非对称信道传输效率的测量设备无关量子密钥分配研究*

东晨[1)2)†] 赵尚弘[1)] 赵卫虎[1)] 石磊[1)] 赵顾颢[1)]

1) (空军工程大学信息与导航学院, 西安 710077)

2) (西安通信学院信息安全系, 西安 710006)

(2013 年 10 月 2 日收到; 2013 年 11 月 3 日收到修改稿)

测量设备无关量子密钥分配方案可以移除所有的探测器侧信道漏洞, 通过结合诱骗态方案可以生成无条件安全的密钥. 本文研究了非对称信道传输效率下三强度诱骗态测量设备无关量子密钥分配系统的密钥生成率与信道传输损耗的关系, 比较了对称信道传输效率和非对称信道传输效率下的距离比率对单边传输效率、单光子误码率和量子密钥生成率的影响, 仿真结果表明随着信道不匹配度逐渐增加, 可容忍信道传输损耗由对称信道情形下的62 dB分别降至38 dB(距离比率为0.5)和17 dB(距离比率为0.1), 能够安全提取密钥的可容忍传输损耗下降较快, 密钥生成率的安全传输距离也随之降低. 实验中可以采取调节信号光强度的方式提高非对称传输效率下测量设备无关量子密钥分配系统的密钥生成率, 为实用的量子密钥分配实验提供了重要的理论参数.

关键词: 诱骗态, 测量设备无关量子密钥分配, 非对称信道传输效率

PACS: 03.67.Dd **DOI:** 10.7498/aps.63.030302

1 引 言

量子密钥分配[1](quantum key distribution, QKD)是量子信息科学的重要分支, 以其建立在量子力学和信息论框架下的无条件安全性特点[2−4], 近年来已成为国内外的研究热点[5−10]. 然而在建立实际的量子密钥分配系统时, 由于所采用的光学和电学设备存在各种非完美性, 使得系统存在安全漏洞: 如针对光源非完美性提出的光子数分流攻击[11]、相位部分随机化攻击[12]等; 针对探测器非完美性提出的伪态攻击[13]、时移攻击[14]、致盲攻击[15]等. 为了克服上述光源和探测设备的非完美性问题, 人们提出了设备无关量子密钥分配方案[16](device independent QKD, DI QKD), 该方案不需要刻画光源和探测设备的具体模型, 只需通过验证Bell不等式来判断窃听者的存在, 确保密钥的无条件安全, 但是该方案要求Bell不等式判断时的单光子探测器效率接近100%[17], 目前的实验技术很难实现. 最近Lo等[18]提出了测量设备无关量子密钥分配方案(measurement device independent QKD, MDI-QKD). 在该方案中, Alice和Bob不在进行Bell不等式的验证, 而是将光脉冲发送至非可信任的第三方进行Bell态测量, 进一步提取无条件安全的密钥, 由于该方案的测量过程在第三方进行, 故其可以移除所有的探测器侧信道漏洞. 在实际的MDI-QKD系统中, Alice和Bob通常使用相干光源代替单光子光源, 故在MDI-QKD实现中可结合诱骗态方案[19]有效的估计密钥生成率. 在理论方面, Ma[20]、王向斌[21]、孙仕海[22]等分析了MDI-QKD的统计波动问题, 在实验方面, Liu[23]、Tang[24]等分别实现了相位编码和偏振编码的MDI-QKD.

* 国家自然科学基金 (批准号: 61106068) 资助的课题.

† 通讯作者. E-mail: dongchengfkd@163.com

在上述的理论分析与实验中, 均假设 Alice 和 Bob 到第三方的信道传输距离相同, 即单边信道传输效率相同, 事实上在实际的量子密钥分配系统中存在信道传输效率不对称的情形[25,26]. 本文研究了非对称信道传输效率下, 三强度诱骗态 MDI-QKD 系统密钥生成率与信道传输损耗的关系, 比较了对称信道传输效率和非对称信道传输效率下距离比率对单光子误码率及量子密钥生成率的影响.

2 理论与模型

测量设备无关量子密钥分配系统模型如图 1 所示.

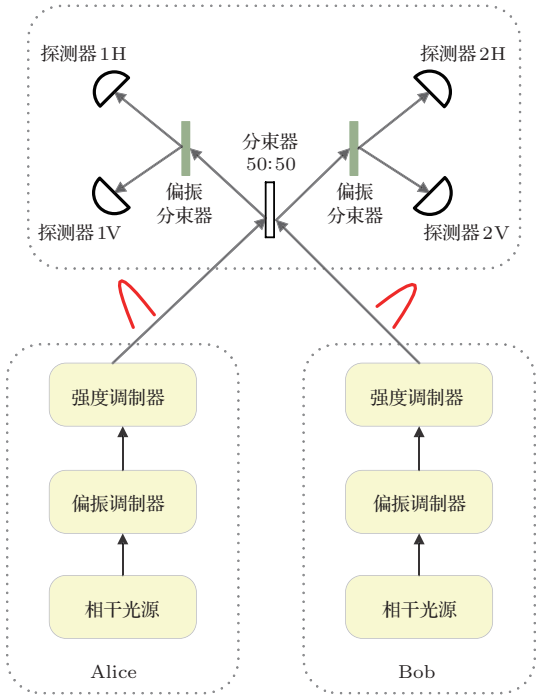

图 1 测量设备无关量子密钥分配系统结构[18]

Alice 和 Bob 发送的相干光脉冲先经过偏振调制器进行偏振编码 (选取 x 基 z 基), 再经过强度调制器调制为 3 强度 μ_i, v_j:

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

分别对应真空态、诱骗态和信号态, 第三方通过分束器、偏振分束器和探测器对接收到的相干光脉冲进行 Bell 态测量并公布测量结果, Alice 和 Bob 根据基比对过程提取出安全密钥生成率的公式[18]:

$$R \geqslant \mu_2\nu_2\,\mathrm{e}^{-\mu_2-\nu_2}\,\overset{\vee}{Y}{}^{z}_{11}\left[1-H\left(\hat{e}{}^{x}_{11}\right)\right] - Q^{z}_{\mu_2\nu_2} f H\left(E^{z}_{\mu_2\nu_2}\right), \tag{2}$$

式中 $w=x,z$ 分别代表 x 基和 z 基, 其中 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. Alice 和 Bob 发送的相干态均服从泊松分布, 定义 Alice 脉冲强度为 μ_i 且 Bob 脉冲强度为 v_j 时的增益 $Q_{\mu_i v_j}$ 和误码率 $E_{\mu_i v_j}$:

$$Q^{w}_{\mu_i\nu_j} = \sum_{n,m=0}^{\infty} \frac{\mu_i^n \nu_j^m}{n!m!}\,\mathrm{e}^{-\mu_i-\nu_j} Y^{w}_{nm}, \tag{3a}$$

$$E^{w}_{\mu_i\nu_j} Q^{w}_{\mu_i\nu_j} = \sum_{n,m=0}^{\infty} \frac{\mu_i^n \nu_j^m}{n!m!}\,\mathrm{e}^{-\mu_i-\nu_j} Y^{w}_{nm} e^{w}_{nm}, \tag{3b}$$

利用文献 [22] 中的不等式估计可以推出

$$\begin{aligned} &\mathrm{e}^{\mu_2+\nu_2} Q^{w}_{\mu_2\nu_2} - \mathrm{e}^{\mu_1+\nu_1} Q^{w}_{\mu_1\nu_1} \\ &\geqslant g^{w}_{1} + g^{w}_{2} + g^{w}_{3} - (\mu_1\nu_1 - \mu_2\nu_2 \\ &\quad + \kappa\mu_2\nu_1 + \kappa\mu_1\nu_2) Y^{w}_{11}, \end{aligned} \tag{4}$$

进一步推出单光子增益的下界 $\overset{\vee}{Y}{}^{w}_{11}$:

$$\begin{aligned} &Y^{w}_{11} \geqslant \overset{\vee}{Y}{}^{w}_{11} \\ &\equiv \frac{g^{w}_{1} + g^{w}_{2} + g^{w}_{3} - \mathrm{e}^{\mu_2+\nu_2} Q^{w}_{\mu_2\nu_2} + \mathrm{e}^{\mu_1+\nu_1} Q^{w}_{\mu_1\nu_1}}{\mu_1\nu_1 - \mu_2\nu_2 + \kappa\mu_2\nu_1 + \kappa\mu_1\nu_2}, \end{aligned} \tag{5}$$

式中

$$g^{w}_{1} = \mathrm{e}^{\nu_2} Q^{w}_{0\nu_2} + \mathrm{e}^{\mu_2} Q^{w}_{\mu_2 0} - \mathrm{e}^{\nu_1} Q^{w}_{0\nu_1} - \mathrm{e}^{\mu_1} Q^{w}_{\mu_2 0}, \tag{6a}$$

$$g^{w}_{2} = \kappa\left(\mathrm{e}^{\mu_2+\nu_1} Q^{w}_{\mu_2\nu_1} - \mathrm{e}^{\nu_1} Q^{w}_{0\nu_1} - \mathrm{e}^{\mu_2} Q^{w}_{\mu_2 0} + Q^{w}_{00}\right), \tag{6b}$$

$$g^{w}_{3} = \kappa\left(\mathrm{e}^{\mu_1+\nu_2} Q^{w}_{\mu_1\nu_2} - \mathrm{e}^{\nu_2} Q^{w}_{0\nu_2} - \mathrm{e}^{\mu_1} Q^{w}_{\mu_1 0} + Q^{w}_{00}\right), \tag{6c}$$

$$\kappa = \min\left(\frac{\mu_2\nu_2^2 - \mu_1\nu_1^2}{\mu_2\nu_1^2 + \mu_1\nu_2^2}, \frac{\mu_2^2\nu_2 - \mu_1^2\nu_1}{\mu_2^2\nu_1 + \mu_1^2\nu_2}, \frac{\mu_2^2\nu_2^2 - \mu_1^2\nu_1^2}{\mu_2^2\nu_1^2 + \mu_1^2\nu_2^2}\right), \tag{6d}$$

由 (3b) 式可以推出单光子误码率的上界 $\hat{e}{}^{w}_{11}$:

$$e^{w}_{11} \leqslant \hat{e}{}^{w}_{11} \equiv \frac{\mathrm{e}^{\mu_1+\nu_1} Q^{w}_{\mu_1\nu_1} E^{w}_{\mu_1\nu_1} - g^{w}_{4}}{\mu_1\nu_1\,\overset{\vee}{Y}{}^{w}_{11}}, \tag{7}$$

式中

$$g_4^w = \mathrm{e}^{\nu_1} Q_{0\nu_1}^w E_{0\nu_1}^w + \mathrm{e}^{\mu_1} Q_{\mu_1 0}^w E_{\mu_1 0}^w - Q_{00}^w E_{00}^w. \tag{8}$$

为了提取出(2)式中密钥生成率的下限, 我们还需要估计出x基和z基下的增益与QBER, 利用文献[27]的实验结果可以推出x基和z基下的增益与QBER分别为

$$Q_{\mu_i\nu_j}^x = 2y_{ij}^2\left[1 + 2y_{ij}^2 - 4y_{ij} I_0(s_{ij}) + I_0(2s_{ij})\right], \tag{9a}$$

$$E_{\mu_i\nu_j}^x Q_{\mu_i\nu_j}^x = e_0 Q_{\mu_i\nu_j}^x - 2(e_0 - e_d) y_{ij}^2 \times \left[I_0(2s_{ij}) - 1\right], \tag{9b}$$

式中$I_0(s)$表示第一类修正贝塞尔函数.

$$Q_{\mu_i\nu_j}^z = Q_{Cij} + Q_{Eij}, \tag{10a}$$

$$E_{\mu_i\nu_j}^z Q_{\mu_i\nu_j}^z = e_d Q_{Cij} + (1 - e_d) Q_{Eij}, \tag{10b}$$

其中

$$Q_{Cij} = 2(1-P_d)^2 \mathrm{e}^{-\mu'_{ij}/2} \times \left[1 - (1-P_d)\mathrm{e}^{-\eta_a\mu_i/2}\right] \times \left[1 - (1-P_d)\mathrm{e}^{-\eta_b\nu_j/2}\right], \tag{11a}$$

$$Q_{Eij} = 2P_d(1-P_d)^2 \mathrm{e}^{-\mu'_{ij}/2} \times \left[I_0(2s_{ij}) - (1-P_d)\mathrm{e}^{-\mu'_{ij}}/2\right], \tag{11b}$$

式中参数分别为

$$\mu'_{ij} = \eta_a\mu_i + \eta_b\nu_j, \tag{12a}$$

$$s_{ij} = \sqrt{\eta_a\mu_i\eta_b\nu_j}/2, \tag{12b}$$

$$y_{ij} = (1-P_d)\mathrm{e}^{\mu_{ij}/4}. \tag{12c}$$

对于对称信道($L_{\mathrm{AC}} = L_{\mathrm{BC}}$), 全局传输效率为信道传输效率$t$与探测效率$\eta_{\mathrm{D}}$的乘积:

$$t = 10^{-\alpha l/10}, \quad \eta = \eta_a = \eta_b = t\eta_{\mathrm{D}}, \tag{13}$$

代入(2)式可以得到最终的密钥生成率. 对于非对称信道传输效率($L_{\mathrm{AC}} \neq L_{\mathrm{BC}}$), 分别考虑单边信道传输效率为

$$t_{\mathrm{AC}} = 10^{-\alpha L_{\mathrm{AC}}/10}, \quad t_{\mathrm{BC}} = 10^{-\alpha L_{\mathrm{BC}}/10}, \tag{14}$$

令$\sigma = L_{\mathrm{AC}}/L_{\mathrm{BC}}$为Alice与Bob到第三方的距离比率, 由Alice与Bob信源的对称性, 不妨假设$0 \leqslant \sigma \leqslant 1$, 即第三方的位置偏向Bob一方, 当$\sigma = 0$时, 测量发生在Bob处, MDI-QKD退化为传统的准备-测量协议, 当$\sigma = 1$时, 非对称信道MDI-QKD退化为对称信道MDI-QKD.

考虑非对称信道MDI-QKD的单边传输效率, 由(13), (14)式可以得到

$$\eta_a = \eta^{(2\sigma/\sigma+1)}, \quad \eta_b = \eta^{(2/\sigma+1)}, \tag{15}$$

此时(12b)式中s_{ij}不变, 而平均光强μ'_{ij}变为

$$\mu'_{ij} = \eta^{(2\sigma/\sigma+1)}\mu_i + \eta^{(2/\sigma+1)}\nu_j, \tag{16}$$

即第三方位置的改变通过影响单边传输效率, 改变脉冲到达第三方的平均光子数, 从而对单光子误码率及密钥生成率产生影响.

3 仿真结果与分析

根据(16)式代入(9), (10)式分别得到非对称MDI-QKD的x基和z基下的增益和QBER, 然后利用(5), (7)式估计出单光子计数率的下限和单光子误码率的上限, 最后通过(2)式可以得到最终的安全密钥生成率与信道传输损耗之间的关系. 在计算过程中, 诱骗态和信号态的光强分别取为0.01和0.36, 其余参数如表1所示.

表1 主要仿真参数设置

文献[27]	e_0	e_d	P_d	f
	0.5	1.5%	3×10^{-6}	1.16

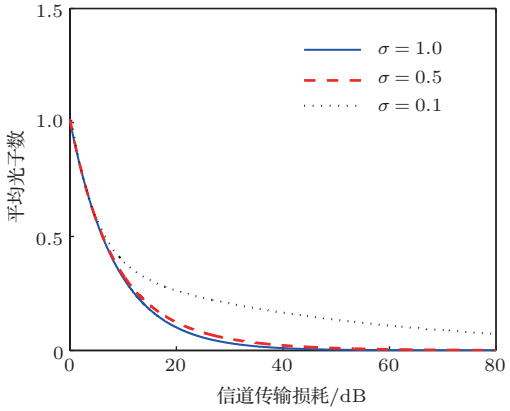

图2 平均光子数与信道传输损耗的关系

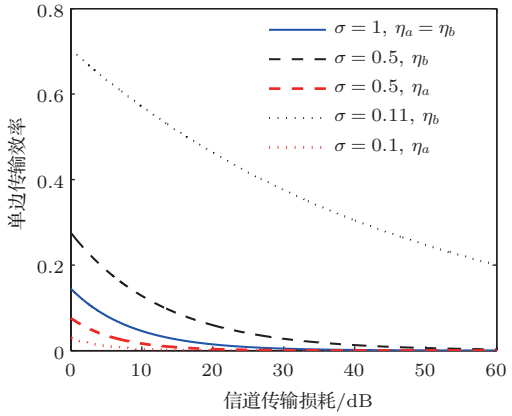

图 3 单边传输效率与信道传输损耗的关系

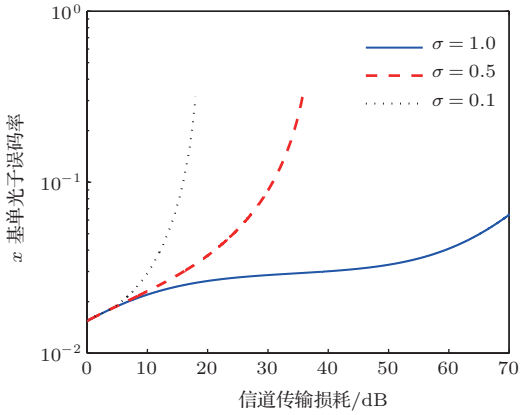

图 4 单光子误码率与信道传输损耗的关系

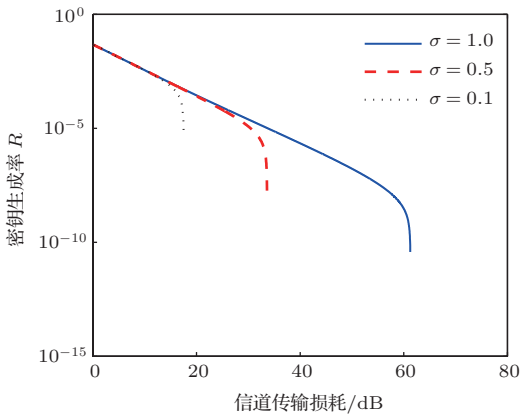

图 5 密钥生成率与信道传输损耗的关系

由图 2 可知, 随着距离比率的减小, 到达第三方进行 Bell 态测量的脉冲平均光子数逐渐增大, 等价于传统 QKD 信号光强增大时, 脉冲中多光子态的比率逐渐增加而单光子态的比例逐渐减小, 降低了安全密钥生成率. 随着第三方的位置向 Bob 端移动, 如图 3 所示, Alice 端单边传输效率逐渐减小, 反之, Bob 端单边传输效率逐渐增加, 造成信道的不匹配度逐渐增大, 使得信道单光子误码率不断增加, 如图 4 所示, 当 $\sigma = 1$ 时即信道输效率对称时, 单光子误码率随着传输损耗的增加由 0.027 上升到 0.05, 而当 $\sigma = 0.5$ 时, 传输损耗为 38 dB 时, 误码率已接近 1, 当 $\sigma = 0.1$ 时, 传输损耗为 17 dB 时误码率已接近 1, 对应于安全密钥生成率如图 5 所示, MDI-QKD 在对称信道传输效率下能够容忍 62 dB 的损耗, 而随着单边传输信道效率的改变 ($\sigma = 0.5$, 0.1), 信道传输损耗分别降至 38 dB 和 17 dB, 在光纤损耗为 0.21 dB/km 时, 分别对应传输距离为 181 km 和 81 km.

4 结 论

本文研究了非对称信道传输效率下测量设备无关量子密钥分配系统的密钥生成率与距离比率的关系, 在三强度诱骗态 MDI-QKD 协议下, 比较了对称和非对称信道传输效率情形不同距离比率下单边传输效率、单光子误码率和密钥生成率与信道传输损耗的关系. 仿真结果表明随着信道的不匹配度逐渐增加, 能够安全提取密钥的可容忍传输损耗下降较快, 密钥生成率的安全传输距离也随之降低, 在实际的实验中可以采取调节信号光强度的方式提高非对称传输效率下 MDI-QKD 的密钥生成率.

感谢国防科学技术大学孙仕海博士的讨论与帮助.

参考文献

[1] Bennet C H, Brassard G 1984 *Proc IEEE International Conference Computers, Systems, and Signal Processing* Bangalore, India, December 9–12, 1984, p175–179
[2] Shor P W, Preskill J 2000 *Phys. Rev. Lett.* **85** 441
[3] Mayers D 2001 *Journal of the ACM* **48** 351
[4] Gottesman D, Lo H K, Lutkenhaus N, Preskill J 2004 *Quantum Infor. Comput* **4** 325
[5] Zhou Y Y, Zhou X T, Tian P G, Wang Y J 2013 *Chin. Phys. B* **22** 010305
[6] Sheng Y B, Zhou L, Cheng W W, Gong L Y, Wang L, Zhan S M 2013 *Chin. Phys. B* **22** 030314
[7] Wang J D, Qin X J, Wei Z J, Liu X B, Liao C J, Liu S H 2010 *Acta Phys. Sin.* **59** 281 (in Chinese)[王金东, 秦晓娟, 魏正军, 刘小宝, 廖常俊, 刘颂豪 2010 物理学报 **59** 281]

[8] Zhang Y, Wang S, Yin Z Q, Chen W, Liang W Y, Li H W, Guo G C, Han Z F 2012 *Chin. Phys. B* **21** 100307
[9] Zhou R R Yang L 2012 *Chin. Phys. B* **21** 080301
[10] Qin X J, Zhong P P, Zhang H N, Wang J D, Wei Z J, Chen S, Liu S H 2011 *Chin. Phys. B* **20** 050307
[11] Brassard G Lutkenhaus N, Mor T, Sanders B C 2000 *Phys. Rev. Lett.* **85** 1330
[12] Sun S H, Liang L M 2012 *Appl. Phys. Lett* **101** 071107
[13] Makarov V, Skaar J 2008 *Quantum Infor. Comput.* **86** 0622
[14] Zhao Y, Fung C H F, Qi B, Chen C, Lo H K 2008 *Phys. Rev. A* **78** 042333
[15] Makarov V 2009 *New Journal of Modern Optics.* **11** 065003
[16] Acín A, Brunner N, Gisin N, Massar S, Pironio S, Scarani V 2007 *Phys. Rev. Lett* **98** 230501
[17] Pironio S, Acín A, Brunner N, Gisin N, Massar S, Scarani V 2009 *New J. Phys.* **11** 045021
[18] Lo H K, Curty M Qi B 2012 *Phys. Rev. Lett* **108** 130503
[19] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901
[20] Ma X F, Fung C H F, Razavi M 2012 *Phys. Rev. A* **86** 052305
[21] Wang X B 2013 *Phys. Rev. A* **87** 012320
[22] Sun S H Gao M, Li C Y, Liang L M 2013 *Phys. Rev. A* **87** 052329
[23] Liu Y, Chen T Y, Wang L J, Lao H, Shentu G L, Wian J, Cui K, Yin H L, Liu N L, Li L, Ma X F, Pele J S, Fejer M M, Zhang Q, Pan J W 2013 *Phys. Rev. Lett* **111** 130502
[24] Tang Z, Liao Z, Xu F, Qi B, Qian L, Lo H K 2013 *arXiv:* 13066134
[25] Rubenok A, Slater J A, Chan P, Martinez I L, Tittel W 2013 *Phys. Rev. Lett.* **111** 130501
[26] Sasaki M, Fujiwara M, Ishizuka H, Klaus W, Wakui K, Takeoka M, Tanaka A, Yoshino K, Nambu Y, Takahashi S, Tajima A, Tomita A, Domeki T, Hasegawa T, Sakai Y, Kobayashi H, Asai T, Shimizu K, Tokura T, Tsurumaru T, Matsui M, Honjo T, Tamaki K, Takesue H, Tokura Y, Dynes J F, Dixon A R, Sharpe A W, Yuan Z L, Shields A J, Uchikoga S, Legre M, Robyr S, Trinkler P, Monat L, Page J B, Ribordy G, Poppe A, Allacher A, Maurthart O, Langer T, Peev M, Zeilinger A 2011 *Opt. Express* **19** 10387
[27] Ma X F, Razavi M 2012 *Phys. Rev. A* **86** 62319

Analysis of measurement device independent quantum key distribution with an asymmetric channel transmittance efficiency*

Dong Chen[1)2)†] Zhao Shang-Hong[1)] Zhao Wei-Hu[1)] Shi Lei[1)] Zhao Gu-Hao[1)]

1) (*School of Information and Navigation, Air Force Engineering University, Xi'an 710077, China*)

2) (*Department of information security, Xi'an Communication College, Xi'an 710006, China*)

(Received 2 October 2013; revised manuscript received 3 November 2013)

Abstract

Measurement-device-independent quantum key distribution is immune from all the detection attacks, thus when it is combined with the decoy state method, the final key is unconditional secure. In this paper, the performance of three-intensity decoy state measurement-device-independent quantum key distribution at an asymmetric channel transmittance efficiency is considered and compared with each other at the symmetric choice scenario. Simulation result shows that the key rate at the symmetric scenario can tolerate 62 dB channel loss, otherwise when the distance ratio changes, the tolerated channel loss will decrease to 37 dB and 19 dB. A method to choose the optimal intensity is proposed for asymmetric channel transmittance regardless of distance ratio, which can be easily adapted to practical experimental settings.

Keywords: decoy state, measurement device independent quantum key distribution, asymmetric channel transmittance efficiency

PACS: 03.67.Dd **DOI:** 10.7498/aps.63.030302

* Project supported by the National Natural Science Foundation of China (Grant No. 61106068).

† Corresponding author. E-mail: dongchengfkd@163.com