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

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

吴承峰 杜亚男 王金东 魏正军 秦晓娟 赵峰 张智明

Analysis on performance optimization in measurement-device-independent quantum key distribution using weak coherent states

Wu Cheng-Feng Du Ya-Nan Wang Jin-Dong Wei Zheng-Jun Qin Xiao-Juan Zhao Feng Zhang Zhi-Ming

引用信息 Citation: Acta Physica Sinica, 65, 100302 (2016) DOI: 10.7498/aps.65.100302
在线阅读 View online: http://dx.doi.org/10.7498/aps.65.100302
当期内容 View table of contents: http://wulixb.iphy.ac.cn/CN/Y2016/V65/I10

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*

吴承峰[1)] 杜亚男[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), 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)

(2015 年 12 月 3 日收到; 2016 年 2 月 12 日收到修改稿)

测量设备无关量子密钥分发系统能够抵御任何针对单光子探测器边信道的攻击, 进一步结合诱惑态的方案, 可以同时规避准单光子源引起的实际安全漏洞. 测量设备无关量子密钥分发系统中, 非对称传输、分束器的不对称以及各个单光子探测器存在实际参数差异等光学系统的具体实现特征会对系统误码率和成码率等性能产生一定的影响. 本文针对采用弱相干光源的测量设备无关量子密钥分发系统, 引入单光子探测器品质因子的实验参数 (暗计数与探测效率的比值), 通过量子化描述, 理论推导并模拟了误码率与单光子探测器品质因子、分束器反射率以及通信双方弱相干光源平均光子数之间的关系. 结果表明: 在 X 基偏振编码和相位编码系统中, 当分束器的反射率趋近于 0.5 时, 误码率取最小值; 在偏振编码和相位编码系统中, 误码率随着单光子探测器品质因子的增大而增大; 在 Z 基偏振编码系统中, 误码率随分束器的反射率的变化会呈现较小的波动, 当分束器的反射率为 0.5 时, 若通信双方采用的平均光子数相差较大, 则误码率取最大值; 分束器的反射率和平均光子数对误码率的影响在 Z 基情况下不能等同, 但是对于 X 基编码和相位编码却能等同.

关键词: 量子密钥分发, 测量设备无关, 误码率, 分束器

PACS: 03.67.Dd, 03.67.Hk **DOI:** 10.7498/aps.65.100302

1 引 言

量子密钥分发[1] (quantum key distribution, QKD) 基于量子力学和信息论, 允许合法通信双方 Alice 和 Bob, 在即使存在窃密者 Eve 的情况下, 仍旧可以产生安全密钥, 近几年已经成为国内外的研究热点[2−7]. 在理论上, 尽管有些 QKD 协议已经被证明是无条件安全的[8−10], 但实际的 QKD 系统却由于设备的不完美性而存在各种安全漏洞, 例如窃密者可以利用探测器的非完美性实施探测效率不匹配攻击[11]、时移攻击[12,13], 针对光源的非完美特征实施光子数分裂攻击[14], 相位部分随机化攻击等[15]. 为了规避设备非完美性导致的安全漏洞, Acin 等[16] 提出了设备无关 QKD (device independent QKD, DI-QKD), 其优点是不需要知道 QKD 系统的实际工作状态就可以基于 Bell 理论证明其无条件安全性, 但是该方案要求单光子探测器的探测效率接近 100%, 目前的实验技术还很难实现, 而且密钥率较低[17]. 2012 年 Lo 等[18] 提出了测量设备无关 QKD (measurement device inde-

* 国家自然科学基金重大研究计划 (批准号: 91121023)、国家自然科学基金 (批准号: 61378012, 11374107, 60978009, 61108039, 61401176, 61401262)、广东省自然科学基金 (批准号: 2014A030310205, 2015A030313388)、国家重点基础研究发展计划 (批准号: 2011CBA00200)、广东省科技计划 (批准号: 2014B090901016) 和广东省应用型科技研发专项资金 (批准号: 2015B010128012) 资助的课题.

† 通信作者. E-mail: wangjd@scnu.edu.cn

pendent QKD, MDI-QKD), 在该方案中, Alice和Bob将单光子脉冲发送到第三方进行贝尔态测量, 故其可免疫于任何探测器边信道攻击, 系统同时结合诱惑态[19]的方法规避了光源的不完美所导致的攻击. 自从该方案提出以来, 在理论和实验上均取得了一定的进展[20−23].

为了优化MDI-QKD系统的性能, 一些研究小组对实验参数与误码率之间的关系进行了研究. 文献[24]研究了基于弱相干态(weak coherent states, WCS)光源MDI-QKD系统误码率和诱惑态平均光子数、信号态平均光子数以及脉冲比的定量关系, 并得到了相关实验结果. 文献[25]通过高稳定的系统和高效率的单光子探测器使安全传输距离超过200 km, 并且实验上得出了使用空+弱诱惑态方案的密钥率随损耗的变化关系. 文献[26]提出了基于量子存储的长距离测量设备无关量子密钥分配协议, 分析了其密钥生成率与存储效率、信道传输效率和安全传输距离等参数间的关系. 文献[27]讨论了非对称传输信道和对称传输信道情况下的传输距离比对单光子X基偏振编码系统误码率的影响. 文献[28]在实现偏振编码MDI-QKD实验的基础上, 得到了每脉冲平均光子数为几组离散值时的误码率和筛选码率. 文献[29]使用2个诱惑态+1个信号态, 准确地推导了密钥生成率的下限和误码率上限的公式. 最近, 文献[30]针对通信双方采用的平均光子数对称和不对称的情况, 研究了相位编码和偏振编码MDI-QKD的误码率随距离的变化关系. 由于在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, 因此文献[31, 32]分别用预报单光子源(HSPS)和修正相干态(MCS)光源来代替WCS光源. 除此之外, 单光探测器的品质因子和分束器(beam splitter, BS)的反射率对误码率的影响以及WCS的平均光子数连续变化时误码率的变化规律目前尚未见到报道, 而这些参数都会在一定程度上影响系统的性能.

本文针对WCS光源的具体特征, 在偏振编码系统和相位编码系统中, 采用量子力学的描述, 对各个器件进行量子化处理, 同时为了探究单光子探测器的性能对误码率的影响, 引入了单光子探测器的品质因子作为模拟参量. 在此基础上, 针对不同品质因子的单光子探测器和不同反射率的BS, 分别推导了通信双方各自发送特定平均光子数和连续变化平均光子数的WCS脉冲所产生的成功贝尔态概率、错误贝尔态概率和误码率的公式, 并模拟了误码率与反射率、品质因子和平均光子数的关系, 此外, 还推导并模拟了不同反射率的误码率随距离的变化关系.

本文的结构安排如下: 第二部分介绍了WCS脉冲MDI-QKD编码方案, 计算了通信双方在几种光子数态组合的条件下产生成功和错误贝尔态的概率, 进而得出了对应条件下MDI-QKD的误码率公式; 第三部分对误码率和参数之间的关系进行模拟和分析; 第四部分对本文进行了总结.

2 基于WCS光源的误码率分析

2.1 MDI-QKD相位编码方案及误码率分析

图1为相位编码MDI-QKD方案图, 其中左、右、上、下四个BS的反射率分别用$r_{\rm a}$, $r_{\rm b}$, $r_{\rm c}$和$r_{\rm d}$表示, 四个单光子探测器的探测效率分别为η_{r_0}, η_{r_1}, η_{s_0}和η_{s_1}, 品质因子(为了更全面地描述单光子探测器的性能, 定义品质因子为暗计数与探测效率的比值)分别为P_{r_0}, P_{r_1}, P_{s_0}和P_{s_1}, Alice到Charlie的距离为$L_{\rm AC}$, 输出WCS的平均光子数为$\mu_{\rm a}$, Bob到Charlie的距离为$L_{\rm BC}$, 输出WCS的平均光子数为$\mu_{\rm b}$, 传输损耗值为0.2 dB/km.

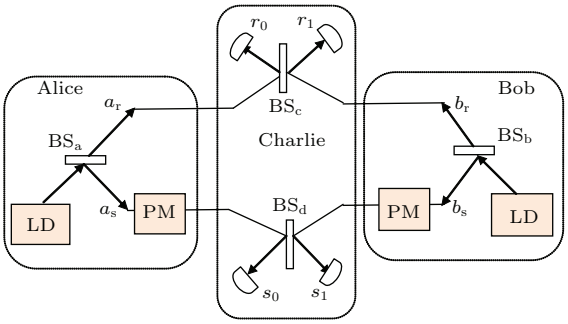

图1 相位编码MDI-QKD方案[20]

Fig. 1. The phase encoding MDI-QKD scheme[20].

在使用WCS脉冲进行MDI-QKD相位编码时, 通信双方发送的WCS脉冲在分别通过各自的BS后形成了参考脉冲和信号脉冲, 相位调制器从$(\pi/2, 3\pi/2)$, $(0, \pi)$两组相位基中随机地选择要加载到$a_{\rm s}$路和$b_{\rm s}$路的信号脉冲的相位. Charlie对参考脉冲和信号脉冲进行贝尔态测量并公布测量结果.

由于光子的偏振方向在相位编码中需要保持一致, 因此在描述相位编码时只需要考虑空间模和假设脉冲的相位在传输中能够很好地保持. 在

Alice和Bob选择的编码基相同时, 若r_0和s_0或者r_1和s_1同时发生响应, 表示投影到贝尔态$|\psi_{\rm p}^{+}\rangle$, 此时Alice和Bob加载的相位相同; 若r_0和s_1或者r_1和s_0同时发生响应, 表示投影到贝尔态$|\psi_{\rm p}^{-}\rangle$, 此时Alice和Bob加载的相位差为π. 若上述4种响应情况中的任何一种发生, 则说明产生了成功的贝尔态[28], 其中: $|\psi_{\rm p}^{+}\rangle = |0101-1010\rangle_{r_0r_1s_0s_1}$, $|\psi_{\rm p}^{-}\rangle = |0110-1001\rangle_{r_0r_1s_0s_1}$. 由于Alice和Bob在通信过程中会进行对基并抛弃基不相同的码, 因此$\theta_{\rm a}-\theta_{\rm b}=\pm\dfrac{\pi}{2}, \pm\dfrac{3\pi}{2}$所形成的码将会被抛弃.

相位随机化的WCS光子数分布满足泊松分布:

$$P_n(\mu)=\frac{\mu^n}{n!}\,{\rm e}^{-\mu}, \tag{1}$$

该公式表示平均光子数为μ的WCS脉冲含有n个光子的概率为$P_n(\mu)$. 在Charlie处, WCS脉冲也有一定概率包含0个光子和多光子, 所以在计算误码率时, 除了需要计算WCS脉冲包含单个光子时的成功贝尔态的概率和错误贝尔态的概率, 还应该考虑包含0个光子和多光子的情况. 但由于$n\geqslant 3$时的$P_n(\mu)$相对较小, 因此本文只考虑$n<3$的情况.

依照文献[20]的算法, 当通信双方发送的WCS脉冲在Charlie处均包含1个光子时, 输入BS的量子态为

$$\begin{aligned}&\left[\sqrt{1-r_{\rm a}}|1\rangle_{a_{\rm r}}|0\rangle_{a_{\rm s}}+\sqrt{r_{\rm a}}\,{\rm e}^{{\rm i}\theta_{\rm a}}|0\rangle_{a_{\rm r}}|1\rangle_{a_{\rm s}}\right]\\&\otimes\left[\sqrt{1-r_{\rm b}}|1\rangle_{b_{\rm r}}|0\rangle_{b_{\rm s}}+\sqrt{r_{\rm b}}\,{\rm e}^{{\rm i}\theta_{\rm b}}|0\rangle_{b_{\rm r}}|1\rangle_{b_{\rm s}}\right],\end{aligned} \tag{2}$$

进一步推导得出输出态的表达式, 根据输出态的表达式可得$\theta_{\rm a}-\theta_{\rm b}=0$和π时的$Y_{11}$, $E_{11}Y_{11}$. Y_{mn}和$E_{mn}Y_{mn}$分别表示Alice和Bob的脉冲在Charlie端含有m和n个光子时获得的成功贝尔态的概率和错误贝尔态的概率. 其中n个光子到达同一个ON/OFF光子探测器的探测效率η_n为

$$\eta_n=1-(1-\eta)^n, \tag{3}$$

当通信双方发送的WCS脉冲在Charlie处均包含0个光子时, 4个单光子探测器在暗计数率均为0的情况下都不会发生响应. 但是, 如果暗计数率不为0, 则可能出现成功贝尔态对应的4种探测器响应情况, 此时, 若通信双方使用的基相同, 将会有一半的概率产生误码, 其中产生成功贝尔态以及错误贝尔态的概率分别为

$$\begin{aligned}&Y_{00}\\&=\eta_{r_0}\eta_{s_0}P_{r_0}P_{s_0}(1-\eta_{r_1}P_{r_1})(1-\eta_{s_1}P_{s_1})\\&+\eta_{r_0}\eta_{s_1}P_{r_0}P_{s_1}(1-\eta_{r_1}P_{r_1})(1-\eta_{s_0}P_{s_0})\\&+\eta_{r_1}\eta_{s_0}P_{r_1}P_{s_0}(1-P_{r_0}\eta_{r_0})(1-\eta_{s_1}P_{s_1})\\&+\eta_{r_1}\eta_{s_1}P_{r_1}P_{s_1}(1-P_{r_0}\eta_{r_0})(1-\eta_{s_0}P_{s_0}),\end{aligned} \tag{4}$$

$$\begin{aligned}&E_{00}Y_{00}\\&=\frac{1}{2}\big[\eta_{r_0}\eta_{s_0}P_{r_0}P_{s_0}(1-\eta_{r_1}P_{r_1})(1-\eta_{s_1}P_{s_1})\\&+\eta_{r_0}\eta_{s_1}P_{r_0}P_{s_1}(1-\eta_{r_1}P_{r_1})(1-\eta_{s_0}P_{s_0})\\&+\eta_{r_1}\eta_{s_0}P_{r_1}P_{s_0}(1-P_{r_0}\eta_{r_0})(1-\eta_{s_1}P_{s_1})\\&+\eta_{r_1}\eta_{s_1}P_{r_1}P_{s_1}(1-P_{r_0}\eta_{r_0})(1-\eta_{s_0}P_{s_0})\big],\end{aligned} \tag{5}$$

按照上述计算方法, 本文计算了$n+m\leqslant 3$且m, $n<3$时8种情况下的Y_{mn}和$E_{mn}Y_{mn}$.

考虑WCS脉冲在传输过程中的衰减, 可得Alice和Bob发送的脉冲到达Charlie处的BS时的每脉冲平均光子数分别为

$$\mu_{\rm a}'=\mu_{\rm a}10^{-0.02L_{\rm AC}}, \tag{6a}$$

$$\mu_{\rm b}'=\mu_{\rm b}10^{-0.02L_{\rm BC}}, \tag{6b}$$

误码率的定义[24]为

$${\rm QBER}=\frac{E_{\mu_{\rm a}\mu_{\rm b}}Q_{\mu_{\rm a}\mu_{\rm b}}}{Q_{\mu_{\rm a}\mu_{\rm b}}}, \tag{7}$$

$$Q_{\mu_{\rm a}\mu_{\rm b}}=\sum_{m=0}^{2}\sum_{n=0}^{2}P_n^{\rm A}P_m^{\rm B}Y_{nm}, \tag{8}$$

$$E_{\mu_{\rm a}\mu_{\rm b}}Q_{\mu_{\rm a}\mu_{\rm b}}=\sum_{m=0}^{2}\sum_{n=0}^{2}P_n^{\rm A}P_m^{\rm B}e_{nm}Y_{nm}, \tag{9}$$

其中, $Q_{\mu_{\rm a}\mu_{\rm b}}$表示当Alice和Bob光源输出端的平均光子数分别为$\mu_{\rm a}$, $\mu_{\rm b}$时, 在Charlie端得到成功贝尔态的概率; $E_{\mu_{\rm a}\mu_{\rm b}}Q_{\mu_{\rm a}\mu_{\rm b}}$表示对应产生错误贝尔态的概率; $P_n^{\rm A}$和$P_m^{\rm B}$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, 其可根据(6)式和(1)式推导得出. 结合BS两端WCS脉冲的8种不同光子数脉冲组合所对应的Y_{nm}和$E_{nm}Y_{nm}$, 将其代入(7)—(9)式, 可得相位编码MDI-QKD中成功贝尔态的概率和错误贝尔态的概率, 进而可以推导得出误码率的表达式.

2.2 偏振编码MDI-QKD方案及误码率分析

如图2所示, Alice和Bob各自发送的WCS脉冲先经过Pol-M进行偏振调制编码, 再经过Decoy-IM进行强度调制, 之后Charlie使用BS, PBS和单光子探测器对接收到的WCS脉冲进行贝尔态测量并公布测量结果. 成功的贝尔态输出对应4种可能

的两个单光子探测器的响应组合, 即同侧或对角的两个单光子探测器同时响应. 同侧的两个单光子探测器同时响应, 表示投影到贝尔态$|\psi^+\rangle$; 对角的两个单光子探测器同时响应, 表示投影到贝尔态$|\psi^-\rangle$. 其中: $|\psi^\pm\rangle=\frac{1}{\sqrt{2}}(|\updownarrow\rangle|\leftrightarrow\rangle\pm|\leftrightarrow\rangle|\updownarrow\rangle)$, $|\leftrightarrow\rangle$表示水平偏振态, $|\updownarrow\rangle$表示竖直偏振态. 最后, Alice和Bob进行对基, 抛弃基不相同的密钥比特.

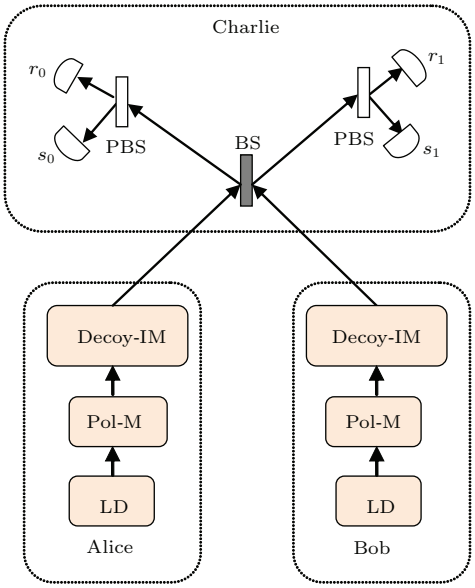

图2 偏振编码MDI-QKD方案[18]

Fig. 2. The polarization encoding MDI-QKD scheme[18].

2.2.1 双方偏振态都属于Z基

若BS的反射率为r, 探测器的品质因子分别为P_{r_0}, P_{r_1}, P_{s_0}和P_{s_1}, 当通信双方发送的WCS脉冲在Charlie处均包含1个光子时, 通信双方发送的偏振态相互正交时的输出态表示如下:

$$\begin{aligned}&|\leftrightarrow\rangle_1|\updownarrow\rangle_2|a\rangle_1|b\rangle_2\\=&\frac{1}{\sqrt{2}}\Big\{\mathrm{i}\sqrt{r(1-r)}\big[|\leftrightarrow\rangle_1|\updownarrow\rangle_2+|\updownarrow\rangle_1|\leftrightarrow\rangle_2\big]|c\rangle_1|c\rangle_2\\&+\big[(1-r)|\updownarrow\rangle_1|\leftrightarrow\rangle_2-r|\leftrightarrow\rangle_1|\updownarrow\rangle_2\big]|c\rangle_1|d\rangle_2\\&-\big[-r|\updownarrow\rangle_1|\leftrightarrow\rangle_2+(1-r)|\leftrightarrow\rangle_1|\updownarrow\rangle_2\big]|d\rangle_1|c\rangle_2\\&+\mathrm{i}\sqrt{r(1-r)}\big[|\leftrightarrow\rangle_1|\updownarrow\rangle_2+|\updownarrow\rangle_1|\leftrightarrow\rangle_2\big]|d\rangle_1|d\rangle_2\Big\},\end{aligned}\tag{10}$$

其中, a和b表示BS的两个输入端, c和d表示BS的两个输出端, 1和2表示两个光子的编号.

如果Alice和Bob发送的光子的偏振方向相同, 则不管产生ψ^-还是ψ^+都会引起误码; 如果光子的偏振方向正交, 不管产生ψ^-还是ψ^+都不会引起误码. 在光源为WCS光源的情况下, 利用上述计算相位编码误码率的方法, 分别计算$n+m\leqslant 2$时对应6种情况下的Y_{nm}和$E_{nm}Y_{nm}$, 再根据(6)式和(1)式计算得到在Charlie处Alice和Bob的脉冲中分别含有n和m个光子的概率P_n^{A}和P_m^{B}, 将其代入(7)—(9)式得到Z基偏振编码MDI-QKD中成功贝尔态的概率和错误贝尔态的概率, 进而可以推导得出Z基偏振编码MDI-QKD误码率的表达式.

2.2.2 双方偏振态属于X基

若通信双方发送的WCS脉冲在Charlie处均包含1个光子且偏振态相同, 不管双方同时发送$|\nearrow\rangle$还是$|\nwarrow\rangle$, BS输出的量子态均相同. 以两边同时发送$|\nearrow\rangle$计算为例:

$$\begin{aligned}&|\nearrow\rangle_1|\nearrow\rangle_2|a\rangle_1|b\rangle_2\\=&\frac{1}{\sqrt{2}}\big[2\mathrm{i}\sqrt{r(1-r)}(\psi^++\Phi^+)(|c\rangle_1|c\rangle_2+|d\rangle_1|d\rangle_2)\\&+(1-2r)(\psi^++\Phi^+)(|c\rangle_1|d\rangle_2+|d\rangle_1|c\rangle_2)\big],\end{aligned}\tag{11}$$

其中

$$\Phi^+=|\leftrightarrow\rangle_1|\leftrightarrow\rangle_2+|\updownarrow\rangle_1|\updownarrow\rangle_2.\tag{12}$$

在X基编码中当Alice和Bob发送光子的偏振方向相同时, 如果产生ψ^-, 则会引起误码; 当光子的偏振方向正交时, 如果产生ψ^+, 则会引起误码. 和计算相位编码误码率与Z基偏振编码误码率的计算方法相同, 本文分别计算了$n+m\leqslant 2$时对应6种情况下的Y_{nm}和$E_{nm}Y_{nm}$, 并进一步得到X基偏振编码MDI-QKD误码率的表达式.

3 模拟与分析

根据上述计算得出的相位编码和偏振编码误码率的公式, 分别模拟和分析了对应参数取值的条件下, 误码率与BS反射率、误码率与平均光子数以及误码率与品质因子之间的关系.

图3给出了误码率和反射率r之间的关系, 此时, 探测器的品质因子P为3.25×10^{-7} (探测效率为0.4, 暗计数为1.3×10^{-7}), Alice和Bob采用的平均光子数μ_{a}和μ_{b}都为0.1, 且双方到Charlie的距离L_{AC}和L_{BC}都是0 km. 由图3可知: 在r趋近于0.5时, 相位编码和X基偏振编码的误码率取最小值, Z基偏振编码的误码率取最大值. 这主要是因为在Z基偏振编码时, 通信双方采用的平均光子数相等, 此时, 如果BS两端输入的脉冲含有的光子数较大, 那么r越趋近于1或0, 误码率越小.

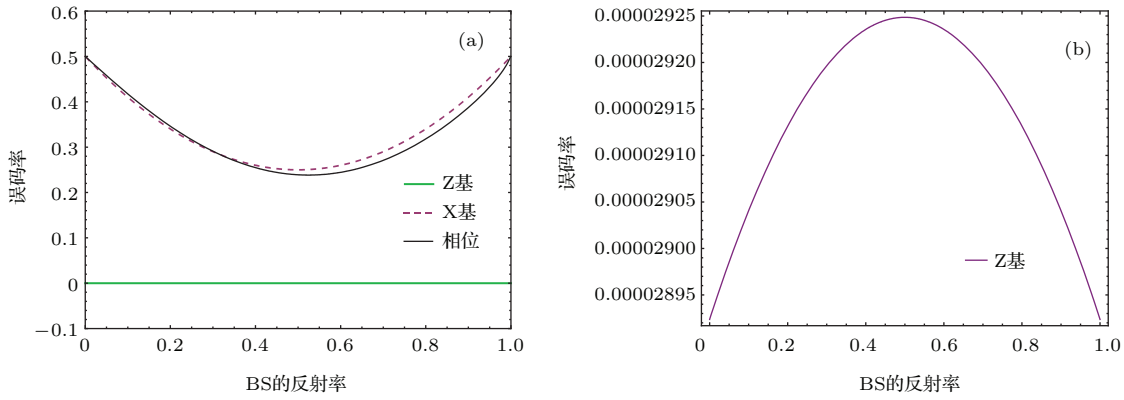

图 3 (网刊彩色) 误码率与反射率之间的关系 (a) Z 基, X 基, 相位; (b) Z 基

Fig. 3. (color online) The relationship between the QBER and the reflectivity: (a) Z basis, X basis, phase; (b) Z basis.

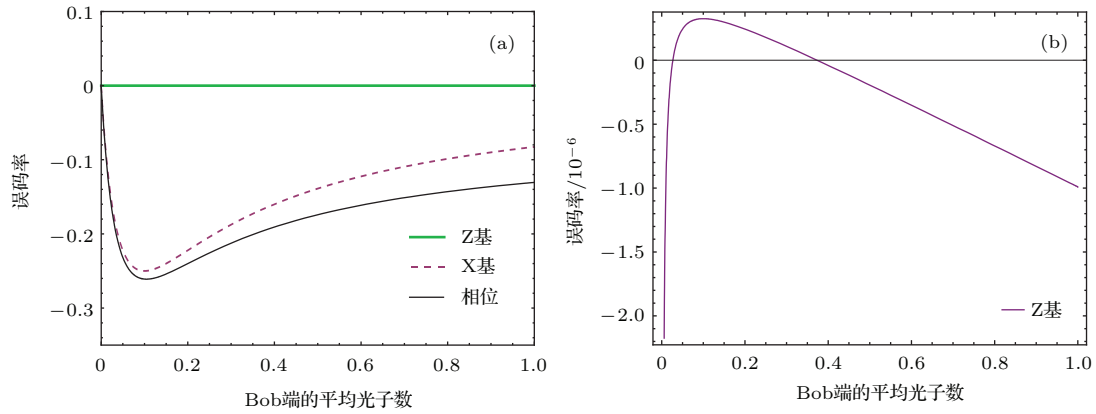

图 4 (网刊彩色) 误码率 $E_{r=0.5}-E_{r=0}$ 和平均光子数之间的关系 (a) Z 基, X 基, 相位; (b) Z 基

Fig. 4. (color online) The relationship between $E_{r=0.5}-E_{r=0}$ and average photon number: (a) Z basis, X basis, phase; (b) Z basis.

图 4 给出了误码率差值 ($r=0.5$ 和 $r=0$ 时误码率的差值) 与 $\mu_{\rm b}$ 之间的关系, 此时, P 为 3.25×10^{-7}, $L_{\rm AC}$ 和 $L_{\rm BC}$ 均为 0 km, $\mu_{\rm a}$ 为 0.1. 结合图 3 可知: 在 Z 基偏振编码系统中, 当 $\mu_{\rm b}$ 较大或者较小时, 误码率在 $r=0.5$ 附近才取最小值, 主要受暗计数和多光子数的影响, 而且相位编码和 X 基偏振编码受 r 的影响不大.

图 5 给出了误码率和品质因子之间的关系, 此时, r 为 0.5, $L_{\rm AC}$ 和 $L_{\rm BC}$ 均为 0 km, $\mu_{\rm a}$ 和 $\mu_{\rm b}$ 均为 0.1. 图 5 (a) 将 Z 基偏振编码、X 基偏振编码和相位编码下的误码率和探测器的品质因子的关系曲线整合在一起, 以便对三种编码方式的误码率进行对比. 由图 5 可知: Z 基偏振编码的误码率远小于 X 基偏振编码和相位编码下的误码率, 且三种编码方式的误码率受品质因子影响不大. 为了获知三种编码方式的误码率更细节的变化规律, 本文分别对三种编码方式的误码率曲线的纵轴进行了不同程度的放大, 如图 5 (b)—(d) 所示. 可以看出: 误码率随品质因子的增大而缓慢变大, 即单光子探测器的性能越差, 误码率越高.

图 6—图 8 分别给出了 Z 基偏振编码、X 基偏振编码以及相位编码系统不同反射率的误码率和传输距离 L 之间的关系. 为了体现短距离传输情况下的区别, 图 6 (b)、图 7 (b) 和图 8 (b) 分别给出了对应编码方式下局部放大的误码率变化关系. 此时, P 为 3.25×10^{-7}, $\mu_{\rm a}$ 和 $\mu_{\rm b}$ 都为 0.4, $L_{\rm AC}$ 和 $L_{\rm BC}$ 都为 L. 可知: 三种编码方式中, 在 Z 基和 X 基偏振编码条件下, $r=0.75$, $r=0.25$ 的误码率随距离的变化规律相同; 在相位编码的条件下, $r=0.75$ 时的误码率小于 $r=0.25$ 时的误码率, r 取 3 个不同值时所对应的误码率均随着传输距离的增加而不断增大, 最终接近 50%.

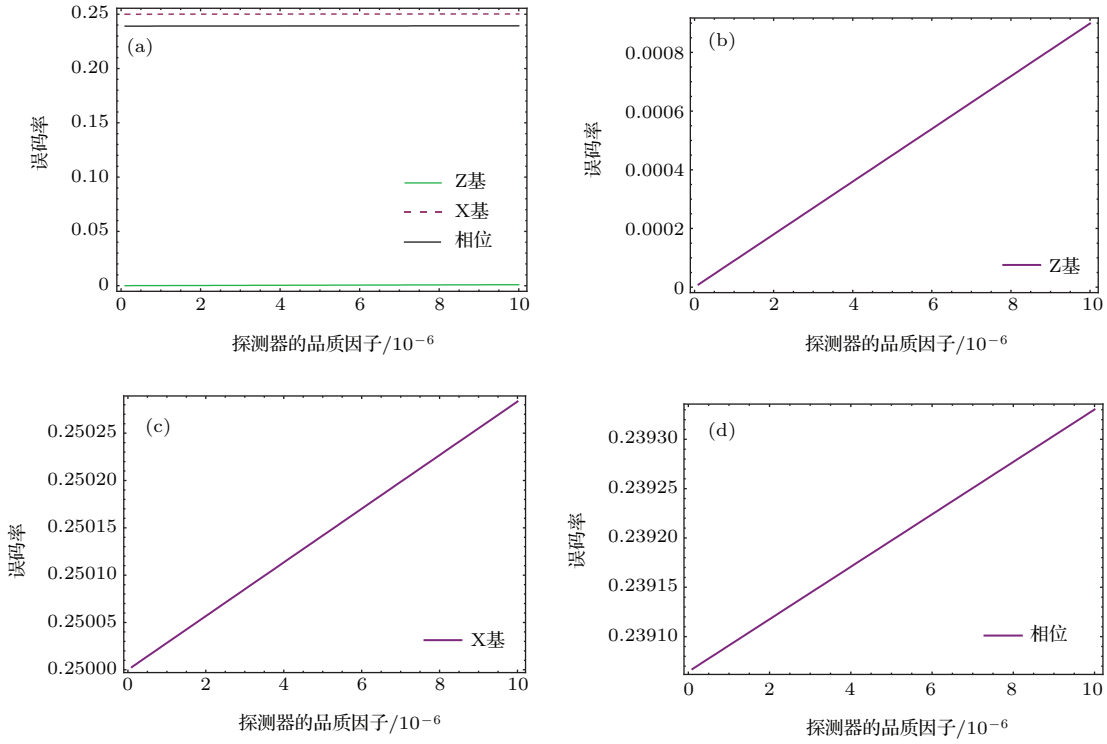

图 5 (网刊彩色) 误码率和探测器品质因子之间的关系 (a) Z 基、X 基和相位编码系统误码率对比关系; (b), (c) 和 (d) 分别为 Z 基、X 基和相位编码系统局部放大的误码率变化关系

Fig. 5. (color online) The relationship between the QBER and quality factor: (a) The correlation between the QBER of Z basis Systems, X basis Systems and the phase encoding systems; (b) the enlarged variable relationship of the QBER in Z basis encoding; (c) the enlarged variable relationship of the QBER in X basis encoding; (d) the enlarged variable relationship of the QBER in phase encoding.

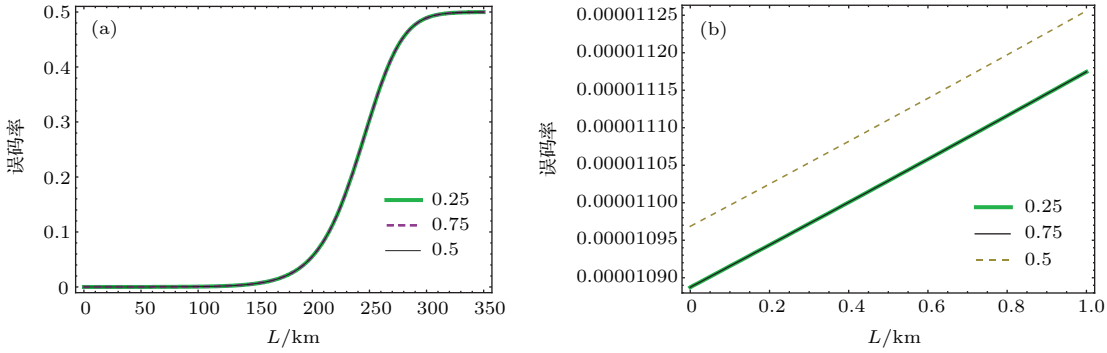

图 6 (网刊彩色) Z 基编码中不同反射率的误码率和传输距离之间的关系 (a) L 取值范围为 0—350 km, 三条线重合; (b) L 取值范围为 0—1 km, $r = 0.25$ 和 $r = 0.75$ 的曲线重合

Fig. 6. (color online) The relationship between the QBER of different reflectivity and transmission distance in Z basis encoding: (a) The range of L is 0 km to 350 km, the three lines are superimposed; (b) the range of L is 0 km to 1 km, the line of $r = 0.25$ superpose the line of $r = 0.75$.

图 9 (a) 给出了 Z 基、X 基和相位编码系统的误码率与通信双方所采用平均光子数的比值 k 的关系模拟曲线, 图 9 (b) 给出了 Z 基编码方式下局部放大的误码率与平均光子数的比值 k 之间的变化关系. 此时, P 为 3.25×10^{-7}, r 为 0.5, $L_{\rm AC}$ 和 $L_{\rm BC}$ 都为 0 km, $\mu_{\rm a}$ 和 $\mu_{\rm b}$ 分别为 0.1 和 $0.1k$. 由图 9 可知: 当通信双方采用的平均光子数相差不大时, 只有 Z 基偏振编码的误码率不能取到最小值.

由图 3 和图 9 比较可得: 在 Z 基编码中, 反射率和信道损耗对误码率的影响不能等同, 但是在 X 基编码和相位编码中, 两者对误码率的影响却能等同. 这主要是因为在偏振编码系统中, 偏振分束器是理想的, 能够完美地分开竖直偏振态和水平偏振态, 而在 X 基中, ±45° 投影到水平偏振态和竖直偏振态的概率都是 0.5.

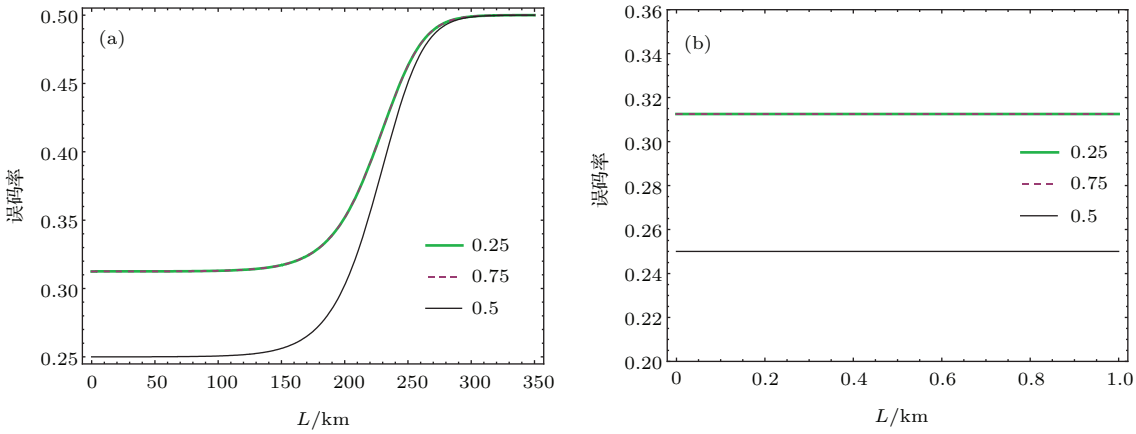

图 7 (网刊彩色) X 基编码中不同反射率的误码率和传输距离之间的关系 (a) L 的取值范围为 0—350 km, $r = 0.25$ 和 $r = 0.75$ 的曲线重合; (b) L 的取值范围为 0—1 km, $r = 0.25$ 和 $r = 0.75$ 的曲线重合

Fig. 7. (color online) The relationship between the QBER of different reflectivity and transmission distance in X basis encoding: (a) The range of L is 0 km to 350 km, the line of r =0.25 superpose the line of $r = 0.75$; (b) the range of L is 0 km to 1 km, the line of $r = 0.25$ superpose the line of $r = 0.75$.

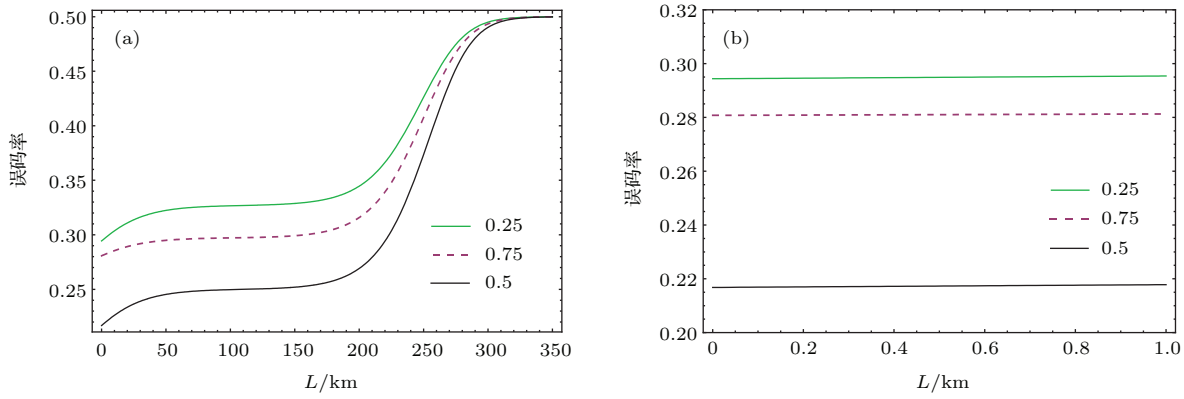

图 8 (网刊彩色) 相位编码中不同反射率的误码率和传输距离之间的关系 (a) L 的取值范围为 0—350 km; (b) L 的取值范围为 0—1 km

Fig. 8. (color online) The relationship between the QBER of different reflectivity and transmission distance in phase encoding: (a) The range of L is 0 km to 350 km; (b) the range of L is 0 km to 1 km.

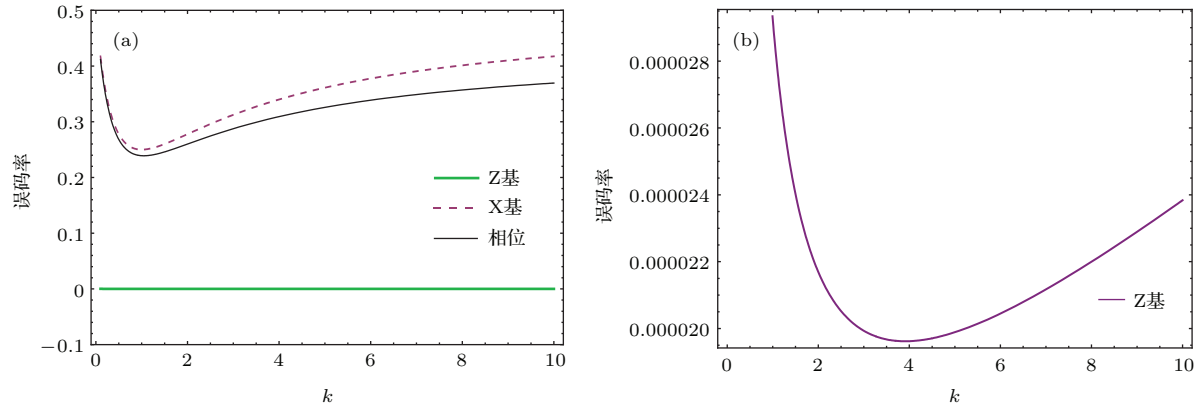

图 9 (网刊彩色) 误码率与通信双方所采用平均光子数的比值之间的关系 (a) Z 基, X 基, 相位; (b) Z 基编码方式下局部放大的误码率和平均光子数之间的关系

Fig. 9. (color online) The relationship between the QBER and the ratio of average photon number: (a) Z basis, X basis, phase; (b) the partial enlarged relationship between the QBER and the ratio of average photon number in Z basis encoding.

4 结 论

本文研究了在偏振编码和相位编码MDI-QKD系统中, 采用WCS光源产生的误码率与BS的反射率、单光子探测器品质因子、WCS的平均光子数以及不同折射率的误码率和距离之间的关系. 结果显示, 品质因子越大, 误码率越大; 当通信双方发送相同平均光子数的WCS脉冲时, 在X偏振编码和相位编码中, 误码率随 $\Delta = |r - 0.5|$ 变大而变大, 在 r 趋近于0.5时达到最小; 在Z基偏振编码中, 当通信双方采用的平均光子数成一定比例时, 误码率最小, 且误码率受BS反射率的影响不大; 对比得出: BS的反射率和通信双方发送的脉冲平均光子数, 两者对误码率的影响在Z基编码中不能等同. 本文结合BS反射率、探测器的品质因子、通信距离以及脉冲平均光子数等参数对误码率的变化规律进行了研究, 对实际搭建性能较好的MDI-QKD系统具有一定的参考价值.

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] 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 F, Chen T Y, Zhang Q, Pan J W 2015 *IEEE J. Select. Topics Quantum Electron.* **21** 6600407

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

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

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

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

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

[13] Qi B, Fung C H F, Lo H K, Ma X 2007 *Quantum Inf. Comput.* **7** 073

[14] Brassard G, Lutkenhaus N, Mor T, Sanders B C 2000 *Phys. Rev. Lett.* **85** 1330

[15] Sun S H, Liang L M 2012 *Appl. Phys. Lett.* **101** 071107

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

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

[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, Razavi M 2012 *Phys. Rev. A* **86** 062319

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

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

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

[24] Tang Z Y, Liao Z F, Xu F H, Qi B, Qian L, Lo H K 2014 *Phys. Rev. Lett.* **112** 190503

[25] 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 F, Chen T Y, Zhang Q, Pan J W 2015 *Phys. Rev. Lett.* **114** 069901

[26] Sun Y, Zhao S H, Dong C 2015 *Acta Phys. Sin.* **64** 140304 (in Chinese) [孙颖, 赵尚弘, 东晨 2015 物理学报 **64** 140304]

[27] 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]

[28] 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 F, Pelc J S, Fejer M M, Peng C Z, Zhang Q, Pan J W 2013 *Phys. Rev. Lett.* **111** 130502

[29] Sun S H, Gao M, Li C Y, Liang L M 2013 *Phys. Rev. A* **87** 052329

[30] Du Y N, Xie W Z, Jin X, Wang J D, Wei Z J, Qin X J, Zhao F, Zhang Z M 2015 *Acta Phys. Sin.* **64** 110301 (in Chinese) [杜亚男, 解文钟, 金璇, 王金东, 魏正军, 秦晓娟, 赵峰, 张智明 2015 物理学报 **64** 110301]

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

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

Analysis on performance optimization in measurement-device-independent quantum key distribution using weak coherent states*

Wu Cheng-Feng[1)] Du Ya-Nan[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 3 December 2015; revised manuscript received 12 February 2016)

Abstract

Measurement-device-independent quantum key distribution (MDI-QKD) is immune to all detection side-channel attacks, thus when combined with the decoy-state method, it can avoid the actual security loophole caused by quasi-single-photon source simultaneously. A practical weak coherent source is used as a quasi-single-photon source in the current MDI-QKD experiments; it may contain percentage of vacuum- and multi-photon pulses. Moreover, in order to study how the performance of the threshold detector affects the quantum bit error rate (QBER), we introduce the quality factor (the ratio of the dark count rate to the detection efficiency) of the threshold detector. Here, through taking into account the weak coherent source, the quality factor of the threshold detector and the reflectivity of beam splitter, we deduce and evaluate the gain, the probability for successful Bell measurement, incorrect Bell measurement when Alice and Bob send pulses with different photon numbers which have a high probability to appear in weak coherent source, and then we obtain QBER in combination with the probabilities of different photon number states, besides, we also do some simulations. The simulations show how QBER varies with the reflectivity of beam splitter and the quality factor of the threshold detector when the average photon numbers per pulse from Alice and Bob are symmetric. Furthermore, the simulations show how QBER varies with the average photon number per pulse from Alice when average photon number per pulse from Bob is 0.1. Result shows that QBER is affected by the reflectivity of beam splitter, but QBER cannot reach the minimum value in Z basis encoding scheme when the average photon numbers per pulse from Alice and Bob are both 0.1 and the reflectivity of beam splitter is 0.5, which is different from X basis encoding and phase encoding. In addition, QBER increases with the increase of the quality factor of the threshold detector, which means that better performance of the threshold detector will reduce QBER. We show that QBER in Z basis encoding reaches the minimum value when reflectivity of beam splitter is 0.5 and there is large difference between in average photon number per pulse between two sides. In conclusion, for QBER, the effect from the reflectivity of beam splitter is equal to average photon numbers from the two arms only in X basis encoding and phase encoding. Our work will provide a reference for setting up a system with better performance.

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

PACS: 03.67.Dd, 03.67.Hk **DOI:** 10.7498/aps.65.100302

* Project supported by the Major Research Plan of the National Natural Science Foundation of China (Grant No. 91121023), the National Natural Science Foundation of China (Grant Nos. 61378012, 11374107, 60978009, 61108039, 61401176, 61401262), the Natural Science Foundation of Guangdong Province, China (Grant Nos. 2014A030310205, 2015A030313388), the National Basic Research Program of China (Grant No. 2011CBA00200), the Science and Technology Planning Project of Guangdong Province, China (Grant No. 2014B090901016), and the Application-oriented Special Scientific Research Fund of Application Type of Guangdong Province, China (Grant No. 2015B010128012).

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