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

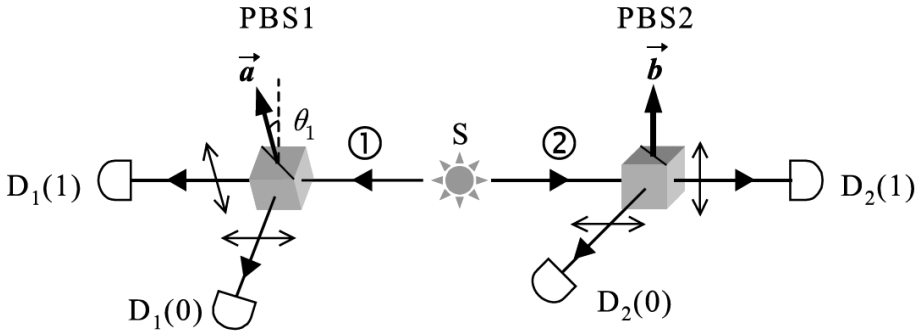
浙江大学

C5-2 不可克隆原理和量子密码学

课程回顾

EPR佯谬和贝尔不等式：

- EPR佯谬：假设光源*S*发射一对关联光子，由于出射光子的偏振是不同偏振态$|\leftrightarrow\rangle$和$|\updownarrow\rangle$的线性组合，这意味着光子①和光子②无论距离多远都会因为对某一光子的测量，瞬时坍缩到同一本征态上。“定域实在论”和量子论在此产生了矛盾。
- 如果一个多粒子体系波函数无法写作单个粒子波函数的乘积形式，这种量子态称为纠缠态。
- 在“定域实在论”的范畴内，贝尔不等式始终成立。量子理论的预测显著违反了贝尔不等式，因此贝尔不等式为“定域实在论”和量子理论的哲学分歧提供了实验判据。



量子测量问题

- 如果我们知道微观系统的波函数为$|\psi\rangle$，这时算符$\hat{A}$的平均值为$\langle A\rangle = \langle\psi|\hat{A}|\psi\rangle$，如果$|\psi\rangle$不是$A$的本征态，那么获得$\langle A\rangle$需要通过多次测量取平均。每次测量随机获得$A$的本征值$A_n$。如果我们把波函数通过本征波函数展开$|\psi\rangle = \sum_n c_n|\psi_n\rangle$，我们知道测量得到$A_n$的几率为$|c_n|^2$。如果持续同样的测量，由于系统的状态已经坍缩到了$|\psi_n\rangle$，所以我们会一直得到同样的$A_n$。
- 量子测量问题的本质困难在于，我们无法利用量子力学的线性算符来建立一个有关“量子测量”的数学模型。假设我们有一个测量算符$\widehat{M}$，系统处于的初始态$|\uparrow\rangle$是系统的一个本征态

$$\widehat{M}|\uparrow\rangle = |\uparrow\rangle$$

如果初始态是另外一个本征态$|\downarrow\rangle$，则有

$$\widehat{M}|\downarrow\rangle = |\downarrow\rangle$$

假设系统的初始态为两个本征态的线性组合$\alpha|\uparrow\rangle + \beta|\downarrow\rangle$，我们使用测量算符

$$\widehat{M}(\alpha|\uparrow\rangle + \beta|\downarrow\rangle) = \alpha\widehat{M}|\uparrow\rangle + \beta\widehat{M}|\downarrow\rangle = \alpha|\uparrow\rangle + \beta|\downarrow\rangle$$

这显然和量子测量的过程不符，所以量子力学所使用的线性代数理论本身并不能有效地描述波函数坍缩的过程。

不可克隆原理

- 量子测量是一种破坏性测量，在此基础上可以得出量子不可克隆原理，即没有方法可以严格地复制系统的任意量子态。（想一想：如果量子态可以克隆，我们将会得到什么？）
- 假设我们拥有两个粒子，分别处在$|\psi\rangle$和$|X\rangle$态上，我们希望通过一种方法使得

$$|\psi\rangle|X\rangle \to |\psi\rangle|\psi\rangle$$

如果我们具有这样的能力，那么不难获得

$$|\psi_1\rangle|X\rangle \to |\psi_1\rangle|\psi_1\rangle \qquad |\psi_2\rangle|X\rangle \to |\psi_2\rangle|\psi_2\rangle$$

如果我们希望克隆一个线性组合态$|\psi\rangle = \alpha|\psi_1\rangle + \beta|\psi_2\rangle$，那么

$$|\psi\rangle|X\rangle \to \alpha|\psi_1\rangle|\psi_1\rangle + \beta|\psi_2\rangle|\psi_2\rangle$$

但其实我们希望得到是

$$|\psi\rangle|X\rangle \to (\alpha|\psi_1\rangle + \beta|\psi_2\rangle)(\alpha|\psi_1\rangle + \beta|\psi_2\rangle) = \alpha^2|\psi_1\rangle|\psi_1\rangle + \beta^2|\psi_2\rangle|\psi_2\rangle + \alpha\beta|\psi_1\rangle|\psi_2\rangle + \alpha\beta|\psi_2\rangle|\psi_1\rangle$$

这实际上是说：我们可以克隆一个本征态，但无法克隆一个非平庸的线性叠加态。

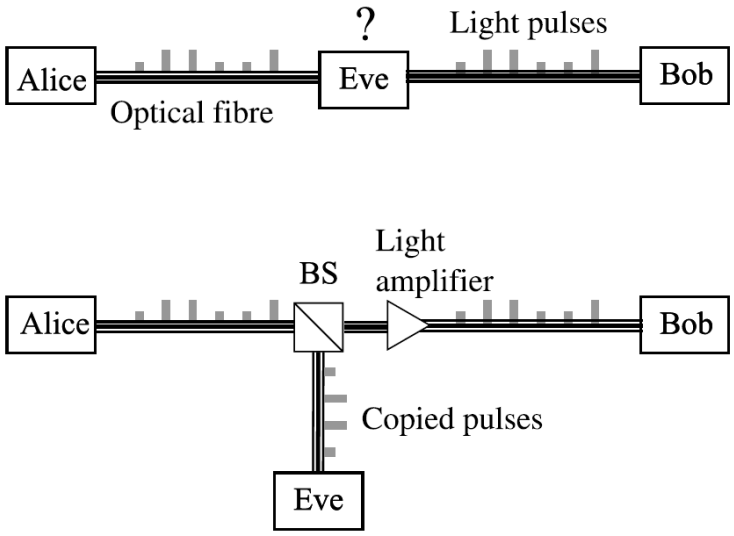
- 量子不可克隆原理提供了量子密码学的理论基础。

传统密码学

- 密码学是研究编制密码和破译密码的科学。在通信过程中，待加密的信息称为明文，已被加密的信息称为密文，仅由收发双方知道的信息称为密钥。在密码系统中，存在非法截收者，他们试图通过各种办法窃取机密或窜改信息。
- 密码学在军事上得到了显著的应用。在二战中，英国破译了德国使用的恩尼格玛密码机。人工智能之父艾伦·图灵（1912-1954）在破译截获的编码信息方面发挥了关键作用，使盟军能够在包括大西洋战役在内的许多重要交战中击败纳粹，并因此赢得了战争。
- 由于收发双方必须交换密钥才能顺利实现信息的加密和解密，因此原理上总能存在窃密的手段。保证密钥系统安全的前提是保证密钥的绝对安全，但这种条件是无法实现的。
- 真正随机产生的一次性密钥，不会有任何重复的可能。量子密码学提供了完美的一次性密钥解决方案。

量子密码学(1)

- 量子密码学的目的是提供一个可靠的方法（或者信道）使得没有人能够截获密钥。这种基于量子密码学的技术手段，被称之为量子密钥分发。
- 量子密码学的技术架构中涉及的三方为Alice(A)，Bob(B)，和Eve(E)。其中Alice和Bob为交换密钥的双方，Eve是窃听者。量子密码学的目的是提供一种方法让Eve的窃听被暴露出来。
- 在传统信道中，如果Alice想要给Bob传送一条信息。例如，信息通过光纤来传输，强光代表“1”，弱光代表“0”，Eve在途中试图截获和破解光信号。
- Eve可以选用的最简单的方法，就是在信道中增加一个光纤分束器，分出光信号强度的1/2，然后在原始信道中增加一个放大器，把放大倍数设置为2倍。这样Alice和Bob就无法意识到Eve的存在。

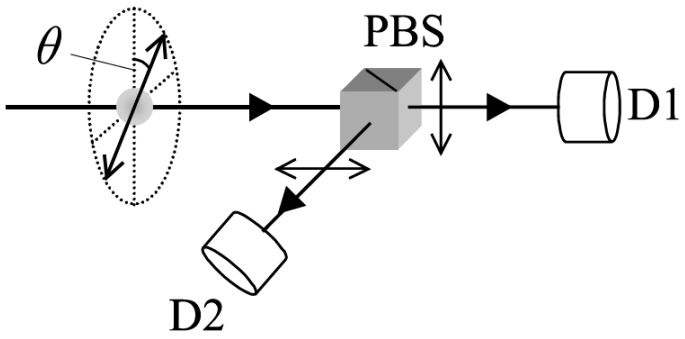


量子密码学(2)

- 量子力学告诉我们，我们无法测量一个处于非平庸线性叠加态的粒子而不改变其状态。而量子不可克隆原理告诉我们，我们无法截获和测量一个粒子，然后克隆一个完全一样的粒子，进入原始信道。通过量子理论定义的方法，我们有可能暴露窃听者，这是量子密码学的本质。
- 对光子的偏振态的测量是当前实用化量子密钥分发系统的基本技术手段。如果我们假设入射光子与垂直偏振方向的夹角为θ，当$\theta = 0^o$，D1会探测到光子；当$\theta = 90^o$，D2会探测到光子。我们把任意偏振态写为垂直偏振态$|\updownarrow\rangle$和水平偏正态$|\leftrightarrow\rangle$的线性叠加

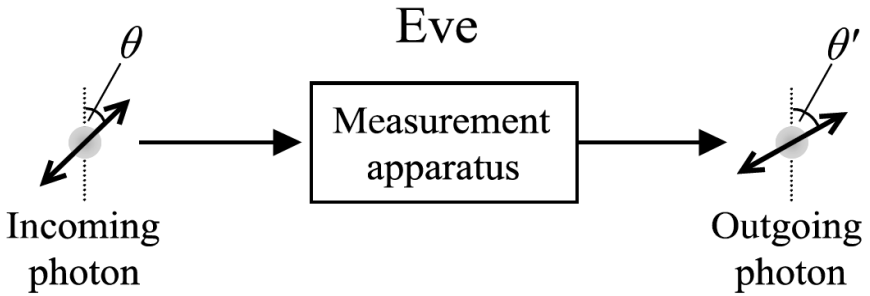
$$|\theta\rangle = \cos\theta\,|\updownarrow\rangle + \sin\theta\,|\leftrightarrow\rangle$$

- 对接收端来说，接收到垂直偏振态$|\updownarrow\rangle$的几率为$\cos^2\theta$，接收水平偏正态$|\leftrightarrow\rangle$的几率为$\sin^2\theta$。



量子密码学(3)

- 如果Eve使用同样的偏振分束器在信息传播的途中进行窃听，那么她只能窃听到垂直偏振态$|\updownarrow\rangle$或者水平偏正态$|\leftrightarrow\rangle$这两个本征态中的一个，然后复制并送出一个本征态。这意味着Eve的存在破坏了原始的被量子加密的信息。
- 更为一般的，Eve的目的在于探测出信道中光子的偏振角度θ，然后送出一个同样偏振为θ的光子。但是，量子不可克隆原理禁止了这样的过程。因此，Eve的存在，或者说测量仪器的存在，破坏了原有信道中的量子信息，只能送出一个偏振角度θ'的新光子。
- 量子测量从原理上禁止了隐秘窃听的存在。



量子货币

- 量子货币(Quantum Money)这概念是由哥伦比亚大学一位研究生Stephen Wiesner在1970年提出，但被多本科学期刊拒绝刊登。
- 量子货币在每次交易时均需银行方面核实。每张量子货币上除了印上一个编号外，拥有一个具有两个量子态的量子系统。即垂直偏振态$|\updownarrow\rangle$和水平偏振态$|\leftrightarrow\rangle$，或者与垂直方向夹角分别为45°和135°的两个偏振态$|\nearrow\rangle$和$|\nwarrow\rangle$。这两组偏振分别属于不同的两组基$\oplus$和$\otimes$ 。
- 货币上只印有编号，偏振方向则被隐藏。由于银行拥有偏振方向的纪录，它能在任何时候在不干涉量子态的情况下测量它量子态，但对不清楚基底的伪币制造者来说，即使他知道银行使用哪两种基底，也有可能使用了错误基底来测量光子。
- 对于每一个光子，伪造者有3/4的机会成功测量。如果测量的光子数量是 N ，这个机会几率将随着N的增大而以指数形式下降。

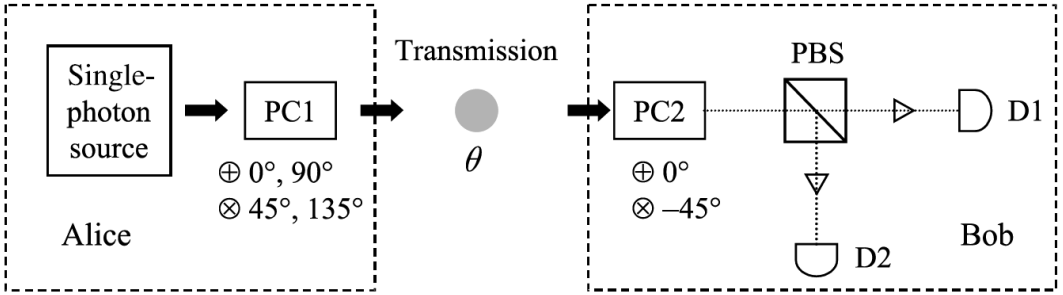
BB84协议(1)

Basis	Binary 1	Binary 0
$\oplus$	$\|\updownarrow\rangle$ $\theta = 0°$	$\|\leftrightarrow\rangle$ $\theta = 90°$
$\otimes$	$\|\nearrow\rangle$ $\theta = 45°$	$\|\nwarrow\rangle$ $\theta = 135°$

- 基于量子密码学的原理，科学文献中提出了各种量子密钥分发的架构，其中最著名的架构是所谓的Bennett-Brassard 84（BB84）协议。
- 在BB84协议中，我们不仅定义垂直偏振态$|\updownarrow\rangle$和水平偏正态$|\leftrightarrow\rangle$，同时我们定义与垂直方向夹角分别为45°和135°的两个偏振态$|\nearrow\rangle$和$|\nwarrow\rangle$。这两组偏振分别属于不同的两组基$\oplus$和$\otimes$ 。
- 从算符和矩阵的学习中，我们知道$\oplus$和$\otimes$代表了两组完备的基。也就是说，垂直偏振态$|\updownarrow\rangle$和水平偏正态$|\leftrightarrow\rangle$正交归一，在它们张开的二维希尔伯特空间中的任意矢量都可以表示为两个基矢量（偏振态）的线性组合。同样，与垂直方向夹角分别为45°和135°的两个偏振态 $|\nearrow\rangle$和$|\nwarrow\rangle$正交归一，在它们张开的二维的希尔伯特空间中的任意矢量都可以表示为两个基矢量（偏振态）的线性组合。
- 这两组基之间可以通过基于幺正算符的线性变化联系起来。

BB84协议(2)

- 在发射端，Alice的设备包括单光子源和与单光子源同步的普克尔盒（Pockels cell，普克尔盒可以选择输出光子的偏振方向）。 Alice可以发出0°，45°，90°，135°偏振的光子，因此她可以在两组基之间随机切换。
- 在接收端，Bob的设备包括普克尔盒以及一套完整的偏振测量系统。通过控制普克尔盒，Bob的测量在⊕和⊗代表了两组基之间随机切换。Bob并不知道Alice对基的选择，因此他只能随机地选择测量的基。只有在发射端和接受端的基的选择一致的时候，Bob的测量会得到确定的值，反之，测量的结果是D1和D2各占50%。



BB84协议(3)

- 在BB84协议中规定：

1) Alice对信息的编码在⊕和⊗两组基之间随机切换，但不告诉任何人她对基的选择。然后她把编码后的光子经过相同的时间间隔发送给Bob；
2) Bob随机地选择⊕和⊗两组基进行解码；
3) Bob通过一个公开的信道告诉Alice他对基的选择，但不告诉Alice他的解码结果；
4) Alice检查Bob的选择，挑选出她和Bob选择一致的情况。然后通过公开信道告诉Bob哪些基的选择是一致的。Alice和Bob各自舍弃不一致比特；
5) Bob通过公开信道把剩下的比特信息传输给Alice，Alice再度检查后，分析其中的误码率；
6) 如果误码率小于25%，Alice确认没有窃听存在，通信继续。

BB84协议(4)

- 我们通过一个例子来检验BB84协议的6个步骤：（1）Alice编码；（2）Bob解码；（3）Bob发送基的选择；（4）Alice对照后发现50%左右一致的选择，然后发送给Bob，各自舍弃选择不一致的比特；（5）Bob发送剩下的比特给Alice，Alice检查误码率；（6）如果误码率小于25%，通信继续。

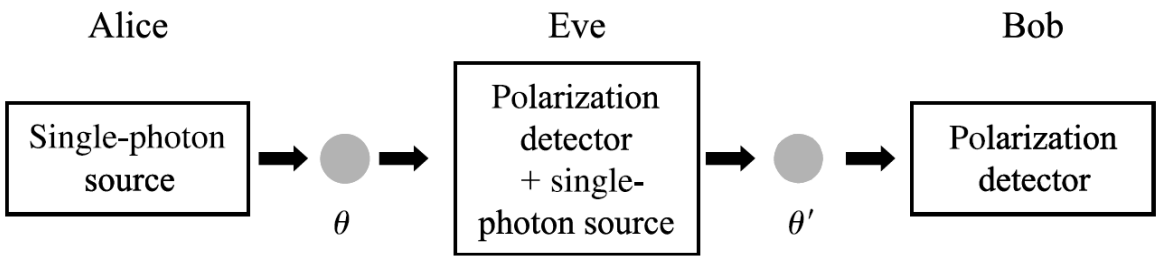
A's data	1	0	0	1	1	1	0	0	1	0	0	1
A's basis	⊕	⊗	⊕	⊗	⊗	⊕	⊕	⊗	⊕	⊗	⊗	⊕
θ (°)	0	135	90	45	45	0	90	135	0	135	135	0
B's basis	⊗	⊗	⊕	⊕	⊗	⊕	⊗	⊕	⊕	⊗	⊕	⊗
B's result	1	0	0	0	1	1	0	1	1	0	1	1
Same basis ?	n	y	y	n	y	y	n	n	y	y	n	n
Sifted bits		0	0		1	1			1	0		
Data check ?		y	n		y	n			y	n		
Private key			0			1				0		

BB84协议(5)

- 当Alice检查误码率的时候，她能够意识到Eve这个窃听者的存在。
- 假设Eve可以使用和Bob同样的设备解码，和Alice同样的设备编码并发送量子比特。因为她无法知道Alice对基的选择，她只能随机地选择基进行解码。有50%的可能性她的猜测是正确的。另外50%的可能，她的猜测是错误的，所以她会使用旋转45°的基，然后有50%的可能性Bob会认为误码。所以

$$\mathcal{P}_{error} = \mathcal{P}_{Eve\ has\ wrong\ basis} \times \mathcal{P}_{Bob\ gets\ wrong\ results} = 50\% \times 50\% = 25\%$$

- 25%的误码率在光纤通信系统中是非常显著的，所以一旦有窃听发生，Alice能够及时地中断通信。



误差校正

- 量子信道中的误差来源一般有三种主要形式：（1）由于传输、收集、探测过程导致的随机漏码；（2）由于光纤双折射导致的误码；（3）由于探测器暗计数导致的误码。

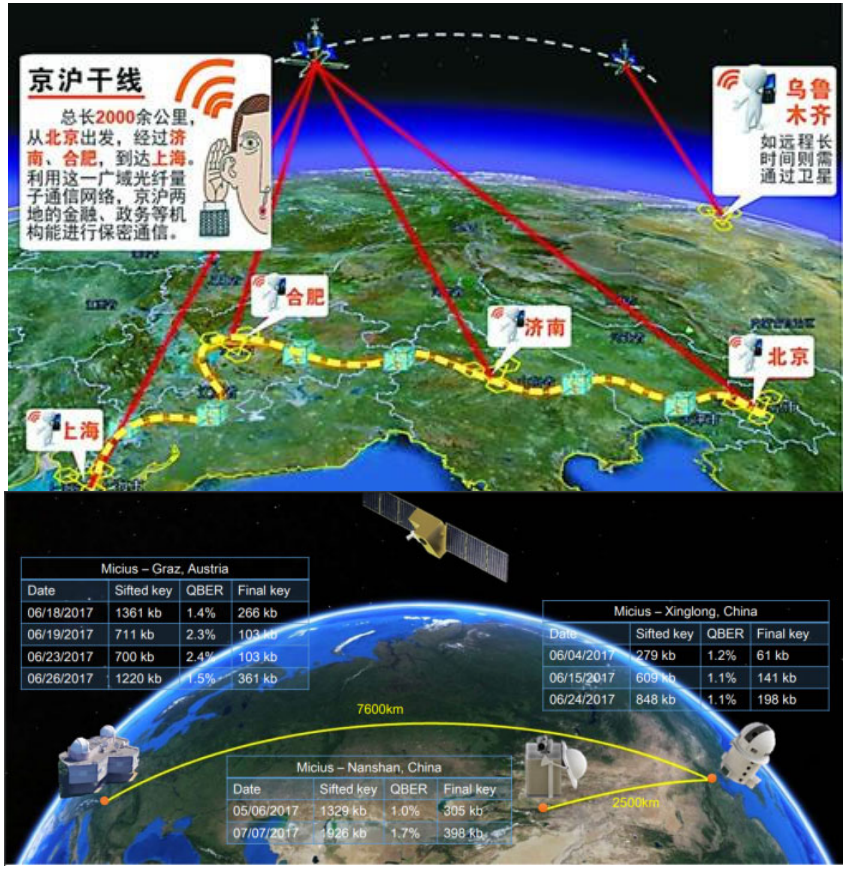
- 程度可控的随机漏码并不会影响量子信道的功能。但是误码有可能严重扰乱量子信道的正常使用，因此需要进行误差校正。误差校正的方法和传统通信的误差校正类似，由Shannon–Hartley theorem描述。

- 假设我们接收到N位的信息，其误码率为ε，需要的误差校正位数量为

$$N_{correction} = N(-\varepsilon \log \varepsilon - (1-\varepsilon)\log(1-\varepsilon))$$

- 量子保密通信无法排除Eve假扮Bob的情况，因此和传统通信一样，需要引入身份验证。

量子通信实验



- 我国是量子密钥分发技术的主要推动力量，已经实现了量子通信京沪干线和墨子号量子卫星的部署和测试。
- 京沪干线总长2000公里，从北京出发，经过济南，合肥，到达上海。利用这一广域光纤量子通信网络，京沪两地的金融政务等机构有可以实现理论上绝对保密的通信。
- 2016年，“墨子号”量子卫星于酒泉卫星发射中心搭载长征二号丁运载火箭发射升空，成为全球第一颗设计用于进行量子科学实验的卫星。

参考文献

- 量子测量和不可克隆原理主要参考：
  - 教材David J. Griffiths, and Darrell F. Schroeter, Introduction to Quantum Mechanics (3rd Edition), Cambridge University Press (2018). 第12.4节。
  - David A.B. Miller, Quantum Mechanics for Scientists and Engineers, Cambridge University Press (2008). 第18.1-18.2小节的内容。

- 量子密钥分发主要参考
  - Mark Fox, Quntum Optics – An Introduction, Oxford University Press (2006). 第12.1-12.3节。