测量设备无关的经典-量子信号共纤传输方案

程康，周媛媛*，王欢
海军工程大学电子工程学院，湖北 武汉 430033

摘要 提出了一种基于测量设备无关协议的经典-量子信号共纤传输方案。推导了自发拉曼散射噪声计数率公式，分析了经典信号入射功率、量子信号复用路数和量子信号平均光子数对量子密钥分配性能的影响。数值仿真结果表明，当经典信号入射功率为 0 dBm(即通信容量为 84.8 Gbit/s)时，所提方案量子密钥分配的最大安全传输距离可达 141 km；当入射功率增加到 11 dBm(即通信容量为 1.068 Tbit/s)时，仍然可达 100 km。相比于现有的最优传输方案，所提方案量子密钥分配的最大安全传输距离延长了 26 km；虽然随着经典信号入射功率的增加，量子密钥分配性能有所下降，但是可以通过采用多路量子信号复用和优化量子信号的平均光子数来进行性能补偿。

关键词 量子光学；测量设备无关；拉曼散射；经典-量子信号
中图分类号 TN918.8+1 **文献标识码** A **doi**：10.3788/LOP56.082701

Scheme of Measurement-Device-Independent Classical-Quantum Signal Transmission in Shared Fiber

Cheng Kang, Zhou Yuanyuan*, Wang Huan
School of Electronic Engineering, Naval University of Engineering, Wuhan, Hubei 430033, *China*

Abstract A scheme of classical-quantum signal transmission in a shared fiber is proposed based on a measurement-device-independent protocol. The counting rate formula of spontaneous Raman scattering noise is deduced and the effects of the incident power of classical signals, channel number of quantum signals and average photon numbers of quantum signals on the quantum key distribution (QKD) performances are analyzed. The numerical simulation results show that the maximum safe transmission distance for the QKD by the proposed scheme is up to 141 km when the incident power of classical signals is 0 dBm (i.e., the communication capacity of 84.8 Gbit/s). Even when the incident power increases to 11 dBm (i.e., the communication capacity of 1.068 Tbit/s), it is still up to 100 km. Compared with the existing optimal transmission scheme, the maximum safe transmission distance of the QKD by the proposed scheme is extended by 26 km. Although the QKD performance decreases with the increase of the incident power of classical signals, the performance can be compensated by the multiplexing channels of quantum signals and the optimization of the average photon numbers of quantum signals.

Key words quantum optics; measurement-device-independence; Raman scattering; classical-quantum signal
OCIS codes 270.5565; 270.5568; 290.5860; 270.5585

1 引 言

考虑到量子信号强度很弱，实际量子密钥分配(QKD)系统会为量子信号单独分配一根光纤并将其与经典光信号隔离，但这种做法会极大地浪费光纤资源。因此，经典信号与量子信号融合在一根光纤中进行传输已成为解决这一问题的重要途径[1-4]。其中，如何提高经典-量子信号共纤传输的安全传输距离和密钥生成率是需要解决的核心问题。

1997 年，英国电信实验室的 Townsend 博士[5]首次完成了一路量子密钥分配和一路经典信号共传的实验，但由于没有采取有效的噪声抑制措施，量子误比特率很高。2005 年，美国电信科学实验室的 Nweke 等[6]通过采取一系列抑制噪声的措施，使得共

收稿日期：2018-10-26；**修回日期**：2018-10-29；**录用日期**：2018-11-03
* **E-mail**：zyy_hjgc@aliyun.com

传距离为 10 km 时对应的最大密钥生成率达到 70 bit/s。2009 年，美国的卓讯科技公司的 Chapuran 等[7]在距离为 25 km 的光纤上实现了安全密钥生成率为 9 bit/s 的传输。2016—2017 年，中国科学技术大学王留军博士等[1-2]基于诱骗态 BB84 协议，将一路量子信号和入射功率为 11 dBm(1.068 Tbit/s)的经典信号反向传输，传输距离达到 70 km，这在目前共纤传输方面性能较优。以上实验都是基于 BB84 协议，但是最大安全传输距离都较近。

近年来，QKD 研究在理论[8-11]和实践[12-15]上都取得了重大的进展，2003 年，Hwang[16]提出了诱骗态的方法，该方法为抵御非理想单光子源导致的光子数分离攻击，提高 QKD 的性能，提供了一种可靠手段。2012 年，多伦多大学的 Tamaki 等[11]提出一种与测量设备无关(MDI)的量子密钥分配方案，该方案的优势在于利用非可信任的第三方进行贝尔态(Bell)测量(BSM)，能够消除所有探测器侧的信道漏洞，同时使得 QKD 的安全传输距离得到了大幅提升。诱骗态思想[16]与测量设备无关协议[17-19]结合使得 QKD 系统在现有技术条件下的安全性和传输距离都有了很大的提升[11-12]。

因此，为提升经典-量子信号共纤传输的最大安全传输距离，本文基于 MDI 诱骗态协议提出了一种新的经典-量子信号共纤传输方案(以下简称“MDI 共传方案”)，重点讨论该方案中量子信号受到的噪声影响，推导出自发拉曼散射(SRS)噪声计数率的计算公式，分析了经典信号入射功率、量子信号复用路数和量子信号平均光子数对量子密钥分配性能的影响。

2 与测量设备无关的经典-量子信号共纤传输方案

2.1 方案描述

经典-量子信号共纤传输系统中一般将经典信号分配在 C 波段(波长 1550 nm 附近)，由于本方案主要考虑大功率经典信号(10 dBm 左右)的传输需求，若将量子信号也分配在 C 波段，就会使得量子信号和经典信号的波长间隔较近，导致量子信号受到的噪声干扰较大，难以产生安全密钥。因此，本方案将量子信号设置在 O 波段(波长 1310 nm 附近)。

本方案提出的 MDI 共传方案原理图如图 1 所示。由于本方案只关心经典信号的总功率，所以假设经典信号为单一波长(λ_c)信号。为了提高量子密钥分配的性能，采用多路量子信号[20](波长 λ_{q1}，λ_{q2}，λ_{q3}，…，λ_{qn})复用来补偿强光噪声对量子信号造成的不良影响。在系统的两端，合法通信双方 Alice 和 Bob 各自将调制后的 n 路量子信号和经典信号通过波分复用(WDM)的方式融合在同一根光纤布拉格光栅(FBG)中进行传输。复用信号到达第三方平台 Charlie 后，通过解复用器(De-WDM)，将量子信号提取出来进行贝尔态测量，经过后处理进而产生安全密钥。本方案假设双端经典信号经过解复用后继续向前传输到达系统终端，且 Alice 至 Charlie 和 Bob 到 Charlie 的信道为对称信道。

系统的编码器采用 Ma 等[19]提出的时间相位复用方案，贝尔态测量装置由一个 50∶50 的分束器及 2 个单光子探测器组成。

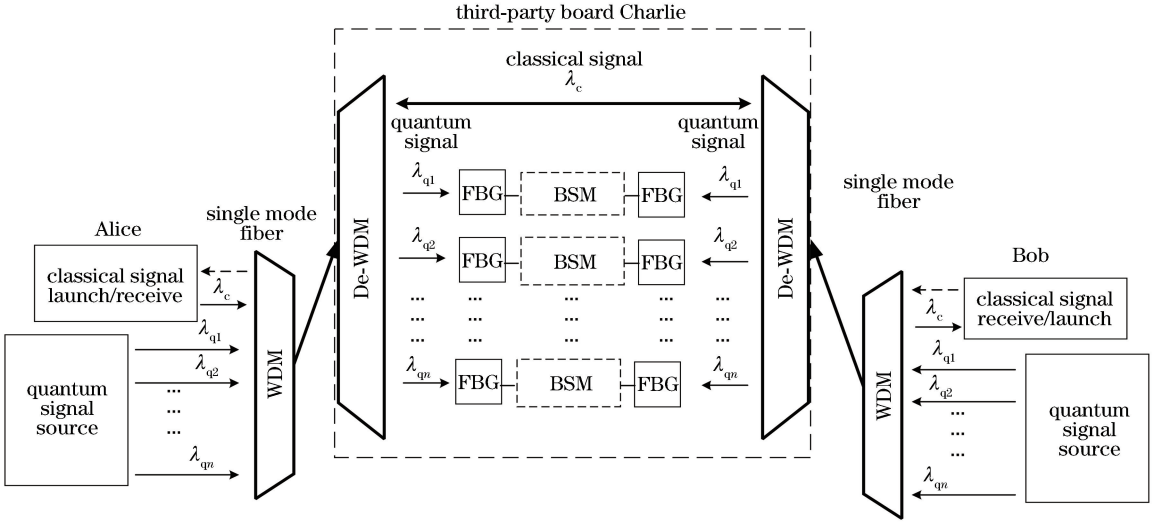

图 1 与测量设备无关的经典-量子信号共纤传输原理图

Fig. 1 Schematic of measurement-device-independent classical-quantum signal transmission in a shared fiber

2.2 背景噪声分析

在多路量子信号与经典信号共纤传输的过程中，量子信号的背景噪声主要来自经典信号的SRS噪声、四波混频、布里渊散射、瑞利散射[2,21]。瑞利散射为弹性散射，其波长与经典信号的波长一致，故不会对量子信道产生影响。由于本方案中，量子信道设置在O波段，与经典信道波长相距200 nm以上，四波混频和布里渊散射噪声带宽较窄，故这两种噪声源同样不会影响到量子信道。但由于SRS噪声的带宽最大可达50 THz[2,22]，故SRS噪声会影响量子信道。此外，SRS噪声的强度虽然不大，但相比平均光子数小于1的量子信号，其影响不可忽视。对于多路量子信号，由于其本身强度很弱，相互之间的影响可忽略。综上，在本方案中主要考虑对量子信号影响最大的噪声源——SRS噪声。下面对该方案中的SRS噪声进行分析。

SRS噪声的产生机理如下：抽运光注入光纤后，其部分能量转化为拉曼散射光，当抽运光的强度小于阈值时（一般情况下，这个阈值非常高[21]），光纤分子的热平衡没有被破坏，产生的拉曼散射光为自发拉曼散射光。自发辐射光子向任意方向辐射，且它们之间没有相位关系[21]，沿经典信号传输方向向前辐射的SRS噪声称为前向自发拉曼散射噪声，沿经典信号传输方向向后辐射的SRS噪声称为后向自发拉曼散射噪声。

前向自发拉曼散射噪声功率 P_{f} 和后向自发拉曼散射的噪声功率 P_{b} 一般计算公式为[23-24]

$$P_{\mathrm{f}}=\frac{P_{\mathrm{in}}(0)\rho\Delta x}{\alpha_{\mathrm{q}}-\alpha_{\mathrm{d}}}\left[\exp(-\alpha_{\mathrm{d}}L)-\exp(-\alpha_{\mathrm{d}}L)\right],\tag{1}$$

$$P_{\mathrm{b}}=\frac{P_{\mathrm{in}}(0)\rho\Delta x}{\alpha_{\mathrm{q}}+\alpha_{\mathrm{d}}}\{1-\exp[-(\alpha_{\mathrm{q}}+\alpha_{\mathrm{d}})L]\},\tag{2}$$

式中：$P_{\mathrm{in}}(0)$ 为经典信号入射功率；ρ 为自发拉曼散射系数，与经典信号和量子信号的波长以及量子信号的接收带宽 Δx 有关，前向、后向自发拉曼散射系数相同；α_{q} 为量子信号的光纤损耗系数；α_{d} 为经典信号的光纤损耗系数；L 为光纤长度。

本方案中，前向自发拉曼散射光和后向自发拉曼散射光经过的光路有所不同，经典入射光经过Alice端的波分复用器之后进入到光纤中，产生的前向自发拉曼散射光经过波分解复用器、光纤布拉格光栅滤波器进入到Bell态测量装置，经典信号穿过第三方平台进入到Charlie与Bob端之间的光纤时，产生的后向自发拉曼散射光再次返回经过波分解复用器、第三方平台的FBG滤波器进入到Bell态测量装置。若Bell态测量装置检测到的不是量子信号而是噪声光子就会出现误码，进而影响经典-量子信号共纤传输的密钥生成率。

因此，进入到测量装置的前向SRS的光功率 P_{Af}、后向SRS的光功率 P_{Ab} 表示为

$$P_{\mathrm{Af}}=\frac{\rho\Delta xP_{\mathrm{in}}(0)}{\alpha_{\mathrm{q}}-\alpha_{\mathrm{d}}}\left[\exp(-\alpha_{\mathrm{d}}L)-\exp(-\alpha_{\mathrm{q}}L)\right]10^{-(l_{\mathrm{wdm}}+l_{\mathrm{B}}+l_{\mathrm{FBG}})/10},\tag{3}$$

$$P_{\mathrm{Ab}}=\rho\Delta xP_{\mathrm{in}}(0)\left\{\frac{1-\exp[-(\alpha_{\mathrm{d}}+\alpha_{\mathrm{q}})L]}{\alpha_{\mathrm{d}}+\alpha_{\mathrm{q}}}\right\}\times\exp(-\alpha_{\mathrm{d}}L)10^{-(2l_{\mathrm{wdm}}+l_{\mathrm{B}}+l_{\mathrm{FBG}})/10},\tag{4}$$

式中：l_{wdm} 为波分复用器的插入损耗；l_{B} 为单光子探测器的内部损耗；l_{FBG} 为用于波长滤波的滤波器的插入损耗。

此处，定义一个系统时钟周期内被单光子探测器探测到的自发拉曼散射噪声光子数为自发拉曼散射噪声的计数率，除了与SRS噪声的功率有关外，还受到单光子探测器性能的影响，与探测效率 η_{det}、单光子探测器的时间门限 Δt 有关。

由于本文假设的系统是对称的，因此在经典信号入射功率相同的情况下，该方案量子信号相对经典信号同向传输或反向传输进入单光子探测器的SRS噪声计数率是相同的。另外，信号进入单光子探测器之前需要经过分束器（BS），噪声强度衰减为1/2。因此，该方案量子信号相对经典信号同向传输或反向传输进入到单光子探测器的SRS噪声的计数率分别为

$$P_{\mathrm{rcount}}=\frac{(P_{\mathrm{Af}}+P_{\mathrm{Ab}})}{2hc/\lambda_{1310}}\eta_{\mathrm{det}}\Delta t=\frac{P_{\mathrm{in}}(0)\rho_1\Delta x}{2hc/\lambda_{1310}}\left\{\frac{\exp(-\alpha_{\mathrm{d}}L)-\exp(-\alpha_{\mathrm{q}}L)}{\alpha_{\mathrm{q}}-\alpha_{\mathrm{d}}}+\frac{1-\exp[-(\alpha_{\mathrm{d}}+\alpha_{\mathrm{q}})L]}{\alpha_{\mathrm{d}}+\alpha_{\mathrm{q}}}\exp(-\alpha_{\mathrm{d}}L)\,10^{-l_{\mathrm{wdm}}/10}\right\}\times\eta_{\mathrm{det}}\Delta t\,10^{-(l_{\mathrm{wdm}}+l_{\mathrm{FBG}}+l_{\mathrm{B}})/10},\tag{5}$$

式中：hc/λ_{1310} 为波长为1310 nm的单个噪声光子的能量，h 为普朗克常量，c 为光速；ρ_1 为采用本方案的自发拉曼散射系数。

当同时存在Alice到Bob和Bob到Alice两个方向的经典信号时，此时进入到单光子探测器的自发拉曼散射噪声计数率为

$$P_{\mathrm{rcount2}}=P_{\mathrm{rcount}}\times2=\frac{(P_{\mathrm{Af}}+P_{\mathrm{Ab}})}{hc/\lambda_{1310}}\eta_{\mathrm{det}}\Delta t=$$

$$\frac{P_{\mathrm{in}}(0)\rho_1\Delta x}{hc/\lambda_{1310}}\left\{\frac{\exp(-\alpha_{\mathrm{d}}L)-\exp(-\alpha_{\mathrm{q}}L)}{\alpha_{\mathrm{q}}-\alpha_{\mathrm{d}}}+\frac{1-\exp[-(\alpha_{\mathrm{d}}+\alpha_{\mathrm{q}})L]}{\alpha_{\mathrm{d}}+\alpha_{\mathrm{q}}}\exp(-\alpha_{\mathrm{d}}L)\ 10^{-l_{\mathrm{wdm}}/10}\right\}\times\eta_{\mathrm{det}}\Delta t\,10^{-(l_{\mathrm{wdm}}+l_{\mathrm{FBG}}+l_{\mathrm{B}})/10}。\tag{6}$$

2.3 密钥生成率的计算

为便于分析，假设量子信号的复用路数为 N，认为各量子信道的物理特性一致，即各信道的 SRS 噪声和光纤损耗系数不存在差异。因此，总的密钥生成率 R 与第 i 路波长为 λ_i 的密钥生成率 R_i 的关系为

$$R=NR_i。\tag{7}$$

对单路波长为 λ_i 的量子信号与经典强光信号共传过程，由诱骗态原理和 MDI-QKD 协议，可得密钥生成率[19,25]，即

$$R_i=G_{Z_i}^{11}[1-H(e_{X_i}^{11})]-G_{Z_i}fH(E_{Z_i}),\tag{8}$$

式中：$G_{Z_i}^{11}$ 为当 Alice 和 Bob 同时选择相同的 Z 基且都发送单光子态时的增益；$H(e_{X_i}^{11})$ 对应密钥放大过程，$e_{X_i}^{11}$ 为 Alice 和 Bob 同时选择 X 基且都发送单光子态时的量子比特误码率(QBER)；G_{Z_i} 和 E_{Z_i} 分别为光源选择 Z 基时的总增益和总 QBER，二者均可以由实验测得；f 为数据协调纠错的效率函数；$H(x)$ 为二元熵函数；$G_{Z_i}fH(E_{Z_i})$ 为进行协调纠错产生的损耗。

设 Alice 和 Bob 发送的平均光子数分别为 μ_{A_i}、μ_{B_i}，Alice 和 Bob 信道的传输效率分别为 η_{A_i}、η_{B_i}，背景噪声计数率为 P_{k}，基不匹配率为 e_{d}，则

$$G_{Z_i}=G_{Z_i}^{\mathrm{C}}+G_{Z_i}^{\mathrm{E}},\tag{9}$$

$$E_{Z_i}G_{Z_i}=e_{\mathrm{d}}G_{Z_i}^{\mathrm{C}}+(1-e_{\mathrm{d}})G_{Z_i}^{\mathrm{E}},\tag{10}$$

而

$$G_{Z_i}^{\mathrm{C}}=2(1-P_{\mathrm{k}})^2\exp\left(-\frac{\mu_i'}{2}\right)\times\left[1-(1-P_{\mathrm{k}})\exp\left(-\frac{\eta_{\mathrm{A}_i}\mu_{\mathrm{A}_i}}{2}\right)\right]\times\left[1-(1-P_{\mathrm{k}})\exp\left(-\frac{\eta_{\mathrm{B}_i}\mu_{\mathrm{B}_i}}{2}\right)\right],\tag{11}$$

$$G_{Z_i}^{\mathrm{E}}=2P_{\mathrm{k}}(1-P_{\mathrm{k}})^2\exp\left(-\frac{\mu_i'}{2}\right)\times\left[\mathrm{I}_0(2x_i)-(1-P_{\mathrm{k}})\exp\left(-\frac{\mu_i'}{2}\right)\right],\tag{12}$$

式中：$\mathrm{I}_0(x_n)$ 为第一类修正贝塞尔函数。P_{k} 为一个单光子探测器的背景噪声[19]，即

$$P_{\mathrm{k}}\approx P_{\mathrm{dc}}+P_{\mathrm{rcount}},\tag{13}$$

式中：P_{dc} 为单光子探测器的暗计数率；P_{rcount} 为自发拉曼散射噪声计数率。因此(5)、(6)式将通过影响(13)式进而影响共纤传输的量子密钥生成率。

由于本文所述系统的第三方 Charlie 在 Alice 和 Bob 的中间，因此有 $\eta_{\mathrm{A}_i}=\eta_{\mathrm{B}_i}=\eta_i$，$\mu_{\mathrm{A}_i}=\mu_{\mathrm{B}_i}=\mu_i$。于是

$$\mu_i'=\eta_{\mathrm{A}_i}\mu_{\mathrm{A}_i}+\eta_{\mathrm{B}_i}\mu_{\mathrm{B}_i}=2\eta_i\mu_i,\tag{14}$$

$$x_i=\frac{\sqrt{\eta_{\mathrm{A}_i}\mu_{\mathrm{A}_i}\eta_{\mathrm{B}_i}\mu_{\mathrm{B}_i}}}{2}=\frac{\eta_i\mu_i}{2},\tag{15}$$

因此，将(14)、(15)式代入到(11)、(12)式可化简得

$$G_{Z_i}^{\mathrm{C}}=2(1-P_{\mathrm{k}})^2\exp(-\eta_i\mu_i)\times[1-(1-P_{\mathrm{k}})\exp(-\eta_i\mu_i/2)]^2,\tag{16}$$

$$G_{Z_i}^{\mathrm{E}}=2P_{\mathrm{k}}(1-P_{\mathrm{k}})^2\exp(-\eta_i\mu_i)\times[\mathrm{I}_0(\eta_i\mu_i)-(1-P_{\mathrm{k}})\exp(-\eta_i\mu_i)]。\tag{17}$$

将(16)、(17)式代入(9)、(10)式，可得

$$G_{Z_i}=2(1-P_{\mathrm{k}})^2\exp(-\eta_i\mu_i)\{[1-(1-P_{\mathrm{k}})\exp(-\eta_i\mu_i/2)]^2+P_{\mathrm{k}}[\mathrm{I}_0(\eta_i\mu_i)-(1-P_{\mathrm{k}})\exp(-\eta_i\mu_i)]\},\tag{18}$$

$$E_{Z_i}=\frac{e_{\mathrm{d}}[1-(1-P_{\mathrm{k}})\exp(-\eta_i\mu_i/2)]^2+(1-e_{\mathrm{d}})P_{\mathrm{k}}[\mathrm{I}_0(\eta_i\mu_i)-(1-P_{\mathrm{k}})\exp(-\eta_i\mu_i)]}{[1-(1-P_{\mathrm{k}})\exp(-\eta_i\mu_i/2)]^2+P_{\mathrm{k}}[\mathrm{I}_0(\eta_i\mu_i)-(1-P_{\mathrm{k}})\exp(-\eta_i\mu_i)]}。\tag{19}$$

此外，(8)式中的 $G_{Z_i}^{11}$ 和 $e_{X_i}^{11}$，可表示为

$$G_{Z_i}^{11}=\mu_{\mathrm{A}_i}\mu_{\mathrm{B}_i}\exp[-(\mu_{\mathrm{A}_i}+\mu_{\mathrm{B}_i})]Y_{Z_i}^{11}=\mu_i\exp(-2\mu_i)Y_{Z_i}^{11},\tag{20}$$

$$e_{X_i}^{11}Y_{X_i}^{11}=e_0Y_{X_i}^{11}-(e_0-e_{\mathrm{d}})(1-P_{\mathrm{k}})^2\frac{\eta_{\mathrm{A}_i}\eta_{\mathrm{B}_i}}{2}=e_0Y_{X_i}^{11}-(e_0-e_{\mathrm{d}})(1-P_{\mathrm{k}})^2\frac{\eta_i^2}{2},\tag{21}$$

式中：$Y_{X_i}^{11}$ 和 $Y_{Z_i}^{11}$ 分别代表当 Alice 和 Bob 均发送单光子且同时选择 X 基或 Z 基的计数率，当采用无限多个诱骗态时，$Y_{X_i}^{11}$ 被估计为

$$Y_{X_i}^{11}=Y_{Z_i}^{11}=(1-P_{\mathrm{k}})^2\left[\frac{\eta_{\mathrm{A}_i}\eta_{\mathrm{B}_i}}{2}+(2\eta_{\mathrm{A}_i}+2\eta_{\mathrm{B}_i}-3\eta_{\mathrm{A}_i}\eta_{\mathrm{B}_i})P_{\mathrm{k}}+4(1-\eta_{\mathrm{A}_i})(1-\eta_{\mathrm{B}_i})P_{\mathrm{k}}^2\right]=(1-P_{\mathrm{k}})^2\left[\frac{\eta_i^2}{2}+(4\eta_i-3\eta_i^2)P_{\mathrm{k}}+4(1-\eta_i)^2P_{\mathrm{k}}^2\right]。\tag{22}$$

将(22)式代入到(20)式和(21)式得到 $G_{Z_i}^{11}$ 和 $e_{X_i}^{11}$ 的表达式为

$$G_{Z_i}^{11}=\mu_i^2\exp(-2\mu_i)\,(1-P_{\mathrm{k}})^2\times\left[\frac{\eta_i^2}{2}+(4\eta_i-3\eta_i^2)P_{\mathrm{k}}+4\,(1-\eta_i)^2P_{\mathrm{k}}^2\right],\tag{23}$$

$$e_{X_i}^{11}=e_0-\frac{(e_0-e_{\mathrm{d}})\,\eta_i^2}{\eta_i^2+(8\eta_i-6\eta_i^2)P_{\mathrm{k}}+8\,(1-\eta_i)^2P_{\mathrm{k}}^2}。\tag{24}$$

根据文献[1],系统的全局传输损耗为

$$\eta_i=10^{-l_B/10}\exp(-\alpha_{\mathrm{q}}L)\,\eta_{\mathrm{det}},\tag{25}$$

将(18)、(19)、(23)、(24)、(25)式代入到(8)式,并利用(7)式可得总的密钥生成率 R。

3 数值仿真与分析

为了方便与文献[1]的工作进行比较,选取文献[1]的仿真参数:自发拉曼散射系数 ρ_1 为 1.057×10^{-11} nm^{-1}·km^{-1},量子信号源的脉冲发射频率 625 MHz,信号态、弱诱骗态、空诱骗态的发射概率比为 6∶1∶1,单光子探测效率 η_{det} 为 10%,探测器的频率为 1.25 GHz,探测器的暗计数率和内部损耗分别为 1×10^{-6} 和 3 dB。O 波段光纤损耗为 0.33 dB/km,C 波段的光纤损耗为 0.20 dB/km。波分复用设备的插入损耗为 1.6 dB,FBG 窄带滤波器的带宽和插入损耗分别为 0.572 nm 和 0.5 dB,光子击中错误探测的概率 e_{d} 为 0.005,错误纠正效率 f 为 1.25,背景噪声产生的误码率 e_0 为 0.5。本仿真平均光子数根据传输距离选取最优平均光子数。

图 2 是采用 MDI 共传方案,一路量子信号与入射功率分别为 0 dBm,5 dBm,10 dBm,15 dBm 的经典信号共传得到的密钥生成率随传输距离的变化曲线。从图中可以看出,当经典信号入射功率为 0 dBm(相当于通信容量为 84.8 Gbit/s)时,所提 MDI 共传方案最大安全传输距离为 141 km,当经典信号入射功率增加到 10 dBm 和 15 dBm(分别相当于 0.85 Tbit/s 和 3.38 Tbit/s 的通信容量)时,所提 MDI 共传方案仍然可达 108 km 和 62 km。

图 3 为经典光功率为 11 dBm 时,MDI 共传方案和 BB84 共传方案[1]的密钥生成率与传输距离的关系图。从图中可以看出,在量子信号为 1 路时,MDI 共传方案的最大安全传输距离为 100 km,较 BB84 共传方案的最大安全传输距离延长了26 km,但是密钥生成率较 BB84 共传方案要低。随着量子信号复用路数的增加,MDI 共传方案的密钥生成率显著提升,当复用路数达到 40 路时,总的密钥生成

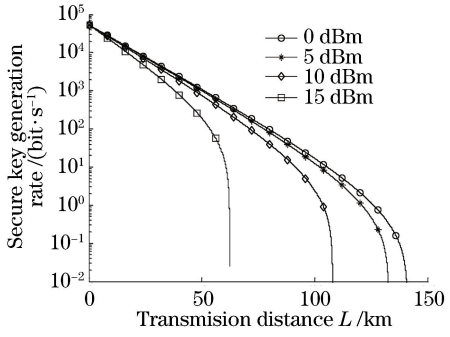

图 2 一路量子信号与不同入射功率的经典信号共传得到的密钥生成率与传输距离 L 的关系

Fig. 2 Relationship between key generation rate and transmission distance L obtained by co-transmission of one quantum channel and classical signals with different incident powers

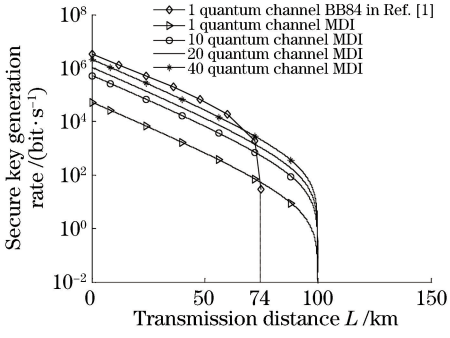

图 3 不同共传方案下的密钥生成率与传输距离 L 间的关系

Fig. 3 Relationship between key generation rate and transmission distance L under different co-transmission schemes

率接近 BB84 共传方案的密钥生成率。可见,量子信号的多路复用可有效补偿 MDI 共传方案的单路密钥生成率较低的弱势。

图 4 为不同经典信号入射功率条件下,MDI 共传方案最优平均光子数与传输距离的关系图。从该曲线可以看出,相比于文献[1]的 BB84 共传方案,MDI 共传方案的最优平均光子数偏低,这也从另一个角度解释了图 3 中在传输距离较近时,MDI 共传方案的密钥生成率低于 BB84 共传方案的现象。因此,在实际经典-量子信号共纤传输系统中,可以通过优化量子信号的平均光子数来提高总的密钥生成率。

4 结 论

与以往基于 BB84 协议的经典-量子信号共纤传输方案不同,提出了一种基于测量设备无关的经典-量子信号共纤传输方案,进一步提升了共纤传输

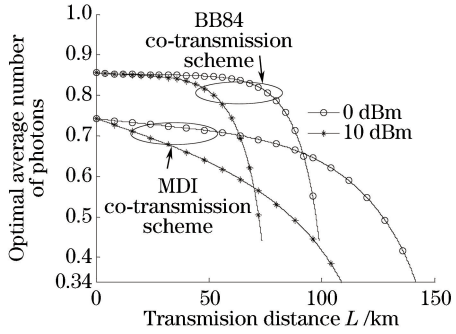

图 4 不同经典信号入射功率下最优平均光子数与传输距离的关系

Fig. 4 Relationship between optimal averagenumber of photons and transmission distance under different incident powers of classical signals

的最大安全传输距离。在推导 SRS 噪声计数率计算公式的基础上，分析了经典信号入射功率、量子信号复用路数和平均光子数对本方案密钥生成率的影响。根据数值仿真分析得出：本方案不仅在经典信号入射功率较低（0 dBm）时能实现较远距离（141 km）的共纤传输，即使在经典信号入射功率增加到 11 dBm 时，最大安全传输距离也能达到 100 km；相比于文献[1]的 BB84 共传方案，本方案将一路量子信号与 11 dBm（相当于 1.068 Tbit/s 的通信容量）经典信号共传的最大安全传输距离延长 26 km；在实际经典-量子信号共纤传输系统中，可以通过复用多路量子信号和优化量子信号的平均光子数来进行性能补偿。

参 考 文 献

[1] Wang L J, Zou K H, Sun W, *et al*. Long distance co-propagation of quantum key distribution and terabit classical optical data channels[J]. Physical Review A, 2017, 95(1):012301.

[2] Mao Y Q, Wang B X, Zhao C X, *et al*. Integrating quantum key distribution with classical communications in backbone fiber network [J]. Optics Express, 2018, 26(5): 6010.

[3] Luo J W, Li Y X, Shi L, *et al*. Co-fiber-transmission technology for quantum signal and classical optical signal based on mode division multiplexing in few-mode fiber [J]. Laser & Optoelectronics Progress, 2017, 54(2): 022702.
罗均文, 李云霞, 石磊, 等. 基于少模光纤模分复用的量子信号-经典光信号共纤同传技术[J]. 激光与光电子学进展, 2017, 54(2): 022702.

[4] Luo J W, Li Y X, Meng W, *et al*. Quantum private communication system based on wavelength-mode division co-multiplexing [J]. Acta Optica Sinica, 2017, 37(9): 0927001.
罗均文, 李云霞, 蒙文, 等. 基于波长-模式双复用的量子保密通信系统[J]. 光学学报, 2017, 37(9): 0927001.

[5] Townsend P D. Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fiber using wavelength-division multiplexing[J]. Electronics Letters, 1997, 33(3): 188-190.

[6] Nweke N I, Toliver P, Runser R J, *et al*. Experimental characterization of the separation between wavelength: multiplexed quantum and classical communication channels [J]. Applied Physics Letters, 2005, 87(17): 174103.

[7] Chapuran T E, Toliver P, Peter N A, *et al*. Optical networking for quantum key distribution and quantum communications[J]. New Journal of Physics, 2009, 11(10): 105001.

[8] Grosshans F, Grangier P. Continuous variable quantum cryptography using coherent states [J]. Physical Review Letters, 2002, 88(5): 057902.

[9] Scarani V, Acín A, Ribordy G, *et al*. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations [J]. Physical Review Letters, 2004, 92(5): 057901.

[10] Ma X F, Qi B, Zhao Y, *et al*. Practical decoy state for quantum key distribution[J]. Physical Review A, 2005, 72(1): 012326.

[11] Tamaki K, Lo H K, Fung C H F, *et al*. Phase encoding schemes for measurement-device-independent quantum key distribution with basis-dependent flaw [J]. Physical Review A, 2012, 85(4): 042307.

[12] Yin H L, Chen T Y, Yu Z W, *et al*. Measurement-device-independent quantum key distribution over a 404 km optical fiber [J]. Physical Review Letters, 2016, 117(19): 190501.

[13] Peng C Z, Pan J W. Quantum science experimental satellite "Micius"[J]. Bulletin of Chinese Academy of Sciences, 2016, 31(9): 1096-1104.
彭承志, 潘建伟. 量子科学实验卫星："墨子号"[J]. 中国科学院院刊, 2016, 31(9): 1096-1104.

[14] Poppe A, Peev M, Maurhart O. Outline of the SECOQC quantum-key-distribution network in vienna [J]. International Journal of Quantum Information, 2008, 6(2): 209-218.

[15] Chen G, Zhang L J, Zhang W H, *et al*. Achieving Heisenberg-scaling precision with projective measurement on single photons[J]. Physical Review Letters, 2018, 121(6): 060506.

[16] Hwang W Y. Quantum key distribution with high loss: Toward global secure communication [J]. Physical Review Letters, 2003, 91(5): 057901.

[17] Sun Y, Zhao S H, Dong C. Measurement device independent quantum key distribution network based on quantum memory and entangled photon sources [J]. Acta Optica Sinica, 2016, 36(3): 0327001.
孙颖, 赵尚弘, 东晨. 基于量子存储和纠缠光源的测量设备无关量子密钥分配网络[J]. 光学学报, 2016, 36(3): 0327001.

[18] Tang Y L, Yin H L, Chen S J, *et al*. Publisher′s note: Measurement-device-independent quantum key distribution over 200 km [J]. Physical Review Letters, 2015, 114(6): 069901.

[19] Ma X F, Razavi M. Alternative schemes for measurement-device-independent quantum key distribution[J]. Physical Review A, 2012, 86(6): 062319.

[20] Mao Q P, Zhao S M, Wang L, *et al*. Measurement-device-independent quantum key distribution based on wavelength division multiplexing technology [J]. Chinese Journal of Quantum Electronics, 2017, 34(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, 34(1): 46-53.

[21] Agrawal G P. Fiber-optic communication systems [M]. Jia D F, Xin X J, Transl. 4th ed. Beijng: Publishing House of Electronics Industry, 2016: 60.
Agrawal G P.光学与光电子学: 光纤通信系统[M]. 贾东方, 忻向军, 译. 4 版. 北京: 电子工业出版社, 2016: 60.

[22] Aleksic S, Hipp F, Winkler D, *et al*. Perspectives and limitations of QKD integration in metropolitan area networks[J]. Optics Express, 2015, 23(8): 10359.

[23] Wang L J. Experimental study of multiplexing quantum key distribution and classical optical communications[D]. Hefei: University of Science and Technology of China, 2016.
王留军. 量子密钥分发与经典光通信融合的实验研究[D]. 合肥: 中国科学技术大学, 2016.

[24] Wang Y S, Li Y X, Shi L, *et al*. The analysis of the noise in multiplexed classical and quantum transmission system based on DWDM [J]. Acta Sinica Quantum Optica, 2014, 20(4): 296-301.
王宇帅, 李云霞, 石磊, 等. 基于 DWDM 的经典-量子信息共信道同传系统噪声分析[J]. 量子光学学报, 2014, 20(4): 296-301.

[25] Zhu F, Zhang C H, Liu A P, *et al*. Enhancing the performance of the measurement-device-independent quantum key distribution with heralded pair-coherent sources[J]. Physics Letters A, 2016, 380(16): 1408-1413.