量子密码实验系统 实验讲义

【实验概述】

在当今，信息安全的重要性是毋庸置疑的，然而当前广泛使用的经典密码学的安全性面临着巨大的挑战。与安全性基于计算复杂度高的数论难题的经典密码学不同，量子密钥分发（Quantum Key Distribution,QKD）能够提供理论上无条件安全的密码传输，其安全性由量子力学中的基本原理保证，任何窃听行为都将因引入可观测的错误而暴露，自 1984 年 IEEE 计算机科学技术大会被提出至今，QKD 备受关注，在理论和实验上都得到了充分的发展机会。

量子密码学不只是一门科学，而且是结合多领域的一门通信艺术，通过量子密码实验系统，可以让我们直观地理解 BB84 协议以及量子密钥分发，并以此为平台，展开更多的研究。

【实验目的】

1. 学习 BB84 协议以及熟悉实验中涉及到的常用仪器设备；
2. 理解量子通信中的 BB84 协议理论；
3. 观察量子通信实验中的成码率、误码率、加密解密的效果；

【实验仪器】

1. 量子信号发射器（Alice）

量子信号发射机（Alice）机箱主要由发送方主控板、光源板以及 Alice 光模板组成，主控板控制光源板的四个 850nm 的激光器随机地发出频率为 1MHz 的激光脉冲，四路激光发出的光信号是经过调制的，即发出的光是被制备好的四种偏振态，这里记为 H、V、+、-；四路光信号通过 Alice 光模块合成为 1 路光信号，我们把它称为信号光（Signal），同时主控板的激光器发出一路同步光信号，

波长为 1310nm，为信号光提供同步参考。量子发射机机箱前面板的外观如下图所示，USB 接口，以及四路光出口。

图 1 前面板部分示意图

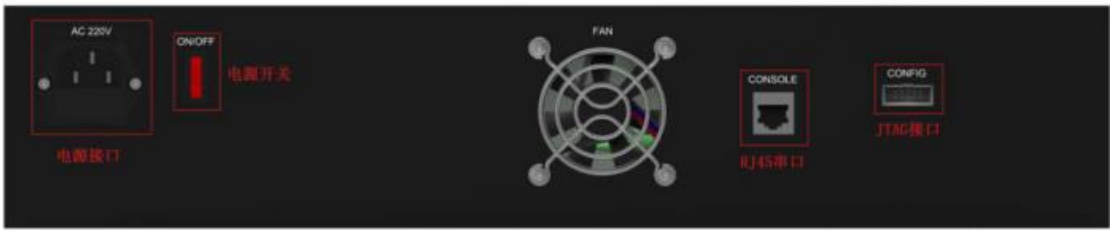

图 2 后面板示意图

量子信号发射机（Alice）和量子信号接收机（Bob）的后面板完全相同，如图所示，里面有电源接口、电源开关、RJ45 串口以及 JTAG 接口，如图标志所示。

2. 量子信号接收机（Bob）

量子信号接收机主要由接收方主控板、单光子探测器（SPD）及接收端光模块组成。主控板根据同步电信号和延时、门宽等参数，让探测器开门探测到接收的光子，单光子探测器 SPD 是利用雪崩效应探测接收端模块的光子，输出电脉冲信号给主控板处理，主控板根据同步光信号，计算同步光和信号光之间的延时，并根据设定的探测门宽来判别探测到的光子状态。量子信号接收机前面板如图所示。

图 3 前面板示意图

3. 手动偏振控制器（MPC）

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。

手动偏振控制器是由三个光纤环组成，其功能结构等效为“1/4 波片+1/2 波片+1/4 波片”（第一个环作用是将圆偏振光变成线偏振光，第二个环是将线偏振光补偿旋转一定角度，第三个环的作用是将线偏振光还原为圆偏振光），这样传输到 PBS 后，相互垂直的偏振光将和 PBS 的两个轴相吻合，从而被正确的偏振分束。

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。

4. 光纤盘及其他光纤器件

BB84 教学系统需要传输两路光信号，因此涉及到光纤光路以及相关的光学器件，例如光纤盘、法兰、分束器（BS）、偏振分束器（PBS）、衰减器（ATT）等等。可以参考下面的光路图。

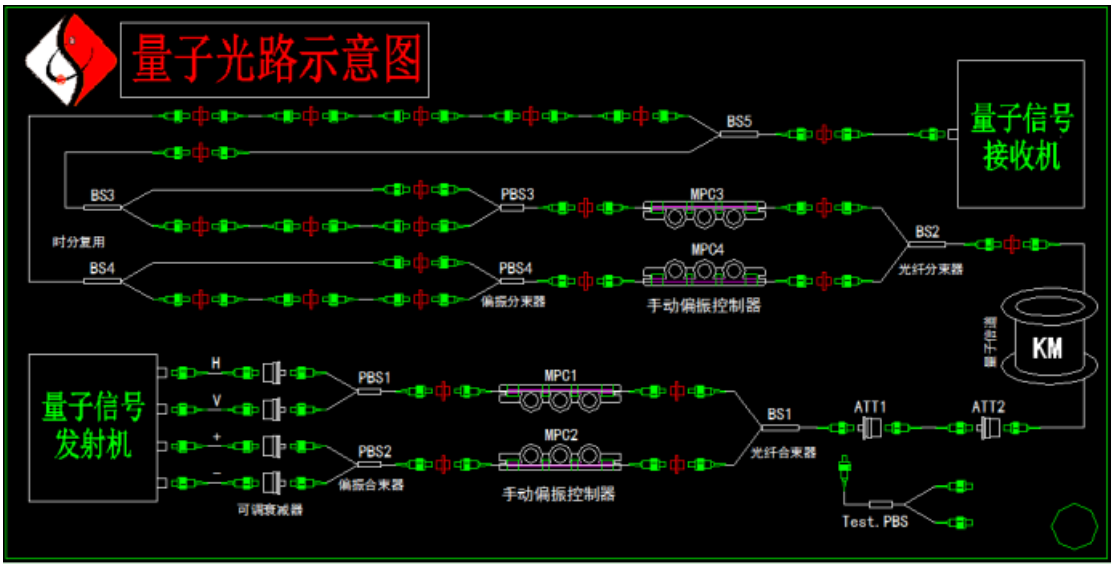

图 4 量子光路示意图

5. 计算机软件

软件分为 Alice 端和 Bob 端，主要功能有流程控制、后处理的基矢比对和纠错、密钥存储和简单的加密解密演示。软件和设备之间通过网口的链路层通信，软件两端之间通过 TCP/IP 协议通信。

【实验原理】

1. BB84 协议

BB84 协议是 Charles H. Bennett 与 Gilles Brassard 1984 年提出的描述如何利用单光子偏振态来传输信息的量子密钥分发协议，也是目前应用最广泛的量子密钥分发协议。其具体实施过程可以分为量子传输通信（quantum communication）以及经典后处理（classical postprocessing）两个过程。其中我们这个实验用的是偏振编码（还有其他的编码方式），因此以偏振编码为例来介绍 BB84 协议的具体实施过程。

量子传输通信过程

（1）量子态制备

作为发送方，Alice 分别随机从两个基矢{Z，X}中及经典编码集{0,1}中各选择一个，按照编码表利用单光子源进行制备，将制备好的单光子态通过量子信道发送给接收方 Bob。

基矢	经典比特	量子态	描述
Z	0	$\|H\rangle$	水平偏振态
Z	1	$\|V\rangle$	垂直偏振态
X	0	$\|+\rangle$	+45° 偏振态，$\frac{1}{\sqrt{2}}(\|H\rangle+\|V\rangle)$
X	1	$\|-\rangle$	−45° 偏振态，$\frac{1}{\sqrt{2}}(\|H\rangle-\|V\rangle)$

图 5 BB84 协议编码表

（2）量子态测量

作为接收方，Bob 随机从两个基矢{Z，X}中选择一个对 Alice 发送过来的单光子态进行测量。若 Bob 选择的基矢和 Alice 制备基矢一致，则 Bob 测量所得的量子态所对应的经典比特值与 Alice 制备的一致，否则 Bob 的测量结果将是随机的。重复上述步骤，直到完成足够的量子态制备和测量后，Alice 和 Bob 各自拥有经典比特序列，称之为原始密钥（Raw Key）。

（3）基矢比对

当上述量子信道传输完成后，Bob 通过经典信道（经过认证）告知 Alice 他测

量单光子态时所使用的基矢以及他测量是否得到有效的响应。Alice 向 Bob 公布她所使用的的基矢。Alice 和 Bob 抛弃掉无测量响应位置的单光子态及制备与测量时使用不同基矢的单光子态，如果制备与测量都是完美的，且没有窃听者 Eve 对单光子态进行窃听干扰，Alice 和 Bob 此时将得到完全一样的比特值序列。我们称之为筛后密钥（Sifed Key）。

经典后处理过程

由于信道干扰、制备不完美、测量噪声、窃听者攻击等因素存在，需要对筛后密钥进行经典后处理，才能获得完全相同且安全的最终密钥（Final Key），即安全密钥（Secret Key）。这里经典后处理通常包括误码率估计、比特纠错、隐私放大三个步骤。

（1）误码率估计：Alice 和 Bob 经过协商后随机选择筛后密钥的一部分比特进行抽样比对，并计算错误率。若错误率低于设定值，则剩余的密钥继续做后处理，否则中止本次密钥传输。

（2）比特纠错。为了获得完全相同的密钥，Alice 和 Bob 需要利用纠错算法对剩余的筛后密钥进行纠错，该步骤可以保证在泄露信息尽量小的前提下，Alice 和 Bob 所拥有的密钥产生的错误的概率足够小，即此时 Alice 和 Bob 已经拥有完全相同的密钥。

（3）隐私放大。Alice 和 Bob 通过一定隐私放大算法压缩原始密钥，保证压缩后的密钥被 Eve 获取信息足够小，最终形成安全密钥（Secret Key）。

【实验步骤】

1. 硬件连接

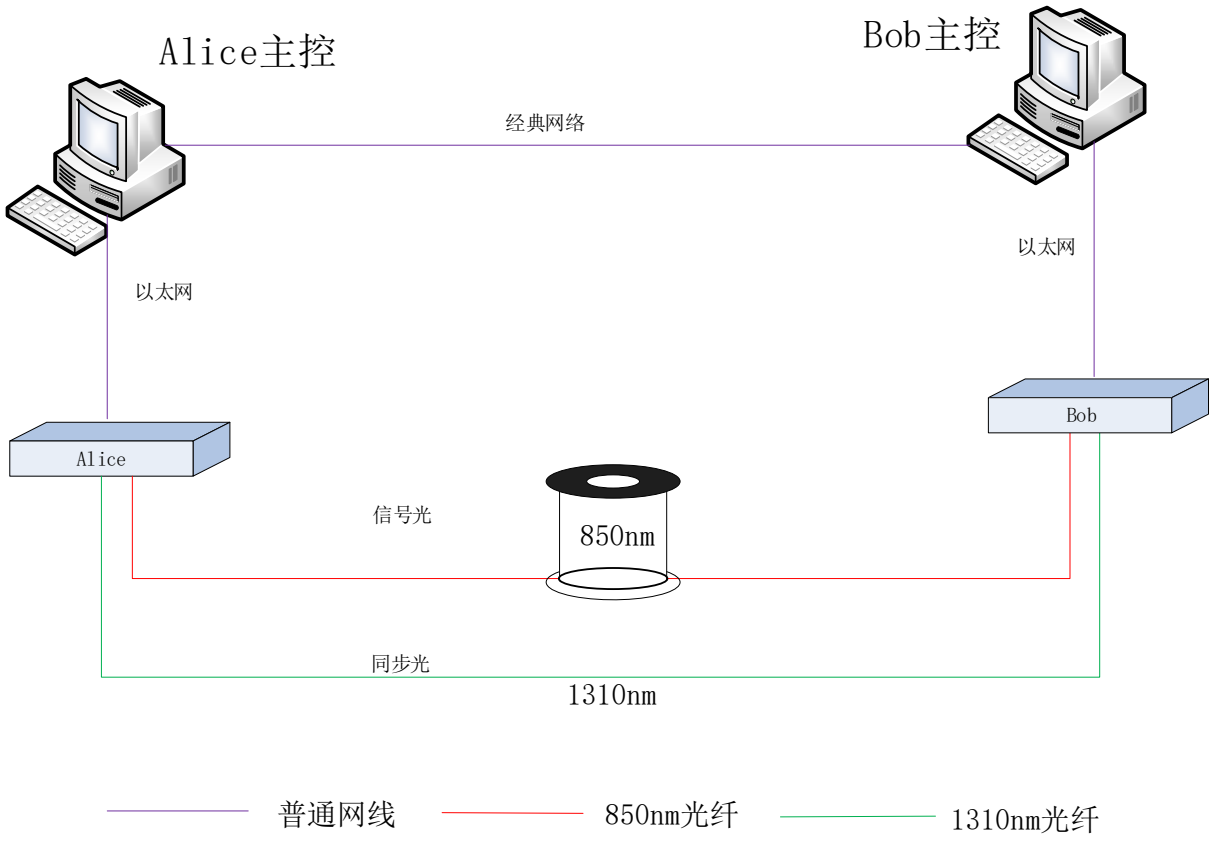

图 6 设备连接图

注意：

1. 设备和主机之间的以太网链路层通信通过 MAC 地址进行。

2. 设备连接后，需要对两台主机电脑互联的外置 USB 网络适配器配置 IP 地址，该地址在软件配置中作为对端地址，即 Alice 端软件配置 Bob 的主机 IP 地址，Bob 端软件配置 Alice 主机的 IP 地址，两端的地址必须要在同一个网段。IP 地址配置完成后可以用 PING 命令检测连通性。连接设备的网络适配器不需要配置 IP 地址。

3. 注意检查光路是否连接好；

2. 软件配置

2.1 启动配置窗口

软件启动后首先要进行配置，配置的参数包括选择设备的类型，配置设备的地址、对端的地址等。第一次运行如果没有配置文件则默认会先打开配置窗口，也可以在软件启动后通过菜单栏中设备→设置，或者工具栏的设置按钮打开配置窗口：

图 7 打开配置窗口

2.2 配置说明

打开配置窗口后，界面如图 8 ，配置项总体分为设备配置、对端地址配置和密钥管理的配置，说明如下：

设备类型：根据连接的设备，指定软件连接的设备类型为 Alice 还是 Bob。

地址类型：连接设备的地址类型，目前仅支持以太网连接设备。

适配器：以太网适配器，该适配器为运行软件的主机连接到设备所使用的以太网适配器，不是外置 USB 网络适配器。如果选择不正确则无法与设备通信。

设备地址：连接设备的以太网 MAC 地址，默认为 ee-11-22-33-44-50，一般不需要修改。

控制协议：与设备进行通信时，控制命令所使用的协议号，默认为 0xfffd，一般不需要修改。

数据协议：与设备进行通信时，数据上传所使用的协议号，默认为 0xfffe，一般不需要修改。

对端地址：运行对端软件的外置 USB 网卡的 IP 地址。

各模块的地址配置：对端地址为连接到对端的 IP 端口，要与对端软件的对应配置保持一致，数据上传地址为自己各模块上传的地址，不重复即可。

密钥管理：密钥的存储路径，该密钥存储路径为安装包中“key”文件夹，存储路径应避免包含汉字，否则容易出现密钥不存储的现象。

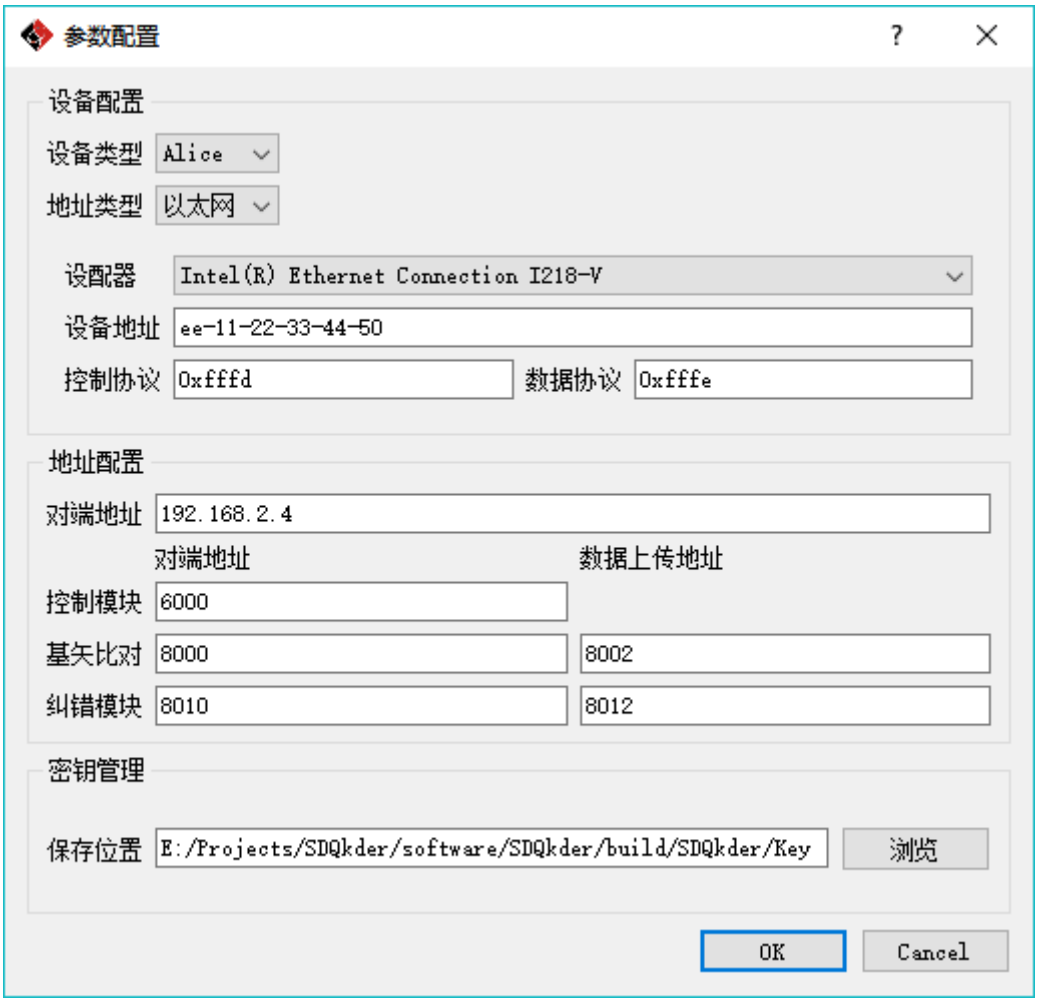

图 8 配置窗口

配置完成后点击确认保存。

注：设备启动后修改配置必须重启软件才能生效。

3. 软件操作

3.1 启动设备

使用菜单栏的设备→启动设备，或者工具栏的启动设备按钮启动设备：

图 9 启动设备

设备启动后设备状态会显示自检状态，设备版本，对端状态以及每个模块时候与对端连接成功，日志窗口会打印相关日志。

图 10 设备启动状态

3.2 同步校准

量子信号发射机主控板以 1MHz 频率(周期 1us)发出两路电脉冲信号,一路驱动激光器发随机光,一路输出为同步电信号。因此在接收方一个同步电信号后面必然有一个对应的单光子信号脉冲。但是由于同步光和信号光走的光路不同，因此电信号和单光子信号有一定的延时差，（信号光要比同步光更晚到达探测器）因此需要调节探测器以校准延时。

该软件自动同步校准启动后由设备自动执行，完成后返回每个通道的延时。

延时参数说明：

角偏移量：单位为 1us，是延时的周期数。

延时：单位为 10ns，为一个周期内的延时值。

门宽：单位为 10ns，为探测信号的门宽。

实际的延时计算为角偏移量 * 1000 + 延时值 * 10，单位为 ns。该延时值反应的是同步光达到后，信号光经过多长时间到达。

3.3 自动同步校准及偏振反馈

自动同步校准在 Bob 端启动,启动方式为点击 Bob 端延时设置中的启动同步校准按钮，启动后设备进入同步校准状态，在同步校准状态下不允许设备门宽和延时。

图 11 启动自动同步校准

启动后可以通过点击停止同步校准来终止正在执行的同步校准：

图 12 停止自动同步校准

同步校准执行成功后会自动停止，并显示上传的延时值，自动同步校准不会修改门宽，默认的门宽为 1。

图 13 同步校准结束

同步校准完成后，探测器已经可以探测到正确的信号，需要进行偏振反馈来

补偿链路中的偏振变化。

执行偏振反馈的步骤如下：

1.在 Bob 端启动偏振反馈。

图 14 启动偏振反馈

2. 发 H 光，观察探测器的计数，手动调节 H/V 的偏振控制器（MPC），使 H 的计数达到最大，V 的计数最小，调节到比值大于 20:1 可以满足基矢比对的要求。调节 MPC 时，可以先从调节一个找到最大值，再调另外一个，如此反复，直到找到最佳值。

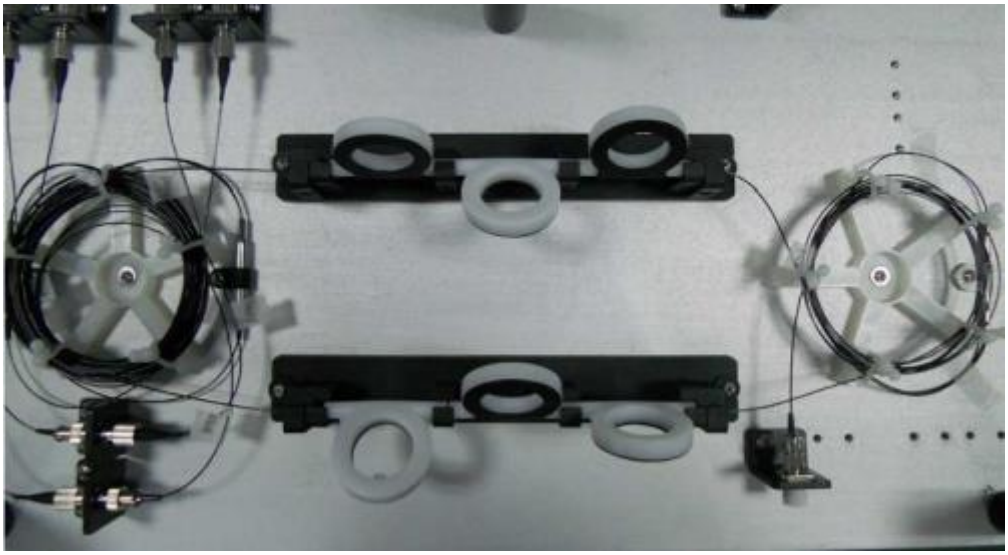

图 15 偏振控制器

3.发 V 光，观察探测器计数，此时 V 的计数应该最大，H 最小，V 比 H 的比值应该大于 20:1，如果不满足，则再微调 H/V 的偏振控制器，找到一个最大值，再返回到第二部看看结果。

图 16 偏振反馈发光控制

4. 切换到 P、N 光，重复第二步和第三步。

5. 停止发光，停止偏振反馈。

图 17 停止发光、停止偏振反馈

4. 基矢比对

在 Alice 端启动基矢比对，启动后设备进入基矢比对状态，上传发光数据和探测数据，软件接收到数据后进行基矢比对和纠错，最后保存纠错成功的密钥。比对过程中，软件会显示每秒处理比对数据的速率，比对后密钥的错误率，和成码率，以及保存密钥的密钥量。基矢比对的界面如图 18。

基矢比对结束后使用停止基矢比对结束基矢比对状态。

图 18 基失比对

5. 量子密钥应用演示

该软件提供量子密钥应用演示功能，主要包括聊天、TXT 文件传输、BMP 图片传输三个功能演示，如下图：

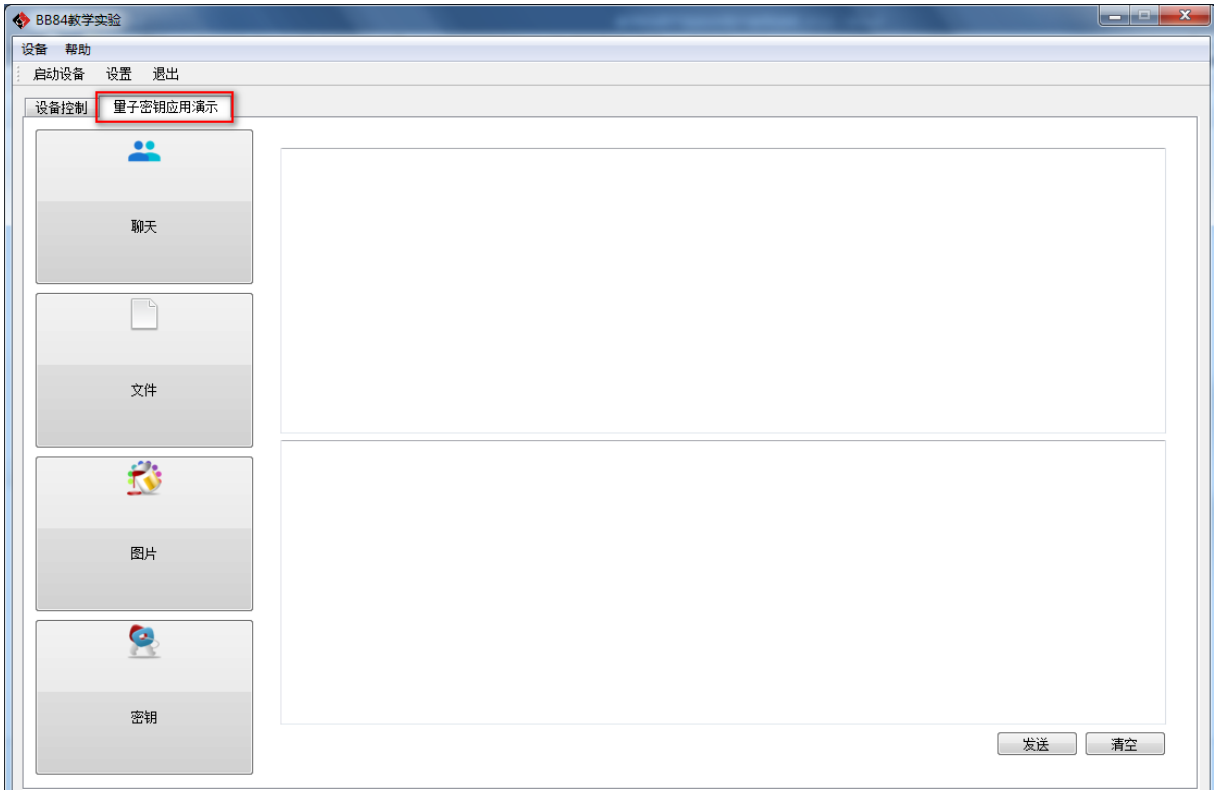

图 19 量子密钥应用演示界面

Alice 和 Bob 软件界面，选择一端作为发送端，另一端作为接收端；

1. 点击相应的功能按钮，会显示相应的功能演示界面；
2. 若选择不加密传输，则发送端无需点击加密勾选框，接收端无需（也不可以）点击解密勾选框；
3. 若选择加密传输，发送端需点击加密勾选框，接收端可选择是否解密显示，
4. 点击解密勾选框，则接收端界面会显示解密后的数据，可以正常显示；若不选择解密勾选框，则接收端界面会显示加密后的数据，文档打开后是乱码，图片无法显示，聊天信息也是乱码；

注意：发送端（或接收端）不可以同时勾选加密和解密。

1.聊天功能演示，界面如下：

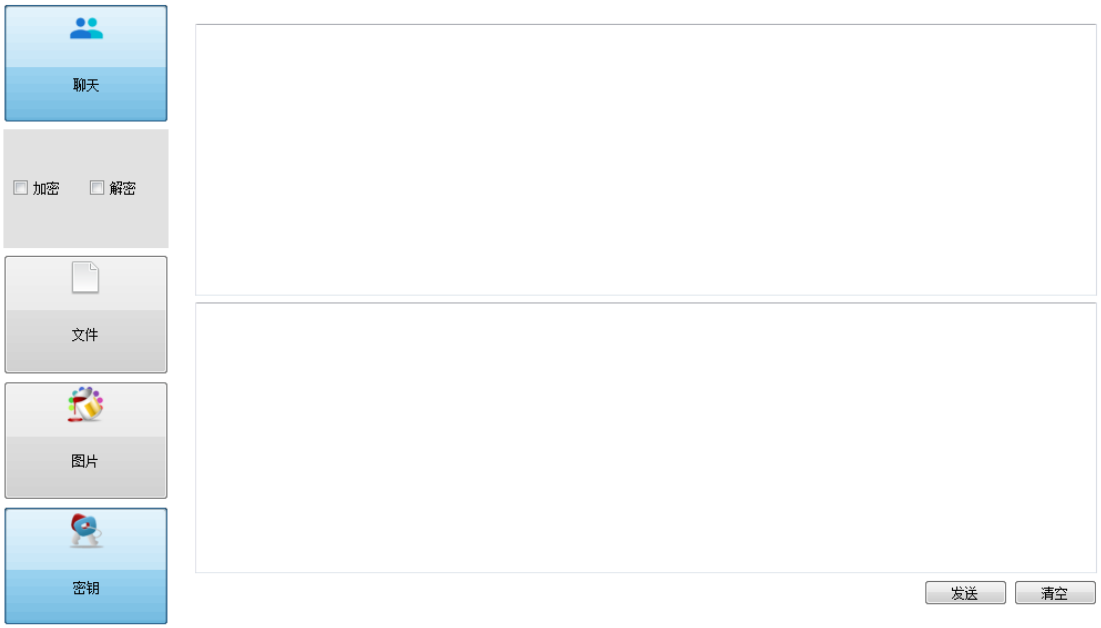

图 20 聊天功能演示界面

在聊天界面下方的窗体，输入需要发送的信息，点击发送，发送的时间和信息即可会显示在发送端和接收端的上方窗体中，清空按钮可清空界面窗体中的信息。

2.文件传输功能演示，界面如下：

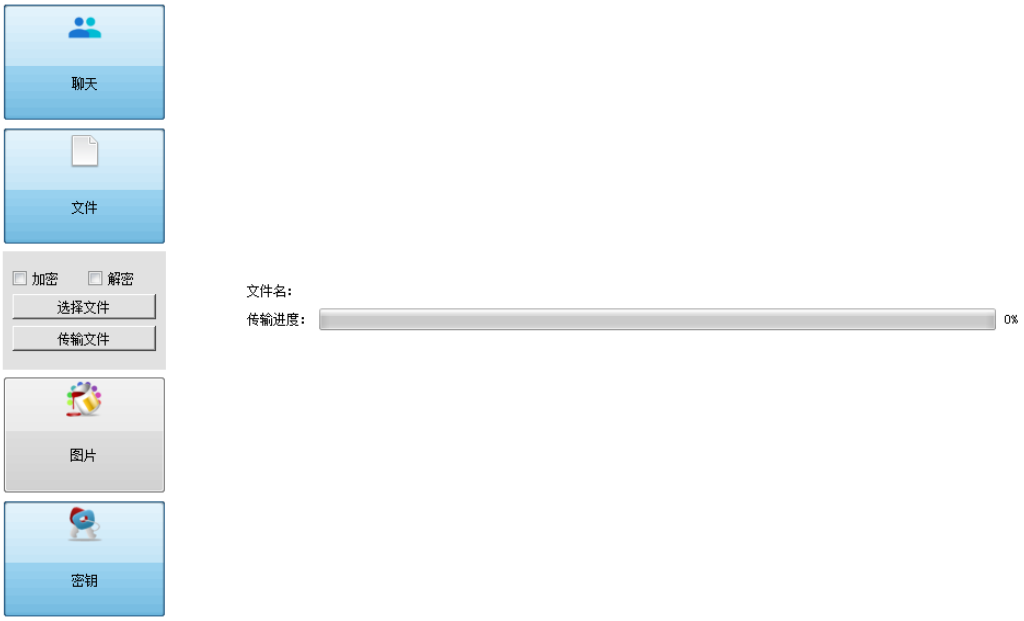

图 21 TXT 文件传输功能演示界面

点击选择文件，在可执行文件相同的目录下，选择“textfile”文件，选择完成，文件名显示在界面上，选择是否加解密传输，在发送端和接收端分别显示

文件的发送和接收进度，文档会保存在安装文件目录下；两端可通过文件的生成日期来区分传输的文件。

3. 图片传输功能演示，界面如下：

图 22 BMP 图片传输功能演示界面

点击选择图片，在可执行文件相同的目录下，找到 BMP 图片或图片文件，图片选择完成，图片显示在界面上，选择是否加解密传输，在接收端显示图片。

1、密钥应用界面

图 23 密钥应用界面

密钥应用界面，会显示密钥存储总量和演示已消耗的密钥量，并打印了相关的功能演示信息，选择加解密传输数据，如果两端的密钥不一致，则传输的数据对端无法解密显示。

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？

2、量子不可克隆定理是什么？

3、实验中所使用的光源是单光子源还是其它什么光源？

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）

5、如何降低实验中的错误率？

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？