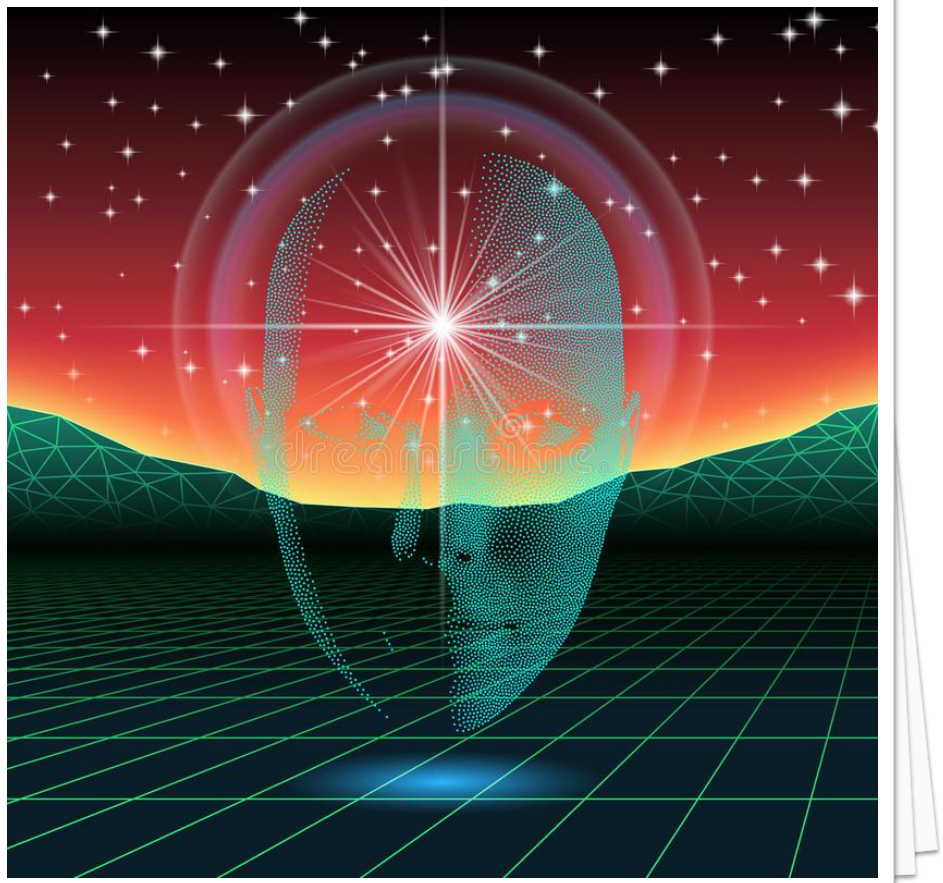


量子信息简介

EPR佯谬

量子纠缠

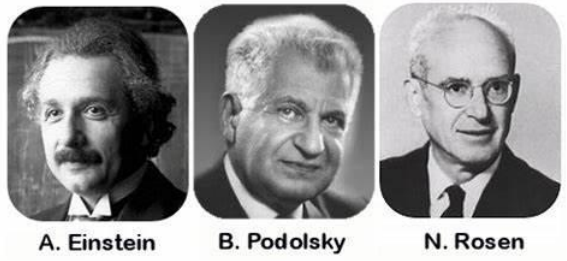
量子不可克隆定理

量子隐形传态

量子密钥分发

EPR佯谬

- 1935年，Einstein，Podolsky，Rosen共同发表了一篇文章



- 文章对正统量子力学基本原理和概念的诠释提出尖锐的批评：

❶波函数对“物理实在”的描述不完备

（1）物理实在：爱因斯坦等人认为，一个“物理实在”，如果所属系统不受扰动，相应的可观测量应当具有确定的数值。

（2）例如在动量本征态

$$\psi_{p_0}(x) = e^{\frac{i}{\hbar}p_0 x}$$

，粒子动量是“物理实在”，粒子坐标不是“物理实在”。

（3）完备：不存在理论所不能描述的“物理实在”。

❷波函数描述不自洽

（1）定域假设：两个粒子相距很远时，对粒子1进行的任何测量，都不会影响粒子2 的状态。

（2）两粒子波函数$\psi(x_1, x_2)$必然可展开为两种形式

$$\psi(x_1, x_2) = \sum_n \xi_n(x_2) u_n(x_1), \qquad \hat{A}u_n(x) = a_n u_n(x)$$

$$\psi(x_1, x_2) = \sum_n \eta_n(x_2) v_n(x_1), \qquad \hat{B}v_n(x) = b_n v_n(x)$$

其中 $\hat{A}, \hat{B}$ 是两个不同的物理量， $u_n(x), v_n(x)$ 分别是两者的本征态。

厄米算符的本征态完备，所以可以用来展开波函数。

（3）对相距很远的两粒子系统，

测粒子1的物理量A，则粒子2必然处于某个$\xi_n(x_2)$状态；

测粒子1的物理量B，则粒子2必然处于某个$\eta_n(x_2)$状态。

对粒子1的不同操作，影响到粒子2所处的状态，与定域假设矛盾。

- 量子力学与定域实在论不相容

EPR Paradox-Bohm

- Bohm改用自旋状态来陈述EPR佯谬
- 考虑正负电子对，处于自旋单态

$$|\chi\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle|\downarrow\rangle - |\downarrow\rangle|\uparrow\rangle)$$

- 产生电子对后，正负电子运动到相距很远的位置，在无扰动时自旋状态不变
- 自旋状态可展开成两种形式：

$$|\uparrow\rangle_z = \begin{pmatrix}1\\0\end{pmatrix}, \quad |\downarrow\rangle_z = \begin{pmatrix}0\\1\end{pmatrix}, \quad |\chi\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle_z|\downarrow\rangle_z - |\downarrow\rangle_z|\uparrow\rangle_z)$$

$$|\uparrow\rangle_y = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\i\end{pmatrix}, \quad |\downarrow\rangle_y = \frac{1}{\sqrt{2}}\begin{pmatrix}i\\1\end{pmatrix}, \quad |\chi\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle_y|\downarrow\rangle_y - |\downarrow\rangle_y|\uparrow\rangle_y)$$

- 同一个状态$|\chi\rangle$，

  Alice测量粒子1的σ_z，则同时确定了粒子2的状态处于σ_z的本征态

  Alice测量粒子1的σ_y，则同时确定了粒子2的状态处于σ_y的本征态

- EPR的出发点是反驳量子力学的正统理论，却揭示了量子纠缠这一重要现象

量子纠缠

- 纯态纠缠态

可分态：$|\psi\rangle = |\xi\rangle_A \otimes |\eta\rangle_B$

纠缠态：不能写成两个态的直积

- 例

$$|\psi\rangle = \frac{\sqrt{3}}{2}|00\rangle + \frac{\sqrt{3}}{2}|01\rangle + \frac{1}{\sqrt{6}}|10\rangle + \frac{1}{\sqrt{6}}|11\rangle$$

$$= \left(\sqrt{\frac{3}{2}}|0\rangle + \frac{1}{\sqrt{3}}|1\rangle\right)\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right)$$

是可分态

- 例：双光子偏振态

$$|\chi\rangle = \frac{1}{\sqrt{2}}(|\leftrightarrow\rangle|\leftrightarrow\rangle + |\updownarrow\rangle|\updownarrow\rangle)$$

是纠缠态

- 混合态纠缠态

可分态：

$$\hat{\rho} = \sum_j p_j |\xi_j\rangle_{A\,A}\langle\xi_j| \otimes |\eta_j\rangle_{B\,B}\langle\eta_j|$$

纠缠态：不能写成上式形式

- 可控的纠缠态直到1982年才在实验中实现，并被用于检验EPR佯谬

Bell基

- 两粒子系统，用$(\sigma_{1z},\sigma_{2z})$的共同本征态为基，定义

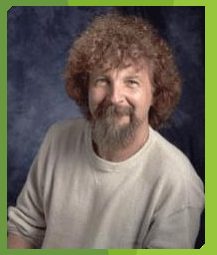
$$|\psi^{\pm}\rangle \overset{\text{def}}{=} \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$$

$$|\phi^{\pm}\rangle \overset{\text{def}}{=} \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$$

称为Bell基

- 4个Bell基构成2-qubit的完备基
- 4个Bell基都是最大纠缠态
- 也可选用$(\sigma_{1x},\sigma_{2x})$或$(\sigma_{1y},\sigma_{2y})$的共同本征态作为Bell基
- 可对两个粒子进行Bell基联合测量，测量值是$(\sigma_{1z},\sigma_{2z})$的4组本征值；测量之后系统处于4个Bell基之一的状态

量子不可克隆定理

- 在量子信息理论的建立过程中，1982年W.K. Wootters,W.H. Zurek提出

单个任意未知量子态不可能精确克隆

"A Single Quantum cannot be Cloned," Nature, Vol. 299, No. 5886, 1982, pp. 802-803.

- 该定理是叠加原理的推论

- 如果存在么正变换可以把A的两个量子态复制到B，那么

$$\hat{U}|\psi\rangle_A|0\rangle_B|0\rangle_E = |\psi\rangle_A|\psi\rangle_B|x\rangle_E$$
$$\hat{U}|\phi\rangle_A|0\rangle_B|0\rangle_E = |\phi\rangle_A|\phi\rangle_B|y\rangle_E$$
$$\hat{U}^\dagger\hat{U} = \mathbf{1}$$

- 取内积得

$$\begin{aligned} &{}_A\langle\psi|\phi\rangle_A = {}_A\langle\psi|\phi\rangle_A\,{}_B\langle\psi|\phi\rangle_B\,{}_E\langle x|y\rangle_E \\ \Leftrightarrow\ &{}_A\langle\psi|\phi\rangle_A = 0 \text{ or } {}_B\langle\psi|\phi\rangle_B\,{}_E\langle x|y\rangle_E = 1 \\ \Rightarrow\ &{}_A\langle\psi|\phi\rangle_A = 0 \text{ or } \left|{}_B\langle\psi|\phi\rangle_B\right| = 1 \end{aligned}$$

- 即$|\psi\rangle_A, |\phi\rangle_A$正交；或者$|\psi\rangle_A = e^{i\theta}|\phi\rangle_A$是同一个状态。所以两者的叠加态不可克隆。
- 任意未知的量子态不可克隆

量子隐形传态Quantum Teleportation

- 我们可以用量子隐形传态方案，打破量子不可克隆定理对量子态传输的限制

理论方案：C.H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. Wootters, "Teleporting an Unknown Quantum State via Dual Classical and EPR Channels", Phys. Rev. Lett. vol. 70, pp 1895-1899, 1993.

首次实验：D. Bouwmeester, JW. Pan, K. Mattle, Manfred Eibl, Harald Weinfurter & Anton Zeilinger. Experimental quantum teleportation. Nature 390, 575–579 (1997). https://doi.org/10.1038/37539

(top, left) Richard Jozsa, William K. Wootters, Charles H. Bennett. (bottom, left) Gilles Brassard, Claude Crépeau, Asher Peres. Photo: André Berthiaume.

- 问题：

Alice在发送站T，Bob在接收站R。Alice需要把量子态（光子1）

$$|\chi\rangle = a|0\rangle + b|1\rangle$$

发送给Bob。Alice和Bob对$|\psi\rangle$的状态一无所知。

- 量子不可克隆定理告诉我们，量子态不能直接拷贝。

Quantum Teleportation

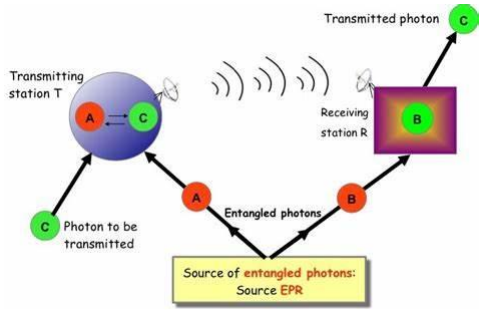
- 制备（光子2、3的）纠缠态

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

- 其中光子2被发送给Alice，光子3被发送给Bob
- 三光子态矢为

$$|\chi\rangle \otimes |\psi^-\rangle = (a|0\rangle + b|1\rangle) \otimes \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

$$= \frac{a}{\sqrt{2}}|001\rangle - \frac{a}{\sqrt{2}}|010\rangle + \frac{b}{\sqrt{2}}|101\rangle - \frac{b}{\sqrt{2}}|110\rangle$$



- Alice对光子1+2进行Bell基联合测量

$$|\chi\rangle \otimes |\psi^-\rangle$$

$$= \frac{1}{2}\cdot\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)(-a|0\rangle - b|1\rangle) + \frac{1}{2}\cdot\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)(a|0\rangle - b|1\rangle)$$

$$+ \frac{1}{2}\cdot\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)(b|0\rangle + a|1\rangle) + \frac{1}{2}\cdot\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)(-b|0\rangle + a|1\rangle)$$

$$= \frac{1}{2}|\psi^+\rangle(-a|0\rangle - b|1\rangle) + \frac{1}{2}|\psi^-\rangle(a|0\rangle - b|1\rangle) + \frac{1}{2}|\phi^+\rangle(b|0\rangle + a|1\rangle)$$

$$+ \frac{1}{2}|\phi^-\rangle(-b|0\rangle + a|1\rangle)$$

❶Alice测量结果有四种可能，各有1/4概率

❷Alice的测量，使得光子1+2处于最大纠缠态，同时光子2+3的纠缠被破坏

❸在Alice测量后,光子1的量子态$|\chi\rangle$被破坏，光子3将处于4种状态之一

- Alice将测量结果通过传统信道告知Bob
- Bob根据得知的结果选择不同的么正变换：

$$-\sigma_0\begin{pmatrix}-a\\-b\end{pmatrix} = \begin{pmatrix}a\\b\end{pmatrix}, \qquad \sigma_z\begin{pmatrix}a\\-b\end{pmatrix} = \begin{pmatrix}a\\b\end{pmatrix}$$

$$\sigma_x\begin{pmatrix}b\\a\end{pmatrix} = \begin{pmatrix}a\\b\end{pmatrix}, \qquad i\sigma_y\begin{pmatrix}-b\\a\end{pmatrix} = \begin{pmatrix}a\\b\end{pmatrix}$$

- 结果：粒子1的状态被传送到粒子3，同时粒子1的状态被破坏
- 由于需要用到经典信道，信息的传递速度必然不超过光速

量子密钥分发

- 在经典通讯中，信息被编码于某个经典物理系统（纸张、电路电压、无线电波等）
- 经典系统可以被测量，并且不引起系统的变化
- 不可能确切知道窃听者Eve是否在监听通信

- 在量子通讯中，信息被编码于量子态
- 量子力学中，测量过程对系统的扰动具有原理方面的根源——测量即制备
- 一对不对易的物理量，测量其中一个物理量，不可避免的扰动另一个物理量
- 这一内在量子性质，使得探测入侵成为可能

- 该可能性被用来产生通讯双方之间的量子密钥
- 大部分量子保密体系的安全性，由量子不可克隆定理保证

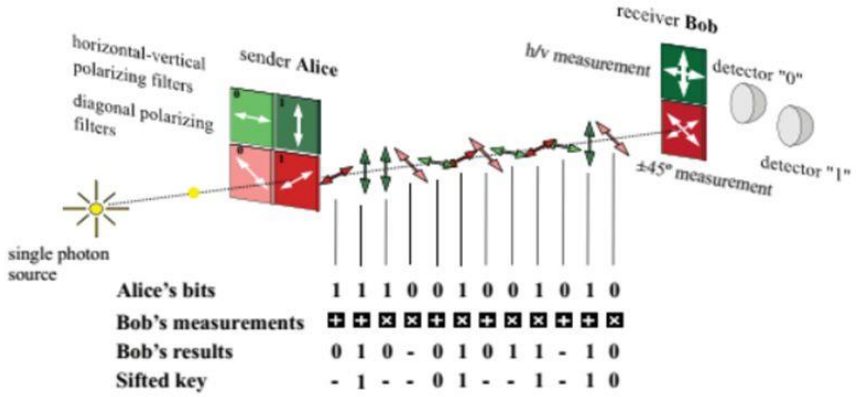
BB84方案

- 1984年，Bennett和Brassard提出第一个量子密码协议
- 发送者Alice，接收者Bob
- 用光子的偏振态编码信息

$$|\leftrightarrow\rangle, |\circlearrowleft\rangle \to 0, \qquad |\updownarrow\rangle, |\circlearrowright\rangle \to 1$$

- BB92改编码方式为

$$|\leftrightarrow\rangle, |\nearrow\rangle \to 0, \qquad |\updownarrow\rangle, |\nwarrow\rangle \to 1$$



Alice产生随机数	1	1	1	0	0	1	0	0	1	0	1	0
随机选择基发送	×	+	+	+	+	×	×	+	×	×	+	×
Bob随机选择测量基	+	+	×	×	+	×	+	×	×	+	+	×
Bob的测量结果	0	1	0	–	0	1	0	1	1	–	1	0
Alice核对测量基	F	T	F	F	T	T	F	F	T	F	T	T
筛选后的raw key	–	1	–	–	0	1	–	–	1	–	1	0
抽检部分字节核对	如果噪声和窃听者造成的错误率过大，则放弃本次发送的字串											
信息调整	经典纠错											
保密增强												

如果窃听者Eve
（1）截获Alice发送的每个量子比特
（2）沿某个轴测量偏振态
（3）把测得的态发给Bob
那么她在生钥中引入了1/4的错误率