量子通信技术及应用

DOI：10.16818/j.issn1001－5868.20251224001

测量设备无关量子密钥分发时间戳相位编码量子比特制备

陈继豪，王柳珑，黄绍霖，张丰艺，杨奎星*

（深圳技术大学 工程物理学院，广东 深圳 518118）

摘　要： 在测量设备无关量子密钥分发（Measurement-Device-Independent Quantum Key Distribution，MDI-QKD）系统中，时间戳相位编码因对光纤信道偏振扰动不敏感性而备受关注。传统制备方法通常采用不等臂马赫-曾德尔干涉仪，需借助复杂的相位锁定技术，导致系统复杂度和成本较高。针对该问题，文章提出一种结合激光器直接调制与外调制的高效制备方案：首先直接调制激光二极管产生相位随机的弱相干宽脉冲，再利用强度调制器将其斩波为两个相位差固定的时间戳脉冲，最后通过相位调制器加载相对相位信息。结果表明，该方案能够简单、稳定地制备出满足MDI-QKD要求的时间戳相位编码量子比特，有效降低了系统实现的复杂度。

关键词： 量子密钥分发；测量设备无关；时间戳相位编码

中图分类号： TN918　**文章编号：** 1001－5868(2026)02－0259－05

Preparation of Time-Bin Phase-Encoded Qubits for Measurement-Device-Independent Quantum Key Distribution

CHEN Jihao, WANG Liulong, HUANG Shaolin, ZHANG Fengyi, YANG Kuixing

(**College of Engineering Physics, Shenzhen Technology University, Shenzhen 518118, CHN**)

Abstract: In measurement-device-independent quantum key distribution (MDI-QKD) systems, time-bin phase encoding is widely applied owing to its robustness against polarization perturbations in fiber channels. The traditional preparation methods of time-bin phase qubits typically rely on asymmetric Mach - Zehnder interferometers, requiring complex phase-locking techniques, which increase the system complexity and costs. To address these limitations, in this study, an efficient preparation scheme—combining direct laser modulation with external modulation—is proposed. In this scheme, a directly modulated laser diode generates phase-randomized weak coherent wide pulses. These pulses are chopped into two time-bin pulses, with a fixed phase difference, using an intensity modulator, and the relative phase information is subsequently encoded using a phase modulator. Theoretical analysis demonstrates that this scheme enables the simple and stable preparation of time-bin phase-encoded qubits that satisfy the requirements of MDI-QKD, thus effectively reducing the complexity of system implementation.

Key words: quantum key distribution; measurement-device-independent; time-bin phase encoding

收稿日期：2025－12－24.

* **通信作者：**杨奎星

0 引言

量子密钥分发(Quantum Key Distribution, QKD)能够为通信双方提供无条件安全的密钥[1-2]。然而,实际系统中的非理想性,特别是探测器侧信道漏洞,使得QKD系统面临各种攻击威胁[3-4]。测量设备无关量子密钥分发(Measurement-Device-Independent Quantum Key Distribution, MDI-QKD)协议[5]的提出,彻底消除了所有针对探测器的攻击,是目前实用化程度最高的QKD协议之一。

在MDI-QKD系统中,编码方式的选择至关重要。相比于自由空间QKD系统常用的偏振编码方式,时间戳相位编码利用光子在不同时间模式下的叠加态携带信息,该编码方式对光纤信道中的偏振扰动和相位漂移具有极强的鲁棒性,因此更适合长距离光纤传输[6-7]。

在MDI-QKD实验中,时间戳相位量子比特的制备通常采用不等臂马赫-曾德尔干涉仪(Asymmetric Mach-Zehnder Interferometer, AMZI)[8]。然而,这种方案要求干涉仪两臂的光程差必须保持极高的稳定性,通常需要引入复杂的有源相位锁定反馈系统。这不仅增加了系统的体积和成本,还降低了系统的长期稳定性。

针对上述问题,本文提出一种无需不等臂干涉仪的时间戳相位编码量子比特制备方案。该方案利用激光二极管直接调制产生相位随机的宽脉冲,结合强度调制器(IM)的"斩波"效应和相位调制器(PM)的相位加载,实现了简单、高稳定性的时间戳相位量子比特制备。

1 系统方案设计

1.1 时间戳相位量子比特常见制备方法

在MDI-QKD协议中,Alice和Bob分别制备了一个光量子比特并发送给不可信的第三方Charlie。Charlie进行贝尔态测量(BSM)。对于时间戳相位编码,Alice和Bob发送的量子态形式为$|\psi\rangle=\frac{1}{\sqrt{2}}\left(|e\rangle+e^{i\phi}|l\rangle\right)$,其中$|e\rangle$和$|l\rangle$分别代表早(early)和晚(late)两个时间模式,ϕ为相对相位。

为了制备时间戳相位量子比特,传统方案广泛采用如图1所示的AMZI。由激光器产生窄脉冲,经AMZI分为两路,长臂引入延时Δt,得到时间差为Δt的两个Bin脉冲,后续进一步通过在其中一个Bin脉冲施加相位调制,实现编码。然而,为保证$|e\rangle$和$|l\rangle$之间相位的稳定性,AMZI两臂的光程差必须稳定在亚波长量级,外界微小的温度变化或机械振动都会导致相位漂移。因此,实验中通常需要引入额外的同频参考激光、光电探测器及移相器等组成的反馈回路来实时相位锁定[9]。这不仅显著增加了系统的体积和功耗,还提高了控制系统的复杂度。

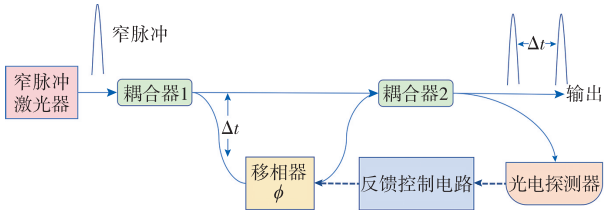


图1 AMZI干涉仪示意图

1.2 基于直接调制与外调结合的制备方案

本文提出一种"先宽脉冲,后切割,再调相"的制备方案,如图2所示。

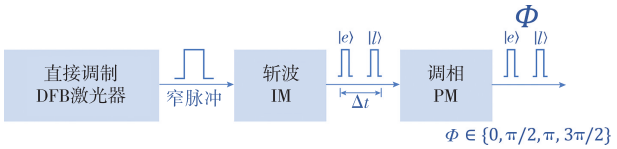


图2 斩波方法制备时间戳相位量子比特

1.2.1 方案流程

首先,直接调制分布反馈(DFB)激光器产生宽脉冲。由于激光器从阈值电流以下开始被驱动,每个光脉冲的全局相位是随机的。随后,光脉冲进入IM,IM由特定的双脉冲电信号驱动,将宽脉冲"雕刻"为两个时间间隔为Δt的窄脉冲(即$|e\rangle$和$|l\rangle$)。最后,PM在$|l\rangle$脉冲处加载相对相位信息$\phi\in\{0,\pi/2,\pi,3\pi/2\}$。

1.2.2 方案理论分析

假设激光器输出的宽脉冲电场为$E_{\text{in}}(t)=A(t)e^{i[\omega t+\theta(t)]}$,其中$A(t)$为包络幅度,$\theta(t)$为随机相位。经过强度调制器后,输出光场为:

$$E_{\text{out1}}(t)=E_{\text{in}}(t)\cdot T(t) \tag{1}$$

式中,$T(t)$为IM的透射函数,理想情况下为两个矩形窗函数:$T(t)=\text{rect}\left(\frac{t}{\tau}\right)+\text{rect}\left(\frac{t-\Delta t}{\tau}\right)$,$\tau$为脉冲宽度。

此时,两个脉冲来自同一相干宽脉冲的截取,若宽脉冲内的相位$\theta(t)$变化缓慢(即激光线宽较窄,相干时间$\tau_c\gg\Delta t$),则两个脉冲具有相同的全局

初始相位 θ_0。

随后经过相位调制器，对第二个脉冲施加相位 ϕ_m：

$$E_{out2}(t)\approx A(t)\left[\mathrm{rect}\left(\frac{t}{\tau}\right)+e^{i\phi_m}\mathrm{rect}\left(\frac{t-\Delta t}{\tau}\right)\right]e^{i(\omega t+\theta_0)} \tag{2}$$

在 MDI-QKD 的接收端 Charlie，来自 Alice 和 Bob 的光脉冲在分束器处发生双光子干涉。只要 Alice 和 Bob 各自制备的时间戳脉冲内部相对相位稳定，且脉冲波形重叠良好（但两组脉冲对之间的相位是随机的），即可获得高可见度的干涉曲线。

1.3　时间戳相位量子比特保真度验证

为了验证所制备量子比特的保真度，需要测量其时间戳之间的相位关系。验证装置如图 3 所示。

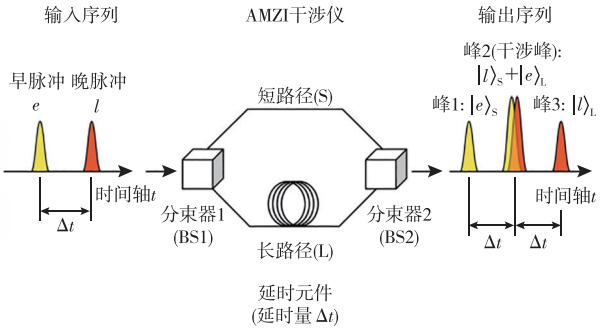


图 3　时间戳相位量子比特保真度验证

如图 3 所示，制备好的时间戳相位量子比特序列进入一个不等臂量为 Δt，且在相位差锁定的 AMZI 中。该 AMZI 将输入态转换为三个时间峰：

（1）短路径的 $|e\rangle$（最早到达）；

（2）短路径的 $|l\rangle$ 与长路径的 $|e\rangle$ 重叠（中间到达，发生干涉）；

（3）长路径的 $|l\rangle$（最晚到达）。

关注中间的干涉峰，通过扫描 AMZI 其中一臂的相位 δ，探测器上的计数率将随相位差变化呈现正弦振荡。干涉条纹可见度（Visibility，V）定义为：

$$V=\frac{C_{max}-C_{min}}{C_{max}+C_{min}} \tag{3}$$

式中，C_{max} 和 C_{min} 分别为最大和最小计数率。可见度 V 直接反映了制备态的保真度。如果 V 接近 1，说明制备的 $|e\rangle$ 和 $|l\rangle$ 具有极好的相干性和确定的相位关系，验证了本方案的可行性。

2　啁啾效应的影响分析

在半导体激光器中，通过改变注入电流的大小来直接调制输出光功率，注入电流的变化不仅改变了光子密度，还不可避免地改变了有源区（Active Region）内的载流子密度（Carrier Density）。当电流调制改变载流子密度时，增益的调整引起折射率实部变化，进而导致谐振频率偏移 $\Delta\nu(t)$，即出现频率啁啾（Chirp）[10-11]。使用直接调制制备相位随机的持续时间为 τ 的宽脉冲，由于啁啾的存在，脉冲相干时间 $\tau_c\leqslant\tau$，光场的瞬时相位 $\Phi(t)$ 不再是线性的，而是：

$$\Phi(t)=2\pi\nu_0 t+2\pi\int_0^t\Delta\nu(\tau)\mathrm{d}\tau+\theta_0 \tag{4}$$

式中，ν_0 是中心频率。如果从宽脉冲中截取时刻 t_1 和 t_2 的两个片段作为时间戳，它们之间的固有相位差为：

$$\Delta\Phi_{int}=\Phi(t_2)-\Phi(t_1)=2\pi\nu_0(t_2-t_1)+2\pi\int_{t_1}^{t_2}\Delta\nu(\tau)\mathrm{d}\tau \tag{5}$$

式中，第一项 $2\pi\nu_0(t_2-t_1)$ 称为中心频率项，不影响截取时间戳之间的相位差。因此，主要需要考虑的是由啁啾效应引起的第二项：

$$\Delta\Phi_{chirp}=2\pi\int_{t_1}^{t_2}\Delta\nu(\tau)\mathrm{d}\tau \tag{6}$$

根据经典公式[11]公式（6）中的频率偏移 $\Delta\nu(t)$ 与输出光功率 $P(t)$ 及其对时间的变化率的关系为：

$$\Delta\nu(t)=\frac{\alpha}{4\pi}\left[\frac{\mathrm{d}}{\mathrm{d}t}\ln P(t)+\kappa P(t)\right] \tag{7}$$

式中，α 是线宽增强因子，绝热啁啾系数 κ 是非线性增益效应与激光器几何结构/效率的复合参数，公式（7）中前后两项分别称为瞬态啁啾和绝热啁啾。第一项（瞬态啁啾）$\frac{\alpha}{4\pi}\frac{1}{P(t)}\frac{\mathrm{d}P(t)}{\mathrm{d}t}$ 主要受到光功率的变化率影响，即主要出现在光脉冲的上升沿和下降沿，同时受到 α 因子影响，是导致高速调制下频谱展宽的主要原因。第二项（绝热啁啾）$\frac{\alpha\kappa}{4\pi}P(t)$ 与光功率强度成正比，来源于增益饱和效应（Gain Saturation）或热效应。在高功率下，为了维持稳态，载流子密度需要略微高于阈值，导致频率产生一个与功率成正比的直流偏移。

将之前提到的半导体激光器频率啁啾公式代入积分中可以得到：

$$\Delta\Phi_{chirp}=\frac{\alpha}{2}\ln\left[\frac{P(t_2)}{P(t_1)}\right]+\frac{\alpha\kappa}{2}\int_{t_1}^{t_2}P(\tau)\mathrm{d}\tau \tag{8}$$

其中，第一项（瞬态项）$\frac{\alpha}{2}\ln\left[\frac{P(t_2)}{P(t_1)}\right]$只取决于两个斩波时刻光功率的比值，如果取$P(t_1)=P(t_2)$（例如宽脉冲顶部平坦区域内两点），则这一项为0。第二项（绝热项）$\frac{\alpha\kappa}{2}\int_{t_1}^{t_2}P(\tau)\mathrm{d}\tau$则与时间间隔（$t_2-t_1$）内光脉冲的功率积分有关，该项反映了高功率折射率的持续偏移导致的相位变化，这表明斩波方法制备时间戳相位量子比特方案需要保证直接调制宽脉冲的一致性。

如果频率偏移$\Delta\nu(t)$在脉冲持续期间剧烈变化，或者脉冲间的啁啾特性不稳定，将导致$\Delta\Phi_{\mathrm{chirp}}$出现随机抖动，从而破坏量子比特的编码精度。

图4展示了几种典型的啁啾脉冲形态，有些激光器瞬态啁啾现象较为明显，例如图4（a）与（c）有些激光器绝热啁啾现象较为明显，图4（b）与（d）需要分辨不同激光器的特征。

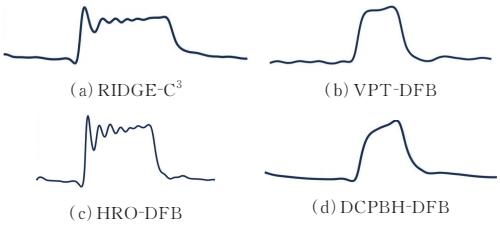


图4 四种单频激光器的啁啾现象[10]

3 啁啾效应的抑制

3.1 精准斩波方法抑制啁啾效应

为克服啁啾的不利影响，在电驱动信号设计上，确保宽脉冲具有平坦的顶部区域，使得在该区域内载流子密度相对稳定，频率啁啾最小化。同时，IM的切割窗口被设定在宽脉冲的平稳段，避开脉冲上升沿和下降沿的剧烈啁啾区。

3.2 注入锁定方法进一步抑制啁啾效应

为了有效抑制啁啾、改善激光器输出脉冲的相干性，除了在电驱动信号上优化脉冲波形（例如确保宽脉冲顶部平坦以稳定载流子密度）外，采用脉冲光种子技术[12-13]能够从物理机制上优化啁啾抑制效果，显著提升激光脉冲的时间相干性和模式质量[14]。该技术的原理是通过注入外部种子光，主导激光腔内的光子建立过程，从而取代由自发辐射随机触发激光发射的机制。这一方法可以大幅降低时间抖动，抑制啁啾的不利影响。

激光器中，脉冲的发射由自发辐射的随机性触发，引入了显著的时间抖动。脉冲光种子技术通过注入确定性的外部光子，为激光振荡提供精确的起始信号，将时间抖动降低[15]。即使激光脉冲本身仍存在频率啁啾，只要两个独立激光器的啁啾特性能实现同步，它们之间仍能产生高可见度的干涉。同时，光学注入还有助于抑制光谱中的边模，改善光源之间的光谱匹配度，从而支持高可见度的干涉。

4 与传统方案的对比

时间戳相位编码量子比特的制备通常采用传统的AMZI方案。激光脉冲经过AMZI后分成两路，长臂引入固定延时Δt，通过在一臂上施加相位调制实现编码。然而，该方案对环境干扰极其敏感。为保证前后两个脉冲之间的相对相位稳定，AMZI两臂的光程差必须控制在亚波长量级（$\sim10^{-8}$ m），这通常需要引入复杂的主动相位锁定系统。另一方面，基于AMZI的方案在光子集成芯片（PIC）化方面面临挑战。由于引入纳秒级延时需要较长的波导，这不仅占用巨大的芯片面积，还会带来显著的光损耗及热串扰问题，不利于低成本开发。所提出的基于激光器直接调制与外调制相结合的时间片编码制备方案可以有效规避上述问题。该方案无需物理上的长臂干涉结构，免除了主动相位锁定的需求，具有极高的稳定性，且结构紧凑，非常适用于片上集成量子发射机的研制。

5 结论

本文针对MDI-QKD系统中时间戳相位编码量子比特制备的复杂性与稳定性难题，提出一种基于半导体激光器直接调制与外调制相结合的高效制备方案。与传统依赖AMZI的方案相比，所提方案采用“宽脉冲制备—强度斩波—相位加载”的时序控制方法，从物理结构上摒弃了对长光程差干涉仪的依赖，从而天然免除了复杂的主动相位锁定系统，显著降低了硬件实现的复杂度与成本。针对半导体激光器直接调制过程中不可避免的频率啁啾效应，建立了包含瞬态啁啾与绝热啁啾的理论模型，并提出了“精准斩波”与“光学注入锁定”两种针对性的抑制策略。结果表明，通过截取宽脉冲顶部的平坦区域以及引入外部种子光进行注入锁定，可以有效抑制相位抖动，确保制备出的时间戳脉冲具

有极高的相位一致性与干涉可见度。综上所述，该方案不仅解决了传统方案环境鲁棒性差的问题，更具备结构紧凑、易于控制等优势，非常适用于未来片上集成量子发射机的研制，为高性能、低成本MDI-QKD系统的实用化部署提供了一条极具潜力的技术路径。

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] Lo H K, Chau H F. Unconditional security of quantum key distribution over arbitrarily long distances[J]. Science, 1999, 283(5410): 2050-2056.

[3] Lydersen L, Wiechers C, Wittmann C, et al. Hacking commercial quantum cryptography systems by tailored bright illumination[J]. Nature Photonics, 2010, 4(10): 686-689.

[4] Fung C F, Qi B, Tamaki K, et al. Phase-remapping attack in practical quantum-key-distribution systems [J]. Physical Review A, 2007, 75(3): 032314.

[5] Lo H K, Curty M, Qi B. Measurement-device-independent quantum key distribution[J]. Physical Review Letters, 2012, 108(13): 130503.

[6] Brendel J, Gisin N, Tittel W, et al. Pulsed energy-time entangled twin-photon source for quantum communication[J]. Physical Review Letters, 1999, 82(12): 2594-2597.

[7] Vijayadharan K, Bolaños M R, Avesani M, et al. A Sagnac-based arbitrary time-Bin state encoder for quantum communication applications [J]. EPJ Quantum Technology, 2025, 12(1): 129.

[8] Liu Y, Chen T Y, Wang L J, et al. Experimental measurement-device-independent quantum key distribution[J]. Physical Review Letters, 2013, 111(13): 130502.

[9] Lo H K, Curty M, Qi B. Measurement-device-independent quantum key distribution[J]. Physical Review Letters, 2012, 108(13): 130503.

[10] Koch T L, Bowers J E. Nature of wavelength chirping in directly modulated semiconductor lasers [J]. Electronics Letters, 1984, 20(25/26): 1038-1040.

[11] Koch T L, Linke R A. Effect of nonlinear gain reduction on semiconductor laser wavelength chirping[J]. Applied Physics Letters, 1986, 48(10): 613-615.

[12] Chauchard E A, Wey J S, Lee C H, et al. Coherent pulsed injection seeding of two gain-switched semiconductor lasers [J]. IEEE Photonics Technology Letters, 1991, 3(12): 1069-1071.

[13] Comandar L C, Lucamarini M, Fröhlich B, et al. Near perfect mode overlap between independently seeded, gain-switched lasers[J]. Optics Express, 2016, 24(16): 17849.

[14] Comandar L C, Lucamarini M, Fröhlich B, et al. Quantum key distribution without detector vulnerabilities using optically seeded lasers[J]. Nature Photonics, 2016, 10(5): 312-315.

[15] Seo D S, Kim D Y, Liu H F. Timing jitter reduction of gain-switched DFB laserby external injection-seeding [J]. Electronics Letters, 1996, 32(1): 44-45.

作者简介：

陈继豪(2000—)男，广东省广州市人，硕士研究生，主要研究方向为量子通信等；

杨奎星(1991—)男，广东省深圳市人，博士，副研究员，主要研究方向为量子通信、量子精密测量等。