实用化态制备误差容忍参考系无关量子密钥分发协议*

周阳[1)2)#] 马啸[1)2)#] 周星宇[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)

(2023 年 7 月 15 日收到; 2023 年 9 月 7 日收到修改稿)

在实际量子密钥分发系统中, 实际器件不理想可能导致系统存在安全性隐患. 比如, 光源端的编码设备不理想, 可能导致量子态存在误差; 探测端的探测器存在缺陷, 可能产生后脉冲或死时间效应, 从而影响系统的实际安全性. 因此, 本文提出了一种同时考虑光源端和探测器缺陷的实用化态制备误差容忍参考系无关量子密钥分发协议. 本文采用三强度诱骗态方案开展建模分析与数值仿真计算. 本协议通过利用虚拟态方法估算相位误码率, 降低了态制备误差对密钥率的影响; 同时对探测器端的缺陷进行相应参数刻画, 具有较强的鲁棒性, 为参考系无关量子密钥分发协议的实际应用提供了重要参考价值.

关键词: 量子密钥分发, 态制备误差, 参考系无关协议, 后脉冲效应, 死时间效应

PACS: 03.65.–w, 03.67.Hk, 42.50.Ex, 42.79.Sz **DOI:** 10.7498/aps.72.20231144

1 引 言

量子密钥分发 (quantum key distribution, QKD) 可以在两个远距离用户 Alice 和 Bob 之间形成一致密钥, 其安全性基于量子力学的基本原理, 且已被证明具有信息论安全性[1,2]. 经过几十年的发展, QKD 理论已经比较成熟, 且在不同的场景下得到了实验验证, 如基于光纤的 QKD[3–6] 和自由空间信道 QKD[7,8]. 在上面提到的大多数 QKD 系统中, Alice 和 Bob 之间需要一个共享的参考系, 而实时校准参考系在一定程度上增加了系统的成本并降低了性能. 幸运的是, 参考系无关 (reference-frame-independent, RFI)QKD 协议[9] 的概念被提出, 克服了参考系漂移问题, 从而受到了广泛的关注.

实际器件特性的不理想使得 QKD 的理论和实践之间存在一定矛盾. 在实际 QKD 系统中, 存在光源缺陷和探测端缺陷等问题, 使得系统的安全性降低. 针对光源端态制备误差问题, 2014 年, 在 GLLP 协议[10] 的基础上, Tamaki 等[11] 提出了一种态制备误差容忍 (loss tolerant, LT) 的 QKD 协议. 随后, 出现了一系列与光源安全性相关的工作[12–15], 其中, 2015 年 Wang 等[12] 将损耗容忍方案与参考系无关协议结合, 有效提升了 RFI QKD 协议的光源安全性.

但除了源端缺陷之外, 由于探测器固有的半导体结构缺陷, 在正常的探测信号之后也容易产生虚假的非光子探测脉冲输出, 会造成错误的计数,

* 国家自然科学基金 (批准号: 12074194, 11774180) 、江苏省自然科学基金前沿技术项目 (批准号: BK20192001)、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) 和江苏省研究生科研创新计划 (批准号: SJCX22_0276, KYCX23_1039).

同等贡献作者.

† 通信作者. E-mail: qinw@njupt.edu.cn

也就是后脉冲效应[16–18], 从而导致误码率增大. 同时, 单光子探测器在探测事件发生后会进入一段“恢复期”, 在此期间, 探测器不会对其他的光脉冲响应, 这将带来死时间效应[19–21]. 对于一般的 QKD 系统, 死时间和后脉冲效应可以忽略不计, 但随着系统重复频率的增大, 尤其进入千兆赫兹, 这种假设就不再合理. 基于以上问题, 本文提出了一种同时考虑光源端和探测器缺陷的实用化态制备误差容忍参考系无关 (loss tolerant reference-frame-independent, LT-RFI) QKD 协议, 并且以三强度诱骗态方案[22] (信号态+弱诱骗态+真空态) 为例进行相应的模型分析与数值仿真计算. 该协议通过利用虚拟态方法来估算相位误码率, 显著降低了态制备缺陷对密钥率的影响, 这意味着本文的协议在传输过程中能够更有效地防止由于态制备误差而导致的信息损失. 此外, 通过刻画后脉冲和死时间对密钥率带来的影响, 本文的协议还表现出更高的鲁棒性, 能够有效应对探测器端的缺陷问题.

2 理论模型

在实际的量子密钥分发系统中, 由于器件的不完美, 不可避免地存在量子态制备误差、后脉冲效应与死时间效应. 针对 3 种缺陷, 本文提出了同时考虑光源和探测器缺陷的实用性态制备误差容忍参考系无关量子密钥分发协议, 该协议通过将态制备误差、后脉冲与死时间等缺陷分别进行建模和刻画, 并对 QKD 系统重新进行了安全性分析证明, 使得该模型的结果可以对误差具有较好的容忍性能, 模型的鲁棒性得以增强.

在 LT-RFI 协议中, Alice 随机制备 4 种量子态 $\hat{\rho}_{0Z}$, $\hat{\rho}_{1Z}$, $\hat{\rho}_{0X}$ 与 $\hat{\rho}_{0Y}$. 量子态 $\hat{\rho}_{j\alpha}$, $\alpha\in\{X,Y,Z\}$, $j\in\{0,1\}$ 的 Bloch 系数记为 ($P_X^{j\alpha}$, $P_Y^{j\alpha}$, $P_Z^{j\alpha}$). 也就是说 $\hat{\rho}_{j\alpha,\mathrm{vir}}=\dfrac{1}{2}(\hat{I}+P_X^{j\alpha}\hat{\sigma}_X+P_Y^{j\alpha}\hat{\sigma}_Y+P_Z^{j\alpha}\hat{\sigma}_Z)$, 其中 $\hat{I}$ 和 $\hat{\sigma}_X,\hat{\sigma}_Y,\hat{\sigma}_Z$ 分别表示单位算符和泡利矩阵. Bob 接收到 Alice 发送的态后随机选择 X 基或 Z 基测量, 然后通过经典信道公开基矢信息, 并记录匹配基和不匹配基的事件. Alice 和 Bob 使用匹配基和不匹配基的探测计数率进行参数估计, 再经过后处理, 则可得到最终安全密钥.

下面以相位编码的 QKD 系统为例进行具体模型介绍. 由于现实环境下编码系统在态制备过程存在一定的缺陷, 制备出的量子态与理想的量子态之间存在一定偏差, 因此考虑态制备误差时, Alice 对量子态中的误差刻画如下:

$$\begin{aligned}
|\phi_{0Z}\rangle &= \cos\frac{\delta_1}{2}|0_Z\rangle+\sin\frac{\delta_1}{2}|1_Z\rangle,\\
|\phi_{1Z}\rangle &= \sin\frac{\delta_2}{2}|0_Z\rangle+\cos\frac{\delta_2}{2}|1_Z\rangle,\\
|\phi_{0X}\rangle &= \sin(\pi/4+\delta_3/2)|0_Z\rangle\\
&\quad+\cos(\pi/4+\delta_3/2)\,\mathrm{e}^{\mathrm{i}\theta_1}|1_Z\rangle,\\
|\phi_{0Y}\rangle &= \sin(\pi/4+\delta_4/2)|0_Z\rangle\\
&\quad+\cos(\pi/4+\delta_4/2)\,\mathrm{e}^{\mathrm{i}(\pi/2+\theta_2)}|1_Z\rangle,
\end{aligned}\tag{1}$$

其中 δ_1 和 δ_2 表示由于衰减器或强度调制器不理想造成的态制备误差, δ_3 和 δ_4 表示由于分束器不理想造成的误差, θ_1 和 θ_2 表示由相位调制器不理想造成的偏差.

在 RFI 协议之中, Eve 获取的信息量由 I_{E} 表示为

$$I_{\mathrm{E}}=\left(1-E_{ZZ}^{(1)}\right)h\left(\frac{1+m}{2}\right)+E_{ZZ}^{(1)}h\left(\frac{1+n}{2}\right),\tag{2}$$

其中

$$m=\min\left\{\frac{\sqrt{C/2}}{\left(1-E_{ZZ}^{(1)}\right)},1\right\},$$

$$n=\frac{1}{E_{ZZ}^{(1)}}\sqrt{C/2-\left(1-E_{ZZ}^{(1)}\right)^2m^2},$$

$E_{ZZ}^{(1)}$ 为 Z 基下单光子比特误码率, $C=(1-2E_{XX})^2+(1-2E_{XY})^2+(1-2E_{YX})^2+(1-2E_{YY})^2$, $h(x)$ 是二进制香农熵函数, 表达式为 $h(x)=-x\log_2(x)-(1-x)\log_2(1-x)$[10].

接下来, 使用虚拟协议[23] 来更紧致估计 4 组不同基矢下的误码率: $E_{XX},E_{XY},E_{YX},E_{YY}$. 以误码率 E_{XX} 为例, 其表征为虚拟协议中 X 基下的比特误码率, 表达式如下:

$$E_{XX}=\frac{Y_{0X,1X}^{(Z)\mathrm{vir}}+Y_{1X,0X}^{(Z)\mathrm{vir}}}{Y_{0X,0X}^{(Z)\mathrm{vir}}+Y_{1X,0X}^{(Z)\mathrm{vir}}+Y_{0X,1X}^{(Z)\mathrm{vir}}+Y_{1X,1X}^{(Z)\mathrm{vir}}},\tag{3}$$

其中 $Y_{sX,jX}^{(Z)\mathrm{vir}}$ 表示 Alice(Bob) 使用 X 基矢测量态 $|\psi_Z\rangle_{AA_eB}$ 且获得比特值 $j\,(s)$ 的概率, 且 $s,j\in\{0,1\}$. $Y_{sX,jX}^{(Z)\mathrm{vir}}$ 由虚拟态发送的概率与虚拟态在对应基下成功测量的概率两部分构成, 经过与泡利算符在信道传输速率的变量代换, 表示如下:

$$Y_{sX,jX}^{(Z)\mathrm{vir}}=\frac{1}{4}p_{jX,\mathrm{vir}}\Big(q_{sX|Id}+P_X^{jX,(\mathrm{vir})}q_{sX|X}+P_Y^{jX,(\mathrm{vir})}q_{sX|Y}+P_Z^{jX,(\mathrm{vir})}q_{sX|Z}\Big),\quad(4)$$

其中 $p_{jX,\mathrm{vir}}$ 表示发送 Alice 在系统 B 发送虚拟态的概率; $1/4$ 表示 Bob 选择 X 基矢测量的概率; $q_{sX|t}=\mathrm{tr}(\hat{D}_{S_X}\hat{\sigma}_t)/2$ 表示泡利矩阵 $\hat{\sigma}_t$ 的传输率, 且 $t\in\{\mathrm{Id},X,Y,Z\}$; $\hat{D}_{S_X}$ 表示 Eve 窃听的测量算符.

对于虚拟态的发送概率 $p_{jX,\mathrm{vir}}$, 其可表示为 $p_{0(1)X,\mathrm{vir}}=\{1\pm\sin[(\delta_1+\delta_2)/2]\}/2$, 而对于泡利矩阵 $\hat{\sigma}_t$ 的传输率 $q_{sX|t}$, 与真实量子态的计数率满足如下关系:

$$\begin{aligned}&\left(q_{sX|Id},q_{sX|X},q_{sX|Y},q_{sX|Z}\right)\\&=16\left(Y_{sX,0Z}^{(Z)},Y_{sX,1Z}^{(Z)},Y_{sX,0X}^{(X)},Y_{sX,0Y}^{(Y)}\right)/\hat{A},\end{aligned}\quad(5)$$

其中, $\hat{A}:=(\boldsymbol{V}_{0Z}^{\mathrm{T}},\boldsymbol{V}_{1Z}^{\mathrm{T}},\boldsymbol{V}_{0X}^{\mathrm{T}},\boldsymbol{V}_{0Y}^{\mathrm{T}})$, T 表示转置; $\boldsymbol{V}_{j\alpha}^{\mathrm{T}}:=(1,P_X^{j\alpha},P_Y^{j\alpha},P_Z^{j\alpha})$. 结合 (1) 式, 矩阵 $\hat{A}$ 表示如下:

$$\hat{A}=\begin{pmatrix}1&1&1&1\\\sin\delta_1&\sin\delta_2&\cos\delta_3\cos\theta_1&-\cos\delta_4\sin\theta_2\\0&0&\cos\delta_3\sin\theta_1&\cos\delta_4\cos\theta_2\\\cos\delta_1&-\cos\delta_2&\sin\delta_3&\sin\delta_4\end{pmatrix}.\quad(6)$$

由此, 可以求得相位误码率 E_{XX}, 其他相位误码率 E_{XY},E_{YX},E_{YY} 求解方法相同. 以上, 可精准求得窃听者 Eve 在量子密钥分发过程中获取的信息量.

由于在接收端有两个探测器, 因此协议有效的探测事件分为两种情况: 两个探测器同时响应或者只有一个探测器响应. 首先考虑探测端带来的后脉冲效应, 探测器的响应正确 (错误) 的概率 $\hat{D}_{\mathrm{one},\surd}$ ($\hat{D}_{\mathrm{one},\times}$) 以及两个探测器同时响应的概率 $\hat{D}_{\mathrm{two}}$ 满足如下表达式:

$$\hat{D}_{\mathrm{one},\surd(\times)}=\begin{cases}(1+P_{\mathrm{ap}})\,D_{\mathrm{one},\surd(\times)},&n\neq0,\\P_{\mathrm{dc}}\,(1-P_{\mathrm{dc}}),&n=0,\end{cases}\qquad\hat{D}_{\mathrm{two}}=\begin{cases}(1+P_{\mathrm{ap}})\,D_{\mathrm{two}},&n\neq0.\\P_{\mathrm{dc}}^2,&n=0.\end{cases}\quad(7)$$

其中 P_{dc} 表示暗计数率, P_{ap} 表示后脉冲概率.

当使用弱相干态 (weak coherent state, WCS) 光源时, 认为只有一个探测器响应且测得正确的概率为 $D_{\mathrm{one},\surd}$、只有一个探测器响应但测得错误的概率为 $D_{\mathrm{one},\times}$、两个探测器同时响应的概率为 D_{two}. 相应的表达式如下:

$$\begin{aligned}D_{\mathrm{one},\surd}&=(1-\eta C_{1Z|0Z})^n(1-P_{\mathrm{dc}})-(1-\eta)^n(1-P_{\mathrm{dc}})^2,\\D_{\mathrm{one},\times}&=(1-\eta C_{0Z|0Z})^n(1-P_{\mathrm{dc}})-(1-\eta)^n(1-P_{\mathrm{dc}})^2,\\D_{\mathrm{two}}&=1-[(1-\eta C_{0Z|0Z})^2(1-P_{\mathrm{dc}})-(1-\eta)^n(1-P_{\mathrm{dc}})^2]-(1-\eta C_{0Z|0Z})^n(1-P_{\mathrm{dc}}),\end{aligned}\quad(8)$$

其中 η 表示系统的总透射率, Alice 发送量子态 $|\phi_{0Z}\rangle$ 且 Bob 使用 Z 基测量得到正确比特值 0 的概率为 $C_{0Z|0Z}$, 错误结果的概率为 $C_{1Z|0Z}$.

结合诱骗态方法, 可以得到平均光子数为 λ 的增益为

$$Q_{\lambda,s\alpha|j\gamma}=\sum_{n=0}^{\infty}V_{n,s\alpha|j\gamma}\frac{\lambda^n}{n!}\mathrm{e}^{-\lambda}=\frac{1}{2}(1+P_{\mathrm{ap}})\left\{1+D\left[\mathrm{e}^{-(\eta+a)\lambda}-\mathrm{e}^{-a\lambda}-D\mathrm{e}^{-\lambda\eta}\right]\right\}-P_{\mathrm{ap}}P_{\mathrm{dc}}\left(1-\frac{1}{2}P_{\mathrm{dc}}\right),\quad(9)$$

其中 $\lambda\in\{\mu,v\}$, $a=\eta C_{n,s\alpha|j\gamma}$, $D=1-P_{\mathrm{dc}}$. $V_{n,s\alpha|j\gamma}$ 表示 Alice 发送量子态 $|\phi_{j\gamma}\rangle$ 且 Bob 选择 α 基测量得到 s 比特的条件概率, $s,j\in\{0,1\}$, $\alpha,\gamma\in\{X,Y,Z\}$. 其表达式为

$$V_{n,s\alpha|j\gamma}=\frac{1}{2}\hat{D}_{\mathrm{two}}+\hat{D}_{\mathrm{one},\surd}=\begin{cases}\frac{1}{2}(1+P_{\mathrm{ap}})\left(1+P_{\mathrm{dc}}\vartheta_{s\alpha|j\gamma}\right),&n\neq0,\\P_{\mathrm{dc}}\left(1-\frac{1}{2}P_{\mathrm{dc}}\right),&n=0,\end{cases}\quad(10)$$

其中 $\vartheta_{s\alpha|j\gamma}=\left(1+\eta C_{s\alpha|j\gamma}-\eta\right)^n-\left(1-\eta C_{s\alpha|j\gamma}\right)^n-(1-P_{\mathrm{dc}})\,(1-\eta)^n$.

当考虑死时间效应时, Alice 制备 $|j\gamma\rangle$ 量子态并发送平均光子数为 λ 的脉冲, 然后 Bob 使用 $|s\alpha\rangle$ 量子态测量的探测概率为 $P_{\lambda,s\alpha|j\gamma}=c_{\rm dt}P_\lambda P_{\gamma|\lambda}P_\alpha Q_{\lambda,s\alpha|j\gamma}$. 其中, P_λ 表示 Alice 发送 λ 强度脉冲的概率, $P_{\gamma|\lambda}$ 表示 Alice 发送 λ 强度脉冲条件下选择 γ 基的概率, P_α 表示 Alice 选择 α 基矢的概率. $c_{\rm dt}$ 表示死时间效应引起的修正系数, 满足关系式:

$$c_{\rm dt}=\frac{1}{1+F\tau_{\rm dt}\sum_\lambda P^\lambda_{\xi,\rm det}}, \tag{11}$$

其中 F 为系统重复频率, $\tau_{\rm dt}$ 为死时间大小, $P^\lambda_{\xi,\rm det}$ 为基于 ξ 基下 λ 强度的探测效率.

根据信号态 μ、诱骗态 v 的增益, 可以得到单光子计数率的下限 $Y^{\rm L}_{1,s\alpha,j\gamma}$, 从而得到 Z 基下的单光子增益 $Q^{(1)}_Z$ 和比特误码率 $E^{(1)}_{ZZ}$:

$$Y^{\rm L}_{1,s\alpha,j\gamma}=\frac{\mu}{\mu\nu-\nu^2}\times\left(Q_v{\rm e}^\nu-Q_\mu{\rm e}^\mu\frac{\nu^2}{\mu^2}-\frac{\mu^2-\nu^2}{v^2}V_{0,s\alpha|j\gamma}\right), \tag{12}$$

$$Q^{(1)}_Z={\rm e}^{-\mu}\mu\left(Y^{\rm L}_{1,0Z,0Z}+Y^{\rm L}_{1,0Z,1Z}+Y^{\rm L}_{1,1Z,0Z}+Y^{\rm L}_{1,1Z,1Z}\right), \tag{13}$$

$$E^{(1)}_{ZZ}=\left(Y^{\rm L}_{1,0Z,1Z}+Y^{\rm L}_{1,1Z,0Z}\right)/Q^{(1)}_Z. \tag{14}$$

Z 基下的整体增益 Q_Z 和比特误码率 e_Z, 满足关系式:

$$Q_Z=\frac{c_{\rm dt}}{4}\left(Q_{\mu,0Z,0Z}+Q_{\mu,1Z,1Z}+Q_{\mu,1Z,0Z}+Q_{\mu,0Z,1Z}\right),$$

$$e_Z=\frac{c_{\rm dt}}{4}\left(Q_{\mu,1Z,0Z}+Q_{\mu,0Z,1Z}\right)/Q_Z. \tag{15}$$

结合以上参数和公式, 代入下面密钥率公式, 即可得到安全密钥率[12]大小:

$$R=-Q_Z f h\left(e_Z\right)+Q^{(1)}_Z\left(1-I_{\rm E}\right), \tag{16}$$

其中, f 为系统纠错系数; $I_{\rm E}$ 为 Eve 获取的信息量. 通过对上述参数求解, 可以计算出最终密钥.

3 数值仿真结果及分析讨论

在数值仿真中, 使用合理的实验系统参数[12], 如表 1 所列.

为了更直观地说明光源端和探测端不同设备缺陷对 LT-RFI 协议的影响, 基于 WCS 且考虑有限长效应的 RFI 协议的密钥率随距离的变化曲线如图 1 所示. 其中, 实线表示不考虑态制备误差容忍下 RFI 协议的结果, 虚线对应 LT-RFI 协议的结果.

图 1 基于 RFI 协议和 LT-RFI 协议分别比较了两种不同缺陷条件下的安全密钥率. 图 1(a), (b) 中从上到下实线分别依次表示 $\delta\left(P_{\rm ap}\right)$ 为 0(0), 0.2004 (5%) 和 0.3006(10%) 的 RFI 协议的安全密钥率曲线; 从上到下的折点线则分别依次代表与对应实线 $\delta\left(P_{\rm ap}\right)$ 相同的 LT-RFI 协议的安全密钥率曲线. 当 $\delta=0.3006$ 时, 与理想状态相比, 与传统 RFI 不同, 在估算不同基的比特误码率时, 不是直接对不完美态进行投影测量计算, 而是通过引入虚拟态、虚拟协议和过渡矩阵, 对测量过程做了一定变换和优化处理, 原理上降低了态制备误差对估算结果的影响. 但是, 在此过程中不可避免地增加了一些统计量参与估算, 在考虑有限长效应时, 在一定程度上增加了有限长效应的影响, 故在态制备误差为 0 时, LT 协议的码率相比于传统 RFI 协议有一定的下降; 随着态制备误差的增大, LT 协议的鲁棒性和优势才逐渐显示出来. 与理想状态相比 ($\delta=0.3006$), LT-RFI(RFI) 协议的密钥率下降了约 1/2 (4/5), 最远传输距离减小了 5(12) km.

同样, 当 $P_{\rm ap}$ =10% 时, LT-RFI (RFI) 协议比后脉冲大小为 0 条件下的密钥率下降了 1/2 (3/4), 最远传输距离减小了 6 (25) km. 值得注意的是, 与传统 RFI 不同, LT-RFI 在估算不同基的单光子比特误码率时, 不是直接使用对不完美态做投影测量的结果进行计算, 而是通过引入虚拟态、虚拟协议和传输矩阵, 对测量过程进行一定变换和优化处理, 原理上降低了态制备误差对估算结果的影响. 但是, 在此过程中不可避免地增加了一些统计量参与估算过程, 因此, 在一定程度上增加了有限长效应的影响, 故在态制备误差为 0 时, LT 协议的码率相比于传统 RFI 协议有一定下降, 于是图 1 中

表 1 基于后脉冲效应和死时间效应的 LT-RFI 协议仿真参数列表

Table 1. Parameter list used in simulation of LT-RFI protocol based on after-pulse effect and dead time effect.

Bob探测器暗计数率 $P_{\rm dc}$	Bob探测器效率 $\eta_{\rm Bob}$	系统纠错系数 f	Alice发送的总脉冲数 N	系统重复频率 F	信道损耗系数 α /(dB·km^{-1})	系统本底误码 $e_{\rm d}$
3×10^{-6}	0.145	1.16	10^{12}	10^9	0.2	0.0015

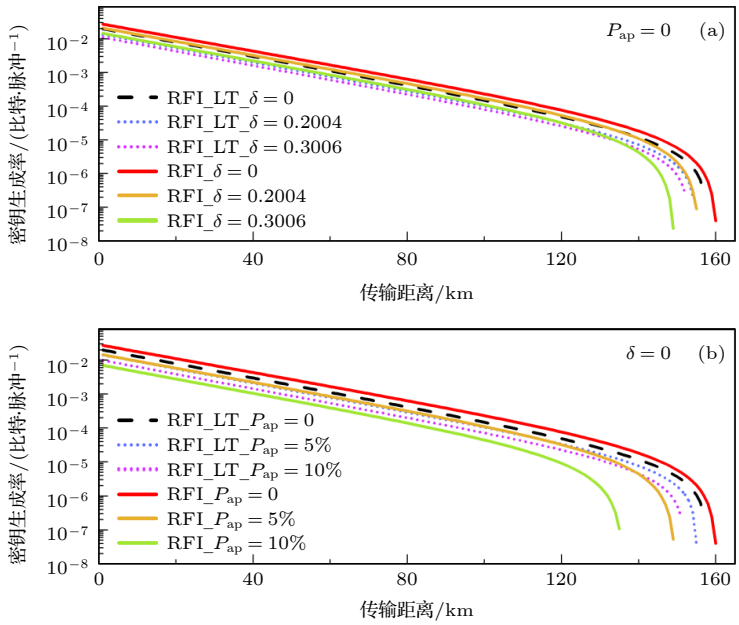

图 1 (a) 基于态制备缺陷 δ 的 RFI 协议以及 LT-RFI 协议的密钥生成率图; (b) 基于后脉冲效应 P_{ap} 的 RFI 协议以及 LT-RFI 协议的密钥生成率图

Fig. 1. (a) Key generation rates of the RFI protocol and LT-RFI protocol based on state preparation flaws δ; (b) the key generation rates of the RFI protocol and LT-RFI protocol based afterpulse effect P_{ap}.

出现态制备误差为 0 时, 红色实线略高于黑色虚线的现象; 但随着态制备误差的增大, LT 协议的鲁棒性和优势又逐渐显示出来.

图 2 给出了同时考虑态制备缺陷和后脉冲效应条件下的密钥率结果. 当态制备缺陷 $\delta=0.2004$, $P_{ap}=5\%$ 时, RFI 协议的密钥率比理想情况 ($\delta=0$, $P_{ap}=0$) 下该协议的密钥率降低了 67%, 最远传输距离减小了 18 km. 而我们提出的实用性 LT-RFI 协议的密钥率仅仅降低了 50%, 最远传输距离减小 5 km. 此外, 当 $\delta=0.3006$, $P_{ap}=10\%$ 时, RFI 协议的密钥率比理想情况下的密钥率降低了一个数量级以上, 最远传输距离更是急剧减小 45 km. 与之相比, LT-RFI 协议的密钥率虽然降低了 70%, 但最远传输距离仅仅减小了 10 km. 通过以上结果可以得出, 基于诱骗态方法的传统 RFI协议虽然对态制备缺陷和后脉冲效应具有一定的鲁棒性, 但依旧不如 LT-RFI 协议. 主要由于与传统的 RFI 协议相比, LT-RFI 协议除了对态制备误差具有鲁棒性, 对探测端的后脉冲效应也具有良好的鲁棒性. 主要原因与上面类似, LT-RFI 协议通过引入虚拟态、虚拟协议和传输矩阵, 对测量过程做了一定变换和优化处理, 原理上降低了测量端的不完美对估算结果的影响, 从而使得 Eve 获取的信息量降低, 从而具有更好的鲁棒性.

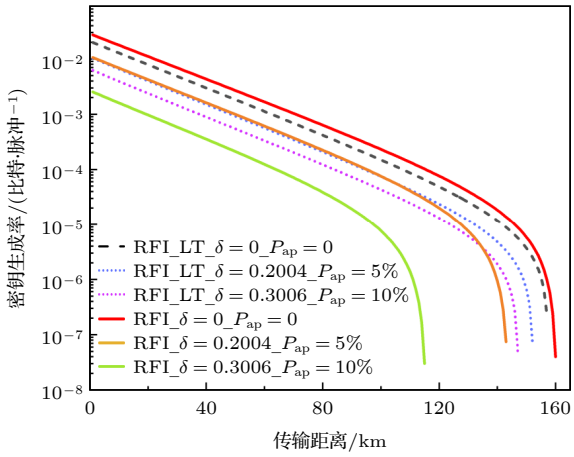

图 2 基于态制备缺陷和后脉冲效应的 RFI 协议以及 LT-RFI 协议的密钥生成率图

Fig. 2. Key generation rates of the RFI protocol and LT-RFI protocol based on state preparation flaws and afterpulse effect.

如图 3 所示, 当不考虑态制备缺陷时, RFI 协议中 Eve 获取的信息量明显要高于 LT-RFI 协议对应的 Eve 获取的信息量. 在距离相同的条件下, 随着态制备缺陷 δ 和后脉冲概率 P_{ap} 的增大, 前者显著增大, 而 LT-RFI 协议对应的 Eve 获取的信息量仅略微增加. 这是由于在 LT-RFI 协议中使用的虚拟比特误密钥率更加紧致地估计了相位误密钥率, 进而更加紧致地估计 Eve 获取的信息量.

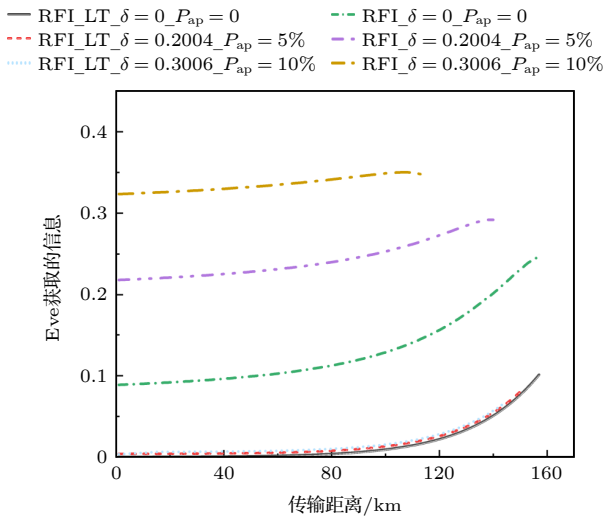

图 3 基于态制备缺陷和后脉冲效应的 RFI 协议与 LT-RFI 协议的 Eve 获取的信息量

Fig. 3. Information leakage to Eve of the RFI protocols and LT-RFI protocols based on state preparation flaws and after-pulse effect.

为了进一步展示不同设备缺陷同时对 LT-RFI 协议造成的影响, 下面给出了基于态制备缺陷、后脉冲效应和死时间效应的 LT-RFI 协议的密钥率随距离变化的曲线, 如图 4 所示. 其中, 黑色实线表示 3 种设备缺陷都为 0 的密钥率结果, 红色实线与绿色虚线表示 $\delta = 0.2004$, $P_{ap} = 5\%$ 但死时间大小不同的密钥率结果. 为了更好地表现 LT-RFI 协议的性能, 对 3 种缺陷进行放大 ($\delta = 0.3006$, $P_{ap} = 10\%$ 且 $\tau_{dt} = 1$ μs) 并对密钥率进行仿真 (紫色虚线). 结果表明, 当同时考虑这 3 种设备缺陷时, LT-RFI 协议的传输距离和安全密钥率有不同程度的下降. 通过对比红色实线与绿色虚线发现死时间效应会导致短距离内的密钥率大幅下降, 但这种影响会随着距离的增大而下降, 因此最远传输距离下的密钥率几乎相同. 此外, 与绿色虚线相比, 紫色虚线的 3 种缺陷分别是前者的 1.5 倍、2 倍与 50 倍, 后者的密钥率减小了一个数量级, 但最远传输距离仅减小 5 km. 因此, 对于 LT-RFI 协议, 死时间效应只是在近距离时进一步降低密钥率, 而没有影响最远传输距离.

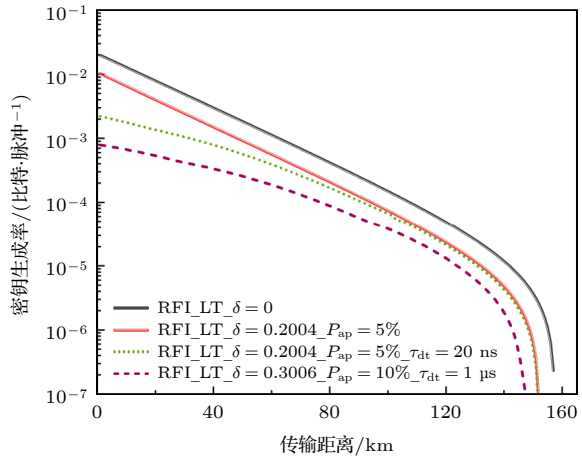

图 4 基于不同设备缺陷的 RFI 协议以及 LT-RFI 协议密钥生成率图

Fig. 4. Key generation rates of the RFI protocol and LT-RFI protocol based on different defects in equipments.

4 结 论

本文提出了一种同时考虑光源端与探测器缺陷的实用化态制备误差容忍参考系无关 QKD 协议. 本文首先考虑了 QKD 系统中光源的不完美性, 将发送端制备态误差大小进行刻画并代入安全性分析之中, 并考虑了损耗容忍方法. 然后进一步考虑了探测器的不完美性 (后脉冲效应和死时间效应) 对该协议的影响. 以三强度诱骗态方法为例来进行模型构建和参数估计方法介绍, 同时开展相应数值仿真计算. 结果表明, 本文提出的协议通过利用虚拟态测量相位误密钥率不仅减小了态制备缺陷对密钥率的影响, 还对探测器端的缺陷 (后脉冲效应、死时间效应) 更具有鲁棒性.

需要指出, 本文对 RFI QKD 的分析中, 在接收端使用了两个单光子探测器来构建模型, 为了简化计算, 在仿真中假设两个探测器的性能完全一致. 倘若两个探测器性能不一致, 如探测效率和暗计数等, 则可能会引入一定安全隐患, 进而降低整个 QKD 系统的实际性能 [24,25]. 当然, 在实际应用中, 不同探测器的性能不可避免存在一定差异, 是需要实际考虑和解决的问题, 也将成为我们后继的工作重点之一. 本方法还可以拓展到其他安全性等级更高的量子密钥分发协议, 如与测量设备无关的量子密钥分发协议 [26–30] 以及双场量子密钥分发 [31,32] 等, 进一步降低实用化进程中 QKD 系统因器件缺陷所带来的不利影响. 因此, 本文工作将对 QKD 系统的实用化起到一定推进作用.

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) pp175–179

[2] Brassard G, Lütkenhaus N, Mor T, Sanders B C 2000 *Phys. Rev. Lett.* **85** 1330
[3] Yuan Z, Plews A, Takahashi R, Doi K, Tam W, Sharpe A W, Dixon A R, Lavelle E, Dynes J F, Murakami A, Kujiraoka M, Lucamarini M, Tanizawa Y, Sato H, Shields A J 2018 *J. Light. Technol.* **36** 16
[4] Boaron A, Korzh B, Houlmann R, Boso G, Rusca D, Gray S, Li M, Nolan D, Martin A, Zbinden H 2018 *Appl. Phys. Lett.* **112** 17
[5] Minder M, Pittaluga M, Roberts G, Lucamarini M, Dynes J F, Yuan Z L, Shields A J 2019 *Nat. Photonics* **13** 5
[6] Liu Y, Yu Z W, Zhang W, Guan J Y, Chen J P, Zhang C, Hu X L, Li H, Jiang C, Lin J, Chen T Y, You L, Wang Z, Wang X B, Zhang Q, Pan J W 2019 *Phys. Rev. Lett.* **123** 100505
[7] Bennett C H, Bessette F, Brassard G, Salvail L, Smolin J 1992 *J Cryptol* **5** 3
[8] Kurtsiefer C, Zarda P, Halder M, Weinfurter H, Gorman P M, Tapster P R, Rarity J G 2002 *Nature* **419** 450
[9] Laing A, Scarani V, Rarity J G, O'Brien J L 2018 *Phys. Rev. A* **82** 012304
[10] Gottesman D, Lo H K, Lütkenhaus N, Preskill J 2004 *Quantum Inf. Comput.* **4** 325
[11] Tamaki K, Curty M, Kato G, Lo H K, Azuma K 2014 *Phys. Rev. A* **90** 052314
[12] Wang C, Sun S H, Ma X C, Tang G Z, Liang L M 2015 *Phys. Rev. A* **92** 042319
[13] Xu F H, Wei K J, Sajeed S, Kaiser S, Sun S H, Tang Z Y, Qian L, Makarov V, Lo H K 2015 *Phys. Rev. A* **92** 032305
[14] Tang Z Y, Wei K J, Bedroya O, Qian L, Lo H K 2016 *Phys. Rev. A* **93** 042308
[15] Zhou X Y, Ding H J, Zhang C H, Li J, Zhang C M, Wang Q 2020 *Opt. Lett.* **45** 4176
[16] Fan Y G J, Wang C, Wang S, Yin Z Q, Liu H, Chen W, He D Y, Han Z F, Guo G C 2018 *Phys. Rev. Appl.* **10** 064032
[17] Campbell L 1992 *Rev. Sci. Instrum.* **63** 5794
[18] Rusca D, Boaron A, Grünenfelder F, Martin A, Zbinden H 2018 *Appl. Phys. Lett.* **112** 171104
[19] Mo X F 2006 *Ph. D. Dissertation* (Hefei: University of Science and Technology of China) (in Chinese) [莫小范 2006 博士毕业论文 (合肥: 中国科学技术大学)]
[20] Wang W J, Zhou X Y, Zhang C H, Ding H J, Wang Q 2022 *Quantum Inf. Process* **21** 1
[21] Fan Y G J 2020 *Ph. D. Dissertation* (Hefei: University of Science and Technology of China) (in Chinese) [范元冠杰 2020 博士毕业论文 (合肥: 中国科学技术大学)]
[22] Wang X B 2005 *Phys. Rev. Lett.* **94** 30503
[23] Ma X, Sun M S, Liu J Y, Ding H J, Wang Q 2022 *Acta Phys. Sin.* **71** 030301 (in Chinese) [马啸, 孙铭铄, 刘靖阳, 丁华建, 王琴 2022 物理学报 **71** 030301]
[24] Fung C F, Tamaki K, Qi B, Lo H K, Ma X F 2009 *Quantum Inf. Comput.* **9** 1533
[25] Sun S H, Xu F H 2021 *New J. Phys.* **23** 023011
[26] Zhou Y H, Yu Z W, Wang X B 2016 *Phys. Rev. A* **93** 042324
[27] Zhang C H, Zhang C M, Guo G C, Wang Q 2018 *Opt. Express* **26** 4219
[28] Zhou X Y, Zhang C H, Zhang C M, Wang Q 2017 *Phys. Rev. A* **96** 052337
[29] Jiang C, Yu Z W, Hu X L, Wang X B 2021 *Phys. Rev. A* **103** 012402
[30] Huang L Y, Zhang Y C, Yu S 2021 *Chin. Phys. Lett.* **38** 040301
[31] Lucamarini M, Yuan Z L, Dynes J F, Shields A J 2018 *Nature* **557** 400
[32] Wang X B, Yu Z W, Hu X L 2018 *Phys. Rev. A* **98** 062323

Study of practical state-preparation error tolerant reference-frame-independent quantum key distribution protocol*

Zhou Yang [1)2)#] Ma Xiao [1)2)#] Zhou Xing-Yu [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 of Ministry of Education, Nanjing University of Posts and Telecommunications, Nanjing* 210003, *China*)

(Received 15 July 2023; revised manuscript received 7 September 2023)

Abstract

Quantum key distribution (QKD) enables the establishment of shared keys between two distant users, Alice and Bob, based on the fundamental principles of quantum mechanics, and it has proven to possess information-theoretic security. In most of QKD systems, Alice and Bob require a shared reference frame, and real-time calibration of the reference frame increases system costs and reduces its performance. Fortunately, the reference-frame-independent QKD protocol has been proposed, overcoming reference-frame drift issues and receiving widespread attention. However, in practical QKD systems, the non-ideal characteristics of realistic devices introduce certain inconsistency between the theory and the practice. In real-world quantum key distribution systems, device imperfections can lead to security vulnerabilities, thereby reducing system security. For example, imperfections in the encoding apparatus at the source end may result in errors in the quantum states. The inherent defects in the detection part may cause after-pulse effects and dead-time effects, thus reducing the key rate. Therefore, in this work, we propose a practical state-preparation error tolerant reference-frame-independent quantum key distribution protocol by taking imperfections in both the source and the detectors into account. Moreover, a three-intensity decoy-state scheme for modeling analysis and numerical simulations is employed. In this protocol, we reduce the influence of state-preparation errors on the key rate by utilizing virtual state methods to precisely estimate the phase-error rate. Furthermore, by characterizing the effects of after-pulses and dead-time on the key rate, our protocol exhibits higher robustness and can effectively address issues related to detector imperfections. This approach can also be extended to other quantum key distribution protocols with higher security levels, such as measurement-device-independent quantum key distribution protocol and twin-field quantum key distribution, further mitigating the influence of device imperfections on practical implementation of QKD system. Therefore, our present work provide important reference value for putting the quantum key distributions into practical application.

Keywords: quantum key distribution, state preparation error, reference-frame-independent protocol, after-pulse effect, dead-time effect

PACS: 03.65.–w, 03.67.Hk, 42.50.Ex, 42.79.Sz **DOI:** 10.7498/aps.72.20231144

* Project supported by the National Natural Science Foundation of China (Grant Nos. 12074194, 11774180), the Leading-edge Technology Program of Natural Science Foundation of Jiangsu Province, China (Grant No. BK20192001), the Industrial Prospect and Key Core Technology Projects of Key R & D Program of Jiangsu Province, China (Grant No. BE2022071), and the Postgraduate Research & Practice Innovation Program of Jiangsu Province, China (Grant Nos. KYCX20_0726, KYCX23_1039).

# 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

实用化态制备误差容忍参考系无关量子密钥分发协议

周阳 马啸 周星宇 张春辉 王琴

Study of practical state-preparation error tolerant reference-frame-independent quantum key distribution protocol

Zhou Yang Ma Xiao Zhou Xing-Yu Zhang Chun-Hui Wang Qin

引用信息 Citation: Acta Physica Sinica, 72, 240301 (2023) DOI: 10.7498/aps.72.20231144
在线阅读 View online: https://doi.org/10.7498/aps.72.20231144
当期内容 View table of contents: http://wulixb.iphy.ac.cn