量子密码学演示实验报告

物理 32/物理 31 冯家琦/周方远 2023011338/2023011263

摘要

本实验通过 EDU-QCRY1 量子密码学演示套件，模拟和演示了量子密码学中的 BB84 协议原理。实验展示了量子密钥分发 (QKD) 的基本过程，包括密钥生成、消息加密传输以及窃听检测等关键环节。通过实验加深了对量子密码学原理的理解。

1 实验原理

1.1 一次性密码本原理

一次性密码本 (One-Time Pad) 是一种理论上完全安全的加密方法。它使用与明文等长的随机密钥，通过二进制加法对明文进行加密。加密过程需满足以下要求：

- 密钥长度不短于明文
- 密钥只能使用一次
- 密钥必须完全随机
- 密钥只能由发送方和接收方知道

具体的加密算法为：Alice 将每位明文异或上对应位密钥作为密文，Bob 收到密文后将每位异或上对应位密钥即可得到明文。

1.2 BB84 协议

BB84 协议是一种量子密钥分发协议，用于安全地在通信双方间建立共享密钥。其基本步骤为：

1. 定义两组基底:+ 基 (0° 和 90° 偏振) 和 × 基 (-45° 和 45° 偏振)
2. Alice 随机选择基底发送随机比特
3. Bob 随机选择基底进行测量
4. 通过公开信道交换使用的基底信息
5. 保留使用相同基底的测量结果作为密钥

2 实验仪器

- 铝制光学平台
- 635nm 激光二极管模块
- lambda/2 波片
- 偏振分束器
- 光电探测器
- 旋转支架
- 控制电路
- 其他光学支架和紧固件

3 实验步骤

3.1 系统调试

1. 安装激光器并调节光路
2. 校准 lambda/2 波片的角度设置
3. 调节探测器的灵敏度

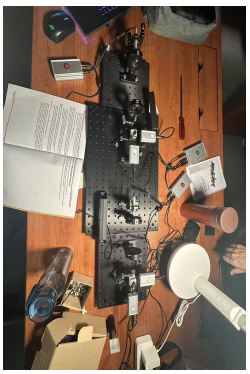

图 1: 包含 Bob, Eve, Alice 的完整实验系统

3.2 密钥生成实验

先将实验平台中的 Eve 部分移除，重新校对好 Alice 和 Bob，确保对于 Alice 发射的四种可能偏振与 Bob 测量偏振的两种可能基底的任意组合均能得到正确结果。

Alice 生成两段 52 bits 的随机基底和密钥，Bob 生成一段 52 bits 的随机基底。

```
Alice Base: x+x++xxx+x++++xx+x+xxx+x++x++++++x+x+xxx+xx++xxx++xx
Alice Key:


Bob Base:   xx++++x++x++x+++xx+x+x++++x++xxxx+xx++xx+x+x+++++x+x
```

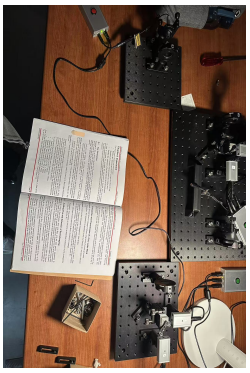

图 2: 仅包含 Bob, Alice 的实验系统

Alice 用其选择的基底发送其生成的密钥，Bob 用自己选择的基底测量收到的光子。

1. 设置 Alice 和 Bob 的基底选择装置
2. 进行一系列比特传输
3. 记录双方使用的基底和测量结果
4. 通过比对确定共享密钥

3.3 窃听检测实验

1. 在光路中加入 Eve 的测量装置
2. 重复密钥生成过程
3. 分析错误率变化

4 实验思考

1. 本实验使用的是脉冲激光而非单光子源，这与实际的量子密码系统有何区别?
2. BB84 协议中为什么要使用两组不同的基底?
3. 在有窃听者的情况下，为什么会出现约 25% 的错误率?
4. 量子密码学相比经典密码学有哪些优势和局限性?

5 总结

- 通过实验成功演示了 BB84 量子密钥分发协议的工作原理
- 验证了窃听检测机制的有效性
- 理解了量子密码学中的关键概念如基底选择、量子测量等
- 掌握了量子通信系统的基本组成和调试方法