





Alice 想安全地发送一串密码（密钥）给 Bob，但又担心有窃听者 Eve 在偷听。BB84 量子密钥分发协议（QKD）就是一种利用量子物理来解决这个问题的方法，其核心步骤如下：

1. 编码：Alice 随机生成一串 0 和 1。对于每一个数字，她再随机选择一种编码“基”（可以理解作为一种编码规则）来发送。
 - 直线基 (+)：用水平偏振 (—) 的光子代表 0，垂直偏振 (|) 的光子代表 1。
 - 对角基 (X)：用 135°偏振 (＼) 的光子代表 0，45°偏振 (/) 的光子代表 1。Alice 将这些携带了信息的单个光子逐一发送给 Bob。

“横竖”组量子：			“+”形接收器
“撇捺”组量子：			“x”形接收器
	代表0	代表1	

CSDN @Tang World

2. 测量：Bob 接收光子，但他不知道 Alice 每次用的是哪种“基”，所以他也只能为每个光子随机选择一种“基”（直线基或对角基）来测量。
3. 筛选：Alice 和 Bob 通过一个公开的普通信道（比如打电话）核对他们各自使用的“基”序列。他们会保留那些两人恰好选择了相同“基”的测量结果，并丢弃其余结果。这串筛选后的 0 和 1 就成了他们的共享密钥。
4. 安全检测：量子力学有一个关键原则——“测量即干扰”。如果窃听者 Eve 在半路试图测量光子，她也必须猜测用哪种基。只要她猜错，光子的状态就会被她改变，这会导致 Alice 和 Bob 最终筛选出的密钥出现异常高的错误率。通过比对一小部分密钥，他们就能发现窃听行为。

在 BB84 量子密钥分发系统中，需要使用单光子作为信息载体。一种可靠的单光子源是利用单个囚禁原子。该原子的电子可被激光从基态激发到激发态，随后电子自发跃迁回基态，并释放一个光子。

为精确控制出射光子的特性，现对该囚禁原子施加一个强度为 $B=1.0\text{ T}$ 的匀强磁场。已知原子的基态是 $^2S_{1/2}$ 态，其未受场扰动的能量为 $E_1=-3.40\text{ eV}$ ；原子的激发态是 $^2P_{1/2}$ 态，其未受场扰动的能量为 $E_2=-1.50\text{ eV}$ 。

- (1) 根据电偶极跃迁选择定则 ($\Delta m_J=0,\pm 1$)，计算从 $^2P_{1/2}$ 激发态所有可能的子能级跃迁回 $^2S_{1/2}$ 基态所有可能的子能级时，所释放光子的最大能量 E_γ 。
- (2) 要实现 BB84 协议，还需要对光子的偏振态进行调控。从塞曼效应的跃迁选择定则角度，设想一种可能的方法，用于产生线偏振光。

- (3) 在 BB84 协议中，为什么必须使用“单光子”而非包含多个光子的弱激光脉冲？请从安全性的角度，结合光子的量子特性简要说明。