基于双参数扫描的量子存储辅助测量设备无关量子密钥分发协议*

刘畅[1)2)#] 孙铭烁[1)2)#] 罗一振[1)2)] 董书言[1)2)] 张春辉[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)

(2025 年 8 月 29 日收到; 2025 年 10 月 23 日收到修改稿)

基于量子存储辅助的测量设备无关量子密钥分发 (MDI-QKD) 协议原理上能有效提升量子密钥分发系统的传输距离和密钥率, 但现有三强度诱骗态方案受有限长效应影响严重, 仍存在密钥率低、安全传输距离受限等问题. 针对以上问题, 本文提出了一种基于双参数扫描的量子存储辅助 MDI-QKD 协议, 一方面, 通过使用四强度诱骗态方法降低有限长效应的影响; 另一方面, 结合集体约束模型与双参数扫描算法来优化有限样本下的单光子计数率和相位误码率的估算精度, 从而有效提升系统的整体性能. 同时, 本文开展了相关数值仿真计算, 仿真结果显示, 本方案与现有其他同类 MDI-QKD 方案, 比如基于存储辅助的三强度诱骗态方案以及不使用存储的四强度诱骗态方案相比, 在相同的实验条件下, 分别提升了超过 30 km 和 100 km 的安全传输距离. 因此, 本文工作将为未来发展远距离量子通信网络提供重要的参考价值.

关键词: 量子密钥分发, 量子存储, 双参数扫描, 集体约束

DOI: 10.7498/aps.75.20251171 **CSTR:** 32037.14.aps.75.20251171

1 引 言

BB84 协议作为最早且最具代表性的量子密钥分发 (QKD) 协议[1], 在理想条件下可以实现合法通信双方 Alice 与 Bob 之间的无条件安全性. 然而, 实际的物理实现不可避免地受到态制备误差、信道损耗与噪声、探测器灵敏度有限等非理想因素的影响, 使得潜在的窃听者 (Eve) 能够利用漏洞对系统进行攻击, 从而导致协议安全性下降. 与传统 QKD 协议相比, 测量设备无关协议 (MDI-QKD)[2] 通过将易受攻击的测量过程交由不可信第三方 Charlie 执行, 从根本上消除了测量端可能存在的侧信道漏洞, 显著提高了量子密钥分发系统的整体安全性, 目前已有众多 MDI-QKD 方案和实验被提出并得到验证[3–6].

然而, 由于 MDI-QKD 协议需要 Charlie 同时接收到从 Alice 和 Bob 发送的光子以完成贝尔态测量 (BSM), 因此对信道损耗敏感, 导致密钥率较低且传输距离受限. 为了解决这一问题, 研究人员提出了存储辅助的初步方案: 在测量端部署量子存储器 (QM) 用以存储较早到达的光子, 等到另外一个光子也到达时将两者同时释放出来, 从而有效提升双光子符合概率[7–12]. 然而, 这些方案大多没有考虑光子数分离 (PNS) 攻击, 并做出了一些理想化假设, Sun 等[13] 提出了基于三强度诱骗态方法

* 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) 和国家自然科学基金 (批准号: 62471248, 12074194) 资助的课题.

同等贡献作者.

† 通信作者. E-mail: qinw@njupt.edu.cn

的存储辅助 MDI-QKD 协议, 在不考虑有限长效应的情况下, 有效提升了 MDI-QKD 协议的性能. 但是在有限长效应下, 该方案仍存在密钥率低、传输距离有限的问题. 为了解决上述问题, 本文在 Sun 等[13] 以及 Jiang 等[5] 的工作基础上提出一种基于双参数扫描的量子存储辅助 MDI-QKD 协议. 通过对存储辅助模型引入集体约束模型与双参数扫描算法, 对系统误差计数和真空相关计数进行联合估计和优化, 有效抑制了有限样本带来的统计误差, 从而能够对单光子脉冲对计数率的下界和相位翻转错误率的上界进行更准确的估计, 进而提升系统的整体性能.

2 理论模型分析与计算方法

图 1 为本协议所采用的主要实验装置结构示意图. 该系统由通信双方 Alice 与 Bob 及一个不可信的第三方 Charlie 构成. Alice 和 Bob 分别独立产生标记单光子源 (HSPS), 并将所生成的单光子脉冲发送至 Charlie 端进行贝尔态测量 (BSM). HSPS 的光子数分布可以根据不同的实验条件采用不同模型[14]. 本方案以热分布为例进行仿真分析, 即

$$P_{\mu}^{n}=\frac{\mu^{n}}{(1+\mu)^{n+1}}.$$

式中, n 表示光子个数, μ 表示每个脉冲包含的平均光子数.

在发送端使用强度调制器 (IM_1) 将激光器 (Laser) 的泵浦光调制为 4 种不同的强度 $(\mu,\nu,\omega,0)$, μ 表示信号态, $\nu,\omega,0$ 表示诱骗态. 当泵浦光入射到泵浦非线性晶体 (NC) 时, 发生参量下转换生成信号光子 (S) 和闲置光子 (I). 随后通过二向色镜分离, 闲置光子 (I) 被送入本地探测器 (D_0), 而信号光子 (S) 则被收集到编码模块 (encoding) 用于编码不同的量子态. 本方案采用法拉第-迈克耳孙干涉仪 (FMI) 来实现时间戳-相位编码[12,15]. 该编码器具有装置成熟, 切换不同量子态的速度快, 以及前后时间戳脉冲之间的距离可以自由设计等优点.

QM 模块主要由泡克耳斯盒 (PC)[16]、偏振光束分离器 (PBS) 以及反射镜组成. PC 具有两种工作状态: 在“关闭”状态下不施加电压, 入射脉冲的偏振态保持不变; 在“开启”状态下施加高压脉冲, 可使入射光的偏振态发生反转. PC 初始保持在“关闭”状态. 当 Alice/Bob 其中一侧的信号光脉冲较早达到 QM 模块, 且对应休闲光脉冲被本地探测器检测后触发 PC, PC 迅速切换为“开启”, 将该脉冲的偏振态翻转, 使其在 PBS 与反射镜组成的闭合光学路径中被存储; 随后, PC 迅速复位为“关闭”. 当后一个脉冲到达并被本地探测器触发时, PC 再次“开启”, 将之前被存储的脉冲恢复为初始

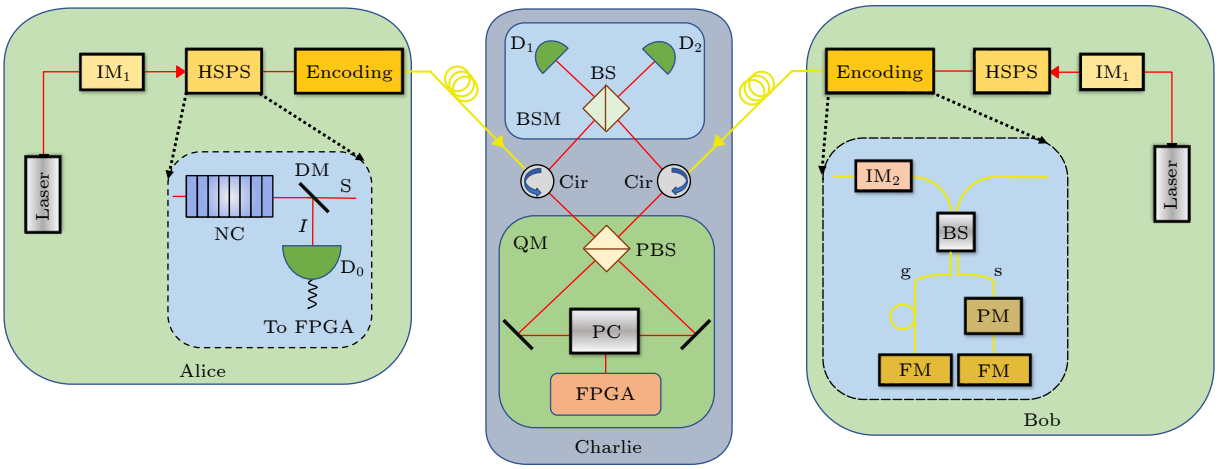

图 1 基于量子存储辅助的 MDI-QKD 系统装置示意图, 其中 IM 为强度调制器, NC 为非线性晶体, DM 为二色镜, PM 为相位调制器, FM 为法拉第反射镜, Cir 为环形器, D_0, D_1, D_2 为单光子探测器, PC 为泡克耳斯盒, BS 为光束分离器, PBS 为偏振光束分离器, BSM 代表贝尔态测量装置, FPGA 代表现场可编程逻辑门阵列

Fig. 1. Schematic diagram of a quantum memory-assisted MDI-QKD system, where IM represents intensity modulator, NC represents nonlinear crystal, DM represents dichroic mirror, PM represents phase modulator, FM represents Faraday mirror, Cir represents circulator, D_0, D_1, D_2 represent single-photon detectors, PC represents pockels cell, BS represents beam splitter, PBS represents polarization beam splitter, BSM represents Bell-state measurement device, FPGA represents field programmable gate array.

偏振态, 实现两个脉冲在时间域的同步释放, 并送入 BSM 模块执行贝尔态测量. 投影测量的成功概率可以写成[17]:

$$P_{\rm suc}^{k_{\rm A},k_{\rm B}} = P_{\rm l}(k_{\rm A}|1)P_{\rm l}(k_{\rm B}|1)+\sum_{j=2}^{M}\big[P_{\rm l}(k_{\rm A}|j)P_{\rm e}(k_{\rm B}|j) + P_{\rm l}(k_{\rm B}|j)P_{\rm e}(k_{\rm A}|j)+P_{\rm l}(k_{\rm A}|j)P_{\rm l}(k_{\rm B}|j)\big], \tag{1}$$

其中, M 表示 QM 进行量子态存储操作的存储轮数; $P_{\rm l}(k|j)$ 表示一个 HSPS 在第 j 个时隙中恰好成功发送出 k 个单光子的概率, $P_{\rm e}(k|j)$ 表示在第 j 个时隙中, 从前 $j-1$ 个时隙成功储存并发射出 k 个光子的概率. 详细公式可见附录 A.

在光脉冲被成功存入和读出 QM 的过程中, 量子态的保真度 $F\approx 1-e_{\rm d}$, 其中 $e_{\rm d}$ 表示光学系统的本底误码[13]. 详细解释可见附录 B.

本存储辅助 MDI-QKD 协议中, 系统的增益 $S_{x_{\rm A},y_{\rm B}}^{K}$ 和误码率 $E_{x_{\rm A},y_{\rm B}}^{K}$ 满足[13,18,19]:

$$S_{x_{\rm A},y_{\rm B}}^{K} = \sum_{k_1,k_2}\left[q_{\rm W}^{K,x_{\rm A},y_{\rm B}}(k_{\rm A},k_{\rm B})+q_{\rm C}^{K,x_{\rm A},y_{\rm B}}(k_{\rm A},k_{\rm B})\right], \tag{2}$$

$$E_{x_{\rm A},y_{\rm B}}^{K} = e_{\rm d}\left(1-2\tilde{E}_{x_{\rm A},y_{\rm B}}^{K}\right)+\tilde{E}_{x_{\rm A},y_{\rm B}}^{K}, \tag{3}$$

$$\tilde{E}_{x_{\rm A},y_{\rm B}}^{K} = \frac{\sum\limits_{k_1,k_2} q_{\rm W}^{K,x_A,y_B}(k_{\rm A},k_{\rm B})}{\sum\limits_{k_1,k_2}\left[q_{\rm W}^{K,x_A,y_B}(k_{\rm A},k_{\rm B})+q_{\rm C}^{K,x_{\rm A},y_{\rm B}}(k_{\rm A},k_{\rm B})\right]}, \tag{4}$$

其中, Alice(Bob) 以强度 $x_{\rm A}$ ($y_{\rm B}$) ($x_{\rm A},y_{\rm B}\in\{0,\omega,\nu\}$) 发送 $k_{\rm A}$ ($k_{\rm B}$) 光子脉冲时, 在 K ($K\in\{Z,X\}$) 基下各种“正确事件”和“错误事件”的条件概率分别为

$$q_{\rm W}^{K,x,y}(k_{\rm A},k_{\rm B}) = P_{\rm suc}^{k_{\rm A},k_{\rm B}}P_{\rm W}^{K,k_{\rm A},k_{\rm B}},$$

$$q_{\rm C}^{K,x,y}(k_{\rm A},k_{\rm B}) = P_{\rm suc}^{k_{\rm A},k_{\rm B}}P_{\rm C}^{K,k_{\rm A},k_{\rm B}}.$$

$P_{\rm W}^{K,k_{\rm A},k_{\rm B}}$ ($P_{\rm C}^{K,k_{\rm A},k_{\rm B}}$) 表示在探测器响应的条件下, 当 Alice 和 Bob 在 K 基下分别发送 $k_{\rm A}$, $k_{\rm B}$ 个光子的情况时, 事件为错误 (正确) 的条件概率.

基于 QM 的 MDI-QKD 协议与标准的 MDI-QKD 协议相比, 原理上提升了密钥率, 但是该协议仍然受有限长效应影响严重. 为了降低这种影响, 高效的优化算法尤为重要. 现有的单参数扫描方案只关注了单一参数的变化对结果的影响, 忽略了其他参数的关联性, 对关键物理参数的估计仍不够紧致, 对有限数据长度效应的抑制能力有限. 为此, 我们采用双参数扫描方法[5]: 首先确定两个关键参数系统误差计数 $\mathcal{M}$ 和真空相关计数 $\mathcal{H}$ 的合理物理区间, 然后同时对这两个参数进行扫描, 精准考量参数间联合作用对系统性能指标的综合影响, 有效规避参数间的孤立估算偏差, 抑制多参数波动的叠加干扰, 得到更为紧致且更贴合实际系统运行状态的边界条件, 最终得到更高精度的单光子对响应率的下界和单光子误码率的上界[5,20]:

$$Y_{11}^{X} \geqslant \langle Y_{11}^{X}\rangle^{\rm L} = \frac{\langle S_{+}\rangle^{\rm L}+P_{\nu}^{1}P_{\nu}^{2}\dfrac{\mathcal{M}}{N_{\omega\omega}}-\langle S_{-}\rangle^{\rm U}-P_{\nu}^{1}P_{\nu}^{2}\mathcal{H}}{P_{\nu}^{1}P_{\omega}^{1}(P_{\omega}^{2}P_{\nu}^{1}-P_{\omega}^{2}P_{\nu}^{1})}, \tag{5}$$

$$e_{11}^{X} \leqslant \langle e_{11}^{X}\rangle^{\rm U} = \frac{\mathcal{M}/N_{\omega\omega}-\mathcal{H}/2}{P_{\omega}^{1}P_{\omega}^{1}Y_{11}^{X,\rm L}}. \tag{6}$$

其中, 上标 L 和 U 表示下界和上界, $N_{x_{\rm A}y_{\rm B}}=p_{x_{\rm A}}p_{y_{\rm B}}N$ 表示 Alice 选择强度 $x_{\rm A}$、Bob 选择强度 $y_{\rm B}$ 的脉冲对个数; $p_{x_{\rm A}}$ ($p_{y_{\rm B}}$) 表示选基概率, 表示 Alice 或 Bob 发射端发送总光脉冲数.

同时, 为了降低统计误差影响, 更准确评估统计波动带来的不确定性, 更精确地得到 (5) 式和 (6) 式的估计值, 采用了联合估计技术[18]:

$$\langle S_{+}\rangle^{\rm L} := \mathbb{F}_{\rm L}\times \left(\frac{P_{\nu}^{1}P_{\nu}^{2}}{N_{\omega\omega}},\frac{P_{\omega}^{1}P_{\omega}^{2}P_{\nu}^{0}}{N_{o\nu}},\frac{P_{\omega}^{1}P_{\omega}^{2}P_{\nu}^{0}}{N_{\nu o}},\bar{m}_{\omega\omega},n_{o\nu},n_{\nu o},\xi^{\rm L},\xi^{\rm L},\xi^{\rm L}\right),$$

$$\langle S_{-}\rangle^{\rm U} := \mathbb{F}_{\rm U}\left(\frac{P_{\omega}^{1}P_{\omega}^{2}}{N_{\nu\nu}},\frac{P_{\omega}^{1}P_{\omega}^{2}P_{\nu}^{0}P_{\nu}^{0}}{N_{oo}},0,n_{\nu\nu},n_{oo},0,\xi^{\rm U},\xi^{\rm U},0\right).$$

$$\mathcal{H}^{\rm L} := \mathbb{F}_{\rm L}\left(\frac{P_{\omega}^{0}}{N_{o\omega}},\frac{P_{\omega}^{0}}{N_{\omega o}},0,n_{o\omega},n_{\omega o},0,\xi^{\rm L},\xi^{\rm L},0\right) - \frac{P_{\omega}^{0}P_{\omega}^{0}}{N_{oo}}\mathbb{E}^{\rm U}(n_{oo},\xi^{L}).\mathcal{M}^{\rm L} := \mathbb{E}^{\rm L}(m_{\omega\omega},\xi^{\rm L}),$$

$$\mathcal{H}^{\rm U} := \mathbb{F}_{\rm U}\left(\frac{P_{\omega}^{0}}{N_{o\omega}},\frac{P_{\omega}^{0}}{N_{\omega o}},0,n_{o\omega},n_{\omega o},0,\xi^{\rm U},\xi^{\rm U},0\right) - \frac{P_{\omega}^{0}P_{\omega}^{0}}{N_{oo}}\mathbb{E}^{\rm L}(n_{oo},\xi^{\rm U}).\mathcal{M}^{\rm U} := \mathbb{E}^{\rm U}(m_{\omega\omega},\xi^{\rm U}).$$

式中, 上标 L 和 U 表示下界和上界, $\mathbb{F}$ 表示计算上下界的函数, $\mathbb{E}$ 表示期望值函数[5], ξ 表示 Chernoff 界预先设定的失败概率. Alice 和 Bob 分别发送强度为 $x_{\rm A}$ 和 $y_{\rm B}$ 的光脉冲表示为

$$n_{x_{\rm A}y_{\rm B}} = N_{x_{\rm A}y_{\rm B}}\cdot S_{x_{\rm A},y_{\rm B}}^{K},$$

在测量端得到有效事件的计数值; 正确的有效事件

和错误的有效事件分别表示为

$$m_{x_{\rm A}y_{\rm B}} = N_{x_{\rm A}y_{\rm B}} \cdot E^{K}_{x_{\rm A},y_{\rm B}}$$

$$\overline{m}_{x_{\rm A}y_{\rm B}} = N_{x_{\rm A}y_{\rm B}} \cdot \left(S^{K}_{x_{\rm A},y_{\rm B}} - E^{K}_{x_{\rm A},y_{\rm B}}\right).$$

通过扫描每一组 $(\mathcal{H},\mathcal{M})$ 对密钥率函数进行优化, 可以得到最终的密钥生成率[5]:

$$\begin{aligned} R^{*} =& \min_{\substack{H\in[H^{\rm L},H^{\rm U}]\\ M\in[M^{\rm L},M^{\rm U}]}} R^{*}(\mathcal{H},\mathcal{M}) \\ =& p_{\mu}p_{\mu}\Big\{P^{1}_{\mu}P^{1}_{\mu}\left\langle Y^{X}_{11}\right\rangle^{\rm L}\left[1-H_2\left(\left\langle e^{X}_{11}\right\rangle^{\rm U}\right)\right] \\ & - fS^{Z}_{\mu,\mu}H_2(E^{Z}_{\mu,\mu})\Big\}, \end{aligned} \tag{7}$$

式中, f 为纠错效率; $H_2(x)$ 代表香农熵函数, 可写为

$$-x\log_2(x)-(1-x)\log_2(1-x).$$

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. 其中, Pd 和 $Pd_{\rm t}$ 表示测量部分和本地部分探测器的暗计数率; $e_{\rm d}$ 是光学系统的本底误码; $\eta_{\rm d}$ 和 $\eta_{\rm t}$ 分别表示测量部分和本地部分探测器的探测效率; f 是纠错效率; ξ 是统计波动分析中设定的失败概率; α 是光纤的损耗系数. 仿真结果如图 2—图 6 所示.

表 1 基于量子存储的四强度诱骗态 MDI-QKD 协议仿真使用的参数

Table 1. Simulation parameters used in the quantum-memory-based four-intensity decoy-state MDI-QKD protocol.

$e_{\rm d}$	Pd	$Pd_{\rm t}$	$\eta_{\rm d}$	$\eta_{\rm t}$	ξ	f	$\alpha/({\rm dB\cdot km^{-1}})$
0.015	10^{-7}	10^{-7}	0.6	0.75	10^{-10}	1.16	0.2

为了验证本研究方案的有效性, 将其与其他已有的 MDI-QKD 协议进行对比, 包括使用标记单光子源的四强度诱骗态 MDI-QKD 协议[21] 以及基于量子存储的三强度诱骗态 MDI-QKD 协议[13]. 相关结果如图 2 和图 3 所示. 在仿真中, 我们为所使用的 QM 设定了一组合理的参数: 存储轮数 $M=20$, 传输效率 $T_{\rm QM}=98\%$, 存储保真度 $F=98.5\%$.

从图 2(a) 可以看出, 所有方案的系统增益随着传输距离的增大而迅速下降, 与其他方案相比, 本文提出的方案在整个距离范围内始终保持更高的系统增益, 说明其计数率估计更加紧致且更为有效. 同时, 图 2(b) 表明系统误码率整体呈上升趋势, 表明信道损耗加剧, 探测概率逐渐降低. 本文提出的方案在误码率上界方面保持较低水平, 尤其在远距离传输中优势更加显著, 体现出估计的高效性, 有助于保障密钥的安全性.

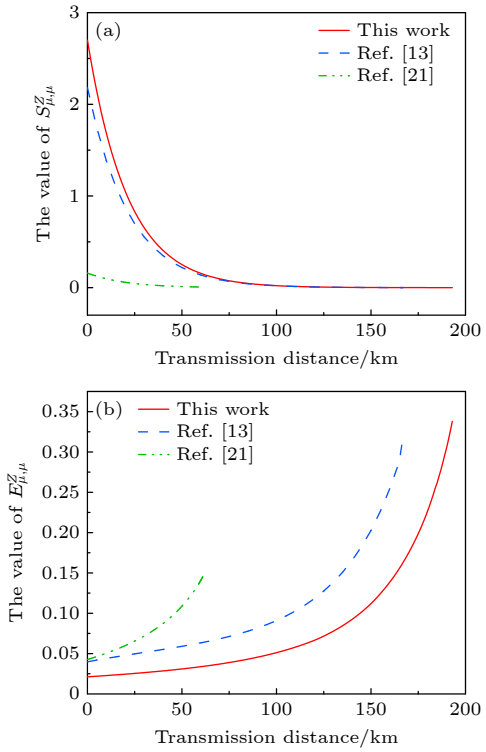

图 2 本文提出的方案与已有 MDI-QKD 方案的系统的增益 $S^{K}_{x_{\rm A},y_{\rm B}}$ (a) 和误码率 $E^{K}_{x_{\rm A},y_{\rm B}}$ (b) 曲线对比. 总脉冲数 $N=10^{10}$

Fig. 2. Comparison of the system gain $S^{K}_{x_{\rm A},y_{\rm B}}$ (a) and quantum bit-error rate $E^{K}_{x_{\rm A},y_{\rm B}}$ (b) between the proposed scheme and existing MDI-QKD schemes. Total number of pulses $N=10^{10}$.

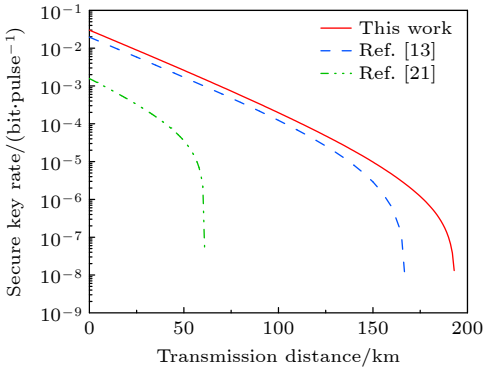

图 3 本文提出的方案与已有 MDI-QKD 方案的密钥率曲线对比. 总脉冲数 $N=10^{10}$, 存储轮数 $M=20$

Fig. 3. Comparison between the proposed scheme and existing MDI-QKD schemes. Total number of pulses $N=10^{10}$, and the number of storage rounds $M=20$.

将本方案与已有基于存储辅助的三强度诱骗态 MDI-QKD 协议[13] 以及基于 HSPS 的四强度诱骗态 MDI-QKD 协议[21] 的密钥率与传输距离曲线进行对比, 如图 3 所示, 设定存储轮 $M = 20$ 、总脉冲数 $N = 10^{10}$. 从图 3 可以看出, 本方案相对于其他同类 MDI 两种方案在密钥率和传输距离上都有明显的提升, 与文献 [21] 相比, 在短距离传输场景 (<50 km) 下, 本方案在距离区间均保持更高密钥率, 且在高损耗条件下保持了一个数量级上的密钥率提升. 这是因为 QM 在物理层面提升了 MDI-QKD 的码率, 解决了长距离传输中双光子同时到达接收端概率低的问题, 为密钥生成提供了更多有效光子资源. 在长距离传输场景 (>50 km) 下, 本方案在接近 180 km 时仍能保持非零的密钥率, 而其他同类协议已无法成码. 这是因为双参数扫描能够更精准地估计单光子脉冲计数率、相位翻转错误率等关键物理参数, 减小因参数估计偏差带来的密钥率损耗, 同时抑制有限数据长度效应的干扰.

图 4 展示了在传输距离为 20 km、存储轮数 $M = 10$ 时, 有限长效应对不同方案的影响分析. 当总脉冲数 $N < 10^{11}$ 时, 随着 N 的不断增大, 密钥率逐渐上升, 这是由于样本数越多, 统计波动越小, 从而使得参数估计更精确, 进而提高了最终的密钥生成率; 但是, 当 $N > 10^{11}$ 时, 曲线趋于平稳, 说明在大样本条件下, 有限长效应的影响显著减弱. 同时本文提出的方案 (红线实线) 始终优于其他两个方案, 在整个 N 取值范围内都保持较高的密钥率, 显示出良好的稳定性和鲁棒性.

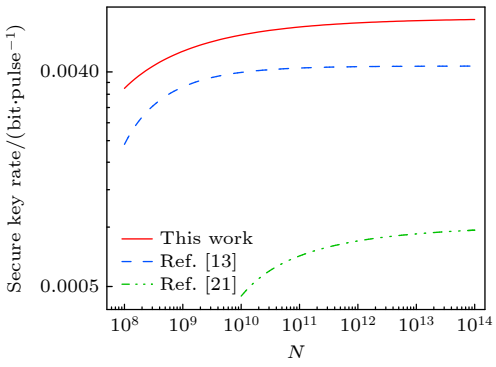

图 4 有限长效应对不同 QKD 方案的影响. 存储轮数 $M = 10$

Fig. 4. Comparison of the impact of finite-size effects on different QKD schemes. Number of storage rounds $M = 10$.

我们进一步分析了系统参数对存储辅助型 MDI-QKD 性能的影响, 例如固定存储轮数 $M = 10$ 时, 量子存储器传输效率 $T_{\rm QM}$ 在 68%—98% 范围以及存储保真度 F 在 95%—98.5% 范围, 如图 5(a), (b) 所示. 结果表明, 在现有实验计数条件下, 密钥率和传输距离随着量子存储器传输效率的增大而增大, 同时随着存储保真度的增大而增大. 这是因为更高的存储效率意味着成功存储并可用于后续操作的光子数量更多, 能在长距离传输中抵消部分损耗, 维持较高的密钥生成率, 而更高的存储保真度意味着量子态在存储过程中受到的干扰更小, 从而提升协议在长距离传输下的性能.

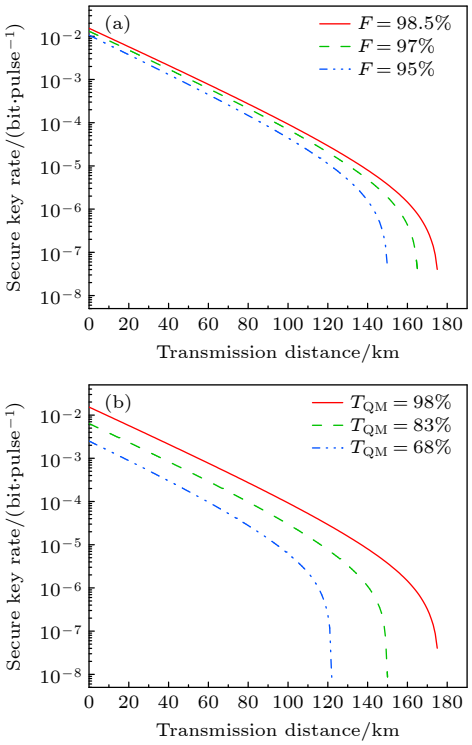

图 5 在不同存储保真度 (a) 与存储效率 (b) 下密钥率随传输距离的变化. 存储轮数 $M = 10$, 总脉冲数 $N = 10^{10}$

Fig. 5. Variation of the key rate with transmission distance under (a) different storage fidelities and (b) different storage efficiencies. Number of storage rounds $M = 10$, and the total number of pulses $N = 10^{10}$.

图 6 为固定传输距离 50 km 时, 在不同存储效率 $T_{\rm QM}$ 下, 密钥率对存储轮数 M 的变化情况. 对于所有存储效率曲线, 密钥率都随着存储轮数的增加而上升, 但是增益随轮数增加逐渐减缓, 尤其是在轮数达到约 10 之后, 提升幅度明显趋缓, 趋向饱和, 当存储轮数超过一定值 (如 15—20), 继续增大带来的密钥率提升有限. 这是由于随着存储轮数的增大, 光子在存储过程中的损耗增大.

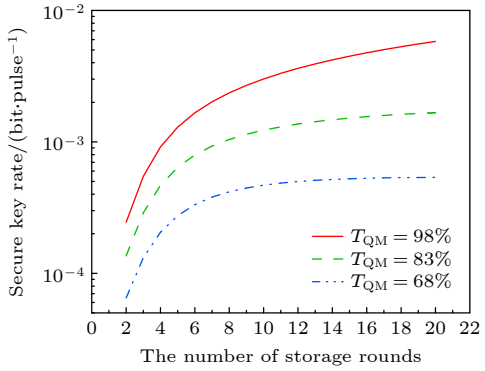

图 6 不同存储效率下密钥率随存储轮数的变化. 总脉冲数 $N = 10^{10}$

Fig. 6. Variation of the key rate with the number of storage rounds under different storage efficiencies. Total number of pulses $N = 10^{10}$.

4 结 论

本文提出了一种基于双参数扫描的量子存储辅助 MDI-QKD 协议. 通过使用量子存储器将早到的单光子存储起来, 等到另外一个光子到达后再释放出来执行双光子测量, 可以提升双光子符合效率; 通过使用集体约束模型与双参数扫描算法对单光子对计数率和相位误码率进行联合估计, 可以提升参数估计的精度; 通过将以上优点结合起来, 能够大幅提升 MDI-QKD 系统的整体性能. 我们将本方案与已有同类 MDI-QKD 协议进行比较, 包括基于标记单光子源的四强度诱骗态方案, 以及三强度诱骗态存储辅助 MDI-QKD 方案等, 证明了在相同参数设置条件下, 本文方案在密钥率和安全传输距离上均能显示出突出的优势. 但是必须承认, 与现有其他同类 MDI-QKD 协议相比, 本文提出的基于双参数扫描的量子存储辅助 MDI-QKD 协议的实验系统复杂性增加; 同时使用双参数扫描算法进行参数优化, 可能导致在实际应用中后处理的复杂度增加. 不过可以通过结合人工智能技术来解决 [22,23], 不仅能够降低资源优化的时间开销, 同时能提升实际工作性能. 此外, 本文使用的存储器存在无法给出存储成功与否的预报信息问题, 而预报式存储器能够弥补这一缺陷 [24–28], 从而进一步提升系统性能. 因此, 本文工作有望为未来远距离量子通信的实际部署提供新的思路与可行路径.

附录A 对公式 (1) 的解释

(1) 式中 $P_{\mathrm{l}}(k|j)$ 和 $P_{\mathrm{e}}(k|j)$ 可以表示为 [17]

$$P_{\mathrm{l}}(k|j) = [1 - P_{\mathrm{h}}(j-1)] \sum_{k'=k}^{\infty} P_{\mu}^{k'} P_{\mathrm{d}}(k') P_{\mathrm{t}}(k|k', j, j), \tag{A1}$$

$$\begin{aligned} P_{\mathrm{e}}(k|j) = & \sum_{j'=1}^{j-1} [1 - P_{\mathrm{h}}(j - j' - 1)] \\ & \times \sum_{k'=1}^{\infty} \left[P_{\mu}^{k'} P_{\mathrm{d}}(k') P_{\mathrm{t}}(k|k', j, j')(1 - P_{\mathrm{h}}(1)) \right] \\ & + P_{\mathrm{h}}(j-1) \sum_{k'=1}^{\infty} P_{\mu}^{k'} P_{\mathrm{d}}(k') P_{\mathrm{t}}(k|k', j, j), \end{aligned} \tag{A2}$$

式中, $P_{\mathrm{d}}(k)$ 表示信号源产生 k 对光子后, 信号光子被触发探测器检测到的概率, $P_{\mathrm{t}}(k'|k, j, j')$ 表示在第 j 时隙生成 k 个光子对, 且在第 j' 时隙成功发射 k' 个闲置光子的概率, $P_{\mathrm{h}}(j)$ 表示一个 HSPS 在前 j 个时隙中成功产生标记响应的概率:

$$P_{\mathrm{d}}(k) = \sum_{m=1}^{k} \eta_{\mathrm{d}}^{m} (1 - \eta_{\mathrm{d}})^{k-m} C_k^m (1/D)^{m-1}, \tag{A3}$$

$$P_{\mathrm{t}}(k'|k, j, j') = \left(T_{\mathrm{C}} T_{\mathrm{QM}}^{j-j'+1} \right)^{k'} \left(1 - T_{\mathrm{C}} T_{\mathrm{QM}}^{j-j'+1} \right)^{k-k'} C_k^{k'}, \tag{A4}$$

$$P_{\mathrm{h}}(j) = 1 - [1 - P_{\mathrm{h}}(1)]^{j}, \tag{A5}$$

式中, η_{d} 表示信号光从光子对的生成过程到信号光子的探测过程的总体透过率; D 表示探测器的数量; T_{QM} 表示量子存储器的存储效率; T_{C} 表示其他光学器件的传输效率;

$$P_{\mathrm{h}}(1) = \sum_{m=1}^{\infty} P_{\mathrm{d}}(k) P_{\mu}^{k}.$$

附录B 对保真度 F 的解释

由于量子存储器 (QM) 存入和读出过程中可能对量子态产生一定的误差, 我们对一个量子态在进入 QM 之前与离开 QM 之后的变化进行分析. 若输入为理想的竖直偏振态 $|V\rangle$, 光学系统的本底误码为 e_{d}, 则系统可能以概率 e_{d} 将其改变为水平偏振态 $|H\rangle$. 同时, 由于存在背景噪声, QM 有 e_{BG} 的概率加载的是背景噪声光子. 则光子经过 QM 之后的量子态为

$$\begin{aligned} \rho_{\mathrm{out}} = & (1 - e_{\mathrm{BG}}) \left[(1 - e_{\mathrm{d}}) |V\rangle\langle V| + e_{\mathrm{d}} |H\rangle\langle H| \right] \\ & + \frac{e_{\mathrm{BG}}}{2} \left(|V\rangle\langle V| + |H\rangle\langle H| \right), \end{aligned} \tag{B1}$$

因此, 存储保真度可以写为 [28]

$$F_X = \frac{(1 - e_{\mathrm{BG}})(1 - 2e_{\mathrm{d}}) + 1}{2}, \tag{B2}$$

$$F_Z = (1 - e_{\mathrm{BG}})(1 - e_{\mathrm{d}}) + \frac{e_{\mathrm{BG}}}{2}. \tag{B3}$$

由于 e_{BG} 值较小, 通常可以忽略 [29], 则可简化 (B2) 式和 (B3) 式为 $F \approx 1 - e_{\mathrm{d}}$.

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] Lo H K, Curty M, Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[3] Zhou Y H, Yu Z W, Wang X B 2016 *Phys. Rev. A* **93** 042324
[4] Yin H L, Chen T Y, Yu Z W, Liu H, You L X, Zhou Y H, Chen S J, Mao Y, Huang M Q, Zhang W J, et al. 2016 *Phys. Rev. Lett.* **117** 190501
[5] Jiang C, Yu Z W, Hu X L, Wang X B 2021 *Phys. Rev. A* **103** 012402
[6] Chen Y P, Liu J Y, Sun M S, et al. 2021 *Opt. Lett.* **46** 3729
[7] Chanelière T, Matsukevich D, Jenkins S, Lan S Y, Kennedy T A B, Kuzmich A 2005 *Nature* **438** 833
[8] Panayi C, Razavi M, Ma X F, Lütkenhaus N 2014 *New J. Phys.* **16** 043005
[9] Piparo N L, Razavi M, Panayi C 2015 *IEEE J. Sel. Top. Quantum Electron.* **21** 138
[10] Pittman T B, Franson J D 2002 *Phys. Rev. A* **66** 062302
[11] Evans C J, Nunn C M, Cheng S W L, Franson J D, Pittman T B 2023 *Phys. Rev. A* **108** L050601
[12] Sun M S, Zhang C H, Luo Y Z, Wang S, Liu Y, Li J, Wang Q 2025 *Appl. Phys. Lett.* **126** 104001
[13] Sun M S, Zhang C H, Ding H J, Zhou X Y, Li J, Wang Q 2023 *Phys. Rev. Appl.* **20** 024029
[14] Wang Q, Karlsson A 2007 *Phys. Rev. A* **76** 014309
[15] Mo X F, Zhu B, Han Z F, Gui Y Z, Guo G C 2005 *Opt. Lett.* **30** 2632
[16] Goswami I, Mandal M, Mukhopadhyay S 2022 *J. Opt.* **51** 379
[17] Kaneda F, Xu F H, Chapman J, Kwiat P G 2017 *Optica* **4** 1034
[18] Yu Z W, Zhou Y H, Wang X B 2015 *Phys. Rev. A* **91** 032318
[19] Wang Q, Wang X B 2014 *Sci. Rep.* **4** 4612
[20] Curty M, Xu F H, Cui W, Lim C C W, Tamaki K, Lo H K 2014 *Nat. Commun.* **5** 4732
[21] Zhou X Y, Zhang C H, Zhang C M, Wang Q 2017 *Phys. Rev. A* **96** 052337
[22] Ren Z A, Chen Y P, Liu J Y, Ding H J, Wang Q 2021 *IEEE Commun. Lett.* **25** 940
[23] Xu J X, Ma X, Liu J Y, Zhang C H, Li H W, Zhou X Y, Wang Q 2024 *Sci. China Inf. Sci.* **67** 202501
[24] Duan L M, Lukin M, Cirac L, Zoller P 2001 *Nature* **414** 413
[25] Duan L M, Cirac J I, Zoller P 2002 *Phys. Rev. A* **66** 023818
[26] Gujarati T P, Wu Y K, Duan L M 2018 *Phys. Rev. A* **97** 033826
[27] Li X K, Song X Q, Guo Q W, Zhou X Y, Wang Q 2021 *Chin. Phys. B* **30** 060305
[28] Abruzzo S, Kampermann H, Bruß D 2014 *Phys. Rev. A* **89** 012301
[29] Jozsa R 1994 *J. Mod. Opt.* **41** 2315

Dual-paramter-scanning-based quantum- memory- assisted measurement-device-independent quantum key distribution protocol*

LIU Chang [1)2)#] SUN Mingshuo [1)2)#] LUO Yizhen [1)2)] DONG Shuyan [1)2)]
ZHANG Chunhui [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 29 August 2025; revised manuscript received 23 October 2025)

Abstract

Measurement-device-independent quantum key distribution (MDI-QKD) protocol can effectively resist all possible attacks targeting the measurement devices in a quantum key distribution (QKD) system, thus exhibiting high security. However, due to the protocol's high sensitivity to channel attenuation, its key generation rate and transmission distance are significantly limited in practical applications.

To improve the performance of MDI-QKD, researchers have proposed quantum-memory (QM)-assisted MDI-QKD protocol, which has enhanced the protocol's performance to a certain extent. Nevertheless, under finite-size conditions where the total number of transmitted pulses is limited, accurately estimating the relevant statistical parameters is still a challenge. As a result, existing QM-assisted MDI-QKD schemes still encounters issues such as low key rates and limited secure transmission distances.

To solve these problems, this work proposes a novel improved finite-size QM-assisted MDI-QKD protocol. By utilizing quantum memories to temporarily store early-arriving pulses and release them synchronously, the protocol effectively reduces the influence caused by channel asymmetry. Additionally, the protocol introduces a four-intensity decoy-state method to improve the estimation accuracy of single-photon components. Meanwhile, to mitigate the influence of finite-length effects on QM schemes, the proposed protocol combines a collective constraint model and a double-scanning algorithm to jointly estimate scanning error counts and vacuum-related counts. This approach enhances the estimation accuracy of the single-photon detection rate and phase error rate under finite-size conditions, thereby significantly improving the secure key rate of the MDI-QKD system.

Simulation results show that under the same experimental conditions, compared with the existing QM-assisted three-intensity decoy-state MDI-QKD protocol and the four-intensity decoy-state MDI-QKD protocol based on Heralded Single-photon Source (HSPS), the proposed protocol extends the secure transmission distance by more than 30 km and 100 km, respectively. This proves that under the same parameter settings, the proposed scheme exhibits significant advantages in both key rate and secure transmission distance. Therefore, this research provides important theoretical references and valuable benchmarks for developing long-distance, high-security quantum communication networks.

Keywords: quantum key distribution, quantum memory, double-scanning, joint constraints

DOI: 10.7498/aps.75.20251171 **CSTR:** 32037.14.aps.75.20251171

* Project supported by the Key Research and Development Program Industry Outlook and Key Core Technology Program of Jiangsu Province, China (Grant No. BE2022071) and the National Natural Science Foundation of China (Grant Nos. 62471248, 12074194).

# These authors contributed equally.

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

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

基于双参数扫描的量子存储辅助测量设备无关量子密钥分发协议

刘畅 孙铭烁 罗一振 董书言 张春辉 王琴

Dual-paramter-scanning-based quantum- memory- assisted measurement-device-independent quantum key distribution protocol

LIU Chang SUN Mingshuo LUO Yizhen DONG Shuyan ZHANG Chunhui WANG Qin

引用信息 Citation: Acta Physica Sinica, 75, 010602 (2026) DOI: 10.7498/aps.75.20251171
CSTR: 32037.14.aps.75.20251171
在线阅读 View online: https://doi.org/10.7498/aps.75.20251171
当期内容 View table of contents: http://wulixb.iphy.ac.cn
