综述

标记单光子源在量子密钥分发中的应用*

孟杰 1)2)# 徐乐辰 1)2)# 张成峻 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)

(2022 年 2 月 27 日收到; 2022 年 4 月 15 日收到修改稿)

本文主要介绍标记单光子源的制备、特性, 及其在 3 种主流量子密钥分发 (BB84, 测量设备无关, 双场) 协议中的应用与发展, 同时通过对比标记单光子源和基于弱相干态光源在同类协议中的性能, 分析讨论不同光源的优缺点. 此外, 针对双场量子密钥分发协议中对单光子干涉特性的要求, 分析了标记单光子源在双场协议应用中的局限性, 并讨论了可能的解决方案, 对今后发展实用化量子保密通信系统将起到有价值的指导和推进作用.

关键词: 量子密钥分发, 标记单光子源, 弱相干态光源, 被动式诱骗态

PACS: 03.65.–w, 03.67.Hk, 42.50.Ex, 42.79.Sz **DOI:** 10.7498/aps.71.20220344

1 引 言

量子密钥分发 (quantum key distribution, QKD) 不仅是量子保密通信的核心, 也是当前研究的热点. 从第一个 BB84[1] 协议被提出到目前为止, 该方向已有近四十年的发展历程. 1991 年, Ekert[2] 提出了基于量子纠缠和贝尔不等式的密钥分发协议, 称为 E91 协议. 1992 年, Bennett 等 [3] 提出了不需要做贝尔不等式检测的纠缠类量子密钥分发协议, 即 BBM92 协议, 同时指出纠缠协议和 BB84 协议的等效性. 同年, Bennett[4] 又给出了简化版的 BB84 协议, 即 B92 协议. 随后, 出现一系列其他种类的协议, 如高斯调制协议、离散类协议、SARG04 协议 [5]、差分相位协议 [6] 和六态协议 [7] 等. 随着 QKD 的发展, 人们也会关注其实际应用中的安全性问题. 以单光子协议为例, 协议模型中包含光源、量子态的制备、信道以及探测器. 而由于光源的不完美, 容易受到光子数分离攻击 [8,9]; 由于探测器的不完美, 可能导致伪态攻击 [10]、时移攻击 [11,12]、探测器致盲攻击 [13,14]、死时间攻击 [15] 以及后门攻击 [16]. 针对非理想光源的解决方案中, 人们最为熟知的解决方案是针对光子数分离攻击的诱骗态方案 [17–19], 给出了实用化光源情况下安全密钥生成率的下限. 为了抵御针对探测器的侧信道攻击, 科学家提出了测量设备无关量子密钥分发 (measurement device independent-QKD, MDI-QKD) 协议 [20,21]. 随后, 一系列 MDI-QKD 的实验被先后验证 [22–24].

科学家已经证明在不使用量子中继的情况下, 常用协议 (BB84, MDI) 的密钥率容量存在上界 (PLOB 界), 即密钥率线性依赖于信道透过率 [25]. 2018 年, Lucamarini 等 [26] 提出了双场量子密钥分发协议 (twin-field-QKD, TF-QKD), 此协议既保留了测量设备无关的特性, 又得到了密钥率的显著提升, 即密钥率与信道透过率成平方根关系, 因此

* 国家重点研究发展计划 (批准号: 2018YFA0306400, 2017YFA0304100)、国家自然科学基金 (批准号: 12074194, 12104240) 和江苏省自然科学基金 (批准号: BK20192001, BK20210582) 资助的课题.

同等贡献作者.

† 通信作者. E-mail: qinw@njupt.edu.cn

可突破 PLOB 界. 为解决原始 TF-QKD 可能存在的安全性漏洞及实用性问题, 后继研究者提出了一系列变体 TF-QKD 协议, 如相位匹配协议 (phase-matching, PM) [27]、发送不发送协议 (sending-or-not-sending, SNS)[28] 和无需相位后选择 (without phase postselection, NPP)[29–31] 等量子密钥分发协议. 紧接着, 一系列相关实验被报道[32–36].

现有大部分 QKD 实验使用的光源是弱相干态 (weak coherent source, WCS) 光源, 优点是低成本且容易制备, 缺点是其真空态脉冲所占比重较高, 导致接收方在进行远距离传输时其误码率受探测器暗计数影响较为严重, 从而限制了最远安全传输距离的大小. 针对 WCS 的这些缺点, 研究者提出使用标记单光子源 (heralded single-photon source, HSPS) 来代替 WCS 进行量子密钥分发[37,38]. HSPS 具有单光子性质好, 真空脉冲概率低等内在优点, 能在量子保密通信中显示出独特的优势, 因此在未来量子保密通信中具有重要的应用前景.

2 标记单光子源

HSPS 是利用同时产生的光子对中的一个光子来标识另外一个光子到达时间的一种光源. 该类光源在制备时, 一般通过自发参量下转换 (spontaneous parametric down-conversion, SPDC) 过程产生具有同时性和相同模场分布的双模光场, 对应光场模式分别为信号光 (signal, S) 模式和闲置光 (idler, I) 模式[39]. 由于该双模光场存在内在的关联特性, 所以可通过探测器对 I 模式的探测来实现对 S 模式中光子到达时间的预测.

SPDC 过程的原理[40] 示意图如图 1 所示, 使用一束激光去泵浦一个非线性晶体, 会以一定概率发生 SPDC 过程, 此过程满足能量守恒和动量守恒. 满足能量守恒定律:

$$\omega_{\rm p} = \omega_{\rm i} + \omega_{\rm s},$$

其中 $\omega_{\rm p}, \omega_{\rm s}, \omega_{\rm i}$ 分别代表泵浦光、信号光、闲置光的角频率. 满足动量守恒定律:

$$\boldsymbol{k}_p = \boldsymbol{k}_i + \boldsymbol{k}_s,$$

其中 $\boldsymbol{k}_{\rm p}$, $\boldsymbol{k}_{\rm i}$, $\boldsymbol{k}_{\rm s}$ 分别为泵浦光、信号光、闲置光的波矢向量. SPDC 产生的双模态可表示为[40]

$$\begin{aligned}|\psi\rangle_{\rm IS} &= \cosh^{-1}x \sum_{n}^{\infty} \tanh^n x |n\rangle_{\rm I}|n\rangle_{\rm s} \\ &= \sum_{0}^{\infty} \sqrt{P_n}|n\rangle_{\rm I}|n\rangle_{\rm s}, \end{aligned} \tag{1}$$

其中 x 代表耦合系数, 其大小与泵浦光场的幅度成正比[40]; $|n\rangle$代表 n 光子态, P_n 为产生 n 光子对的概率; I 代表闲置光模式, S 代表信号光模式.

通过本地阈值探测器对 I 光的标记, S 光所处的光子态表达式为[41]

$$\rho = \sum_{n}[1-(1-d_{\rm A})(1-\eta_{\rm A})^n]p_n^{\mu}|n\rangle\langle n|, \tag{2}$$

其中 $d_{\rm A}$ 和 $\eta_{\rm A}$ 分别为本地探测器的暗计数率和探测效率, p_n^{μ} 为原始信号光模式中 n 光子态的概率分布. WCS, HSPS 在不同条件下可能具有不同的光子数概率分布, 如热分布、泊松分布、亚泊松分布等[42]. 研究者通过对不同光子数概率分布进行分析对比, 总结了不同概率分布对 QKD 性能的影响[42]. 在后文介绍中倘若没有特殊说明, 默认采用泊松分布.

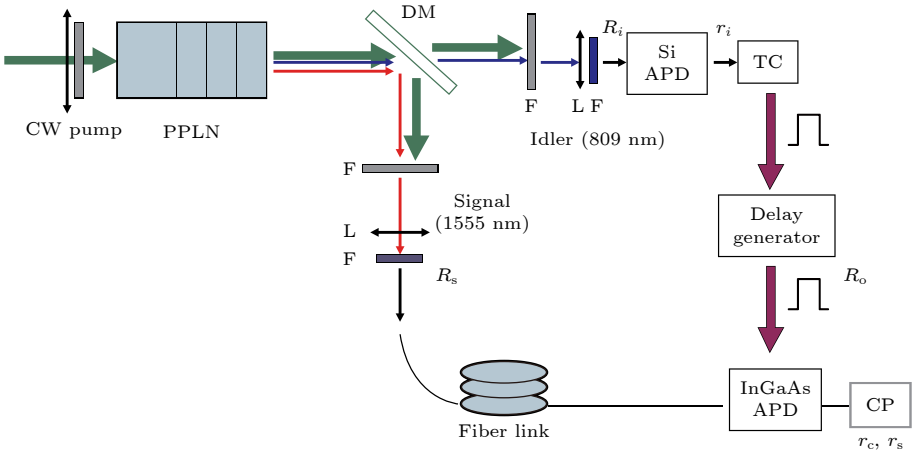

图 1 HSPS 制备原理示意图[40]

Fig. 1. Schematic diagram of the setup for HSPS generation[40].

表 1 和图 2 分别给出了当平均光子数为 0.5 时, WCS 和 HSPS 中不同光子数的分布概率[41,43–48]. 通过对比表 1 和图 2, 可看出 HSPS 比 WCS 具有更高的单光子概率和更低的真空态概率, 这些特性对提升 QKD 性能具有重要作用, 进而显示出在 QKD 实验中使用 HSPS 替代 WCS 提升系统性能的可行性. 目前用于制备 HSPS 的非线性材料包括 PPLN, PPKTP, BBO 晶体或波导等, 其中 PPLN 和 PPKTP 属于周期性极化介质, 一般通过准位相匹配条件产生参量光, 非线性系数较高. BBO 一般是块状晶体, 利用位相匹配条件产生参量光, 非线性系数低. 不同材料在不同指标上各有优缺点, 具体参数指标可参见表 2.

表 1 WCS 与 HSPS 光源光子数分布概率对比[41]

Table 1. Comparison of photon number distribution probabilities between WCS and HSPS[41].

光源	P_0	P_1	P_m
WCS	6.065×10^{-1}	0.3033	0.0902
HSPS	6.065×10^{-7}	0.2274	0.0853

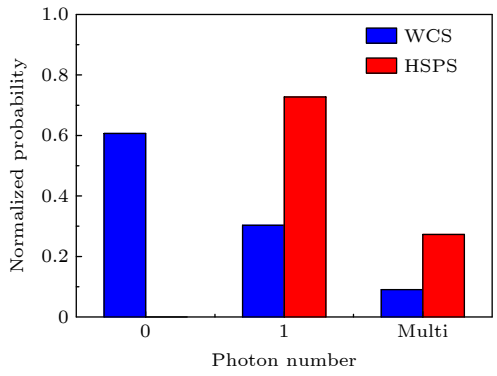

图 2 WCS 光源与 HSPS 光源光子数分布概率对比[41]

Fig. 2. Comparison of photon number distribution probabilities between WCS and HSPS[41].

将 HSPS 应用于 QKD 时, 人们比较关注光源的几项参数指标. 倘若使用光纤进行密钥分发, 一般需要将信号光谱线中心制备在通信波段 (1530—1565 nm), 如果在自由空间进行密钥分发, 一般制备在 700—800 nm. 光源亮度 (每秒钟单位泵浦强度下产生光子对的数目) 和标记效率 (一个标记光子预测一个信号光子到达的概率) 对 3 种主流 (BB84, MDI, TF) QKD 协议的密钥率影响最大, 因此也是人们关注的重点. 光源纯度决定独立双光子干涉可见度的上限, 对 MDI-QKD 的性能影响较大. 对于 BB84 和 TF 协议而言, 光源纯度对信号光可能存在的测信道漏洞产生影响, 因此如何制备光源纯度接近 100% 的 HSPS 也是人们追求的目标. 从表 2 可看出, 目前无论是使用 PPLN (Nice2010), PPKTP (Griffith2016) 或是 BBO (USTC2018), 人们已经可以得到接近 100% 的光源纯度, 但是其他指标还存在一定缺陷, 比如 Nice2010 和 Griffith2016 中分别使用半高宽为 0.25, 8.00 nm 的滤波片对信号光进行滤波, 将导致光源亮度和标记效率降低; USTC2018 设计并产生了解关联的光子对, 光源纯度接近 100%, 但是参量光谱线较宽 (30 nm), 在光纤中传输时带来的色散效应明显, 不太适合做远距离传输. 综合来看, Illinois2016 除了标记效率有待提升之外, 其他参数指标较为均衡.

3 HSPS 在 BB84 协议中的应用

目前, 诱骗态方法在 QKD 系统中已广泛应用, 其基本思路是发送方随机制备并发射不同强度的光脉冲发送给接收方, 由于计数率和误码率仅依赖于光子数, 而与脉冲是信号态或诱骗态无关, 窃听者不能够区分信道中传输的 n 光子态是信号态还

表 2 不同 HSPS 实现方案关键指标对比

Table 2. Comparison of core parameters of different HSPS schemes.

晶体类型	信号光中心谱线/nm	滤波片半高宽/nm	纯度/%	光源亮度	标记效率滤波前/%/后/%	参考文献
PPLN	1557	0.10	78.0	1.40×10^3 pairs·(s·μW)$^{-1}$	39.9 / 64.0	Saarlandes2016 [43]
	1536	0.25	99.0	1.60×10^3 pairs·(s·mW)$^{-1}$	—	Nice2010 [44]
PPKTP	1590	0.00	90.0	1.10×10^4 pairs·(s·mW)$^{-1}$	77.0 / 0	Illinois2016 [45]
	1570	8.00	98.0	3.29×10^2 pairs·(s·μW)$^{-1}$	52.0 / 0	Griffith2016 [46]
BBO	1550	10.00	99.7	1.70×10^2 pairs·(s·mW)$^{-1}$	91.0 / 94.0	USTC2018 [47]
	532	24.00	—	9.50×10^3 pairs·(s·mW)$^{-1}$	18.9 / 16.7	Fraunhofer2022 [48]

注: 晶体类型为自发参量下转换过程中使用的非线晶体; PPLN: periodically-poled potassium titanyl phosphate, 周期极化磷酸钛钾晶体; PPKTP: periodically-poled potassium titanyl phosphate, 周期极化磷酸钛钾晶体; BBO: β–barium-borate, 偏硼磷钡晶体.

是诱骗态, 只能采取相同的攻击策略. 因此, 合法用户可以根据实验结果的统计特性来监测是否存在窃听者. 理论上, 如果诱骗态个数足够多时, 可以精确地求出不同光子态的条件计数率和误码率的大小, 从而利用 Gottesman-Lo-Lütkenhaus-Preskill (GLLP) 公式[49] 计算系统的成码率. 但在实际实验中无法制备无穷多个诱骗态, 因此通常使用少强度诱骗态方案. 此外, 根据发送端是否主动调制光源强度产生诱骗态, 可将诱骗态方案分为两类, 即主动式诱骗态方案和被动式诱骗态方案.

3.1 基于 HSPS 的主动式诱骗态 BB84 协议

2006 年, 王琴等[50] 首次提出基于 HSPS 的三强度诱骗态方案, 该协议中发送端 Alice 在三个强度之间随机切换泵浦光强度, 使参量光的强度在 0, μ 和 μ' ($\mu' > \mu$) 之间变化. Alice 将 S 模式随机制备成不同的偏振态 ($|H\rangle$, $|V\rangle$, $|+\rangle$, $|-\rangle$) 并发送给 Bob, 同时使用本地探测器对 I 模式进行探测, 将探测结果转化为标记信号发送给接收端 Bob; Bob 根据 Alice 发送过来的标记信号, 随机选取一组基矢 (X 或 Z) 对发送来的信号光进行探测, 并记录探测结果. 待所有信号传输完成后, Alice 和 Bob 公开宣布它们对每一个脉冲使用的基矢, 只留下使用相同基的结果, 丢弃使用不同基的结果, 获得初始密钥. 接着 Alice 和 Bob 对初始密钥进行后处理操作, 获得安全密钥.

在该过程中, 定义 Y_n 为 n 光子态的条件计数率, 即当 Alice 发出 $|n\rangle$ 光子态脉冲时, Bob 的探测器检测到信号的概率, Y_0 代表真空脉冲引起的计数率. Y_μ 和 $Y_{\mu'}$ 分别代表强度为 μ, μ' 的脉冲所引起的平均计数率. 假设状态 ρ_x 有 N_x 个脉冲, 其中 N_{xt} 个被触发. 在这些 N_{xt} 脉冲的时间窗口中, Bob 探测器探测次数为 n_x, 根据计数率的定义, 得到 $Y_x = n_x/N_{xt}$. 信号光 (μ) 和诱骗态 (μ') 引起的平均计数率可表示为[50](此处参量光采用热分布)

$$\tilde{Y}_\mu = Y_0\frac{d_{\rm A}}{1+\mu}+\sum_{i=1}^{\infty}Y_n[1-(1-\eta_{\rm A})^n]\frac{\mu^n}{(1+\mu)^{n+1}}, \quad (3)$$

$$\tilde{Y}_{\mu'} = Y_0\frac{d_{\rm A}}{1+\mu'}+\sum_{i=1}^{\infty}Y_n[1-(1-\eta_{\rm A})^n]\frac{\mu'^n}{(1+\mu')^{n+1}}, \quad (4)$$

其中 $\tilde{Y}_x = (N_{xt}/N_x)\,Y_x$, $x = \mu, \mu'$. 根据 (3) 式和 (4) 式可以推导出单光子脉冲条件计数率的下界 Y_1, 强度为 x 的触发脉冲中由单光子引起计数的比重 $\Delta_1(x)$, 以及单光子脉冲引起的比特误码率 e_1 的上界, 并最终得到该方案的密钥率[50]:

$$R \geqslant \frac{Y_{\mu'}P_{\rm post}(\mu')}{2}\{-f(E_{\mu'})H_2(E_{\mu'}) + \Delta_1(\mu')[1-H_2(e_1)]\}, \quad (5)$$

其中 f 代表纠错系数, $P_{\rm post}$ 代表归一化因子, E_x 代表强度为 x 的触发脉冲的平均误码率, $x = \mu$, μ'. 具体仿真结果如图 3 所示. 图 3 对比了基于 HSPS 和 WCS 的 BB84 协议成码率, 其中绿色实线和蓝色虚线分别代表使用 HSPS 的无穷诱骗态 (H1) 和三强度诱骗态 (H2) 情况, 黑色实线 (W1) 和红色点线 (W2) 对应于 WCS 的结果. 显然, 基于 HSPS 的协议具有更远的安全传输距离. 主要由于 HSPS 中真空态脉冲的概率极低, 与 WCS 光源相比, 在远距离处由真空态产生的误码率极低, 因此能够在远距离处显示出更优的性能.

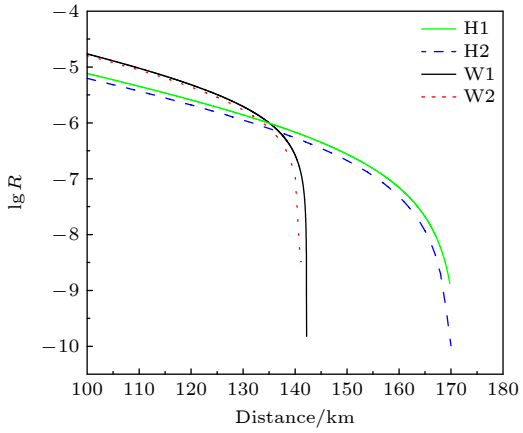

图 3 基于 HSPS 和基于 WCS 的 BB84 协议成码率对比[50]

Fig. 3. Comparison of the key rate between using HSPS and WCS[50].

2008 年, 王琴等[37] 在实验上首次实现了基于 HSPS 的三强度诱骗态 QKD 实验, 其所用实验装置图和实验结果分别如图 4 和图 5 所示, 图 5 中蓝色点线 (B) 和红色短划线 (R) 分别代表信号光子的理论计数率和考虑统计起伏的实际成码率. 该实验初步显示了量子光源在实用化 QKD 中应用的潜力.

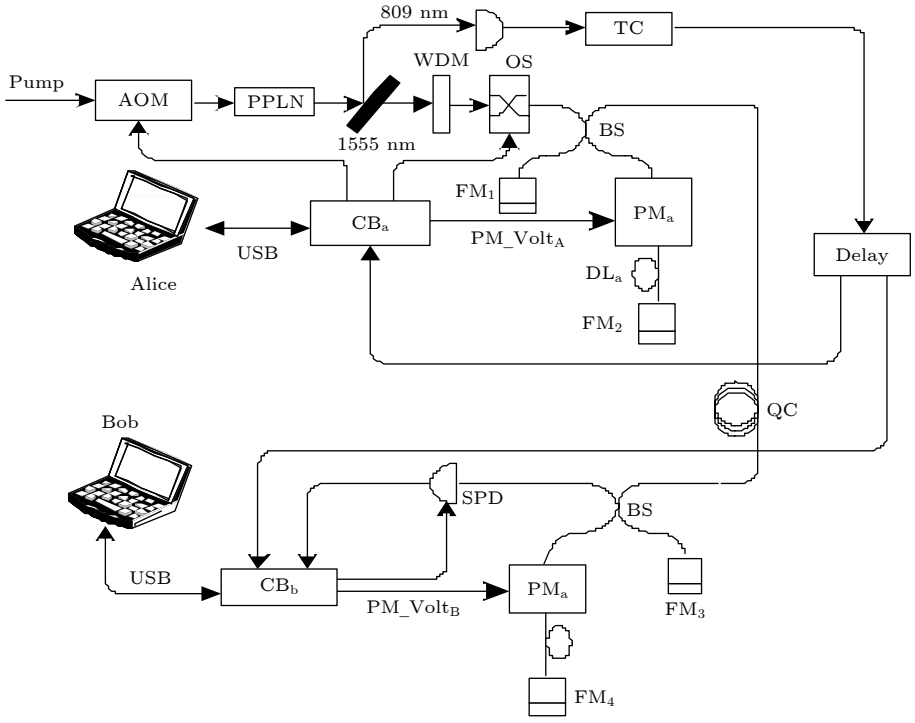

图 4 基于 HSPS 的三强度诱骗态 QKD 实验装置示意图[37]

Fig. 4. Schematic diagram of the setup for three-intensity decoy state QKD based on HSPS[37].

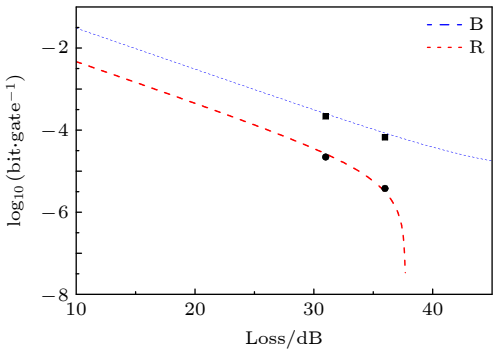

图 5 基于 HSPS 的三强度诱骗态 QKD 实验与理论对比[37]

Fig. 5. Comparisons between experiment and theory for the three-intensity decoy state QKD based on HSPS[37].

3.2 基于 HSPS 的被动式诱骗态 BB84 协议

目前主动式诱骗态一般通过主动调制光源强度来实现, 由于现有强度调制器的不完美, 可能在调制过程中使得信号光与诱骗态在某些自由度上可以区分, 导致攻击者可以据此实施攻击获取密钥. 此外, 使用主动式诱骗态会产生额外的调制误差, 导致信道参数估计不够准确, 从而降低系统性能. 2008 年, Adachi 等[51] 提出了一种基于阈值探测器的被动式诱骗态方案, 称为 AYKI 方案[51]. 在 AYKI 方案中响应事件仅包括触发和非触发两种情况, 造成信道参数估计不够紧致, 从而影响了系统的性能.

2016 年, 王琴等[52] 提出了基于 HSPS 的新型被动式诱骗态 QKD 方案, 如图 6 所示, 使用一束激光去泵浦一个非线性晶体, 通过 SPDC 过程产生双模光场, 分别记为 S 模式和 I 模式. Alice 对 I 模式进行分束探测, 对 S 模式通过采用偏振旋转器 (polarization rotator, PR) 调制成不同的偏振态 ($|H\rangle, |V\rangle, |+\rangle, |-\rangle$) 后发送给 Bob. 接收端 Bob 采用 PR 选择不同的测量基 (X 或 Z) 执行投影测量.

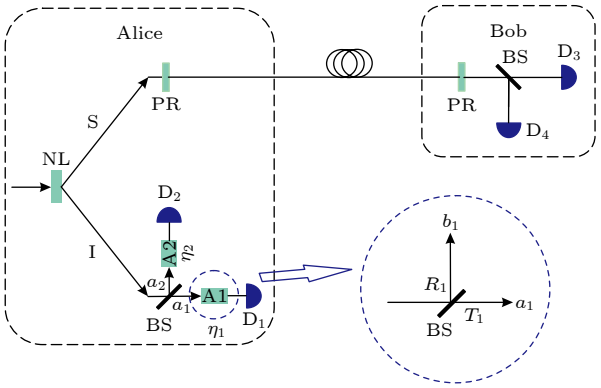

图 6 基于 HSPS 的新型被动式诱骗态 QKD 方案示意图[52]

Fig. 6. Schematic diagram of the new passive decoy state QKD protocol based on HSPS[52].

在进行分束探测时, Alice 使用分束器 (beam splitter, BS) 将闲置光分成两路 (a_1和a_2), 分别送入两个本地单光子探测器中 (D_1和D_2), 对应探测事件可以分为 4 种情况: 1)D_1, D_2都不响应; 2)D_1响应, D_2不响应; 3)D_1不响应, D_2响应; 4)D_1, D_2都响应. 由于信号光和闲置光具有相同的光子数分布, 所以根据闲置光的探测可以将信号光投影到不同的态空间, 用 $\rho=\sum_{n,s_1,s_2}P_n^{\mu}P_{X_i|n}|n\rangle\langle n|$表示. 首先定义以上 4 种事件在信号光模式所对应的投影态分别为x, y, z, w四种量子态, 所对应的光子数分布概率分别为[52]

$$
\begin{aligned}
a_n^x &= (1-d_{\rm A})^2(1-\eta_{\rm A})^n\frac{\mu^n}{n!}{\rm e}^{-\mu},\\
a_n^y &= (1-d_{\rm A})(1-\eta_{\rm A})^n\\
&\quad\times\left[\left(1+\frac{t\eta_{\rm A}}{1-\eta_{\rm A}}\right)^n+d_{\rm A}-1\right]\frac{\mu^n}{n!}{\rm e}^{-\mu},\\
a_n^z &= (1-d_{\rm A})(1-\eta_{\rm A})^n\\
&\quad\times\left[\left(\frac{1-t\eta_{\rm A}}{1-\eta_{\rm A}}\right)^n+d_{\rm A}-1\right]\frac{\mu^n}{n!}{\rm e}^{-\mu},\\
a_n^w &= \frac{\mu^n}{n!}{\rm e}^{-\mu}-a_n^x-a_n^y-a_n^z, \qquad (6)
\end{aligned}
$$

其中μ为参量光强度, $\eta_{\rm A}$, $d_{\rm A}$分别为本地探测器的探测效率和暗计数率, t为分束探测时分束器的透射率.

至此, 根据本地探测器的响应事件被动地构造了 4 种态. 我们可以选择将y, z作为信号态, x作为诱骗态, 进而可推导出单光子计数率的下界以及单光子误码率的上界. 最终, 可以得到新型被动式诱骗态 QKD 方案的密钥生成率为[52]

$$
\begin{aligned}
R \geqslant\ & (a_1^y+a_1^z)Y_1^{Z,L}\left[1-H_2(e_1^{X,U})\right]\\
& -Q_y f(E_y)H_2(E_y)-Q_z f(E_z)H_2(E_z), \qquad (7)
\end{aligned}
$$

其中$Y_1^{Z,L}$表示Z基下单光子脉冲引起的条件计数率; $e_1^{X,U}$表示X基态制备下的单光子脉冲引起的误码率; Q_ξ和E_ξ分别表示光强为ξ($\xi\in\{y,z\}$)的脉冲引起的平均响应率和平均误码率. 仿真结果如图 7 所示. 图 7(a) 表示不同方案的成码率绝对数值对比, 图 7(b) 表示新型被动式诱骗态方案的成码率与现有其他 3 个方案的比值. 图 7 中 Q1 代表新型被动式诱骗态方案, A1 代表 AYKI 方案[51], H3 代表使用 HSPS 的标准三强度诱骗态[50], W3 代表使用 WCS 的标准三强度诱骗态[53]. 由图 7 可以看出, 无论是与 AYKI 方案对比, 还是与基于 HSPS 或 WCS 的三强度诱骗态方案对比, 该新型被动式诱骗态方案均表现出优异的性能.

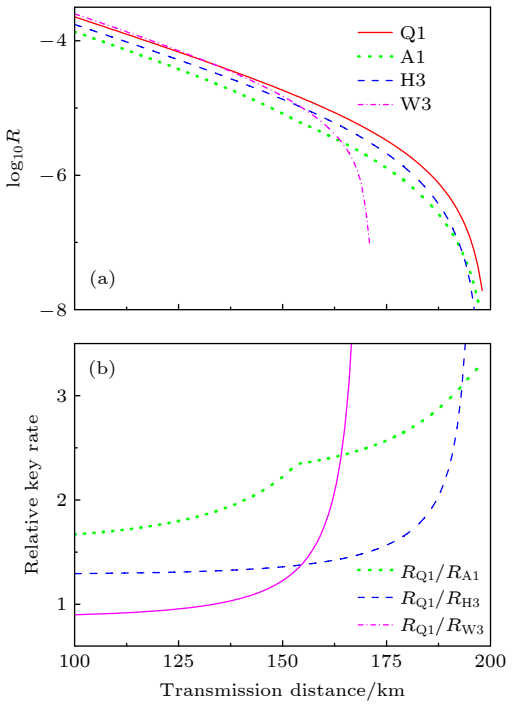

图 7 最终密钥生成率比较[52] (a) 对数尺度下的密钥生成率; (b) 密钥生成率的相对值

Fig. 7. The comparison of the final key generation rate[52]: (a) Absolute values of the key generation rate with logarithm scale; (b) relative value for the key generation rate.

2019 年, 张春辉等[38] 在以上理论方案的基础上开展了相关实验, 完成了超过 40 dB 衰减的被动式诱骗态 QKD 的实验验证, 如图 8 所示. 该实验进一步验证了上面所述被动式诱骗态的可行性和优越性. 除了上面介绍的三强度、被动式诱骗态协议之外, 研究者还提出其他基于 HSPS 的诱骗态的方案[54] 并证明了其在 QKD 实际应用中的优越性.

4 HSPS 光源在 MDI-QKD 协议中的应用

2013 年, 王琴等[55] 提出基于 HSPS 的三强度诱骗态 MDI-QKD 协议的同时, 并提出使用触发与非触发事件估计信道参数的思想, 结构示意图如图 9 所示. 通信双方 (Alice 和 Bob) 独立地将泵浦激光随机调制成 3 种不同光强, 通过 SPDC 过程产生 3 种不同强度的双模参量光 (0, μ, μ'), 将两种模式分别命名为 S 模式和 I 模式. Alice 和 Bob 分别将信号光随机制备成 4 种不同的偏振态 ($|H\rangle$, $|V\rangle$, $|+\rangle$, $|-\rangle$) 中的一个并通过量子信道发送给不可靠的第三方测量端 (Charlie), 同时将 I 模式送入本地探测器进行探测, 随即根据本地探测器的探测

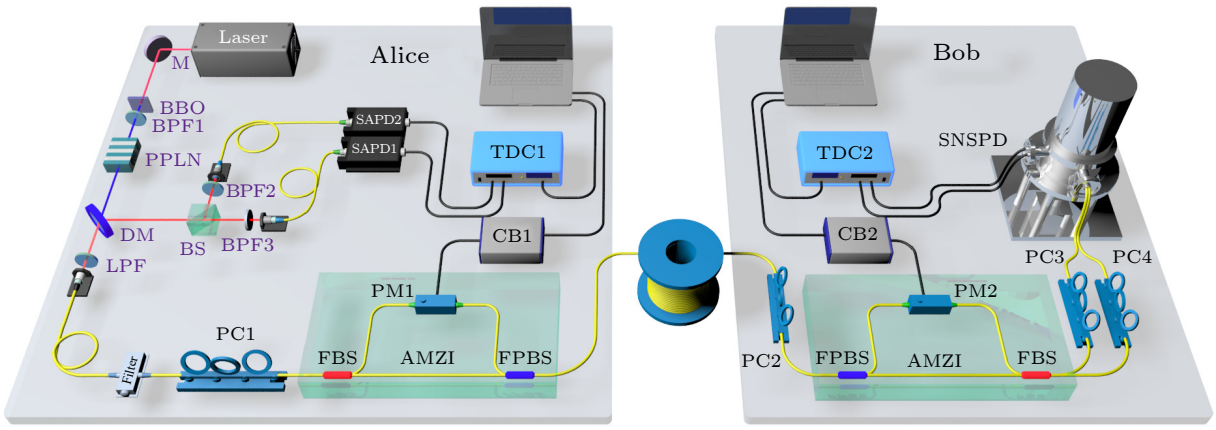

图 8 新型被动式诱骗态实验装置示意图[38]

Fig. 8. Schematic diagram of the passive decoy state QKD setup[38].

结果发送触发或非触发信号给 Charlie. Charlie 对 Alice 和 Bob 发送过来的光脉冲执行贝尔态投影测量, 并记录测量结果. 通信双方 (Alice 和 Bob) 中的一方需要根据贝尔态投影的结果进行比特翻转等操作, 得到筛选密钥; 然后通过对筛选后密钥进行后处理, 得到安全密钥.

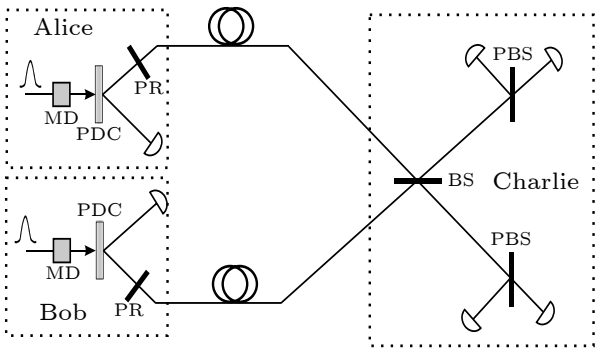

图 9 基于 HSPS 光源的 MDI-QKD 原理示意图[55]

Fig. 9. Schematic diagram of the principle of MDI-QKD based on HSPS light source[55].

闲置光被本地探测器探测响应后光子数分布满足[55]

$$P_i(\xi) = [1-(1-d_{\rm A})(1-\eta_{\rm A})^i]\frac{\xi^i}{i!}{\rm e}^{-\xi}, \qquad (8)$$

其中 $d_{\rm A}$, $\eta_{\rm A}$ 代表探测器的暗计数率和效率, ξ 代表信号光脉冲的平均光强 ($\xi \in (0, \mu, \mu')$ 代表真空态、诱骗态、信号态的光强度). 不同强度的双模光在本地探测器的探测下, 会发生探测器响应和不响应事件. 可以使用不同强度的闲置光在本地探测器产生的不同触发事件来估计单光子脉冲对的计数率 Y_{11} 和单光子脉冲对的比特误码率 e_{11}, 从而得到最终的密钥成码率[55]:

$$R^t = \left\{q^2 P_1^2(\mu') Y_{11}^{Z,t}[1-H_2(e_{11}^X)] - S_{\mu',\mu'}^{Z,t} f\left(E_{\mu',\mu'}^{Z,t}\right) H_2\left(E_{\mu',\mu'}^{Z,t}\right)\right\}, \qquad (9)$$

其中 $Y_{11}^{Z,t}$ 代表 Z 基触发事件下单光子脉冲对的计数率, e_{11}^X 代表 X 基单光子脉冲对的误码率, $S_{\mu',\mu'}^{Z,t}$, $E_{\mu',\mu'}^{Z,t}$ 分别代表 Z 基信号光引起触发事件对应的平均增益和误码率. 相关仿真结果如图 10 所示.

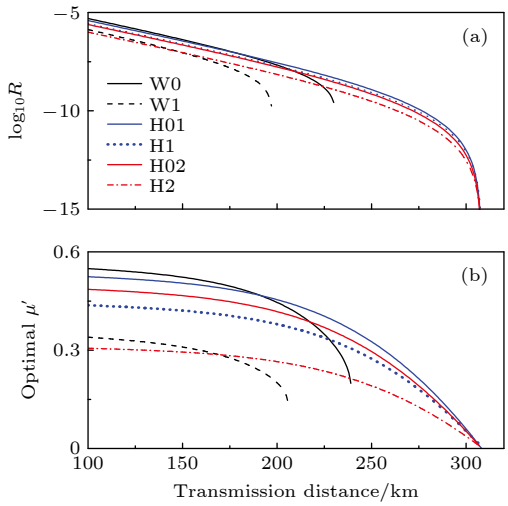

图 10 基于不同光源情况的诱骗态 MDI-QKD 协议的成码率仿真对比[55] (a) 密钥率对比; (b) 信号光强度对比

Fig. 10. Comparison between MDI-QKD protocols based on different light sources[55]: (a) Comparisons of the key rate; (b) comparisons of the signal intensity.

图 10(a), (b) 分别代表密钥率和最优信号光强度对比图, 其中 W0 (W1) 代表基于 WCS 光源的无穷多诱骗态 (标准三强度诱骗态) 方案结果[21]; H01(H1) 代表基于 HSPS 光源的无穷多诱骗态 (标准三强度诱骗态) 方案结果; H02(H2) 代表基于

HSPS 光源的无穷多诱骗态 (改进的三强度诱骗态) 方案结果. 由图 10 可以看出, 与基于 WCS 光源的 MDI-QKD 方案相比, 基于 HSPS 的两种方案均在远距离处显示出优越性. 此外, 与传统基于 HSPS 的三强度诱骗态方案相比, 新方案在近距离处成码率更高. 此外, 作者还分析了统计涨落对 3 种协议性能的影响, 仿真结果显示统计起伏对基于 HSPS 和基于 WCS 光源的 MDI-QKD 成码率影响均比较严重. 不过, 总体来说, 对后者的影响尤为突出.

在此基础之上, 2018 年, 张春辉等 [56] 提出了基于标记单光子源的偏选基三强度诱骗态 MDI-QKD 方案, 通过具体仿真证明了使用偏选基方案比使用标准三强度方案 [57,58] 能够得到更高的密钥率. 2019 年, 他们又提出改进的被动式诱骗态 MDI-QKD 方案 [59], 通过对闲置光采用分束探测的方法, 并结合集合约束和联合参数估计等技术 [57], 对信道参数进行更紧致地估计, 同时避免了主动式诱骗态方案中可能存在的信息泄露. 仿真结果显示, 该方案与其他现有方案相比具有更高的密钥生成速率和更远的安全传输距离, 如图 11 所示, 其中蓝色虚线和黑色点线分别对应改进的基于 HSPS 的三强度诱骗态方案 [60] 和基于 WCS 的四强度诱骗态方案 [57] 的结果.

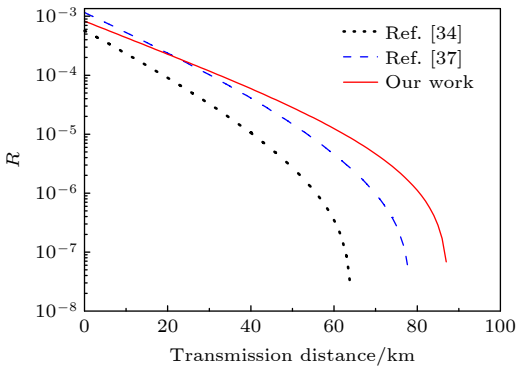

图 11 改进的被动式诱骗态 MDI-QKD 仿真 [57]

Fig. 11. Simulation of new passive decoy state MDI-QKD[57].

以上工作均显示: 在相同条件下, 基于 HSPS 光源的 MDI-QKD 比基于 WCS 光源的 MDI-QKD 具有更远的安全传输距离和密钥率. 主要原因为: 前者由于 Alice 和 Bob 本地探测器的标记作用, 使得 Charlie 测量双光子符合事件中的两个光子同时来自于发送端 Alice 或同时来自于发送端 Bob 的概率大幅降低, 而在基于 WCS 光源的 MDI-QKD 方案中, Charlie 无法区分两个光子同时来自同一个发送方还是两个不同的发送方 (注: 双光子同时来自一个发送方的事件将在 X 基上产生误码). 因此, 前者可以在 Charlie 端提升双光子干涉可见度, 降低单光子对产生的误码率, 进而提升安全传输距离和密钥率.

MDI-QKD 虽然具有安全性等级高, 干涉稳定等优点, 但是该类协议的最大缺点是安全密钥率低. 主要由于 MDI-QKD 基于双光子干涉, 接收端需要执行双光子符合测量, 与 BB84 协议和 TF 协议中的单光子测量相比, 双光子符合测量的成功概率极低. 一方面由于目前使用的线性光学元件无法对 4 个贝尔态做完全区分, 若把其中一个贝尔态作为有效事件, 此时双光子符合投影测量的最高成功概率仅为 1/4; 另一方面, 若定义一个单光子从 Alice/Bob 端成功到达 Charlie 端的概率为 p, 则一对双光子同时到达的概率仅为 p^2. 为了解决该问题, 2014 年, Abruzzo 等 [61] 和 Panayi 等 [62] 提出使用量子存储器装置提升双光子同时到达的概率, 进而提升 MDI-QKD 的密钥率. 不过以上理论工作中对存储器做了一些不实际的假设, 因而在基于 WCS 光源的 MDI-QKD 实验中尚无法进行实验验证. 而由于 HSPS 光源的特殊标记特性, 把以上存储方案应用到基于 HSPS 的 MDI-QKD 中, 则具有一定可行性.

2017 年 Kaneda 等 [63] 通过使用光存储方案初步演示了来自于两个独立 HSPS 的贝尔态投影测量实验, 可惜由于受实验条件的限制, 例如参量光平均光子数较低 (0.013 个/脉冲), 闲置光的耦合和探测整体效率低 (0.18), 信号光编码装置损耗过大 (14 dB), 信号光整体传输效率仅为 0.083, 探测器探测效率不高 (0.75), 用于光存储的主要设备——泡克尔斯盒的工作频率较低 (1 MHz), 导致同步过程不能在同步两个光子后立即重复, 而是在固有周期 (1 μs) 后重复, 导致双光子符合率提升不高 (30 倍); 用于编码 time-bin 的前后两个小脉冲的时间间隔为 25 ps, 在现有超导探测器时间上无法区分, 导致测量误码率数值偏高等. 文献 [63] 在附录中已经对目前的限制条件和可能改进的方向进行了详细列表讨论, 在此不再累述. 相信随着技术的不断进步, 基于 HSPS 的 MDI-QKD 实验将会被验证并显示出自身优势.

5 HSPS 光源在 TF-QKD 协议中的应用

近几年, TF-QKD 协议发展十分迅速, 目前已有好几种高效的协议方案[26−32], 图 12 是其中一个 TF-QKD 协议的实验装置结构示意图. 鉴于不同方案的具体操作流程在文献 [26—32] 中已分别做了详细介绍, 此处将不再累述. 需要强调, TF-QKD 系统与 MDI-QKD 系统的主要区别在于前者基于单光子干涉, 后者基于双光子干涉. 因此, 在测量端前者执行的是单光子测量, 而后者执行的是双光子测量. 正是由于 TF-QKD 系统对单光子干涉的要求, 不同光源在 TF-QKD 实际应用中可能具有一定局限性. 首先, WCS 由衰减激光光源产生, 两束独立的 WCS 可以通过锁相等技术产生稳定的相位干涉, 进而能够满足 TF-QKD 系统中对单光子干涉的要求, 但由于该类光源中真空脉冲的比例较高, 因此其最远安全传输距离受到一定限制. 其次, HSPS 主要由参量下转换过程产生, 而该过程产生的双光子对之间具有内在的时间-频率纠缠特性, 对其中闲置光的探测标记操作将使信号光塌缩到混态状态, 因此两束独立的 HSPS 无法在测量端 (Charlie) 产生稳定的单光子干涉, 从而无法满足 TF-QKD 协议的要求.

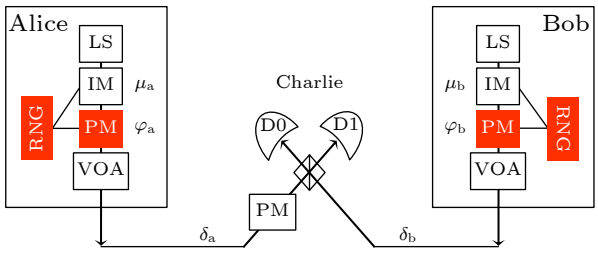

图 12 TF-QKD 协议的实验结构示意图[26]

Fig. 12. Schematic diagram of the TF-QKD protocol[26].

为弥补不同光源的缺点, 2020 年王向斌团队[64]提出了一种基于混合光源的 TF-QKD 协议, 通过采用复合光源结构, 在适用性和效率上达到较好的平衡. 该协议的核心是在信号态上使用 HSPS代替 WCS, 而诱骗态源仍然使用 WCS. 基于复合光源的 SNS TF-QKD 协议中, Alice 和 Bob 双方随机互不影响地以一定概率将时间窗口定义为诱骗态窗口或信号态窗口. 在信号态窗口上使用 HSPS, 以一定概率随机地产生比特 0 或 1, 针对不同比特信息, 选择发或不发信号态脉冲. 而对于诱骗态窗口, 使用 WCS 光源随机调制成不同强度的诱骗态, 然后将调制后的脉冲发送给第三方 Charlie; Charlie 对 Alice 和 Bob 发过来的光脉冲执行单光子测量, 并公布测量结果. 如果其中一个探测器有响应, 则定义该事件为有效事件, 对应的匹配窗口为有效窗口. 双方进行多次通信, 保存有效事件的数据. Alice 和 Bob 使用 X 基对应窗口事件去估计单光子脉冲引起的误码率, 使用 Z 基窗口事件来估计单光子脉冲引起的条件计数率, 然后使用对应的密钥率公式来计算安全密钥[64]. 仿真结果显示, 与基于 WCS 的同类 TF-QKD 协议相比, 使用该复合光源协议得到的密钥率和安全传输距离均显示较优的性能.

总之, 通过使用复合光源的方案, 即使用 WCS 作为诱骗态和使用 HSPS 作为信号态的方法, 既可以保留 HSPS 安全传输距离上的优点, 又能够满足 TF-QKD 协议中对单光子干涉的要求, 因此理论上具有可行性和高效性 (HSPS 仅适用于 SNS 这类基于单光子成码的 TF-QKD 协议, 而不适用于其他类型的 TF 协议, 如 PM-QKD, NPP-QKD 等). 不过考虑到实验上在不同类型的光源之间进行高速随机切换具有比较大的操作难度, 此外可能产生一定侧信道漏洞, 因此该协议离实际应用还有比较长的距离.

6 总结与展望

自第一个 BB84 协议被提出以来, QKD 已经经历了近四十年的发展历程, 在理论和实验方面均取得了许多重大突破. 目前, QKD 已经成为量子信息领域中最成熟也最接近于实用化的技术之一. 本文从 HSPS 的基本原理出发, 结合目前 QKD 协议的 3 个主流协议 (BB84, MDI 和 TF), 阐述了 HSPS 在不同 QKD 协议中的应用与表现, 通过与基于 WCS 的 QKD 协议做比较, 证明了 HSPS 在 QKD 应用中能够使安全传输距离大幅提升. 此外, 考虑到 HSPS 主要利用光子的关联特性产生, 可以通过结合被动式诱骗态等技术进一步提升 QKD 系统的可靠性、安全性, 以及协议的多样性. 不过受到现有实验技术条件的限制 (如参量光耦合效率偏低、编码装置损耗较大, 单光子探测器最大计数率受限等), 目前基于 HSPS 的 QKD 系统实用性

仍低于基于 WCS 的同类系统. 但我们相信, 随着实验技术的不断提升和发展, HSPS 终将会逐步显示出在 QKD 系统中的优越性.

参考文献

[1] Bennett C H, Brassard G 1984 *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing* (Bangalore: IEEE) p175
[2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[3] Bennett C H, Brassard G, Mermin N D 1992 *Phys. Rev. Lett.* **68** 557
[4] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121
[5] Scarani V, Acín A, Ribordy G, Gisin N 2004 *Phys. Rev. Lett.* **92** 057901
[6] Inoue K, Waks E, Yamamoto Y 2002 *Phys. Rev. Lett.* **89** 037902
[7] Bruß D 1998 *Phys. Rev. Lett.* **81** 3018
[8] Brassard G, Lütkenhaus N, Mor T, Sanders BC 2000 *Phys. Rev. Lett.* **85** 1330
[9] Lütkenhaus N, Jahma M 2002 *New J. Phys.* **4** 44
[10] Makarov V, Hjelme D R 2005 *J. Mod. Opt.* **52** 691
[11] Qi B, Fung C H F, Lo H K, Ma X F 2007 *Quantum Inf. Comput.* **7** 73
[12] Zhao Y, Fung C H F, Qi B, Chen C, Lo H K 2008 *Phys. Rev. A* **78** 042333
[13] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J, Makarov V 2010 *Nat. Photonics* **4** 686
[14] Gerhardt I, Liu Q, Lamas-Linares A, Skaar J, Kurtsiefer C, Makarov V 2011 *Nat. Commun.* **2** 1
[15] Weier H, Krauss H, Rau M, Fürst M, Nauerth S, Weinfurter H 2011 *New J. Phys.* **13** 073024
[16] Wiechers C, Lydersen L, Wittmann C, Elser D, Skaar J, Marquardt Ch, Makarov V, Leuchs G 2011 *New J. Phys.* **13** 013043
[17] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901
[18] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503
[19] Lo H K, Ma X, Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[20] Braunstein S L, Pirandola S 2012 *Phys. Rev. Lett.* **108** 130502
[21] Lo H K, Curty M, Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[22] Silva T F, Vitoreti D, Xavier G B, do Amaral G C, Temporão G T, von derWeid J P 2013 *Phys. Rev. A* **88** 052303
[23] Liu Y, Chen T Y, Wang L J, Pan J W 2013 *Phys. Rev. Lett.* **111** 130502
[24] Rubenok A, Slater J A, Chan P, Lucio-Martinez I, Tittel W 2013 *Phys. Rev. Lett.* **111** 130501
[25] Pirandola S, Laurenza, Ottaviani C, Banchi L 2017 *Nature Commun.* **8** 15043
[26] Lucamarini M, Yuan Z L, Dynes J F, Shields A J 2018 *Nature* **557** 400
[27] Ma X, Zeng P, Zhou H 2018 *Phys. Rev. X* **8** 031043
[28] Wang X B, Yu Z W, Hu X L 2018 *Phys. Rev. A* **98** 062323
[29] Cui C H, Zhen Y Q, Wang R, Chen W, Wang S, Guo G C 2019 *Phys. Rev. Appl.* **11** 034053
[30] Curty M, Azuma K, Lo H K 2019 *Npj Quantum Inf.* **5** 1
[31] Lin J, Lütkenhaus N 2018 *Phys. Rev. A* **98** 042332
[32] Wang S, He D Y, Yin Z Q, Lu F Y, Cui C H, Chen W, Zhou Z, Guo G C, Han Z F 2019 *Phys. Rev. X* **9** 021046
[33] Liu Y, Yu Z W, Zhang W, et al. 2019 *Phys. Rev. Lett.* **123** 100505
[34] Zhong X, Hu J, Curty M, Qian L, Lo H K 2019 *Phys. Rev. Lett.* **123** 100506
[35] Pittaluga M, Minder M, Lucamarini M, Sanzaro M, Shields A J 2021 *Nat. Photon.* **15** 530
[36] Wang S, Yin Z Q, He D Y, Chen W, Wang R Q, Ye P, Zhou Y, Yuan-Fan G J, Wang F X, Chen W, Zhu Y G, Morozov P V, Divochiy A V, Zhou Z, Guo G C, Han Z F 2022 *Nat. Photon.* **16** 154
[37] Wang Q, Chen W, Xavier G, Swillo M, Zhang T, Sauge S, Tengner M, Han Z F, Guo G C, Karlsson A 2008 *Phys. Rev. Lett.* **100** 090501
[38] Zhang C H, Wang D, Zhou X Y, Wang S, Zhang L B, Yin Z Q, Chen W, Han Z H, Guo G C, Wang Q 2018 *Opt. Express* **26** 25921
[39] Zhu F, Wang Q 2014 *Acta Opt. Sin.* **6** 0627002 (in Chinese) [朱峰, 王琴 2014 光学学报 **6** 0627002]
[40] Wang D 2017 *Ph. D. Dissertation* (Hefei: University of Science and Technology of China) (in Chinese) (in Chinese) [王东 2017 博士学位论文 (合肥: 中国科学技术大学)]
[41] Zhang C H 2020 *Ph. D. Dissertation* (Nanjing: nanjing University of Posts and Telecommunications) (in Chinese) [张春辉 2020 博士学位论文 (南京: 南京邮电大学)]
[42] Wang Q, Karlsson A 2007 *Phys. Rev. A* **76** 014309
[43] Bock M, Lenhard A, Chunnilall C, Becher C 2016 *Opt. Express* **24** 23992
[44] Aboussouan P, Alibart O, Ostrowsky D B, Baldi P, Tanzilli S 2010 *Phys. Rev. A* **81** 021801
[45] Kaneda F, Garay-Palmett K, U'Ren A B, Kwiat P G 2016 *Opt. Express* **24** 10733
[46] Weston M M, Chrzanowski H M, Wollmann S, Boston A, Ho J, Shalm L K, Verma V B, Allman M S, Nam S W, Patel R B, Slussarenko S, Pryde G J 2016 *Opt. Express* **24** 10869
[47] Zhong H S, Li Y, Li W, et al. 2018 *Phys. Rev. Lett.* **121** 250505
[48] Sansa Perna A, Ortega E, Gräfe M, Steinlechner F 2022 *Appl. Phys. Lett.* **120** 074001
[49] Gottesman D, Lo H K, Lütkenhaus N, Preskill J 2004 *Quantum Inf. Comput.* **5** 325
[50] Wang Q, Wang X B, Guo G C 2007 *Phys. Rev. A* **75** 012312
[51] Adachi Y, Yamamoto T, Koashi M, Imoto N 2007 *Phys. Rev. Lett.* **99** 180503
[52] Wang Q, Zhang C H, Wang X B 2016 *Phys. Rev. A* **93** 032312
[53] Ma X, Qi B, Zhao Y, Lo H K 2005 *Phys. Rev. A* **72** 012326
[54] Zhang C H, Luo S L, Guo G C, Wang Q 2015 *Phys. Rev. A* **92** 022332
[55] Wang Q, Wang X B 2013 *Phys. Rev. A* **88** 052332
[56] Zhang C H, Zhang C M, Guo G C, Wang Q 2018 *Opt. Express* **26** 4219
[57] Zhou Y H, Yu Z W, Wang X B 2016 *Phys. Rev. A* **93** 042324
[58] Xu F, Xu H, Lo H K 2014 *Phys. Rev. A* **89** 052333
[59] Zhang C H, Zhang C M, Wang Q 2019 *Phys. Rev. A* **99** 052325
[60] Hu X L, Yu Z W, Wang X B 2018 *Phys. Rev. A* **98** 032303
[61] Abruzzo S, Kampermann H, Bruß D 2014 *Phys. Rev. A* **89** 012301
[62] Panayi C, Razavi M, Ma X, Lütkenhaus N 2014 *New J. Phys.* **16** 043005
[63] Kaneda F, Xu F, Chapman J, Kwiat P G 2017 *Optica* **4** 1034
[64] Xu H, Hu X L, Feng X L, Wang X B 2020 *Opt. Lett.* **45** 4120

REVIEW

Overview of applications of heralded single photon source in quantum key distribution*

Meng Jie [1)2)#] Xu Le-Chen [1)2)#] Zhang Cheng-Jun [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 27 February 2022; revised manuscript received 15 April 2022)

Abstract

In this paper, we mainly introduce the preparation and physical properties of the heralded single-photon source, the development history and its applications in three typical quantum key distribution protocols, including BB84, measurement-device-independent and twin-field quantum key distribution protocols. Moreover, we make comparisons of the above quantum key distribution protocols between using heralded single-photon source and using weak coherent sources, and analyze their advantages and disadvantages. Besides, according to the characteristics of single-photon interference in twin-field quantum key distributions, the limitations of separately applying heralded single-photon sources to twin-field quantum key distributions are revealed, and possible solutions are discussed. Therefore, this work may provide valuable references and help for the practical implementation of quantum secure communication in the near future.

Keywords: quantum key distribution, heralded single photon source, weak coherent state light source, passive decoy state

PACS: 03.65.–w, 03.67.Hk, 42.50.Ex, 42.79.Sz **DOI:** 10.7498/aps.71.20220344

* 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, 12104240), and the Jiangsu Natural Science Foundation, China (Grant Nos. BK20192001, BK20210582).

# 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

标记单光子源在量子密钥分发中的应用

孟杰 徐乐辰 张成峻 张春辉 王琴

Overview of applications of heralded single photon source in quantum key distribution

Meng Jie Xu Le-Chen Zhang Cheng-Jun Zhang Chun-Hui Wang Qin

引用信息 Citation: Acta Physica Sinica, 71, 170304 (2022) DOI: 10.7498/aps.71.20220344
在线阅读 View online: https://doi.org/10.7498/aps.71.20220344
当期内容 View table of contents: http://wulixb.iphy.ac.cn
