基于奇相干光源和轨道角动量的量子密钥分配协议

何业锋[1,2]，李东琪[2*]，宋畅[2]，高建国[3]

[1]西安邮电大学无线网络安全技术国家工程实验室，陕西 西安 710121；

[2]西安邮电大学通信与信息工程学院，陕西 西安 710121；

[3]陕西瑞祥石油技术服务有限公司，陕西 西安 710018

摘要 针对基于弱相干光源(WCS)和轨道角动量(OAM)的测量设备无关量子密钥分配(MDI-QKD)协议的密钥生成率较低的问题，研究了基于奇相干光源(OCS)和 OAM 的 MDI-QKD 协议，并对其性能参数进行了分析。分析了密钥生成率、探测器的品质因子与安全传输距离之间的关系，并对比了基于 OCS 和 OAM 的 MDI-QKD 协议与基于 WCS 和 OAM 的 MDI-QKD 协议的性能优劣。仿真结果表明，随着安全传输距离的增大，密钥生成率减小。采用 OCS 大大减少了多光子脉冲数，弥补了 WCS 的不足，而采用 OAM 解决了基的依赖性缺陷问题，从而增大了最大安全传输的距离，该研究为实用的量子密钥分配协议提供了重要的理论参考。

关键词 量子光学；轨道角动量；测量设备无关；量子密钥分配；奇相干光源

中图分类号 TN918 **文献标识码** A **doi**：10.3788/CJL201845.0712001

Quantum Key Distribution Protocol Based on Odd Coherent Sources and Orbital Angular Momentum

He Yefeng[1,2], Li Dongqi[2], Song Chang[2], Gao Jianguo[3]

[1]*National Engineering Laboratory of Wireless Network Security Technology, Xi'an University of Posts and Telecommunications, Xi'an, Shaanxi* 710121, *China*;

[2]*School of Communications and Information Engineering, Xi'an University of Posts and Telecommunications, Xi'an, Shaanxi* 710121, *China*;

[3]*Shaanxi Ruixiang Petroleum Technology Service Co. Ltd., Xi'an, Shaanxi* 710018, *China*

Abstract In view of the problem of the low key generation rate for the measurement device independent quantum key distribution (MDI-QKD) protocol based on weak coherent sources (WCS) and orbital angular momentum (OAM), the MDI-QKD protocol based on odd coherent sources (OCS) and OAM is investigated, and its performance and parameters are analyzed. The relationships between key generation rate, quality factor of detector and secure transmission distance are investigated. The performance comparison between the MDI-QKD protocol based on OCS and OAM and the MDI-QKD protocol based on WCS and OAM is compared. The simulation results show that the key generation rate decreases with the increase of secure transmission distance. The adoption of OCS makes up the deficiency of WCS and reduces the photon number greatly, while the adoption of OAM can solve the problem of the dependence defect of the base and increase the maximum secure transmission distance, which provides an important theoretical reference for the practical quantum key distribution protocol.

Key words quantum optics; orbital angular momentum; measurement device independent; quantum key distribution; odd coherent source

OCIS codes 270.3430; 270.1670; 270.5568; 270.5565

收稿日期：2017-12-25；**收到修改稿日期**：2018-02-06

基金项目：国家重点研发计划(2017YFB0802000)、国家自然科学基金(61472472)、陕西省自然科学基础研究计划(2017JM6037)

作者简介：何业锋(1978—)，女，博士，副教授，主要从事网络安全与量子密钥分配方面的研究。E-mail：yefenghe1978@163.com

* **通信联系人**。E-mail：dongqi_Li@163.com

1　引　　言

量子密钥分配(QKD)是量子密码的重要组成部分之一。第一个 QKD 协议是由 Bennett 等[1]在 1984 年提出的,也称为 BB84 协议,该协议在量子力学和信息论原理下被证明是无条件安全的[2]。近年来,QKD 一直是国内外研究的热点之一[3-7]。但是,QKD 的无条件安全性只是理论上的,在实际应用中,由于设备不够完善,系统存在一些安全漏洞,探测器和光源都会受到一些攻击。例如,针对非理想探测器实施的致盲攻击[8]、伪态攻击[9]等;针对非理想光源实施的相位部分的随机化攻击[10]、光子数分流攻击[11]等。2012 年,Lo 等[12]提出了一种测量设备无关量子密钥分配(MDI-QKD)方案。在 MDI-QKD 系统中,通信双方不需要作任何测量,只需将制备的光子态发送给不可信的第三方进行贝尔态测量(BSM)[13],最终得到安全密钥,其优点是可以避开探测器侧信道的漏洞[14-15]。MDI-QKD 被提出以后,在理论和实验上的发展都十分迅猛,现在正朝着实用性方向发展[16-17]。目前,MDI-QKD 的实现方案主要有两种:相位编码方案[18]和极化编码方案[12]。这两种方案虽然消除了探测器的影响,但是在制备光子的过程中均会受到基的依赖性[18]影响。即在基的制备和测量阶段,通信双方需要实时地对参考系进行检测和调整,这会使密钥生成率受到一定的影响。而文献[19]所用到的轨道角动量(OAM)可以作为量子信息的载体[20-21],并且用 OAM 态编码时,OAM 的测量值不会因测量参考系的旋转而发生变化,因此,基于 OAM 的 MDI-QKD 可以有效地解决基的依赖性问题。目前,基于 OAM 的 MDI-QKD 主要采用的是弱相干光源(WCS),不足之处是密钥生成率低。

本文研究了奇相干光源(OCS)下的 OAM-MDI-QKD 协议,分析了密钥生成率、探测器的品质因子与安全传输距离间的关系,并对其性能参数进行了评估。与基于 WCS 的 OAM-MDI-QKD 协议相比,基于 OCS 的 OAM-MDI-QKD 协议大大减少了多光子脉冲数,从而得到了更高的密钥生成率;另一方面,OAM 编码方案避免了极化编码和相位编码方案中基的依赖性缺陷,因此增大了密钥生成率。

2　基本原理

2.1　奇相干态

OCS 只包含奇数光子脉冲的状态,产生的奇相干态可以表示为

$$|\alpha\rangle_{\mathrm{ocs}}=\frac{1}{\sin \mathrm{h}|\alpha|^{2}}\sum_{t=0}^{\infty}\frac{\alpha^{2t+1}}{\sqrt{(2t+1)!}}|2t+1\rangle,\tag{1}$$

式中 α 为消灭算符的本征值,整数 $t=0,1,2,3,\cdots$。

OCS 的光子数分布[22]为

$$p(2t+1)=\frac{|\alpha|^{2(2t+1)}}{\sin \mathrm{h}(|\alpha|^{2})(2t+1)!}。\tag{2}$$

在同一光强下,WCS 和 OCS 的光子脉冲概率分布见表 1[23]。

表 1　WCS 与 OCS 的光子脉冲概率分布[23]

Table 1　Photon pulse probability distributions of WCS and OCS[23]

Pulse source	Single photon number	Multiphoton number
WCS	0.3293	0.1219
OCS	0.9424	0.0576

从表 1 可以看出,在相同光强下,OCS 的单光子脉冲数大于 WCS 的,而多光子脉冲数小于 WCS 的。

2.2　基于 OCS 的 OAM-MDI-QKD 协议

基于 OCS 的 OAM-MDI-QKD 系统模型如图 1 所示[19],其中 BS 为分束器,SLM 为空间光调制器,decoy-IM 为光强度调节器,Alice、Bob 代表通信双方。

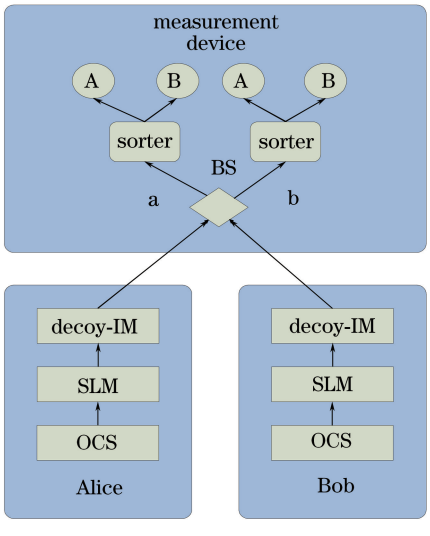

图 1　OCS 下的 OAM-MDI-QKD 方案[19]

Fig. 1　OAM-MDI-QKD protocol with OCS[19]

OAM 一般用拉盖尔-高斯(LG)模[24]来描述,其方位角相位 $\exp(\mathrm{i}l\theta)$(θ 为方位角)中的拓扑电荷 l 即为 OAM 态 $|l\rangle$。通信双方 Alice 和 Bob 首先随机选取两组相互无偏基[25] B_1 和 B_2,利用这两组基的其中一个来编码信息,其中 $B_1=\{|l\rangle,|-l\rangle\}$,$B_2=\{(|l\rangle+|-l\rangle)/\sqrt{2},(|l\rangle-|-l\rangle)/\sqrt{2}\}$,一般

将$|l\rangle$编码为‘0’，$|-l\rangle$编码为‘1’，$(|l\rangle+|-l\rangle)/\sqrt{2}$编码为‘0’，$(|l\rangle-|-l\rangle)/\sqrt{2}$编码为‘1’。然后分别利用 SLM 和 decoy-IM 来制备不同 l 值的 OAM 态和诱骗态。最后将制备的态发送给第三方进行测量，测量装置由 BS、高效 OAM 分离装置 sorter 和探测器组成。

该方案的具体实现过程如下。假设 Alice 和 Bob 均选择 B_1 基来编码信息，当一方处于$|l\rangle$态而另一方处于$|-l\rangle$态时，二者经过 BS 发生干涉后出射的状态[26]为

$$|\Psi\rangle=\frac{1}{2}\left[\frac{|l\rangle|-l\rangle+|-l\rangle|l\rangle}{\sqrt{2}}\times(\mathrm{i}|a\rangle_1|a\rangle_2+i|b\rangle_1|b\rangle_2)+\frac{|l\rangle|-l\rangle-|-l\rangle|l\rangle}{\sqrt{2}}\times(|b\rangle_1|a\rangle_2-|a\rangle_1|b\rangle_2)\right],\tag{3}$$

式中$|a\rangle_1$表示通过 a 支路出射的第一个光子的光子态，$|a\rangle_2$表示通过 a 支路出射的第二个光子的光子态，$|b\rangle_1$表示通过 b 支路出射的第一个光子的光子态，$|b\rangle_2$表示通过 b 支路出射的第二个光子的光子态。(3)式第一项表示光子从 BS 同一侧射出的几率为 1/2，经过的 sorter 装置后测量的结果为同一侧的探测器 A 和 B 均响应；而第二项表示光子以 1/2 的几率从 BS 的两侧射出，这种情况下的测量结果为一侧探测器 A 响应，另一侧探测器 B 响应。等第三方公布测量结果后，才能验证 Alice 和 Bob 得到的结果是否正确。

经分析可知，通信双方最终需要的测量结果是一个探测器 A 和一个探测器 B 响应。保留正确测量结果中的数据，通过经典信道基比对，最终只保留相同基下的数据，然后对 Alice 和 Bob 两者中的其中一个作比特翻转，经过以上操作得到的数据用作原始密钥。当原始密钥足够时，通信双方用由 B_1 基获得的原始密钥生成最终的安全密钥，用由 B_2 基获得的原始密钥检测错误概率。如果错误概率低于误码率的阈值，则进行纠错和私钥放大以进一步提取安全密钥，否则放弃此次通信。

2.3　密钥生成率分析

基于 OAM 的 MDI-QKD 方案解决了基的依赖性缺陷。根据 GLLP(Gottesman-Lo-Lütkenhaus-Preskill)[27]和诱骗态技术[28]，得到密钥生成率的公式[12]为

$$R=P_{\mu_2}(1)P_{\nu_2}(1)Y_{B_1}^{11}[1-H(e_{B_2}^{11})]-Q_{B_1}^{11}f(E_{B_1})H(E_{B_1}),\tag{4}$$

式中 $P_{\mu_2}(1)$表示 Alice 发送信号态时单光子脉冲的概率，$P_{\nu_2}(1)$表示 Bob 发送信号态时单光子脉冲的概率，$Y_{B_1}^{11}$表示单光子计数率，E_{B_1}表示误码率，$Q_{B_1}^{11}$为 Alice 和 Bob 均选择 B_1 基时发送单光子态的增益，$e_{B_2}^{11}$为通信双方均选择 B_2 基时的错误比特率，f 函数为数据协调的协调效率，二进制香农熵 $H=-x\mathrm{lb}(x)-(1-x)\mathrm{lb}(1-x)$。

根据 OCS 光子数分布，利用文献[12]的方法，可以得到总增益和总误码率分别为

$$Q_{\mu_i\nu_j}^{\omega}=\sum_{n,m=0}^{\infty}P_{\mu_i}(n)P_{\nu_j}(m)Y_{nm}^{\omega},$$

$$E_{\mu_i\nu_j}^{\omega}Q_{\mu_i\nu_j}^{\omega}=\sum_{n,m=0}^{\infty}P_{\mu_i}(n)P_{\nu_j}(m)e_{nm}^{\omega}Y_{nm}^{\omega},\tag{5}$$

式中 $P_{\mu_i}(n)$为 Alice 发送 n 个光子脉冲的概率；$P_{\nu_j}(m)$为 Bob 发送 m 个光子脉冲的概率；Y_{nm}^{ω}为第三方含有 n 和 m 个光子时 Alice 和 Bob 获得成功贝尔态的概率；e_{nm}^{ω}为 Alice 和 Bob 分别发送 n 个光子和 m 个光子时的误码率；$n=0,1,2,\ldots$；$m=0,1,2,\ldots$；μ_i 为 Alice 发送的相干光的强度，其中 $i=0,1,2$，分别对应真空态、诱骗态和信号态；ν_j 为 Bob 发送的相干光的强度，同样的 $j=0,1,2$，分别对应真空态、诱骗态和信号态；$\omega=B_1,B_2$ 表示两个基。

由(2)、(5)式可以得到信号态和诱骗态情况下的总增益 $Q_{\mu_i\nu_j}$ 分别为

$$Q_{\mu_2\nu_2}=\sum_{n,m=0}^{\infty}P_{\mu_2}(2n+1)P_{\nu_2}(2m+1)Y_{(2n+1)(2m+1)},\tag{6}$$

$$Q_{\mu_1\nu_1}=\sum_{n,m=0}^{\infty}P_{\mu_1}(2n+1)P_{\nu_1}(2m+1)Y_{(2n+1)(2m+1)}。\tag{7}$$

由(5)、(7)式可知单光子增益 Y_{11} 满足

$$Y_{11}\geqslant\frac{P_{\mu_1}(3)P_{\nu_1}(3)Q_{\mu_2\nu_2}-P_{\mu_2}(3)P_{\nu_2}(3)Q_{\mu_1\nu_1}}{P_{\mu_2}(1)P_{\nu_2}(1)P_{\mu_1}(3)P_{\nu_1}(3)-P_{\mu_2}(3)P_{\nu_2}(3)P_{\mu_1}(1)P_{\nu_1}(1)}。\tag{8}$$

由(5)、(8)式可知单光子误码率 e_{11} 满足

$$e_{11} \leqslant \frac{Q_{\mu_2\nu_2} E_{\mu_2\nu_2}}{P_{\mu_2}(1) P_{\nu_2}(1) Y_{11}}。\tag{9}$$

根据文献[29]得到 B_1 基与 B_2 基下的增益和误码率分别为

$$Q_{\mu_i^1\nu_j}^{B_1} = Q_C + Q_E,\tag{10a}$$

$$Q_{\mu_i^1\nu_j}^{B_1} E_{\mu_i^1\nu_j}^{B_1} = Q_E\tag{10b}$$

$$Q_{\mu_i^2\nu_j}^{B_2} = 2y^2[1 + 2y^2 - 4y\mathrm{I}_0(s) + \mathrm{I}_0(2s)],\tag{11a}$$

$$Q_{\mu_i^2\nu_j}^{B_2} E_{\mu_i^2\nu_j}^{B_2} = e_0 Q_{\mu_i^2\nu_j}^{B_2} - 2e_0 y^2[\mathrm{I}_0(2s) - 1],\tag{11b}$$

式中 Q_C 为光子从同侧射出时的探测概率，Q_E 为光子从两侧射出时的探测概率，s 和 y 为常数，$\mathrm{I}_0(s) \approx 1 + \frac{s^2}{4}$ 为第一类修正贝塞尔函数，e_0 为背光错误概率。Q_C 和 Q_E 的表达式分别为

$$Q_C = 2(1-P_d)^2 \exp(-\mu'/2)[1-(1-P_d)\times \exp(-\eta_a\mu_i/2)][1-(1-P_d)\exp(-\eta_b\nu_j/2)],\tag{12a}$$

$$Q_E = 2P_d(1-P_d)^2\exp(-\mu'/2)\times [\mathrm{I}_0(2s) - (1-P_d)\exp(-\mu'/2)],\tag{12b}$$

式中 P_d 为单光子探测器的暗计数率，η_a 和 η_b 分别为 Alice 和 Bob 信道的传输效率，μ' 为到达继电器的平均光子数。其余参数的表达式分别为

$$\begin{cases} \mu' = \eta_a\mu_i + \eta_b\nu_j \\ s = \sqrt{\eta_a\mu_i\eta_b\nu_j}/2 \\ y = (1-P_d)^2\exp(-\mu'/4) \end{cases}。\tag{13}$$

将(13)式代入(4)式就可以求得最终的密钥生成率。

3　基于 OCS 的 OAM-MDI-QKD 的仿真结果与分析

用 OCS 代替 WCS 后，多光子脉冲明显减少，从而有效地减小了误码率。由(8)、(9)式可以近似得到单光子增益的下界 Y_{11} 与单光子误码率的上界 e_{11}，将其代入(4)式，就可以得到最终的密钥生成率与安全传输距离之间的关系。推导所用的主要参数见表 2。

表 2　主要仿真参数

Table 2　Main simulation parameters

Parameter	Signal state	Decoy state	e_0	P_d	f
Value	0.5	0.1	0.5	3×10^{-6}	1.16

如图 2 所示，三种方案下的密钥生成率均随安全传输距离的增大而逐渐减小，且基于 OCS 和 OAM 的密钥生成率大于基于 WCS 和 OAM 的，也大于只含 OCS 的。这是由于光源由 WCS 换成 OCS 后，多光子脉冲数减小了，并且 OAM 解决了基的依赖性问题，这都增大了密钥生成率。综合来考虑，基于 OCS 和 OAM 的密钥生成率最大，而基于 WCS 和 OAM 的密钥生成率次之。单独使用 OCS 或 OAM 都能增大密钥生成率，而将二者相结合能使密钥生成率增大得更快。

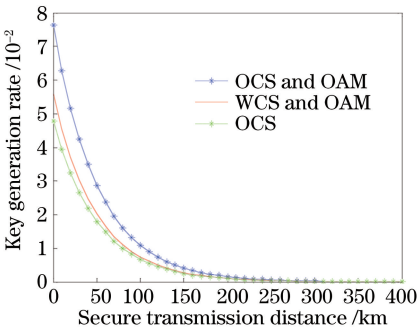

图 2　密钥生成率与安全传输距离间的关系

Fig. 2　Key generation rate versus secure transmission distance

r0 和 s0 分别代表图 1 左侧的 A 和 B，r1 和 s1 分别代表右侧的 A 和 B。图 3(a)所示为探测器 r0、r1 的品质因子 P_{r0}、P_{r1} 与安全传输距离间的关系，可以看出，随着安全传输距离的增大，P_{r0}、P_{r1} 逐渐增大。图 3(b)所示为探测器 s0 和 s1 的品质因子

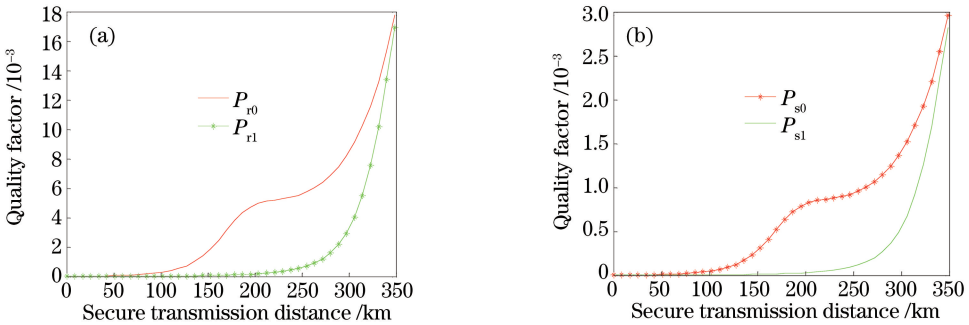

图 3　品质因子与安全传输距离间的关系

Fig. 3　Quality factor versus secure transmission distance

P_{s0}、P_{s1}与安全传输距离间的关系，同样地，二者均随安全传输距离的增大而增大。对比可知，探测器 r0 和探测器 s0 的品质因子的增大趋势一致，而探测器 r1 和探测器 s1 的品质因子的增大趋势一致。这是由于 BSM 成功测量的结果为同侧或对角的两个探测器同时响应。

经分析可知，探测器的品质因子对密钥生成率也有影响，由于品质因子是暗计数与探测器的探测效率的比值，因此探测效率越高，品质因子越小，即密钥生成率越大。故为了增大密钥生成率，在选择探测器时其品质因子不宜过大。

4　结　论

研究了一种基于 OCS 和 OAM 的 MDI-QKD 方案。研究了密钥生成率、探测器的品质因子与安全传输距离之间的关系，并推导了 OCS 单光子增益的下界和单光子误码率的上界。与 WCS 相比，OCS 可以有效地减少多光子脉冲数，从而增大最大安全传输距离；与极化编码方案相比，OAM 有效地解决了基的依赖性缺陷问题。仿真结果表明，三种方案中的密钥生成率均随安全传输距离的增大而减小，而探测器的品质因子随安全传输距离的增大而增大，但是基于 OCS 和 OAM 方案的效果较好。在实际中，可以通过基于 OCS 和 OAM 的 MDI-QKD 方案来得到更大的密钥生成率。

参　考　文　献

[1] Bennet C H, Brassard G. Quantum cryptography [C]. IEEE International Conference on Computers, Systems, and Signal Processing, 1984: 175-179.

[2] Gottesman D, Lo H K, Lutkenhaus N, *et al*. Security of quantum key distribution with imperfect devices[J]. Quantum Information & Computation, 2004, 4(5): 325-360.

[3] Wang J D, Qin X J, Wei Z J, *et al*. An effective active phase compensation method for quantum key distribution system[J]. Acta Physica Sinica, 2010, 59(1): 281-286.
王金东, 秦晓娟, 魏正军, 等. 一种高效量子密钥分发系统主动相位补偿方法[J]. 物理学报, 2010, 59(1): 281-286.

[4] Zhou R R, Yang L. Quantum election scheme based on anonymous quantum key distribution[J]. Chinese Physics B, 2012, 21(8): 080301.

[5] Zhou Y Y, Zhou X J, Tian P G, *et al*. New protocols for non-orthogonal quantum key distribution[J]. Chinese Physics B, 2013, 22(1): 010305.

[6] Zhu Y, Shi L, Wei J H, *et al*. Progress in mobile quantum key distribution technique[J]. Laser & Optoelectronics Progress, 2017, 54(12): 120004.
朱宇, 石磊, 魏家华, 等. 移动量子密钥分发技术进展[J]. 激光与光电子学进展, 2017, 54(12): 120004.

[7] Zhu J R, Li J, Zhang C M, *et al*. Parameter optimization in biased decoy-state quantum key distribution with both source errors and statistical fluctuations[J]. Quantum Information Process, 2017, 16(10): 238.

[8] Makarov V. Controlling passively quenched single photon detectors by bright light[J]. New Journal of Physics, 2012, 11(6): 065003.

[9] 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.

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

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

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

[13] Sangouard N, Simon C, Riedmatten H D, *et al*. Quantum repeaters based on atomic ensembles and linear optics[J]. Review of Modern Physics, 2011, 83(1): 33-34.

[14] Rubenok A, Slater J A, Chan P, *et al*. A quantum key distribution system immune to detector attacks [EB/OL]. (2012-6-20) [2017-11-15]. https://arXiv.org/pdf/1204.0738v2.pdf.

[15] Liu Y, Chen T Y, Wang L J, *et al*. Experimental measurement device independent quantum key distribution[EB/OL]. (2012-9-27) [2017-11-15]. http://arXiv.org/pdf/1209.6178v1.pdf.

[16] Jasim O K, Abbas S, El-Horbaty E S M, *et al*. Quantum key distribution: Simulation and characterizations[C]. Procedia Computer Science, 2015, 65(75): 701-710.

[17] Kang D N, He Y F. Quantum key distribution protocol based on asymmetric channels of odd coherent source [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.

[18] 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.

[19] Yan L, Sun H, Zhao S M. Study on Decoyed measurement device independent quantum key distribution protocol using orbital angular momentum [J]. Journal of Signal Processing, 2014, 30(11): 1275-1278.
颜龙, 孙豪, 赵生妹. 应用诱骗态的光子轨道角动量测量设备无关量子密钥分发协议的研究[J]. 信号处理, 2014, 30(11): 1275-1278.

[20] Zhao S M, Gong L Y, Li Y Q, *et al*. A large-alphabet quantum key distribution protocol using orbital angular momentum entanglement[J]. Chinese Physics Letters, 2013, 30(6): 060305.

[21] Qiao W, Gao S C, Lei T, *et al*. Transmission of orbital angular momentum modes in grapefruit-type microstructure fiber[J]. Chinese Journal of Lasers, 2017, 44(4): 0406002.
乔文, 高社成, 雷霆, 等. 轨道角动量模式在柚子型微结构光纤中的传输[J]. 中国激光, 2017, 44(4): 0406002.

[22] Sun S H, Gao M, Dai H Y, *et al*. Decoy state quantum key distribution with odd coherent state[J]. Chinese Physics Letters, 2008, 25(7): 2358-2361.

[23] Dong C, Zhao S H, Zhang N, *et al*. Measurement-device-independent quantum key distribution with odd coherent state [J]. Acta Physica Sinica, 2014, 63(20): 200304.
东晨, 赵尚弘, 张宁, 等. 奇相干光源的测量设备无关量子密钥分配研究[J]. 物理学报, 2014, 63(20): 200304.

[24] Ekert A, Ericsson M, Hayden P, *et al*. Geometric quantum computation[J]. Journal of Modern Optics, 2000, 47(14/15): 2501-2513.

[25] Li C Z. Quantum communication and quantum computing[M]. Changsha: National University of Defense Technology Press, 2000: 255-349.
李承祖. 量子通信和量子计算[M]. 长沙: 国防科技大学出版社, 2000: 255-349.

[26] Hong C K, Ou Z Y, Mandel L. Measurement of subpicosecond time intervals between two photons by interference[J]. Physical Review Letters, 1987, 59(18): 2044.

[27] Gottesman D, Lo H K, Lutkenhaus N, *et al*. Security of quantum key distribution with imperfect devices[J]. International Symposium on Information Theory, 2002, 4(5): 325-360.

[28] Hwang W Y. Quantum key distribution with high loss: Toward global secure communication[J]. Physical Review Letters, 2003, 91(5): 057901.

[29] Ma X F, Razavi M. Alternative schemes for measurement-device-independent quantum key distribution[J]. Physical Review A, 2012, 86(6): 062319.