第 58 卷 第 3 期/2021 年 2 月/激光与光电子学进展 研究论文

激光与光电子学进展

接收端基矢旋转对星舰量子密钥分发的影响

聂敏[1]，张帆[1*]，杨光[1,2]，张美玲[1]，孙爱晶[1]，裴昌幸[3]

[1]西安邮电大学通信与信息工程学院，陕西 西安 710121；

[2]西北工业大学电子信息工程学院，陕西 西安 710072；

[3]西安电子科技大学综合业务网国家重点实验室，陕西 西安 710071

摘要 在星舰量子密钥分发系统中，发送量子密钥的量子卫星是低轨道卫星，追踪量子卫星的接收设备安装在船舰上。接收设备需要追踪卫星的运动，接收端基矢不可避免地会发生旋转。分析了导致基矢旋转的原因，针对BB84协议，建立了基矢旋转角与量子误码率、获取信息量的定量关系。结果表明，当传输距离为200 km，基矢旋转角分别为2°和10°时，量子误码率和获取的信息量分别为8.255×10^{-5}和0.99、2.044×10^{-3}和0.91。基矢旋转角大于2°时，星舰量子密钥分发系统的性能有明显下降，这表明进行星舰量子密钥分发时，需根据基矢旋转角的大小提前进行自适应校正。

关键词 量子光学；基矢旋转；星舰量子密钥分发；量子误码率；安全密钥

中图分类号 TN929.12 **文献标志码** A **doi**：10.3788/LOP202158.0327001

Influence of Receiver Basis Vectors Rotation on Satellite-to-Ship Quantum Key Distribution

Nie Min[1], Zhang fan[1*], Yang Guang[1,2], Zhang Meiling[1], Sun Aijing[1], Pei Changxing[3]

[1]*School of Communication and Information Engineering, Xi´an University of Post & Telecommunications, Xi´an, Shaanxi* 710121, *China*;

[2]*School of Electronics and Information, Northwestern Polytechnical University, Xi´an, Shaanxi* 710072, *China*;

[3]*State Key Laboratory of Integrated Service Networks, Xidian University, Xi´an, Shaanxi* 710071, *China*

Abstract In the satellite-to-ship quantum key distribution system, the quantum satellite that sends the quantum key is a low-orbiting satellite. The receiver equipment that tracks the quantum satellite is installed on the ship. Because the receiver equipment needs to track the movement of the satellite, the basis vectors of receiver equipment are inevitably rotated. In this work, the reason for the rotation of the basis vector is analyzed, and the quantitative relationship between the rotation angle of the basis vector, the quantum error rate, and the amount of information obtained, is established for the BB84 protocol. The results show that when the transmission distance is 200 km and the rotation angle of the basis vector is 2° and 10°, respectively, the quantum error rate and the amount of information acquired are 8.255×10^{-5} and 0.99, 2.044×10^{-3} and 0.91, respectively. When the rotation angle of the basis vector is greater than 2°, the performance of the satellite-to-ship quantum key distribution system is significantly reduced. This indicates that when the satellite-to-ship quantum key is distributed, it is necessary to perform an adaptive correction in advance according to the rotation angle of the basis vector.

收稿日期：2020-05-18；**修回日期**：2020-06-04；**录用日期**：2020-06-24

基金项目：国家自然科学基金(61971348,61201194)、陕西省国际科技合作与交流计划(2015KW-013)、陕西省教育厅科研计划(16JK1711)

* **E-mail**：13310997259@163.com

Key words　quantum optics; base vectors rotation; satellite-to-ship quantum key distribution system; quantum error rate; security key

OCIS codes　270.5565; 060.5565; 120.2130; 060.2605

1　引　　言

量子密钥分发(QKD)以其严格的安全性和实用性,成为量子信息领域的研究热点[1-5]。人们在量子信息领域展开了深入研究,为QKD系统的民用化奠定了基础[5-8]。Huang等[9]提出了一种基于单个粒子和集体窃听检测策略的多用户QKD协议,可在服务中心的帮助下实现任意两个用户的QKD。Yin等[10]实现了与测量设备无关的404 km光纤QKD,大大提升了QKD能达到的最远距离,为量子保密通信走向大规模应用奠定了坚实的基础。中国科学家自主研制的"墨子号"科学实验卫星在中国酒泉卫星发射中心成功发射,为未来覆盖全球的天地一体化量子通信网络建立了基础,量子通信网络的研究也得到了不断的完善。杨璐等[11]研究了基于量子隐形传态的量子保密通信方案,Zhao等[12]提出了一种基于相位编码和QKD的量子安全成像方案。

量子信号进入测量系统之前,会受到多种因素影响。焦海松等[13]研究了相位编码QKD系统中存在的相位漂移和截获-重发攻击问题。张志永等[14]分析了有偏振漂移量子保密系统中的截听-重发攻击问题。Liu等[15]研究了基于连续随机选择的连续变量QKD。Ma等[16]提出了一种具有离散调制的长距离连续变量测量且与设备无关的QKD协议。聂敏等[17]分析了非均匀水流中涌浪运动对水下量子通信性能的影响。聂敏等[18]提出了一种基于袋鼠纠缠跳跃模型的量子状态自适应跳变通信策略,可以有效提升自由空间量子通信在自然环境背景下的抗干扰能力。

在QKD系统的研究中,接收端主要集中在陆地上,而星舰QKD系统也是QKD的一个重要应用场合。因此,本文主要研究了基矢旋转下的星舰QKD性能。针对BB84协议,考虑接收望远镜方位轴和俯仰轴转动的问题,得到基矢旋转角与QKD系统相关参数的关系。仿真结果表明,系统的性能与光量子信号基矢旋转角密切相关,可为星舰QKD的实际应用提供一定的参考。

2　基矢旋转对接收端信号测量的影响

图1为基矢旋转下的星舰QKD模型,其中,A为量子卫星(密钥发送卫星),B为船舰,CD为海平面,接收端是位于B上的望远镜。设光量子信号发送时的基矢为$x_1o_1y_1$,船舰上接收望远镜成功捕获光量子信号且不发生转动时的基矢为$x_2o_2y_2$。由于量子卫星是低轨道运动的卫星,轨道高度约为500 km,量子卫星的位置相对于船舰是不断变化的,因此船舰上的接收望远镜会继续跟踪量子卫星信号。望远镜在跟踪过程中,接收量子信号的基矢会随望远镜方位轴和俯仰轴的转动而旋转,在接收端基矢相对于发送端基矢发生了转动,旋转角度为α,即由$x_2o_2y_2$旋转为$x_2'o_2y_2'$。

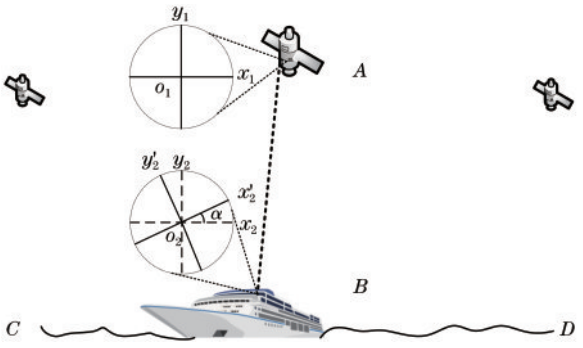

图1　基矢旋转下的星舰QKD模型

Fig. 1　QKD model of the satellite-to-ship under the rotation of the basis vector

光子进入接收机后的测量过程可由半正定算子值测量(POVM)描述,设进入望远镜的光子偏振角为零,则此时光量子的状态为

$$|\phi\rangle=|0\rangle, \tag{1}$$

式中,$|\phi\rangle$为量子态初态。接收端望远镜方位轴和俯仰轴的转动,导致基矢角旋转了α,即偏振角的变化量为α,进入测量子系统的状态为

$$|\phi'\rangle=\cos\alpha|0\rangle+\sin\alpha|1\rangle。 \tag{2}$$

用水平、垂直基测得原量子比特为$|0\rangle$的概率为

$$p(0)=\langle\phi'|E|\phi'\rangle=\cos^2\alpha, \tag{3}$$

式中,$E=|0\rangle\langle 0|$为半正定算子,满足完备性关系。同

理，测得原量子比特为$|1\rangle$的概率，即基矢旋转引起的误判概率为

$$p(1)=\sin^2\alpha。\tag{4}$$

假设时间窗口为τ，则接收端探测器每个时间窗口出现误码的概率为

$$P_b=\tau\sin^2\alpha。\tag{5}$$

3　基矢旋转对量子误码率的影响

针对BB84协议，海洋上方星舰QKD的量子误码率可表示为[19]

$$Q_e=R_{bas}/R_{sift},\tag{6}$$

式中，Q_e为海洋上方星舰QKD误码率，R_{bas}为基矢旋转引起误码的量子比特率，R_{sift}为经过数据筛选的量子比特率，可表示为

$$R_{sift}=F_sR_r[1-exp(-\mu T_0P_aT_a\eta_dF_m)],\tag{7}$$

式中，F_s为筛选因子，R_r为发射机的脉冲重复率，μ为每脉冲平均光子数，T_0为海洋大气信道的传输率，P_a为单光子的捕获概率，T_a为系统装置的传输率，η_d为单光子探测器的量子效率，F_m为测量因子。

$$T_0=exp(-a_e\cdot L),\tag{8}$$

式中，a_e为海洋大气的消光系数，L为传输距离。根据Mie散射理论，海洋大气消光系数a_e与消光效率因子、气溶胶粒子谱分布之间的关系可表示为[20]

$$a_e=\pi\int r^2Q_{ext}(r,\lambda,m)n(r)\mathrm{d}r,\tag{9}$$

式中，r为气溶胶粒子的半径，λ为入射光波长，m为折射率，$n(r)$为气溶胶的粒子谱分布，Q_{ext}为气溶胶粒子消光效率因子，可表示为

$$Q_{ext}(r,\lambda,m)=\frac{2}{x^2}\sum_{n=1}^{\infty}(2n+1)\mathrm{Re}(a_n+b_n),\tag{10}$$

式中，a_n、b_n为Mie系数，x为尺度参数，可表示为

$$x=2\pi r/\lambda。\tag{11}$$

海洋大气气溶胶粒子谱分布可看成粒子半径小于0.8 μm的细粒模和粒子半径为1 μm左右中间膜的叠加[21]。细粒模和中间膜均可用对数正态分布拟合，细粒模态的几何平均半径、几何标准偏差分别为0.2 μm、0.38；中间膜态的几何平均半径、几何标准偏差分别为1 μm、0.45，其余各参量的取值如表1所示。

结合(5)式，得到R_{bas}为

$$R_{bas}=F_sR_r\tau\sin^2\alpha。\tag{12}$$

表1　参量的取值

Table 1　Values of parameters

Parameter	μ	P_a	T_a	η_d	F_m
Value	1	0.5	1	0.65	1

海洋上方星舰QKD的量子误码率可表示为

$$Q_e=\frac{\tau\sin^2\alpha}{1-exp(-\mu T_0P_aT_a\eta_dF_m)}。\tag{13}$$

量子误码率与传输距离、基矢旋转角之间的关系如图2所示，其中，x轴为基矢旋转角，y轴为传输距离，z轴为量子误码率。可以发现，当基矢旋转角增大，传输距离增加时，量子误码率呈上升趋势；当传输距离不变时，量子误码率随基矢旋转角的增加而增加。传输距离为200 km，基矢旋转角为10°时，量子误码率为2.044×10^{-3}；传输距离为200 km，基矢旋转角由0°增加到2°时，量子误码率由0增加为8.255×10^{-5}。这表明当基矢旋转角小于2°时，基矢旋转对QKD误码率的影响较小。

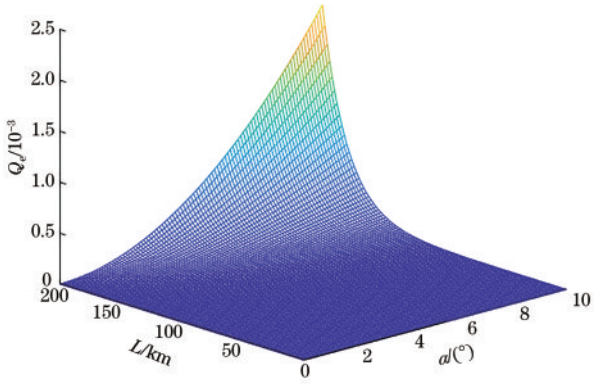

图2　量子误码率与基矢旋转角、传输距离的关系

Fig. 2　Relationship between quantum error rate and rotation angle of basis vector and transmission distance

4　基矢旋转对信息量的影响

以一组正交偏振态为例，量子卫星上以等概率制备量子态$|0\rangle=[1\quad0]^T$和$|1\rangle=[0\quad1]^T$，记发送端序列集合为X，在船舰上对X进行测量，测量结果为Y。正确测量基获取的最大信息量$I(X;Y)$满足[22]

$$I(X;Y)\leqslant S(\rho)-\sum_i p_iS(\rho_i),\tag{14}$$

式中，ρ为密度矩阵，$S(\rho)$为冯·诺依曼熵，可表示为

$$S(\rho)=-\mathrm{Tr}(\rho\log\rho)。\tag{15}$$

假设进入测量子系统的两个量子态都发生了基矢旋转，角度为α，则基矢旋转后的两个量子态可表示为

$$|0'\rangle=[\cos\alpha\quad\sin\alpha]^{\mathrm{T}},\tag{16}$$

$$|1'\rangle=[\sin\alpha\quad\cos\alpha]^{\mathrm{T}}。\tag{17}$$

两个量子态的密度矩阵可表示为

$$\boldsymbol{\rho}'=\frac{1}{2}|0'\rangle\langle 0'|+\frac{1}{2}|1'\rangle\langle 1'|=\frac{1}{2}\begin{bmatrix}1 & 2\cos\alpha\sin\alpha\\ 2\cos\alpha\sin\alpha & 1\end{bmatrix}。\tag{18}$$

(18)式的本征值可表示为

$$\lambda_1=\frac{1+\sqrt{\sin^2(2\alpha)}}{2},\tag{19}$$

$$\lambda_2=\frac{1-\sqrt{\sin^2(2\alpha)}}{2}。\tag{20}$$

冯·诺依曼熵为

$$S(\boldsymbol{\rho}')=-\frac{1+\sqrt{\sin^2(2\alpha)}}{2}\log_2\frac{1+\sqrt{\sin^2(2\alpha)}}{2}-\frac{1-\sqrt{\sin^2(2\alpha)}}{2}\log_2\frac{1-\sqrt{\sin^2(2\alpha)}}{2}。\tag{21}$$

由于

$$S(|0'\rangle\langle 0'|)=S(|1'\rangle\langle 1'|)=0,\tag{22}$$

则测量端可获取的最大信息量为

$$I(X;Y)=-\frac{1+\sqrt{\sin^2(2\alpha)}}{2}\log_2\frac{1+\sqrt{\sin^2(2\alpha)}}{2}-\frac{1-\sqrt{\sin^2(2\alpha)}}{2}\log_2\frac{1-\sqrt{\sin^2(2\alpha)}}{2}。\tag{23}$$

信息量与基矢旋转角之间的关系如图 3 所示，其中，x 轴为基矢旋转角，y 轴为接收端可获取的信息量。可以发现，接收端可获取的信息量随基矢旋转角的增加呈先上升后下降趋势。基矢旋转角由 0°增加到 45°时，信息量由 1 bit 减少为 0 bit，这表明基矢旋转会干扰接收端获取信息。

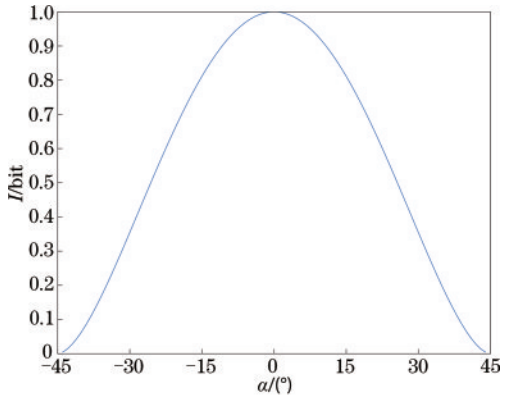

图 3　信息量与基矢旋转角的关系

Fig. 3　Relationship between the amount of information and the rotation angle of the basis vector

5　结　　论

为了探讨接收端基矢旋转对星舰 QKD 的影响，针对 BB84 协议，分析了基矢旋转的原因，研究了基矢旋转角与量子误码率、信息量的定量关系。仿真结果表明，量子误码率随舰载望远镜基矢旋转角的增大而增大。接收端获取的信息会受到基矢旋转角的干扰，QKD 的性能也会受到基矢旋转的影响。因此，可根据舰载望远镜基矢旋转角的大小，提前进行补偿，以保证 QKD 系统的性能。

参　考　文　献

[1] Shor P W, Preskill J. Simple proof of security of the BB84 quantum key distribution protocol [J]. Physical Review Letters, 2000, 85(2): 441-444.

[2] Yin J, Ren J G, Lu H, et al. Quantum teleportation and entanglement distribution over 100-kilometre free-space channels[J]. Nature, 2012, 488(7410): 185-188.

[3] Wang X L, Cai X D, Su Z E, et al. Quantum teleportation of multiple degrees of freedom of a single photon[J]. Nature, 2015, 518(7540): 516-519.

[4] Li Y, Huang P, Wang S Y, et al. A denial-of-service attack on fiber-based continuous-variable quantum key distribution [J]. Physics Letters A, 2018, 382(45): 3253-3261.

[5] Gyongyosi L. Multicarrier continuous-variable quantum key distribution[J]. Theoretical Computer Science, 2020, 816: 67-95.

[6] Yu H L, Ho T S, Rabitz H. Optimal control of orientation and entanglement for two dipole-dipole coupled quantum planar rotors[J]. Physical Chemistry Chemical Physics, 2018, 20(18): 13008-13029.

[7] Luo Y H, Zhong H S, Erhard M, et al. Quantum teleportation in high dimensions [J]. Physical Review Letters, 2019, 123(7): 070505.

[8] Guan Q, Klinkhamer V, Klemt R, et al. Density oscillations induced by individual ultracold two-body collisions[J]. Physical Review Letters, 2019, 122(8): 083401.

[9] Huang W, Wen Q Y, Liu B, et al. Multi-user quantum key distribution with collective eavesdropping detection over collective-noise channels [J]. Chinese Physics B, 2015, 24(7): 112-122.

[10] Yin H L, Chen T Y, Yu Z W, et al. Measurement-device-independent quantum key distribution over a 404 km optical fiber[J]. Physical Review Letters,

2016, 117(19): 190501.

[11] Yang L, Ma H Y, Zheng C, et al. Quantum communication scheme based on quantum teleportation [J]. Acta Physica Sinica, 2017, 66(23): 230303.
杨璐, 马鸿洋, 郑超, 等. 基于量子隐形传态的量子保密通信方案[J]. 物理学报, 2017, 66(23): 230303.

[12] Zhao Y B, Zhang W L, Wang D, et al. Proof-of-principle experimental demonstration of quantum secure imaging based on quantum key distribution [J]. Chinese Physics B, 2019, 28(10): 104203.

[13] Jiao H S, Wang Y B, He M, et al. Research about effect of phase drift on phase-coding QKD system and intercept-resend attack [J]. Laser & Optoelectronics Progress, 2015, 52(4): 042703.
焦海松, 王衍波, 何敏, 等. 相位漂移对相位编码QKD系统及截获-重发攻击的影响研究[J]. 激光与光电子学进展, 2015, 52(4): 042703.

[14] Zhang Z Y, Wang Y B, He M, et al. Intercept-resent eavesdropping in polarization-drift quantum cryptography [J]. Chinese Journal of Quantum Electronics, 2016, 33(1): 44-50.
张志永, 王衍波, 何敏, 等. 实际量子保密系统中偏振漂移对截听重发攻击的影响[J]. 量子电子学报, 2016, 33(1): 44-50.

[15] Liu W Q, Peng J Y, Huang P, et al. Continuous-variable quantum key distribution based on continuous random basis choice[J]. Chinese Physics B, 2018, 27(7): 219-224.

[16] Ma H X, Huang P, Bai D Y, et al. Long-distance continuous-variable measurement-device-independent quantum key distribution with discrete modulation [EB/OL]. [2020-05-01]. http://export.arxiv.org/abs/1812.0 5254.

[17] Nie M, Pan Y, Yang G, et al. Influence of surge movement in non-uniform water flow on performance of underwater quantum communication [J]. Acta Physica Sinica, 2018, 67(14): 140305.
聂敏, 潘越, 杨光, 等. 非均匀水流中涌浪运动对水下量子通信性能的影响[J]. 物理学报, 2018, 67(14): 140305.

[18] Nie M, Wei R Y, Yang G, et al. An adaptive quantum state-hopping communication strategy based on kangaroo entanglement hopping model[J]. Acta Physica Sinica, 2019, 68(11): 110301.
聂敏, 卫容宇, 杨光, 等. 基于袋鼠纠缠跳跃模型的量子状态自适应跳变通信策略[J]. 物理学报, 2019, 68(11): 110301.

[19] Zhang G Y, Yu S Y, Ma J, et al. Influence of background light on quantum bit error rate in satellite-to-ground quantum key distribution [J]. Opto-Electronic Engineering, 2007, 34(2): 126-129.
张光宇, 于思源, 马晶, 等. 背景光对星地量子密钥分配量子误码率的影响[J]. 光电工程, 2007, 34(2): 126-129.

[20] Nie M, Chang L, Yang G, et al. Influence of different mixing patterns of haze particles and water cloud particles on the performance of quantum satellite communication[J]. Acta Photonica Sinica, 2017, 46(7): 0701002.
聂敏, 常乐, 杨光, 等. 灰霾粒子与水云粒子不同混合方式对量子卫星通信性能影响[J]. 光子学报, 2017, 46(7): 0701002.

[21] Lu X Y, Li X B, Qin W B, et al. Particle size distribution and extinction characteristic analysis of marine atmospheric aerosol[J]. Infrared and Laser Engineering, 2017, 46(12): 1211002.
鲁先洋, 李学彬, 秦武斌, 等. 海洋大气气溶胶粒子谱分布及其消光特征分析[J]. 红外与激光工程, 2017, 46(12): 1211002.

[22] Yin H, Han Y, et al. Quantum communication principle and technology [M]. Beijing: Publishing House of Electronics industry, 2013: 64-65.
尹浩, 韩阳, 等. 量子通信原理与技术[M]. 北京: 电子工业出版社, 2013: 64-65.