

连续变量量子密钥分发系统中动态偏振控制研究*

张光伟 白建东 颌琦 靳晶晶 张永梅 刘文元†

(中北大学半导体与物理学院物理系, 太原 030051)

(2023 年 11 月 30 日收到; 2023 年 12 月 14 日收到修改稿)

连续变量量子密钥分发系统中, 本地光场和信号光场采用时分复用, 偏振复用方式通过长距离单模光纤传输. 外界复杂环境会使单模光纤产生双折射效应, 导致本地光场和信号光场的偏振态漂移, 严重影响接收端平衡零拍探测结果. 因此, 高效动态偏振控制单元是推动系统外场实用化进程的关键技术. 本文理论上证明了系统接收端仅考虑任意偏振消光比输出时, 偏振控制单元只需两个控制自由度即可. 在此基础上将贝叶斯参数估计方法有效融入混沌-猴群算法, 同时在现场可编程逻辑门阵列硬件上实现控制算法, 结合积分型光场探测器建立动态偏振控制单元, 仿真和实验结果表明单次偏振控制静态消光比达到 30 dB 以上的平均周期为 400 μ s. 为了应对偏振态连续变化情况, 将动态偏振控制单元集成到连续变量量子密钥分发系统, 实验测试了偏振态扰动速率在 0—2 krad/s 范围内系统仍然能够正常运转.

关键词: 连续变量量子密钥分发, 贝叶斯参数估计方法, 猴群算法, 动态偏振控制器**PACS:** 03.67.Hk, 02.50.Tt, 07.05.Kf, 42.79.-e**DOI:** 10.7498/aps.73.20231890

1 引言

量子保密通信是基于量子物理原理而非数学计算的复杂性, 结合“一次一密”, 理论上可以使通信双方共享无条件安全性密钥. 面对量子计算, Shor 算法等对现代密码体系安全性造成的威胁, 建立绝对安全的量子保密通信系统在国防、军事和金融领域等都具有重要意义. 量子保密通信技术手段主要有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)^[1-3]. 在 CV-QKD 系统中, 相干态连续变量量子密钥分发协议 (coherent state quantum key distribution protocol), 凭借光源易制备, 中短距离上成码率高, 与现有的光纤通信网络兼容性好等优点, 是最接近实际应用

的量子保密通信方式之一^[4-17]. 在外场复杂环境下的长距离 CV-QKD 系统中, 光场信号传输介质有埋地光纤、架空光纤等, 外界环境的剧烈变化会使单模光纤产生双折射效应, 即理想光纤的圆对称性被打破, 原来各向同性的光纤变为各向异性, x 偏振方向的折射率与 y 偏振方向的折射率不同, 使得光纤中本地光场和信号光场偏振态发生变化, 影响接收端平衡零拍探测结果, 导致系统无法正常运转^[18]. 为了进一步推动 CV-QKD 系统从实验室环境走向实际外场应用, 引入光纤链路中的动态偏振控制技术, 同时此技术也被广泛应用于光通信领域.

光纤链路中偏振态实时跟踪和控制单元, 利用动态偏振控制器响应速度快, 无迟滞效应, 插入损耗小的特点, 基于现场可编程逻辑门阵列 (field-programmable gate array, FPGA) 硬件, 结合梯度算法 (gradient algorithm, GA)^[19,20]、多步长模拟退火算法 (simulated annealing algorithm, SA)^[21,22]、

* 国家自然科学基金 (批准号: 12104419, 12104417, 12104418) 和山西省基础研究计划 (批准号: 20210302124689, 20210302124161, 20210302124025) 资助的课题.

† 通信作者. E-mail: liuweny@nuc.edu.cn

遗传算法 (genetic algorithm, GA)^[23]、粒子群算法 (particle swarm optimization, PSO)^[24] 以及差分进化 (differential evolution, DE) 和 GA 相结合算法^[25] 等, 加入外围电路, 同时考虑庞加莱球盲区问题^[26], 实现实时跟踪和控制偏振态. 电控挤压型偏振控制器的响应速度一般在几十微秒, 为了提高反馈效率, 可以采用铌酸锂型的偏振控制器, 响应速度在百纳秒, 但其插入损耗高于电控挤压型偏振控制器, 跟踪和控制偏振态变化速率的快慢, 取决于偏振控制器件的响应速度和算法收敛性. DV-QKD 系统中, 通常采用时分复用和波长复用的方法, 通过强参考光作为反馈信号实现实时偏振控制^[27-29], 利用量子密钥分发后处理中冗余密钥作为反馈控制偏振态^[30], 其基于双区域计数的优点, 缩短偏振态搜索时间, 提高搜索效率^[31,32], 利用自动生成和确定偏振态验证了在极端条件下长时间稳定运转的可行性^[33,34]. 本地本振 CV-QKD 实验系统中, 通过数据后处理补偿偏振态的变化^[35]. 近年来, 随着人工智能与量子信息深度融合, 引入了贝叶斯参数估计方法^[36-42]、卡尔曼滤波器方法^[43-45]、量子启发式方法^[46,47] 以及模拟神经网络结构和极大似然法^[48] 等对数据进行区域块传输, 从而提高量子信息传输的效率和容量^[49]. 针对通信系统中多用户问题, 利用机器学习迭代算法提高收敛速率^[50]. 人工智能和机器学习等新方法的出现, 为突破高斯调制相干态 CV-QKD 系统中动态偏振控制的关键技术提供了新的解决思路.

为了应对外场复杂环境下偏振态实时变化对于 CV-QKD 系统的影响^[51-53], 本文理论上证明了系统仅考虑偏振消光比输出时, 只需两个偏振控制自由度即可. 通过建立传输矩阵, 以偏振消光比大于 30 dB 作为目标偏振态, 在混沌-猴群算法^[54,55] 基础上有效融入贝叶斯参数估计方法^[56-58], 对比了高斯分布、泊松分布、指数分布等作为贝叶斯先验分布对偏振控制效果的影响机制; 对比了偏振控制自由度个数对偏振控制的效果; 基于 FPGA 硬件实现偏振控制算法, 结合积分型探测器和数据采集系统建立动态偏振控制单元, 实验测试了脉冲光情况下静态偏振控制效果. 针对实际偏振态连续变化情况, 实验测试了不同偏振扰动速率情况下 CV-QKD 系统运转情况.

论文的第 2 部分详细地介绍了偏振控制原理, 证明了接收端仅考虑光场任意偏振消光比输出时,

偏振控制单元只需两个自由度即可. 第 3 部分详细介绍了混沌-猴群算法有效融入贝叶斯参数估计方法的流程, 理论仿真了不同先验分布和控制自由度对于偏振控制效果的影响机制. 第 4 部分基于 FPGA 硬件实验测试了智能控制算法对于偏振控制的性能; 同时将偏振控制单元集成到 CV-QKD 系统, 在扰偏速率 0—2 krad/s 范围内测试了系统稳定性. 第 5 部分是总结.

2 基本原理

偏振态可以用两个变量 (α, δ) 的琼斯矢量表示, 其中 α 为偏振态振幅比角, δ 为相位差角. 偏振态也可以用两个变量 $(2\chi, 2\varepsilon)$ 的斯托克斯矢量表示, 2χ 为纬度角, 2ε 为经度角, 即偏振态用庞加莱球表示. 琼斯矢量和斯托克斯矢量之间的关系满足^[59]:

$$\begin{aligned}\tan(2\varepsilon) &= \tan(2\alpha) \cos \delta, \\ \cos(2\chi) &= \sin(2\alpha) \sin \delta.\end{aligned}\quad (1)$$

偏振控制器可以通过方位角或延迟量改变输入偏振态, 主要分为方位角固定, 调节延迟量和延迟量固定, 调节方位角两大类. 电控偏振控制器一般是方位角固定, 延迟量可调的偏振控制器. 目前商用的 Pola RITE III 型偏振控制器由 4 个挤压器组成, 即 4 个控制自由度. 如图 1 所示方位角依次按照 $0^\circ, 45^\circ, 0^\circ, 45^\circ$ 排列, 通过所加电压驱动压电陶瓷挤压光纤改变相应的延迟量, 实现任意目标偏振态输出. 理论上偏振控制器至少需要 3 个自由度组合方可实现庞加莱球上任意入射光场偏振态到任意目标偏振态的输出^[60].

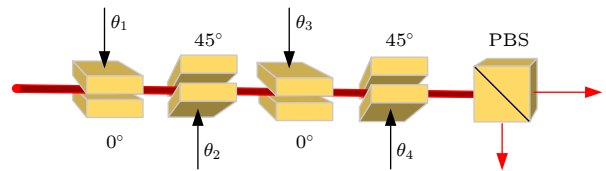


图 1 挤压型电控偏振控制器

Fig. 1. Extrusion type electronically polarization controller.

任意入射偏振态可利用斯托克斯矢量表示^[61]:

$$\mathbf{S}_{\text{in}} = \begin{bmatrix} 1 \\ \sin 2\chi \cos 2\varepsilon \\ \sin 2\chi \sin 2\varepsilon \\ \cos 2\chi \end{bmatrix}. \quad (2)$$

由于连续变量量子密钥分发系统接收端只考虑偏振消光比这一指标, 无需使得任意入射偏振态变换到任意偏振态, 考虑庞加莱球上的坐标 $x = \sin 2\chi \cos 2\varepsilon$, 由 (1) 式可得 $x = \frac{1 - \tan^2 \alpha}{1 + \tan^2 \alpha}$, 其中 $\tan^2 \alpha$ 即为偏振消光比. 由以上推导可知, 具有相同消光比的偏振态是以 x 为圆心, $\cos 2\chi$ 为半径

的圆环分布.

两个互成 45° 级联挤压器改变延迟量分别为 θ_1, θ_2 , 其中方位角为 0° 的挤压器对应传输矩阵 T_1 , 方位角为 45° 的挤压器对应传输矩阵 T_2 , 入射偏振态 S_{in} 经过两个自由度的偏振控制器后, 输出偏振态矩阵形式 S_{out} :

$$S_{out} = \begin{bmatrix} 1 \\ -\cos \theta_1 \cos 2\chi \sin \theta_2 + \sin 2\chi (\cos \theta_2 \cos 2\varepsilon + \sin \theta_1 \sin \theta_2 \sin 2\varepsilon) \\ \cos 2\chi \sin \theta_1 + \cos \theta_1 \sin 2\chi \sin 2\varepsilon \\ \cos \theta_1 \cos \theta_2 \cos 2\chi + \sin 2\chi (\cos 2\varepsilon \sin \theta_2 - \cos \theta_2 \sin \theta_1 \sin 2\varepsilon) \end{bmatrix}. \quad (3)$$

对应的 $x = -\cos \theta_1 \cos 2\chi \sin \theta_2 + \sin 2\chi (\cos \theta_2 \cos 2\varepsilon + \sin \theta_1 \sin \theta_2 \sin 2\varepsilon)$, 理论上通过调整延迟量 θ_1, θ_2 得到任意 x , 即可得到任意偏振消光比覆盖.

如图 2(a) 所示, 设输入偏振态 $\varepsilon = 0.32\pi$, $\chi = 0.32\pi$, 方位角为 0° 挤压器相位延迟量 θ_1 在 $(0, 2\pi)$

范围内以 $2\pi/9$ 的间隔固定, 方位角为 45° 挤压器延迟量 θ_2 在 $(0, 2\pi)$ 范围变化, 形成多组同心圆, 但此时并不能遍历 x 轴, 只有当输入偏振态是特殊点如“南北极点”时, 调节 θ_2 可实现 x 轴全覆盖. 如图 2(b) 所示, 当两个挤压器同时在 $(0, 2\pi)$ 范围变化, 同心圆环绕 y 轴旋转, 此时虽然没有完成偏振态在庞加莱球上全覆盖, 但实现了 x 轴全覆盖, 所以在仅考虑恢复偏振态消光比的系统中, 两个自由度即可满足要求.

3 混沌-猴群算法与贝叶斯参数估计方法

动态偏振控制单元包括外围电路和智能控制算法, 本文基于混沌-猴群算法 (chaotic monkey algorithm, CMA), 利用其全局搜索能力强, 并行化搜索效率快的优点, 同时参考贝叶斯方法通过对少量数据进行序列分析和实时更新的优点, 有效融入贝叶斯参数估计方法, 贝叶斯先验、后验分布是通过消光比构建分布算子模型, 定义偏振消光比遵循的统计分布, 即先验分布, 根据测量得到的数据, 不断对先验假设进行更新和修正, 最后形成后验分布. 通过智能算法控制偏振过程中, 持续产生新的消光比数据, 不断优化先验和后验分布. 同时拓展多自由度级联偏振控制条件提高偏振控制效率. 理论上仿真对比了高斯分布、泊松分布、指数分布作为先验, 后验分布对偏振控制算法效果的影响机制, 基于贝叶斯参数估计方法的混沌-猴群算法具体步骤如图 3 所示.

1) 初始化. 设种群规模 $M = 1$, 偏振控制器的挤压器取值为的一组可行解, 对应一只猴子; 种群

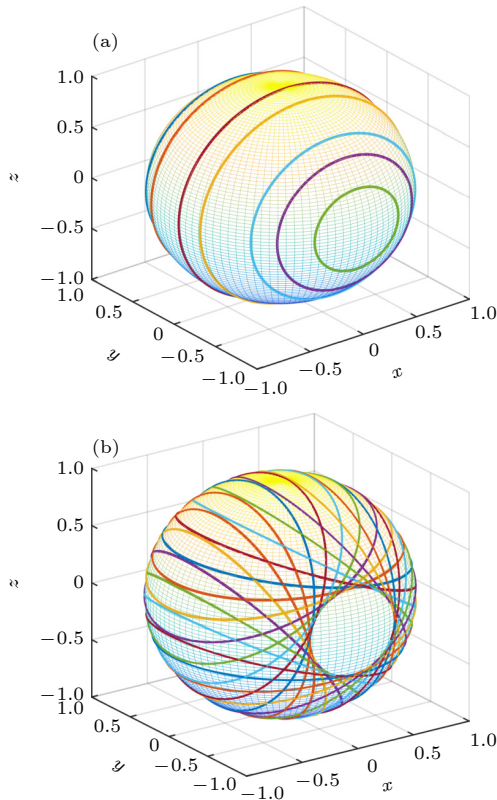


图 2 调节挤压器延迟量偏振态的变化轨迹 (a) 固定 0° 挤压器, 调节 45° 挤压器相位延迟量; (b) 调节 0° 和 45° 挤压器相位延迟量

Fig. 2. Change trajectory of state of polarization when adjusting phase retardation of extruder: (a) Fixing 0° extruder, adjusting phase retardation of the 45° extruder; (b) adjusting phase retardation of the 0° and 45° extruders.

维数为 D , 对应偏振控制器的自由度; 同时引入 Logistic 混沌映射 [62]:

$$H(k+1) = 4H(k) \times (1 - H(k)), \quad (4)$$

其中, $H(k)$ 表示 $(0, 1)$ 之间的混沌随机变量, 初始值设置为 $H(k) = 0.01$. 算法中第 i 只猴子在第 D 维中的分量 θ_{iD} 可以表示为

$$\theta_{iD} = (\theta_{\max} - \theta_{\min}) \times H(k+1) + \theta_{\min}, \quad (5)$$

其中 $i = 1, 2, \dots, M$, $\theta_{iD} \in [\theta_{\min}, \theta_{\max}]$. θ_{\min} 和 θ_{\max} 是解空间的下界和上界, 范围在 $(0, 2\pi)$.

2) 爬过程. 以输出偏振态消光比作为目标函数值, 偏振控制自由度以步长 α 爬行, 寻找目标偏振态消光比为 30 dB 的位置. 构建递减步长:

$$\alpha^{k+1} = \beta \alpha^k, \quad (6)$$

$k = 1$ 为爬次数, $\beta = 0.7$ 为递减因子, 初始步长 $\alpha = 37\pi/70$.

3) 望过程. 偏振控制自由度经过“爬”过程后, 进行望过程, 目的是使当前偏振态消光比跳出局部最优值. 构建递增视野长度:

$$b^{G+1} = \gamma b^G, \quad (7)$$

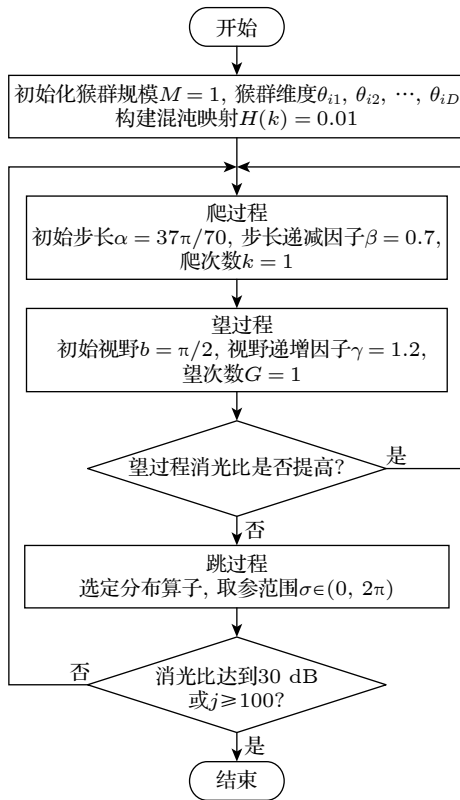


图 3 贝叶斯-混沌猴群算法流程图

Fig. 3. Program flow diagram of Bayesian-chaotic monkey algorithm.

其中 b 表示望的范围, $G = 1$ 为望次数, 初始望范围 $b = \pi/2$; γ 为递增因子, 初始值 $\gamma = 1.2$. 利用“爬”和“望”过程得到偏振控制自由度对应值 $\theta_{1D}, \theta_{2D}, \dots, \theta_{MD}$, 同时通过对应当前消光比集合构建先验分布.

4) 跳过程: 针对上述分布中偏振态消光比的最大值, 在其对应参数 θ_{iD} 附近 $\sigma \in (0, 2\pi)$ 范围内随机取值, 作为新的参数值 θ'_{iD} , 判断其消光比是否增大, 取代原分布中最小的消光比值, 构建后验分布, 重新进行“爬”、“望”、“跳”等步骤, 程序中设置最大“跳”次数 $j = 100$, 目标函数值达到 30 dB 或 $j = 100$ 程序结束.

偏振控制过程中, 以偏振态消光比达到 30 dB 作为目标偏振态, 分别以高斯分布、指数分布、泊松分布、二项分布、Beta 分布和均匀分布作为混沌猴群算法的先验和后验分布; 依次对二、四、六、八、十和十二自由度级联控制任意入射偏振态进行仿真, 相应的偏振控制结果如图 4 所示.

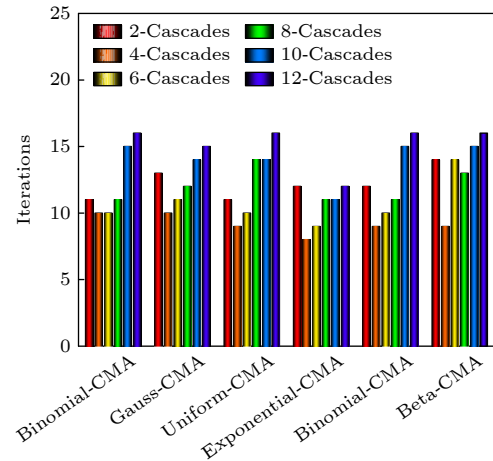


图 4 先验分布类型和偏振自由度达到目标偏振态所需迭代次数

Fig. 4. Average number of iterations to achieve target state of polarization based on prior distribution and degrees of freedom of polarization.

对于任意入射偏振态, 通过对比不同先验分布对于算法控制目标偏振态的效果. 图 4 结果表明同一种先验分布下, 不同级联自由度个数对于偏振控制效果不同, 不同的先验分布对于偏振控制效果影响不同. 同时也表明先验分布为指数分布的混沌猴群算法能够在最少的迭代次数内实现目标偏振态控制; 同一种先验分布中, 4 个自由度级联的偏振控制器对于目标偏振态控制效果最优.

综上, 实验中选择以先验分布为指数分布的四级联偏振控制算法作为动态偏振控制单元核心算法.

4 偏振控制实验

连续变量量子密钥分发系统中, 发送端 Alice 的本地光场和信号光场相互垂直进入偏振合束器, 采用时分复用, 偏振复用的技术使本地光场和信号光场在同一根长距离光纤中传输到接收端 Bob. 实际外场环境的剧烈变化会使单模光纤产生双折射效应, 使得本地光场和信号光场之间发生串扰, 严重影响接收端对信号光场正交分量的测量. 因此光场进入接收端 Bob 需要进行偏振解复用, 动态偏振控制单元偏振解复用的效果直接影响连续变量量子密钥分发系统性能.

图 5 所示为动态偏振控制单元示意图. 动态偏振控制单元主要有 3 部分组成: 基于电荷放大器的积分型光信号探测器、挤压型电控偏振控制器、FPGA 硬件. 其中, 积分型光信号探测器是时域脉冲平衡零拍探测器的一臂, 将接收到的脉冲光场信号实时转换为输出电脉冲的峰值电压, 并作为反馈信号输入动态偏振控制单元. 挤压型电控偏振控制器采用 General Photonics 公司生产的 PCD-M02 偏振控制模块, 信号的偏振态可通过 0—5 V 的模拟信号或者 12 位 TTL 数字信号控制, 作为偏振控制器, 可以控制任意入射偏振态输出任意目标偏振态, 响应时间为 30 μs ; 作为扰偏器, 可以输出随机变化的偏振态. 实验过程中利用 FPGA 数字信号口驱动偏振控制器, 实验中采用 Xilinx Artix-7FPGA 硬件, 利用其集成度高, 灵活性强, 可重复编程特点作为控制核心. 接收端 Bob 时钟恢复模块得到的系统同步时钟作为触发信号, 通过 FPGA 控制高速 A/D 采集探测器峰值电压作为反馈信号. 同时在 FPGA 硬件上运行智能偏振控制算法, 计算得到的控制电压通过数字信号驱动偏振控制器, 实现对偏振态的实时控制.

高速偏振控制过程中, 通过采集多点求平均的方法, 提高测量系统的信噪比, 降低探测器电子学噪声的影响. 实验过程中用于求平均的电压值越多, 测量系统的信噪比越高, 但是采集数据所用时间越长^[18,63]. 综合考虑, 选择采集 25 个峰值电压点求平均作为实时反馈信号, 测量系统信噪比为 38 dB.

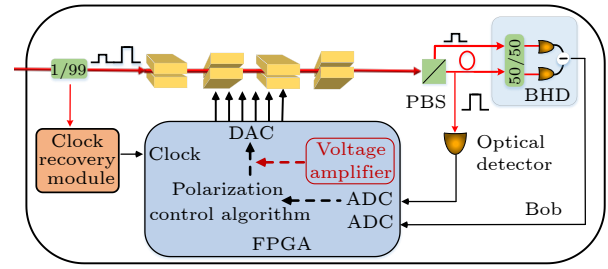


图 5 动态偏振控制单元示意图

Fig. 5. Schematic diagram of the dynamic polarization control unit.

4.1 基于 FPGA 的动态偏振控制单元运行结果

实验中对动态偏振控制单元中每次循环迭代各部分时间分布进行分析, 每次循环迭代控制偏振的过程中, 由 FPGA 硬件控制 A/D 采集数据时间 (10 μs) 占 20%, 动态偏振控制器响应 (30 μs) 时间占 60%, FPGA 硬件程序计算时间 (10 μs) 占 20%, 每次循环迭代需要 50 μs .

单次偏振随机扰动情况下, 以接收端 Bob 偏振消光比大于 30 dB 作为目标偏振态, 实验测试了以指数分布为先验分布, 4 个自由度级联的混沌-猴群算法对于偏振控制性能的影响, 如图 6 所示任意入射偏振态情况下, 多次测量输出静态偏振态消光比达到 30 dB.

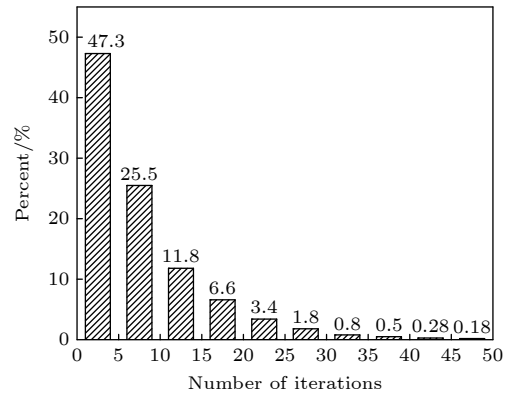


图 6 控制目标偏振态迭代次数统计分布

Fig. 6. Statistical distribution of iterations to achieve target of state of polarization.

图 6 表明, 47.3% 任意入射偏振态可以在迭代 5 次以内达到目标偏振态, 72.8% 的任意入射偏振态在迭代 10 次内达到目标偏振态. 经过多次测试, 任意入射偏振态达到目标偏振态平均迭代 8 次, 对应平均偏振控制周期 400 μs .

实验中针对单次偏振控制过程, 系统实时偏振

消光比和偏振控制时间的关系如图 7 所示. 可以看出, 随着控制时间增长, 输出偏振态消光比逐渐升高, 但并非一个线性过程; 当迭代次数大约到 9 次时, 当前偏振态消光比达到 30 dB, 迭代次数继续增加, 偏振消光比在 30 dB 附近波动. 实验中实时监测偏振消光比变化, 当偏振消光比达到 30 dB, 偏振控制程序停止运转, 寻优过程的当前解即为最优解.

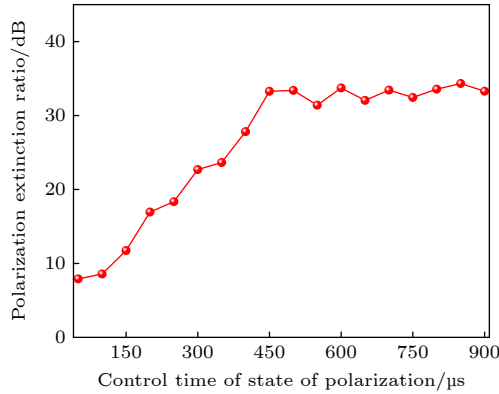


图 7 单次偏振控制过程中消光比与时间关系

Fig. 7. Observed polarization extinction ratio versus the time for a typical single random polarization control process.

4.2 动态偏振控制单元与连续变量量子密钥分发系统集成化

在 CV-QKD 系统中, 发送端 Alice 光源为波长 1550 nm, 线宽 15 kHz, 输出功率 20 mW 的连续光源, 经过振幅调制器调制为脉宽 100 ns, 重复速率为 500 kHz 的高消光比脉冲光, 经过 99/1 分束器分成强的本地光场和弱的信号光场, 信号光场经过振幅和相位调制器实现高斯调制, 本地光场和信号光场相互垂直进入偏振合束器, 并通过同一根单模光纤传输到接收端 Bob, 单模光纤衰减器设置为固定衰减 10 dB. 接收端 Bob 首先经过一个动态偏振控制器作为扰偏器用来模拟由于外界复杂环境造成的偏振扰动. 然后, 动态偏振控制单元对光场进行偏振解复用, 使得信号光场和本地光场分开, 进行光场相对相位锁定, 完成平衡零拍探测. 根据测量结果, 发送端 Alice 和接收端 Bob 之间经过认证的经典信道评估系统参数和数据后处理, 最终共享一组无条件安全密钥.

实验中将基于 FPGA 硬件的动态偏振单元集成到 CV-QKD 系统中, 实验测试了在不同偏振扰

动速率情况下, 系统的额外噪声和通道损耗等关键参数. 在此状态下, 发送端 Alice 的调制方差 $V_A = 5.4$, 探测器电子学噪声 $v_{\text{ele}} = 0.033$, 接收端 Bob 的探测效率 $\eta = 0.68$, 数据协调效率 $\beta = 0.95$. 实验室环境下, 分别测试了扰偏速率为 500, 1000, 1500 和 2000 rad/s 情况下, 动态偏振控制单元进行偏振控制, 系统长时间运转时的关键参数. 测试结果如图 8 所示.

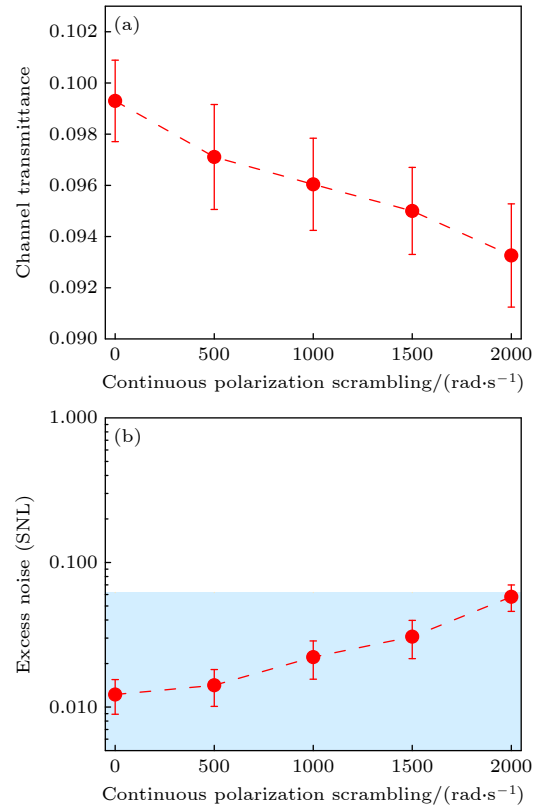


图 8 连续偏振扰动速率对系统关键参数影响 (a) 通道传输效率; (b) 额外噪声

Fig. 8. Influence of continuous polarization scrambling on key parameters of the system: (a) Channel transmittance; (b) excess noise.

图 8(b) 阴影部分为考虑有限码长效应情况下可以提取安全密钥的区域. 从图 8 可以看出, 没有主动加入偏振扰动情况下, 即当前实验室环境下偏振变化情况, 由于实验室环境相对比较稳定, 偏振态变化缓慢, 系统额外噪声维持在一个较低水平; 系统评估的通道损耗为 0.099; 通过扰偏器主动加入偏振态变化, 模拟实际外界环境的偏振态变化情况. 系统的动态偏振控制单元检测到偏振态变化开始运转控制当前偏振态到目标偏振态, 随着扰偏速率逐渐增大, 实验测试结果如图 8 所示, 系统额外

噪声明显增大, 通道传输效率评估下降, 原因是偏振态变化不可避免会影响到本地光场和信号光场相对相位锁定效果, 从而引入系统额外噪声; 当扰偏速率为 2 krad/s 时, 额外噪声已经有部分超出阈值范围, 系统不能提取安全密钥, 动态偏振控制单元跟踪和控制偏振态能力已经达到上限, 继续增大扰偏速率, 系统不能够正常运转。

5 结 论

本文基于外场复杂环境下偏振态变化实际情况, 在 CV-QKD 系统基础上构建了偏振控制单元理论模型. 理论上证明了仅考虑接收端偏振消光比情况下, 偏振控制单元只需控制 2 个自由度即可. 在混沌-猴群算法基础上有效融入了贝叶斯参数估计方法, 仿真结果表明以指数分布为先验分布, 同时以 4 个自由度为偏振控制核心的偏振控制单元控制效果最佳. 基于 FPGA 硬件实验上测试了动态偏振控制单元对于任意入射偏振态的控制效果, 实验结果表明控制任意入射偏振态到目标偏振态的平均周期为 400 μ s. 考虑到实际偏振态连续变化情况, 实验测试了不同偏振扰动速率情况下 CV-QKD 系统的关键参数, 实验结果表明基于贝叶斯-混沌猴群算法的动态偏振控制单元相较于遗传算法, 在同等外部激励条件下偏振控制效率提高 3 倍, 集成了动态偏振控制单元的 CV-QKD 系统在偏振扰动速率为 0—2 krad/s 范围可以正常运转. 为了进一步缩短控制目标偏振态的平均周期, 可以将挤压型动态偏振控制器更换为响应速率为百纳秒级的铌酸锂晶体偏振控制器; 进一步优化算法, 根据不同的入射偏振态消光比, 自适应设置初始步长和相关控制参数, 缩短程序运转时间; 加快探测端 A/D 模块采样速率缩短数据采集时间; 通过以上方法可以缩短平均控制周期, 进而提高系统抗偏振扰动的速率以适应更复杂外界环境。

参考文献

- [1] 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
- [2] Ren S Y, Wang Y, Su X L 2022 *Sci. China Inform. Sci.* **65** 200502
- [3] Ma L, Yang J, Zhang T, Shao Y, Liu J L, Luo Y J, Wang H, Huang W, Fan F, Zhou C, Zhang L L, Zhang S, Zhang Y C, Li Y, Xu B J 2023 *Sci. China Inform. Sci.* **66** 180507
- [4] Gisin N, Ribordy G, Tittel W, Zbinden H 2002 *Rev. Mod.*

- Phys.* **74** 145
- [5] Grosshans F, Grangier P 2002 *Phys. Rev. Lett.* **88** 057902
- [6] Grosshans F, Assche G V, Wenger J, Brouri R, Cerf N J, Grangier P 2003 *Nature* **421** 238
- [7] Lodewyck J, Bloch M, García-Patrón R, Fossier S, Karpov E, Diamanti E, Debuisschert T, Cerf N J, Tualle-Brouri R, McLaughlin S W, Grangier P 2007 *Phys. Rev. A* **76** 042305
- [8] Jouguet P, Kunz-Jacques S, Leverrier A, Grangier P, Diamanti E 2013 *Nat. Photonics* **7** 378
- [9] Weedbrook C, Pirandola S, García-Patrón R, Cerf N J, Ralph T C, Shapiro J H, Lloyd S 2012 *Rev. Mod. Phys.* **84** 621
- [10] 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, 白增量, 李永民 2016 物理学报 **65** 100303]
- [11] Huang D, Huang P, Li H S, Wang T, Zhou Y M, Zeng G H 2016 *Opt. Lett.* **41** 3511
- [12] Li Y M, Wang X Y, Bai Z L, Liu W Y, Yang S S, Peng K C 2017 *Chin. Phys. B* **26** 040303
- [13] Zhang Y C, Li Z Y, Chen Z Y, Weedbrook C, Zhao Y J, Wang X Y, Huang Y D, Xu C C, Zhang X X, Wang Z Y, Li M, Zhang X Y, Zheng Z Y, Chu B J, Gao X Y, Meng N, Cai W W, Wang Z, Wang G, Yu S, Guo H 2019 *Quantum Sci. Technol.* **4** 035006
- [14] Xu F H, Ma X F, Zhang Q, Lo H K, Pan J W 2020 *Rev. Mod. Phys.* **92** 025002
- [15] Zhong H, Ye W, Wu X D, Guo Y 2021 *Acta Phys. Sin.* **70** 020301 (in Chinese) [钟海, 叶炜, 吴晓东, 郭迎 2021 物理学报 **70** 020301]
- [16] Liu J L, Yang J, Zhang T, Fan F, Huang W, Xu B J 2021 *Acta Phys. Sin.* **70** 240303 (in Chinese) [刘金璐, 杨杰, 张涛, 樊矾, 黄伟, 徐兵杰 2021 物理学报 **70** 240303]
- [17] Liao Q, Liu H J, Wang Z, Zhu L J 2023 *Acta Phys. Sin.* **72** 040301 (in Chinese) [廖毅, 柳海杰, 王铮, 朱凌瑾 2023 物理学报 **72** 040301]
- [18] Liu W Y, Cao Y X, Wang X Y, Li Y M 2020 *Phys. Rev. A* **102** 032625
- [19] Noé R, Heidrich H, Hoffmann D 1988 *Opt. Lett.* **13** 527
- [20] Koch B, Hidayat A, Zhang H B, Mirvoda V, Lichtinger M, Sandel D, Noé R 2008 *IEEE Photon. Technol. Lett.* **20** 961
- [21] Li W W, Zhang X M, Chen K S, Zou Y Y 2005 *Acta Photon. Sin.* **34** 820 (in Chinese) [李伟文, 章献民, 陈抗生, 邹英寅 2005 光子学报 **34** 820]
- [22] Liu W Y, Cao L, Chen X W, Zhang L, Li Y, Cao Y, Ren J G, Cai W Q, Liao S K, Peng C Z 2016 *J. Infrared Millim. Waves* **35** 210 (in Chinese) [刘尉悦, 曹蕾, 陈厦微, 张亮, 李扬, 曹原, 任继刚, 蔡文奇, 廖胜凯, 彭承志 2016 红外与毫米波学报 **35** 210]
- [23] Li W W, Jin X F, Zhang X M, Chen K S 2006 *J. Zhejiang Univ. (Eng. Sci.)* **40** 443 (in Chinese) [李伟文, 金晓峰, 章献民, 陈抗生 2006 浙江大学学报:工学版 **40** 443]
- [24] Zhu J J, Zhang X G, Duan G Y, Wang Q G 2006 *Semi. Photon. Tech.* **12** 217
- [25] You Y, Qi Y F, Shen H, Zou X X, He B, Zhou J 2020 *Acta Opt. Sin.* **40** 2314002 (in Chinese) [尤阳, 漆云凤, 沈辉, 邹星星, 何兵, 周军 2020 光学学报 **40** 2314002]
- [26] Zhang Q Y, Zhu Y, Su Y, Zhou H, Jing J S 2013 *Acta Opt. Sin.* **33** 0506001 (in Chinese) [张启业, 朱勇, 苏洋, 周华, 经继松 2013 光学学报 **33** 0506001]
- [27] Xavier G B, Walenta N, Faria G V D, Temporão G P, Gisin N, Zbinden H, Weid J P V D 2009 *New J. Phys.* **11** 045015
- [28] Chen J, Wu G, Xu L, Gu X, Wu E, Zeng H 2009 *New J. Phys.* **11** 065004
- [29] Li D D, Gao S, Li G C, Xue L, Wang L W, Lu C B, Xiang Y,

- Zhao Z Y, Yan L C, Chen Z Y, Yu G, Liu J H 2018 *Opt. Express* **26** 22793
- [30] Ding Y Y, Chen H, Wang S, He D Y, Yin Z Q, Chen W, Zhou Z, Guo G C, Han Z F 2017 *Opt. Express* **25** 27923
- [31] Cao R L, Peng Q X, Wang J D, Chen Y J, Huang Y F, Yu Y F, Wei Z J, Zhang Z M 2022 *Acta Phys. Sin.* **71** 130306 (in Chinese) [曹若琳, 彭清轩, 王金东, 陈勇杰, 黄云飞, 於亚飞, 魏正军, 张智明 2022 物理学报 **71** 130306]
- [32] Zhou Q, Su C Z, Ma W Z 2022 *Laser J.* **43** 32 (in Chinese) [周琦, 苏成志, 马万卓 2022 激光杂志 **43** 32]
- [33] Muga N J, Ramos M F, Mantey S T, Silva N A, Pinto A N 2020 *IET Optoelectron.* **14** 350
- [34] Mekhtiev E E, Gerasin I S, Rudavin N V, Duplinsky A V, Kurochkin Y V 2021 *J. Phys. Conf. Ser.* **2086** 012092
- [35] Wang T, Huang P, Wang S Y, Zeng G H 2019 *Opt. Express* **27** 26689
- [36] Zhou M S, Li Y Q, Xiang Z H, Swoboda G, Cen Z Z 2007 *Tsinghua Sci. Technol.* **12** 546
- [37] Jin B T 2008 *Int. J. Numer. Meth. Eng.* **76** 230
- [38] CappÉ O, Godsill S J, Moulines E 2007 *Proc. IEEE* **95** 899
- [39] An M J 2012 *Geophys. J. Int.* **191** 849
- [40] Fox E P 1998 *Technometrics* **40** 155
- [41] Schönfeld P 1989 *Statistical Papers* **30** 212
- [42] Toussaint U V 2011 *Rev. Mod. Phys.* **83** 943
- [43] Barker A L, Brown D E, Martin W N 1995 *Comput. Math. Appl.* **30** 55
- [44] Cohn S E 1997 *J. Meteor. Soc. Jpn.* **75** 257
- [45] Zhuang L F, Pan F, Ding F 2012 *Appl. Math. Model.* **36** 3454
- [46] Ying M S 2010 *Artif. Intell.* **174** 162
- [47] Lamata L, Sanz M, Solano E 2019 *Adv. Quantum Technol.* **2** 1900075
- [48] Liu D, Pei C X, Quan D X, Zhao N 2010 *Chin. Phys. Lett.* **27** 050306
- [49] Li X H, Zhou P, Liang Y J, Li C Y, Zhou H Y, Deng F G 2006 *Chin. Phys. Lett.* **23** 1080
- [50] Haykin S 2005 *IEEE J. Sel. Area. Comm.* **23** 201
- [51] Corsi F, Galtarossa A, Palmieri L 1998 *J. Lightw. Technol.* **16** 1832
- [52] Galtarossa A, Schiano M, Someda C G, Daino B, Matera F, Zaninello R, Bergamin F 1991 *Electron. Lett.* **27** 595
- [53] Xie X X, Xu S L 1990 *J. Shaanxi Normal Univ. (Nat. Sci. Ed.)* **18** 82 (in Chinese) [谢晓新, 徐森禄 1990 陕西师大学报 (自然科学版) **18** 82]
- [54] Xu X P, Zhang D J 2018 *Comput. Eng. Appl.* **54** 144
- [55] Zhao R Q, Tang W S 2008 *J. Uncertain Syst.* **2** 165
- [56] Alfaro M E, Holder M T 2006 *Annu. Rev. Ecol. Evol. Syst.* **37** 19
- [57] Dempster A P, Laird N M, Rubin D B 1977 *J. R. Stat. Soc. Series B* **39** 1
- [58] Reimherr M, Meng X L, Nicolae D L 2021 *J. R. Stat. Soc. Series B* **83** 413
- [59] Zhang X G, Xi L X, Cui N, Zhang H, Xiao X S, Tang X F 2023 *Polarization Optics in Optical Fiber Communication* (Beijing: Tsinghua University Press) pp18–36 (in Chinese) [张晓光, 席丽霞, 崔楠, 张虎, 肖晓晟, 唐先锋 2023 光纤通信系统中的偏振光学 (北京: 清华大学出版社) 第 18—36 页]
- [60] Zhang X G, Duan G Y, Xi L X 2009 *Acta Opt. Sin.* **29** 1173 (in Chinese) [张晓光, 段高燕, 席丽霞 2009 光学学报 **29** 1173]
- [61] Franceschetti G, Smith C P 1981 *J. Opt. Soc. Am.* **71** 1487
- [62] Baptista M S 1998 *Phys. Lett. A* **240** 50
- [63] An Y Y, Zeng X D, Feng Z J 2010 *Photoelectric Detection and Signal Processing* (Beijing: Science Press) pp172–180 (in Chinese) [安毓英, 曾晓东, 冯喆珺 2010 光电探测与信号处理 (北京: 科学出版社) 第 172—180 页]

Research on dynamic polarization control in continuous variable quantum key distribution systems^{*}

Zhang Guang-Wei Bai Jian-Dong Jie Qi Jin Jing-Jing
Zhang Yong-Mei Liu Wen-Yuan[†]

(Department of Physics, School of Semiconductor and Physics, North University of China, Taiyuan 030051, China)

(Received 30 November 2023; revised manuscript received 14 December 2023)

Abstract

In a commercial fiber-based quantum key distribution system, the local and signal optical fields are transmitted through long distance fibers by using time division multiplexing and polarization multiplexing. The state of polarization of the optical field is inevitably disturbed by random birefringence of the standard single-mode fiber caused by external complex environments. This drift of the state of polarization significantly affects the balanced homodyne detection results and the secret key rate. Therefore, the key technology of the dynamic polarization control unit is crucial for the system in a large-scale commercial application. We theoretically analyze and prove that the polarization control unit only needs the combination of two degrees of freedom when considering the result of an arbitrary polarization extinction ratio at the receiver of the system. To overcome the influence of polarization variations, we propose a chaotic monkey algorithm based on Bayesian parameter estimation method and implement intelligence algorithm on field programmable gate array (FPGA) hardware under pulsed light with an integral-type detector for the dynamic polarization control unit. The simulation results show that the optimal combination is four degrees of freedom and the optimal prior distribution is an exponential distribution among various distributions in the dynamic polarization control unit. According to the simulation results, the experimental results show that the achieved polarization extinction ratio is over 30 dB and the average time of polarization control is 400 μ s for a single random polarization scrambling. By combining the dynamic polarization control unit with the system, we demonstrate the continuous variable quantum key distribution (CV-QKD) under a continuous polarization scrambling scope of 0–2 krad/s and verify its effectiveness. In addition, the methods presented will improve the performance of the system and expand the range of applications even under strong external disturbance.

Keywords: continuous variable quantum key distribution, Bayesian parameter estimation method, monkey algorithm, dynamic polarization controller

PACS: 03.67.Hk, 02.50.Tt, 07.05.Kf, 42.79.–e

DOI: [10.7498/aps.73.20231890](https://doi.org/10.7498/aps.73.20231890)

^{*} Project supported by the National Natural Science Foundation of China (Grant Nos. 12104419, 12104417, 12104418) and the Basic Research Program of Shanxi Province, China (Grant Nos. 20210302124689, 20210302124161, 20210302124025).

[†] Corresponding author. E-mail: liuweny@nuc.edu.cn

连续变量量子密钥分发系统中动态偏振控制研究

张光伟 白建东 颀琦 靳晶晶 张永梅 刘文元

Research on dynamic polarization control in continuous variable quantum key distribution systems

Zhang Guang-Wei Bai Jian-Dong Jie Qi Jin Jing-Jing Zhang Yong-Mei Liu Wen-Yuan

引用信息 Citation: *Acta Physica Sinica*, 73, 060301 (2024) DOI: 10.7498/aps.73.20231890

在线阅读 View online: <https://doi.org/10.7498/aps.73.20231890>

当期内容 View table of contents: <http://wulixb.iphy.ac.cn>

您可能感兴趣的其他文章

Articles you may be interested in

基于峰值补偿的连续变量量子密钥分发方案

Continuous-variable quantum key distribution based on peak-compensation

物理学报. 2021, 70(11): 110302 <https://doi.org/10.7498/aps.70.20202073>

基于量子催化的离散调制连续变量量子密钥分发

Discrete modulation continuous-variable quantum key distribution based on quantum catalysis

物理学报. 2020, 69(6): 060301 <https://doi.org/10.7498/aps.69.20191689>

基于实际探测器补偿的离散调制连续变量测量设备无关量子密钥分发方案

Discrete modulation continuous-variable measurement-device-independent quantum key distribution scheme based on realistic detector compensation

物理学报. 2022, 71(24): 240304 <https://doi.org/10.7498/aps.71.20221072>

连续变量量子计算和量子纠错研究进展

Research advances in continuous-variable quantum computation and quantum error correction

物理学报. 2022, 71(16): 160305 <https://doi.org/10.7498/aps.71.20220635>

无噪线性放大的连续变量量子隐形传态

Continuous variable quantum teleportation with noiseless linear amplifier

物理学报. 2022, 71(13): 130307 <https://doi.org/10.7498/aps.71.20212341>

量子密钥分发系统中抗扰动偏振编码模式的实验研究

Experimental research on disturbance resistant polarization modulation mode for quantum key distribution

物理学报. 2021, 70(18): 180302 <https://doi.org/10.7498/aps.70.20210749>