Quantum Key Distribution 实验报告

何金铭 PB21020660

实验目的，实验原理，实验内容已于预习报告中给出，这里不再赘述。

1 实验结果与分析

1.1 基矢对比

在完成:

1. 同步设置
2. 利用 MPC 进行偏振调节

等操作后，我们进行基矢对比得错误率为 4%，小于错误率要求 5%

1.2 量子密钥应用演示

1.2.1 聊天加密

Bob 传输一串字母”Hello! How are you? Nice to meet you!”，在接收端 ALice 解密后得到原文；若不解密，则接受到的是乱码。

1.2.2 图片加密

Bob 传输一张图片，在接收端 Alice 解密后得到原图；若不解密，则接受到的是带有很多噪声的图片。

2 实验结论

1. 同步对于实验结果的影响很大，若未同步，则会使得光子计数率低，导致错误率高，几乎不能通信；
2. 通过了这个实验，我们了解了 QKD 的基本工作原理，并且利用了 QKD 进行了几个简单的加密通信；

3 思考题

3.1 量子保密通信为什么是无条件安全的，其物理基础是什么?

其物理基础是量子态不可克隆定理，即未知量子态不能精确克隆（对任意输入态)。

3.2 量子不可克隆定理是什么?

未知量子态不能精确克隆（对任意输入态）
下面证明这个定理:

$|\phi\rangle$ 和 $|\psi\rangle$ 是两个任意的量子状态，我们要把这两个状态拷贝到另一个与他们完全无关的状态 $|k\rangle$ 上。我们用一个幺正算符 U 来描述这个过程。则这个拷贝算符必须具备以下性质:

$$U(|\phi\rangle \otimes |k\rangle) = |\phi\rangle \otimes |\phi\rangle$$
$$U(|\psi\rangle \otimes |k\rangle) = |\psi\rangle \otimes |\psi\rangle$$

内积 $\langle U(\phi \otimes k)|U(\psi \otimes k)\rangle$ 可得出以下两个等式:

$$\langle U(\phi \otimes k)|U(\psi \otimes k)\rangle = \langle \phi \otimes \phi|\psi \otimes \psi\rangle$$
$$\langle U(\phi \otimes k)|U(\psi \otimes k)\rangle = \langle \phi \otimes k|\psi \otimes k\rangle$$

这样便得到了:

$$\langle \phi \otimes \phi|\psi \otimes \psi\rangle = \langle \phi \otimes k|\psi \otimes k\rangle,$$
$$\rightarrow$$
$$\langle \phi|\psi\rangle\langle \phi|\psi\rangle = \langle \phi|\psi\rangle\langle k|k\rangle\ .$$

因为 $\langle k|k\rangle = 1$, 所以得出

$$\langle \phi|\psi\rangle^2 = \langle \phi|\psi\rangle.$$

这个等式仅有的两个解是 $\langle \phi|\psi\rangle = 0$ 和 $\langle \phi|\psi\rangle = 1$。这意味着，要么 $\phi = \psi$ (当 $\langle \phi|\psi\rangle = 1$), 要么 ϕ 与 ψ 正交 (当 $\langle \phi|\psi\rangle = 0$)。只能够克降相同或正交的状态，这并不是我们最初假设的任意状态的完全克隆，不可克隆原理证明完毕。

3.3 实验中所使用的光源是单光子源还是其它什么光源?

实际情况中，我们不使用单光子源，而是使用弱相干光源，因为:

1. 单光子源实现较困难;
2. 信道损耗大;

3.4 使用非单光子源可能会有什么问题，有没有办法消除?（调研，选做）

解决方法: Decoy State (诱骗态方案)

由于 Eve 只分裂发送多光子脉冲，分裂导致多光子脉冲的损耗特性发生改变，一般表现为损耗降低；原因：Eve 为了保证多光子脉冲尽可能的被 Bob 接受到，从而让 Bob 以为是有用传输，用以生成密钥，这样 Eve 等 AB 公开测量基信息后就可以提取密钥；我们可以发送一个主要以多光子脉冲分布的光场，如果 Eve 用这种方式攻击，则我们会看到多光子脉冲的损耗会降低！从而探测到 Eve 的存在;

Decoy State QKD 协议如下:

1. Alice 随机发送信号态或诱骗态给 Bob;
2. Bob 公开每一次发送信号时候接收到;
3. Alice 公开说明具体每一次发送的是信号态还是诱骗态;
4. Alice 和 Bob 计算信号态和诱骗态各自传输成功的概率；如果 Eve 只选择的发送两光子态，则 A、B 会发现诱骗态 B) 的接受成功概率非常高，从而确认 Eve 的存在；没有 Eve 时，获取密钥的方法如 BB84 同。

3.5 如何降低实验中的错误率?

1. 提升激光器的单光子性
2. 降低光纤中的光子损耗
3. 提高单光子探测器的探测效率
4. 提升偏振度的对比度

3.6 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?

作用为调节光子的偏振态 $|H\rangle, |V\rangle, |+\rangle, |-\rangle$

判断的标准是偏振对比度 $|H\rangle : |V\rangle, |+\rangle : |-\rangle$ 大于 20:1 或小于 1:20，因为说明两者强度比很大，可近似为理想线性偏振光了。