

量子密钥分发

【关于实验报告的注意事项】

1. 实验前完成预习报告；
2. 实验前独立完成“实验前预习思考题”；
3. 实验后完成“实验后思考题”；
4. 实验后完成一份完整的实验报告。

注：所有的作业可以小组讨论，但每位同学需要独立完成撰写及表述。对于共同完成的内容，需清楚说明或标记每位同学的贡献。

【实验安全注意事项】

1. 系统工作温度在 $15^{\circ} \sim 30^{\circ}$ 的环境中，尤其避免过高温度下使用本系统。
2. 实验元件会单独给出，实验前检查是否完整。除给出的元件外，整体密钥分发系统不要触碰。
3. 镜筒等光机械安装时，螺丝拧紧避免晃动。光机械元件的调节旋钮，安装前，将螺丝行程旋至中间位置，方便实验过程中调节。
4. 所有镜片避免用手接触光学面，拿捏过程中，光学面垂直于平台，避免灰尘，使用完收入对应的盒子中。安装镜片需靠近台面，避免镜片跌落摔碎。
5. 请不要打开单光子探测器的黑色遮盖物。
6. 不要使眼睛与光路处于同一水平面，不要用手直接接触激光，激光为 30mw 紫外激光，必须戴好护目镜。

【实验目的】

掌握制备、控制以及测量单光子态的基本原理。了解量子密钥分发的物理原理及其安全性基础。通过四个实验的学习，达成如下学习目标：

1. 掌握控制和测量光子的偏振；
2. 掌握单光子的标定；
3. 掌握单光子的探测及相应探测器效率的测量；
4. 掌握 BB84 量子密钥分发过程的数据处理。

【实验前预习思考题】

****上课前提交预习报告时完成下列思考题**

- 1、回顾偏振光实验，说明 $\lambda/2$ 波片， $\lambda/4$ 波片的工作原理；
- 2、如何检测一个任意方向的线偏振光？
- 3、单光子为什么不能直接用普通功率计测量？

- 4、检验单光子探测器的探测效率可以用强光吗？
- 5、BB84 协议的原理和步骤。
- 6、密钥分发过程中，为什么需要有同步信号？

【实验后思考题】

****课后提交实验报告时完成下列思考题**

- 1、是否可以通过直接衰减任意的光源（比如白炽灯）的强度到单光子级别来得到真正的单光子源？（真正的单光子源是指每次触发可以确定性的得到一个仅包含一个光子的光脉冲信号）。
- 2、了解单光子探测器暗计数的原理，并设计实验装置测量探测器的暗计数率。
- 3、量子密钥分发实验中对基后的数据，为什么会有误码出现，如何降低误码？

【仪器用具】

表 1- 1 偏振测量实验

编号	仪器用具名称	数量	主要参数（型号，规格等）
1	准直激光器		波长：404nm，最大功率：150mW
2	偏振分光棱镜	2	波长：404nm，消光比>500
3	半波片	2	波长：404nm，零级
4	小型磁性底座		MB105
5	PH 系列杆架	6	PH102
6	SP 系列接杆	6	SP104
7	激光器镜架	6	OM311
8	精密棱镜台	2	PPM101
9	偏光镜架	2	PM101
10	可见光功率计	2	PM100、S120VC
11	直流稳压电源	1	GPD-3303D

表 1- 2 单光子标定的用具

编号	仪器用具名称	数量	主要参数（型号，规格等）
1	密钥分发系统	1	波长：404nm
2	可见光功率计	1	PM100、S120VC

表 1- 3 单光子的探测及相应探测器探测效率测量的用具

编号	仪器用具名称	数量	主要参数（型号，规格等）
1	反射镜	1	波长：404nm，45 度入射
2	滤波片	1	波长：405nm，带宽：3nm
3	光纤准直器	1	F671FC-405
4	反射镜折叠架	1	OM402
5	透镜固定架	1	LH102
6	光纤耦合架	1	PFC201
7	小型磁性底座	3	MB105
8	PH 系列杆架	3	PH102
9	SP 系列接杆	1	SP104
10	SP 系列接杆	2	SP134
11	可见光功率计	1	PM100、S120VC
12	密钥分发系统	1	波长：404nm

表 1- 4 密钥分发过程数据处理的用具

编号	仪器用具名称	数量	主要参数（型号，规格等）
1	密钥分发系统	1	波长：404nm

【量子密钥分发原理】

1 保密通信简介

随着计算机科学技术日新月异的发展，经典密码系统的安全性越来越受到挑战。经典密码体制主要包括对称密钥体制和非对称密钥体制两大类。对称密钥密码体制最主要的问题是如何进行两端的密钥分发管理，最优秀的算法，如果密钥在分发时泄露，则整个安全体系毁于一旦；而公钥密码则有效的避免了密钥分发管理的难题。公钥密码算法都是基于一些复杂的数学难题，例如广泛使用的 RSA 算法就是基于大整数因子分解这一著名的数学难题。所以，公钥密码的安全性始终无法得到严格意义上的数学证明，而只能依赖于不可靠的计算复杂性。例如：600 台计算机需要花费 17 年时间才能质因数分解一个 129 位的阿拉伯数字。而随着计算机技术的不断发展，特别是量子计算机的不断研究，研究表明如果使用一个 2000 个量子比特的量子计算机，只需要 1 秒钟就可以破解成功。所以量子计算给经典密码带来了巨大的威胁。

量子密钥分发完美的解决经典密码体系中密钥安全分发的安全问题。量子密钥分发的安全性不是通过算法的复杂性保证的，而是基于量子力学的物理定律保证的，分别是测量塌缩理论、海森堡不确定原理、量子不可克隆定律；然而上述定律保证量子密钥分发安全性的基础是单光子量子态的传输。例如：A 和 B 通过单光子量子态的编码、传输、解码、探测、后处理等

过程，A 和 B 可以得到对称的安全密钥，再通过一次一密加密技术实现信息论条件下的信息安全传输。

1.1 经典保密通信

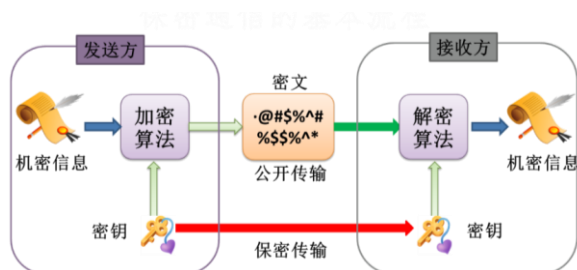


图 1：保密通信流程图

上图给出了保密通信的一般性流程图。保密通信分为加密、传输、解密 3 个过程：发送者将需要发送的机密信息通过某种加密机制（密钥+加密算法）转化为密文；接收方接收到密文后采用和发送方匹配的解密机制（密钥+解密算法）对密文进行解密，从而得到所传递的机密信息。

在保密通信过程中，密钥和解密算法（一般来说，加密算法和解密算法都是匹配一致的）是保证信息安全的關鍵。在安全性证明中，一般认为解密算法是公开的。因此，保密通信中信息的安全完全取决于密钥的安全和解密算法的复杂性。根据发送方和接收方密钥是否对称一致，现代密码体制可以分为公钥体制（也称为对称密码体制）和私钥体制（也称为非对称密码体制）。

（1）公钥密码体制：在该密码体制中，接收方的密钥分为私钥（自己保存的密钥）和公钥（公开发布的密钥）两部分。发送方采用接收方的公钥来加密信息，然后将信息传输给接收方，接收方收到信息后再采用自己的私钥进行解密操作，从而获取信息。根据上面的描述可以看出，要在公钥密码体制中保证信息的安全，就必须保证窃听者无法通过接收方公开的公钥推算出私钥，而这一点可以通过数学上的单向函数来解决。所谓单向函数是指，从条件 A 推算出条件 B 很容易，但从条件 B 推算出条件 A 的难度会随着 B 的长度呈指数级增加。比如，目前广泛用于网络、金融行业的 RSA 加密算法就是基于数学上大数质因子分解的难题来设计的。

虽然数学上的单向函数能够在一定程度上保证公钥密码体制的安全性，但从理论上讲其安全性对计算机的能力具有明显的依赖。特别是，1994 年 Peter Shor 提出，如果能够构建量子计算机，那么就可以在多项式时间内完成大数质因子的分解，从而使得公钥密码体制的安全性受到严重威胁。

（2）私钥密码体制：在该密码体制中，发送方和接收方事先共享了完全相同的密钥。发送方用这个密钥加密信息，然后将密文传输给接收方，而接收方则采用相同的密钥来解密信息。因此，私钥密码体制的安全性完全取决于密钥的安全性和解密算法的复杂性。不过，

幸运的是,Shannon 在 1954 年从信息论上证明了一种称为“一次一密(One-time pad,OPT)”的加解密方法,利用该加解密方法后仅需要保证密钥的安全性就可以保证信息的安全性。换言之,在 OPT 加解密算法下,密钥的安全性是决定信息安全的唯一因素。OPT 的具体方法如下:密钥具有完全的随机性;密钥的长度和需要传递的信息长度一致;密钥仅使用一次。可以看出,虽然 OPT 方法可以保证信息的安全,但其对密钥量具有较高的要求,因此无法满足日常实际应用的要求。

1.2 量子密钥分发及 BB84 协议

量子密钥分发(Quantum key distribution, QKD)是一种利用量子力学基本原理来进行密钥分发的方法,其主要目的是解决 OPT 加密方法中密钥高速、安全、实时分发这一关键问题。和传统的经典密钥分发协议相比较,QKD 的最大优势在于,利用了量子力学的基本原理后,任何针对密钥的窃听行为都会扰乱传递密钥的量子状态,从而留下痕迹被合法通信双方发现。换言之,QKD 提供了一种信息论安全(information-theoretical security),或称无条件安全(unconditional security)的密钥分发技术。

早在 1969 年,哥伦比亚大学的 Stephen Wiesner 就基于量子态的特性提出了“不可伪造的电子钞票”的概念,其中就蕴含了 QKD 的基本思想,但由于该思想过于新奇,而且在当时的技术条件下根本无法实现,所以一直没有引起大家的关注,文章也直到 1983 年才得以发表。随后,受 Wiesner 思想的启发,C.H. Bennett 和 G. Brassard 指出可以利用量子态的特性来解决密码学中的密钥安全分发问题,并于 1984 年提出了第一个 QKD 协议,即现在被广泛使用的 BB84 协议。

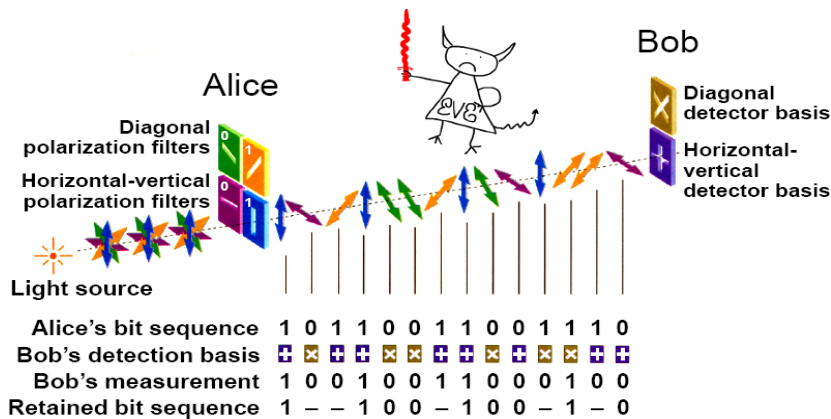


图 2: 偏振编码 BB84 协议流程图

BB84 协议采用粒子(包括光子、原子、粒子、电子等均可)作为量子态的编码载体,但对于通信而言,光子在传输速度、抗环境噪声等方面具有天然的优势,因此我们采用光子的偏振为例来简要说明 BB84 协议的工作原理(如图 2 所示)。

Step1: 发送方 Alice 和接收方 Bob 约定如下的编码规则

批注 [zz1]: This is very long. Shorten a bit. Plus BB84 belongs to (2). This should be said somewhere.

批注 [豌豆让2R1]: This part introduced the classic secret communication, it is the background knowledge which can help student to know why we now want to study quantum communication. I think shorten some sentence will influence the completeness. Below has the introduction of BB84.

表 1: Alice 和 Bob 编码规则，其中 \oplus 称为水平基， \otimes 称为对角基。

制备-测量基 \ 比特	0	1
\oplus	竖直偏振 (H)	水平偏振 (V)
\otimes	右旋偏振 (R)	左旋偏振 (L)

- Step2: Alice 采用偏振控制器随机的将光子的偏振状态制备为 H、V、R、L 之一，并通过窃听者控制的信道传输给 Bob。
- Step3: Bob 接收到 Alice 的光子后，随机采用水平基 (\oplus) 或者对角基 (\otimes) 进行测量，并记录测量结果。由于信道损耗的存在，Alice 发送的单光子仅能以一定的概率到达 Bob 的接收装置 (单光子探测器)，因此 Alice 和 Bob 仅记录保留 Bob 探测到信号时的数据比特信息。
- Step4: Alice 和 Bob 从记录的 N 个数据比特中随机选取 m 个比特并估计数据的比特错误率 (quantum bit error rate, QBER)。如果 QBER 大于给定的阈值，则 Alice 和 Bob 放弃此次通信，并重新返回 Step2；如果 QBER 小于给定的阈值，则 Alice 和 Bob 进入 Step5。。
- Step5: Alice 和 Bob 对剩余的 $N-m$ 个比特数据进行纠错和私密放大处理，进而提取出无条件安全的密钥。纠错的目的是保证 Alice 和 Bob 的密钥的一致性；私密放大的目的是擦除窃听者的信息，保证密钥的私密性。

BB84 协议提出后，众多研究者对其安全性进行了证明，但由于详细的数学证明过程比较复杂，在此不进行详细说明，感兴趣的同学可以参考文献【3-5】。不过，QKD 的安全性基础主要包括以下基本思想：

- (1) 单光子是光场的最小能量单元，具有不可分割性；
- (2) 单光子量子态具有不可克隆性，即无法通过一次测量 100% 准确的单光子的偏振状态；
- (3) 单光子偏振状态的测量结果具有概率性，即仅当量子态处于测量算子的本征态时，测量者才能 100% 的得到精确的测量结果。

1.3 基于 BB84 协议的 QKD 实验

我们利用 BB84 协议来进行 QKD 的演示，其光路图和实验步骤如下所示。

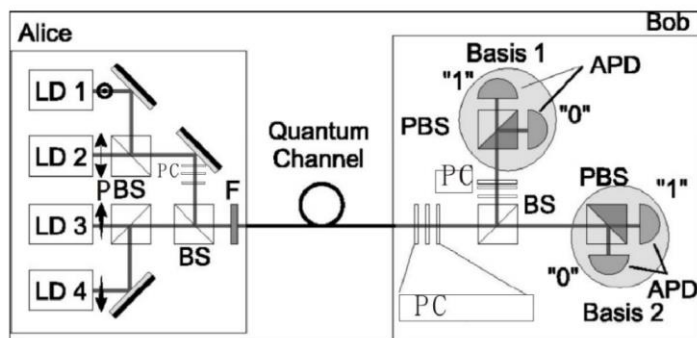


图 3. BB84 协议 QKD 实验光路示意图

实验步骤

发送方：采用 4 个激光二极管，并分别将每个激光二极管的输出光信号的偏振制备为 H、V、R、L。然后通过两个偏振分束器（PBS）和一个分束器（BS）将四个激光二极管的输出光信号耦合到一个统一的输出信道上。发送方采用一个光衰减器将光信号的强度衰减到单光子水平（平均光子数约为 0.1~0.5 左右）。实验中，发送方随机的触发四个激光二极管中的一个发光，从而保证每次随机的发送一个偏振量子态。

接收方：接收方采用一个 BS 来随机选择测量基。经 BS 透射的光信号经过一个 PBS，从而完成对 H/V 偏振的测量。经 BS 反射的光信号，先经过一个偏振控制器（偏振旋转波片），然后再经过一个 PBS，从而完成对 R/L 偏振的测量。

【实验原理及步骤】

针对量子密钥分发所涉及的基本原理，本实验设计了四个实验：（1）通过实验一掌握制备、控制和测量想要的光子偏振。（2）通过设计单光子的标定实验，光子的探测及相应探测器效率的测量实验，研究单光子的近似制备，掌握单光子的测量方法。（3）通过设计量子密钥分发的数据处理实验，掌握量子密钥分发过程的基本原理和流程。

实验 1：光的偏振的测量和控制

在这个实验中。我们回顾如何使用半波片和偏振分束器（PBS）来控制和分析从二极管激光器发出的光子的偏振。

1.1 实验原理

偏振分光棱镜（PBS）：分光棱镜根据光的偏振态进行分光，当一束光垂直入射面入射，水平分量的光将会透射，垂直分量的光将会反射；即透射端口为水平偏振光，反射端口为垂直透射光。不考虑光子间的关联，单个光子的偏振态宏观表现为光束的偏振。

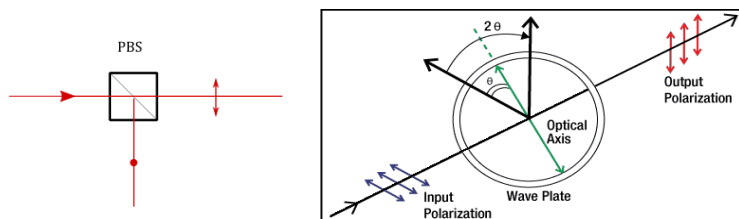


图 1-1 PBS 和半波片原理图

例如，量子密钥分发过程中，光子的量子态 D 宏观表现为一个与水平面呈 45° 夹角的线偏振光。实验上可以利用一个起偏元件，例如偏振分光棱镜的透射端来产生一个水平偏振的光，然后利用半波片旋转 θ 角来制备一个偏振方向为 2θ 的线偏振光。那么对于 45° 偏振光的制备，半波片需要旋转 22.5° 。此时，如果通过一个偏振分光棱镜后，在透射端和反射端探测功率，得到的比值为 $0.5:0.5$ ；如果先放置一个 22.5° 的半波片再在偏振分光棱镜后检测，根据图 1 所示，则得到反射端口功率为 0。上述两种现象，只有后者可以作为检测 45° 偏振光的方法，为什么？因为前者没有考虑水平偏振和竖直偏振方向之间的夹角，例如，输入一个左旋光或右旋光一样得到前者现象。

得到检测偏振态的方法后，我们就接着探究是否可以通过将水平偏振光与竖直偏振光按 $0.5:0.5$ 的比例混合得到 45° 偏振光。

1.2 实验内容及步骤

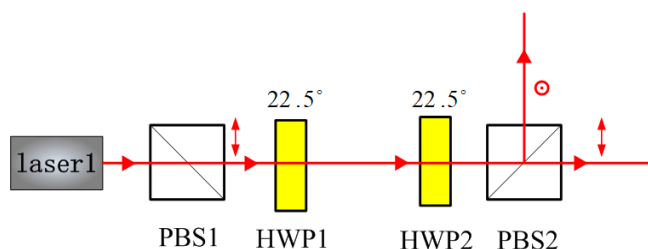


图 1-2 偏振控制和探测示意图

注意：实验一使用的是光学平台透明罩外的激光器和相关实验器材。在使用该激光器时注意不要超过它的最大工作电压和最大工作电流，最大工作电压为： $5V$ ；最大工作电流为： $60mA$ 。

- 1) 以激光器出射光高度为基准，安装光学元件，使光束从轴心位置通过；
- 2) 在激光器后放置 PBS1，PBS1 要与激光光束相垂直，之后测量激光通过 PBS1 后的反射和透射功率，记下数值（附录 1）。假设激光器发出的光是线偏振光，求激光器发出的线偏振光与水平方向的夹角是多少？
- 3) 在激光器和 PBS1 之间放置半波片 1 (HWP1)，转动半波片 1 的角度找到透过 PBS1 的光功率的最大值和最小值并记录下来，并通过测量推倒该激光器是否完美的线偏振

光？

- 4) 在激光器后依次放置 PBS1, HWP1 和 PBS2。转动半波片 1 的角度 360 度，记下转动不同角度时，PBS2 出射端的功率变化，确定出光功率最大或最小时刻的镜架的刻度，此时的刻度即 HWP1 为的 0° 光轴（半波片光轴对应角度）。此步骤一定要注意半波片的光轴和镜架的 0 刻度不一定重合，所以需要通过实验测试确定半波片的光轴。
- 5) 使用上述图 1-2 的实验装置，将 HWP1 的角度调至光轴位置来制备偏振态 D（或与态 D 垂直的态）。转动 HWP2，记录透过 PBS2 的光功率随着 HWP2 角度的变化。HWP2 应该位于什么位置才可以确定地测量 PBS2 之前的光确实在 D 态(或垂直于 D 态)

1.3 实验数据记录及处理

表格格式见附录表一：偏振控制和探测实验记录表格。

实验 2：单光子的探测及相应探测器效率的测量

在下面的实验中，我们提出测量光电倍增管（PMT）的效率，因此，需要在激光到达光电倍增管之前将光束衰减至单光子水平。

2.1 实验原理

光子计数是一种测量极弱光的检测方法，具有计数稳定性高、抗干扰能力强、低噪声、高探测效率等特点，应用于弱光精密测量分析领域，在生物、医学、化学等各个领域的发光分析技术中已经得到普遍应用¹。

微弱光通过探头前端面窗口入射到光电倍增管的光电面，激发出电子，经电子倍增后被阳极收集，由阳极输出一个电流脉冲，再由放大器转换为电压脉冲并放大，经甄别、成形后转换为一个具有固定脉冲幅度和宽度的电压脉冲输出，光电倍增管工作原理如图 2-1 所示。

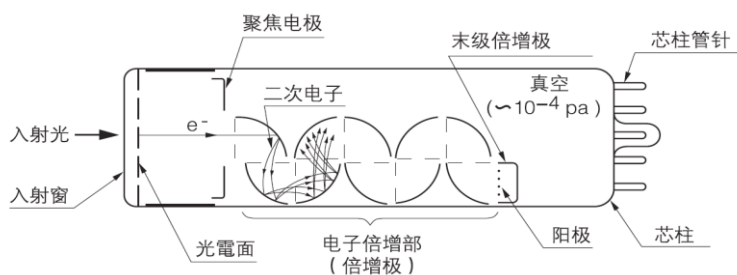


图 2-1 光电倍增管（PMT）原理示意图

¹ 目前的单光子探测技术主要有光电倍增管、雪崩二极管、超导单光子探测三种探测器。在本实验中，主要采用光电倍增管来进行单光子探测。

单个 404nm 光子的能量为：

$$E = h\nu = \frac{hc}{\lambda} = 6.626 \times 10^{-34} \times 3 \times \frac{10^8}{404 \times 10^{-9}} = 4.92 \times 10^{-19} \text{J}$$

上式中， h 为普朗克常量， c 为光速， λ 为光波长。

由于我们采用的 404nm 激光器的发光重复频率为 10MHz，因此，当计算每个脉冲平均光子数为 0.1 个光子时出口需要的功率时

$$P = \mu \times f \times E = 0.1 \times 10 \times 10^6 \times 4.92 \times 10^{-19} = 4.92 \times 10^{-13} \text{W}$$

上式中， μ 为平均光子数脉冲， f 为光触发频率， P 即为光功率。设脉冲激光器发光功率为 P_0 ，则从激光发光出口处所加衰减值为

$$10 \log \frac{P_0}{P} = ?$$

时，单光子制备完成。例如：激光器发光功率测量结果为 $20 \mu\text{W}$ ，则所加衰减值为：

$$10 \log \frac{20 \times 10^{-6}}{4.92 \times 10^{-13}} = 76.1 \text{dB};$$

即在脉冲激光器出口处加衰减 76.1dB，便可得到平均光子数为 0.1 个光子/脉冲的激光。此时将单光子探测器直接放在出口处接收，通过空间偏振 QKD 系统可以得到单光子探测器的扫描计数 N ；则：

$$N = f \times \mu \times \eta$$

式中 η 为单光子探测器的探测效率；由于 f 、 μ 、 N 已知， η 则可计算出。

2.2 实验内容及步骤

在这个实验中，我们使用透明保护箱里面的实验装置。

整个实验过程中我们不需要触碰箱子里面的光学元件。实验装置图如图 2-2 所示。本实验只需要使用 M 路激光器， M 路激光经过强衰减后，在到达光纤耦合器（OC-M）时光功率已经足够小，之后通过光纤进入单光子探测器（SPD-M）。

光电倍增管（PMT）被封闭在一个盒子里，以避免任何杂散的光进入光电倍增管。千万不要打开 PMT 的遮盖物！

注意：我们实验室中的三套实验装置彼此略有不同，详见附录 5。

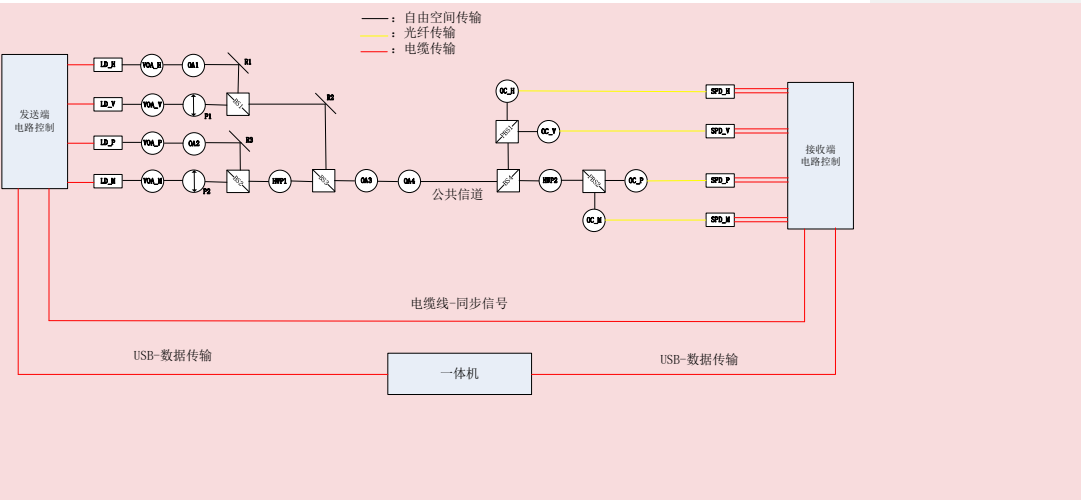


图 2-2 探测器效率测量示意图

附注 1：系统图标号解释

标号	器件
LD_H, LD_V, LD_P, LD_M	激光器（ $404\pm 1\text{nm}$ ）
VOA 和 OA	可调衰减器和衰减器
P	偏振控制器
R	反射镜
NPBS 或者 BS	消偏振分光棱镜
HWP	半波片
PBS	偏振分光棱镜
OC	光纤耦合器
SPD_H, SPD_V, SPD_P, SPD_M	单光子探测器

附注 2：在可变衰减器之后，如有必要，在一些光束路径上也可以使用一些可调偏振器（旋转偏振器）。可调偏振器通常是一种吸收型偏振器。这些偏振器沿偏振器的光轴传输偏振分量，并吸收垂直分量。仅在必要的情况下，该套实验装置才需要使用可调偏振器代替偏振分束器。是否需要使用可调偏振器取决于激光器发出的光的偏振特性以及实验对水平或垂直偏振的要求。

附注 3：偏振 QKD 系统的软件部分会对单光子探测器的计数进行实时扫描上传，所以通过打开 QKD 系统软件的同时，我们通过调节圆形可调衰减器的衰减值，可在 QKD 软件上实时观察到单光子探测器的计数值；调节至所需要的计数值即可（请参见附录 3 了解如何启动 QKD 软件以及如何触发四路激光器）。

1. 如图 2-2 所示，利用图中 M 的光路进行单光子的探测和探测器探测效率的测量；其中 M 路光路包括：LD_M、VOA_M、P2、BS2、HWP1、BS3、OA3、OA4、BS4、HWP2、PBS2、OC_M、SPD_M。
2. 发送端电路控制模块上电，启动 QKD 软件，点击 QKD 软件中的触发 M 路激光器发光；使用可见光功率计测量 M 路激光器输出功率并记录（请参见附录 3 了解如何启动 QKD 软件以及如何触发四路激光器）；
3. 查看激光器 LD_M 每秒发射脉冲数，理论计算，当到达单光子探测器的平均光子数为 0.1 光子/脉冲时，LD_M 和 SPD_M 之间需要多少衰减；
4. M 路光路中除可调衰减元件，其余元件的衰减值均在实验平台上给出，利用上述理论计算值和其余元件的衰减值，推导当到达单光子探测器的平均光子数为 0.1 光子/脉冲时，可调衰减元件需增加多少衰减；
5. 转动可调衰减片，使用功率计测量衰减，使得其衰减和上部分推导值一致停止转动；
6. 接收端电路模块上电，点击 M 路扫描，得到 M 路计数值并记录（可通过工具栏中的实时数据获取计数值），见附件 4 图 4-4；（实际扫描时，会出现四路计数，分别对于四个探测器，其中 SPD_H 对应 Scan0 计数，SPD_V 对应 Scan1 计数，SPD_P 对应 Scan2 计数，SPD_M 对应 Scan3 计数）
7. 使用 M 路探测计数值计算出单光子探测器的探测效率。（扫描模式每秒脉冲数设置为 10MHz）

2.3 实验数据记录及处理

表格格式见附录表二：单光子的探测及相应探测器效率的数据记录表。

实验 3：单光子的标定

本实验的目的是为所有的四路激光器（M、P、H、V）设置相同的平均光子数，这将在接下来的实验四 QKD 演示实验中使用。

3.1 实验原理

在 BB84 协议中，信息的物理载体是单个光子。因此在量子密钥分发实验中应当使用某种每触发一次就发射且仅发射一个光子的设备作为光源，这样的设备被称为“单光子光源”。目前，不同的实验室基于 NV 色心、量子点等技术已经制备了高亮度的单光子源，但是其设备还较为复杂、成本也比较高。因此，在现阶段的单光子量子密钥分发实验中，比较常用的

方法是用经过强衰减的脉冲激光代替单光子光源²。

同实验二所操作的相类似，在实验三中偏振 QKD 系统通过调节光路衰减模块，包括固定衰减片和圆形可调衰减片，使得密钥分发系统发送端出射光子达到单光子水平。实验用的 404nm 脉冲激光器的发光重复频率为 10MHz。严格来说，单光子的标定需要额外的高功率激光器来标定衰减器的衰减值，但为了实验的简单，在本实验中采用单光子探测器来标定衰减器的衰减值。例如，标定单光子为 0.05 光子/脉冲时，探测器效率为 20%时，则到达单光子探测器的计数应该 $(N)=\text{激光器发光频率}(f) \times \text{平均光子数脉冲}(\mu) \times \text{单光子探测器探测效率}(\eta)=10 \times 10^6 \times 0.05 \times 20\% = 10^5 \text{ Hz}$ 。

3.2 实验内容及步骤

该实验过程是为四路激光器在公共信道中设置 0.2 个光子/脉冲。整个实验过程用到的实验装置同实验二装置图 2-2。

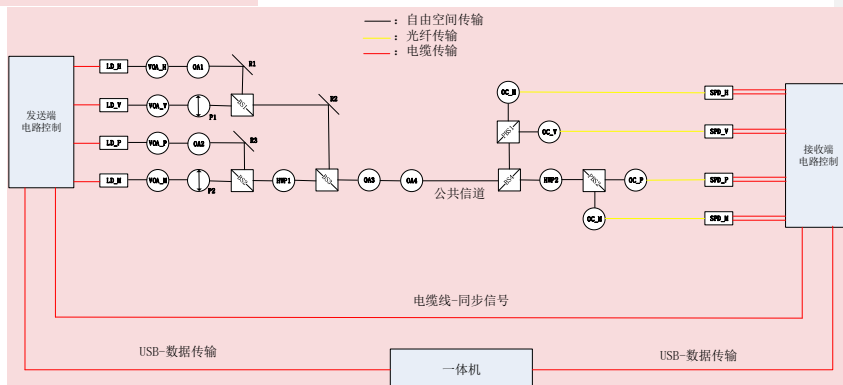


图 3-1 单光子标定测量示意图

1. 单光子的标定如图 3-1 所示，H、V、P、M 路光路到达公共信道时，出射光为单光子状态；
2. 理论计算当公共信道平均光子数为 0.2 光子/脉冲时，经过接收端光路衰减到达单光子探测器的探测计数 N；（以 M 路光路为例计算）
3. 发送端和接收端电路控制模块上电，启动 QKD 软件；
4. 选中 QKD 软件 Alice-Bob 链路，点击软件上方的工具栏，选择扫描模式；
5. 选择 M 路扫描，调节 VOA_M 可调衰减片，使得 SPD_M 扫描计数接近 N；
6. 依次分别选择 H、V、P 路扫描，也使得对应的探测器扫描计数接近 N；上述过程

² 严格讲，当激光二极管产生光脉冲的强度被大幅度衰减值极弱时，其光子数分布服从泊松分布。即每个光脉冲中包含 n 个光子的概率为 $P_n = e^{-\mu} \mu^n / n!$ ，其中 μ 表示光脉冲的平均强度。因此，强衰减激光仅是一种近似单光子源，当 $\mu \approx 0.1$ 量级时，这是一种较好的近似。

即完成密钥分发系统的单光子标定。

3.3 实验数据记录及处理

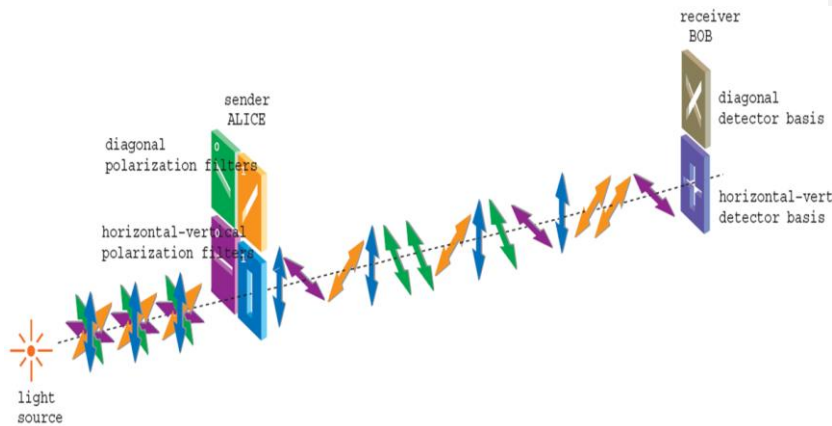
表格格式见附录表三：单光子的标定实验数据记录表。

实验 4：密钥分发过程数据处理

4.1 实验原理

发送方 Alice 制备一系列的光子发送给接收方 Bob，每个光子的偏振态随机地从水平偏振态 $|\rightarrow\rangle$ 、竖直偏振态 $|\uparrow\rangle$ 、右斜 45 度偏振态 $|\nearrow\rangle$ 和左斜 45 度偏振态 $|\nwarrow\rangle$ 四个偏振态中选取，如果 Alice 发送光子的偏振态为水平偏振态 $|\rightarrow\rangle$ 或者竖直偏振态 $|\uparrow\rangle$ ，则称 Alice 选择+基制备光子，如果 Alice 发送光子的偏振态是右斜 45 度偏振态 $|\nearrow\rangle$ 或者左斜 45 度偏振态 $|\nwarrow\rangle$ ，则称 Alice 选择×基制备光子。

批注 [zz3]: Rewrite sections 2 and 3 such that the objectives is very clear. Furthermore, all the definitions given in section 3 should appear in section 2. These two sections need full rewriting. Clear explanations about how to use the software for running the lasers must be given in appendix.



Alice产生的随机序列	0	0	1	1	1	0	1	0	1
Alice选用的基	+	×	+	+	×	×	×	+	×
光子的偏振态	\rightarrow	\nearrow	\uparrow	\uparrow	\nwarrow	\nearrow	\nwarrow	\rightarrow	\nwarrow
Bob随机选择的基	+	+	×	+	+	×	+	+	×
Bob的测量结果	\rightarrow	\rightarrow	\nearrow	\uparrow	\uparrow	\nearrow	\rightarrow	\rightarrow	\nwarrow
对基结果	√			√		√		√	√
生成的密钥序列	0			1		0		0	1

图 4-1 密钥分发原理图

接收方 Bob 与 Alice 完全独立地随机选取+基和 X 基测量 Alice 发送过来光子的偏振态，并记录下测量到光子的位置信息。

Alice 和 Bob 对基，即双方仅保留基相同（Alice 制备基和 Bob 测量基）并且 Bob 测量到光子位置的光子偏振态信息，双方基不同时则直接抛弃相关信息。

Alice 和 Bob 将保留的光子偏振态信息转换成相应的密钥比特信息，即对基后保留的光子偏振态按水平偏振态 $| \rightarrow \rangle$ 和右斜 45 度偏振态 $| \nearrow \rangle$ 转换为比特“0”，竖直偏振态 $| \uparrow \rangle$ 和左斜 45 度偏振态 $| \nwarrow \rangle$ 转换为比特“1”。

Alice 和 Bob 通过经典公开信道对上一步中获得的密钥比特进行处理，其过程主要分成纠错和保密放大来进行，纠错就是使得密钥比特一致，而保密放大（Privacy Amplification）就是将可能泄漏给窃听者的信息剔除掉。

实际量子密钥分发时，用两位的 bit 编码表示光子信息，其中个位 bit 代表基矢信息，十位 bit 代表密钥信息；例如：Alice 端水平偏振编码为 00，垂直偏振编码为 10，右斜 45 度偏振编码为 01，左斜 45 度偏振编码为 11；相应的 Bob 端四路探测器探测到信号，分别也是按照上述编码方式进行编码。

密钥分发的过程中，光子传输探测后，会得到一系列的这种两位编码的信息数据，如何从这些数据中提取出有用信息，需要经过对基、纠错、保密放大等过程，以保证密钥的安全性。当然，考虑到是否存在窃听，需要对系统的每次传输过程进行误码估计。以保证此次的传输数据有效。

Alice 和 Bob 两端传输探测完成后会得到一系列两位编码的信息数据，首先需要对两端的数据进行对基，再对对基的数据进行比对，计算出系统的误码率。当误码率低于理论安全界限 11% 时，本次传输有效，继续进行后续处理过程。

4.2 实验内容及步骤

1. 发送端和接收端电路控制模块上电，启动 QKD 软件；
2. 点击 QKD 的接收端控制界面（Bob-Alice），选择误码平均采样率后点保存；点击 QKD 的发送端控制界面（Alice-Bob），勾选中间密钥输出功能，点击保存；选中工具栏中的蓝色 R（密钥随机分发），点击右侧的运行按钮；待系统运行 5-10 秒后，点击停止按钮。此时，记录下系统的平均误码率；

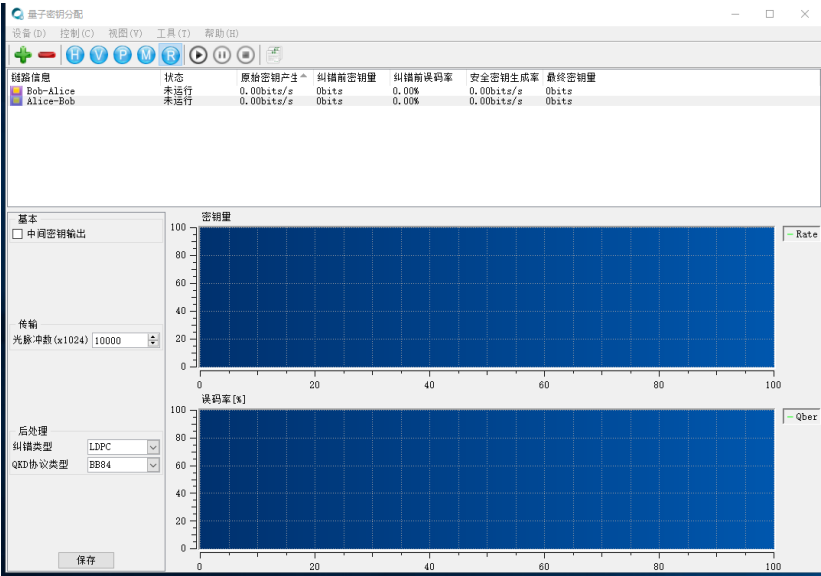


图 4-2 QKD 发送端界面

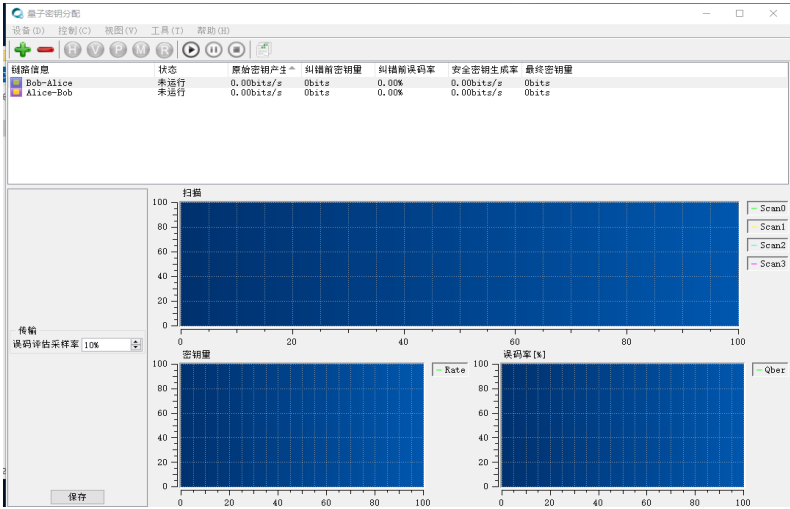


图 4-3 QKD 接收端界面

3. 在桌面的自由空间偏振文件夹中查看中间密钥输出的数据，输出的数据主要包括原始数据（raw），对基后数据（sift），纠错后数据（reconcile），最终安全密钥数

据 (key)，对应的发送端分别为：transmitter-raw、transmitter-sift、transmitter-reconcile、transmitter-key，接收端分别为：receiver-raw、receiver-sift、receiver-reconcile、receiver-key；

4. 打开桌面上的软件 Beyond Compare，选择文本比较，进入界面，点击最上方的会话选项（如图 4-4），比较文件用，选择十六进制文件。分别打开 transmitter-sift 和 receiver-sift，然后通过会话中 16 进制比较信息进行误码估计，由于 OKD 软件保存的数据格式均为十六进制，所以实际误码估计时需要将十六进制转为二进制文件进行比对。（例如总共 100 个二进制数据，两端有 5 个错误位，则误码率为 5%）

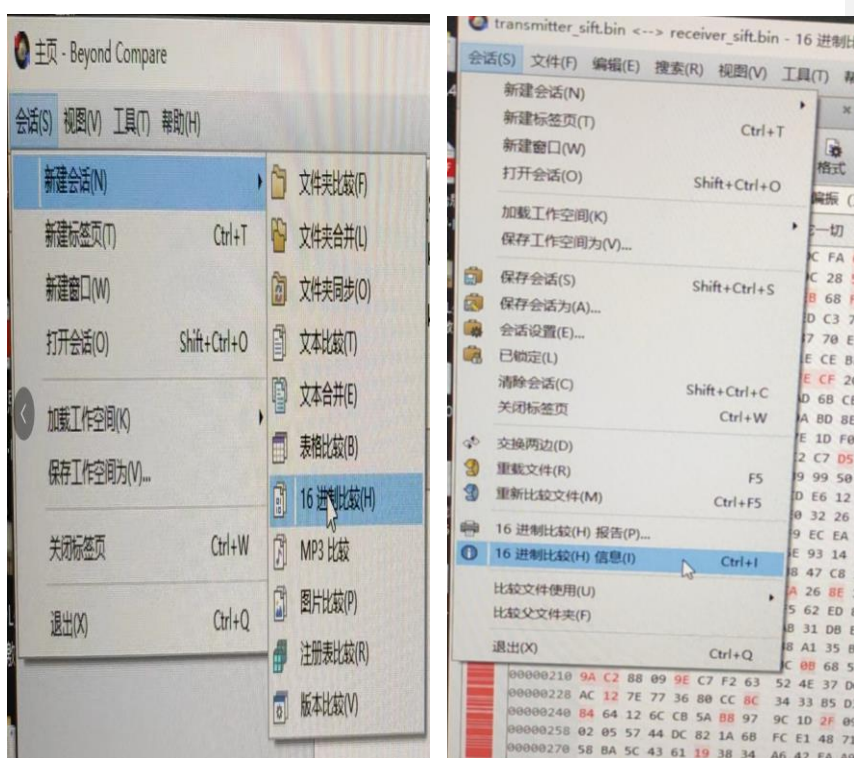


图 4-4 Beyond Compare 软件

4.3 实验数据记录及处理

表格格式见附录表四：密钥分发过程数据处理实验数据记录表。

【附录 1：实验数据表格】

1、偏振控制和测量记录表格 a

序号	名称		数据	单位
1	Laser + PBS1 反射功率			dbm
2	Laser + PBS1 透射功率			dbm
1	Laser + HWP1+PBS1 最大反射功率			dbm
2	Laser + HWP1+PBS1 最大透射功率			dbm
3	Laser + HWP1+PBS1 最小反射功率			dbm
4	Laser + HWP1+PBS1 最小透射功率			dbm
1	半波片 1 转动 0°	PBS2 透射功率		dbm
2	半波片 1 转动 22.5°	PBS2 透射功率		dbm
3	半波片 1 转动 45°	PBS2 透射功率		dbm
4	半波片 1 转动 67.5°	PBS2 透射功率		dbm
5	半波片 1 转动 90°	PBS2 透射功率		dbm
6	半波片 1 转动 112.5°	PBS2 透射功率		dbm
7	半波片 1 转动 135°	PBS2 透射功率		dbm
8	半波片 1 转动 157.5°	PBS2 透射功率		dbm
9	半波片 1 转动 180°	PBS2 透射功率		dbm
10	半波片 1 转动 202.5°	PBS2 透射功率		dbm
11	半波片 1 转动 225°	PBS2 透射功率		dbm
12	半波片 1 转动 247.5°	PBS2 透射功率		dbm
13	半波片 1 转动 270°	PBS2 透射功率		dbm
14	半波片 1 转动 292.5°	PBS2 透射功率		dbm
15	半波片 1 转动 315°	PBS2 透射功率		dbm
16	半波片 1 转动 337.5°	PBS2 透射功率		dbm
17	半波片 1 转动 360°	PBS2 透射功率		dbm
1	放置半波片 1 且与光轴呈 22.5°	PBS2 透射功率		dbm
2	放置半波片 1 且与光轴呈 22.5°	PBS2 反射功率		dbm
1	半波片 2 转动 0°	PBS2 透射功率		dbm
2	半波片 2 转动 22.5°	PBS2 透射功率		dbm
3	半波片 2 转动 45°	PBS2 透射功率		dbm
4	半波片 2 转动 67.5°	PBS2 透射功率		dbm
5	半波片 2 转动 90°	PBS2 透射功率		dbm

6	半波片 2 转动 112.5°	PBS2 透射功率		dbm
7	半波片 2 转动 135°	PBS2 透射功率		dbm
8	半波片 2 转动 157.5°	PBS2 透射功率		dbm
9	半波片 2 转动 180°	PBS2 透射功率		dbm
10	半波片 2 转动 202.5°	PBS2 透射功率		dbm
11	半波片 2 转动 225°	PBS2 透射功率		dbm
12	半波片 2 转动 247.5°	PBS2 透射功率		dbm
13	半波片 2 转动 270°	PBS2 透射功率		dbm
14	半波片 2 转动 292.5°	PBS2 透射功率		dbm
15	半波片 2 转动 315°	PBS2 透射功率		dbm
16	半波片 2 转动 337.5°	PBS2 透射功率		dbm
17	半波片 2 转动 360°	PBS2 透射功率		dbm

2、单光子的探测及相应探测器效率的数据记录表

序号	名称	数据	单位
1	LD_M 激光器功率		dbm
2	总需要衰减值		db
3	VOA_M 可调衰减片理论需调节衰减值		db
4	VOA_M 可调衰减片实际调节衰减值		db
5	QKD 扫描 M 路 SPD_M 探测计数值		Hz
6	SPD_M 探测器探测效率		%

3、单光子的标定实验数据记录表

序号	名称	数据	单位
1	M 路到达公共信道时为单光子，探测器计数值		Hz
2	M 路扫描，SPD_M 计数值		Hz
3	H 路扫描，SPD_H 计数值		Hz
4	V 路扫描，SPD_V 计数值		Hz
5	P 路扫描，SPD_P 计数值		Hz

4、密钥分发过程数据处理实验数据记录表

序号	名称	数据	单位
1	QKD 系统软件统计密钥率		bits/s
2	QKD 系统软件统计误码率		%
3	QKD 系统误码估计采样率		%
4	手动误码率计算时所得数据误码率		%

【附录 2：提高知识】

****学有余力的同学参考学习**

BB84 协议的安全性

BB84 协议的严格安全性证明需要用到纠缠和量子熵等概念，因此较为复杂，感兴趣的同学们可以参考文献，这里我们仅在最简单的截取-重发攻击下进行简单的说明介绍。

1、截取-重发攻击模型：
Step1: 窃听者 Eve 随机的选择水平基 (\oplus) 或者对角基 (\otimes) 测量 Alice 发送的量子态；
Step2: Eve 根据自己的测量结果重新制备一个量子态发送给 Bob，具体对应规则如下

Eve 测量基	Eve 测量结果	Eve 重新发送量子态
水平基 (\oplus)	H	H
	V	V
对角基 (\otimes)	R	R
	L	L

2、安全性分析（误码率分析）
下面分析窃听者在截取-重发攻击模型下对系统误码率的影响。为了分析的简单，假设 Alice 和 Bob 的信道是理想信道，即当没有窃听者存在时系统的误码率为 0（所谓误码率是指 Alice 和 Bob 最后共享密钥不一致的概率）。
根据 Alice 所发送四个量子态的等价性，仅分析 Alice 发送水平偏振 H 时的情况，其余三种情况具有完全相同的结果。此时，Alice 和 Bob 测量结果的概率如下表所示：

Alice 发送量子态	Eve		Bob \oplus	
	测量结果	概率	测量结果	概率
H	H	1/2	H	1

	V	0	/	/
	R	1/4	H	1/2
			V	1/2
	L	1/4	H	1/2
			V	1/2

注：根据 BB84 协议的规定，只有 Alice 和 Bob 的基一致时，所对应的 bit 才会保留下来做密钥，因此只考虑 Bob 采用水平基测量的情况。

从上表可以看出，Bob 测得 V 态的概率为

$$P_V = \frac{1}{4} \times \frac{1}{2} + \frac{1}{4} \times \frac{1}{2} = \frac{1}{4}$$

即由于 Eve 的存在，Alice 和 Bob 最终的数据中将存在 25% 的误码率。此时，Alice 和 Bob 仅需在最后的数据中拿出小部分来进行误码率计算就可以发现窃听者的存在。

在前面的讨论中，假设 Alice 和 Bob 的信道是理想的，但实际的信道总是存在一定噪声，因此，在实际系统中，即使没有窃听者存在，Alice 和 Bob 的数据也存在一定的误码率，那这是否会影响 QKD 的应用呢？答案是否定的，因为我们可以在噪声信道模型下进行安全性分析。事实上，信道噪声只会降低密钥产生量，而不会影响其安全性。理论分析表明，只要系统的误码率小于 11%，Alice 和 Bob 就可以通过纠错和私密放大步骤提取出无条件安全的密钥。

【参考文献】

苗二龙，自由空间量子密钥分配，博士学位论文，中国科学技术大学，2006 年；
陈彦，基于单光子源的量子密码术研究，博士学位论文，电子科技大学，2007 年。

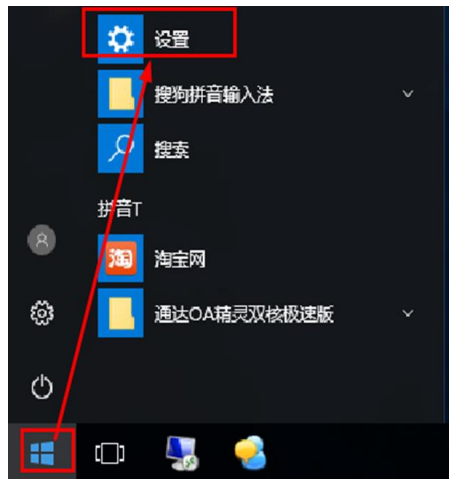
【附录 3：QKD 软件的启动】

1. 实验前的准备工作（该部分工作无需同学们操作）

1.1 数字签名消除操作

因 Win10 系统存在一个问题“驱动程序强制签名，导致系统在创建链路时无法读取到设备固件号”，所以要将签名禁用，具体操作步骤如下：

- a) 点击“开始—>设置”



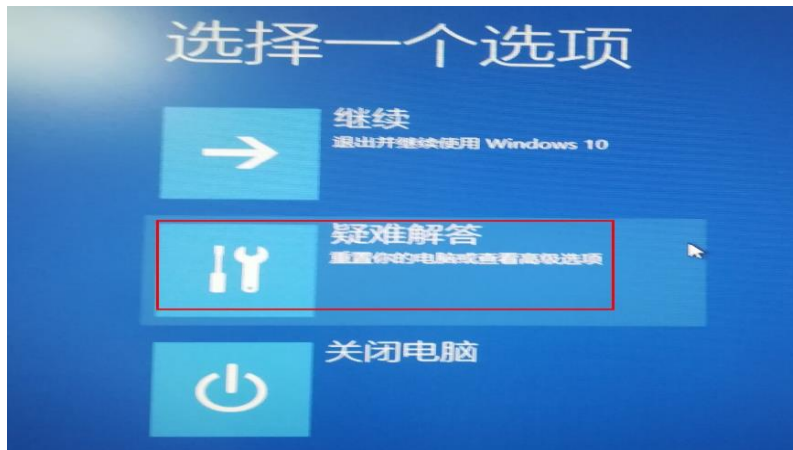
b) 点击“更新和安全”



c) 点击“恢复—>立即重启”



d) 点击“疑难解答”



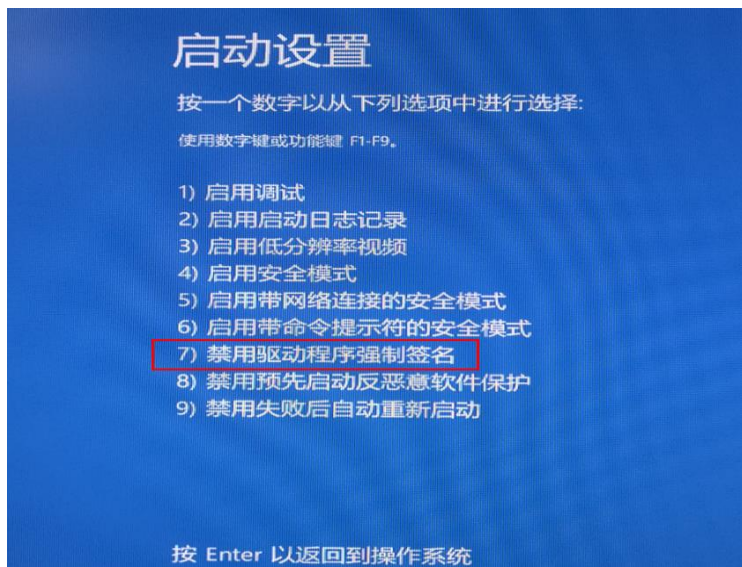
e) 点击“高级选项—>启动设置”



f) 点击“启动设置—>重启”



- g) 电脑重新启动，待显示以下界面后，在键盘上按下 7，设置完成，电脑重启成功。之后再打开 QKD 软件，创建链路时系统能成功读取到设备固件号。



2 发送端和接收端电路控制模块上电，启动 QKD 软件，调试设备 2.1 设备连接

2.1.1 上位机软件启动

设备通电后，QKD后台程序已经自启动。通过运行PC上的上位机软件可监控QKD系统运行情况。

启动上位机软件，直接进入主界面。

2.1.2 链路建立（链路信息已经建立在软件里，该过程无需操作，请阅读了解此过程）


上位机界面点击【设备】->【添加新链路】，或者点击图中的，如图2所示，进行链路添加，弹出图3所示对话框。



图 2 菜单栏

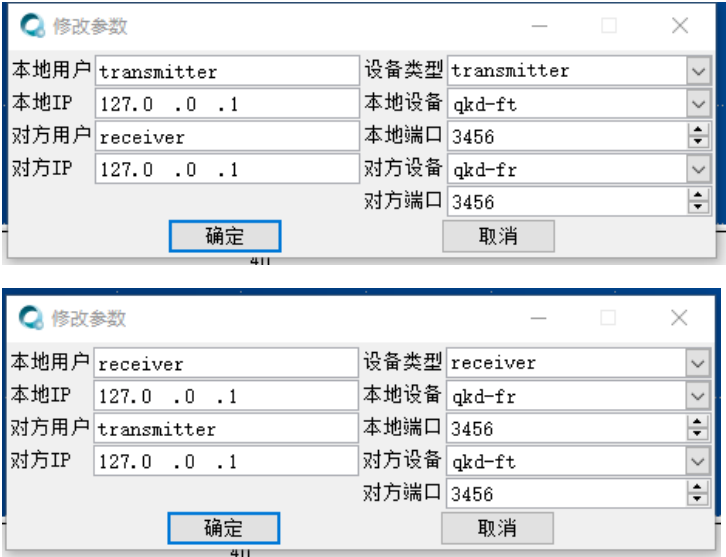


图 3 链路配置界面

参数填写说明如下：

本地用户	本地系统名称，用户可根据实际需要自定义名称。
设备类型	可选transmitter（发射端）或receiver（接收端），根据实际添加的设备类型进行选择
本地设备	此项为本地设备收发类型相应的USB固件号，不可更改
本地IP	发射端分配的IP地址，默认为本机IP
本地端口	系统端口号，默认为3456
对方用户	对端设备名称，用户可根据实际需要自定义名称
对方设备	此项为对方设备收发类型相应的USB固件号，即为选定的QKD系统另一端的设备固件号，不可更改
对方IP	接收端IP地址
对方端口	系统端口号，默认为3456

附：菜单栏说明

菜单栏		
设备	添加	添加偏振量子密钥分配系统设备 本地用户：本地系统名称，用户可根据实际需要自定义名称。 设备类型：可选transmitter（发送端）或receiver（接收端），根据实际添加的设备类型进行选择

		本地设备：此项为本地设备收发类型相应的USB固件号，不可更改 本地IP：发送端分配的IP地址，默认为本机IP 本地端口：系统端口号，默认为3456 对方用户：对端设备名称，用户可根据实际需要自定义名称。 对方设备：此项为对方设备收发类型相应的USB固件号，即为选定的QKD系统另一端的设备固件号，不可更改 对方IP：接收端IP地址 对方端口：系统端口号，默认为3456
	删除	删除被选中的 QKD 链路
	最小化	将操作界面最小化
	退出	退出操作界面
	关闭系统	关闭偏振量子密钥分配系统
控制	开始	选中要开始运行的链路，点击开始后启动相应链路上的偏振量子密钥分配系统
	暂停	选中要暂停运行的链路，点击暂停后相应链路上的偏振量子密钥分配系统将暂停运行
	停止	选中要停止运行的链路，点击停止后相应链路上的偏振量子密钥分配系统将停止运行
	日志	记录偏振量子密钥分配系统纠错前采样密钥统计信息
	高级设置	设置扫描——单次采集脉冲数
		设置传输——随机数种子
	H 扫描（种子4）	触发水平偏振激光器发光
	V 扫描（种子11）	触发垂直偏振激光器发光
	P 扫描（种子1）	触发+45。偏振激光器发光
	M 扫描（种子14）	触发-45。偏振激光器发光
视图	R 传输	进行密钥传输
	工具栏	设置是否在操作界面显示工具栏
	参数设置	设置是否在操作界面显示参数设置栏
工具	激光触发器	触发指定的激光器发射激光脉冲，可设置发射脉冲数目以及是否循环发送

	扫描	利用偏振控制器，调出光的四种偏振状态
	实时数据	显示发送端和接收端实时数据显示
帮助	关于	查看系统版本信息

- a) 菜单栏下设设备、控制、视图、工具及帮助菜单。
- b) 工具栏包括添加、删除、H、V、P、M 激光器扫描、R（传输）、开始、暂停、停止、日志 10 个功能项，功能与菜单栏下对应项一致。
- c) 链路信息栏包括链路信息、状态、原始密钥产生率、纠错前密钥量、纠错前误码率、安全密钥生成率、最终密钥量。
- d) 参数设置栏用于设置发送端的传输脉冲数以及后处理方式。

2.1.3 链路参数设置

收发两端链路创建成功后，在发送端可更改相应的配置参数（当链路处于已连接状态，在发送端配置完成后，运行一次软件，相关参数会自动同步到接收端），单击选中需要修改的链路，点击控制菜单中的高级设置选项，如图4所示。



图 4 菜单界面

- a) 将【扫描】中单次采集脉冲数设置为 10000000，如图 5 所示。；
- b) 将【传输】中随机数种子设置为 127，如图 6 所示；
- c) 点【确定】，保存参数设置；

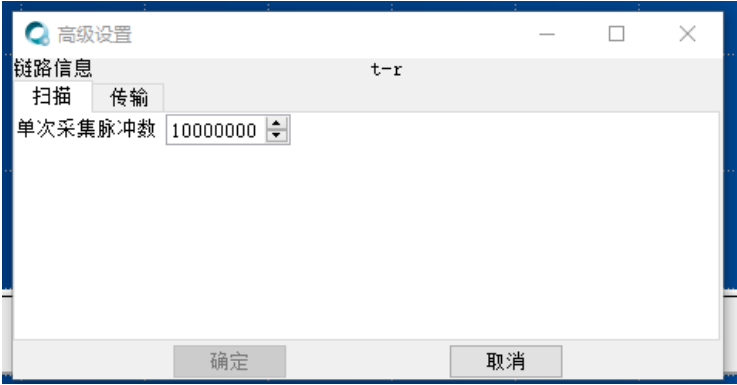


图 5 扫描配置界面

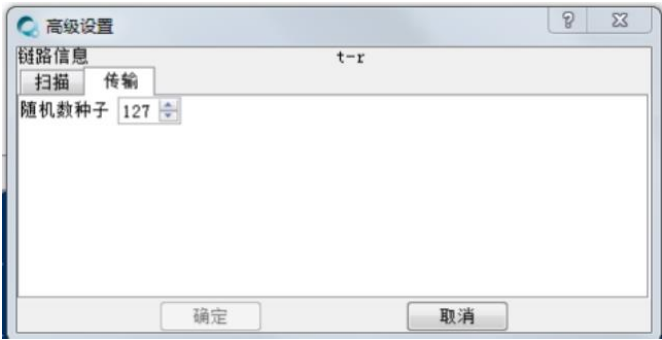


图 6 传输配置界面

附注：链路信息栏说明

链路信息栏	
链路信息	本地至对端的链路
状态	状态包括未运行、运行、暂停、停止
原始密钥产生率	系统生成的原始密钥的产生速率
纠错前密钥量	系统产生的原始密钥经过误码采样评估后剩余的密钥量
纠错前误码率	原始密钥通过无码采样评估得出的平均误码率
安全密钥生成率	经过纠错、保密放大处理后产生的安全密钥的生成速率
最终密钥量	系统经过纠错、保密放大后产生的安全密钥量

【附录 4：QKD 软件的运行】

2.1.4 运行基本参数设置

a) 发送端基本参数设置



图 7 发送端基本参数配置界面

基本	中间密钥输出	勾选“中间密钥输出”， QKD文件夹同级目录下会生成产生安全密钥之前各阶段的中间密钥文件
传输	光脉冲数（*1024）	随机数个数
后处理	纠错类型	可选LDPC（低密度奇偶校验）、CASCADE（级联纠错），系统默认使用LDPC
	QKD协议	可选BB84或B92协议，系统默认使用BB84协议
保存	保存发射端参数配置	

b) 接收端基本参数设置



图 8 接收端基本参数配置界面

传输	误码评估采样率	可输入范围1%-100%。输入100%时，所有原始密钥均用于误码评估，将无法产生安全密钥。输入10%时，10%的原始密钥将用于误码评估
保存	保存接收端参数配置。	

3 传输过程

点击 QKD 的接收端控制界面（Bob-Alice），选择误码平均采样率后点保存；点击 QKD 的发送端控制界面（Alice-Bob），勾选中间密钥输出功能，点击保存；选中工具

栏中的蓝色 R（密钥随机分发），点击右侧的运行按钮；正常情况下，系统原始密钥生成率>20kbps，平均误码率≤3%。待系统运行 5-10 秒后，点击停止按钮。此时，记录下系统的平均误码率：

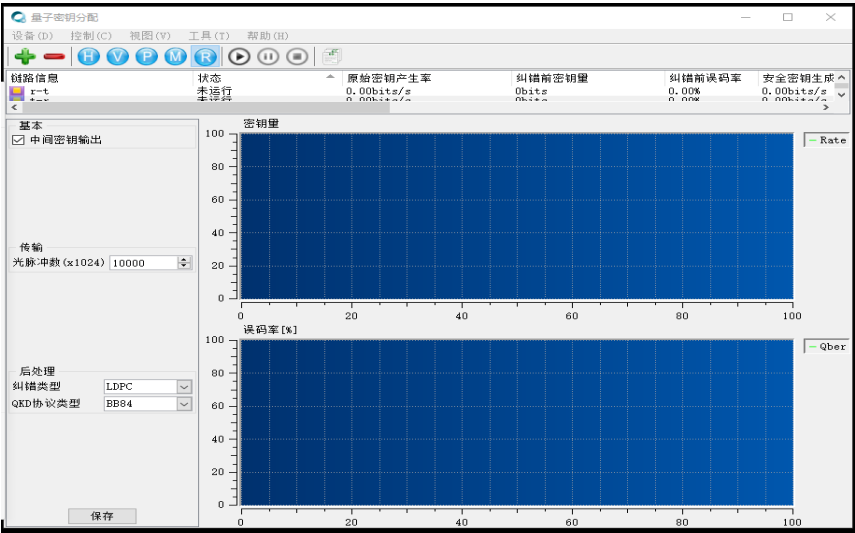


图 4-2 QKD 发送端界面

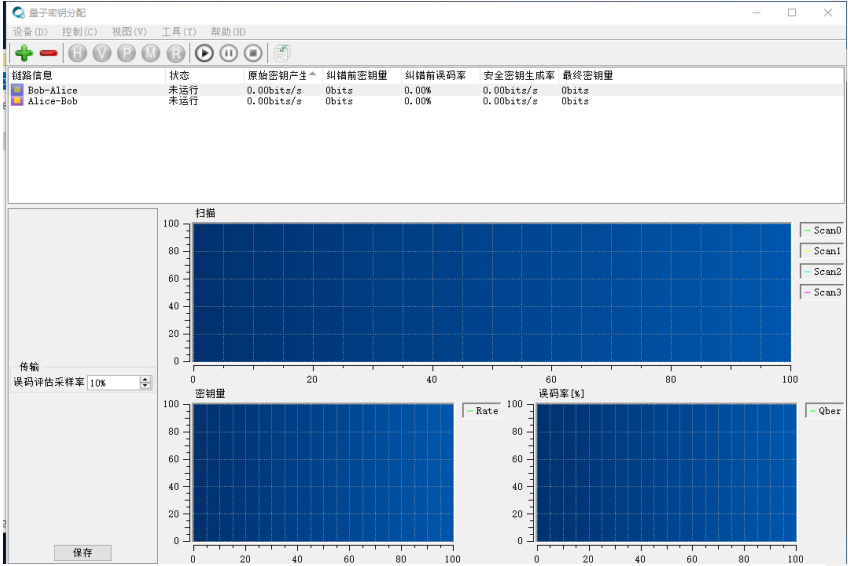


图 4-3 QKD 接收端界面

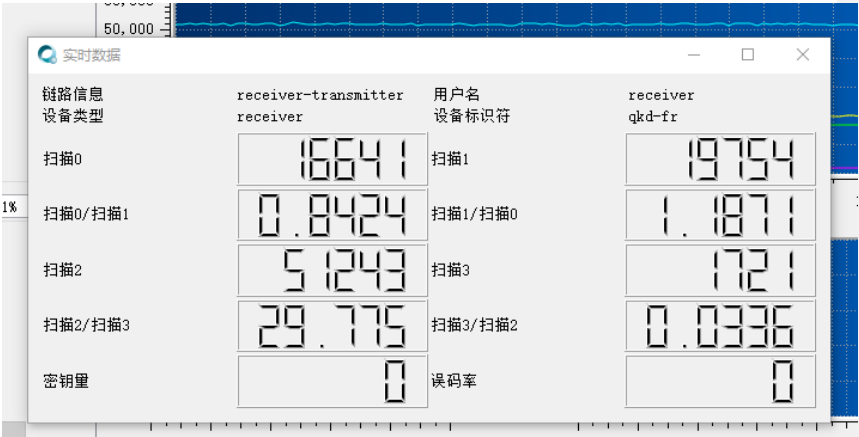


图 4-4 QKD 软件中的实时数据

【附录 5：实验室三套 QKD 实验装置图】

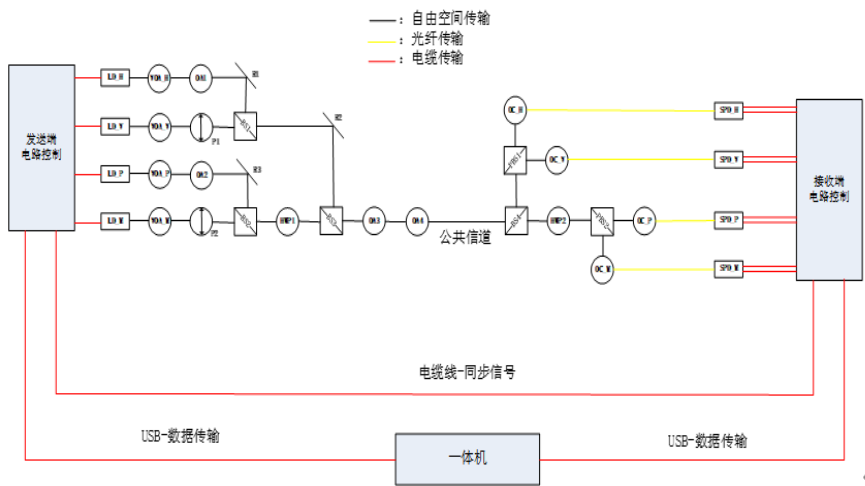


图 5-1 标号 C3 的第一套实验装置图

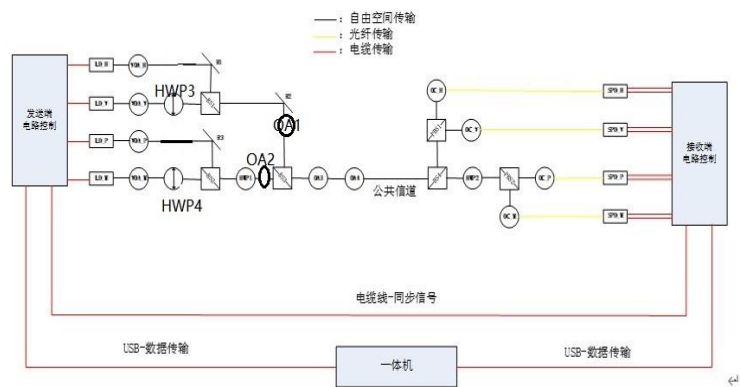


图 5-2 标号 C2 的第二套实验装置图

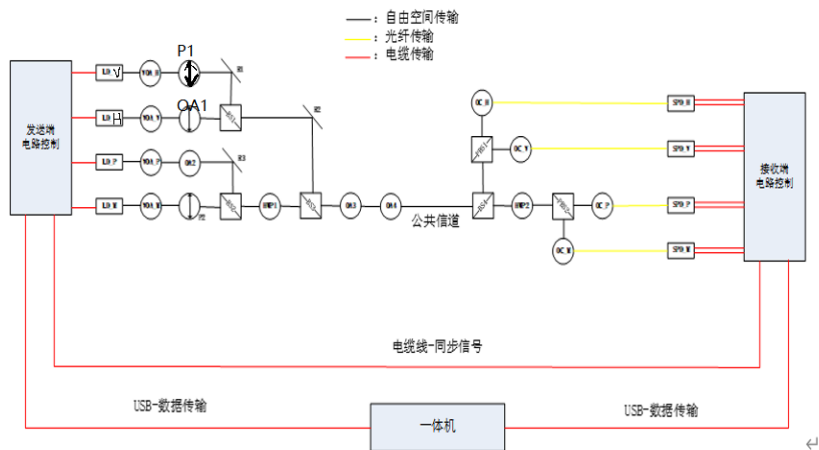


图 5-3 第三套实验装置图