引用本文：何翼龙，郭邦红：实时跟踪补偿的 OAM 测量设备无关量子密钥分发[J]. 光通信技术，2019，43(8)：42-46.

实时跟踪补偿的 OAM 测量设备无关量子密钥分发

何翼龙[1]，郭邦红[2,1*]

（1.华南师范大学 信息光电子科技学院，广州 510631；2.深圳大学 计算机与软件学院，广东 深圳 518060）

摘要：大气信道传输过程引入的畸变相位严重限制了基于自由空间的轨道角动量(OAM)量子密钥分发的安全传输距离，为了实现畸变相位的实时监测和补偿，基于自适应光学技术提出一种实时跟踪补偿的 OAM 编码的测量设备无关量子密钥分发(OAM-MDI-QKD)方案。方案采用波前补偿和相位共轭，设计了双重补偿的自适应光学系统；采用单一光源的结构，解决了双光源的波长模式不匹配问题；利用 OAM 进行编码，解决了传统 MDI-QKD 的测量基参考系对不准问题。仿真结果表明：在信道损耗相同的情况下，本方案的损耗容错比传统的 MDI-QKD 方案高 42 dB，比无补偿的 OAM-MDI-QKD 方案高 2 dB。

关键词：测量设备无关量子密钥分发；轨道角动量；自适应光学补偿；安全码率

中图分类号：TN256　**文献标识码**：A　**文章编号**：1002-5561(2019)08-0042-05

DOI：10.13921/j.cnki.issn1002-5561.2019.08.011　**开放科学(资源服务)标识码(OSID)**：

Measurement-device-independent QKD based on orbital angular momentum with real-time tracking compensation

HE Yilong[1], GUO Banghong[2,1*]

(1. School of Information and Optoelectronic Science and Engineering, South China Normal University, Guangzhou 510631, China;
2. School of Computer Science & Software Engineering, Shenzhen University, Shenzhen Guangdong 518060, China)

Abstract: Distortion phase introduced in atmospheric channel transmission seriously limits the secure transmission distance of orbital angular momentum (OAM) quantum key distribution based on free space. In order to realize real-time monitoring and compensation of distortion phase, based on adaptive optics technology, a measurement-device-independent quantum key distribution (OAM-MDI-QKD) scheme for real-time tracking compensation of OAM coding is proposed. Wavefront compensation and phase conjugation, are used to design an adaptive optical system with double compensation. The structure of a single light source is used to solve the problem of wavelength mode mismatch between two light sources. The problem of inaccuracy in the measurement reference frame of traditional MDI-QKD is solved by coding with OAM. The simulation results show that the loss tolerance of the proposed scheme is 42 dB higher than that of the traditional MDI-QKD scheme and 2 dB higher than that of the uncompensated OAM-MDI-QKD scheme under the same channel loss.

Key words: measurement-device-independent quantum key distribution; OAM; adaptive optical compensation; security bit rate

0 引言

自 1984 年第一个量子密钥分发(QKD)协议[1]问世以来，QKD 一直被认为是量子信息领域最接近实际应用的技术。QKD 允许 2 个用户(Alice 和 Bob)基于量子物理定律产生具有理论上无条件安全的密钥。然而，在实际系统中，由于 QKD 系统的理想模型和实际设备之间存在较大的差距[2]，导致不同类型的安全漏洞[3]。理想的 QKD 协议需要理想的单光子源和单光子探测器，这对于目前的技术而言是难以实现的。这些漏洞可能被窃听者利用，引发 QKD 系统的时间移位[4]、探测器致盲[5]和被动法拉第镜像[6]等各种攻击。窃听者(Eve)利用这些手段可以窃取部分或全部的密钥比特。为了克服这些技术缺陷，人们提出了设备无关的量子密钥分发(DI-QKD)的概念[7]。DI-QKD 的安全性不取

收稿日期：2019-05-28。

基金项目：国家自然科学基金面上项目(No. 61572203)资助；广东省重点领域研发计划(No.2018B030325002)资助；瞬态光学与光子技术国家重点实验室开放基金(No. SKLST201602)资助；中国科学院量子信息重点实验室项目(No. KQI201508)资助。

作者简介：何翼龙(1993-)，男，硕士，现就读于华南师范大学信息光电子科技学院光学工程专业，主要从事量子保密通信及其网络工程方面的研究，设计轨道角动量编码的测量设备无关的量子密钥分发系统。

*** 通信作者**：郭邦红(E-mail：guobangh@163.com)。

决于设备的特性，即使设备不理想，量子黑客也无法利用这一缺陷窃取到任何信息。因此，DI-QKD 总是能保证无条件的理论安全。然而，DI-QKD 的实现是一项艰难的挑战，它需要完美的 Bell 态测量和非常高效率的单光子检测技术，现有技术难以达到。2012 年，Lo 等人提出了测量设备无关的 QKD 协议（MDI-QKD）[8]，减小了 DI-QKD 与实用化的距离，消除了所有与探测相关的潜在安全漏洞。同时，该协议引入诱骗态方案，利用相位随机化使得光子态转化为光子数的混态，可以抵御光子数分裂攻击。

目前，人们已提出多种 MDI-QKD 方案，如偏振编码方案[9]、相位编码方案[10]和 time-bin 编码方案[11]等。但这些方案大多都存在测量基参考系不完全匹配的问题。对此，人们提出了基于轨道角动量态（OAM）编码的 MDI-QKD 方案[12,13]，不需要参考系的匹配。对于偏振编码的 MDI 方案而言，2 个重要的误码源是参考系失配和模式失配，而采用 OAM 编码可以避免参考系失配问题，减小误码率。但是，该方案采用的是用户独立的双光源结构，存在模式失配的问题，并且针对信道环境也没有进行监测和信号补偿，因此系统容易受到外界环境的干扰，导致成码速率降低，甚至无法成码。本文基于即插即用 MDI-QKD 的思想[14]，设计并提出单一光源的 OAM-MDI-QKD 方案。

1 OAM-MDI-QKD 方案原理

OAM-MDI-QKD 系统由 Alice 端、Bob 端和测量单元 3 部分构成，如图 1 所示。其中，AP1~AP4 是望远镜系统，F1、F2 是窄带滤波器，BS1~BS3 是分束器，CCD1、CCD2 是电荷耦合元件，D1、D2 是光延时线，PBS1~PBS3 是偏振分束器，WC1~WC4 是波前校正器，HP1、HP2 是半波片，SLM1、SLM2 是空间光调制器，IM1-2 是强度调制器，Laser 是脉冲激光器，OS1、OS2 为 OAM 分离装置，SPD1~SPD4 是单光子探测器。

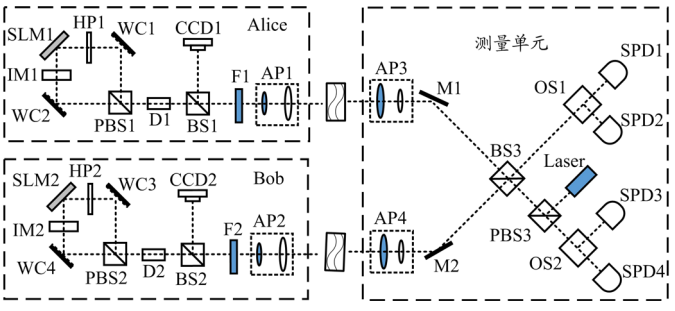


图 1 OAM-MDI-QKD 系统的原理图

OAM-MDI-QKD 方案原理为：

首先，测量单元产生光脉冲通过自由空间信道分别发往 Alice 端和 Bob 端，Alice 端和 Bob 端分别利用自适应光学系统测量并补偿光脉冲的畸变相位，同时随机将光脉冲编码到 4 个 OAM 态中。然后，Alice 端和 Bob 端对光脉冲进行相位共轭补偿，并沿着原自由空间信道发往测量单元进行 Bell 态测量。测量单元公布成功的测量结果，Alice 端和 Bob 端公布它们编码使用的基矢。对于它们使用相同基矢的部分，根据测量单元的 Bell 态测量结果，Alice 端或 Bob 端选择翻转或不翻转它们手中的比特数据。最后，它们根据诱骗态方法得到单光子部分的增益和误码率，经过密钥协商过程得到最终的安全密钥。

具体过程如下：

①测量单元的脉冲激光器发出基模高斯光束经过 PBS3 后，竖直偏振光被反射至 BS3，其过程如式（1）所示：

$$|L_0\rangle(|H\rangle+|V\rangle)\xrightarrow{\text{PBS3}}|L_0\rangle|V\rangle \tag{1}$$

其中，L_0 代表拓扑荷数为 0 的高斯光，H、V 分别为水平偏振和竖直偏振。该光束被 BS3 分成 2 束，再利用 AP3、AP4 准直，控制远场发散角，通过自由空间信道发往用户端 Alice 和 Bob。在经过自由空间信道时，OAM 态容易受到大气湍流的影响，导致相位畸变，此时状态变为：

$$|L_0\rangle|V\rangle\xrightarrow{\text{大气}}e^{i\varphi(r,\theta)}|L_0\rangle|V\rangle \tag{2}$$

其中，$\varphi(r,\theta)$为大气湍流引入的畸变相位，r 为径向分量，θ 为方位角。

用户端 Alice（Bob）的 AP1（AP2）接收来自测量单元的脉冲激光，先经过窄带滤波器 F1（F2）滤除通信波段以外的噪声，再经过 BS1（BS2）将入射的脉冲激光分成强弱 2 路，分别为较强的上支路和较弱的下支路。上支路连接 CCD1（CCD2）用于监测激光脉冲的强度和大气湍流造成的畸变相位 $\varphi(r,\theta)$，为时钟同步以及相位畸变补偿提供参考信息；下支路的脉冲经过 D1（D2）延时后，被 PBS1（PBS2）反射至 WC1（WC3）。波前校正器可通过改变光波波前传输的光程来改变入射光波波前的相位结构[15]，其根据上支路提供的参考信息，可对波前相位进行第一次畸变补偿，并且直接校正畸变的相位波前，将脉冲恢复成 $|L_0\rangle$ $|V\rangle$，然后通过 HWP1（HWP2）将其偏振旋转 90°，状态变成 $|L_0\rangle|H\rangle$，进入 SLM1（SLM2）进行轨道角动量编码。由于任意阶数的 OAM 态间相互独立，因此取任意 2 个不同阶数

的 OAM 都可以组成一组相互无偏基进行编码。这里假设编码的基组为:

X 基,$\{|L_1\rangle,|L_2\rangle\}$

Z 基,$\{(|L_1\rangle+|L_2\rangle)/\sqrt{2},(|L_1\rangle-|L_2\rangle)/\sqrt{2}\}$

其中,$|L_1\rangle$和$(|L_1\rangle+|L_2\rangle)/\sqrt{2}$代表比特 0;$|L_2\rangle$和$(|L_1\rangle-|L_2\rangle)/\sqrt{2}$代表比特 1;$|L_1\rangle$、$|L_2\rangle$分别代表不同拓扑荷数的 OAM 态,$L_1$ 和 L_2 代表拓扑荷值。用户双方随机选择任意基下的任意一个状态进行编码,编码后的状态变为$|L_{code}|V\rangle$。其中,$|L_{code}|V\rangle$为编码的 OAM 态。

②用户端 Alice(Bob)利用 IM1(IM2)将脉冲调制成不同平均光子数强度的 OAM 信号态与诱骗态。在发往测量单元前,本文利用 WC2(WC4)对 OAM 光束进行第二次补偿,即相位共轭补偿。此时加载的相位是与畸变相位共轭的相位,携带这个共轭相位的光束反向穿过同样的大气时,光束将被还原,从而达到校正的目的。该过程 OAM 态的变化如下:

$$|L_{code}|H\rangle\xrightarrow{WC2/WC4}e^{-i\varphi(r,\theta)}|L_{code}|H\rangle\xrightarrow{大气}|L_{code}|H\rangle \quad (3)$$

其中,$e^{-i\varphi(r,\theta)}$为加载的共轭相位。此时,经过相位共轭校正的光束将透过 PBS1(PBS2),沿原光路发往测量单元,并在测量单元的 BS3 处干涉,分束器将擦除光子态的路径信息,使得光子态不可区分。由于双光子干涉效应(HOM 效应),相同的光子态会从分束器的同一输出端口输出,不同的光子态则相互独立输出。输出的光子态通过OAM 分离装置分离后进入探测器产生响应。

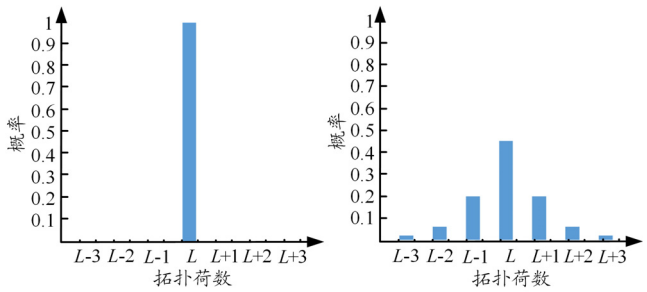
③用户端 Alice 和 Bob 根据测量单元的响应情况,经过基的对比和密钥协商等过程后,在本地产生一致的密钥。

2 系统性能分析

2.1 密钥速率分析

与偏振编码的 MDI-QKD 方案类似,OAM-MDI-QKD 方案中,用户端 Alice 和 Bob 同样也是利用 X 基下获得的数据成码、Y 基下获得的数据用于检测误码。不同的是,使用 OAM 进行编/解码,不需要进行测量基的参考系校准,因此消除了偏振失配造成的误码,并且 OAM 的旋转不变性 [13] 使得 OAM 光的传输更具鲁棒性。另外,本文方案采用了单一光源的结构,具有天然的波长模式一致性,可以消除波长模式不匹配造成的误码,进一步提升安全码率。

然而,由于 OAM 态的纯度对大气湍流和链路衰减比较敏感,容易受到大气湍流和链路衰减的影响,导致光线的随机漂移,造成光束横截面的重新分布(光束畸变、光束展宽、光强起伏和像点抖动)等一系列的大气湍流效应,使传输的 OAM 态偏离原本的模式,散射到相邻的 OAM 模式上成负面影响 [16]。假设传输前 OAM 态的拓扑荷数为 L,经过大气信道后,OAM 态一定概率散射至相邻的 OAM 模式上,即拓扑荷数一定概率变为相邻的数值,其概率分布如图 2 所示。



(a) 经过大气湍流前　　(b) 经过大气湍流后

图 2 大气湍流对拓扑荷数为 L 的 OAM 光的散射效应

为简化分析,下面考虑 Kolmogorov 模型下的大气湍流影响。由文献[17]可知,经过大气信道后,发送的 OAM 态与接收方测量到的 OAM 态一致的概率为:

$$P_0=\frac{1}{\pi}\int_0^1\rho d\rho\int_0^{2\pi}\exp\left[-6.88\times3^{2/3}\left(\frac{r}{r_0}\sin\frac{\Delta\theta}{2}\right)^{5/3}\right]d\Delta\theta \quad (4)$$

其中,$\Delta\theta$ 为经过湍流前后的方位角系数差值;r_0 为大气相干长度,取决于大气湍流强度;r 为径向分量;$\rho=r/R$,其中 R 为接收孔半径。而接收方测量到的 OAM 态是相邻的 OAM 态的概率为:

$$P_{\Delta l}=\frac{1}{\pi}\int_0^1\rho d\rho\int_0^{2\pi}\exp\left[-6.88\times3^{2/3}\left(\frac{r}{r_0}\sin\frac{\Delta\theta}{2}\right)^{5/3}\right]\times\cos(\Delta l\Delta\theta)d\Delta\theta \quad (5)$$

其中,Δl 为拓扑荷数的差值。为了降低大气湍流带来的影响,本文运用波前补偿和相位共轭 2 种自适应光学补偿技术,设计了双重补偿的自适应光学系统,可实现大气信道的实时监测和补偿,补偿效率为 30%~50%。经过补偿后,方案系统的串扰和功率损耗可被有效降低。本方案的安全密钥生成率为:

$$R=\mu_a\mu_b\exp(-\mu_a-\mu_b)Y_Z^{11}[1-H_2(e_X^{11})]-Q_zf_e(E_z)H_2(E_z) \quad (6)$$

其中,μ_a、μ_b 分别是 Alice、Bob 的信号态强度,Y_Z^{11} 是 Z 基下的单光子计数率,e_X^{11} 是 X 基下的单光子误码率,f_e 函数为数据协调过程的纠错效率,$H_2(X)$为二元熵函数,Q_z、E_z 分别为 Z 基下的总增益和总误码。Y_Z^{11}、e_X^{11}、

Q_z、E_z 的计算方法请参考文献[18]，本文不再赘述。

2.2 安全分析

MDI-QKD 协议的安全性来源于基于纠缠态的 QKD 协议[19]和诱骗态方法[20]。MDI-QKD 协议可以看成是时间反演的纠缠态协议(EPR-QKD)[19]，其与基于纠缠态的 QKD 协议具有相同的安全性。因为 Charlie/Eve 的测量是用来对 Alice 和 Bob 之间的纠缠进行后选择的，所以可以用时间反转的思想来证明 MDI-QKD 的安全性。

在原始 MDI-QKD 协议中，Alice 和 Bob 都不执行任何测量，它们仅将量子信号发送到测量单元，即使窃听者 Eve 控制了测量单元，也无法窃听到任何信息。MDI-QKD 消除了探测端的所有潜在的漏洞，并且协议中的 Alice和 Bob 都使用了诱骗态方法，可抵御光子数分裂攻击。此外，当发送给 Charlie 的信号光为单光子时，Alice 和 Bob 就能获得增益和量子密钥误码率(QBER)。

本文提出的实时跟踪补偿的 OAM-MDI-QKD 方案是建立在原始 MDI-QKD 协议的基础之上的。在本文的方案中，OAM 编码的过程不影响偏振模式，Alice 和 Bob 采用 X 基$\{|L_1\rangle, |L_2\rangle\}$和 Y 基$\{1/\sqrt{2}(|L_1\rangle+|L_2\rangle), 1/\sqrt{2}(|L_1\rangle-|L_2\rangle)\}$对信息进行编码，并将量子信号发送到测量单元进行 Bell 态测量。虽然本方案的编码过程与传统的 MDI-QKD 不同，但仍然是使用了 Alice 和 Bob 之间的后选择纠缠。因此，利用时间反演的思想也可以证明 OAM-MDI-QKD 的安全性。另外，本文提出的方案引入了类似即插即用 MDI-QKD 的结构[14]，采用了第三方的单一光源。光源可以由完全不可信的第三方控制，这在某种程度上其更容易受到各种针对光源的攻击，但通过保留一些假设，包括单模假设、相位随机化假设和监控设备的信任等，可以保证其安全性，这在文献[14]中有较为完整的安全性分析。文献[14]表明：通过对光源的监控，精确监测每个信号脉冲的能量和到达时间，即使用户使用不可信的光源，也能保证获得的密钥是安全的。本文的方案利用 CCD 来监控信号脉冲，用窄带滤波器来保证光束的单模性，采用了自适应光学技术，可有效抵消补偿大气湍流造成的影响，提升系统的抗干扰性。因此，本文的协议也是无条件安全的，具有更好的性能。

3 仿真结果

本文根据式(4)和式(5)仿真了大气湍流对 OAM 态传输造成的影响。

概率随参数 r/r_0 的变化如图 3 所示。参数 r/r_0 与大气湍流引起的波前相位畸变相关，当参数 r/r_0 变大，此时接收方收到初始 OAM 态的概率 P_0 逐渐减小，最后趋于稳定；而接收方收到相邻 OAM 态的概率 $P(\Delta l=1)$则先随着 r/r_0 的增加而快速增大，在 $r/r_0\geqslant1.2$ 时，稍有减小，随后趋于稳定。这一现象的主要原因是随着大气湍流效应的不断增强，光子的 OAM 将逐渐趋于随机分布[17]。

本文采用 50%的补偿效率对本方案的安全码率进行仿真，μ_a、μ_b 均设置为 0.3，并且只有传输正确的 OAM 光才能成码，即经过补偿后 OAM 态保持原本状态的信号光才能成码，选取设定的参数(失配误码 e_d=1.5%，暗计数 $Y_0=3\times10^{-6}$，探测效率 η_d=14.5%，数据协调的协调效率 f_e=1.16)进行仿真，其安全码率情况如图 4 所示。

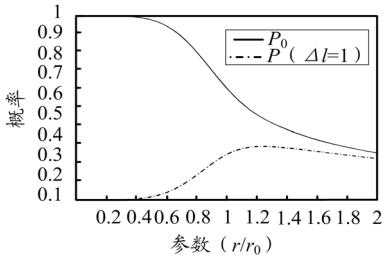


图 3 概率随参数 r/r_0 的变化

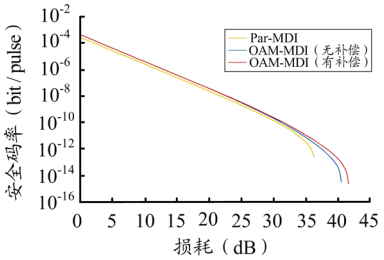


图 4 安全码率与信道损耗的关系

如图 4 所示，本文对比了偏振编码的 MDI-QKD 方案[8]和未加补偿的 OAM 编码的 MDI-QKD 方案[12](如表 1 所示)。仿真结果表明：在信道衰减的参数一致的情况下，OAM 编码的安全码率要比偏振(Par-MDI)编码的方案高出约 1.82×10^{-4}bit/pulse，这是因为 OAM 编码的方案消除了用户端和测量端之间偏振失配造成的误码，提高了安全码率。而本文的方案借鉴了即插即用 MDI-QKD 的思想[14]，使用单光源解决了光源模式的不匹配问题，进一步提高了码率。在加入补偿系统后，本方案可容纳更高的信

表 1 4 种 MDI-QKD 方案对比

方案	参考基对准	光源	光源模式不匹配
Par-MDI	需要	双光源	存在
即插即用的 MDI	需要	单光源	不存在
无补偿 OAM-MDI	不需要	双光源	存在
有补偿 OAM-MDI	不需要	单光源	不存在

道损耗(超过 42 dB),比无补偿的 OAM-MDI-QKD 方案高 2 dB。在大气环境较好时,即大气衰减系数 β 在 0.2~0.4 dB/km 之间时,本方案可以在大气信道传输 24.2~48.4 km,比无补偿方案远 2.4 km。

本方案是基于自由空间的 OAM 编码的 MDI-QKD 方案。在通信距离方面,本方案比基于光纤的 OAM-MDI-QKD 方案更远,但仍然不如基于光纤的其它自由度(偏振、相位等)编码的 QKD 方案。这是由于在光纤中高阶矢量模式容易发生简并,OAM 难以稳定传输造成。但在成码率方面,由于 OAM 具有无限个本征态,理论上可承载无穷比特的信息,因此在进行量子秘钥分发时,如果系统采用 OAM 进行编码或复用,将极大提高成码率,增大信道容量。

4 结束语

由于量子偏振态极易受到温度、压力等外界因素影响,导致其状态发生变化,通信的发送方和接收方在进行实时检测和校准基参考系时,会出现对不准的情况,使得 MDI-QKD 协议的密钥速率受到影响。针对这一问题,本文提出了单一光源结构的 OAM-MDI-QKD 方案,其以 OAM 作为量子通信的载体,不需要进行测量基参考系的对准,解决了光源模式不匹配的问题,并且本文引入自适应光学系统,通过波前补偿和相位共轭 2 种自适应光学补偿技术,设计了双重补偿的自适应光学系统,减小了大气湍流带来的相位畸变。最后,本文通过仿真说明了本方案在参数设置一致的情况下,对比其它方案能容纳更高的信道损耗,在大气环境较好的情况下,传输距离可达 48.4 km。

参考文献:

[1] BENNETT C H, BRASSARD G. Quantum cryptography: Public key distribution and coin tossing [J]. Theoretical Computer Science, 2014, 560: 7–11.

[2] MA X, QI B, ZHAO Y, et al. Practical decoy state for quantum key distribution[J]. Physical Review A, 2005, 72(1): 012326-1–012326-15.

[3] MAKAROV V, ANISIMOV A, SKAAR J. Effects of detector efficiency mismatch on security of quantum cryptosystems [J]. Physical Review A, 2005, 74(2): 022313-1–022313-11.

[4] QI B, FUNG C H F, LO H K, et al. Time-shift attack in practical quantum cryptosystems [J]. Quantum Information & Computation, 2007, 7(1): 73–82.

[5] LYDERSEN L, WIECHERS C, WITTMANN C, et al. Hacking commercial quantum cryptography systems by tailored bright illumination[J]. Nature Photonics, 2010, 4(10): 686–689.

[6] SUN S H, JIANG M S, LIANG L M. Passive Faraday-mirror attack in a practical two-way quantum-key-distribution system[J]. Physical Review A, 2011, 83(6): 062331-1–062331-7.

[7] ACÍN ANTONIO, BRUNNER N , GISIN N, et al. Device-Independent Security of Quantum Cryptography against Collective Attacks [J]. Physical Review Letters, 2007, 98(23): 230501-1–230501-4.

[8] LO H K, CURTY M, QI B. Measurement-Device-Independent Quantum Key Distribution [J]. Physical Review Letters, 2012, 108 (13), 130503-1–130503-5.

[9] XU F, QI B, LIAO Z, et al. Long distance measurement-device-independent quantum key distribution with entangled photon sources [J]. Applied Physics Letters, 2013, 103(6): 061101-1–061101-4.

[10] 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): 042307-1 –042307-14.

[11] MA X F, RAZAVI M. Alternative schemes for measurement-device-independent quantum key distribution[J]. Physical Review A, 2012, 86 (6): 3818–3821.

[12] WANG L, ZHAO S M, GONG L Y, at al. Free-space measurement-device-independent quantum-key-distribution protocol using decoy states with orbital angular momentum[J]. Chinese Physics B, 2015, 24(12): 120307-1 –120307-8.

[13] DONG Chen, ZHAO Shang-hong, SUN Ying. Measurement-device-independent quantum key distribution with q-plate [J]. Quantum Information Processing, 2015, 14(12): 4575–4584.

[14] XU Feihu. Measurement-device-independent quantum communication with an untrusted source [J]. Physical Review A, 2015, 92 (1): 012333-1–012333-11.

[15] KOTOVA S, KVASHNIN M, RAKHMATULIN M, et al. Modal liquid crystal wavefront corrector[J]. Optics Express, 2002, 10(22): 1258–1272.

[16] REN Y, XIE G, HUANG H, et al. Adaptive optics compensation of multiple orbital angular momentum beams propagating through emulated atmospheric turbulence[J]. Optics Letters, 2014, 39(10): 2845–2848.

[17] 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,2019,38 (12):1227002-1 –1227002-6.

[18] XU F, CURTY M, QI B, et al. Practical aspects of measurement-device-independent quantum key distribution [J]. New Journal of Physics, 2013, 15(11): 113007-1–113007-28.

[19] BENNETT C H, BRASSARD G, MERMIN N D. Quantum cryptography without Bell's theorem[J]. Physical Review Letters, 1992, 68(5): 557–559.

[20] LO H K, MA X, CHEN K. Decoy state quantum key distribution[J]. Physical Review Letters, 2005, 94(23): 230504-1–230504-4.