预习报告		实验记录		分析讨论		总成绩	
25		30		25		80	

专业：	物理学	年级：	2022 级
姓名：	戴鹏辉	学号：	2344016
日期：	2024/9/23	教师签名：	

D3　量子密钥分发

【实验报告注意事项】

(1) 实验报告由三部分组成：

(1) 预习报告：（提前一周）认真研读**实验讲义**，弄清实验原理；实验所需的仪器设备、用具及其使用（强烈建议到实验室预习），完成课前预习思考题；了解实验需要测量的物理量，并根据要求提前准备实验记录表格（第一循环实验已由教师提供模板，可以打印）。预习成绩低于 10 分（共 20 分）者不能做实验。

(2) 实验记录：认真、客观记录实验条件、实验过程中的现象以及数据。实验记录请用珠笔或者钢笔书写并签名（**用铅笔记录的被认为无效**）。**保持原始记录，包括写错删除部分，如因误记需要修改记录，必须按规范修改。**（不得输入电脑打印，但可扫描手记后打印扫描件）；离开前请实验教师检查记录并签名。

(3) 分析讨论：处理实验原始数据（学习仪器使用类型的实验除外），对数据的可靠性和合理性进行分析；按规范呈现数据和结果（图、表），包括数据、图表按顺序编号及其引用；分析物理现象（含回答实验思考题，写出问题思考过程，必要时按规范引用数据）；最后得出结论。

实验报告就是将预习报告、实验记录、和数据处理与分析合起来，加上本页封面。

(2) 实验报告注意事项

i. 系统工作温度在 15°-30° 的环境中，尤其避免过高温度下使用本系统。

ii. 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。

iii. 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。

iv. 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。

v. 请不要打开单光子探测器的黑色遮盖物。

vi. 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。

目录

D3　量子密钥分发　预习报告

1.1　实验目的

(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。

1.2　仪器用具

表 1: 偏振测量实验

编号	仪器用具名称	数量	主要参数（型号，测量范围，测量精度等）
1	准直激光器	1	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: 单光子标定的用具

编号	仪器用具名称	数量	主要参数（型号，测量范围，测量精度等）
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，测量范围，测量精度等）
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	直流稳压电源	1	GPD-3303D

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，测量范围，测量精度等）
1	密钥分发系统	1	波长：404nm

1.3　原理概述

- **量子密钥分发的基本原理：**
  - 量子密钥分发（Quantum Key Distribution, QKD）是一种利用量子力学基本原理进行密钥分发的方法，主要解决经典密码体系中密钥安全分发的问题。QKD 的安全性并不是依赖算法复杂性，而是基于量子力学的物理定律，如测量塌缩理论、海森堡不确定原理和量子不可克隆定律。这些定律确保了任何窃听行为都会干扰量子态，从而被合法通信双方检测到。
  - QKD 采用单光子作为信息的物理载体，单光子是光场的最小能量单元，具有不可分割性；单光子的量子态不可克隆，无法通过一次测量完全准确地复制单光子的状态；测量单光子的偏振态具有概率性，测量结果依赖于量子态处于测量算子的本征态时才能精确获得。
- **BB84 协议的工作原理：**
  - BB84 协议是最早提出的 QKD 协议，利用光子的偏振态来编码信息。光子的偏振态随机选自两个基：水平/垂直基（$\oplus$ 基）和对角基（$\otimes$ 基）。在通信中，发送方（Alice）随机选择基和态来制备光子并发送给接收方（Bob）。
  - Bob 接收到光子后，也随机选择一个基进行测量。由于 Bob 的基选择是随机的，只有当测量基与 Alice 的制备基一致时，Bob 的测量结果才是有意义的；当基不同时，测量结果无效。
  - Alice 和 Bob 在公开信道上公布各自的基的选择，而不公布测量结果，仅保留基相同的测量结果用于密钥生成。这种随机选择和匹配的机制使得窃听者难以获取信息，因为窃听者的任何测量都会引入错误，并被 Alice 和 Bob 检测到。
- **QKD 的安全性基础：**
  - 单光子态的不可分割性和不可克隆性使得窃听者无法在不被发现的情况下复制或测量这些光子。
  - 在 BB84 协议中，如果窃听者试图测量光子状态，其随机选择的测量基可能与 Alice 的基不匹配，从而干扰量子态，导致误码率增加。Alice 和 Bob 通过检测误码率来判断是否存在窃听，当误码率超过安全阈值时，说明存在窃听行为。
  - QKD 的安全性是信息论上的无条件安全，即只要误码率低于一定阈值，通过后续的纠错和隐私放大步骤，Alice 和 Bob 可以提取出无条件安全的共享密钥。

1.4　实验前思考题

思考题 1.1： 回顾偏振光实验，说明 $\lambda/2$ 波片，$\lambda/4$ 波片的工作原理；

晶体介质的折射率与光波的偏振方向有关，是各向异性的。当晶体介质的折射率在两个方向上不同时，分别记作 n_x 和 n_y，且 $n_x > n_y$ 时，可以定义两个方向上的相位速度 c_x 和 c_y，其中 $c_x < c_y$。晶体中的 x 轴被称为慢轴，y 轴被称为快轴。在晶体中，一条折射线总符合普通的折射定律，称作寻常光（或 o 光），而另一条折射线不遵守普通的折射定律，称作非常光（或 e 光）。o 光和 e 光都是偏振光，且两光束的振动方向相互垂直。

因为通过该偏振片导致 x 和 y 方向偏振光的光程差为：$\delta = (n_x - n_y)d$，d 为偏振片厚度。

(1) $\lambda/2$ 波片指，对于一个给定的波长 λ 平行光正入射波晶片时，o 光和 e 光的光程差 $\delta = \frac{\lambda}{2}$。另外，$\lambda/2$ 波片是对特定波长的光通过，否则没有任何意义。

若线偏振光经过 $\lambda/2$ 波片，出射光还是线偏振光，但相对于 o 轴或 e 轴对称。特别的，平行于 o 轴或 e 轴入射的偏振光，经过波片后方向保持不变。

若椭圆偏振光经过 $\lambda/2$ 波片，出射光仍是椭圆偏振光，但旋转方向相反。

(2) $\lambda/4$ 波片指，对于一个给定的波长 λ 平行光正入射波晶片时，o 光和 e 光的光程差 $\delta = \frac{\lambda}{4}$。同样的，$\lambda/4$ 波片是对特定波长的光通过，否则没有任何意义。

线偏振光通过 $\lambda/4$ 波片后，当入射角为 0°、90°、180°、270° 时，出射光仍然是线偏振光。
当入射角为 45°、135°、225°、315° 时，出射光变为圆偏振光。
对于其他入射角度，出射光为椭圆偏振光。

思考题 1.2： 如何检测一个任意方向的线偏振光？

通过使用线偏振片和光功率计，可实现任意方向的线偏振光的检测，具体方法如下：

(1) 将一个线偏振片置于入射光路中，并让光通过该线偏振片。

(2) 缓慢旋转线偏振片，记录光强随角度的变化。检测器记录透过偏振片的光强度 I。

(3) 当透过光强达到最大值时，说明此时线偏振片的偏振方向与入射线偏振光的偏振方向平行；

当透过光强达到最小值（理论上为零）时，线偏振片的偏振方向与入射线偏振光的偏振方向垂直。

具体的数学关系可以用马吕斯定律（Malus's Law）描述：

$$I = I_0 \cos^2 \theta$$

其中 I 为透过偏振片的光强，I_0 为入射光强，θ 为入射光的偏振方向与偏振片方向之间的夹角。

思考题 1.3： 单光子为什么不能直接用普通功率计测量？

单光子不能直接用普通功率计测量，主要原因如下：

(1) **功率计的灵敏度不足：** 普通功率计通常用于测量宏观光强（如 mW 或 W 级别），它们的探测器需要足够多的光子来产生可测的电信号；而单光子的能量极其微小，通常在 eV 量级，对普通功率计来说，这样的能量远低于其探测阈值，导致无法检测单光子事件。

(2) **响应时间和噪声问题：** 普通功率计的响应时间较长且噪声较大，难以分辨单个光子的到达。单光子事件发生的时间间隔可能非常短，并且在单光子水平下，信号很容易被背景噪声淹没。

(3) **检测原理不同：** 普通功率计测量的是光的平均功率，通过探测大量光子的累积效应获得信号。单光子测量需要通过专门设计的单光子探测器（如光电倍增管、雪崩光电二极管或超导纳米线单光子探测器），这些探测器能够在单光子事件发生时产生响应，记录单个光子的到达时间和数量。

(4) **量子效率和探测机制：** 普通功率计的量子效率通常较低，对单光子的探测效率不足。而单光子探测器则设计有高量子效率，能够可靠地探测并计数单个光子。

思考题 1.4：检验单光子探测器的探测效率可以用强光吗？

不可直接使用强光，因为单光子探测器设计用于探测极低光强度下的单光子事件。使用强光源可能会导致以下问题：

(1) **饱和效应：**单光子探测器的探测机制是基于对单个光子的响应设计的。当入射光强度过高时，探测器会进入饱和状态，无法区分单个光子事件，导致信号失真，并且探测效率测量不准确。

(2) **探测器损坏风险：**单光子探测器通常具有较高的增益，用于放大微弱的单光子信号。强光会产生过大的电流，可能会损坏探测器的电子元件或造成永久性损坏。

(3) **非线性响应：**单光子探测器在强光下的响应不再是线性的，这与单光子探测的条件不符，导致效率评估失真。探测效率是定义在单光子条件下的，即探测器对单个光子的响应概率。

正确的探测效率检验方法检验单光子探测器的探测效率一般采用低强度的光源，保证光强度足够低，使得光子事件是稀疏的且近似服从泊松分布。具体步骤如下：

(1) **使用弱光源：**使用经过强度衰减的激光器或 LED，光强控制在单光子水平上。通常通过中性密度滤光片或分束器来精确控制光子的通量。

(2) **参考探测器：**使用已知效率的标准探测器或计数装置作为参考，与待测单光子探测器同时测量同一光源的光子通量。

(3) **统计计数事件：**记录单光子探测器和参考探测器在相同条件下的响应事件数量，通过比较计数来计算单光子探测器的探测效率。

(4) **量子效率计算：**探测效率（量子效率）定义为探测到的光子数与实际入射光子数之比。

使用弱光源和统计方法能够精确测量单光子探测器的探测效率，确保测量结果的准确性。

思考题 1.5：BB84 协议的原理和步骤。

- **BB84 协议的基本原理：**
  - BB84 协议利用了量子态不可克隆原理和测量干扰原理。在量子通信中，量子比特（qubit）不能被精确复制，并且任何对量子态的测量都会不可避免地对量子态产生干扰。因此，窃听者试图在通信过程中窃听信息时，必然会在数据中留下痕迹，这些痕迹可以被通信双方检测到。
- **BB84 协议的步骤：**
  (1) **量子态编码：**
  - 通信双方称为发送者 Alice 和接收者 Bob。Alice 随机选择两种基和两个状态来发送比特。
  - Alice 使用两种正交基态来编码信息：
    * 直角基（$\oplus$ 基）：$\{|0\rangle, |1\rangle\}$
    * 对角基（$\otimes$ 基）：$\{|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}, |-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}\}$

  - Alice 随机选择这些基态中的一个，来表示经典比特 0 或 1。例如：
    * 用 $\oplus$ 基的 $|0\rangle$ 表示比特 0，用 $\oplus$ 基的 $|1\rangle$ 表示比特 1。
    * 用 $\otimes$ 基的 $|+\rangle$ 表示比特 0，用 $\otimes$ 基的 $|-\rangle$ 表示比特 1。

(2) **量子态传输：**

  - Alice 将随机选择的量子态发送给 Bob。由于量子态的不可克隆性，Eve 无法准确复制或窃听而不被察觉。

(3) **基的选择与测量：**

  - Bob 在接收到量子态后，随机选择 $\oplus$ 基或 $\otimes$ 基对每个光子进行测量。由于 Bob 的基选择是随机的，测量结果在 Alice 的基与 Bob 的基相同时是正确的，在基不同的时候则是随机的。

(4) **基的公布与筛选：**

  - Alice 和 Bob 通过经典通信渠道（可以公开，但不保密）公布他们选择的基，**但不公布测量结果**。然后，他们保留那些在基选择相同的情况下的测量结果，丢弃基不同的测量结果。

(5) **错误率检查：**

  - Alice 和 Bob 各自拥有一组相同基的比特序列，为了检测是否有窃听者存在，他们随机选择一部分比特进行比较。如果误码率低于一定阈值（通常设定在 11% 以内），则说明没有明显的窃听，或者说窃听干扰较小，可以认为是安全的；如果误码率过高，则表明可能存在窃听，他们会丢弃这些密钥并重新开始协议。

(6) **密钥提纯和隐私放大：**

  - Alice 和 Bob 根据检测到的错误率，使用纠错和隐私放大技术来去除误差和窃听者可能获取的信息，生成一个更短但更安全的密钥。

(7) **共享密钥的生成：**

  - 经过上述步骤后，Alice 和 Bob 共享一条安全密钥，可以用于后续的加密通信。

- **BB84 协议的安全性：**
  - BB84 协议的安全性来自于量子测量的不可逆性和不可克隆定理：任何第三方在尝试窃听量子信道时，必然会干扰量子态，从而导致测量误差。这些误差可以被 Alice 和 Bob 检测到，从而保证密钥分发的安全性。即便第三方窃听了经典通信信道，由于该信道上不传输实际密钥值，仅基的选择信息，因此不会危及密钥的安全性。
  - BB84 协议是量子密码学的基础，广泛用于研究和实际应用中，确保通信安全性。

思考题 1.6： 密钥分发过程中，为什么需要有同步信号？

- 在量子密钥分发过程中，特别是在 BB84 协议中，同步信号的作用至关重要。具体原因如下：

(1) **确保接收者正确接收每个量子态：**在量子密钥分发过程中，发送方（Alice）会按照一定的时间顺序发送一系列量子态给接收方（Bob）。同步信号用于确保 Bob 在正确的时间窗口内进行测量，这样他能够与 Alice 发送的量子态一一对应。如果没有同步信号，Bob 可能会在错误的时刻进行测量，从而导致数据对不上，增加误码率。

(2) **减少测量误差和丢包率：**如果发送和接收没有时间上的同步，量子态可能在 Bob 还未准备好时就已经发出或者被测量，导致测量失败或丢失。这会增加数据损失，降低密钥生成效率。而同步信号可以帮助双方在测量时刻上匹配，减少测量误差和丢包率。

(3) **避免干扰和重叠：**没有同步信号时，不同量子态之间可能会发生重叠或干扰，尤其是在高速传输的情况下。同步信号确保每个量子态在独立的时间窗口内被测量，避免相邻态之间的干扰，保证密钥分发的准确性。

(4) **提高协议效率：**通过同步信号，Alice 和 Bob 可以协调他们的设备运行在相同的时间步伐下，最大限度地提高密钥分发速率。否则，由于不匹配的时序问题，可能会频繁出现测量空闲或无效的情况，降低系统整体效率。

(5) **检测和对抗窃听：**时间同步能够提高对潜在窃听者的检测能力。如果窃听者试图在信道中插入或篡改数据，同步不当可能会导致显著的误码率上升，从而暴露窃听行为。通过同步，Alice 和 Bob 更容易检测到任何异常的时序变化。

专业：	物理学	年级：	2022 级
姓名：	戴鹏辉	学号：	22344016
室温：	26℃	实验地点：	A
学生签名：		评分：	
实验时间：	2024/XXXX	教师签名：	

D3　量子密钥分发　实验记录

2.1　实验内容和步骤

2.1.1　实验一　XXXXXXXXX

2.2　实验数据记录

2.3　实验过程中遇到的问题记录

(1)

专业：	物理学	年级：	2022 级
姓名：	戴鹏辉	学号：	22344016
日期：	2024/XXXX	评分：	

D3　量子密钥分发　分析与讨论

3.1　实验数据分析

3.1.1　实验一 XXXXXX