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

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

马啸 孙铭烁 刘靖阳 丁华建 王琴

State preparation error tolerant quantum key distribution protocol based on heralded single photon source

Ma Xiao Sun Ming-Shuo Liu Jing-Yang Ding Hua-Jian Wang Qin

引用信息 Citation: Acta Physica Sinica, 71, 030301 (2022) DOI: 10.7498/aps.71.20211456
在线阅读 View online: https://doi.org/10.7498/aps.71.20211456
当期内容 View table of contents: http://wulixb.iphy.ac.cn

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*

马啸 1)2) 孙铭烁 1)2) 刘靖阳 1)2) 丁华建 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技术教育部重点实验室, 南京 210003)

(2021 年 8 月 7 日收到; 2021 年 9 月 11 日收到修改稿)

在实际量子密钥分发系统中, 由于设备、器件存在缺陷, 在量子态制备过程中往往存在误差, 而这些态制备误差会导致一定的系统安全性漏洞. 本文在 Tamaki 等 (*Phys. Rev. A* **90** 052314) 的工作基础之上, 提出了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. 本文将发送端制备态误差进行参数刻画并带入量子密钥协议安全性分析之中, 避免了实际应用中由于态制备装置的不理想可能引入的安全性漏洞, 提高了系统的安全性. 同时, 为了方便起见, 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. 仿真结果显示, 本文提出的协议对态制备误差具有很好的鲁棒性. 同时, 由于标记单光子源具有真空脉冲概率低的优点, 与此前基于弱相干态脉冲的同类协议相比, 我们的协议在传输距离较远时能够显示出更优的性能. 因而, 该工作有望为未来发展长距离量子保密通信应用与研究提供重要的参考价值.

关键词: 量子密钥分发, 标记单光子源, 误差容忍协议, 态制备误差

PACS: 03.65.–w, 03.67.Hk, 42.50.Ex, 42.79.Sz **DOI:** 10.7498/aps.71.20211456

1 引 言

量子密钥分发 (quantum key distribution, QKD) 协议主要利用量子态编码信息来实现密钥安全分发的目的, 其安全性基于量子力学基本原理, 理论上具有无条件安全性[1−5]. 在实际应用中, 通信的双方通过 QKD 结合“一次一密”操作[6], 可以实现无条件安全的保密通信, 在避开泄漏隐患的同时, 也降低了保存密码本的资源与成本, 因此受到了广泛关注. 在早期的 QKD 协议安全性分析过程中, 如原始的 GLLP 协议[7], 没有考虑态制备误差, 一般假定量子态的制备过程是理想的. 而在实际实验条件下, 由于设备存在缺陷, 比如相位调制器、偏振调制器等器件存在调制误差, 导致态制备存在误差, 降低了系统的现实安全性. 随着研究的深入, 将态制备误差考虑进量子密钥协议安全性分析过程中的思想引起研究者的关注. 2014 年, Tamaki 等[8] 在 GLLP 协议[7] 的基础上考虑了调制误差在内的源缺陷, 提出了一种误差容忍 (loss tolerant, LT) QKD 协议. 随后徐飞虎等[9] 和唐志远等[10] 分别在实验上进行了演示验证. 在此基础之上, 一系列与光源安全性相关的研究工作相继开展[11−15].

不过, 以上研究工作使用的大多数是弱相干态光源 (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, 因而使得基于 WCS 的误差容忍协议的最远安全

* 国家重点研发计划 (批准号: 2018YFA0306400, 2017YFA0304100)、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) 和江苏省研究生科研创新计划 (批准号: KYCX20_0726, KYCX19_0951) 资助的课题.

† 通信作者. E-mail: qinw@njupt.edu.cn

传输距离收到一定限制. 针对以上问题, 本文提出了基于一种基于标记单光子源 (heralded single-photon source, HSPS) 的态制备误差容忍 (state preparation error tolerant, SPT) 量子密钥分发协议, 并且以三强度诱骗态方案 [16,17] (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.

2 HSPS 与 WCS 光源比较

标记单光子源一般由参量下转换 (PDC) 过程产生, 其产生示意图如图 1 所示. 泵浦激光作用在非线性晶体上, 经 PDC 过程产生分布一致的双模压缩光场, 即参量光, 其中一路通常称为信号光 (signal), 另一路称为休闲光 (idler)[18–22]. 选择合适的实验条件, 可以使参量光服从热分布或是泊松分布 [23,24]. 本文以具有泊松分布的参量光为例来进行介绍.

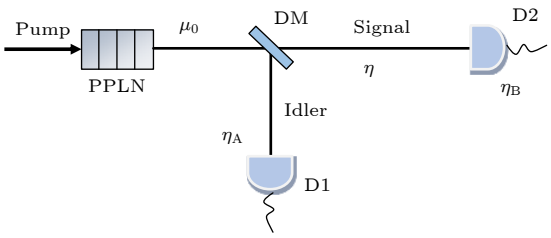

图 1 实际系统中的标记单光子源的光路装置模型

Fig. 1. Model of optical path device for marking single photon source in experimental system.

如图 1 所示, 参量光经二向色镜 (DM) 分开后, 其中休闲光经本地探测器 (D1) 探测后, 产生同步电信号, 可以对信号光起到标记作用. 被标记后的信号光被称为标记单光子源 (HSPS), 在光子数空间可表示为: $\rho_l = \sum_{i=0}^{\infty} b_i^l |i\rangle\langle i|$, 其中 l 为每脉冲包含的平均光子数; b_i^l 为在 l 平均光子数强度下包含 i 光子态的概率. 假如本地探测器的探测效率和暗计数率分别记为 $\eta_{\rm A}$ 和 $d_{\rm A}$, 则被标记后的光子数分布可表示为: $b_i^l = [1-(1-d_{\rm A})\cdot(1-\eta_{\rm A})^i]\cdot\dfrac{l^i}{i!}\cdot {\rm e}^{-l}$. 在 QKD 过程中, 发送方 Alice 在本地制备 HSPS, 然后通过量子信道发送给接收方 Bob, Bob 使用探测器 D2 进行探测, 探测器效率为 $\eta_{\rm B}$.

表 1 比较了在平均光子数强度为 0.4 时, HSPS 与 WCS 两种光源中不同光子数脉冲在总脉冲数中所占概率 (此处假设 $\eta_{\rm A}=0.75$, $d_{\rm A}=10^{-6}$)[23–25]. 由表 1 可见, WCS 中包含大量的正空脉冲的比例, 而 HSPS 中包含真空态脉冲的概率几乎可以忽略不计.

表 1 在平均光子数强度为 0.4 时, WCS 和 HSPS 光源中不同光子数脉冲出现的概率

Table 1. Proportion of different photon number pulses in WCS and HSPS when the average photon intensity is 0.4.

光源类型	光子分布		
	真空态	单光子	多光子
WCS	0.743218	0.221746	0.035036
HSPS	7.432×10^{-7}	0.454683	0.545316

3 理论模型

在实际的 QKD 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, 若不对此种情况加以考虑, 窃听者 Eve 可能会利用这一安全性漏洞进行攻击, 窃取信息从而导致系统性能的下降. 针对这一问题, 我们提出了基于标记单光子源的态制备误差容忍量子密钥分发协议, 该协议通过将态制备误差加以刻画, 将其纳入考虑范围, 使得窃听者不能利用这一缺陷窃取信息, 理论上减小了系统对量子态制备过程的漏洞, 使得该模型的结果可以对误差具有一定程度的容忍性能, 模型的鲁棒性得以增强. 并且研究了该协议在不同态制备误差条件下的性能.

3.1 计算相位误码率 e_X

首先, Alice 利用相位调制器随机制备三种量子态 $\{|\varphi_{0Z}\rangle, |\varphi_{1Z}\rangle, |\varphi_{0X}\rangle\}$. 由于现实环境下相位编码或偏振编码等系统在态制备过程存在一定的缺陷, 制备出的量子态本身不可避免地会与预期存在一定偏差, 通过借鉴文献 [8] 中的定义, 对量子态中的误差刻画如下:

$$\begin{aligned}
&|\varphi_{0Z}\rangle = |0_Z\rangle,\\
&|\varphi_{1Z}\rangle = -\sin\frac{\delta}{2}|0_Z\rangle + \cos\frac{\delta}{2}|1_Z\rangle,\\
&|\varphi_{0X}\rangle = \cos\left(\frac{\pi}{4}+\frac{\delta}{4}\right)|0_Z\rangle + \sin\left(\frac{\pi}{4}+\frac{\delta}{4}\right)|1_Z\rangle, \quad (1)
\end{aligned}$$

其中 δ ($\delta \geqslant 0$) 表示相位调制器 (PM) 或偏振调制器 (PR) 与预期结果相比的调制偏差, 也称为态制备误差 [8].

我们所选用的标记单光子源采用了光子对纠缠的方法, 在纠缠的光子对中假定一个光子到达的时间可以由另外一个光子表示. 由于纠缠的光子具有同时性, 通过被指示的那个光子到达时间标记, 可以较为准确地控制探测器的开关时间以降低真空脉冲和多光子脉冲的概率值, 从而提高单光子脉冲的概率, 有效地减少长距离量子密钥分发过程中暗计数的影响, 进而增加系统的安全传输距离 [23,24,26].

基于纠缠协议, Alice 发送量子态等价于制备量子态, 具体表示如下:

$$|\Psi_X\rangle_{\mathrm{AA_eB}} = |0_X\rangle_{\mathrm{A}}|\varphi_{0X}\rangle_{\mathrm{A_eB}},$$
$$|\Psi_Z\rangle_{\mathrm{AA_eB}} = \frac{1}{\sqrt{2}}\sum_{j=0,1}|j_Z\rangle_{\mathrm{A}}|\varphi_{jZ}\rangle_{\mathrm{A_eB}}, \tag{2}$$

其中 A 表示 Alice 方所拥有的系统, $\mathrm{A_e}$ 表示 Alice 拥有的扩展系统, B 表示发送给 Bob 方的系统, Alice 经过选基测量系统 A 后发送系统 B 给 Bob 方. (2) 式表述的是 Alice 针对发送量子态的态制备过程, 是态制备的等价纠缠态. 通过 (2) 式可以看出, Alice 在选择 X 基时只制备对应于比特 0 的量子态, 选择 Z 基时制备对应于比特 0 与比特 1 的量子态, 制备的量子态可以通过偏振编码或者相位编码应用于量子密钥分发过程. 该态制备过程不依赖于具体光源, 同样适用于 HSPS 光源.

接下来, 考虑一个虚拟协议: 发送方制备量子态 $|\Psi_Z\rangle_{\mathrm{AA_eB}}$后开始进行虚拟态的传输. Alice 发送的虚拟态: $\hat{\sigma}_{\mathrm{B};j_X,\mathrm{vir}} = \mathrm{tr}_{\mathrm{AA_e}}[\hat{P}(|j_X\rangle_{\mathrm{A}}) \otimes I_{\mathrm{A_eB}}\hat{P}(|\Psi_Z\rangle_{\mathrm{AA_eB}})]$ 位于 X-Z 平面, 其中 $\hat{P}(x) = |x\rangle\langle x|$且 $\mathrm{tr}_{\mathrm{AA_e}}$表示偏迹过程. 其归一化形式可以表示为一组单位矩阵 $\hat{\sigma}_{\mathrm{I}}$及泡利矩阵 $\hat{\sigma}_t$的线性组合: $\hat{\sigma}'_{\mathrm{B};j_X,\mathrm{vir}} = \frac{1}{2}\times\left(\hat{\sigma}_{\mathrm{I}} + \sum_{t=X,Y,Z} P_t^{j_X,(\mathrm{vir})}\hat{\sigma}_t\right)$, $P_t^{j_X,(\mathrm{vir})}$ 为对应的 Bloch 系数.

然后将定义相位误码率定征为 X 基的虚拟比特误码率, 表达式如下表示:

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

若要求虚拟协议下的比特误码率, 首先要求出虚拟协议下的传输速率 $Y_{s_X,j_X}^{(Z)\mathrm{vir}}$. 研究表明, 虚拟态传输速率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者构成, 具体表示如下:

$$Y_{s_X,j_X}^{(Z)\mathrm{vir}} = \mathrm{tr}\left[\hat{\sigma}_{\mathrm{B};j_X,\mathrm{vir}}\right]\mathrm{tr}\left[\hat{D}_{s_X}\hat{\sigma}'_{\mathrm{B};j_X,\mathrm{vir}}\right]/2, \tag{4}$$

其中参数 $\mathrm{tr}[\hat{\sigma}'_{\mathrm{B};j_X,\mathrm{vir}}]$为 Alice 发送虚拟态的概率, $\hat{\sigma}'_{\mathrm{B};j_X,\mathrm{vir}}$ 为$\hat{\sigma}_{\mathrm{B};j_X,\mathrm{vir}}$ 的归一化形式, 参数$\mathrm{tr}[\hat{D}_{s_X}\hat{\sigma}'_{\mathrm{B};j_X,\mathrm{vir}}]$为虚拟态在对应基下成功测量的概率. 泡利算符$\hat{\sigma}_t$的信道传输速率与对应基成功测量概率关系为: $q_{s_X|t} = \mathrm{tr}[\hat{D}_{s_X}\hat{\sigma}'_t]/2$. 通过变量代换, 虚拟态传输速率表示如下:

$$Y_{s_X,j_X}^{(Z)\mathrm{vir}} = \mathrm{tr}\left[\hat{\sigma}_{\mathrm{B};j_X,\mathrm{vir}}\right]\Big(q_{s_X|\mathrm{Id}} + P_X^{j_X,(\mathrm{vir})}q_{s_X|X} + P_Z^{j_X,(\mathrm{vir})}q_{s_X|Z}\Big). \tag{5}$$

考虑到真实态也位于 X-Z 平面, 由实验数据, 可以得出实际传输速率表达式为 $Y_{s_X,j_\alpha}^{(\alpha)} = P(j_\alpha)\,\mathrm{tr}[\hat{D}_{s_X}\hat{\rho}_{j\alpha}]/2$. 经过变量代换, 可以表示如下:

$$Y_{s_X,j_\alpha}^{(\alpha)} = P(j_\alpha)\left(q_{s_X|\mathrm{Id}} + P_X^{j\alpha}q_{s_X|X} + P_Z^{j\alpha}q_{s_X|Z}\right)/2, \tag{6}$$

其中参数 $P(j_\alpha)$表示 Alice 方实际发射 $\hat{\rho}_{ja}$态的概率, 分母表示 Bob 选基的概率, $q_{s_X|t}$表示 σ_t的传输速率. 进而可得出实际传输速率的表示形式:

$$\begin{aligned}&\left(q_{s_X|\mathrm{Id}}, q_{s_X|X}, q_{s_X|Z}\right)\\ &= 6\cdot\left(Y_{s_X,0_Z}^{(Z)}, Y_{s_X,1_Z}^{(Z)}, Y_{s_X,0_X}^{(X)}\right)\cdot\hat{A}^{-1},\end{aligned} \tag{7}$$

其中 $\hat{A} = (\boldsymbol{V}_{0Z}^{\mathrm{T}}, \boldsymbol{V}_{1Z}^{\mathrm{T}}, \boldsymbol{V}_{0X}^{\mathrm{T}})$, 且 $\boldsymbol{V}_{j\alpha} = (1, P_X^{j\alpha}, P_Z^{j\alpha})$. 由此分别得出了虚拟态传输速率、实际传输速率与信道传输速率的关系.

本文通过建立等价虚拟协议, 不仅可以针对目标参数——相位误码率 e_X 进行了准确表征, 而且在真实的 QKD 协议框架中, 测得实际传输速率结果后, 通过分别探寻实际传输速率、虚拟态传输速率与信道参数 $q_{s_X|t}$的数学关系, 以信道参数 $q_{s_X|t}$为媒介可以反向求出虚拟态传输速率, 最后代入相位误码的表达式得出结果大小.

3.2 单光子脉冲增益 Q_1 与系统增益 Q_μ

为了计算最终安全密钥生成率, 需要对单光子的穿透率 (Y_1) 下界和单光子的误码率 (e_1) 上界进行估计. 理想情况下, Alice 发送 n 光子, 接收方探测器响应的概率 Y_n 为

$$\begin{aligned}Y_n = {}& 0.5 + 0.5\cdot(1-d_{\mathrm{B}})\cdot\big[1 + (\eta\cdot C_{s\alpha|j\gamma} - \eta)^n\\ &- (1-\eta\cdot C_{s\alpha|j\gamma})^n - (1-d_{\mathrm{B}})(1-\eta)^n\big],\end{aligned} \tag{8}$$

其中 $C_{s\alpha|j\gamma}$表示接收端选择 α作为测量基时对$|\varphi_{j\gamma}\rangle$态进行测量并获得强度 S 的理想概率. η 代表光子从 Alice 端到 Bob 端的传输效率, 其表达式可写

表 2 基于 HSPS 的三强度诱骗态态制备误差容忍 QKD 协议仿真使用的参数列表

Table 2. Parameter list used in simulation of state-preparation-error tolerant QKD protocol for three strength decoy states based on HSPS.

Bob探测器暗计数率 $d_{\rm B}$	Bob探测器效率 $\eta_{\rm B}$	系统纠错系数 f	Alice探测器暗计数率 $d_{\rm A}$	Alice探测器探测效率 η_A	信道损耗系数 α /(dB·km^{-1})
0.5×10^{-6}	0.15	1.22	10^{-6}	0.75	0.2

为: $\eta=\eta_{\rm B}\cdot10^{-\alpha l/10}$, 其中 α 为信道的衰减系数, l 为信道的长度. 光子态增益由光源分布 b_i^l 以及探测器响应概率 Y_n 组成, 由于增益受到 HSPS 光源亚泊松分布的影响, 其表达式所示如下:

$$Q^{\mu}_{Zi,Zj}=\sum_{n=0}^{\infty}Y_n[1-(1-d_A)\cdot(1-\eta_A)^n]\frac{\mu^n}{n!}e^{-\mu}, \quad (9)$$

$$Q^{v}_{Zi,Zj}=\sum_{n=0}^{\infty}Y_n[1-(1-d_A)\cdot(1-\eta_A)^n]\frac{v^n}{n!}e^{-v}. \quad (10)$$

将增益的求和定义式进行展开, 进行不同的放缩移项, 分别利用信号态增益、单光子增益与单光子响应率的关系, 可以得到使用 HSPS 光源时单光子脉冲响应率的上下界、单光子的增益 (Q_1) 以及系统总增益 (Q_μ), 具体表示如下:

$$Y_1^U=\frac{Q_\nu {\rm e}^{\nu}-Y_0\cdot d_{\rm A}}{\nu[1-(1-d_{\rm A})\cdot(1-\eta_{\rm A})]}, \quad (11)$$

$$Y_1^L=\frac{\mu\left(Q_v{\rm e}^{\nu}-Q_\mu{\rm e}^{\mu}\dfrac{\nu^2}{\mu^2}-\dfrac{\mu^2-\nu^2}{\mu^2}Y_0\cdot d_{\rm A}\right)}{\mu\nu-\nu^2[1-(1-d_{\rm A})\cdot(1-\eta_A)]}, \quad (12)$$

$$Q_1=[1-(1-d_{\rm A})\cdot(1-\eta_{\rm A})]{\rm e}^{-\mu}\cdot\mu\cdot\sum_{(i,j=0,1)}Y^{1L}_{Zi,Zj}, \quad (13)$$

$$Q_\mu=\frac{(Q^{\mu}_{Z0,Z0}+Q^{\mu}_{Z0,Z1}+Q^{\mu}_{Z1,Z0}+Q^{\mu}_{Z1,Z1})}{4}. \quad (14)$$

3.3 密钥生成率 R

系统量子比特误码率 E_μ 定义为

$$E_\mu=W_\mu/Q_\mu, \quad (15)$$

$$W_\mu=\frac{(Q^{\mu}_{Z0,Z1}+Q^{\mu}_{Z1,Z0})}{4}. \quad (16)$$

将以上参数代入下面密钥率公式, 即可计算密钥率大小:

$$R=-\{Q_1[1-h(e_X)]-f\cdot Q_\mu\cdot h(E_\mu)\}, \quad (17)$$

其中, f 为系统纠错系数; e_X 为相位误码率; E_μ 为系统量子比特误码率; $h(x)$ 为香农熵函数: $h(x)=-x\log_2(x)-(1-x)\log_2(1-x)$; 通过求解前面参数, 可以算出最终的安全密钥[9,17].

4 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[23–25], 如表 2 所列.

为了说明本协议与基于 WCS 光源的误差容忍协议的区别, 分别画出了态制备误差为 0 和 0.4 时两者的密钥率随距离的变化曲线, 如图 2 所示.

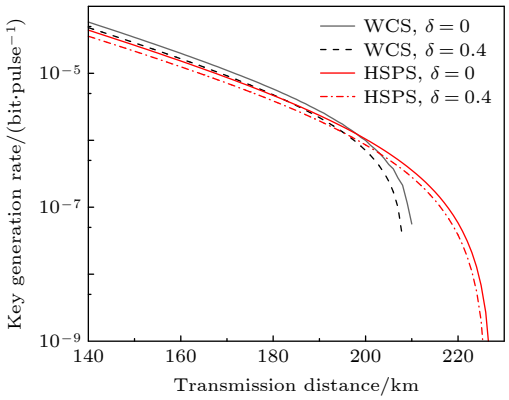

图 2 基于不同光源的态制备误差容忍协议密钥生成率对比图

Fig. 2. Comparison of the key generation rates of the two different state-preparation-error tolerant protocols using either HSPS or WCS.

由图 2 可看出, 在相同的态制备误差的情况下, 当近距离时 (<150 km), 基于 WCS 光源的协议显示出高于基于 HSPS 协议的密钥生成率, 主要由于在后者方案中所使用的本地探测器的探测效率较低所致. 不过在远距离时 (>200 km), 基于 WCS 光源方案的密钥生成率急剧下降, 而基于 HSPS 光源方案的密钥生成率下降趋势相对平缓. 比如, 前者在 211 km 后已经不再能生成密钥, 而后者最大传输距离可达到 228 km. 以上结果说明了本协议更适合应用于远距离量子密钥分发应用.

下面考察使用相同的光源 (HSPS), 但是不同的态制备误差下 ($\delta=0,0.2,0.4,0.6$), 使用本文提出的协议与使用 GLLP 协议[24] 的密钥生成率有何区别, 如图 3 所示.

图 3 中的两种协议使用的仿真参数与表 2 相同, 其中虚线代表本协议在不同的态制备误差条件

下密钥生成率随距离变化的曲线, 从上到下四条虚线分别对应态制备误差为$\delta=0, 0.2, 0.4, 0.6$时的结果; 四条实线分别代表使用 GLLP 协议的对应结果. 由图 3 可看出, 在态制备误差为零时, 后者 (使用 GLLP 协议) 的码率更高; 但是随着态制备误差的增大, 后者的码率急剧下降. 而本协议随着态制备误差的增大, 密钥生成率变化非常缓慢, 尤其是在态制备误差相对较小时, 比如$\delta=0.2$时密钥率曲线几乎与$\delta=0$时密钥率曲线重合. 以上结果证明了本协议对态制备误差具有极好的鲁棒性.

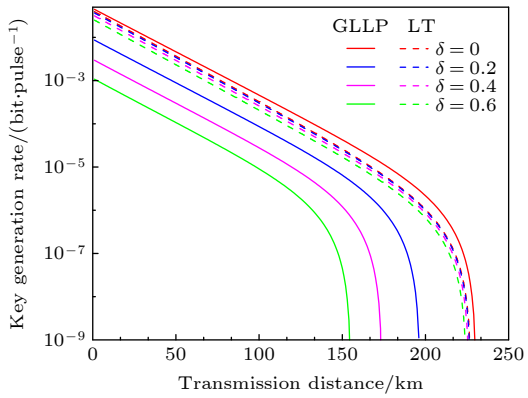

图 3 在不同态制备误差下, 对比本协议与 GLLP 协议[24]的密钥生成率随传输距离变化趋势

Fig. 3. Comparison of the key generation rate between the present work and GLLP protocol under different state preparation errors.

5 结 论

本文提出了基于 HSPS 的态制备误差容忍量子密钥分发协议, 随后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. 该协议对发送端制备态误差大小进行刻画并带入安全性分析之中, 避免了可能存在的安全性漏洞, 提高了系统的安全性. 由于本协议所使用光源自身的优势, 与此前基于 WCS 光源的同类协议相比, 在远距离传输时具有更优的性能. 同时, 本协议对实际量子密钥分发系统中存在的态制备误差具有良好的鲁棒性, 几乎不影响其密钥产生率大小.

本方法原则上同样可以与测量设备无关的量子密钥分发协议[27–30]以及双场量子密钥分发[31–34]等协议结合, 进一步增大系统所能支持的安全通信传输距离. 因而, 该工作为未来发展长距离量子保密通信实际应用起到重要促进作用.

感谢南京邮电大学通信与信息工程学院张春辉老师和周星宇老师的帮助与讨论.

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] Shor P W, Preskill J 2000 *Phys. Rev. Lett.* **85** 441
[3] Mayers D 2001 *J. ACM* **48** 351
[4] Lo H K, Chau H F 1999 *Science* **283** 2050
[5] Brassard G, Lütkenhaus N, Mor T, Sanders B C 2000 *Phys. Rev. Lett.* **85** 1330
[6] Shannon C E 1949 *Bell Syst. Tech. J.* **28** 656
[7] Gottesman D, Lo H K, Lütkenhaus N, Preskill J 2004 *Quantum Inf. Comput.* **4** 325
[8] Tamaki K, Curty M, Kato G, Lo H K, Azuma K 2014 *Phys. Rev. A* **90** 052314
[9] Xu F H, Wei K J, Sajeed S H, Kaiser S, Sun S H, Tang Z Y, Qian L, Makarov V, Lo H K 2015 *Phys. Rev. A.* **92** 032305
[10] Tang Z Y, Wei K J, Bedroya O, Qian L, Lo H K 2016 *Phys. Rev. A.* **93** 042308
[11] Wang J P, Liu H W, Ma H Q, Sun S H 2019 *Phys. Rev. A* **99** 032309
[12] Yin Z Q, Fung C H F, Ma X F, Zhang C M, Li H W, Chen W, Wang S, Guo G C, Han Z F 2013 *Phys. Rev. A* **88** 062322
[13] Zhou X Y, Zhang C M, Guo G C, Wang Q 2019 *IEEE Photonics J.* **11** 7600207
[14] Zhou X Y, Ding H J, Zhang C H, Li J, Zhang C M, Wang Q 2020 *Opt. Lett.* **45** 4176
[15] Pereira M, Curty M, Tamaki K 2019 *npj Quantum Inf.* **5** 62
[16] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503
[17] Lo H K, Ma X F, Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[18] Riedmatten H D, Scarani V, Marcikic I, Acín A, Tittel W, Zbinden H, Gisin N 2004 *J. Mod. Opt.* **51** 1637
[19] Ljunggren D, Tengner M 2005 *Phys. Rev. A* **72** 062301
[20] Castelletto S, Degiovanni I P, Schettini V, Migdall A 2005 *Opt. Express* **13** 6709
[21] Pittmann T B, Jacobs B C, Franson J D 2005 *Opt. Commun.* **246** 545
[22] Mori S, Söderholm J, Namekata N, Inoue S 2006 *Opt. Commun.* **264** 156
[23] Zhu F, Wang Q 2014 *Acta Opt. Sin.* **34** 0627002 (in Chinese) [朱峰, 王琴 2014 光学学报 **34** 0627002]
[24] Wang Q, Wang X B, Guo G C 2007 *Phys. Rev. A* **75** 012312
[25] Wang Q, Chen W, Xavier G, et al. 2008 *Phys. Rev. Lett.* **100** 090501
[26] Lütkenhaus N 2000 *Phys. Rev. A* **61** 052304
[27] Zhou Y H, Yu Z W, Wang X B 2016 *Phys. Rev. A* **93** 042324
[28] Zhang C H, Zhang C M, Guo G C, Wang Q 2018 *Opt. Express* **26** 4219
[29] Zhou X Y, Zhang C H, Zhang C M, Wang Q 2017 *Phys. Rev. A* **96** 052337
[30] Jiang C, Yu Z W, Hu X L, Wang X B 2021 *Phys. Rev. A* **103** 012402
[31] Lucamarini M, Yuan Z L, Dynes J F, Shields A J 2018 *Nature* **557** 400
[32] Ma X F, Zeng P, Zhou H Y 2019 *Phys. Rev. X* **9** 029901
[33] Wang X B, Yu Z W, Hu X L 2018 *Phys. Rev. A.* **98** 062323
[34] Cui C H, Yin Z Q, Wang R, et al. 2019 *Phys. Rev. Appl.* **11** 034053

State preparation error tolerant quantum key distribution protocol based on heralded single photon source*

Ma Xiao [1)2)] Sun Ming-Shuo [1)2)] Liu Jing-Yang [1)2)]

Ding Hua-Jian [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 of Ministry of Education, Nanjing University of Posts and Telecommunications, Nanjing* 210003, *China*)

(Received 7 August 2021; revised manuscript received 11 September 2021)

Abstract

In practical quantum key distribution systems, there inevitably exist errors in the quantum state preparation process due to imperfections in realistic equipment and devices. Those errors would lead to some security loopholes in the quantum key distribution systems. According to the work of Tamaki et al. (*Phys. Rev. A* **90** 052314), here in this work we propose a state preparation error tolerant quantum key distribution protocol through using heralded single-photon sources.

In this protocol, we characterize the size of the error in the preparation state of Alice and bring it into the security analysis, thereby avoiding possible security loopholes and improving the security of the system. Moreover, we take the three-intensity decoy-state method for example to introduce the method of constructing the model and estimating the parameters, and carry out corresponding numerical simulations.

We make a comparison between the loss tolerant protocol with weak coherent source (WCS) and our present protocol using heralded single-photon source (HSPS). Simulation results show that under the same state preparation error, the key generation rate of the protocol based on WCS is higher than that of protocol based on HSPS at short transmission distances (e.g. less than 150 km). The main reason is that the detection efficiency of the local detector used in the latter scheme is low. However, in the case of long transmission distances (e.g. greater than 200 km), the key generation rate of scheme with WCS drops deeply, while the decline of the key generation rate of the present scheme is much flatter. As a result, the former can no longer generate keys after 211 km, while the latter can transmit a maximum distance of 228 km.

Moreover, we also make a comparison between the present scheme and the GLLP protocol with HSPS. The simulation results show that the GLLP protocol with HSPS is very sensitive to the state preparation error and its key generation rate will rapidly decrease with the increase of the state preparation error. On the contrary, our present protocol shows almost no performance degradation under practical state preparation errors. It thus verify the robustness against the state preparation errors of our present work.

In addition, in principle, the method can also be combined with the measurement-device-independent quantum key distribution protocol and the twin-field quantum key distribution protocol to further increase the secure communication transmission distance that the present system can reach. Therefore, this work may provide an important reference value for the practical application of long-distance quantum secure communication in the near future.

Keywords: quantum key distribution, heralded single photon source, loss tolerant protocol, state preparation errors

PACS: 03.65.–w, 03.67.Hk, 42.50.Ex, 42.79.Sz **DOI:** 10.7498/aps.71.20211456

* Project supported by the National Key R&D Program of China (Grant Nos. 2018YFA0306400, 2017YFA0304100), the National Natural Science Foundation of China (Grant Nos. 12074194, 11774180), the Leading-edge Technology Program of Jiangsu Natural Science Foundation, China (Grant No. BK20192001), and the Postgraduate Scientific Research & Innovation Program of Jiangsu Province, China (Grant Nos. KYCX20_0726, KYCX19_0951).

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