基于标记配对相干态的量子密钥分配协议的统计涨落分析

何业锋[1,3]，赵艳坤[2*]，郭佳瑞[1]，李春雨[2]

[1]西安邮电大学网络空间安全学院，陕西 西安 710121；

[2]西安邮电大学通信与信息工程学院，陕西 西安 710121；

[3]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

摘要 为了更加全面分析测量设备无关量子密钥分配协议，对基于标记配对相干态的测量设备无关量子密钥分配协议进行了统计涨落分析。首先分析了当光源在统计涨落时，随着发送信号脉冲数的增加，误码率和密钥生成率与传输距离的关系。结果表明，增加脉冲数能增大密钥生成率和最大传输距离，降低误码率，且基于标记配对相干态的协议性能比基于指示单光子源的协议性能要好。进一步分析了光源在统计涨落时，基于标记配对相干态的测量设备无关量子密钥分配协议在非对称信道中的密钥生成率与传输距离的关系，由仿真结果得知，非对称信道时的性能比对称信道时的性能好。

关键词 量子光学；量子密钥分配；测量设备无关；标记配对相干态；非对称信道

中图分类号 TN918 **文献标志码** A **doi**：10.3788/AOS202040.0727002

Statistical Fluctuation Analysis of Quantum Key Distribution Protocols Based on Heralded Pair Coherent State

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

[1] *School of Cyberspace Security, Xi'an University of Posts and Telecommunications, Xi'an, shaanxi* 710121, *China*;

[2] *School of Communication and Information Engineering, Xi'an University of Posts and Telecommunications, Xi'an, shaanxi* 710121, *China*;

[3] *National Engineering Laboratory for Wireless Security, Xi'an University of Posts and Telecommunications, Xi'an, shaanxi* 710121, *China*

Abstract In order to analyze the measurement-device-independent quantum key distribution protocol more comprehensively, the statistical fluctuation analysis of measurement-device-independent quantum key distribution protocols based on heralded pair coherent state is carried out. First, with the increase of the number of transmitted signal pulses in the statistical fluctuation of light source, the relationships of bit error rate and key generation rate with transmission distance are analyzed. The results show that increasing the number of pulses can improve the key generation rate and the maximum transmission distance, and can reduce the bit error rate. Moreover, the measurement-device-independent quantum key distribution protocol based on heralded pair coherent state has better performance than the one based on heralded single photon sources. When the light source is statistical fluctuating, the relationship between the key generation rate and the transmission distance of measurement-device-independent quantum key distribution protocol based on heralded pair coherent state in asymmetric channels is further analyzed, and the simulation results show that this protocol in asymmetric channels has better performance than that in symmetric channels.

Key words quantum optics; quantum key distribution; measurement device independent; heralded pair coherent state; asymmetric channel

OCIS codes 270.5565; 270.5568; 270.1670; 270.343

收稿日期：2019-10-30；**修回日期**：2019-11-07；**录用日期**：2019-12-26

基金项目：国家自然科学基金(61802302，61772418)

* **E-mail**：1364853816@qq.com

1 引　言

量子密钥分配(QKD)以量子力学和信息论为基础,具有无条件安全特性[1-2],受到了人们的广泛关注,已成为通信安全领域内的研究热点。自1984年BB84协议被提出以来[3],量子密钥分配有了极大的发展[4-6]。虽然量子密钥分配的无条件安全特性在理想情况下已得到证明,但现实中量子密钥分配由于光源和测量设备等的非完美性而易遭到各种攻击。例如:光子数分离攻击[7]、时移攻击[8]、随机部分相位攻击[9]、探测器致盲攻击[10]等。其中攻击最多的是针对探测器侧信道的攻击。Lo等[11]提出了测量设备无关的量子密钥分配(MDI-QKD),避免了所有针对探测器漏洞的攻击,并且将通讯距离增加为原QKD协议的两倍。该方案自提出以来得到了人们的广泛研究,取得了一系列的成果[12-15]。Tamaki等[16]研究了基于离散变量的相位编码的MDI-QKD协议,Abruzzo等[17]研究了加量子存储单元的MDI-QKD协议。

在实际量子密钥分配协议中,往往利用弱相干态光源[13](WCS)来代替理想单光子源。事实上用WCS时,真空脉冲和多光子脉冲会导致密钥生成率降低。指示单光子源[18](HSPS)与WCS光源相比,降低了真空脉冲和多光子的比率,从而能提高基于HSPS的MDI-QKD协议的密钥生成率[19],因此也用HSPS来代替理想单光子源。文献[20]研究了基于指示单光子源的非对称信道量子密钥分配。文献[21]在基于指示单光子源的MDI-QKD的基础上添加了量子存储单元,增大了量子密钥分配的传输距离。标记配对相干态(HPCS)光源比HSPS有更高的单光子比率[22]。Wang等[23]的研究表明,基于HPCS的MDI-QKD协议要比基于HSPS的MDI-QKD协议性能好。文献[24]研究了基于HPCS和轨道角动量的密钥分配。

在实际的量子密钥分配中,发送的信号脉冲数是有限的,这种情况下会引入统计涨落的因素,减小密钥生成率和最大安全传输距离。Yu等[25]通过研究基于不同光源的MDI-QKD协议的统计涨落,得到了受统计涨落影响的密钥生成率公式。文献[26]给出了HSPS下的MDI-QKD协议的统计涨落分析,并与WCS的情况进行对比,结果表明,统计涨落下HSPS比WCS拥有更好的稳定性。本文研究基于HPCS的MDI-QKD协议的统计涨落,研究结果对分析MDI-QKD的安全性具有重要意义。

本文先就对称信道情况下基于HPCS的MDI-QKD协议和基于HSPS的MDI-QKD协议的误码率和密钥生成率的统计涨落情况进行了分析和比较。然后对非对称信道情况下基于HPCS的MDI-QKD协议的密钥生成率的统计涨落情况进行了分析。仿真结果表明,脉冲数无论是有限还是无限,基于HPCS的MDI-QKD协议比基于HSPS的MDI-QKD协议的性能要好,并且基于HPCS的MDI-QKD协议在非对称信道下的性能始终比对称信道下的性能好。

2 基本原理

2.1 HPCS及性质

标记配对相干态[27]能同时产生两种模式的光子(空闲模式和信号模式),被触发探测器探测的是空闲模式光子,可以用来预测另一模式的光子到达第三方的时间,减小了暗计数的影响。对信号模式的光子进行编码后将其发送给第三方(非可信任)进行Bell态测量。HPCS的光子数$P(n)$服从亚泊松分布,即

$$P(n)=\frac{1}{\mathrm{I}_0(2\mu)}\frac{\mu^{2n}}{(n!)^2}\left[1-(1-\eta_{\mathrm{d}}^{(H)})^n(1-P_{\mathrm{d}}^{(H)})\right],\tag{1}$$

式中:n为光子数;μ为光脉冲强度;$\eta_{\mathrm{d}}^{(H)}$为触发探测器的探测效率;$P_{\mathrm{d}}^{(H)}$为暗计数率,其中H代表a或b,表示Alice或Bob端的触发探测器;$\mathrm{I}_0(\cdot)$为修正的第一类贝塞尔函数。在同一光强下HSPS和HPCS光子数的分布如表1所示[28]。

表1　HSPS和HPCS的光子数分布

Table 1　Photon number distribution of HSPS and HPCS

Source	Single photon	Multi photon	Probability of vacuum
HSPS	0.7274	0.2726	1.94×10^{-6}
HPCS	0.9255	0.0744	4.93×10^{-6}

2.2 基于HPCS的MDI-QKD协议

基于HPCS的MDI-QKD系统模型如图1所示,其中Alice和Bob是发送方,Charlie是第三方,PBS是偏振分束器,BS是分束器,Pol-M是偏振调制器,IM是强度调制器,1H、2H、1V、2V是第三方的四个单光子探测器。

1) Alice和Bob发送HPCS纠缠光子对。其中空闲模式的光子被触发探测器a、b探测,并根据探测结果来预测信号模式的光子到达第三方的时间。

2) 利用Pol-M选取X基或Z基,对信号模式的光子进行编码。然后利用IM将光子调制成三种

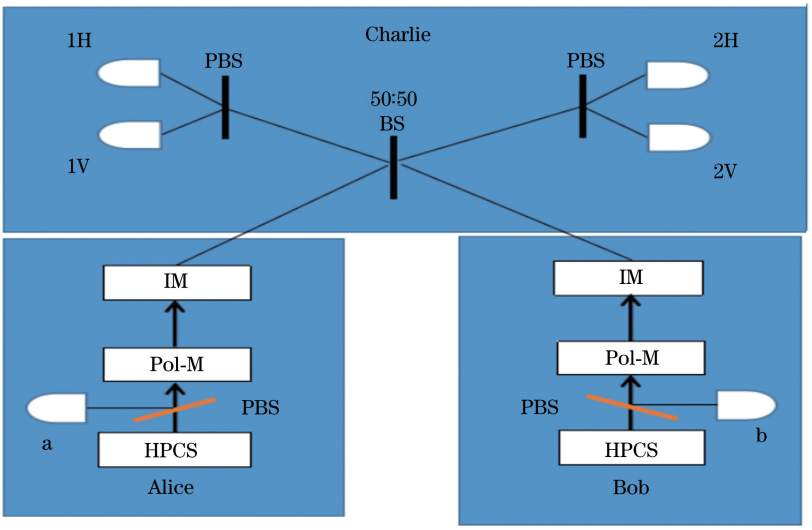

图 1　基于 HPCS 的 MDI-QKD 协议的系统模型

Fig. 1　System model of MDI-QKD protocol based on HPCS

强度即 μ_i 和 v_j，其中，μ_i 为 Alice 端的光脉冲强度，v_j 为 Bob 端的光脉冲强度，$i(j)=0,1,2$，分别对应于真空态、诱骗态和信号态，且 $\mu_2>\mu_1>\mu_0=0$，$v_2>v_1>v_0=0$。

3) Charlie 对 Alice 和 Bob 发送的光子进行贝尔态测量，当信号脉冲传输完毕后，第三方公布测量结果。发送方(Alice 和 Bob)中的一个根据第三方公布的成功测量结果进行比特翻转，进而筛选出原始密钥。

4) 对原始密钥进行纠错和保密加强处理，得到安全密钥。

3　密钥生成率分析

当 Alice 和 Bob 发送的信号脉冲强度分别为 x 和 y 时，总增益 $Q_{x,y}^{(W)}$ 和误码率 $E_{x,y}^{(W)}Q_{x,y}^{(W)}$ 分别为

$$Q_{x,y}^{(W)}=\sum_{n,m=0}^{\infty}P_n(x)P_m(y)Y_{n,m}^{(W)},\tag{2}$$

$$E_{x,y}^{(W)}Q_{x,y}^{(W)}=\sum_{n,m=0}^{\infty}P_n(x)P_m(y)e_{n,m}^{(W)}Y_{n,m}^{(W)},\tag{3}$$

式中：$P_n(x)$ 为 Alice 端光脉冲强度为 x 时，光脉冲数为 n 的概率；$P_m(y)$ 为 Bob 端光脉冲强度为 y 时，光脉冲数为 m 的概率；W 表示编码选用的 X 基或 Z 基；$Y_{n,m}^{(W)}$ 表示 Alice 和 Bob 发送脉冲数为 n 和 m 时第三方成功进行贝尔态测量(BSM)的概率；$e_{n,m}^{(W)}$ 为相应的误码率；$Q_{x,y}^{(W)}$ 和 $E_{x,y}^{(W)}$ 可以通过实验测得，本文用文献[29]的方式来获得实验结果。通过(2)式和(3)式，由文献[26]的方法可以估算出 $Y_{1,1}^{W}$ 的下界 $Y_{1,1}^{(W),\mathrm{L}}$ 和 $e_{1,1}^{(W)}$ 的上界 $e_{1,1}^{(W),\mathrm{U}}$，即

$$Y_{1,1}^{(W)}\geqslant Y_{1,1}^{(W),\mathrm{L}}=\frac{P_1(\mu_2)P_2(v_2)(Q_{\mu_1,v_1}^{(W)}-\tilde{Q}_{0,0})-P_1(\mu_1)P_2(v_1)(Q_{\mu_2,v_2}^{(W)}-\tilde{Q}'_{0,0})}{P_1(\mu_2)P_1(v_1)[P_1(\mu_1)P_2(v_2)-P_1(\mu_2)P_2(v_1)]},\tag{4}$$

式中：$\tilde{Q}_{0,0}=Q_{\mu_1,0}+Q_{0,v_1}-Q_{0,0}$，$\tilde{Q}'_{0,0}=Q_{\mu_2,0}+Q_{0,v_2}-Q_{0,0}$，其中 $Q_{\mu_1,0}$ 是 Alice 发送光脉冲强度为 μ_1，Bob 发送光脉冲强度为 0 时的增益；Q_{0,v_1} 是 Alice 发送光脉冲强度为 0，Bob 发送光脉冲强度为 v_1 时的增益；$Q_{0,0}$ 是 Alice 和 Bob 发送光脉冲强度均为 0 时的增益；$Q_{\mu_2,0}$ 是 Alice 发送光脉冲强度为 μ_2，Bob 发送光脉冲强度为 0 时的增益；Q_{0,v_2} 是 Alice 发送光脉冲强度为 0，Bob 发送光脉冲强度为 v_2 时的增益。

$$e_{1,1}^{(W)}\leqslant e_{1,1}^{(W),\mathrm{U}}=\frac{E_{\mu_1,v_1}^{(W)}Q_{\mu_1,v_1}^{(W)}-E_{\mu_1,0}^{(W)}Q_{\mu_1,0}^{(W)}-E_{0,v_1}^{(W)}Q_{0,v_1}^{(W)}+E_{0,0}^{(W)}Q_{0,0}^{(W)}}{P_1(\mu)P_1(v)Y_{1,1}^{(W)}}。\tag{5}$$

最后可以得到密钥生成率为

$$R\geqslant P_1(\mu_2)P_1(v_2)Y_{1,1}^{(Z)}[1-H_2(e_{1,1}^{(X)})]-Q_{\mu_2,v_2}^{(Z)}f(E_{\mu_2,v_2}^{(Z)})H(E_{\mu_2,v_2}^{(Z)}),\tag{6}$$

式中：$f(\cdot)$ 为纠错效率函数，取 $f=1.16$[11]；　$H_2(\cdot)$ 是二进制香浓熵函数。

4　基于 HPCS 的 MDI-QKD 协议的统计涨落分析

4.1　对称信道下 MDI-QKD 协议的统计涨落分析

在实际 MDI-QKD 协议中，Alice 和 Bob 发送的是具有有限数据集大小的信号脉冲，在参数估计过程中不可避免地会产生统计涨落。考虑到有限的数据尺寸效应，下面进行了基于 HPCS 的 MDI-QKD 的统计涨落分析。

估计统计涨落时的增益（$Q_{x,y}^{(W)}$）和误码率（$E_{x,y}^{(W)}$）为

$$\begin{cases} |\hat{Q}_{x,y}^{(W)}-Q_{x,y}^{(W)}|\leqslant\nabla_{x,y}^{(W)} \\ |\hat{E}_{x,y}^{(W)}-E_{x,y}^{(W)}|\leqslant\nabla_{x,y}^{\prime(W)} \end{cases}, \tag{7}$$

式中：$\nabla_{x,y}^{(W)}=\gamma\sqrt{\frac{Q_{x,y}^{(W)}}{N_{x,y}^{(W)}}}$，$\nabla_{x,y}^{\prime(W)}=\gamma\sqrt{\frac{E_{x,y}^{(W)}}{N_{x,y}^{(W)}}}$，$N_{x,y}^{(W)}$ 是当 Alice 和 Bob 各自发送的光源脉冲强度为 x 和 y 时的脉冲数，标准偏差 $\gamma=5.3$[25]；$\hat{Q}_{x,y}^{(W)}$，$\hat{E}_{x,y}^{(W)}$ 分别为 $Q_{x,y}^{(W)}$，$E_{x,y}^{(W)}$ 的界限值。由(7)式得

$$\begin{cases} Q_{x,y}^{(W)}\leqslant Q_{x,y}^{(W),\mathrm{U}}=\hat{Q}_{x,y}^{(W)}+\nabla_{x,y}^{(W)} \\ Q_{x,y}^{(W)}\geqslant Q_{x,y}^{(W),\mathrm{L}}=\hat{Q}_{x,y}^{(W)}-\nabla_{x,y}^{(W)} \\ E_{x,y}^{(W)}\leqslant E_{x,y}^{(W),\mathrm{U}}=\hat{E}_{x,y}^{(W)}+\nabla_{x,y}^{\prime(W)} \\ E_{x,y}^{(W)}\geqslant E_{x,y}^{(W),\mathrm{L}}=\hat{E}_{x,y}^{(W)}-\nabla_{x,y}^{\prime(W)} \end{cases}。 \tag{8}$$

由(4)式、(5)式、(8)式得到考虑统计涨落时的 $Y_{1,1}^{(W)}$，$e_{1,1}^{(W)}$ 为

$$Y_{1,1}^{(W)}\geqslant Y_{1,1}^{(W),\mathrm{L}}=\frac{P_1(\mu_2)P_2(v_2)(Q_{\mu_1,v_1}^{(W),\mathrm{L}}-Q_{0,0}^{(W),\mathrm{U}})-P_1(\mu_1)P_2(v_1)(Q_{\mu_2,v_2}^{(W),\mathrm{U}}-Q_{0,0}^{(W),\mathrm{L}})}{P_1(\mu_2)P_1(v_1)[P_1(\mu_1)P_2(v_2)-P_1(\mu_2)P_2(v_1)]}, \tag{9}$$

$$e_{1,1}^{(W)}\leqslant e_{1,1}^{(W),\mathrm{U}}=\frac{E_{\mu_1,v_1}^{(W),\mathrm{U}}Q_{\mu_1,v_1}^{(W),\mathrm{U}}-E_{\mu_1,0}^{(W),\mathrm{L}}Q_{\mu_1,0}^{(W),\mathrm{L}}-E_{0,v_1}^{(W),\mathrm{L}}Q_{0,v_1}^{(W),\mathrm{L}}+E_{0,0}^{(W),\mathrm{U}}Q_{0,0}^{(W),\mathrm{U}}}{P_1(\mu)P_1(v)Y_{1,1}^{(W)}}, \tag{10}$$

密钥生成率为

$$R\geqslant P_1(\mu_2)P_1(v_2)Y_{1,1}^{(Z),\mathrm{L}}[1-H_2(e_{1,1}^{(X),\mathrm{U}})]-Q_{\mu_2,v_2}^{(Z)}f(E_{\mu_2,v_2}^{(Z)})H(E_{\mu_2,v_2}^{(Z)})。 \tag{11}$$

利用文献[29]的方法得到 X 基的增益 $Q_{\mu_i,v_j}^{(X),11}$ 和误码率 $E_{\mu_i,v_j}^{(X),11}Q_{\mu_i,v_j}^{(X),11}$ 分别为

$$Q_{\mu_i,v_j}^{(X),11}=2y_{i,j}^2[1+2y_{i,j}^2-4y_{i,j}\mathrm{I}_0(x_{i,j})+\mathrm{I}_0(2x_{i,j})], \tag{12}$$

$$E_{\mu_i,v_j}^{(X),11}Q_{\mu_i,v_j}^{(X),11}=e_0Q_{\mu_i,v_j}^{(X),11}-2(e_0-e_\mathrm{d})y_{ij}^2[\mathrm{I}_0(2x_{ij})-1], \tag{13}$$

式中：e_0 是偏正系数；e_d 是修正系数。Z 基的增益和误码率为

$$\begin{cases} Q_{\mu_i,v_j}^{(Z),11}=Q_{c_{ij}}+Q_{e_{ij}} \\ E_{\mu_i,v_j}^{(Z),11}Q_{\mu_i,v_j}^{(Z),11}=e_\mathrm{d}Q_{c_{ij}}+(1-e_\mathrm{d})Q_{e_{ij}} \end{cases}, \tag{14}$$

$$Q_{c_{ij}}=2(1-P_\mathrm{d})^2\exp(-\mu_{ij}^{\prime}/2)[1-(1-P_\mathrm{d})\exp(-\eta_\mathrm{a}\mu_i/2)][1-(1-P_\mathrm{d})\exp(-\eta_\mathrm{b}v_j/2)], \tag{15}$$

$$Q_{e_{ij}}=[2P_\mathrm{d}(1-P_\mathrm{d})^2\exp(-\mu_{ij}^{\prime}/2)][\mathrm{I}_0(2x_{ij})-(1-P_\mathrm{d})\exp(-\mu_{ij}^{\prime}/2)], \tag{16}$$

式中：$Q_{c_{ij}}$ 为光子从同侧射出时的探测概率；$Q_{e_{ij}}$ 为光子从两侧射出时的探测概率；P_d 为第三方探测器的暗计数率；平均光子数 $\mu_{ij}^{\prime}=\eta_\mathrm{a}\mu_i+\eta_\mathrm{b}v_j$，其中 η_a 为 Alice 的传输效率，η_b 为 Bob 的传输效率；$x_{ij}=\sqrt{\eta_\mathrm{a}\mu_i\eta_\mathrm{b}v_j}/2$；$y_{ij}=(1-P_\mathrm{d})\exp(\mu_{ij}^{\prime}/4)$。

当 Alice 到 Charlie 的传输信道长度和 Bob 到 Charlie 的传输信道长度相等时（$L_\mathrm{AC}=L_\mathrm{BC}=L$），则称传输信道为对称信道。此时系统传输效率为信道传输效率 t 和探测效率 η_d 的乘积：$\eta_\mathrm{a}=\eta_\mathrm{b}=\eta=t\eta_\mathrm{d}$，$t=10^{-\alpha L/10}$，$\alpha$ 为信道损耗，取 $\alpha=0.2\ \mathrm{dB\cdot km^{-1}}$。

4.2　非对称信道下 MDI-QKD 协议的统计涨落分析

当信道为非对称信道时（$L_\mathrm{AC}\neq L_\mathrm{BC}$），单边信道的传输效率分别为 $t_\mathrm{AC}=10^{-\alpha L_\mathrm{AC}/10}$，$t_\mathrm{BC}=10^{-\alpha L_\mathrm{BC}/10}$。令 $\sigma=L_\mathrm{AC}/L_\mathrm{BC}$（$0\leqslant\sigma<1$），得到单边传输效率为 $\eta_\mathrm{a}=\eta^{2\sigma/(\sigma+1)}$，$\eta_\mathrm{b}=\eta^{2/(\sigma+1)}$，由此可以分别分析对称信道下基于 HPCS 的 MDI-QKD 协议和非对称信道下基于 HPCS 的 MDI-QKD 协议。

5　仿真结果及分析

用数值模拟来研究统计涨落对 MDI-QKD 协议的影响，对比了基于 HSPS 的 MDI-QKD 协议和基于 HPCS 的 MDI-QKD 协议在统计涨落时的性能。

在仿真时诱骗态和信号态光强分别取 0.05 和 0.36，信号态、诱骗态和真空态的脉冲数的比值关系为 $N_{\mu_2}^{(W)}:N_{\mu_1}^{(W)}:N_{\mu_0}^{(W)}=6:3:1$。Alice 和 Bob 端的触发探测器效率和暗计数率分别取 $\eta_{\mathrm{d}}^{(H)}=0.9$ 和 $P_{\mathrm{d}}^{(H)}=10^{-6}$。其他参数如表 2 所示。

表 2　主要模拟仿真参数

Table 2　Main simulation parameters

Parameter	P_{d}	e_0	η_{d}
Value	3.6×10^{-6}	0.5	0.145

图 2 为传输距离与 $e_{1,1}^{(X)}$ 的关系，可以看出，基于 HPCS 的 MDI-QKD 协议的误码率曲线位于基于 HSPS 的 MDI-QKD 协议的下方，表明在相同传输距离和相同发送脉冲数的情况下，基于 HPCS 的 MDI-QKD 协议的误码率较小。例如：在脉冲数 $N=10^{13}$ 且传输距离为 200 km 时，基于 HPCS 的 MDI-QKD 协议的误码率是 0.1184，而基于 HSPS 的 MDI-QKD 协议的误码率是 0.1528，显然前者的误码率小于后者。在脉冲数为无穷且传输距离达到 255 km 时，基于 HPCS 的 MDI-QKD 协议的误码率为 0.0179，而基于 HSPS 的 MDI-QKD 协议误码率为 0.0366，前者的误码率小于后者。

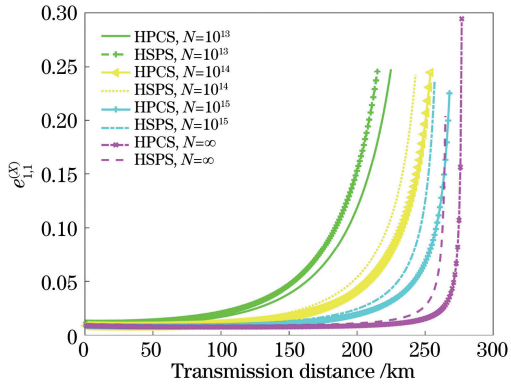

图 2　传输距离与 $e_{1,1}^{(X)}$ 的关系

Fig. 2　Relationship between transmission distance and $e_{1,1}^{(X)}$

在同种光源下，脉冲数为 $N=10^{15}$ 的误码率曲线在 $N=10^{14}$ 的误码率曲线下方；脉冲数为 $N=10^{14}$ 的误码率曲线在 $N=10^{13}$ 的误码率曲线下方；表明随着脉冲数的逐渐增加，误码率曲线逐渐向脉冲数无穷时的曲线逼近。说明增加脉冲数可以有效地降低误码率，但是通过这种方法降低误码率存在理论极限。当脉冲数趋近无穷时，通过增加脉冲数来降低误码率的效果将降低，直到增加脉冲数对降低误码率失去效果。

图 3 为对称信道中密钥生成率与传输距离的关系，可以看出，在对称信道中，考虑统计涨落时，基于 HPCS 的 MDI-QKD 的密钥生成率整体比基于 HSPS 的 MDI-QKD 的密钥生成率更高。从密钥生成率来看，基于 HPCS 的 MDI-QKD 协议在脉冲数有限和无限时的性能比基于 HSPS 的 MDI-QKD 协议的性能要好。例如：在脉冲数为 $N=10^{13}$ 且传输距离为 200 km 时，基于 HPCS 的 MDI-QKD 协议的密钥生成率是 4.8×10^{-6}，而基于 HSPS 的 MDI-QKD 协议的密钥生成率是 3.6×10^{-8}，显然前者高于后者。在脉冲数为无穷且传输距离为 250 km 时，基于 HPCS 的 MDI-QKD 协议的密钥生成率为 1.5×10^{-6}，而基于 HSPS 的 MDI-QKD 协议的密钥生成率为 1.4×10^{-8}，前者高于后者。从最大传输距离来看，基于 HPCS 的 MDI-QKD 协议的优势不太明显。例如：在脉冲数为 $N=10^{14}$ 时，基于 HPCS 的 MDI-QKD 协议的最大传输距离为 250 km，而基于 HSPS 的 MDI-QKD 协议的最大传输距离为 244 km。在脉冲数为无穷时，基于 HPCS 的 MDI-QKD 协议的最大传输距离为 275 km，而基于 HSPS 的 MDI-QKD 协议的最大传输距离为 265 km。随着脉冲数的增加，基于 HPCS（或 HSPS）的 MDI-QKD 协议的最大安全传输距离也逐渐增加，但当脉冲数趋于无穷时，基于 HPCS（或 HSPS）的 MDI-QKD 协议的最大安全传输距离存在理论上界。这是由于当传输距离达到 275 km 时误码率会急剧增大，此时的密钥生成率会陡然降低，信号脉冲达到 MDI-QKD 的最大安全传输距离。

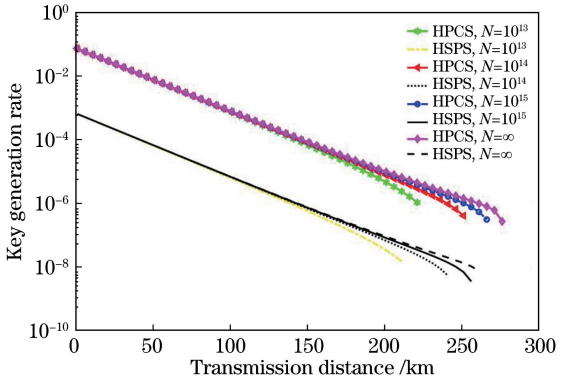

图 3　对称信道中密钥生成率与传输距离的关系

Fig. 3　Relationship between key generation rate and transmission distance in symmetric channel

图 4 为非对称信道中密钥生成率与传输距离的关系。在图 4 中，Alice 到第三方的距离 L_{AC} 与 Bob 到第三方的距离 L_{BC} 之比 $\sigma\in\{0.4,0.6,1.0\}$。$\sigma<1$ 表明 Alice 距离第三方较近，$\sigma=1$ 为对称信道的情况。由图 4 可知，脉冲数无论是有限还是无限，基于

HPCS 的 MDI-QKD 协议在非对称信道情况下的密钥生成率和最大安全传输距离都更大。例如：脉冲数为 10^{13} 时，$\sigma=0.4$ 的情况下基于 HPCS 的 MDI-QKD 协议的最大安全传输距离为 410 km，$\sigma=1$ 的情况下基于 HPCS 的 MDI-QKD 协议的最大安全传输距离为 230 km。在脉冲数趋于无穷时，$\sigma=0.4$ 的情况下基于 HPCS 的 MDI-QKD 协议的最大安全传输距离为 510 km；$\sigma=1$ 的情况下基于 HPCS 的 MDI-QKD 协议的最大安全传输距离为 275 km。

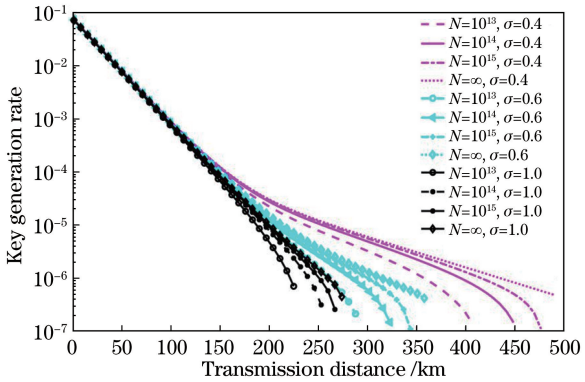

图 4　非对称信道中密钥生成率与传输距离的关系

Fig. 4　Relationship between key generation rate and transmission distance in asymmetric channel

6　结　　论

研究了在不同信号脉冲数的情况下基于 HPCS 的 MDI-QKD 协议的统计涨落的情况。比较了基于 HPCS 的 MDI-QKD 协议和基于 HSPS 的 MDI-QKD 协议在统计涨落时的密钥生成率和误码率。结果表明，随着传输距离的增加，误码率增大，密钥生成率减小；通过增加信号脉冲数，可以延缓 MDI-QKD 协议的误码率增加幅度，提高 MDI-QKD 协议的密钥生成率和密钥的最大传输距离。与基于 HSPS 的 MDI-QKD 协议相比，基于 HPCS 的 MDI-QKD 协议在统计涨落时的性能更加优越，密钥生成率更高。分析了在非对称信道的情况下基于 HPCS 的 MDI-QKD 协议的统计涨落，仿真了密钥生成率的情况，其结果表明，脉冲数无论是有限还是无限，协议在非对称信道下的性能始终比在对称信道下的性能好。因此，在实际应用中可以通过增加信号脉冲数和采用非对称信道的方法来提高 MDI-QKD 协议在脉冲数有限时的性能。

参　考　文　献

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

[2] Gottesman D, Lo H, Lutkenhaus N, et al. Security of quantum key distribution with imperfect devices [C]//International Symposium on Information Theory, June 27-July 2, 2004, Chicago, IL, USA. New York: IEEE, 2003: 8178599.

[3] 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: Springer, 1984, 196: 475-480.

[4] Bennett C H, Brassard G, Ekert A K. Quantum cryptography [J]. Scientific American, 1992, 267(4): 50-57.

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

[6] Zhu Q L, Shi L, Wei J H, et al. Background light suppression in free space quantum key distribution [J]. Laser & Optoelectronics Progress, 2018, 55(6): 060004.
朱秋立, 石磊, 魏家华, 等. 自由空间量子密钥分配的背景光抑制[J]. 激光与光电子学进展, 2018, 55(6): 060004.

[7] Brassard G, Lütkenhaus N, Mor T, et al. Limitations on practical quantum cryptography [J]. Physical Review Letters, 2000, 85(6): 1330-1333.

[8] Zhao Y, Fung C HF, 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.

[9] Sun S H, Liang L M. Experimental demonstration of an active phase randomization and monitor module for quantum key distribution [J]. Applied Physics Letters, 2012, 101(7): 071107.

[10] Makarov V, Skaar J. Faked states attack using detector efficiency mismatch on SARG04, phase-time, DPSK, and Ekert protocols [J]. Quantum Information & Computation, 2007, 8(6): 0622-0635.

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

[12] Dong C, Zhao S H, Zhang N, et al. Measurement-device-independent quantum key distribution with odd coherent state [J]. Acta Physica Sinica, 2014, 63(20): 200304.
东晨, 赵尚弘, 张宁, 等. 奇相干光源的测量设备无关量子密钥分配研究[J]. 物理学报, 2014, 63(20): 200304.

[13] 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.

[14] 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.

[15] Zhu Z D, Zhao S H, Wang X Y, et al. Phase modulate free measurement device independent quantum key distribution [J]. Journal of Optoelectronics • Laser, 2018, 29(2): 181-186.
朱卓丹, 赵尚弘, 王星宇, 等. 相位调制无关的测量设备无关量子密钥分配协议[J]. 光电子 • 激光, 2018, 29(2): 181-186.

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

[17] Abruzzo S, Kampermann H, Bruss D. Measurement-device-independent quantum key distribution with quantum memories [J]. Physical Review A, 2013, 89(1): 012301.

[18] 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.

[19] 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.

[20] He Y F, Song C, Li D Q, et al. Asymmetric-channel quantum key distribution based on heralded single-photon sources [J]. Acta Optica Sinica, 2018, 38(3): 0327001.
何业锋, 宋畅, 李东琪, 等. 基于指示单光子源的非对称信道量子密钥分配[J]. 光学学报, 2018, 38(3): 0327001.

[21] 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.

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

[23] Wang X, Wang Y, Chen R K, et al. Measurement-device-independent quantum key distribution with heralded pair coherent state [J]. Laser Physics, 2016, 26(6): 065203.

[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] Yu Z W, Zhou Y H, Wang X B. Statistical fluctuation analysis for measurement-device-independent quantum key distribution with three-intensity decoy-state method[J]. Physical Review A, 2015, 91(3): 032318.

[26] 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.

[27] Zhou Y Y, Zhang H Q, Zhou X J, et al. Analysis of the performance of decoy quantum key distribution based on heralded paired coherent state light source [J]. Acta Physica Sinica, 2013, 62(20): 200302.
周媛媛, 张合庆, 周学军, 等. 基于标记配对相干态光源的诱骗态量子密钥分配性能分析[J] .物理学报, 2013, 62(20): 200302.

[28] Dong C, Zhao S H, Shi L. Measurement device-independent quantum key distribution with heralded pair coherent state [J]. Quantum Information Processing, 2016, 15(10): 4253-4263.

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