基于被动态制备的星间太赫兹连续变量量子密钥分发方案*

吴晓东[1)] 黄端[2)†]

1) (福建理工大学管理学院, 福州 350118)

2) (中南大学电子信息学院, 长沙 410083)

(2025 年 12 月 27 日收到; 2026 年 2 月 20 日收到修改稿)

太赫兹通信作为下一代大容量无线网络背景下的一个重要研究课题, 对构建高速星间量子通信网络具有重要意义. 基于高斯调制相干态的星间太赫兹连续变量量子密钥分发方案通常采用主动调制的方式进行量子态的制备, 即需要振幅与相位调制器以及量子随机数发生器. 然而, 具有高消光比和高稳定性的高速主动调制在实际中实现起来极具挑战性, 并且主动调制其调制格式相对复杂, 仅能容忍较小的调制误差, 这些都不利于构建高速星间量子通信网络. 鉴于上述分析, 本文提出了基于被动态制备的星间太赫兹连续变量量子密钥分发方案, 即采用热太赫兹信源、分束器、光衰减器以及零差探测器来进行量子态的被动调制, 从而无需使用振幅与相位调制器以及量子随机数发生器, 有效简化星间太赫兹连续变量量子密钥分发方案的实施. 本文详细分析了基于被动态制备的星间太赫兹连续变量量子密钥分发方案的安全性以及性能. 仿真结果表明随着热太赫兹信源的平均光子数以及量子信号频率的增大, 所提出方案的性能得到显著提升, 并且越来越接近理想高斯调制星间太赫兹连续变量量子密钥分发方案的性能. 此外, 本文还给出了该方案的本振系统原理图并从实际角度分析所提出方案的物理可行性与现有技术实现途径, 为构建低成本、低复杂度的星间量子通信网络提供参考.

关键词: 被动态制备, 连续变量, 量子密钥分发, 星间链路, 太赫兹

DOI: 10.7498/aps.75.20251774 **CSTR:** 32037.14.aps.75.20251774

1 引 言

量子密钥分发 (quantum key distribution, QKD) 基于量子力学的基本定律, 能够在由攻击者 Eve 控制的不安全信道上允许合法通信方 Alice 与 Bob 建立一串安全密钥[1,2]. 一般而言, QKD 根据不同的实现方式, 可以进一步分为离散变量 (discrete-variable, DV)QKD[3–8] 与连续变量 (continuous-variable, CV)QKD[9–15]. DV-QKD 方案通常采用单光子自由度来对密钥信息进行编码, 并采用单光子探测器来对所编码的密钥信息进行测量. 而 CV-QKD 方案则是采用光场的正则分量来进行密钥信息的分发, 并且容易与现有的光学设备比如零差或外差探测器进行结合, 有效避免单光子计数的缺陷所带来的影响.

高斯调制相干态 (Gaussian-modulated coherent state, GMCS) 方案作为一种重要的 CVQKD 方案, 在理论上已经被证明能够抵御任意的集体攻击[16,17] 与相干攻击[18,19]. 不仅如此, 该方案已在实验室[20–23] 和现场测试[24,25] 中通过实验实现, 这证明了其在城域量子网络中的优越适用性. 在 GMCS

* “量子通信与量子计算机”国家科技重大专项 (批准号: 20212D0300703) 和福建省自然科学基金 (批准号: 2023J01940) 资助的课题.

† 通信作者. E-mail: duanhuang@csu.edu.cn

第二十八届中国科协年会学术论文

方案中, 发送方 Alice 首先利用真随机数发生器生成服从高斯分布的随机数 $x_{\rm A}$ 与 $p_{\rm A}$, 随后制备相干态 $|x_{\rm A}+{\rm i}p_{\rm A}\rangle$ 并将其经非可信信道发送给探测方 Bob. 在上述过程中, 量子态的制备是采用振幅与相位调制器对激光器的输出光进行调制, 通常称为"量子态的主动制备". 然而, 在 GMCS 方案中, 由于主动调制其调制格式相对复杂并且仅能够容忍较小的调制误差, 因此实际情况下实现该调制方案存在挑战性.

针对 GMCS 方案中主动调制所存在的缺点, 一种有效的方法是采用基于被动态制备的 CVQKD 方案 [26]. 在该方案中, 无需采用振幅与相位调制器以及随机数发生器来进行信息编码, 取而代之的则是采用热光源、分束器、光衰减器以及零差探测器, 在很大程度上简化了 CVQKD 方案的实现并使其更具实用性. 根据文献 [26] 可知, 当 Alice 端的发送装置是可信时, 基于被动态制备的 CVQKD 方案等价于 GMCS CVQKD 方案. 这意味着 GMCS CVQKD 方案中已建立的安全性证明方法可以直接用于基于被动态制备的 CVQKD 方案中. 最近, Qi 等 [27] 与 Huang 等 [28] 通过实验对被动态制备方案进行验证. 此外, 该被动态制备方案已被应用于测量设备无关 CVQKD 方案 [29]、连续变量量子秘密共享方案 [30]、本地本振 CVQKD 方案 [31] 以及自由空间 CV-QKD 方案 [32].

CVQKD 方案通常是通过光通信或微波通信系统来对信息进行处理. 换言之, 目前大多数 CVQKD 方案以光场的正则分量或微波光子作为密钥信息的载体, 经由光纤或自由空间信道实现信息传输. 随着无线通信的飞速发展, 无线频谱资源的稀缺性日趋明显. 众所周知, 太赫兹 (terahertz, THz) 通信 [33–39] 具有带宽大、传输速率高等特点, 因此被认为在满足高速数据传输需求方面拥有巨大潜力. THz 通信能够应用于高速无线通信的室内信道 [33–37], 但是 THz 波段容易被普遍存在的大气水分子吸收, 因此基于室内信道的 THz 通信其传输距离受到极大的限制 [36,40]. 幸运的是, THz 通信在星间通信领域具有巨大潜力 [41,42], 主要原因是在真空中水分子的浓度非常小, 可以忽略不计, 并且 Liu 等 [35] 与 Wang 等 [41] 对其可行性进行了研究. 此外, 与微波频带 [43] 相比, THz 频带的环境热噪声相对较低, 这表明 THz 频带的安全阈值更高. 因此, 研究 THz 通信以构建高速星间量子通信网络具有重要意义.

基于上述被动态制备方案以及 THz 通信在星间通信领域的优势, 本文提出基于被动态制备的星间 THz-CVQKD 方案. 在该方案中, 采用热 THz 信源、分束器、光衰减器以及零差探测器来进行量子态的被动制备, 因此无需采用传统 GMCS CV-QKD 方案中主动调制器件, 能够显著简化 THz-CVQKD 方案的实现. 此外, 所提出的方案将星间信道模型应用于基于被动态制备的 THz-CVQKD 方案中用于进行方案的安全性以及性能分析. 仿真结果表明随着热 THz 信源平均光子数以及频率的增大, 所提出方案的性能能够得到显著提升, 并且越来越接近理想 GMCS 星间 THz-CVQKD 方案的性能, 从而验证了长距离被动调制 THz-CVQKD 方案在星间链路中的可行性. 最后, 本文还给出了该方案的本振系统原理图并从实际角度分析所提出方案的物理可行性与现有技术实现途径, 为构建低成本、低复杂度的星间量子通信网络提供参考. 本文第 2 节对所提出的基于被动态制备的星间 THz-CVQKD 方案进行描述; 第 3 节进行方案密钥率计算; 第 4 节进行方案性能分析; 第 5 节总结全文.

2 基于被动态制备的星间 THz-CVQKD 方案

基于被动态制备的星间 THz-CVQKD 方案的原理图如图 1 所示. 在所提出的方案中, 首先, 发送方 Alice 采用 50∶50 分束器将 THz 热源的输出模分成两部分, 即 M_1 与 M_2, 其中 M_1 经由衰减器 ${\rm Att}_1$ 进行衰减后, Alice 再将其通过星间链路信道发送给接收方 Bob, 而另一部分 M_2 则由发送方 Alice 采用外差探测器直接进行本地测量. 其次, 接收方 Bob 对所接收到的量子态进行外差探测, 得到其正则分量 $x_{\rm B}$ 与 $p_{\rm B}$. 经过帧同步与过噪声抑制操作后, 发送方 Alice 与接收方 Bob 进一步通过认证的经典信道执行参数估计. 最后, Alice 与 Bob 通过执行协商以及保密增强, 提取出一串安全密钥.

从上述步骤中可以发现, 第 1 步中 Alice 的密钥信息的获取无需采用高消光比的振幅和相位调制器进行主动调制, 而是由 Alice 在本地执行外差探测直接获得. 除了第 1 步外, 其余步骤都和传统

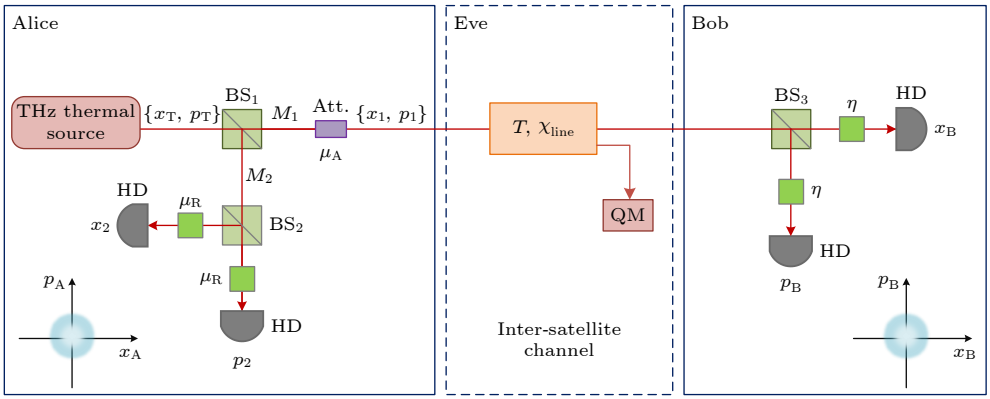

图 1 基于被动态制备的星间 THz-CVQKD 方案的原理图, 其中 $BS_{1—3}$, 分束器; HD, 零差探测器; THz, 太赫兹; Att, 光衰减器; QM, 量子存储器; μ_R, Alice 零差探测器的量子效率; η, Bob 零差探测器的量子效率; μ_A, 光衰减器的透过率; T, 非可信星间信道的透过率; χ_{line}, 归结于信道输入端的信道附加噪声

Fig. 1. Schematic diagram of inter-satellite THz-CVQKD protocol based on passive state preparation. BS_{1-3}, beam splitter; HD, homodyne detector; THz, terahertz; Att, optical attenuator; QM, quantum memory; μ_R, the quantum efficiencies of Alice's homodyne detectors; η, the quantum efficiencies of Bob's homodyne detectors; μ_A, the transmittance of optical attenuator; T, transmittance of inter-satellite channel; χ_{line}, the channel-added noise referred to the channel input.

的高斯调制 CVQKD 方案相同. 此外, 从攻击者 Eve 的角度出发, 在被动态制备方案中, 上述被 Alice 通过星间链路信道发送给接收方 Bob 的量子态与传统的主动态制备方案中的量子态是相同的. 因此, 传统 GMCS CVQKD 方案已构建完备的安全性证明方法, 可以直接应用到本文方案中[26].

计算方案的密钥率之前, 需要先确定在被动态制备过程中会引入多少额外过噪声. 为了简化分析, 此处只考虑量子态正则分量 X, 另一个正则分量 P 可以通过类似的方法进行分析. 根据文献 [26], 发送给 Bob 的量子态其正则分量 X 的表达式可写为

$$x_1 = \sqrt{\frac{\mu_A}{2}}x_T + \sqrt{1-\frac{\mu_A}{2}}x_{\omega 1}, \tag{1}$$

其中 x_T 表示 THz 热源的输出模的正则分量 X, μ_A 表示可变衰减器的透过率, $x_{\omega 1}$ 表示由分束器和衰减器所引入的真空噪声.

类似地, Alice 直接进行本地测量的 M_2, 其正则分量 X 的表达式为

$$x_2 = \sqrt{\frac{\mu_R}{4}}x_T + \sqrt{1-\frac{\mu_R}{4}}x_{\omega 2} + D_{Ael}, \tag{2}$$

其中 $x_{\omega 2}$ 表示由两个平衡分束器以及探测器损耗所引入的真空噪声, μ_R 与 D_{Ael} 分别表示发送方 Alice 探测器的量子效率与电噪声. 此处, D_{Ael} 是均值为零并且方差为 υ_{Ael} 的高斯噪声. 值得一提的是, 本文中所有噪声方差都定义在散粒噪声单元中.

需要指出的是, Alice 可以利用其测量结果 x_2 来对 x_1 进行估计, 其估计值 x_A 的表达式可写为

$$x_A = \sqrt{\frac{2\mu_A}{\mu_R}}x_2. \tag{3}$$

结合 (1) 式—(3) 式, Alice 对 x_1 的不确定性为 Θ, 则 Θ 的表达式可写为

$$\Theta = \left\langle (x_A - x_1)^2 \right\rangle = \frac{2\mu_A}{\mu_R}\left(1 - \frac{\mu_R}{2} + \upsilon_{Ael}\right) + 1. \tag{4}$$

根据 (4) 式, 在所提出的方案中, 由被动态制备所引入的过噪声其表达式为

$$\xi_A = \Theta - 1 = \frac{2\mu_A}{\mu_R}\left(1 - \frac{\mu_R}{2} + \upsilon_{Ael}\right). \tag{5}$$

由于调制方差 $V_A = \mu_A r_0$, 其中 r_0 表示热源的平均光子数, 因此 (5) 式可重新写为

$$\xi_A = \frac{2V_A}{\mu_R r_0}\left(1 - \frac{\mu_R}{2} + \upsilon_{Ael}\right). \tag{6}$$

因为由被动态制备所引入的过噪声 ξ_A 在所提出的方案中总是存在的, 所以为了获得理想的方案性能, 有必要对其进行抑制. 图 2 给出了在不同调制方差 V_A 下, 由被动态制备引入的过噪声 ξ_A 与平均光子数 r_0 的关系. 从图 2 可以发现, 平均光子数 r_0 越大, 由被动态制备引入的过噪声 ξ_A 则越小. 特别是在 V_A 值较大的情况下, 平均光子数 r_0 的增大对 ξ_A 的抑制效果更加显著. 此外, 调制方差 V_A 的减小也能够有效抑制由被动态制备引入的过噪声 ξ_A. 由于在本方案中采用的是可变衰减器, 其透过率数值可以根据实际需求进行调整. 因此, 若在实际条件下要对基于被动态制备的星间 THz-CVQKD

系统的调制方差进行数值调整, 可在保持 THz 热源的平均光子数不变的情况下, 通过利用可变衰减器来对透过率参数 $\mu_{\rm A}$ 进行调整, 以达到调整系统调制方差数值的目的.

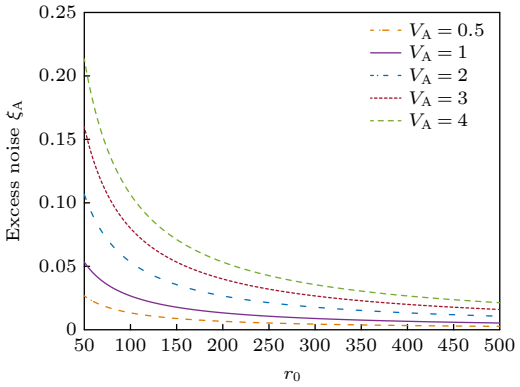

图 2 不同调制方差 $V_{\rm A}$ 下由被动态制备引入的过噪声 $\xi_{\rm A}$ 与平均光子数 r_0 的关系

Fig. 2. Excess noise $\xi_{\rm A}$ introduced by passive state preparation vs. the average photon number r_0 under different modulation variances $V_{\rm A}$.

3 方案密钥率计算

本节首先介绍基于被动态制备的 THz-CVQKD 方案的自由空间星间链路的信道模型, 之后利用该信道模型来计算方案的密钥率.

3.1 信道模型

近年来, 太赫兹通信被认为是支撑高速无线通信网络需求增长的关键技术之一. 在本方案中, Alice 与 Bob 之间的信道为一条星间太赫兹信道. 当太赫兹波通过自由空间信道进行传输时, 其会受到湍流、散射和吸收等影响. 这些大气效应 (尤其是大气水分子的吸收) 极大限制了太赫兹波的通信性能. 然而在星间链路中, 大气吸收所带来的影响以及光束漂移效应实际上都可以忽略不计. 这使得我们能够将单衍射信道模型近似表征为固定衰减, 而衍射效应所造成的损耗仅考虑由接收孔径处的衍射光束的尺寸来推导得出 [38,39]. 因此, 星间链路中透过率 T 的表达式可写为 [41]

$$T = 1 - \exp\left(-\frac{2P_{\rm r}^2}{\Psi(L)^2}\right), \tag{7}$$

式中 $P_{\rm r}$ 表示 Bob 端接收器孔径的半径; L 表示光束的传输距离; $\Psi(L)$ 表示传输距离 L 处的波束半径, 采用高斯近似, $\Psi(L)$ 的表达式可写为

$$\Psi(L) = \sigma_0\sqrt{1+\left(\frac{\gamma L}{\pi\sigma_0^2}\right)^2}, \tag{8}$$

其中 σ_0 表示光束腰半径, γ 表示太赫兹波的波长. 值得一提的是, 接收器孔径和光束腰会受到实际硬件局限性的影响. 在本方案的信道模型中, 将接收器孔径半径 $P_{\rm r}$ 以及光束腰半径 σ_0 设定为 0.6 m[39,44], 并且将环境温度设定为 30 K[45].

3.2 方案密钥率

本文所提出的方案在反向协商下, 其渐近密钥率的表达式可写为 [46,47]

$$K = \beta I_{\rm AB} - \chi_{\rm BE}, \tag{9}$$

其中 $I_{\rm AB}$ 为 Alice 和 Bob 的互信息量, β 为反向协商效率, $\chi_{\rm BE}$ 为 Bob 与攻击者 Eve 的 Holevo 界.

由于探测方 Bob 执行外差探测, 因此 Bob 输入端的探测噪声为

$$\chi_{\rm het} = [1 + (1-\eta) + 2\upsilon_{\rm Bel}]/\eta, \tag{10}$$

其中 η 表示 Bob 端探测器的量子效率, $\upsilon_{\rm Bel}$ 表示探测器的电噪声.

归结于信道输入端的信道附加噪声其表达式可写为

$$\chi_{\rm line} = 1/T - 1 + \xi_{\rm A} + \xi_0, \tag{11}$$

其中 $\xi_{\rm A}$ 表示由被动态制备所引入的过噪声, ξ_0 表示其他非理想因素引入的等效噪声. 需要指出的是, 在 3.1 节中所采用的衍射主导型无衰减星间信道模型主要基于文献 [38,39], 其中并没有着重分析星间链路 THz-CVQKD 方案中卫星平台抖动、指向误差等实际因素的影响. 该模型聚焦于衍射效应这个主要损耗因素, 其主要原因在于星间链路处于近真空环境, 在分析时可忽略大气吸收、散射等地面或低空信道的损耗因素. 而对于卫星平台抖动、指向误差等实际因素的影响, 本质上可归结为引入额外的链路损耗、对准偏差噪声等, 最终均表现为系统的额外不可控噪声. 在 (11) 式中, 参数 ξ_0 表示其他非理想因素引入的等效噪声. 因此在进行方案性能分析时, 可以将卫星平台抖动、指向误差等因素引入的过噪声归并到参数 ξ_0 中, 即可保证原有模型的简洁性, 又通过此种方式充分考虑了实际约束因素对方案性能的影响.

归结于信道输入端的总噪声为

$$\chi_{\rm tot} = \chi_{\rm line} + \chi_{\rm het}/T. \tag{12}$$

Alice 与 Bob 互信息量的表达式可写为

$$I_{\mathrm{AB}}=\log_2\frac{V+\chi_{\mathrm{tot}}}{1+\chi_{\mathrm{tot}}}, \tag{13}$$

式中 $V=V_{\mathrm{A}}+V_0$, 其中 V_{A} 为调制方差; V_0 表示散粒噪声, 其表达式可写为[48]

$$V_0=2\overline{n}_0+1. \tag{14}$$

这里

$$\overline{n}_0=\frac{1}{\exp[f\hbar/(\varphi_{\mathrm{w}}\phi_{\mathrm{b}})]-1}, \tag{15}$$

其中 f 表示量子信号频率, $\hbar$ 表示普朗克常数, φ_{w} 表示温度 (开尔文), ϕ_{b} 表示玻尔兹曼常数. 一般来说, 散粒噪声 V_0 其表达式可写为 $V_0=1+\kappa$. 当参数 $\kappa=0$ 时, 量子态为相干态; 而当参数 $\kappa>0$ 时, 量子态为热态.

为了计算 χ_{BE}, 此处采用实际噪声模型, 即在该模型中攻击者 Eve 无法控制探测方 Bob 系统内部的损耗, 并且 Bob 端的探测器电噪声被认为是可信任的[14]. 该噪声模型已经被广泛应用于 CV-QKD 实验中[14,22,46]. 基于此种实际噪声模型, Eve 与 Bob 之间信息量的 Holevo 界表达式可写为

$$\chi_{\mathrm{BE}}=\sum_{i=1}^{2}G\left(\frac{\rho_i-1}{2}\right)-\sum_{i=3}^{5}G\left(\frac{\rho_i-1}{2}\right), \tag{16}$$

式中 $G(x)=(x+1)\log_2(x+1)-x\log_2 x$; 并且

$$\rho_{1,2}^2=\frac{1}{2}\left(\Delta\pm\sqrt{\Delta^2-4D}\right), \tag{17}$$

其中,

$$\begin{aligned}&\Delta=V^2+T^2(V+\chi_{\mathrm{line}})^2-2T(V^2-1),\\&D=(T+TV\chi_{\mathrm{line}})^2;\end{aligned} \tag{18}$$

而 $\rho_{3,4}$ 其表达式可写为

$$\rho_{3,4}^2=\frac{1}{2}\left(A\pm\sqrt{A^2-4B}\right), \tag{19}$$

其中,

$$\begin{aligned}A=&\frac{1}{T^2(V+\chi_{\mathrm{tot}})^2}\Big\{\Delta\chi_{\mathrm{het}}^2+D+1\\&+2\chi_{\mathrm{het}}\left[V\sqrt{D}+T(V+\chi_{\mathrm{line}})\right]\\&+2T(V^2-1)\Big\},\\B=&\left[\frac{V+\sqrt{D}\chi_{\mathrm{het}}}{T(V+\chi_{\mathrm{tot}})}\right]^2;\end{aligned} \tag{20}$$

$$\rho_5=1. \tag{21}$$

基于 (13) 式—(21) 式, 可以计算出 (9) 式中方案的渐近密钥率.

4 基于被动态制备的星间 THz-CVQKD 方案性能分析与讨论

本节首先对基于被动态制备的星间 THz-CVQKD 方案性能进行分析, 之后从关键现实技术的角度对本文方案进行讨论.

4.1 方案性能分析

本节从安全密钥率和传输距离的角度对基于被动态制备的星间 THz-CVQKD 方案的性能进行分析, 并与理想 GMCS 星间 THz-CVQKD 方案 (采用振幅与相位调制器进行量子态主动调制) 的性能进行比较. 涉及全局的仿真参数以及设定如下: 根据文献 [36,38], Alice 端探测器的量子效率 $\mu_{\mathrm{R}}=0.6$, 电噪声 $\upsilon_{\mathrm{Ael}}=0.1$, Bob 端探测器的量子效率与电噪声同样分别设为 $\eta_{\mathrm{H}}=0.6$ 与 $\upsilon_{\mathrm{Bel}}=0.1$. 接收器孔径半径 P_{r} 以及光束腰半径 σ_0 均为 0.6 m[39,44], 环境温度 φ_{w} 为 30 K[45], 方案中其他非理想因素引入的等效噪声 $\xi_0=0.01$.

基于被动态制备的星间 THz-CVQKD 方案的密钥率与调制方差 V_{A} 的关系如图 3 所示, 协商效率 $\beta=0.96$, 传输距离 $L=100$ km, 其中图 3(a) 基于不同量子信号频率的情况下, 而图 3(b) 则基于不同平均光子数的情况下. 在图 3(a) 中频率 $f=20,\ 30,\ 40,\ 50$ THz, 并且平均光子数 $r_0=100$. 在图 3(b) 中平均光子数 $r_0=50,\ 80,\ 100,\ 150$, 并且频率 $f=50$ THz. 从图 3(a), (b) 可以发现, 随着频率 f 以及平均光子数 r_0 的减小, 调制方差 V_{A} 的可选择区域被逐渐压缩, 并且所提出方案的密钥率也逐渐降低. 然而当调制方差 $V_{\mathrm{A}}=2$ 时, 图 3(a), (b) 中的密钥率曲线总是存在峰值, 这表明调制方差 V_{A} 的最优值为 2. 因此, 在下面的仿真中, 调制方差 V_{A} 的取值为 2.

图 4 给出了在不同平均光子数下方案密钥率与传输距离的关系, 其中协商效率 $\beta=0.96$, 调制方差 $V_{\mathrm{A}}=2$. 图 4(a) 对应频率 $f=10$ THz, 图 4(b) 对应频率 $f=20$ THz, 图 4(c) 对应频率 $f=30$ THz, 而图 4(d) 对应频率 $f=50$ THz. 从图 4(a)—(d) 可以发现, 在相同的频率 f 下, 随着平均光子数 r_0 的增大, 所提出方案的密钥率与传输距离都有

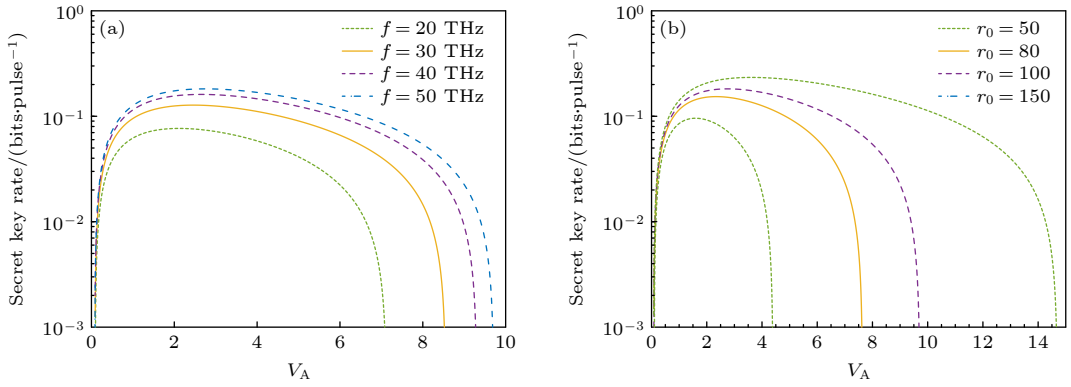

图 3 本文方案密钥率随调制方差 V_A 的变化 (a) $f = 20, 30, 40, 50$ THz, $r_0 = 100$; (b) $r_0 = 50, 80, 100, 150$, $f = 50$ THz

Fig. 3. Secret key rate vs. modulation variance V_A: (a) $f = 20, 30, 40, 50$ THz, $r_0 = 100$; (b) $r_0 = 50, 80, 100, 150$, $f = 50$ THz.

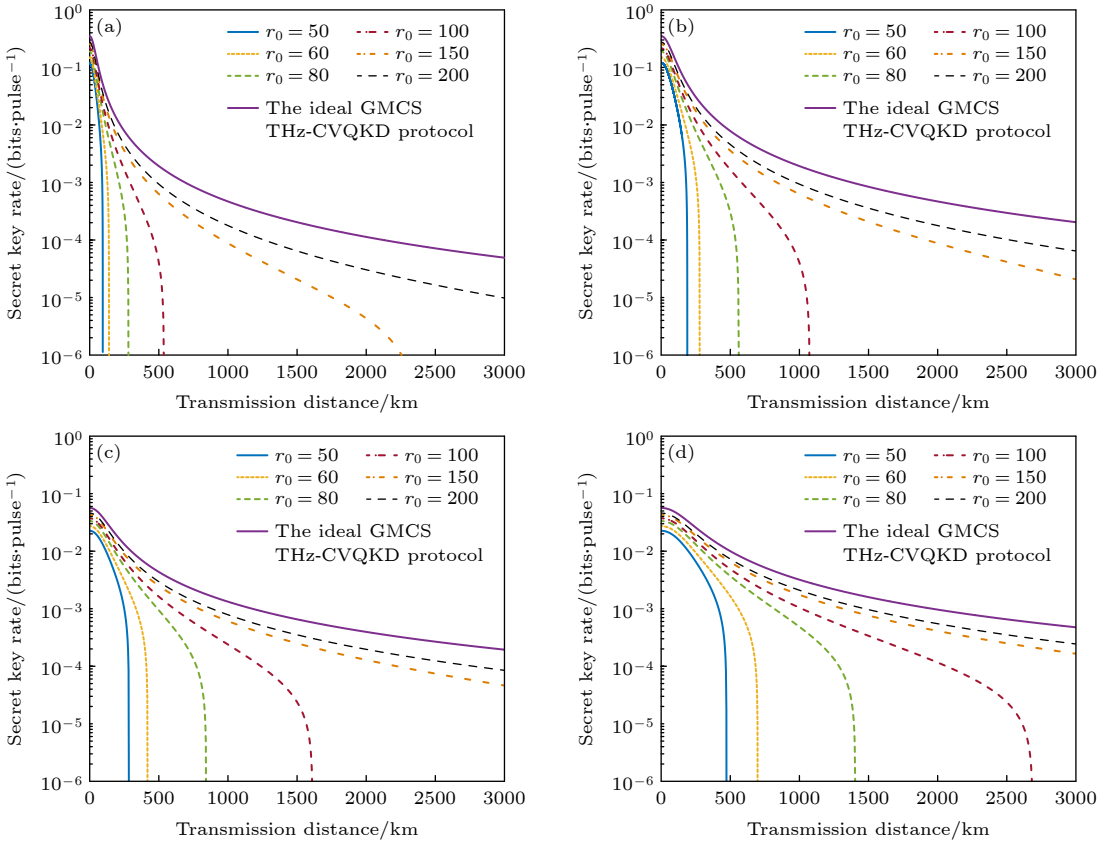

图 4 在不同平均光子数 r_0 下方案密钥率与传输距离的关系 (a) $f = 10$ THz; (b) $f = 20$ THz; (c) $f = 30$ THz; (d) $f = 50$ THz

Fig. 4. Secret key rate vs. distance under different average photon number r_0: (a) $f = 10$ THz; (b) $f = 20$ THz; (c) $f = 30$ THz; (d) $f = 50$ THz.

显著提升, 并且越来越接近理想 GMCS 星间 THz-CVQKD 方案的性能 (在图中简记为 The ideal GMCS case). 比如当频率 $f = 30$ THz 时, 平均光子数 $r_0 = 60$, 所提出方案的最大传输距离不超过 500 km; 而当 $r_0 = 100$ 时, 所提出方案的最大传输距离则超过 1500 km. 由 (11) 式可知, 出现此现象的原因在于当 THz 热源平均光子数 r_0 增大时, 由被动态制备所引入的过噪声 ξ_A 减小, 因此能够有效提升方案的密钥率与传输距离. 当 THz 热源平均光子数 r_0 足够大时, 即能够将 ξ_A 抑制到足够小的值时, 本文所提出的方案其性能就越来越接近理想高斯调制星间 THz-CVQKD 方案的性能. 此外, 随着频率 f 的增大, 采用具有相同平均光子数的 THz 热源可以获得更高的密钥率以及更远的传输距离. 例如当频率 $f = 10$ THz 时, 平均光子数 $r_0 = 80$ 所得到的方案最大传输距离不超过 300 km; 而

当频率 $f=50$ THz 时, 平均光子数 $r_0=80$ 所得到的方案最大传输距离则接近 1500 km.

图 5 给出了方案密钥率与传输距离 L 以及调制方差 $V_{\rm A}$ 的关系, 其中协商效率 $\beta=0.96$. 此外, 图 5 也给出了理想 GMCS 星间 THz-CVQKD 方案 (The ideal GMCS case) 的性能曲面, 用于和所提出的方案的性能进行比较. 从图 5 可以观察到, 随着调制方差 $V_{\rm A}$ 的增大, 本文所提出的方案其密钥率先增大后减小, 即所提出的方案其性能曲面呈"拱形"形状. 当调制方差 $V_{\rm A}$ 的取值较大时, 方案的密钥率与最大传输距离将减小. 比如当 $V_{\rm A}=6$ 时, 平均光子数 $r_0=80$ 所对应的性能曲面其最大传输距离仅为 200 km 左右; 而当 $V_{\rm A}=8$ 时, 平均光子数 $r_0=80$ 所对应的性能曲面其最大传输距离缩减为 100 km 左右. 此外, 随着平均光子数 r_0 的增大, 本文所提出方案的性能曲面越来越接近理想 GMCS 星间 THz-CVQKD 方案的性能曲面.

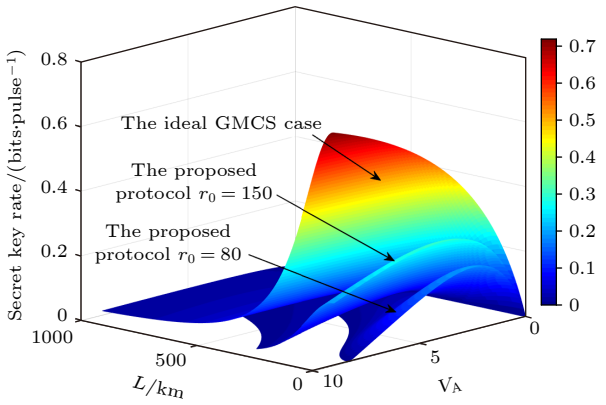

图 5 方案密钥率与传输距离 L 以及调制方差 $V_{\rm A}$ 的关系

Fig. 5. Secret key rate vs. distance L and modulation variance $V_{\rm A}$.

图 6 给出了在不同传输距离 L 下方案密钥率与频率 f 的关系, 其中调制方差 $V_{\rm A}=2$, 平均光子数 $r_0=80$, 并且 $L=200,\ 400,\ 600$ km. 图 6 也分别给出了理想 GMCS 星间 THz-CVQKD 方案在上述每个传输距离处的性能曲线作为比较. 由图 6 可知, 随着传输距离 L 的增大, 频率 f 的可使用范围减小. 换言之, 传输距离 L 的增大使得所提出的方案需要更高的频率 f 以保证密钥的正常生成. 比如当 $L=200$ km 时, 本方案所需的频率 f 仅为 8 THz 左右; 而当 $L=600$ km 时, 本方案所需的频率 f 则超过 20 THz. 因此, 为了实现远距离星间量子通信, 需要采用合适的频率 f. 此外, 在相同的传输距离的情况下, 理想 GMCS 星间 THz-CVQKD 方案的性能 (图 6 中虚线所表示的性能曲线) 要优于本文所提出方案的性能.

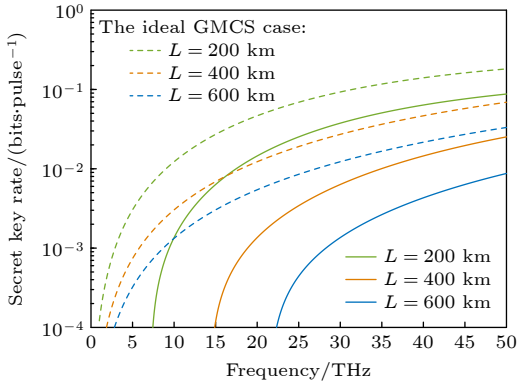

图 6 不同传输距离 L 下方案密钥率与频率 f 的关系

Fig. 6. Secret key rate vs. the frequency f under different distances L.

值得一提的是, 从图 4—图 6 可以发现, 理想 GMCS 星间 THz-CVQKD 方案的性能始终优于所提出的基于被动态制备的星间 THz-CVQKD 方案的性能. 而这也符合我们的预期, 主要原因是在理想 GMCS 星间 THz-CVQKD 方案中为了简化分析通常假定信源是完美的, 因此并没有考虑信源的不完美所引入的过噪声对方案性能的影响, 而只考虑信道过噪声对方案性能的影响. 在本文所提出的方案中, 将被动态制备所引入的过噪声 $\xi_{\rm A}$ 对方案性能的影响考虑进去并进行详细分析, 因此理想 GMCS 星间 THz-CVQKD 方案的性能要优于本文所提出方案的性能.

4.2 方案关键技术讨论

基于被动态制备的星间 THz-CVQKD 方案本振系统原理图如图 7 所示. 在发送端, Alice 采用平衡分束器将 THz-ASE 源产生的信号脉冲 S_0 分为两部分: 其中一部分经过可变光衰减器, 该部分脉冲用 S_1 表示; 而另一部分 S_2 则直接由 Alice 利用外差探测器进行直接测量. 与此同时, Alice 利用 THz 本振源 (例如 THz 量子级联激光器) 发射一束激光脉冲 L_0, 同样用平衡分束器将其分为两部分: 其中一部分 L_1 通过偏振分束器与信号脉冲 S_1 进行耦合, 之后由喇叭天线发射, 通过星间链路传输到 Bob 端; 另一部分用 L_2 进行表示, 该部分作为本振光脉冲用于连续对信号脉冲 S_2 进行本地外差探测, 得到测量结果 $\{X_2, P_2\}$.

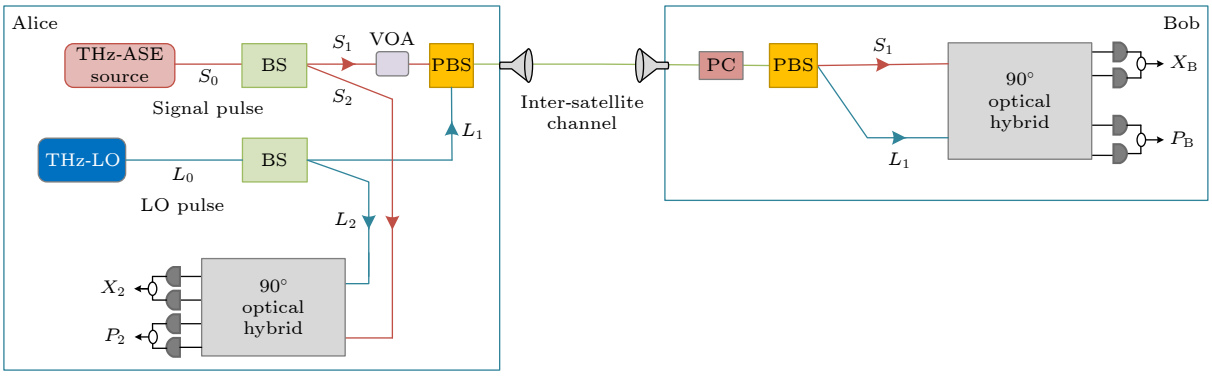

图 7 基于被动态制备的星间 THz-CVQKD 方案本振系统原理图, 其中 THz, 太赫兹; ASE, 放大自发辐射; LO, 本振源; VOA, 可变光衰减器; PBS, 偏振分束器; PC, 偏振控制器

Fig. 7. Schematic diagram of local oscillator system based on inter-satellite THz-CVQKD protocol with passive state preparation. THz, terahertz; ASE, amplified spontaneous emission; LO, local oscillator; VOA, variable optical attenuator; PBS, polarization beam splitter; PC, polarization controller.

当 Bob 利用喇叭天线接收到从 Alice 处发送过来的脉冲时, 经过偏振控制器后, Bob 用另一个偏振分束器将所接收到的脉冲清楚地分束为 S_1 与 L_1, 并共同传输到 Bob 的外差探测器进行测量, 得到测量结果 $\{X_{\rm B}, P_{\rm B}\}$. 最后 Alice 和 Bob 执行包括参数估计、纠错和保密增强等标准的后处理过程, 从而获得共享密钥.

根据文献 [26] 可知, 可以采用放大自发辐射 (amplified spontaneous emission, ASE) 源作为热源实现基于被动态制备的 CV-QKD 方案. ASE 源是由光纤放大器 (半导体增益介质) 产生, 输入为真空态时, 输出为天然热态, 即其光子统计遵循 Bose-Einstein 分布, 二阶关联函数 $g^{(2)}(0)=2.012$, 与理想热态理论值 2 非常接近. 由 Voss 等 [49] 的研究可知, 半导体增益介质受非相干泵浦后, 铒离子能级上的电子发生自发辐射, 产生非相干的热态光子, 而这正是 ASE 源的辐射机制. 虽然 Qi 等 [26] 研究所采用的 ASE 源是针对光波段的, 但 ASE 源的辐射机制并没有涉及频段, 即 ASE 源的辐射机制与频段无关, 其物理原理无论是在光波段还是在太赫兹波段均适用. 换言之, ASE 源的辐射机制既能在光波段实现高亮度 (平均光子数足够多), 同样也能够在太赫兹波段实现此类高亮度.

由上述分析可知, ASE 源的辐射机制其物理原理无论是在光波段还是在太赫兹波段均适用. 然而, 从现实技术的角度看, ASE 源辐射具体频段的实现主要依赖于增益介质的材料以及相应的结构参数. 根据光子能量公式 $E=h\nu=hc/\lambda$, 若要实现不同频段的 ASE 源, 可通过对增益介质的能级间距进行精准调控, 使得载流子跃迁的能量差能够匹配目标频段的光子能量. 针对本文方案中的 THz 热源 (THz 波段 ASE 源), 可采用基于 InP 基量子级联结构的 THz-ASE 源, 即以 InP 基量子级联异质结构 (如 InGaAs/InAlAs 异质结构) 为增益介质 [50–52], 通过对其中的能级间距进行精准调控来满足 THz 波段光子能量的需求, 使载流子传输稳定, 适用于星间传输环境. 为确保辐射的非相干性, 可采用低电压非相干电注入泵浦的方式使得增益介质内载流子形成粒子数反转, 为后续非相干自发辐射的实现奠定基础.

5 结 论

本文提出了基于被动态制备的星间 THz-CVQKD 方案. 相比于 GMCS 星间 THz-CVQKD 方案, 所提出的方案无需使用振幅与相位调制器以及 QRNG 进行量子态的主动调制, 取而代之的则是采用热 THz 信源、分束器、光衰减器以及零差探测器来进行量子态的被动调制, 从而显著简化星间 THz-CVQKD 方案的实施并使其更具实用性. 仿真结果表明在相同的频率 f 下, 随着平均光子数 r_0 的增大, 所提出方案的密钥率与传输距离都有显著的提升, 并且越来越接近理想 GMCS 星间 THz-CVQKD 方案的性能, 并且随着频率 f 的增大, 采用具有相同平均光子数的 THz 热源可以获得更高的密钥率以及更远的传输距离. 此外, 随着调制方差 $V_{\rm A}$ 的增大, 本文所提出的方案其密钥率先增大后减小, 即存在一个最优调制方差, 当调制方差 $V_{\rm A}$

的取值超过最优值时, 所提出方案的密钥率和传输距离将减小. 因此, 为了实现高速远距离星间量子通信, 需要采用合适的量子信号频率 f 以及调制方差 $V_{\rm A}$. 最后, 本文给出了基于被动态制备的星间 THz-CVQKD 方案本振系统原理图并从实际角度分析本方案的物理可行性与现有技术实现途径. 本文提出的方案具有较低的成本与复杂性, 为推动星间量子通信网络的实用化发展提供参考.

参考文献

[1] Xu F, Ma X, Zhang Q, Lo H K, Pan J W 2020 *Rev. Mod. Phys.* **92** 025002

[2] Pirandola S, Andersen U L, Banchi L, Berta M, Bunandar D, Colbeck R, Englund D, Gehring T, Lupo C, Ottaviani C, Pereira J L, Razavi M, Shaari J S, Tomamichel M, Usenko V C, Vallone G, Villoresi P, Wallden P 2020 *Adv. Opt. Photon.* **12** 1012

[3] Nadlinger D P, Drmota P, Nichol B C, Araneda G, Main D, Srinivas R, Lucas D M, Balance C J, Ivanov K, Tan E Y Z, Sekatski P, Urbanke R L, Renner R, Sangouard N, Bancal J D 2022 *Nature* **607** 682

[4] Liu W Z, Zhang Y Z, Zhen Y Z, Li M H, Liu Y, Fan J, Xu F, Zhang Q, Pan J W 2022 *Phys. Rev. Lett.* **129** 050502

[5] Wang S, Yin Z Q, He D Y, et al. 2022 *Nat. Photon.* **16** 154

[6] Zhu H T, Huang Y, Liu H, Zeng P, Zou M, Dai Y, Tang S, Li H, You L, Wang Z, Chen Y A, Ma X, Chen T Y, Pan J W 2023 *Phys. Rev. Lett.* **130** 030801

[7] Zahidy M, Mikkelsen M T, Müller R, et al. 2024 *npj Quantum Inf.* **10** 2

[8] Khodadad Kashi A, Kues M 2025 *Light Sci. Appl.* **14** 49

[9] Weedbrook C, Pirandola S, García-Patrón R, Cerf N J, Ralph T C, Shapiro J H, Lloyd S 2012 *Rev. Mod. Phys.* **84** 621

[10] Laudenbach F, Pacher C, Fung C H, Poppe A, Peev M, Schrenk B, Hentschel M, Walther P, Hübel H 2018 *Adv. Quantum Technol.* **1** 1800011

[11] Wu X D, Huang D 2023 *Acta Phys. Sin.* **72** 050303 (in Chinese) [吴晓东, 黄端 2023 物理学报 **72** 050303]

[12] Zhang Y, Bian Y, Li Z, Yu S, Guo H 2024 *Appl. Phys. Rev.* **11** 011318

[13] Wang T, Huang P, Li L, Zhou Y M, Zeng G H 2024 *New J. Phys.* **26** 023002

[14] Mele F A, Lami L, Giovannetti V 2025 *Nat. Photon.* **19** 329

[15] Wang P, Tian Y, Li Y M 2025 *Sci. China Inf. Sci.* **68** 180501

[16] Navascues M, Grosshans F, Acin A 2006 *Phys. Rev. Lett.* **97** 190502

[17] Leverrier A 2017 *Phys. Rev. Lett.* **118** 200501

[18] Scarani V, Renner R 2008 *Phys. Rev. Lett.* **100** 200501

[19] Leverrier A, García-Patrón R, Renner R, Cerf N J 2013 *Phys. Rev. Lett.* **110** 030502

[20] Jouguet P, Kunz-Jacques S, Leverrier A, Grangier P, Diamanti E 2013 *Nat. Photon.* **7** 378

[21] Huang D, Huang P, Lin D K, Zeng G H 2016 *Sci. Rep.* **6** 19201

[22] Zhang Y C, Chen Z Y, Pirandola S, Wang X Y, Zhou C, Chu B J, Zhao Y J, Xu B J, Yu S, Guo H 2020 *Phys. Rev. Lett.* **125** 010502

[23] Hajomer A A, Derkach I, Jain N, Chin H M, Andersen U L, Gehring T 2024 *Sci. Adv.* **10** eadi9474

[24] Huang D, Huang P, Li H S, Wang T, Zhou Y M, Zeng G H 2016 *Opt. Lett.* **41** 3511

[25] Zhang Y C, Li Z Y, Chen Z Y, Weedbrook C, Zhao Y J, Wang X Y, Huang Y D, Xu C C, Zhang X X, Wang Z Y, Li M, Zhang X Y, Zheng Z Y, Chu B J, Gao X Y, Meng N, Cai W W, Wang Z, Wang G, Yu S, Guo H 2019 *Quantum Sci. Technol.* **4** 035006

[26] Qi B, Evans P G, Grice W P 2018 *Phys. Rev. A* **97** 012317

[27] Qi B, Gunther H, Evans P G, Williams B P, Camacho R M, Peters N A 2020 *Phys. Rev. Appl.* **13** 054065

[28] Huang P, Wang T, Chen R, Wang P, Zhou Y M, Zeng G H 2021 *New J. Phys.* **23** 113028

[29] Bai D Y, Huang P, Ma H X, Wang T, Zeng G H 2019 *J. Phys. B* **52** 135502

[30] Wu X D, Wang Y J, Huang D 2020 *Phys. Rev. A* **101** 022301

[31] Wu X D, Wang Y J, Guo Y, Zhong H, Huang D 2021 *Phys. Rev. A* **103** 032604

[32] Zhang M Q, Huang P, Wang P, Wei S, Zeng G 2023 *Opt. Lett.* **48** 1184

[33] Ottaviani C, Woolley M J, Erementchouk M, Federici J F, Mazumder P, Pirandola S, Weedbrook C 2020 *IEEE J. Sel. Areas Commun.* **38** 483

[34] Kundu N K, Dash S P, Mckay M R, Mallik R K 2021 *IEEE Commun. Lett.* **25** 3345

[35] Liu C J, Zhu C H, Liu X, Nie M, Yang H, Pei C X 2021 *IEEE Photon. J.* **13** 7600113

[36] He Y, Mao Y, Huang D, Liao Q, Guo Y 2020 *Opt. Express* **28** 32386

[37] Liu X, Zhu C H, Chen N, Pei C X 2018 *Quantum Inf. Process.* **17** 304

[38] Liu C J, Zhu C H, Li Z H, Nie M, Yang H, Pei C X 2021 *Entropy* **23** 1223

[39] Liu C J, Zhu C H, Nie M, Yang H, Pei C X 2022 *Opt. Express* **30** 14798

[40] Seeds A J, Shams H, Fice M J, Renaud C C 2015 *J. Lightwave Technol.* **33** 579

[41] Wang Z, Malaney R, Green J 2019 *Proceedings of the ICC IEEE International Conference on Communications (ICC)* Shanghai, China, May 20–24, 2019 p1

[42] Walker C K, Kulesa C A 2005 *Proceedings of the Joint 30th International Conference on Infrared and Millimeter Waves & 13th International Conference on Terahertz Electronics*, Williamsburg, USA, September 19–23, 2005 p3

[43] Papanastasiou P, Ottaviani C, Pirandola S 2018 *Phys. Rev. A* **98** 032314

[44] Derkach I, Usenko V C 2021 *Entropy* **23** 55

[45] Hechenblaikner G, Hufgard F, Burkhardt J, Kiesel N, Johann U, Aspelmeyer M, Kaltenbaek R 2014 *New J. Phys.* **16** 013058

[46] Lodewyck J, Bloch M, García-Patrón R, Fossier S, Karpov E, Diamanti E, Debuisschert T, Cerf N J, Tualle-Brouri R, McLaughlin S W, Grangier P 2007 *Phys. Rev. A* **76** 042305

[47] Fossier S, Diamanti E, Debuisschert T, Tualle Brouri R, Grangier P 2009 *J. Phys. B* **42** 114014

[48] Weedbrook C, Pirandola S, Ralph T C 2012 *Phys. Rev. A* **86** 022318

[49] Voss P, Vasilyev M, Levandovsky D, Noh T G, Kumar P 2000 *IEEE Photon. Technol. Lett.* **12** 1340

[50] Fischer M, Scalari G, Walther C, Faist J 2009 *J. Cryst. Growth* **311** 1939

[51] Fischer M, Scalari G, Celebi K, Amanti M, Walther C, Beck M, Faist J 2010 *Appl. Phys. Lett.* **97** 221114

[52] Vitiello M S, Scalari G, Williams B, De Natale P 2015 *Opt. Express* **23** 5167

Inter-satellite terahertz continuous variable quantum key distribution protocol based on passive state preparation*

WU Xiaodong [1)] HUANG Duan [2)†]

1) (*School of Management, Fujian University of Technology, Fuzhou* 350118, *China*)

2) (*School of Electronic Information, Central South University, Changsha* 410083, *China*)

(Received 27 December 2025; revised manuscript received 20 February 2026)

Abstract

Terahertz communication, as an important research topic in the context of next-generation large-capacity wireless networks, is significant for constructing high-speed inter-satellite quantum communication networks. The inter-satellite terahertz continuous-variable quantum key distribution (CV-QKD) scheme based on Gaussian-modulated coherent states usually employs active modulation to prepare quantum states; namely, amplitude and phase modulators and a quantum random number generator (QRNG) are required. However, implementing high-speed active modulation with high extinction ratio and high stability is challenging in practice. Furthermore, the modulation format of active modulation is relatively complex and tolerates only small modulation errors, which hinders the construction of high-speed inter-satellite quantum communication networks. In view of the above analysis, this paper proposes an inter-satellite terahertz CV-QKD scheme based on passive state preparation, in which a thermal terahertz source, beam splitter, optical attenuator, and homodyne detector are used for passive modulation of quantum states. This approach eliminates the need for amplitude and phase modulators and a QRNG, effectively simplifying the implementation of the inter-satellite terahertz CV-QKD protocol. This paper analyzes the security and performance of the proposed protocol. Simulation results show that the performance of the proposed protocol improves significantly with increasing average photon number of the thermal terahertz source and quantum signal frequency, approaching the performance of the ideal Gaussian-modulated inter-satellite CV-QKD protocol. In addition, this paper provides a schematic diagram of the local oscillator system for the proposed scheme, analyzes its physical feasibility and existing technical implementation from a practical perspective, and offers a reference for constructing a low-cost and low-complexity inter-satellite quantum communication network.

Keywords: passive state preparation, continuous variable, quantum key distribution, inter-satellite link, terahertz

DOI: 10.7498/aps.75.20251774 **CSTR:** 32037.14.aps.75.20251774

* Project supported by the Quantum Science and Technology-National Science and Technology Major Project (Grant No. 20212D0300703) and the Fujian Provincial Natural Science Foundation of China (Grant No. 2023J01940).

† Corresponding author. E-mail: duanhuang@csu.edu.cn

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

基于被动态制备的星间太赫兹连续变量量子密钥分发方案

吴晓东　黄端

Inter-satellite terahertz continuous variable quantum key distribution protocol based on passive state preparation

WU Xiaodong　HUANG Duan

引用信息 Citation: Acta Physica Sinica, 75, 120602 (2026)　DOI: 10.7498/aps.75.20251774
CSTR: 32037.14.aps.75.20251774
在线阅读 View online: https://doi.org/10.7498/aps.75.20251774
当期内容 View table of contents: http://wulixb.iphy.ac.cn
