基于硬件同步的四态离散调制连续变量量子密钥分发*

张云杰[1)2)] 王旭阳[1)3)†] 张瑜[1)] 王宁[2)] 贾雁翔[1)]
史玉琪[1)2)] 卢振国[1)3)] 邹俊[4)] 李永民[1)3)‡]

1) (山西大学光电研究所, 量子光学与光量子器件国家重点实验室, 太原 030006)

2) (山西大学物理电子工程学院, 太原 030006)

3) (山西大学, 省部共建极端光学协同创新中心, 太原 030006)

4) (浙江大学, 浙江大学杭州国际科创中心, 杭州 311215)

(2023 年 11 月 7 日收到; 2023 年 12 月 6 日收到修改稿)

在连续变量量子密钥分发系统中, 同步技术是确保通信双方时钟和数据一致的关键技术. 本文通过巧妙设计发送端和接收端仪器的硬件时序, 采用时域差拍探测方式和峰值采集技术, 实验实现了可硬件同步的四态离散调制连续变量量子密钥分发. 通信双方在设计好的硬件同步时序下可实现时钟的恢复和数据的自动对齐, 无需借助软件算法实现数据的对齐. 本文采用了加拿大滑铁卢大学 Norbert Lütkenhaus 研究组提出的针对连续变量离散调制协议的安全密钥速率计算方法. 该方法需计算出接收端所测各种平移热态的一阶矩和二阶 (非中心) 矩, 以此为约束条件结合凸优化算法可计算出安全密钥速率. 计算过程中无需假设信道为线性信道, 无需额外噪声的估算. 密钥分发系统重复频率为 10 MHz, 传输距离为 25 km, 平均安全密钥比特率为 24 kbit/s. 本文提出的硬件同步方法无需过采样和软件帧同步, 减小了系统的复杂度和计算量, 在一定程度上降低了系统所需的成本、功耗和体积, 有效地增强了连续变量量子密钥分发的实用性.

关键词: 连续变量量子密钥分发, 硬件同步, 四态离散调制, 时域差拍探测

PACS: 03.67.Hk, 03.67.Dd **DOI:** 10.7498/aps.73.20231769

1 引 言

在量子通信领域, 量子密钥分发 (quantum key distribution, QKD) 技术基于量子力学基本原理, 具有理论无条件安全性, 在信息安全领域具有重要的应用前景[1–4]. 根据编码和测量方式的不同, 量子密钥分发技术主要分为离散变量量子密钥分发 (discrete-variable quantum key distribution, DV-QKD) 和连续变量量子密钥分发 (continuous-variable quantum key distribution, CV-QKD)[5–24]. DV-QKD 采用单光子探测器, 具有通信距离长等优势, 是目前实现 QKD 城际组网的优选方案. 近期, 基于双场方案和光纤信道, 密钥分发距离已相继拓展至 830 km 和 1002 km[25–27], 为实现 QKD 的长距离和大规模城际组网奠定了很好的基础. CV-QKD 通常采用相干探测器, 与现有的经典相干通信系统具有良好的兼容性, 具有高传输速率等

* 山西省应用基础研究计划 (批准号: 202103021224010)、山西省省筹资金资助回国留学人员科研项目 (批准号: 2022-016)、国家自然科学基金 (批准号: 62175138, 62205188, 11904219)、量子光学与光量子器件国家重点实验室开放课题 (批准号: KF202006) 和山西“1331 工程”重点项目资助课题.

† 通信作者. E-mail: wangxuyang@sxu.edu.cn

‡ 通信作者. E-mail: yongmin@sxu.edu.cn

特点[28,29], 在传输速率方面目前已达 10 GHz 带宽[30]. CV-QKD 通信距离相对较短, 光纤信道下目前最远距离为 202 km [31]. QKD 在实现城域组网和大规模应用的过程中, 降低系统成本、体积、功耗、系统复杂度和高计算量等是目前面临的主要问题. CV-QKD 整体系统可实现芯片化集成, 特别是除了光源以外的其他部分, 可基于标准的硅基光电子芯片实现集成, 在低成本城域组网方面具有优势, 已陆续有科研小组在 CV-QKD 集成化方向展开工作[32–35].

本文的工作主要集中在降低系统的复杂度和计算量方面, 基于四态调制方案简化了调制方法和时序结构, 实现了硬件同步, 避免了过采样和软件帧同步算法的使用. CV-QKD 根据调制方式的不同, 又分为高斯调制方案和非高斯调制方案. 非高斯调制方案主要包括二态、四态、八态等协议, 具有调制简单, 容易实现高传输速率等优势. 该协议最早在 2009 年由 Leverrier 等[36,37] 提出, 并基于线性信道初步证明了该方案的安全性. 此后, 研究人员对其安全性证明进行了不断的改进和优化[38–42], 同时, 相关方案也陆续得到了实验验证[43–46]. 从相关实验验证中不难看出, 离散调制方案和高斯调制方案的实验装置基本相似, 在目前的实现方式中普遍采用了过采样技术和数据帧软件同步技术[47–49]. 过采样技术中, 数据采集速率通常比数据脉冲速率高出很多, 不仅需要高速的 AD 采样, 而且数据处理量较大. 在数据帧软件同步技术中, Alice 和 Bob 需要采用部分数据进行两者数据的对齐, 该种同步技术需要一定的计算资源来实现, 影响通信系统的实时性. 文献 [47] 在时钟系统中引入了高精度时钟, 有效地提高了对脉冲峰值的采集精度, 但是系统的采集还是基于过采样技术. 过采样技术使得系统采样点较多, 需采用算法将峰值点从多采样点中找出, 同时还需要结合一定的帧同步方法实现双方数据的对齐.

针对上述问题, 本文将高精度可延时脉冲发生器输出的时钟信号和时域差拍探测 (time domain heterodyne detection, THD) 器输出的脉冲信号分别直接作为 ADC 转换器的时钟和采样信号, 可通过精确延迟时钟上升沿对脉冲信号的峰值进行精确采集, 避免了过采样技术的使用, 同时接收端的采样以延迟的时钟作为触发, 可实现数据的自动对齐. 这种硬件同步方法巧妙利用了系统的时序, 相比过采样和软件层的数据帧同步算法, 降低了系统对 AD 采样速率的需求和计算量, 能够有效增强 CV-QKD 的实用性.

在计算安全密钥速率方面, 引入了加拿大滑铁卢大学 Norbert Lütkenhaus 研究组[38,50] 提出的算法, 无需额外噪声的估算, 仅需计算出接收端平移热态正交分量的一阶矩和二阶矩. 本文实验验证了该安全密钥速率算法在时域 CV-QKD 系统中的可行性. 希望相关技术能够为 CV-QKD 低成本, 高效城域组网做出贡献.

论文的第 2 部分对四态离散调制协议的制备测量 (prepare-and-measure, PM) 方案和纠缠等效 (entanglement-based, EB) 方案进行了介绍, 第 3 部分是硬件时序的设计, 第 4 部分是实验系统的时序实现和安全密钥速率的实验结果, 第 5 部分是总结.

2 四态离散调制协议

在基于相干态的 CV-QKD 实验中, 通常采用 PM 方案实现量子态的产生, 传输与测量, 而在安全性证明中, 通常基于等效的 EB 方案进行证明. 下面对四态离散调制协议的 PM 和 EB 方案进行详细的介绍.

2.1 制备测量方案

对于四态离散调制协议的 PM 方案, 发送方 Alice 随机制备和发送集合 $S=\{|\alpha\rangle,|\mathrm{i}\alpha\rangle,|-\alpha\rangle,|-\mathrm{i}\alpha\rangle\}$ 中的相干态, 可表示为

$$|\alpha_k\rangle=|\alpha \mathrm{e}^{\mathrm{i}k\pi/2}\rangle,\ k\in\{0,1,2,3\}. \tag{1}$$

其在相空间的 Winger 函数如图 1(a) 所示, 子图为其俯视图, 这里取 $\alpha=0.75$, 其中红色圆圈为相干态的误差圆, 其半径为散粒噪声的标准差 $\sigma_{\mathrm{a}}=1/2$. 本文中所有方差参数均归一化到散粒噪声. 经过 25 km 标准单模光纤传输后相干态的强度被衰减, 并且叠加了从系统引入的额外噪声, 此时相干态 $|\alpha_k\rangle$ 转变为平移热态 ρ_k^{th}, 其 Winger 函数 $W(\gamma)$ 相比 Alice 发送的相干态向原点移动, 可表示为

$$W(\gamma)=\frac{2}{\pi(1+T\varepsilon)}\exp\left[\frac{-2|\gamma-\sqrt{T}\alpha_k|^2}{1+T\varepsilon}\right], \tag{2}$$

其中 $\gamma=X+\mathrm{i}Y$, 信道透射率 $T=0.316$, 探测效

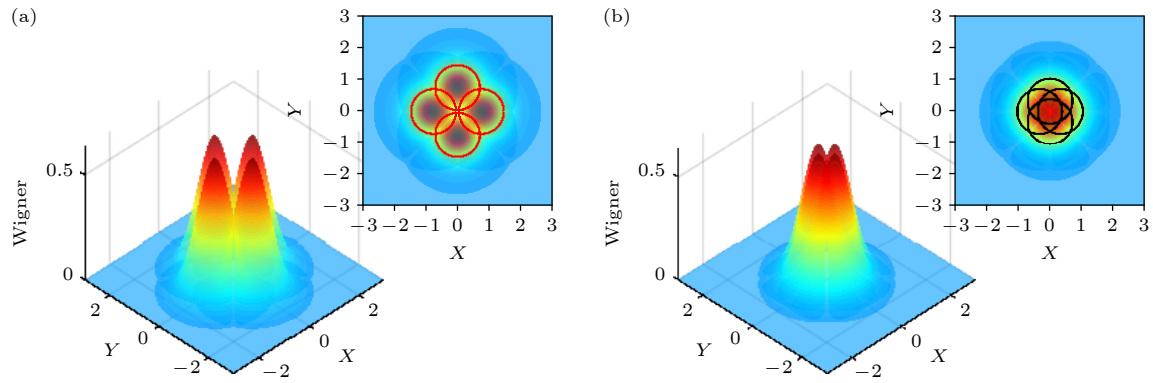

图 1 发送端和接收端的量子态在相空间中的 Wigner 函数图形 (a) 发送端 Alice 制备的四个相干态的 Wigner 函数图形和其俯视图; (b) 接收端 Bob 接收到的四个平移热态的 Wigner 函数图形和其俯视图

Fig. 1. Wigner pictures of the quantum states of Alice and Bob: (a) The Wigner pictures of four coherent states prepared by Alice and their top view; (b) the Wigner functions of four displaced thermal states received by Bob and their top view.

率 $\eta=0.6$, 假设等效到信道输入端的额外噪声 $\varepsilon=0.02$. 平移热态的 Wigner 函数在相空间的图形如图 1(b) 所示, 子图为俯视图, 其中黑色圆圈为每个平移热态的误差圆, 其半径为标准差 $\sigma_b=\sqrt{1+T\varepsilon}/2$.

接收端 Bob 采用时域差拍探测器 THD 对每个量子态的正交分量进行测量. 测量完成后通信双方利用各自的数据进行数据后处理, 主要包括一阶矩和二阶矩的估计, 基于凸优化方法计算安全密钥速率、数据协调和私密放大等.

2.2 纠缠态方案

四态离散调制协议的 EB 方案中, 发送端 Alice 制备的量子态为纠缠态 $|\psi\rangle_{AA'}$, 通常表示为如下纯态的形式:

$$|\psi\rangle_{AA'}=\sum_{k=0}^{3}\sqrt{p_k}|k\rangle_A|\alpha_k\rangle_{A'}. \tag{3}$$

概率幅 $\sqrt{p_k}=1/2$, 量子态 $|k\rangle_A$, $k=(0,1,2,3)$ 存储在 Alice 端寄存器 A 中, 可构成一组正交归一基矢. Alice 对量子态 $|k\rangle_A$ 进行正算符取值测量 $\hat{M}^A=|k\rangle\langle k|$, 同时发送寄存器 A' 中的量子态 $|\alpha_k\rangle$. 当量子态传送至接收端时, Alice 和 Bob 将共享如下形式的联合态:

$$\hat{\rho}_{AB}=(\mathrm{id}_A\otimes\mathcal{E}_{\mathcal{A}'\to\mathcal{B}})(|\psi\rangle\langle\psi|_{AA'}), \tag{4}$$

id_A 用于对寄存器 A 中的量子态进行标识操作, 可用单位算符表示. $\mathcal{E}_{A'\to B}$ 表示寄存器 A' 中的量子态传输至接收端的过程中等效的正定保迹量子操作. 安全密钥速率可用如下表达式进行计算:

$$R=\min_{\hat{\rho}_{AB}\in\mathcal{S}}D[\mathcal{G}(\hat{\rho}_{AB})\mathcal{Z}(\mathcal{G}(\hat{\rho}_{AB}))]-p_{\mathrm{pass}}\delta_{\mathrm{EC}}. \tag{5}$$

集合 $\mathcal{S}$ 包含了所有满足实验观测条件的量子态密度算符 $\hat{\rho}_{AB}$, $D(\hat{\rho}\,\|\hat{\sigma})$ 代表量子相对熵, 可用如下表达式进行计算:

$$D(\hat{\rho}\,\|\hat{\sigma})=\mathrm{Tr}(\hat{\rho}\log_2\hat{\rho})-\mathrm{Tr}(\hat{\rho}\log_2\hat{\sigma}), \tag{6}$$

其中 $\mathcal{G}(\hat{\sigma})$ 为量子态的后处理映射, $\mathcal{Z}(\hat{\sigma})$ 为量子信道的约束,

$$\mathcal{G}(\hat{\sigma})=\hat{K}\hat{\sigma}\hat{K}^{\dagger}, \tag{7}$$

$$\hat{K}=\sum_{j=0}^{3}|j\rangle_R\otimes\mathbb{I}_A\otimes\left(\sqrt{\hat{R}_j}\right)_B, \tag{8}$$

$$\mathcal{Z}(\hat{\sigma})=\sum_{j=0}^{3}(|j\rangle\langle j|_R\otimes\mathbb{I}_{AB})\,\hat{\sigma}\,(|j\rangle\langle j|_R\otimes\mathbb{I}_{AB}), \tag{9}$$

其中 $\hat{R}_j$ 为区域算符; p_{pass} 是用于产生密钥的数据所占的比例, 两者由后处理方式决定; δ_{EC} 是每个信号的信息泄漏量, 其详细计算方法可参考相关文献 [23,38,50].

3 硬件同步时序

实验中, 四态调制协议的实现采用脉冲光方案, 在基于脉冲光实现 CV-QKD 的系统中, 通常采用级联两个或多个振幅调制器的方式产生高消光比脉冲光, 之后将高消光比脉冲光分为信号光和本振光[51,52]. 为了同步实现对信号光的振幅和相位进行调制, 还需要与信号光同步的两至三路调制信号. 基于该思路采用了图 2(a) 所示时序结构. 发送端 Alice 采用四通道任意波形发生器 (arbitrary waveform generator, AWG) 产生四路同步的输出. 其中一路 AWG. CH1 为方波信号, 用于触发

脉冲发生器 PG1 产生两路可精确延时的时钟信号. AWG 其余三路 (AWG.CH2—4) 用于同步输出信号光的振幅和相位调制信号, 具体电压值取决于调制器的半波电压. 需要注意的是脉冲发生器 PG1 输出的电脉冲信号需延时 Δt_1, Δt_1 大于调制信号的上升时间, 这样可将信号光移动至调制信号的平坦区域, 实现信号光振幅或相位的精确调制; 同时两电脉冲间需要有延时 Δt_2, 用于补偿两振幅调制器间的尾纤引起的光程差.

接收端 Bob 采用时域差拍探测装置 THD 对脉冲信号光进行测量, 可输出与脉冲信号光同步且峰值与正交分量呈线性关系的电脉冲信号 THD.X&Y. 为了能够精确采集到峰值, Bob 利用本振光场恢复出所需时钟, 实现与 Alice 端的时钟同步, 避免持续采集峰值的过程中采集值因时钟不同步而出现错位. 基于该思路我们设计的接收端时序如图 2(b) 所示. RCLK (recovery clock, RCLK) 为 Bob 采用时钟恢复装置恢复出的时钟信号, 该恢复时钟输入到数字脉冲发生器 PG2, 经过精确的延时 Δt_3 后由脉冲发生器 PG2.CH1 通道输出. PG2.CH1 和 THD.X&Y 信号同时输入到数据采集卡的外部时钟输入端和信号输入端口, 为了实现信号峰值的精确采集, 延时时钟的上升沿与 THD 的两路信号峰值需保持固定的时间差 Δt_4.

在双方通信时, 发送端 Alice 同步启动任意波形发生器 AWG 的四个通道, 信号光和本振光以数据帧的结构向 Bob 发送, 每个数据帧又由若干个数据块构成, 每个数据块由测试脉冲和数据脉冲构成[53]. 测试脉冲主要用于相对相位的计算, 探测器的平衡锁定和散粒噪声的校准等; 数据脉冲主要用于量子态的振幅和相位调制. 在接收端, Bob 基于恢复的时钟信号依次对 THD 输出的每个脉冲信号进行采集, 以数据帧为单位对数据进行存储. 系统启动时 Alice 从第一个时钟信号开始, 将第一对正交分量信号加载在第一个光脉冲上, Bob 接收到第一个时钟信号时, 便开始采集第一对电脉冲信号的峰值, 其他脉冲信号依序发送与接收, 因此双方的数据会自动对齐, 无需借助额外的数据帧对齐算法.

4 CV-QKD 实验与安全密钥分析

4.1 CV-QKD 实验系统

为实现上述硬件同步方案, 设计并实验验证了脉冲重复速率为 10 MHz 的四态离散调制相干态 CV-QKD 系统 (图 3). 下面将对其进行详细的介绍.

在发送端, Alice 端光源采用 1550 nm DFB 连续激光器, 振幅调制器 AM 是基于铌酸锂晶体电光效应的马赫-曾德尔调制器, 两个级联的振幅调制器 AM1, AM2 在脉冲发生器 PG1 (ASG8100) 输出的两路电脉冲信号的驱动下将连续光调制成脉宽为 10 ns、重复速率为 10 MHz、消光比大于 70 dB 的脉冲光. 脉冲光经过 99/1 的保偏光纤分束器分为信号光场和本振光场. 在信号光路中, AM3, AM4 用来调制测试脉冲和数据脉冲的强度, 相位调制器 PM1 用来完成信号光相位的调制, 这三个调制器的调制电压由任意波形发生器 AWG (TFG 2944A) 的 CH2-4 通道提供. 信号光路中的 90/10 保偏光纤耦合器分出一小部分信号光场并接入光电探测器 PD1, 其输出信号由多功能数据输入输出卡 USB 6259 的模拟输入通道 AI 采集, 结合四通道输出信号 (AO0-3) 可用于扫描和稳定四个振幅调制器的偏置电压. 10 m 保偏光纤 PMF1 用于时分复用, 光纤偏振合束器 PBC 用于偏振复用, 两器件使信号光场和本振光场以时分复用和偏振复用的方式在 25 km 的单模光纤中传输.

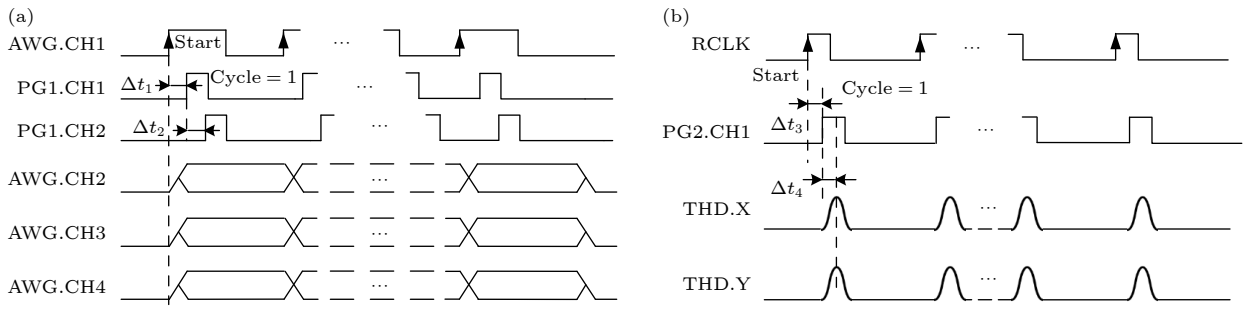

图 2 CV-QKD 系统的电信号时序图 (a) 发送端 Alice 的电信号时序图; (b) 接收端 Bob 的电信号时序图

Fig. 2. Timing diagrams of the CV-QKD system: (a) The timing diagram of Alice; (b) the timing diagram of Bob.

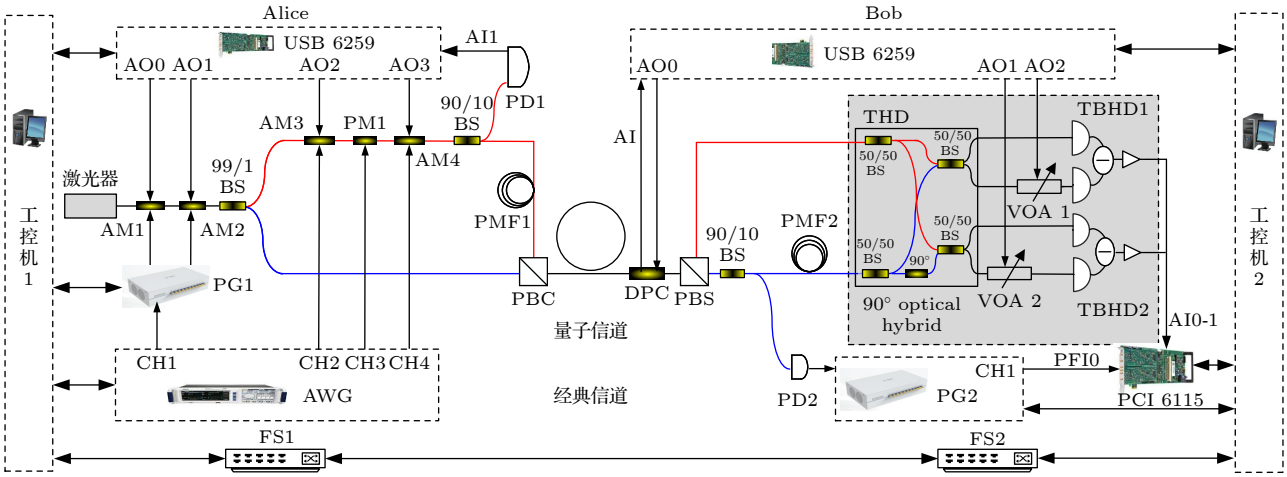

图 3 基于硬件同步方案的四态离散调制 CV-QKD 系统光路图. AM, 振幅调制器; PM, 相位调制器; PG, 脉冲发生器; AWG, 任意波形发生器; PD, 光电探测器; PMF, 保偏光纤; PBC, 偏振合束器; PBS, 偏振合束器; DPC, 动态偏振控制器; VOA, 可调光衰减器; THD, 时域差拍探测器; TBHD, 时域平衡零拍探测器; FS, 光纤交换机

Fig. 3. Scheme of the four-state discrete modulation CV-QKD system based on the hardware synchronization method. AM, amplitude modulator; PM, phase modulator; PG, pulse generator; AWG, arbitrary waveform generator; PD, photodetector; PMF, polarization maintaining fiber; PBC, polarization beam combiner; PBS, polarization beam splitter; DPC, dynamic polarization controller; VOA, variable optical attenuator; THD, time domain heterodyne detector; TBHD, time domain balanced homodyne detector; FS, fiber switch.

两光场在单模光纤中传输后到达 Bob 端, 动态偏振控制器可对单模光纤引起的双折射效应进行补偿, 使两光场偏振重新恢复至线偏振光场, 然后经光纤偏振分束器 PBS 后, 分别进入信号光路和本振光路. 本振光路中, 90/10 保偏光纤耦合器将一小部分光场分出并连接至高速光电探测器 PD2. PD2 产生的电脉冲信号作为恢复的时钟信号 RCLK, 并接入到脉冲发生器 PG2 中, 输出可精确延时的时钟信号. 本振光场经 10 m 保偏光纤延迟线后与信号光场同时进入时域差拍探测装置 THD. THD 主要由 90°光混频器和两个时域平衡零拍探测器 TBHD1 和 TBHD2 构成, 可输出与信号光场的正交 X 和 Y 分量成线性关系的电脉冲信号, 探测效率为 0.6 [54,55]. 精确延时的时钟信号和 THD 输出的脉冲信号分别输入至多功能数据输入输出卡 PCI6115 的时钟端口 PFI0 和数据采集端口 AI0-1, PCI6115 可对脉冲信号的峰值进行精确的采集. 接收端没有相位调制器对信号光和脉冲光的相对相位进行锁定, Bob 端可根据测试脉冲计算出当前的相位, 并对正交分量进行旋转, 得出正确的正交分量 [56]. 两个电动光纤可变衰减器 VOA1 和 VOA2 分别用于自动调节时域平衡零拍探测器 TBHD1 和 TBHD2 的平衡. 自动平衡过程中, 反馈信号可基于测试脉冲计算出, 并经由 USB 6259 输出至电动可变光纤衰减器中 [57].

系统运行过程中, 信号反馈, 参数估计和安全密钥速率的计算均由各方的工控机完成, 两工控机通过光纤交换机 FS1 和 FS2 完成经典通信. 基于硬件同步方案, 硬件发送和采集的速率理论上可以达到百兆赫兹甚至千兆赫兹, 受限于当前时域差拍探测器的速率, 将系统的脉冲重复速率调整至 10 MHz[54].

4.2 系统硬件时序

实验中, 发送端 AWG 同步输出的四通道波形和脉冲发生器 PG1 输出的脉冲波形由示波器 (MSO 5204B) 捕捉测量, 如图 4 所示. 图 4(a) 是 AWG.CH1 输出的时钟波形, 展开后如图 4(b) 所示, 周期为 10 MHz, 电压幅度为 0—3.3 V, 占空比 50%. 图 4(c) 是 AWG.CH2-4 输出的一个数据块的振幅和相位调制的波形, 每个调制数据的持续时间为 100 ns, 对应于脉冲通道 TFG.CH1 的周期. 一个数据块含有 100 个调制脉冲, 持续时间为 10 μs, 由测试脉冲和数据脉冲构成. 数据块是数据帧的基本构成单元, 一个数据帧含有 10^7 个脉冲, 持续时间为 1 s. AWG.CH1 产生的时钟脉冲可触发 PG1 同步产生两路可精确延时的脉冲信号, 主要用于高消光比脉冲光的产生, 如图 4(d) 所示. 脉

宽为 10 ns, 周期为 100 ns、两脉冲总体延时为 $\Delta t_1 = 20$ ns, 脉冲间相对延时为 $\Delta t_2 = 15$ ns, 对应于振幅调制器 AM1 和 AM2 间 3 m 长的尾纤.

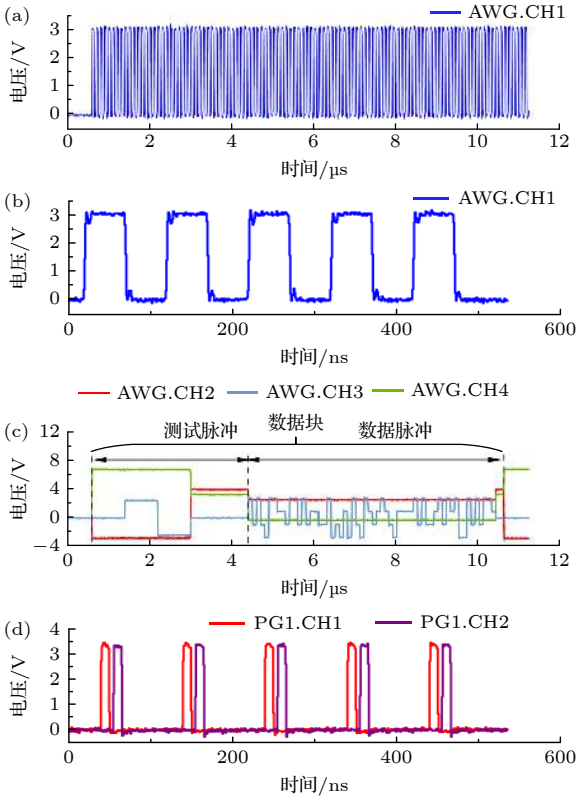

图 4 发送端 Alice 的各种信号波形 (a) AWG.CH1 输出的时钟信号波形; (b) 图 (a) 的展开波形; (c) AWG.CH2-4 输出的一个数据块的调制信号波形; (d) PG1.CH1-2 输出的脉冲信号波形

Fig. 4. Various waveform at Alice's side: (a) The waveform of clock signals generated by AWG.CH1; (b) the expanded waveform of panel (a); (c) the waveform of one block modulated signals generated by AWG.CH2-4; (d) the waveform of pulse signals generated by PG1.CH1-2.

实验中, 接收端光电探测器 PD2, 脉冲发生器 PG2 和 THD 输出信号波形由示波器 (MSO 5204B) 捕捉测量, 如图 5 所示. RCLK 为 PD2 探测器输出的时钟恢复信号, 周期为 10 MHz, 电压幅值为 0—700 mV, 脉宽约为 10 ns, 如图 5(a) 所示. RCLK 输入到 PG2, 触发 PG2.CH1 产生采集时钟信号, 周期为 10 MHz, 电压幅度为 0—3.3 V, 占空比 30%, 如图 5(b) 所示. 利用示波器的数字荧光示波功能, 记录了 THD 输出的散粒噪声波形色温图和四平移热态的波形色温图, 分别如图 5(c) 和图 5(d) 所示. 其中真空散粒噪声与电子学噪声比为 11.2 dB. 通过精确控制 PG2.CH1 的延时时间 Δt_3, 确保 PG2.CH1 的上升沿与 THD 的输出的峰值信号保持固定的时间差 $\Delta t_4 = 35$ ns, 从而实现峰值的精确采集.

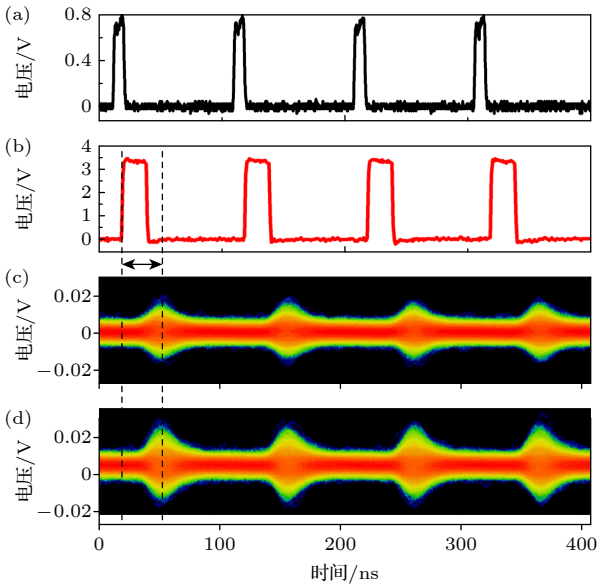

图 5 接收端 Bob 的各种信号波形 (a) PD2 输出的恢复时钟信号波形; (b) PG 2.CH1 输出的时钟信号波形; (c) THD 输出的散粒噪声色温图; (d) THD 输出的平移热态的色温图

Fig. 5. Various waveform at Bob's side: (a) The waveform of recovery clock signals generated by PD2; (b) the waveform of clock signals generated by PG2.CH1; (c) the color temperature waveform of the shot noise generated by THD; (d) the color temperature waveform of the displaced thermal states generated by THD.

4.3 实验结果

接收端 Bob 对量子态的两个正交分量的一阶矩 $\langle \hat{X}_k \rangle$, $\langle \hat{Y}_k \rangle$ 和二阶非中心矩 $\langle \hat{X}_k^2 \rangle$, $\langle \hat{Y}_k^2 \rangle$ 进行测量. 发送端 Alice 公开其随机发送的部分量子态的信息, Bob 基于该数据和自己的测量数据对系统的安全密钥速率进行计算. 该计算过程是一个凸优化过程, 基于通信双方的测量数据可建立如下的约束方程:

$$\begin{aligned}
&\mathrm{Tr}\left[\rho_{AB}\left(|k\rangle\langle k|_A \otimes \hat{X}\right)\right] = p_k \left\langle \hat{X}_k \right\rangle \\
&\mathrm{Tr}\left[\rho_{AB}\left(|k\rangle\langle k|_A \otimes \hat{Y}\right)\right] = p_k \left\langle \hat{Y}_k \right\rangle, \\
&\mathrm{Tr}\left[\rho_{AB}\left(|k\rangle\langle k|_A \otimes \hat{X}^2\right)\right] = p_k \left\langle \hat{X}_k^2 \right\rangle, \\
&\mathrm{Tr}\left[\rho_{AB}\left(|k\rangle\langle k|_A \otimes \hat{Y}^2\right)\right] = p_k \left\langle \hat{Y}_k^2 \right\rangle, \ \ \mathrm{Tr}[\rho_{AB}]=1, \\
&\mathrm{Tr}_B[\rho_{AB}] = \sum_{i,j=0}^{3} \sqrt{p_i p_j}\,\langle \varphi_j|\varphi_i\rangle\,|i\rangle\langle j|, \ \ \rho_{AB} \geqslant 0.
\end{aligned} \tag{10}$$

利用满足上述约束条件的联合态密度算符 ρ_{AB}, 求出相对熵的最小值 $\min\limits_{\hat{\rho}_{AB}\in\mathcal{S}} D[\mathcal{G}(\hat{\rho}_{AB})\times \mathcal{Z}(\mathcal{G}(\hat{\rho}_{AB}))]$, 进而利用 (5) 式计算出安全密钥速率. 此方案不依赖于线性信道假设, 能够有效地对抗集体攻击. 实验中只需要测量上述量子态一阶矩和二阶非中心矩的值, 无需估算额外噪声. 基于凸优化过程求解安全密钥速率时截断光子数 $N_{\rm c}=11$, 即计算过程在有限维希尔波特空间 $N_{\rm c}+1$ 中进行. 此时平移热态的平均光子数 $\bar{n}=0.564$ 远小于 $N_{\rm c}$; 当 $N_{\rm c}=11$ 时, 光子数概率为 $P(n=11)=3.4\times10^{-11}$, 已趋于 0; 当 $N_{\rm c}>11$ 时, 计算出的安全密钥速率已趋于稳定, 因此该截断光子数的选取是合理的. 详细的计算过程可参考文献 [50].

在系统运行过程中, 每个数据帧包含 10^7 个脉冲, 其中数据脉冲为 6×10^6, 平均每个态的脉冲数量为 1.5×10^6. 其中 0.5×10^6 个数据用于参数的估算, 1×10^6 个数据用于安全密钥速率的提取. CV-QKD 系统中, 在测试脉冲和数据脉冲的比例选取方面, 当测试脉冲较少时, 数据脉冲比例会提高, 但是系统的相位和散粒噪声测量精度会下降, 引入较大的测量误差, 影响系统的性能. 反之, 测试脉冲较多时会提高测量精度, 但是数据脉冲比例会下将, 同样会降低系统性能. 目前论文在测试脉冲和数据脉冲的使用方面借鉴了之前 CV-QKD 的系统使用率, 接近 50% 左右.

数据脉冲中, 在估算参数数据和提取密钥数据方面, 比例的选取一般与系统的稳定性、传输距离、方案和统计误差等因素有关, 通常由上述因素综合决定. 当系统的稳定性较好, 通常可以单次采集较长时间的数据, 数据帧长度增加, 用于估算的数据比例会下降, 即数据使用效率会提升. 由于当前该安全密钥算法中所涉及的统计误差效应尚未系统进行研究, 因此, 无法系统地进行优化. 将在今后的研究中, 展开对该算法 finite-size 效应的研究, 同时进一步提高 CV-QKD 系统的稳定性, 延长采集时间, 增加系统用于提取密钥的数据占比.

实验系统没有采用相位调制器对相位进行锁定, 需利用测试脉冲计算出相应数据的相对相位, 然后对直接测量到的量子态的正交分量值进行旋转, 得出所需正交分量值. 图 6 所示是各平移热态的一阶矩和二阶矩测量值, 其中 (a), (b), (c), (d) 分别对应 $\rho_0^{\rm th}$, $\rho_1^{\rm th}$, $\rho_2^{\rm th}$, $\rho_3^{\rm th}$. 每个子图中, 空心三角形和实心三角形分别表示正交分量 X 的一阶矩 $\langle\hat{X}_k\rangle$ 和二阶矩 $\langle\hat{X}_k^2\rangle$, 空心正方形和实心正方形分别表示正交分量 Y 的一阶矩 $\langle\hat{Y}_k\rangle$ 和二阶矩 $\langle\hat{Y}_k^2\rangle$. 一阶矩的数据需归一化到散粒噪声标准差, 二阶矩的数据需归一化到散粒噪声方差.

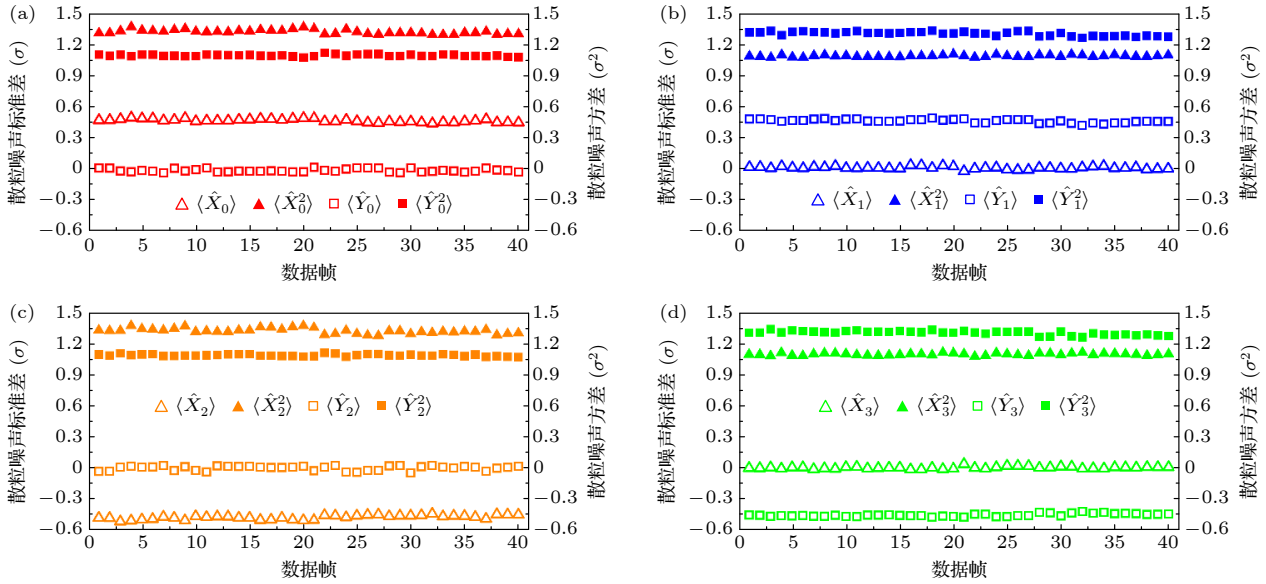

图 6 各平移热态正交分量的一阶矩和二阶矩的测量值 (a) 平移热态 $\rho_0^{\rm th}$ 测量值; (b) 平移热态 $\rho_1^{\rm th}$ 测量值; (c) 平移热态 $\rho_2^{\rm th}$ 测量值; (d) 平移热态 $\rho_3^{\rm th}$ 测量值

Fig. 6. Measurement results of the first and second moments of quadratures of the displaced thermal states: (a) Measurement results of displaced thermal state $\rho_0^{\rm th}$; (b) measurement results of displaced thermal state $\rho_1^{\rm th}$; (c) measurement results of displaced thermal state $\rho_2^{\rm th}$; (d) measurement results of displaced thermal state $\rho_3^{\rm th}$.

表 1 列出了各一阶矩和二阶矩均值、方差、最大值、最小值和期望值, 其中表中的期望值采用的等效额外噪声为 0.01. 根据测得的一阶矩和二阶矩, 可计算出如图 7(a) 所示的安全密钥速率, 无需提前估算出系统的额外噪声. 图中黑色的圆点代表每帧数据计算出的安全密钥速率, 其范围为 0.0022—0.0091 bits/pulse, 均值为 0.0061 bits/pulse. 四种平移热态的有效数据为 4×10^6 pulses/s, 因此平均安全密钥比特率为 24 kbit/s. 一帧数据中, 由于统计效应的影响, 一阶矩和二阶矩值有波动, 从而导致安全密钥速率波动. 红色实线代表信道为 25 km 时, 当系统额外噪声为 $\varepsilon=0$ 时, 可获得的最大安全密钥速率 $R_{\varepsilon=0}$, 其值为 0.0350 bits/pulse. 绿色点划线表示系统可获得的最大安全密钥速率 $R^{\max}_{\varepsilon=0.016}=0.0091$ bits/pulse, 其对应的等效额外噪声为 $\varepsilon_{\min}=0.016$; 蓝色虚线表示系统获得的最小安全密钥速率 $R^{\min}_{\varepsilon=0.103}=0.0022$ bits/pulse, 其对应的等效额外噪声为 $\varepsilon_{\max}=0.103$.

图 7(b) 是实际测量到的每个态的正交分量值在相空间中的分布, 该部分点取自最大安全密钥速率 $R^{\max}_{\varepsilon=0.016}$ 所在帧, 红色、蓝色、橙色和绿色点分别为平移热态 $\rho_0^{\rm th}$, $\rho_1^{\rm th}$, $\rho_2^{\rm th}$ 和 $\rho_3^{\rm th}$ 的正交分量值, 每个态的数据量为 7.5 k. 其中黑色圆圈为误差圆, 其半径为 $r=\sqrt{(1+0.5\eta T\varepsilon_{\min}+V_{\rm el})/2}$, $V_{\rm el}$ 为电子学噪声. 四个平移热态基本重叠在一起.

本文使用的安全密钥速率算法无需对系统的额外噪声进行计算, 为了使其与之前使用额外噪声算法的系统进行比较, 引入了等效额外噪声. 使用了实验室静态校准的通道透射率, 结合探测器的量子效率和电子学噪声等参数算出了各平移热态的一阶矩和二阶矩的期望值. 在此基础上, 将等效额外噪声引入算法中, 当计算出的安全密钥速率与实验中采用实际一阶矩和二阶矩计算出的安全密钥速率相同时, 该值为系统的等效额外噪声值.

在实验室中, 通常的额外噪声其实是 CV-QKD 系统制备, 传输和测量量子态过程中引入的各种系

表 1 正交分量一阶矩和二阶矩的相关统计量

Table 1. Statistical quantities of the first and second moments of quadratures.

	$\langle\hat{X}_0\rangle$	$\langle\hat{X}_0^2\rangle$	$\langle\hat{Y}_0\rangle$	$\langle\hat{Y}_0^2\rangle$	$\langle\hat{X}_1\rangle$	$\langle\hat{X}_1^2\rangle$	$\langle\hat{Y}_1\rangle$	$\langle\hat{Y}_1^2\rangle$
最大值	0.494	1.37	0.017	1.12	0.037	1.11	0.492	1.34
最小值	0.438	1.29	–0.035	1.07	–0.021	1.07	0.421	1.27
均值	0.467	1.32	–0.012	1.09	0.012	1.09	0.470	1.31
方差	2.35×10^{-4}	4.09×10^{-4}	2.37×10^{-4}	8.69×10^{-5}	1.58×10^{-4}	7.22×10^{-5}	2.81×10^{-4}	3.98×10^{-4}
期望值	0.470	1.31	-9.09×10^{-5}	1.08	-2.44×10^{-4}	1.08	0.4710	1.30
	$\langle\hat{X}_2\rangle$	$\langle\hat{X}_2^2\rangle$	$\langle\hat{Y}_2\rangle$	$\langle\hat{Y}_2^2\rangle$	$\langle\hat{X}_3\rangle$	$\langle\hat{X}_3^2\rangle$	$\langle\hat{Y}_3\rangle$	$\langle\hat{Y}_3^2\rangle$
最大值	–0.444	1.38	0.024	1.11	0.034	1.11	–0.425	1.34
最小值	–0.514	1.28	–0.047	1.07	–0.018	1.08	–0.478	1.26
均值	–0.477	1.33	–0.002	1.09	–0.007	1.10	–0.458	1.30
方差	3.86×10^{-4}	6.51×10^{-4}	4.74×10^{-4}	1.01×10^{-4}	1.07×10^{-4}	9.70×10^{-5}	1.90×10^{-4}	3.90×10^{-4}
期望值	–0.469	1.31	-1.56×10^{-4}	1.08	-3.11×10^{-4}	1.09	–0.472	1.30

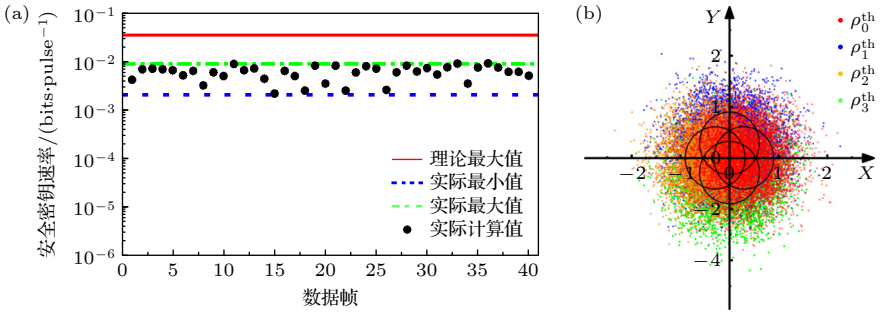

图 7 安全密钥速率和正交分量值的相空间分布图 (a) 每帧数据的安全密钥速率; (b) 平移热态正交分量值的相空间分布图

Fig. 7. Secure key rates and the phase space distribution of quadratures: (a) The secret key rate of each frame; (b) the phase space distribution of quadratures of displaced thermal states.

统噪声的统称. 为了能够进一步提高系统性能, 降低额外噪声, 提高安全密钥速率, 需在各环节提高系统的精度和稳定性, 减少各种系统噪声. 例如, 在制备环节, 提高制备量子态的调制方差的稳定性和精度. 在传输环节可以采用降低本振光功率的方法减少本振光对信号光的影响, 在接收端重新引入光放大; 同时还可采取提高偏振和相位的控制或计算精度, 量子态的测量精度等措施. 系统的稳定性整体提高后, 可通过增加数据帧的长度, 减少统计误差 (finite-size) 对安全密钥速率计算的影响; 需避免在不稳定情况下增加数据帧长度后反而使统计误差增加, 安全密钥速率降低.

5 总结与展望

本文基于四态离散调制协议, 设计并实验实现了一种基于硬件同步的 CV-QKD. 发送端 Alice 以多通道 AWG 输出波形的同步性和灵活性为基础, 结合多通道可精确延时脉冲发生器, 可以同步产生发送端所需的所有调制信号, 有效简化了发送端的时序结构, 增强了系统的实用性. 接收端 Bob 采用脉冲 LO 光场恢复接收端所需时钟源, 结合多通道可精确延时脉冲发生器, 产生了接收端所需的所有时钟信号, 可自动同步时域差拍探测器输出的电脉冲信号. 由于时域探测器的使用, 仅需采集探测器输出的脉冲信号峰值. 将精确延时的时钟信号和探测器输出的电脉冲信号同时输入采集卡中, 可实现对峰值信号的精确采集; 同时接收端的采样以延时的时钟作为触发, 可实现数据的自动对齐. 该硬件同步方法无需采用过采样技术, 同时避免了由于过采样技术带来的峰值计算和软件帧同步等方法.

安全密钥速率的计算采用加拿大滑铁卢大学 Norbert Lütokenhaus 研究组[38,50] 提出的离散调制协议安全密钥率计算方法, 精确测量了接收端所测正交分量的一阶矩和二阶矩, 并计算了相应的统计量, 以此为约束条件, 利用凸优化方法计算出系统的安全密钥速率. 同时本文采用等效额外噪声的方法估算了系统的额外噪声水平, 讨论了截断光子数选取的合理性和优化系统性能的措施和方法.

CV-QKD 系统的重复速率为 10 MHz, 传输通道为 25 km 单模光纤, 安全密钥速率为 0.0022—0.0091 bits/pulse, 等效额外噪声水平处于 0.016 至 0.103 之间, 平均安全密钥比特率为 24 kbit/s. 实验的成功运行验证了该计算方法在时域 CV-QKD 中的可行性. 实验过程中发现, 由于受到 finite-size 效应的影响, 接收端量子态的一阶矩和二阶矩存在统计起伏, 限制了系统安全密钥速率大小和安全通信距离. 下一步, 将展开 finite-size 效应对安全密钥速率影响的理论和实验研究, 并提高探测器的带宽, 基于该硬件同步方案实现更高性能的离散调制 CV-QKD.

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, Pereira J L, Razavi M, Shamsul Shaari J, Tomamichel M, Usenko V C, Vallone G, Villoresi P, Wallden P 2020 *Adv. Opt. Photonics* **12** 1012

[3] Fan-Yuan G J, Lu F L, Wang S, Yin Z Q, He D Y, Zhou Z, Teng J, Chen W, Guo G C, Han Z F 2021 *Photonics Res.* **9** 1881

[4] Liu H, Jiang C, Zhu H T, Zou M, Yu Z W, Hu X L, Xu H, Ma S, Han Z, Chen J P, Dai Y, Tang S B, Zhang W, Li H, You L, Wang Z, Hua Y, Hu H, Zhang H, Zhou F, Zhang Q, Wang X B, Chen T Y, Pan J W 2021 *Phys. Rev. Lett.* **126** 250502

[5] Grosshans F, Van Assche G, Wenger J, Brouri R, Cerf N J, Grangier P 2003 *Nature* **421** 238

[6] Xu H, Hu X L, Jiang C, Yu Z W, Wang X B 2023 *Phys. Rev. Res.* **5** 023069

[7] Jiang C, Yu Z W, Hu X L, Wang X B 2023 *Natl. Sci. Rev.* **10** 186

[8] Yin J, Li Y H, Liao S K, Yang M, Cao Y, Zhang Y, Ren J G, Cai W Q, Liu W Y, Li S L, Shu R, Huang Y M, Deng L, Li L, Zhang Q, Liu N L, Chen Y A, Lu C Y, Wang X B, Xu F H, Wang J Y, Peng C Z, Ekert A K, Pan J W 2020 *Nature* **582** 501

[9] Fang X T, Zeng P, Liu H, Zou M, Wu W J, Tang Y L, Sheng Y J, Zhang W, Li L, Li M J, Chen H A, Zhang Q, Peng C Z, Ma X, Chen T Y, Pan J W 2020 *Nat. Photonics* **14** 422

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

[11] Du Y Q, Zhu X, Hua X, Zhao Z G, Hu X, Qian Y, Xiao X, Wei K J 2023 *Chip* **2** 100039

[12] Wei K J, Li W, Tan H, Li Y, Min H, Zhang W J, Li H, You L X, Wang Z, Jiang X, Chen T Y, Liao S K, Peng C Z, Xu F H, Pan J W 2020 *Phys. Rev. X* **10** 031030

[13] Huang P, Wang T, Huang D, Zeng G H 2022 *Symmetry* **14** 568

[14] Wang H, Pan Y, Shao Y, Pi Y D, Ye T, Li Y, Zhang T, Liu J L, Yang J, Ma L, Huang W, Xu B J 2023 *Opt. Express* **31** 5577

[15] Sun S H, Xu F H 2021 *New J. Phys.* **23** 023011

[16] Sun S H 2021 *Phys. Rev. A* **104** 022423

[17] Huang P, Huang J Z, Zhang Z S, Zeng G H 2018 *Phys. Rev. A* **97** 042311

[18] Zhang Y C, Li Z Y, Yu S, Gu W Y, Peng X, Guo H 2014

Phys. Rev. A **90** 052325
[19] Qi B, Gunther H, Evans P G, Williams B P, Camacho R M, Peters N A 2020 *Phys. Rev. Appl.* **13** 054065
[20] Tian Y, Wang P, Liu J Q, Du S N, Liu W Y, Lu Z G, Wang X Y, Li Y M 2022 *Optica* **9** 492
[21] Tian Y, Zhang Y, Liu S S, Wang P, Lu Z G, Wang X Y, Li Y M 2023 *Opt. Lett.* **48** 2953
[22] Wang T, Xu Y, Zhao H, Li L, Huang P, Zeng G H 2023 *Opt. Lett.* **48** 719
[23] Wang P, Zhang Y, Lu Z G, Wang X Y, Li Y M 2023 *New J. Phys.* **25** 023019
[24] Du S N, Wang P, Liu J Q, Tian Y, Li Y M 2023 *Photonics Res.* **11** 463
[25] Chen J P, Zhang C, Liu Y, Jiang C, Zhang W, Han Z Y, Ma S Z, Hu X L, Li Y H, Liu H, Zhou F, Jiang H F, Chen T Y, Li H, You L X, Wang Z, Wang X B, Zhang Q, Pan J W 2021 *Nat. Photonics* **15** 570
[26] Wang S, Yin Z Q, He D Y, Chen W, Wang R Q, Ye P, Zhou Y, Fan-Yuan G J, Wang F X, Chen W, Zhu Y G, Morozov P V, Divochiy A V, Zhou Z, Guo G C, Han F Z 2022 *Nat. Photonics* **16** 154
[27] Liu Y, Zhang W J, Jiang C, Chen J P, Zhang C, Pan W X, Ma D, Dong H, Xiong J M, Zhang C J, Li H, Chen T Y, You L X, Wang X B, Zhang Q, Pan J W 2023 *Phys. Rev. Lett.* **130** 210801
[28] Pan Y, Wang H, Shao Y, Pi Y D, Liu B, Huang W, Xu B J 2022 *Opt. Lett.* **47** 3307
[29] Wang H, Li Y, Pi Y D, Pan Y, Shao Y, Ma L, Zhang Y C, Yang J, Zhang Tao, Huang W, Xu B J 2022 *Commun. Phys.* **5** 162
[30] Hajomer A A E, Bruynsteen C, Derkach I, Jain N, Bomhals A, Bastiaens S, Andersen U L, Yin X, Gehring T 2023 arXiv: 2305.19642v1[quant-ph]
[31] 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
[32] Zhang G, Haw J Y, Cai H, Xu F H, Assad S M, Fitzsimons J F, Zhou X, Zhang Y, Yu S, Wu J, Ser W, Kwek L C, Liu A Q 2019 *Nat. Photonics* **13** 839
[33] Wang X Y, Jia Y X, Guo X B, Liu J Q, Wang S F, Liu W Y, Sun F Y, Zou J, Li Y M 2022 *Chin. Opt. Lett.* **20** 041301
[34] Jia Y X, Wang X Y, Hu X, Hua X, Zhang Y, Guo X B, Zhang S X, Xiao X, Yu S H, Zou J, Li Y M 2023 *New J. Phys.* **25** 103030
[35] Li L, Wang T, Li X H, Huang P, Guo Y Y, Lu L J, Zhou L J, Zeng G H 2023 *Photonics Res.* **11** 504
[36] Leverrier A, Grangier P 2009 *Phys. Rev. Lett.* **102** 180504
[37] Leverrier A, Grosshans F, Grangier P 2010 *Phys. Rev. A* **81** 062343
[38] Lin J, Upadhyaya T, Lutkenhaus N 2019 *Phys. Rev. X* **9** 041064
[39] Ghorai S, Grangier P, Diamanti E, Leverrier A 2019 *Phys. Rev. X* **9** 021059
[40] Lupo C, Ouyang Y K 2022 *PRX Quantum* **3** 010341
[41] Ma H X, Huang P, Bai D Y, Wang T, Wang S Y, Bao W S, Zeng G H 2019 *Phys. Rev. A* **99** 022322
[42] 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
[43] Wang X Y, Bai Z L, Wang S F, Li Y M, Peng K C 2013 *Chin. Phys. Lett.* **30** 010305
[44] Pereira D, Almeida M, Facao M F, Pinto A N, Silva N A 2022 *Opt. Lett.* **47** 3948
[45] Kleis S, Rueckmann M, Schaeffe C G 2017 *Opt. Lett.* **42** 1588
[46] Milovancev D, Vokic N, Laudenbach F, Pacher C, Hübel H, Schrenk B 2021 *J. Lightwave Technol.* **39** 3445
[47] Li H S, Wang C, Huang P, Huang D, Wang T, Zeng G H 2016 *Opt. Express* **24** 20481
[48] Wang C, Huang P, Huang D, Lin D K, Zeng G H 2016 *Phys. Rev. A* **93** 022315
[49] Liu Y M, Wang C, Huang D, Huang P, Feng X Y, Peng J Y, Cao Z W, Zeng G H 2015 *Acta Opt. Sin.* **35** 0106006 (in Chinese) [刘友明, 汪超, 黄端, 黄鹏, 冯晓毅, 彭进业, 曹正文, 曾贵华 2015 光学学报 **35** 0106006]
[50] Lin J, Lütkenhaus N 2020 *Phys. Rev. Appl.* **14** 064030
[51] Lodewyck J, Bloch M, Garcia-Patron 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
[52] Wang X Y, Liu J Q, Li X F, Li Y M 2015 *IEEE J. Quantum Electron.* **51** 5200206
[53] Wang X Y, Liu W Y, Wang P, Li Y M 2017 *Phys. Rev. A* **95** 062330
[54] Du S N, Li Z Y, Liu W Y, Wang X Y, Li Y M 2018 *J. Opt. Soc. Am. B* **35** 481
[55] Wang X Y, Guo X B, Jia Y X, Zhang Y, Lu Z G, Liu J Q, Li Y M 2023 *J. Lightwave Technol.* **41** 5518
[56] Qi B, Lougovski P, Pooser R, Grice W, Bobrek M 2015 *Phys. Rev. X* **5** 041009
[57] Liu J Q, Wang X Y, Bai Z L, Li Y M 2016 *Acta Phys. Sin.* **65** 100303 (in Chinese) [刘建强, 王旭阳, 白增亮, 李永民 2016 物理学报 **65** 100303]

Four-state discrete modulation continuous variable quantum key distribution based on hardware synchronization*

Zhang Yun-Jie [1)2)] Wang Xu-Yang [1)3)†] Zhang Yu [1)] Wang Ning [2)]
Jia Yan-Xiang [1)] Shi Yu-Qi [1)2)] Lu Zhen-Guo [1)3)]
Zou Jun [4)] Li Yong-Min [1)3)‡]

1) (*State Key Laboratory of Quantum Optics and Quantum Optics Devices, Institute of Opto-Electronics, Shanxi University, Taiyuan* 030006, *China*)

2) (*School of Physics and Electronics Engineering, Shanxi University, Taiyuan* 030006, *China*)

3) (*Collaborative Innovation Center of Extreme Optics, Shanxi University, Taiyuan* 030006, *China*)

4) (*ZJU-Hangzhou Global Scientific and Technological Innovation Center, Zhejiang University, Hangzhou* 311215, *China*)

(Received 7 November 2023; revised manuscript received 6 December 2023)

Abstract

In the case of continuous-variable quantum key distribution (CV-QKD) systems, synchronization is a key technology that ensures that both the transmitter and receiver obtain corresponding data synchronously. By designing an ingenious time sequence for the transmitter and receiver and using the peaking value acquisition technique and time domain heterodyne detection, we experimentally realize a four-state discrete modulation CV-QKD with a repetition rate of 10 MHz, transmitting over a distance of 25 km. With well-designed time sequence of hardware, Alice and Bob can obtain corresponding data automatically without using numerous software calculation methods.

The secure key rates are calculated by using the method proposed by the Lütkenhaus group at the University of Waterloo in Canada. In the calculation, we first estimate the first and the second moment by using the measured quadratures of displaced thermal states, followed by calculating the secret key rate by using the convex optimization method through the reconstruction of the moments. There is no need to assume a linear quantum transmission channel to estimate the excess noise. Finally, secure key rates of 0.0022—0.0091 bit/pulse are achieved, and the excess noise is between 0.016 and 0.103.

In this study, first, we introduce the prepare-and-measure scheme and the entanglement-based scheme of the four-state discrete modulation protocol. The Wigner images of the four coherent states on Alice's side, and four displaced thermal states on Bob's side are presented. Second, the design of hardware synchronization time series is introduced comprehensively. Third, the CV-QKD experiment setup is introduced and the time sequence is verified. Finally, the calculation method of secure key rate using the first and the second moment of quadrature is explained in detail. The phase space distribution of quadratures is also presented. The secret key rate ranges between 0.0022 and 0.0091 bits/pulse, and the equivalent excess noise are between 0.016 and 0.103.

* Project supported by the Natural Science Foundation of Shanxi Province, China (Grant No. 202103021224010), the Shanxi Provincial Foundation for Returned Scholars, China (Grant No. 2022-016), the National Natural Science Foundation of China (Grant Nos. 62175138, 62205188, 11904219), the Open Fund of State Key Laboratory of Quantum Optics and Quantum Optics Devices, China (Grant No. KF202006), and the "1331Project" for Key Subject Construction of Shanxi Province, China.

† Corresponding author. E-mail: wangxuyang@sxu.edu.cn

‡ Corresponding author. E-mail: yongmin@sxu.edu.cn

The average secret key bit rate is 24 kbit/s. During the experiment, the first and the second moment of the quantum state at the receiver end are found to fluctuate owing to the finite-size effect. This effect reduces the value of the secure key rate and limits the transmission distance of the CV-QKD system.

In conclusion, four-state discrete modulation CV-QKD based on hardware synchronization is designed and demonstrated. The proposed hardware synchronization method can effectively reduce the cost, size, and power consumption. In the future, the finite-size effect will be investigated theoretically and experimentally to improve the performance of system.

Keywords: continuous variable quantum key distribution, hardware synchronization, four-state discrete modulation, time domain heterodyne detection

PACS: 03.67.Hk, 03.67.Dd **DOI:** 10.7498/aps.73.20231769

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

基于硬件同步的四态离散调制连续变量量子密钥分发

张云杰 王旭阳 张瑜 王宁 贾雁翔 史玉琪 卢振国 邹俊 李永民

Four-state discrete modulation continuous variable quantum key distribution based on hardware synchronization

Zhang Yun-Jie Wang Xu-Yang Zhang Yu Wang Ning Jia Yan-Xiang Shi Yu-Qi Lu Zhen-Guo Zou Jun Li Yong-Min

引用信息 Citation: Acta Physica Sinica, 73, 060302 (2024) DOI: 10.7498/aps.73.20231769
在线阅读 View online: https://doi.org/10.7498/aps.73.20231769
当期内容 View table of contents: http://wulixb.iphy.ac.cn