

# 实验 D3 量子密钥分发

2019 年 10 月 28 日

实验方案	实验记录	分析讨论	总成绩
年级、专业:	17 级物理学	组号:	6
姓名:	徐昊霆	学号:	17353071
日期:	2019 年 10 月 28 日	教师签名:	

贡献度说明: 第一部分实验原理部分实验一二三部分为组员贡献, 实验四及本报告其他内容为本人书写。第二部分--实验方案与步骤, 由小组分工合作完成。本人负责实验方案与步骤实验四部分, 实验一二三由其他组员贡献。

## 目录

<b>1 实验原理与方案</b>	<b>3</b>
1.1 实验目的 . . . . .	3
1.2 仪器用具 . . . . .	3
1.3 实验安全注意事项 . . . . .	4
1.4 实验原理 . . . . .	5
1.4.1 经典保密通信简介 . . . . .	5
1.4.2 量子密钥分发及 BB84 协议 . . . . .	6
1.4.3 基于 BB84 协议的 QKD 实验 . . . . .	8
1.4.4 实验一--量子叠加 (概率幅叠加) 与经典混合 (概率相加) 的差异 . . . . .	9
1.4.5 实验二--单光子的探测及相应探测器效率的测量 . . . . .	9
1.4.6 实验三--单光子的标定 . . . . .	10
1.4.7 实验四--密钥分发过程中数据处理 . . . . .	11
1.5 实验前思考题 . . . . .	12
<b>2 实验步骤与记录</b>	<b>16</b>
2.1 实验一 . . . . .	16
2.2 实验二--单光子的探测及相应探测器效率的测量 . . . . .	19
2.3 实验三--单光子的标定 . . . . .	20
2.4 实验四步骤 . . . . .	21
2.5 实验中遇到的问题记录 . . . . .	23
2.6 实验原始记录与教师签名 . . . . .	25
<b>3 分析与讨论</b>	<b>29</b>
3.1 实验一--经典混合与量子混合的差异 . . . . .	29
3.2 实验二--单光子的探测及相应探测器效率的测量 . . . . .	29
3.3 实验三--单光子的标定实验 . . . . .	30
3.4 实验四--量子密钥分发实验 . . . . .	30
3.5 实验后思考题 . . . . .	34

# 1 实验原理与方案

## 1.1 实验目的

1. 掌握量子叠加 (概率幅叠加) 与经典混合 (概率相加) 的差异;
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. 掌握密钥分发过程数据处理。

## 1.2 仪器用具

表 1: 量子叠加与经典混合差异的用具

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	2	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 2: 单光子的标定用具

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 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 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

### 1.3 实验安全注意事项

1. 系统工作温度在 15°C ~ 30°C 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. 探测器光电倍增管打开盖子前, 一定要确认暗室条件并且无激光直接照射探测面。使用完后, 断电并盖好盖子。

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。

## 1.4 实验原理

### 1.4.1 经典保密通信简介

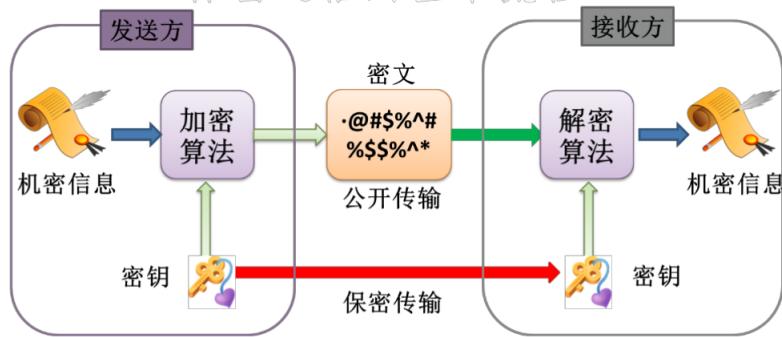


图 1: 保密通信流程图

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, 密钥和加解密算法(一般来说, 加密算法和解密算法都是匹配一致的)是保证信息安全的关键。在安全性证明中, 一般认为加解密算法是公开的。因此, 保密通信中信息的安全完全取决于密钥的安全和加解密算法的复杂性。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, 但要从条件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依赖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加解密算法的复杂性。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。

#### 1.4.2 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送密钥的量子状态, 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。

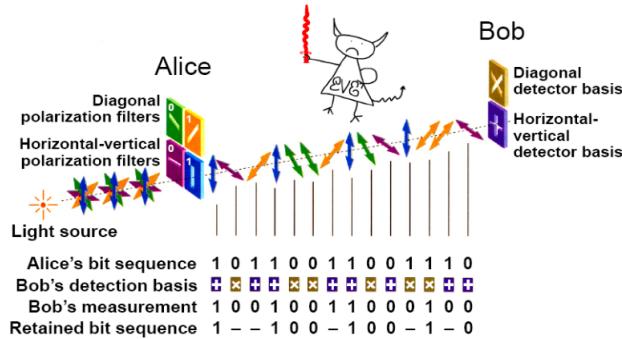


图 2: 偏振编码 BB84 协议流程图

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。<sup>1</sup>

表 5: 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

<sup>1</sup>下标中 1 和 0 反了, 讲义似乎有误

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。

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。

### 1.4.3 基于 BB84 协议的 QKD 实验

理论分析表明，E91 协议和 BB84 协议具有完全相同的安全性证明基础，换言之，两者在安全性上具有等价性。因此，我们主要利用 BB84 协议来进行 QKD 的演示，其光路图和实验步骤如下所示。

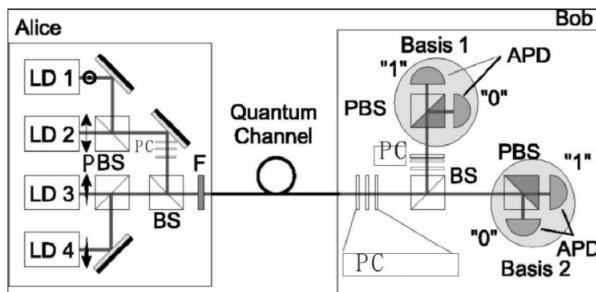


图 3: BB84 协议 QKD 实验光路示意图

#### 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。

#### 1.4.4 实验一--量子叠加 (概率幅叠加) 与经典混合 (概率相加) 的差异

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。

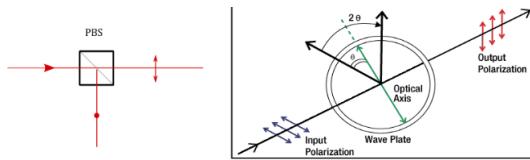


图 4: PBS 和半波片原理图

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  $45^\circ$  夹角的线偏光。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  $\theta$  角来制备一个偏振方向为  $2\theta$  的线偏光。那么对于  $45^\circ$  偏振光的制备, 半波片需要旋转  $22.5^\circ$ 。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  $22.5^\circ$  的半波片再在偏振分光棱镜后检测, 根据图 4 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  $45^\circ$  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  $45^\circ$  偏振光。

#### 1.4.5 实验二--单光子的探测及相应探测器效率的测量

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。

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  $M$ ；则：

$$M = f \times \mu \times \eta \quad (1)$$

式中  $\eta$  为单光子探测器的探测效率；由于  $f$ 、 $\mu$ 、 $M$  已知， $\eta$  则可计算出。

#### 1.4.6 实验三--单光子的标定

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。实验的偏振 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。单个 404nm 光子的能量为：

$$E = \hbar\omega \simeq 4.92 \times 10^{-19} \text{ J} \quad (2)$$

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。

$$P = \mu f E \simeq 4.92 \times 10^{-13} \text{ W} \quad (3)$$

上式中， $\mu$  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：

$$10 \log \frac{p_0}{p} = 1 - \log \frac{20 \times 10^{-6}}{4.92 \times 10^{-13}} = 76.1 \text{ dB} \quad (4)$$

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。当标

定单光子为 0.1 光子 / 脉冲时, 则到达单光子探测器的计数应该 = 激光器发光频率 ( $f$ )  $\times$  平均光子数脉冲 ( $\mu$ )  $\times$  单光子探测器探测效率 ( $\eta$ ) =  $10 \times 10^6 \times 0.1 \times 20\% = 200K$ ; (此处根据实验所使用单光子探测器的参数, 设定探测器效率为 20%)。

#### 1.4.7 实验四--密钥分发过程中数据处理

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  $\times$  基制备光子。

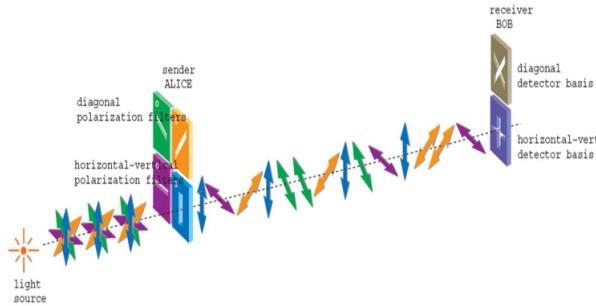


图 5: 量子密钥分发原理图

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

图 6: 量子密钥分发原理

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”, 坚直偏振态  $|\uparrow\rangle$  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。

## 1.5 实验前思考题

1、回顾偏振光实验, 说明  $\lambda/2$  波片,  $\lambda/4$  波片的工作原理;

一般来说, 沿着  $z$  方向传播的电磁波可以由  $x, y$  方向的电场来描述

$$E_x = E_{0x} \cos(\omega t + \varphi_1) \quad (5)$$

$$E_y = E_{0y} \cos(\omega t + \varphi_2) \quad (6)$$

$\lambda/2$  波片和  $\lambda/4$  波片都有一个快轴和慢轴, 其中快轴传播速度较快, 根据公式

$$v = \frac{c}{n} \quad (7)$$

可知, 传播速度较快的折射率较小, 所以经过快轴的光相位相较于经过慢轴的光相位滞后, 对于  $\lambda/2$  波片, 调节了合适的厚度, 使得快轴和慢轴的光程差为

$$\Delta = (n_f - n_s) d = \frac{\lambda}{2} \quad (8)$$

因此引起的相位差为

$$\Delta\varphi = \pi \quad (9)$$

因此如果快轴为  $y$  轴, 则  $y$  轴相位之后  $\pi$ , 故通过  $\lambda/2$  波片之后的电场为

$$E_X = E_{0x} \cos(\omega t + \varphi_1) \quad (10)$$

$$E_y = E_{0y} \cos(\omega t + \varphi_2 + \pi) \quad (11)$$

可见, 如果入射光是线偏振光 ( $\varphi_1 = \varphi_2$ ), 那么出射仍然是一个线偏振光, 只不过方向相反。如果入射光为圆偏振  $\varphi_1 = \varphi_2 + \frac{\pi}{2}$ , 出射仍然是圆偏振, 只不过旋转方向相反。

对于  $\lambda/4$  波片, 调节了合适的厚度, 使得快轴和慢轴的光程差为

$$\Delta = (n_f - n_s) d = \frac{\lambda}{4} \quad (12)$$

因此引起的相位差为

$$\Delta\varphi = \frac{\pi}{2} \quad (13)$$

因此如果快轴为  $y$  轴, 则  $y$  轴相位之后  $\pi$ , 故通过  $\lambda/2$  波片之后的电场为

$$E_X = E_{0x} \cos(\omega t + \varphi_1) \quad (14)$$

$$E_y = E_{0y} \cos(\omega t + \varphi_2 + \frac{\pi}{2}) \quad (15)$$

可见, 如果入射光是线偏振光 ( $\varphi_1 = \varphi_2$ ), 那么出射光是一个圆偏振光。如果入射光为圆偏振  $\varphi_1 = \varphi_2 + \frac{\pi}{2}$ , 出射是线偏振光。

2、如何检测一个任意方向的线偏振光?

可以使用线偏振片检测, 将线偏振片放在探测器和光源中间, 旋转线偏振片, 根据马吕斯定律

$$I = I_0 \cos^2 \theta \quad (16)$$

如果探测器探测到的光强为 0, 则此时线偏振方向与偏振片的透光方向垂直, 如果光强最大, 则此时光线的线偏振方向恰好与偏振片的透光方向相同。

3、是否可以通过将水平偏振的光与竖直偏振的光合束得到一个  $45^\circ$  线偏光?

前提是两束光的相位一致。如果相位不一致, 得到的甚至不是一个线偏振光。所以一般来说, 不可以将水平偏振的光与竖直偏振的光合束得到一个  $45^\circ$  线偏光。

4、单光子为什么不能直接用功率计测量?

因为单光子的能量为

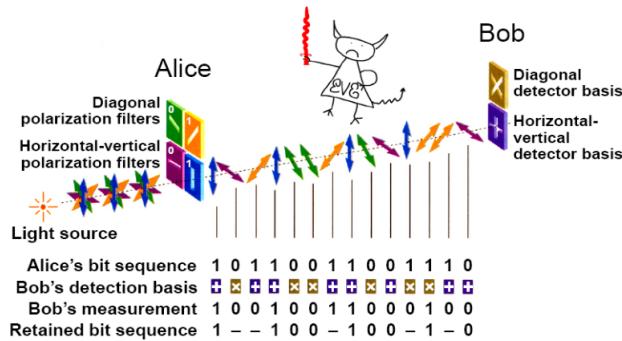
$$E = \hbar\omega \quad (17)$$

在实验中使用的一个光子的能量较小，功率计无法探测到，甚至环境的热噪声都远远大于一个光子的能量。

#### 5、检验单光子探测器的探测效率可以用强光吗？

不可以使用强光，因为单光子探测器是用来探测微弱的光子的，使用强光检验单光子探测器的效率会导致单光子探测器损坏。

#### 6、BB84 协议的原理和步骤。



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 [1]，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

表 6: 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	比特 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。

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。

7、密钥分发过程中, 为什么需要有同步信号? 因为 Alice 和 Bob 需要对剩余的  $N-m$  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。如果密钥分发过程中不同步, 则会导致纠错步骤无法知道纠错的是哪个光子, 从而导致纠错次序的错乱, 进而量子秘钥分发无法进行。

## 2 实验步骤与记录

专业:	Physics	年级:	17
姓名:	徐昊霆	学号:	17353071
室温:		实验地点	教学楼
学生签名:		评分:	
日期:	2019 年 10 月 28 日	教师签名:	

### 2.1 实验一

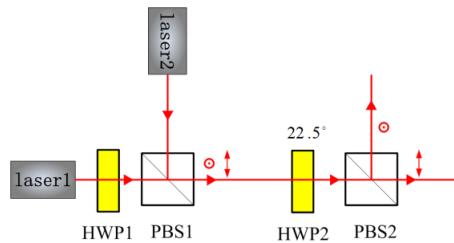


图 7: 经典混合测量示意图

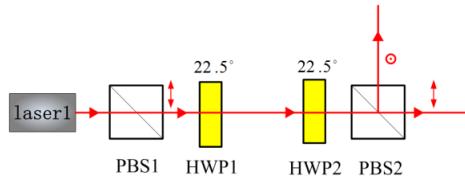


图 8: 量子叠加测量示意图

- 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) 放置激光器 laser2, 放置 PBS1, 测量 PBS1 反射端功率, 记下数值。按图示位置放置激光器 laser1 和半波片 1(HWP1)。这里需要将 laser1 出来的光与 laser2 出来的光调重合, 可以通过调节激光器位置和 PBS1 摆角使两束光重合; 测量示意图如图 7 所示;
- 3) 关闭 laser2 激光, 通过半波片 1 调节 laser1 激光偏振, 使 laser1 在透射端功率与之前测的 laser2 功率一致;

4) 关闭 Laser2, 放置半波片 2 和 PBS2, 转动半波片 2 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, 此时的刻度即为半波片的  $0^\circ$  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  $\theta$  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) 将半波片 2 的光轴转到与水平位置呈  $22.5^\circ$ , 打开 laser2 处的激光, 检  
测合束的光是否为  $45^\circ$  偏振光, 即单光子的量子态是否为 D;

6) 关闭 laser2 激光器, 如图 8 所示, 直接在 PBS1 后放置  $22.5^\circ$  半波片  
1(请先思考如何确定此处半波 1 的光轴), 制备量子态 D, 同样装置检测制备态  
(半波片 2 和 PBS2 不要移动)。

表 7: 量子叠加与经典混合差异测量实验数据记录表

序号	名称	数据	单位
1	Laser2 + PBS1 反射功率		dbm
2	Laser1 + PBS1 透射功率		dbm
3	半波片 2 转动 0°	PBS2 透射功率	dbm
		PBS2 反射功率	dbm
4	半波片 2 转动 22.5°	PBS2 透射功率	dbm
		PBS2 反射功率	dbm
5	半波片 2 转动 45°	PBS2 透射功率	dbm
		PBS2 反射功率	dbm
6	半波片 2 转动 67.5°	PBS2 透射功率	dbm
		PBS2 反射功率	dbm
7	半波片 2 转动 90°	PBS2 透射功率	dbm
		PBS2 反射功率	dbm
8	半波片 2 转动 112.5°	PBS2 透射功率	dbm
		PBS2 反射功率	dbm
9	半波片 2 转动 135°	PBS2 透射功率	dbm
		PBS2 反射功率	dbm
10	半波片 2 转动 157.5°	PBS2 透射功率	dbm
		PBS2 反射功率	dbm
11	半波片 2 转动 180°	PBS2 透射功率	dbm
		PBS2 反射功率	dbm
12	半波片 2 转动 202.5°	PBS2 透射功率	dbm
		PBS2 反射功率	dbm
13	半波片 2 转动 225°	PBS2 透射功率	dbm
		PBS2 反射功率	dbm
14	半波片 2 转动 247.5°	PBS2 透射功率	dbm
		PBS2 反射功率	dbm
15	半波片 2 转动 270°	PBS2 透射功率	dbm
		PBS2 反射功率	dbm

表 8: 量子叠加与经典混合差异测量实验数据记录表

16	半波片 2 转动 $292.5^\circ$	PBS2 透射功率		dbm
		PBS2 反射功率		dbm
17	半波片 2 转动 $315^\circ$	PBS2 透射功率		dbm
		PBS2 反射功率		dbm
18	半波片 2 转动 $337.5^\circ$	PBS2 透射功率		dbm
		PBS2 反射功率		dbm
19	半波片 2 转动 $360^\circ$	PBS2 透射功率		dbm
		PBS2 反射功率		dbm
20	半波片 2 的光轴转至于水平方向 呈 $22.5^\circ$ 打开 Laser2	PBS2 透射功率		dbm
		PBS2 反射功率		dbm
21	关闭 Laser2 + 放置半波片 1 且光 轴呈 $22.5^\circ$	PBS2 透射功率		dbm
		PBS2 反射功率		dbm

## 2.2 实验二--单光子的探测及相应探测器效率的测量

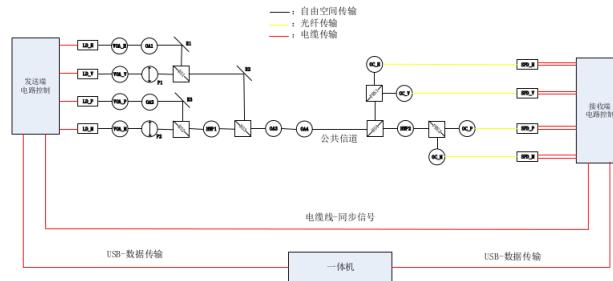


图 9: 探测器效率测量示意图

- 如图 9 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。
- 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; 使用可见光光功率计测量 M 路激光器输出功率并记录;

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. 接收端电路模块上点, 点击 M 路扫描, 得到 M 路计数值并记录; (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)

表 9: 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/s
6	SPD_M 探测器探测效率		%

### 2.3 实验三--单光子的标定

1. 单光子的标定如图 10 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 0.1 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; 上述过程即完成密钥分发系统的单光子标定。

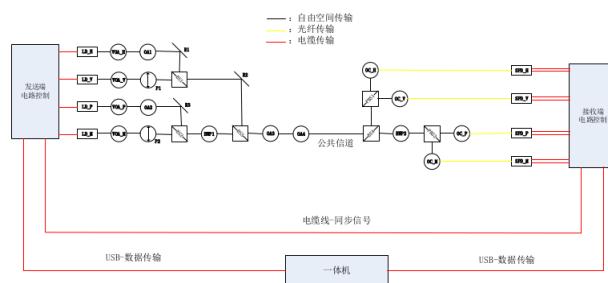


图 10: 单光子标定测量示意图

表 10: 单光子的标定数据记录表

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/s
2	M 路扫描, SPD_M 计数值		Hz/s
3	H 路扫描, SPD_H 计数值		Hz/s
4	V 路扫描, SPD_V 计数值		Hz/s
5	P 路扫描, SPD_P 计数值		Hz/s

## 2.4 实验四步骤

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;

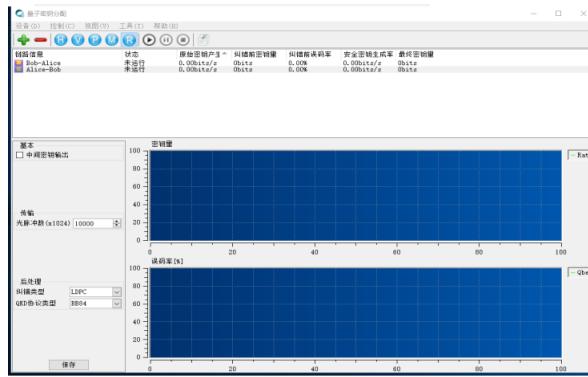


图 11: QKD 发送端界面

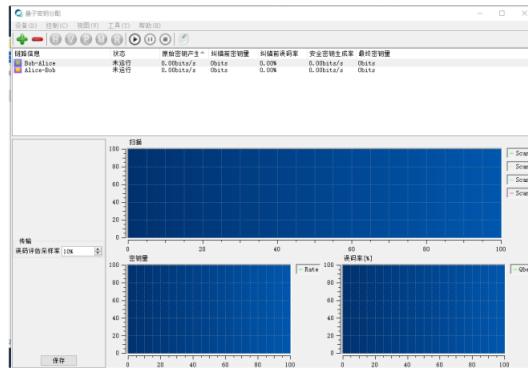


图 12: QKD 接收端界面

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；

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，比较文件用，选择十六进制文件。分别打开 transmitter-sift 和 receiver -sift，然后进行误码估计，由于 QKD 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%)

5. 采用毛玻璃或者纸片遮挡信道(在可调衰减片后遮挡), 观察系统统计数率和误码率变化情况。

序号	名称	数据	单位
1	QKD 系统软件统计密钥量		Hz
2	QKD 系统软件统计误码率		%
3	QKD 系统误码估计采样率		%
4	手动提取原始数据比例		%
5	对基后数据误码率		%
6	遮挡信道后系统密钥量		Hz
7	遮挡信道后系统误码率		%

## 2.5 实验中遇到的问题记录

无



## 2.6 实验原始记录与教师签名

表 7: 量子叠加与经典混合差异测量实验数据记录表

序号	名称	数据	单位
1	Laser2 + PBS1 反射功率	-12.32 <sup>12.05</sup>	dbm
2	Laser1 + PBS1 透射功率	-12.04	dbm
3	半波片 2 转动 0°	PBS2 透射功率 -9.96	dbm
		PBS2 反射功率 -5.49	dbm
4	半波片 2 转动 22.5°	PBS2 透射功率 -4.52	dbm
		PBS2 反射功率 -15.15	dbm
5	半波片 2 转动 45°	PBS2 透射功率 -15.28	dbm
		PBS2 反射功率 -4.63	dbm
6	半波片 2 转动 67.5°	PBS2 透射功率 -10.27	dbm
		PBS2 反射功率 -5.60	dbm
7	半波片 2 转动 90°	PBS2 透射功率 -5.83	dbm
		PBS2 反射功率 -9.14	dbm
8	半波片 2 转动 112.5°	PBS2 透射功率 -5.50	dbm
		PBS2 反射功率 -10.05	dbm
9	半波片 2 转动 135°	PBS2 透射功率 -15.58	dbm
		PBS2 反射功率 -4.60	dbm
10	半波片 2 转动 157.5°	PBS2 透射功率 -10.11	dbm
		PBS2 反射功率 -5.59	dbm
11	半波片 2 转动 180°	PBS2 透射功率 -4.48	dbm
		PBS2 反射功率 -14.85	dbm
12	半波片 2 转动 202.5°	PBS2 透射功率 -5.61	dbm
		PBS2 反射功率 -9.80	dbm
13	半波片 2 转动 225°	PBS2 透射功率 -14.97	dbm
		PBS2 反射功率 -4.58	dbm
14	半波片 2 转动 247.5°	PBS2 透射功率 -10.21	dbm
		PBS2 反射功率 -5.55	dbm
15	半波片 2 转动 270°	PBS2 透射功率 -4.52	dbm
		PBS2 反射功率 -15.45	dbm

2 实验步骤与记录

19  
表 8: 量子叠加与经典混合差异测量实验数据记录表

16	半波片 2 转动 292.5°	PBS2 透射功率	-5.45	dbm
		PBS2 反射功率	-10.12	dbm
17	半波片 2 转动 315°	PBS2 透射功率	-15.48	dbm
		PBS2 反射功率	-4.59	dbm
18	半波片 2 转动 337.5°	PBS2 透射功率	-15.48	dbm
		PBS2 反射功率	-4.59	dbm
19	半波片 2 转动 360°	PBS2 透射功率	-10.33	dbm
		PBS2 反射功率	-5.52	dbm
20	半波片 2 的光轴转至于水平方向 呈 22.5° 打开 Laser2	PBS2 透射功率	-5.99	dbm
		PBS2 反射功率	-5.98	dbm
21	关闭 Laser2 + 放置半波片 1 且光 轴呈 22.5°	PBS2 透射功率	4.41	dbm
		PBS2 反射功率	-16.45	dbm

2.2 实验二--单光子的探测及相应探测器效率的测量

图 7: 探测器效率测量示意图

- 如图 7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。
- 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; 使用可见光光功率计测量 M 路激光器输出功率并记录;

图 8: 单光子标定测量示意图

表 10: 单光子的标定数据记录表

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	68716160199	Hz/s
2	M 路扫描, SPD_M 计数值	6812815977	Hz/s
3	H 路扫描, SPD_H 计数值	68127159884	Hz/s
4	V 路扫描, SPD_V 计数值	68127161549	Hz/s
5	P 路扫描, SPD_P 计数值	68386	Hz/s
			31435 68378 31825 31118 31515 31590 160971

## 2.4 实验四步骤

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, 点击右侧的运行按钮;

单光子的探测及相应探测器效率的数据记录表

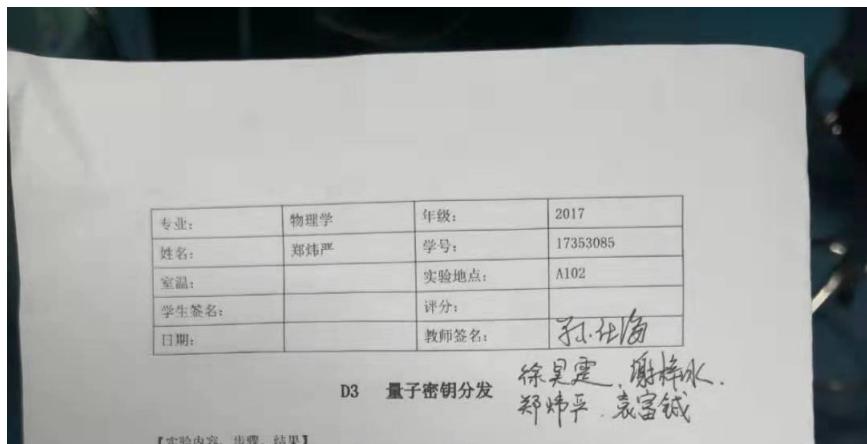
名称	数据	单位
M 激光器功率	10.63	dbm
总需要衰减值	103.695	db
衰减片理论需调节衰减值	7.695 4.323	db
衰减片实际调节衰减值	7.74 7.7374.21	db
路 SPD_M 探测计数值	6876 160199	Hz/s
探测器探测效率	6.87 16.02	%

11.52 mW

## 的标定

$$\text{dbm} = \log \frac{P}{1\text{mW}}$$

图 8 所示, H、V、P、M 路光路到达公共信道时, 出射



### 3 分析与讨论

专业:	Physics	年级:	17
姓名:	徐昊霆	学号:	17353071
日期	2019 年 10 月 28 日		
评分		教师签名	

#### 3.1 实验一--经典混合与量子混合的差异

简单地说，本实验就是验证将一束水平偏振的光与一束垂直偏振光叠加，如果这两束光来源于同一束光，则他们的相位差为 0，这时得到的就是  $45^\circ$  线偏振光，如果这两束光源不来自同一束光，那么他们叠加之后便不是  $45^\circ$  的线偏振光。在实验中，我们通过测量功率来确定它的偏振方向。在实验中，我们先通过不断旋转半波片找到半波片的光轴，之后我们同时打开了 laser1 和 laser2，得到的 PBS2 透射功率为

$$P_{\text{classical}} = -5.99 \text{ dBm} \quad (18)$$

发现它与反射功率几乎相同，这说明两个激光器叠加出来的光并不是  $45^\circ$  线偏振光。反而当只打开一个激光器的时候，我们发现透射功率很大，而反射功率实际上比透射功率小几个数量级（反射功率大约为  $-16.45 \text{ dBm}$ ，相比于透射功率  $4.41 \text{ dBm}$  很小），这说明一个激光器经过两个半波片之后得到的是  $45^\circ$  线偏振光。

从这个实验我们可以体会到经典叠加和量子叠加的区别，对于经典叠加，两个相位差不固定，从而一个水平的线偏振光和一个垂直的线偏振光不能合成一个  $45^\circ$  的线偏振光，而对于经典叠加，我们发现确实得到了  $45^\circ$  的线偏振光，这是因为相位差恒定的缘故。

#### 3.2 实验二--单光子的探测及相应探测器效率的测量

在实验中，我们首先要将一个激光衰减到单光子的态。为了达到这一目的，我们首先使用单光子的能量  $4.92 \times 10^{-13} \text{ W}$ ，和激光器的实际功率，计算总共需要的衰减值，再根据实验箱内的标记，计算出光路中间的衰减值。光路中间的衰减值应当比总需要的衰减值小，这时剩下的衰减值使用 VOA\_M 可调衰减片补充。之后我们打开激光，使单光子探测器运作，记录下计算机得到

的探测计数值。经过公式

$$M = f\mu\eta \quad (19)$$

计算出效率。其中  $M$  为单光子探测器的计数值， $f$  为激光的频率， $\mu$  为平均光子数脉冲。最后我们实验计算得到单光子探测器的探测效率为

$$\eta = 16.02\% \quad (20)$$

与实验讲义中 [1] 进行对比，实验讲义中给出的参考值为 20% 量级上是正确的，差异是由于各个仪器的差异性造成的。

### 3.3 实验三--单光子的标定实验

之前我们的理论计算是使得到达单光子探测器时使得平均光子数为 0.1 光子/脉冲，这时为了后面的量子秘钥分发实验做准备，我们将公共信道上的平均光子数调整为 0.1 光子/脉冲。这个计算与前面的计算类似，只不过不要计入公共信道之后的元器件。经过计算得到探测器计数值应有的数值，调节每一条光路前面的 VOA 衰减片，使得探测器计数值与理论值相符<sup>2</sup>。具体的理论计算结果请看数据记录表。在实验中我们非常成功地将各个值调节到理论值附近，相对误差大致为

$$\frac{\delta N}{N} \simeq 1\% \quad (21)$$

可见标定到了非常高的精度。

### 3.4 实验四--量子秘钥分发实验

实验中我们开启了随机分发偏振光的模式，最终运行得到的软件界面如图 13 所示。

---

<sup>2</sup>在具体实验中，由于有些 VOA 比较松动，调节起来比较困难，但是我一上去调就调出来了，我因此非常有成就感。

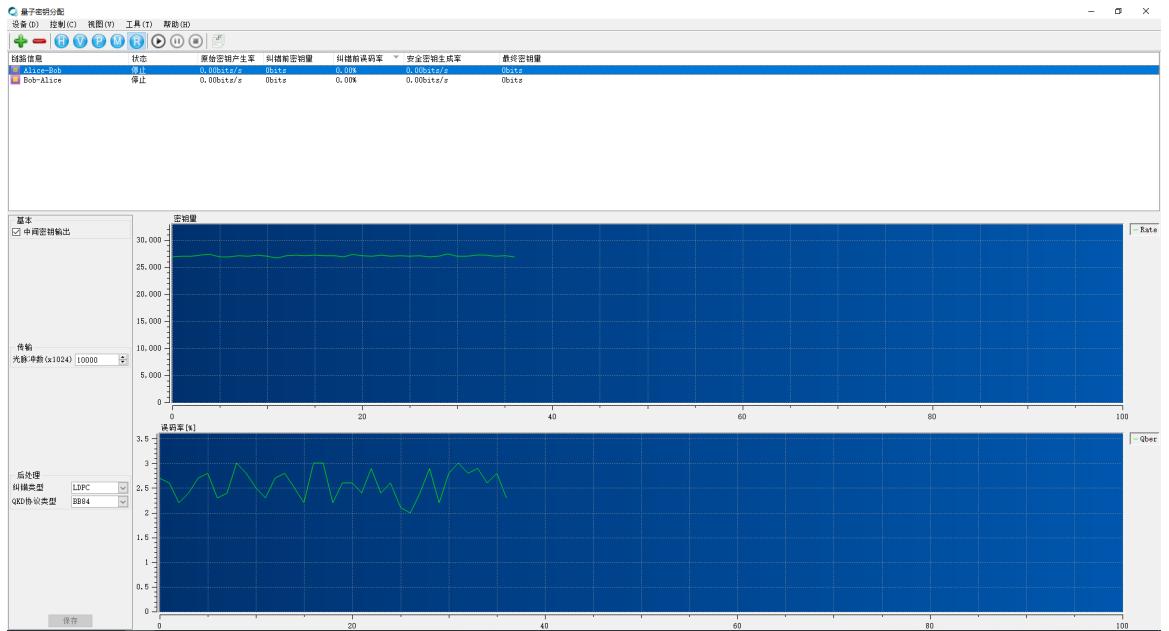


图 13: 量子秘钥分发实验的运行结果

通过软件上显示的数值，我们得知 QKD 系统的统计密钥量为

$$N = 10397 \text{Hz} \quad (22)$$

可知单位时间内传输的信息量很大，软件上自动估计的误码率为 2.64%，小于有效通信的最大误码率 11%，故可以认为这次通信有效。遮挡信道后，我们发现系统的密钥量显著降低，只有 800Hz，而且误码率大幅提升，大约为 55%。

为了得到更加准确的误码率，我们将发送和接收的数据提取出来。并将 16 进制数据格式转换为 2 进制数据格式，并算出误码率，具体的 python 代码如下所示

```
import math
import numpy as np

path_r = "receiver_sift.bin"
path_t = "transmitter_sift.bin"

with open(path_r, "rb") as f1:
    receiver = f1.read()
```

```

with open(path_t, "rb") as f2:
    transmitter = f2.read()

def hex2bin(sift):
    out = []
    for he in sift:
        bi = "{:0>8}".format(bin(he)[2:])
        bi = np.array(list(bi))
        out.append(bi)
    return out

sift_r = np.array(hex2bin(receiver))
sift_t = np.array(hex2bin(transmitter))

judge = (sift_r == sift_t)

correct = np.sum(judge)
total = judge.shape[0] * judge.shape[1]

print("误码率:", (total - correct) / total)

```

通过运行上面的代码，我们求得对基后的误码率为 2.60%，与软件中给的数值十分接近，我们下面来分析对基前，raw data 的误码率，我们预测如果没有对基，那么误码率则会非常高。经过计算我们得到误码率为 49.68%。可见因为不同偏振态的光子是随机分发的，误码率接近与 50%，上面的计算代码如下所示。计算代码和原文件也可以在 [?] 上找到。

```

program convert_raw
    !!Reading and computing the error rate of quantum key distribution
    !!Code by Haoting Xu
    !!2019/10/26
    !_____
    !input file
    implicit none
    character(LEN=*), parameter :: receive_file = "receiver_raw.bin"

```

```
character(LEN=*),parameter :: transmit_file = "transmitter_raw.bin"
character(LEN=1024) line
integer n,i,j! n is the amount of keys
integer ,dimension(:, :) ,allocatable :: receive,transmit
character(LEN=17) tmp1
character(LEN=2) tmp2
character(LEN=1) TMP3
integer error
real*8 rate
open(10,FILE = receive_file)
n=0
do
  read(10,* ,ERR=100,END=100) line
  n=n+1
end do
write(*,*) line
100 close(10)
write(*,*) "Read",n, "key samples ."
allocate(receive(2,n),transmit(2,n))
open(10,FILE = receive_file)
do i=1,n
  read(10,'(A17,I1,A2,I1,A1)') tmp1, receive(1,i),tmp2, receive(2,i),tmp3
end do
close(10)
error=0
do i=1,n
  if (receive(1,i) /= receive(2,i)) then
    error = error +1
  end if
end do
write(*,*)"Error is ",error
rate = 100.*error/n
```

```

write(*,*) "Error rate is ",rate,"%"
end program convert_raw

```

### 3.5 实验后思考题

1、量子相干叠加与经典概率混合的本质区别是什么，为什么说经典概率混合是量子相干叠加的特例？

量子相干叠加是概率幅的叠加之后平方得到概率，而经典概率混合是概率的直接相加，通常来说，如果一个态的波函数为

$$\Psi_1 = \psi_1 e^{i\varphi_1} \quad (23)$$

$$\Psi_2 = \psi_2 e^{i\varphi_2} \quad (24)$$

将概率幅叠加，并作内积得到概率

$$P = \langle \Psi_1 + \Psi_2 | \Psi_1 + \Psi_2 \rangle = |\psi_1|^2 + |\psi_2|^2 + 2|\psi_1||\psi_2|e^{i(\varphi_1-\varphi_2)} \quad (25)$$

经典叠加的表达式为

$$P = P_1 + P_2 = |\psi_1|^2 + |\psi_2|^2 \quad (26)$$

为什么说经典叠加是量子叠加的特例呢？我们考虑两个波函数的相位差  $\varphi_1 - \varphi_2$  随时间变化。比如，对于  $\omega$  相同的两个波函数，那么他们的相位差就不随时间变化，如果两个波函数的  $\omega$  不同，那么相位差就会随着时间变化，可以假定，相位差随着时间变化的表达式为

$$\Delta\varphi = \Delta\omega t \quad (27)$$

那么，将量子叠加的表达式 25 对于时间取平均值，那么最后一项对于时间的平均值为 0，所以当两个波函数的相位差随时间振荡时，量子相干叠加退化为经典的概率叠加。

2、是否可以通过直接衰减任意的光源，比如白炽灯，到单光子级别来得到真正的单光子源吗？（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）。

光子应该用量子场论来描述，在量子场论中将场量子化得到光子的。将下面的场做二次量子化

$$\mathcal{L} = -\frac{1}{4} F_{\mu\nu} F^{\mu\nu} \quad (28)$$

对于特定的动量和偏振，引入产生和湮灭算符  $a_{\vec{k},\lambda}^\dagger, a_{\vec{k},\lambda}$ ，他们满足像谐振子中升降算符一样的对易关系 [2]

$$[a_{\vec{k},\lambda}, a_{\vec{k}',\lambda'}^\dagger] = \delta_{\vec{k}\vec{k}'}\delta_{\lambda\lambda'} \quad (29)$$

因此  $|n_{\vec{k},\lambda}\rangle$  记为

$$|n_{\vec{k},\lambda}\rangle = \prod_{\vec{k},\lambda} \frac{(a_{\vec{k},\lambda}^\dagger)^{n_{\vec{k},\lambda}} |0\rangle}{\sqrt{n_{\vec{k},\lambda}!}} \quad (30)$$

因此，光子的哈密顿量为

$$H = \sum_{\vec{k},\lambda} \left( \hbar\omega a_{\vec{k},\lambda}^\dagger a_{\vec{k},\lambda} + \frac{1}{2} \right) \quad (31)$$

由这个哈密顿量实际上可以得到  $|n_{\vec{k},\lambda}\rangle$  是本征态，能量的本征值为

$$E = n_{\vec{k},\lambda} \hbar\omega \quad (32)$$

在激光中，光子的态可以由下面的相干态来描述，在量子力学中，它模拟了经典力学的谐振子。

$$|\alpha\rangle = e^{-|\alpha|^2/2} e^{\alpha a^\dagger} |0\rangle \quad (33)$$

其中  $e^{\alpha a^\dagger}$  满足

$$e^{\alpha a^\dagger} |0\rangle = \sum_n \frac{\alpha^n}{n!} (a^\dagger)^n |0\rangle \quad (34)$$

其中参数  $\alpha$  与总光子数有关

$$n = \langle \alpha | a^\dagger a | \alpha \rangle = |\alpha|^2 \quad (35)$$

从上面的相干态实际上可以得到出射的光子满足泊松分布。所以，当衰减这样的一个态（这样的状态就是激光中的状态），会得到单光子，因为相干态系数  $\alpha$  直接与光子数  $n$  有关。而衰减别的态（一般来说是许许多多这样的相干态的线性组合），则不能单纯的得到光子数很少的态。

### 3、理解单光子探测器后脉冲效应的产生原因。

后脉冲现象是导致单光子探测噪声的主要来源之一 [3]。在雪崩发生时，雪崩倍增区中的任何缺陷都有可能成为载流子的俘获区域。当有光子入射单光子探测器时，基于光电效应产生的电荷穿越探测器的雪崩倍增区，一些载流子被这些缺陷俘获。当光电转换过程结束后，这些从缺陷中心释放的载流子受到电

场加速，会再次引发雪崩，产生与前一次雪崩脉冲相关联的后脉冲，从而引起探测器误计数。

4、理解单光子探测器的暗计数原理，并设计实验装置测量探测器的暗计数率。

单光子探测器使用光电效应来将光信号转化为电信号，但是这样转化的电信号较为微弱，这时使用雪崩效应来放大原来的电信号，使其变为可测量的信号。

5、对基后的数据，为什么会有误码出现，如何降低误码？

对基之后，如果传输的信道理想，应该不会出现误码。但是由于光子的传输信道上的元器件可能改变光子的偏振状态。如果偏振状态发生了质的改变，那么 Alice 和 Bob 有一定概率不能得到相同的结果，因此会有误码出现。降低误码率的办法可以降低光子传输信道上的损耗。

6、部分遮挡信道后，QKD 系统的计数率和误码率会怎么变化，为什么？

部分遮挡信道后，系统的计数率降低，误码率升高。遮挡信道之后单位时间内接收器接收到的光子减少，故系统的计数率减小。而部分遮挡信号则意味着 Alice 不再是发射 H,V,R,L 四种偏振状态的光子，而是少发送一种特定的光子，误码率大大提升。

## 参考文献

- [1] LOVEPHYSICS, 量子密钥分发. <http://lovephysics.sysu.edu.cn/lib/exe/fetch.php?media=courses:modernphysicslabzhuhai:lecture-d3-1-2017.pdf>.
- [2] D. TONG, *Applications of quantum mechanics*. <http://www.damtp.cam.ac.uk/user/tong/aqm.html>.
- [3] F. XIAOXIA, H. TAO, D. SHAUNGLI, X. LIANTUAN, AND J. SUOTANG, *Analysis of afterpulse characteristics in detecting single photon synchronously*, Journal of Test and Measurment Technology, (2008).