

量子信息基础

第五章：量子通信

金潮渊

浙江大学信息与电子工程学院



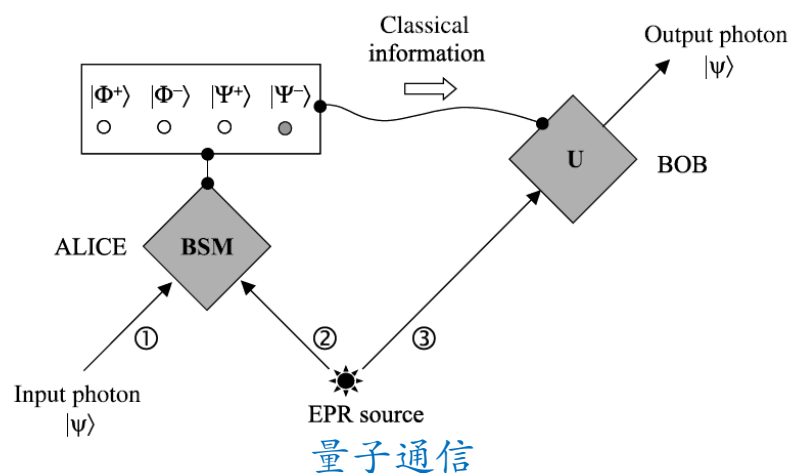
C5-4 单光子源和量子中继



课程回顾

纠缠态和量子隐形传态：

- 如果一个多粒子体系的波函数无法写作单个粒子波函数的乘积形式，这种量子态被称之为纠缠态。纠缠态可以看作张量空间中单态的线性组合，表达为张量积的形式。
- 量子隐形传态（Quantum teleportation）是一种利用量子纠缠来传送量子态至任意距离的技术，是一种全新的通信方式。1993年，Charles H. Bennett提出了第一个量子隐形传态的方案。1997年，Bouwmeester, Pan和Zeilinger在实验中实现了量子隐形传态。
- 量子隐形传态是量子非定域性的自然结果。但传递信息的速度不能超过光速。



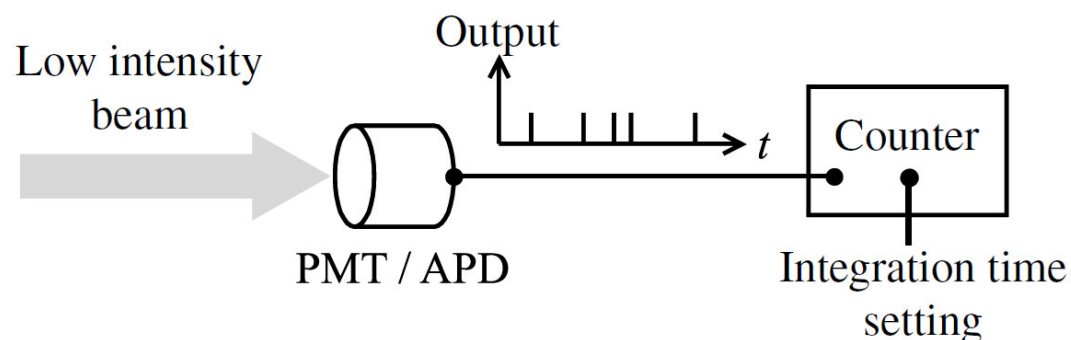
量子密钥分发的破绽与防御

- 在QKD中，通常使用弱相干态（Weak Coherent State, WCS）作为信息载体，该状态是一个包含少量光子的概率分布（泊松统计）。
- 攻击者（Eve）可以截取传输给接收方（Bob）的光子脉冲，并尝试将其分割成多个较低能量的脉冲（PNS）。攻击者测量或存储分割后的光子，以获取关于密钥的信息，然后将剩余的光子发送给接收方或者丢弃。如果分割过程没有被检测到，攻击者就可以在不被发现的情况下获得密钥信息。
- 举一个简单的例子：Alice某次发送的光脉冲中包含2个光子。Eve选择错误基的情况下，有50%概率获知自己选错，因而可以选择性抛弃改组光子，降低自己发射错误基信号的概率。该情况随多发光子数增加而恶化。
- 解决光子数攻击（PNS）的一种途径是使用单光子源。该技术目前需要解决的难点是提高触发式单光子产生速率。



光子计数(1)

- 光电效应代表了光吸收的过程，其解释能够在量子化原子能级的基础上进行。光的粒子性的真正确认要等到单光子反聚束效应（photon antibunching, Kimble, Dagenais and Mandel, 1977）和双光子干涉现象（two-photon interference, Hong, Ou, and Mandel, 1987）的实验验证。两者的基础都是光子计数。
- 考虑一束极弱的光入射到一个光子计数器上。光子计数器包含一个单光子探测器，比如光电倍增管（PMT）或者雪崩光电二极管（APD），和一个电子计数器。单光子探测器产生一个一个的电压短脉冲，而电子计数器记录一段时间内的脉冲数量。



光子计数(2)

考虑一束单色的相干光线，角频率为 ω ，功率为 P ，定义光子速流 Φ 为单位时间内经过光束截面的光子数

$$\Phi = \frac{P}{\hbar\omega}$$

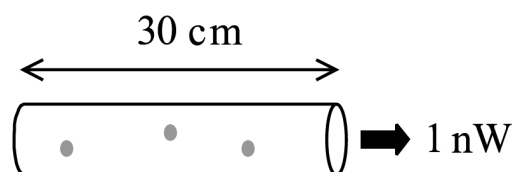
光子计数器的量子效率 η 为光子计数和入射光子总数之间的比例，所以在计数时间 T 内被计数器记录的平均光子数为

$$N(T) = \eta\Phi T = \frac{\eta PT}{\hbar\omega}$$

光子计数器一般具有一个最大计数，一般由单光子探测器的死区时间（dead time）所决定，也就是完成一个计数后，探测器恢复正常状态所需要的时间。比如死区时间1微秒，对应的最大计数为 10^6 每秒。如果假设量子效率为10%，那么可计数光束的功率极限大约是 $\sim 10^{-12}\text{W}$ 。这是非常弱的光功率！



光子计数(3)



考虑氦氖激光器发出波长为633nm（对应的单光子能量为2eV）的红光，如果激光功率为1mW，并衰减 10^6 倍。平均光子速流为：

$$\Phi = \frac{P}{\hbar\omega} = \frac{10^{-9}}{2.0 \times (1.6 \times 10^{-19})} = 3.1 \times 10^9$$

光的速度为 3×10^8 m/s，考虑3米长的光束，平均会有31个光子，对应的光子计数时间为 10^{-8} 秒。如果考虑更短的光子计数时间，比如1纳秒= 10^{-9} 秒，那么光子的数量会变成一个非整数3.1个光子，但光子计数必须是一个整数，如果测量多次，会得到类似于下面的结果

1, 6, 3, 1, 2, 2, 4, 4, 2, 3, 4, 3, 1, 3, 6, 5, 0, 4, 1, 1, 6, 2, 2, 6, 4, 1, 4, 3, 4, 6, ...

30次计数总共观测到大约95个光子。

如果计数时间更短，比如0.1纳秒= 10^{-10} 秒，平均每次测量会有0.31个光子，如果测量多次，会得到类似于下面的结果：

1, 0, 0, 1, 0, 0, 0, 0, 0, 1, ...

10次计数总共观测到大约3个光子。

量子通信

泊松统计(1)

- 由于光子的量子化特点，它的浮动范围遵循一定的统计规律。对于完美的相干光束（单色性非常理想的激光），光强和平均光子速流恒定，其遵循泊松光子统计。

考虑功率恒定为 P 的一束光，长度 L 内的平均的光子数为 $\bar{n} = \frac{\Phi L}{c} = \frac{PL}{c\hbar\omega}$

假设我们把 L 分成 N 段， N 是足够大的一个大数。对于长度 L/N 中发现一个光子的概率 $p = \bar{n}/N$ 是非常小的，这种情况下在长度 L/N 上发现2个或者多个光子的概率可以忽略。现在的问题为在 L 上发现 n 个光子概率 $\mathcal{P}(n)$ 是多大？

$$\mathcal{P}(n) = \frac{N!}{n!(N-n)!} p^n (1-p)^{N-n} = \frac{N!}{n!(N-n)!} \left(\frac{\bar{n}}{N}\right)^n \left(1 - \frac{\bar{n}}{N}\right)^{N-n} = \frac{1}{n!} \left(\frac{N!}{(N-n)! N^n}\right) \bar{n}^n \left(1 - \frac{\bar{n}}{N}\right)^{N-n}$$

利用斯特林近似

$$\ln(N!) \approx N \ln(N) - N, \quad N \gg 1$$



泊松统计(2)

$$\lim_{N \rightarrow \infty} \left[\ln \left(\frac{N!}{(N-n)! N^n} \right) \right] = 0$$

所以

$$\lim_{N \rightarrow \infty} \left[\frac{N!}{(N-n)! N^n} \right] = 1$$

另外

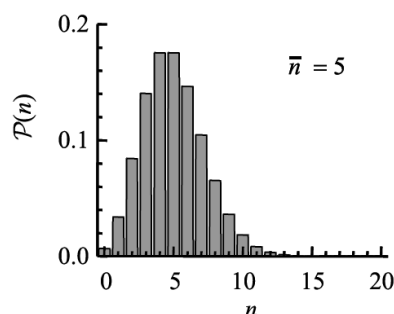
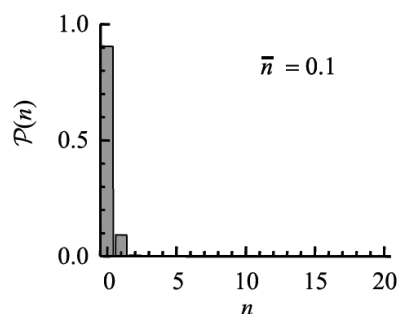
$$\left(1 - \frac{\bar{n}}{N}\right)^{N-n} = 1 - (N-n) \frac{\bar{n}}{N} + \frac{1}{2!} (N-n)(N-n-1) \left(\frac{\bar{n}}{N}\right)^2 - \dots \xrightarrow{N \rightarrow \infty} 1 - \bar{n} + \frac{\bar{n}^2}{2!} - \dots = e^{-\bar{n}}$$

$$\mathcal{P}(n) = \frac{\bar{n}^n}{n!} e^{-\bar{n}}, \quad n = 1, 2, 3, \dots$$

光子的泊松统计公式



泊松统计(3)

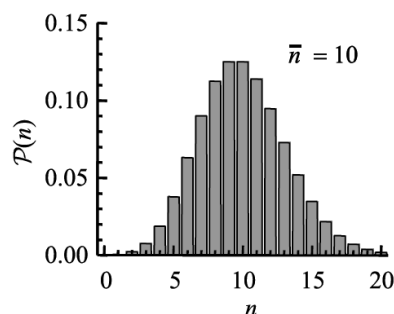
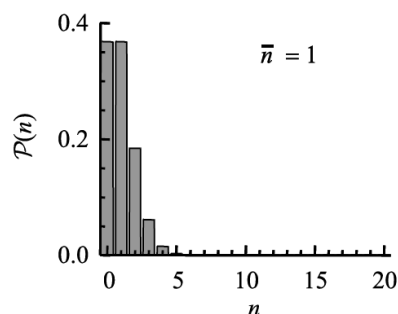


在泊松统计中，随着平均光子数增加，可能探测到的光子计数范围变得更加宽广。因此可以定义光子计数的变化量为标准方差的平方，即

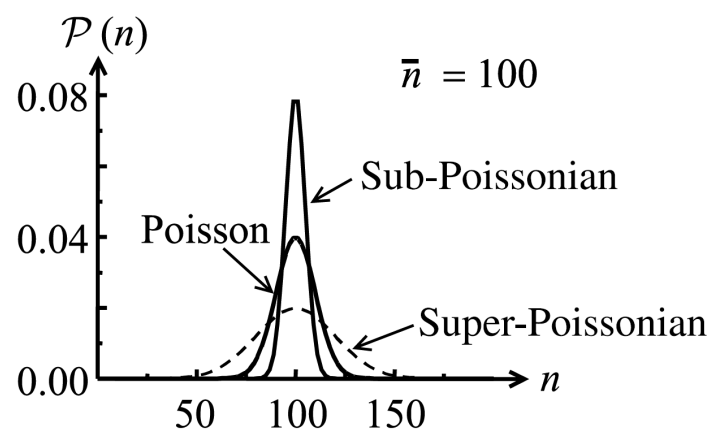
$$\text{Var}(n) \equiv (\sigma(n))^2 = \sum_{n=0}^{\infty} (n - \bar{n})^2 \mathcal{P}(n) = \bar{n}$$

所以

$$\sigma(n) = \sqrt{\bar{n}}$$

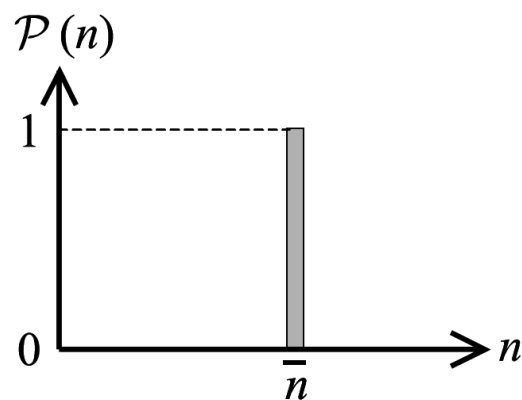
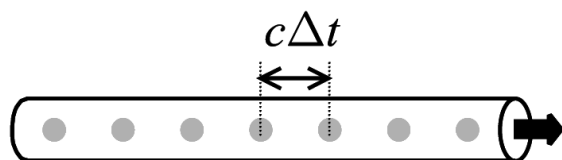


光源的分类



- 光源的统计性质，根据其涨落与泊松统计的关系可以分为以下三类：
 - 亚泊松统计， $\sigma(n) < \sqrt{\bar{n}}$;
 - 泊松统计， $\sigma(n) = \sqrt{\bar{n}}$;
 - 超泊松统计， $\sigma(n) > \sqrt{\bar{n}}$ 。
- 超泊松分布代表着更宽的光子数分布，不难想象这代表着更为不稳定的光源。所以非激光的传统光源由于光强不稳定，会导致超泊松分布。
- 亚泊松分布代表着比完美激光更为稳定的光源，也被称为非经典光源，典型的代表是单光子源。

亚泊松光源(1)



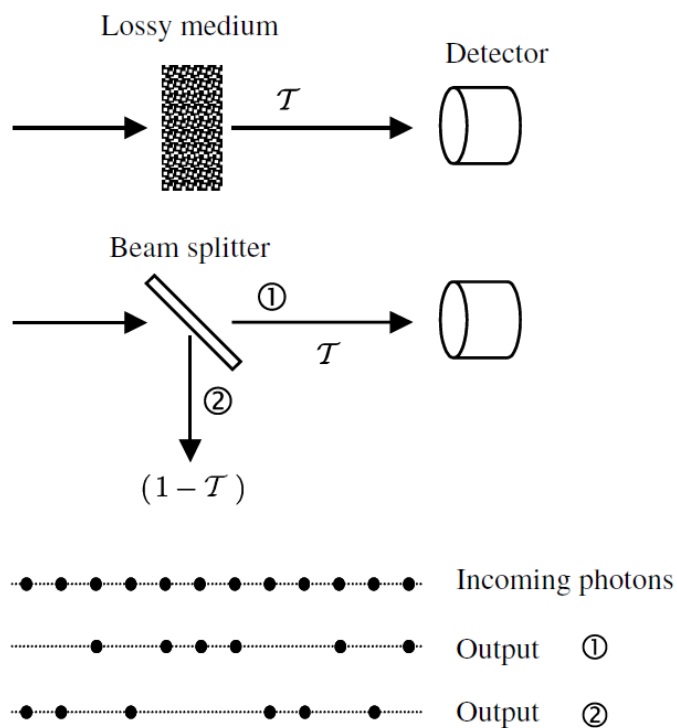
- 亚泊松光源满足 $\sigma(n) < \sqrt{\bar{n}}$ ，是超经典的，因而没有经典对应光源的例子。

如果我们考虑一队光子等间距地出现，间距满足 $\Delta x = c\Delta t$ ，因此 T 时间内的光子计数为

$$N(T) = \ln t \left(\eta \frac{T}{\Delta t} \right)$$

每次测量得到的结果都是一样的，因此 $\bar{n} = N$ 而且 $\sigma(n) = 0$ 。这也就是一个完美的单光子源。

亚泊松光源(2)



假设一个完美的单光子源发射的单光子经过一个光损媒介，如果这时光子的通过率是 \mathcal{T} ，那么光损媒介可以看作是一个 $\mathcal{T}:1 - \mathcal{T}$ 的光分束器，也就是分束后的两路光中平均光子数的比例为 $\mathcal{T}:1 - \mathcal{T}$ 。

由于光损（或者分束）是一个随机过程，所以实际的单光子源测试不可避免地偏离完美单光子源。造成光损的原因有：

- (1) 不充分的采集；
- (2) 光学元件引入的损耗，比如吸收，散射，反射等不完美过程；
- (3) 不完美的探测。

而这些都是不可避免的！因此单光子源是非常脆弱的光源。

长距离量子保密通信

- 在二十一世纪初之前的很长时间内，量子保密通信的安全传输距离只有10公里的量级。因此学术界曾经认为量子密码术的发展已经到头了，没有太大前途。然而，2003至2005年期间，韩国、加拿大和中国科学家提出了“诱骗态协议”，使得安全传输距离可以提高到百公里的量级。从此以后，量子密码术蓬勃发展，而中国获得了领先地位，大部分新纪录都是科大的研究团队创造的。（安全性和抵抗窃听方面的考量）
- 但量子信号在传输过程中会因为消相干和量子比特的丢失而衰减，限制了量子通信的有效距离。量子通信的安全传输距离可通过如下方式获得扩展：
 - 量子中继
 - 隐形传态
 - QKD改进协议，如双场量子密钥分发
 - 量子网络拓扑结构



量子中继

- 传统中继：通信网络中用来扩展通信距离的中继站。
- 量子中继：量子中继通过在长距离通信链路中插入一系列中继节点，对量子信号进行放大和纠错，从而扩展量子通信的有效距离。量子通信网络的中继站分为量子中继和可信中继。
 - 可信中继：这个中继站在按照**传统方式储存数据**，比如说用磁盘。发送方和接收方知道的所有数据，中继站也都知道。
 - 量子中继是让发送方和接收方通过它建立连接，但**中继站本身并不存储数据**。量子中继是“比可信中继更可信的中继”
- 量子中继的关键技术包括：
 - **纠缠交换**：在节点之间可靠地创建量子纠缠。
 - **纠缠纯化**：从纠缠纯度较低的系统中精炼出纯度较高的子系统。
 - **量子存储**：用于存放量子中间态，非量子信息本身。

量子通信



京沪干线：2000公里、
32个中继站（可信中继）

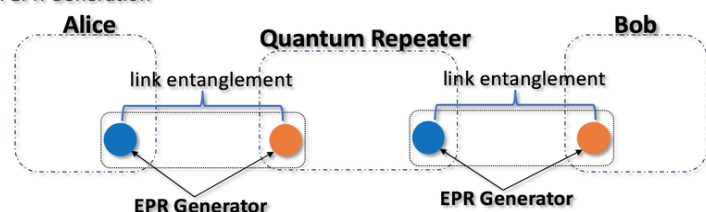
15



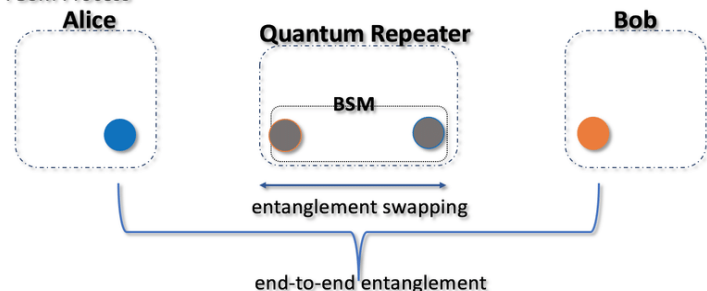
浙江大学

纠缠交换

1st: EPR Generation



2nd: BSM Process



- 假设粒子1, 2和3, 4分别处于两个最大纠缠态

$$|\Phi^+\rangle_{12} = \frac{1}{\sqrt{2}}(|00\rangle_{12} + |11\rangle_{12})$$

$$|\Psi^+\rangle_{12} = \frac{1}{\sqrt{2}}(|01\rangle_{34} + |10\rangle_{34})$$

- 四粒子系统态矢量:

$$\begin{aligned} |\psi\rangle &= |\Phi^+\rangle_{12} \otimes |\Psi^+\rangle_{12} = \frac{1}{2}(|0001\rangle + |0010\rangle + |1101\rangle + |1110\rangle) \\ &= \frac{1}{2}[|\Psi^+\rangle_{23}|\Phi^+\rangle_{14} + |\Psi^-\rangle_{23}|\Phi^-\rangle_{14} + |\Phi^+\rangle_{23}|\Psi^+\rangle_{14} + |\Phi^-\rangle_{23}|\Psi^-\rangle_{14}] \end{aligned}$$

对粒子2和3做Bell基测量后，系统将塌缩到随机等概率塌缩到任意一项。从而建立A-B两端的量子纠缠。

- 纠缠交换是实现量子中继和量子网络的关键技术，它允许在没有直接物理连接的情况下建立量子纠缠。它为量子密钥分发（QKD）提供了一种扩展通信距离的方法。纠缠交换在量子通信、量子网络和分布式量子计算中有着广泛的应用。

量子通信

16



浙江大学

纠缠纯化

- 在量子通信和量子计算过程中，预先制备的纠缠态是初始必要资源。例如二粒子的Bell态、三粒子GHZ态等。但实际物理世界对待考察系统总存在不可避免的相互作用，使其与环境产生量子纠缠，导致待考察系统退相干，导致纠缠模式丧失。
- 纯化的任务是从原来已被污染的量子系综中，精选分离出一个子系综，这个系综具有较高纠缠纯度。下面给出系统被污染的数学表述：

假设存在一个纯态系综 $\rho_{AB} = |\Psi^-\rangle_{AB}\langle\Psi^-|$ ，EPR对中的两个粒子分属于空间分离的Alice和Bob。当引入退相干后，混入了优先态 $|11\rangle$ ，系综变为纠缠混态：

$$\rho_{AB} = (1-x)|\Psi^-\rangle_{AB}\langle\Psi^-| + x|11\rangle_{AB}\langle 11| \quad x \in [0,1)$$

问题：x增加到什么值时，该混态还能破坏CHSH不等式，也即一定具有量子关联？

$$S = 2\sqrt{2} - x\sqrt{2}$$

CHSH不等式破坏条件： $S > 2$ ，也即 $x < 2 - \sqrt{2}$

- 纠缠纯化的基本思想是利用多个部分纠缠的粒子对，通过一系列的量子操作和后选择（post-selection），生成少数几个高保真度的纠缠态。

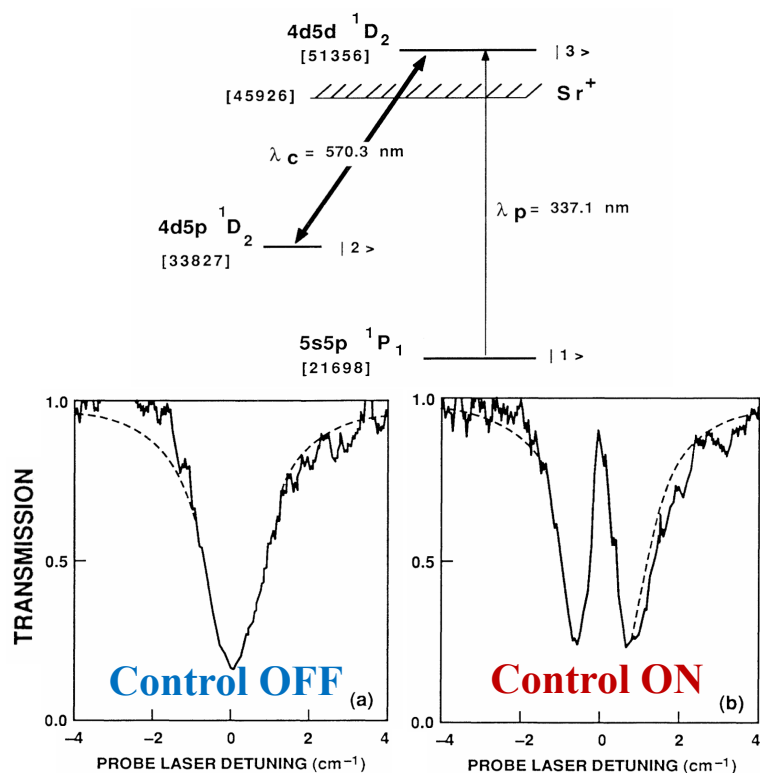
量子通信



量子存储

- 量子存储器, 顾名思义就是可以将量子态存储起来, 并且过一段时间还可以将存储的量子态读取出来的器件。
- 常见的量子存储方案有: 电磁感应透明、DLCZ(段路明)存储方案、法拉第相互作用、原子频率梳等。本质都是光与物质相互作用、物质内部状态干涉或者相位关系的演化和恢复。
- 量子存储介质包括固态存储器(金刚石NV色心的核自旋、稀土离子掺杂的固态晶体)、原子气体、光路存储器等。
- 衡量一个量子存储是否使用的维度: 高存储读取效率、低噪音、长寿命(或者大的时间带宽积)、室温条件下运行。

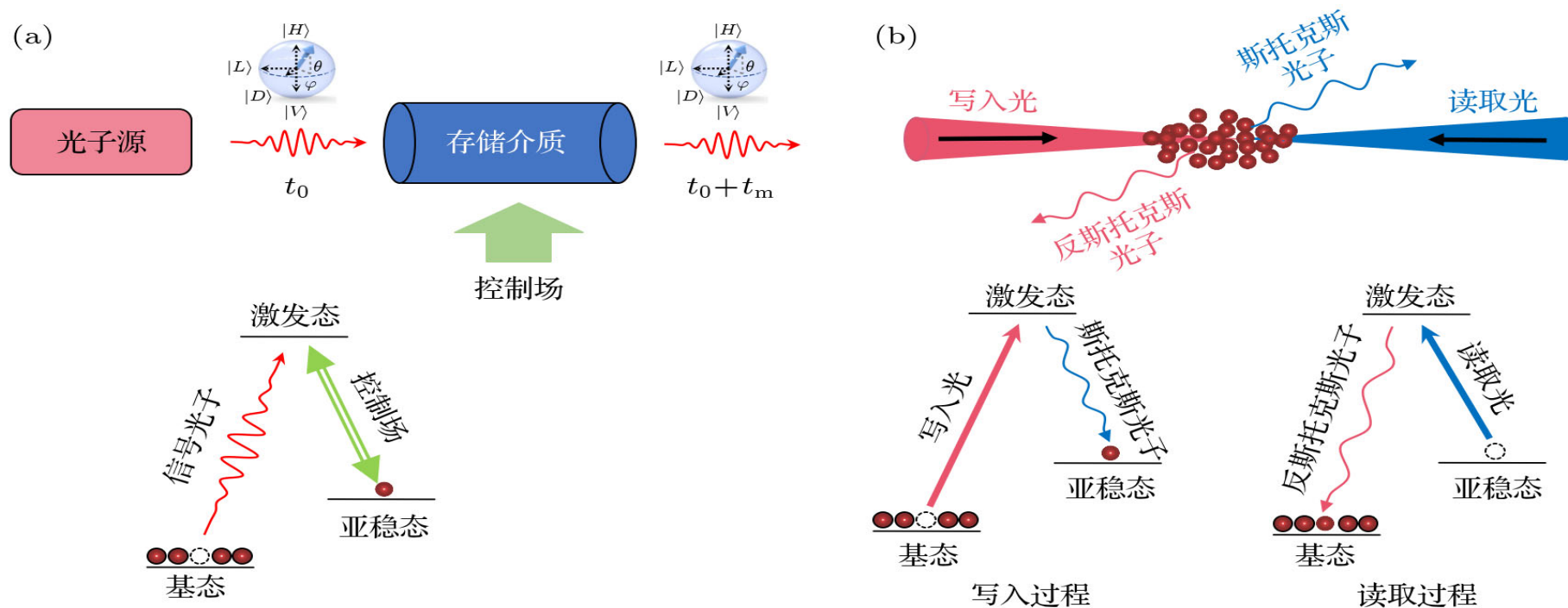
EIT与量子存储（吸收型方案）



- Electromagnetic induced transparency, 利用外电磁场控制材料光响应特性，实现对特定波段光的透过率调制。该现象最早由Harris 和Imamoglu在理论上提出，并在铯原子系统中被观察到。
- 通过control光（570.3nm）将原子 $|2\rangle$ 和 $|3\rangle$ 态耦合；probe光的强度受到调制（337.1nm）
- 吸收系数的变化可对应于折射率调制 \rightarrow 色散调制。在EIT附近的 $dn/d\omega$ 较大，群速降低，甚至可降低到0。光子被多次吸收/发射，从而实现存储。

$$V_g = \frac{d\omega}{dk} = \frac{c}{n + \omega \frac{dn}{d\omega}}$$

DLCZ型方案



- DLCZ 型量子存储其物理过程是首先通过一束写入激光来激发存储介质, 在介质内建立单激发状态的同时释放一个单光子。存储一定时间后, 再利用读取激光将介质中的激发状态转化为光子释放, 同时保证先后释放的两个光子具有关联性。

量子通信

20



浙江大学

参考文献

- 单光子源和泊松统计主要参考
 - Mark Fox, Quntum Optics – An Introduction, Oxford University Press (2006). 第5章。
- 量子中继主要参考：
 - 你完全可以理解全光量子中继 | 袁岚峰 - 知乎 (zhihu.com)
 - 窦建鹏, 李航, 庞晓玲, 张超妮, 杨天怀, 金贤敏. 量子存储研究进展[J]. 物理学报, 2019, 68(3): 030307-1-030307-14. doi: 10.7498/aps.68.20190039
 - 纠缠交换：量子信息物理原理 张永德 9.2节
 - Cacciapuoti, Angela Sara & Caleffi, Marcello & Tafuri, F. & Cataliotti, Francesco & Gherardini, Stefano & Bianchi, Giuseppe. (2018). Quantum Internet: Networking Challenges in Distributed Quantum Computing.
 - 王云飞, 周颖, 王英, 颜辉, 朱诗亮. 量子存储性能及应用分析[J]. 物理学报, 2023, 72(20): 206701-1-206701-13. doi: 10.7498/aps.72.20231203

