山西大学学报(自然科学版)48(5):973—982,2025
Journal of Shanxi University(Nat. Sci. Ed. )

**DOI**:10.13451/j.sxu.ns.2025049

# 不平衡调制的连续变量测量设备无关量子密钥分发方案

刘文元*,刘泽慧
(中北大学 半导体与物理学院,山西 太原 030051)

**摘 要**:离散调制连续变量测量设备无关量子密钥分发协议在低信噪比条件下,具有较高的协调效率,且实验实现条件相比于高斯调制方案更简单。然而,发送端传统的平衡调制模式并不能使协议安全密钥速率和安全传输距离达到最佳。本文采用不平衡调制模式,并利用等效纠缠理论模型,分别在对称和非对称信道条件下,详细计算了发送端不平衡调制下三态和十二态离散调制连续变量测量设备无关量子密钥分发协议的安全密钥速率和安全传输距离。结果表明,对称和非对称传输距离条件下,不平衡调制模式相比平衡调制模式安全传输距离分别提高了0.16 km和5.43 km。在不改变协议基本框架前提下,本文使用的调制方法优于传统调制模式,对进一步简化系统,降低实验成本提供了理论支撑。

**关键词**:量子通信;等效纠缠模型;离散调制;不平衡调制
**中图分类号**:O431 **文献标志码**:A **文章编号**:0253-2395(2025)05-0973-10

# Continuous Variable-measurement Device Independent-quantum Key Distribution Scheme Based on Imbalanced Modulation

LIU Wenyuan*, LIU Zehui
(*School of Semiconductor and Physics, North University of China, Taiyuan* 030051*, China*)

**Abstract:** Continuous variable-measurement device independent-quantum key distribution (CV-MDI-QKD) protocol with discrete modulation exhibits high coordination efficiency under low signal-to-noise ratio conditions, and the experimental implementation is simpler compared to Gaussian modulation schemes. However, the traditional balanced modulation mode at the transmitter does not optimize the protocol's secure key rate and secure transmission distances. This paper provides a detailed analysis of the performance of the CV-MDI-QKD protocol with discrete modulation under imbalanced modulation mode at the transmitter. Based on an equivalent entanglement theory model, we calculate the secure key rate and secure transmission distance both symmetric and asymmetric quantum channel conditions under the case of three-state and twelve-state discrete modulation CV-MDI-QKD protocols. The results show that under symmetric and asymmetric transmission conditions, the secure transmission distance with imbalanced modulation is improved by 0.16 km and 5.43 km, respectively, compared to balanced modulation. Without changing the basic framework of the protocol, the modulation method proposed in this paper outperforms the traditional modulation modes, providing theoretical support for further simplifying the system and reducing experimental costs.

**Key words:** quantum communication; equivalent entanglement-based model; discrete modulation; imbalanced modulation

**收稿日期**:2024-12-10;**接受日期**:2025-05-06
**基金项目**:国家自然科学基金(12104419);山西省基础研究计划(20210302124689)
* **通信作者**:刘文元(1990—),男,山西大同人,博士,讲师,研究方向为量子通信。E-mail:liuweny@nuc.edu.cn
**引文格式**:刘文元,刘泽慧.不平衡调制的连续变量测量设备无关量子密钥分发方案[J].山西大学学报(自然科学版),2025,48(5):973-982. DOI:10.13451/j.sxu.ns.2025049.

## 0 引言

量子保密通信是量子信息科学的重要分支,理论上能够使合法通信双方共享一组绝对安全的密钥。与传统加密技术依赖数学计算的复杂性不同,量子保密通信的安全性依赖于量子力学基本原理,如量子不可克隆定理,量子纠缠等,结合“一次一密”方法,通信双方能够检测到第三方的窃听行为,从而保证通信的绝对安全。为了应对未来通用量子计算机对传统密码体系的冲击,建立绝对安全的量子保密通信系统在政务、军事和金融领域具有重要意义。量子密钥分发(Quantum Key Distribution,QKD)是实现量子保密通信的重要手段[1-6],按照信源端编码空间的维度,QKD可以分为离散变量类量子密钥分发(Discrete Variable-QKD,DV-QKD)[7-8]和连续变量类量子密钥分发(Continuous Variable-QKD,CV-QKD)[9-18]。DV-QKD类协议是通过离散量子态进行信息编码,通常使用单光子态的偏振或相位作为量子信息的载体,利用量子态的不可克隆性,使得通信双方共享一组安全密钥[19-22]。CV-QKD类协议是通过光场的正交分量作为信息载体,探测端采用平衡零拍探测器或外差探测器探测信号光场的正交分量。其中基于高斯调制相干态的CV-QKD协议在实验实现过程中,以光源易制备,城际距离范围内安全密钥率较高,与现有已经建设完成的光纤通信链路兼容性好等优点,受到研究人员广泛关注[23-29]。为了进一步提高协议性能,法国研究组提出了离散调制CV-QKD协议,其采用四态离散调制编码方式将相位或幅度离散化处理[30-31]。相比于高斯调制CV-QKD协议,简化了调制和解调过程,且在低信噪比下协调效率更高,进一步提升了协议的安全性能。

在实验实现QKD协议的过程中,要求实验的仪器设备都要符合理想模型是很困难的,由于不完美的通信设备,有限的探测效率以及复杂的外界环境,窃听者可以利用系统设备与理想模型之间的缺陷实施窃听和攻击,如时移攻击[32]、伪态攻击[33]、探测器强光致盲攻击[34]、波长攻击[35]、本地光抖动攻击[36],截取-测量-再发送[37]等。同时窃听者可以利用不可信光源,控制接收端探测器工作状态和探测结果,此外探测器荧光信息、时间信息、频域信息的泄露都可能导致系统的安全性漏洞,使得通信双方高估系统安全性,QKD系统随之被攻破。为了从根本上消除实际的安全性问题和潜在的攻击,研究人员提出了测量设备无关量子密钥分发(Measurement Device Independent-QKD,MDI-QKD)协议[38-41],此方案的测量部分由不可信终端完成,其安全性由联合贝尔态测量的结果保证,能够有效消除已知或未知的探测器侧信道攻击。

基于高斯调制的CV-MDI-QKD协议具有较高的安全性,但其在实际应用中仍面临一系列挑战,包括信道噪声的高敏感性、光源须具备低噪声和高稳定性,以及后处理过程中需要计算资源较大等问题。这些因素在一定程度上限制了其在长距离传输和复杂环境下的应用效率,尤其是信号光场受到噪声干扰时,可能导致信噪比降低,安全密钥速率和安全传输距离随之下降。针对以上问题,研究者提出了离散调制CV-MDI-QKD协议[23,30,42-48]。与高斯调制相比,离散调制通过有限的离散信号集合对信息进行编码,有效降低了信号光场对信道噪声的敏感度。同时简化了后处理过程的复杂度,提高了协议的性能和抗噪声能力,即使在相对恶劣环境条件下,系统仍然能够正常运转。

为了进一步简化实验系统,同时降低实验系统成本,本文基于离散调制CV-MDI-QKD协议,建立发送端不平衡调制对系统安全性能影响的理论模型,详细分析了不平衡调制方式对三态和十二态离散调制CV-MDI-QKD协议的影响机制。具体在非对称和对称传输距离条件下,针对任意双模高斯态信道攻击,详细分析了安全密钥速率和安全传输距离影响机制,数值仿真结果表明,相比于传统的发送端平衡调制方式,不平衡调制方式显著提升了系统性能,同时进一步分析了互信息量和Holevo边界。在不改变系统结构的条件下,不平衡调制方式能够有效提升系统的安全密钥速率和安全传输距离。

## 1 离散调制CV-MDI-QKD方案

CV-MDI-QKD协议可以采用制备-测量

(Prepare and Measure, PM)方案描述,PM方案如图1所示,发送端Alice和Bob各自独立进行量子态制备,且要求制备的量子态不受窃听者Eve控制,双方独立制备的量子态发送到Charlie端在50∶50分束器干涉,然后进行连续变量贝尔态测量,同时将测量结果公布,发送端Alice和Bob通过判断各自保留数据的关联性,经过后处理生成安全密钥。

PM实验方案步骤如下:

A. 发送端Alice和Bob初始时分别独立制备相干态,同时通过离散调制将信息加载到信号光场,生成的相干态可以表示为$|\alpha_k\rangle=|\alpha e^{ik\pi/M}\rangle$,本文重点分析三态和十二态离散调制,即$M=3$或$M=11$,$\alpha>0$。然后,发送端Alice和Bob采用时分复用和偏振复用技术将调制相干态通过两条量子信道分别发送到不可信第三方Charlie端。

B. Charlie端将接收到的信号光场进行干涉,输出的量子态分别记为$A_2$和$B_2$。在此基础上探测量子态$B_2$的$x$分量和$A_2$的$p$分量,同时将探测结果$r\rightarrow\{X_{B_2},P_{A_2}\}$公布。

C. 发送端Alice和Bob根据Charlie公布的测量结果进行不同程度的数据修正,同时利用修正后的数据进行信道参数评估,数据后处理等步骤,最终通信双方得到一组相同的安全密钥。

为了进一步分析协议的安全性能,一般采用与制备-测量方案等效的纠缠(Entanglement-Based, EB)模型[8],具体步骤如图2所示。

A. 发送端Alice和Bob分别制备量子态$|\psi_m\rangle_{AA_1}$和$|\psi_m\rangle_{B_1B_3}$,其中$m=0,1,2$或$m=0,1,2,\cdots,11$,对应于三态和十二态离散调制情况。发送端Alice将一个模式$A$保留下来,将另一个模式$A_1$发送到不可信第三方Charlie端。同理,Bob端保留模式$B_3$同时发送模式$B_1$到不可信第三方Charlie端。

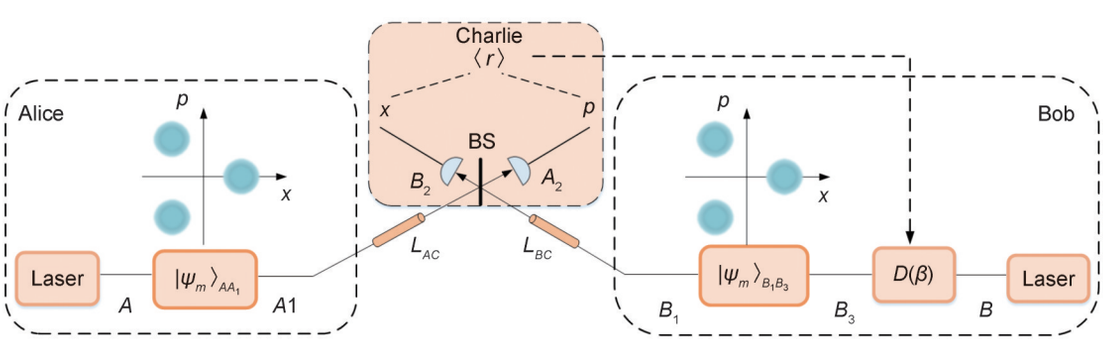



**图1** 离散调制CV-MDI-QKD协议制备-测量方案

**Fig. 1** A frame of the PM scheme based on CV-MDI-QKD protocol with discrete modulation

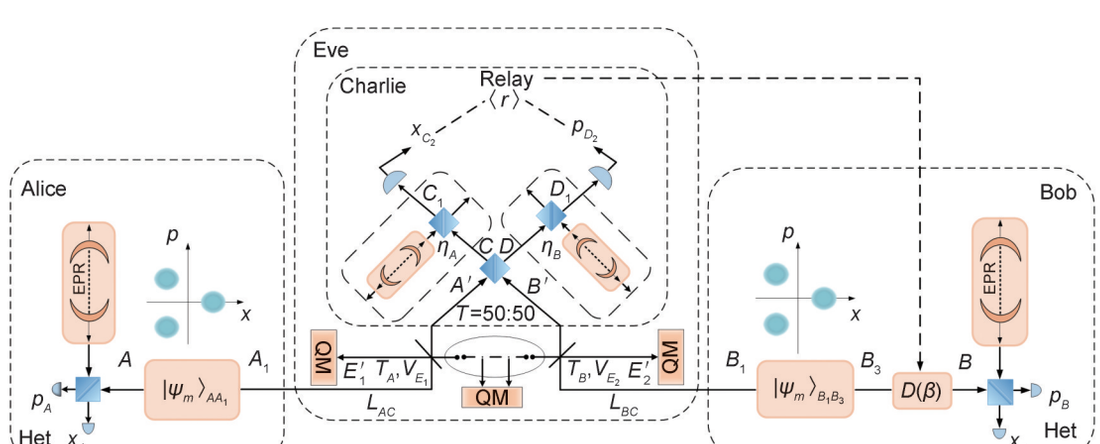



**图2** 离散调制CV-MDI-QKD协议等效纠缠方案

**Fig. 2** A frame of the EB scheme based on CV-MDI-QKD protocol with discrete modulation

B. Charlie端将接收到的两个量子态$A'$和$B'$经过50∶50分束器进行干涉后得到量子态$C$和量子态$D$,同时探测量子态$C$的$x$分量和量子态$D$的$p$分量,探测结果$r=(x_{C_2}+\mathrm{i}p_{D_2})/\sqrt{2}$,记为$\{X_C,P_D\}$。随后Charlie端将测量结果$\{X_C,P_D\}$公布。

C. 发送端Alice和Bob根据公布测量数据进行相应的平移操作$D(\beta)$。经过参数估计,正向或者反向数据协调和私密放大等步骤后,最终生成一组相同的安全密钥。

## 2 安全密钥速率

本节理论上建立了三态和十二态离散调制CV-MDI-QKD协议的等效纠缠模型,详细计算了对称和非对称传输距离情况下,不平衡调制模式对协议安全传输距离和安全密钥速率的影响。同时针对实验设备的不完美性,本节还分析了探测端有限探测效率对于系统安全性能的影响。

发送端Alice和Bob制备的双模压缩态可以表示为[22]。

$$|\psi_m\rangle=\sum_{k=0}^{m}\sqrt{\lambda_k}|\phi_k\rangle|\phi_k\rangle, \tag{1}$$

其中:$|\phi_k\rangle=\frac{\mathrm{e}^{-\alpha^2/2}}{\sqrt{\lambda_k}}\sum_{n=0}^{\infty}\frac{\alpha^{nm+k}}{\sqrt{(nm+k)!}}|nm+k\rangle$,$\alpha=\sqrt{V_{MA}/2}$,

$$\lambda_k=\sum_{0}^{\infty}\frac{\alpha^{2(nM+k)}}{(nM+k)!}。 \tag{2}$$

$|\psi_m\rangle_{AA_1}$的协方差矩阵可以表示为[45]

$$\boldsymbol{\gamma}_{AA_1}=\begin{pmatrix}X\boldsymbol{I}_2 & Z\boldsymbol{\sigma}_z\\ Z\boldsymbol{\sigma}_z & Y\boldsymbol{I}_2\end{pmatrix}, \tag{3}$$

其中$\boldsymbol{I}_2$是$2\times2$的单位矩阵,$\boldsymbol{\sigma}_z=\mathrm{diag}(1,-1)$为泡利矩阵,且协方差矩阵中的参数$X,Y,Z$可以表示为[22]

$$\begin{aligned}X&=\langle\psi_m|\ \ 1+\hat{a}_1^{\dagger}\hat{a}_1|\psi_m\rangle=1+2\alpha^2,\\ Y&=\langle\psi_m|\ \ 1+\hat{a}_2^{\dagger}\hat{a}_2|\psi_m\rangle=1+2\alpha^2,\\ Z&=\langle\psi_m|\ \ \hat{a}_1\hat{a}_2+\hat{a}_1^{\dagger}\hat{a}_2|\psi_m\rangle=2\alpha^2\sum_{k=0}^{M-1}\frac{\lambda_{k-1}^{3/2}}{\lambda_k^{1/2}}。\end{aligned} \tag{4}$$

发送端Alice和Bob之间的协方差矩阵$\boldsymbol{\gamma}_{AB}$:

$$\boldsymbol{\gamma}_{AB}=\begin{bmatrix}a\boldsymbol{I}_2 & c\boldsymbol{\sigma}_z\\ c\boldsymbol{\sigma}_z & b\boldsymbol{I}_2\end{bmatrix}=\begin{bmatrix}(V_A+1)\boldsymbol{I}_2 & \sqrt{T}\,Z\boldsymbol{\sigma}_z\\ \sqrt{T}\,Z\boldsymbol{\sigma}_z & [T(V_A+1+\chi)]\boldsymbol{I}_2\end{bmatrix}。 \tag{5}$$

其中$\chi=\frac{1}{T}-1+\varepsilon$,$L_{AC}$和$L_{BC}$分别为Alice到Charlie的距离和Bob到Charlie的距离。假设光纤信道衰减系数为0.2 dB/km,系统的额外噪声分别记为$\varepsilon_A,\varepsilon_B$。进入Charlie端的量子态$A'$和$B'$,经过干涉输出量子态$D$和$C$,同时使用平衡零拍探测量子态$C$的$x$分量和量子态$D$的$p$分量,将测量结果记为$\{X_C,P_D\}$。考虑到实际探测器的不完美性,探测效率分别为$\eta_A$和$\eta_B$的探测器可以用分束器模型进行仿真,$v_{elA}$和$v_{elB}$分别为探测器电子学噪声。然后,Charlie端将探测结果$\{X_C,P_D\}$公布。Bob端根据公布的数据进行相应的平移操作,等效单路协议下的协方差矩阵。针对量子信道窃听Eve采取的高斯单模攻击,等效通道透射率$T=\frac{T_Ag^2}{2}$,其中增益$g$可以表示为

$$g=\sqrt{\frac{2(V_B-1)}{T_B(V_B+1)}}, \tag{6}$$

相应的等效额外噪声$\varepsilon$可以表示为[42]

$$\varepsilon=\varepsilon_A+\frac{1}{T_A}\left[T_B(\varepsilon_B-2)+2\right]。 \tag{7}$$

基于上述协方差矩阵表达式,离散调制CV-MDI-QKD协议的安全密钥速率$K$:

$$K=\beta I_{AB}-\chi_{BE}, \tag{8}$$

其中$\beta$是协调效率,Alice和Bob的互信息$I_{AB}$可以表示为[45]

$$I_{AB}=\log_2\frac{a+1}{a+1-c^2/(b+1)}。 \tag{9}$$

信息熵$\chi_{BE}$表示Bob和Eve之间的Holevo边界,即窃听者Eve窃取的信息量上界,可以表示为

$$\begin{aligned}\chi_{BE}&=S(\rho_{AB})-S(\rho_A^{m_B})=\\ &\sum_{i=1}^{2}G\left(\frac{\upsilon_i-1}{2}\right)-G\left(\frac{\upsilon_3-1}{2}\right),\end{aligned} \tag{10}$$

其中冯·诺依曼熵的表达式为$G(x)=(x+1)\log_2(x+1)-x\log_2(x)$,$S(\rho_{AB})$是协方差矩阵$\boldsymbol{\gamma}_{AB}$辛特征值$\upsilon_1$和$\upsilon_2$的函数,由下式给出:

$$\upsilon_{1,2}^2=\frac{1}{2}\left[\Delta\pm\sqrt{\Delta^2-4D^2}\ \right], \tag{11}$$

其中 $\Delta=a^2+b^2-2c^2$ 和 $D=ab-c^2$。Eve 的条件熵 $S\left(\rho_A^{m_B}\right)$,基于 Bob 的测量结果 $m_B$,协方差矩阵 $\gamma_A^{m_B}=a\boldsymbol{I}_2-c\boldsymbol{\sigma}_z^{\mathrm{T}}(b\boldsymbol{I}_2+\boldsymbol{I}_2)^{-1}c\boldsymbol{\sigma}_z$ 的辛特征值 $\upsilon_3$ 的表达式

$$\upsilon_3=\frac{a(b+1)-c^2}{b+1}。\tag{12}$$

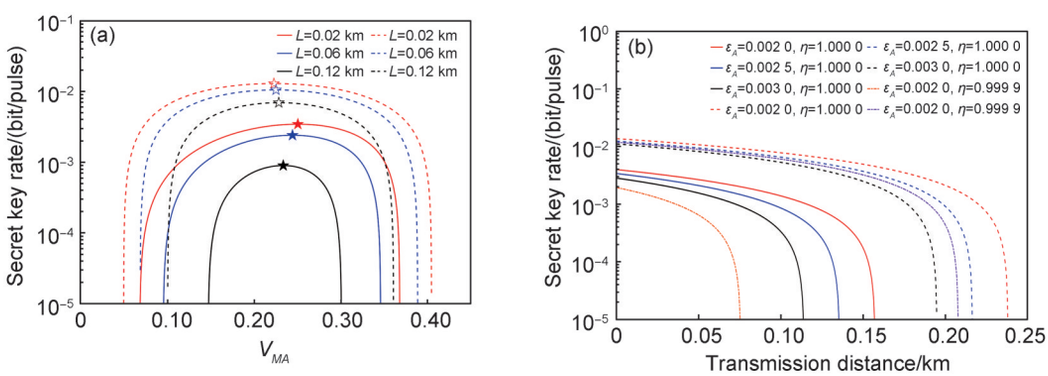
## 3 对称传输距离下的离散调制 CV-MDI-QKD 方案

对称传输距离情况下,发送端 Alice 到第三方 Charlie 的距离 $L_{\mathrm{AC}}$ 等于发送端 Bob 到达 Charlie 端的距离 $L_{\mathrm{BC}}$,即 $L_{\mathrm{AC}}=L_{\mathrm{BC}}$。本节讨论了对称传输距离下,不平衡调制模式对离散调制 CV-MDI-QKD 协议在渐近情况下的安全性能,同时将结果与平衡调制模式下的离散调制 CV-MDI-QKD 协议进行了对比,方案的协调效率设置为 $\beta=0.95$,总的传输距离 $L=L_{\mathrm{AC}}+L_{\mathrm{BC}}$。

图 3(a)和图 4(a)分别给出了三态和十二态离散调制情况下,不同传输距离安全密钥速率随调制方差变化情况。实线表示平衡调制模式下的结果,虚线对应不平衡调制模式下的结果。图中结果表明三态和十二态离散调制条件下,传输距离 $L$ 分别为 0.02 km 和 0.12 km 时,不平衡调制模式获得最佳安全密钥速率分别高于平衡调制模式 275.05% 和 147.09%。且不平衡调制模式下,随着调制方差的变化,安全密钥速率呈现较为对称的分布,这些结果为各种对称距离情况下生成安全密钥速率提供了较好的鲁棒性。随着传输距离的增加,相比于平衡调制模式,不平衡调制方案具有较强的抗噪声能力,且调制方差在一定范围内,安全密钥速率下降速度较为缓慢。综上所述,不平衡调制方案可以显著增加协议安全密钥速率和安全传输距离。

图 3(b)和图 4(b)分别给出了三态和十二态离散调制情况下,安全密钥速率随传输距离的变化情况,实线表示平衡调制模式,虚线代表不平衡调制模式,图中显示同种条件下,不平衡调制模式的安全密钥速率总是高于平衡调制模式,且在额外噪声 $\varepsilon_A=\varepsilon_B$ 条件下,不平衡调制模式下的最远传输距离较平衡调制模式分别增加了 0.08 km,0.16 km。发送端 Alice 和 Bob 通过调整调制方差可以增加安全密钥速率和安全传输距离,具备更强的抗噪声能力。

为了分析不平衡调制模式可以增加协议安全传输距离的原因,本文详细计算了平衡调制和不平衡调制模式互信息量 $I_{AB}$ 和 Eve 窃取信息量上界 $\chi_{BE}$,如图 5(a)和图 5(b)所示,分别表示三态和十二态离散调制 CV-MDI-QKD 方案中的互信息量 $I_{AB}$ 与 $\chi_{BE}$ 随调制方差变化情况,实线是平衡调制模式,虚线是不平衡调制模式。不平衡调制模式下 $I_{AB}$ 与 $\chi_{BE}$ 均高于平衡调制模式,且随着调制方差增加,$I_{AB}$ 与 $\chi_{BE}$ 在两种调制模式下均呈现增加情况,但是二者之差在




注:图中五角星表示安全密钥速率取最大值的点。下同。

Note: The pentagram in the figure indicates the point where the secure key rate reaches its maximum value. The same below.

**图 3** 对称条件下三态离散调制 CV-MDI-QKD 方案

(a)三态离散调制不同传输距离下安全密钥速率随调制方差变化情况;(b)三态离散调制安全密钥速率随传输距离变化情况

**Fig. 3** Symmetric CV-MDI-QKD scheme with three-state modulation

(a) The variation of secure key rate with modulation variance for three-state discrete modulation under different transmission distances; (b) The variation of the secure key rate with transmission distance for three-state discrete modulation

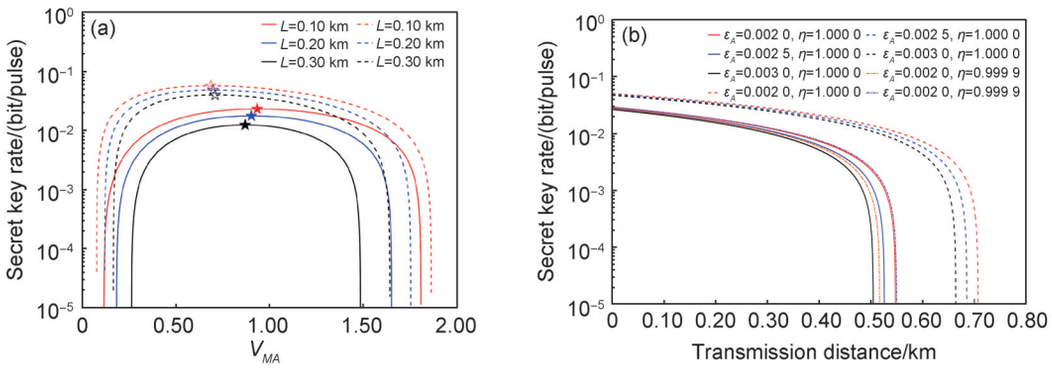



**图4** 对称条件下十二态离散调制CV-MDI-QKD方案

(a)十二态离散调制不同传输距离下安全密钥速率随调制方差变化情况;(b)十二态离散调制安全密钥速率随传输距离变化情况

**Fig. 4** Symmetric CV-MDI-QKD scheme with twelve-state modulation

(a)The variation of secure key rate with modulation variance for twelve-state discrete modulation under different transmission distances; (b) The variation of the secure key rate distance for twelve-state discrete modulation

不平衡调制模式下增加快于平衡调制模式,导致不平衡调制模式下获得更高的安全密钥速率。因此,在不改变方案结构的前提下,采用不平衡调制模式,通过调整发送端调制方差能够使得协议获得更高的安全密钥速率和更远的安全传输距离,这些结果为离散调制CV-MDI-QKD协议性能进一步提高提供了理论依据。

## 4 非对称传输距离的离散调制CV-MDI-QKD方案

本节详细讨论了非对称传输距离条件下,不平衡调制模式对三态和十二态离散调制CV-MDI-QKD方案性能的影响机制,同等情况下与平衡调制模式对安全密钥速率和安全传输距离进行了对比。

图6(a)为三态离散调制CV-MDI-QKD方案在传输距离极不对称情况下,调制方差变化对安全密钥速率的影响情况。虚线为不平衡调制模式,实线为平衡调制模式,当传输距离分别为5 km,10 km,15 km时,不平衡调制模式下最佳安全密钥速率相比平衡调制模式分别提高了274.23%,289.61%,351.81%。且不平衡调制模式下安全密钥速率曲线平坦部分较大,对由于实际调制方差波动造成的影响较低。基于图6(a)获得最佳安全密钥速率方法,图6(b)显示不同额外噪声条件下,总的安全传输距离与安全密钥速率关系。图中显示额外噪声分别为0.002 0,0.002 5,0.003 0情况下,不平衡调制模

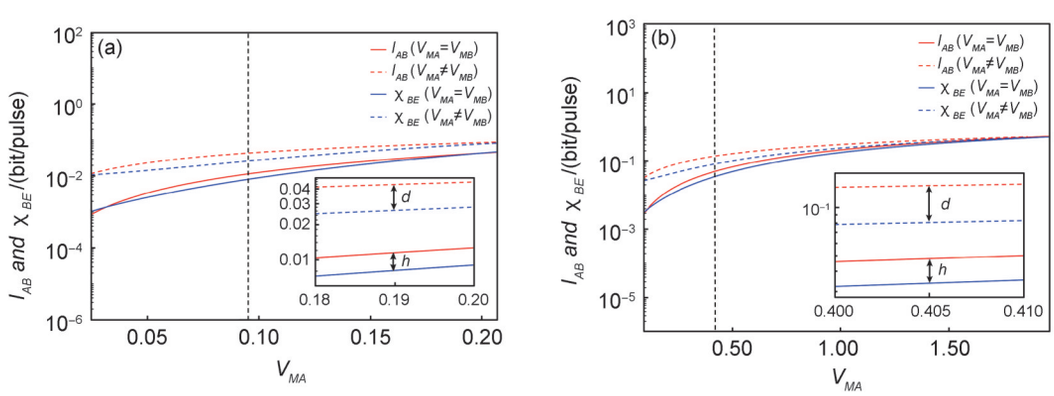



**图5** 对称条件下三态和十二态调制的$I_{AB}$和$\chi_{BE}$

(a)三态离散调制的$I_{AB}$和$\chi_{BE}$随调制方差变化情况;(b)十二态离散调制的$I_{AB}$和$\chi_{BE}$随调制方差变化情况

**Fig. 5** $I_{AB}$ and $\chi_{BE}$ for symmetric CV-MDI-QKD scheme with three-state and twelve-state modulation

(a) The variation of $I_{AB}$ and $\chi_{BE}$ with modulation variance for three-state discrete modulation; (b) The variation of $I_{AB}$ and $\chi_{BE}$ with modulation variance for twelve-state discrete modulation

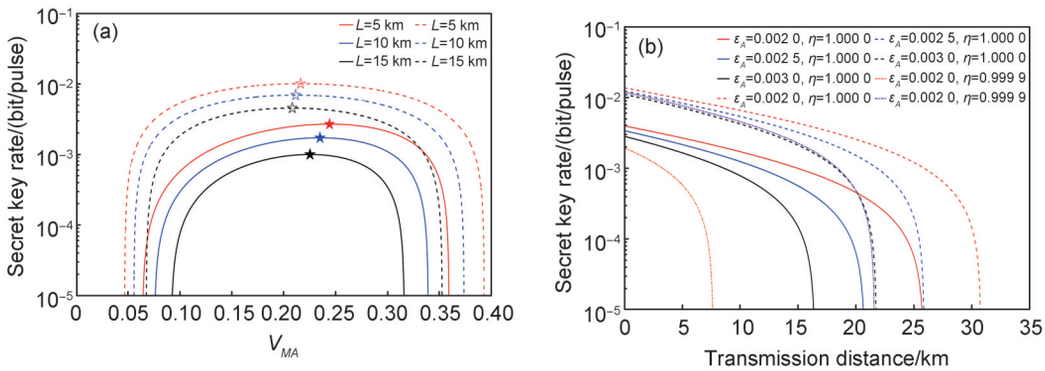



**图6** 极不对称条件下三态离散调制CV-MDI-QKD方案

(a)传输距离极不对称条件下安全密钥速率随调制方差变化情况;(b)不同额外噪声条件下安全传输距离与安全密钥速率关系

**Fig. 6** Extreme asymmetric CV-MDI-QKD scheme with three-state modulation

(a) The variation of secure key rate with modulation variance for three-state discrete modulation under different extreme asymmetric transmission distances; (b) The relationship between the secure transmission distance and the secure key rate under various conditions of excess noise

式相比于平衡调制模式最大安全传输距离分别提高5.43 km,5.35 km,5.08 km。同等条件下,不平衡调制模式的安全密钥速率均高于平衡调制模式。为了进一步验证不平衡调制方式能够提升离散调制CV-MDI-QKD协议性能,本文详细分析了十二态离散调制CV-MDI-QKD协议性能,如图7(a)和图7(b)所示,分析了不平衡调制模式和平衡调制模式下对于协议性能的影响,从图中可以看出不平衡调制模式可以提升协议性能。

在极不对称传输距离条件下,不平衡调制模式可以增加协议安全传输距离和安全密钥速率。平衡调制和不平衡调制模式互信息量$I_{AB}$和Eve窃取信息量上界$\chi_{BE}$,如图8(a)和图8(b)所示,分别表示三态和十二态离散调制的互信息量$I_{AB}$与$\chi_{BE}$随调制方差变化情况,实线是平衡调制模式,虚线是不平衡调制模式。如图8(b)所示,十二态离散调制情况下,不平衡调制模式下$I_{AB}$与$\chi_{BE}$均高于平衡调制模式,当调制方差$V_M=0.39$时,不平衡调制模式下二者之差$d=0.020$明显高于平衡调制模式下$h=0.006$。

综上所述,在协调效率$\beta$,探测效率$\eta$和额外噪声$\varepsilon$等外部参数相同的条件下,传统的平衡调制模式发送端Alice和Bob调制方差一致,此种情况下并不能使得安全密钥速率最佳,而不平衡调制模式可以通过调整发送端Alice和

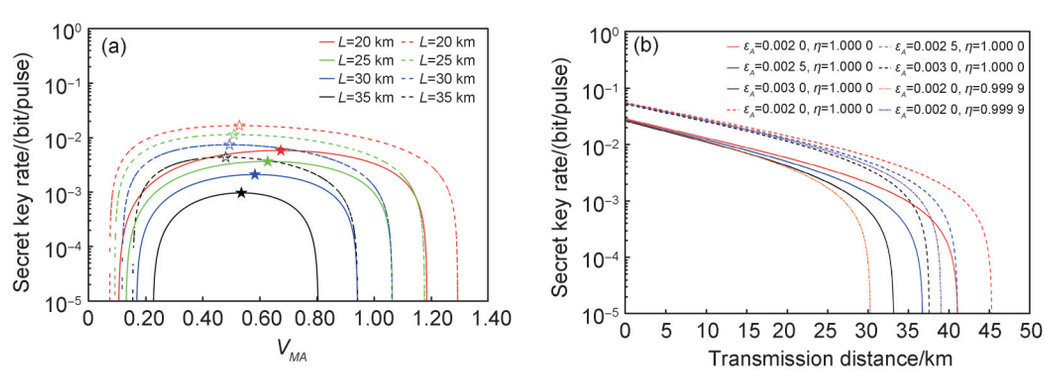



**图7** 极不对称条件下十二态离散调制CV-MDI-QKD方案

(a)传输距离极不对称条件下安全密钥速率随调制方差变化情况;(b)不同额外噪声条件下安全传输距离与安全密钥速率关系

**Fig. 7** Extreme asymmetric CV-MDI-QKD scheme with twelve-state modulation

(a)The variation of secure key rate with modulation variance for twelve-state discrete modulation under different extreme asymmetric transmission distances; (b) The relationship between the secure transmission distance and the secure key rate under various conditions of excess noise

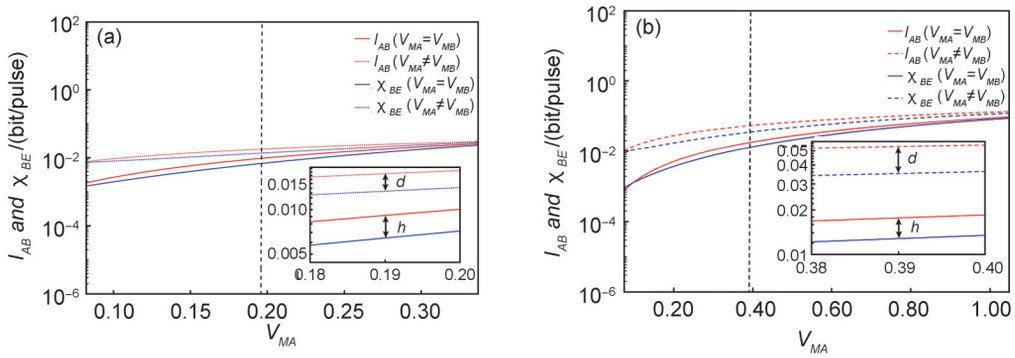



**图8** 极不对称条件下三态和十二态调制的$I_{AB}$和$\chi_{BE}$

(a) 三态离散调制的$I_{AB}$和$\chi_{BE}$随调制方差变化情况；(b) 十二态离散调制的$I_{AB}$和$\chi_{BE}$随调制方差变化情况

**Fig. 8** $I_{AB}$ and $\chi_{BE}$ for extreme asymmetric CV-MDI-QKD scheme with three-state and twelve-state modulation

(a) The variation of $I_{AB}$ and $\chi_{BE}$ with modulation variance for three-state discrete modulation under asymmetric transmission distances; (b) The variation of $I_{AB}$ and $\chi_{BE}$ with modulation variance for twelve-state discrete modulation under asymmetric transmission distances

Bob的调制方差使得互信息量$I_{AB}$增加，在此条件下Eve窃取的信息量上界$\chi_{BE}$同样增加，但安全密钥速率较平衡调制模式显著增加。因此，在不改变方案结构的前提下，采用不平衡调制模式能够使得协议获得更高的安全密钥速率和更远的传输距离。本文理论分析中采用的第三方Charlie端探测效率为1或0.999 9，相当于理想状态下的探测结果，考虑实际情况由于探测效率的不完美和电子学噪声引入等效额外噪声，同时本文采用的离散调制类协议信号光强度弱于高斯调制类协议，这样额外噪声对探测效率非常敏感，但是这一缺陷可以通过加入无噪声线性放大器加以改善。以上理论分析结果为离散调制CV-MDI-QKD协议性能进一步提高提供了理论依据。

## 5 结论

综上所述，基于等效纠缠模型，采用不平衡调制模式建立理论模型。针对三态和十二态离散调制CV-MDI-QKD协议，理论分析了对称和非对称传输距离条件下协议的安全密钥速率和安全传输距离，对比了不平衡调制模式和平衡调制模式对于协议安全性能的影响。结果表明：在对称或非对称传输距离条件下，不平衡调制模式相比平衡调制模式安全传输距离分别增加了0.16 km和5.43 km，且不平衡调制模式下获得安全密钥速率区间更为平坦，针对调制方差抖动的实际情况适应能力更强。本文的研究只考虑了不平衡调制对于三态和十二态离散调制CV-MDI-QKD协议安全性能影响机制，下一步会针对四态和八态离散调制协议进行详细分析。在不改变协议结构的前提下，通过调整发送端调制模式可以提升协议性能，为实验实现提供了理论支撑。

**参考文献：**


[1] GISIN N, RIBORDY G, HUGO Z, *et al*. Quantum Cryptography[J]. *Rev Mod Phys*, 2002, **74**(1): 145-195. DOI: 10.1103/RevModPhys.74.145.

[2] SCARANI V, BECHMANN-PASQUINUCCI H, CERF N J, *et al*. The Security of Practical Quantum Key Distribution[J]. *Rev Mod Phys*, 2009, **81**(3): 1301-1350. DOI: 10.1103/revmodphys.81.1301.

[3] WEEDBROOK C, PIRANDOLA S, GARCÍA-PATRÓN R, *et al*. Gaussian Quantum Information[J]. *Rev Mod Phys*, 2012, **84**(2): 621-669. DOI: 10.1103/revmodphys.84.621.

[4] LO H K, CURTY M, TAMAKI K. Secure Quantum Key Distribution[J]. *Nat Photonics*, 2014, **8**(8): 595-604. DOI: 10.1038/nphoton.2014.149.

[5] PIRANDOLA S, ANDERSEN U L, BANCHI L, *et al*. Advances in Quantum Cryptography[J]. *Adv Opt Photon*, 2020, **12**(4): 1012. DOI: 10.1364/aop.361502.

[6] XU F H, MA X F, ZHANG Q, *et al*. Secure Quantum Key Distribution with Realistic Devices[J]. *Rev Mod Phys*, 2020, **92**(2): 025002. DOI: 10.1103/revmodphys.92.025002.

[7] EKERT A K. Quantum Cryptography Based on Bell's Theorem[J]. *Phys Rev Lett*, 1991, **67**(6): 661-663. DOI: 10.1103/PhysRevLett.67.661.

[8] BENNETT C H, BRASSARD G, MERMIN N D. Quantum Cryptography without Bell's Theorem[J]. *Phys Rev*

*Lett*, 1992, **68**(5): 557−559. DOI: 10.1103/PhysRevLett.68.557.

[9] GROSSHANS F, VAN ASSCHE G, WENGER J, *et al*. Quantum Key Distribution Using Gaussian-modulated Coherent States[J]. *Nature*, 2003, **421**(6920): 238−241. DOI: 10.1038/nature01289.

[10] QI B, HUANG L L, QIAN L, *et al*. Experimental Study on the Gaussian-modulated Coherent-state Quantum Key Distribution over Standard Telecommunication Fibers[J]. *Phys Rev A*, 2007, **76**(5): 052323. DOI: 10.1103/physreva.76.052323.

[11] MADSEN L S, USENKO V C, LASSEN M, *et al*. Continuous Variable Quantum Key Distribution with Modulated Entangled States[J]. *Nat Commun*, 2012, **3**: 1083. DOI: 10.1038/ncomms2097.

[12] PIRANDOLA S, OTTAVIANI C, SPEDALIERI G, *et al*. High-rate Measurement-device-independent Quantum Cryptography[J]. *Nat Photonics*, 2015, **9**(6): 397−402. DOI: 10.1038/nphoton.2015.83.

[13] LI Y M, WANG X Y, BAI Z L, *et al*. Continuous Variable Quantum Key Distribution[J]. *Chin Phys B*, 2017, **26**(4): 040303. DOI: 10.1088/1674-1056/26/4/040303.

[14] LIU W Y, WANG X Y, WANG N, *et al*. Imperfect State Preparation in Continuous-variable Quantum Key Distribution[J]. *Phys Rev A*, 2017, **96**(4): 042312. DOI: 10.1103/physreva.96.042312.

[15] LIU W Y, CAO Y X, WANG X Y, *et al*. Continuous-variable Quantum Key Distribution Under Strong Channel Polarization Disturbance[J]. *Phys Rev A*, 2020, **102**(3): 032625. DOI: 10.1103/PhysRevA.102.032625.

[16] TIAN Y, WANG P, LIU J Q, *et al*. Experimental Demonstration of Continuous-variable Measurement-device-independent Quantum Key Distribution over Optical Fiber[J]. *Optica*, 2022, **9**(5): 492−500. DOI: 10.1364/OPTICA.450573.

[17] KARINOU F, BRUNNER H H, FUNG C F, *et al*. Toward the Integration of CV Quantum Key Distribution in Deployed Optical Networks[J]. *IEEE Photonics Technol Lett*, 2018, **30**(7): 650−653. DOI: 10.1109/LPT.2018.2810334.

[18] KLEIS S, STEINMAYER J, DERKSEN R H, *et al*. Experimental Investigation of Heterodyne Quantum Key Distribution in the S-band or L-band Embedded in a Commercial C-band DWDM System[J]. *Opt Express*, 2019, **27**(12): 16540−16549. DOI: 10.1364/OE.27.016540.

[19] SCARANI V, ACÍN A, RIBORDY G, *et al*. Quantum Cryptography Protocols Robust Against Photon Number Splitting Attacks for Weak Laser Pulse Implementations[J]. *Phys Rev Lett*, 2004, **92**(5): 057901. DOI: 10.1103/PhysRevLett.92.057901.

[20] SHOR P W, PRESKILL J. Simple Proof of Security of the BB84 Quantum Key Distribution Protocol[J]. *Phys Rev Lett*, 2000, **85**(2): 441−444. DOI: 10.1103/PhysRevLett.85.441.

[21] BECHMANN-PASQUINUCCI H, GISIN N. Incoherent and Coherent Eavesdropping in the Six-state Protocol of Quantum Cryptography[J]. *Phys Rev A*, 1999, **59**(6): 4238−4248. DOI: 10.1103/physreva.59.4238.

[22] DENYS A, BROWN P, LEVERRIER A. Explicit Asymptotic Secret Key Rate of Continuous-variable Quantum Key Distribution with an Arbitrary Modulation[J]. *Quantum*, 2021, **5**: 540. DOI: 10.22331/q-2021-09-13-540.

[23] PAN Y, WANG H, SHAO Y, *et al*. Experimental Demonstration of High-rate Discrete-modulated Continuous-variable Quantum Key Distribution System[J]. *Opt Lett*, 2022, **47**(13): 3307−3310. DOI: 10.1364/OL.456978.

[24] WANG H, LI Y, PI Y D, *et al*. Sub-Gbps Key Rate Four-state Continuous-variable Quantum Key Distribution within Metropolitan Area[J]. *Commun Phys*, 2022, **5**: 162. DOI: 10.1038/s42005-022-00941-z.

[25] JOUGUET P, KUNZ-JACQUES S, DEBUISSCHERT T, *et al*. Field Test of Classical Symmetric Encryption with Continuous Variables Quantum Key Distribution [J]. *Opt Express*, 2012, **20**(13): 14030−14041. DOI: 10.1364/oe.20.014030.

[26] HUANG D, HUANG P, LI H S, *et al*. Field Demonstration of a Continuous-variable Quantum Key Distribution Network[J]. *Opt Lett*, 2016, **41**(15): 3511−3514. DOI: 10.1364/OL.41.003511.

[27] ZHANG Y C, LI Z Y, CHEN Z Y, *et al*. Continuous-variable QKD over 50 km Commercial Fiber[J]. *Quantum Sci Technol*, 2019, **4**(3): 035006. DOI: 10.1088/2058-9565/ab19d1.

[28] SUN S H, XU F H. Security of Quantum Key Distribution with Source and Detection Imperfections[J]. *New J Phys*, 2021, **23**(2): 023011. DOI: 10.1088/1367-2630/abdf9b.

[29] JAIN N, CHIN H M, MANI H, *et al*. Practical Continuous-variable Quantum Key Distribution with Composable Security[J]. *Nat Commun*, 2022, **13**(1): 4740. DOI: 10.1038/s41467-022-32161-y.

[30] LEVERRIER A, GRANGIER P. Unconditional Security Proof of Long-distance Continuous-variable Quantum Key Distribution with Discrete Modulation[J]. *Phys Rev Lett*, 2009, **102**(18): 180504. DOI: 10.1103/physrevlett.102.180504.

[31] LI Y Y, WANG T Y. Security Analysis of Unidimensional Continuous-variable Quantum Key Distribution with Discretized Amplitude Modulation[J]. *J Phys B: At Mol Opt Phys*, 2024, **57**(14): 145502. DOI: 10.1088/1361-6455/ad5891.

[32] ZHAO Y, FUNG C F, QI B, *et al*. Quantum Hacking: Experimental Demonstration of Time-shift Attack against Practical Quantum-key-distribution Systems[J]. *Phys Rev A*, 2008, **78**(4): 042333. DOI: 10.1103/PhysRevA.78.042333.

[33] MAKAROV V, HJELME D R. Faked States Attack on Quantum Cryptosystems[J]. *J Mod Opt*, 2005, **52**(5): 691−705. DOI: 10.1080/09500340410001730986.

[34] LYDERSEN L, AKHLAGHI M K, HAMED MAJEDI A, *et al*. Controlling a Superconducting Nanowire Single-photon Detector Using Tailored Bright Illumination[J]. *New J Phys*, 2011, **13**(11): 113042. DOI: 10.1088/1367-2630/13/11/113042.

[35] KURTSIEFER C, ZARDA P, MAYER S, *et al*. The Breakdown Flash of Silicon Avalanche Photodiodes-back Door for Eavesdropper Attacks?[J]. *J Mod Opt*, 2001, **48**(13): 2039−2047. DOI: 10.1080/09500340108240905.

[36] MA X C, SUN S H, JIANG M S, *et al*. Local Oscillator Fluctuation Opens a Loophole for Eve in Practical Continuous-variable Quantum-key-distribution Systems [J]. *Phys Rev A*, 2013, **88**(2): 022339. DOI: 10.1103/physreva.88.022339.

[37] BARRETT J, COLBECK R, KENT A. Memory Attacks on Device-independent Quantum Cryptography [J]. *Phys Rev Lett*, 2013, **110**(1): 010503. DOI: 10.1103/PhysRevLett.110.010503.

[38] LO H K, CURTY M, QI B. Measurement-device-independent Quantum Key Distribution[J]. *Phys Rev Lett*, 2012, **108**(13): 130503. DOI: 10.1103/PhysRevLett.108.130503.

[39] LIU Y, CHEN T Y, WANG L J, *et al*. Experimental Measurement-device-independent Quantum Key Distribution[J]. *Phys Rev Lett*, 2013, **111**(13): 130502. DOI: 10.1103/PhysRevLett.111.130502.

[40] LIU H, WANG W Y, WEI K J, *et al*. Experimental Demonstration of High-rate Measurement-device-independent Quantum Key Distribution over Asymmetric Channels[J]. *Phys Rev Lett*, 2019, **122**(16): 160501. DOI: 10.1103/PhysRevLett.122.160501.

[41] CHEN Z Y, ZHANG Y C, WANG G, *et al*. Composable Security Analysis of Continuous-variable Measurement-device-independent Quantum Key Distribution with Squeezed States for Coherent Attacks[J]. *Phys Rev A*, 2018, **98**(1): 012314. DOI: 10.1103/physreva.98.012314.

[42] MA H X, HUANG P, BAI D Y, *et al*. Long-distance Continuous-variable Measurement-device-independent Quantum Key Distribution with Discrete Modulation [J]. *Phys Rev A*, 2019, **99**(2): 022322. DOI: 10.1103/physreva.99.022322.

[43] SILBERHORN C, RALPH T C, LÜTKENHAUS N, *et al*. Continuous Variable Quantum Cryptography: Beating the 3 DB Loss Limit[J]. *Phys Rev Lett*, 2002, **89**(16): 167901. DOI: 10.1103/PhysRevLett.89.167901.

[44] ALMEIDA M, PEREIRA D, MUGA N J, *et al*. Secret Key Rate of Multi-ring M-APSK Continuous Variable Quantum Key Distribution[J]. *Opt Express*, 2021, **29**(23): 38669−38682. DOI: 10.1364/OE.439992.

[45] LIU C J, CHAO Y, WANG L, *et al*. Continuous-variable Measurement-device-independent Quantum Key Distribution with Multi-ring Discrete Modulation [J]. *Opt Express*, 2024, **32**(18): 31549−31565. DOI: 10.1364/OE.531896.

[46] DING J Z, LI Y, MAO Y, *et al*. Discrete Modulation Continuous Variable Quantum Secret Sharing[J]. *Int J Theor Phys*, 2022, **61**(4): 108. DOI: 10.1007/s10773-022-04985-3.

[47] LIU W Y, LIU Z H, BAI J D, *et al*. Impact of Imbalanced Modulation on Security of Continuous-variable Measurement-device-independent Quantum Key Distribution[J]. *Photonics*, 2024, **11**(7): 649. DOI: 10.3390/photonics11070649.

[48] WANG P, ZHANG Y, LU Z G, *et al*. Discrete-modulation Continuous-variable Quantum Key Distribution with a High Key Rate[J]. *New J Phys*, 2023, **25**(2): 023019. DOI: 10.1088/1367-2630/acb964.