

doi:10.13756/j.gtxyj.2025.250070.

专题: 光子量子芯片

李振华, 韩雁鑫, 窦天琦, 等. 模式匹配量子密钥分发中的后脉冲效应[J]. 光通信研究, 2025(3): 250070.

Li Z H, Han Y X, Dou T Q, et al. Afterpulse Effects in Mode-Pairing Quantum Key Distribution[J]. Study on Optical Communications, 2025(3): 250070.

模式匹配量子密钥分发中的后脉冲效应(特邀)

李振华¹, 韩雁鑫², 窦天琦¹, 颜旭², 华昕², 肖希², 唐建军¹

(1. 中国电信股份有限公司研究院, 北京 102209; 2. 国家信息光电子创新中心, 武汉 430074)

摘要:【目的】模式匹配(MP)-量子密钥分发(QKD)因其突破了无中继量子信道码率-距离限制,并且无需相位锁定,受到广泛关注。然而,随着QKD系统频率的提升,探测器的后脉冲效应逐渐显现,并对系统的安全性和鲁棒性产生了不利影响。【方法】文章提出了一种基于MP-QKD的后脉冲改进方案,并且通过优化系统参数减少了后脉冲效应对安全密钥率的影响。【结果】研究表明,在后脉冲概率高达10%的情况下,文章所提方案也能保证在长距离下系统的安全密钥率仍能保持与无后脉冲情况下的基准曲线相当,表明此方案具有较强的鲁棒性。【结论】文章所提MP-QKD改进方案能够有效抑制后脉冲效应的影响,提升系统在高频率和长距离通信中的稳定性和安全性。未来,随着QKD技术的普及和高频系统的广泛应用,提升MP-QKD在更加复杂的通信场景中的表现,将有效促进量子通信网络的规模化部署和商业化应用。

关键词: 模式匹配; 量子密钥分发; 后脉冲效应; 参数优化

中图分类号: TN918

文献标志码: A

Afterpulse Effects in Mode-Pairing Quantum Key Distribution

LI Zhenhua¹, HAN Yanxin², DOU Tianqi¹, YAN Xu², HUA Xin², XIAO Xi², TANG Jianjun¹

(1. China Telecom Research Institute, Beijing 102209, China;

2. National Information Optoelectronics Innovation Center, Wuhan 430074, China)

Abstract: 【Objective】 Mode-Pairing (MP)-Quantum Key Distribution (QKD) has garnered widespread attention due to its ability to overcome the repeaterless quantum channel rate-distance limit and its independence from phase locking. However, as the frequency of QKD systems increases, the afterpulse effect in detectors becomes more pronounced, negatively affecting the system's security and robustness. 【Methods】 In this paper, we propose an improved afterpulse model for MP-QKD and optimize the system parameters to reduce the afterpulse effect on the secure key rate. 【Results】 The results show that, even with an afterpulse probability as high as 10%, the proposed scheme ensures that the system's secure key rate remains comparable to the baseline curve without afterpulse, indicating the robustness of the scheme. 【Conclusion】 The proposed MP-QKD method effectively suppresses the afterpulse effect, enhancing the system's stability and security in high-frequency and long-distance communications. In the future, as QKD technology becomes more widespread and high-frequency systems are increasingly deployed, improving the performance of MP-QKD in more complex communication scenarios will significantly promote the large-scale deployment and commercialization of quantum communication networks.

Key words: MP; QKD; afterpulse effect; parameter optimization

0 引言

量子密钥分发(Quantum Key Distribution, QKD)基于量子力学的内禀属性产生安全密钥,即使在面对无限计算能力的窃听者 Eve 时,也能确保通信双方 Alice 和 Bob 在信息论上的通信安全。自从第 1 个 QKD 协议,即 BB84 协议^[1]提出以后, QKD 理论^[2-4]和实验^[5-6]得到了快速发展,引起了国家和社会的广泛关注。在 QKD 过程中,单光子作为密钥传输的载体,无法被放大或者复制克隆,但

容易受到传输信道的影响,具体表现为安全密钥率 R 与信道透过率 η 呈线性关系^[7],即 $R \propto O(\eta)$ 。双场(Twin-Field, TF)-QKD^[8]利用单光子干涉生成密钥,突破了无中继量子信道码率-距离的限制,使得 $R \propto O(\sqrt{\eta})$ 。然而为了保持远距离量子态的相干性,TF-QKD 需要部署全局的锁频锁相技术^[6,9],增加了 QKD 系统的复杂度和额外的资源消耗。

近期清华大学马雄峰团队提出的模式匹配(Mode-Pairing, MP)-QKD^[10],也称为异步测量设备无关协议 QKD^[11],除了具有 $R \propto O(\sqrt{\eta})$ 的优

收稿日期:2025-03-04; 修回日期:2025-04-08; 纸质出版日期:2025-06-10

基金项目:科技创新 2030 资助项目(2021ZD0301300)

作者简介:李振华(1995-),男,山东泰安人。工程师,博士,主要研究方向为量子密码与量子通信。

通信作者:唐建军,正高级工程师。E-mail:tangjj6@chinatelecom.cn

© Editorial Office of Study on Optical Communications. This is an open access article under the CC BY-NC-ND license.

势外,还无需复杂的全局锁相的需求;2023年,中国科学技术大学潘建伟、陈腾云团队等首次在实验室内实现了400 km级的MP-QKD实验,相较于原始的测量设备无关实验,安全密钥率提升了3个数量级^[12];随后,北京量子院袁之良团队和南京大学尹华磊团队,实现了508 km的MP-QKD,打破了安全码率-距离界限^[13];2024年,清华大学马雄峰团队、中国科学技术大学潘建伟团队、陈腾云团队和中国电信研究院合作,首次在城际光纤环境下实现了MP-QKD^[14],并且讨论了强度波动对实验的影响^[15]。目前,MP-QKD已经成为量子通信网络部署的有力候选者。

虽然TF-QKD和MP-QKD可以避免探测器端的攻击,但是如果忽略探测器的设备缺陷,就可能无法充分利用实际QKD系统的性能。无论是单光子雪崩探测器(Single-Photon Avalanche Detector, SPAD)还是超导纳米线单光子探测器(Superconducting Nanowire Single Photon Detector, SNSPD)都存在后脉冲效应。SPAD的后脉冲是当光子触发雪崩时,由于SPAD材料中的缺陷,一部分光生载流子会被困在较深的能级中^[16-18]。随着时间的推移,这些载流子会释放出来,如果SPAD的偏置电压高于击穿电压,就可能触发伪探测事件。作为SPAD的固有特性,后脉冲会引入随机的探测响应,从而增加量子比特误码率^[19-20]。而SNSPD的并行纳米线结构中,后脉冲通常发生在纳秒级时间尺度内,其成因主要归因于偏置电流的恢复与瞬时的临界电流^[21]。对于单根纳米线,后脉冲可能源于探测器读出电路反射引起的偏置电流扰动^[22-23],或者在高计数率下,由交流耦合放大器中的电容器放电导致偏置电流的过冲^[24-25]。

在之前对MP-QKD的分析中,基本忽略了后脉冲的影响,但随着QKD系统频率的提高,后脉冲的影响不容忽视。中国科学技术大学韩正甫团队通过实验验证了SPAD的后脉冲具有非马尔可夫特性,并构建了一种兼容后脉冲的模型,以解决QKD中的后脉冲效应^[19]。随后,针对有限码长QKD^[26]和测量设备无关QKD^[27]的后脉冲分析相继展开。本文进一步分析了后脉冲效应对MP-QKD的影响,提出了一种适用于MP-QKD的后脉冲分析方案,并将该方案通过粒子群算法进行优化,有效抑制了后脉冲效应对QKD系统性能的影响。研究结果表明,尽管后脉冲引入的噪声影响了量子态的计数率和误码率,但通过本文所提方案有效抑制了密钥

率的下降,缓解了后脉冲效应带来的不利影响,保证了MP-QKD系统的鲁棒性。特别是在不同的通信距离下,系统的安全密钥率变化较小,表明该方法具备较好的实际应用潜力。

1 MP-QKD

由于MP-QKD测量后匹配特性,诸如双扫描诱骗态方案^[28]或者多强度诱骗态方案^[29]对安全密钥率的提升有限,因此常规的3强度诱骗态方案^[2,30]是部署MP-QKD的最佳方案。3强度诱骗态方案要求通信双方随机地制备信号态 $\mu_{a(b)}$ 、诱骗态 $\nu_{a(b)}$ 和真空态 $o_{a(b)}$,并且满足 $\mu_{a(b)} > \nu_{a(b)} > o_{a(b)} \geq 0$,下标a和b分别代表通信端Alice和Bob。3强度诱骗态方案的MP-QKD协议具体的流程如图1所示。

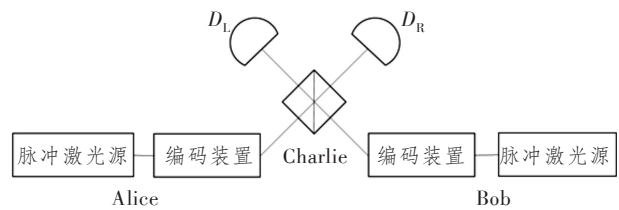


图1 MP-QKD流程简图

Figure 1 A schematic diagram of the MP-QKD protocol

①量子态的制备:在第*i*时间窗口,Alice随机从 $\left\{0, \frac{2\pi}{\Delta}, \frac{4\pi}{\Delta}, \dots, \frac{2\pi(\Delta-1)}{\Delta}\right\}$ 中选择相位值 θ_a^i ,一般情况下相位片 $\Delta=16$;然后她以概率 p_{k_i} 随机选择强度 $k_a^i \in \{\mu_a, \nu_a, o_a\}$ 。Alice根据其选择通过编码装置制备一个弱相干态 $|e^{i\theta_a^i} \sqrt{k_a^i}\rangle$,*e*为自然常数,*i*为虚数单位。Bob以同样的方式制备一个弱相干态 $|e^{i\theta_b^i} \sqrt{k_b^i}\rangle$ 。随后,Alice和Bob制备的光脉冲经过量子信道发送给测量端Charlie。

②测量:对于每个时间窗口,Charlie对Alice和Bob发送过来的光脉冲进行干涉测量,并且宣布探测器的响应结果为 D_L 和 D_R 。经过*N*轮重复步骤①和步骤②后,仅保留 D_L 和 D_R 有且仅有一次响应的脉冲数据,丢弃其他情况下的脉冲数据。

③MP:对于所有保留下的脉冲数据,Alice和Bob会在最大配对间隔 l_{\max} 内将两个脉冲配对。假设配对成功的两个脉冲的时间窗口序号为*i*和*j*,并且 $j < i + l_{\max}$ 。

④基矢筛选:为了方便描述,这里定义第*i*窗口和第*j*窗口的强度组为 $(k_a, k_b) = (k_a^i + k_a^j, k_b^i + k_b^j)$ 。当 $k_{a(b)} = 2\mu_{a(b)}$ 或 $2\nu_{a(b)}$ 时,则定义其为X基;当 $k_{a(b)} = \mu_{a(b)}$ 或 $\nu_{a(b)}$ 时,则定义其为Z基;当 $k_{a(b)} =$

$o_{a(b)}$ 时,则定义其为 0 基;丢弃其余情况的强度组数据。随后, Alice 和 Bob 执行基矢的匹配,保留 (k_a, k_b) 基矢相同的数据,得到一系列 Z 基对、X 基对和 0 基对的数据,丢弃基矢不相同的数据。值得注意的是,0 基的所有数据都要保留。

⑤ 密钥映射:在 Z 基对中,当第 i 个脉冲窗口为真空态,并且第 j 个脉冲窗口为非真空态时, Alice 记作 Z 基下的比特 0,而 Bob 记作 Z 基下的比特 1;反之,当 i 脉冲窗口为非真空态,并且第 j 个脉冲窗口为真空态时, Alice 记作 Z 基下的比特 1,而 Bob 记作 Z 基对下的比特 0。在 X 基对中, Alice 和 Bob 从相对相位中提取比特 $\kappa_{a(b)} = \left[(\theta_{a(b)}^i - \theta_{a(b)}^j) / \pi \right] \bmod 2$, \bmod 为求模运算。此外,在 X 基对中,如果 Charlie 的测量结果为一左一右响应时, Bob 需要翻转其比特;其他情况下 Bob 的比特值保持不变。

⑥ 参数估计:Z 基对中 (μ_a, μ_b) 的数据用来生成安全密钥,其中最终密钥的配对数 $M_{(\mu_a, \mu_b)}$ 和相应的比特错误率 $E_{(\mu_a, \mu_b)}$ 可以直接从实验中获取。Z 基对的单光子部分计数 M_{11} 和对应的相位错误率 e_{11}^{ph} 可以结合诱骗态理论来估计。

⑦ 密钥提取: Alice 和 Bob 执行纠错和隐私放大获取到最终安全密钥。结合平滑熵的不确定性关系^[31-32],有限码长下的 MP-QKD 密钥长度 ℓ 为

$$\ell \geq M_{11} \left[1 - h(e_{11}^{\text{ph}}) \right] - f M_{(\mu_a, \mu_b)} h(E_{(\mu_a, \mu_b)}) - \log_2 \frac{2}{\epsilon_{\text{cor}}} - 2 \log_2 \frac{1}{\sqrt{2} \hat{\epsilon} \epsilon_{\text{PA}}}, \quad (1)$$

式中: f 为纠错效率; $h(x) = -x \log_2 x - (1-x) \log_2 (1-x)$; ϵ_{cor} 、 $\hat{\epsilon}$ 和 ϵ_{PA} 分别为与密钥正确性和保密性相关的安全参数。

2 探测器后脉冲分析

如图 1 所示, MP-QKD 协议一般使用两个单光子探测器。在之前的分析中,基本会忽略后脉冲对计数增益和错误率的影响。 Alice 和 Bob 发送的弱相干态脉冲经过量子信道后,到达 Charlie 端进行干涉。干涉后左右单光子探测器响应的概率分别为

$$\begin{aligned} D_{k'_i k'_i}^{\text{L}} &= 1 - (1 - p_d) e^{-\frac{\eta_a k'_i + \eta_b k'_i}{2} \sqrt{\eta_a k'_i \eta_b k'_i} \cos \theta}, \\ D_{k'_i k'_i}^{\text{R}} &= 1 - (1 - p_d) e^{\frac{\eta_a k'_i + \eta_b k'_i}{2} \sqrt{\eta_a k'_i \eta_b k'_i} \cos \theta}, \end{aligned} \quad (2)$$

式中: p_d 为单光子探测器的暗计数; η_a 和 η_b 分别为 Alice-Charlie 和 Bob-Charlie 的信道透过率; $\theta = \theta_a^i - \theta_b^i$ 。 SPAD 的后脉冲与雪崩倍增过程中载流子

复合电荷捕获效应密切相关,通常表现为探测到光子后载流子复合或电荷捕获导致的额外电流脉冲; SNSPD 产生的后脉冲受到外部电路反射、放大器特性以及偏置电流等因素的影响,导致额外的脉冲。这些后脉冲不仅由当前的探测响应引起,还受到过去探测事件的影响,表现出历史相关性,因此可以近似认为 SPAD 和 SNSPD 的后脉冲计数是由不同阶后脉冲计数组成的,一阶后脉冲是由光脉冲或者暗计数引起的,而 m 阶的后脉冲是由 $m-1$ 阶的后脉冲引起的,表明每一阶后脉冲可能源于前一阶后脉冲的能量释放或延续过程,后脉冲现象不仅涉及初次的光子探测事件,还包括探测器内部能量的积累与逐步释放机制。因此一阶后脉冲的概率 $P_{\text{ap}}^{(1)}$ 为

$$P_{\text{ap}}^{(1)} = \sum_{n=1} p_n Q_n = p_{\text{ap}} Q, \quad (3)$$

式中: p_n 为监测窗口 n 内的后脉冲率系数,可在实验开始之前准确测量;总体的后脉冲率 $p_{\text{ap}} = \sum_{n=1} p_n$;

Q_n 为不同强度增益的加权平均值,即 $Q_n = Q = \sum_{(k_a, k_b)} \frac{p_k p_{k_b}}{2\pi} \int_0^{2\pi} D_{k'_i k'_i}^{\text{L}} d\theta$ 。高阶后脉冲可以由一个递归链表示出来:

$$\begin{cases} P_{\text{ap}}^{(2)} = \sum_{n=1} p_n P_{\text{ap}}^{(1)} = (p_{\text{ap}})^2 Q, \\ P_{\text{ap}}^{(3)} = \sum_{n=1} p_n P_{\text{ap}}^{(2)} = (p_{\text{ap}})^3 Q, \\ \dots \\ P_{\text{ap}}^{(m)} = \sum_{n=1} p_n P_{\text{ap}}^{(m-1)} = (p_{\text{ap}})^m Q. \end{cases} \quad (4)$$

后脉冲的概率是上述不同阶后脉冲事件的一个交集,直接计算较为复杂。可以计算各阶后脉冲事件均不发生的概率,该事件的相反事件即为产生后脉冲的概率:

$$P_{\text{ap}} = 1 - \prod_{m=1} (1 - P_{\text{ap}}^{(m)}) \approx \sum_{m=1} P_{\text{ap}}^{(m)} = \quad (5)$$

$$\sum_{m=1} (p_{\text{ap}})^m Q_n = \frac{p_{\text{ap}}}{1 - p_{\text{ap}}} Q_n \circ$$

考虑到后脉冲后,令 $y = (1 - p_d)(1 - P_{\text{ap}}) e^{-\frac{\eta_a k'_i + \eta_b k'_i}{2}}$, $x = \sqrt{\eta_a k'_i \eta_b k'_i}$, MP-QKD 中的左右探测器响应的概率变为

$$\begin{aligned} D_{k'_i k'_i}^{\text{L}} &= 1 - (1 - p_d)(1 - P_{\text{ap}}) e^{-\frac{\eta_a k'_i + \eta_b k'_i}{2} \sqrt{\eta_a k'_i \eta_b k'_i} \cos \theta} = 1 - y e^{-x \cos \theta}, \\ D_{k'_i k'_i}^{\text{R}} &= 1 - (1 - p_d)(1 - P_{\text{ap}}) e^{\frac{\eta_a k'_i + \eta_b k'_i}{2} \sqrt{\eta_a k'_i \eta_b k'_i} \cos \theta} = 1 - y e^{x \cos \theta}. \end{aligned} \quad (6)$$

根据第 1 章的叙述,有效响应是当且仅当 $D_{k'_i k'_i}^{\text{L}}$ 和 $D_{k'_i k'_i}^{\text{R}}$ 只有一个探测器的响应。因此,整体的增益 $q_{k'_i k'_i}$ 为

$$q_{k_i k_i} = \frac{1}{2\pi} \int_0^{2\pi} [D_{k_i k_i}^L (1 - D_{k_i k_i}^R) + D_{k_i k_i}^R (1 - D_{k_i k_i}^L)] d\theta = 2y [I_0(x) - y], \quad (7)$$

式中, $I_0(\cdot)$ 为修正后的一阶贝塞尔函数。

进而可以得到每个脉冲窗口的平均响应概率为 $p = \sum_{k_a^* k_b^*} p_{k_a^*} p_{k_b^*} q_{k_a^* k_b^*}$, 每个脉冲的预期配对数 r_p 为

$$r_p = \left[\frac{1}{p[1 - (1-p)^{l_{\max}}]} + \frac{1}{p} \right]^{-1}. \quad (8)$$

为了后面叙述方便, 这里把 Z 基对和 X 基对的配对强度集合分类, 如表 1 所示。

表 1 根据有效探测计数计算方式的不同, 对 Z 基对和 X 基对的分类

Table 1 Classification of Z-basis and X-basis pairs based on the different methods for calculating effective detection counts

| 基矢配对 集合 | (k_a, k_b) |
|---------|--|
| Z 基对 | Z_1 $(\mu_a, \mu_b), (\mu_a, \nu_b), (\nu_a, \mu_b), (\nu_a, \nu_b)$ |
| | Z_2 $(\mu_a, o_b), (o_a, \mu_b), (\nu_a, o_b), (o_a, \nu_b), (o_a, o_b)$ |
| X 基对 | X_1 $(2\mu_a, 2\mu_b), (2\mu_a, 2\nu_b), (2\nu_a, 2\mu_b), (2\nu_a, 2\nu_b)$ |
| | X_2 $(2\mu_a, o_b), (o_a, 2\mu_b), (2\nu_a, o_b), (o_a, 2\nu_b)$ |

根据文献[33], Z 基对和 X 基对的有效探测计数 $n_{(k_a, k_b)}^Z$ 和 $n_{(k_a, k_b)}^X$ 分别为

$$n_{(k_a, k_b)}^Z = \frac{Nr_p}{p^2} \sum_{(k_a, k_b)} p_{k_a^*} p_{k_b^*} p_{k_a^*} p_{k_b^*} q_{k_a^* k_b^*} q_{k_a^* k_b^*},$$

$$n_{(k_a, k_b)}^X \approx \frac{Nr_p}{p^2} \frac{2\Delta}{\pi} p_{k_a^*} p_{k_b^*} p_{k_a^*} p_{k_b^*} \times (4y^4 - 8y^3 I_0(x) + 2y^2 (I_0(x\sqrt{2-2\cos\Delta}) + I_0(x\sqrt{2+2\cos\Delta}))). \quad (9)$$

而 Z 基对的有效错误探测计数 $t_{(k_a, k_b)}^Z$ 为

$$t_{(k_a, k_b)}^Z = \begin{cases} \frac{Nr_p}{p^2} \sum_{\substack{(k_a, k_b) \\ k_i^* = k_j^* = 0}} T_Z + \frac{Nr_p}{p^2} \sum_{\substack{(k_a, k_b) \\ k_i^* = k_j^* = 0}} T_Z, & \text{if } Z \in Z_1, \\ \frac{n_{(k_a, k_b)}^{Z_2}}{2}, & \text{if } Z \in Z_2, \end{cases} \quad (10)$$

式中, $T_Z = p_{k_i^*} p_{k_j^*} p_{k_i^*} p_{k_j^*} q_{k_i^* k_j^*} q_{k_i^* k_j^*}$ 。X 基对的有效错误探测计数 $t_{(k_a, k_b)}^X$ 为

$$t_{(k_a, k_b)}^X = \begin{cases} \frac{Nr_p}{p^2} \frac{2\Delta}{\pi} p_{k_i^*} p_{k_j^*} p_{k_i^*} p_{k_j^*} T_X, & \text{if } X \in X_1, \\ n_{(k_a, k_b)}^X, & \text{if } X \in X_2, \end{cases} \quad (11)$$

式中, $T_X = (4y^4 - 8y^3 I_0(x) + 2y^2 (I_0(x\sqrt{2-2\cos\Delta}) + I_0(x\sqrt{2+2\cos\Delta})))$ 。

3 仿真分析

Z 基对的单光子部分计数 M_{11} 和对应的相位错误率 e_{11}^{ph} 无法直接从实验中获取, 结合诱骗态理论可以估算出这些参数的边界。Z 基对的单光子部分计数 M_{11} 表示为

$$M_{11} = N_{(\mu_a, \mu_b)}^Z \mu_a \mu_b e^{-\mu_a - \mu_b} y_{11}^Z = \frac{N_{(\mu_a, \mu_b)}^Z \mu_a \mu_b e^{-\mu_a - \mu_b} (F^L - F^U)}{a_1^{\nu_a} a_1^{\mu_a} (b_1^{\nu_b} b_2^{\mu_b} - b_1^{\mu_b} b_2^{\nu_b})}, \quad (12)$$

$$F^L = \frac{a_1^{\mu_a} b_2^{\mu_b}}{N_{(\nu_a, \nu_b)}^Z} n_{(\nu_a, \nu_b)}^Z + \frac{a_1^{\nu_a} b_2^{\nu_b} a_0^{\mu_a}}{N_{(o_a, \mu_b)}^Z} n_{(o_a, \mu_b)}^Z + \frac{a_1^{\nu_a} b_2^{\nu_b} b_0^{\mu_a}}{N_{(\mu_a, o_b)}^Z} n_{(\mu_a, o_b)}^Z + \frac{a_1^{\mu_a} b_2^{\mu_a} a_0^{\nu_a} - a_1^{\nu_a} b_2^{\nu_a} a_0^{\mu_a} b_0^{\mu_b}}{N_{(o_a, o_b)}^Z} n_{(o_a, o_b)}^Z,$$

$$F^U = \frac{a_1^{\nu_a} b_2^{\nu_b}}{N_{(\mu_a, \mu_b)}^Z} n_{(\mu_a, \mu_b)}^Z + \frac{a_1^{\mu_a} b_2^{\mu_a} a_0^{\nu_a}}{N_{(o_a, \nu_b)}^Z} n_{(o_a, \nu_b)}^Z + \frac{a_1^{\mu_a} b_2^{\mu_a} b_0^{\nu_a}}{N_{(\nu_a, o_b)}^Z} n_{(\nu_a, o_b)}^Z, \quad (13)$$

式中: $a_n^{k_a}, b_n^{k_b}$ 意味着 Alice 和 Bob 发送的光子数分布满足泊松分布; 上标 k_a, k_b 分别为 Alice 和 Bob 发送光脉冲的强度; 下标 n 为发送光子数的数量。

相位错误率 e_{11}^{ph} 为

$$e_{11}^{\text{ph}} = \frac{T^U - T^L}{a_1^{2\nu_a} b_1^{2\nu_b} y_{11}^Z}, \quad (14)$$

式中, $T^U = \frac{t_{(2\nu_a, 2\nu_b)}^X}{N_{(2\nu_a, 2\nu_b)}^X} + \frac{a_0^{2\nu_a} b_0^{2\nu_b} t_{(2o_a, 2o_b)}^X}{N_{(2o_a, 2o_b)}^X}$, $T^L = \frac{a_0^{2\nu_a} t_{(0, 2\nu_b)}^X}{N_{(0, 2\nu_b)}^X} + \frac{b_0^{2\nu_b} t_{(2\nu_a, 0)}^X}{N_{(2\nu_a, 0)}^X}$ 。

在本文的仿真过程中, 假设 Alice 与 Bob 到达中心节点 Charlie 的通信距离相同, 也就可以认为 Alice 和 Bob 的光源设置相同, 即 $\mu_a = \mu_b = \mu, \nu_a = \nu_b = \nu, o_a = o_b = o, p_{\mu_a} = p_{\mu_b} = p_\mu, p_{\nu_a} = p_{\nu_b} = p_\nu, p_{o_a} = p_{o_b} = p_o$ 。为了更精确地考虑统计波动对安全密钥率的影响, 本文采用了切尔诺夫界限方法^[34]对仿真结果进行期望数据的界限估计。此方法能够有效地提供给定误差容限下安全密钥率的上界和下界, 从而为密钥率的计算提供更加可靠的估计结果。在优化方面, 为了提高系统的性能, 仿真中采用了基于粒子群优化算法的全局优化方案^[35]。相较于常用的局部搜索算法^[36], 粒子群算法能有效避免陷入局部最优解, 通过全局搜索策略探索解空间。其通过多个粒子同时搜索, 利用群体信息共享, 加速了寻找全局最优解的过程。因此粒子群算法消除了对初始值的依

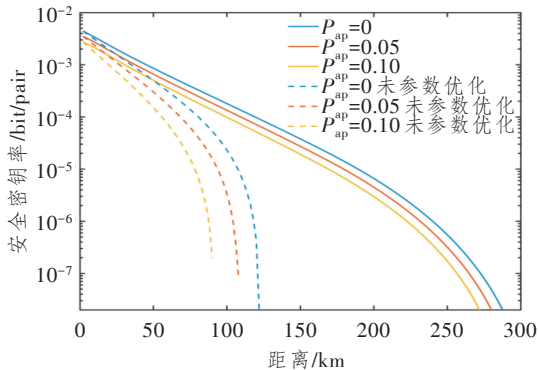
赖,可以显著提升安全密钥率,并确保在复杂的噪声和误差条件下,系统仍能保持较高的密钥率。仿真参数如表 2 所示,表中, η_d 为单光子探测器的效率, α 为光纤衰减系数, ϵ 为正确性和保密性的失败概率, e_d^Z 为 Z 基的对准误差, e_d^X 为 X 基的对准误差。

表 2 仿真所用参数

Table 2 Parameters used in the simulation

| p_d | η_d | $\alpha/\text{dB/km}$ | Δ | ϵ | f | e_d^Z | e_d^X | l_{\max} |
|-----------|----------|-----------------------|----------|------------|------|-----------|---------|------------|
| 10^{-8} | 70% | 0.2 | 16 | 10^{-10} | 1.16 | 10^{-6} | 0.1 | 2 000 |

根据本文所提分析方法,图 2 所示为后脉冲对 MP-QKD 安全密钥率的影响。图中的蓝线实线为基准曲线,反映了在没有后脉冲的情况下 MP-QKD 的安全密钥率。随着后脉冲增大到 0.05 和 0.10,安全密钥率出现一定程度下降。这是由于后脉冲会引入额外的噪声,影响信号的检测和误差率,从而降低密钥率。然而,值得注意的是,尽管存在后脉冲的影响,基于本文所提方案,密钥率的下降幅度仍然较小。具体而言,此方案能够有效抑制后脉冲的负面影响,从而确保了密钥率在较大范围内仍保持较高的水平。这表明,本文所提 MP-QKD 后脉冲分析方案在面对脉冲噪声时具有较强的鲁棒性。如图所示,基于粒子群优化算法的全局优化方案在提升安全密钥率方面优势显著。通过参数优化,该方案能够有效改善系统性能,而在未进行参数优化的情况下,安全密钥率则出现了急剧下降,凸显了粒子群优化算法在提升密钥率和确保系统安全性方面的重要作用。

图 2 不同后脉冲率下安全密钥率与距离的关系比较(总脉冲数为 10^{11})Figure 2 Comparison of the relationship between secure key rate and distance at different afterpulse rates (total pulse count: 10^{11})

由于后脉冲现象是由光脉冲或暗计数引起的,图 2 主要分析了 SNSPD 后脉冲对安全密钥率的影响。当暗计数增大时,即采用 SPAD 的参数模拟时(探测效率为 20%,暗计数为 10^{-6}),图 3 所示为不同

后脉冲概率对安全密钥率的影响。图中蓝色曲线为基准曲线,表示在无后脉冲情况下,基于 SPAD 的 MP-QKD 安全密钥率。随后脉冲概率增大至 0.05 和 0.10,安全密钥率曲线呈现一定程度的下降,其趋势与图 2 类似。图 3 进一步表明,本文所提方案在采用 SPAD 时同样能够抑制后脉冲的影响。然而,相较于 SNSPD,SPAD 具有较低的探测效率。对比图 2 和图 3 可知,采用 SPAD 的 MP-QKD 在安全密钥率和传输距离方面均存在显著劣势,难以满足实际应用中的性能要求。

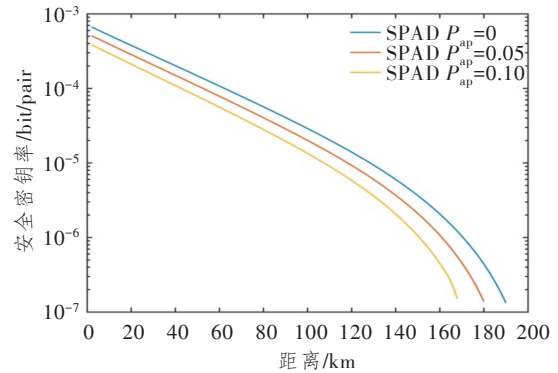
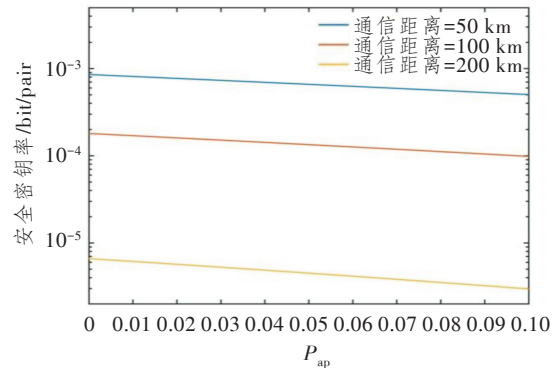
图 3 使用 SPAD 时,不同后脉冲率下安全密钥率与距离的关系比较(总脉冲数为 10^{11})Figure 3 Comparison of the relationship between secure key rate and distance at different afterpulse rates using SPAD (total pulse count: 10^{11})

图 4 所示为不同通信距离下,随着后脉冲率的增加,MP-QKD 系统安全密钥率的变化情况。

图 4 不同通信距离下安全密钥率与后脉冲率 P_{ap} 的关系比较(总脉冲数为 10^{11})Figure 4 Comparison of the relationship between secure key rate and afterpulse rates P_{ap} at different communication distances (total pulse count: 10^{11})

由图可知,尽管后脉冲率的增加导致安全密钥率有所下降,但其数量级基本保持不变。这表明,本文所提方案在应对后脉冲效应方面具有显著的优势。在不同的通信距离下,后脉冲效应的影响虽然

逐渐显现,但通过优化的方案,密钥率的下降得到了有效地抑制。这表明,本文所提方案在实际应用中能够较好地维持密钥率的稳定性,特别是在长距离传输的情况下,依然能有效应对后脉冲带来的不利影响,从而提高了 MP-QKD 系统的实用性和鲁棒性。

图 5 所示为通信距离为 100 km 时,信号态、诱骗态和真空态的优化参数变化情况。经过全参数优化后,信号态的强度明显大于诱骗态的强度,约为诱骗态强度的 15 倍。因此,后脉冲主要影响信号态,对 Z 基增益的估计产生了较大的影响。在实验中,类似于暗计数,后脉冲引起的量子比特误码率约为 0.5,这同样对相位错误率的估计产生了一定的干扰。为了抑制后脉冲效应带来的误码率上升,由图可知,随着后脉冲的增加,信号态的强度和概率均有所下降。这表明后脉冲的引入确实削弱了信号的强度,从而影响了量子密钥的生成。类似于信号态强度的变化,诱骗态强度也随着后脉冲的增加而逐渐降低。然而,与信号态概率的变化趋势不同,诱骗态的概率反而随着后脉冲的增加呈上升趋势。这一变化与 MP-QKD 的特殊结构密切相关。由于 MP-QKD 系统需要保留真空态以构成 Z 基对,因此在真空态的概率基本保持不变的情况下,诱骗态的概率自然会增加。这是为了维持协议的整体稳定性和安全性。尽管后脉冲引起的变化不可避免,但通过优化信号态和诱骗态的参数,本文所提方案能够有效减小后脉冲对安全密钥率的负面影响。

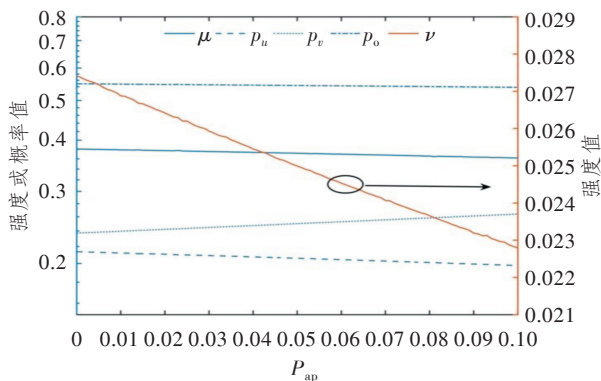


图 5 当总脉冲数为 10^{11} 且距离为 100 km 时,优化变量随 P_{ap} 增加的变化情况

Figure 5 Variation of the optimization variable with increasing P_{ap} when the total pulse count is 10^{11} and the distance is 100 km

4 结束语

本文提出了一种针对 MP-QKD 系统后脉冲效

应的分析方法,并通过优化方案有效抑制了后脉冲对安全密钥率的影响。研究表明,虽然后脉冲的引入会导致安全密钥率有所下降,但通过本文所提方法,密钥率的下降幅度较小,系统仍能保持较高的鲁棒性和稳定性。这表明,本文所提方案能够在实际应用中有效应对后脉冲带来的挑战,尤其是在复杂的通信环境中。展望未来,随着量子通信技术的发展,特别是在高频 QKD 系统中,后脉冲效应带来的影响将变得更加显著。高频率下的后脉冲效应会加剧噪声引入,从而影响系统的性能和安全性。因此,如何在高频 QKD 系统中进一步优化后脉冲抑制策略,提升系统的抗噪声能力,成为了未来研究的关键方向。通过改进信号态和诱骗态的优化方法,结合新的检测技术和噪声控制手段,将进一步有效降低后脉冲带来的负面影响。此外,随着量子通信网络的扩展,系统的长距离传输性能和抗干扰能力仍需进一步强化,以确保 MP-QKD 在多变和复杂的通信环境中的实际应用。

参考文献:

- [1] Bennett C H, Brassard G. Quantum Cryptography: Public Key Distribution and Coin Tossing[J]. Theoretical Computer Science, 2014, 560: 7-11.
- [2] Wang X B. Beating the Photon-number-splitting Attack in Practical Quantum Cryptography [J]. Physical Review Letters, 2005, 94(23): 230503.
- [3] 靳安然,李鹤.混合连续-离散变量量子密钥分发[J].光通信研究,2023(3):24-31.
- [4] 赵常兰,王天一.基于GMM的幅度相位联合编码 CVQKD 安全性分析[J].激光技术,2024,48(3):295-302.
- [5] Liao S K, Cai W Q, Liu W Y, et al. Satellite-to-ground Quantum Key Distribution[J]. Nature, 2017, 549(7670): 43-47.
- [6] Liu Y, Zhang W J, Jiang C, et al. Experimental Twin-field Quantum Key Distribution over 1 000 km Fiber Distance[J]. Physical Review Letters, 2023, 130(21): 210801.
- [7] Pirandola S, Laurenza R, Ottaviani C, et al. Fundamental Limits of Repeaterless Quantum Communications[J]. Nature Communications, 2017, 8: 15043.
- [8] Lucamarini M, Yuan Z L, Dynes J F, et al. Overcoming the Rate-distance Limit of Quantum Key Distribu-

- tion without Quantum Repeaters [J]. *Nature*, 2018, 557(7705): 400–403.
- [9] Pittaluga M, Minder M, Lucamarini M, et al. 600-km Repeater-like Quantum Communications with Dual-band Stabilization[J]. *Nature Photonics*, 2021, 15(7): 530–535.
- [10] Zeng P, Zhou H, Wu W, et al. Mode-pairing Quantum Key Distribution [J]. *Nature Communications*, 2022, 13: 3903.
- [11] Xie Y M, Lu Y S, Weng C X, et al. Breaking the Rate-loss Bound of Quantum Key Distribution with Asynchronous Two-photon Interference [J]. *PRX Quantum*, 2022, 3(2): 020315.
- [12] Zhu H T, Huang Y, Liu H, et al. Experimental Mode-pairing Measurement-device-independent Quantum Key Distribution without Global Phase Locking[J]. *Physical Review Letters*, 2023, 130(3): 030801.
- [13] Zhou L, Lin J, Xie Y M, et al. Experimental Quantum Communication Overcomes the Rate-loss Limit without Global Phase Tracking [J]. *Physical Review Letters*, 2023, 130(25): 250801.
- [14] Zhu H T, Huang Y, Pan W X, et al. Field Test of Mode-pairing Quantum Key Distribution [J]. *Optica*, 2024, 11(6): 883.
- [15] Li Z, Dou T, Cheng M, et al. Field Experimental Mode-pairing Quantum Key Distribution with Intensity Fluctuations[J]. *Optics Letters*, 2024, 49(23): 6609–6612.
- [16] Zhang J, Itzler M A, Zbinden H, et al. Advances in InGaAs/InP Single-photon Detector Systems for Quantum Communication [J]. *Light: Science & Applications*, 2015, 4(5): e286.
- [17] Li H, Jiang H, Gao M, et al. Statistical-fluctuation Analysis for Quantum Key Distribution with Consideration of After-pulse Contributions[J]. *Physical Review A*, 2015, 92(6): 062344.
- [18] Wang F X, Chen W, Li Y P, et al. Non-markovian Property of Afterpulsing Effect in Single-photon Avalanche Detector[J]. *Journal of Lightwave Technology*, 2016, 34(15): 3610–3615.
- [19] Yoshizawa A, Kaji R, Tsuchida H. After-pulse-discarding in Single-photon Detection to Reduce Bit Errors in Quantum Key Distribution [J]. *Optics Express*, 2003, 11(11): 1303.
- [20] Jain N, Stiller B, Khan I, et al. Risk Analysis of Trojan-horse Attacks on Practical Quantum Key Distribution Systems[J]. *IEEE Journal of Selected Topics in Quantum Electronics*, 2015, 21(3): 6600710.
- [21] Marsili F, Najafi F, Dauler E, et al. Afterpulsing and Instability in Superconducting Nanowire Avalanche Photodetectors[J]. *Applied Physics Letters*, 2012, 100(11): 112601.
- [22] Fujiwara M, Tanaka A, Takahashi S, et al. After-pulse-like Phenomenon of Superconducting Single Photon Detector in High Speed Quantum Key Distribution System [J]. *Optics Express*, 2011, 19(20): 19562–19571.
- [23] Burenkov V, Xu H, Qi B, et al. Investigations of Afterpulsing and Detection Efficiency Recovery in Superconducting Nanowire Single-photon Detectors [J]. *Journal of Applied Physics*, 2013, 113(21): 213102.
- [24] Kerman A J, Rosenberg D, Molnar R J, et al. Readout of Superconducting Nanowire Single-photon Detectors at High Count Rates [J]. *Journal of Applied Physics*, 2013, 113(14): 144511.
- [25] Miki S, Yabuno M, Yamashita T, et al. Stable, High-performance Operation of a Fiber-coupled Superconducting Nanowire Avalanche Photon Detector [J]. *Optics Express*, 2017, 25(6): 6796–6804.
- [26] Fan-Yuan G J, Wang C, Wang S, et al. Afterpulse Analysis for Quantum Key Distribution [J]. *Physical Review Applied*, 2018, 10(6): 064032.
- [27] Wang Z H, Wang S, Fan-Yuan G J, et al. Afterpulse Effect in Measurement-device-independent Quantum Key Distribution [J]. *Optics Express*, 2022, 30(16): 28534–28549.
- [28] Jiang C, Yu Z W, Hu X L, et al. Higher Key Rate of Measurement-device-independent Quantum Key Distribution through Joint Data Processing [J]. *Physical Review A*, 2021, 103: 012402.
- [29] Chau H F. Security of Finite-key-length Measurement-device-independent Quantum Key Distribution Using an Arbitrary Number of Decoys [J]. *Physical Review A*, 2020, 102: 012611.
- [30] Xu F, Curty M, Qi B, et al. Practical Aspects of Measurement-device-independent Quantum Key Distribution [J]. *New Journal of Physics*, 2013, 15(11): 113007.
- [31] Tomamichel M, Lim C C W, Gisin N, et al. Tight Finite-key Analysis for Quantum Cryptography [J]. *Nature Communications*, 2012, 3: 634.
- [32] Curty M, Xu F, Cui W, et al. Finite-key Analysis for Measurement-device-independent Quantum Key Distribution [J]. *Nature Communications*, 2014, 5: 3732.
- [33] Li Z, Dou T, Xie Y, et al. Mode Pairing Quantum Key Distribution with Light Source Monitoring [J]. *New Journal of Physics*, 2024, 26(9): 093011.
- [34] Yin H L, Zhou M G, Gu J, et al. Tight Security Bounds for Decoy-state Quantum Key Distribution [J]. *Scientific Reports*, 2020, 10(1): 14312.
- [35] Kennedy J. *Encyclopedia of Machine Learning* [M]. Boston, MA: Springer, 2011.
- [36] Xu F, Xu H, Lo H K. Protocol Choice and Parameter Optimization in Decoy-state Measurement-device-independent Quantum Key Distribution [J]. *Physical Review A*, 2014, 89(5): 052333.