基于指示单光子源和轨道角动量的密钥分配协议的波动分析

何业锋[1,2]，郭佳瑞[1*]，李春雨[3]，赵艳坤[3]

[1]西安邮电大学网络空间安全学院，陕西 西安 710121；

[2]西安邮电大学无线网络安全技术国家工程实验室，陕西 西安 710121；

[3]西安邮电大学通信与信息工程学院，陕西 西安 710121

摘要 针对基于指示单光子源的测量设备无关量子密钥分配协议存在基的依赖性问题和信源统计波动问题，研究了基于服从泊松分布的指示单光子源和轨道角动量的量子密钥分配协议，并进行了统计波动分析。分析了对称信道和非对称信道下，该协议的单边传输效率、密钥生成速率与安全传输距离的关系，模拟了信源的统计波动对该协议密钥生成速率和传输距离的影响。仿真结果表明，应用轨道角动量编码解决了该协议基的依赖性问题，提高了密钥生成速率和安全传输距离。统计波动对该协议密钥生成速率的影响随着传输距离的增大而扩大，在脉冲数量相同时，非对称信道下的密钥生成速率、安全传输距离大于对称信道下的。

关键词 量子光学；量子密钥分配；测量设备无关；轨道角动量；指示单光子源；统计波动

中图分类号 TN918 **文献标志码** A **doi**：10.3788/CJL202047.0412001

Fluctuation Analysis of Key Distribution Protocol Based on Heralded Single-Photon Source and Orbital Angular Momentum

He Yefeng[1,2], Guo Jiarui[1*], Li Chunyu[3], Zhao Yankun[3]

[1]*School of Cyberspace Security, Xi′an University of Posts & Telecommunications, Xi′an, Shaanxi* 710121, *China*;

[2]*National Engineering Laboratory for Wireless Security, Xi′an University of Posts & Telecommunications, Xi′an, Shaanxi* 710121, *China*;

[3]*School of Communications and Information Engineering, Xi′an University of Posts & Telecommunications, Xi′an, Shaanxi* 710121, *China*

Abstract Basis dependence and statistical fluctuation of light sources are problems for the measurement-device-independent quantum key distribution protocol based on heralded single-photon source (HSPS). To solve these problems, in this work, the quantum key distribution protocol based on HSPS in Poisson distribution and orbital angular momentum (OAM) was studied. Moreover, its statistical fluctuation was analyzed. The relationship among the transmission efficiency, key generation rate, and safe transmission distance of the protocol under symmetric and asymmetric channels was examined. Furthermore, the effect of statistical fluctuation on the key generation rate and transmission distance was simulated. Simulation results show that the problem of basis dependence is solved by OAM coding, and the key generation rate and transmission distance of the protocol are improved. The effect of statistical fluctuation on the key generation rate of the protocol increases with the transmission distance. For the same number of pulses, the key generation rate and safe transmission distance under the asymmetric channel are greater than those under the symmetric channel.

Key words quantum optics; quantum key distribution; measurement-device-independent; orbit angular momentum; heralded single-photon source; statistical fluctuation

OCIS codes 270.1670; 270.5565; 270.5568; 190.4410

收稿日期：2019-10-24；**修回日期**：2019-12-11；**录用日期**：2019-12-16

基金项目：国家自然科学基金(61802302,61772418)

* **E-mail**：1271745041@qq.com

1 引　言

在量子密码中，量子密钥分配(QKD)是热点研究问题之一。随着 QKD 协议即“BB84 协议[1]”的提出，QKD 的发展开始受到广泛关注。尽管 QKD 协议在理论上能实现无条件安全[2-4]，但在实际应用中，由于光源和探测器等设备的不完美性，QKD 协议常受到针对光源和探测器的各种攻击。例如，探测器的不完美性可能导致系统受到致盲攻击[5]、时移攻击[6]、伪态攻击[7]等，光源的不完美性可能导致系统受到光子束分流攻击[8]等。2012 年，Lo 等[9]提出了测量设备无关量子密钥分配(MDI-QKD)协议，通信双方准备光子态并发送给第三方进行贝尔态测量(BSM)，最终获得安全密钥。该协议能避免所有针对探测器漏洞的攻击，并且能够增大安全传输距离。随后，国内外学者对 MDI-QKD 协议展开了深入研究[10-13]。

实际应用中，MDI-QKD 方案最常用的光源是弱相干光源和奇相干光源。2004 年，Fasel 等[14]提出了指示单光子源(HSPS)的实验实现。HSPS 较弱相干光源在光子数分布中占很大优势，它的单光子脉冲率大于弱相干光源，因此研究基于 HSPS 的 MDI-QKD 协议的意义更大。朱峰等[15]对热分布下的基于 HSPS 的 MDI-QKD 协议结合诱骗态理论进行研究，仿真分析了密钥生成速率与通信距离之间的关系。Zhou 等[16]比较了基于 HSPS 的 MDI-QKD 协议在通信双方不同探测效率下的性能优劣。何业锋等[17]研究了基于 HSPS 和量子存储的 MDI-QKD 协议，增大了安全传输距离。目前，相位编码[18]和极化编码[9]是 MDI-QKD 的主要编码方案，但是这两种方案存在基的依赖性问题[18]，这会降低密钥生成速率。经研究发现，轨道角动量(OAM)可以作为量子信息的载体[19-20]，使用 OAM 进行编码时，测量参考系的旋转不会影响测量值的结果[21]，因此可用于改进 MDI-QKD 协议，解决基的依赖性问题。之后，学者们对使用 OAM 编码的 MDI-QKD 协议进行了研究[22-24]。文献[25]分析了大气湍流下基于 OAM 编码的 MDI-QKD 的密钥生成速率与最大传输距离。文献[26]将光子 OAM 应用于循环差分相移量子密钥分配协议，提高了密钥生成速率。在实际通信中，通信双方的光源存在统计涨落[27-28]，这会改变光源发送的脉冲数目，进而影响 MDI-QKD 协议的性能。Zhou 等[29]对基于 HSPS 的 MDI-QKD 协议在对称信道下的密钥生成速率进行了统计波动分析。朱卓丹等[30]研究了基于标记配对光源的 MDI-QKD 协议在统计波动影响下的密钥生成速率的变化情况。目前，MDI-QKD 协议在非对称信道情况下的统计涨落问题还需要进一步考虑。

本文主要研究在光源强度涨落时，基于泊松分布的 HSPS 和 OAM 编码的 MDI-QKD 协议的密钥生成速率与安全传输距离之间的关系。分析了该协议在非对称信道情况下的密钥生成速率的变化趋势，模拟了采用不同信道参数时统计波动对该协议密钥生成速率和传输距离的影响。

2 基本原理

2.1 HSPS

采用 HSPS 实现 MDI-QKD 协议的主要思想是发送方产生一对纠缠光子，分别称为信号光子和闲频光子，依据纠缠光子对具有完美的同时性，发送方可以使用闲频光子来预报信号光子到达第三方的时间，因此 HSPS 的单光子脉冲率高于弱相干光源。该光源光子数的泊松分布为

$$P(n)=\exp(-x)\frac{x^n}{n!},\tag{1}$$

式中：n 为光子数目；x 为脉冲强度。

2.2 基于 HSPS 和 OAM 的 MDI-QKD 协议

基于 HSPS 与 OAM 的 MDI-QKD 系统模型如图 1 所示，A、B、C、D 分别表示第三方的单光子探测器，E、F 分别表示通信双方的触发探测器，BS 表示分束器，PBS 表示偏振分束器，decoy-IM 表示光强调制器，SLM 表示产生光子 OAM 光束的空间光调制器，sorter 表示高效 OAM 分离装置。

基于 HSPS 和 OAM 的 MDI-QKD 协议的具体步骤如下：

1) Alice 和 Bob 采用 HSPS 产生两种模式的光子，闲频光子被发送至各自的触发探测器 E 或 F，信号光子经过 SLM 后会产生具有不同 l 值的 OAM 态[31-32]。然后 Alice 和 Bob 随机选择 B_1 基或 B_2 基进行 OAM 编码，其中 $B_1=\{|l\rangle,|-l\rangle\}$，$B_2=\{(|l\rangle+|-l\rangle)/\sqrt{2},(|l\rangle-|-l\rangle)/\sqrt{2}\}$。一般，将 $|l\rangle$ 和 $(|l\rangle+|-l\rangle)/\sqrt{2}$ 编码为“0”，$|-l\rangle$ 和 $(|l\rangle-|-l\rangle)/\sqrt{2}$ 编码为“1”。Alice 和 Bob 利用 decoy-IM 将编码后的光子随机调制成三种光子态，对应的光子态强度(即平均光子数)分别为 u_i、v_j $(i,j=0,1,2)$ 且 $u_2>u_1>u_0=0$，$v_2>v_1>v_0=0$。u_0、u_1、u_2 分别表示 Alice 的真空态、诱骗态和信号

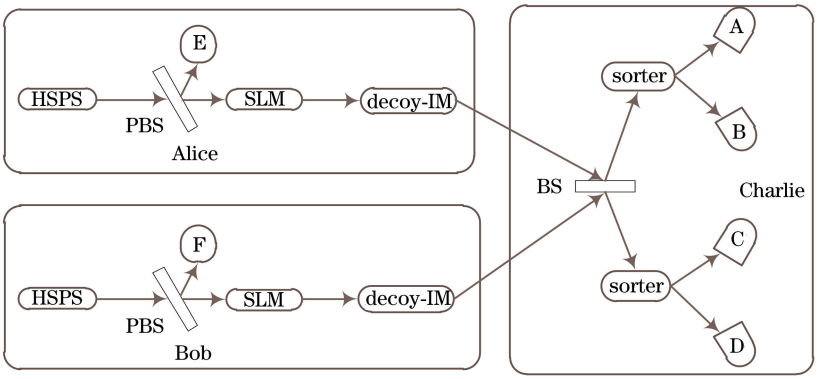

图 1　基于 HSPS 与 OAM 的 MDI-QKD 的系统模型

Fig. 1　System model of MDI-QKD based on HSPS and OAM

态的强度，v_0、v_1、v_2 分别表示 Bob 的真空态、诱骗态和信号态的强度，其中信号态为通信双方用来产生安全密钥的光子态。然后 Alice 和 Bob 将调制后的光子态发送给第三方。

2）第三方 Charlie 对接收到的信号光子进行 Bell 态测量，并公布测量结果。通信双方再根据测量结果进行基比对，筛选出初始密钥。

3）最后通过对初始密钥进行纠错和保密放大来产生安全密钥。

3　密钥生成率的统计波动分析

3.1　密钥生成速率

基的依赖性问题影响安全密钥的生成速率，而基于 OAM 的 MDI-QKD 方案正好可以解决这个问题。根据 GLLP（Gottesman-Lo-Lutkenhaus-Preskill）[4] 和诱骗态技术，该协议最终的密钥生成速率公式为

$$R \geqslant P_{u_2}(1)P_{v_2}(1)Y_{11}^{(B_1)}[1-H(e_{11}^{(B_2)})]-Q_{11}^{(B_1)}f(E^{(B_1)})H(E^{(B_1)}),\tag{2}$$

式中：$P_{u_2}(1)$、$P_{v_2}(1)$ 分别表示通信双方发送信号光子时信号光子为单光子脉冲的概率；$Y_{11}^{(B_1)}$、$E^{(B_1)}$ 表示通信双方都选择 B_1 基时的单光子增益和误码率；$Q_{11}^{(B_1)}$ 表示通信双方都选择 B_1 基时发送单光子脉冲的总增益；$e_{11}^{(B_2)}$ 表示通信双方都选择 B_2 基时的单光子误码率；$f(*)$ 函数为数据协调的协调效率；H 表示二进制香农熵，$H(x)=x\log_2 x-(1-x)\log_2(1-x)$。由于单光子增益和单光子误码率无法通过实验直接获得，因此需要通过通信双方发送的不同光强的脉冲时所获得的总增益和总误码率来估计单光子增益 Y_{11} 和单光子误码率 e_{11}。基于服从于泊松分布的 HSPS 与 OAM 编码的 MDI-QKD 协议的总增益和总误码率为

$$Q_{u_iv_j}^{(W)}=\sum_{n,m=0}^{\infty}\exp(-u_i-v_j)\frac{u_i^n v_j^m}{n!\ m!}[1-(1-p_d)(1-\eta_d)^n][1-(1-p_d)(1-\eta_d)^m]Y_{nm}^{(W)},\tag{3}$$

$$E_{u_iv_j}^{(W)}Q_{u_iv_j}^{(W)}=\sum_{n,m=0}^{\infty}\exp(-u_i-v_j)\frac{u_i^n v_j^m}{n!\ m!}[1-(1-p_d)(1-\eta_d)^n][1-(1-p_d)(1-\eta_d)^m]e_{nm}^{(W)}Y_{nm}^{(W)},\tag{4}$$

式中：W 表示 B_1 基或 B_2 基；η_d 表示探测器的探测效率；p_d 表示探测器的暗计数率；$Y_{nm}^{(W)}$ 表示第三方接收到 Alice 和 Bob 分别发送的光子数为 n、m 的脉冲并成功进行 Bell 态测量的概率，$e_{nm}^{(W)}$ 为与之相对应的误码率。

根据文献[33]的总增益展开式，可由(3)式推出 $Y_{11}^{(W)}$ 的下界值为

$$Y_{11}^{(W)}\geqslant[Q_{u_2v_2}^{(W)}-Q_{u_1v_1}^{(W)}-g_1^{(W)}-g_2^{(W)}-g_3^{(W)}]/\{[\exp(-u_2-v_2)u_2v_2-\exp(-u_1-v_1)u_1v_1-k\exp(-u_2-v_1)u_2v_1-k\exp(-u_1-v_2)u_1v_2][1-(1-p_d)(1-\eta_d)]^2\},\tag{5}$$

由(4)式和(5)式可得到 $e_{11}^{(W)}$ 的上界值为

$$e_{11}^{(W)}\leqslant\frac{Q_{u_1v_1}^{(W)}E_{u_1v_1}^{(W)}-Q_{u_10}^{(W)}E_{u_10}^{(W)}-Q_{0v_1}^{(W)}E_{0v_1}^{(W)}+Q_{00}^{(W)}E_{00}^{(W)}}{\exp(-u_1-v_1)u_1v_1[1-(1-p_d)(1-\eta_d)]^2Y_{11}^{(W)}},\tag{6}$$

令 $k=\min\{a,b,c\}$，a、b、c 可表示为

$$\begin{cases} a=\dfrac{\exp(-u_2-v_2)u_2v_2^2-\exp(-u_1-v_1)u_1v_1^2}{\exp(-u_2-v_1)u_2v_1^2-\exp(-u_1-v_2)u_1v_2^2} \\ b=\dfrac{\exp(-u_2-v_2)u_2^2v_2-\exp(-u_1-v_1)u_1^2v_1}{\exp(-u_2-v_1)u_2^2v_1-\exp(-u_1-v_2)u_1^2v_2} \\ c=\dfrac{\exp(-u_2-v_2)u_2^2v_2^2-\exp(-u_1-v_1)u_1^2v_1^2}{\exp(-u_2-v_1)u_2^2v_1^2-\exp(-u_1-v_2)u_1^2v_2^2} \end{cases}。\tag{7}$$

(5)式中的 $g_1^{(W)}$、$g_2^{(W)}$、$g_3^{(W)}$ 可表示为

$$\begin{cases} g_1^{(W)}=Q_{0v_2}^{(W)}+Q_{u_20}^{(W)}-Q_{0v_1}^{(W)}-Q_{u_10}^{(W)} \\ g_2^{(W)}=k(Q_{u_2v_1}^{(W)}-Q_{u_20}^{(W)}-Q_{0v_1}^{(W)}+Q_{00}^{(W)}) \\ g_3^{(W)}=k(Q_{u_1v_2}^{(W)}-Q_{u_10}^{(W)}-Q_{0v_2}^{(W)}+Q_{00}^{(W)}) \end{cases},\tag{8}$$

式中：$Q_{u_iv_j}^{(W)}$ 表示通信双方发送脉冲强度为 u_i 和 v_j 时的增益；$Q_{0v_j}^{(W)}$ 表示 Alice 发送零光子同时 Bob 发送的脉冲强度为 v_j 时的增益；$Q_{u_i0}^{(W)}$ 表示 Alice 发送的脉冲强度为 u_i 同时 Bob 发送零光子时的增益；$Q_{00}^{(W)}$ 表示通信双方都发送零光子时的增益；$E_{u_iv_j}^{(W)}$、$E_{0v_j}^{(W)}$、$E_{u_i0}^{(W)}$、$E_{00}^{(W)}$ 分别表示各自相应的误码率。

根据文献[27]可知，总增益和总误码率可以通过实验直接测量，B_1 基和 B_2 基的总增益和总误码率分别为

$$\begin{cases} Q_{u_iv_j}^{(B_1)}=Q_{\mathrm{C}}+Q_{\mathrm{E}} \\ E_{u_iv_j}^{(B_1)}Q_{u_iv_j}^{(B_1)}=e_{\mathrm{d}}Q_{\mathrm{C}}+(1-e_{\mathrm{d}})Q_{\mathrm{E}} \end{cases},\tag{9}$$

$$\begin{cases} Q_{u_iv_j}^{(B_2)}=2y^2[1+2y^2-4y\mathrm{I}_0(s)+\mathrm{I}_0(2s)] \\ Q_{u_iv_j}^{(B_2)}E_{u_iv_j}^{(B_2)}=e_0Q_{u_iv_j}^{(B_2)}-2(e_0-e_{\mathrm{d}})y^2[\mathrm{I}_0(2s)-1] \end{cases},\tag{10}$$

式中：$Q_{\mathrm{C}}=2(1-p_{\mathrm{d}})^2\exp(-u'/2)\times[1-(1-p_{\mathrm{d}})\exp(-\eta_{\mathrm{a}}u_i/2)]\times[1-(1-p_{\mathrm{d}})\exp(-\eta_{\mathrm{b}}v_j/2)]$；$Q_{\mathrm{E}}=2p_{\mathrm{d}}(1-p_{\mathrm{d}})^2\exp(-u'/2)\times[\mathrm{I}_0(2s)-(1-p_{\mathrm{d}})\exp(-u'/2)]$；$\mathrm{I}_0(s)\approx1+\dfrac{s^2}{4}$，为第一类修正贝塞尔函数；$e_0$ 为修正系数；e_{d} 为探测器的调节误差；u'为平均光子数。相关参数 u'，s 和 y 的表达式[23]分别为 $u'=\eta_{\mathrm{a}}u_i+\eta_{\mathrm{b}}v_j$、$s=\sqrt{\eta_{\mathrm{a}}u_i\eta_{\mathrm{b}}v_j}/2$、$y=(1-p_{\mathrm{d}})^2\exp(-u'/4)$，其中 η_{a} 和 η_{b} 分别表示 Alice 和 Bob 的单边传输效率。由于本文采用的是 OAM 编码，参考系的旋转不会改变 OAM 的测量值，即解决了基的依赖性问题，因此 $e_{\mathrm{d}}=0$。

3.2　非对称信道

由于非对称信道相比对称信道更符合实际通信需求，因此下面重点考虑非对称信道的情况。令第三方与 Alice 和 Bob 之间的距离之比 $\alpha=L_{\mathrm{CA}}/L_{\mathrm{CB}}$。其中 $\alpha=1$ 表示对称信道，系统总传输效率 $\eta=\eta_{\mathrm{a}}=\eta_{\mathrm{b}}=t\eta_{\mathrm{d}}$，$t=10^{-\alpha L/10}$ 为信道传输效率，η_{d} 为探测器的探测效率，L 表示传输信道长度。$\alpha<1$ 表示非对称信道，第三方更加靠近 Alice，此时 Alice 和 Bob 各自信道的单边传输效率分别为

$$\begin{cases} \eta_{\mathrm{a}}=\eta^{2\alpha/(\alpha+1)} \\ \eta_{\mathrm{b}}=\eta^{2/(\alpha+1)} \end{cases}。\tag{11}$$

3.3　统计波动分析

在实际系统中，信号脉冲的发送数量有限，这在参数估计的过程中会造成统计波动。考虑到实际通信双方与测量第三方的距离不一定相同即存在对称信道和非对称信道两种情况，本文利用文献[29]中的方法对基于 HSPS 和 OAM 编码的 MDI-QKD 协议的密钥生成速率进行统计波动分析。

脉冲增益及误码率的波动表达式为

$$\begin{cases} Q_{u_iv_j}^{(W)}\geqslant Q_{u_iv_j}^{(W,\mathrm{L})}:=Q_{u_iv_j}^{(W)}-\Delta_{u_iv_j}^{(W)} \\ Q_{u_iv_j}^{(W)}\leqslant Q_{u_iv_j}^{(W,\mathrm{U})}:=Q_{u_iv_j}^{(W)}+\Delta_{u_iv_j}^{(W)} \end{cases},\tag{12}$$

$$\begin{cases} E_{u_iv_j}^{(W)}Q_{u_iv_j}^{(W)}\geqslant E_{u_iv_j}^{(W,\mathrm{L})}Q_{u_iv_j}^{(W,\mathrm{L})}:=E_{u_iv_j}^{(W)}Q_{u_iv_j}^{(W)}-\Delta'^{(W)}_{u_iv_j} \\ E_{u_iv_j}^{(W)}Q_{u_iv_j}^{(W)}\leqslant E_{u_iv_j}^{(W,\mathrm{U})}Q_{u_iv_j}^{(W,\mathrm{U})}:=E_{u_iv_j}^{(W)}Q_{u_iv_j}^{(W)}+\Delta'^{(W)}_{u_iv_j} \end{cases},\tag{13}$$

式中：$\Delta_{u_iv_j}^{(W)}=\gamma\sqrt{Q_{u_iv_j}^{(W)}/N_{u_iv_j}^{(W)}}$，表示脉冲增益的波动值，$N_{u_iv_j}^{(W)}$ 为 Alice 和 Bob 发送的脉冲数量；$\Delta'^{(W)}_{u_iv_j}=\gamma\sqrt{E_{u_iv_j}^{(W)}Q_{u_iv_j}^{(W)}/N_{u_iv_j}^{(W)}}$，表示误码率的波动值；上标 U 表示表达式的上界，L 表示下界；γ 为统计波动分析中的标准方差。

在统计波动分析中，随着脉冲增益的改变，单光子增益与误码率也发生改变，最终得到

$$Y_{11}^{(W,\mathrm{L})}:=[Q_{u_2v_2}^{(W,\mathrm{L})}-Q_{u_1v_1}^{(W,\mathrm{U})}-g_1^{(W,\mathrm{U})}-g_2^{(W,\mathrm{U})}-g_3^{(W,\mathrm{U})}]/\{[\exp(-u_2-v_2)u_2v_2-\exp(-u_1-v_1)u_1v_1-$$

$$k\exp(-u_2-v_1)u_2v_1-k\exp(-u_1-v_2)u_1v_2]\left[1-(1-p_{\mathrm{d}})(1-\eta_{\mathrm{d}})\right]^2\},\tag{14}$$

$$e_{11}^{(W,\mathrm{U})}:=\frac{Q_{u_1v_1}^{(W,\mathrm{U})}E_{u_1v_1}^{(W,\mathrm{U})}-Q_{u_10}^{(W,\mathrm{L})}E_{u_10}^{(W,\mathrm{L})}-Q_{0v_1}^{(W,\mathrm{L})}E_{0v_1}^{(W,\mathrm{L})}+Q_{00}^{(W,\mathrm{U})}E_{00}^{(W,\mathrm{U})}}{\exp(-u_1-v_1)u_1v_1\left[1-(1-p_{\mathrm{d}})(1-\eta_{\mathrm{d}})\right]^2Y_{11}^{(W,\mathrm{L})}},\tag{15}$$

式中：$g_1^{(W,\mathrm{U})}$、$g_2^{(W,\mathrm{U})}$ 和 $g_3^{(W,\mathrm{U})}$ 为(8)式中受统计波动影响产生的波动表达式。

经统计波动分析之后，可得密钥生成速率为

$$R\geqslant P_{u_2}(1)P_{v_2}(1)Y_{11}^{(B_1,\mathrm{L})}\left[1-H(e_{11}^{(B_1,\mathrm{U})})\right]-Q_{11}^{(B_1)}f(E^{(B_1)})H(E^{(B_1)})。\tag{16}$$

4　数值仿真与分析

根据上面的公式推导，将(1)式、(5)式和(6)式带入(2)式中，得到密钥生成速率与安全传输距离之间的关系。随着 α 取值的改变，通信双方各自信道的传输效率发生改变。将(14)式和(15)式带入(16)式中，得到对称信道和非对称信道情况下，基于 HSPS 和 OAM 的 MDI-QKD 协议受统计波动影响时的密钥生成速率与安全传输距离之间的关系。下面主要使用表 1 中的参数进行仿真[16]，信号态和诱骗态的光强分别为 0.70 和 0.01。

采用泊松分布的 HSPS 时，基于 OAM 编码和极化编码的 MDI-QKD 协议的密钥生成速率与安全传输距离之间的关系曲线如图 2 所示。由图 2 可知，两协议的最大传输距离的理论值分别为 171 km 和 149 km。随着脉冲数量的增加，最大传输距离也逐渐靠近理论值。当 $N=10^{16}$ 时，采用上述两种不同编码方案的 MDI-QKD 协议的最大传输距离分别为 169 km 和 146 km。并且相同传输距离下，采用 OAM 编码方案的 MDI-QKD 协议的密钥生成速率高于采用极化编码方案的，原因是 OAM 编码解决了基的依赖性问题，测量值不会受参考系旋转的影响。

表 1　主要仿真参数

Table 1　Main simulation parameters

Parameter	η_{d}	e_0	p_{d}	f	γ
Value	0.6	0.5	3×10^{-6}	1.16	5.3

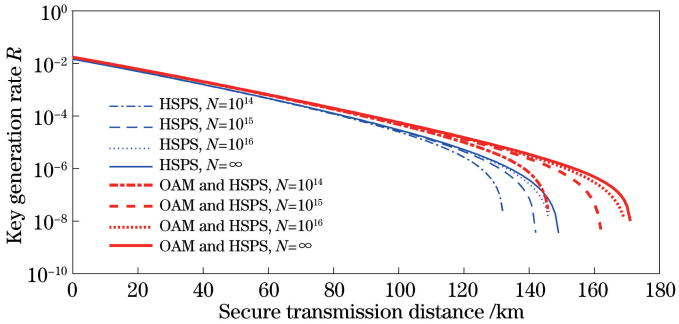

图 2　不同方案的密钥生成速率

Fig. 2　Key generation rate under different schemes

图 3 所示为通信双方各自的单边传输效率与安全传输距离的关系曲线。由图 3 可知，随着传输距离的增大，单边传输效率发生改变。当 $\alpha=0.3$ 时，Bob 的传输效率远远低于 Alice；随着 α 的增大，Bob

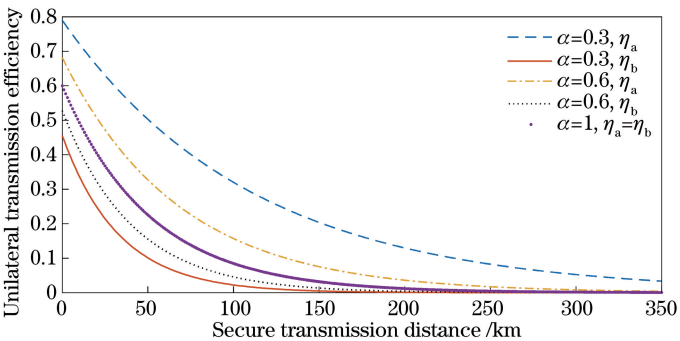

图 3　单边传输效率与安全传输距离的关系

Fig. 3　Relationship between unilateral transmission efficiency and secure transmission distance

的传输效率随之增大，但仍然低于 Alice；直到 $\alpha=1$ 时，双方的传输效率相等，此时信道是对称的。

图 4 所示为非对称信道下不同脉冲数量对基于 HSPS 和 OAM 的 MDI-QKD 协议密钥生成速率的影响。由图 4 可知，通信双方发送脉冲的数量会改变密钥生成速率以及安全传输距离。非对称信道通信时，随着 α 的减小，密钥生成速率增大。同时当 $\alpha=0.3$、$N=10^{16}$ 时，基于 HSPS 和 OAM 的 MDI-QKD 协议的最大传输距离为 215 km；当 $\alpha=0.6$、$N=10^{16}$，协议的最大传输距离为 188 km。与图 2 对比可知，当脉冲数量一致时，非对称信道的安全密钥生成速率、安全传输距离都大于对称信道的。这是因为 α 的减小使得 Alice 的单边传输效率增加，第三方成功进行贝尔态测量的概率增大，进而提高了密钥生成速率，增大了安全传输距离。分别采用不同距离比通信且传输距离达到最大时，基于 HSPS 和 OAM 的 MDI-QKD 协议的单光子误码率、单光子增益和密钥生成速率如表 2 所示。

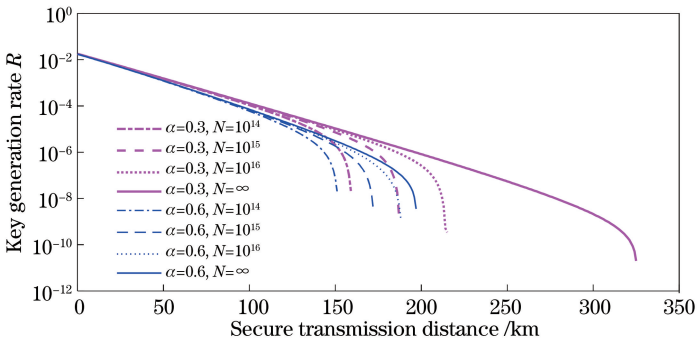

图 4　非对称信道下不同脉冲数量对密钥生成速率的影响

Fig. 4　Influence of number of pulses on key generation rate under asymmetric channels

表 2　非对称信道协议在 $N=10^{16}$ 时的参数比较

Table 2　Comparison of parameters of asymmetric channel protocol under $N=10^{16}$

Parameter	$\alpha=0.6$	$\alpha=0.3$	$\alpha=0.3$
Maximum distance /km	188	188	215
e_{11}	0.4228	0.0904	0.5211
Y_{11}	2.076×10^{-6}	3.422×10^{-5}	8.198×10^{-6}
R	1.404×10^{-9}	8.364×10^{-7}	3.422×10^{-10}

由表 2 可知，相同传输距离时，$\alpha=0.6$ 时的单光子误码率高于 $\alpha=0.3$ 时，同时 $\alpha=0.6$ 时的单光子增益和密钥生成速率均小于 $\alpha=0.3$ 时的。相同距离比时，误码率随传输距离的增大而增大，单光子增益及密钥生成速率随之减小。

5　结　　论

本文研究了在光源存在统计波动时，基于服从泊松分布的 HSPS 和 OAM 编码的 MDI-QKD 协议的性能。仿真分析了该协议的单边传输效率与安全传输距离的关系，对比了不同信道情况下统计波动对该协议密钥生成速率的影响。从仿真结果可知，采用 OAM 编码的 MDI-QKD 协议可以解决基的依赖性问题，从而提高了该协议的密钥生成速率。统计波动会改变该协议的密钥生成速率以及安全传输距离，随着脉冲数量的增加，密钥生成速率和安全传输距离逐渐接近理论值，同时该协议在非对称信道下的性能优于对称信道。因此，脉冲数量有限或者无限时，MDI-QKD 协议在非对称信道情况下的整体性能都优于对称信道下的性能，所以在实际量子密钥分配协议中可以优先考虑使用非对称信道提高 MDI-QKD 协议的性能。

参　考　文　献

[1] Bennett C H, Brassard G. An update on quantum cryptography [M] // Blakley G R, Chaum D. Advances in cryptology. Lecture notes in computer science. Berlin, Heidelberg: Springer, 1985, 196: 475-480.

[2] Shor P W, Preskill J. Simple proof of security of the BB84 quantum key distribution protocol[J]. Physical Review Letters, 2000, 85(2): 441-444.

[3] Mayers D. Unconditional security in quantum cryptography[J]. Journal of the ACM, 2001, 48(3): 351-406.

[4] Gottesman D, Lo H K, Lutkenhaus N, et al. Security of quantum key distribution with imperfect devices[J]. Quantum Information and Computation, 2004, 4(5): 325-360.

[5] Makarov V. Controlling passively quenched single photon detectors by bright light[J]. New Journal of Physics, 2009, 11(6): 065003.

[6] Zhao Y, Fung C H F, Qi B, et al. Quantum

hacking: experimental demonstration of time-shift attack against practical quantum-key-distribution systems[J]. Physical Review A, 2008, 78(4): 042333.

[7] Makarov V, Skaar J. Faked states attack using detector efficiency mismatch on SARG04, phase-time, DPSK, and Ekert protocols[J]. Quantum Information and Computation, 2007, 8(6): 622-635.

[8] Lydersen L, Skaar J, Makarov V. Tailored bright illumination attack on distributed-phase-reference protocols[J]. Journal of Modern Optics, 2011, 58(8): 680-685.

[9] Lo H K, Curty M, Qi B. Measurement-device-independent quantum key distribution[J]. Physical Review Letters, 2012, 108(13): 130503.

[10] 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.

[11] Dong C, Zhao S H, Zhao W H, et al. Analysis of measurement device independent quantum key distribution with an asymmetric channel transmittance efficiency[J]. Acta Physica Sinica, 2014, 63(3): 030302.
东晨, 赵尚弘, 赵卫虎, 等. 非对称信道传输效率的测量设备无关量子密钥分配研究[J]. 物理学报, 2014, 63(3): 030302.

[12] Kang D N, He Y F. Quantum key distribution protocols based on asymmetric channels of odd coherent sources[J]. Acta Optica Sinica, 2017, 37(6): 0627001.
康丹娜, 何业锋. 基于奇相干光源非对称信道的量子密钥分配协议[J]. 光学学报, 2017, 37(6): 0627001.

[13] Zhang Y C, Yu S, Gu W Y. Squeezed-state measurement-device-independent quantum key distribution[J]. Scientific Reports, 2018, 8(1): 4115.

[14] Fasel S, Alibart O, Tanzili S, et al. High quality asynchronous heralded single photon source at telecom wavelength[J]. New Journal of Physics, 2004, 6(1): 628-629.

[15] Zhu F, Wang Q. Quantum key distribution protocol based on heralded single photon source[J]. Acta Optica Sinica, 2014, 34(6): 0627002.
朱峰, 王琴. 基于指示单光子源的量子密钥分配协议[J]. 光学学报, 2014, 34(6): 0627002.

[16] Zhou Y Y, Zhou X J, Su B B. A measurement-device-independent quantum key distribution protocol with a heralded single photon source[J]. Optoelectronics Letters, 2016, 12(2): 148-151.

[17] He Y F, Wang D, Yang H J, et al. Quantum key distribution based on heralded single photon sources and quantum memory[J]. Chinese Journal of Lasers, 2019, 46(4): 0412001.
何业锋, 王登, 杨红娟, 等. 基于指示单光子源和量子存储的量子密钥分配[J]. 中国激光, 2019, 46(4): 0412001.

[18] 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.

[19] Zhao S M, Gong L Y, Li Y Q, et al. A large-alphabet quantum key distribution protocol using orbital angular momentum entanglement[J]. Chinese Physics Letters, 2013, 30(6): 060305.

[20] Qiao W, Gao S C, Lei T, et al. Transmission of orbital angular momentum modes in grapefruit-type microstructure fiber[J]. Chinese Journal of Lasers, 2017, 44(4): 0406002.
乔文, 高社成, 雷霆, 等. 轨道角动量模式在柚子型微结构光纤中的传输[J]. 中国激光, 2017, 44(4): 0406002.

[21] Su Z K, Wang F Q, Lu Y Q, et al. Study on quantum cryptography using orbital angular momentum states of photons[J]. Acta Physica Sinica, 2008, 57(5): 3016-3021.
苏志锟, 王发强, 路轶群, 等. 基于光子轨道角动量的密码通信方案研究[J]. 物理学报, 2008, 57(5): 3016-3021.

[22] Yan L, Sun H, Zhao S M. Study on decoyed measurement device independent quantum key distribution protocol using orbital angular momentum[J]. Journal of Signal Processing, 2014, 30(11): 1275-1278.
颜龙, 孙豪, 赵生妹. 应用诱骗态的光子轨道角动量测量设备无关量子密钥分发协议的研究[J]. 信号处理, 2014, 30(11): 1275-1278.

[23] He Y F, Li D Q, Song C, et al. Quantum key distribution protocol based on odd coherent sources and orbital angular momentum[J]. Chinese Journal of Lasers, 2018, 45(7): 0712001.
何业锋, 李东琪, 宋畅, 等. 基于奇相干光源和轨道角动量的量子密钥分配协议[J]. 中国激光, 2018, 45(7): 0712001.

[24] He Y F, Yang H J, Wang D, et al. Quantum key distribution based on heralded pair coherent state and orbital angular momentum[J]. Acta Optica Sinica,

2019, 39(4): 0427001.
何业锋, 杨红娟, 王登, 等. 基于标记配对相干态和轨道角动量的量子密钥分配[J]. 光学学报, 2019, 39(4): 0427001.

[25] Zhu Z D, Zhao S H, Gu W Y, et al. Orbital-angular-momentum-encoded measurement-device-independent quantum key distributions under atmospheric turbulence[J]. Acta Optica Sinica, 2018, 38(12): 1227002.
朱卓丹, 赵尚弘, 谷文苑, 等. 大气湍流下的轨道角动量编码测量设备无关量子密钥分发[J]. 光学学报, 2018, 38(12): 1227002.

[26] Shen Z G, Wang L, Mao Q P, et al. Round-robin differential phase shift quantum key distribution protocol based on orbital angular momentum [J]. Acta Optica Sinica, 2019, 39(2): 0227001.
沈志冈, 王乐, 毛钱萍, 等. 基于轨道角动量的循环差分相移量子密钥分发[J]. 光学学报, 2019, 39(2): 0227001.

[27] Ma X F, Fung C H F, Razavi M. Statistical fluctuation analysis for measurement-device-independent quantum key distribution [J]. Physical Review A, 2012, 86(5): 052305.

[28] Sun S H, Gao M, Li C Y, et al. Practical decoy-state measurement-device-independent quantum key distribution[J]. Physical Review A, 2013, 87(5): 052329.

[29] Zhou X Y, Zhang C H, Guo G C, et al. The statistical fluctuation analysis for the measurement-device-independent quantum key distribution with heralded single-photon sources [J]. Quantum Information Processing, 2016, 15(6): 2455-2464.

[30] Zhu Z D, Zhang X, Zhao S H, et al. Measurement-device-independent quantum key distribution protocols for heralded pair coherent state[J]. Laser & Optoelectronics Progress, 2017, 54(12): 122703.
朱卓丹, 张茜, 赵尚弘, 等. 预报相干光子对的测量设备无关量子密钥分发协议[J]. 激光与光电子学进展, 2017, 54(12): 122703.

[31] Curtis J E, Grier D G. Modulated optical vortices [J]. Optics Letters, 2003, 28(11): 872-874.

[32] Lü H, Ke X Z. Research on the beam with orbital angular momentum used in encoding and decoding of optical communication[J]. Acta Optica Sinica, 2009, 29(2): 331-335.
吕宏, 柯熙政. 具轨道角动量光束用于光通信编码及解码研究[J]. 光学学报, 2009, 29(2): 331-335.

[33] Wang Q, Wang X B. Efficient implementation of the decoy-state measurement-device-independent quantum key distribution with heralded single-photon sources [J]. Physical Reviews A, 2013, 88(5): 052332.