量子保密通信实验 · 预习报告

唐延宇* PB22030853

2025 年 4 月 13 日

1 实验背景及相关领域前沿调研

信息安全在现代通信中至关重要。经典密码学的安全性依赖于大整数分解或离散对数等数论难题的计算复杂度，而这些假设在量子计算出现后将面临被破解的风险。量子密钥分发（Quantum Key Distribution, QKD）利用量子力学基本原理，实现理论上无条件安全的密钥传输。自 1984 年 BB84 协议提出以来，QKD 在理论和实验方面迅速发展。目前研究前沿包括：

- 测量装置无关 *QKD*（Measurement-Device-Independent QKD, MDI-QKD），该方案消除了接收端探测器漏洞，实现对探测器侧信道攻击的免疫；
- 双字段 *QKD*（Twin-Field QKD），该协议通过中继干涉测量将密钥率与信道衰减的平方根成比例，提高了远距离传输性能；
- 连续变量 *QKD*（Continuous-Variable QKD），采用光场的强度和相位信息进行编码，在现有光通信基础设施上具有兼容优势；
- 卫星量子通信，通过卫星平台实现全球范围内的量子密钥分发，已在多国实现数百公里级链路；
- 集成光子芯片 *QKD*，将光源、调制器和探测器集成于芯片平台，提升系统体积小型化和可扩展性。

2 实验目的

本实验旨在深入理解量子密钥分发的基本原理与操作流程。我们将在实验过程中掌握 BB84 协议所涉及的量子态制备、测量和经典后处理的核心机制，并对量子信号发射器和接收器、手动偏振控制器等关键实验设备的功能与使用方法有清晰的认知。此外，实验者将完成设备的硬件连接、软件配置、同步校准以及偏振反馈等操作步骤，从而实现完整的量子密钥传输过程。通过观测实验中生成密钥的成码率、误码率及最终密钥的应用效果，我们能够分析量子通信系统的性能，并理解误码产生的原因及其可能的改进方法。实验还包括量子密钥在加密聊天、文本传输和图像传输中的实际应用演示，帮助我们全面了解量子通信技术的潜在应用价值。

3 实验原理

本实验基于 BB84 协议，采用单光子偏振态编码。协议分为量子传输阶段与经典后处理阶段两部分。

*近代物理系，19942431972，yanyutang@mail.ustc.edu.cn

3.1 量子传输阶段

发送方 Alice 随机选择两个偏振基中的一个（Z 基或 X 基），并在对应基上编码经典比特 0 或 1：

$$Z \text{ 基：} \quad |0_Z\rangle = |H\rangle, \quad |1_Z\rangle = |V\rangle,$$
$$X \text{ 基：} \quad |0_X\rangle = |+\rangle = \tfrac{1}{\sqrt{2}}(|H\rangle + |V\rangle), \quad |1_X\rangle = |-| = \tfrac{1}{\sqrt{2}}(|H\rangle - |V\rangle).$$

Alice 将制备好的单光子通过量子信道发送给 Bob。

Bob 同样随机选择 Z 基或 X 基对到达的单光子进行测量。当 Bob 的测量基与 Alice 制备基一致时，测量结果与 Alice 编码比特一致；否则测量结果随机。重复多次后，Alice 和 Bob 分别得到原始比特序列。

3.2 经典后处理阶段

量子传输结束后，Alice 和 Bob 通过经典认证信道公开各自使用的测量基，并丢弃基不匹配或未检测到光子的时隙，得到筛后密钥（sifted key）。随后进行：

1. **误码率估计**：公开一部分筛后密钥进行比对，若误码率低于阈值，则继续，否则终止；
2. **比特纠错**：采用纠错编码算法消除比特差异，保证 Alice 和 Bob 拥有完全一致的密钥；
3. **隐私放大**：利用哈希压缩等方法，将纠错后密钥压缩为最终安全密钥，以减少可能泄露给窃听者的信息。

4 实验仪器

本实验系统由以下主要部分组成：

- **量子信号发射器（Alice）**：包含主控板、四路 850 nm 激光器与偏振调制模块，用于以 1 MHz 频率产生四种偏振态光脉冲，并输出同步光（1310 nm）；
- **量子信号接收机（Bob）**：由主控板、单光子探测器（SPD）与接收光模块组成，根据同步电信号与延时参数打开探测门，实现单光子探测；
- **手动偏振控制器（MPC）**：由三个光纤环等效“$\lambda/4$ 波片 $+\lambda/2$ 波片 $+\lambda/4$ 波片”组成，用于补偿传输中光纤引起的偏振扰动；
- **光纤光路及器件**：包括光纤盘、分束器（BS）、偏振分束器（PBS）、可调衰减器（ATT）等，用于构建偏振编码与解码光路；
- **控制与处理软件**：分别在 Alice 端和 Bob 端运行，通过以太网 MAC 层与设备通信，完成流程控制、后处理、密钥存储及加解密演示。

5 实验内容与操作

5.1 硬件连接

按照图1示连接 Alice 和 Bob 设备：

- 使用 850 nm 光纤和 1310 nm 光纤分别连接发射器与接收器的信号光与同步光端口；
- 将主控板与计算机通过以太网（MAC 层）连接，并配置对应网卡 IP，确保 Alice 与 Bob 处于同一子网，可通过 `ping` 命令验证连通性；
- 检查光路和电源连接，确保所有接口牢固。

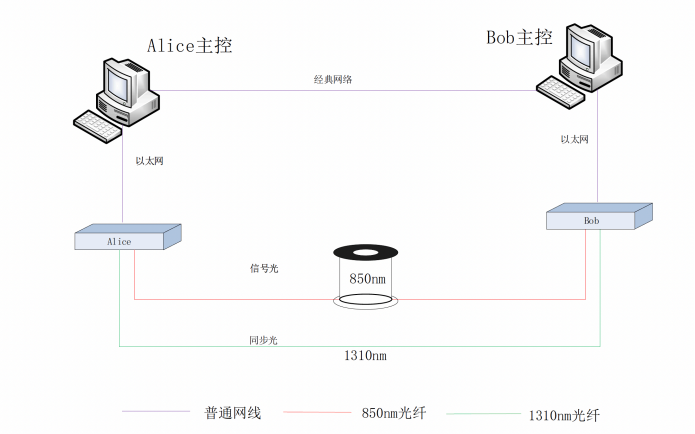

图 1: 量子密钥分发实验系统连接示意图

5.2 软件配置与启动

1. 启动控制软件，打开配置窗口，选择设备类型（Alice 或 Bob），填写网卡、MAC 地址及对端 IP 地址，保存并重启软件；
2. 在菜单栏或工具栏启动设备，观察自检日志与模块连接状态；
3. 在 Bob 端启动自动同步校准，获取延时参数：

$$t_{\text{delay}} = N_{\text{offset}} \times 1\,\mu\text{s} + d_{\text{fine}} \times 10\,\text{ns}.$$

5.3 偏振反馈与基矢比对

1. 在 Bob 端启动偏振反馈，依次发射 H、V、+、− 偏振光，手动调节两个 MPC 环，使对应通道计数比大于 20:1；
2. 在 Alice 端启动基矢比对，软件上传发光与探测数据，完成基矢匹配、误码率统计及纠错，保存最终密钥，并显示成码率与误码率。

5.4 量子密钥应用演示

实验软件提供聊天、TXT 文件传输与 BMP 图像传输三种演示功能。在 Alice 端选择发送，Bob 端选择接收，可分别测试不加密与加密传输效果，并观察加解密后的数据显示情况。

量子保密通信实验

唐延宇* PB22030853

2025 年 4 月 30 日

摘要

本实验基于 BB84 协议, 利用偏振态单光子源实现量子密钥分发. 通过对量子信号的制备、测量和经典后处理, 我们深入理解了量子密钥分发的基本原理与操作流程. 实验中, 我们观察了成码率、误码率及最终密钥的应用效果, 并分析了量子通信系统的性能及误码产生的原因. 实验结果表明, 量子密钥分发具有无条件安全性, 为未来信息安全提供了新的解决方案.

关键词: 量子密钥分发, *BB84* 协议, 信息安全

1 引言

1.1 实验背景

信息安全在现代通信中至关重要. 经典密码学的安全性依赖于大整数分解或离散对数等数论难题的计算复杂度, 而这些假设在量子计算出现后将面临被破解的风险. 量子密钥分发(Quantum Key Distribution, QKD)利用量子力学基本原理, 实现理论上无条件安全的密钥传输. 自 1984 年 BB84 协议提出以来, QKD 在理论和实验方面迅速发展. 目前研究前沿包括:

- 测量装置无关 *QKD*(Measurement-Device-Independent QKD, MDI-QKD), 该方案消除了接收端探测器漏洞, 实现对探测器侧信道攻击的免疫;
- 双字段 *QKD*(Twin-Field QKD), 该协议通过中继干涉测量将密钥率与信道衰减的平方根成比例, 提高了远距离传输性能;
- 连续变量 *QKD*(Continuous-Variable QKD), 采用光场的强度和相位信息进行编码, 在现有光通信基础设施上具有兼容优势;
- 卫星量子通信, 通过卫星平台实现全球范围内的量子密钥分发, 已在多国实现数百公里级链路;
- 集成光子芯片 *QKD*, 将光源、调制器和探测器集成于芯片平台, 提升系统体积小型化和可扩展性.

1.2 实验目的

本实验旨在深入理解量子密钥分发的基本原理与操作流程. 我们将在实验过程中掌握 BB84 协议所涉及的量子态制备、测量和经典后处理的核心机制, 并对量子信号发射器和接收器、手动偏振控制器等关键实验设备的功能与使用方法有清晰的认知. 通过观测实验中生成密钥的成码率、误码率及最终密钥的应用效果, 我们能够分析量子通信系统的性能, 并理解误码产生的原因及其可能的改进方法.

*近代物理系, 19942431972, yanyutang@mail.ustc.edu.cn

1.3 实验原理

本实验基于 BB84 协议, 采用单光子偏振态编码. 协议分为量子传输阶段与经典后处理阶段两部分.

量子传输阶段 发送方 Alice 随机选择两个偏振基中的一个（Z 基或 X 基）, 并在对应基上编码经典比特 0 或 1:

$$Z \text{ 基:} \quad |0_Z\rangle = |H\rangle, \quad |1_Z\rangle = |V\rangle,$$
$$X \text{ 基:} \quad |0_X\rangle = |+\rangle = \tfrac{1}{\sqrt{2}}(|H\rangle + |V\rangle), \quad |1_X\rangle = |-| = \tfrac{1}{\sqrt{2}}(|H\rangle - |V\rangle).$$

Alice 将制备好的单光子通过量子信道发送给 Bob.

Bob 同样随机选择 Z 基或 X 基对到达的单光子进行测量. 当 Bob 的测量基与 Alice 制备基一致时, 测量结果与 Alice 编码比特一致; 否则测量结果随机. 重复多次后, Alice 和 Bob 分别得到原始比特序列.

经典后处理阶段 量子传输结束后, Alice 和 Bob 通过经典认证信道公开各自使用的测量基, 并丢弃基不匹配或未检测到光子的时隙, 得到筛后密钥（sifted key）. 随后进行:

1. **误码率估计**: 公开一部分筛后密钥进行比对, 若误码率低于阈值, 则继续, 否则终止;
2. **比特纠错**: 采用纠错编码算法消除比特差异, 保证 Alice 和 Bob 拥有完全一致的密钥;
3. **隐私放大**: 利用哈希压缩等方法, 将纠错后密钥压缩为最终安全密钥, 以减少可能泄露给窃听者的信息.

2 实验装置

本实验系统由以下主要部分组成:

- **量子信号发射器（Alice）**: 包含主控板、四路 850 nm 激光器与偏振调制模块, 用于以 1 MHz 频率产生四种偏振态光脉冲, 并输出同步光（1310 nm）;
- **量子信号接收机（Bob）**: 由主控板、单光子探测器（SPD）与接收光模块组成, 根据同步电信号与延时参数打开探测门, 实现单光子探测;
- **手动偏振控制器（MPC）**: 由三个光纤环等效“$\lambda/4$ 波片 $+\lambda/2$ 波片 $+\lambda/4$ 波片”组成, 用于补偿传输中光纤引起的偏振扰动;
- **光纤光路及器件**: 包括光纤盘、分束器（BS）、偏振分束器（PBS）、可调衰减器（ATT）等, 用于构建偏振编码与解码光路;
- **控制与处理软件**: 分别在 Alice 端和 Bob 端运行, 通过以太网 MAC 层与设备通信, 完成流程控制、后处理、密钥存储及加解密演示.

3 实验内容

3.1 硬件连接

按照图1示连接 Alice 和 Bob 设备:

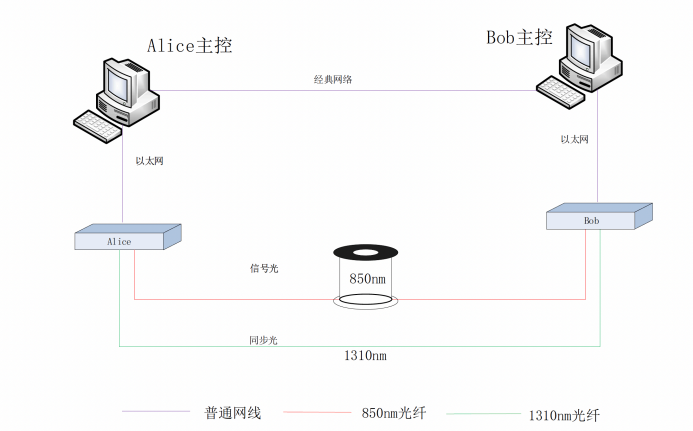

图 1: 量子密钥分发实验系统连接示意图

- 使用 850 nm 光纤和 1310 nm 光纤分别连接发射器与接收器的信号光与同步光端口;
- 将主控板与计算机通过以太网(MAC 层)连接, 并配置对应网卡 IP, 确保 Alice 与 Bob 处于同一子网, 可通过 `ping` 命令验证连通性;
- 检查光路和电源连接, 确保所有接口牢固.

3.2 软件配置与启动

1. 启动控制软件, 打开配置窗口, 选择设备类型(Alice 或 Bob), 填写网卡、MAC 地址及对端 IP 地址, 保存并重启软件;
2. 在菜单栏或工具栏启动设备, 观察自检日志与模块连接状态;
3. 在 Bob 端启动自动同步校准, 获取延时参数:

$$t_{\mathrm{delay}} = N_{\mathrm{offset}} \times 1\,\mu\mathrm{s} + d_{\mathrm{fine}} \times 10\,\mathrm{ns}.$$

3.3 偏振反馈与基矢比对

1. 在 Bob 端启动偏振反馈, 依次发射 H、V、+、− 偏振光, 手动调节两个 MPC 环, 使对应通道计数比大于 20:1;
2. 在 Alice 端启动基矢比对, 软件上传发光与探测数据, 完成基矢匹配、误码率统计及纠错, 保存最终密钥, 并显示成码率与误码率.

3.4 量子密钥应用演示

实验软件提供聊天、TXT 文件传输与 BMP 图像传输三种演示功能. 在 Alice 端选择发送, Bob 端选择接收, 可分别测试不加密与加密传输效果, 并观察加解密后的数据显示情况.

4 实验结果

在实验过程中, 我们首先启动自动同步校准, 之后在 Bob 端开启偏振反馈, 手动调节 MPQ, 对探测器计数进行优化. 之后软件系统可以自动进行基矢比对, 然后便能获得存储密钥, 可以开启保密通信. 实验中, 我们进行了文字聊天、文件及图片传输的演示, 取得了较好的成果, 具体通信现象如图2所示.

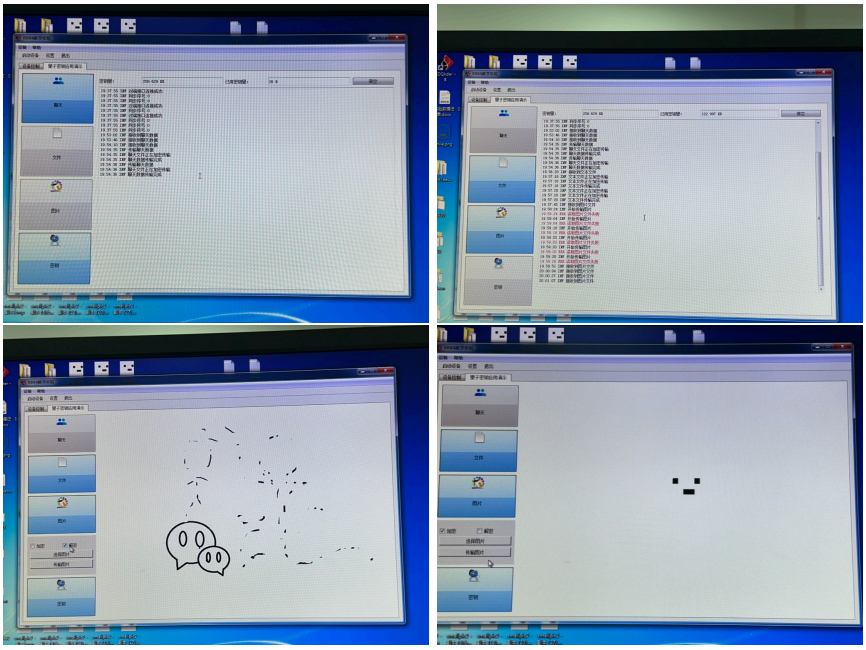

图 2: 量子保密通信结果

5 实验讨论（思考题）

1. 量子保密通信为什么是无条件安全的，其物理基础是什么？

量子保密通信（Quantum Key Distribution, QKD）被称为无条件安全，是基于量子力学的几项基本原理. 首先，测量—干扰原理表明，对任意量子态的测量都会不可避免地扰动其原始状态，因此当窃听者试图测量传输中的量子信号时，合法通信双方能够通过误码率的升高察觉到这一扰动. 其次，量子不可克隆定理保证了任何未知量子态都无法被完美复制，因此窃听者无法通过复制量子信号并分离后重放的方式而不被发现. 最后，量子纠缠的单亲性意味着若一对粒子处于纠缠态，则第三方无法同时与这对粒子保持同等程度的纠缠，从而限制了窃听者获取纠缠信息的能力，这一特性进一步巩固了 QKD 的安全性.

2. 量子不可克隆定理是什么？

量子不可克隆定理指出：对于任意未知量子态 $|\psi\rangle$，都不存在一个幺正变换 U 能够将该态与一个初始的空白态 $|s\rangle$ 同时输出两个相同的态，即

$$U\big(|\psi\rangle \otimes |s\rangle\big) = |\psi\rangle \otimes |\psi\rangle.$$

该定理的核心在于量子力学的线性叠加原理和态叠加的不可分性，正是这一性质阻止了对任意量子态的完美复制.

3. 实验中所使用的光源是单光子源还是其他什么光源？

实验中使用的标记单光子源（Heralded Single-Photon Source, HSPS）是一种特殊的光源，利用同时产生的光子对中的一个光子来标识另外一个光子到达时间. 这种光源在量子保密通信中具有独特的优势. 一方面，这种光源避免了多光子的干扰，另一方面有助于减小接收方在远距离传输时受探测器暗计数影响的问题.

4. 使用非单光子源可能会有哪些问题，有没有办法消除？

采用弱相干光源时会产生一定比例的多光子脉冲，这使得窃听者可能实施光子数分裂（Photon-Number Splitting, PNS）攻击，即截获部分光子而不被合法通信方察觉. 为了消除这一潜在风

险, QKD 系统中普遍引入诱骗态(decoy-state)技术:发送端在发送过程中会随机切换不同平均光子数的衰减脉冲, 接收端通过对这几种态的检测率和误码率进行统计分析, 从而有效识别并限制窃听者的 PNS 攻击行为, 恢复量子通信的无条件安全性.

5. 如何降低实验中的错误率?

为了在 QKD 实验中尽可能降低误码率, 需要从多个方面进行优化. 首先, 应精确调节光路对准与光程匹配, 确保干涉仪的可见度(visibility)达到最高水平;其次, 需要选用性能优越的雪崩光电二极管(APD), 并通过降低暗计数率和缩短探测死区来减少探测噪声;再次, 严格同步发送端和接收端的时钟, 并精细设定探测时窗, 从而有效减少定时误差;此外, 在光纤链路中增设无源光学滤波器和光隔离器, 可以抑制来自散射光、背景光以及其他光源的干扰;最后, 结合高效的误差校正(error correction)和隐私放大(privacy amplification)算法, 能够进一步修正传输误差并提取安全密钥.

6. 请说说实验中调节 MPC 起到的作用是什么, 如何判断调节好了, 为什么这样判断?

在基于偏振编码的光纤 QKD 系统中, 手动偏振控制器(Manual Polarization Controller, MPC)用于补偿光纤传输过程中因温度变化和机械应力引起的偏振态漂移, 以保证发送端和接收端采用相同的偏振基进行编码和解码. 手动偏振控制器每个环对偏振的调节是按照正弦曲线变化的, 因此调节的方法是:先旋转第一个环找到极值点后, 接着旋转第二个环找到极值点, 然后旋转第三个环, 直至偏振达到要求, 同时观察接收端两个探测器的计数率变化, 当其中一个探测器的点击率达到最大值而另一个则处于最低水平时, 即表明光路中两条偏振分量的相对相位差已被最佳调整. 此时, 干涉仪的可见度处于最高水平, 同时误码率(Quantum Bit Error Rate, QBER)达到最小, 因此可以判定偏振控制已达到最佳状态.

参考文献

[1] 中国科学技术大学物理实验教学中心. 量子保密通信实验讲义. 2021.04.12.