 7(a)、(b)所示。

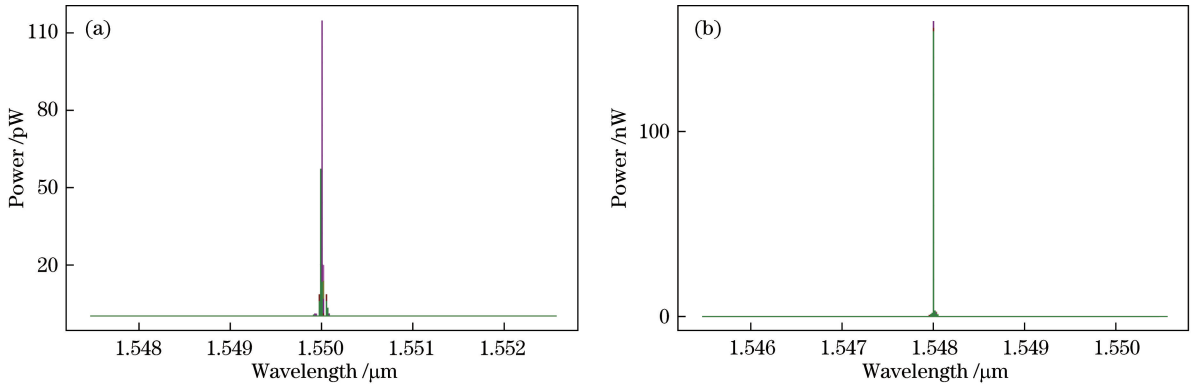

图 6　(a)量子信号和(b)经典光信号的频谱

Fig. 6　Frequency spectra of (a) quantum signal and (b) classical optical signal

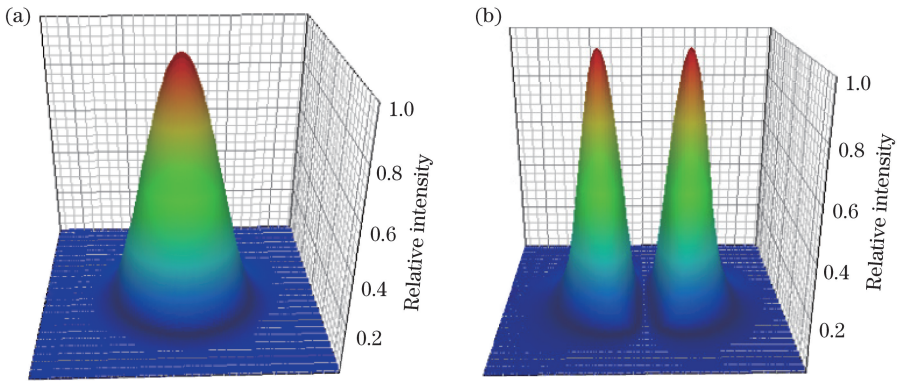

图 7　(a)量子信号和(b)经典光信号的模场能量分布图

Fig. 7　Mode field energy distributions of (a) quantum signal and (b) classical optical signal

结合图 5 中解复用器的波长-模式分组可以发现，相应信号的波长和模式在传输中得到了较好的保持，而且波长-模式双复用的方案使得信号的隔离度和正交性均得到了提高。信号在接收端易于区分，且产生的其他模式可视作噪声，经解复用器滤除，从而不影响接收端的判断。

为检验基于波长-模式双复用的量子保密通信系统能否正常进行 QKD，分析了 QKD 接收端的光时域波形观测器结果。当 Alice 和 Bob 所选相位差 $\Delta\varphi=0$ 时，第一个探测器(D1)探测到干涉增长的波形，而第二个探测器(D2)探测到干涉减弱的波形，此时认为所传输密钥为 0，两探测器波形如图 8(a)、(b)所示。

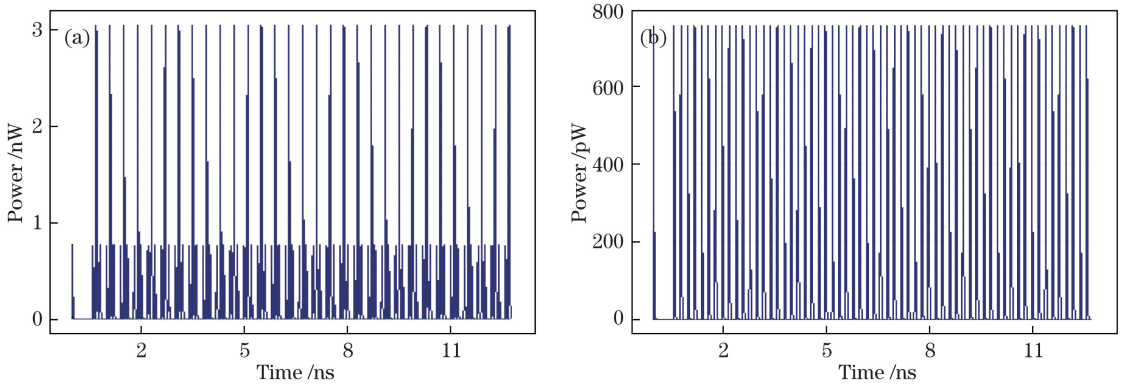

图 8　当 $\Delta\varphi=0$ 时，(a)D1 和(b)D2 里的时域波形

Fig. 8　Time domain waveforms in (a) D1 and (b) D2 when $\Delta\varphi=0$

当 Alice 和 Bob 所选相位相差为 π 时，D1 探测到干涉减弱的波形，而 D2 探测到干涉增长的波形，此时认为所传输密钥为 1，两探测器波形如图 9(a)、(b)所示。

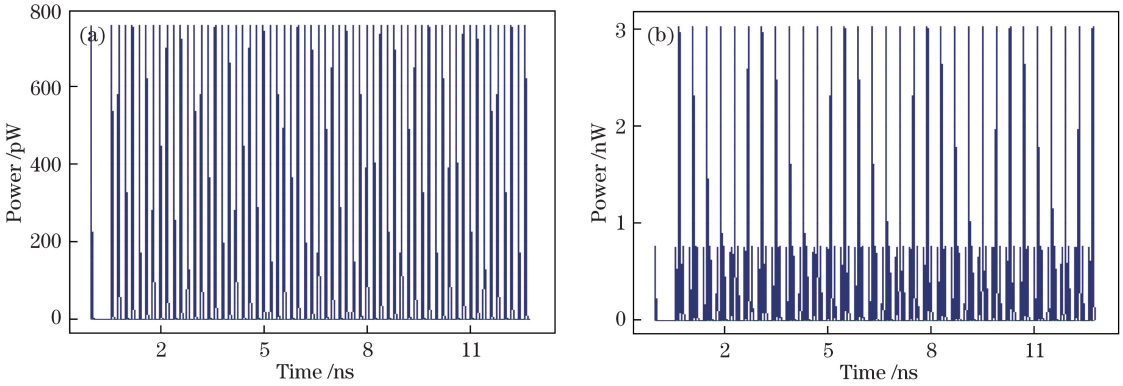

图 9　当 $\Delta\varphi=\pi$ 时，(a)D1 和(b)D2 里的时域波形

Fig. 9　Time domain waveforms in (a) D1 and (b) D2 when $\Delta\varphi=\pi$

当 Alice 和 Bob 所选相位相差为 π/2 或 3π/2 时，两个探测器无明显区别，此时无法判断所传输密钥，两探测器波形如图 10(a)、(b)所示。

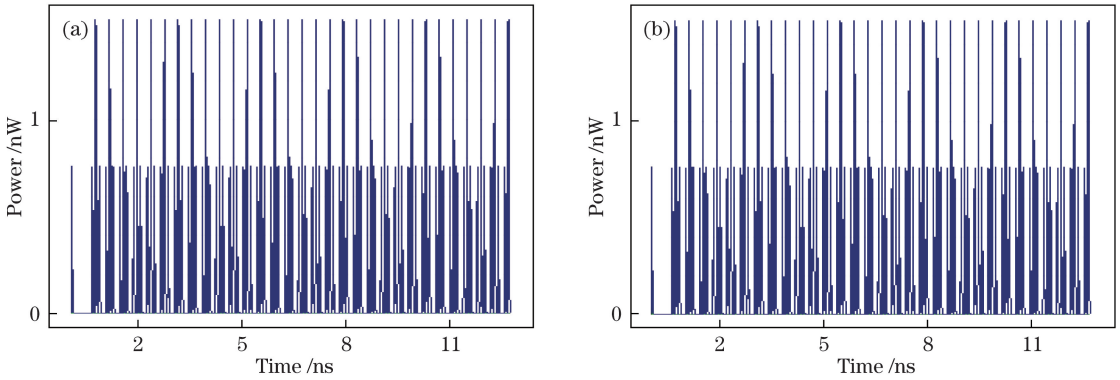

图 10　当 $\Delta\varphi$ 为 π/2 或 3π/2 时，(a)D1 和(b)D2 里的时域波形

Fig. 10　Time domain waveforms in (a) D1 and (b) D2 when $\Delta\varphi$ is π/2 or 3π/2

表 1　系统 QKD 过程

Table 1　QKD process of system

No.	Key sent	Phase chosen by Alice	Phase chosen by Bob	$\Delta\varphi$	Key received by D1	Key received by D2	Key received finally
1	1	π	0	π	0	1	1
2	1	3π/2	0	3π/2	Uncertain	Uncertain	
3	0	π/2	π/2	0	1	0	0
4	1	π	π/2	π/2	Uncertain	Uncertain	
5	1	3π/2	π/2	π	0	1	1
6	1	π	0	π	0	1	1
7	1	π	π/2	π/2	Uncertain	Uncertain	
8	0	0	0	0	1	0	0
9	1	π	π/2	π/2	Uncertain	Uncertain	
10	0	π/2	π/2	0	1	0	0

10 次传输实验中的相位选择以及密钥协商过程如表 1 所示。分析上述结果可知，当相位差为 0 及 π 时，Alice 和 Bob 对基成功，可以正确协商出量子密钥；而当相位差为 π/2 或 3π/2 时，双方对基失败，无法协商出量子密钥。因此，当 Alice 发送 1101111010 时，经与 Bob 协商最终得到的密钥为 101100。

为了研究经典光信号的传输质量，使用光时域波形探测器得到了其传输前后的波形图，如图 11(a)、(b)所示。

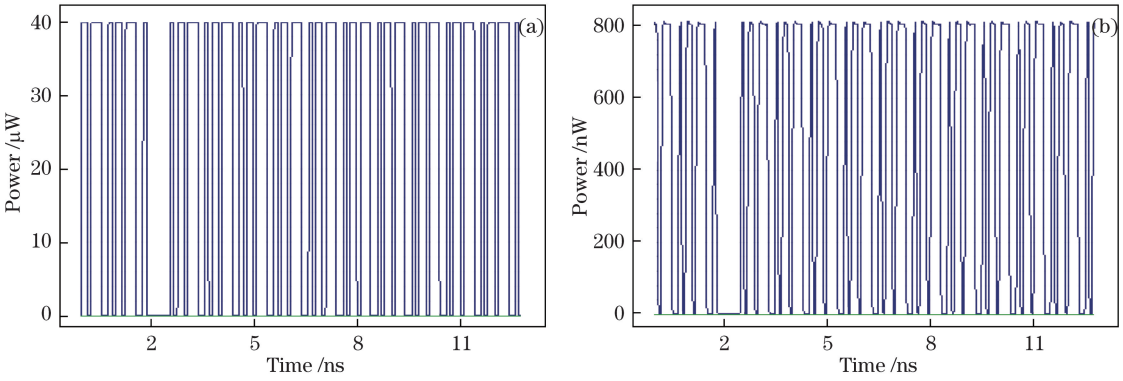

图 11　经典光信号传输(a)前和(b)后的波形

Fig. 11　Waveforms of classical signals (a) before and (b) after transmission

通过比较图 11(a)和图 11(b)，可以发现，除了功率的衰减，波形没有出现较大失真，且具有较小的时延，

说明在两模式发生复用时，波长-模式双复用模式间的色散也较小。

经典光信号的眼图如图 12 所示，可以清楚看到，经典光信号的眼图睁开程度大，不存在明显闭合，迹线清晰，存在重叠但相互影响较小。从误比特率分析仪中得到的信号最低误比特率为 2.7×10^{-15}，品质因数 Q 为 7.8，说明传输过程中信号间串扰和噪声影响小，信号传输质量好。

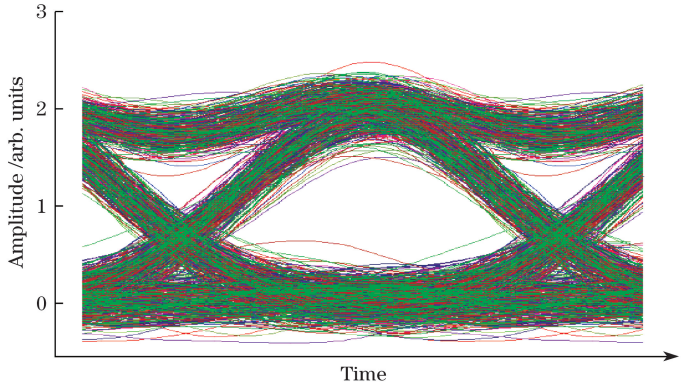

图 12　经典光信号眼图

Fig. 12　Eye diagram of classical light signals

通过对各项实验结果进行分析，发现基于波长-模式双复用的量子保密通信系统能够提高信号的传输质量。

5　结　　论

提出并设计了一种基于波长-模式双复用的量子保密通信系统，对其设计思想进行了详细介绍，在 Optisystem 上建立了相应的模型并进行了 10 次发送实验。结果表明，基于波长-模式双复用的量子保密通信系统充分融合了两种复用方式的优势，能够有效提高信号的隔离度和正交性，减小非线性效应的影响及信号间的串扰，降低系统复杂度，有利于量子-经典信号同传时对量子弱信号的保护，在增加新复用自由度的同时提高了量子-经典信号同传方案的传输质量。下一步可以考虑使用连续变量的 QKD 方案。同时，可以考虑增加系统的复用信号数量，并进一步验证多波长、多模式情况下系统的稳定性和可靠性。

参　考　文　献

[1] Bennett C H, Brassard G. Quantum cryptography: Public key distribution and coin tossing[C]. Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, 1984: 175-179.

[2] Bennett C H. Quantum cryptography using any two non-orthogonal states[J]. Phys Rev Lett, 1992, 68(21): 3121-3124.

[3] Ralph T C. Continuous variable quantum cryptography[J]. Phys Rev A, 1999, 61(1): 010303.

[4] Lo H K, Chau H F, Ardehali M. Efficient quantum key distribution scheme and a proof of its unconditional security[J]. Journal of Cryptology, 2005, 18(2): 133-165.

[5] Patel K A, Dynes J F, Choi I, *et al*. Coexistence of high-bit-rate quantum key distribution and data on optical fiber[J]. Phys Rev X, 2012, 2(4): 041010.

[6] Patel K A, Dynes J F, Lucamarini M, *et al*. Quantum key distribution for 10 Gb/s dense wavelength division multiplexing networks[J]. Appl Phys Lett, 2014, 104(5): 051123.

[7] Chang Yuxin. Research on the two-input two-output mode division multiplexing communication technology[D]. Jilin: Jilin University, 2016.
常玉鑫. 两输入两输出模式复用通信技术研究[D]. 吉林: 吉林大学, 2016.

[8] Tkach R W. Network traffic and system capacity: Scaling for the future[C]. IEEE European Conference and Exhibition on Optical Communication, 2010.

[9] Le Yansi, Wang Zhi, Li Qiang, *et al*. Research of three mode fiber multiplexers and demultiplexers[J]. Chinese J Lasers, 2016, 43(6): 0606004.

乐燕思, 王　智, 李　强, 等. 光纤型三模式复用解复用器的研究[J]. 中国激光, 2016, 43(6): 0606004.

[10] Mao Qianping, Zhao Shengmei, Wang Le, *et al*. Wavelength division multiplexing for measurement-device-independent quantum key distribution[J]. Chinese Journal of Quantum Electronics, 2017(1): 46-53.
毛钱萍, 赵生妹, 王　乐, 等. 基于波分复用技术的测量设备无关量子密钥分发[J]. 量子电子学报, 2017(1): 46-53.

[11] Ren F, Li J, Wu Z, *et al*. Three-mode mode-division-multiplexing passive optical network over 12-km low mode-crosstalk FMF using all-fiber mode MUX/DEMUX[J]. Opt Commun, 2017, 383: 525-530.

[12] Liu Lingling, Jing Mingyong, Yu Bo, *et al*. Polarization control in single photons phase coding quantum key distribution system[J]. Laser & Optoelectronics Progress, 2015, 52(7): 072701.
刘令令, 景明勇, 于　波, 等. 单光子相位编码量子密钥分发系统中的偏振控制[J]. 激光与光电子学进展, 2015, 52(7): 072701.

[13] Qian Chunlin, Chen Mingyang. Investigation on refractive index sensing based on interference effect in multimode optical fiber[J]. Laser & Optoelectronics Progress, 2016, 53(5): 050601.
钱春霖, 陈明阳. 基于多模干涉效应的光纤折射率传感技术研究[J]. 激光与光电子学进展, 2016, 53(5): 050601.