# 标记配对相干态下有限探测器死时间的测量设备无关量子密钥分配

何业锋[1,3]，赵艳坤[2*]，李春雨[2]，郭佳瑞[1]

[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]桂林电子科技大学广西密码学与信息安全重点实验室，广西 桂林 541004

**摘要** 量子密钥分配在实际应用中会受到有限探测器死时间的影响，当信号脉冲发送速率过大时，探测器测量失败的概率增加，安全密钥生成速率降低。对标记配对相干态光源下测量设备无关量子密钥分配的有限探测器死时间问题进行了分析。研究并仿真了安全密钥生成速率与信号发送速率的关系。考虑探测器死时间时，基于标记配对相干态光源的测量设备无关量子密钥分配协议的安全密钥生成速率比基于弱相干光源的测量设备无关量子密钥分配协议的安全密钥生成速率高。分析了有限探测器死时间 $\tau$ 分别为 50，100，150 ns 时安全密钥生成速率的情况。结果表明，有限探测器死时间越大，安全密钥生成速率的极限值越低。安全密钥生成速率的极限与有限探测器死时间的关系为 $8.1\times10^3/\tau$。

**关键词** 量子光学；量子密钥分配；标记配对相干态；探测器死时间

**中图分类号** TN918 **文献标志码** A **doi**：10.3788/AOS202040.2427001

# Measurement-Device-Independent Quantum Key Distribution of Finite Detector′s Dead Time in Heralded Pair Coherent State

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

[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] *Guangxi Key Laboratory of Cryptography and Information Security, Guilin University of Electronic Technology, Guilin, Guangxi* 541004, *China*

**Abstract** In its practical applications, quantum key distribution is affected by the finite detector dead time. When the signal pulse transmission rate is too large, the probability of detector′s measurement failure increases and the security key generation rate decreases. In this paper, the finite detector dead time problem is analyzed for measurement-device-independent quantum key distribution under the heralded pair coherent state photon source. The relationship between the security key generation rate and the signal transmission rate is studied and simulated. Considering the detector′s dead time, the secure key generation rate of the measurement-device-independent quantum key distribution protocol based on the heralded pair coherent state photon source is higher than that of the measurement-device-independent quantum key distribution protocol based on the weak coherent state photon source. In addition, the security key generation rates are analyzed with the respective finite detector′s dead time $\tau$ of 50, 100, and 150 ns. The results show that the higher the detector′s dead time is, the lower the limit value of the security key generation rate is. The relation between the limit value of the security key generation rate and the finite detector′s dead time is $8.1\times10^3/\tau$.

**Key words** quantum optics; quantum key distribution; heralded pair coherent state; detector′s dead time

**OCIS codes** 270.5565; 270.5568; 270.1670; 270.343

**收稿日期**：2020-07-28；**修回日期**：2020-08-16；**录用日期**：2020-09-15

**基金项目**：国家自然科学基金(61802302)、广西密码学与信息安全重点实验室研究课题(GCIS201923)

* **E-mail**：1364853816@qq.com

## 1 引　言

量子密钥分配(QKD)可用于密钥协商,量子力学定律保证了密钥的无条件安全特性[1-2]。其中BB84协议[3]是一种常用的QKD协议,可以以原始形式使用,也可以通过添加诱骗态来提高性能[4-5]。近年来量子密钥分配因其独特的特性而成为研究的热点,取得了一些不错的成果[6-8]。虽然QKD具有无条件安全的特性,但由于理想单光子源难以实现,而替代的光源发送的脉冲中存在较多的多光子脉冲以及测量设备缺陷等问题,因此量子密钥分配系统易遭受各种攻击。例如:针对光源进行的光子数分离攻击[9-10]和随机部分相位攻击[11]等,以及针对光子探测器实施的时移攻击[12]和致盲攻击等[13],其中针对探测器侧信道的攻击是最多的。2012年,Lo等[14]提出了三方的量子密钥分配方案,即测量设备无关的量子密钥分配(MDI-QKD)方案。该方案解决了探测器侧信道攻击的问题,并将通信距离提高为原QKD协议的两倍。自MDI-QKD方案发表以来,其受到了普遍关注并得到了广泛研究[15-18]。Tamaki等[19]进行了相位编码的MDI-QKD协议的研究,Abruzzo等[20]研究了含有量子存储单元的MDI-QKD协议。文献[21]通过引入矢量涡流光束,提出了表现不同自由度之间单粒子量子纠缠形式的改进MDI-QKD方案。Yu等[22]进行了基于不同光源的MDI-QKD协议的统计涨落的研究。Wang等[23]进行了大气湍流条件下轨道角动量(OAM)编码的MDI-QKD协议的研究。近年来研究者提出了一些四方的MDI-QKD协议。文献[24]提出了一种基于四粒子簇态的半量子密钥分配协议,该协议可以同时实现一个量子方和两个经典方之间的密钥分配。

在QKD中,通常用弱相干态(WCS)光源[15]或指示单光子源(HSPS)[25]作为信源。文献[26]研究了传输信道为非对称信道时基于HSPS的MDI-QKD协议,分析了非对称信道情况下的密钥生成率。文献[27]在信源采用HSPS的情况下将量子存储单元与MDI-QKD协议相结合,增大了量子密钥分配的传输距离。相比于WCS光源和HSPS,标记配对相干态(HPCS)光源具有更高的单光子比率,在量子密钥分配中具有更好的性能[28]。

在实现一次一密时,密钥和信息具有同样的长度才能保证信息的安全性,因此密钥的生成速率是一个重要的指标。通常情况下增加传输速率就可以使得密钥生成速率增加,但是实际应用中的单光子探测器都具有死时间的特性,即在探测器检测完一个单光子的一段时间中需要恢复到一个状态,在此期间将不能检测另一个进入的光子。探测器的死时间用$\tau$表示,在考虑探测器死时间时,探测器的最大计数率不会超过$1/\tau$。若信号传输速率过大,将会有一部分信号无法被探测器检测到,从而造成较高的误码率[29]。Rogers等[30]研究发现窃听者窃取密钥时,探测器死时间不能提供更高的安全性。Burenkov等[31]将有限探测器死时间的安全性分析扩展到诱骗态BB84协议。本文在考虑有限探测器死时间时,分析了基于HPCS的MDI-QKD协议。本文所开展的研究有利于全面分析MDI-QKD协议的密钥生成速率的影响因素,关于安全密钥生成速率与信号传输速率关系的研究对实际的MDI-QKD协议研究具有一定的意义。

本文在考虑有限探测器死时间时,研究并仿真了基于HPCS光源的MDI-QKD协议的安全密钥生成速率与信号传输速率$\rho$的关系,并将基于HPCS光源的MDI-QKD协议与基于WCS光源的MDI- QKD协议进行了对比。研究结果显示,在相同的传输速率下,基于HPCS光源的MDI-QKD协议的安全密钥生成速率比基于WCS光源的MDI-QKD协议的安全密钥生成速率高。进一步研究了有限探测器死时间$\tau$分别取50,100,150 ns时安全密钥生成速率与传输速率的关系。仿真结果表明:有限探测器死时间越小,安全密钥生成速率的极限值越大,而且在相同信号速率下安全密钥生成速率也越大。

## 2 基本原理

### 2.1 HPCS光源及其性质

配对相干态(PCS)[32]能同时产生信号模式(S)和空闲模式(T),这两种模式的特性完全相同。每个模式的光子数分布服从sub-Poisson分布,即

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

式中:$P_n(\mu)$为光脉冲强度为$\mu$时光子数为$n$的概率;$\mu$为光脉冲强度;$n$为光子数;$\eta_{\mathrm{d}}^{(\mathrm{H})}$为触发探测器的探测效率;$P_{\mathrm{d}}^{(\mathrm{H})}$为暗计数率;H为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,$\mathrm{I}_0(s)\approx1+\frac{s^2}{4}$,考虑量子密钥分配中

信号光源的情况，则 $0 \leqslant s < 1$。

在 HPCS 光源中，Alice(Bob)将 PCS 光源中的 S 模式发送给 Charlie，T 模式则被 Alice(Bob)端的 a(b)探测器探测，可以标记 S 模式到达第三方的时间。HPCS 光源的光子数分布和 PCS 光源的光子数分布一样。当光强相同时，WCS 光源和 HPCS 光源的光子数分布如表 1 所示[33]。

### 2.2　基于 HPCS 光源的 MDI-QKD 协议

图 1 为 MDI-QKD 协议的模型图，HPCS 光源是信号源。Alice、Bob 和 Charlie 是通信的三方。Alice 和 Bob 是信号的发送方，Charlie 是信号的接收方。1H、2H、1V、2V 是 Charlie 端的四个单光子探测器，BS 是分束器，PBS 是偏振分束器，IM 是强度调制器，Pol-M 是偏振调制器。

表 1　WCS 光源和 HPCS 光源的光子数分布[33]

Table 1　Photon number distributions of WCS and HPCS photon sources[33]

| Source | Single photon | Multi photon | Vacuum event |
|---|---|---|---|
| WCS | 0.3033 | 0.0902 | 0.6065 |
| HPCS | 0.9255 | 0.0744 | $4.93\times10^{-6}$ |

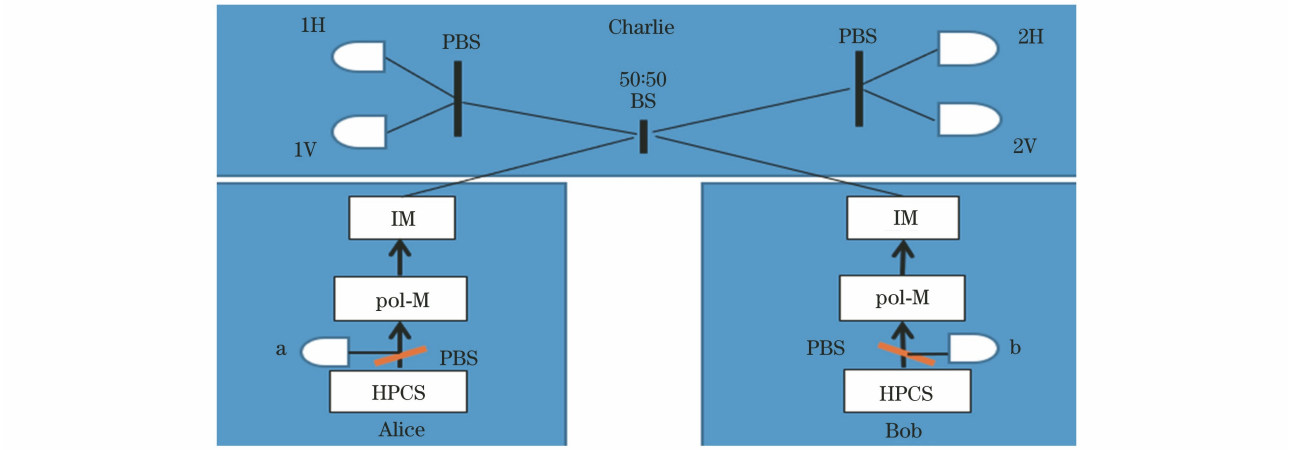


图 1　基于 HPCS 光源的 MDI-QKD 协议的系统模型

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

基于 HPCS 光源的 MDI-QKD 协议流程如下。

1) Alice 和 Bob 发送 HPCS 纠缠光子对，T 模式光子被触发探测器 a(b)探测，可标记信号模式的光子数和到达时间。S 模式作为信号模式经过编码被发送给 Charlie。

2) 利用 Pol-M 选取 $X$ 基或 $Z$ 基对 S 模式光子进行编码，然后利用 IM 将其调制成三种光强：

$$\begin{cases}\{\mu_i\}, i=0,1,2\\ \{\nu_j\}, j=0,1,2\end{cases}, \tag{2}$$

式中：$\mu_i$ 为调制后 Alice 端的光强；$\nu_j$ 为调制后 Bob 端的光强；下标 $i(j)=0,1,2$ 用来标注光强，与真空态、诱骗态和信号态相对应，且 $\mu_2>\mu_1>\mu_0=0$，$\nu_2>\nu_1>\nu_0=0$。

3) Charlie 对接收到的信号进行 Bell 态测量(BSM)[26]，Charlie 接收完所有的信号并完成 BSM 后公布测量结果。Alice 或 Bob 根据 Charlie 公布的测量结果，把对应于测量成功事件的编码进行比特翻转，进而筛选出原始密钥。

4) Alice 和 Bob 对原始密钥进行纠错和保密加强等处理，得到安全密钥。

## 3　密钥生成率分析

信号发送方 Alice 和 Bob 分别发送脉冲强度为 $x$ 和 $y$ 时，估计总增益($Q_{x,y}^{(W)}$)和误码率($E_{x,y}^{(W)}Q_{x,y}^{(W)}$)的计算公式分别为

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

$$E_{x,y}^{(W)}Q_{x,y}^{(W)}=\sum_{n,m=0}^{\infty}P_n(x)P_m(y)e_{n,m}^{(W)}Y_{n,m}^{(W)}, \tag{4}$$

式中：$P_n(x)$为 Alice 端光脉冲强度为 $x$、光子数为 $n$ 时的概率；$P_m(y)$为 Bob 端光脉冲强度为 $y$、光子数为 $m$ 时的概率；$W$ 可以是 $X$ 或 $Z$，表示编码选用的是 $X$ 基或 $Z$ 基；$Y_{n,m}^{(W)}$ 为 Alice 端的脉冲光子数为 $n$，Bob 端的脉冲光子数为 $m$ 时成功进行 BSM 的概率；$e_{n,m}^{(W)}$ 为相应的误码率；$Q_{x,y}^{(W)}$ 和 $E_{x,y}^{(W)}Q_{x,y}^{(W)}$ 可以通过文献[34]的方法来估计。利用文献[35]估计单光子增益($Y_{1,1}^{(W)}$)下界和单光子误码率上界($e_{1,1}^{(W)}$)的方法：

$$Y_{1,1}^{(W)} \geqslant Y_{1,1}^{(W),\mathrm{L}} = \frac{P_1(\mu_2)P_2(v_2)(Q_{\mu_1,v_1}^{(W)} - \tilde{Q}_{0,0}) - P_1(\mu_1)P_2(v_1)(Q_{\mu_2,v_2}^{(W)} - \tilde{Q}'_{0,0})}{P_1(\mu_2)P_1(v_1)[P_1(\mu_1)P_2(v_2) - P_1(\mu_2)P_2(v_1)]}, \tag{5}$$

式中：$Y_{1,1}^{(W),\mathrm{L}}$ 为单光子增益下界，L 表示下界；$\tilde{Q}_{0,0} = Q_{\mu_1,0} + Q_{0,\nu_1} - Q_{0,0}$，$\tilde{Q}'_{0,0} = Q_{\mu_2,0} + Q_{0,\nu_2} - Q_{0,0}$，其中 $Q_{\mu_1,0}$，$Q_{\mu_2,0}$，$Q_{0,\nu_1}$，$Q_{0,\nu_2}$，$Q_{0,0}$ 为 Alice 和 Bob 分别发送相应的信号脉冲强度时的总增益。

$$e_{1,1}^{(W)} \leqslant e_{1,1}^{(W),\mathrm{U}} = \frac{E_{\mu_1,v_1}^{(W)}Q_{\mu_1,v_1}^{(W)} - E_{\mu_1,0}^{(W)}Q_{\mu_1,0}^{(W)} - E_{0,v_1}^{(W)}Q_{0,v_1}^{(W)} + E_{0,0}^{(W)}Q_{0,0}^{(W)}}{P_1(\mu)P_1(v)Y_{1,1}^{(W)}}, \tag{6}$$

式中：$e_{1,1}^{(W),\mathrm{U}}$ 为单光子误码率上界，U 表示上界。

结合(1)～(6)式，可以计算密钥生成率 $R$：

$$R \geqslant P_1(\mu_2)P_1(v_2)Y_{1,1}^{(Z)}[1 - H_2(e_{1,1}^{(X)})] - Q_{\mu_2,v_2}^{(Z)} f(E_{\mu_2,v_2}^{(Z)})H(E_{\mu_2,v_2}^{(Z)}), \tag{7}$$

式中：$H_2(\cdot)$ 为二进制香农熵函数；$f(\cdot)$ 为纠错效率函数，根据文献[14]，取 $f=1.16$。

## 4　基于 HPCS 光源的有限探测器死时间的 MDI-QKD 协议

在 MDI-QKD 协议中分析筛选的密钥速率时，一般不考虑有限探测器死时间 $\tau$，此时随着信号速率的增加，筛选的密钥速率也增加。但在实际的 MDI-QKD 协议中，探测器存在死时间 $\tau$，当信号传输速率过高，超过探测器最大计数率 $1/\tau$ 时，在死时间间隔中探测器会同时检测到多个光子，这违反了一些安全假定，会对安全密钥生成速率造成影响。2010 年，Burenkov 等[31]在考虑有限探测器死时间时，研究得到了有限探测(即可以成功筛选密钥)的概率 $N_a$ 为

$$N_a = \frac{1}{1 + (k-1)Q_{\mu_2,\nu_2}}, \tag{8}$$

式中：$k = \rho\tau$；$Q_{\mu_2,\nu_2}$ 为发送端光强是 $\mu_2$，$\nu_2$ 时的总增益。

因此，考虑有限探测器死时间时，密钥生成率为

$$R \geqslant N_a P_1(\mu_2)P_1(v_2)Y_{1,1}^{(Z)}[1 - H_2(e_{1,1}^{(X)})] - Q_{\mu_2,v_2}^{(Z)} f(E_{\mu_2,v_2}^{(Z)})H(E_{\mu_2,v_2}^{(Z)}), \tag{9}$$

安全密钥生成速率为 $R_n = \rho R$。

$X$ 基下的增益($Q_{\mu_i,v_j}^{(X)}$)和误码率($E_{\mu_i,v_j}^{(X)}Q_{\mu_i,v_j}^{(X)}$)的模拟公式为

$$Q_{\mu_i,v_j}^{(X)} = 2y_{i,j}^2[1 + 2y_{i,j}^2 - 4y_{i,j}\mathrm{I}_0(x_{i,j}) + \mathrm{I}_0(2x_{i,j})], \tag{10}$$

$$E_{\mu_i,v_j}^{(X)}Q_{\mu_i,v_j}^{(X)} = e_0 Q_{\mu_i,v_j}^{(X)} - 2(e_0 - e_d)y_{i,j}^2[\mathrm{I}_0(2x_{i,j}) - 1], \tag{11}$$

式中：$e_0$ 为背景噪声产生的误码率；$e_d$ 为光子击中错误探测器的概率；$x_{i,j} = \sqrt{\eta_a\mu_i\eta_b v_j}/2$，其中，$\eta_a$ 为 Alice 端的传输效率，$\eta_b$ 为 Bob 端的传输效率；$y_{i,j} = (1-P_d)\exp(\mu'_{ij}/4)$，$P_d$ 为第三方探测器的暗记数率，平均光子数 $\mu'_{ij} = \eta_a\mu_i + \eta_b v_j$。系统传输效率 $\eta = t\eta_d$，其中信道传输效率 $t = 10^{-\alpha S/10}$，$\eta_d$ 为探测效率，信道损耗 $\alpha = 0.2\ \mathrm{dB}\cdot\mathrm{km}^{-1}$，$S$ 为传输距离。本文所用信道为对称信道，因此可得 $\eta_a = \eta_b = \eta$。

$Z$ 基下的增益($Q_{\mu_i,v_j}^{(Z)}$)和误码率($E_{\mu_i,v_j}^{(Z)}Q_{\mu_i,v_j}^{(Z)}$)模拟公式为

$$Q_{\mu_i,v_j}^{(Z)} = Q_{\mathrm{c}_{ij}} + Q_{\mathrm{e}_{ij}}, \tag{12}$$

$$E_{\mu_i,v_j}^{(Z)}Q_{\mu_i,v_j}^{(Z)} = e_d Q_{\mathrm{c}_{ij}} + (1-e_d)Q_{\mathrm{e}_{ij}}, \tag{13}$$

式中：$Q_{\mathrm{e}_{ij}}$ 为光子两侧射出时的探测概率；$Q_{\mathrm{c}_{ij}}$ 为光子同侧射出时的探测概率。

$$Q_{\mathrm{c}_{ij}} = 2(1-P_d)^2\exp(-\mu'_{ij}/2)[1-(1-P_d)\exp(-\eta_a\mu_i/2)][1-(1-P_d)\exp(-\eta_b v_j/2)], \tag{14}$$

$$Q_{\mathrm{e}_{ij}} = [2P_d(1-P_d)^2\exp(-\mu'_{ij}/2)][\mathrm{I}_0(2x_{i,j}) - (1-P_d)\exp(-\mu'_{ij}/2)]。 \tag{15}$$

## 5　仿真结果及分析

在考虑有限探测器死时间时，通过数值模拟来仿真基于 HPCS 光源的 MDI-QKD 协议的安全密钥生成速率与信号传输速率即每秒发送的脉冲数的关系。本文考虑脉冲数为无限的情况，且假设信号传输速率较高，探究信号传输速率为 $10^{10}$～$10^{16}$ bit/s 时信号传输速率与安全密钥生成速率的关系。在传输距离 $S=100$ km，有限探测器死时间 $\tau=100$ ns 时，基于 HPCS 光源的 MDI-QKD 协议和基于 WCS 光源的 MDI-QKD 协议的传输速率与安全密钥生成速率的关系如图 2 所示。为了进一步探究有限探测器死时间对基于 HPCS 光源的 MDI-QKD 协议的影响，仿真了有限探测器死时间 $\tau$ 分别取 50，100，150 ns，传输距离 $S=100$ km 时安全密钥生成速率与传输速率的关系，如图 3 所示。信号

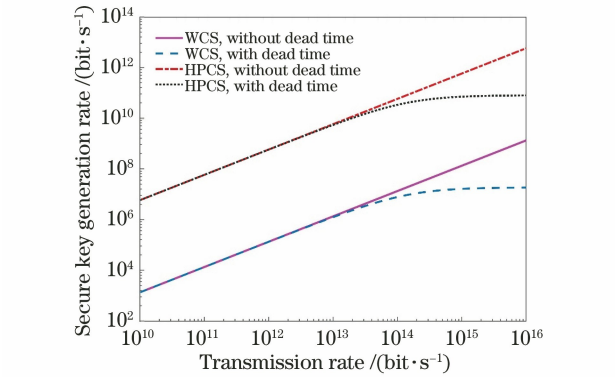


图 2　传输速率与安全密钥生成速率的关系

Fig. 2　Relationship between transmission rate and secure key generation rate

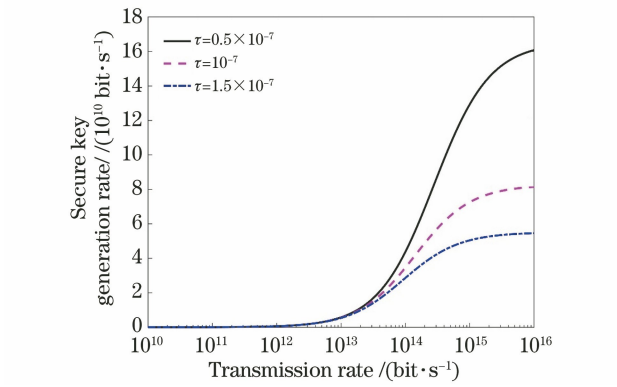


图 3 不同探测器死时间下安全密钥生成速率与传输速率的关系

Fig. 3　Relationship between secure key generation rate and transmission rate under each detector′s dead time

发送端(Alice 和 Bob)的探测器效率 $\eta_{\mathrm{d}}^{(H)}$ 和暗记数率 $P_{\mathrm{d}}^{(H)}$ 分别取：$\eta_{\mathrm{d}}^{(H)}=0.9$，$P_{\mathrm{d}}^{(H)}=10^{-6}$。其他参数如表 2 所示。

表 2　主要仿真参数

Table 2　Main simulation parameters

| Parameter | $P_{\mathrm{d}}$ | $e_0$ | $\eta_{\mathrm{d}}$ |
|---|---|---|---|
| Value | $3.6\times10^{-6}$ | 0.5 | 0.145 |

由图 2 可以看出，当信号传输速率相同且考虑有限探测器死时间时，基于 HPCS 光源的 MDI-QKD 协议的安全密钥生成速率比基于 WCS 光源的 MDI-QKD 协议的安全密钥生成速率高。相同探测器死时间下基于 HPCS 光源的协议和基于 WCS 光源的协议的安全密钥生成速率如表 3 所示。HPCS 光源比 WCS 光源具有更高的单光子比率，从而在 MDI-QKD 过程中增益较高以及误码率较低，因此具有较高的安全密钥生成速率。从安全密钥生成速率的极限来看，基于 HPCS 光源的 MDI-QKD 协议的安全密钥生成速率的极限值为 $8.1\times10^{10}$ bit·s$^{-1}$，基于 WCS 光源的 MDI-QKD 协议的安全密钥生成速率的极限值为 $1.8\times10^{7}$ bit·s$^{-1}$，显然前者高于后者。

表 3　相同探测器死时间时 HPCS 光源和 WCS 光源在不同信号传输速率下的安全密钥生成速率

Table 3　Secure key generation rates of HPCS and WCS sources at different signal transmission rates but same detector′s dead time　　unit：bit·s$^{-1}$

| Source | $\rho=10^{12}$ bit·s$^{-1}$ | $\rho=10^{14}$ bit·s$^{-1}$ | $\rho=10^{15}$ bit·s$^{-1}$ |
|---|---|---|---|
| WCS | $1.3\times10^{5}$ | $7.7\times10^{6}$ | $1.6\times10^{7}$ |
| HPCS | $5.7\times10^{8}$ | $3.4\times10^{10}$ | $7.2\times10^{10}$ |

当传输速率 $1/\tau$ 为 $10^{7}$ bit·s$^{-1}$ 时，安全密钥生成速率仍随传输速率的增加而正比例增长，这是因为信号在传输到第三方进行测量的过程中存在损耗，每秒到达第三方的信号比特数还未超出探测器的最大计数率。当到达第三方探测器的信号速率大于 $1/\tau$ 时，探测器死时间对光子的检测产生影响，安全密钥生成速率降低，不再随传输速率的增加而线性增长。同时可以看出，当基于 HPCS 光源的 MDI-QKD 协议的安全密钥生成速率曲线和基于 WCS 光源的 MDI-QKD 协议的安全密钥生成速率曲线发生扭曲时，信号传输速率相同。这是因为在同一个系统模型中，若传输损耗相同，则信号到达第三方的实际传输速率也相同。

由图 3 可以看出，在传输速率超过 $10^{13}$ bit·s$^{-1}$ 以后，当传输速率相同时，探测器死时间越小，安全密钥生成速率越大，如表 4 所示。这是因为探测死时间越小，则探测器的最大计数率就越大，故单位时间内就可以成功探测更多的光子信号。当有限探测器死时间 $\tau=50$ ns 时，安全密钥生成速率的极限值为 $1.62\times10^{11}$ bit·s$^{-1}$；当有限探测器死时间 $\tau=100$ ns 时，安全密钥生成速率的极限值为 $8.1\times10^{10}$ bit·s$^{-1}$；当有限探测器死时间 $\tau=150$ ns 时，安全密钥生成速率的极限值为 $5.8\times10^{10}$ bit·s$^{-1}$。可以看出，随着探测器死时间的增大，安全密钥生成速率的极限值减小。传输距离 $S=100$ km 时，通过仿真结果可知，基于 HPCS 光源的 MDI-QKD 协议的安全密钥生成速率与有限探测器死时间 $\tau$ 的关系接近 $8.1\times10^{3}/\tau$。

表 4　不同探测器死时间和信号传输速率下 HPCS 光源的安全密钥生成速率

Table 4　Secure key generation rates of HPCS sources under different detector′s dead time and signal transmission rates　unit: bit·s$^{-1}$

| Detector′s dead time | $\rho=10^{14}$ bit·s$^{-1}$ | $\rho=10^{15}$ bit·s$^{-1}$ |
|---|---|---|
| $\tau=50$ ns | $4.2\times10^{10}$ | $12.8\times10^{10}$ |
| $\tau=100$ ns | $3.4\times10^{10}$ | $7.2\times10^{10}$ |
| $\tau=150$ ns | $2.8\times10^{10}$ | $5.0\times10^{10}$ |

## 6　结　论

在考虑有限探测器死时间时，分析了基于 HPCS 光源的 MDI-QKD 协议的安全密钥生成速率与传输速率的关系。由仿真结果可知，当传输距离 $S=100$ km 且有限探测器死时间相同时，基于 HPCS 光源的 MDI-QKD 协议与基于 WCS 光源的 MDI-QKD 协议相比，在传输速率相同的情况下，前者的安全密钥生成速率高于后者的安全密钥生成速率，并且前者的安全密钥生成速率的极限比后者的安全密钥生成速率的极限大。当有限探测器死时间 $\tau$ 分别取 50，100，150 ns 时，仿真了基于 HPCS 光源的 MDI-QKD 协议的安全密钥生成速率。从仿真结果可知，有限探测器死时间越小，安全密钥生成速率的极限越大。

## 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 K, 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, 2004: 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. Heidelberg: Springer, 1985, 196: 475-480

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

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

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

[7] 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.

[8] 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.

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

[10] 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.

[11] 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.

[12] Zhao Y, Fung C 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.

[13] Makarov V, Skaar J. Faked states attack using detector efficiency mismatch on SARG04, phase-time, DPSK, and Ekert protocols [J]. Quantum Information & Computation, 2008, 8(6): 622-635.

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

[15] 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.

[16] 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.

[17] 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.

[18] Kang G D, Zhou Q P, Fang M F. Measurement-device-independent quantum key distribution with uncharacterized coherent sources [J]. Quantum Information Processing, 2019, 19(1): 1-18.

[19] 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.

[20] Abruzzo S, Kampermann H, Bruß D. Measurement-device-independent quantum key distribution with quantum memories[J]. Physical Review A, 2014, 89(1): 012301.

[21] Chen D, Zhao S H, Shi L, et al. Measurement-device-independent quantum key distribution with pairs of vector vortex beams[J]. Physical Review A, 2016, 93(3): 032320.

[22] 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.

[23] Wang X Y, Zhao S H, Dong C, et al. Orbital angular momentum-encoded measurement device independent quantum key distribution under atmospheric turbulence [J]. Quantum Information Processing, 2019, 18(10): 304.

[24] Zhou N R, Zhu K N, Zou X F. Multi-party semi-quantum key distribution protocol with four-particle cluster states [J]. Annalen Der Physik, 2019, 531(8): 1800520.

[25] 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.

[26] 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.

[27] 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.

[28] 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.

[29] Dixon A R, Yuan Z L, Dynes J F, et al. Continuous operation of high bit rate quantum key distribution [J]. Applied Physics Letters, 2010, 96(16): 161102.

[30] Rogers D, Bienfang J C, Nakassis A, et al. Detector dead-time effects and paralyzability in high-speed quantum key distribution [J]. New Journal of Physics, 2007, 9: 319.

[31] Burenkov V, Qi B, Fortescue B, et al. Security of high speed quantum key distribution with finite detector dead time [J]. Quantum Information & Computation, 2014, 14(3/4): 217-235.

[32] 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.

[33] 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.

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

[35] He Y F, Zhao Y K, Guo J R, et al. Statistical fluctuation analysis of quantum key distribution protocols based on heralded pair coherent state [J]. Acta Optica Sinica, 2020, 40(7): 0727002.
何业锋, 赵艳坤, 郭佳瑞, 等. 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[J]. 光学学报, 2020, 40(7): 0727002.