ilab-x 实验报告

马若般 物理学系 19307110031

实验二：量子保密通信

1. 实验目的

量子保密通信是将量子密钥分发和一次一密相结合的安全通信方案，是量子物理与信息科学交叉融合的新兴技术。本项目利用3D虚拟仿真技术，真实还原实验场景，不受时间和空间限制，完成光路搭建、量子密钥分发、一次一密等实验内容，有助于提高实验教学效率，激发学习量子信息的兴趣，培养自主探究学习能力、多学科交叉融合与创新思维。

2. 实验原理

2.1. 理论原理

注：有关2.1节和2.2节中量子密钥分发（BB84协议）的具体原理，见附件。

量子保密通信是将量子密钥分发和“一次一密”加密法相结合的安全通信方案。通信双方先利用量子力学方法产生并分享安全的密钥，然后利用“一次一密”，在公开信道上进行无条件安全的信息传输。实验原理包括量子密钥分发原理和“一次一密”原理。

2.1.1. 量子密钥分发原理

量子密钥分发利用量子物理特性产生绝对安全的随机密钥，典型的量子密钥分发协议是偏振编码的BB84协议。通信双方利用单光子的偏振态作为信息载体，共享两组偏振基矢：HV基矢和DA基矢，使用水平偏振H/垂直偏振V/+45°偏振D/−45°偏振A这四种偏振态，并约定各偏振态对应的经典编码如H-0, V-1, D-0, A-1。密钥分发流程如下：

1. 发送端
   发射端Alice随机地将单光子的偏振态制备为H/V/D/A的一种，发送给接收端，并记录偏振基矢和光子的偏振态。
2. 接收端
   接收端Bob首先随机地选择偏振基矢，再用该基矢对Alice发来的单光子的偏振态进行测量，记录选择的偏振基矢和偏振态测量结果。
3. 对基
   Alice和Bob通过经典信道公布发送给和接收偏振基矢，相互比对，仅保留发送与接收使用相同基矢的情况，舍弃基矢不同的情况。经过对基之后双方就分享了密钥，也称为筛后密钥。
4. 后处理
   由于信道存在损耗和错误，也可能存在窃听者，Alice和Bob得到的筛后密钥需要进一步的处理。一般而言，Alice和Bob随机抽取一部分筛后密钥在经典信道中公开，相互进行比对并估计筛后密钥的误码率与窃听者获取的信息量。随后，Alice和Bob执行密钥协商(Key Reconciliation)（或称纠错，Error Correction）和错误校验（Error Verification）过程，将筛后密钥中不一致的部分进行纠正，使Alice和Bob拥有完全相同的密钥序列，

称为协商后密钥(Reconciled Key)。随后，Alice和Bob将进行密性放大(Privacy Amplification)操作，将窃听者获取的信息量压缩为零。此时得到的密钥称为安全密钥(Secret Key)或最终密钥(Final Key)。

2.1.2. 量子密钥分发的安全性原理

量子密钥分发的安全性由量子力学的基本原理所保障。

1. 单光子不可分割性，窃听者无法对单光子进行分割，只能复制或测量。
2. 量子态不可克隆定律，是指未知量子态不可精确克隆，因此窃听者无法复制单光子的偏振态，只能测量。
3. 海森堡不确定原理。BB84协议中HV基矢测量H/V偏振可以得到确定的结果，但是测量D/A偏振的结果不确定。同理，DA基矢测量D/A偏振可以得到确定的结果，但是测量H/V偏振的结果不确定。
4. 量子态测量塌缩理论，经过测量之后，量子态以一定概率塌缩到测量本征态上，原来的量子态发生改变。对单光子偏振态的测量与重发将以一定的概率引入错误，从而被通信双方发现。

2.1.3. 一次一密原理

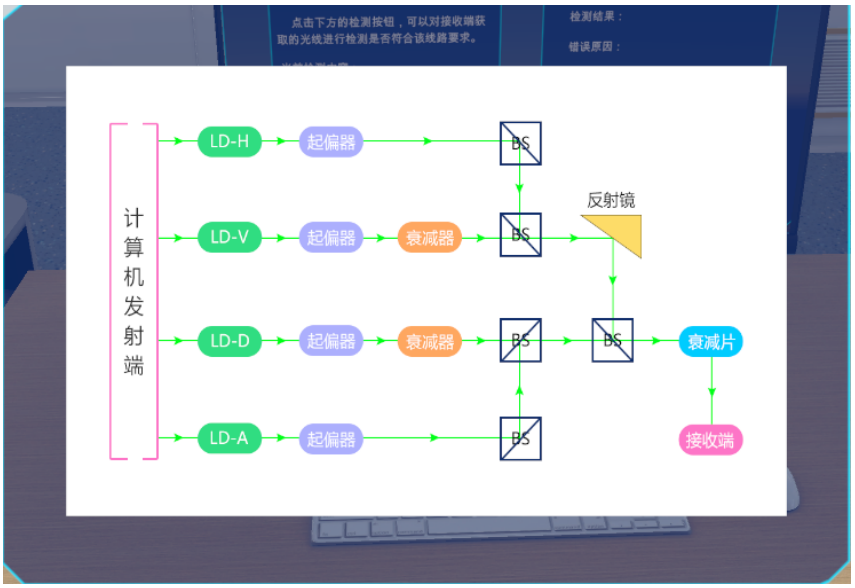
一次一密(one-time pad)加密法由Vernam等在1917年发明，要求密钥完全随机，密钥和明文的长度相等，密钥只能使用一次。加密时，密钥和明文逐比特进行“异或”运算即得密文，密文和密钥逐比特“异或”运算即得明文。1949年香农证明“一次一密”完全不可破解。

2.2. 仪器原理

光路分为发射端和接收端。

2.2.1. 发射端

发射端要产生四种不同偏振态光子，方法如下：本实验使用的激光器可以发出光强为1.496×10^{-17}w的圆偏振光，让圆偏振光经过偏振片获得线偏振光；用反射镜和分光镜改变四束线偏振光的方向，让它们合束；再让这一束光通过衰减器，光强减弱为1.87×10^{-20}w时即认为满足单光子条件。此时每次会有一个光子最终到达接收端，只要合束前四束线偏光的强度一样，每种偏振态的光子到达接收端的概率就相同！

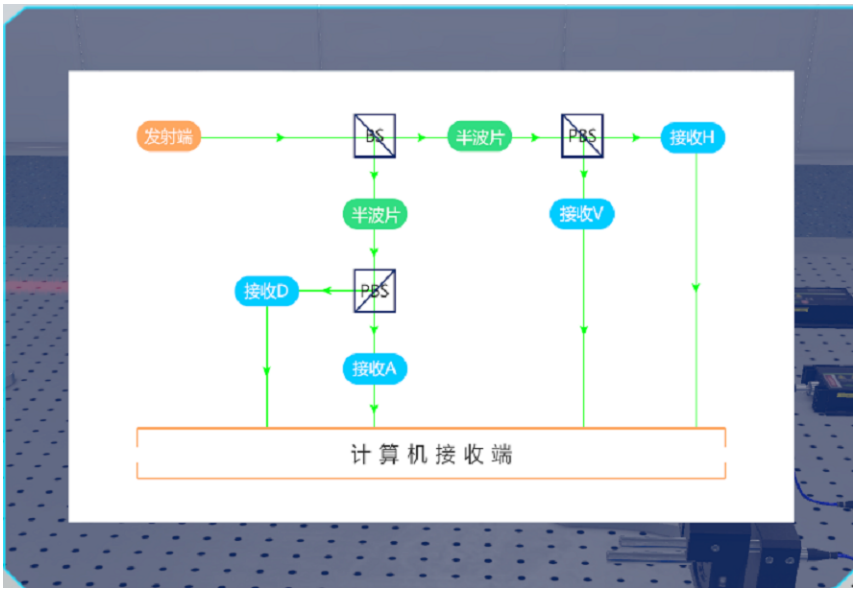


2.2.2. 接收端

接收端要实现以下功能：随机选择HV或DA基矢作为测量基矢，以及在该基矢下测量单光子的偏振态。光子从发射端部分进入接收端部分后，首先通过一个50%分光器，以相同的概率进入HV基测量部分或DA基测量部分。单光子偏振态测量通过偏振分束器PBS来实现。PBS只有在接收相位为$k\pi/2$的偏振光时，才会实现分光。因此

1. 进入HV基矢测量部分的光子可以直接通过PBS，它可以顺利地分出H偏振及V偏振的光子；
2. 而进入DA基矢测量部分的光子应先通过一个22.5°的半波片（光线通过半波片后其偏振角会增加两倍的半波片快轴方向），然后才能实现PBS区分D偏振及A偏振的光子。

光子通过PBS后即进入接收器被测量。



3. 实验仪器

发射端计算机(Alice机)、激光模块(激光器)、起偏器(半波片)、分光器(BS，透射率50%)、高反镜(反射率100%)、衰减器、耦合器、PBS、SPCM(接收光子的仪器)、接收端计算机(Bob机)。

4. 实验记录

1. 搭建发射端光路
   (a) 打开激光模块（激光器）H，按光路图依次摆放起偏器、两个分束器、反射镜、分束器和衰减片，起偏器快轴调整为0°以满足H模块的偏振要求。调整各元件位置和角度以使H模块的激光正确地通过以上六个元件并被接收端接收。调整最后一个衰减片的衰减率为99%，以使最后被接收的光满足单光子条件。然后在接收端计算机上检验H模块的激光是否被正常接收并满足单光子要求，系统提示检测合格这说明H模块光路调节正确，此时关闭激光模块H。
   (b) 按与(a)相同的步骤搭建模块V的光路，但是注意：(1)该光路上起偏器快轴要调至90°；(2)要在起偏器后加一个衰减率50%的衰减器，因为我们要求四束激光合束时强度相同，而由光路可见，模块H的激光比模块V的激光多经过了一个50%的分光器。
   (c) 按与(b)相同的步骤搭建模块D的光路，注意：该光路上起偏器快轴要调至45°；
   (d) 按与(a)相同的步骤搭建模块A的光路，注意：该光路上起偏器快轴要调至135°；
   此时发射端光路搭建完毕。
2. 搭建接收端光路：为了简便考虑，实验系统设置这部分只需要调节半波片快轴方向，光路其他部分由系统自动设定。按照仪器原理中的阐述，将DA接收端的半波片快轴方向调节至22.5度，HV接收端的半波片的快轴方向调节至0度即可。
3. 检查量子密钥分发是否正常工作：在Alice机上的软件内让光路开始分发密钥，并到Bob机上的软件内检查接收情况。

(a) 若来自HV(DA)基的信号出现且仅出现“只有H(D)接收响应”、“只有V(A)接收响应”和“D、A(H、V)同时响应”3种情况，则说明接收端光路搭建正确。

(b) 若来自HV(DA)基的信号出现了“H、V(D、A)接收同时响应”的情况，则说明接收端光路搭建错误。

4. 量子保密通信：根据系统自动生成的三种密钥和密文，译出明文，填入数据记录栏中。译码方法：逐比特“异或运算”，即密钥和密文的某一比特若同为0或同为1，则明文的该比特为0；若密钥和密文的某一比特一个是0另一个是1，则明文的该比特为1。

	第一组	第二组	第三组
密钥	0000010100	0111001101	0110001110
密文	1110001000	1000000010	1000101000
明文	1110011100	1111001111	1110100110

5. 实验结论

通过量子密钥分发（BB84协议）和一次一密加密法，根据量子力学的基本原理，可以实现100%的加密通信。这是量子保密通信的最基础的实现方法之一，目前已经实现了商业应用。量子通信的发展前景十分广阔，值得引起我们的重视。

在系统中的数据记录及其他操作过程的截图，见附件。