空间信道离散调制连续变量量子密钥分发可行性分析*

孙新 郭俊杰 陈宇杰 程锦 刘奥 刘文博
尹鹏 陈兰剑 吴田宜 东晨†

(国防科技大学信息通信学院, 武汉 430030)

(2024 年 12 月 4 日收到; 2025 年 2 月 20 日收到修改稿)

在光纤信道中, 连续变量量子密钥分发 (continuous-variable quantum key distribution, CV-QKD) 协议已经展现出获得更高安全码率的能力, 但是 CV-QKD 协议可容忍的信道衰减相对较低, 空间衍射、大气折射、信号衰减和湍流等实际因素都会影响空间信道中 CV-QKD 协议的可行性. 本文研究了实际空间信道环境下离散调制 CV-QKD 协议的可行性, 分析了空间衍射和大气衰减、湍流信道退化模型对于空间信道离散调制 CV-QKD 协议的影响, 讨论了卫星轨道高度、天顶角、接收器孔径、束腰尺寸和过量噪声等实际参数对空间离散调制 CV-QKD 的密钥生成率影响, 搭建了星地动态运动场景仿真分析了实际环境下空间信道离散调制 CV-QKD 协议的可行性, 仿真结果可为空间信道离散调制 CV-QKD 实验的设计和优化提供参考.

关键词: 空间信道, 连续变量量子密钥分发, 星地下行链路, 离散调制

PACS: 03.67.Hk, 03.67.Dd, 92.60.hk **DOI:** 10.7498/aps.74.20241682

CSTR: 32037.14.aps.74.20241682

1 引 言

量子密钥分发 (quantum key distribution, QKD)[1–3] 以其建立在量子力学和信息论框架下的安全特性, 能够在通信双方之间分配安全密钥, 结合“一次一密”[4] 加密算法可以实现信息论意义下的安全保密通信. 量子密钥分发根据密钥信息编码方式可以分为离散变量量子密钥分发 (discrete-variable QKD, DV-QKD) 和连续变量量子密钥分发 (continuous-variable QKD, CV-QKD), “墨子号”量子科学实验卫星验证了空间信道星地下行 DV-QKD 的可行性[5], 在地面光纤 QKD 技术逐渐成熟[6,7] 和空间信道 DV-QKD 实验成功的背景下, 借鉴空间 DV-QKD 理论和实验发展路径, 依托经典激光通信链路、捕获跟踪瞄准系统等物理实现技术基础, 探索空间 CV-QKD 的可行性理论与实验研究, 是全天候、高稳定、高码率的空间量子保密通信发展方向.

CV-QKD 从调制方式上可分为高斯调制和离散调制. 高斯调制 CV-QKD (Gaussian modulation CV-QKD, GM CV-QKD)[8] 采用对称性相对较高的高斯分布, 利用高斯最优定理可证明较高的安全性, 每个脉冲可编码多比特信息, 但是调制过程相对复杂, 效率相对较低. 离散调制 CV-QKD (discrete modulation CV-QKD, DM CV-QKD)[9–15] 将离散调制后处理纠错相对简单优势与连续调制安全性证明优势结合在一起, 能够容忍较强的过量

* 湖北省自然科学基金 (批准号: 2024AFB991) 资助的课题.

† 通信作者. E-mail: dongchengfkd@163.com

噪声, 采用类似于经典激光通信中的正交相移键控 (quadrature phase shift keying, QPSK) 调制方式, 与现有系统的兼容性更高, 近年来在理论和实验方面都得到越来越多的关注和研究[16–20].

Vasylyev 等[21] 在下行链路场景中分析了地球大气对卫星量子光学通信的影响, 发现大气折射、大气吸收和湍流引起的信号失真与天顶角有很大的相关性. Pirandola[22] 分析卫星量子通信在各种实际场景下的极限性能, 探讨其在远距离安全密钥分发和纠缠分发中的可行性及优势, 特别是展示了连续变量量子密钥分发协议在上下行链路中的实现潜力. Li 等[20] 在自由空间信道下通过数值模拟, 证明离散调制连续变量量子密钥分发协议适用于卫星到地面的量子通信, 具备实现简便、抗噪性强和兼容性高的优势. 目前研究中大部分采用固定的圆形轨道进行星地几何建模, 采用固定距离和俯仰角参数进行协议可行性分析. 然而, 低轨卫星的空间 DM CV-QKD 面临星地链路动态时变、大气信道湍流、光束指向误差等实际环境因素的影响. 此外, 卫星平台的轨道选择、通信链路损耗的补偿、核心器件参数的优化都会影响空间信道 DM CV-QKD 的可行性理论.

本文研究实际空间信道环境下 DM CV-QKD 协议的可行性, 分析空间衍射和大气衰减、湍流信道退化模型对于空间信道 DM CV-QKD 协议的影响, 讨论卫星轨道高度、天顶角、接收器孔径、束腰尺寸和过量噪声等实际参数对空间 DM CV-QKD 的密钥生成率影响, 搭建星地量子密钥分发仿真平台分析空间信道 DM CV-QKD 协议的可行性, 并进一步研究 DM CV-QKD 协议幅度优化和后处理优化选择, 为后续空间信道 DM CV-QKD 的实验提供理论依据和参数选择.

本文第 2 节是 DM CV-QKD 协议、星地链路信道模型及渐近极限下 DM CV-QKD 密钥率的相关理论; 第 3 节基于墨子号卫星轨道, 仿真分析实际参数对空间 DM CV-QKD 密钥生成率的影响; 第 4 节对空间信道 DM CV-QKD 可行性分析研究进行总结.

2 星地 DM CV-QKD 协议模型

本工作基于 QPSK 调制的零差探测 CV-QKD 协议开展[17], 在理想探测下使用严密的数值方法求解在渐近状态下针对集体攻击的密钥率, 协议的空间信道制备测量模型和 QPSK 星座图如图 1 所示.

2.1 星地链路信道模型的建立

本文首先建立空间信道离散调制相干态信道传输退化模型. 通常把从海平面以上 1000—1400 km 高度内的气层作为地球大气层的厚度, 其中大气总质量的 98.2% 集中在 30 km 以下. 在这个范围内, 大气衰减和湍流现象较为显著. 如图 2(a) 所示, 将卫星与地面站通信时间划分为 N 段, 时间间隔 $\Delta t = 1$ s, 相干光的传播距离 $L(t)$. 相干光经过大气湍流发生衰减和偏移的过程如图 2(b) 所示. 可以得到:

$$L(t) = \sqrt{h(t)^2 + 2h(t)R_{\rm e} + R_{\rm e}^2(\cos(\theta(t)))^2} - R_{\rm e}(\cos(\theta(t))), \tag{1}$$

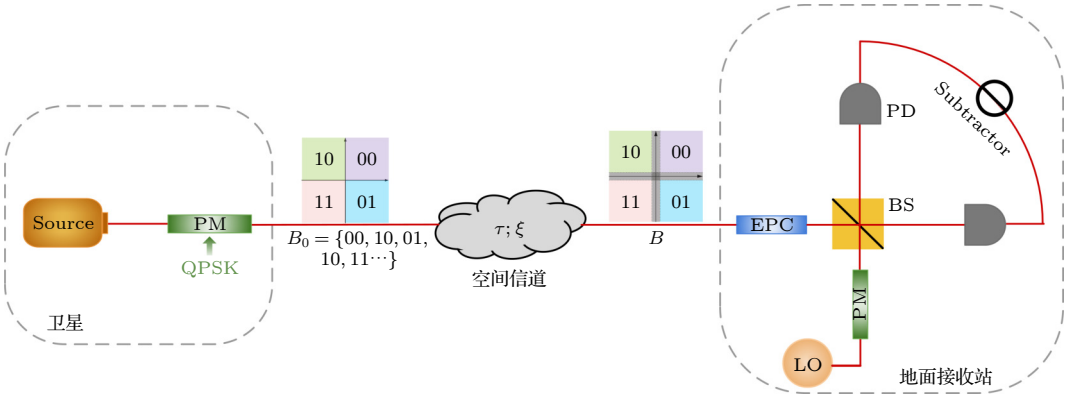


图 1 QPSK 协议的空间信道制备测量模型和星座示意图 (PM, 相位调制器; EPC, 电极化控制器; LO, 本地振荡器; BS, 分束器; PD, 光电探测器)

Fig. 1. Prepare & Measure model and constellation schematic of spatial channel for QPSK protocol. PM, phase modulator; EPC, electrical polarization controller; LO, local oscillator; BS, beam splitter; PD, photodetector.

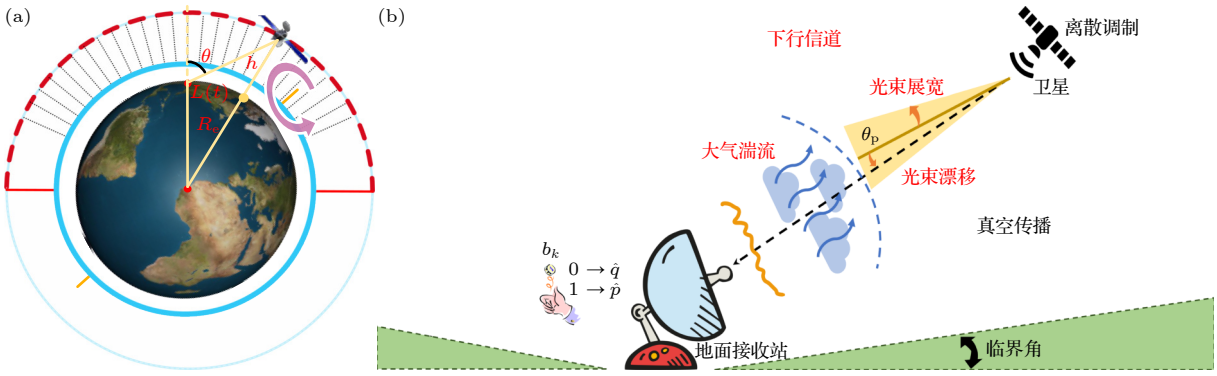


图 2 星地量子密钥分发场景图 (a) 卫星动态通信轨道图; (b) 光的传输遍历过程图

Fig. 2. Scenario graph of star-earth quantum key distribution: (a) Satellite dynamic communications orbit graph; (b) graph of the light transmission traversal process.

其中地球半径 $R_e \simeq 6371$ km, $\theta(t)$ 是卫星与地面站的实时天顶角, $h(t)$ 是卫星离地面实时高度.

地球大气的光学折射率与真空中的折射率不同, 折射率值随海拔、地理位置和气象条件变化而变化. 由于折射率的不同, 相干光在大气中发生折射现象. 相干光束在大气层中的传播距离变大, 但是当天顶角小于 70°时, 光路长度伸长因子接近于 1[21]. 假设本文分析的天顶角范围限制在 70°以内, 可以忽略折射带来的路径影响. 本文对波长 $\lambda = 1550$ nm, 下行链路弱湍流、能见度为 20 km 的中纬度夏季大气模型开展研究, 考虑空间衍射和大气衰减、湍流信道退化对于空间信道 DM CV-QKD 协议的影响.

2.1.1 空间衍射

在空间信道 CV-QKD 协议传输过程中, 相干光束初始束腰半径为 w_0, 经过距离 L 的传播后到达接收端, 受到空间衍射的影响, 接收端的光斑尺寸为

$$\omega_{\rm d}^2 = \omega_0^2 \left[\left(1 - \frac{L}{R_0}\right)^2 + \left(\frac{L}{Z_{\rm R}}\right)^2 \right], \tag{2}$$

其中 $Z_{\rm R} = \pi\omega_0^2\lambda^{-1}$ 为瑞利距离, λ 是相干光的波长, R_0 为曲率[23]. 理论上聚焦光束可以减小接收口径有限带来的损耗, 但对光学系统的对准和跟踪精度提出了更高的要求, 在模型中采用准直光束 ($R_0 \approx +\infty$), 接收端光斑尺寸可简化为[22]

$$\omega_{\rm d} = \omega_0\sqrt{1 + L^2/Z_{\rm R}^2}. \tag{3}$$

接收端望远镜的孔径为 $a_{\rm R}$, 由于接收望远镜的孔径尺寸限制, 光束只有一部分能被望远镜接收, 因此空间衍射影响下的透过率为

$$\tau_{\rm d} = 1 - {\rm e}^{-2a_{\rm R}^2/\omega_{\rm d}^2}. \tag{4}$$

2.1.2 大气衰减

气溶胶的吸收和瑞利散射会导致光的消失, 这取决于链路长度以及气溶胶分布模型[21]. 大气衰减还很大程度上取决于天空条件和传输波长. 在天顶角小于 70°时, 大气透射效率 $\tau_{\rm atm}$ 可以表示为[24]

$$\tau_{\rm atm} = \tau_{\rm zen}^{\sec\theta}, \tag{5}$$

其中 $\tau_{\rm zen}$ 是 $\theta = 0°$ 的传输效率. 天顶传输效率 $\tau_{\rm zen}$ 的估算采用广泛使用的大气透射率和辐射度网络应用程序计算器 MODTRAN[25]. 考虑波长 $\lambda = 1550$ nm、能见度为 20 km 的中纬度夏季大气模型, 得到高度 $h = 50$ km 处的天顶传输效率 $\tau_{\rm zen} = 0.90$. 由于高度 50 km 以上的空气密度几乎为 0, 大气影响可以忽略不计, $\tau_{\rm zen} = 0.90$ 可以适用于此模型下的任何高度的卫星平台. 光束在传播中经历空间衍射和大气衰减后, 望远镜还会带来探测损耗 $\tau_{\rm eff} \simeq 0.4$ 等固定损耗[26], 因此空间信道透过率可表示为

$$\tau_{\rm tot} = \tau_{\rm eff}\tau_{\rm atm}\tau_{\rm d}. \tag{6}$$

2.1.3 大气湍流

大气温度的随机变化会导致空气运动, 带来强度波动、光束漂移和光束展宽, 从而导致信道透射率的波动, 具有一定的统计特性. 在大气湍流的影响下, 卫星信号光束中心与接收平台中心瞬时偏转距离 r 的概率分布遵循 Weibull 分布[24], 表示为

$$P(r;\sigma_{\mathrm{r}})=\frac{r}{\sigma_{\mathrm{r}}^2}\exp\left[-\left(\frac{r}{\sqrt{2}\sigma_{\mathrm{r}}}\right)\right], \tag{7}$$

其中, 标准差 $\sigma_{\mathrm{r}}=\sqrt{(L\theta_{\mathrm{p}})^2+\sigma_{\mathrm{turb}}^2}$, 指向误差 θ_{p} 为光束中心与接收望远镜中心之间的夹角. 这里 σ_{turb}^2 是大气湍流产生的光束中心方差, 取决于湍流强度、传播距离和光束初始束腰半径. 在弱湍流的条件下光束偏差主要由卫星指向误差决定, 可以得到 $\sigma_{\mathrm{r}}\simeq L\theta_{\mathrm{p}}$ [27]. 透射效率 τ_{end} 与瞬时偏转距离 r 之间的近似解析关系可以表示为

$$\tau_{\mathrm{end}}=\tau_{\mathrm{tot}}\exp\left[-(r/S)^{\gamma}\right], \tag{8}$$

其中 S 和 γ 分别是尺度参数和形状参数 [28].

2.1.4 过量噪声

星地间通信的噪声来源多样, 除了在传播信道中不可避免的固定噪声外 [24], 还有检测噪声 [17]、相位波动噪声 [29] 等. 所有的噪声随机相互独立, 由于方差的可加性可以表示为

$$\xi_{\mathrm{tot}}=\xi_{\mathrm{fix}}+\xi_{\mathrm{det}}+\xi_{\mathrm{phase}}, \tag{9}$$

其中 ξ_{fix} 是信号进行光纤耦合产生的; ξ_{det} 是检测设备的不完美导致的, 本质上不可避免; ξ_{phase} 是振荡器初始频率偏移以及大气闪烁引起的随机相位波动.

2.2 渐近极限下的 DM CV-QKD 密钥率

位于卫星平台的发送端采用相干光源随机生成 4 种等概率的相干光, 分别代表{00, 10, 11, 01}, 经过自由空间退化信道传输到达接收望远镜, 位于地面站的接收端等概率随机地使用正交基 $\hat{q}$ 和 $\hat{p}$ 进行测量, 反向调和后生成密钥. 在渐近极限下进行联合窃听时, 空间信道 DM CV-QKD 协议的密钥生成率 R^{∞} 可以表示为 [17]

$$R^{\infty}=\frac{1}{2}\left\{\min_{\rho_{\mathrm{AB}}\in S}\sum_{y\in\{\hat{q},\hat{p}\}}D\left(\varsigma_y\left(\boldsymbol{\rho}_{\mathrm{AB}}\right)\parallel Z\left[\varsigma_y\left(\boldsymbol{\rho}_{\mathrm{AB}}\right)\right]\right)-\sum_{y\in\{\hat{q},\hat{p}\}}p_{\mathrm{pass}}^{y}\delta_{\mathrm{EC}}^{y}\right\}, \tag{10}$$

其中 $\boldsymbol{\rho}_{\mathrm{AB}}$ 是描述卫星和接收望远镜之间信息的状态, $\sum_{y\in\{\hat{q},\hat{p}\}}D\left(\varsigma_y\left(\boldsymbol{\rho}_{\mathrm{AB}}\right)\parallel Z\left[\varsigma_y\left(\boldsymbol{\rho}_{\mathrm{AB}}\right)\right]\right)$ 是通过量子相对熵衡量窃听者对接收望远镜产生密钥的不确定度, $\sum_{y\in\{\hat{q},\hat{p}\}}p_{\mathrm{pass}}^{y}\delta_{\mathrm{EC}}^{y}$ 是卫星对接收望远镜产生密钥的经典信息.

在时间间隔 Δt 内, 光的传播距离 L 和星地之间的天顶角 θ 基本不变, 本文假设在时间间隔内信道的统计特性不变. 由于后选择的筛选概率 p_{pass} 和信息泄漏量 δ_{EC} 只涉及卫星和接收望远镜掌握的信息, $\sum_{y\in\{\hat{q},\hat{p}\}}p_{\mathrm{pass}}^{y}\delta_{\mathrm{EC}}^{y}$ 可以根据定义计算 [30]. 采用优化数值方法 [30,31] 计算密钥率部分 $\sum_{y\in\{\hat{q},\hat{p}\}}D\left(\varsigma_y\left(\boldsymbol{\rho}_{\mathrm{AB}}\right)\parallel Z\left[\varsigma_y\left(\boldsymbol{\rho}_{\mathrm{AB}}\right)\right]\right)$:

$$\begin{aligned}
&\min\sum_{y\in\{\hat{q},\hat{p}\}}D\left(\varsigma_y\left(\boldsymbol{\rho}_{\mathrm{AB}}\right)\parallel Z\left[\varsigma_y\left(\boldsymbol{\rho}_{\mathrm{AB}}\right)\right]\right)\\
&\text{subject to}\\
&\mathrm{Tr}\left[\boldsymbol{\rho}_{\mathrm{AB}}\left(|x\rangle\langle x|_{\mathrm{A}}\otimes\hat{q}\right)\right]=p_x\langle\hat{q}\rangle_x,\\
&\mathrm{Tr}\left[\boldsymbol{\rho}_{\mathrm{AB}}\left(|x\rangle\langle x|_{\mathrm{A}}\otimes\hat{p}\right)\right]=p_x\langle\hat{p}\rangle_x,\\
&\mathrm{Tr}\left[\boldsymbol{\rho}_{\mathrm{AB}}\left(|x\rangle\langle x|_{\mathrm{A}}\otimes\hat{n}\right)\right]=p_x\langle\hat{n}\rangle_x,\\
&\mathrm{Tr}\left[\boldsymbol{\rho}_{\mathrm{AB}}\left(|x\rangle\langle x|_{\mathrm{A}}\otimes\hat{d}\right)\right]=p_x\langle\hat{d}\rangle_x,\\
&\mathrm{Tr}_{\mathrm{B}}\left[\boldsymbol{\rho}_{\mathrm{AB}}\right]=\sum_{i,j=0}^{3}\sqrt{p_ip_j}\langle\phi_j|\,\phi_i\rangle|i\rangle\langle j|_{\mathrm{A}},\\
&\mathrm{Tr}_{\mathrm{B}}\left[\boldsymbol{\rho}_{\mathrm{AB}}\right]=1,\\
&\boldsymbol{\rho}_{\mathrm{AB}}\geqslant 1.
\end{aligned} \tag{11}$$

其中 x 属于{00, 10, 11, 01}, $\langle\hat{q}\rangle_x$, $\langle\hat{p}\rangle_x$, $\langle\hat{n}\rangle_x$ 和 $\langle\hat{d}\rangle_x$ 是接收望远镜测量 x 的算子期望值.

在空间信道中, 卫星轨道高度 $h(t)$、天顶角 $\theta(t)$、接收器孔径 a_{R} 和束腰尺寸 ω_0 这些变量决定空间衍射、大气衰减和大气湍流对信号的损耗. 通过信道透射效率 τ_{end} 和过量噪声 ξ_{tot} 确定空间信道中算子 $\langle\hat{q}\rangle_x=\sqrt{2\tau_{\mathrm{end}}}R_{\mathrm{e}}(a_x)$, $\langle\hat{p}\rangle_x=\sqrt{2\tau_{\mathrm{end}}}\mathrm{Im}(a_x)$, $\langle\hat{n}\rangle_x=\tau_{\mathrm{end}}|a_x|^2+\tau_{\mathrm{end}}\xi_{\mathrm{tot}}/2$ 和 $\langle\hat{d}\rangle_x=\tau_{\mathrm{end}}[(a_x)^2+(a_x^*)^2]$ 的期望值, 代入 (11) 式求解密钥率, a_x 为接收到的信号状态.

3 仿真结果分析

仿真中采用墨子号卫星轨道数据进行场景建模, 具体使用了墨子号 2016 年 3 月 22 日 17 时 28 分—17 时 35 分 (国际标准时间) 的星历数据进行卫星轨道参数设定. 地面站可以选择兴隆、德令哈、丽江、南山地面站, 考虑卫星与地面站的通连时间和信道损耗, 本文选择丽江地面站开展分析.

卫星与地面站的相关参数, 即用于模拟墨子号-丽江站的参数和 DM CV-QKD 系统参数设置分别如表 1 和表 2 所列.

表 1 用于模拟墨子号-丽江站的参数

Table 1. Parameters used to simulate the Mercury-Lijiang station.

参数	参考值
光束尺寸 ω_0	20 cm
接收孔径 α_R	0.9 m
探测效率 τ_{eff}	0.4
天顶传输效率 τ_{zen}	0.90
指向误差 θ_p	1 μrad

表 2 DM CV-QKD 系统参数设置

Table 2. DM CV-QKD system parameter setting.

参数	参考值
波长 λ	1550 nm
调制幅度 α	0.6
后处理值 Δ	0
过量噪声 ξ_{tot}	0.01
光子截止数 N_c	12

仿真得到在通信窗口内卫星与地面站的距离、天顶角以及传输损耗与时间的关系如图 3 所示, 其中传输损耗是由传输效率 τ_{end} 取对数后计算得到. 从图 3 可以看到, 墨子号卫星与丽江站通信接入时间持续了大约 288 s, 信道最高损耗约为 39.3 dB, 距离约为 1205.3 km, 天顶角约为 69.9°. 最低损耗约为 26.2 dB, 距离约为 566.7 km, 天顶角约为 28.3°.

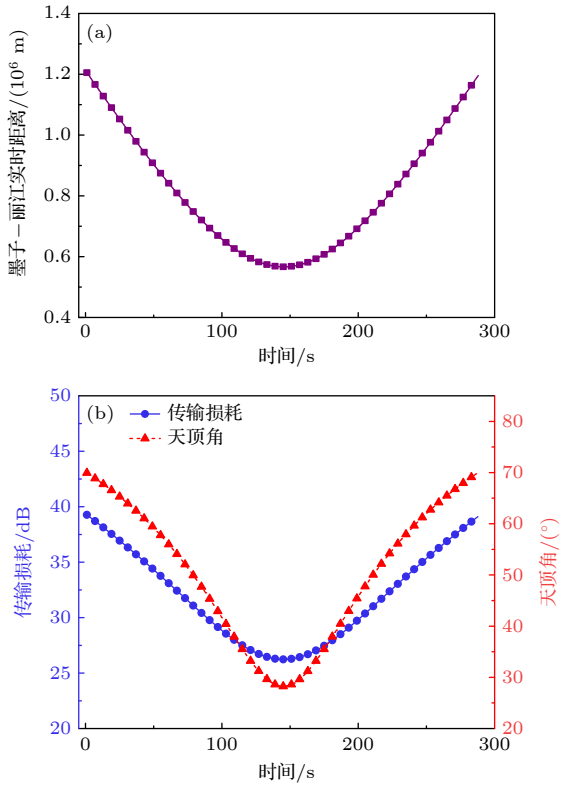


图 3 卫星与地面站之间的距离、天顶角以及传输损耗随轨道运动变化图 (a) 距离变化; (b) 天顶角和传输损耗变化

Fig. 3. Graphs of distance, zenith angle and transmission loss between the satellite and the ground station as a function of orbital motion: (a) Change in distance; (b) change in zenith angle and transmission loss.

链路的损耗与距离和天顶角有关, 在相同条件下, 距离越短, 天顶角越小, 传输损耗越小. 图 4 分析了轨道高度和天顶角对传输损耗以及密钥率生成的影响. 如图 4(a) 所示, 在下行链路中, 传输损耗随着天顶角和轨道高度的增加而增大. 在通信传输损耗的分析中, 当保持天顶角不变时, 传输损耗随轨道高度变化的影响相对较小; 而当轨道高度保持不变时, 天顶角的变化对传输损耗的影响则更为显著. 从图 4(b) 可以看到, 密钥率随着传输损耗的增大而减小, 即轨道高度和天顶角这两个参数同时影响着传输损耗和密钥率. 由于密钥量是持续时间和密钥率的乘积, 参数优化过程需要考虑通信接入时间与密钥率的平衡.

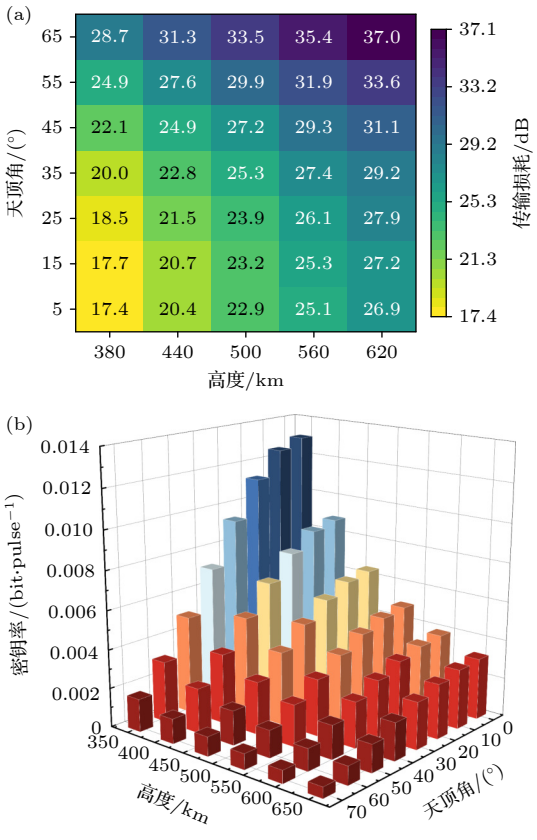


图 4 传输损耗及密钥率与轨道高度和天顶角的关系图 (a) 传输损耗与轨道高度和天顶角的关系; (b) 密钥率与轨道高度和天顶角的关系

Fig. 4. Graph of transmission loss and key rate versus orbital altitude and zenith angle: (a) Transmission loss versus orbit height and zenith angle; (b) key rate versus orbital altitude and zenith angle.

本文分析了卫星发射的光束腰尺寸和接收孔径对于协议性能的影响. 目前, 接收望远镜的孔径最大可达 2.4 m[32]. 为了探究两者对传输损耗的影响, 设置卫星高度为 400 km, 天顶角为 70°的情况下, 光束腰尺寸 $w_0 \in [0.2, 0.6]$ 和接收孔径 $a_{\mathrm{R}} \in [0.6, 1.4]$ 对传输损耗和密钥率生成的影响如图 5 所示. 如图 5(a) 所示, 光束腰尺寸增大, 传输损耗逐渐减小, 尤其是在较小的接收孔径 (0.6, 0.8) 范围内更加明显. 较小的光束腰尺寸会导致空间衍射影响更加突出, 空间衍射透过率 τ_{d} 变小, 带来更多的损耗. 接收孔径增大, 空间衍射透过率 τ_{d} 变大, 损耗逐渐减小. 这表明增大接收孔径可以减少损耗, 提高传输效率, 较低的损耗出现在接收孔径较大和光束腰尺寸较大的组合中. 从图 5(b) 可以看到, 密钥率随着传输损耗的增大而减小, 光束腰尺寸和接收孔径这两个参数同时影响着传输损耗和密钥率.

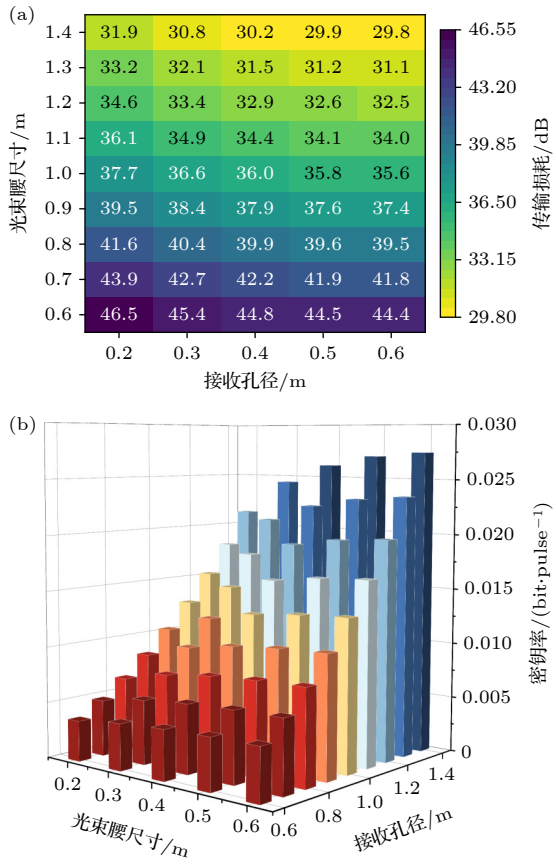


图 5 传输损耗及密钥率与光束腰尺寸和接收孔径的关系图 (a) 传输损耗与光束腰尺寸和接收孔径的关系; (b) 密钥率与光束腰尺寸和接收孔径的关系

Fig. 5. Graph of transmission loss and key rate versus beam waist size and acceptance aperture: (a) Transmission loss versus beam waist size and acceptance aperture; (b) key rate as a function of beam waist size and acceptance aperture.

现实环境中不可避免的噪声因素会对量子信号产生破坏, 从而影响到密钥率的生成. 本文分析了过量噪声在实际动态轨道变化中对密钥率的影响, 不同过量噪声下的协议密钥生成率如图 6 所示. 在墨子号-丽江站实时动态轨道中, 卫星与地面站实时的距离 L 和天顶角 θ 不断变化, 影响着空间衍射、大气衰减和大气湍流变化, 进而影响透射效率 τ_{end} 变化, 其中 L, θ 和 τ_{end} 变化成正相关. 在过量噪声固定时, 密钥率随着透射效率变化而变化, 当透射效率最小时, 密钥率最大. 协议对 0.01, 0.02 和 0.03 的过量噪声具有较好的耐受性, 过量噪声超过 0.03 后空间信道 DM CV-QKD 协议不可行.

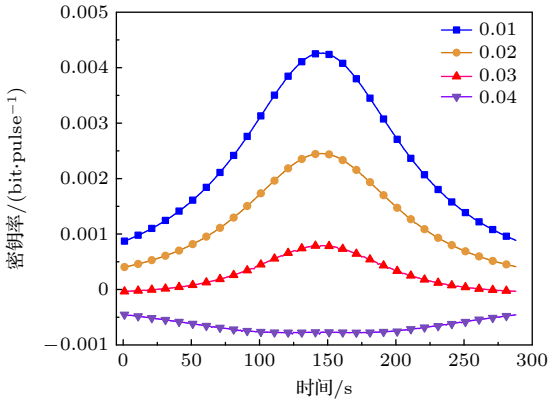


图 6 DM CV-QKD 在不同过量噪声下的密钥率

Fig. 6. Key rate of DM CV-QKD with different additional noises.

光量子调制幅度的改变, 密钥率也会发生变化. 较大的调制幅度会提高信号的识别概率, 从而在理论上提升密钥率, 但在实际应用中, 过大的调制幅度也会导致错误增多, 需要进行更多的纠错, 进而降低密钥率. 本文通过优化墨子号-丽江站实时轨道所对应的最佳幅值, 得到最佳幅值和优化后的密钥率如图 7 所示, 优化过程选取的过量噪声 $\xi_{\mathrm{tot}} = 0.02$, 后处理 $\Delta = 0$. 从图 7(a) 可得到, 在墨子号-丽江站实时动态轨道中, 最佳幅值集中在 0.66. 在最佳幅值下计算密钥率与预置调制幅度为 0.6 的密钥率进行比较, 从图 7(b) 可以看出密钥率有一定的提升. 通过后处理调整 Δ 进一步优化密钥率, 本文在过量噪声 $\xi_{\mathrm{tot}} = 0.02$ 和调制幅度 $\alpha = 0.66$ 的条件下, 分析不同后处理 Δ 对密钥的影响如图 8 所示.

从图 8 可以看出, 在每条曲线的峰值位置, 即

传输损耗最小时, 光量子在传输过程中受到的影响较小, 后处理对密钥率的提升效果并不明显. 然而, 当传输损耗较大时, 尤其是在曲线的两端区域, 后处理的作用则显得尤为显著. 在实际空间实验中当空间环境变化较大或传输条件更为恶劣时, 可以通过调整后处理参数来优化密钥率, 以适应不同的传输状况.

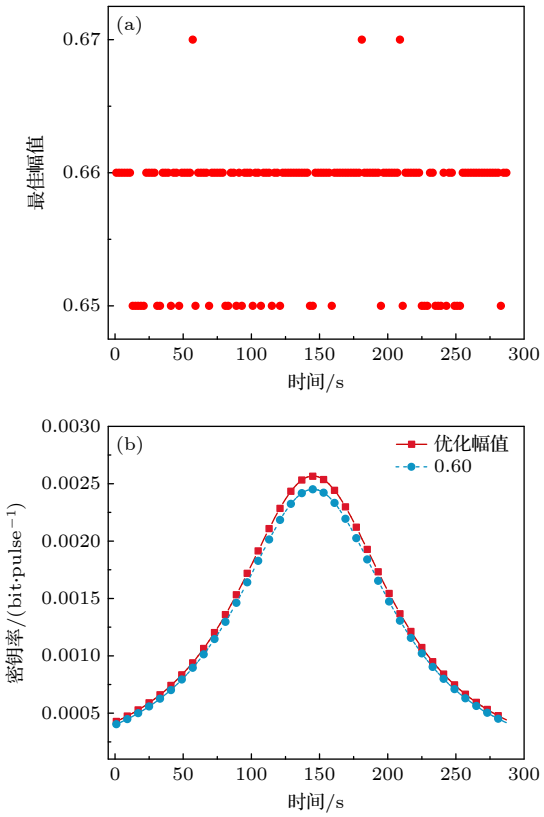


图 7 DM CV-QKD 在动态轨道下的最佳幅值和密钥率 (a) 最佳幅值; (b) 密钥率

Fig. 7. Optimal magnitude and key rate for DM CV-QKD in dynamic orbit: (a) Optimal amplitude; (b) key rate.

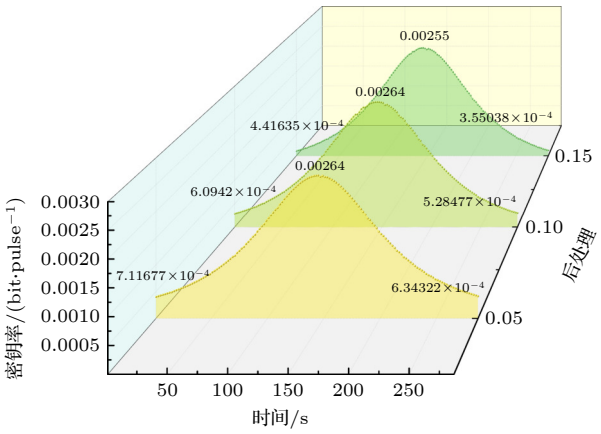


图 8 不同后处理值与密钥率的关系

Fig. 8. Different post-processing values versus key rate.

类比 QKD 在光纤信道中的结果分析对比, 本文比较了在墨子号-丽江站的相同轨道参数场景下, 空间 GM CV-QKD 与 DM CV-QKD 协议的性能. 其中 GM CV-QKD 采用的是在渐近极限时联合窃听下的 GG02 协议 [3], 部分仿真参数如表 3 所列, 协议对比效果如图 9 所示. 在墨子号-丽江站的轨道中, GM CV-QKD 协议的密钥率明显优于 DM CV-QKD 协议, 即便通过幅值优化提升DM CV-QKD 的密钥率, 其效果在 GM CV-QKD的密钥率尺度上仍不显著. 高斯调制通过利用连续分布的信号空间, 实现了更高的信息熵, 从理论上提升了量子信道的容量和信息提取效率, 从而显著增强了量子密钥分发的性能. 而离散调制由于信号点的离散性, 其密钥率受到一定限制.

表 3 GM CV-QKD 系统参数设置

Table 3. GM CV-QKD system parameter setting.

参数	参考值
制备方差 V	4
电子噪声 $\xi_{\rm el}$	0.1
反向调和效率 β	0.95
过量噪声 ξ	0.02

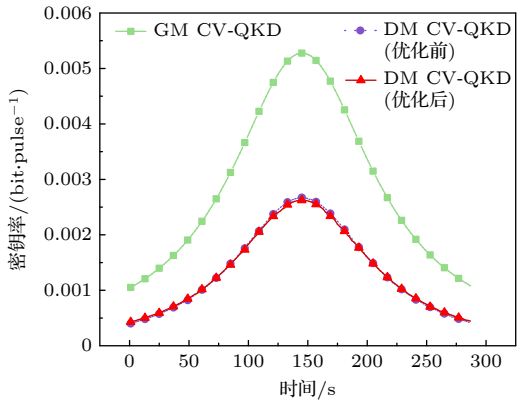


图 9 两种 CV-QKD 协议的密钥率对比图

Fig. 9. Comparison of key rate of two CV-QKD protocols graph.

4 结 论

本文建立了星地轨道几何参数模型和大气信道退化模型, 分析了空间信道 DM CV-QKD 的可行性. 首先研究了卫星轨道高度、天顶角、接收器孔径、束腰尺寸和过量噪声对密钥生成率的影响, 考虑到轨道选择具有约束性, 可以通过增大接收孔径和束腰尺寸来提高密钥率. 其次是协议性能方

面, 由于光量子在传输过程中受大气湍流影响, 其方差变大对后处理产生影响. 针对不同的大气环境, 在制备和后处理中, 找到最佳调制幅度和后处理值组合来提高密钥率. 文章对比分析了低轨卫星场景下空间信道渐近极限 GM CV-QKD 与 DM CV-QKD 的密钥生成率, 仿真结果表明在低轨卫星对地通信场景, 过量噪声 $\xi_{\text{tot}} = 0.02$ 时, GM CV-QKD 的密钥率性能优于 DM CV-QKD. 但是考虑现有系统的兼容性和后处理的复杂程度, 离散调制的耦合性更高, 需要后处理计算量更少, 使其在现代通信系统中更具优势. 本文的参数选择优化方法可以为空间信道 DM CV-QKD 的实验研究提供理论支撑和参数选择.

参考文献

[1] Bennett C, Brassard G 1984 *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* Bangalore, December 9–12, 1984 p175
[2] Ralph T C 1999 *Phys. Rev. A* **61** 010303
[3] Grosshans F, Grangier P 2002 *Phys. Rev. Lett.* **88** 057902
[4] Vernam G S 1926 *J. AIEE* **45** 109
[5] Liao S K, Cai W Q, Liu W Y, et al. 2017 *Nature* **549** 43
[6] Aguado A, Lopez V, Lopez D, Peev M, Poppe A, Pastor A, Folgueira J, Martin V 2019 *IEEE Commun. Mag.* **57** 20
[7] Zhang Y, Chen Z, Chu B, et al. 2020 *Bull. Am. Phys. Soc.* **65** 857
[8] García-Patrón R, Cerf N J 2009 *Phys. Rev. Lett.* **102** 130501
[9] Leverrier A, Grangier P 2009 *Phys. Rev. Lett.* **102** 180504
[10] Zhou J, Guo Y, Huang D, Zeng G 2017 arXiv: 1711.09039 [quant-ph]
[11] Li Z, Zhang Y C, Guo H 2018 arXiv: 1805.04249 [quant-ph]
[12] Ghorai S, Grangier P, Diamanti E, Leverrier A 2019 *Phys. Rev. X* **9** 021059
[13] Wang P, Zhang Y, Lu Z G, Wang X Y, Li Y M 2023 *New J. Phys.* **25** 023019
[14] Bäuml S, Pascual-García C, Wright V, Fawzi O, Acín A 2024 *Quantum* **8** 1418
[15] Wu M Z, Li J H, Xu B J, Yu S, Zhang Y C 2024 *Phys. Rev. Appl.* **22** 034024
[16] Lin J, Lütkenhaus N 2020 *Phys. Rev. Appl.* **14** 064030
[17] Liu W B, Li C L, Xie Y M, Weng C X, Gu J, Cao X Y, Lu Y S, Li B H, Yin H L, Chen Z B 2021 *PRX Quantum* **2** 040334
[18] Zhou S, Xie Q M, Zhou N R 2024 *Laser Phys. Lett.* **21** 065207
[19] Gong L H, Li M L, Cao H, Wang B 2024 *Laser Phys. Lett.* **21** 055209
[20] Li S G, Li C L, Liu W B, Yin H L, Chen Z B 2024 *Adv. Quantum Technol.* **7** 2400140
[21] Vasylyev D, Vogel W, Moll F 2019 *Phys. Rev. A* **99** 053830
[22] Pirandola S 2021 *Phys. Rev. Res.* **3** 023130
[23] Svelto O, Hanna D C 2010 *Principles of Lasers* (New York: Springer) p153
[24] Dequal D, Trigo Vidarte L, Roman Rodriguez V, et al. 2021 *npj Quantum Inf.* **7** 3
[25] Spectral Sciences Inc. http://modtran.spectral.com/modtran_home [2025-01-12]
[26] Liorni C, Kampermann H, Bruß D 2019 *New J. Phys.* **21** 093055
[27] Fante R L 1975 *Proc. IEEE* **63** 1669
[28] Vasylyev D Y, Semenov A, Vogel W 2012 *Phys. Rev. Lett.* **108** 220501
[29] Liu X, Lu H M, He Y F, Wu F L, Zhang C X, Wang X L 2023 *Symmetry* **15** 2053
[30] Lin J, Upadhyaya T, Lütkenhaus N 2019 *Phys. Rev. X* **9** 041064
[31] Hu H, Im J Y, Lin J, Lütkenhaus N, Wolkowicz H 2022 *Quantum* **6** 792
[32] Prosser C F, Kennicutt Jr R C, Bresolin F, et al. 1999 *Astrophys. J.* **525** 80

Feasibility analysis study of discrete modulation continuous variable quantum key distribution for spatial channels*

SUN Xin GUO Junjie CHEN Yujie CHENG Jin LIU Ao LIU Wenbo YIN Peng CHEN Lanjian WU Tianyi DONG Chen †

(*Institute of Information and Communication, National University of Defense Technology, Wuhan* 430030, *China*)

(Received 4 December 2024; revised manuscript received 20 February 2025)

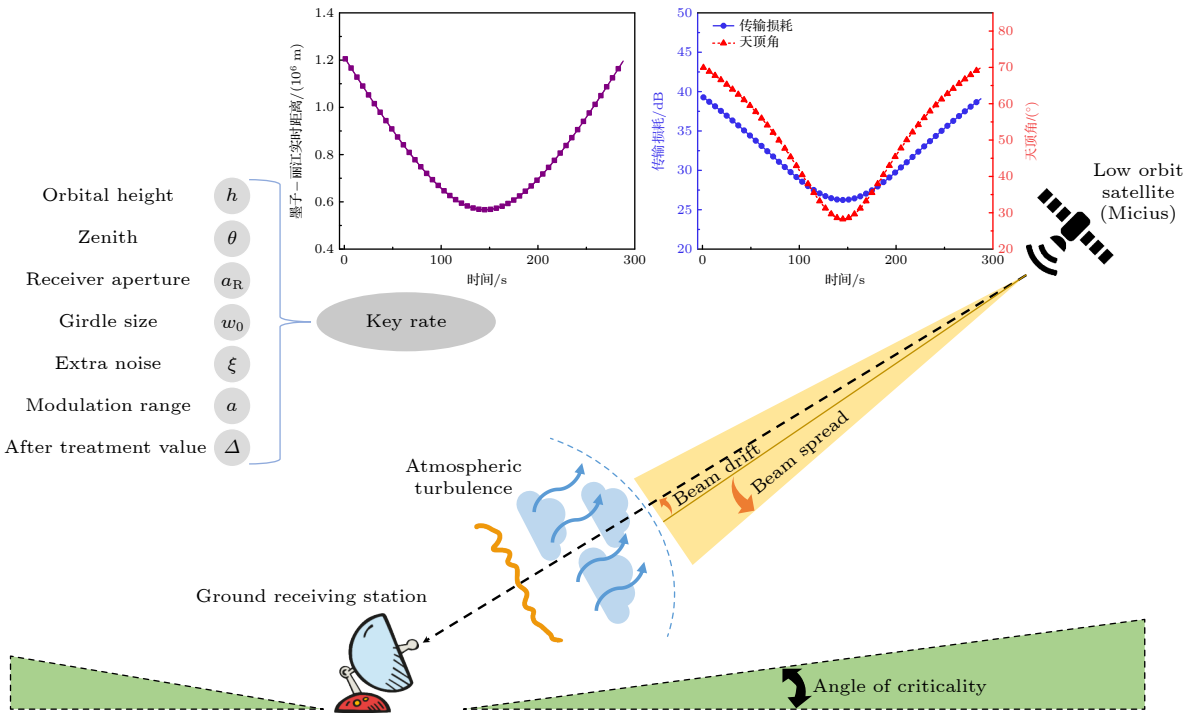
Abstract

Continuous variable quantum key distribution (CV-QKD) has emerged as a promising candidate for quantum-secure communication due to its experimentally demonstrated high key rates in fiber-optic channels. However, the feasibility of discrete modulation CV-QKD in satellite-to-ground downlinks remains an open

* Project supported by the Natural Science Foundation of Hubei Province, China (Grant No. 2024AFB991).

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

question due to practical challenges such as high transmission loss, limited communication windows, and atmospheric turbulence. In this work, a comprehensive framework is proposed to evaluate the feasibility of discrete modulation CV-QKD by integrating orbital dynamics and atmospheric channel models, and to comprehensively analyze the influence of the parameter space on free-space discrete modulation CV-QKD. To achieve this, a free-space CV-QKD simulation platform is employed, which calculates the elevation angle and transmission distance based on precise orbital models, thereby providing a more practical assessment of the key rate for discrete modulation CV-QKD. Simulation results verify the feasibility and practicality of discrete modulation CV-QKD in satellite-based quantum communication systems. Furthermore, the critical factors influencing the key rate performance are identified, and parameter optimization strategies are proposed, providing theoretical support for realizing the future satellite-to-ground discrete modulation CV-QKD.



Keywords: space channel, continuous-variable quantum key distribution, satellite underground links, discrete modulation

PACS: 03.67.Hk, 03.67.Dd, 92.60.hk **DOI:** 10.7498/aps.74.20241682

CSTR: 32037.14.aps.74.20241682

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

空间信道离散调制连续变量量子密钥分发可行性分析

孙新 郭俊杰 陈宇杰 程锦 刘奥 刘文博 尹鹏 陈兰剑 吴田宜 东晨

Feasibility analysis study of discrete modulation continuous variable quantum key distribution for spatial channels

SUN Xin GUO Junjie CHEN Yujie CHENG Jin LIU Ao LIU Wenbo YIN Peng CHEN Lanjian WU Tianyi DONG Chen

引用信息 Citation: Acta Physica Sinica, 74, 090303 (2025) DOI: 10.7498/aps.74.20241682
CSTR: 32037.14.aps.74.20241682
在线阅读 View online: https://doi.org/10.7498/aps.74.20241682
当期内容 View table of contents: http://wulixb.iphy.ac.cn
