基于监控标记单光子源的量子密钥分发协议*

罗一振[1)2)] 马洛嘉[1)2)] 孙铭烁[1)2)] 吴思睿[1)2)]
邱丽华[1)2)] 王禾[1)2)] 王琴[1)2)†]

1) (南京邮电大学, 量子信息技术研究所, 南京 210003)

2) (南京邮电大学, 宽带无线通信与传感网教育部重点实验室, 南京 210003)

(2024 年 9 月 9 日收到; 2024 年 11 月 9 日收到修改稿)

现有量子密钥分发系统的光源主要是弱相干态光源, 但是由于该类光源中含有大量的真空态脉冲, 并且在光源调制过程中可能存在一定信息泄漏, 从而限制了量子密钥分发系统的最远安全传输距离. 为克服这一局限, 本文提出了一种基于监控标记单光子源的量子密钥分发协议. 一方面, 通过借助标记单光子源中极低的真空态概率, 提升了系统的极限传输距离; 另一方面, 在系统发射端添加了 Hong-Ou-Mandel (HOM) 光源监控模块, 通过测量 HOM 干涉可见度的大小来精确刻画出源端可能泄漏信息量的大小, 从而更加准确地估算出系统可提取密钥率的大小. 此外, 将本工作与其他同类协议进行数值仿真对比, 仿真结果显示, 本协议在传输距离和密钥率等方面具有更加优越的性能. 因此, 本工作为未来发展更安全可靠的量子通信网络提供了重要的参考价值.

关键词: 量子密钥分发, Hong-Ou-Mandel 干涉, 光源监控, 标记单光子源

PACS: 03.67.Hk, 42.50.Ex, 42.79.Sz, 42.65.Lm **DOI**: 10.7498/aps.73.20241269

CSTR: 32037.14.aps.73.20241269

1 引 言

量子密钥分发 (quantum key distribution, QKD) 可以在合法的通信双方 Alice 和 Bob 之间形成安全的密钥, 从而为通信提供安全保障[1–3]. 从第一个 BB84 协议提出, QKD 到目前已经有 40 年的发展历程, 目前正在向更加安全、可靠的方向发展[4–7]. 然而, 在实际 QKD 系统中不可避免地存在设备缺陷[8,9], 比如: 光源端通常使用强度调制器和相位调制器来制备不同的量子态和不同强度的诱骗态脉冲, 由于相位调制器和强度调制器等器件存在一定缺陷, 导致产生的量子态或诱骗态在更高维度存在一定可区分性, 从而产生侧信道漏洞[10–12], 窃听者可以对这些侧信道漏洞进行相应的攻击, 进而威胁 QKD 系统的实际安全性. 此外, 现有大多数量子通信系统中使用的光源是弱相干态光源 (weak coherent source, WCS), 该光源服从泊松分布, 包含相当比例的真空态脉冲. 由于真空态脉冲在远距离时会对系统误码率产生重要影响, 因而使得该系统的最远安全传输距离受限.

另一方面, 标记单光子源 (heralded single-photon source, HSPS) 是一种重要的量子光源[13–17], 在量子通信、量子计算等领域具有广泛的应用前景. 在此前的研究中有学者提出过一种基于监控 WCS 的 QKD 方案来解决源端设备不完美的问题[18], 但

* 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)、江苏省自然科学基金前沿技术项目 (批准号: BK20192001)、国家自然科学基金 (批准号: 12074194) 和江苏省研究生科研创新计划项目 (批准号: KYCX22_0954) 资助的课题.

† 通信作者. E-mail: qinw@njupt.edu.cn

© 2024 中国物理学会 Chinese Physical Society

是只考虑了不同基矢之间的可区分性, 而忽略了信号态和诱骗态的可区分性, 此外, 由于受 WCS 本身性质的限制, 该工作还存在远距离处系统误码率急剧上升导致密钥传输距离受限等问题. 为了解决以上问题, 本文提出了一种基于监控标记单光子源的 QKD 协议. 该协议主要在标记单光子源调制过程中设置光源监测模块, 通过测量 Hong-Ou-Mandel (HOM) 干涉可见度大小来实时监控光源调制过程中可能产生的信息泄漏大小[18], 从而保障 QKD 系统的源端安全性. 此外, 通过借助标记单光子源的标记特性, 降低真空脉冲对探测端暗计数率的影响, 从而提升 QKD 系统在远距离处的性能.

2 理论模型分析与计算方法

图 1 为本协议的主要实验装置结构示意图, 该装置主要包括发送端 (Alice) 与接收端 (Bob) 两部分, 其中发送端主要包括参量光源、编码器 (encoder)、光开关 (optical switching, OS)、本地探测器 (avalanche photodiode, APD1), 以及光源监测模块; 接收端主要包括编码器 (decoder) 和单光子探测器 (APD4). 首先, 激光源发射一束激光经过一块Ⅱ型周期极化铌酸锂晶体 (periodically poled LiNbO3, PPLN), 以一定概率发生自发参量下转换 (spontaneous parametric down-conversion, SPDC) 过程, 产生关联光子对, 经过偏振分束器 (polarization beam splitter, PBS) 之后分别进入上下两路, 分别称为信号光和闲置光. 信号光经过强度调制器 (IM) 被随机调制成 3 种不同的强度 $(\mu,\nu,0)$, 其中 μ 为信号光强度, ν 和 0 为诱骗态强度; 随后进入 Encoder 进行编码调制, 经过调制后到达光开关; OS1 可以将信号光送入光纤信道发送给 Bob, 或者送入光源监控模块; OS2 可以将闲置光送入本地单光子探测器 (APD1), 或者送入光源监控模块; 这里光源监控模块主要由一个光延时器 (optical delay, OD)、一个偏振旋转器 (polarization rotator, PR)、一个分束器 (beam splitter, BS), 以及两个单光子探测器 (APD2 和 APD3) 组成.

QKD 系统在工作过程中主要包括密钥分发和光源监控两种工作模式. 在系统实施密钥分发模式时, 发送者控制 OS1 和 OS2, 分别将信号光和闲置光送入光纤信道和本地单光子探测器 (APD1), 由于信号光和闲置光的光子数服从相同的概率分布, 且具有同时性, 可以通过探测闲置光来精确标记信号光的到达时间, 从而控制接收端探测器的打开时间, 进而降低信号光中的真空态脉冲对暗计数率的影响. 另一方面, 为了实施光源监控模式, 发送者随机选取一段时间控制 OS1 和 OS2, 将信号光和闲置光同时引入光源监测模块, 通过检测信号光和闲置光之间 HOM 干涉大小来估算信号光在调制过程中可能产生的侧信道信息泄漏大小.

下文介绍基于监控标记单光子源的量子密钥分发协议的密钥率估计方法. 这里假定参量下转换光源的光子数分布服从泊松分布[19], 则产生标记单光子源的光子数分布为

$$P_n^{\lambda}=[1-(1-d_{\rm A})(1-\eta_{\rm A})^n]\frac{\lambda^n}{n!}{\rm e}^{-\lambda},$$

其中 n 代表光子数, λ 代表每个时间窗口的平均光强, $d_{\rm A}$ 和 $\eta_{\rm A}$ 分别代表本底单光子探测器 APD1 的暗计数率和探测效率.

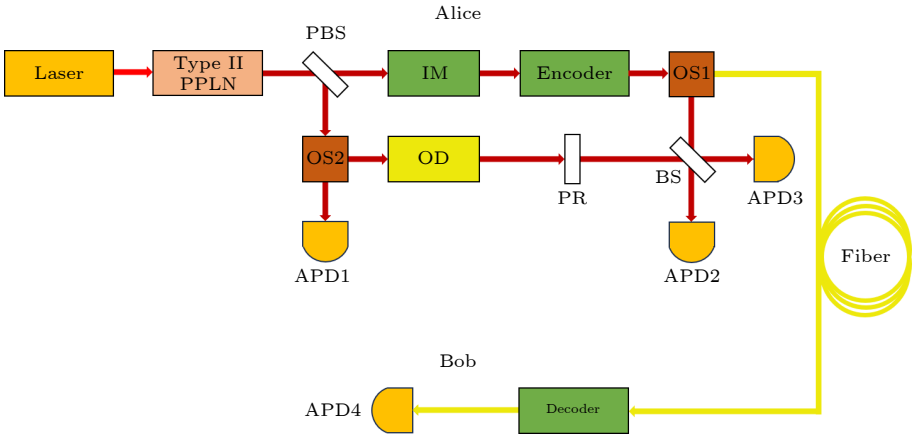

图 1 基于监控标记单光子源的 QKD 实验装置结构示意图

Fig. 1. Schematic diagram of QKD experimental device structure based on monitoring marker single photon source.

在发射端对信号光进行量子态制备和诱骗态调制过程中, 由于设备存在缺陷, 可能产生侧信道漏洞, 进而泄漏信息给 Eve 来区分信号态和诱骗态. 因此, 需要建立一个能够容忍这种侧信道的通用安全模型, 为此引入可区分度参数 $D_{\omega\omega'}$ ($\omega,\omega'\in\{\mu,\nu,0\}$), 以刻画诱骗态 ω 与 ω' 之间的差异大小, 根据信道透过率 Y_n^{ω} 和误码率 e_n^{ω} 与可区分度 $D_{\omega\omega'}$ 的关系, 建立可区分度 $D_{\mu\nu}$ 与保真度 $F(\hat{\rho}_x,\hat{\rho}_z)$ 之间的关系[8,20]: $D_{\mu\nu}=\sqrt{1-F(\hat{\rho}_x,\hat{\rho}_z)}$.

首先, 结合三强度诱骗态方法[21,22]可以得到单光子透过率 Y_1^{μ} 和单光子误码率 e_1^{μ} 的表达式:

$$\begin{aligned}Y_1^{\mu}\geqslant&\frac{\mu}{(\mu\nu-\nu^2)\left[1-(1-d_{\rm A})(1-\eta_{\rm A})\right]}\\&\times\left\{e^{\nu}Q_{\nu}^{\rm L}-\frac{\nu^2}{\mu^2}e^{\mu}Q_{\mu}^{\rm U}-\frac{d_{\rm A}\left(\mu^2-\nu^2\right)}{\mu^2}Y_0^{\rm U}\right.\\&\left.-D_{\mu\nu}\left(e^{\nu}-1\right)+D_{\mu\nu}(1-d_{\rm A})[e^{\nu(1-\eta_{\rm A})}-1]\right\},\end{aligned}\tag{1}$$

$$e_1^{\mu}\leqslant\min\{K^{\mu},K^{\nu},K^{\mu\nu}\}.\tag{2}$$

其中,

$$K^{\mu}=\frac{1}{P_1^{\mu}Y_1^{\mu}}(Q_{\mu}E_{\mu}-e_0Y_0^{\rm L}P_0^{\mu}),$$

$$K^{\nu}=\frac{1}{\nu Y_1^{\mu}}(e^{\nu}Q_{\nu}E_{\nu}-e_0Y_0^{\rm L}+\nu D_{\mu\nu}),$$

$$\begin{aligned}K^{\mu\nu}=&\frac{1}{(P_1^{\mu}-P_1^{\nu})Y_1^{\mu}}\left[Q_{\mu}E_{\mu}-Q_{\nu}E_{\nu}\right.\\&\left.-e_0Y_0^{\rm L}(P_0^{\mu}-P_0^{\nu})+D_{\mu\nu}(1-P_0^{\nu})\right],\end{aligned}$$

Q_{λ} 和 E_{λ} 分别代表强度为 λ 的光脉冲产生的平均增益和平均量子比特误码率 (简称平均误码率), $Q_{\lambda}=\sum_{n=0}^{\infty}P_n^{\lambda}Y_n^{\lambda}$, $E_{\lambda}Q_{\lambda}=\sum_{n=0}^{\infty}P_n^{\lambda}Y_n^{\lambda}e_n^{\lambda}$; Y_n^{λ} 和 e_n^{λ} 分别代表强度为 λ 的光脉冲中 n 光子态的透过率和误码率, 这里 $\lambda\in\{\mu,\nu,0\}$, 上角标 L 和 U 分别代表考虑统计起伏效应之后的下界和上界值, 本文在分析中采用了高斯分析法来估算统计起伏带来的影响[23].

其次, 为了表征光源监测模块中光子的不可区分性, 将 HOM 干涉的干涉可见度定义为最大和最小符合计数的差值除以最大符合计数, 完全正交时, 干涉可见度等于 0, 而在完全不可区分的情况下, 干涉可见度等于 1. 理想情况下, 攻击者 Eve 无法区分 Z 基和 X 基, 因为它们的密度矩阵相同; 不完美的模式匹配导致不同基的密度矩阵存在差异, 从而产生漏洞, Eve 可以利用该漏洞对 QKD 设备进行攻击. 用于量化这种影响的参数被称为基矢失配误差: $\Delta=\dfrac{1-\sqrt{F(\hat{\rho}_x,\hat{\rho}_z)}}{2}$ [24], 其中 $\hat{\rho}_x$ 和 $\hat{\rho}_z$ 分别是 X 基和 Z 基的密度矩阵, $F(\hat{\rho}_x,\hat{\rho}_z)$ 是 X 基和 Z 基密度矩阵之间的保真度. 干涉可见度和保真度之间存在如下关系:

$$\sqrt{F(\hat{\rho}_1,\hat{\rho}_2)}=\mathrm{e}^{\mu(\sqrt{2V}-1)},\tag{3}$$

其中, V 代表 $\hat{\rho}_1$和$\hat{\rho}_2$ 之间的干涉可见度. 由 (3) 式可以得出干涉可见度与基矢失配误差之间的关系:

$$\begin{aligned}&1-2\Delta\geqslant\\&\cos\left(2\arccos\frac{1+\mathrm{e}^{\mu(\sqrt{2V}-1)}}{2}+\arccos\mathrm{e}^{\mu(\sqrt{2V}-1)}\right).\end{aligned}\tag{4}$$

为了模拟基矢失配误差的影响, 考虑到 Eve 具有使用无损信道的能力, 可以将基矢失配误差修正为 $\Delta'=\Delta/Y_1^{\mu}$, 进而得到修正后的单光子误码率 $e_1^{\mu'}$:

$$\begin{aligned}e_1^{\mu'}=&4\left(1-\Delta'\right)\Delta'\left(1-2e_1^{\mu}\right)+4\left(1-2\Delta'\right)\\&\times\sqrt{\Delta'\left(1-\Delta'\right)e_1^{\mu}\left(1-e_1^{\mu}\right)}+e_1^{\mu}.\end{aligned}\tag{5}$$

接着, 将以上单光子透过率 Y_1^{μ} 和修正后的单光子误码率 $e_1^{\mu'}$ 代入下面密钥率公式, 得到最终的安全密钥率:

$$R\geqslant q\{-Q_{\mu}H_2(E_{\mu})f(E_{\mu})+P_1^{\mu}Y_1^{\mu}[1-H_2(e_1^{\mu'})]\},\tag{6}$$

其中, q 是对基成功因子, 取值 1/2; $f\left(E_{\mu}\right)$ 表示纠错效率, 取值 1.16; $H_2\left(x\right)$ 为二进制熵函数, $H_2\left(x\right)=-x\log_2x-(1-x)\log_2(1-x)$.

3 数值分析及仿真结果讨论

本文在仿真过程中使用的系统参数如表 1 所列[16]. 其中 N 代表 Alice 发送的总脉冲数; α 代表信道损耗系数; $d_{\rm A}$ 和 $\eta_{\rm A}$ 分别代表 Alice 端单光子探测器的暗计数率和探测效率; Y_0 和 $\eta_{\rm B}$ 分别表 Bob 端的探测器的暗计数率和探测效率; $e_{\rm d}$ 代表系统的光学本底误差大小. 在相同的实验条件下, 比较了本文提出的基于监控标记单光子源的量子密钥分发协议和基于监控弱相干态光源的协议在安全密钥率和误码率方面的区别, 为了方便对不同光源的干涉可见度进行比较, 定义一个参数来量化实际干涉可见度与理想干涉可见度之间的相对差别, 即干涉误差 (P), 其表达式为 $P:=|V_0-V|/V_0$, 其中 V_0 为理想情况下的干涉可见度 (对于 HSPS,

$V_0=1$; 对于 WCS, $V_0=0.5$), 仿真结果如图 2—图 4 所示.

表 1 基于监控标记单光子源的量子密钥分发协议仿真使用的参数列表

Table 1. List of the parameters used in the source monitoring quantum key distribution protocol based on heralded single photon source.

N	α/(dB·km^{-1})	$d_{\rm A}$	$\eta_{\rm A}$	Y_0	$e_{\rm d}$	$\eta_{\rm B}$
10^{10}	0.2	10^{-6}	0.75	6.02×10^{-6}	0.015	0.145

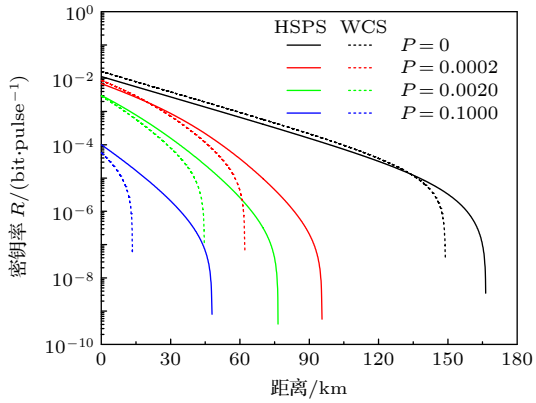

图 2 不同干涉误差下基于监控 HSPS 协议和基于监控 WCS 协议的密钥率对比

Fig. 2. Comparison of the key rates based on monitoring HSPS protocol and monitoring WCS protocol under different interference errors.

图 2 代表基于监控 HSPS 的协议和基于监控 WCS 的协议在不同干涉误差下密钥密钥率 R 随传输距离的变化情况对比. 从图 2 可以看出, 在理想干涉可见度 ($P=0$) 下, 即光源不存在侧信道信息泄漏时, 基于监控 WCS 的协议在近距离处 (<120 km) 的密钥成码率较高, 主要由于基于 HSPS 的协议中所用的本地探测器的探测效率小于 1, 从而影响了其平均计数率; 而在远距离处 (>140 km), 基于监控 HSPS 的协议显示出更远的安全传输距离和更高的密钥率, 主要由于远距离处的误码率主要来自于暗计数率, 而 HSPS 包含极低的暗计数率, 从而在远距离处显示出优势. 当光源存在侧信道信息泄漏时, 即干涉误差大于 0[12,25], 随着干涉误差的增大, 两类协议的传输距离和密钥率都会下降, 但基于监控 WCS 的协议受干涉误差的影响程度更加明显, 不但其传输距离急剧减小, 而且在近距离处的密钥率也迅速下降, 比如当干涉误差 $P=0.1$ 时, 其传输距离和密钥率都明显劣于基于监控 HSPS 的协议.

图 3 所示为基于监控 HSPS 的协议和基于监控 WCS 的协议在不同干涉误差下信号光平均误码率 E_μ 随传输距离的变化曲线对比. 在固定的干涉误差下, 后者的 E_μ 随着传输距离增大而急剧增大, 且干涉误差越大, 上升趋势越剧烈; 而前者的平均误码率一直保持在相对稳定的数值, 在 60 km 之后才出现小幅度上升, 其原因与前面对密钥率变化趋势的解释一致.

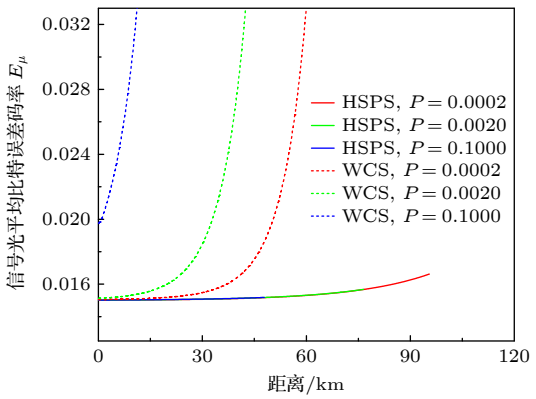

图 3 不同干涉误差下基于监控 HSPS 协议和基于监控 WCS 协议的平均误码率对比

Fig. 3. Comparison of the average bit error rates between monitoring HSPS protocol and monitoring WCS protocol under different interference errors.

图 4 所示为基于监控 HSPS 的协议和基于监控 WCS 的协议在不同干涉误差下信号光的平均增益 Q_μ 随传输距离的变化曲线对比. 首先, 两种协议中信号光平均增益 Q_μ 均随着传输距离的增大而降低, 不过后者的曲线下降速度更快, 因而前者与后者相比具有更高的密钥率和安全传输距离.

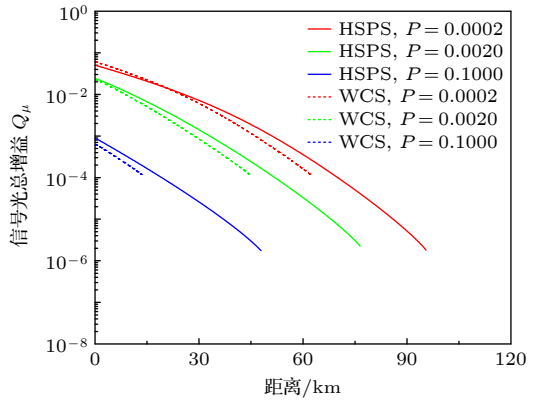

图 4 不同干涉误差下基于监控 HSPS 协议和基于监控 WCS 协议的信号光平均增益对比

Fig. 4. Comparison of the average gain of signal light between monitoring HSPS protocol and monitoring WCS protocol under different interference errors.

4 结 论

本文提出了一种基于监控 HSPS 的量子密钥分发协议, 该协议通过在量子密钥分发过程中随机抽取一段时间监控信号光与闲置光之间的 HOM 干涉可见度来估算光源中可能存在的信息泄漏大小, 进而对密钥率大小做出更准确的估算, 从而保证了量子密钥的安全性和保密性. 此外, 相关数值仿真计算结果显示, 在相同的实验条件下, 基于监控 HSPS 的协议比基于监控 WCS 的协议具有更远的安全传输距离和密钥率, 尤其在干涉误差较大时, 前者的优势更加明显. 此外, 本方案原则上可以和其他 QKD 协议, 比如测量设备无关类 QKD 协议[16,17,26] 相结合, 进一步提升系统的安全性和实用性, 从而为未来 QKD 系统的大规模应用提供重要的参考价值.

参考文献

[1] Bennett C H, Brassard G 1984 *Proceedings of IEEE International Conference on Computers, System and Signal Processing* (Vol. 1 of 3) (Bangalore: IEEE) p175

[2] Shannon C E 1949 *Bell Syst. Tech. J.* **28** 656

[3] Bennett C H, Brassard G, Mermin N D 1992 *Phys. Rev. Lett.* **68** 557

[4] Lo H K, Curty M, Qi B 2012 *Phys. Rev. Lett.* **108** 130503

[5] Lucamarini M, Yuan Z L, Dynes J F, Shields A J 2018 *Nature* **557** 400

[6] Zeng P, Zhou H Y, Wu W J, Ma X F 2022 *Nat. Commun.* **13** 3903

[7] Xie Y M, Lu Y S, Weng C X, Cao X Y, Jia Z Y, Bao Y, Wang Y, Fu Yao, Yin H L, Chen Z B 2022 *PRX Quantum* **3** 020315

[8] Tamaki K, Curty M, Lucamarini M 2016 *New J. Phys.* **18** 065008

[9] Xu F H, Wei K J, Sajeed S, Kaiser S, Sun S, Tang Z Y, Qian L, Makarov V, Lo H K 2015 *Phys. Rev. A* **92** 032305

[10] Sun S H, Gao M, Jiang M S, Li C Y, Liang L M 2012 *Phys. Rev. A* **85** 032304

[11] Nauerth S, Fürst M, Schmitt-Manderbach T, Weier H, Weinfurter H 2009 *New J. Phys.* **11** 065001

[12] Comandar L, Lucamarini M, Fröhlich B, Dynes J F, Yuan Z L, Shields A J 2016 *Opt. Express* **24** 17849

[13] Mauerer W, Avenhaus, Helwig W, Silberhorn C 2009 *Phys. Rev. A* **80** 053815

[14] Faruque I I, Sinclair G F, Bonneau D, Ono T, Silberhorn C, Thompson M G, Rarity J G 2019 *Phys. Rev. Appl.* **12** 054029

[15] Wang J, Zhang C H, Liu J Y, Qian X R, Li J, Wang Q 2021 *Chin. Phys. B* **30** 070304

[16] Zhou X Y, Zhang C H, Zhang C M, Wang Q 2017 *Phys. Rev. A* **96** 052337

[17] Zhang C H, Zhang C M, Wang Q 2019 *Phys. Rev. A* **99** 052325

[18] Alexander D, Denis S 2021 *Phys. Rev. A* **104** 012601

[19] Wang Q, Wang X B, Guo G C 2007 *Phys. Rev. A* **75** 012312

[20] Ma Z, Zhang F L, Chen J L 2009 *Phys. Lett. A* **373** 3407

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

[22] Lo H K, Ma X F, Chen K 2005 *Phys. Rev. Lett.* **94** 230504

[23] Tomamichel M, Lim C C W, Gisin N, Renner R 2012 *Nat. Commun.* **3** 634

[24] Lucamarini M, Choi I, Ward M B, Dynes J F, Yuan Z L, Shields A J 2015 *Phys. Rev. X* **5** 031030

[25] Sun M S, Wang W L, Zhou X Y, Zhang C H, Wang Q 2023 *Phys. Rev. Res.* **5** 043179

[26] Zhan X H, Zhong Z Q, Wang S, Yin Z Q, Chen W, He D Y, Guo G C, Han Z F 2023 *Phys. Rev. Appl.* **20** 034069

Source monitoring quantum key distribution protocol based on heralded single photon source*

Luo Yi-Zhen [1)2)] Ma Luo-Jia [1)2)] Sun Ming-Shuo [1)2)] Wu Si-Rui [1)2)]
Qiu Li-Hua [1)2)] Wang He [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 of Ministry of Education, Nanjing University of Posts and Telecommunications, Nanjing* 210003, *China*)

(Received 9 September 2024; revised manuscript received 9 November 2024)

Abstract

The security of quantum key distribution (QKD) is based on the basic principles of quantum mechanics, and therefore has unconditional security in theory. In existing quantum key distribution systems, weakly coherent sources (WCSs) are often used as light sources due to a high probability of vacuum pulses in these sources, resulting in limited transmission distances. Besides, there inevitably exist equipment defects in actual QKD systems, such as certain defects in phase modulators and intensity modulators, which lead to distinguishability of quantum states in higher dimensions and result in side-channel vulnerabilities. An eavesdropper can carry out corresponding attacks, thereby threatening the actual security of QKD systems. To overcome the above limitations, we propose an improved protocol on quantum key distribution based on monitoring heralded single-photon sources. Due to the simultaneity of parametric down-conversion photon pairs, we can accurately predict the arrival of one photon by measuring the arrival time of another photon. Through this way, we can greatly reduce the probability of vacuum states in the signal light, and increase the longest transmission distance of the QKD system. Moreover, a light source monitoring module is inserted into the sender's side. By randomly selecting a certain period of time through the source monitoring module to measure the Hong-Ou-Mandel interference between the signal light and the idle light , we can estimate the side-channel information leakage of the source and then obtain the key generation rate.

Compared with the QKD protocol based on monitoring weak coherent sources, our present protocol can give a better performance in either the transmission distance or the key generation rate, especially when the interference error is large. In addition, in principle, our present protocol can also be extended to other quantum key distribution protocols, such as the measurement-device-independent protocols, to further improve the security and practicability of QKD systems. Therefore, our present work can provide valuable references for realizing the large-scale application of quantum communication networks in the near future.

Keywords: quantum key distribution, Hong-Ou-Mandel interference, source monitoring, heralded single-photon source

PACS: 03.67.Hk, 42.50.Ex, 42.79.Sz, 42.65.Lm **DOI:** 10.7498/aps.73.20241269

CSTR: 32037.14.aps.73.20241269

* Project supported by the Industrial Prospect and Key Core Technology Projects of Key R & D Program of Jiangsu Province, China (Grant No. BE2022071), the Leading-edge Technology Program of the Natural Science Foundation of Jiangsu Province, China (Grant No. BK20192001), the National Natural Science Foundation of China (Grant No. 12074194), and the Postgraduate Research & Practice Innovation Program of Jiangsu Province, China (Grant No. KYCX22_0954).

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

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

基于监控标记单光子源的量子密钥分发协议

罗一振 马洛嘉 孙铭烁 吴思睿 邱丽华 王禾 王琴

Source monitoring quantum key distribution protocol based on heralded single photon source

Luo Yi-Zhen Ma Luo-Jia Sun Ming-Shuo Wu Si-Rui Qiu Li-Hua Wang He Wang Qin

引用信息 Citation: Acta Physica Sinica, 73, 240302 (2024) DOI: 10.7498/aps.73.20241269
在线阅读 View online: https://doi.org/10.7498/aps.73.20241269
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

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

基于被动式光源监控的参考系无关量子密钥分发
Reference-frame-independent quantum key distribution based on passive light source monitoring
物理学报. 2023, 72(15): 150301 https://doi.org/10.7498/aps.72.20230609

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

纠缠光子对的级联Hong-Ou-Mandel干涉研究及其在多时延参数测量中的应用
Cascaded Hong-Ou-Mandel interference of entangled photon pairs and its application in multiple delay parameters measurement
物理学报. 2021, 70(12): 120302 https://doi.org/10.7498/aps.70.20210071

实用化态制备误差容忍参考系无关量子密钥分发协议
Study of practical state-preparation error tolerant reference-frame-independent quantum key distribution protocol
物理学报. 2023, 72(24): 240301 https://doi.org/10.7498/aps.72.20231144