第 41 卷 第 2 期/2021 年 1 月/光学学报 研究论文

光学学报

基于预报单光子源的相位匹配被动诱骗态量子密钥分配

虞味，周媛媛*

海军工程大学电子工程学院，湖北 武汉 430033

摘要 基于预报单光子源，提出了一种相位匹配被动诱骗态量子密钥分配方案。在此方案中，通信双方仅需各产生单个强度的信号。根据通信双方本地探测器的响应情况，第三方的探测结果被分为四个集合，既起到信号态和诱骗态的作用，又共同参与参数估计和密钥生成，降低了系统实现的难度并改善了方案性能。仿真结果表明：相位匹配被动诱骗态方案的最大安全传输距离可达到 552 km，性能趋近于现有的相位匹配主动诱骗态方案，且无需主动产生诱骗态；在一定程度上克服了相位匹配主动诱骗态方案严重依赖探测器探测效率的缺陷，性能更为稳定；随着数据长度的下降，方案的传输性能有所下降，但数据长度即使下降至 10^7，方案的最大安全传输距离依然可以达到 507 km。

关键词 量子光学；量子密钥分配；预报单光子源；相位匹配协议；被动诱骗态

中图分类号 O431.2 **文献标志码** A **doi**：10.3788/AOS202141.0227001

Phase-Matched Passive-Decoy-State Quantum Key Distribution Based on Heralded Single Photon Source

Yu Wei, Zhou Yuanyuan*

College of Electronic Engineering, Naval University of Engineering, Wuhan, Hubei 430033, *China*

Abstract A scheme for phase-matched passive-decoy-state quantum key distribution is proposed based on the heralded single photon source. In the scheme, both communication parties only need to generate one-intensity signals. The detection results of the third party are divided into four sets according to the response of the local detectors of both communication parties. These four sets not only serve as the signal state and the decoy state, but also jointly participate in parameter estimation and key generation. Thus, the difficulty of system implementation is reduced and the performance of the scheme is improved. The simulation results show that the maximum safe transmission distance of the phase-matched passive-decoy-state scheme can reach 552 km, and the performance is close to those of the existing phase-matched active-decoy-state schemes. Moreover, there is no need to generate decoy states actively. To some extent, this scheme overcomes the drawback that the phase-matched active-decoy-state scheme relies on the detection efficiency heavily and makes the performance more stable. As the data length decreases, the transmission performance of the scheme is declined. Even if the data length drops to 10^7, the maximum safe transmission distance of the scheme can still reach 507 km.

Key words quantum optics; quantum key distribution; heralded single photon source; phase-matching protocol; passive decoy state

OCIS codes 270.5565; 270.5568

收稿日期：2020-07-08；**修回日期**：2020-07-30；**录用日期**：2020-08-31

基金项目：湖北省自然科学基金(2019CFC900)

* **E-mail**：zyy_hjgc@aliyun.com

1 引 言

量子密钥分配(Quantum Key Distribution, QKD)[1]以量子力学为基础,具有经典保密通信无法企及的无条件安全性[2],为军事、金融等各类保密信息融入互联网提供了可能。但这一目标的实现受现有技术水平的限制,面临着实际应用需求等各方面的挑战,其中设计密钥生成效率更高、安全传输距离更远和实现更为简单的 QKD 方案是学者们一直关注的焦点。

在探索远距离、安全和实用的 QKD 的征程上,各种 QKD 协议被不断提出:1984 年第一个 QKD 协议——BB84 协议[1]被提出;2003 年,Hwang[3]提出了诱骗态思想,为抵制非理想光源带来的光子数分离(Photon Number Splitting, PNS)[4]攻击的威胁指明了思路;2012 年,测量设备无关(Measurement Device Independent, MDI)[5]协议的提出,克服了现实条件下测量器件的不完美性带来的安全隐患;2018 年,双场(Twin Field, TF)[6-8]协议以及 TF 协议的改进变式——相位匹配(Phase-Matching, PM)[9-10]协议的提出,突破了传统无中继量子密钥分配方案所限定的密钥容量界限[11]。

针对理想单光子源的缺失,将 QKD 协议与诱骗态思想相结合是实际 QKD 系统采用的经典方案。诱骗态和信号态在物理本质上没有任何区别,只是强度不同而已。诱骗态方法的核心思想是窃听方 Eve 不能区分合法通信双方 Alice(Bob)随机发送的诱骗态和信号态,因此 Eve 进行 PNS 攻击时对诱骗态和信号态一视同仁。但是,由于诱骗态和信号态的强度不一样,因此 Eve 进行 PNS 攻击时对诱骗态和信号态造成的影响是不一样的,这样 Alice 和 Bob 就可以“逮住”Eve。诱骗态的数目越多,QKD 方案的性能就越优越,但实际 QKD 系统的实现难度也越大。如果在诱骗态方案中,Alice(Bob)需要主动制备诱骗态,则把这种方案称之为主动诱骗态(Active Decoy State, ADS)方案[12-14]。如果 Alice(Bob)不需要主动制备诱骗态,信号态和诱骗态是系统根据 Alice(Bob)端探测器的检测结果,通过被动选择的方式来产生的,则这类方案称之为被动诱骗态(Passive Decoy State, PDS)方案[15]。最典型的是 Adachi 等[16]提出的基于门限探测器的 BB84 被动诱骗态方案(AYKI),该方案只需产生单个强度的信号,无需对基于标准 BB84 的 QKD 系统的原有硬件作任何改动,实现起来非常容易。也有很多研究者尝试把主动诱骗态和被动诱骗态结合起来[17-19],寻求性能提升和实现简单之间的平衡。

目前,关于 PM 协议的研究主要集中在理想条件下的性能界限讨论。为了进一步探寻高效简单的 PM 诱骗态方案,本文基于实际常用的预报单光子源(Heralded Single Photon Source, HSPS)[20-22],提出了一种 PM 被动诱骗态量子密钥分配方案,对方案的传输性能进行了仿真分析,并在数据长度有限的实际条件下,研究其传输性能的变化。

2 基于 HSPS 的 PM 被动诱骗态方案

2.1 方案描述

预报单光子源是一类双模态光源,其原理是利用未退化参数下转换来产生纠缠光子对,由于这对光子几乎是同时产生的,因此两个模式具有完全相同的特性。在每个模式中,强度为 x 的 HSPS 产生 k-光子态脉冲($k\in[0,+\infty]$)的概率服从热分布[16]:

$$P^x(k)=\frac{x^k}{(1+x)^{k+1}}。\tag{1}$$

如图 1 所示,HSPS 发出的双模态经偏振分束器被分为信号量子态(S 模态,$|k\rangle_S$)和标记量子态(T 模态,$|k\rangle_T$),于是 HSPS 所产生的双模态 $|\psi\rangle_{TS}$ 可以写为

$$|\psi\rangle_{TS}=\sum_{k=0}^{\infty}\left[P^x(k)|k\rangle_T|k\rangle_S\right]。\tag{2}$$

本文基于 HSPS 提出了 PM 被动诱骗态方案,设置信号态强度为 μ。在此方案中,第三方的探测结果根据本地探测器的响应情况可被分为多个集合,既起到信号态和诱骗态的作用,又共同参与参数估计和密钥生成。

具体方案流程如图 1 所示。

1) 假设 Alice 与 Bob 光源产生的强度完全相等,即 $\mu_a=\mu_b=\mu$,其中 μ_a 为 Alice 光源产生的强度,μ_b 为 Bob 光源产生的强度。光脉冲信号经过偏振分束器后,被分为 S 模态和 T 模态。T 模态可用来预报 S 模态的光子数和到达时间,可减小长距离量子密钥分配过程中暗计数的影响。

2) Alice 和 Bob 将 T 模态发送给本地探测器 D_0 和 D_1,根据本地探测器的响应情况,获得四类探测结果:D_0 和 D_1 都不响应,D_0 不响应但 D_1 响应,D_0 响应但 D_1 不响应以及 D_0 和 D_1 都响应。

3) Alice 和 Bob 将 S 模态进行调制编码后发送给第三方 Charlie,Charlie 对接收到的一对光脉冲执行干涉测量,若两个探测器 D_2 和 D_3 有且只有一

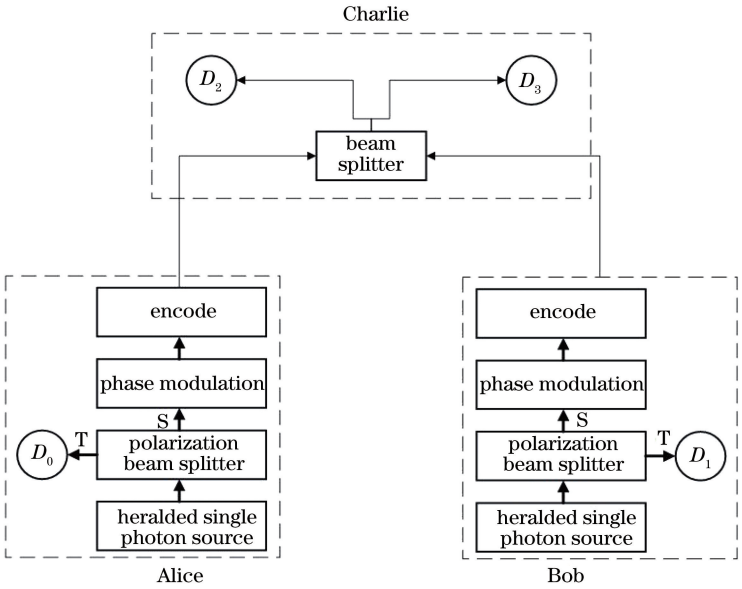

图 1 基于 HSPS 的 PM 被动诱骗态方案的流程图

Fig. 1 Flow chart of PM passive-decoy-state scheme based on HSPS

个响应，则表示探测成功。此外根据 Alice 和 Bob 端本地探测器的探测结果，可以将 Charlie 端探测器的所有探测结果分为四个集合：$\{i=0,j=0\}$、$\{i=0,j=1\}$、$\{i=1,j=0\}$以及$\{i=1,j=1\}$。此处用 i 和 j 分别表示 Alice 和 Bob 端本地探测器的探测结果，$i(j)=0$ 表示本地探测器 $D_0(D_1)$因未探测到光子而没有响应，$i(j)=1$ 表示本地探测器 D_0 (D_1)因检测到光子而发生响应。全局计数率相应可以分为 $Q_{\mu,00}$、$Q_{\mu,01}$、$Q_{\mu,10}$ 以及 $Q_{\mu,11}$，全局误码率可以分为 $E^{Z}_{\mu,00}$、$E^{Z}_{\mu,01}$、$E^{Z}_{\mu,10}$ 以及 $E^{Z}_{\mu,11}$。本文假设 Charlie 端的探测器性能指标与 Alice 和 Bob 端的完全相同。设探测器 D_0、D_1、D_2 和 D_3 探测效率分别为 η_0、η_1、η_2 和 η_3，即 $\eta_0=\eta_1=\eta_2=\eta_3=\eta_d$。

4）利用上述观测数据便可对相关参数进行估计，并进一步得到密钥生成效率。

PM 协议的密钥生成效率的计算公式[9]为

$$R_{PM}=\frac{2}{M}Q_{\mu}\left[-fH(E^{Z}_{\mu})+1-H(E^{X}_{\mu})\right], \quad (3)$$

式中：$H(\cdot)$为二进制信息熵；$2/M$ 为筛选因子；f 为纠错效率；Q_{μ} 为发送光脉冲强度为 μ 时的全局计数率；E^{Z}_{μ} 为误码率；E^{X}_{μ} 为相位误差。Q_{μ} 和 E^{Z}_{μ} 可在实验中观测得到。

$$E^{X}_{\mu}\leqslant q_0 e^{Z}_{0}+\sum_{k=0}^{\infty}(e^{Z}_{2k+1}q_{2k+1})+(1-q_0-q_{odd}), \quad (4)$$

式中：e^{Z}_{k} 为 k-光子态误码率；Y_k 为 k-光子态计数率；odd 表示奇数；q_k 为强度为 μ 的光源发送 k-光子态的概率与全局计数率的比值，计算公式为

$$q_k=\frac{P^{\mu}(k)Y_k}{Q_{\mu}}=\frac{\mu^k}{(1+\mu)^{k+1}}\times\frac{Y_k}{Q_{\mu}}。 \quad (5)$$

设光源发送 k-光子态脉冲时，探测器 D_0 和 D_1 响应状态的概率为 $\varepsilon_{ij/k}$。则信号强度为 x 的光源的全局计数率计算公式为

$$Q_{x,ij}=\sum_{k=0}^{\infty}Q_{k,ij}=\sum_{k=0}^{\infty}\left[\frac{x^k}{(1+x)^{k+1}}\varepsilon_{ij/k}Y_k\right]。 \quad (6)$$

对应各集合的探测器响应状态的概率分别为

$$\begin{cases}\varepsilon_{00/k}=(1-p_d)^2(1-\eta_d)^{2k}\\ \varepsilon_{01/k}=(1-p_d)(1-\eta_d)^k\left[1-(1-p_d)(1-\eta_d)^k\right]\\ \varepsilon_{10/k}=\left[1-(1-p_d)(1-\eta_d)^k\right](1-p_d)(1-\eta_d)^k\\ \varepsilon_{11/k}=\left[1-(1-p_d)(1-\eta_d)^k\right]^2\end{cases}, \quad (7)$$

式中：p_d 为探测器的暗计数；η_d 为探测器的探测效率。

同理，信号强度为 μ 的光源的全局误码率也可以写为

$$E^{Z}_{\mu,ij}Q_{\mu,ij}=\sum_{k=0}^{\infty}(e^{Z}_{k}Q_{k,ij})=\sum_{k=0}^{\infty}\left[\frac{\mu^k}{(1+\mu)^{k+1}}\varepsilon_{ij/k}Y_k e^{Z}_{k}\right]。 \quad (8)$$

本文所提方案中的各个集合都参与密钥生成，所以方案的最终密钥生成效率可以看成是各个集合对应的密钥生成效率 R_{00}、R_{01}、R_{10} 以及 R_{11} 的总和，即 $R_{sum}=R_{00}+R_{01}+R_{10}+R_{11}$，其中

$$R_{00}\geqslant\frac{2}{M}Q_{\mu,00}\left[-fH(E^{Z}_{\mu,00})+1-H(E^{X}_{\mu})\right], \quad (9)$$

$$R_{01}\geqslant\frac{2}{M}Q_{\mu,01}[-fH(E^{Z}_{\mu,01})+1-H(E^{X}_{\mu})],\tag{10}$$

$$R_{10}\geqslant\frac{2}{M}Q_{\mu,10}[-fH(E^{Z}_{\mu,10})+1-H(E^{X}_{\mu})],\tag{11}$$

$$R_{11}\geqslant\frac{2}{M}Q_{\mu,11}[-fH(E^{Z}_{\mu,11})+1-H(E^{X}_{\mu})]。\tag{12}$$

由于只有在传输距离不是很远时，R_{00}、R_{01} 和 R_{10} 才对密钥生成有积极的贡献，因此为了得到传输全程每处的最佳密钥生成效率，取最终密钥生成效率 $R=\max\{R_{11},R_{\mathrm{sum}}\}$。

为了计算密钥生成效率，接下来我们将对相关 Y_k 和 e^{Z}_{k} 的值进行估计。

2.2 参数估计

随着 k 的增加，k-光子态对密钥生成效率的贡献越来越小[23]。因此，本文仅考虑 $0\leqslant k\leqslant 3$ 的光子态对密钥生成效率的贡献，于是相位误差的计算公式变为

$$E^{X}_{\mu}\leqslant q_0e^{Z}_{0}+(q_1e^{Z}_{1}+q_3e^{Z}_{3})+(1-q_0-q_1-q_3)。\tag{13}$$

方案需要对 0-光子态的计数率上限、单光子态和 3-光子态的计数率下限及误码率上限进行估计。

2.2.1 估计 Y_0 的上限

由(8)式可得

$$E^{Z}_{\mu,00}Q_{\mu,00}=\frac{1}{1+\mu}(1-p_{\mathrm{d}})^{2}Y_0e^{Z}_{0}+\sum_{k=0}^{\infty}\left[\frac{\mu^{k}}{(1+\mu)^{k+1}}\times(1-p_{\mathrm{d}})^{2}(1-\eta_{\mathrm{d}})^{2k}Y_ke^{Z}_{k}\right],\tag{14}$$

于是可以求得 Y_0 的上限 Y^{U}_{0} 为

$$Y_0\leqslant Y^{U}_{0}=\frac{(1+\mu)E^{Z}_{\mu,00}Q_{\mu,00}}{e^{Z}_{0}(1-p_{\mathrm{d}})^{2}}。\tag{15}$$

2.2.2 估计 Y_1 和 Y_3 的下限

现利用 $Q_{\mu,00}$、$Q_{\mu,01}$、$Q_{\mu,10}$ 和 $Q_{\mu,11}$ 来估计 Y_1 和 Y_3 的下限，可得

$$[(1+\mu)Q_{\mu,00}-Y_0](2\eta_{\mathrm{d}}-\eta^{2}_{\mathrm{d}})-[(1+\mu)Q_{\mu,01}-p_{\mathrm{d}}Y_0](1-\eta_{\mathrm{d}})^{2}=\frac{\mu}{1+\mu}Y_1(1-\eta_{\mathrm{d}})^{2}\eta_{\mathrm{d}}+\frac{\mu^{3}}{(1+\mu)^{3}}Y_1(1-\eta_{\mathrm{d}})^{5}(-\eta_{\mathrm{d}})+\sum_{k=4}^{\infty}\left\{\frac{\mu^{k}}{(1+\mu)^{k+1}}Y_k[(1-\eta_{\mathrm{d}})^{2k}-(1-\eta_{\mathrm{d}})^{2}]\right\}。\tag{16}$$

当 $k\geqslant 4$ 时，由于探测器效率 $0\leqslant\eta_{\mathrm{d}}\leqslant 1$，容易得到

$$[(1-\eta_{\mathrm{d}})^{2k}-(1-\eta_{\mathrm{d}})^{2}]\leqslant 0。\tag{17}$$

结合(15)式，得到单光子态的计数率 Y_1 的下限为

$$Y_1\geqslant Y^{L}_{1}=[(1+\mu)Q_{\mu,00}-Y^{U}_{0}]\times\frac{1+\mu}{\mu}\times\frac{1-(1-\eta_{\mathrm{d}})^{3}}{(1-\eta_{\mathrm{d}})^{2}\eta_{\mathrm{d}}}-[(1+\mu)Q_{\mu,01}-p_{\mathrm{d}}Y^{U}_{0}]\times\frac{1+\mu}{\mu}\times\frac{1-(1-\eta_{\mathrm{d}})^{3}}{\eta_{\mathrm{d}}(2\eta_{\mathrm{d}}-\eta^{2}_{\mathrm{d}})}-[(1+\mu)Q_{\mu,10}-p_{\mathrm{d}}Y^{U}_{0}]\times\frac{1+\mu}{\mu}\times\frac{1-\eta_{\mathrm{d}}}{\eta_{\mathrm{d}}}+[(1+\mu)Q_{\mu,11}-Y^{U}_{0}]\times\frac{1+\mu}{\mu}\times\frac{(1-\eta_{\mathrm{d}})^{3}}{\eta_{\mathrm{d}}(2\eta_{\mathrm{d}}-\eta^{2}_{\mathrm{d}})}。\tag{18}$$

同理，可得 Y_3 的下限为

$$Y_3\geqslant Y^{L}_{3}=[(1+\mu)Q_{\mu,00}-Y^{U}_{0}]\times\frac{(1+\mu)^{3}}{\mu^{3}}\times\frac{1}{(1-\eta_{\mathrm{d}})^{3}}-[(1+\mu)Q_{\mu,01}-p_{\mathrm{d}}Y^{U}_{0}]\times\frac{(1+\mu)^{3}}{\mu^{3}}\times\frac{1}{(1-\eta_{\mathrm{d}})(2\eta_{\mathrm{d}}-\eta^{2}_{\mathrm{d}})}-[(1+\mu)Q_{\mu,10}-p_{\mathrm{d}}Y^{U}_{0}]\times\frac{(1+\mu)^{3}}{\mu^{3}}\times\frac{1}{(1-\eta_{\mathrm{d}})^{2}\eta_{\mathrm{d}}}+[(1+\mu)Q_{\mu,11}-Y^{U}_{0}]\times\frac{(1+\mu)^{3}}{\mu^{3}}\times\frac{1}{\eta_{\mathrm{d}}(2\eta_{\mathrm{d}}-\eta^{2}_{\mathrm{d}})}。\tag{19}$$

2.2.3 估计 e^{Z}_{1} 和 e^{Z}_{3} 的上限

同样，利用 $E^{Z}_{\mu,00}$、$E^{Z}_{\mu,01}$、$E^{Z}_{\mu,10}$ 和 $E^{Z}_{\mu,11}$，可估计 e^{Z}_{1} 和 e^{Z}_{3} 的上限为

$$e_1^{\mathrm{Z}} \leqslant e_1^{\mathrm{ZU}} = \frac{1}{Y_1} \times \left\{ [(1+\mu)E_{\mu,00}^{\mathrm{Z}} Q_{\mu,00} - Y_0^{\mathrm{U}} e_0^{\mathrm{Z}}] \times \frac{1+\mu}{\mu} \times \frac{1-(1-\eta_{\mathrm{d}})^3}{(1-\eta_{\mathrm{d}})^2 \eta_{\mathrm{d}}} - [(1+\mu)E_{\mu,01}^{\mathrm{Z}} Q_{\mu,01} - p_{\mathrm{d}} Y_0^{\mathrm{U}} e_0^{\mathrm{Z}}] \times \frac{1+\mu}{\mu} \times \frac{1-(1-\eta_{\mathrm{d}})^3}{\eta_{\mathrm{d}}(2\eta_{\mathrm{d}} - \eta_{\mathrm{d}}^2)} - [(1+\mu)E_{\mu,10}^{\mathrm{Z}} Q_{\mu,10} - p_{\mathrm{d}} Y_0^{\mathrm{U}} e_0^{\mathrm{Z}}] \times \frac{1+\mu}{\mu} \times \frac{1-\eta_{\mathrm{d}}}{\eta_{\mathrm{d}}} + [(1+\mu)E_{\mu,11}^{\mathrm{Z}} Q_{\mu,11} - Y_0^{\mathrm{U}} e_0^{\mathrm{Z}}] \times \frac{1+\mu}{\mu} \times \frac{(1-\eta_{\mathrm{d}})^3}{\eta_{\mathrm{d}}(2\eta_{\mathrm{d}} - \eta_{\mathrm{d}}^2)} \right\}, \tag{20}$$

$$e_3^{\mathrm{Z}} \leqslant e_3^{\mathrm{ZU}} = \frac{1}{Y_3} \times \left\{ [(1+\mu)E_{\mu,00}^{\mathrm{Z}} Q_{\mu,00} - Y_0^{\mathrm{U}} e_0^{\mathrm{Z}}] \times \frac{(1+\mu)^3}{\mu^3} \times \frac{1}{(1-\eta_{\mathrm{d}})^3} - [(1+\mu)E_{\mu,01}^{\mathrm{Z}} Q_{\mu,01} - p_{\mathrm{d}} Y_0^{\mathrm{U}} e_0^{\mathrm{Z}}] \times \frac{(1+\mu)^3}{\mu^3} \times \frac{1}{(1-\eta_{\mathrm{d}})(2\eta_{\mathrm{d}} - \eta_{\mathrm{d}}^2)} - [(1+\mu)E_{\mu,10}^{\mathrm{Z}} Q_{\mu,10} - p_{\mathrm{d}} Y_0^{\mathrm{U}} e_0^{\mathrm{Z}}] \times \frac{(1+\mu)^3}{\mu^3} \times \frac{1}{(1-\eta_{\mathrm{d}})^2 \eta_{\mathrm{d}}} + [(1+\mu)E_{\mu,11}^{\mathrm{Z}} Q_{\mu,11} - Y_0^{\mathrm{U}} e_0^{\mathrm{Z}}] \times \frac{(1+\mu)^3}{\mu^3} \times \frac{1}{\eta_{\mathrm{d}}(2\eta_{\mathrm{d}} - \eta_{\mathrm{d}}^2)} \right\}。 \tag{21}$$

将(18)～(21)式代入(9)～(12)式，便可计算方案的密钥生成效率。

2.3 基于切诺夫界的数据有限长分析

实际 QKD 系统在一定时间内处理的数据长度是有限的，这将导致数据的统计涨落问题，从而降低密钥生成效率和安全传输距离。下面利用基于切诺夫界[24]的统计分析方法对本文方案进行分析。

定理 1(切诺夫界)：若 $X_1, X_2, \cdots, X_t, \cdots, X_n'$ 是服从伯努利分布 $\Pr(X_t=1)$ 且独立同分布的随机变量，编号 $t=1,2,\cdots,n'$，n' 为随机变量个数，令 $c=\sum_{t=1} E[X_t]$，那么 $\forall \delta>0$，有

$$\Pr\left\{\sum_{t=1} X_t \geqslant (1+\delta)c\right\} \leqslant \left[\frac{\exp(\delta)}{(1+\delta)^{1+\delta}}\right]^c < \exp\left(-c \cdot \frac{\delta^2}{2}\right), \tag{22}$$

$$\Pr\left\{\sum_{t=1} X_t \leqslant (1-\delta)c\right\} \leqslant \left[\frac{\exp(-\delta)}{(1-\delta)^{1-\delta}}\right]^c < \exp\left(-c \cdot \frac{\delta^2}{2}\right), \tag{23}$$

式中：δ 为随机变量的偏差量。

由定理 1 计算 X 的偏差为 $\varepsilon_X = \sqrt{\frac{2(\ln 2 - \ln\theta)}{nX}}$，其中 n 为数据长度，置信度为 $1-\theta$。

根据(16)式可知，为了估计单光子脉冲计数率 Y_1 的下限，需要得到 $Q_{\mu,00}$ 和 $Q_{\mu,11}$ 的下限以及 $Q_{\mu,01}$ 和 $Q_{\mu,10}$ 的上限。

$$\begin{cases} Q_{\mu,00}^{\mathrm{L}} = Q_{\mu,00}(1-\varepsilon_{Q_{\mu,00}}) \\ \varepsilon_{Q_{\mu,00}} = \sqrt{\dfrac{2(\ln 2 - \ln\theta)}{n_{\mu,00} Q_{\mu,00}}} \end{cases}, \tag{24}$$

$$\begin{cases} Q_{\mu,01}^{\mathrm{U}} = Q_{\mu,01}(1+\varepsilon_{Q_{\mu,01}}) \\ \varepsilon_{Q_{\mu,01}} = \sqrt{\dfrac{2(\ln 2 - \ln\theta)}{n_{\mu,01} Q_{\mu,01}}} \end{cases}, \tag{25}$$

$$\begin{cases} Q_{\mu,10}^{\mathrm{U}} = Q_{\mu,10}(1-\varepsilon_{Q_{\mu,10}}) \\ \varepsilon_{Q_{\mu,10}} = \sqrt{\dfrac{2(\ln 2 - \ln\theta)}{n_{\mu,10} Q_{\mu,10}}} \end{cases}, \tag{26}$$

$$\begin{cases} Q_{\mu,11}^{\mathrm{L}} = Q_{\mu,11}(1-\varepsilon_{Q_{\mu,11}}) \\ \varepsilon_{Q_{\mu,11}} = \sqrt{\dfrac{2(\ln 2 - \ln\theta)}{n_{\mu,11} Q_{\mu,11}}} \end{cases}, \tag{27}$$

式中：$Q_{\mu,00}^{\mathrm{L}}$ 为 $Q_{\mu,00}$ 的下限；$Q_{\mu,01}^{\mathrm{U}}$ 为 $Q_{\mu,01}$ 的上限；$Q_{\mu,10}^{\mathrm{U}}$ 为 $Q_{\mu,10}$ 的上限；$Q_{\mu,11}^{\mathrm{L}}$ 为 $Q_{\mu,11}$ 的下限；$\varepsilon_{Q_{\mu,00}}$ 为 $Q_{\mu,00}$ 的偏差量；$\varepsilon_{Q_{\mu,01}}$ 为 $Q_{\mu,01}$ 的偏差量；$\varepsilon_{Q_{\mu,10}}$ 为 $Q_{\mu,10}$ 的偏差量；$\varepsilon_{Q_{\mu,11}}$ 为 $Q_{\mu,11}$ 的偏差量；$n_{\mu,00}$ 为 $\{i=0,j=0\}$ 的数据长度；$n_{\mu,01}$ 为 $\{i=0,j=1\}$ 的数据长度；$n_{\mu,10}$ 为 $\{i=1,j=0\}$ 的数据长度；$n_{\mu,11}$ 为 $\{i=1,j=1\}$ 的数据长度。

同理，也可以重新估计 Y_3、e_1 以及 e_3 的边界值，从而得到在数据有限长条件下的密钥生成效率的下界值。

3 数值仿真与分析

本文仿真采用的参数主要来自文献[9]，其中传输损耗 α 选取了波长为 1550 nm 的光在光纤传输中的损耗典型值 0.21 dB·km^{-1}，暗计数 p_{d} 为 8×10^{-8}，纠错效率 f 为 1.15，探测器探测效率 η_{d} 为 14.5%，相位片数量为 16，系统失调误差 e_{d} 为 1.5%。仿真中信号态 μ 根据传输距离选取了最优信号强度。

图 2 仿真的是 BB84 协议、MDI 协议和 PM 协议在主动无穷诱骗态条件(等效于系统采用理想单光子源)下的密钥生成效率随安全传输距离的变化曲线。可以看出，BB84 协议、MDI 协议和 PM 协议的密钥生成效率随传输距离的增加而衰减，衰减的程度由剧烈变为缓慢。这是由于 BB84 协议与 MDI

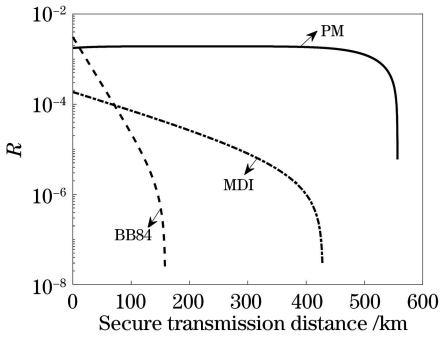

图 2 在主动无穷诱骗态条件下不同协议的密钥生成效率随安全传输距离的变化

Fig. 2 Key generation rate versus secure transmission distance for each protocol under active infinite decoy state

协议的密钥生成效率受到密钥容量界限的限制，而 PM 协议的密钥生成效率突破了密钥容量的界限；在无穷诱骗态条件下，BB84、MDI 和 PM 协议的最大安全传输距离分别达到 158，428，556 km，可见 PM 协议的性能最优。

图 3 是基于弱相干态光源（Weak Coherent Source，WCS）的 PM 主动三诱骗态方案、基于 HSPS的PM主动三诱骗态方案以及本文提出的基于 HSPS 的 PM 被动诱骗态方案的密钥生成效率随安全传输距离的变化曲线。

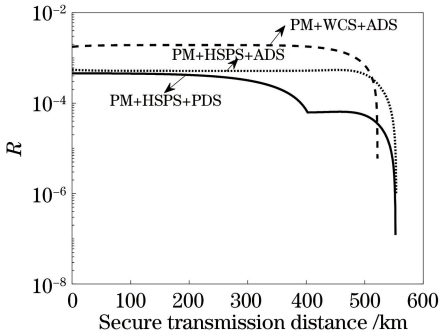

图 3 不同方案的密钥生成效率随安全传输距离变化的曲线

Fig. 3 Key generation rate versus secure transmission distance for each scheme

仿真结果显示：基于 WCS 的 QKD 方案的密钥生成效率较基于 HSPS 的 QKD 方案大，但是在安全传输距离上，前者可以达到 521 km，后者可以达到 552 km。这是由于相较于 HSPS，WCS 光子数分布中的多光子脉冲的比例小，基于 WCS 的 QKD 方案的密钥生成效率较高，但是 HSPS 的双模态可以降低系统暗计数的影响，从而延长安全传输距离。

在基于 HSPS 的被动诱骗态 QKD 方案中，诱骗态除了可以用来估计参数，还可以参与密钥生成，并且诱骗态的参与可以改善密钥生成效率。但是这部分数据在信道中进行传输时受损耗的影响，传输距离受限，所以只能改善近距离传输时 QKD 的密钥生成效率。因此，本文方案的传输性能曲线在 405 km 处出现了明显的拐点，而在该拐点之前，基于 HSPS 的被动诱骗态 QKD 方案的密钥生成效率接近基于 HSPS 的主动诱骗态 QKD 方案。

基于 WCS 的 PM 主动诱骗态方案与基于 HSPS 的 PM 主动诱骗态方案都采用了三个诱骗态，而基于 HSPS 的 PM 被动诱骗态方案无需主动制备诱骗态，就实际操作的难度来说，基于 HSPS 的 PM 被动诱骗态方案更为简单。

图 4 仿真的是在不同本地探测器探测效率 η_d 条件下，基于 HSPS 的 PM 主动三诱骗态方案与基于 HSPS 的 PM 被动诱骗态方案的传输性能曲线。可以看出，随着本地探测器的探测效率 η_d 的减小，基于 HSPS 的 PM 主动三诱骗态方案的密钥生成效率明显减小，而基于 HSPS 的 PM 被动诱骗态方案的传输性能曲线在拐点之前几乎重合。这说明基于 HSPS 的 PM 被动诱骗态方案的密钥生成效率对探测效率的依赖性较小。被动诱骗态思想的加入在一

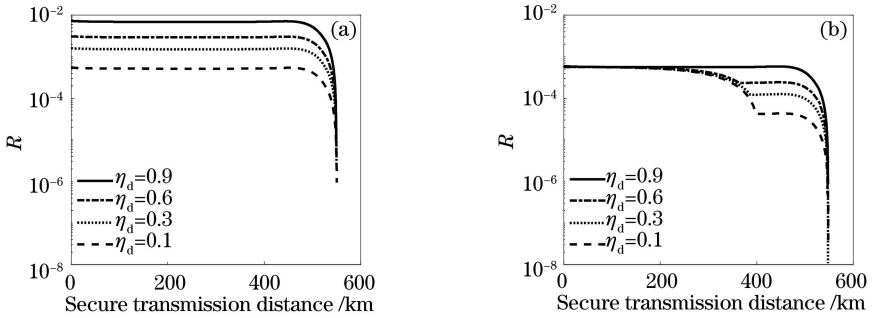

图 4 探测效率对不同量子密钥分配方案传输性能的影响。(a)基于 HSPS 的 PM 主动三诱骗态方案；(b)基于 HSPS 的 PM 被动诱骗态方案

Fig. 4 Effect of detection efficiency on transmission performance of each quantum key distribution scheme. (a) PM three-intensity active-decoy-state scheme based on HSPS; (b) PM passive-decoy-state method based on HSPS

定程度上弥补了实际探测器探测效率低下的缺陷。

图 5 仿真的是基于 HSPS 的 PM 被动诱骗态方案在不同数据长度下的传输性能曲线。仿真置信度设定为 $\theta=1-8.7\times10^{-3}$，分别采用三种数据长度，即 $N=6\times10^{11}$，$N=6\times10^{9}$ 和 $N=6\times10^{7}$。可以看出，随着数据长度的减小，本文方案的传输性能也下降，在以上三种数据长度下，最大安全传输距离分别减小至 523，513，507 km。但数据长度即使下降至 10^{7}，其最大安全传输距离仍然可以达到 507 km，性能依旧很优越。

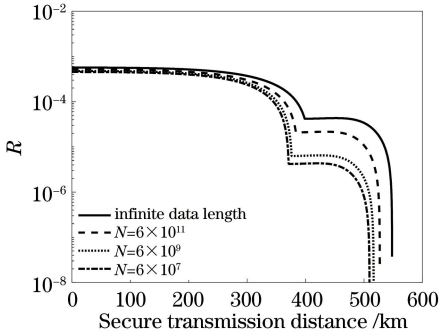

图 5 数据长度对基于 HSPS 的 PM 被动诱骗态方案传输性能的影响

Fig. 5 Effect of data length on transmission performance of PM passive-decoy-state scheme based on HSPS

4 结 论

为了探索高效简单的量子密钥分配方案，提出了基于 HSPS 的 PM 被动诱骗态方案，并对方案的性能进行了仿真分析。相比于现有基于 WCS 的 PM 主动诱骗态方案，所提方案的最大安全传输距离更远，并且所提方案的传输性能趋近于基于 HSPS 的 PM 主动诱骗态方案；通信双方无需主动制备诱骗态，这降低了实际 QKD 系统的实现难度。随着本地探测器探测效率的减小，本地探测器均响应的集合对密钥生成效率的贡献相对减小，被动诱骗态思想的加入可以弥补实际探测器探测效率低下的缺陷。随着数据长度的下降，所提方案的传输性能也下降，数据长度下降至 10^{7} 时，其最大安全传输距离仍然可以达到 507 km，性能依旧很优越。因此，所提出的基于 HSPS 的 PM 被动诱骗态方案是一种性能优越且实现简单的量子密钥分配方案。

参 考 文 献

[1] Bennett C H, Brassard G. Quantum cryptography: public key distribution and coin tossing [J]. Theoretical Computer Science, 2014, 560(1): 7-11.

[2] Wootters W K, Zurek W H. A single quantum cannot be cloned[J]. Nature, 1982, 299(5886): 802-803.

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

[4] Lütkenhaus N, Jahma M. Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack[J]. New Journal of Physics, 2002, 4(1): 44.

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

[6] Lucamarini M, Yuan Z, Dynes J F, et al. Overcoming the rate-distance limit of quantum key distribution without quantum repeaters[J]. Nature, 2018, 557(7705): 400-403.

[7] Wang X B, Yu Z W, Hu X L. Twin-field quantum key distribution with large misalignment error[J]. Physical Review A, 2018, 98(6): 062323.

[8] Grasselli F, Curty M. Practical decoy-state method for twin-field quantum key distribution[J]. New Journal of Physics, 2019, 21(7): 073001.

[9] Ma X F, Zeng P, Zhou H Y. Phase-matching quantum key distribution[J]. Physical Review X, 2018, 8(3): 031043.

[10] Wang H, Zhou Y Y, Yu W, et al. Quantum-classical hybrid optical network scheme based on PM protocol[J]. Laser & Optoelectronics Progress, 2020, 57(1): 012701.
王欢, 周媛媛, 虞味, 等. 基于 PM 协议的量子-经典混合光网络方案[J]. 激光与光电子学进展, 2020, 57(1): 012701.

[11] Pirandola S, Laurenza R, Ottaviani C, et al. Fundamental limits of repeaterless quantum communications[J]. Nature Communications, 2017, 8(1): 15043.

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

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

[14] Wang Q, Wang X B, Guo G C. Practical decoy-state method in quantum key distribution with a heralded single-photon source[J]. Physical Review A, 2007, 75(1): 012312.

[15] Mauerer W, Silberhorn C. Quantum key distribution with passive decoy state selection [J]. Physical Review A, 2007, 75(5): 050305.

[16] Adachi Y, Yamamoto T, Koashi M, et al. Simple

and efficient quantum key distribution with parametric down-conversion [J]. Physical Review Letters, 2007, 99(18): 180503.

[17] 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.

[18] Zhou X Y, Zhang C H, Zhang C M, et al. Obtaining better performance in the measurement-device-independent quantum key distribution with heralded single-photon sources[J]. Physical Review A, 2017, 96(5): 052337.

[19] Zhang C H, Zhang C M, Guo G C, et al. Biased three-intensity decoy-state scheme on the measurement-device-independent quantum key distribution using heralded single-photon sources[J]. Optics Express, 2018, 26(4): 4219-4229.

[20] Wang Q, Chen W, Xavier G B, et al. Experimental decoy-state quantum key distribution with a sub-poissionian heralded single-photon source [J]. Physical Review Letters, 2008, 100(9): 090501.

[21] Quan D X, Pei C X, Zhu C H, et al. New method of decoy state quantum key distribution with a heralded single-photon source[J]. Acta Physica Sinica, 2008, 57(9): 5600-5604.
权东晓, 裴昌幸, 朱畅华, 等. 一种新的预报单光子源诱骗态量子密钥分发方案[J]. 物理学报, 2008, 57(9): 5600-5604.

[22] 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.

[23] Zhou Y Y. Research on quantum key distribution theory based on optical fiber transmission [D]. Wuhan: Naval University of Engineering, 2010: 54-74.
周媛媛. 基于光纤传输的量子密钥分配理论研究[D]. 武汉: 海军工程大学, 2010: 54-74.

[24] Wei Z C, Gao M, Ma Z. Method of analyzing the statistical fluctuation in quantum key distribution based on Chernoff bound[J]. Journal of Information Engineering University, 2014, 15(4): 399-404.
魏正超, 高明, 马智. 基于切尔诺夫界的量子密钥分发统计涨落分析方法[J]. 信息工程大学学报, 2014, 15(4): 399-404.