量子保密通信实验报告

姓名：杨博涵　　学号：PB20000328　　实验日期：2023 年 5 月 5 日

一、实验结果

按照实验步骤，我们进行了自动同步校准和偏振反馈工作。其中偏振反馈校准后所得结果如下面四幅图所示

图 1　发 H 光时的探测器计数

图 2　发 V 光时的探测器计数

图 3　发 P 光时的探测器计数

图 4　发 N 光时的探测器计数

可以看到偏振结果符合实验的要求。

在基矢比对时可以达到 3%左右的准确率，认为校准成功。

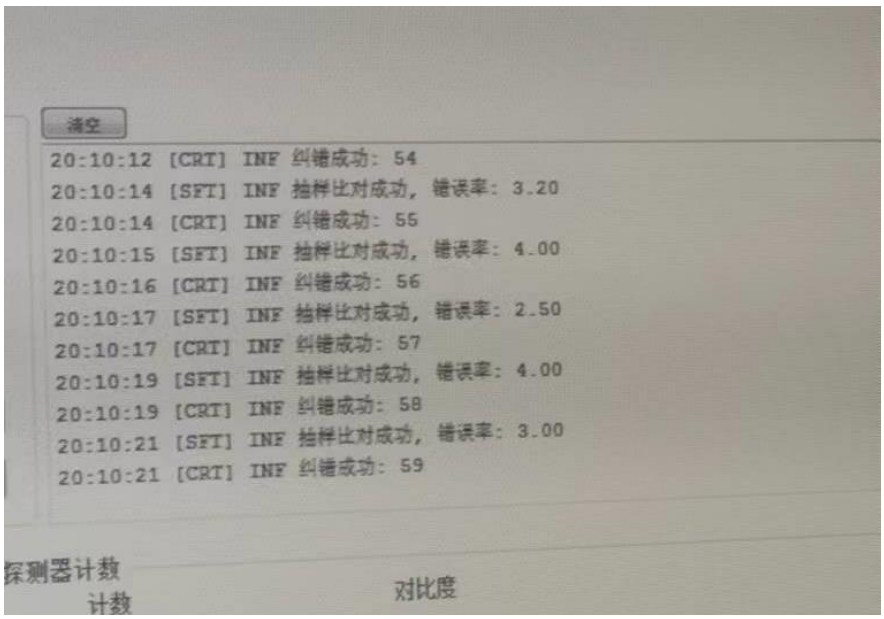

图 5　基矢比对结果

最后我们进行了信息收发操作

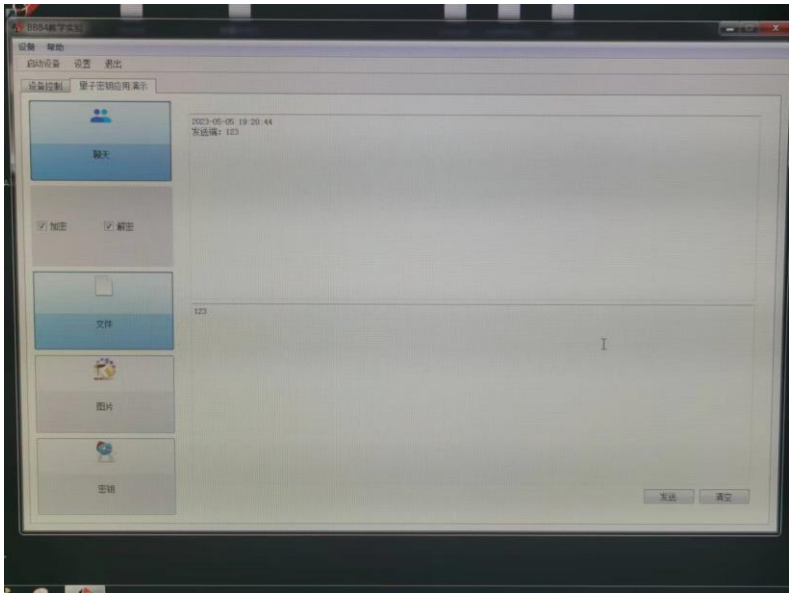

图 6　发送端发送 123

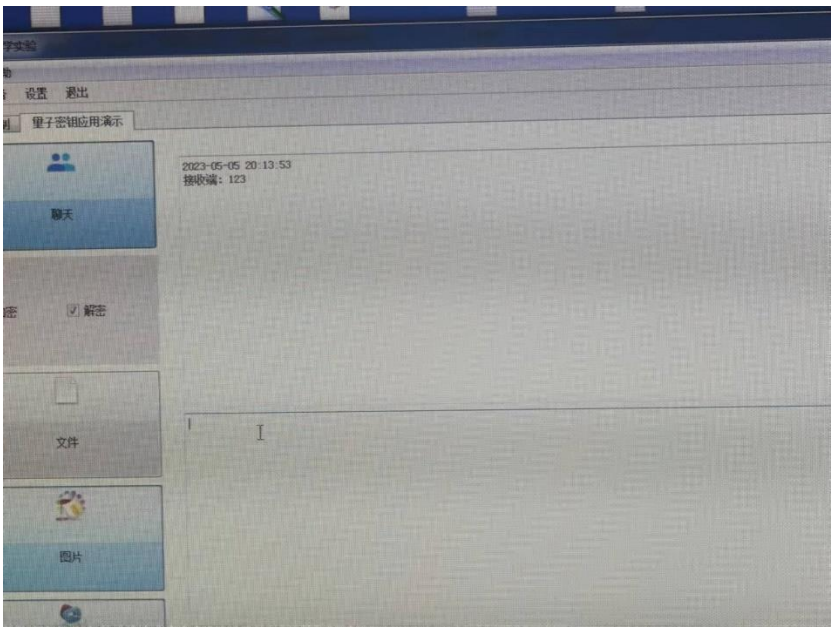

图 7　接收端得到 123

二、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？

A: 量子通信的安全性基于量子物理基本原理，作为光的最小颗粒，单个光量子在传输信息的时候具有量子不可分割和量子不可克隆两大特性，同时量子态具有可叠加性，从而能保证信息的不可窃听和不可破解，任何窃听行为都将因原有态的塌缩而引入可观测的错误从而暴露。

2. 量子不可克隆定理是什么？

A: 量子不可克隆定理是指量子力学中对任意一个未知的量子态进行完全相同的复制的过程是不可实现的，也即在量子力学中，不存在这样一个物理过程能实现对一个未知量子态的精确复制，使得每个复制态与初始量子态完全相同。

3. 实验中所使用的光源是单光子源还是其它什么光源？

A: 使用的是弱相干态光源，这是一种近似单光子源，虽然理想中的 BB84 协议要求使用单光子源，否则窃听者可以利用光子数分离攻击，但是适用于量子密钥分发的理想单光子源至今仍不存在，所以实际中采用的是弱相干光源结合诱骗态粒子来抵御光子数分离攻击。

4. 使用非单光子源可能会有什么问题，有没有办法消除？

A: 非理想单光子源中最典型的是弱相干态光源。虽然弱相干态光源大多数情况下发射的是单光子，但仍然存在一定的概率，每次会发射两个甚至多个相同量子态的光子。而通道存在损耗，距离越远损耗越大。假设窃听者拥有物理学原理所允许的一切能力，例如拥有无损耗或低损耗通道。窃听者可以将单光子事件全部阻隔，而在光源同时发射出两个光子的时候保留其中一个，将另一个（以无损耗或低损耗通道）发送给接收方，从而完全掌握通信双方的密钥，这就是“光子数分离攻击”。只要通道损耗达到一定程度，窃听者便不会因其实施光子数分离攻击而暴露自己的存在，因为其总可以用通道损耗掩盖自己的攻击行为。

解决办法是采用诱骗态方法，即在诱骗态协议中，Alice 随机制备多种不同光强的相位随机化的弱相干脉冲，其中一种为信号态用于产生密钥，其余的为诱骗态，Bob 可以根据探测到的各个强度相干态的统计结果的异常来判断是否存在 Eve 的窃听。

5. 如何降低实验中的错误率？

A: 可以通过使用干扰小信噪比高的通信线路，采用更加准确灵敏的 MPC，使用特性更加理想的光源和

接收器等。

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?

A: 经过单模光纤传输到接收方的偏振光，由于受到各种因素的影响，例如光纤的椭圆度、残余应力、环境震动以及温度等等，光的偏振态会发生未知的变化，因此接收方用两个 MPC，通过调节偏振反馈，来补偿光在路径传输中的偏振变化。

通过偏振反馈可以判断是否调节完毕，调节完毕时当发射 H 光时通道一应该明显大于通道二，当发射 V 光时通道二应该明显大于通道一，当发射 P 光时通道三应该明显大于通道四，当发射 N 光时通道四应该明显大于通道三。因为在调节完毕的时候偏振方向应该是和理想情况近似重合的，正交的两个基矢的计数率应该有着很大的差别。