第 41 卷 第 16 期/2021 年 8 月/光学学报 研究论文

光学学报

基于多晶体指示源的测量设备无关量子密钥分配协议

何业锋[1,2]，白倩[1*]，李丽娜[1]，陈思昊[1]，强雨薇[1]

[1]西安邮电大学网络空间安全学院，陕西 西安 710121；

[2]桂林电子科技大学广西密码学与信息安全重点实验室，广西 桂林 541004

摘要 为提高测量设备无关量子密钥分配协议的性能，研究了基于多晶体指示源和脉冲位置调制的测量设备无关量子密钥分配协议。在多晶体指示源下，比较了有脉冲位置调制和无脉冲位置调制下测量设备无关量子密钥分配协议性能的优劣。仿真结果表明，引入脉冲位置调制可以提高该协议的密钥生成率并增大安全传输距离。并且，随着时隙的增加，密钥生成率逐渐提高，安全传输距离也逐渐增大。随后，进一步地分析了探测器在不同探测效率下，安全传输距离与密钥生成率之间的关系。结果表明，探测器探测效率越高，密钥生成率越高，安全传输距离越长。

关键词 量子光学；测量设备无关；量子密钥分配；脉冲位置调制；多晶体指示源

中图分类号 TN918 **文献标志码** A **doi**：10.3788/AOS202141.1627001

Measurement-Device-Independent Quantum Key Distribution Protocols Based on Multiple Crystal Heralded Source

He Yefeng[1,2], Bai Qian[1*], Li Lina[1], Chen Sihao[1], Qiang Yuwei[1]

[1] *School of Cyberspace Security, Xi'an University of Posts and Telecommunications, Xi'an, Shaanxi* 710121, *China*;

[2] *Guangxi Key Laboratory of Cryptography and Information Security, Guilin University of Electronic Technology, Guilin, Guangxi* 541004, *China*

Abstract This paper studies a measurement-device-independent quantum key distribution protocol based on a multiple crystal heralded source and pulse position modulation to improve its performance. The performances of the protocols with or without pulse position modulation are compared under the multiple crystal heralded source. The simulation results show that the application of pulse position modulation can further improve the key generation rate and increase secure transmission distance of the protocol. Moreover, as the time slot increases, the key generation rate and the secure transmission distance gradually rise. Furthermore, we analyze the relationship between the secure transmission distance and the key generation rate under different detection efficiencies of the detector. The results show that the higher detection efficiency of the detector leads to the greater key generation rate and the longer secure transmission distance.

Key words quantum optics; measurement device independent; quantum key distribution; pulse position modulation; multiple crystal heralded source

OCIS codes 270.5565; 270.5568; 270.3430; 190.4410

1 引 言

量子密钥分配[1](QKD)是量子信息科学中一个非常重要的分支，其基本原理是基于量子力学和信息论，因而具有无条件安全特点[2-4]，是目前量子密码学研究领域的热点[5-7]。但是，实际的 QKD 系

收稿日期：2021-02-05；**修回日期**：2021-03-10；**录用日期**：2021-03-18

基金项目：国家自然科学基金(61802302)、陕西省自然科学基础研究项目(2021JM-462)、广西密码学与信息安全重点实验室研究课题(GCIS201923)

通信作者：*1572318226@qq.com

统中所使用的设备具有不符合理论要求的非理想特性，进而容易受到不同类型的攻击。比如，针对非理想光源的相位部分随机化攻击[8]和光子数分离攻击[9]等，针对非理想探测器的致盲攻击[10]和时移攻击[11]等。测量设备无关量子密钥分配(MDI-QKD)方案[12]的提出引起了广大学者的关注，MDI-QKD方案使得 QKD 系统不易受探测器侧信道的攻击，并增大了通信系统的安全传输距离。随着 MDI-QKD 方案的不断完善，其在实验和理论上都得到了广泛的研究[13-16]。

在 MDI-QKD 协议中，常用弱相干态(WCS)光源代替理想的单光子源，但 WCS 光源中的真空脉冲与多光子脉冲占比相对较大，这将会降低密钥生成率。另一种方案是利用线性晶体中的自发参量下转换(SPDC)过程[17]，其在 QKD 中被广泛用作激发源或指示单光子源。朱峰等[18]提出基于指示单光子源的 QKD 协议，介绍了具体的理论方案并推导出了具有泊松分布的指示源的 MDI-QKD 的误码率上界和计数率的下界。带有后选择的多晶体指示源简称多晶体指示源或 MHPS，它的引入改善了指示源的单光子特性。文献[19]中提出一种具有 MHPS 的 MDI-QKD 方案，与基于 WCS 光源的 QKD 协议相比，密钥生成速率得到了提高，且传输距离得到了增大。这是因为 MHPS 为高单光子事件和低多光子事件提供了很好的折衷方案。文献[20]中提出一种修正的 MHPS MDI-QKD 方案，结合诱骗态方法，分析了对称结构和非对称结构下 QKD 系统的性能。

目前，MDI-QKD 协议中主要采用极化编码[21]和相位编码[22]方案。但是，这两种方案都存在基的依赖性问题。近年来，轨道角动量(OAM)编码已被广泛应用于 QKD 系统的研究[23-26]。当采用 OAM 编码时，参考系统的旋转不会改变 OAM 的测量值。因此，基于 OAM 编码的 MDI-QKD 协议能够有效解决基的依赖性问题。此外，在传统的 MDI-QKD 协议中，只能使用单光子脉冲来提取安全密钥，但单光子脉冲仅能携带 1 bit 的信息。采用脉冲位置调制(PPM)技术可以将每个脉冲调制到 PPM 帧内的某个时隙中进而增加单光子脉冲携带的信息量[27]，这表明 PPM 技术可以提高 MDI-QKD 协议的密钥生成率[28-29]。文献[30]中提出一种基于 PPM 技术的 MDI-QKD 协议，该协议能够进一步增大系统的安全传输距离。

本文在基于 MHPS 的 MDI-QKD 协议基础上结合 PPM 技术，通过将每个脉冲调制到 PPM 帧内的某个时隙中来增加单光子脉冲携带的信息量，进而提高 MDI-QKD 协议的密钥生成率和增大安全传输距离。仿真比较了无脉冲位置调制和有脉冲位置调制下 MDI-QKD 的密钥生成率与安全传输距离之间的关系。此外，还比较了该协议在探测器的不同探测效率下，密钥生成率与安全传输距离之间的关系。

2 基本原理

2.1 多晶体指示源

MHPS 由 M 个指示源(HS)组成，其中 HS 能利用强相干场泵浦的非线性晶体(NLC)上的 SPDC 效应产生纠缠光子对[20]。对于每个 HS，光子对中的空闲光子被发送到触发探测器端，信号光子被发送到输出端。MHPS 的光子数分布[20]为

$$P_X^{\mathrm{MHPS}}(u,M)=\begin{cases}\exp(-Mu), & X=0\\ \dfrac{u^X}{X!}\exp(-u)\dfrac{1-\exp(-Mu)}{1-\exp(-u)}, & X\geqslant 1\end{cases},\tag{1}$$

式中：X 为光子数；u 为平均强度。

2.2 基于 MHPS 和 PPM 技术的 MDI-QKD 协议

基于 MHPS 和 PPM 技术的 MDI-QKD 系统模型如图 1 所示。其中，Alice 和 Bob 使用了并行的 NLC，D_A、D_B 分别表示 Alice 端和 Bob 端的触发探测器，O. S 表示光开关，Pol-M、PPM、IM、BS、PBS 分别表示偏振调制器、脉冲位置调制、强度调制器、分束器和偏振分束器，D_{1H}、D_{2H}、D_{1V}、D_{2V} 分别为第三方的单光子探测器，Charile 为不可信的第三方。

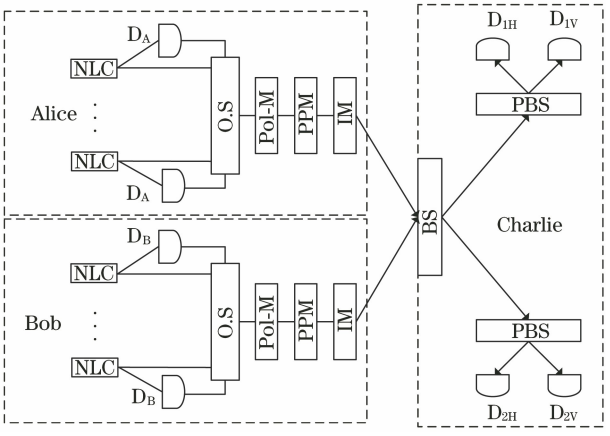

图 1 基于 MHPS 和 PPM 技术的 MDI-QKD 的系统模型

Fig. 1 System model of MDI-QKD based on MHPS and PPM technology

该方案的具体步骤如下。

1) Alice 和 Bob 利用 NLC 产生纠缠光子对，

光子对中的空闲光子被发送到触发探测器 D_A 和 D_B，信号光子经过 Pol-M 后，选取 x 基或 z 基进行偏振编码，x 基用于检测错误，z 基用于提取安全密钥。

2) 利用 PPM 技术将信号脉冲编码为 PPM 帧。每个 PPM 帧中的一个脉冲仅占用一个时隙，其他为空脉冲不携带信息。如果发送 X 个光子脉冲，则 PPM 技术将其编码为拥有 k 个时隙的 PPM 帧的概率为 $P_{X,\mathrm{PPM}}^{\mathrm{MHPS}}(u,M)=k\cdot P_X^{\mathrm{MHPS}}(u,M)\cdot[P_X^{\mathrm{MHPS}}(u,M)]^{k-1}$，即

$$P_X^{\mathrm{MHPS}}(u,M)=\begin{cases}k\cdot\exp(-kMu), & X=0\\ k\cdot\dfrac{u^X}{X!}\exp[-(k-1)Mu-u]\dfrac{1-\exp(-Mu)}{1-\exp(-u)}, & X\geqslant 1\end{cases}。\tag{2}$$

之后，Alice 和 Bob 中的信号光子被发送到 IM 中并被随机调制为真空态、诱骗态和信号态，分别表示为 u_0,u_1,u_2 和 v_0,v_1,v_2。此外，参数满足 $u_2>u_1>u_0=0$ 和 $v_2>v_1>v_0=0$。

3) 当 Charlie 接收到来自 Alice 和 Bob 的脉冲信号后，在两个 PPM 帧的相应时隙上进行 Bell 态测量，并公布测量结果。然后，Alice 和 Bob 比较所使用的测量基，保留相同基情况下的数据信息，并由其中一方进行比特翻转，得到各自的初始密钥。接着，通信双方对初始密钥进行隐私放大和保密加强。

2.3 密钥生成率分析

当 Alice 和 Bob 的脉冲强度分别为 $u_i(i=0,1,2)$ 和 $v_j(j=0,1,2)$时，根据 MHPS 的光子数分布和文献[20]，总增益 $Q_{u_iv_j}^w$ 和总误码率 $E_{u_iv_j}^w$ 被定义为

$$Q_{u_iv_j}^w=\sum_{n,m=0}^{\infty}P_{n,\mathrm{PPM}}^{\mathrm{MHPS}}(u_i,M)P_{m,\mathrm{PPM}}^{\mathrm{MHPS}}(v_j,M)Y_{nm}^w,\tag{3}$$

$$E_{u_iv_j}^wQ_{u_iv_j}^w=\sum_{n,m=0}^{\infty}P_{n,\mathrm{PPM}}^{\mathrm{MHPS}}(u_i,M)P_{m,\mathrm{PPM}}^{\mathrm{MHPS}}(v_j,M)e_{nm}^wY_{nm}^w,\tag{4}$$

式中：w 为 x 或 z，表示选取 x 基或 z 基进行编码；n 和 m 分别为 Alice 和 Bob 发送的光子数目；Y_{nm}^w 为第三方成功进行 Bell 态测量的概率；e_{nm}^w 为第三方成功进行 Bell 态测量的误码率。

将(2)、(3)式与文献[14]的估计方法结合可以得到

$$\begin{aligned}&\frac{1}{k^2}\left\{[\exp[(k-1)Mu_2+u_2]\frac{1-\exp(u_2)}{1-\exp(-Mu_2)}\exp[(k-1)Mv_2+v_2]\frac{1-\exp(-v_2)}{1-\exp(-Mv_2)}Q_{u_2v_2}^w-\right.\\&\left.\exp[(k-1)Mu_1+u_1]\frac{1-\exp(u_1)}{1-\exp(-Mu_1)}\exp[(k-1)Mv_1+v_1]\frac{1-\exp(v_1)}{1-\exp(-Mv_1)}Q_{u_1v_1}^w\right\}\geqslant\\&g_1+g_2+g_3-(\lambda u_2v_1+\lambda u_1v_2-u_2v_2+u_1v_1)Y_{11}^w,\end{aligned}\tag{5}$$

进一步，由(5)式推导得到单光子计数率的下界 Y_{11}^w 为

$$\begin{aligned}Y_{11}^w\geqslant&\frac{-\frac{1}{k^2}\exp[(k-1)Mu_2+u_2]\frac{1-\exp(u_2)}{1-\exp(-Mu_2)}\exp[(k-1)Mv_2+v_2]\frac{1-\exp(-v_2)}{1-\exp(-Mv_2)}Q_{u_2v_2}^w}{\lambda u_2v_1+\lambda u_1v_2-u_2v_2+u_1v_1}+\\&\frac{\frac{1}{k^2}\exp[(k-1)Mv_1+v_1]\frac{1-\exp(-v_1)}{1-\exp(-Mv_1)}\exp[(k-1)Mu_1+u_1]\frac{1-\exp(-u_1)}{1-\exp(-Mu_1)}Q_{u_1v_1}^w+g_1+g_2+g_3}{\lambda u_2v_1+\lambda u_1v_2-u_2v_2+u_1v_1},\end{aligned}\tag{6}$$

式中：

$$\begin{aligned}g_1=&\frac{1}{k^2}\left\{\exp[(k-1)Mv_2+v_2]\frac{1-\exp(-v_2)}{1-\exp(-Mv_2)}Q_{0v_2}^w+\exp[(k-1)Mu_2+u_2]\frac{1-\exp(-u_2)}{1-\exp(-Mu_2)}Q_{u_20}^w-\right.\\&\left.\exp[(k-1)Mu_1+u_1]\frac{1-\exp(-u_1)}{1-\exp(-Mu_1)}Q_{u_10}^w-\exp[(k-1)Mv_1+v_1]\frac{1-\exp(-v_1)}{1-\exp(-Mv_1)}Q_{0v_1}^w\right\},\end{aligned}\tag{7}$$

$$g_2=\frac{\lambda}{k^2}\left\{\exp[(k-1)Mu_1+u_1]\frac{1-\exp(-u_1)}{1-\exp(-Mu_1)}\exp[(k-1)Mv_2+v_2]\frac{1-\exp(-v_2)}{1-\exp(-Mv_2)}Q_{u_1v_2}^w-\right.$$

$$\exp[(k-1)Mv_2+v_2]\frac{1-\exp(-v_2)}{1-\exp(-Mv_2)}Q^{w}_{0v_2}-\exp[(k-1)Mu_1+u_1]\frac{1-\exp(-u_1)}{1-\exp(-Mu_1)}Q^{w}_{u_10}+Q^{w}_{00}\Big\},\tag{8}$$

$$g_3=\frac{\lambda}{k^2}\Big\{\exp[(k-1)Mu_2+u_2]\frac{1-\exp(-u_2)}{1-\exp(-Mu_2)}\exp[(k-1)Mv_1+v_1]\frac{1-\exp(-v_1)}{1-\exp(-Mv_1)}Q^{w}_{u_2v_1}-$$
$$\exp[(k-1)Mv_1+v_1]\frac{1-\exp(-v_1)}{1-\exp(-Mv_1)}Q^{w}_{0v_1}-\exp[(k-1)Mu_2+u_2]\frac{1-\exp(-u_2)}{1-\exp(-Mu_2)}Q^{w}_{u_20}+Q^{w}_{00}\Big\},\tag{9}$$

$$\lambda=\min\left(\frac{u_2v_2^2-u_1v_1^2}{u_2v_1^2+u_1v_2^2},\frac{u_2^2v_2-u_1^2v_1}{u_2^2v_1+u_1^2v_2},\frac{u_2^2v_2^2-u_1^2v_1^2}{u_2^2v_1^2+u_1^2v_2^2}\right)。\tag{10}$$

由(2)、(4)式可推导得到单光子误码率的上界 e^{w}_{11} 为

$$e^{w}_{11}\leqslant\frac{\exp[(k-1)Mu_1+u_1]\frac{1-\exp(u_1)}{1-\exp(-Mu_1)}\exp[(k-1)Mv_1+v_1]\frac{1-\exp(v_1)}{1-\exp(-Mv_1)}Q^{w}_{u_1v_1}E^{w}_{u_1v_1}}{k^2u_1v_1Y^{w}_{11}}-$$
$$\frac{\exp[(k-1)Mv_1+v_1]\frac{1-\exp(v_1)}{1-\exp(-Mv_1)}Q^{w}_{0v_1}E^{w}_{0v_1}+\exp[(k-1)Mu_1+u_1]\frac{1-\exp(u_1)}{1-\exp(-Mu_1)}Q^{w}_{u_10}E^{w}_{u_10}-Q^{w}_{00}E^{w}_{00}}{k^2u_1v_1Y^{w}_{11}},\tag{11}$$

根据文献[12]，推导得到的密钥生成率 R 的公式为

$$R\geqslant(\log_2 k)P^{\mathrm{MHPS}}_{1,\mathrm{PPM}}(u_2,M)P^{\mathrm{MHPS}}_{1,\mathrm{PPM}}(v_2,M)Y^{z}_{11}[1-H(e^{x}_{11})]-Q^{z}_{u_2v_2}fH(E^{z}_{u_2v_2}),\tag{12}$$

式中：$H(s)=-s\log_2 s-(1-s)\log_2(1-s)$ 为二进制香农熵函数；f 为纠错效率。

3　仿真结果与分析

利用数值模拟来分析 PPM 技术对 MDI-QKD 协议的影响，对比了不同探测器探测效率下密钥生成率和安全传输距离之间的关系。仿真过程中采用的参数如表 1 所示，其中，p_d 为探测器的暗计数率，e_d 为系统的调节误差。仿真结果如图 2 和图 3 所示。诱骗态和信号态的光强分别 0.001 和 0.02。此外，假设探测效率相同，$\eta_A=\eta_B=0.145$ or 0.75。

表 1　主要模拟参数

Table 1　Main simulation parameters

Parameter	p_d	f	e_d
Value	1×10^{-6}	1.16	0.015

图 2 和图 3 展示了在不同探测器探测效率下，MDI-QKD 协议的密钥生成率和安全传输距离之间的关系。可以看出，PPM 技术的引入提高了 MDI-QKD 协议的密钥生成率并增大了安全传输距离。当编码时隙 $k=8$ 时，MDI-QKD 协议的密钥生成率最高。在通信距离相等的情况下，采用 PPM 技术的 MDI-QKD 协议的密钥生成率高于未采用 PPM 技术的 MDI-QKD 协议的密钥生成率。当时隙为 k 时，调制脉冲携带 $\log_2 k$ 位比特信息，增加了单个光子脉冲所具有的信息量，进而提高了 MDI-QKD 协议的密钥生成率。对比图 2 和图 3 可知，当编码时隙 $k=8$ 时，如果探测器的探测效率为 0.145，则 MDI-QKD 协议的最大安全传输距离可达 120 km 左右；如果探测器的探测效率为 0.75，则 MDI-QKD 协议的最大安全传输距离可达 160 km 左右。仿真结果表明：探测器探测效率越高，MDI-QKD 的密钥生成率越高且传输距离越大。这是因为探测器探测效率越高，能够探测到的单光子信号脉冲越多，进而

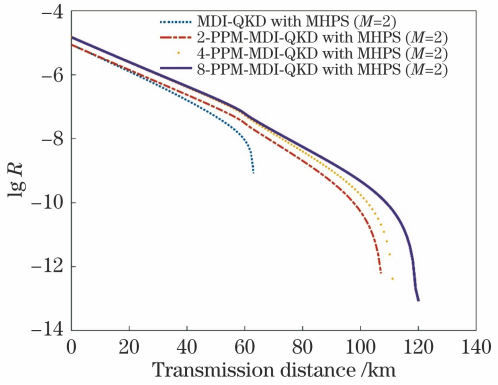

图 2　$\eta_A=\eta_B=0.145$ 时，密钥生成率与安全传输距离的关系

Fig. 2　Relationship between key generation rate and transmission distance when $\eta_A=\eta_B=0.145$

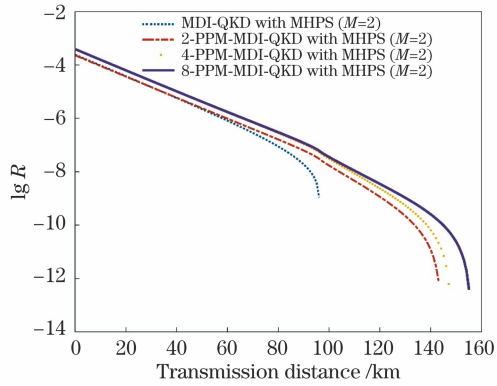

图 3 $\eta_A=\eta_B=0.75$ 时，密钥生成率与安全传输距离的关系

Fig. 3 Relationship between key generation rate and transmission distance when $\eta_A=\eta_B=0.75$

提高了 MDI-QKD 系统的性能。

4 结 论

将 PPM 技术应用于基于 MHPS 的 MDI-QKD 协议中，通过公式推导和模拟仿真，分析了基于 MHPS 和 PPM 技术的 MDI-QKD 协议的性能。对比了在不同单光子探测器探测效率下，MDI-QKD 协议的密钥生成率与安全传输距离的关系。仿真结果表明，与未采用 PPM 技术的 MDI-QKD 协议相比，采用 PPM 技术的 MDI-QKD 协议的密钥生成率和安全传输距离增大。此外，在相同的条件下，单光子探测器的探测效率越高，得到的密钥生成率越高且传输距离越长。

参 考 文 献

[1] Bennett C H, Brassard G. An update on quantum cryptography[M]//Blakley G R, Chaum D. Advances in cryptology. Lecture notes in computer science. Heidelberg: Springer, 1984, 196: 475-480.

[2] Mayers D. Unconditional security in quantum cryptography[J]. Journal of the ACM, 2001, 48(3): 351-406.

[3] Gottesman D, Lo H K, Lutkenhaus N, et al. Security of quantum key distribution with imperfect devices[C]//International Symposium on Information Theory, 2004. ISIT 2004. Proceedings, June 27-July 2, 2004, Chicago, IL, USA. New York: IEEE Press, 2004: 136.

[4] Shor P W, Preskill J. Simple proof of security of the BB84 quantum key distribution protocol[J]. Physical Review Letters, 2000, 85(2): 441-444.

[5] Zhu Q L, Shi L, Wei J H, et al. Background light suppression in free space quantum key distribution[J]. Laser & Optoelectronics Progress, 2018, 55(6): 060004.
朱秋立, 石磊, 魏家华, 等. 自由空间量子密钥分配的背景光抑制[J]. 激光与光电子学进展, 2018, 55(6): 060004.

[6] Du Y N, Xie W Z, Jin X, et al. Analysis on quantum bit error rate in measurement device-independent quantum key distribution using weak coherent states [J]. Acta Physica Sinica, 2015, 64(11): 110301.
杜亚男, 解文钟, 金璇, 等. 基于弱相干光源测量设备无关量子密钥分发系统的误码率分析[J]. 物理学报, 2015, 64(11): 110301.

[7] Zhu Z D, Zhao S H, Wang X Y, et al. Phase modulate free measurement device independent quantum key distribution[J]. Journal of Optoelectronics·Laser, 2018, 29(2): 181-186.
朱卓丹, 赵尚弘, 王星宇, 等. 相位调制无关的测量设备无关量子密钥分配协议[J]. 光电子·激光, 2018, 29(2): 181-186.

[8] Sun S H, Liang L M. Experimental demonstration of an active phase randomization and monitor module for quantum key distribution[J]. Applied Physics Letters, 2012, 101(7): 071107.

[9] Brassard G, Lütkenhaus N, Mor T, et al. Limitations on practical quantum cryptography[J]. Physical Review Letters, 2000, 85(6): 1330-1333.

[10] Makarov V, Skaar J. Faked states attack using detector efficiency mismatch on SARG04, phase-time, DPSK, and Ekert protocols[J]. Quantum Information and Computation, 2008, 8(6/7): 622-635.

[11] Zhao Y, Fung C H F, Qi B, et al. Quantum hacking: experimental demonstration of time-shift attack against practical quantum-key-distribution systems[J]. Physical Review A, 2008, 78(4): 042333.

[12] Lo H K, Curty M, Qi B. Measurement-device-independent quantum key distribution[J]. Physical Review Letters, 2012, 108(13): 130503.

[13] Zhou N R, Zhu K N, Zou X F. Multi-party semi-quantum key distribution protocol with four-particle cluster states[J]. Annalen Der Physik, 2019, 531(8): 1800520.

[14] Sun S H, Gao M, Li C Y, et al. Practical decoy-state measurement-device-independent quantum key distribution[J]. Physical Review A, 2013, 87(5): 052339.

[15] Li H H, Gong L H, Zhou N R. New semi-quantum key agreement protocol based on high-dimensional single-particle states[J]. Chinese Physics B, 2020, 29(11): 110304.

[16] Kang D N, He Y F. Quantum key distribution protocols based on asymmetric channels of odd coherent sources[J]. Acta Optica Sinica, 2017, 37(6):

0627001.
康丹娜, 何业锋. 基于奇相干光源非对称信道的量子密钥分配协议[J]. 光学学报, 2017, 37(6): 0627001.

[17] Adachi Y, Yamamoto T, Koashi M, et al. Simple and efficient quantum key distribution with parametric down-conversion[J]. Physical Review Letters, 2007, 99(18): 180503.

[18] Zhu F, Wang Q. Quantum key distribution protocol based on heralded single photon source[J]. Acta Optica Sinica, 2014, 34(6): 0627002.
朱峰, 王琴. 基于指示单光子源的量子密钥分配协议[J]. 光学学报, 2014, 34(6): 0627002.

[19] Schiavon M, Vallone G, Ticozzi F, et al. Heralded single-photon sources for quantum-key-distribution applications[J]. Physical Review A, 2016, 93: 012331.

[20] Dong C, Zhao S H, Deng M Y. Measurement-device-independent quantum key distribution with multiple crystal heralded source with post-selection [J]. Quantum Information Processing, 2018, 17(3): 1-12.

[21] Tamaki K, Lo H K, Fung C H F, et al. Phase encoding schemes for measurement-device-independent quantum key distribution with basis-dependent flaw [J]. Physical Review A, 2012, 85(4): 042307.

[22] Tang Z Y, Liao Z F, Xu F H, et al. Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution[J]. Physical Review Letters, 2014, 112(19): 190503.

[23] Zhu Z D, Zhao S H, Gu W Y, et al. Orbital-angular-momentum-encoded measurement-device-independent quantum key distributions under atmospheric turbulence [J]. Acta Optica Sinica, 2018, 38(12): 1227002.
朱卓丹, 赵尚弘, 谷文苑, 等. 大气湍流下的轨道角动量编码测量设备无关量子密钥分发[J]. 光学学报, 2018, 38(12): 1227002.

[24] He Y F, Li D Q, Song C, et al. Quantum key distribution protocol based on odd coherent sources and orbital angular momentum[J]. Chinese Journal of Lasers, 2018, 45(7): 0712001.
何业锋, 李东琪, 宋畅, 等. 基于奇相干光源和轨道角动量的量子密钥分配协议[J]. 中国激光, 2018, 45(7): 0712001.

[25] He Y F, Guo J R, Li C Y, et al. Fluctuation analysis of key distribution protocol based on heralded single-photon source and orbital angular momentum [J]. Chinese Journal of Lasers, 2020, 47(4): 0412001.
何业锋, 郭佳瑞, 李春雨, 等. 基于指示单光子源和轨道角动量的密钥分配协议的波动分析[J]. 中国激光, 2020, 47(4): 0412001.

[26] He Y F, Yang H J, Wang D, et al. Quantum key distribution based on heralded pair coherent state and orbital angular momentum[J]. Acta Optica Sinica, 2019, 39(4): 0427001.
何业锋, 杨红娟, 王登, 等. 基于标记配对相干态和轨道角动量的量子密钥分配[J]. 光学学报, 2019, 39(4): 0427001.

[27] Wang L, Zhou Y Y, Zhou X J, et al. Passive measurement-device-independent quantum key distribution with orbital angular momentum and pulse position modulation[J]. Optoelectronics Letters, 2018, 14(2): 138-142.

[28] Zhou H C, Wornell G. Adaptive pulse-position modulation for high-dimensional quantum key distribution[C]//2013 IEEE International Symposium on Information Theory, July 7-12, 2013, Istanbul, Turkey. New York: IEEE Press, 2013: 359-363.

[29] He Y F, Li C Y, Guo J R, et al. Passive measurement-device-independent quantum key distribution based on heralded pair coherent states[J]. Chinese Journal of Lasers, 2020, 47(9): 0912002.
何业锋, 李春雨, 郭佳瑞, 等. 基于标记配对相干态的被动测量设备无关量子密钥分配[J]. 中国激光, 2020, 47(9): 0912002.

[30] Mao Q P, Wang L, Ma Y Y, et al. Measurement-device-independent quantum key distribution with pulse-position modulation[J]. Acta Photonica Sinica, 2018, 47(3): 0306007.