

简明量子力学

量子通信和争鸣会

吴飙

2022.05.31

量子通信

经典通信



0, 1



量子通信



$\alpha|0\rangle + \beta|1\rangle$



Alice


Bob

经典通信是一种特殊的量子通信

信息载体

经典通信: 光或电磁波 (调幅, 调频),
声音, 书信 ...

量子通信:

任何经典媒介:  容量
必须事先知道量子态

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

2^{100} 个分量

1: ~~1, 0, 1~~

光的偏振

水平偏振: $|0\rangle$

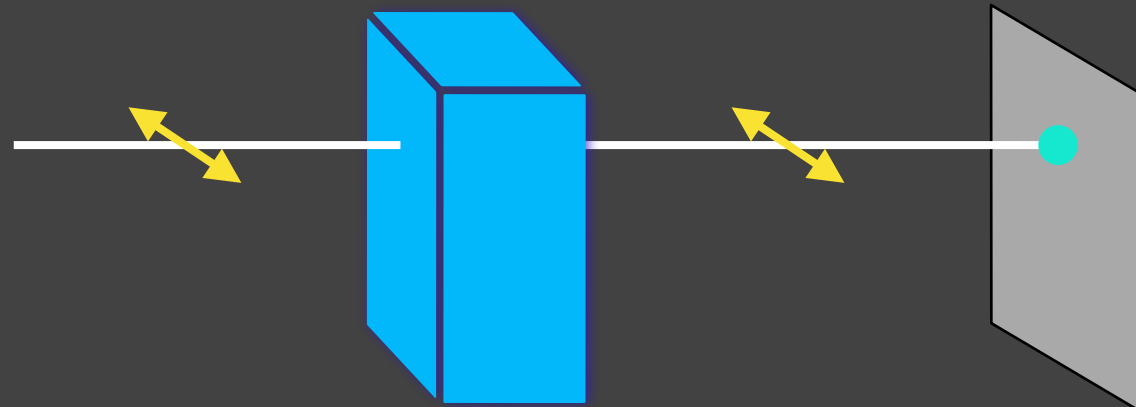
垂直偏振: $|1\rangle$

$$\alpha|0\rangle + \beta|1\rangle$$

光子偏振测量 M_z

方解石晶体

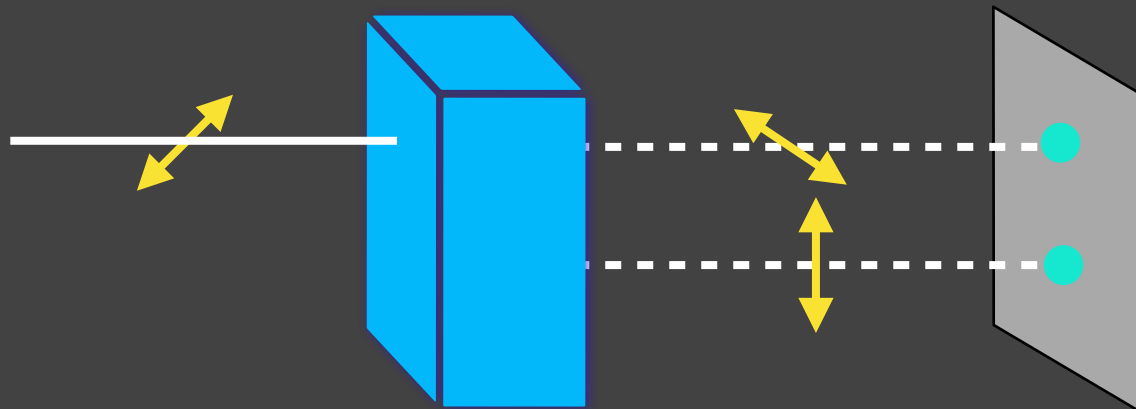
水平偏振: $|0\rangle$



垂直偏振: $|1\rangle$

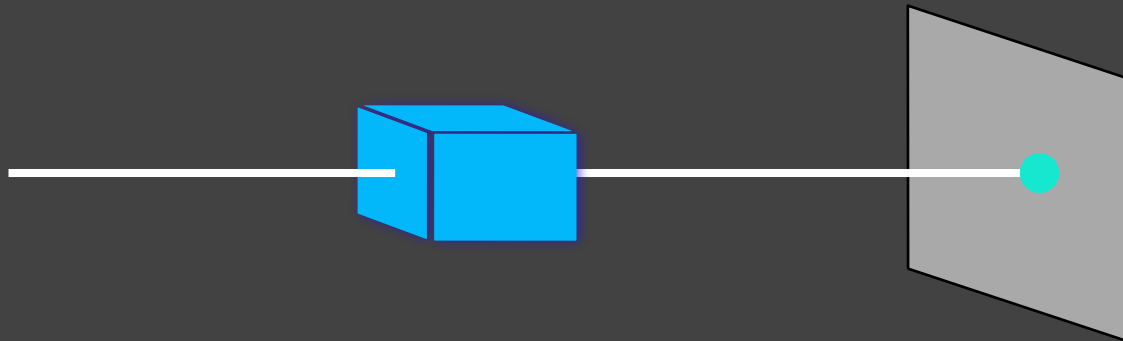


$\alpha|0\rangle + \beta|1\rangle$

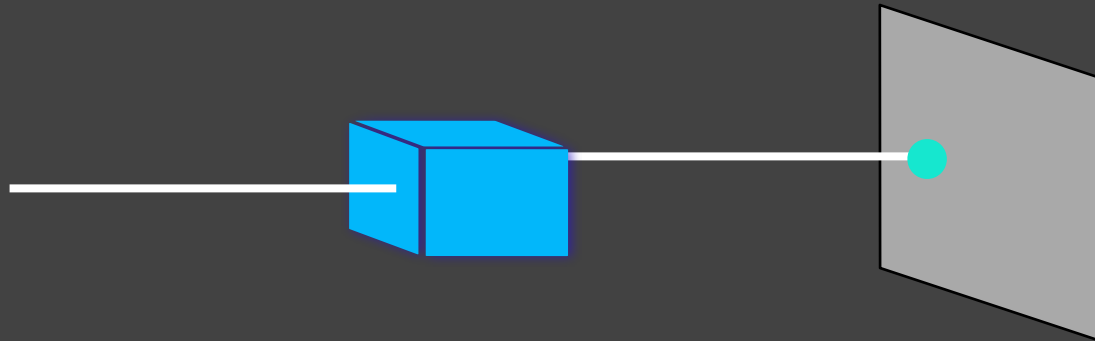


光子偏振测量 M_x

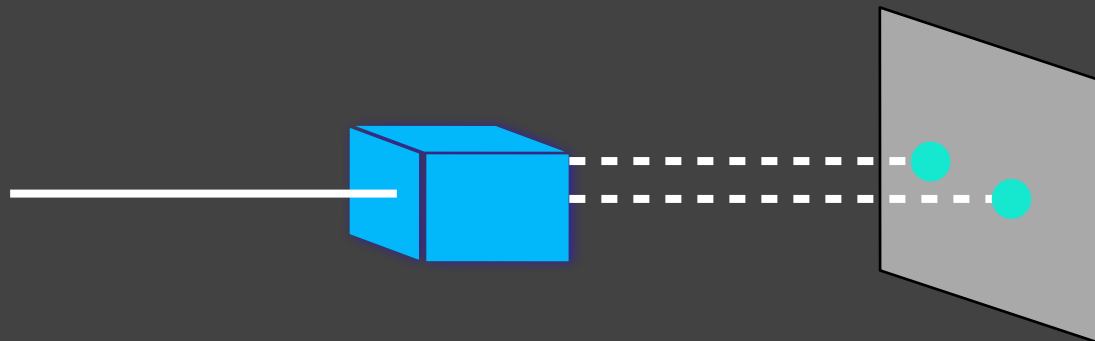
$$|0_x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$




$$|1_x\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$



$$\alpha|0\rangle + \beta|1\rangle$$



量子通信的方式

1. 经典方式 $\frac{1}{2}|0\rangle - \frac{\sqrt{3}}{2}i|1\rangle$ 经典信道 

2. 量子方式

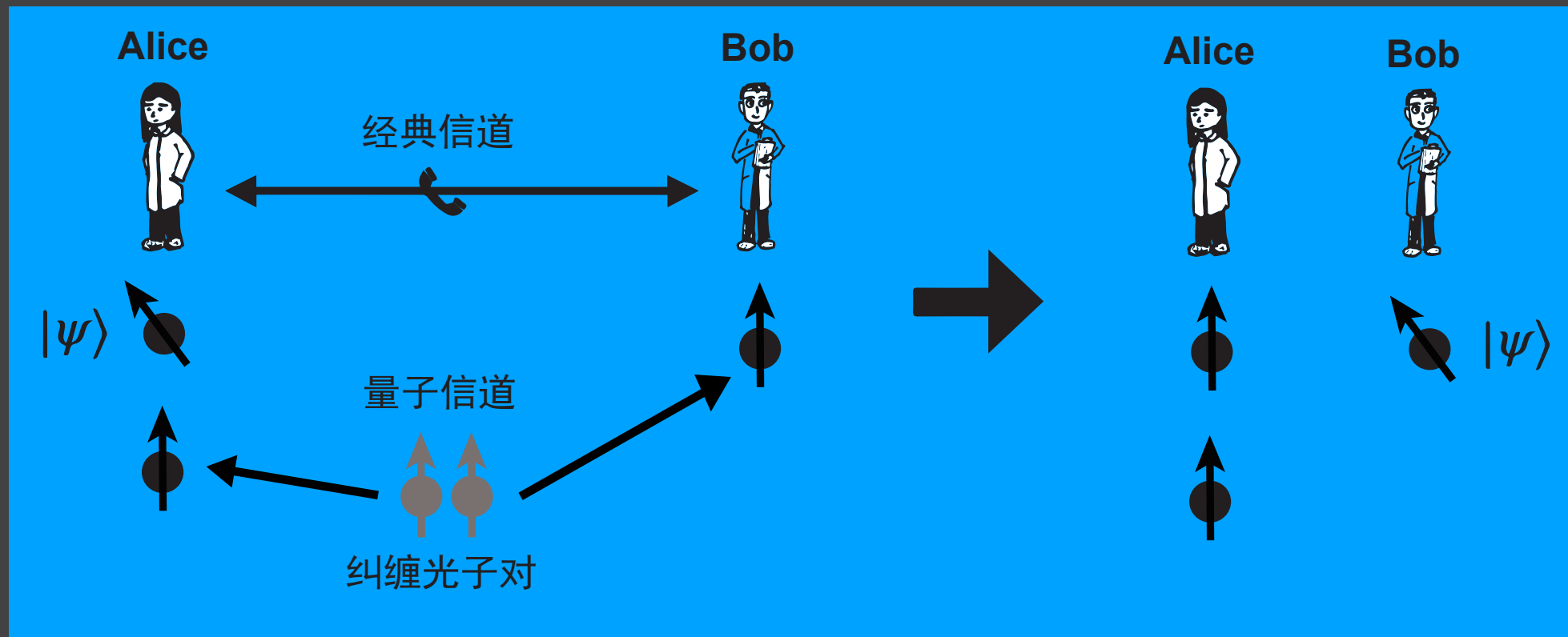


3. 量子隐形传态

Alice

Bob

量子隐形传态



$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

光子

$$|\chi_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

量子隐形传态

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad |\gamma_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$|\Phi_0\rangle = |\psi\rangle \otimes |\gamma_{00}\rangle = \frac{1}{\sqrt{2}}(\alpha|0\rangle + \beta|1\rangle) \otimes (|00\rangle + |11\rangle)$$

$$= \frac{1}{\sqrt{2}} \left\{ \alpha|0\rangle \otimes (|00\rangle + |11\rangle) + \beta|1\rangle \otimes (|00\rangle + |11\rangle) \right\}$$

$$= \frac{1}{\sqrt{2}} \left\{ \alpha|\underline{000}\rangle + \alpha|\underline{011}\rangle + \beta|\underline{100}\rangle + \beta|\underline{111}\rangle \right\} \quad \text{Alice's}$$

Alice CNOT门操作

$$|\Phi_1\rangle = \frac{1}{\sqrt{2}} \left\{ \alpha|000\rangle + \alpha|011\rangle + \beta|110\rangle + \beta|101\rangle \right\}$$

Alice CNOT门操作

$$|\Phi_1\rangle = \frac{1}{\sqrt{2}} \{ \alpha |000\rangle + \alpha |011\rangle + \beta |110\rangle + \beta |101\rangle \}$$

$$|\Phi_1\rangle = \frac{1}{\sqrt{2}} \{ \alpha |0\rangle \otimes (|00\rangle + |11\rangle) + \beta |1\rangle \otimes (|10\rangle + |01\rangle) \}$$

Alice 对第一个光子做哈达玛门操作

$$|\Phi_2\rangle = \frac{1}{2} \left\{ \alpha (|0\rangle + |1\rangle) \otimes (|00\rangle + |11\rangle) + \right. \\ \left. + \beta (|0\rangle - |1\rangle) \otimes (|10\rangle + |01\rangle) \right\}$$

$$|\Phi_2\rangle = \frac{1}{2} \left\{ \underline{|00\rangle} (\alpha |0\rangle + \beta |1\rangle) + |01\rangle (\alpha |1\rangle + \beta |0\rangle) + \right. \\ \left. + |10\rangle (\alpha |0\rangle - \beta |1\rangle) + |11\rangle (\alpha |1\rangle - \beta |0\rangle) \right\}$$

$-\hat{\sigma}_z$

$\hat{\sigma}_z \hat{\sigma}_x$

$\rightarrow |14\rangle$

量子态传递方法比较

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

| 方法 | 纯经典 | 纯量子 | 量子隐形传态 |
|-----------|-----|-----|--------|
| 是否需要知道量子态 | 是 | 否 | 否 |
| 是否需要经典信道 | 是 | 否 | 是 |
| 是否需要量子信道 | 否 | 是 | 是 |
| 隐秘性 | 低 | 高 | 高 |
| 稳定性 | 高 | 低 | 低 |

经典通信

信号强，不容易受干扰

$$W / h\nu \text{ Abits}$$

4G手机：每一个比特的信息是由
100万个光子携带的

数据量大

单比特和多比特信息
的传递没有本质区别

量子通信

(相干) 信号容易受干扰

一个比特的信息是由
一个~~个~~光子携带的

数据量小 $|4\rangle = \alpha|0\rangle + \beta|1\rangle$
 $|\Phi\rangle = \alpha(|00\rangle + |11\rangle)$

单比特和多比特信息
的传递有很大区别

量子通信的用处

- 日常生活中的用处非常有限
- 连接量子计算机
- 分配密码

经典加密

日常生活中的加密：

- 1、登录密码
- 2、家乡话
- 3、公钥加密系统

间谍和军事中的加密：

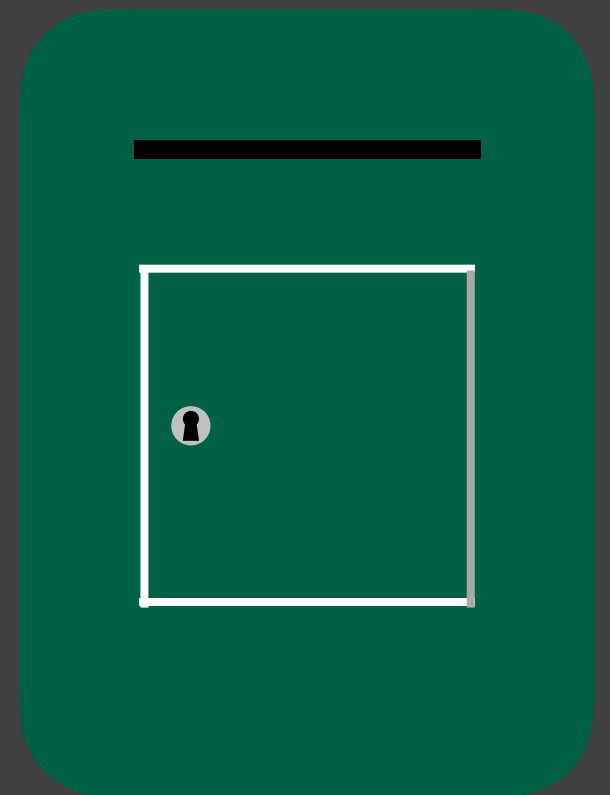
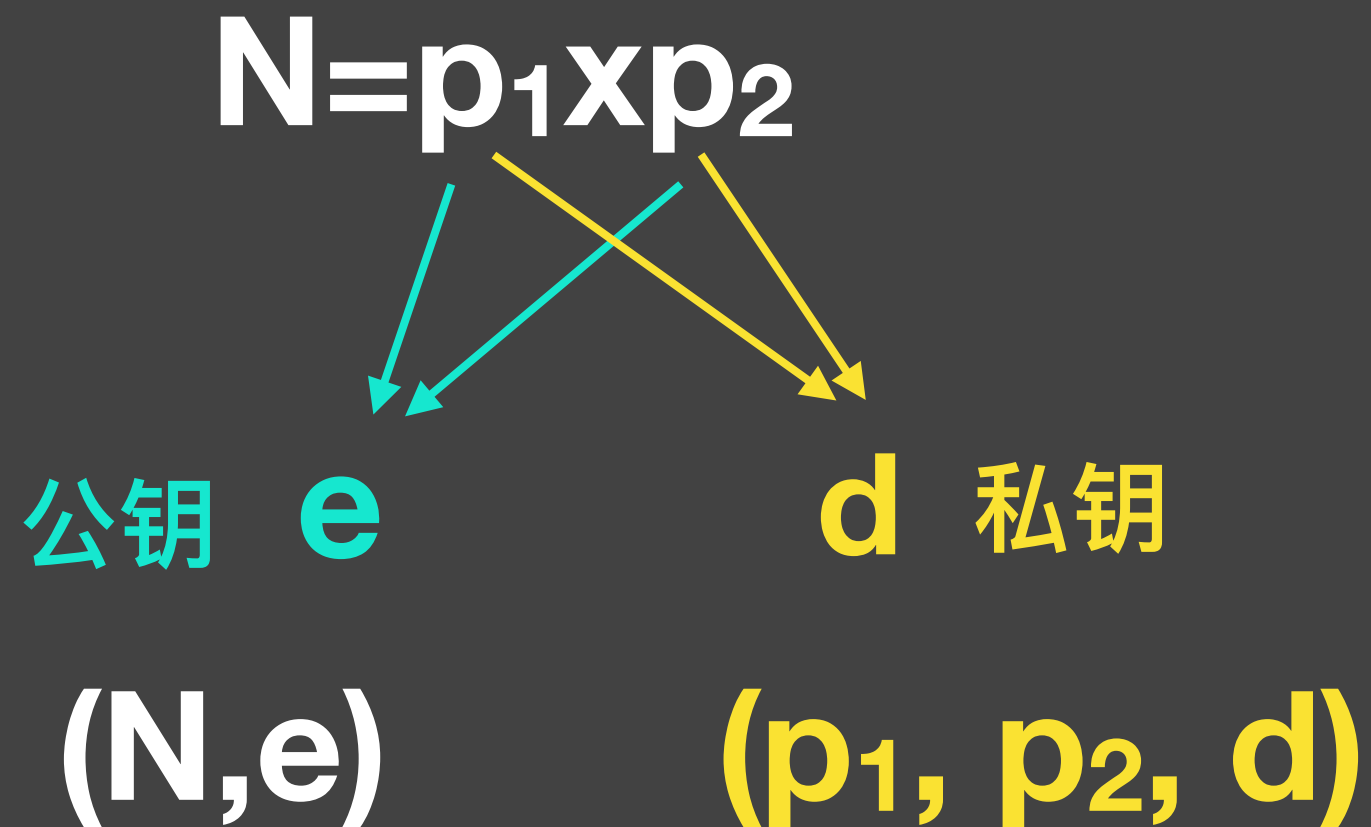
- 1、口令
- 2、系统加密
- 3、维南(Vernam)加密法

RSA密码

Ron Rivest

Adi Shamir

Leonard Adleman



维南(Vernam)加密法

| | | | | | | | |
|--------|-----|-----|-----|-----|-----|-----|-----|
| 信息 | q | u | a | n | t | u | m |
| ASCII | 113 | 117 | 97 | 110 | 116 | 117 | 109 |
| 密码 | 014 | 013 | 000 | 031 | 000 | 012 | 010 |
| ASCII | 099 | 104 | 097 | 079 | 116 | 105 | 099 |
| 加密后的信息 | c | h | a | O | t | i | c |

量子通信以前， 维南密码是近距离分配的！

量子密钥分配方案： BB84

Charles Bennett Gilles Brassard

$$|\varphi_{00}\rangle = |0\rangle \quad |\varphi_{10}\rangle = |1\rangle$$

$$|\varphi_{01}\rangle = |0_x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$|\varphi_{11}\rangle = |1_x\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

0: 不发生偏移

1: 发生偏移

| 偏振态 | $ 0\rangle$ | | $ 1\rangle$ | | $ 0_x\rangle$ | | $ 1_x\rangle$ | |
|-------|-------------|-----|-------------|------|---------------|-----|---------------|------|
| 测量结果 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |
| M_z | 100% | 0% | 0% | 100% | 50% | 50% | 50% | 50% |
| M_x | 50% | 50% | 50% | 50% | 100% | 0% | 0% | 100% |

BB84步骤:

1. Alice 随机产生两个二进制数 a 和 b , a 保密而 b 暂时保密
2. 按照 a 和 b , Alice利用量子隐形传态向Bob传送一系列量子态 $|\varphi_{a_k, b_k}\rangle$
3. Bob 随机产生一个二进制数 b' , 并按 b' 对收到的量子态 $|\varphi_{a_k, b_k}\rangle$ 进行 M_x 或 M_z 测量
4. 记录下相应的测量结果, 这些结果组成另外一个二进制数 a'
5. Alice公布 b , Bob将 b' 和 b 对比, 如果 $b_k=b'_k$, 则保留相应 a'_k .

这些 a_k 就是最后的密码

| | | | | | | | | | |
|-----|------------------------|------------------------|------------------------|------------------------|------------------------|------------------------|------------------------|------------------------|------------------------|
| a | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 1 |
| b | 0 | 0* | 1 | 0* | 0 | 1* | 1 | 0* | 1 |
| 偏振态 | $ \varphi_{10}\rangle$ | $ \varphi_{00}\rangle$ | $ \varphi_{11}\rangle$ | $ \varphi_{10}\rangle$ | $ \varphi_{10}\rangle$ | $ \varphi_{01}\rangle$ | $ \varphi_{01}\rangle$ | $ \varphi_{00}\rangle$ | $ \varphi_{11}\rangle$ |
| | $ 1\rangle$ | $ 0\rangle$ | $ 1_x\rangle$ | $ 1\rangle$ | $ 1\rangle$ | $ 0_x\rangle$ | $ 0_x\rangle$ | $ 0\rangle$ | $ 1_x\rangle$ |
| b' | 1 | 0* | 0 | 0* | 1 | 1* | 0 | 0* | 0 |
| 测量 | M _x | M _z | M _z | M _z | M _x | M _x | M _z | M _z | M _z |
| a' | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 |

Jeremy Knowles, Harvard professor

the most important goal of higher education is to ensure that graduates can recognize when someone is talking rot

高等教育最重要的目的是让学生能辨别有人在胡说八道

- 希望你能辨别有人在胡说八道量子
- 不期望你能用量子力学去解决问题！

然后还有量子纠缠问题，超越光速的超距作用，仿佛空间是不真实存在的，为什么会这样？物理学家还是不知道，哪怕他们可以用公式描述，甚至可以用这个规律来进行保密通讯，但是没有人能给出一个符合直觉和逻辑的简洁解答。

维尔切克(Frank Wilczek)

对年轻学生的寄语：



一，探索知识的海洋。找出哪些学科看起来有前途，哪些学科你喜欢。试着发现你特别擅长什么（你可能会对自己感到惊讶）。不要仅仅满足于你在课本和课程中学到的东西。

二，尽快并尽可能彻底地掌握基础知识。对于理论工作，这包括基础数学（微积分，复变量，线性代数……）。对于实验工作，这包括电子学和熟悉标准工具。熟练运用英语和电脑（搜索工具、文字处理，用于建模和统计的高级编程语言比如Mathematica或者MATLAB）也很重要。

三，阅读大师们的著作，如达尔文、爱因斯坦、费曼，以及你感兴趣的领域的历史名著。他们设定了清晰和深度的标准。我虽然没有达到他们的水平，我也推荐我的书《万物原理》——你可以在我的网站frankwilczek.com上找到大量有趣的材料。

我的大学与我的失败 薄祜