基于轨道角动量的循环差分相移量子密钥分发

沈志冈**, 王乐, 毛钱萍, 赵生妹*
南京邮电大学信号处理与传输研究院, 江苏 南京 210003

摘要 提出了一种基于标记配对相干态(HPCS)和轨道角动量的循环差分相移量子密钥分发(RRDPS-QKD)方案,以光子轨道角动量作为信息载体,使用多种不同拓扑荷的轨道角动量的叠加态进行 RRDPS-QKD 的信息编码,显著提高了密钥生成率。使用 HPCS 作为量子光源,有效减小了空脉冲和多光子脉冲的比例,提高了密钥生成率。分析了光源在湍流大气信道中的传输特性,考虑了信道衰减和大气湍流对系统性能的影响。

关键词 量子光学; 量子密钥分发; 轨道角动量; 标记配对相干态
中图分类号 O431.2 **文献标识码** A **doi**: 10.3788/AOS201939.0227001

Round-Robin Differential Phase Shift Quantum Key Distribution Protocol Based on Orbital Angular Momentum

Shen Zhigang**, Wang Le, Mao Qianping, Zhao Shengmei*
Institute of Signal Processing and Transmission, Nanjing University of Posts and Telecommunications, Nanjing, Jiangsu 210003, *China*

Abstract A round-robin differential phase shift quantum key distribution (RRDPS-QKD) protocol based on heralded pair-coherent source (HPCS) and orbital angular momentum is proposed. The superposition state consisting of multiple orbital angular momentum states with different topological charges is used as the information carriers to remarkably increase the key generation rate. HPCS is used as the quantum source to decrease the ratio of vacuum and multi-photon pulses and to dramatically increase the key generation rate. Moreover, the propagation characteristics in the turbulent atmosphere channel are analyzed, and the influence of both channel attenuation and atmospheric turbulence on the protocol is considered.

Key words quantum optics; quantum key distribution; orbital angular momentum; heralded pair-coherent source
OCIS codes 270.5568; 270.5565; 010.1330

1 引 言

量子密钥分发(QKD)[1-3]能够为分隔两地的用户提供无条件安全的密钥,但是该安全性的前提是以完美的单光子源作为光源,而在现实世界中,完美的单光子源很难实现。Wang 等[4-5]提出了实用的诱骗态方法,促进了 QKD 的实用化发展。用标记配对相干态(HPCS)[6-9]等性能更优的量子光源代替弱相干态,可以减小空脉冲和多光子脉冲的比例,有效地提高密钥生成率,提升 QKD 的性能。

Sasaki 等[10-11]提出的循环差分相移量子密钥分发(RRDPS-QKD)可以不需要通过监控传输过程中的密钥错误率来进行密钥放大,这不仅减少了实际 QKD 过程中的操作步骤,而且可以容忍很高的密钥错误率,理论上可达 50%。Zhang 等[12]将标签技术和诱骗态方法应用到 RRDPS-QKD 协议中,推导得到更为严格的相位错误率上限。Mao 等[13]提出了基于不可信光源的即插即用 RRDPS-QKD 方案,可以对信道产生的双折射效应进行自我补偿,使得系统具有较好的稳定性,也降低了对光源的安全性要求。但是上述方案都是采用一串由 L 个脉冲组成的脉冲序列编码信息,理论上平均每个脉冲只能生成 $1/L$ bit 的密钥。

目前,QKD 主要使用偏振、相位对量子态进行编码,而利用轨道角动量(OAM)的高维性、正交性、旋转对称性特点对量子态进行轨道角动量编码可以

收稿日期: 2018-08-21; **修回日期**: 2018-09-17; **录用日期**: 2018-10-08
基金项目: 国家自然科学基金(61475075)、国家电网科技项目(SGRIXTKJ[2017]459)
* **E-mail**: zhaosm@njupt.edu.cn; ** **E-mail**: shenzg@126.com

获得更好的性能。Mirhosseini 等[14]利用弱相干态作为量子光源验证了轨道角动量编码的高维 QKD 实验。

本文提出了一种基于 HPCS 和轨道角动量的 RRDPS-QKD 方案，采用光子轨道角动量作为信息载体，实现 RRDPS-QKD 协议。使用 L 种不同拓扑荷的轨道角动量的叠加态进行 RRDPS-QKD 的信息编码，理论上一个脉冲就能产生 1 bit 的密钥，显著提高了密钥生成率。本方案还采用 HPCS 作为量子光源，减小空脉冲和多光子脉冲的比例，有效提高了密钥生成率。此外，分析了在湍流大气信道中的传输特性，分别考虑了信道衰减和大气湍流对系统性能的影响。

本文方案具有如下优势：1）使用 L 种不同拓扑荷的轨道角动量的叠加态进行 RRDPS-QKD 的信息编码，理论上一个脉冲就能产生 1 bit 的密钥，显著提高了密钥生成率；2）不需要通过监控传输过程中的密钥错误率来进行密钥放大，这不仅减少了实际 QKD 过程中的操作步骤，而且可以容忍很高的密钥错误率，理论上可达 50%；3）由于光子的轨道角动量具有旋转对称性，使用光子轨道角动量作为编码方式时不需要实时校准轨道角动量的参考系，降低了系统的复杂度，提升了系统性能；4）使用 HPCS 作为量子光源，减小了空脉冲和多光子脉冲的比例，增大了密钥生成率；5）使用三种强度的诱骗态即可有效地估计密钥生成率，提高了方案的可行性。

2　方案描述

目前研究者常使用强度极弱的弱相干态脉冲作为量子光源，脉冲中包含 n 个光子的概率服从泊松分布。但是弱相干态光源存在两个缺点，一是存在大量的空脉冲，计数率小，另一缺陷是存在多光子脉冲，可能受到窃听者的光子数分离攻击[1]，这给 QKD 系统带来了严重的安全问题。多光子脉冲问题可以通过诱骗态技术[4-5]来解决，而针对空脉冲比例高的缺点可以使用改进的光源来减小空脉冲比例，提升 QKD 的性能。

使用 HPCS[6-9]代替弱相干态可以提升 QKD 的性能。其中配对相干态是一个两模式关联的相干态，可以表示为 Fock 态：

$$|\phi\rangle=\frac{1}{\sqrt{\mathrm{I}_0(2|\mu|)}}\sum_n\frac{\mu^n}{n!}|n\rangle_1|n\rangle_2,\qquad(1)$$

式中：μ 为脉冲的平均强度；$\mathrm{I}_0(x)$为第一类修正贝塞尔函数；n 为光子数；$|n\rangle_1|n\rangle_2$为两模式关联的相干态。配对相干态光源由 Agarwal[6]首先提出。将光子标记技术[15]应用于配对相干态光源中，即把配对相干态光源所产生的一个光子送入单光子探测器中，用于标记另一个模式的状态，仅当单光子探测器有响应时才把另一个模式用于编码信息。此时，另一个可用于编码信息的模式中包含 n 个光子的概率为[9]

$$P_n(\mu)=\frac{1}{P_{\mathrm{post}}(\mu)}[1-(1-d_{\mathrm{A}})(1-\eta_{\mathrm{A}})^n]\frac{\mu^{2n}}{(n!)^2},\qquad(2)$$

式中：η_{A} 和 d_{A} 分别为通信一方 Alice 的单光子探测器的探测效率和暗计数率；$P_{\mathrm{post}}(\mu)$为后选择概率，$P_{\mathrm{post}}(\mu)=\mathrm{I}_0(2\mu)-(1-d_{\mathrm{A}})\mathrm{I}_0(2\mu\sqrt{1-\eta_{\mathrm{A}}})$。与弱相干态光源相比，HPCS 光源的空脉冲比例更低，理论上能够提供更高的密钥生成率。

图 1 所示为提出的基于轨道角动量和 HPCS 的 RRDPS-QKD 协议示意图，协议的具体过程如下。

1）Alice 首先利用随机数发生器（RNG）产生一串长 L 的二进制 0-1 随机数 $S_1,S_2,\cdots,S_L$。依据该串随机数，生成一个由 L 个轨道角动量模式（$|l_1\rangle$，$|l_2\rangle,\cdots,|l_L\rangle$）的叠加态 $|L\rangle=\frac{1}{L}\sum_{k=1}^{L}(-1)^{S_k}|l_k\rangle$ 构成的全息图，其中 k 表示第 k 个轨道角动量模式。相邻轨道角动量模式的拓扑荷相差恒定为 Δl，即 $\Delta l=l_{k+1}-l_k$。Alice 使用经过衰减的激光束作为产生配对相干态（PCS）的抽运光，再将配对相干态光源所产生的一对光子中的一个送入单光子探测器中，仅当单光子探测器有响应时才把另一个光子作为 HPCS，用于编码信息。Alice 通过调节衰减器产生不同强度的抽运光，从而可以产生 HPCS 的不同强度的诱骗态脉冲和信号态脉冲。随后，Alice 将 HPCS 脉冲照射到加载有全息图的空间光调制器（SLM），脉冲转变为由 L 个轨道角动量模式叠加的脉冲信号。最后，Alice 通过自由空间量子信道将携带特殊轨道角动量叠加模式的 HPCS 脉冲信号发送给通信的另一方 Bob。

2）Bob 接收 Alice 发送的脉冲信号，并执行测量。Bob 利用一个分束比为 50∶50 的分束器（BS）将接收到的脉冲信号分成两个脉冲信号。两个脉冲信号分别从 Mach-Zehnder 干涉仪的上臂和下臂通过，两臂的长度相同，但上臂比下臂多一个 SLM。Bob 利用随机数生成器产生一个随机数 $\tau\in\{-L+1,\cdots,-2,-1,1,2,\cdots,L-1\}$，并将拓扑荷为 $\tau\cdot\Delta l$ 的轨道角动量模式的相位全息图加载到 SLM 上。

3) Bob 利用另一个 50∶50 的 BS 将两个脉冲信号合并，信号从 BS 的两个输出端输出后，分别进入一个基于坐标变换方法的轨道角动量分离器[16-18]。该轨道角动量分离器由光学元件 R_1、R_2 和透镜组成，可实现由直角坐标 (x, y) 到对数极坐标 $(-a\ln(\sqrt{x^2+y^2}/b), a\arctan(y/x))$ 的坐标变换，其中，a 和 b 为控制变换效果的参数。光学元件 R_1、R_2 将轨道角动量光束的螺旋相位转变为具有横向相位梯度的光束，再利用透镜将横向相位梯度不同的光束聚焦在不同的横向位置上，从而可以将不同轨道角动量模式的光束映射到不同的横向位置予以区分。在轨道角动量分离器的输出端有由 L 个单光子探测器组成的探测器阵列。探测器 D_0^i ($i=1,2,\cdots,L$，其中 i 表示第 i 个探测器) 分别用于探测轨道角动量模式 $|l_1\rangle, |l_2\rangle, \cdots, |l_L\rangle$；探测器 D_1^i 分别用于探测轨道角动量模式 $|-l_1\rangle, |-l_2\rangle, \cdots, |-l_L\rangle$。Bob 依据产生响应的探测器的编号获得 1 bit 的密钥，即当探测器 D_0^i 响应时，Bob 得到密钥 $S_B=0$；当探测器 D_1^i 响应时，Bob 得到密钥 $S_B=1$。

4) Bob 公布产生响应的探测器编号 i 和由随机数 τ 计算得到的参数 $j=i-\tau$。Alice 依据 Bob 公布的数据 (i, j)，通过模 2 加计算 $S_A=S_i\oplus S_j$ 提取安全密钥 S_A，其中 S_i 和 S_j 分别为 Alice 利用随机数计数器产生的第 i 个随机数和第 j 个随机数。

5) Alice 和 Bob 重复以上步骤，积累产生足够的筛选密钥，当 Alice 和 Bob 确定信道安全后，经过差错更正和秘密放大提取出安全密钥。

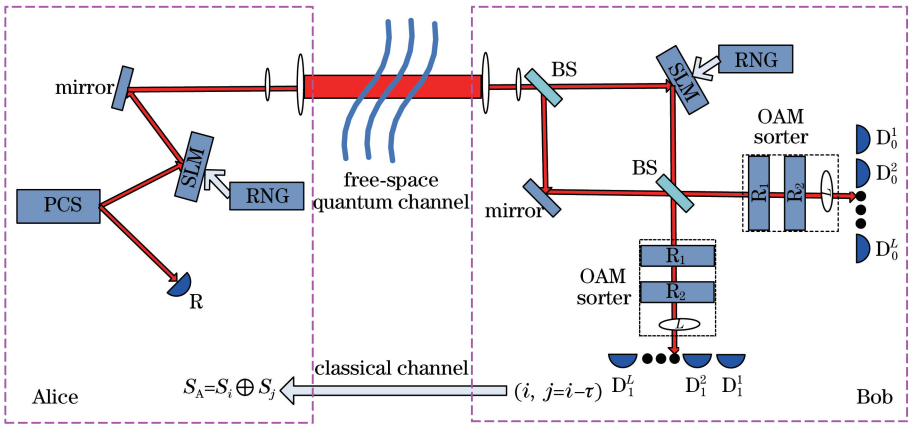

图 1　基于轨道角动量的 RRDPS-QKD 协议示意图

Fig. 1　Schematic of RRDPS-QKD protocol based on orbital angular momentum

3　安全密钥率分析

光子的轨道角动量模式可以表示为

$$|l\rangle=R(r)\exp(\mathrm{i}l\theta), \tag{3}$$

式中：$R(r)$ 为振幅；r 和 θ 分别为径向和角度坐标；l 为轨道角动量的拓扑荷，取值为任意整数。Alice 利用 RNG 产生一串长为 L 的二进制 0-1 随机数 $S_1, S_2, \cdots, S_L$，依据该串随机数，生成一个由 L 个轨道角动量模式 ($|l_1\rangle, |l_2\rangle, \cdots, |l_L\rangle$) 叠加而成的模式 $|L\rangle$，即

$$|L\rangle=\frac{1}{L}\sum_{k=1}^{L}(-1)^{S_k}|l_k\rangle=\frac{1}{L}R(r)\sum_{k=1}^{L}\exp[\mathrm{i}(l_k\theta+\pi S_k)]=\frac{1}{L}R(r)\sum_{k=1}^{L}\exp\{\mathrm{i}[l_1+(k-1)\Delta l]\theta+\pi S_k\}。\tag{4}$$

Bob 接收 Alice 发送的信号 $|L\rangle$ 后，利用两臂长度相同的 Mach-Zehnder 干涉仪对其进行测量。首先利用一个 50∶50 的 BS 将接收到的信号分成两个脉冲信号，分别从 Mach-Zehnder 干涉仪的上臂和下臂通过，经过上臂的信号受到加载有拓扑荷 $\tau\cdot\Delta l$ 的轨道角动量模式的相位全息图的 SLM 的调制，即

$$|L\rangle_u=\frac{1}{L\sqrt{2}}R(r)\sum_{k_u=1}^{L}\exp\{\mathrm{i}\{[l_1+(k_u-1+\tau)\Delta l]\theta+\pi S_{k_u}\}\},\tag{5}$$

式中：下标 u 表示上臂。经过下臂的脉冲信号为

$$|L\rangle_d=\frac{1}{L\sqrt{2}}R(r)\sum_{k_d=1}^{L}\exp\{\mathrm{i}\{[l_1+(k_d-1)\Delta l]\theta+\pi S_{k_d}\}\},\tag{6}$$

式中：下标 d 表示下臂。Bob 利用另一个 50∶50 的 BS 合并两个脉冲信号，得到从 BS 右端输出的信号为

$$\frac{1}{\sqrt{2}}(|L\rangle_d+|L\rangle_u)=\frac{1}{2L}R(r)\sum_{k_d=1}^{L}[\exp(\mathrm{i}\pi S_{k_d})+\exp(\mathrm{i}\pi S_{k_d-\tau})]\exp\{\mathrm{i}[l_1+(k_d-1)\Delta l]\theta\}。\tag{7}$$

由于经历了奇数次反射，从 BS 下端输出的信号为

$$\frac{1}{\sqrt{2}}(|\bar{l}\rangle_{\mathrm{d}}-|\bar{l}\rangle_{\mathrm{u}})=\frac{1}{2L}R(r)\sum_{k_{\mathrm{d}}=1}^{L}[\exp(\mathrm{i}\pi S_{k_{\mathrm{d}}})-\exp(\mathrm{i}\pi S_{k_{\mathrm{d}}-\tau})]\exp\{-\mathrm{i}[l_1+(k_{\mathrm{d}}-1)\Delta l]\theta\}。\quad(8)$$

当第 k_{d} 个和第 $k_{\mathrm{d}}-\tau$ 个随机数相同即 $S_{k_{\mathrm{d}}}=S_{k_{\mathrm{d}}-\tau}$ 时，信号从 BS 右端输出，其结果为

$$\frac{1}{L}R(r)\sum_{k_{\mathrm{d}}=1}^{L}\exp\{\mathrm{i}[l_1+(k_{\mathrm{d}}-1)\Delta l]\theta\}。\quad(9)$$

当第 k_{d} 个和第 $k_{\mathrm{d}}-\tau$ 个随机数不同时，信号从 BS 下端输出，其结果为

$$\frac{1}{L}R(r)\sum_{k_{\mathrm{d}}=1}^{L}\exp\{-\mathrm{i}[l_1+(k_{\mathrm{d}}-1)\Delta l]\theta\}。\quad(10)$$

随后信号被送入轨道角动量分离器，在轨道角动量分离器的输出端有 L 个单光子探测器组成探测器阵列。

基于轨道角动量的 RRDPS-QKD 协议的密钥率公式[14]为

$$R=Q_{\mu}[1-fH(E_{\mu})-H_{\mathrm{PA}}],\quad(11)$$

式中：Q_{μ} 为脉冲信号的密钥生成率；E_{μ} 为脉冲信号的密钥错误率；H_{PA} 为秘密放大导致的密钥损失比例；$H(x)=-x\log_2(x)-(1-x)\log_2(1-x)$ 为二进制香农熵；f 为错误更正效率。RRDPS-QKD 不需要监控比特错误来估计窃听的信息量，因此秘密放大消耗的信息量为

$$Q_{\mu}H_{\mathrm{PA}}=\sum_{n=0}^{n_{\mathrm{th}}}Y_nP_n(\mu)H(e_{\mathrm{ph}}^{n_{\mathrm{th}}})+\sum_{n=n_{\mathrm{th}}+1}^{\infty}Y_nP_n(\mu)H(1/2),\quad(12)$$

式中：参数 $n_{\mathrm{th}}<(L-1)/2$；Y_n 为包含 n 个光子的脉冲的生成率；$e_{\mathrm{ph}}^{n_{\mathrm{th}}}$ 为包含 n_{th} 个光子的脉冲的相位错误率[14]，其表达式为

$$e_{\mathrm{ph}}^{n_{\mathrm{th}}}=\frac{n_{\mathrm{th}}}{L-1}。\quad(13)$$

在本文方案中，采用诱骗态方法来估计生成率 Y_n 和错误率 e_nY_n。考虑轨道角动量具有对称性，不需要校准参考系，但是光子轨道角动量态易受大气湍流和信道衰减的影响。信道衰减的影响为 $\exp(-\alpha Z)$，而大气湍流会导致轨道角动量的串扰。接收光子携带的轨道角动量模式与发送光子携带的轨道角动量模式相同的概率为

$$\eta_0=\frac{1}{\pi}\int_0^1\rho\mathrm{d}\rho\int_0^{2\pi}\exp\left\{-3.44\left[\frac{D}{r_0}\rho\sin\left(\frac{\theta}{2}\right)\right]^{\frac{5}{3}}\right\}\mathrm{d}\theta,\quad(14)$$

式中：D 为接收孔径（直径）；α 为大气吸收、散射等引起的衰减因子；$r_0=0.1853[\lambda^2/(C_n^2Z)]^{3/5}$ 为表征大气湍流的 Fried 参数；C_n^2 为折射率结构参数，表征大气湍流强度；Z 为传输距离；λ 为波长。因此，Bob 接收到轨道角动量光子发生模式串扰的概率为 $1-\eta_0$。当使用无穷种强度诱骗态进行估计时，生成率 Y_n 和错误率 e_nY_n 为

$$Y_n=1-(1-P_{\mathrm{d}})(1-\eta_{\mathrm{t}}\eta_{\mathrm{B}})^n,\quad(15)$$

$$e_nY_n=e_0P_{\mathrm{d}}+(1-\eta_0)(1-P_{\mathrm{d}})[1-(1-\eta_{\mathrm{t}}\eta_{\mathrm{B}})^n],\quad(16)$$

式中：P_{d} 为探测器的暗计数率；η_{t} 为信道传输效率；η_{B} 为 Bob 探测器的效率；e_0 为探测器暗计数导致的错误率。为了获得密钥生成率，需要计算密钥生成率 Q_{μ} 和错误率 E_{μ}，其计算公式分别为

$$Q_{\mu}=\sum_{n=0}^{\infty}Y_nP_n(\mu)=1-\frac{1-P_{\mathrm{d}}}{P_{\mathrm{post}}(\mu)}\mathrm{I}_0(2\mu\sqrt{1-\eta_{\mathrm{t}}\eta_{\mathrm{B}}})+\frac{(1-P_{\mathrm{d}})(1-d_{\mathrm{A}})}{P_{\mathrm{post}}(\mu)}\mathrm{I}_0[2\mu\sqrt{(1-\eta_{\mathrm{t}}\eta_{\mathrm{B}})(1-\eta_{\mathrm{A}})}],\quad(17)$$

$$E_{\mu}Q_{\mu}=\sum_{n=0}^{\infty}e_nY_nP_n(\mu)=e_0P_{\mathrm{d}}+(1-\eta_0)(1-P_{\mathrm{d}})-\frac{(1-\eta_0)(1-P_{\mathrm{d}})}{P_{\mathrm{post}}(\mu)}\{\mathrm{I}_0(2\mu\sqrt{1-\eta_{\mathrm{t}}\eta_{\mathrm{B}}})-(1-d_{\mathrm{A}})\mathrm{I}_0[2\mu\sqrt{(1-\eta_{\mathrm{t}}\eta_{\mathrm{B}})(1-\eta_{\mathrm{A}})}]\}。\quad(18)$$

因此错误率 E_{μ} 为

$$E_{\mu}=\frac{E_{\mu}Q_{\mu}}{Q_{\mu}}。\quad(19)$$

使用无穷种强度诱骗态是不实际的，因而提出了使用三种强度的诱骗态的方案，即强度为 μ 的信号态和 ν_p，$p=1,2,3$ 的诱骗态，其中诱骗态强度满足 $\nu_1\geqslant\nu_2\geqslant\nu_3\geqslant0$ 和 $\nu_1+\nu_2+\nu_3<\mu$。Alice 和 Bob 可以得到增益和量子错误率分别为

$$\begin{cases}Q_{\mu}=\sum_{n=0}^{\infty}Y_nP_n(\mu)\\E_{\mu}Q_{\mu}=\sum_{n=0}^{\infty}e_nY_nP_n(\mu)\\Q_{\nu_i}=\sum_{n=0}^{\infty}Y_nP_n(\nu_i)\\E_{\nu_i}Q_{\nu_i}=\sum_{n=0}^{\infty}e_nY_nP_n(\nu_i)\end{cases}。\quad(20)$$

Alice 和 Bob 可以利用(20)式估计暗计数生成率的下界 Y_0^{L}、单光子脉冲生成率的下界 Y_1^{L}、包含两个光子的脉冲生成率的下界 Y_2^{L}、单光子脉冲错误率的上界 e_1^{U} 以及包含两个光子的脉冲错误率的上界 e_2^{U}。

首先，Alice 和 Bob 需要估计暗计数生成率的下界 Y_0^{L}：

$$\nu_1^2 P_{\mathrm{post}}(\nu_2) Q_{\nu_2} - \nu_2^2 P_{\mathrm{post}}(\nu_1) Q_{\nu_1} = (\nu_1^2 - \nu_2^2) d_{\mathrm{A}} Y_0 - \nu_1^2 \nu_2^2 \sum_{n=2}^{\infty} \left\{ \frac{(\nu_1)^{2n-2} - (\nu_2)^{2n-2}}{(n!)^2} [1 - (1 - d_{\mathrm{A}})(1 - \eta_{\mathrm{A}})^n] Y_n \right\} \leqslant (\nu_1^2 - \nu_2^2) d_{\mathrm{A}} Y_0 。 \tag{21}$$

(21)式中的不等式是由于 $\nu_1^2 \nu_2^2 \sum_{n=2}^{\infty} \left\{ \frac{(\nu_1)^{2n-2} - (\nu_2)^{2n-2}}{(n!)^2} [1 - (1 - d_{\mathrm{A}})(1 - \eta_{\mathrm{A}})^n] Y_n \right\} \geqslant 0$。因此可得

$$Y_0 \geqslant Y_0^{\mathrm{L}} = \max\left[\frac{\nu_1^2 P_{\mathrm{post}}(\nu_2) Q_{\nu_2} - \nu_2^2 P_{\mathrm{post}}(\nu_1) Q_{\nu_1}}{d_{\mathrm{A}}(\nu_1^2 - \nu_2^2)}, 0 \right] 。 \tag{22}$$

当 $\nu_2 = 0$ 时，(22)式取等号。$P_{\mathrm{post}}(\nu_1) Q_{\nu_1} - P_{\mathrm{post}}(\nu_2) Q_{\nu_2}$ 的表达式为

$$\begin{aligned}
&P_{\mathrm{post}}(\nu_1) Q_{\nu_1} - P_{\mathrm{post}}(\nu_2) Q_{\nu_2} = \\
&(\nu_1^2 - \nu_2^2)[1 - (1 - d_{\mathrm{A}})(1 - \eta_{\mathrm{A}})] Y_1 + \sum_{n=2}^{\infty} \left\{ \frac{(\nu_1)^{2n} - (\nu_2)^{2n}}{(n!)^2} [1 - (1 - d_{\mathrm{A}})(1 - \eta_{\mathrm{A}})^n] Y_n \right\} \leqslant \\
&(\nu_1^2 - \nu_2^2)[1 - (1 - d_{\mathrm{A}})(1 - \eta_{\mathrm{A}})] Y_1 + \frac{\nu_1^4 - \nu_2^4}{\mu^4} \sum_{n=2}^{\infty} \left\{ \frac{\mu^{2n}}{(n!)^2} [1 - (1 - d_{\mathrm{A}})(1 - \eta_{\mathrm{A}})^n] Y_n \right\} = \\
&(\nu_1^2 - \nu_2^2)[1 - (1 - d_{\mathrm{A}})(1 - \eta_{\mathrm{A}})] Y_1 + \frac{\nu_1^4 - \nu_2^4}{\mu^4} \{ P_{\mathrm{post}}(\mu) Q_{\mu} - d_{\mathrm{A}} Y_0 - \mu^2 [1 - (1 - d_{\mathrm{A}})(1 - \eta_{\mathrm{A}})] Y_1 \} \leqslant \\
&\left(\nu_1^2 - \nu_2^2 - \frac{\nu_1^4 - \nu_2^4}{\mu^2} \right) [1 - (1 - d_{\mathrm{A}})(1 - \eta_{\mathrm{A}})] Y_1 + \frac{\nu_1^4 - \nu_2^4}{\mu^4} [P_{\mathrm{post}}(\mu) Q_{\mu} - d_{\mathrm{A}} Y_0^{\mathrm{L}}],
\end{aligned} \tag{23}$$

式中：第一个不等式可由公式 $a^i - b^i \leqslant a^2 - b^2 (a \geqslant b \geqslant 0, a + b \leqslant 1, i \geqslant 2)$ 得到；第二个不等式可由(22)式得到。因此，单光子脉冲生成率的下界 Y_1^{L} 为

$$Y_1 \geqslant Y_1^{\mathrm{L}} = \frac{P_{\mathrm{post}}(\nu_1) Q_{\nu_1} - P_{\mathrm{post}}(\nu_2) Q_{\nu_2} - \frac{\nu_1^4 - \nu_2^4}{\mu^4} [P_{\mathrm{post}}(\mu) Q_{\mu} - d_{\mathrm{A}} Y_0^{\mathrm{L}}]}{(\nu_1^2 - \nu_2^2 - \frac{\nu_1^4 - \nu_2^4}{\mu^2})[1 - (1 - d_{\mathrm{A}})(1 - \eta_{\mathrm{A}})]} 。 \tag{24}$$

进一步，Alice 和 Bob 可以估计包含两个光子的脉冲生成率的下界 Y_2^{L}，即

$$\begin{aligned}
&(\nu_2^2 - \nu_3^2) P_{\mathrm{post}}(\nu_1) Q_{\nu_1} - (\nu_1^2 - \nu_3^2) P_{\mathrm{post}}(\nu_2) Q_{\nu_2} + (\nu_1^2 - \nu_2^2) P_{\mathrm{post}}(\nu_3) Q_{\nu_3} = \\
&\frac{L^4}{4} (\nu_1^2 - \nu_2^2)(\nu_1^2 - \nu_3^2)(\nu_2^2 - \nu_3^2)[1 - (1 - d_{\mathrm{A}})(1 - \eta_{\mathrm{A}})^2] Y_2 + \\
&\sum_{n=3}^{\infty} \left\{ \frac{(\nu_2^2 - \nu_3^2)[(\nu_1)^{2n} - (\nu_2)^{2n}] + (\nu_2^2 - \nu_1^2)[(\nu_2)^{2n} - (\nu_3)^{2n}]}{(n!)^2} [1 - (1 - d_{\mathrm{A}})(1 - \eta_{\mathrm{A}})^n] Y_n \right\} \leqslant \\
&\frac{1}{4} (\nu_1^2 - \nu_2^2)(\nu_1^2 - \nu_3^2)(\nu_2^2 - \nu_3^2)[1 - (1 - d_{\mathrm{A}})(1 - \eta_{\mathrm{A}})^2] Y_2 + \\
&\left[(\nu_2^2 - \nu_3^2) \frac{\nu_1^6 - \nu_2^6}{\mu^6} + (\nu_2^2 - \nu_1^2) \frac{\nu_2^6 - \nu_3^6}{\mu^6} \right] \sum_{n=3}^{\infty} \left\{ \frac{\mu^{2n}}{(n!)^2} [1 - (1 - d_{\mathrm{A}})(1 - \eta_{\mathrm{A}})^n] Y_n \right\} = \\
&\frac{1}{4} (\nu_1^2 - \nu_2^2)(\nu_1^2 - \nu_3^2)(\nu_2^2 - \nu_3^2)[1 - (1 - d_{\mathrm{A}})(1 - \eta_{\mathrm{A}})^2] Y_2 + \\
&\frac{(\nu_1^2 - \nu_2^2)(\nu_2^2 - \nu_3^2)(\nu_1^2 - \nu_3^2)(\nu_1^2 + \nu_2^2 + \nu_3^2)}{\mu^6} \{ P_{\mathrm{post}}(\mu) Q_{\mu} - d_{\mathrm{A}} Y_0 - \mu^2 [1 - (1 - d_{\mathrm{A}})(1 - \eta_{\mathrm{A}})] Y_1 - \\
&\frac{\mu^4}{4} [1 - (1 - d_{\mathrm{A}})(1 - \eta_{\mathrm{A}})^2] Y_2 \} \leqslant \frac{1}{4} (\nu_1^2 - \nu_2^2)(\nu_1^2 - \nu_3^2)(\nu_2^2 - \nu_3^2) \left(1 - \frac{\nu_1^2 + \nu_2^2 + \nu_3^2}{\mu^2} \right) \times \\
&[1 - (1 - d_{\mathrm{A}})(1 - \eta_{\mathrm{A}})^2] Y_2 + \frac{(\nu_1^2 - \nu_2^2)(\nu_2^2 - \nu_3^2)(\nu_1^2 - \nu_3^2)(\nu_1^2 + \nu_2^2 + \nu_3^2)}{\mu^6} \times \\
&\{ P_{\mathrm{post}}(\mu) Q_{\mu} - d_{\mathrm{A}} Y_0^{\mathrm{L}} - \mu^2 [1 - (1 - d_{\mathrm{A}})(1 - \eta_{\mathrm{A}})] Y_1^{\mathrm{L}} \},
\end{aligned} \tag{25}$$

式中：第一个不等式可由公式 $a^i - b^i \leqslant a^3 - b^3 (a \geqslant b \geqslant 0, a + b \leqslant 1, i \geqslant 3)$ 得到；第二个不等式可由(22)式和(24)式得到。因此，

$$Y_2 \geqslant Y_2^{\mathrm{L}} = 4\frac{(\nu_2^2-\nu_3^2)P_{\mathrm{post}}(\nu_1)Q_{\nu_1}-(\nu_1^2-\nu_3^2)P_{\mathrm{post}}(\nu_2)Q_{\nu_2}+(\nu_1^2-\nu_2^2)P_{\mathrm{post}}(\nu_3)Q_{\nu_3}}{(\nu_1^2-\nu_2^2)(\nu_1^2-\nu_3^2)(\nu_2^2-\nu_3^2)\left(1-\frac{\nu_1^2+\nu_2^2+\nu_3^2}{\mu^2}\right)[1-(1-d_{\mathrm{A}})(1-\eta_{\mathrm{A}})^2]}-$$
$$4\frac{\frac{\nu_1^2+\nu_2^2+\nu_3^2}{\mu^6}\{P_{\mathrm{post}}(\mu)Q_\mu-d_{\mathrm{A}}Y_0^{\mathrm{L}}-\mu^2[1-(1-d_{\mathrm{A}})(1-\eta_{\mathrm{A}})]Y_1^{\mathrm{L}}\}}{\left(1-\frac{\nu_1^2+\nu_2^2+\nu_3^2}{\mu^2}\right)[1-(1-d_{\mathrm{A}})(1-\eta_{\mathrm{A}})^2]}。\tag{26}$$

然后，估计单光子脉冲错误率的上界 e_1^{U} 和包含两个光子的脉冲错误率的上界 e_2^{U}：

$$P_{\mathrm{post}}(\nu_1)E_{\nu_1}Q_{\nu_1}-P_{\mathrm{post}}(\nu_2)E_{\nu_2}Q_{\nu_2}=(\nu_1^2-\nu_2^2)[1-(1-d_{\mathrm{A}})(1-\eta_{\mathrm{A}})]e_1Y_1+$$
$$\sum_{n=2}^{\infty}\left\{\frac{(\nu_1)^{2n}-(\nu_2)^{2n}}{(n!)^2}[1-(1-d_{\mathrm{A}})(1-\eta_{\mathrm{A}})^n]e_nY_n\right\}\geqslant$$
$$(\nu_1^2-\nu_2^2)[1-(1-d_{\mathrm{A}})(1-\eta_{\mathrm{A}})]e_1Y_1,\tag{27}$$

式中不等式是由于 $\sum_{n=2}^{\infty}\left\{\frac{(\nu_1)^{2n}-(\nu_2)^{2n}}{(n!)^2}[1-(1-d_{\mathrm{A}})(1-\eta_{\mathrm{A}})^n]e_nY_n\right\}\geqslant 0$，可得单光子脉冲错误率的上界 e_1^{U} 为

$$e_1\leqslant e_1^{\mathrm{U}}=\frac{P_{\mathrm{post}}(\nu_1)E_{\nu_1}Q_{\nu_1}-P_{\mathrm{post}}(\nu_2)E_{\nu_2}Q_{\nu_2}}{(\nu_1^2-\nu_2^2)[1-(1-d_{\mathrm{A}})(1-\eta_{\mathrm{A}})]Y_1^{\mathrm{L}}}。\tag{28}$$

$$(\nu_2^2-\nu_3^2)P_{\mathrm{post}}(\nu_1)E_{\nu_1}Q_{\nu_1}-(\nu_1^2-\nu_3^2)P_{\mathrm{post}}(\nu_2)E_{\nu_2}Q_{\nu_2}+(\nu_1^2-\nu_2^2)P_{\mathrm{post}}(\nu_3)E_{\nu_3}Q_{\nu_3}=$$
$$\frac{1}{4}(\nu_1^2-\nu_2^2)(\nu_1^2-\nu_3^2)(\nu_2^2-\nu_3^2)[1-(1-d_{\mathrm{A}})(1-\eta_{\mathrm{A}})^2]e_2Y_2+$$
$$\sum_{n=3}^{\infty}\left\{\frac{(\nu_2^2-\nu_3^2)[(\nu_1)^{2n}-(\nu_2)^{2n}]+(\nu_1^2-\nu_2^2)[(\nu_3)^{2n}-(\nu_2)^{2n}]}{(n!)^2}[1-(1-d_{\mathrm{A}})(1-\eta_{\mathrm{A}})^n]e_nY_n\right\}\geqslant$$
$$\frac{1}{4}(\nu_1^2-\nu_2^2)(\nu_1^2-\nu_3^2)(\nu_2^2-\nu_3^2)[1-(1-d_{\mathrm{A}})(1-\eta_{\mathrm{A}})^2]e_2Y_2,\tag{29}$$

式中不等式是由于

$$\sum_{n=3}^{\infty}\left\{\frac{(\nu_2^2-\nu_3^2)[(\nu_1)^{2n}-(\nu_2)^{2n}]+(\nu_1^2-\nu_2^2)[(\nu_3)^{2n}-(\nu_2)^{2n}]}{(n!)^2}[1-(1-d_{\mathrm{A}})(1-\eta_{\mathrm{A}})^n]e_nY_n\right\}\geqslant 0,\tag{30}$$

可得两个光子脉冲错误率的上界 e_2^{U} 为

$$e_2\leqslant e_2^{\mathrm{U}}=4\frac{(\nu_2^2-\nu_3^2)P_{\mathrm{post}}(\nu_1)Q_{\nu_1}-(\nu_1^2-\nu_3^2)P_{\mathrm{post}}(\nu_2)Q_{\nu_2}+(\nu_1^2-\nu_2^2)P_{\mathrm{post}}(\nu_3)Q_{\nu_3}}{(\nu_1^2-\nu_2^2)(\nu_1^2-\nu_3^2)(\nu_2^2-\nu_3^2)[1-(1-d_{\mathrm{A}})(1-\eta_{\mathrm{A}})^2]Y_2^{\mathrm{L}}}。\tag{31}$$

4　结果与分析

通过数值仿真分析提出协议的性能，仿真使用的参数如下。Alice 的单光子探测器的探测效率 $\eta_{\mathrm{A}}=4.5\%$，暗计数率 $d_{\mathrm{A}}=1.7\times10^{-6}$；Bob 的探测器暗计数率 $P_{\mathrm{d}}=1.7\times10^{-6}L$，探测效率为 $\eta_{\mathrm{B}}=4.5\%$；错误更正效率 $f=1.15$，接收孔径 $D=15$ cm，波长 $\lambda=1550$ nm[19]。

图 2 所示为所提协议的密钥生成率随传输距离的变化，同时还比较了基于轨道角动量的弱相干态 RRDPS-QKD 和传统的使用脉冲序列编码的 RRDPS-QKD 的密钥生成率。仿真参数中，信道衰减为 0.2 dB/km，没有考虑大气湍流的影响。可以看出，基于轨道角动量的 RRDPS-QKD 协议的密钥生成率明显大于传统的使用脉冲序列编码的 RRDPS-QKD，而基于轨道角动量和 HPCS 的 RRDPS-QKD 协议的密钥生成率比基于轨道角动量的弱相干态 RRDPS-QKD 协议大，最大安全传输距离也更远。这是因为 HPCS 的空脉冲比例比弱相干态更小，可以提高密钥生成率。使用无穷诱骗态可以获得最佳性能，但是无法在实际中应用；而有限个诱骗态不仅可以保证性能，而且可以在实际系统中使用。

图 3 和图 4 所示为基于轨道角动量和 HPCS

的 RRDPS-QKD 协议的密钥生成率受信道衰减和大气湍流的影响，均为使用有限个诱骗态的结果。图 3 中信道衰减为 0.2 dB/km，考虑了无大气湍流影响和不同大气湍流条件下[20-21]的系统性能。图 4 所示为大气湍流影响为 $C_n^2=10^{-15}\ \mathrm{m}^{-2/3}$ 时四种不同天气环境下的系统性能。可以看出，在大气湍流

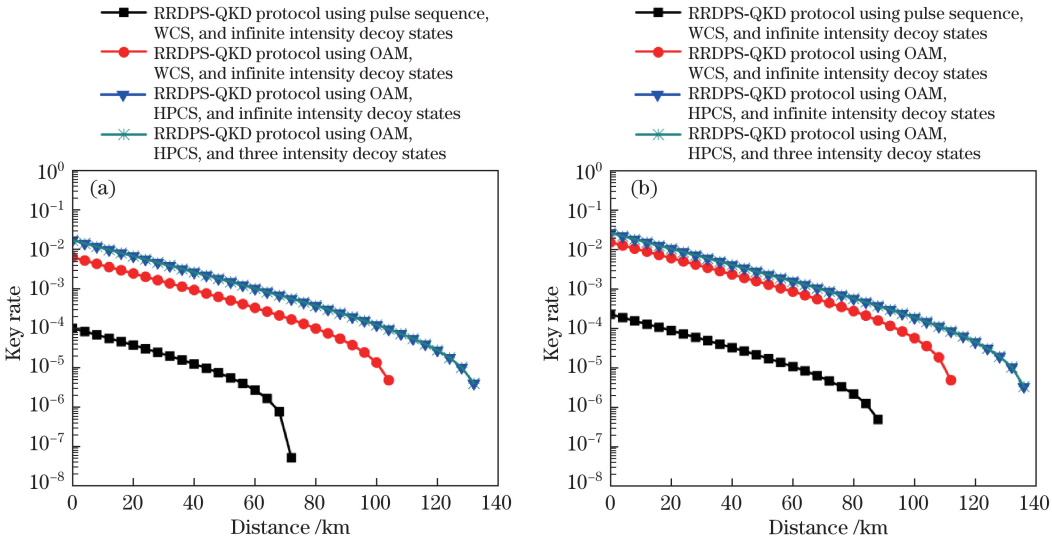

图 2　基于轨道角动量和 HPCS 的 RRDPS-QKD 的密钥生成率随传输距离的变化。(a) $L=8$；(b) $L=16$

Fig. 2　Key generation rate of the RRDPS-QKD protocol based on heralded pair-coherent source and orbital angular momentum against transmission distance. (a) $L=8$; (b) $L=16$

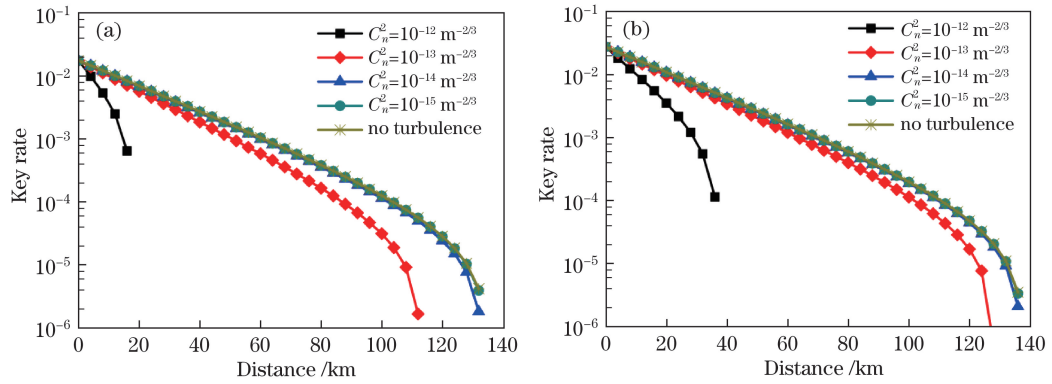

图 3　基于轨道角动量和 HPCS 的 RRDPS-QKD 协议的密钥生成率受大气湍流的影响。(a) $L=8$；(b) $L=16$

Fig. 3　Key generation rate of the RRDPS-QKD protocol based on heralded pair-coherent source and orbital angular momentum against the transmission distance with different strength of atmospheric turbulence. (a) $L=8$; (b) $L=16$

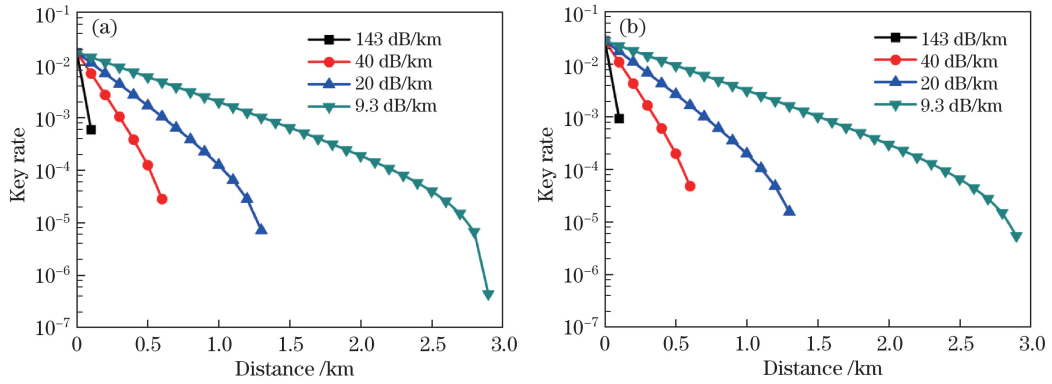

图 4　基于轨道角动量和 HPCS 的 RRDPS-QKD 协议的密钥生成率受信道衰减的影响。(a) $L=8$；(b) $L=16$

Fig. 4　Key generation rate of the RRDPS-QKD protocol based on heralded pair-coherent source and orbital angular momentum against the transmission distance with different link attenuations. (a) $L=8$; (b) $L=16$

和信道衰减条件下，密钥生成率会随传输距离的增大而减小，即大气湍流和信道衰减会使安全密钥的最大传输距离减小。此外，系统性能会受到天气环境的严重影响。但是当湍流较弱如 $C_n^2 \leqslant 10^{-14}\ \mathrm{m}^{-2/3}$ 时，基于轨道角动量的 RRDPS-QKD 协议的性能几乎与无湍流的情况一致，此时湍流对系统性能的影响可以忽略。而当湍流较强如 $C_n^2 \geqslant 10^{-13}\ \mathrm{m}^{-2/3}$ 时，湍流会对系统性能产生显著影响，特别是当 $C_n^2 = 10^{-12}\ \mathrm{m}^{-2/3}$ 时，系统性能明显恶化。

5　结　论

提出了基于 HPCS 和轨道角动量的 RRDPS-QKD，以光子轨道角动量作为信息载体，实现了 RRDPS-QKD 协议。同时使用 L 种不同拓扑荷的轨道角动量的叠加态进行 RRDPS-QKD 的信息编码，显著提高了密钥生成率。分析了系统在湍流大气信道中的传输特性，分别考虑了信道衰减和大气湍流对系统性能的影响。以 HPCS 作为量子光源，有效减小了空脉冲和多光子脉冲的比例，提高了密钥生成率。给出了三种强度诱骗态的方案，在密钥生成率几乎不变的条件下提高了方案的可行性。

参　考　文　献

[1] Zhao S M, Zheng B Y. Quantum information processing technology[M]. Beijing: Beijing University of Posts and Telecommunications Press, 2010.
赵生妹, 郑宝玉. 量子信息处理技术[M]. 北京: 北京邮电大学出版社, 2010.

[2] Zhao G H, Zhao S H, Yao Z S, *et al*. Effect of the pulse broadening caused by atmosphere on satellite based quantum key distribution[J]. Acta Optica Sinica, 2012, 32(11): 1127001.
赵顾颢, 赵尚弘, 幺周石, 等. 大气导致的脉冲展宽对星载量子密钥分发的影响[J]. 光学学报, 2012, 32(11): 1127001.

[3] Hu K, Mao Q P, Zhao S M. Round robin differential phase shift quantum key distribution protocol based on heralded single photon source and detector decoy state[J]. Acta Optica Sinica, 2017, 37(5): 0527002.
胡康, 毛钱萍, 赵生妹. 基于预报单光子源和探测器诱骗态的循环差分相移量子密钥分发协议[J]. 光学学报, 2017, 37(5): 0527002.

[4] Wang X B. Beating the photon-number-splitting attack in practical quantum cryptography[J]. Physical Review Letters, 2005, 94(23): 230503.

[5] Lo H K, Ma X F, Chen K. Decoy state quantum key distribution[J]. Physical Review Letters, 2005, 94(23): 230504.

[6] Agarwal G S. Generation of pair coherent states and squeezing via the competition of four-wave mixing and amplified spontaneous emission[J]. Physical Review Letters, 1986, 57(7): 827-830.

[7] Usenko V C, Paris M G A. Multiphoton communication in lossy channels with photon-number entangled states[J]. Physical Review A, 2007, 75(4): 043812.

[8] Zhang S L, Zou X B, Li C F, *et al*. A universal coherent source for quantum key distribution[J]. Chinese Science Bulletin, 2009, 54(11): 1863-1871.

[9] Wang L, Zhao S M. Round-robin differential-phase-shift quantum key distribution with heralded pair-coherent sources[J]. Quantum Information Processing, 2017, 16(4): 100.

[10] Sasaki T, Yamamoto Y, Koashi M. Practical quantum key distribution protocol without monitoring signal disturbance[J]. Nature, 2014, 509(7501): 475-478.

[11] Takesue H, Sasaki T, Tamaki K, *et al*. Experimental quantum key distribution without monitoring signal disturbance[J]. Nature Photonics, 2015, 9(12): 827-831.

[12] Zhang Z, Yuan X, Cao Z, *et al*. Practical round-robin differential-phase-shift quantum key distribution [J]. New Journal of Physics, 2017, 19(3): 033013.

[13] Mao Q P, Wang L, Zhao S M. Plug-and-play round-robin differential phase-shift quantum key distribution [J]. Scientific Reports, 2017, 7: 15435.

[14] Mirhosseini M, Magaña-Loaiza O S, O'Sullivan M N, *et al*. High-dimensional quantum cryptography with twisted light[J]. New Journal of Physics, 2015, 17(3): 033033.

[15] Horikiri T, Kobayashi T. Decoy state quantum key distribution with a photon number resolved heralded single photon source[J]. Physical Review A, 2006, 73(3): 032331.

[16] Berkhout G C G, Lavery M P J, Courtial J, *et al*. Efficient sorting of orbital angular momentum states of light[J]. Physical Review Letters, 2010, 105(15): 153601.

[17] Mirhosseini M, Malik M, Shi Z M, *et al*. Efficient separation of the orbital angular momentum eigenstates of light[J]. Nature Communications, 2013, 4: 2781.

[18] Wang L, Zhao S M, Gong L Y, *et al*. Free-space measurement-device-independent quantum-key-distribution protocol using decoy states with orbital angular momentum[J]. Chinese Physics B, 2015, 24(12): 120307.

[19] Liu Z H, Chen H W. Cryptanalysis and improvement of quantum broadcast communication and authentication protocol with a quantum one-time pad[J]. Chinese Physics B, 2016, 25(8): 080308.

[20] Wang L, Zhou Y Y, Zhou X J, *et al*. Research on air-water quantum key distribution based on irregular sea surface with foams[J]. Acta Optica Sinica, 2018, 38(10): 1027002.
王澈, 周媛媛, 周学军, 等. 泡沫覆盖不规则海面的空-水量子密钥分发研究[J]. 光学学报, 2018, 38(10): 1027002.

[21] Ke X Z, Wang X Y. Experimental study on the correction of wavefront distortion for vortex beam[J]. Acta Optica Sinica, 2018, 38(3): 0328018.
柯熙政, 王夏尧. 涡旋光波前畸变校正实验研究[J]. 光学学报, 2018, 38(3): 0328018.