基于奇相干光源非对称信道的量子密钥分配协议

康丹娜，何业锋

西安邮电大学通信与信息工程学院，陕西 西安 710121

摘要 针对传统量子密钥分配协议使用非理想单光子源会带来密钥生成率过低的问题，对光源进行优化，以奇相干光源代替传统弱相干光源，提出了基于奇相干光源非对称信道的测量设备无关量子密钥分配协议。在奇相干光源下，对比了对称信道和非对称信道测量设备无关量子密钥分配协议的性能优劣。分析了该协议中密钥生成率、单边效率与信道损耗之间的关系。仿真结果表明，奇相干光源的引入弥补了传统光源的不足，多光子数大大减少。随着信道损耗的增加，密钥生成率降低，但非对称信道的性能仍高于对称信道的。

关键词 量子光学；奇相干光源；量子密钥分配；测量设备无关

中图分类号 TN918 **文献标识码** A

doi：10.3788/AOS201737.0627001

Quantum Key Distribution Protocols Based on Asymmetric Channels of Odd Coherent Sources

Kang Danna, He Yefeng

School of Communication and Information Engineering, Xi'an University of Posts and Telecommunications, Xi'an, Shaanxi 710121, *China*

Abstract In order to solve the problem that the key generation rate is too low when the non-ideal single photon source is used in the traditional quantum key distribution protocol, the light source is optimized, an odd coherent light source is used to replace the traditional weak coherent light source, and a measurement-device-independent quantum key distribution protocol based on the asymmetric channels of odd coherent sources is proposed. The performances of measurement-device-independent quantum key distribution protocols for symmetric and asymmetric channels with the odd coherent light source are compared. The relationship between the channel loss and the key generation rate and single-side efficiency in the proposed protocol is analyzed. The simulation results show that the introduction of the odd coherent light source makes up the deficiency of the traditional light source and also reduces the number of photons greatly. With the increase of the channel loss, the key generation rate decreases, but the performance of the asymmetric channel is still higher than that of the symmetric channel.

Key words quantum optics; odd coherent light source; quantum key distribution; measurement-device-independent

OCIS codes 270.3430; 270.1670; 270.5568; 270.5565

1 引 言

随着计算能力的飞速发展，传统密码学面临巨大的挑战，而量子密码学具有无条件安全性，近年来成为研究热点。针对量子力学的多个原理，学者们分别从纠缠制备[1-2]、量子计算[3]、量子态分配[4]、量子隐形传态[5]等方面进行了不同研究。1984 年，Bennett 等[6]提出了第一个量子密钥分配(QKD)协议，即 BB84 协议[7]，能实现无条件安全。随后，大量量子密钥协议被提出[8-10]。然而，量子密码协议只是理论上的无条件安全，在协议实现中，所使用设备的各种不完美特性导致系统存在安全漏洞，例如：对于非理想光源可利用相位部分随机化攻击[11]、光子数分流攻击[12]；对于非理想探测器可利用时移攻击[13]、致盲攻击[14]、伪态攻击[15]等。为了克服实际中存在的诸多问题，2012 年，Lo 等[16]提出了测量备无关的量子密钥分配

收稿日期：2016-11-25；**收到修改稿日期**：2017-01-19

基金项目：国家自然科学基金(61472472)

作者简介：康丹娜(1993—)，女，硕士研究生，主要从事量子密钥分配方面的研究。E-mail：katherine_luck@sina.com

导师简介：何业锋(1978—)，女，博士，副教授，主要从事网络安全和量子密码方面的研究。E-mail：yefenghe1978@163.com

(MDI-QKD)协议,该方案利用时间反演的纠缠分发协议,将探测器放在不可信第三方,可移除量子密钥分配系统中所有探测器的侧信道攻击。在这之后,不断有学者对其进行优化设计。唐延林通过使用高效的单光子探测器与较稳定的系统得到了超过 200 km 的安全传输距离,并在实验中得到真空态和诱惑态结合方案下的密钥生成率与损耗的关系。孙颖对基于量子存储的量子密钥分配协议进行分析,得到了密钥生成率、信道传输效率与安全传输距离等参数之间的关系。孙世海利用一个信号态与两个诱惑态构造测量设备无关的量子密钥分配协议,且得出了误码率的上限以及密钥生成率的下限。刘杨研究了基于偏振编码的测量设备无关量子密钥分配协议,得出了每个脉冲中平均光子数为定值时的误码率。这些协议大部分要求光源为单光子源,但实际设备难以实现。杜亚男利用弱相干态(WCS)光源代替,较好地模拟了单光子光源的性质,但存在的问题是窃听者会利用其中的多光子来拷贝信息以窃取密钥。同时,以往的研究中假设 Alice 和 Bob 到第三方的距离相同[17],但实际的单边效率往往是不同的。

本文针对现实中常使用的非对称信道的情况,提出奇相干光源(OCS)非对称信道的测量设备无关量子密钥分配协议,通过分析密钥生成率与信道损耗的关系,研究了不同信道下信道损耗对密钥生成率的影响,对比了奇相干光源和弱相干光源的单光子分布情况。

2　理论与模型

2.1　测量设备无关量子密钥分配系统模型

测量设备无关量子密钥分配系统模型[18]如图 1 所示。

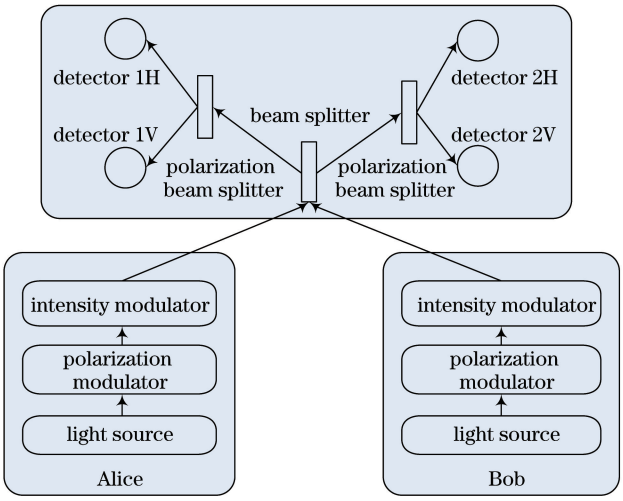

图 1　测量设备无关量子密钥分配系统结构图

Fig. 1　Structural diagram of measurement-device-independent quantum key distribution system

Alice 和 Bob 分别发送相干光脉冲经过偏振调制器,选择 z 基或 x 基进行偏振编码,经强度调制器调制为三强度态 μ_i,ν_j:

$$\begin{cases}\{\mu_i\},\ i=0,1,2\\ \{\nu_j\},\ j=0,1,2\end{cases},\tag{1}$$

式中 0,1,2 分别对应真空态、诱惑态和信号态。在第三方进行贝尔态测量(BSM),主要的测量仪器由一个分束器(BS)、两个偏振分束器(PBS)和 4 个探测器构成。Alice 和 Bob 根据公布的的结果进行基对比,可以得出安全密钥生成率 R 的公式[19]:

$$R\geqslant\mu_2\nu_2\exp(-\mu_2-\nu_2)\hat{Y}^z_{11}\left|1-H(\hat{e}^x_{11})\right|-Q^z_{\mu_2\nu_2}fH(E^z_{\mu_2\nu_2}),\tag{2}$$

式中 Alice 和 Bob 发送的相干光源服从泊松分布,$H(x)$为二进制香农熵函数,f 为纠错过程的低效率函数,Q 为增益,E 为误码率,$\hat{Y}^z_{11}$为单光子计数率的下界,$\hat{e}^x_{11}$为单光子误码率的上界。当 Alice 的脉冲强度为 μ_i,Bob 的脉冲强度为 ν_j 时,定义增益 $Q_{\mu_i\nu_j}$ 与误码率 $E_{\mu_i\nu_j}$:

$$Q^w_{\mu_i\nu_j}=\sum_{n,m=0}^{\infty}\frac{\mu_i^n\nu_j^m}{n!m!}\exp(-\mu_i-\nu_j)Y^w_{nm},\tag{3}$$

$$E^{w}_{\mu_i\nu_j}Q^{w}_{\mu_i\nu_j}=\sum_{n,m=0}^{\infty}\frac{\mu_i^n\nu_j^m}{n!m!}\exp(-\mu_i-\nu_j)Y^{w}_{nm}e^{w}_{nm},\tag{4}$$

式中 m 和 n 分别为 Alice 和 Bob 发送的光子数；$w=x,z$ 分别代表 x 基和 z 基，x 基作为测试集用来估计信道参数，z 基用来产生安全密钥；Y^{w}_{nm} 表示在相应基下的光子计数率；e^{w}_{nm} 表示在相应基下的光子误码率。在(2)式中，可以通过实验测出 $Q^{z}_{\mu\nu}$ 和 $E^{z}_{\mu\nu}$，因此只需要通过奇相干光源代替弱相干脉冲估计单光子计数率 Y^{z}_{11} 的下界 $\hat{Y}^{z}_{11}$ 以及单光子误码率 e^{x}_{11} 的上界 $\hat{e}^{x}_{11}$，从而得到密钥生成率 R。

2.2　奇相干态

奇相干光源即为只含有奇数个光子脉冲的相干光态，奇相干光源由相位相反的相干态 $|\alpha\rangle$ 和 $|-\alpha\rangle$ 构成：

$$|\alpha\rangle_{\mathrm{OCS}}=N(|\alpha\rangle-|-\alpha\rangle),\tag{5}$$

实验中可利用线性光学器件产生奇相干态[20-21]：

$$U|0\rangle=\exp\left[\frac{1}{2}(\zeta^{*}a^{2}-\zeta a^{+2})\right]|0\rangle\xrightarrow{\mathrm{BS}}|\alpha\rangle_{\mathrm{OCS}},\tag{6}$$

式中 U 为幺正压缩算符，ζ 为抽运场的幅度值，BS 表示分束器，可产生如下奇相干态[21]

$$|\alpha\rangle_{\mathrm{OCS}}=\frac{1}{\sin|\alpha|^{2}}\sum_{n=0}^{\infty}\frac{\alpha^{2n+1}}{\sqrt{(2n+1)!}}|2n+1\rangle,\tag{7}$$

得出奇相干光源的光子数分布[22]为

$$P(2n+1)=\frac{|\alpha|^{2(2n+1)}}{\sinh|\alpha|^{2}\cdot(2n+1)!}。\tag{8}$$

在相同光强下，奇相干光源与弱相干光源中单光子和多光子的分布特征如表 1 所示[22]。从表中可以看出，奇相干光脉冲的性能要优于弱相干光脉冲的。

表 1　奇相干光源与弱相干光源的光子分布

Table 1　Photon distributions of odd coherent light source and weak coherent light source

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

2.3　密钥生成率

由(3)式和(4)式可以推出单光子计数率的下界 $\hat{Y}^{w}_{11}$：

$$\hat{Y}^{w}_{11}\geqslant\frac{g^{w}_{1}+g^{w}_{2}+g^{w}_{3}-\exp(\mu_2+\nu_2)Q^{w}_{\mu_2\nu_2}+\exp(\mu_1+\nu_1)Q^{w}_{\mu_1\nu_1}}{\mu_1\nu_1-\mu_2\nu_2+\lambda\mu_2\nu_1+\lambda\mu_1\nu_2},\tag{9}$$

式中[23]

$$\begin{cases}g^{w}_{1}=Q^{w}_{0\nu_2}\exp\nu_2+Q^{w}_{\mu_2 0}\exp\mu_2-Q^{w}_{0\nu_1}\exp\nu_1-Q^{w}_{\mu_2 0}\exp\mu_1\\ g^{w}_{2}=\lambda[Q^{w}_{\mu_2\nu_1}\exp(\mu_2+\nu_1)-Q^{w}_{0\nu_1}\exp\nu_1-Q^{w}_{\mu_2 0}\exp\mu_2+Q^{w}_{00}]\\ g^{w}_{3}=\lambda[Q^{w}_{\mu_1\nu_2}\exp(\mu_1+\nu_2)-Q^{w}_{0\nu_2}\exp\nu_2-Q^{w}_{\mu_1 0}\exp\mu_1+Q^{w}_{00}]。\\ \lambda=\min\left(\dfrac{\mu_2\nu_2^{2}-\mu_1\nu_1^{2}}{\mu_2\nu_1^{2}+\mu_1\nu_2^{2}},\dfrac{\mu_2^{2}\nu_2-\mu_1^{2}\nu_1}{\mu_2^{2}\nu_1+\mu_1^{2}\nu_2},\dfrac{\mu_2^{2}\nu_2^{2}-\mu_1^{2}\nu_1^{2}}{\mu_2^{2}\nu_1^{2}+\mu_1^{2}\nu_2^{2}}\right)\end{cases}\tag{10}$$

由(4)式可得出单光子误码率的上限 $\hat{e}^{w}_{11}$

$$\hat{e}^{w}_{11}\leqslant\frac{\exp(\mu_1+\nu_1)Q^{w}_{\mu_1\nu_1}E^{w}_{\mu_1\nu_1}-g^{w}_{4}}{\mu_1\nu_1\hat{Y}^{w}_{11}},\tag{11}$$

式中

$$g^{w}_{4}=Q^{w}_{0\nu_1}E^{w}_{0\nu_1}\exp\nu_1+Q^{w}_{\mu_1 0}E^{w}_{\mu_1 0}\exp\mu_1-Q^{w}_{00}E^{w}_{00}。\tag{12}$$

通过估算 x 基与 z 基情况下的增益和误码率，可得到(2)式中密钥生成率下限，根据参考文献[24]可得该增益与误码率。

x 基条件下：

$$\begin{cases} Q^{x}_{\mu_i\nu_j} = 2y^{2}_{ij}[1+2y^{2}_{ij}-4y_{ij}\mathrm{I}_0(s_{ij})+\mathrm{I}_0(2s_{ij})] \\ E^{x}_{\mu_i\nu_j}Q^{x}_{\mu_i\nu_j} = e_0 Q^{x}_{\mu_i\nu_j} - 2(e_0-e_\mathrm{d})y^{2}_{ij}\times[\mathrm{I}_0(2s_{ij})-1] \end{cases}, \tag{13}$$

式中 $\mathrm{I}_0(s)\approx 1+\frac{s^2}{4}$ 为第一类修正贝塞尔函数，e_0 为偏正系数，e_d 为修正系数。

z 基条件下：

$$\begin{cases} Q^{z}_{\mu_i\nu_j} = Q_{Cij}+Q_{Eij} \\ E^{z}_{\mu_i\nu_j}Q^{z}_{\mu_i\nu_j} = e_\mathrm{d}Q_{Cij}+(1\text{-}e_\mathrm{d})Q_{Eij} \end{cases}, \tag{14}$$

式中

$$\begin{cases} Q_{Cij} = 2(1-P_\mathrm{d})^2\exp\left(\frac{-\mu'_{ij}}{2}\right)\times\left[1-(1-P_\mathrm{d})\exp\left(\frac{-\eta'_\mathrm{a}\mu'_i}{2}\right)\right]\times\left[1-(1-P_\mathrm{d})\exp\left(\frac{-\eta_\mathrm{b}\mu'_j}{2}\right)\right] \\ Q_{Eij} = 2P_\mathrm{d}(1-P_\mathrm{d})^2\exp\left(\frac{-\mu'_{ij}}{2}\right)\times\left[\mathrm{I}_0(2s_{ij})-(1-P_\mathrm{d})\exp\left(\frac{-\mu'_{ij}}{2}\right)\right] \end{cases}, \tag{15}$$

式中 P_d 为探测器成功的概率，η_a 与 η_b 分别为 Alice 和 Bob 的单边探测效率，e_d 为修正系数，其余参数分别为

$$\begin{cases} \mu'_{ij} = \eta_\mathrm{a}\mu_i+\eta_\mathrm{b}\nu_j \\ s_{ij} = \frac{\sqrt{\eta_\mathrm{a}\mu_i\eta_\mathrm{b}\nu_j}}{2} \\ y_{ij} = (1-P_\mathrm{d})\exp\left(\frac{\mu'_{ij}}{4}\right) \end{cases}。 \tag{16}$$

当 Alice 和 Bob 所使用的信道是对称的，即 $L_\mathrm{AC}=L_\mathrm{BC}=l$ 时，全局传输效率 η 为传递效率 t 和探测效率 η_D 的乘积[25]：

$$\begin{cases} t = 10^{-\alpha l/10} \\ \eta = \eta_\mathrm{a}=\eta_\mathrm{b}=t\eta_\mathrm{D} \end{cases}, \tag{17}$$

式中 η_a 和 η_b 为单边效率。

当其信道为非对称的，即 $L_\mathrm{AC}\neq L_\mathrm{BC}$ 时，设距离比 $\sigma=L_\mathrm{AC}/L_\mathrm{BC}$，则由(17)式可得非对称信道的单边效率分别为

$$\begin{cases} \eta_\mathrm{a} = \eta^{2\sigma/(\sigma+1)} \\ \eta_\mathrm{b} = \eta^{2/(\sigma+1)} \end{cases}。 \tag{18}$$

在(18)式中，当距离比 $\sigma=1.0$ 时，$\eta_\mathrm{a}=\eta_\mathrm{b}$ 即为对称信道；当距离比 $\sigma\in(0,1)$ 时为非对称信道。因此，平均光子数 μ'_{ij} 可以表示为

$$\mu'_{ij} = \eta^{2\sigma/(\sigma+1)}\mu_i+\eta^{2/(\sigma+1)}\nu_j。 \tag{19}$$

通过改变第三方的位置可以改变相应的单边效率，进而改变最终的密钥生成率。

3　仿真结果分析

由于使用奇相干光源代替了一般的弱相干光源，光源处的多光子脉冲明显减少，有效减小了误码率。将(17)式代入(19)式可以得到非对称信道 MDI-QKD 的信道损耗与平均光子数之间的关系，也可同时分别得到 Alice 与 Bob 端到第三方的单边效率，然后通过(9)式与(11)式得到单光子计数率下界和单光子误码率上界的近似值。最后由(2)式估算出密钥生成率与信道损耗之间的关系。在整个推导过程中，所使用的参数如表 2 所示。

表 2　主要参数值

Table 2　Main parameter value

Signal state	Decoy state	e_d /(%)	P_d	Value of f
0.36	0.01	1.5	3×10^{-6}	1.16

图 2 为平均光子数与信道损耗之间的关系曲线，从图中可以看出，无论是对称信道还是非对称信道，随着信道损耗的增加，平均光子数逐渐减少直至趋于稳定，但是曲线 $\sigma=1.0$ 的值始终小于曲线 $\sigma=0.1$ 的值，即对称信道的平均光子数始终少于非对称信道的平均光子数，且下降速度比后者快。当信道损耗为 0 时，即理想非对称信道条件下，曲线 $\sigma=0.1$ 的平均光子数趋于 1.08，与理想单光子源的平均光子数差值较小，这表示在平均光子数上，非对称信道的性能较好。

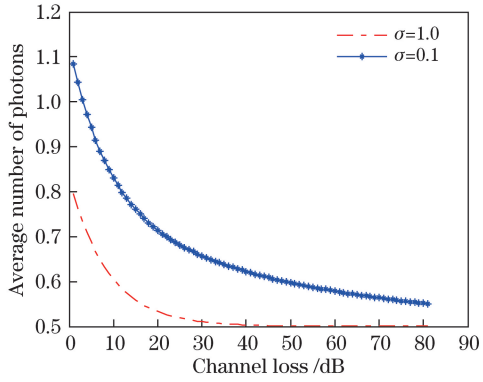

图 2　平均光子数与信道损耗之间的关系

Fig. 2　Relationship between average number of photons and channel loss

图 3 为单边效率与传输损耗之间的关系曲线，从中可以看出，随着信道损耗的增加，三条曲线均呈现下降趋势。并且，对称信道的 $\sigma=1.0$ 曲线居中。当为非对称信道时，Alice 的单边效率高于 Bob 的单边效率，即通信双方中距离第三方较近的那一方的单边效率较高。

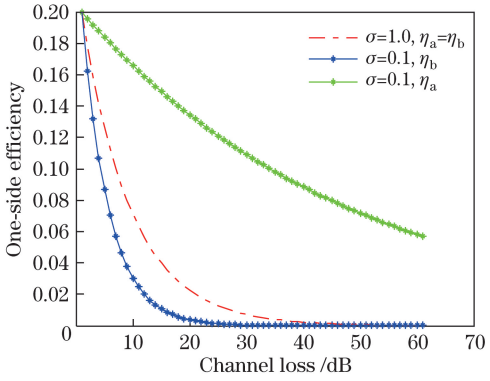

图 3　单边效率与传输损耗之间的关系

Fig. 3　Relationship between single-side efficiency and transmission loss

密钥生成率与传输损耗之间的关系曲线如图 4 所示，从中可以看出，随着信道损耗的增加，非对称信道与对称信道的密钥生成率都逐渐下降，虽然起点相同，但是 $\sigma\in(0,1)$ 所表示的非对称信道的密钥生成率 R 的值始终大于 $\sigma=1.0$ 所表示的对称信道的密钥生成率，且当 $\sigma=0.1$ 时，信道的性能最好。

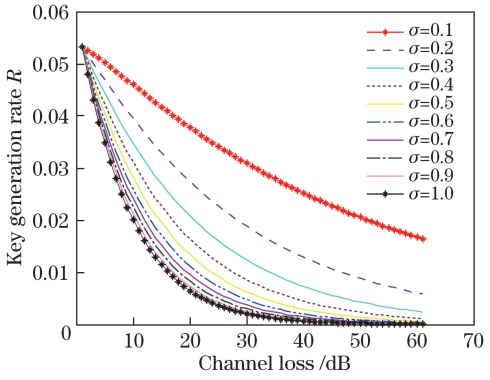

图 4　密钥生成率与传输损耗之间的关系

Fig. 4　Relationship between key generation rate and transmission loss

综上所述，随着距离比 σ 的降低，在第三方进行贝尔态测量的光脉冲的平均光子数 μ'_{ij} 变大，这相当于在传统密钥分发协议中，增大光强时脉冲中单光子和多光子的数量比值降低，进而降低了安全密钥的生成率（图 2）。由于是非对称信道，当第三方不断靠近 Alice 时，Alice 的单边效率不断增大，而 Bob 端的单边效率不断减小，持续增大的不匹配度使得误码率也不断增加（图 3）。随着信道损耗的增加，密钥生成率不断降低，但非对称信道对于噪声的容忍度仍比对称信道高 20 dB（图 4）。

4 结　论

在基于奇相干光源的非对称信道中，研究了测量设备无关量子密钥分配协议的密钥生成率与距离比之间的关系。在三强度诱骗态条件下，对比对称信道与非对称信道不同距离比下的平均光子数、单边效率和密钥生成率与信道损耗的关系。从仿真结果可以看出，随着 Alice 和 Bob 对应信道不匹配程度的增加，密钥生成率下降较快。在奇相干光源降低了光源处的多光子数后，非对称信道的性能整体要优于对称信道的。因此，在实际实验中，可采用奇相干光源代替一般弱相干光源的方式，从而降低光脉冲中的多光子数量比率以得到更好的效果。

参　考　文　献

[1] Huang B H, Chen Y H, Wu Q C, *et al*. Fast generating Greenberger-Horne-Zeilinger state via iterative interaction pictures[J]. Laser Physics Letters, 2016, 13(10): 105202.

[2] Chen Y H, Huang B H, Song J, *et al*. Transitionless-based shortcuts for the fast and robust generation of W states[J]. Optics Communications, 2016, 380: 140-147.

[3] Chen Y H, Xia Y, Chen Q Q, *et al*. Fast and noise-resistant implementation of quantum phase gates and creation of quantum entangled states[J]. Physical Review A, 2014, 91(1): 012325.

[4] Lu P M, Xia Y, Song J. Efficient W polarization state distribution over an arbitrary collective-noise channel with cross-Kerr nonlinearity[J]. Optics Communications, 2011, 284(24): 5866-5870.

[5] Wang Zhongjie, Ruan Fei, Fang Xu. Teleportation for atomic state based on disentanglement-free state[J]. Acta Optica Sinica, 2015, 35(3): 0327001.
王中结，阮　飞，方　旭. 基于免退纠缠态的原子态隐形传输[J]. 光学学报, 2015, 35(3): 0327001.

[6] 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.

[7] Bennett C H, Brassard G. An update on quantum cryptography[C]. Advances in Cryptology, Proceedings of CRYPTO, 1984: 475-480.

[8] Liu Youming, Wang Chao, Huang Duan, *et al*. Study of synchronous technology in high-speed continuous variable quantum key distribution system[J]. Acta Optica Sinica, 2015, 35(1): 0106006.
刘友明，汪　超，黄　端，等. 高速连续变量量子密钥分发系统同步技术研究[J]. 光学学报, 2015, 35(1): 0106006.

[9] Peres A. Quantum cryptography with orthogonal states[J]. Physical Review Letters, 1996, 77(15): 3264-3264.

[10] Bennett C H. Quantum cryptography using any two nonorthogonal states[J]. Physical Review Letters, 1992, 68(68): 3121-3124.

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

[12] 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: 042333.

[13] Lydersen L, Skaar J, Makarov V. Tailored bright illumination attack on distributed-phase-reference protocols[J]. Journal of Modern Optics, 2010, 58(8): 680-685.

[14] Makarov V, Skaar J. Faked states attack using detector efficiency mismatch on SARG04, phase-time, DPSK, and Ekert protocols[J]. Quantum Information & Computation, 2007, 8(6): 622-635.

[15] Makarov V, Hjelme D R. Faked states attack on quantum cryptosystems[J]. Journal of Modern Optics, 2005, 52(5): 691-705.

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

[17] Wu Chengfeng, Du Yanan, Wang Jindong, *et al*. Analysis on performance optimization in measurement-device-independent quantum key distribution using weak coherent states[J]. Acta Physica Sinica, 2016, 65(10): 100302.
吴承峰, 杜亚男, 王金东, 等. 弱相干光源测量设备无关量子密钥分发系统的性能优化分析[J]. 物理学报, 2016, 65(10): 100302.

[18] Yan Long, Sun Hao, Zhao Shengmei. Study on decoyed measurement device independent quantum key distribution protocol using orbital angular momentum[J]. Journal of Signal Processing, 2014, 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, 11: 1275-1278.

[19] Braunstein S L, Pirandola S. Side-channel-free quantum key distribution[J]. Physical Review Letters, 2012, 108(13): 130502.

[20] Sasaki M, Suzuki S. Multimode theory of measurement-induced non-Gaussian operation on wideband squeezed light: Analytical formula[J]. Physical Review A, 2006, 73(4): 043807.

[21] Wenger J, Brouri R T, Grangier P. Non-Gaussian statistics from individual pulses of squeezed light[J]. Physical Review Letters, 2004, 92: 153601.

[22] Dong Chen, Zhao Shanghong, Zhang Ning, *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.

[23] 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): 052329.

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

[25] Dong Chen, Zhao Shanghong, Zhao Weihu, *et al*. Analysis of measurement-device-independent quantum key distribution under asymmetric channel transmittance efficiency[J]. Acta Physica Sinica, 2014, 63(3): 030302.
东　晨,赵尚弘, 赵卫虎, 等. 非对称信道传输效率的测量设备无关量子密钥分配研究[J]. 物理学报, 2014, 63(3): 030302.