# 基于被动式光源监控的参考系无关量子密钥分发*

张佳一[1)2)] 陈华星[1)2)] 张桓毓[1)2)] 钱雪瑞[1)2)] 张春辉[1)2)†] 王琴[1)2)]

1) (南京邮电大学量子信息与技术研究所, 南京 210003)

2) (南京邮电大学, 宽带无线通信与传感器网络技术教育部重点实验室, 南京 210003)

(2023 年 4 月 15 日收到; 2023 年 5 月 10 日收到修改稿)

参考系无关量子密钥分配 (RFI-QKD) 协议可以免疫参考系缓慢漂移的影响, 从而提高系统的鲁棒性, 具有广泛的应用. 然而, 在此前的 RFI-QKD 协议和方案中, 均假设光源是可信且服从某种固定的光子数分布, 该假设在实际系统中不一定满足. 本文提出了一种具有被动式光源监控功能的参考系无关量子密钥分发方案, 采用了三强度诱骗方法, 并且考虑了有限长效应. 仿真结果表明, 当存在光源起伏和参考系偏转角时, 本文的方案比原始 RFI-QKD 协议在成码率上也具有明显的优势.

**关键词:** 量子密钥分配, 参考系无关, 被动式光源监控, 有限长效应

**PACS:** 03.67.Dd, 03.67.Hk, 42.50.–p, 03.67.–a **DOI:** 10.7498/aps.72.20230609

## 1 引 言

量子密钥分发 (quantum key distribution, QKD) 允许合法的双方 (Alice 和 Bob) 根据量子物理定律共享安全的密钥. BB84 协议作为最早提出的 QKD 协议, 其安全性已被许多科学家从理论上证明[1−7]. 在 BB84 QKD 协议[1] 中, Alice 端和 Bob 端用于编码的 $X$ 基和 $Z$ 基构成了各自的参考系. 通常, Alice 和 Bob 需要共享一个相同的参考系, 如果它们的参考系不一致, QKD 系统将无法正常工作. 目前应用最广泛的方法是利用经典通信对两种通信参考系进行主动实时校准. 但是校准参考系需要大量的时间, 降低了整个通信过程的效率, 增加了 QKD 系统的复杂性和成本, 甚至可能存在一定的安全风险[8,9].

为避免参考系的实时校准操作, Anthony 等[10] 2010 年提出了参考系无关量子密钥分配 (reference-frame-independent QKD, RFI-QKD) 协议. 在实际的 QKD 系统中, 总可以找到一组保持稳定对齐的基矢, 因此在 RFI-QKD 协议中仅要求 Alice 和 Bob 保证一组基对齐即可, 剩余的两组基可以在信道中缓慢变化. 然后利用不同基矢组合下的测量数据来紧致地估算信道参数, 严格计算出密钥生成率, 从而避免参考系漂移的影响.

然而, RFI-QKD 协议对光源做了一定假设, 即具有可信和固定的光子数分布 (photon number distribution, PND), 该假设在实际系统中很难完全满足, 将不可避免地降低实际 QKD 系统的安全性和性能[11−16]. 为了解决这一问题, 本文提出了一种 RFI-QKD 的被动式光源监控 (passive light source monitoring, PLSM) 方案, 该方案由一个分束器和源端两个探测器组成的被动式监控模块来实现. 利用 PLSM 模块, 可以通过两个本地探测器获得 4 个监控事件, 然后精确地估计光源分布的界限. 本文以基于三强度诱骗态的 RFI-QKD为例进行介绍协议模型和仿真结果. 结果表明, 与原有的 RFI-QKD[11] 相比, 本文的 PLSM 方法可以被动地

* 国家重点研发计划 (批准号: 2018 YFA0306400)、国家自然科学基金 (批准号: 12074194, 12104240)、江苏省重点研发计划产业前瞻与关键核心技术项目 (批准号: BE2022071) 和江苏省自然科学基金 (批准号: BK20192001, BK20210582) 资助的课题.

† 通信作者. E-mail: chz@njupt.edu.cn

© 2023 中国物理学会 Chinese Physical Society 

监测 PND, 并且在考虑光源波动、有限长效应和参考系偏转角时具有更大的优势.

## 2 RFI-QKD 中的 PLSM 方案

本节介绍具有被动式光源监控功能的参考系无关量子密钥分发方案, 包括步骤和模型. 如图 1 所示, 该装置的示意图涉及发送方 Alice 和接收方 Bob, 其中被动式光源监控模块位于 Alice 一侧. 具体步骤如下:

**步骤 1** 发送端 Alice 通过非理想光源发送 $N$ 个脉冲, 经过强度调制器 IM 随机制备并发送 3 种强度脉冲, 分别是信号态脉冲、诱骗态脉冲和真空态脉冲;

**步骤 2** $N$ 个脉冲经过光纤分束器 BS1 后分为信号光和闲置光, 其中信号光用来编码并发送给接收端 Bob, 闲置光用来执行被动式光源监控 PLSM; 闲置光进入被动式光源监控模块后, 被光纤分束器 BS2 进一步分束, 最终到达本地端探测器 D1 和 D2; 本地端得到 4 种不同的探测事件 $l\in(x,y,z,w)$, 其中 $x$ 代表 D1 和 D2 都不响应; $y$ 代表只有 D1 响应; $z$ 代表只有 D2 响应; $w$ 代表 D1 和 D2 都响应;

**步骤 3** 当信号光经过编码 Encoding 模块后, 对于信号态脉冲和诱骗态脉冲, Alice 分别以不同概率制备 $Z_{\rm A}, X_{\rm A}$ 和 $Y_{\rm A}$ 基下的量子态;

**步骤 4** 在接收端的解码 Decoding 模块中, Bob 分别以概率 $P_{Z_{\rm B}}, P_{X_{\rm B}}$ 和 $1-P_{Z_{\rm B}}-P_{X_{\rm B}}$ 选择 $Z_{\rm B}$, $X_{\rm B}$ 和 $Y_{\rm B}$ 基矢, 并记录下对应的测量结果;

**步骤 5** 测量结束后, Alice 和 Bob 通过已认证的经典信道公布其基矢和强度选择信息; 然后 Alice 和 Bob 保留制备测量基矢组合 $Z_{\rm A}Z_{\rm B}, X_{\rm A}X_{\rm B}$, $X_{\rm A}Y_{\rm B}, Y_{\rm A}X_{\rm B}, Y_{\rm A}Y_{\rm B}$ 下的数据, 其他基矢组合的数据则被丢弃; Alice 和 Bob 随机选取筛后密钥中的部分比特, 得到基矢组合 $Z_{\rm A}Z_{\rm B}, X_{\rm A}X_{\rm B}, X_{\rm A}Y_{\rm B}, Y_{\rm A}X_{\rm B}$, $Y_{\rm A}Y_{\rm B}$ 下的增益和总量子比特误码率;

**步骤 6** 结合诱骗态方法得到单光子计数率的下界和误码率上界, 进而估计最终的码率.

在步骤 1 中, 信号态脉冲平均光子数为 $u$, 诱骗态平均光子数为 $v$, 真空态平均光子数为 0, 并满足 $u>v>0$; Alice 分别以概率 $P_u$ 发送信号态、$P_v$ 发送诱骗态、$1-P_u-P_v$ 发送真空态. 在步骤 2 中, 由于 PLSM 模块中发送端本地探测器的监控作用, 闲置光被投影到量子态 $\rho=\sum P_n(\mu)q_n^l|n\rangle\langle n|$ 上, 则 $n$ 光子被投射到探测事件 $l$ 上的概率 $q_n^l$ [17,18] 为

$$q_n^x=(1-d_{\rm s})^2(1-\eta_{\rm s})^n, \tag{1}$$

$$q_n^y=(1-d_{\rm s})(1-\eta_{\rm s})^n\left[\left(1+\frac{t\eta_{\rm s}}{1-\eta_{\rm s}}\right)^n+d_{\rm s}-1\right], \tag{2}$$

$$q_n^z=(1-d_{\rm s})(1-\eta_{\rm s})^n\left[\left(\frac{1-t\eta_{\rm s}}{1-\eta_{\rm s}}\right)^n+d_{\rm s}-1\right], \tag{3}$$

$$q_n^w=1-q_n^x-q_n^y-q_n^z, \tag{4}$$

其中, $d_{\rm s}$ 和 $\eta_{\rm s}$ 分别是发送端探测器的暗计数率和探测效率, $t$ 表示分束器 BS1 的透射率. 此外定义不同事件下的光子数分布 $a_n^l(\mu)=P_n(\mu)q_n^l$, 其中 $P_n(\mu)$ 表示平均光子数为 $\mu$ 时, $n$ 光子出现的概率. 通过测量闲置光, 得到事件 $l$ 的增益为

$$Q_l(\mu)=\sum a_n^l(\mu). \tag{5}$$

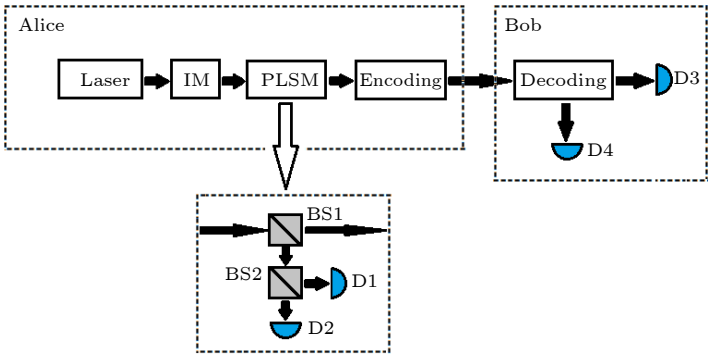


图 1 具有被动式光源监控功能的参考系无关量子密钥分发系统示意图. 被动式光源监控模块由光纤分束器和两个本地单光子探测器构成. IM 表示强度调制器; Laser 表示激光; BS 表示分束器; D 表示单光子探测器

Fig. 1. Schematic of the RFI-QKD system with PLSM. The PLSM module is composed of beam splitters and two local single-photon detectors. The IM stands for the intensity modulator. The Laser stands for laser. BS stands for the beam splitter. D stands for the single-photon detector.

接下来利用本地端的响应事件来进行光源监控, 即估计光源中部分光子数的分布概率. 首先, 由$Q_x(\mu)$可得$P_0(\mu)$的下界和上界:

$$P_0^{\rm L}(\mu)=P_0^{\rm U}(\mu)=\frac{Q_x(\mu)}{(1-d_{\rm s})^2}, \tag{6}$$

结合$Q_y(\mu)$和$Q_z(\mu)$消去参数$P_2(\mu)$:

$$\begin{aligned}&q_2^zQ_y(\mu)-q_2^yQ_z(\mu)\\&=P_0(\mu)(q_0^yq_2^z-q_2^yq_0^z)+P_1(\mu)(q_1^yq_2^z-q_2^yq_1^z)\\&\quad+\sum_{i=3}^{\infty}P_i(\mu)(q_2^zq_i^y-q_i^zq_2^y)\\&\leqslant P_0(\mu)(q_0^yq_2^z-q_2^yq_0^z)+P_1(\mu)(q_1^yq_2^z-q_2^yq_1^z),\end{aligned} \tag{7}$$

则$P_1(\mu)$的下界表示为

$$P_1^{\rm L}(\mu)=\frac{q_2^zQ_y(\mu)-q_2^yQ_z(\mu)-(q_2^zq_0^y-q_0^zq_2^y)P_0^{\rm L}(\mu)}{q_2^zq_1^y-q_1^zq_2^y}, \tag{8}$$

通过适当缩放$Q_y(\mu)$和$Q_z(\mu)$, 可以得到如下 4 个不等式:

$$\sum P_n(\mu)q_n^y\geqslant P_0(\mu)q_0^y+P_1(\mu)q_1^y+P_2(\mu)q_2^y, \tag{9}$$

$$\sum P_n(\mu)q_n^z\geqslant P_0(\mu)q_0^z+P_1(\mu)q_1^z+P_2(\mu)q_2^z, \tag{10}$$

$$\begin{aligned}\sum P_n(\mu)q_n^y\leqslant{}&P_0(\mu)q_0^y+P_1(\mu)q_1^y+P_2(\mu)q_2^y\\&+q_3^y(1-P_0(\mu)-P_1(\mu)-P_2(\mu)),\end{aligned} \tag{11}$$

$$\begin{aligned}\sum P_n(\mu)q_n^z\leqslant{}&P_0(\mu)q_0^z+P_1(\mu)q_1^z+P_2(\mu)q_2^z\\&+q_3^z(1-P_0(\mu)-P_1(\mu)-P_2(\mu)),\end{aligned} \tag{12}$$

结合 (9) 式和 (12) 式消去参数$P_2(\mu)$, 可以得到$P_1(\mu)$的上界:

$$\begin{aligned}P_1^{\rm U}(\mu)={}&\left[(q_2^y-q_3^y)Q_z(\mu)-q_2^zQ_y(\mu)+(q_2^zq_0^y\right.\\&\left.-q_2^zq_3^y-q_0^zq_2^y+q_0^zq_3^y)P_0^{\rm L}(\mu)+q_2^zq_3^y\right]\\&\times\left[q_1^z(q_2^y-q_3^y)-q_2^z(q_1^y-q_3^y)\right]^{-1}.\end{aligned} \tag{13}$$

同理, 通过 (9) 式和 (11) 式以及上述估计出的$P_0^{\rm U}(\mu)$和$P_1^{\rm U}(\mu)$可以得到$P_2(\mu)$的上、下界分别为

$$P_2^{\rm U}(\mu)=\frac{Q_z(\mu)-q_0^zP_0^{\rm L}(\mu)-q_1^zP_1^{\rm L}(\mu)}{q_2^z}, \tag{14}$$

$$P_2^{\rm L}(\mu)=\frac{Q_y(\mu)-(q_0^y-q_3^y)P_0^{\rm L}(\mu)-(q_1^y-q_3^y)P_1^{\rm L}(\mu)-q_3^y}{q_2^y-q_3^y}. \tag{15}$$

在步骤 3 中, 当信号光经过编码模块 Encoding 后, 对于信号态脉冲, Alice 分别以概率$P_{Z_{\rm A}|u}$, $P_{X_{\rm A}|u}$和$1-P_{Z_{\rm A}|u}-P_{X_{\rm A}|u}$制备$Z_{\rm A}$, $X_{\rm A}$和$Y_{\rm A}$基下的量子态; 对于诱骗态脉冲, Alice 分别以概率$P_{Z_{\rm A}|v}$, $P_{X_{\rm A}|v}$和$1-P_{Z_{\rm A}|v}-P_{X_{\rm A}|v}$制备$Z_{\rm A}$, $X_{\rm A}$和$Y_{\rm A}$基下的量子态.

在 RFI-QKD 协议中, $Z$基用来产生安全密钥, $X$基和 $Y$基用来估算 Eve 能够窃取的信息量. Alice 端和 Bob 端的 $Z$基始终保持对齐, 而 $X$基和 $Y$基可以是非对齐的, 它们满足如下公式:

$$\begin{aligned}&Z_{\rm A}=Z_{\rm B},\quad X_{\rm B}=\cos\beta X_{\rm A}+\sin\beta Y_{\rm A},\\&Y_{\rm B}=\cos\beta Y_{\rm A}-\sin\beta X_{\rm A},\end{aligned} \tag{16}$$

其中$\beta$表示参考系的偏转角.

在信号传输阶段完成后, Alice 和 Bob 通过已认证的经典信道公布其基矢和强度选择信息. 然后保留制备测量基矢组合$Z_{\rm A}Z_{\rm B}$, $X_{\rm A}X_{\rm B}$, $X_{\rm A}Y_{\rm B}$, $Y_{\rm A}X_{\rm B}$, $Y_{\rm A}Y_{\rm B}$下的数据, 并估算基矢组合$Z_{\rm A}Z_{\rm B}$, $X_{\rm A}X_{\rm B}$, $X_{\rm A}Y_{\rm B}$, $Y_{\rm A}X_{\rm B}$, $Y_{\rm A}Y_{\rm B}$下脉冲$\mu$的增益, 计算公式如下:

$$S_{\xi_{\rm A}\xi_{\rm B}}^{\mu}=\frac{1}{2}\left(P_{\xi_{\rm A}^0\xi_{\rm B}^0}^{\mu}+P_{\xi_{\rm A}^0\xi_{\rm B}^1}^{\mu}+P_{\xi_{\rm A}^1\xi_{\rm B}^0}^{\mu}+P_{\xi_{\rm A}^1\xi_{\rm B}^1}^{\mu}\right), \tag{17}$$

其中 1/2 代表 Alice 选择量子态$\xi_{\rm A}^0$的概率. $\xi_{\rm A}^0$和$\xi_{\rm A}^1$构成$\xi_{\rm A}$基, $\xi_{\rm B}^0$和$\xi_{\rm B}^1$构成$\xi_{\rm B}$基. $P_{\xi_{\rm A}^0\xi_{\rm B}^0}^{\mu}$表示在 Alice 制备量子态$\xi_{\rm A}^0$的条件下, Bob 使用$\xi_{\rm B}$基测量后对应测量结果为 0 时的概率, 其表达式为

$$\begin{aligned}P_{\xi_{\rm A}^0\xi_{\rm B}^0}^{\mu}={}&\sum_{n=0}^{\infty}P_n(\mu)\sum_{j=0}^{\infty}C_n^j\eta^j(1-\eta)^{n-j}\\&\times\left(\left|\langle\xi_{\rm A}^0|\xi_{\rm B}^0\rangle\right|^2\right)^jF(j),\end{aligned} \tag{18}$$

其中假设$P_n(\mu)$服从泊松分布, $C_n^j$表示二项式系数, $\eta$表示信号从 Alice 端到 Bob 端的传输效率. $F(j)$表示当 Bob 使用两个阈值单光子探测器时, 在 $n$光子态的条件下有效探测事件的概率:

$$F(j)=\begin{cases}1-Y_0, & j>0,\\ Y_0(1-Y_0), & j=0,\end{cases} \tag{19}$$

其中$Y_0$表示单光子探测器的暗记数率. 使用同样的方法得到$P_{\xi_{\rm A}^0\xi_{\rm B}^1}^{\mu}$, $P_{\xi_{\rm A}^1\xi_{\rm B}^0}^{\mu}$, $P_{\xi_{\rm A}^1\xi_{\rm B}^1}^{\mu}$. 此外, $\xi_{\rm A}\xi_{\rm B}$的量子比特误码率表示为

$$\begin{aligned}&E_{\xi_{\rm A}\xi_{\rm B}}^{\mu}=\min\{\widetilde{E}_{\xi_{\rm A}\xi_{\rm B}}^{\mu},1-\widetilde{E}_{\xi_{\rm A}\xi_{\rm B}}^{\mu}\},\\&\widetilde{E}_{\xi_{\rm A}\xi_{\rm B}}^{\mu}=e_{\rm d}(1-2e_{\xi_{\rm A}\xi_{\rm B}}^{\mu})+e_{\xi_{\rm A}\xi_{\rm B}}^{\mu},\end{aligned} \tag{20}$$

其中

$$e_{\xi_{\rm A}\xi_{\rm B}}^{\mu}=\frac{P_{\xi_{\rm A}^0\xi_{\rm B}^1}^{\mu}+P_{\xi_{\rm A}^1\xi_{\rm B}^0}^{\mu}}{2S_{\xi_{\rm A}\xi_{\rm B}}^{\mu}}, \tag{21}$$

这里$e_{\rm d}$代表 QKD 系统的光学本底误码.

考虑到在实际系统中 Alice 发送的脉冲个数是有限的, 需要考虑统计波动对参数估计的影响, 这里使用标准统计误差分析方法 [19]. 此时增益的上界 $S^{\mu,\mathrm{U}}_{\xi_\mathrm{A}\xi_\mathrm{B}}$、增益的下界 $S^{\mu,\mathrm{L}}_{\xi_\mathrm{A}\xi_\mathrm{B}}$、总量子比特误码率的上界 $E^{\mu,\mathrm{U}}_{\xi_\mathrm{A}\xi_\mathrm{B}}S^{\mu,\mathrm{U}}_{\xi_\mathrm{A}\xi_\mathrm{B}}$ 可以表示为

$$S^{\mu,\mathrm{U}}_{\xi_\mathrm{A}\xi_\mathrm{B}} = S^{\mu}_{\xi_\mathrm{A}\xi_\mathrm{B}}\left(1+\frac{\gamma}{\sqrt{NP_\mu P_{\xi_\mathrm{A}|\mu}P_{\xi_\mathrm{B}}S^{\mu}_{\xi_\mathrm{A}\xi_\mathrm{B}}}}\right), \tag{22}$$

$$S^{\mu,\mathrm{L}}_{\xi_\mathrm{A}\xi_\mathrm{B}} = S^{\mu}_{\xi_\mathrm{A}\xi_\mathrm{B}}\left(1-\frac{\gamma}{\sqrt{NP_\mu P_{\xi_\mathrm{A}|\mu}P_{\xi_\mathrm{B}}S^{\mu}_{\xi_\mathrm{A}\xi_\mathrm{B}}}}\right), \tag{23}$$

$$E^{\mu,\mathrm{U}}_{\xi_\mathrm{A}\xi_\mathrm{B}}S^{\mu,\mathrm{U}}_{\xi_\mathrm{A}\xi_\mathrm{B}} = E^{\mu}_{\xi_\mathrm{A}\xi_\mathrm{B}}S^{\mu}_{\xi_\mathrm{A}\xi_\mathrm{B}} \times\left(1+\frac{\gamma}{\sqrt{NP_\mu P_{\xi_\mathrm{A}|\mu}P_{\xi_\mathrm{B}}E^{\mu}_{\xi_\mathrm{A}\xi_\mathrm{B}}S^{\mu}_{\xi_\mathrm{A}\xi_\mathrm{B}}}}\right), \tag{24}$$

其中, $P_{\xi_\mathrm{A}|\mu}$表示 Alice 制备量子态时在强度为$\mu$的条件下选择 $\xi_\mathrm{A}$ 基的条件概率; $P_{\xi_\mathrm{B}}$ 表示 Bob 测量量子态时选择 $\xi_\mathrm{B}$ 基的概率; $\gamma$ 表示统计波动分析选择的标准差系数, 其数值与失败概率 $\varepsilon$ 有关, 他们之间的关系满足:

$$1-\frac{2}{\sqrt{\pi}}\int_0^{\frac{\gamma}{\sqrt{2}}}\mathrm{e}^{-t^2}\mathrm{d}t=\varepsilon. \tag{25}$$

另外, 可以使用文献 [20] 中的方法来进一步提升安全性, 它严格证明了对 BB84 类协议可以用 Chernoff bound 处理, 允许各时间窗口强度涨落带任意关联.

进一步地, 结合被监控的光子数分布 (PND) 以及上述增益及量子比特误码率可以获得基矢组合 $Z_\mathrm{A}Z_\mathrm{B}$ 的单光子计数率下界 $Y^{1,\mathrm{L}}_{Z_\mathrm{A}Z_\mathrm{B}}$ 和单光子误码率上界 $e^{1,\mathrm{U}}_{Z_\mathrm{A}Z_\mathrm{B}}$, 即 [21]

$$Y^{1}_{Z_\mathrm{A}Z_\mathrm{B}} \geqslant Y^{1,\mathrm{L}}_{Z_\mathrm{A}Z_\mathrm{B}} = \frac{P^{\mathrm{L}}_2(u)S^{v,\mathrm{L}}_{Z_\mathrm{A}Z_\mathrm{B}} - P^{\mathrm{U}}_2(v)S^{u,\mathrm{U}}_{Z_\mathrm{A}Z_\mathrm{B}} - [P^{\mathrm{U}}_2(u)P^{\mathrm{U}}_0(v) - P^{\mathrm{L}}_2(v)P^{\mathrm{L}}_0(u)]S^{0,\mathrm{U}}}{P^{\mathrm{U}}_2(u)P^{\mathrm{U}}_1(v) - P^{\mathrm{L}}_2(v)P^{\mathrm{L}}_1(u)}, \tag{26}$$

$$e^{1}_{Z_\mathrm{A}Z_\mathrm{B}} \leqslant e^{1,\mathrm{U}}_{Z_\mathrm{A}Z_\mathrm{B}} = \frac{E^{v,\mathrm{U}}_{Z_\mathrm{A}Z_\mathrm{B}}S^{v,\mathrm{U}}_{Z_\mathrm{A}Z_\mathrm{B}} - P^{\mathrm{L}}_0(v)S^{0,\mathrm{L}}E_0}{P^{\mathrm{L}}_1(v)Y^{1,\mathrm{L}}_{Z_\mathrm{A}Z_\mathrm{B}}}, \tag{27}$$

其中, $S^{v,\mathrm{L}}_{Z_\mathrm{A}Z_\mathrm{B}}$ 和 $S^{u,\mathrm{U}}_{Z_\mathrm{A}Z_\mathrm{B}}$ 分别代表诱骗态脉冲在基矢组合为 $Z_\mathrm{A}Z_\mathrm{B}$ 下的增益的下界和信号态脉冲在基矢组合为 $Z_\mathrm{A}Z_\mathrm{B}$ 下的增益的上界; $S^{0,\mathrm{U}}$ 和 $S^{0,\mathrm{L}}$ 表示真空态脉冲增益的上界和下界; $E^{v,\mathrm{U}}_{Z_\mathrm{A}Z_\mathrm{B}}$ 和 $S^{v,\mathrm{U}}_{Z_\mathrm{A}Z_\mathrm{B}}$ 分别为诱骗态脉冲在基矢组合为 $Z_\mathrm{A}Z_\mathrm{B}$ 下的误码率的上界和增益的上界; $E_0=0.5$ 是背景计数的误码率; 使用同样的方法估计基矢组合 $X_\mathrm{A}X_\mathrm{B}$, $X_\mathrm{A}Y_\mathrm{B}$, $Y_\mathrm{A}X_\mathrm{B}$, $Y_\mathrm{A}Y_\mathrm{B}$的单光子误码率上界 $e^{1,\mathrm{U}}_{X_\mathrm{A}X_\mathrm{B}}$, $e^{1,\mathrm{U}}_{X_\mathrm{A}Y_\mathrm{B}}$, $e^{1,\mathrm{U}}_{Y_\mathrm{A}X_\mathrm{B}}$, $e^{1,\mathrm{U}}_{Y_\mathrm{A}Y_\mathrm{B}}$. 利用上述参数, 得到中间参量 $C$:

$$C = (1-2e^{1,\mathrm{U}}_{X_\mathrm{A}X_\mathrm{B}})^2 + (1-2e^{1,\mathrm{U}}_{X_\mathrm{A}Y_\mathrm{B}})^2 + (1-2e^{1,\mathrm{U}}_{Y_\mathrm{A}X_\mathrm{B}})^2 + (1-2e^{1,\mathrm{U}}_{Y_\mathrm{A}Y_\mathrm{B}})^2, \tag{28}$$

而不可信第三方 Eve 窃取的信息量 $I_\mathrm{E}$ 表示为

$$I_\mathrm{E} = (1-e^{1,\mathrm{U}}_{Z_\mathrm{A}Z_\mathrm{B}})H(1+\psi/2) + e^{1,\mathrm{U}}_{Z_\mathrm{A}Z_\mathrm{B}}H(1+\varphi/2), \tag{29}$$

其中,

$$\psi = \min\left\{\frac{\sqrt{C/2}}{1-e^{1,\mathrm{U}}_{Z_\mathrm{A}Z_\mathrm{B}}}, 1\right\},$$

$$\varphi = \frac{1}{e^{1,\mathrm{U}}_{Z_\mathrm{A}Z_\mathrm{B}}}\sqrt{\frac{C}{2}-(1-e^{1,\mathrm{U}}_{Z_\mathrm{A}Z_\mathrm{B}})^2\psi^2}, \tag{30}$$

$H(x)$ 是二进制香农熵函数$H(x)=-x\log_2(x)-(1-x)\log_2(1-x)$ .

最终得到被动式光源监控的 RFI-QKD 协议的安全密钥率公式:

$$R = P_u P_{Z_\mathrm{A}|u}P_{Z_\mathrm{B}}\left\{P^{\mathrm{L}}_1(u)Y^{1,\mathrm{L}}_{Z_\mathrm{A}Z_\mathrm{B}}(1-I_\mathrm{E}) - fS^{u,\mathrm{U}}_{Z_\mathrm{A}Z_\mathrm{B}}H(E^{\mathrm{U}}_{Z_\mathrm{A}Z_\mathrm{B}})\right\}, \tag{31}$$

其中 $P_u$ 表示 Alice 选择信号态的概率; $P_{Z_\mathrm{A}|u}$ 表示 Alice 制备量子态时在强度为 $u$ 的条件下选择 $Z_\mathrm{A}$ 基的概率; $P_{Z_\mathrm{B}}$ 表示 Bob 选择 $Z_\mathrm{B}$ 基的概率; $f$ 表示密钥协商算法的协商效率; $S^{u,\mathrm{U}}_{Z_\mathrm{A}Z_\mathrm{B}}$ 和 $E^{\mathrm{U}}_{Z_\mathrm{A}Z_\mathrm{B}}$ 分别是信号态脉冲在基矢组合 $Z_\mathrm{A}Z_\mathrm{B}$ 下的增益的上界和量子比特误码率, 它们可以直接从实验数据中观测得到.

## 3 实验系统及测量结果

下面对原始 RFI-QKD 和 PLSM RFI-QKD 进行数值仿真. 首先, 比较不同的光源起伏对原始 RFI-QKD 和 PLSM RFI-QKD 的密钥率的影响. 此外, 分析脉冲数对密钥率的影响. 最后, 分析不同参考系偏转角度对密钥率的影响. 为了模拟实际情况, 使用的参数如表 1 所列, $\gamma$ 取 5.3 时对应的失

败概率为$10^{-7}$, 本地探测器的探测效率和暗计数率分别为$\eta_{\rm s}=0.9$和$d_{\rm s}=2.5\times10^{-6}$.

表 1 数值仿真中使用的基本系统参数

Table 1. Basic system parameters used in our numerical simulations.

| $Y_0$ | $e_{\rm d}$ | $\alpha$ | $f$ | $\gamma$ |
|---|---|---|---|---|
| $1\times10^{-6}$ | 0.015 | 0.2 dB/km | 1.16 | 5.3 |

首先, 比较原始 RFI-QKD 和现有的 PLSM RFI-QKD 在不同光源起伏系数 $\sigma$ 下的性能. 为了模拟实际情况, 使用了表 1 所列的一组实际系统参数. 在实际情况下, 光源起伏系数 $\sigma$ 通常大于 1%[22], 因此这里设光源起伏系数 $\sigma=1\%$和$\sigma=2\%$. 从图 2 可以看出, 当考虑到光源起伏时, PLSM RFI-QKD 协议的性能明显优于原始的 RFI-QKD 协议. 例如, 当 $\sigma$ 从 1% 上升到 2% 时, PLSM RFI-QKD 的性能保持稳定, 而原 RFI-QKD 的传输距离下降了 35 km, 说明 PLSM RFI-QKD在光源起伏下具有良好的鲁棒性.

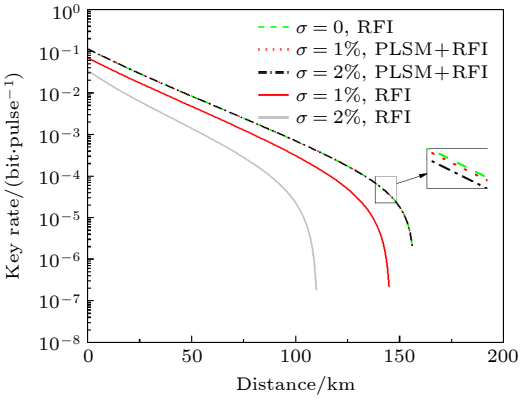


图 2 在固定偏转角和脉冲数, 起伏系数分别为 $\sigma=0$, $\sigma=1\%$ 和 $\sigma=2\%$ 的条件下, 原始 RFI-QKD 和 PLSM RFI-QKD 的安全密钥率. 这里脉冲数 $N=10^{12}$, 偏转角 $\beta=\pi/9$

Fig. 2. Key rate of different schemes with intensity fluctuation $\sigma=0$, $\sigma=1\%$ and $\sigma=2\%$ under fixed deviation angle and with infinite number of pulses. Here the fixed deviation angle $\beta=\pi/9$ and the number of pulses $N=10^{12}$.

接着, 比较原始 RFI-QKD 和 PLSM RFI-QKD 在不同脉冲数下的性能. 为了模拟实际情况, 使用表 1 中设置的系统参数, 将脉冲数分别设置为 $N=10^{11}$和$N=10^{12}$. 从图 3 可以看出, 考虑到光源起伏和脉冲数, PLSM RFI-QKD 的性能明显优于原来的 RFI-QKD. 当脉冲数为 $N=10^{11}$时, 光源起伏系数$\sigma=2\%$时, PLSM RFI-QKD 与原始 RFI-QKD 的最大传输距离差为 14 km. 当脉冲数 $N=10^{12}$, 光源起伏系数$\sigma=2\%$时, PLSM RFI-QKD 与原始 RFI-QKD之间的最大传输距离之差为 31 km. 因此, 可以得出结论, 随着脉冲数量增加, PLSM RFI-QKD 的优势将进一步增强.

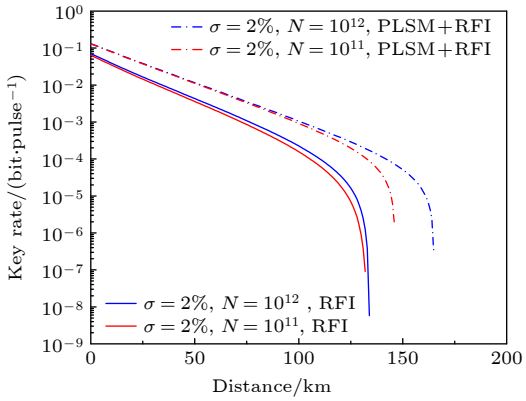


图 3 在考虑光源起伏, 不同脉冲数的条件下, 原始 RFI-QKD 和 PLSM RFI-QKD 的安全密钥率. 这里偏转角 $\beta=0$, 光源起伏系数 $\sigma=2\%$

Fig. 3. Secret key rate of two schemes with different numbers of pulses when light source fluctuation is taken into account. Here the fixed deviation angle $\beta=0$ and fluctuation coefficient $\sigma=2\%$.

最后, 比较原始 RFI QKD 和 PLSM RFI-QKD 在不同参考系偏转角下的性能. 为了模拟实际情况, 分别取偏转角 $\beta=0$, $\beta=\pi/18$, $\beta=\pi/9$. 图 4 的仿真结果表明偏转角为 $\beta=0$, $\beta=\pi/18$, $\beta=\pi/9$时, 且光源起伏存在时, PLSM RFI-QKD 与原始 RFI-QKD 的最大传码距离之差分别为 32, 35 和 37 km. 因此, 同时考虑光源起伏和偏转角的

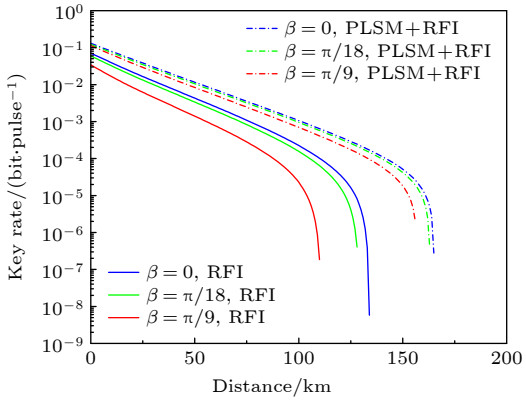


图 4 在固定脉冲数和光源起伏系数, 不同偏转角的条件下, 原始 RFI-QKD 和 PLSM-QKD 的密钥率. 这里脉冲总数 $N=10^{12}$, 光源起伏系数 $\sigma=2\%$

Fig. 4. Secret key rate of two schemes with different deviation angles of reference frame under fixed number of pulses and fluctuation coefficient. Here the number of pulses $N=10^{12}$ and source fluctuation coefficient $\sigma=2\%$.

存在, PLSM RFI-QKD 也可以比原始 RFI-QKD 有更好的性能, 并且随着偏转角的增加, PLSM RFI-QKD 的优势将进一步放大.

## 4 结 论

本文提出了一种具有被动式光源监控功能的参考系无关量子密钥分发方法, 通过使用分束器对光源分束后产生的 4 种响应事件进行参数估算, 进而完成被动式光源监控功能. 本文建立了理论模型, 并进行了相应的数值仿真. 仿真结果表明, 当考虑光源起伏, 有限长效应和参考系偏转角度时, PLSM RFI-QKD 方案优于原始的 RFI-QKD 方案. 但是, 由于该方案加入了分束器和探测器等光源监控装置, 需要和原来的 QKD 系统同步和融合, 因此会增加 QKD 系统的代价和复杂度. 此外, 光源监控方案的性能会受到使用的被动式光源监控装置本身参数的影响, 如分束器的分束比以及本地探测器的探测效率和暗计数率, 实际仿真效果会跟这些参数相关. 尽管如此, 我们相信本工作在未来量子保密通信实际应用中会发挥有益的作用.

## 参考文献


[1] Charles H B, Gilles B 2014 *Theor. Comput. Sci.* **560** 7

[2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661

[3] Shor, Preskill 2000 *Phys. Rev. Lett.* **85** 441

[4] Dominic M 2001 *J. ACM* **48** 351

[5] Lo H K, Chau H F 1999 *Science* **283** 2050

[6] Charles H B, Francois B, Gilles B, Louis S, John S 1992 *J. Cryptol.* **5** 3

[7] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503

[8] Jain N, Wittmann C, Lydersen L, Wiechers C, Elser D, Marquardt C, Makarov V, Leuchs G 2011 *Phys. Rev. Lett.* **107** 110501

[9] Dong Z Y, Yu N N, Wei Z J, Wang J D, Zhang Z M 2014 *Eur. Phys. J. D* **68** 230

[10] Anthony L, Valerio S, John G R, Jeremy L B 2010 *Phys. Rev. A* **82** 012304

[11] Tanumoy P, Byung K P, Cho Y W, Han S W, Kim Y S, Sung M 2017 *Phys. Lett. A* **381** 2497

[12] Zhang C M, Zhu J R, Wang Q 2018 *J. Phys. Commun.* **2** 055029

[13] Zhang C M, Zhu J R, Wang Q 2018 *Eur. Phys. J. D* **72** 1

[14] Zhu J R, Wang C Y, Liu K, Zhang C M, Wang Q 2018 *Quantum Inf. Process.* **17** 1

[15] Zhu J R, Zhang C M, Wang Q 2018 *Phys. Lett. A* **383** 311

[16] Zhang C M, Wang W B, Li H W, Wang Q 2019 *Opt. Lett.* **44** 1226

[17] Wang Q, Zhang C H, Wang X B 2016 *Phys. Rev. A* **93** 032312

[18] Zhang C H, Wang D, Zhou X Y, Wang S, Zhang L B, Yin Z Q, Chen W H, Z F, Guo G C, Wang Q 2018 *Opt. Express* **26** 25921

[19] Chi H H, Yu Z W, Wang X B 2012 *Phys. Rev. A* **86** 042307

[20] Jiang C, Yu Z W, Hu X L, Wang X B 2022 *Natl. Sci. Rev.* **10** 4

[21] Wang X B, Peng C Z, Zhang J, Yang L, Pan J W 2008 *Phys. Rev. A* **77** 042311

[22] Xu F X, Zhang Y, Zhou Z, Chen W, Han Z F, Guo G C 2009 *Phys. Rev. A* **80** 062309

# Reference-frame-independent quantum key distribution based on passive light source monitoring*

Zhang Jia-Yi [1)2)] Chen Hua-Xing [1)2)] Zhang Huan-Yu [1)2)] Qian Xue-Rui [1)2)]
Zhang Chun-Hui [1)2)†] Wang Qin [1)2)]

1) (*Institute of Quantum Information and Technology, Nanjing University of Posts and Telecommunications, Nanjing* 210003, *China*)

2) (*Key Laboratory of Broadband Wireless Communication and Sensor Network Technology, Ministry of Education, Nanjing University of Posts and Telecommunications, Nanjing* 210003, *China*)

( Received 15 April 2023; revised manuscript received 10 May 2023 )

**Abstract**

In quantum key distribution (QKD), the users need to share the same reference frame. If their reference frames are inconsistent, the QKD system will not function properly. The most widely used method today is the active real-time calibration of both communication reference frames by using classical communication. In order to get rid of the real-time calibration operation of the reference frames, a QKD protocol independent of reference frame is proposed, called reference-frame-independent QKD (RFI-QKD). The RFI-QKD protocol is immune to the effects of slowly changing reference frame drift, requiring that only one set of bases should be aligned by Alice and Bob, and the remaining two sets of bases can slowly change in the channel. In the real QKD system, a set of basis vectors can always be found to maintain a stable alignment. However, some assumptions are made for the sources in most reported researches, i.e. with a trusted and fixed photon-number distribution (PND), which usually cannot be satisfied in practical implementations. Those unreasonable assumptions will inevitably compromise the security of practical QKD systems. To solve the problem, in this work, we present a passive light source monitoring (PLSM) scheme for RFI-QKD, which is accomplished by a passive monitoring module consisting of a beam splitter and two detectors on the source side. Through the PLSM module, we can have four monitoring events by using two local detectors and then precisely estimate the bounds of source distributions. Specifically, we take the three-intensity decoy-state-based RFI-QKD for example for illustraing the events. Compared with the original RFI-QKD, our PLSM method can passively monitor the PND and has many advantages, with light source fluctuations, finite-size effects and reference frame deflection angles taken into account.

**Keywords:** quantum key distribution, reference frame independent, passive light source monitoring, finite-size effect

**PACS:** 03.67.Dd, 03.67.Hk, 42.50.–p, 03.67.–a **DOI:** 10.7498/aps.72.20230609

* Project supported by the National Key R&D Program of China (Grant No. 2018YFA0306400), the National Natural Science Foundation of China (Grant Nos. 12074194, 12104240), the Industrial Prospect and Key Core Technology Projects of Jiangsu Provincial Key R&D Program, China (Grant No. BE2022071), and the Natural Science Foundation of Jiangsu Province, China (Grant Nos. BK20192001, BK20210582).

† Corresponding author. E-mail: chz@njupt.edu.cn

物理学报 Acta Physica Sinica
Chinese Physical Society
Institute of Physics, CAS

# 基于被动式光源监控的参考系无关量子密钥分发

张佳一 陈华星 张桓毓 钱雪瑞 张春辉 王琴

# Reference-frame-independent quantum key distribution based on passive light source monitoring

Zhang Jia-Yi Chen Hua-Xing Zhang Huan-Yu Qian Xue-Rui Zhang Chun-Hui Wang Qin

引用信息 Citation: Acta Physica Sinica, 72, 150301 (2023) DOI: 10.7498/aps.72.20230609
在线阅读 View online: https://doi.org/10.7498/aps.72.20230609
当期内容 View table of contents: http://wulixb.iphy.ac.cn

---

**您可能感兴趣的其他文章**
**Articles you may be interested in**

参考系波动下的参考系无关测量设备无关量子密钥分发协议
Reference-frame-independent measurement-device-independent quantum key distribution under reference frame fluctuation
物理学报. 2019, 68(24): 240301 https://doi.org/10.7498/aps.68.20191364

基于混合编码的测量设备无关量子密钥分发的简单协议
A simple protocol for measuring device independent quantum key distribution based on hybrid encoding
物理学报. 2020, 69(19): 190301 https://doi.org/10.7498/aps.69.20200162

标记单光子源在量子密钥分发中的应用
Overview of applications of heralded single photon source in quantum key distribution
物理学报. 2022, 71(17): 170304 https://doi.org/10.7498/aps.71.20220344

一种基于标记单光子源的态制备误差容忍量子密钥分发协议
State preparation error tolerant quantum key distribution protocol based on heralded single photon source
物理学报. 2022, 71(3): 030301 https://doi.org/10.7498/aps.71.20211456

基于峰值补偿的连续变量量子密钥分发方案
Continuous-variable quantum key distribution based on peak-compensation
物理学报. 2021, 70(11): 110302 https://doi.org/10.7498/aps.70.20202073

基于实际探测器补偿的离散调制连续变量测量设备无关量子密钥分发方案
Discrete modulation continuous-variable measurement-device-independent quantum key distribution scheme based on realistic detector compensation
物理学报. 2022, 71(24): 240304 https://doi.org/10.7498/aps.71.20221072