基于旋转不变态的测量设备无关量子密钥分配协议研究*

东晨[1)2)†] 赵尚弘[1)] 董毅[1)] 赵卫虎[1)] 赵静[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)

(2014 年 4 月 20 日收到; 2014 年 5 月 6 日收到修改稿)

本文提出了一种基于旋转不变态的偏振无关测量设备量子密钥分配协议, 既适用于偏振编码测量设备无关量子密钥分配系统, 也应用于相位编码测量设备无关量子密钥分配系统的相干过程. 通过在线偏振基进入信道传输前嵌入 2 块 q 玻片, 使得在传输过程中将线偏振基转化为旋转不变的圆偏振基, 而第三方对接收到的脉冲进行 Bell 态测量前, 利用 q 玻片的算符可逆性, 将圆偏振基还原为线偏振基进行测量, 可以有效消除信道传输中偏振旋转导致的误码. 本文分析了偏振无关的三诱骗态测量设备无关量子密钥分配系统的误码率, 研究了密钥生成率与安全传输距离的关系, 仿真结果表明, 对于偏振编码测量设备无关量子密钥分配系统, 该协议可以有效提高系统的最大安全通信距离, 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: 旋转不变态, 偏振无关, 测量设备无关量子密钥分配协议

PACS: 03.67.Dd **DOI:** 10.7498/aps.63.170303

1 引 言

量子密钥分配[1]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[5−9]. 最近, 为了克服探测设备的非完美性问题, Lo 小组[10]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 将光脉冲发送至非可信任的第三方进行 Bell 态测量, 根据第三方公布的 Bell 态测量结果, 进行相应的比特反转操作得到安全密钥. 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 通常使用弱相干光源代替单光子光源, 故实验中可结合诱骗态方法[11]有效的估计密钥生成率. 理论方面, Ma[12]、Wang[13]、Sun[14]等分析了 MDI-QKD 的统计波动问题; 实验方面, Liu[15], Tang 等[16]分别实现了相位编码和偏振编码的 MDI-QKD.

在基于偏振编码的 MDI-QKD 中, 由于存在光纤双折射、偏振模色散等效应, 使光子在传输过程中不可避免的造成偏振态旋转, 从而破坏了光子编码的信息, 导致系统的误码率升高[17].

本文提出了一种基于旋转不变态的偏振无关测量设备量子密钥分配协议, 既适用于偏振编码的测量设备无关量子密钥分配系统, 同时也可应用于相位编码测量设备无关量子密钥分配系统的相干过程. 在本文的改进方案中, 线偏振基进入信道传输前通过嵌入 2 块 q 玻片[18]使其转化为偏振旋转不变的圆偏振基, 即量子态的变化不受偏振态旋转角度的影响, 而在第三方接收到光脉冲进行 Bell 态测量前, 利用 q 玻片的算符可逆性[19], 将圆偏振基还原为线偏振基进行测量. 通过引入旋转不变的量子态, 本协议可以有效避免信道传输中偏振态旋转

* 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

造成的误差, 有效提高系统的最大安全通信距离与密钥生成率, 同时, 与经典的测量设备无关量子密钥分配协议的实验方案相比, 本协议只是在发送端和接收端间嵌入了4块q玻片, 使得本协议在实验中易于实现.

2 理论与计算公式

本文提出的偏振无关测量设备无关量子密钥分配协议如图1所示.

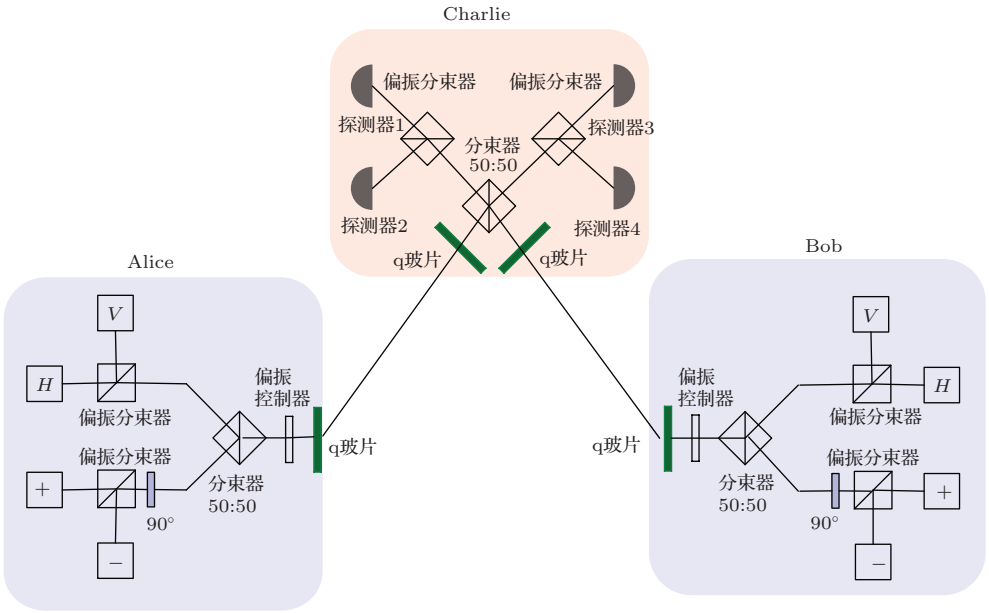

图1 偏振无关测量设备无关量子密钥分配协议

与经典的测量设备无关协议相比, 态制备过程相同, Alice和Bob发送的相干光脉冲进行偏振编码(选取Z基X基): $\{H,V\}^Z$, $\{+,-\}^X$ 其中

$$|+\rangle = 1/\sqrt{2}(|H\rangle + |V\rangle), |-\rangle = 1/\sqrt{2}(|H\rangle - |V\rangle).$$

Bell态测量过程也相同, 第三方通过分束器(BS)、偏振分束器(PBS)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公式[10]:

$$R = \mu_{\rm A}\mu_{\rm B}\,{\rm e}^{-(\mu_{\rm A}+\mu_{\rm B})}Y_Z^{11} \times [1 - H_2({\rm e}_X^{11})] - Q_Z f(E_Z)H_2(E_Z), \quad (1)$$

其中$Q_{\mu_i\nu_j}$和$E_{\mu_i\nu_j}$表示Alice脉冲强度为μ_i且Bob脉冲强度为ν_j时的增益和误码率, Z基用来产生安全密钥, X基作为测试集用来估计信道参数, 采用诱骗态方法有效估计单光子计数率Y_Z^{11}和单光子误码率e_X^{11}可以得到最终的密钥生成率. 而在信道传输过程中, 本文提出的改进方案在Alice和Bob完成信息编码过程后, 通过嵌入q玻片, 使得量子信道的信息载体由线偏振量子态$\{H,V\}^Z$, $\{+,-\}^X$转化为旋转不变的圆偏振量子态, q玻片的算符表示为

$$(\alpha|{\rm R}\rangle + \beta|{\rm L}\rangle)_\pi \otimes |0\rangle_{\rm O} \xrightarrow{\text{q-plate}} \alpha(|{\rm L}\rangle_\pi \otimes |r\rangle_{\rm O}) + \beta(|{\rm R}\rangle_\pi \otimes |l\rangle_{\rm O}), \quad (2)$$

其中式左边$(\alpha|{\rm R}\rangle + \beta|{\rm L}\rangle)_\pi$表示左旋圆偏振态和右旋圆偏振态的任意叠加态, 通过改变α,β可以获得各种偏振态的光, 例如取$\alpha=\beta=1/\sqrt{2}$, 可以得到水平线偏振态$|H\rangle_\pi$; $|0\rangle_{\rm O}$表示光脉冲的轨道角动量为0, 此时式左边可以视为圆偏振叠加态与0轨道角动量的混态; 式右边

$$\alpha(|{\rm L}\rangle_\pi \otimes |r\rangle_{\rm O}) + \beta(|{\rm R}\rangle_\pi \otimes |l\rangle_{\rm O})$$

表示2维Hilbert空间下偏振-轨道角动量的叠加态, 通过轨道角动量的变化$|l\rangle_{\rm O}$和$|r\rangle_{\rm O}$($|l\rangle_{\rm O}$和$|r\rangle_{\rm O}$为轨道角动量等于1时的特征态), 将圆偏振叠加态分解为纯左旋圆偏振态$|{\rm L}\rangle_\pi$和纯右旋圆偏振态$|{\rm R}\rangle_\pi$, 而纯圆偏振态为旋转不变量, 在传输过程中不受偏振旋转的影响. 对于量子密钥分配采用的4个线偏振基, 我们可以得到其经过q玻片后的偏振态为

$$|H\rangle_\pi \otimes |0\rangle_{\rm O} \xrightarrow{\text{q-plate}} \frac{1}{\sqrt{2}}(|{\rm L}\rangle\pi \otimes |r\rangle_{\rm O})$$

$$+\frac{1}{\sqrt{2}}(|\mathrm{R}\rangle_\pi\otimes|l\rangle_\mathrm{O}), \tag{3a}$$

$$|V\rangle_\pi\otimes|0\rangle_\mathrm{O}\xrightarrow{\text{q-plate}}\frac{i}{\sqrt{2}}(|\mathrm{L}\rangle_\pi\otimes|r\rangle_\mathrm{O})-\frac{i}{\sqrt{2}}|\mathrm{R}\rangle_\pi\otimes|l\rangle_\mathrm{O}, \tag{3b}$$

$$|+\rangle_\pi\otimes|0\rangle_\mathrm{O}\xrightarrow{\text{q-plate}}\frac{1+i}{\sqrt{2}}(|\mathrm{L}\rangle_\pi\otimes|r\rangle_\mathrm{O})+\frac{1-i}{\sqrt{2}}(|R\rangle_\pi\otimes|l\rangle_\mathrm{O}), \tag{3c}$$

$$|-\rangle_\pi\otimes|0\rangle_\mathrm{O}\xrightarrow{\text{q-plate}}\frac{1-i}{\sqrt{2}}(|\mathrm{L}\rangle_\pi\otimes|r\rangle_\mathrm{O})+\frac{1+i}{\sqrt{2}}(|\mathrm{R}\rangle_\pi\otimes|l\rangle_\mathrm{O}). \tag{3d}$$

此时, 线偏振基分别变为2维Hilbert空间下纯圆偏振态-轨道角动量混合基:

$$\{H,V\}^Z\xrightarrow{\text{q-plate}}\{|\mathrm{L}\rangle_\pi\otimes|r\rangle_\mathrm{O},|\mathrm{R}\rangle_\pi\otimes|l\rangle_\mathrm{O}\}, \tag{4a}$$

$$\{+,-\}^X\xrightarrow{\text{q-plate}}\frac{1}{\sqrt{2}}\{|\mathrm{L}\rangle_\pi\otimes|r\rangle_\mathrm{O}\pm|\mathrm{R}\rangle_\pi\otimes|l\rangle_\mathrm{O}\}. \tag{4b}$$

在第三方接收到光脉冲进行Bell态测量前, 利用q玻片的算符的可逆性:

$$|\mathrm{R}\rangle_\pi\otimes|0\rangle_\mathrm{O}\xrightarrow{\text{q-plate}}|\mathrm{L}\rangle_\pi\otimes|r\rangle_\mathrm{O}\xrightarrow{\text{q-plate}}|R\rangle_\pi\otimes|0\rangle_\mathrm{O}, \tag{5a}$$

$$|\mathrm{L}\rangle_\pi\otimes|0\rangle_\mathrm{O}\xrightarrow{\text{q-plate}}|\mathrm{R}\rangle_\pi\otimes|l\rangle_\mathrm{O}\xrightarrow{\text{q-plate}}|\mathrm{L}\rangle_\pi\otimes|0\rangle_\mathrm{O}. \tag{5b}$$

将2维Hilbert空间下纯圆偏振态-轨道角动量混合基还原为线偏振基:

$$\frac{1}{\sqrt{2}}(|\mathrm{L}\rangle_\pi\otimes|r\rangle_\mathrm{O})+\frac{1}{\sqrt{2}}(|\mathrm{R}\rangle_\pi\otimes|l\rangle_\mathrm{O})\xrightarrow{\text{q-plate}}\frac{1}{\sqrt{2}}(|\mathrm{R}\rangle_\pi\otimes|0\rangle_\mathrm{O})+\frac{1}{\sqrt{2}}(|\mathrm{L}\rangle_\pi\otimes|0\rangle_\mathrm{O})=|H\rangle_\pi\otimes|0\rangle_\mathrm{O}, \tag{6a}$$

$$\frac{i}{\sqrt{2}}(|\mathrm{L}\rangle_\pi\otimes|\mathrm{R}\rangle_\mathrm{O})-\frac{i}{\sqrt{2}}(|\mathrm{R}\rangle_\pi\otimes|l\rangle_\mathrm{O})\xrightarrow{\text{q-plate}}\frac{i}{\sqrt{2}}(|\mathrm{R}\rangle_\pi\otimes|0\rangle_\mathrm{O})-\frac{i}{\sqrt{2}}(|\mathrm{L}\rangle_\pi\otimes|0\rangle_\mathrm{O})=|V\rangle_\pi\otimes|0\rangle_\mathrm{O}, \tag{6b}$$

$$\frac{1+i}{\sqrt{2}}(|\mathrm{L}\rangle_\pi\otimes|r\rangle_\mathrm{O})+\frac{1-i}{\sqrt{2}}(|\mathrm{R}\rangle_\pi\otimes|l\rangle_\mathrm{O})\xrightarrow{\text{q-plate}}\frac{1+i}{\sqrt{2}}(|\mathrm{R}\rangle_\pi\otimes|0\rangle_\mathrm{O})+\frac{1-i}{\sqrt{2}}(|\mathrm{L}\rangle_\pi\otimes|0\rangle_\mathrm{O})=|+\rangle_\pi\otimes|0\rangle_\mathrm{O}, \tag{6c}$$

$$\frac{1+i}{\sqrt{2}}(|\mathrm{L}\rangle_\pi\otimes|r\rangle_\mathrm{O})+\frac{1-i}{\sqrt{2}}(|\mathrm{R}\rangle_\pi\otimes|l\rangle_\mathrm{O})\xrightarrow{\text{q-plate}}\frac{1+i}{\sqrt{2}}(|\mathrm{R}\rangle_\pi\otimes|0\rangle_\mathrm{O})+\frac{1-i}{\sqrt{2}}(|\mathrm{L}\rangle_\pi\otimes|0\rangle_\mathrm{O})=|-\rangle_\pi\otimes|0\rangle_\mathrm{O}. \tag{6d}$$

采用文献[20]提出的2维幺正矩阵偏振态旋转误差模型:

$$U_k=\begin{pmatrix}\cos\theta_k & -\sin\theta_k\\ \sin\theta_k & \cos\theta_k\end{pmatrix}, \tag{7}$$

其中$k=\mathrm{A},\mathrm{B}$分别表示Alice和Bob到第三方的信道传输, θ_k表示偏振旋转角度, 分别得到偏振旋转造成的单边误码率为

$$e_k=\sin^2\theta_k. \tag{8}$$

求和得到总误码率为

$$e_\mathrm{d}=e_\mathrm{A}+e_\mathrm{B}. \tag{9}$$

本文只考虑暗记数率和偏振旋转误码对系统的影响, 忽略统计波动等其他误码源. 利用文献[20]的估计方法, 可以推出偏振无关测量设备无关量子密钥分配协议的单光子计数率Y_Z^{11}和误码率e_X^{11}为

$$Y_Z^{11}=(1-Y_0)^2\left[4Y_0^2(1-t_\mathrm{A}\eta_\mathrm{d})(1-t_\mathrm{B}\eta_\mathrm{d})+2Y_0\times\left(t_\mathrm{A}\eta_\mathrm{d}+t_\mathrm{B}\eta_\mathrm{d}-\frac{3t_\mathrm{A}t_\mathrm{B}\eta_\mathrm{d}^2}{2}\right)-\frac{t_\mathrm{A}t_\mathrm{B}\eta_\mathrm{d}^2}{2}\right], \tag{10a}$$

$$e_X^{11}=\frac{1}{2}-\frac{t_\mathrm{A}t_\mathrm{B}\eta_\mathrm{d}^2(1-Y_0)^2}{4Y_X^{11}}, \tag{10b}$$

其中$Y_Z^{11}=Y_X^{11}$.

3 仿真结果与分析

根据(7)式、(8)式和(9)式可以估计出信道传输过程中偏振旋转角对误码率的影响; 将(10a)式、(10b)式代入(1)式可以偏振无关测量设备无关量子密钥分配系统安全密钥生成率与安全传输距离之间的关系, 主要仿真参数如表1所示.

表1 主要仿真参数设置

文献[21]	η_d/%	Y_0	f
	14.5	3×10^{-6}	1.16

如图2所示, 当偏振旋转角超过15°时, 造成的误码率将超过密钥分配协议安全性对误码率的最

低要求11%, 此时通信双方得到的比特流将无法提取出安全密钥.

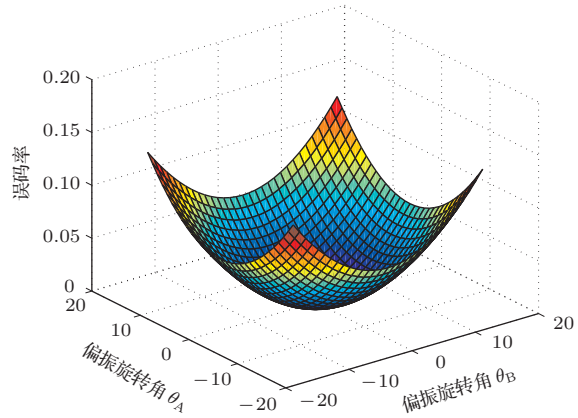

图2 误码率与偏振偏转角的关系

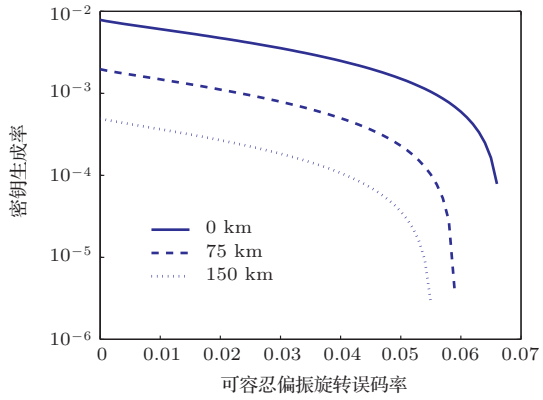

图3 密钥生成率与可容忍偏振旋转误码率关系

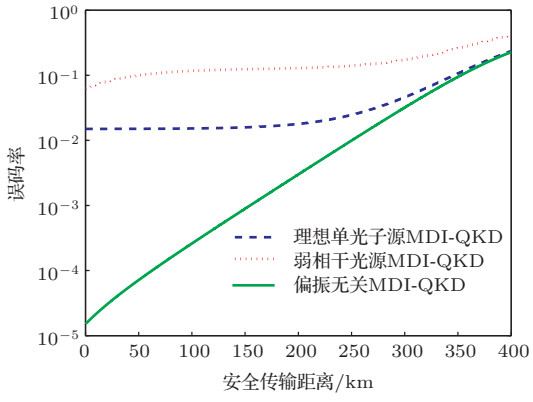

图4 误码率与安全传输距离的关系

如图3所示, 对于基于偏振编码的测量设备无关量子密钥分配系统, 随着可容忍偏振不匹配误码率的增加, 密钥生成率下降较快, 表明偏振编码的测量设备无关量子密钥分配系统对偏振旋转造成误码是比较敏感的.

如图4所示, 由于降低了信道传输中偏振不匹配导致的误码率, 使得偏振无关测量设备量子密钥分配协议的单光子误码率远远低于经典测量设备量子密钥分配协议, 但随着传输距离的增加, 单光子计数率衰减称为影响误码率的主要因素, 使得该协议的误码率迅速上升, 逼近理想单光子源协议的误码率. 如图5所示, 对于偏振编码测量设备无关量子密钥分配系统, 本文的改进方案的最大安全传输距离可以达到355 km, 远远高于经典弱相干光源协议的242 km.

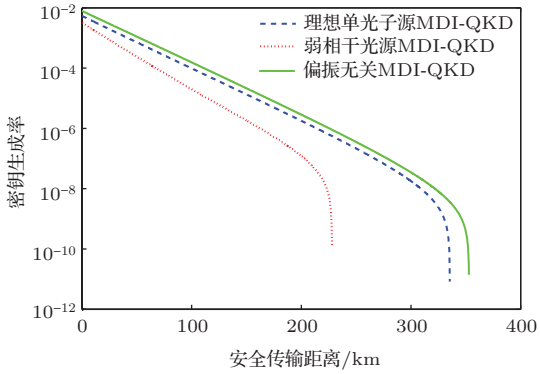

图5 密钥生成率与安全传输距离的关系

4 结 论

本文提出了一种基于旋转不变态的偏振无关测量设备量子密钥分配协议, 既适用于偏振编码测量设备无关量子密钥分配系统, 也应用于相位编码测量设备无关量子密钥分配系统的相干过程. 通过在线偏振基进入信道传输前嵌入2块q玻片, 使得线偏振基转化为圆偏振基, 在传输过程中圆偏振基为旋转不变态, 第三方对接收到的脉冲进行Bell态测量前, 利用q玻片的算符可逆性, 将圆偏振基还原为线偏振基进行测量, 可以有效消除信道传输中偏振旋转导致的误码. 仿真结果表明, 对于偏振编码测量设备无关量子密钥分配系统, 该协议可以有效的消除信道传输中偏振旋转导致的误码, 有效提高系统的最大安全通信距离, 为实用的量子密钥分配实验提供了重要的理论参数.

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 K H, Lutkenhaus N, Preskill J 2004 *Quantum Infor. Comput.* **4** 325-360
[5] Zhou Y Y, Zhou X T, Tian P G, Wang Y J 2013 *Chin.it 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] Jiao R Z, Zhang W H 2009 *Acta Phys. Sin.* **58** 2189 (in Chinese) [焦荣珍, 张文瀚 2009 物理学报 **58** 2189]
[8] Dong C, Zhao S H, Zhao W H, Shi L, Dong Y 2014 *Acta Phys. Sin.* **63** 030302 (in Chinese) [东晨, 赵尚弘, 赵卫虎, 石磊, 董毅 2014 物理学报 **63** 030302]
[9] 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]
[10] H K Lo, M Curty, B Qi 2012 *Phys. Rev. Lett.* **108** 130503
[11] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901
[12] Ma X F, Fung C H F, Razavi M 2012 *Phys. Rev. A* **86** 052305
[13] Wang X B 2013 *Phys. Rev. A* **87** 012320
[14] Sun S H, Gao M, Li C Y, Liang L M 2013 *Phys. Rev. A.* **87** 052329
[15] 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
[16] Tang Z, Liao Z, Xu F, Qi B, Qian L, Lo H K 2013 arXiv:13066134
[17] Tang Z L, Li M, Wei Z J, Lu F, Liao C J, Liu S H 2005 *Acta Phys. Sin.* **54** 2534 (in Chinese) [唐志列, 李铭, 魏正军, 卢非, 廖常俊, 刘颂豪 2005 物理学报 **54** 2534]
[18] Piccirillo B, Dambrosio V, Slussarenko S, Marrucci L, Santamato E 2010 *Appl. Phys. Lett.* **97** 241104
[19] Slussarenko S, Murauski A, Du T, Marrucci L, Santamato E 2011 *Opt. Exp.* **19** 4085
[20] Xu F H, Curty M, Qi B, Lo H K 2013 *New J. of Phys.* **15** 113007
[21] Ma X F, Razavi M 2012 *Phys. Rev. A* **86** 062319

Measurement of device-independent quantum key distribution for the rotation invariant photonic state*

Dong Chen[1)2)†] Zhao Shang-Hong[1)] Dong Yi[1)] Zhao Wei-Hu[1)] Zhao Jing[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 20 April 2014; revised manuscript received 6 May 2014)

Abstract

The original measurement of device-independent(MDI)quantum key distribution(QKD) is reviewed, and a modified protocol using rotation- invariant photonic state is proposed. Initial encoding and final decoding of information in our MDI-QKD implementation protocol can be conveniently performed in the polarization space, while the transmission is done in the rotation-invariant hybrid space. Our analysis indicates that both the secure key rate and transmission distance can be improved by our modified protocol owing to its lower error rate. Furthermore, our hybrid polarization-OAM qubits approach only needs to insert four q-plates in a practical experiment, and our simulation results show that the modified protocol is practical.

Keywords: rotation invariant photonic state, polarization independent, measurement device-independent quantum key distribution

PACS: 03.67.Dd **DOI:** 10.7498/aps.63.170303

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

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