物理学报 Acta Physica Sinica
Chinese Physical Society
Institute of Physics, CAS

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

杜亚男 解文钟 金璇 王金东 魏正军 秦晓娟 赵峰 张智明

Analysis on quantum bit error rate in measurement- device-independent quantum key distribution using weak coherent states

Du Ya-Nan Xie Wen-Zhong Jin Xuan Wang Jin-Dong Wei Zheng-Jun Qin Xiao-Juan Zhao Feng Zhang Zhi-Ming

引用信息 Citation: Acta Physica Sinica, 64, 110301 (2015) DOI: 10.7498/aps.64.110301
在线阅读 View online: http://dx.doi.org/10.7498/aps.64.110301
当期内容 View table of contents: http://wulixb.iphy.ac.cn/CN/Y2015/V64/I11

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*

杜亚男[1)] 解文钟[1)] 金璇[1)] 王金东[1)†] 魏正军[1)] 秦晓娟[2)]
赵峰[3)] 张智明[1)]

1) (华南师范大学广东省微纳光子功能材料与器件重点实验室 (信息光电子科技学院), 华南师范大学广东省量子调控工程与材料重点实验室, 广州 510006)

2) (广东理工职业学院工程技术系, 广州 510091)

3) (陕西理工学院物理与电信工程学院, 汉中 723000)

(2014 年 10 月 21 日收到; 2015 年 1 月 2 日收到修改稿)

测量设备无关量子密钥分发系统可以免疫任何针对探测器边信道的攻击, 并进一步结合诱惑态方法规避了准单光子源引入的实际安全性问题. 目前实验中一般采用弱相干光源, 但是该光源含有一定比例的空脉冲和多光子脉冲. 本文针对弱相干光源的具体特性, 采用量子力学的描述, 将各个器件进行量子化处理, 并同时考虑探测器的具体性能参数的影响, 分别给出了通信双方各自发送的脉冲含有特定光子数时产生的成功贝尔态和错误贝尔态的概率公式, 从理论上对相位编码和偏振编码测量设备无关量子密钥分发系统的误码率进行了定量分析, 分别推导并模拟了通信双方采用的平均光子数对称和不对称时误码率随传输距离的变化情况, 结果表明在偏振编码 Z 基中, 多光子脉冲不会引起误码; 在偏振编码 X 基和相位编码中, 受多光子影响, 产生的误码率较大. 对于不同的编码方式, 误码率均随传输距离的增加有不同程度的升高, 长距离传输时, 平均光子数越小, 产生的误码率越大; 在偏振编码 X 基和相位编码的短距离传输中, 相对于对称, 通信双方采用的平均光子数不对称时产生的误码率较大.

关键词: 量子密钥分发, 测量设备无关, 误码率
PACS: 03.67.Dd, 03.67.Hk **DOI:** 10.7498/aps.64.110301

1 引 言

量子密钥分发[1](quantum key distribution, QKD) 允许处于远距离的两个合法用户, 在即使存在窃听者的情况下, 生成安全密钥, 近年来已成为国内外的研究热点[2−6]. 尽管很多 QKD 协议在理论上被证明是无条件安全的[7−9], 但是利用目前的设备实现无条件安全仍存在很多漏洞, 例如探测效率不匹配攻击[10]、时移攻击[11]、相位重映射攻击[12]、设备校准影响等[13]. 为克服设备的不完美性带来的安全性问题, 设备无关 QKD(device-independent QKD, DI-QKD) 的理论方案被提出[14], 但是该方案以目前的实验技术很难实现, 形成的密钥率也特别低[15]. 2012 年 Lo 等提出的测量设备无关 QKD(measurement-device-independent QKD, MDI-QKD)[16], 免疫于任何针对探测器边信道的攻击, 大大提高了 QKD 系统的现实安全性. 系统进一步结合诱惑态方法规避了非理想光源带来的实际安全性问题. 目前人们对 MDI-QKD 进行了初步的研究[17−20]. 文献 [21] 分

* 国家自然科学基金 (批准号: 61378012, 61401262, 11374107)、国家自然科学基金重大研究计划 (批准号: 91121023)、国家重点基础研究发展计划 (973 计划)(批准号: 2011CBA00200, 2013CB921804)、教育部长江学者和创新团队发展计划 (批准号: IRT1243) 和高等学校博士学科点专项科研基金 (批准号: 20124407110009) 资助的课题.

† 通信作者. E-mail: wangjd@scnu.edu.cn

析了在偏振编码X基中, 通信双方(Alice和Bob)的单光子误码率与信道传输损耗的关系; 文献[22]采用时间段相位编码(time-bin phase-encoding), 在X基中, Alice和Bob发送的多光子脉冲如果恰好使两个探测器都响应, 则会引起50%的误码率(QBER); 文献[23]对Alice和Bob均采用单光子源和相干源时产生的成功贝尔态的概率进行了比较. 考虑到在弱相干态(weak coherent states, WCS)光源中多光子脉冲出现的概率越低, 得到的密钥生成率越高, 文献[24—26]分别用预示单光子源(HSPS)、奇相干光源和修正相干态(MCS)光源来代替WCS光源. 但是上述工作均没有考虑探测器具体性能参数对误码率的影响, 也没有给出在MDI-QKD系统中WCS光源产生的误码率随传输距离变化的定量规律.

本文针对WCS光源的具体特性, 采用量子力学的描述, 将各个器件进行量子化处理, 并同时考虑探测器具体性能参数的影响, 给出了Alice和Bob发送的脉冲中含有特定光子数时产生的成功贝尔态和错误贝尔态的概率公式, 从理论上对相位编码和偏振编码MDI-QKD系统的误码率进行了定量分析, 分别推导并模拟了在相位编码和偏振编码中Alice和Bob采用的平均光子数对称和不对称时误码率随传输距离的变化情况.

2 基于WCS光源的误码率分析

2.1 相位编码MDI-QKD方案及误码率分析

如图1所示, Alice和Bob发送的单光子脉冲通过分束器形成参考脉冲和信号脉冲, 然后相位调制器随机的从两个基$\{0,\pi\}$, $\{\pi/2,3\pi/2\}$中选择相位加载到信号脉冲上, 第三方(Charlie)通过分束器和探测器对接收到的脉冲进行贝尔态测量并公布测量结果. 在相位编码中, 光子的偏振方向需要保持相同, 所以以下描述只考虑空间模. 忽略信道传输损耗和探测器的暗计数率$p_{\rm d}$, 并假设传输路径中的相位可以很好地保持稳定, 通过计算当$\theta_{\rm a}-\theta_{\rm b}=0$, $\pm\pi$($\theta_{\rm a}$和$\theta_{\rm b}$分别表示Alice和Bob给各自的信号脉冲加载的相位)时, 形成的量子态分别为[17]

$$|0101-1010\rangle_{r_0r_1s_0s_1}, \tag{1}$$

$$|0110-1001\rangle_{r_0r_1s_0s_1}, \tag{2}$$

其中下标r_0, r_1, s_0, s_1分别表示Charlie的4个相应的探测器响应事件. (1)式表示Alice和Bob加载的相位相同时, r_0和s_0或r_1和s_1同时响应. (2)式表示Alice和Bob加载的相位相反时, r_0和s_1或r_1和s_0同时响应. 当$\theta_{\rm a}-\theta_{\rm b}=\pm\pi/2$, $\pm3\pi/2$时, 任意的两个探测器响应, 此时Alice和Bob加载相位的基不匹配, 该情况在对基过程中被抛弃. 如不考虑探测器的$p_{\rm d}$, 上述单光子源不会产生误码率. 但以目前的技术还很难实现单光子源, 在实验中一般采用强衰减形成的WCS光源来代替单光子源. 下面假设Alice和Bob采用的是WCS光源, 分析其产生的误码率情况.

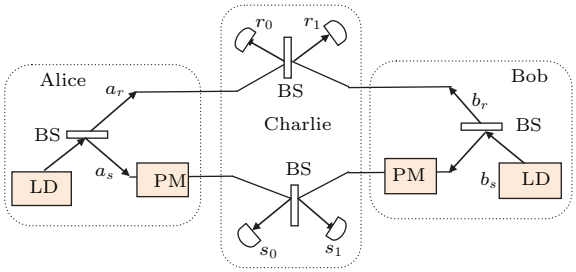

图1 相位编码MDI-QKD方案[17]

Fig. 1. The phase encoding MDI-QKD scheme[17].

采用相位随机化处理的WCS光源, 光子数分布满足泊松分布, 即

$$P_n(\mu)=\frac{\mu^n}{n!}\,{\rm e}^{-\mu}, \tag{3}$$

表示当光源输出端的平均光子数为μ时, 脉冲中含有n个光子的概率. 由于$n\geqslant3$对应的概率相对很小, 本文只考虑$n=0$, 1, 2的情况.

根据文献[17]的量子态计算方法, 当Alice和Bob均发送真空态时, 此时如不考虑探测器$p_{\rm d}$的影响, 则所有探测器均不会响应, 也不会产生有效的探测事件. 但是探测器存在$p_{\rm d}$, 所以同侧的两个探测器(r_0与s_0或r_1与s_1)以及对角的两个探测器(r_0与s_1或r_1与s_0)都有一定的概率同时响应, 此时对应成功的贝尔态输出. Alice和Bob各自随机的给信号脉冲加载相位, 只考虑基相同的情况, 所加载相位满足$\theta_{\rm a}-\theta_{\rm b}=0$或$\theta_{\rm a}-\theta_{\rm b}=\pm\pi$. 假设4个探测器的单光子探测效率$\eta$和$p_{\rm d}$均相同, 用$Y_{nm}$表示在Charlie端Alice和Bob的脉冲中分别含有n和m个光子时获得的成功贝尔态概率; $e_{nm}Y_{nm}$表示对应产生的错误贝尔态概率, 此时$n=m=0$, 则

$$Y_{00}=4p_{\rm d}^2(1-p_{\rm d})^2, \tag{4a}$$

$$e_{00}Y_{00}=2p_{\rm d}^2(1-p_{\rm d})^2. \tag{4b}$$

采用上述的分析方法, 并考虑探测器的η, 对Alice和Bob一方发送单光子态, 另一方发送真空态; 一方发送双光子态, 另一方发送真空态; 一方发送双光子态, 另一方发送单光子态; 双方均发送单光子态以及均发送双光子态8种情况分别进行讨论. 上述每种情况均可得到类似于(4a)和(4b)式的两个概率公式.

其中i个光子到达同一个ON/OFF光子探测器的探测效率η_i为

$$\begin{aligned}\eta_i =&1-(1-\eta)^i\\ =&1-\left[C_i^0 1^i(-\eta)^0+C_i^1 1^{i-1}(-\eta)^1+\cdots\right.\\ &\left.+C_i^i 1^{i-i}(-\eta)^i\right]\approx \mathrm{i}\eta. \end{aligned}\tag{5}$$

假设Alice (或Bob) 到Charlie的距离为L (km), 光纤损耗系数为0.2 dB/km, 则经传输到达Charlie后的平均光子数μ'为

$$\mu'=\mu\cdot 10^{-0.02L}.\tag{6}$$

根据文献[27], 误码率定义为

$$\mathrm{QBER}=\frac{E_{\mu_\mathrm{A}\mu_\mathrm{B}}Q_{\mu_\mathrm{A}\mu_\mathrm{B}}}{Q_{\mu_\mathrm{A}\mu_\mathrm{B}}},\tag{7}$$

$$Q_{\mu_\mathrm{A}\mu_\mathrm{B}}=\sum_{n=0}^{2}\sum_{m=0}^{2}{P'}_n^{\mathrm{A}}{P'}_m^{\mathrm{B}}Y_{nm},$$

$$E_{\mu_\mathrm{A}\mu_\mathrm{B}}Q_{\mu_\mathrm{A}\mu_\mathrm{B}}=\sum_{n=0}^{2}\sum_{m=0}^{2}{P'}_n^{\mathrm{A}}{P'}_m^{\mathrm{B}}e_{nm}Y_{nm},\tag{8}$$

$Q_{\mu_\mathrm{A}\mu_\mathrm{B}}$表示Alice和Bob光源输出端的平均光子数分别为μ_A和μ_B时, 在Charlie端得到的成功贝尔态概率, $E_{\mu_\mathrm{A}\mu_\mathrm{B}}Q_{\mu_\mathrm{A}\mu_\mathrm{B}}$是对应产生的错误贝尔态概率; ${P'}_n^{\mathrm{A}}$和${P'}_m^{\mathrm{B}}$表示在Charlie端Alice和Bob的脉冲中分别含有n和m个光子的概率, 可根据(3)和(6)式计算得到.

2.2 偏振编码MDI-QKD方案及误码率分析

如图2所示, Alice和Bob发送相干光脉冲先经过偏振调制器进行偏振编码(选取Z基X基), 再经过强度调制器调制强度, Charlie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贝尔态测量并公布测量结果. 成功的贝尔态对应的是具体的两个探测器同时响应: r_0和s_0或r_1和s_1同时响应, 表示投影到贝尔态$|\Psi^+\rangle$; r_0和s_1或r_1和s_0同时响应, 表示投影到贝尔态$|\Psi^-\rangle$, 其中$|\Psi^\pm\rangle=1/\sqrt{2}\,(|\updownarrow\rangle|\leftrightarrow\rangle\pm|\leftrightarrow\rangle|\updownarrow\rangle)$, $|\leftrightarrow\rangle$和$|\updownarrow\rangle$表示光子的偏振方向分别为水平和垂直. 只考虑基相同的情况, 下面对Alice和Bob发送的脉冲均处于Z基和X基分别进行讨论.

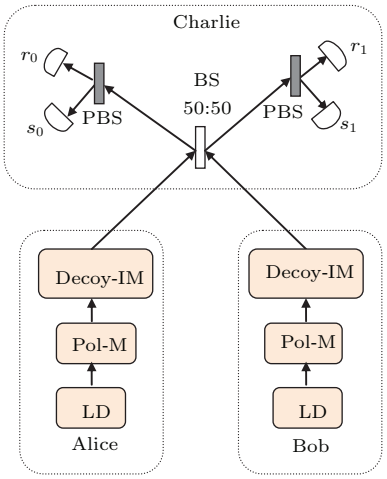

图2 偏振编码MDI-QKD方案[16]

Fig. 2. The polarization encoding MDI-QKD scheme[16].

2.2.1 发送脉冲均处于Z基

如果Alice和Bob均采用单光子源, 不考虑探测器的p_d, 则只有发送光子的偏振方向正交时才会产生成功的贝尔态, 其计算结果如下:

$$\begin{aligned}&|\leftrightarrow\rangle_1|\updownarrow\rangle_2|a\rangle_1|b\rangle_2\\ \rightarrow&\frac{1}{2}\Big[\mathrm{i}\,|\Psi^+\rangle_{12}(|c\rangle_1|c\rangle_2+|d\rangle_1|d\rangle_2)\\ &+|\Psi^-\rangle_{12}(|c\rangle_1|d\rangle_2-|d\rangle_1|c\rangle_2)\Big],\end{aligned}\tag{9}$$

其中a和b表示分束器的两个输入端, c和d表示分束器的两个输出端; 1和2表示两个光子的编号. 此时产生的$|\Psi^+\rangle$和$|\Psi^-\rangle$概率相同.

如果均采用WCS光源, 采用相位编码的分析方法, 对Alice和Bob双方均发送真空态; 均发送单光子态; 一方发送单光子态, 另一方发送真空态以及一方发送双光子态, 另一方发送真空态6种情况分别进行讨论. 通过计算得到每种情况下$|\Psi^+\rangle$和$|\Psi^-\rangle$各自出现的概率. 在Z基中, Alice和Bob发送光子的偏振方向相同时, 不管产生$|\Psi^+\rangle$还是$|\Psi^-\rangle$都会引起误码; 光子的偏振方向正交时, 不管产生$|\Psi^+\rangle$还是$|\Psi^-\rangle$都不会引起误码.

2.2.2 发送脉冲均处于X基

如果Alice和Bob均采用单光子源, 当发送光子的偏振方向相同时, 如45°偏振$|\nearrow\rangle$, 其计算结果如下:

$$|\nearrow\rangle_1|\nearrow\rangle_2|a\rangle_1|b\rangle_2$$

$$\rightarrow\frac{\mathrm{i}}{2}\left[\left|\Phi^{+}\right\rangle_{12}+\left|\Psi^{+}\right\rangle_{12}\right]\times\left(\left|c\right\rangle_{1}\left|c\right\rangle_{2}+\left|d\right\rangle_{1}\left|d\right\rangle_{2}\right),\tag{10}$$

此时产生 $|\Psi^{+}\rangle$. 当发送光子的偏振方向是 $-45°$ 偏振 $|\nwarrow\!\!\searrow\rangle$ 时, 结果与之类似.

当发送光子的偏振方向正交时, 如 Alice 发送 $|\swarrow\!\!\nearrow\rangle$, Bob 发送 $|\nwarrow\!\!\searrow\rangle$, 其计算结果如下:

$$\begin{aligned}&\left|\swarrow\!\!\nearrow\right\rangle_{1}\left|\nwarrow\!\!\searrow\right\rangle_{2}\left|a\right\rangle_{1}\left|b\right\rangle_{2}\\&\rightarrow\frac{1}{2}\Big[\mathrm{i}\left|\Phi^{-}\right\rangle_{12}\left(\left|c\right\rangle_{1}\left|c\right\rangle_{2}+\left|d\right\rangle_{1}\left|d\right\rangle_{2}\right)\\&\quad+\left|\Psi^{-}\right\rangle_{12}\left(\left|c\right\rangle_{1}\left|d\right\rangle_{2}-\left|d\right\rangle_{1}\left|c\right\rangle_{2}\right)\Big],\end{aligned}\tag{11}$$

此时产生 $|\Psi^{-}\rangle$. 当 Alice 发送 $|\nwarrow\!\!\searrow\rangle$, Bob 发送 $|\swarrow\!\!\nearrow\rangle$ 时, 结果与之类似. 其中

$$\left|\Phi^{\pm}\right\rangle=1/\sqrt{2}\left(\left|\leftrightarrow\right\rangle\left|\leftrightarrow\right\rangle\pm\left|\updownarrow\right\rangle\left|\updownarrow\right\rangle\right).$$

如果均采用 WCS 光源, 同相位编码的分析相同, 对 Alice 和 Bob 双方均发送真空态; 均发送单光子态; 一方发送单光子态, 另一方发送真空态以及一方发送双光子态, 另一方发送真空态 6 种情况分别进行讨论, 可以得到每种情况下 $|\Psi^{+}\rangle$ 和 $|\Psi^{-}\rangle$ 各自出现的概率. 在 X 基中, Alice 和 Bob 发送光子的偏振方向相同时, 如果产生 $|\Psi^{-}\rangle$, 则会引起误码; 光子的偏振方向正交时, 如果产生 $|\Psi^{+}\rangle$, 则会引起误码.

3 模拟与分析

根据 (5) 式, 结合 (3) 和 (6) 式, 将上述每种情况计算得到的成功贝尔态概率、错误的贝尔态概率代入 (8) 式, 最后通过 (7) 式可以得到相位编码和偏振编码中误码率与传输距离的关系. 在模拟过程中, 系统采用三强度诱骗态, 信号态和诱惑态的平均光子数分别取为 0.4 和 0.07, 其余参数如表 1 所示.

表 1 主要模拟参数设置

Table 1. The main simulation parameters setting.

文献 [18]	η/%	p_{d}
	40	1.3×10^{-7}

在图 3 和图 4 中, 误码率均随着传输距离的增加不断上升, 最终接近 50%. 这是由于与多光子有关的系统光学误码和探测器的 p_{d} 共同影响误码率, 随着传输距离的增加, 平均光子数不断减小, p_{d} 在影响误码率的因素中的比例逐渐增大. 在相同的 p_{d} 影响下, 平均光子数越小, 产生的误码率越大, 使得经过一定的传输后, 在相同传输距离下, Alice 和 Bob 采用的平均光子数均为 0.07 时产生的误码率大于采用不同平均光子数所产生的误码率, 而平均光子数均为 0.4 时产生的误码率最小. 在图 3 和图 4 (b) 中, 相对于 p_{d}, 光学误码在影响误码率的因

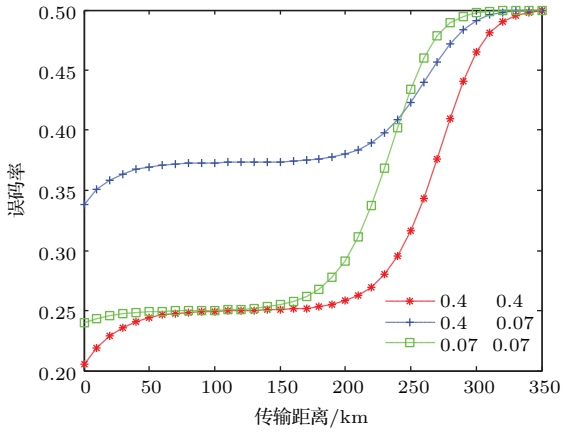

图 3 (网刊彩色) 相位编码中误码率与传输距离的关系

Fig. 3. (color online) The relationship between the QBER and the transmission distance in phase encoding.

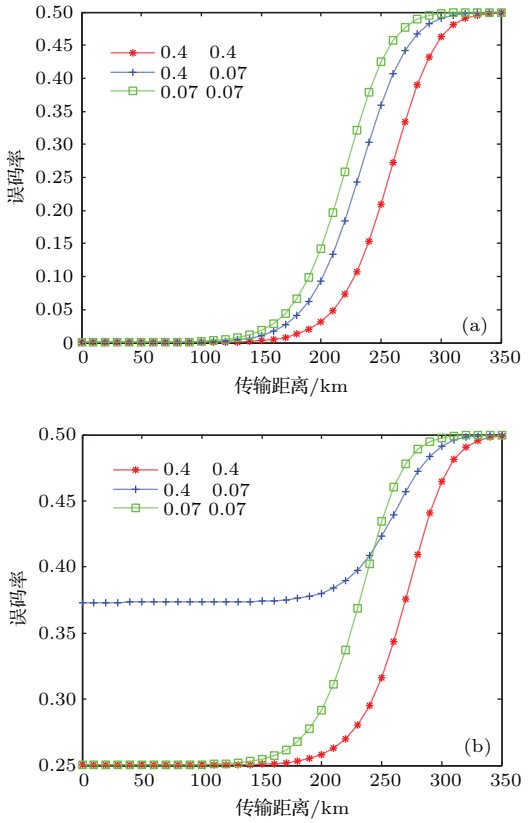

图 4 (网刊彩色) 偏振编码中误码率与传输距离的关系 (a) Z 基; (b) X 基

Fig. 4 (color online) The relationship between the QBER and the transmission distance in polarization encoding: (a) Z basis; (b) X basis.

素中所占比例较大, 使得在传输距离较小时整体的误码率很高, 分别大于20%和25%. 传输距离小于150 km时, 在相同传输距离下, Alice和Bob的平均光子数不同时产生的误码率比相同时产生的误码率大12%, 即平均光子数的不对称导致高误码率. 在图4 (a) 中, 相对于$p_{\rm d}$, 光学误码在影响误码率的因素中所占比例较小, 使得在传输距离较小时整体的误码率较低, 小于2%.

4 结 论

本文研究了在相位编码和偏振编码MDI-QKD系统中, 采用WCS光源产生的误码率与传输距离的关系, 结果表明在偏振编码Z基中, 多光子脉冲不会引起误码; 在偏振编码X基和相位编码中, 受多光子影响, 产生的误码率较大. 对于不同的编码方式, 误码率均随传输距离的增加有不同程度的升高, 长距离传输时, 平均光子数越小, 产生误码率越大. 在偏振编码X基和相位编码的短距离传输中, 相对于对称, Alice和Bob采用的平均光子数不对称时产生的误码率较大.

参考文献

[1] Gisin N, Ribordy G, Tittel W, Zbinden H 2002 *Rev. Mod. Phys.* **74** 145

[2] Li M, Patcharapong T, Zhang C M, Yin Z Q, Chen W, Han Z F 2015 *Chin. Phys. B* **24** 010302

[3] Ma H Q, Wei K J, Yang J H, Li R X, Zhu W 2014 *Chin. Phys. B* **23** 100307

[4] Chen W F, Wei Z J, Guo L, Hou L Y, Wang G, Wang J D, Zhang Z M, Guo J P, Liu S H 2014 *Chin. Phys. B* **23** 080304

[5] Zhou Y Y, Zhou X J, Tian P G, Wang Y J 2013 *Chin. Phys. B* **22** 010305

[6] Zhou R R, Y L 2012 *Chin. Phys. B* **21** 080301

[7] Lo H K, Chau H F 1999 *Science* **283** 2050

[8] Shor P W, Preskill J 2000 *Phys. Rev. Lett.* **85** 441

[9] Mayers D 2001 *J. ACM* **48** 351

[10] Makarov V, Anisimov A, Skaar J 2006 *Phys. Rev. A* **74** 022313

[11] Zhao Y, Fung C H F, Qi B, Chen C, Lo H K 2008 *Phys. Rev. A* **78** 042333

[12] Fung C H F, Qi B, Tamaki K, Lo H K 2007 *Phys. Rev. A* **75** 032314

[13] Jain N, Wittmann C, Lydersen L, Wiechers C, Elser D, Marquardt C, Makarov V, Leuchs G 2011 *Phys. Rev. Lett.* **107** 110501

[14] Acín A, Brunner N, Gisin N, Massar S, Pironio S, Scarani V 2007 *Phys. Rev. Lett.* **98** 230501

[15] Gisin N, Pironio S, Sangouard N 2010 *Phys. Rev. Lett.* **105** 070501

[16] Lo H K, Curty M, Qi B 2012 *Phys. Rev. Lett.* **108** 130503

[17] Ma X, Razavi M 2012 *Phys. Rev. A* **86** 062319

[18] Tang Y L, Yin H L, Chen S J, Liu Y, Zhang W J, Jiang X, Zhang L, Wang J, You L X, Guan J Y, Yang D X, Wang Z, Liang H, Zhang Z, Zhou N, Ma X, Chen T Y, Zhang Q, Pan J W 2015 *IEEE J. Select. Topics Quantum Electron.* **21** 6600407

[19] Zhou C, Bao W S, Chen W, Li H W, Yin Z Q, Wang Y, Han Z F 2013 *Phys. Rev. A* **88** 052333

[20] Wang Y, Bao W S, Li H W, Zhou C, Li Y 2014 *Chin. Phys. B* **23** 080303

[21] Dong C, Zhao S H, Zhao W H, Shi L, Zhao G H 2014 *Acta Phys. Sin.* **63** 030302 (in Chinese) [东晨, 赵尚弘, 赵卫虎, 石磊, 赵顾颖 2014 物理学报 **63** 030302]

[22] Liu Y, Chen T Y, Wang L J, Liang H, Shentu G L, Wang J, Cui K, Yin H L, Liu N L, Li L, Ma X, Pelc J S, Fejer M M, Peng C Z, Zhang Q, Pan J W 2013 *Phys. Rev. Lett.* **111** 130502

[23] da Silva T F, Vitoreti D, Xavier G B, do Amaral G C, Tempor o G P, von der Weid J P 2013 *Phys. Rev. A* **88** 052303

[24] Wang Q, Wang X B 2013 *Phys. Rev. A* **88** 052332

[25] Dong C, Zhao S H, Zhang N, Dong Y, Zhao W H, Liu Y 2014 *Acta Phys. Sin.* **63** 200304 (in Chinese) [东晨, 赵尚弘, 张宁, 董毅, 赵卫虎, 刘韵 2014 物理学报 **63** 200304]

[26] Li M, Zhang C M, Yin Z Q, Chen W, Wang S, Guo G C, Han Z F 2014 *Opt. Lett.* **39** 880

[27] Ma X, Fung C H F, Razavi M 2012 *Phys. Rev. A* **86** 052305

Analysis on quantum bit error rate in measurement-device-independent quantum key distribution using weak coherent states*

Du Ya-Nan[1)] Xie Wen-Zhong[1)] Jin Xuan[1)] Wang Jin-Dong[1)†] Wei Zheng-Jun[1)]
Qin Xiao-Juan[2)] Zhao Feng[3)] Zhang Zhi-Ming[1)]

1) (*Laboratory of Nanophotonic Functional Materials and Devices (SIPSE), and Laboratory of Quantum Engineering and Quantum Materials, South China Normal University, Guangzhou 510006, China*)

2) (*Engineering Technology Department, Guangdong Polytechnic Institute, Guangzhou 510091, China*)

3) (*School of Physics and Telecommunication Engineering, Shaanxi University of Technology, Hanzhong 723000, China*)

(Received 21 October 2014; revised manuscript received 2 January 2015)

Abstract

A measurement-device-independent quantum key distribution (MDI-QKD) protocol is immune to all detection side-channel attacks and guarantees the information-theoretical security even with uncharacterized single photon detectors. A weak coherent source is used in the current MDI-QKD experiments, it inevitably contains a certain percentage of vacuum and multi-photon pulses. The security issues introduced by these source imperfections can be avoided by applying the decoy state method. Here, through modeling experimental devices, and taking into account the weak coherent source and the threshold detectors, we have evaluated the gain, the probability to get successful Bell measurement and incorrect Bell measurement, and the quantum bit error rate (QBER), given a practical setup. In our simulation, we show how QBER varies with different transmission distances in the cases when the average photon numbers per pulse from Alice and Bob are symmetric and asymmetric. Result shows that the multi-photon pulses do not cause error in the Z basis of polarization encoding scheme, but produce a large QBER in phase encoding scheme and in the X basis of polarization encoding scheme. QBER is affected by the dark count rate and the system optical error associated with the multi-photon pulses. For different encoding schemes, QBER caused by each kind of average photon numbers from Alice and Bob increases to different degrees with the transmission distance, and finally is close to 50%. With the increase of the transmission distance, the average photon number per pulse decreases and the fraction of the dark count rate causing QBER gradually increases. Under the same effect of the dark count rate, the smaller the average photon number per pulse, the bigger the QBER. After a certain transmission and at the same transmission distance, the QBER is largest when average photon numbers used by Alice and Bob are both smallest. For the short distance transmission of phase encoding scheme and the X basis, we find that QBER is larger when average photon numbers from the two arms are asymmetric, as compared to the symmetric case. For the Z basis, the QBER caused by the system optical error and the dark count rate is very small.

Keywords: quantum key distribution, measurement-device-independent, quantum bit error rate

PACS: 03.67.Dd, 03.67.Hk **DOI:** 10.7498/aps.64.110301

* Project supported by the National Natural Science Foundation of China (Grant Nos. 61378012, 61401262, 11374107), the Major Research Plan of the National Natural Science Foundation of China(Grant No. 91121023), the National Basic Research Program of China (Grant Nos. 2011CBA00200, 2013CB921804), the Program for Changjiang Scholars and Innovative Research Team in University of Ministry of Education of China (Grant No. IRT1243), and the Specialized Research Fund for the Doctoral Program of Higher Education of China (Grant No. 20124407110009).

† Corresponding author. E-mail: wangjd@scnu.edu.cn