基于不同介质间量子密钥分发的研究*

周飞[1)] 雍海林[2)] 李东东[2)] 印娟[2)] 任继刚[2)] 彭承志[2)†]

1) (清华大学物理系, 低维量子物理国家重点实验室, 北京 100084)

2) (中国科学技术大学, 微尺度物质科学国家实验室, 合肥 230026)

(2014 年 5 月 26 日收到; 2014 年 5 月 28 日收到修改稿)

文章主要解决了偏振编码的光子在不同介质间进行量子密钥分发的问题, 定量地分析了光子不同分量的不同透过率引起的误码率问题, 并实际分析了空气-水介质间量子密钥分发引起的误码率. 进一步给出了可以消除这种非理想 BB84 协议的单光子补偿方案, 以及可以采用更加鲁棒、实用性的抗界面非幺正噪声的双光子编码方案, 从而为未来实现全地域广域量子通信迈出了重要的一步.

关键词: 量子密钥分发, 不同介质, 菲涅耳公式, 误码率

PACS: 03.67.Dd, 03.67.Hk **DOI:** 10.7498/aps.63.140303

1 引 言

量子密钥分发[1,2]作为量子信息学科最有可能走向实用化的一个领域, 它的目的是在遥远的两地 (Alice 和 Bob) 共享一组绝对安全的密钥. 和传统的保密技术相比, 其最大的优势是由量子力学基本原理保证的安全性, 因此量子密钥分发从出现伊始就成为人们研究的热点. 从最初的理想的 BB84 协议[1]提出以来, 不管在理论上还是在实验上, 量子密钥分发都取得了很大的进展[2−11]. 量子密钥分发的研究最主要集中于安全性[12−15]和分发距离的扩展[7−10,16−18]两方面, 最近的研究成果[19,20]表明量子密钥分发已经接近于大规模实用化的阶段, 而且通过有效的高损耗模拟信道[21], 未来也将实现空间上的星地量子通信. 但是目前针对量子密钥分发的研究, 基本上都是基于均匀或类似于均匀介质中的, 或者在光纤中或者在自由空间大气条件下, 而基于不同介质间的量子密钥分发的研究目前还比较少. 在量子密钥分发实用化的过程中, 免不了会有不同介质之间量子密钥分发的问题, 例如水上舰船或者飞机卫星和水下的潜艇之间穿透不同介质的量子密钥分发. 一个重要且绕不过去的问题是要考虑空气-水界面这种不同介质界面上对光子偏振的影响, 从而导致对于整个量子密钥分发过程的影响.

本文主要讨论了不同介质间的量子密钥分发过程, 考虑了水-空气界面对光偏振编码的影响. 由于光子偏振态在空气中或是在水中都相对稳定, 可以用光子的偏振自由度来进行编码. 当采用理想的 BB84 协议进行不同介质间的量子密钥分发时, 因不同的偏振光在不同介质界面上, 透射率会随着入射角变化, 从而影响光子的偏振产生误码, 使最终成码率下降. 本文第 2 部分定量地计算了不同介质界面的影响; 第 3 部分提出了单光子补偿方案可以消除这种影响; 另外, 还提出了一种基于消相干子空间的抗界面非幺正噪声的双光子编码方案, 这种方案可以完全避免这类影响; 随后, 给出了基于这一理论的可行的实验方案.

2 理论分析

首先考虑在不同介质间光子传播的情况, 如光在不同介质中传播时, 在介质表面会发生反射和折射, 如图 1 所示. 有波矢量 $\boldsymbol{k}$ 的光从折射率为

* 国家自然科学基金 (批准号: 61078012) 资助的课题.

† 通讯作者. E-mail: pcz@ustc.edu.cn

n_1 的介质中以角度 θ_1 入射到折射率为 n_2 的介质中, 经反射和折射, 其中折射角为 θ_2, 根据菲涅耳公式 [22], 可以分别求得其 p 分量和 s 分量的反射率和透射率 r_p, t_p 和 r_s, t_s.

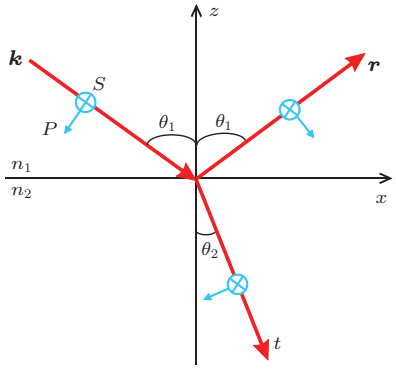

图 1 光子传输示意图

设光的 p 分量和 s 分量的振幅透射率分别为 t_p 和 t_s, 即有

$$t_p = \frac{2\sin\theta_2\cos\theta_1}{\sin(\theta_1+\theta_2)\cos(\theta_1-\theta_2)}, \tag{1}$$

$$t_s = \frac{2\sin\theta_2\cos\theta_1}{\sin(\theta_1+\theta_2)}, \tag{2}$$

又有

$$\frac{n_2}{n_1} = \frac{\sin\theta_1}{\sin\theta_2}. \tag{3}$$

根据 (1)、(2)、(3) 式, s 分量和 p 分量的振幅透射率比值 r 有:

$$r = \frac{t_s}{t_p} = \cos\theta_1\sqrt{1-\left(\frac{n_1\sin\theta_1}{n_2}\right)^2} + \sin\theta_1\frac{n_1\sin\theta_1}{n_2}. \tag{4}$$

当 $\theta_1 = 0°$ 时, $r = 1$ 即 $t_s = t_p$, $0° < \theta_1 < 90°$ 时, $0 < t_s < t_p$. 在上述折射光路中不存在位相的变化, 将具有确定偏振的光子态投影至 s 和 p 这两个方向 $\alpha|p> + \beta|s>$ ($\alpha\beta$ 为复数), 则其透射后光子态为 $\alpha t_p|p> + \beta t_s|s>$ (未归一化), 由上可知, 一般情形下, 两分量的透射率不一致 $t_p \neq t_s$, 对于 $\alpha\beta \neq 0$ 的光子, 其偏振态将发生改变.

如考虑最简单的情形, 我们选择 BB84 协议中的 4 个编码态为 $|p>$, $|s>$, $(|p> + |s>)/\sqrt{2}$ 和 $(|p> - |s>)/\sqrt{2}$ (对应 BB84 协议中的 H、V、+、− 四态). 这样, 经过不同介质分界面后, 后两者的状态会变为

$$(t_p|p> + t_s|s>)\Big/\sqrt{t_p^2+t_s^2},$$

$$(t_p|p> - t_s|s>)\Big/\sqrt{t_p^2+t_s^2},$$

容易看出, 这一变换是非幺正的变换, 且会导致误码率上升, 这种变换是无法用普通的波片或者调制晶体 [23] 补偿, 从而最终影响成码率和安全传输距离.

在理想条件下, 对于两对正交基矢变换前后, 态改变引起的误码率可以由下面计算式得到: 对于一组正交基矢 $|a>$, $|b>$ 的基矢误码率应该为

$$q_{ab} = \frac{(\langle a|b'\rangle)^2 + (\langle b|a'\rangle)^2}{(\langle a|a'\rangle)^2 + (\langle b|b'\rangle)^2 + (\langle a|b'\rangle)^2 + (\langle b|a'\rangle)^2},$$

其中, $|a'>$, $|b'>$ 分别表示 $|a>$, $|b>$ 透射后的偏振态.

由此得到 $|p>$, $|s>$ 基矢条件下, 态不发生变化, 其误码率不发生变化, 可选为 0; 而对于 $(|p> + |s>)/\sqrt{2}$ 和 $(|p> - |s>)/\sqrt{2}$ 基矢下, 非幺正变换引起的误码率 $q_\pm$ 变化为

$$q_\pm = \frac{(t_p - t_s)^2}{2(t_p^2+t_s^2)}. \tag{5}$$

由此可见, 该基矢条件下误码率与两分量的透射率相关, 由于透射率大于 0, 误码率才会有意义, 故不考虑全反射的情形, 即 $t_p > 0$, $t_s > 0$. 一般来说, $t_p \geqslant t_s > 0$, 联立 (4) 式, 我们可以得到

$$q_\pm = \frac{(1-r)^2}{2(1+r^2)}. \tag{6}$$

当取 $0° < \theta_1 < 90°$, 根据 (6) 式可得到, $(|p> + |s>)/\sqrt{2}$ 和 $(|p> - |s>)/\sqrt{2}$ 基矢下误码率 $q_\pm$ 和两分量透射率比值 r 的关系如图 2 所示.

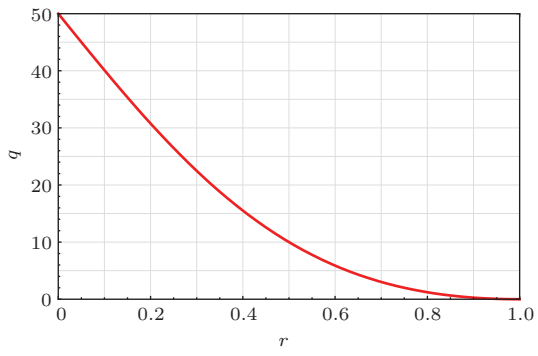

图 2 误码率 $q_\pm$ 与 r 的关系曲线

由图 2 可见, 当比值大于 0.7 时, 误码率较小, 低于 2%; 而当比值小于 0.5 时, 误码率上升较快. 当比值趋于 0 时, 对于发射任意偏振态光子, 透过的光的偏振趋于 $|p>$ 或 $|s>$ 态, 误码率自然趋于 50%.

对于一般的BB84协议的量子密钥分发系统, 其安全成码率 R 可写成:

$$R = 1 - H_2(q_b) - H_2(q_p), \tag{7}$$

q_b, q_p 分别对应同一测量基矢下的比特误码率和相位误码率, $H_2(q_b)$ 和 $H_2(q_p)$ 表示二元香农熵函数. 这里考虑比特误码率基本不发生变化, 理想条件下取为0, 相位误码由 (6) 式可得到, 即可简单得到最终成码率与透过率比值 r 之间的关系, 如图3 所示.

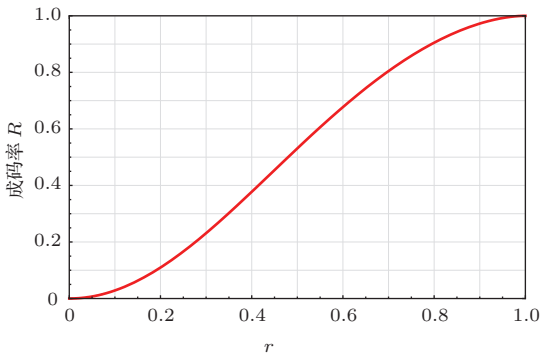

图3 最终成码率与 r 的关系曲线

3 实验方案及模型

3.1 光在空气-水介质之间传输

根据上述分析结果, 由 (4),(6) 式, 对于光从空气进入水中和从水中进入空气两种情形, 分别分析如下 (空气和水的折射率分别取为: $n_{\text{air}} = 1$, $n_{\text{water}} = 1.33$), 如图4 所示.

其中, 两种情形的布鲁斯特角分别为: $\theta_B = 53.1°$ 和 $\theta'_B = 36.9°$. 后者由于光子是从高折射率介质进入低折射率介质中, 当入射角 θ_i 大于临界角 θ_c ($\theta_i > \theta_c = 48.8°$) 时, 会发生全反射, 此时, 光子将无法进入穿过介质面. 我们发现这种情况下, 两透射率较为接近, 比值较接近于1. 当从空气入射水面时, 在入射角大于 75° 时, 误码率开始增加较快; 而从水进入空气时, 在非常接近于全反射临界角时, 误码率也开始迅速增加. 图4 中 T_p, T_s 表示透射光 p 和 s 分量的能流透射率 [22].

3.2 解决方案

3.2.1 单光子补偿方案

由上述推理可见, 对于原始的偏振编码的BB84协议量子密钥分发, 一般偏振态在传输过程中会发生改变, 使得原本正交的一组基矢不再正交, 产生误码率, 从而带来安全隐患. 为利用理想条件下BB84协议方案, 我们在进行不同介质间量子密钥分发时, 可以补偿使得发射的四态为 $|p>$, $|s>$, $(t_s|p> + t_p|s>)\Big/\sqrt{t_p^2 + t_s^2}$, $(t_s|p> - t_p|s>)\Big/\sqrt{t_p^2 + t_s^2}$ 一组正交态和一组非正交态, 则经过界面折射之后, 四态分别变为 $|p>$, $|s>$, $(|p> + |s>)/\sqrt{2}$ 和 $(|p> - |s>)/\sqrt{2}$ 两组正交态, 从而在进行两对正交基矢探测时, 不会因为界面而引入误码, 从而遵照理想BB84协议方案计算最终成码.

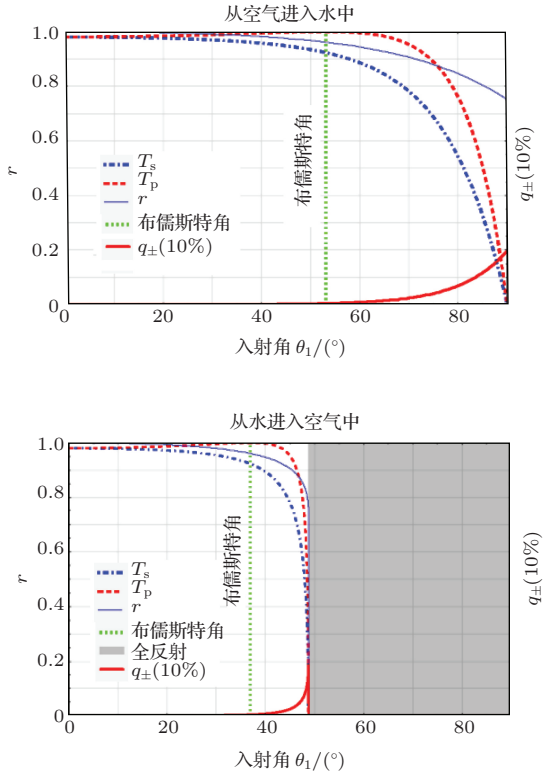

图4 (网刊彩色) r 和误码率 $q_{\pm}$ 与入射角 θ_1 的关系

另外, 我们也可以通过在接收端加以衰减补偿的方式使得编码的四态满足BB84协议中的要求, 如在通道效率一定的情况下, 可以考虑在接收端进行针对性的补偿, 根据不同透射率, 使信号光在接收端再通过一套器件, 该套器件对于 $|p>$, $|s>$ 的透过率分别为: r, 1.

3.2.2 双光子抗噪声方案

我们可以通过简单的单光子补偿方案来消除介质界面不同透射率的影响, 但在实际操作中, 因补偿系数会随着光的入射角度和介质的折射率变化而变化, 所以当界面存在波动或者光入射发生波动时, 需要实时的动态系统来进行单光子的补偿,

在某种程度上给系统带来了一定的复杂性. 为了抵抗介质界面对光子偏振的非幺正影响, 我们可以选择双光子态作为编码态, 选择双量子比特的子空间 $S = \{|sp>, |ps>\}$ 作为编码空间. 对应于原始的BB84方案, 令 $|H> \to |sp>$, $|V> \to |ps>$, 类似消相干子空间抗噪声方案[24,25], 我们可以让Alice随机在以下4个双量子比特态中选择1个, 发送至Bob: $|sp>$, $|ps>$, $\Phi_\pm = (|sp> \pm |ps>)/\sqrt{2}$.

则对于不同介质带来的联合噪声 T, 有:

$$\begin{aligned} T^{\otimes 2}|ps> &= T^p|p> \otimes T^s|s> \\ &= t_p t_s |ps>, \quad \propto |ps>, \\ T^{\otimes 2}|sp> &= T^s|s> \otimes T^p|p> \\ &= t_p t_s |sp>, \quad \propto |sp>, \end{aligned}$$

$$\begin{aligned} T^{\otimes 2}\Phi_\pm &= (T^p T^s|sp> \pm T^p T^s|ps>)/\sqrt{2} \\ &= t_p t_s \Phi_\pm, \quad \propto \Phi_\pm. \end{aligned}$$

可见, 此双光子编码经过不同介质界面的影响后, 不会改变编码态本身, 只会受到双光子传输效率的影响, 效率为 $\eta = T_p T_s$, 所以这是一种能很好地抗界面非幺正噪声的量子密钥分发方案. 而且, 值得注意的是, 在真实环境下, 介质间的入射角往往会发生变化(如海浪、潮汐等), 这种方案还能实时抑制变化角度对偏振误码的影响.

3.2.3 双光子实验模型

利用现有实验技术和理论分析, 我们可以进行相应的双光子编码抗界面噪声实验, 实验装置示意图见图5.

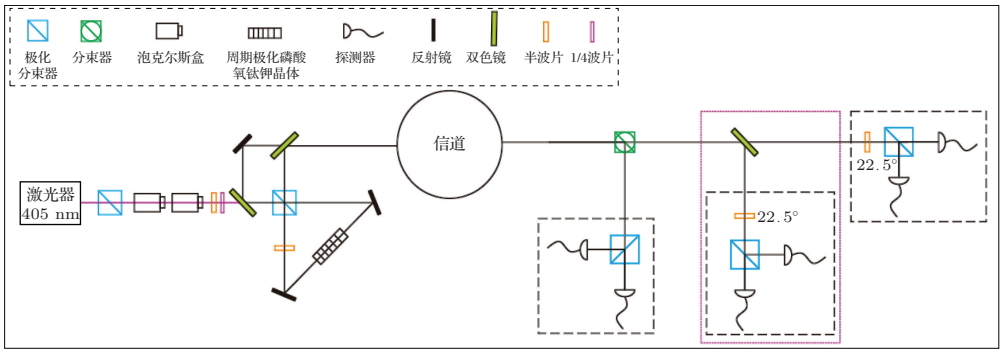

图5 抗界面非幺正噪声的双光子编码实验示意图

在图5中, 可以采用两个泡克尔斯盒偏振调制, 通过不简并的参量光产生如前文中所述四种编码形式的双光子态, 经过噪声通道, 采用被动基矢选择进行符合测量, 最后通过误码率证明此双光子编码可以实现基于消相干子空间的抗界面非幺正噪声.

4 结论与展望

我们主要考虑了在不同介质间进行基于光子偏振编码的BB84协议的量子密钥分发方案. 通过定量分析误码率与不同光分量透过率比值之间的关系, 以及不同光入射角与透过率比值的关系, 计算了不同介质间、不同入射角度下量子密钥分发的相关问题. 在此基础上, 我们还给出了利用理想BB84协议时的单光子补偿方案和基于消相干子空间的抗界面非幺正噪声的双光子编码方案. 我们的方案将有力推动未来实现海陆空一体化广域量子通信的技术发展, 从而使量子通信技术能更快、更好地登上实用化的巅峰.

参考文献

[1] Bennett C H, Brassard G 1984 *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* Bangalore, India, 12–15, December 1984 p175

[2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661

[3] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503

[4] Lo H K, Ma X F, Chen K 2005 *Phys. Rev. Lett.* **94** 230504

[5] Ma X F, Qi B, Zhao Y, Lo H K 2005 *Phys. Rev. A* **72** 012326

[6] Zhao Y, Qi B, Ma X F, Lo H K, Qian L 2006 *Phys. Rev. Lett.* **96** 070502

[7] Peng C Z, Zhang J, Yang D, Gao W B, Ma H X, Yin H, Zeng H P, Yang T, Wang X B, Pan J W 2007 *Phys. Rev. Lett.* **98** 010505

[8] Rosenberg D, Harrington J W, Rice P R, Hiskett P A, Peterson C G, Hughes R J, Lita A E, Nam S W, Nordholt J E 2007 *Phys. Rev. Lett.* **98** 010503

[9] Schmitt-Manderbach T, Weier H, Fürst M, Ursin R, Tiefenbacher F, Scheidl T, Perdigues J, Sodnik Z, Kurtsiefer C, Rarity J G, Zeilinger A, Weinfurter H 2007 *Phys. Rev. Lett.* **98** 010504

[10] Yuan Z L, Sharpe A W, Shields A J 2007 *Appl. Phys. Lett.* **90** 011118

[11] Wang Q, Chen W, Xavier G, Swillo M, Zhang T, Sauge S, Tengner M, Han Z F, Guo G C, Karlsson A 2008 *Phys. Rev. Lett.* **100** 090501

[12] Lo H K, Lütkenhaus N 2007 *Phys. Canada* **63** 191

[13] Gottesman D, Lo H K, Lütkenhaus N, Preskill J 2004 *Quantum Inf. Comput.* **4** 325

[14] Inamori H, Lütkenhaus N, Mayers D 2007 *European Phys. J. D* **41** 599

[15] Brassard G, Lütkenhaus N, Mor T, Sanders B C 2000 *Advances in Cryptology-Eurocrypt* **1807** 289

[16] Takesue H, Nam S W, Zhang Q, Hadfield R H, Honjo T, Tamaki K, Yamamoto Y 2007 *Nat. Photonics* **1** 343

[17] Liu Y, Chen T Y, Wang J, Cai W Q, Wan X, Chen L K, Wang J H, Liu S B, Liang H, Yang L, Peng C Z, Chen K, Chen Z B, Pan J W 2010 *Opt. Express* **18** 8587

[18] Wang S, Chen W, Guo J F, Yin Z Q, Li H W, Zhou Z, Guo G C, Han Z F 2012 *Opt. Lett.* **37** 1008

[19] Chen T Y, Liang H, Liu Y, Cai W Q, Ju L, Liu W Y, Wang J, Yin H, Chen K, Chen Z B, Peng C Z, Pan J W 2009 *Opt. Express* **17** 6540

[20] Chen T Y, Wang J, Liang H, Liu W Y, Liu Y, Jiang X, Wang Y, Wan X, Cai W Q, Ju L, Chen L K, Wang L J, Gao Y, Chen K, Peng C Z, Chen Z B, Pan J W 2010 *Opt. Express* **18** 27217

[21] Yin J, Yong H L, Wu Y P, Peng C Z 2011 *Acta Phys. Sin.* **60** 060307 (in Chinese) [印娟, 雍海林, 吴裕平, 彭承志 2011 物理学报 **60** 060307]

[22] Zhao K H, Zhong X H 1984 *Optics* (Vol. 1) (Beijing: Peking University Press) p248 (in Chinese) [赵凯华, 钟锡华 1984 光学 [上册] (北京: 北京大学出版社) 第 248 页]

[23] Yin J, Ren J G, Lu H, Cao Y, Yong H L, Wu Y P, Liu C, Liao S K, Zhou F, Jiang Y, Cai X D, Xu P, Pan G S, Jia J J, Huang Y M, Yin H, Wang J Y, Chen Y A, Peng C Z, Pan J W 2012 *Nature* **488** 185

[24] Wang X B 2005 *Phys. Rev. A* **72** 050304

[25] Zhang Q, Yin J, Chen T Y, Lu S, Zhang J, Li X Q, Yang T, Wang X B, Pan J W 2006 *Phys. Rev. A* **73** 020301

Study on quantum key distribution between different media*

Zhou Fei[1)] Yong Hai-Lin[2)] Li Dong-Dong[2)] Yin Juan[2)]
Ren Ji-Gang[2)] Peng Cheng-Zhi[2)†]

1) (*Department of Physics and State Key Laboratory of Low Dimensional Quantum Physics, Tsinghua University, Beijing 100084, China*)

2) (*National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei 230026, China*)

(Received 26 May 2014; revised manuscript received 28 May 2014)

Abstract

This paper mainly solves the photon polarization encoding problem of quantum key distribution (QKD) between different media. The influence of the transmission rate of different photon component on quantum bit error rate (QBER) has been quantitatively analyzed, with a practical analysis of QBER of QKD between air and water. Furthermore, we have put forward a single-photon compensation scheme for eliminating such non-ideal BB84 protocol, as well as a more robust and practical dual-photon encoding scheme to offset such interfacial non-unitary noise. This takes an important step towards the air-sea-ground wide area quantum communication in the future.

Keywords: quantum key distribution, different media, Fresnel's formula, quantum bit error rate

PACS: 03.67.Dd, 03.67.Hk **DOI:** 10.7498/aps.63.140303

* Project supported by the National Natural Science Foundation of China (Grant No. 61078012).

† Corresponding author. E-mail: pcz@ustc.edu.cn