

2021-2022学年春季学期

量子信息与量子密码

*Quantum Information &
Quantum Cryptology*

授课团队：杨理，黄震宇
助教：刘霞

课程的背景和意义

- 在量子信息科学中，把量子态序列视为消息，对量子态序列提出信息论问题，是基于自然界基本定律对信息概念的自然推广，是人类在信息概念上的巨大飞跃，是量子信息科学的基石。

- 从量子信息观点来看经典信息仅是量子信息的一个子集（计算基态集合）。

- 经过五十余年的努力，量子信息论已经基本建立起来，如：Holevo定理（1964, 1973），Schumacher定理（1995），HSW定理（1998），等等。这些工作与Shannon1948年关于信息论的经典论文相对应。

(续)

- 随着量子物理实验技术的进步，人类逐渐能够独立操纵仅含单个量子的系统，各类量子技术的发展成为时代技术进步的洪流
- 其中量子密码和量子计算机的发展、量子霸权的争夺已经成为中美等国高新技术竞争的热点。
- 随着量子信息技术的飞速发展，实用量子信息系统的出现已无悬念。信息安全和保密领域的研究者面临的一个新的重要课题是：如何保障包含量子信息系统在内的整个信息系统的安全？

(续)

- 真正解决这一重大理论和应用问题的前提是建立了同时涵盖量子信息系统和经典系统的密码学理论，我们称之为“量子信息密码学”，这些工作与Shannon1949年关于密码学的奠基性论文和后来几十年密码学的发展相对应。

- 由于“量子信息密码学”研究是在一个更大的空间上考察密码学理论框架，它有可能使密码学的结构更清晰、基础更牢固。

(续)

- Shannon把加解密问题抽象为数学问题极大推动了密码学的建立和发展，但密码编码和密码分析需要通过具体的物理过程来实现，将计算技术回归到它的物理本质乃至量子过程来分析，正是30年前Benioff、Feynman和Deutsch等人发展量子计算理论时的思想。
- 量子信息概念是洞察了信息概念的物理本质后提出的，基于此人们发展了量子信息论、量子计算复杂性理论和量子编码理论。今天我们发展量子信息的密码学，奠定量子信息系统安全性的理论基础，正是在密码学和信息安全理论发展中顺应了这样一种大趋势。

教材

- ◆ Michael A. Nielsen and Isaac L. Chuang,
Quantum Computation and Quantum Information,
Cambridge University Press 2000.
(高等教育出版社有引进版)

- ◆ 中译本：赵干川、郑大钟译，
《量子计算与量子信息》（一、二），清华大学出版社，
2003, 2005。

参考书

- John Preskill, *Quantum Information and Computation*, Lecture Notes for Physics 299, 1998
- Jozef Gruska, *Quantum Computing*, McGraw-Hill, London, 1999
- H. –K. Lo, S. Popescu, and T. Spiller, *Quantum Information and Computation*, World Scientific, 1998
- 李承祖、陈平形、梁林梅、戴宏毅编著，《量子计算机研究》，科学出版社，2011

- A. Peres, *Quantum Theory: Concepts and Methods*, Kluwer Academic Publishers, 1995

本课主要内容

- ◆ 绪论：量子信息简介（第一章及补充）
 - ◆ 线性代数与量子力学基础（第二章及补充）
 - ◆ 量子计算模型（第四章的一部分及补充）
 - ◆ Shor算法（第五章），Grover算法（第六章的一部分）
 - ◆ 量子系统的演化与量子操作（第八章的一部分）
 - ◆ 量子态空间的度量（第九章）
 - ◆ 量子纠错码与容错量子计算（第十章的一部分）
 - ◆ 量子熵（第十一章）
 - ◆ 量子信息论与量子密码（第十二章的一部分及补充）
-
- ◆ 如果有时间会介绍量子计算物理实现方案（第七章）

量子信息与量子密码

Quantum Information & Quantum Cryptology

[第1次课] 绪论：量子信息简介

授课教师：杨理

授课时间：2022年3月7日

Science

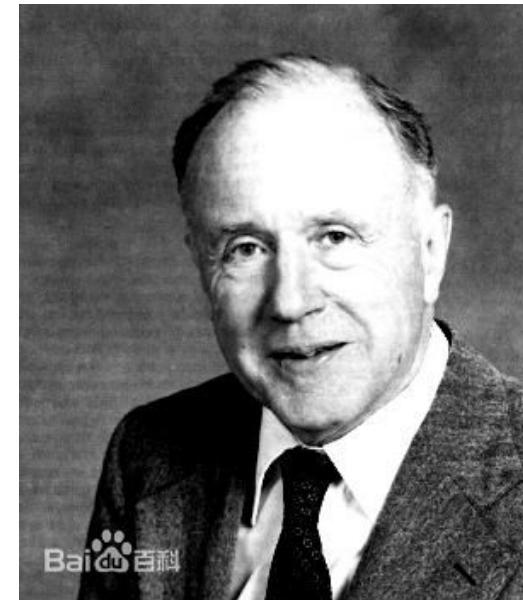
Science offers the boldest metaphysics of the age. It is a thoroughly human construct, driven by the faith that if we dream, press to discover, explain, and dream again, thereby plunging repeatedly into new terrain, the world will somehow come clearer and we will grasp the true strangeness of the universe. And the strangeness will all prove to be connected, and make sense.

— *Edward O. Wilson*

“科学给出了这个时代最为大胆的形而上学。它是受一种信念驱使而建立的纯粹人为的理论，这种信念就是：只要我们敢于梦想、努力发现、解释现象、再去梦想，就可以不断进入新的领域，世界将以某种方式变得清晰起来，我们将抓住宇宙的真正奇妙之处。这些奇妙之处最后将被证明是相互联系的，并呈现出某种意义。”

John Archibald Wheeler 晚年在其自传上写道：

献给多年来启迪指引我的美好教师、学生以及同事；
同时，
也献给目前未见于经传的人们，
因为他们会去探索量子是怎么一回事，
存在又是怎么一回事，
我们因此得以进一步阐扬这个神奇的美丽世界之玄妙。
只有当我们了解宇宙之神奇，
我们才能认识其单纯。



内容概要

- ◆ 量子物理概念的历史发展
- ◆ 量子力学的基本假设
- ◆ 神秘之源：态叠加原理
- ◆ 量子比特与量子信息
- ◆ 量子密码：从QKD到希尔伯特空间上的密码学
- ◆ 丘奇-图灵论题
- ◆ 量子计算
- ◆ 量子计算机
- ◆ 信息处理：经典vs量子

何为量子

- ▶ 普朗克“作用量子”假设（1900年）

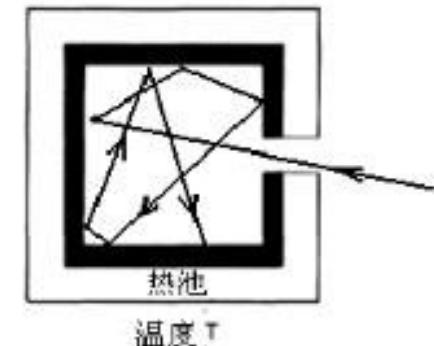
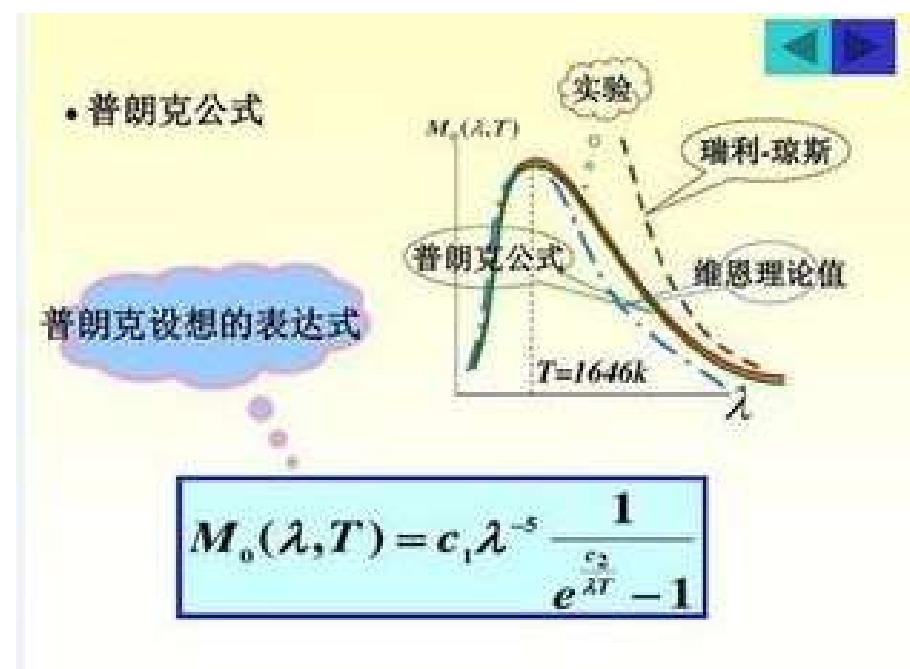
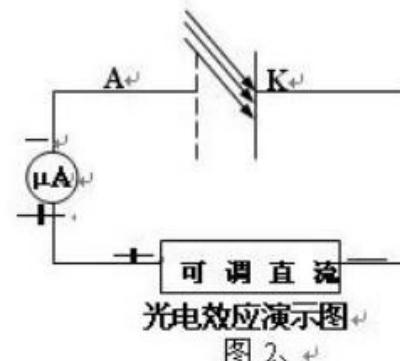
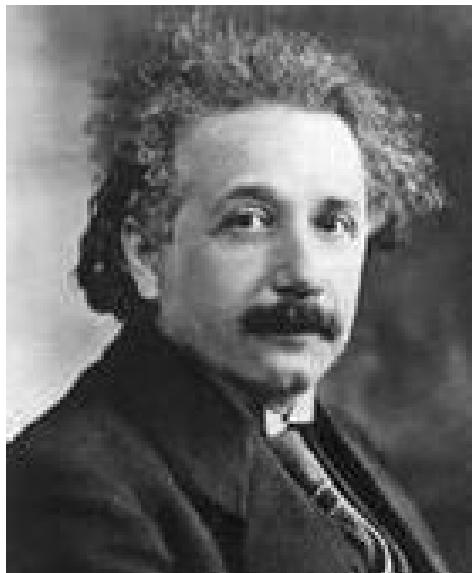


图1 黑体的模拟

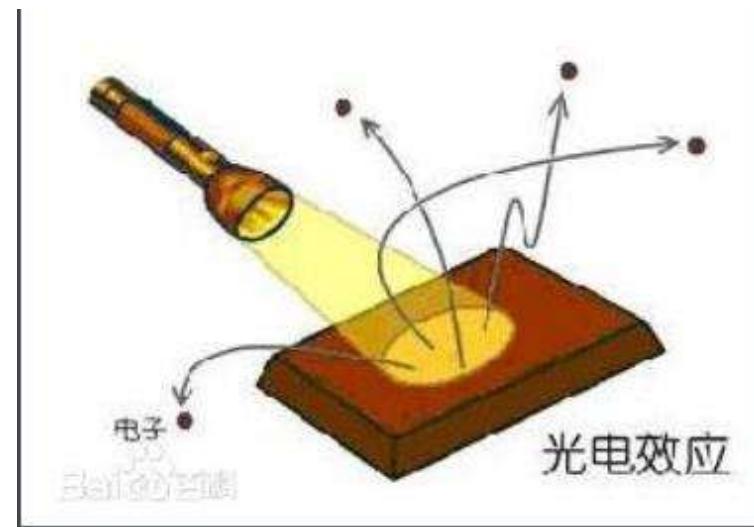


光量子——光子，波粒二象性

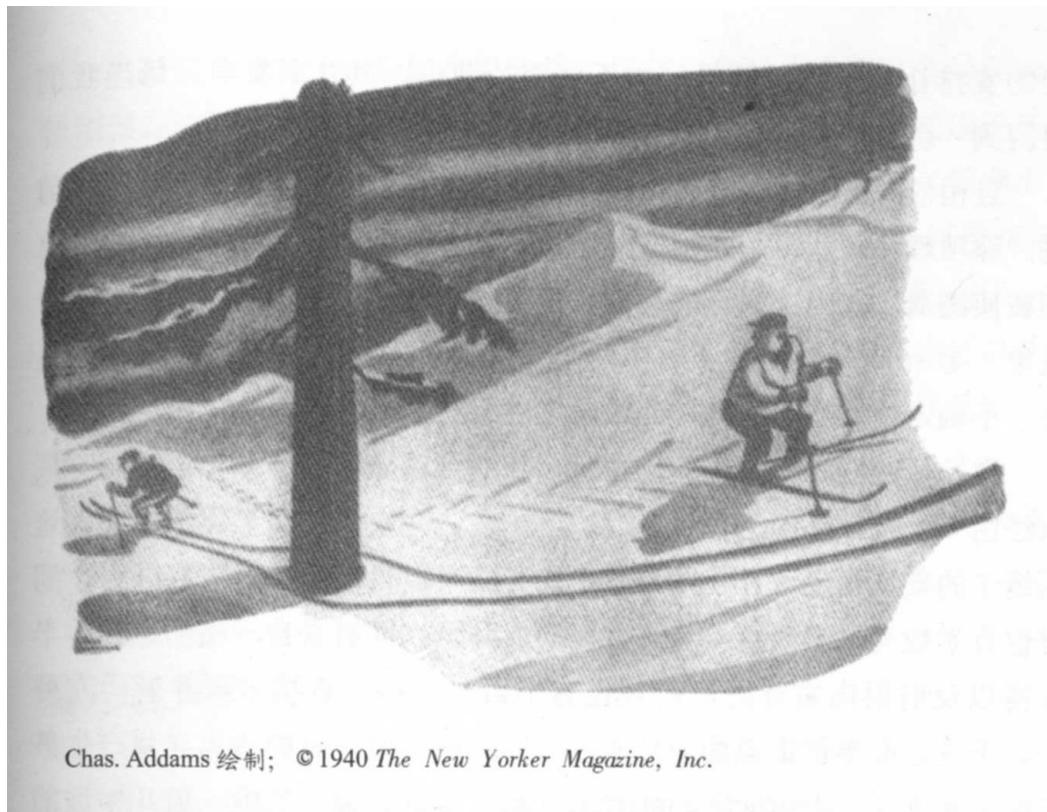
- ▶ 爱因斯坦光电效应理论：波粒二象性（1905年）



光电效应演示图
图 2.4



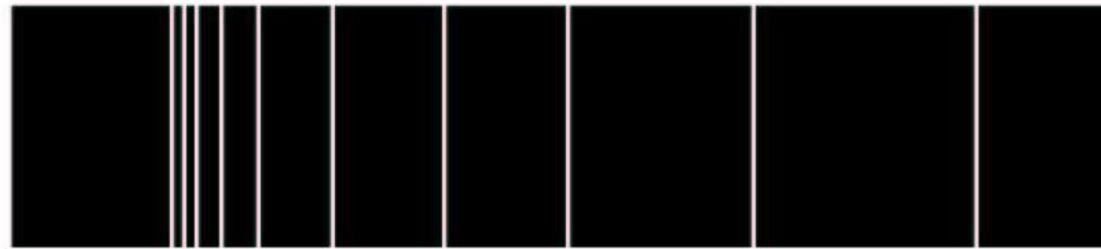
波粒二象性



Quantum Mechanics: Real Black Magic Calculus.
— Albert Einstein



原子的分立光谱



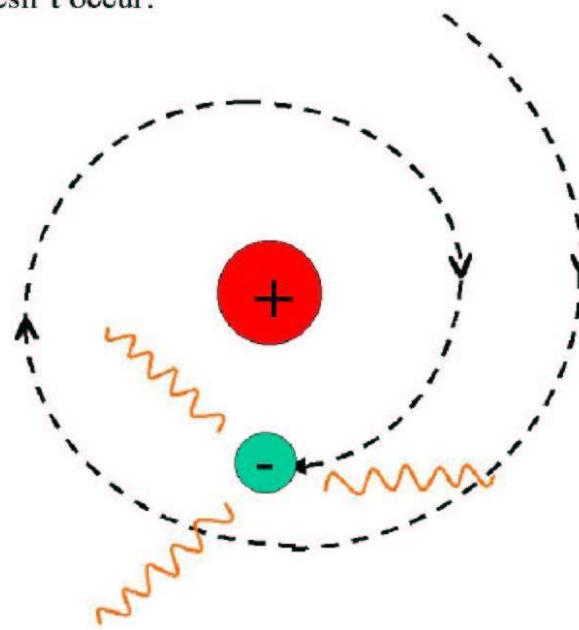
Frequency →



原子核，原子的稳定性问题

This is what should occur according to the Maxwell equations.
But it doesn't occur.

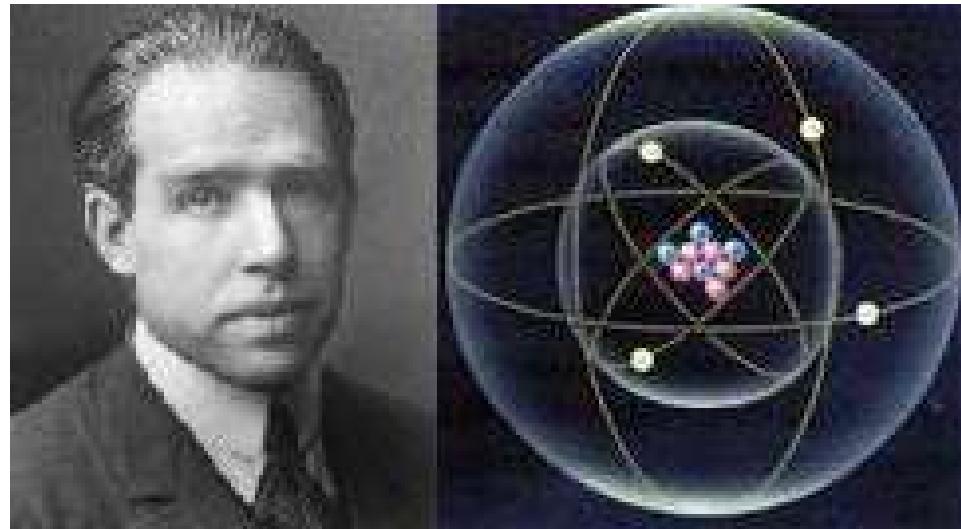
Why?



基于卢瑟福的原子模型，Bohr 提出了氢原子理论，创造性地同时解释了原子光谱的分立性和原子的稳定性问题。

原子模型，定态的提出

- ▶ 玻尔氢原子模型：定态及其跃迁（1913）



量子力学的创立



- ▶ 从玻尔氢原子模型到海森伯矩阵力学：
受爱因斯坦影响，认为只有可观测量才是物理的

Werner Heisenberg

- ▶ 从德布罗意 (*Louis de Broglie*) 物质波到薛定谔波动力学：
尝试为德布罗意物质波建立一个波动方程

Erwin Schrödinger

- ▶ 态叠加原理：量子世界的神秘之源



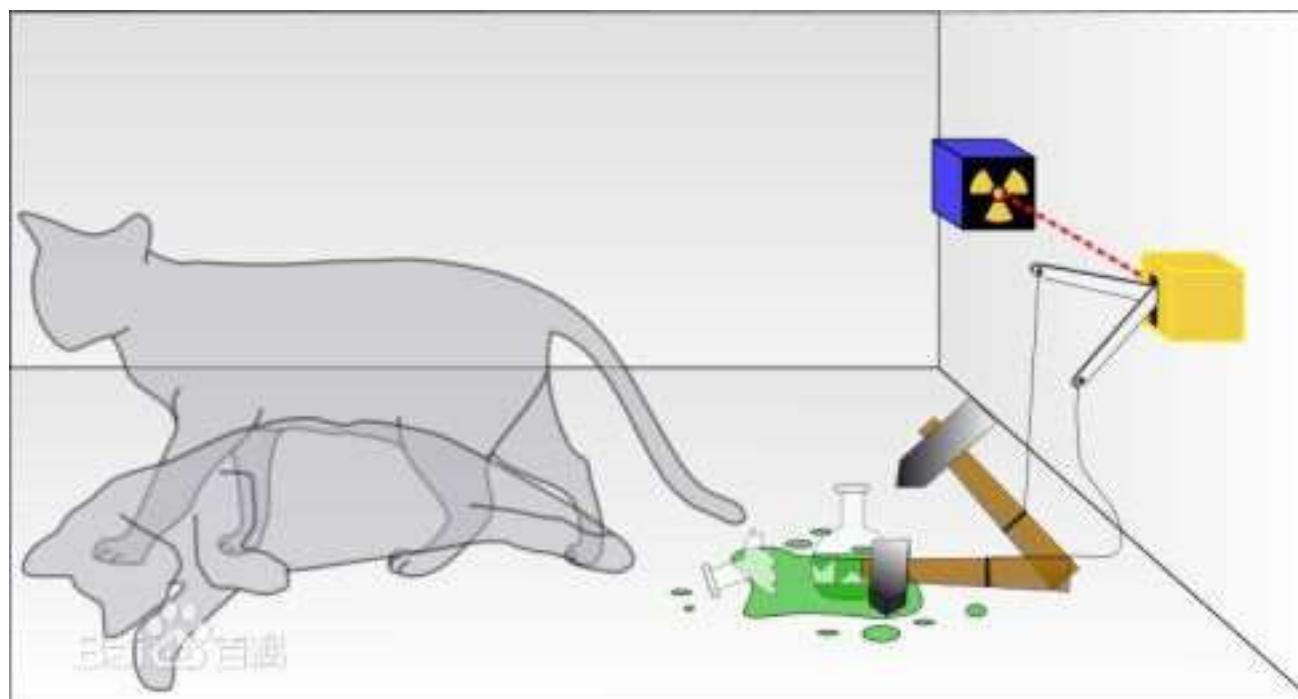
态叠加原理：量子世界的神秘之源

态叠加原理直接导致：

1. 量子态测量的不确定性 → 量子密码的基础
2. 量子态操作的并行性 → 量子计算机的基础



量子纠缠态——薛定谔猫



量子力学的基本假设

1. **波函数假设** 系统状态为 $\psi(\mathbf{r}, t)$, 或记为 $|\psi\rangle$ 。对于孤立系统, 波函数为完全描述, 并有几率波解释。
2. **算符假设** 力学量可用线性厄密算符表示。共轭力学量算符的不可对易性是量子力学的基本特征。

量子力学的基本假设 (2)

3. 测量假设 对力学可观测量的测量使系统随机落入该力学量的一个本征态 $|\varphi_m\rangle$, 概率为 $|\langle\varphi_m|\psi\rangle|^2$ 。

平均值: $\bar{\Omega}_\psi = \int \psi^*(\mathbf{r}) \Omega \psi(\mathbf{r}) d\mathbf{r}$,

用Dirac 符号写为 $\bar{\Omega} = \langle \Omega \rangle_\psi = \langle \psi | \Omega | \psi \rangle$,

不必指出具体采用哪个基展开。

量子力学的基本假设（3）

- 量子系综：大量处于相同的量子态的系统构成量子系综。量子态上的平均值是在量子系综上的平均值。
- 两力学量可同时观测 的充分必要条件：
两力学量算符可对易： $[\hat{A}, \hat{B}] = 0$, 则有共同本征函数系，
可以进行同时测量，测量后系统进入两力学量的一个
共同本征态。

量子力学的基本假设 (4)

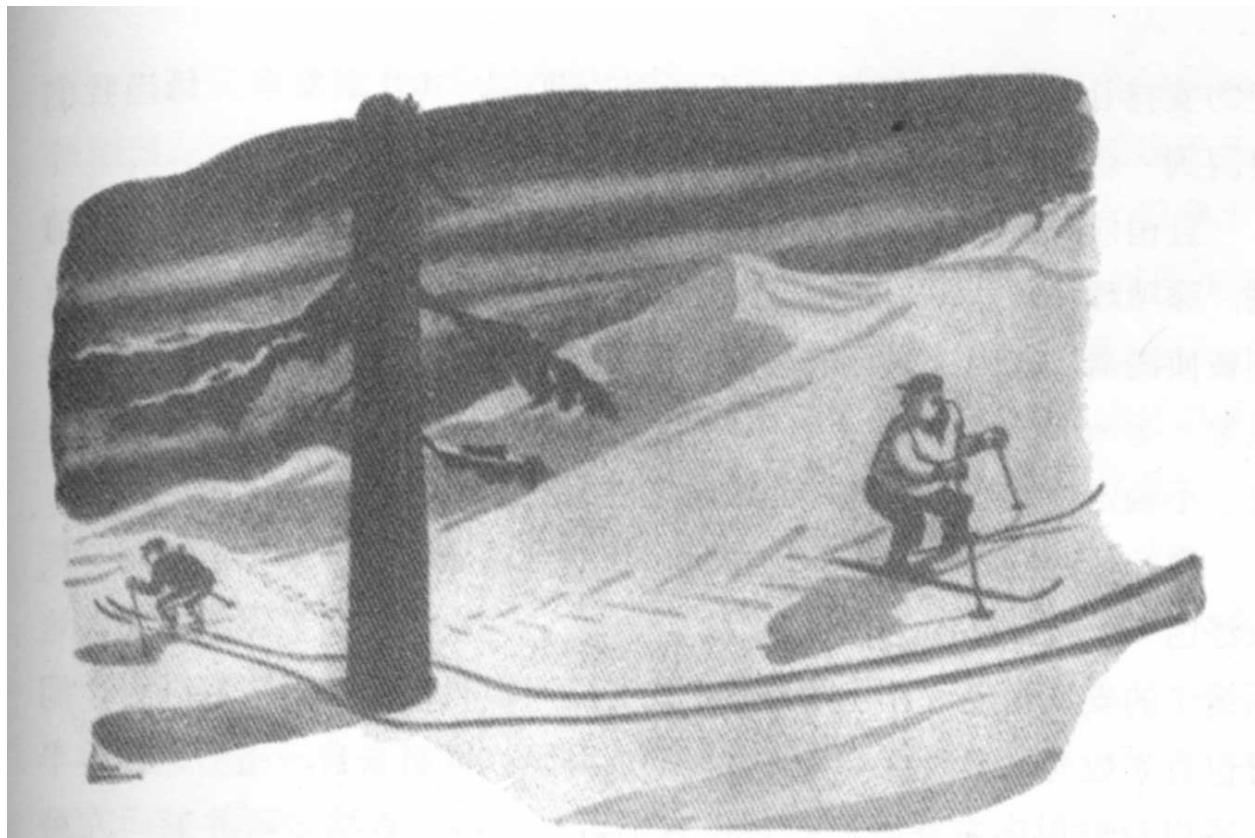
4. 态演化假设 量子态所遵循的演化方程为 Schrödinger 方程：

$$i\hbar \frac{\partial}{\partial t} |\psi(t)\rangle = \hat{H}(p, q, t) |\psi(t)\rangle,$$

其中 $\hat{H}(p, q, t)$ 为系统的哈密顿算符。

5. 全同性假设 全同粒子体系的波函数对于任意两粒子的交换是对称的（玻色子情形）或是反对称的（费米子情形），即自然界存在的态 $|\psi\rangle$ 必须是所有交换算符的本征态： $P_{ij} |\psi\rangle = \pm |\psi\rangle, (i, j = 1, 2, \dots, N).$

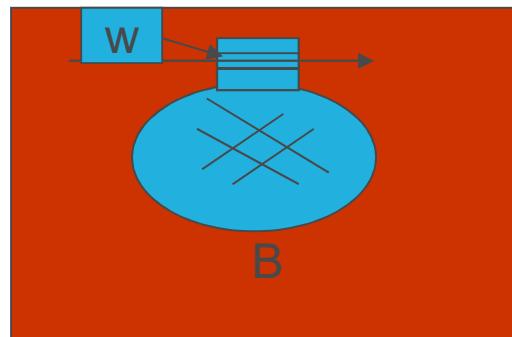
态叠加原理：神秘之源



Chas. Addams 绘制; ©1940 *The New Yorker Magazine, Inc.*

L. Vaidman的光敏炸弹检测问题

◆ 光敏炸弹：光学窗口吸收到光子则爆炸。



◆ 问 题：已知部分炸弹失效。炸弹失效则光子可通过光学窗口。问：如何挑出一部分未失效炸弹？

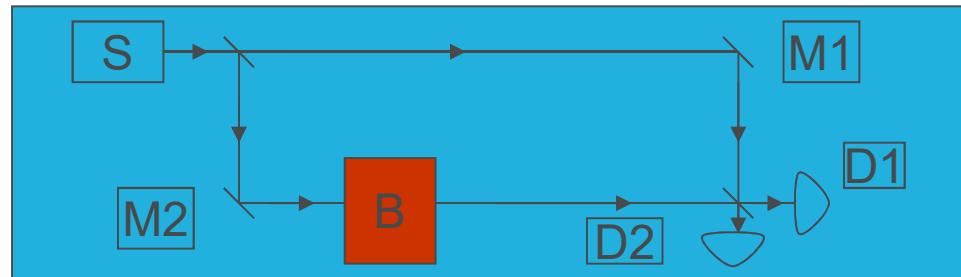
◆ 困 难：采用普通的光学方法时，仅有下述两种情形：

- 1) 炸弹失效则光子通过，可在窗口后面探测到光子；
- 2) 炸弹未失效则光子被吸收，炸弹爆炸。

光敏炸弹检测方案

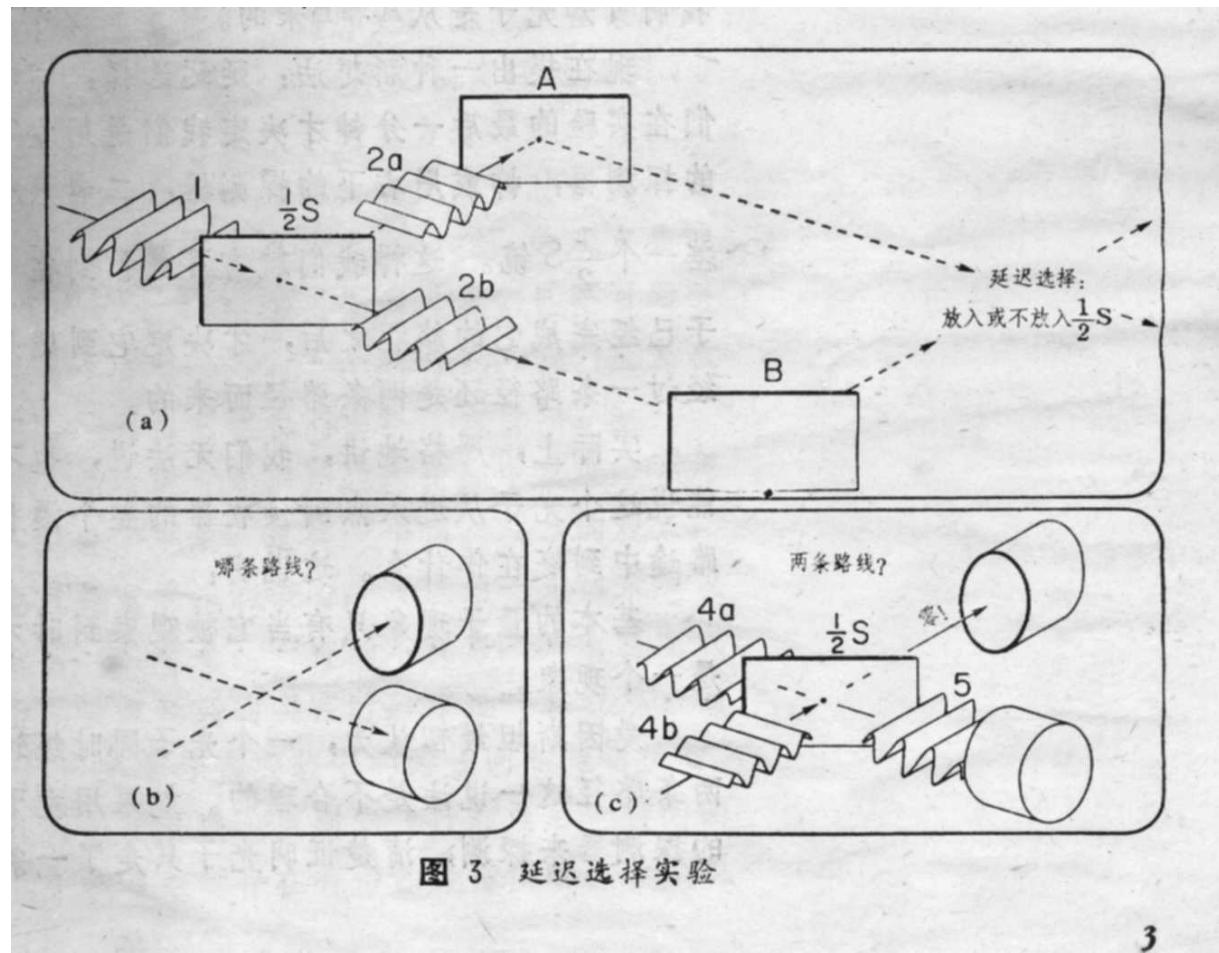
可利用态叠加原理挑出25%的未失效炸弹：

- ◆ 将待检炸弹放置在单光子干涉仪的下臂，如图所示：



- ◆ 炸弹失效，则下臂光路通，干涉仪正常工作，只有探测器1有记录。
- ◆ 炸弹未失效则下臂光路不通，干涉不存在。光子有50%概率引爆炸弹，两个探测器各有25%概率探测到光子。
- ◆ 因为只有一个光子，如果探测器2有记录，则说明炸弹未失效，亦未爆炸。

延迟选择实验（惠勒，1981演讲）



宇宙尺度上的延迟选择实验

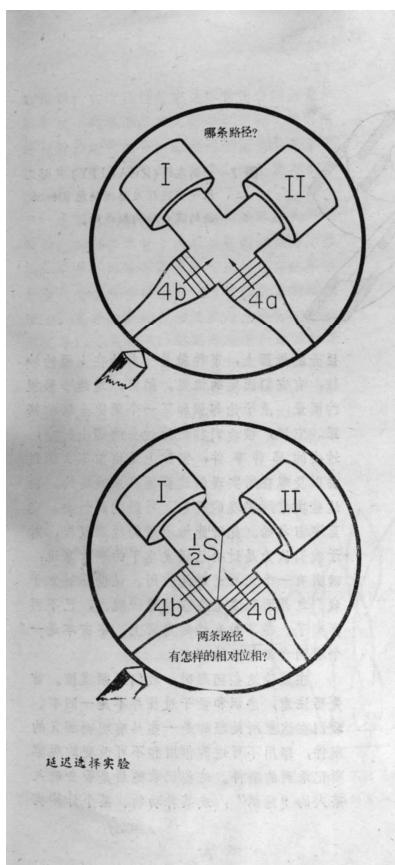
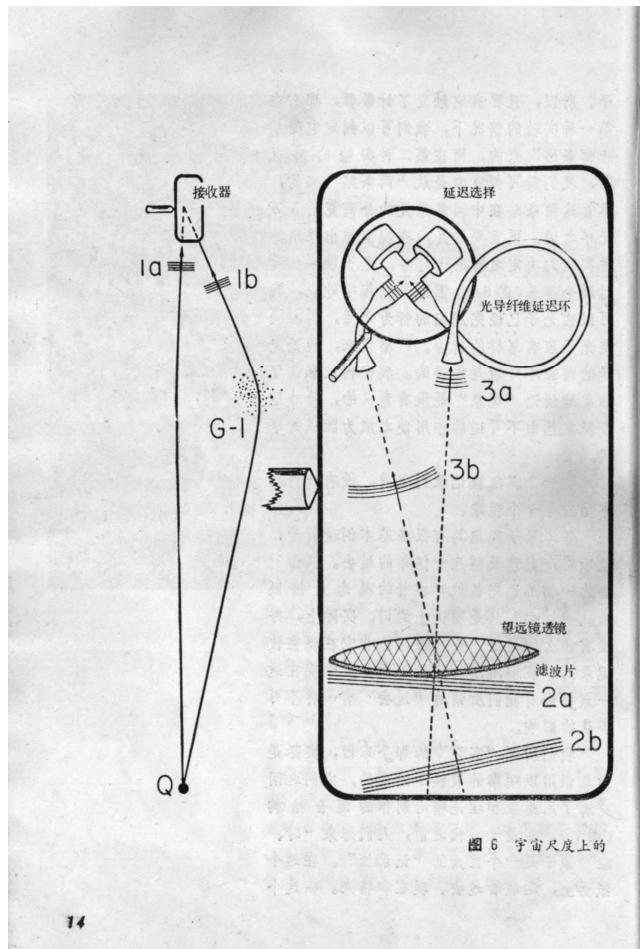


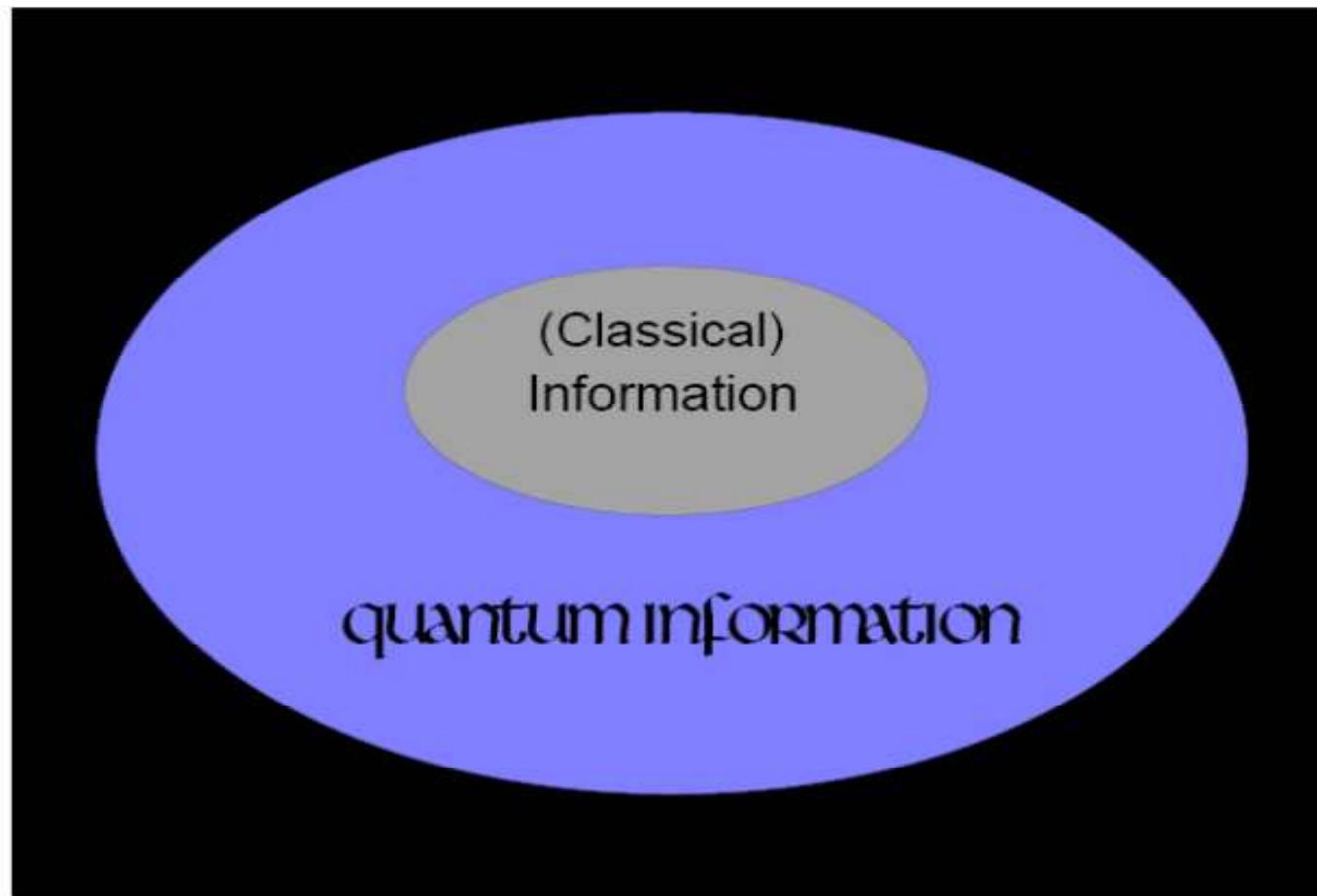
图 5 0957+561A 和 B 两个类星体，实际上是一个类星体的光线经爱因斯坦引力透镜效应后形成的两个像。

什么是信息？

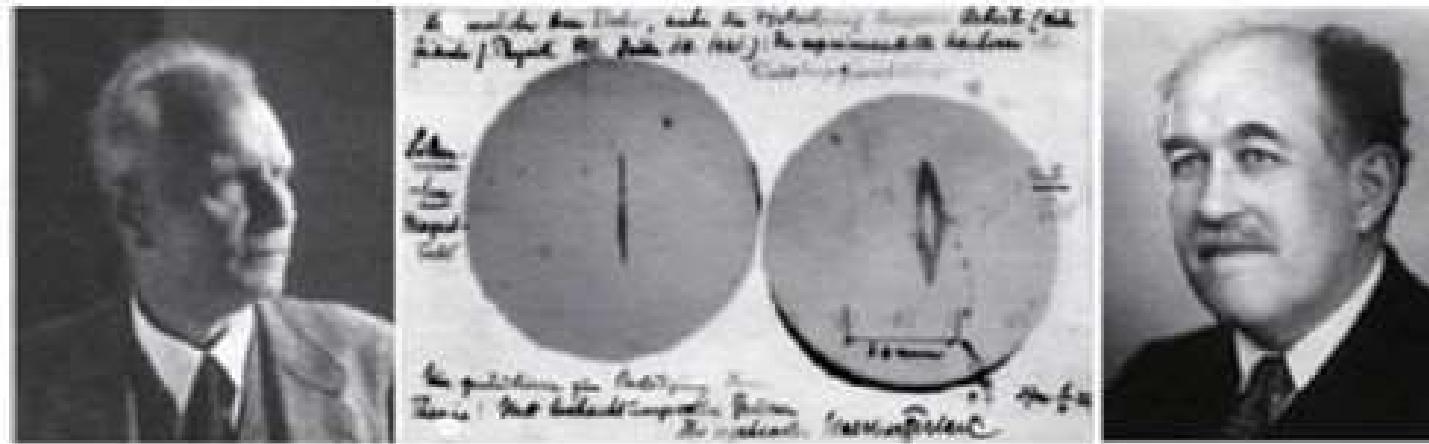
Information is P



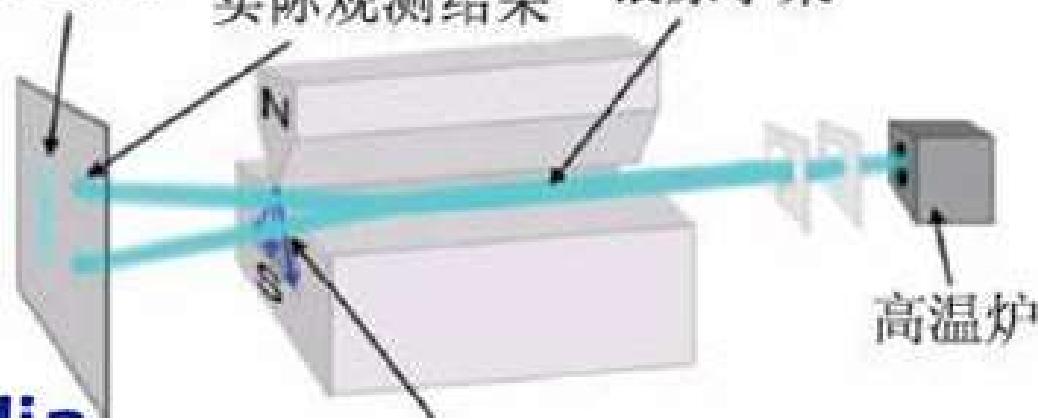
量子比特与量子信息



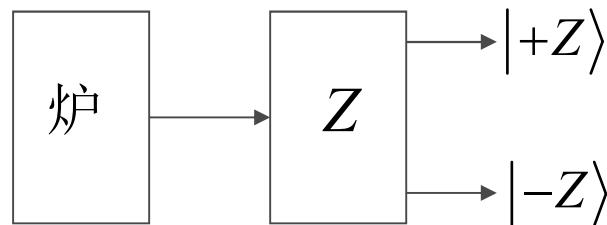
Stern-Gerlach实验



经典预测 实际观测结果 银原子束

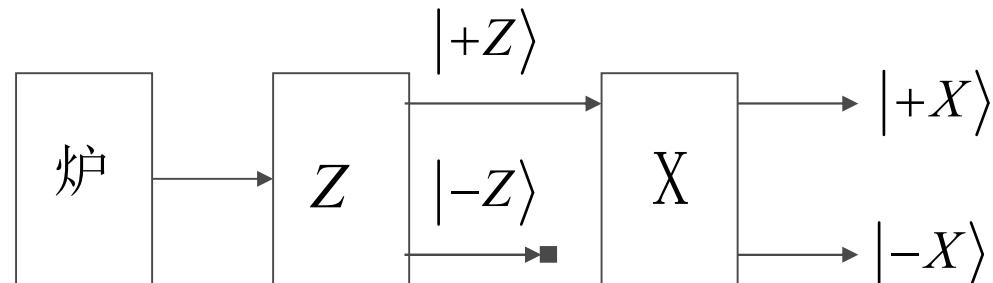


量子比特



Stern-Gerlach实验框图。

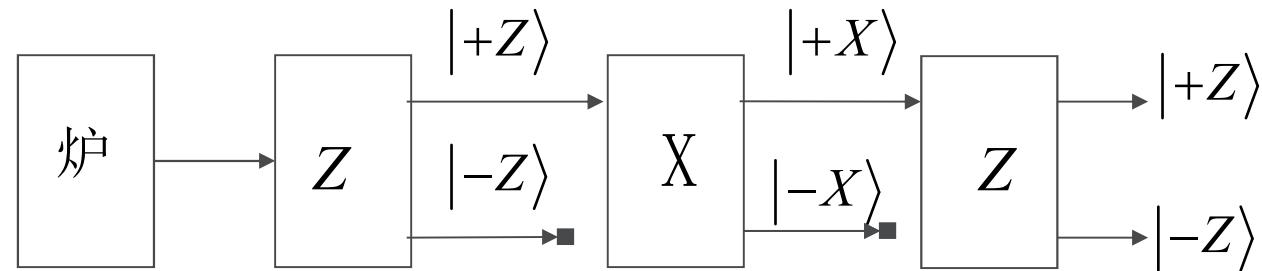
热的银原子从炉体出来经过磁场，引起向上 ($|+z\rangle$) 或向下 ($| - z \rangle$) 的偏转，最终打在一个玻璃片上。



串联的Stern-Gerlach测量。

其中 $|+X\rangle, | - X \rangle$ 代表向左右的偏转。

三阶段串联的Stern-Gerlach实验



三阶段串联的Stern-Gerlach测量。

说 明：即使假设第二套装置的输出是 $|+Z\rangle_{+X}$ 和 $|+Z\rangle_{-X}$ ，第三套装置的输出也是无法解释的。

自旋量子比特

但如果作如下假设：

$$\begin{aligned}|+Z\rangle &\leftarrow |0\rangle, \\ |-Z\rangle &\leftarrow |1\rangle, \\ |+X\rangle &\leftarrow (|0\rangle + |1\rangle)/\sqrt{2}, \\ |-X\rangle &\leftarrow (|0\rangle - |1\rangle)/\sqrt{2},\end{aligned}$$

则可以完满地解释实验现象。

这就是“自旋”态空间假设，“勇敢的海森堡”亦感叹其“勇敢”的假设。

这正是一个自旋量子比特。

量子位的单位球面表示

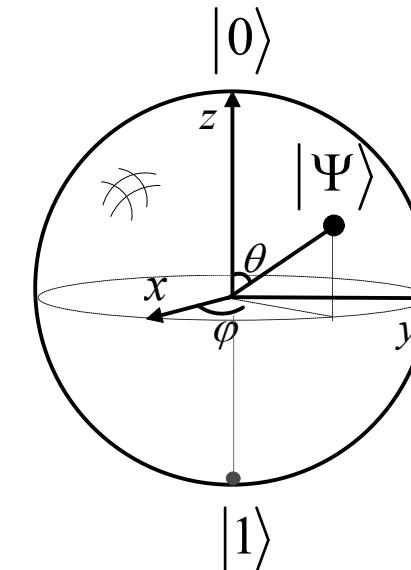
- ◆ 量子比特的几何图像：可表示为单位球面上的点。
- ◆ 由 $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$, $|\alpha|^2 + |\beta|^2 = 1$ ，可得

$$|\Psi\rangle = e^{i\gamma} \left(\cos \frac{\theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\theta}{2} |1\rangle \right).$$

- ◆ 略去整体相因子，得

$$|\Psi\rangle = \cos \frac{\theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\theta}{2} |1\rangle.$$

- ◆ 参数 θ 和 φ 定义了单位球面上的点。



- ◆ 问题：1个量子比特包含多少经典比特的信息？

Poincaré's Sphere

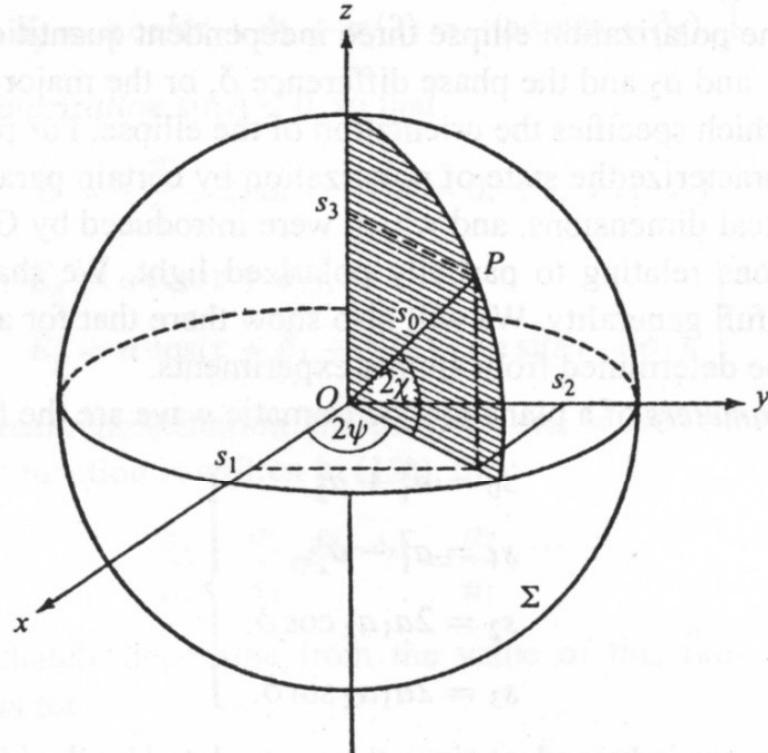


Fig. 1.8 Poincaré's representation of the state of polarization of a monochromatic wave. (The Poincaré sphere.)

Ordinary classical information, such as one finds in a book, can be copied at will and is not disturbed by reading it.

Quantum information is more like the information in a dream

- Trying to describe your dream changes your memory of it, so eventually you forget the dream and remember only what you've said about it.
- You cannot prove to someone else what you dreamed.
- You can lie about your dream and not get caught.

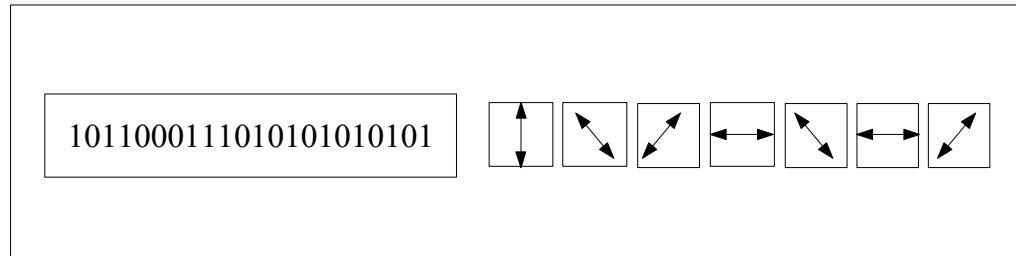


C. Bennett

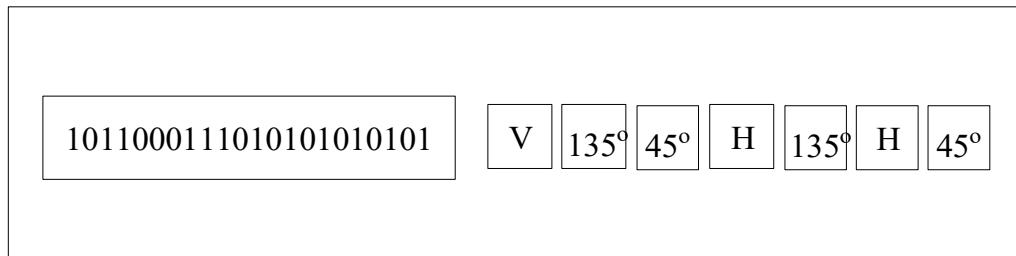
But unlike dreams, quantum information obeys well-known laws.

Quantum Money

○ S. J. Wiesner's quantum bank card or quantum money:

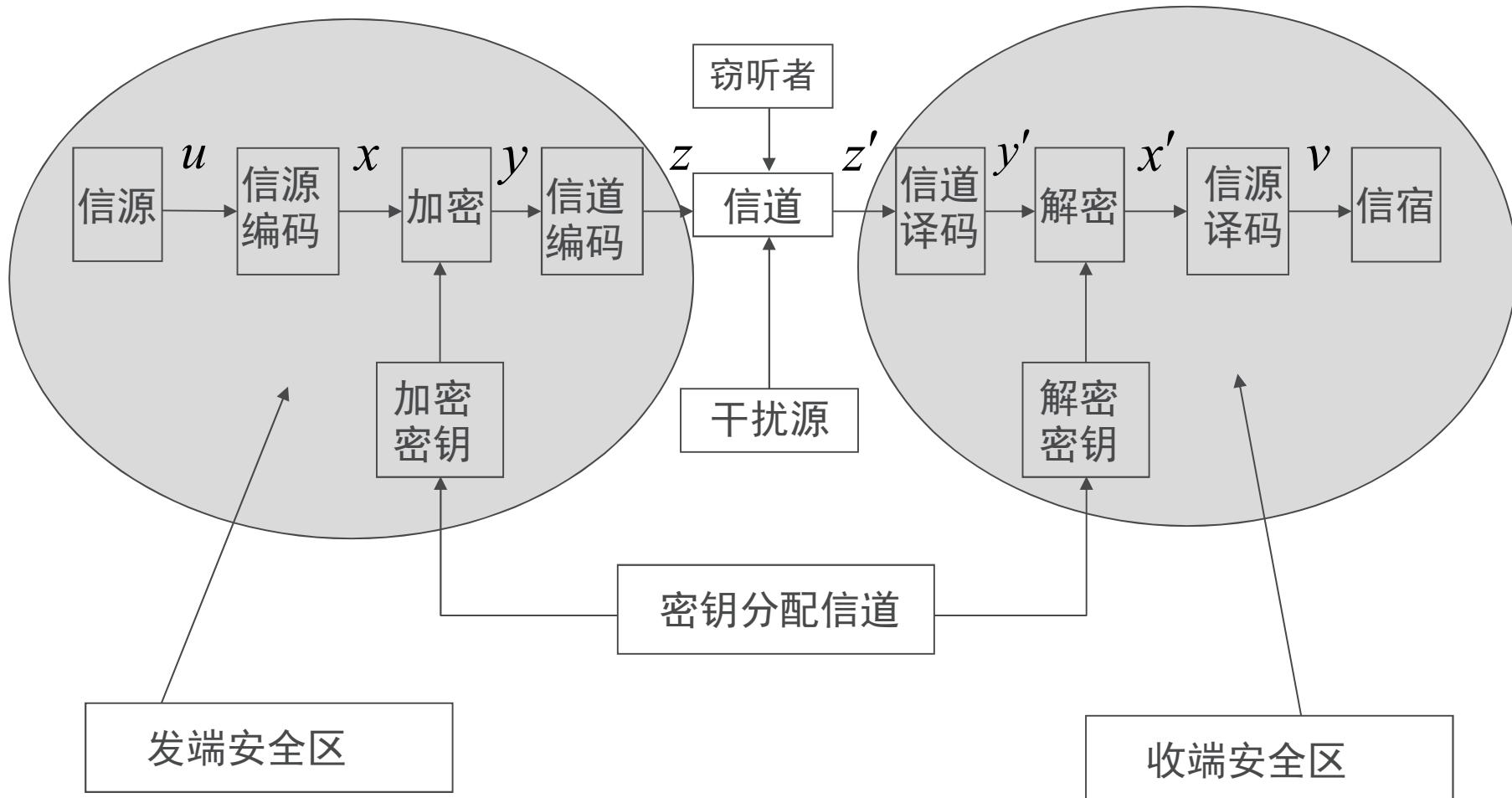


Money

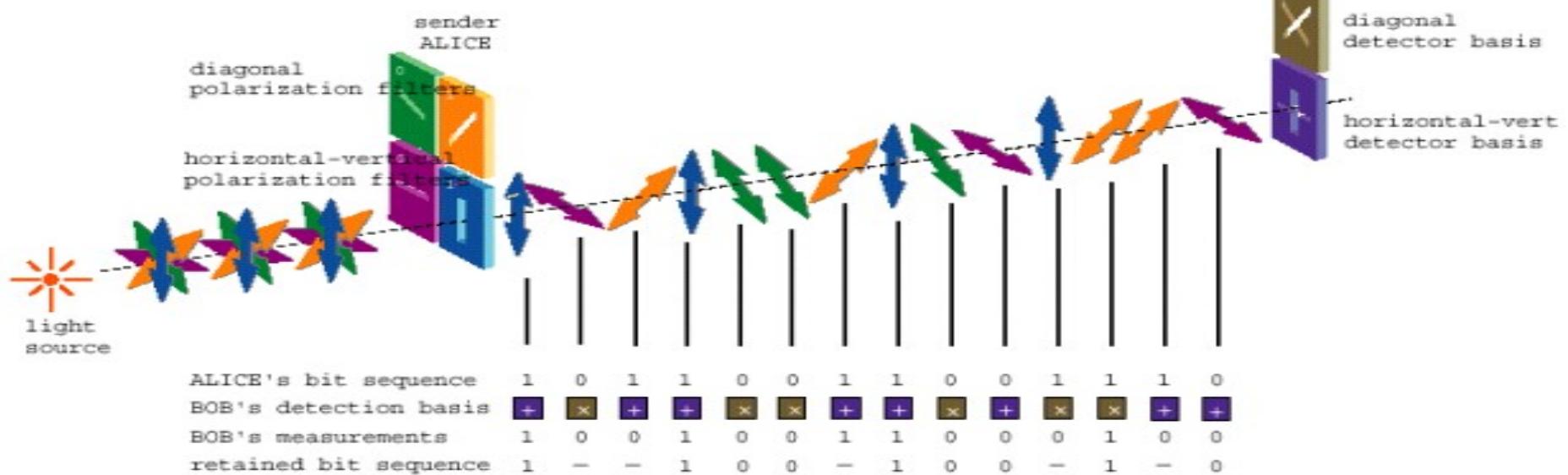


Bank record

保密通信系统的物理模型



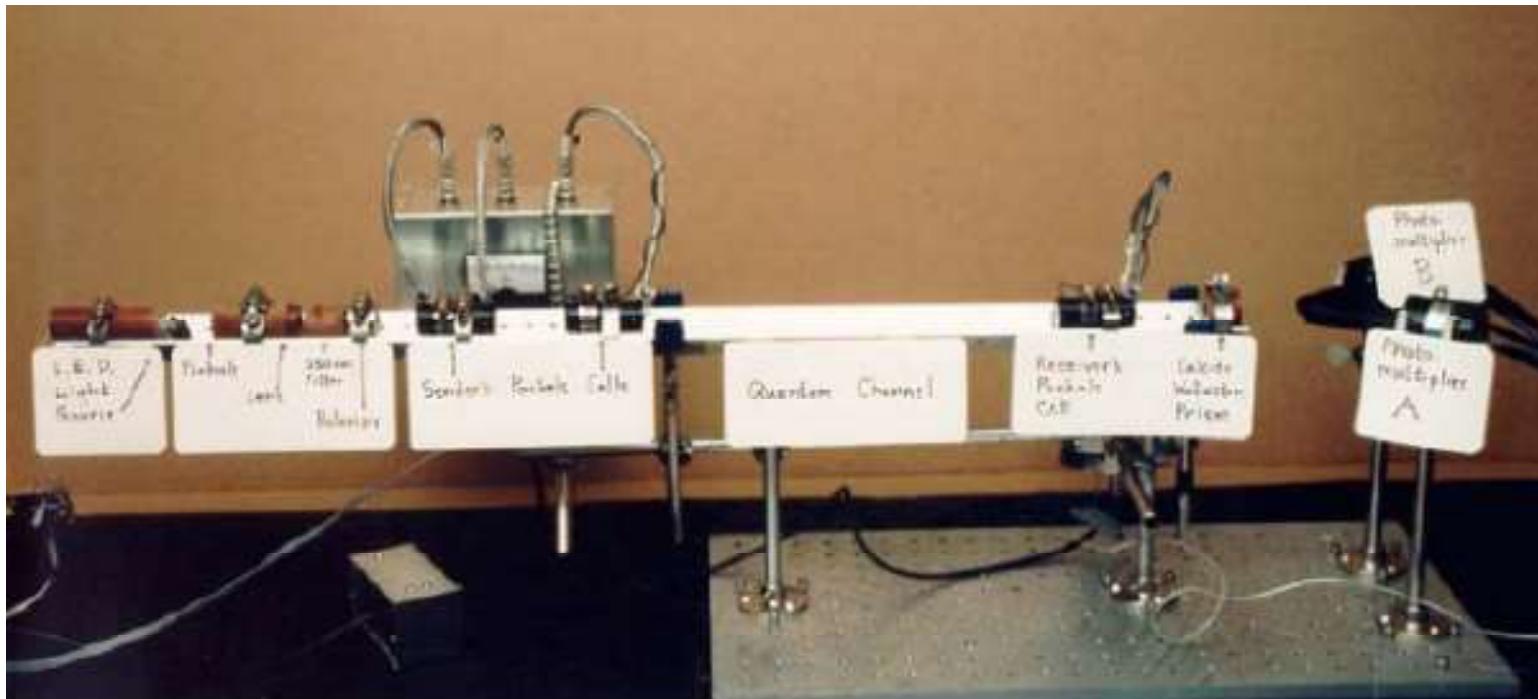
量子密码系统 (QKD, BB84)



QKD (BB84) 协议执行过程举例

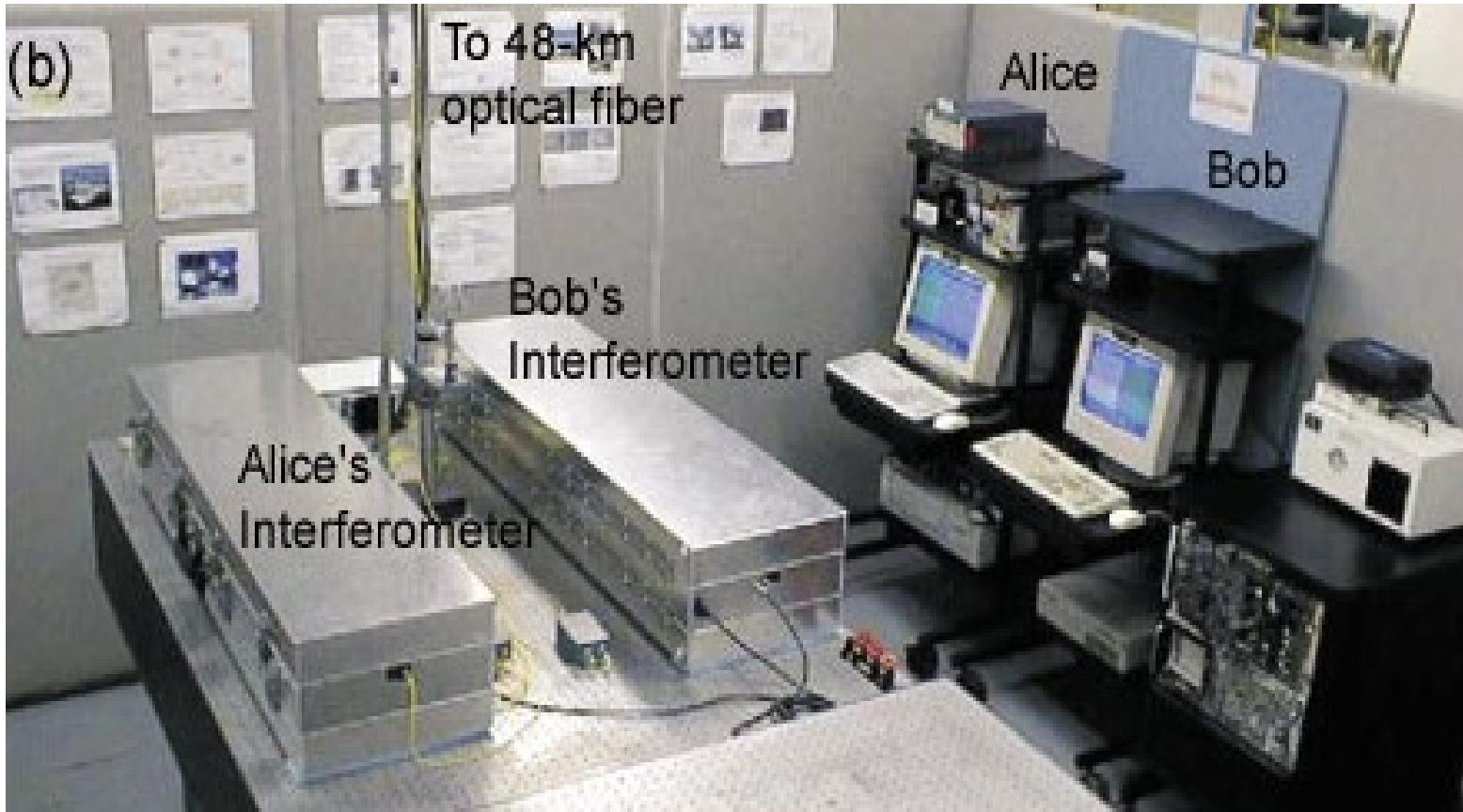
Key	1	0	1	0	1	0	1	0	1	0	1
A basis	\otimes	\oplus	\oplus	\otimes	\oplus	\otimes	\otimes	\otimes	\oplus	\otimes	\otimes
A bit value	0	1	0	1	1	0	1	0	0	0	0
A sends	$ 45^0\rangle$	$ H\rangle$	$ V\rangle$	$ 135^0\rangle$	$ H\rangle$	$ 45^0\rangle$	$ 135^0\rangle$	$ V\rangle$	$ 45^0\rangle$	$ 45^0\rangle$	$ V\rangle$
B basis	\otimes	\oplus	\otimes	\oplus	\oplus	\otimes	\otimes	\otimes	\oplus	\oplus	\oplus
B bit	0	1	0	0	1	0	1	1	0	1	0
Same basis?	y	y	n	n	y	y	y	n	n	n	y
A keeps	0	1			1	0	1				0
B keeps	0	1			1	0	1				0
Test Eve	y	n			y	n	n				n

BB84协议的第一个实验装置

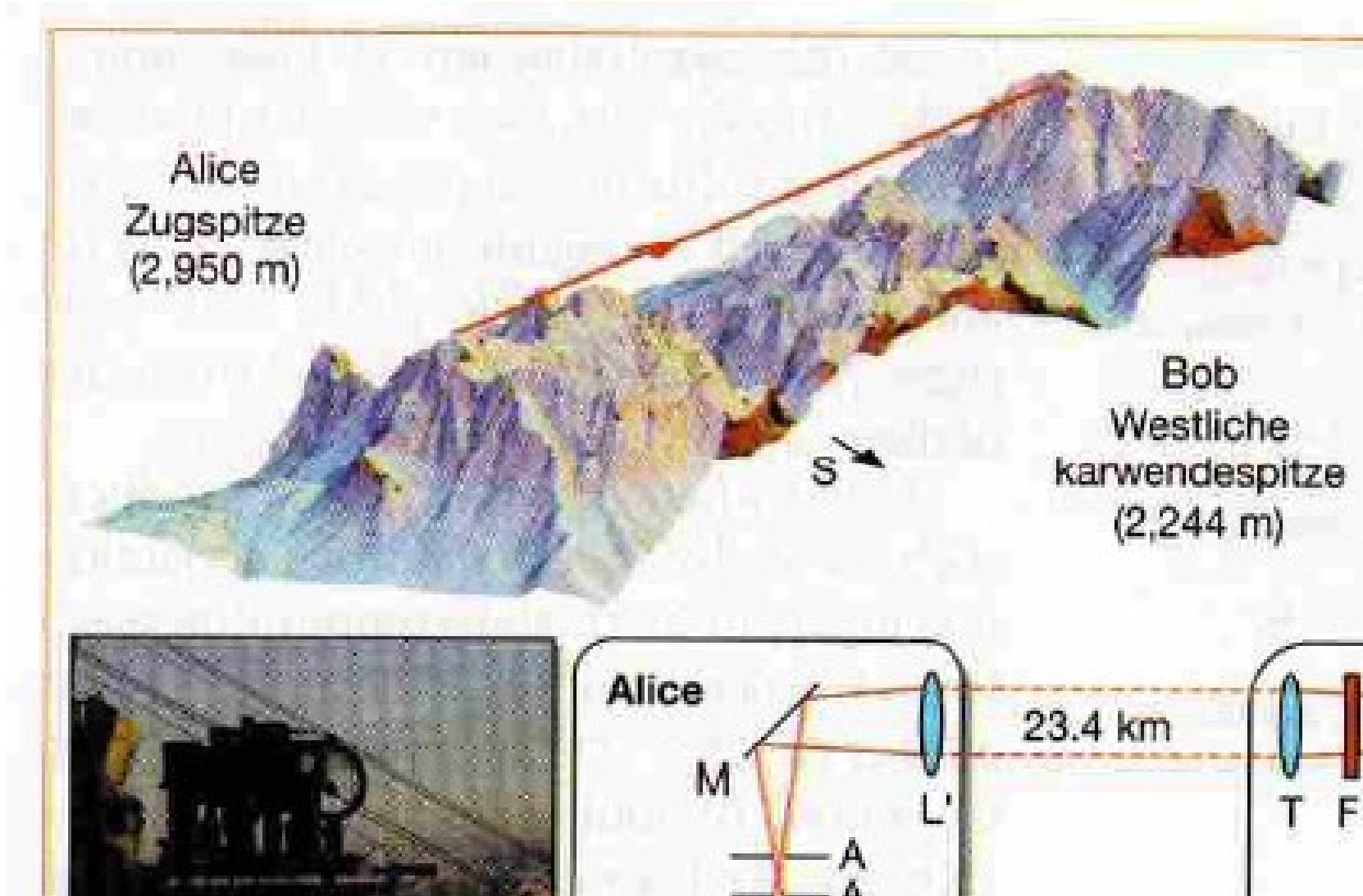


Original Quantum Cryptographic Apparatus built in 1989
transmitted information secretly over a distance of about 30 cm.

Los Alamos国家实验室QKD演示实验



自由空间量子密钥分配：23.4公里



自由空间量子通信：墨子号

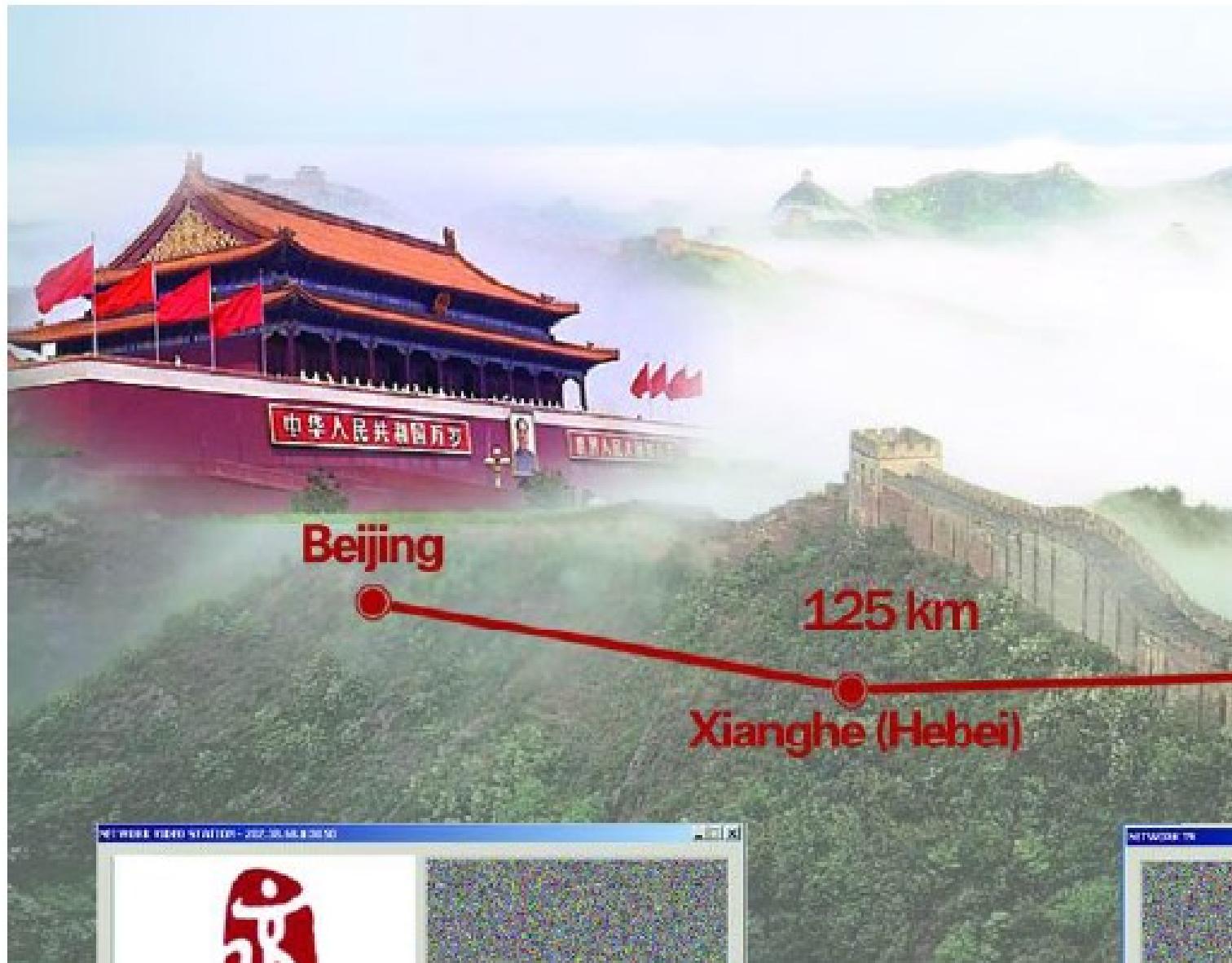


瑞士日内瓦大学的演示实验



即插即用，往返式设计，线路全长67公里，一段线路在日内瓦湖底。

中国科大光纤QKD实验：125公里

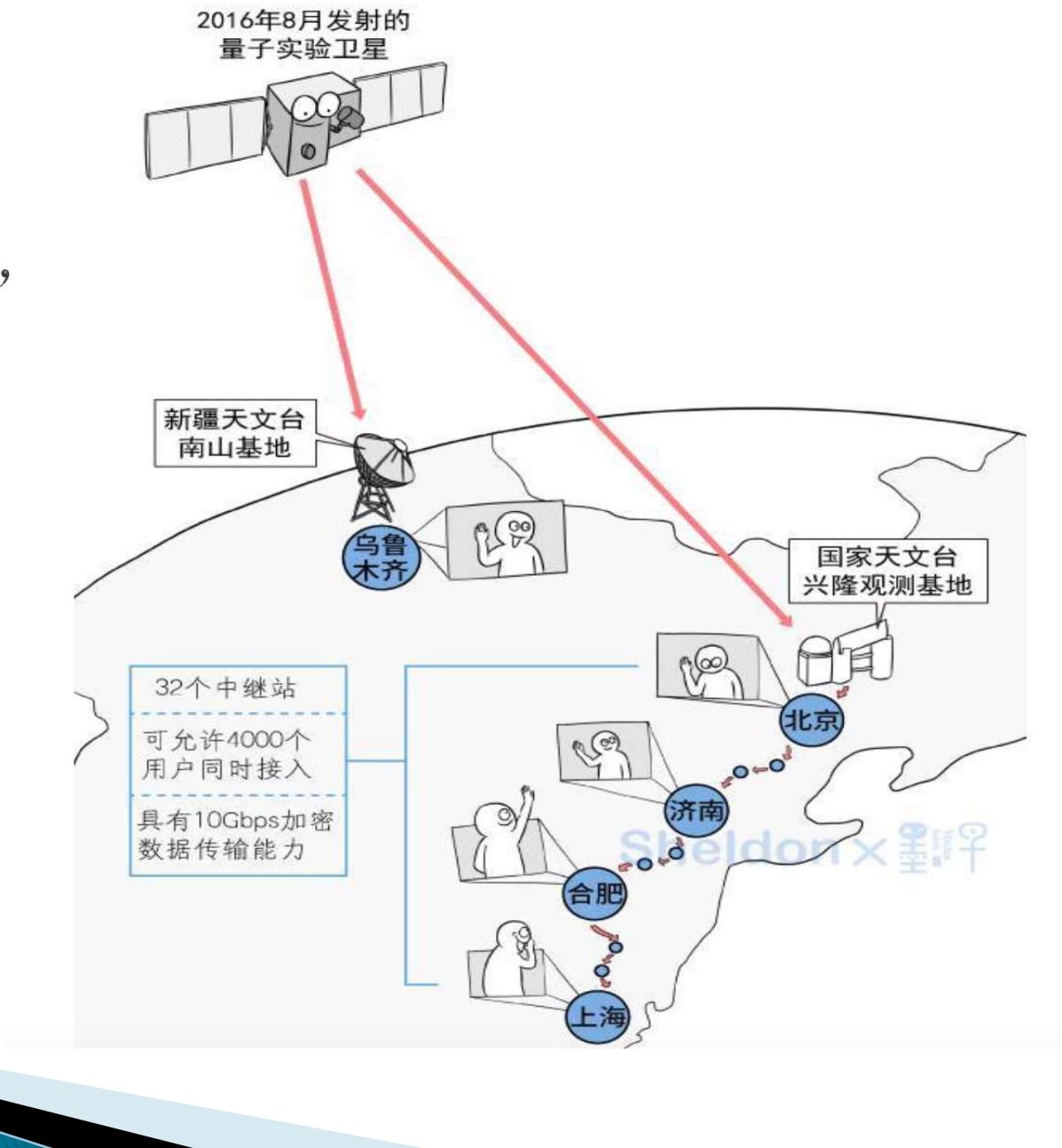


量子通信京沪干线系统

- 建成由32座中继站和31段光纤量子通信线路构成的主干量子通信线路
- 建成北京和上海的城域量子通信网络
- 实现金融、政务领域的多种应用示范，完成广电领域应用研究
- 量子通信系统的安全性规范研究和测评方法、工具研发



墨子号+京沪
干线共同实现
“天地一体化”
的量子保密通
信网络



QKD作为远程同步的随机数生成器

- ▶ QKD的BB84协议可以看作是一个独特的远程同步的（真）随机数生成器：
 1. 用于认证的密钥看作种子。
 2. 双信道，交互式。
 3. 单向变换（算子）：正交编码 → 共轭编码。
 4. 具有无条件安全性（有严格的证明）。
- ▶ 就经典密码学而言，远离的两个相同的PRBG由同一个种子控制，可以异地同步地生成相同的伪随机序列，但所生成序列的熵至多等于该种子的熵，绝对不会增大。
- ▶ 问题是：由BB84协议生成的（真）随机序列的熵会大于种子的熵。熵是从哪里来的？



广义的量子密码学

- ▶ 广义的“量子密码学”是指一切与量子计算、量子通信及其它量子信息技术有关的密码学结果。
- ▶ 量子信息密码学：建立在Hilbert空间的密码学，是涵盖量子和经典密码学的崭新的密码学理论。
- ▶ 因为经典信息是量子信息的一个子集，现代密码学和量子密码学可以统一在“量子信息密码学”框架下，也只能统一在这一理论框架下。



主动防御问题

- ▶ 量子计算机的物理局限性

对量子计算机内部结构和工作原理深入研究
(已建立量子计算机容许逻辑深度理论)

- ▶ 对于发展抗量子攻击的密码算法的意义

可以对抗未来构造的任何量子算法的攻击
(已给出抗量子计算机攻击的密钥交换协议)



建立Hilbert空间上的密码学

- ▶ 量子信息是基于自然界基本定律对经典信息的自然推广，是物理学和信息科学新的交叉点。
- ▶ 经过数十年的努力，量子信息论已经建立起来。
- ▶ 下一步：建立Hilbert空间上的密码学，新型密码学
- ▶ 它有两个已知的退化形式：
一个是现代密码学，一个是狭义的量子密码学。



量子密码研究目标

- 1、建立量子与经典密码学的共同理论基础，是密码学研究面临的一项基本任务。拟给出面向量子消息公钥密码学的理论框架，建立量子密码和经典密码共同的理论基础。
- 2、量子计算机强大的并行性使得量子算法在密码分析中可以发挥巨大的优势。我们将发展基于量子理论发展新的密码分析方法，此类结果将有助于设计抗量子攻击经典密码算法。
- 3、开展量子计算机破译密码能力理论极限的研究可为国家密码管理相关部门的相关决策提供科学依据。我们将遵循主动防御量子计算机攻击的新思路，深入研究量子计算机的内部结构，构造具有后量子安全性的密码算法。

为什么发展Hilbert空间上的密码学

基于量子形式知识理论：

一方面致力于量子信息系统安全性问题的解决

一方面为现代密码学的发展开辟新的道路



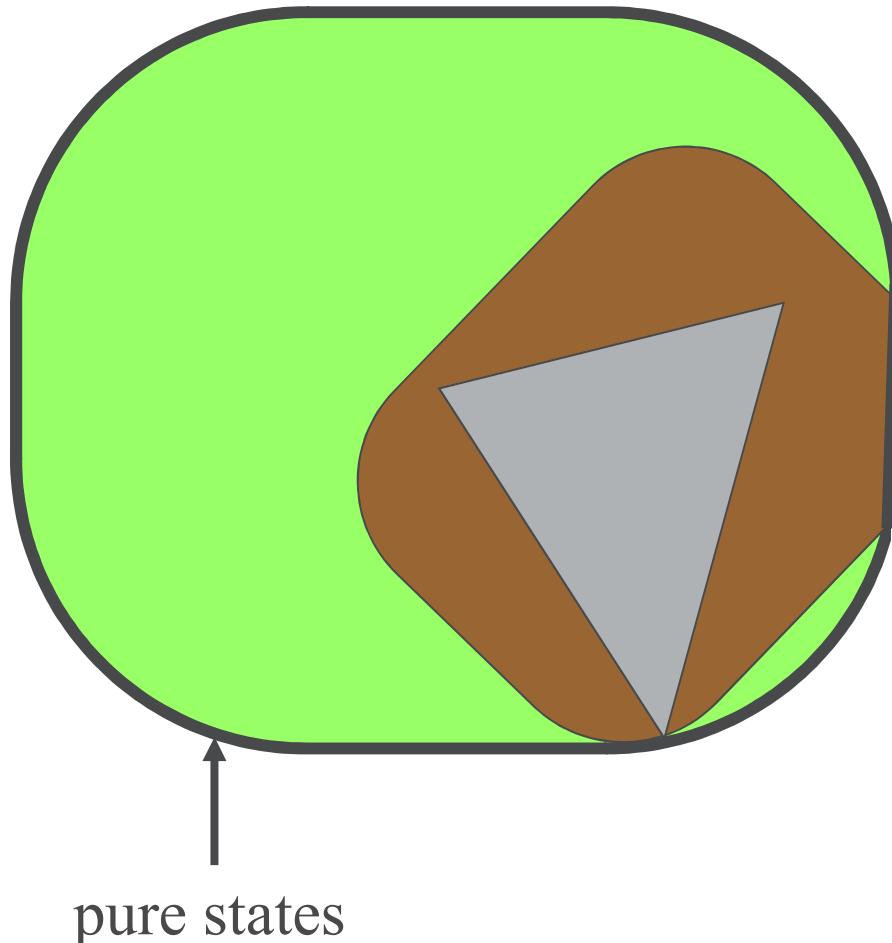
展望

- ▶ 在一个更大的空间上发展密码学有可能使密码学的结构更清晰、基础更牢固。
- ▶ 密码学的未来：智能密码学？
- ▶ **量子知识理论**有可能启发我们从一个新的角度认识生命，认识智能，认识我们自己。



Entanglement

(Comes from SM Fei)



No Classical Counterpart

All states

unentangled states:
mixtures of products

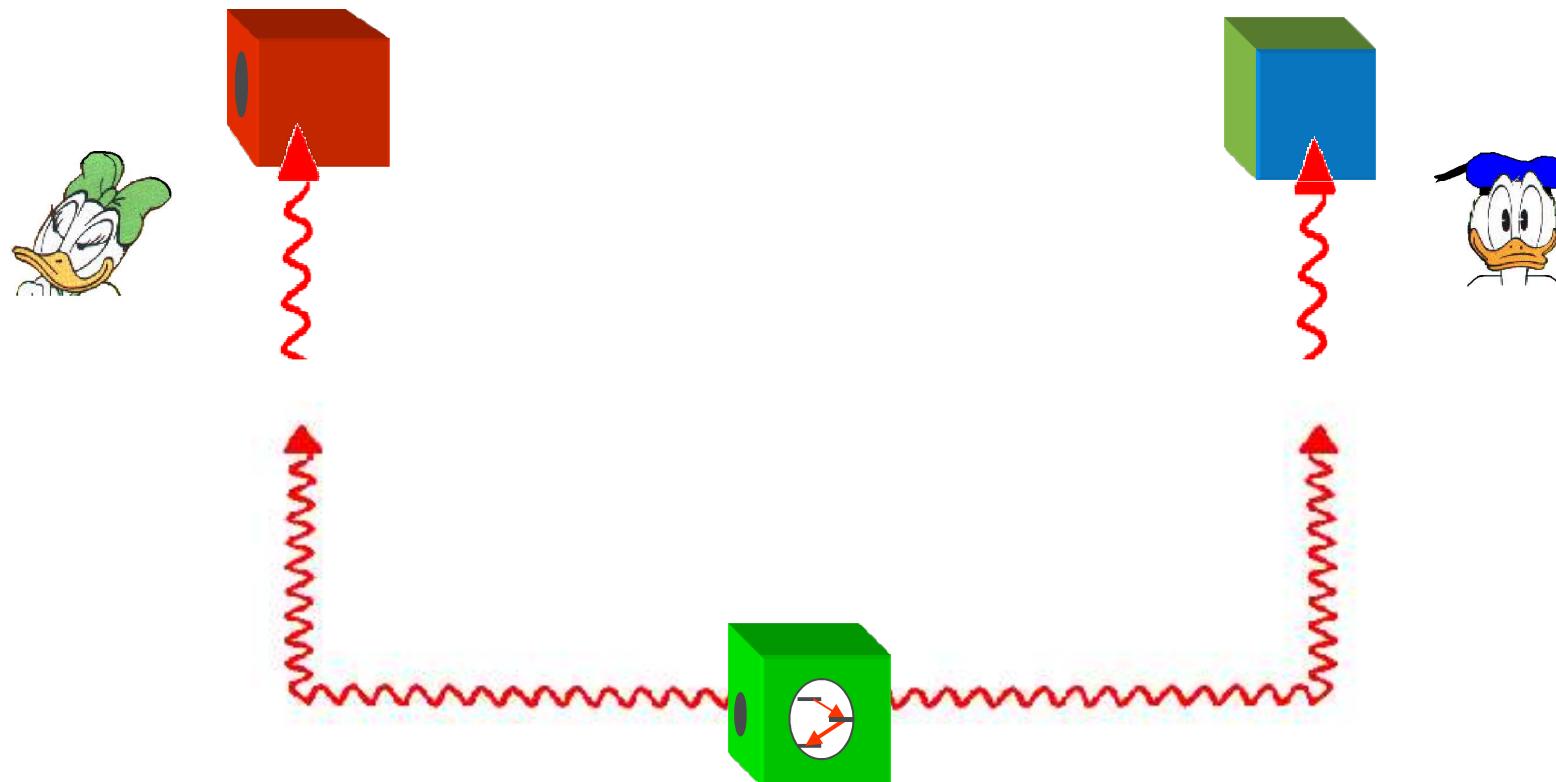
bound entangled states:
not distillable

Much of the **geometry**
remains to be clarified!
Many **Quantitative Notions**
to be made computable

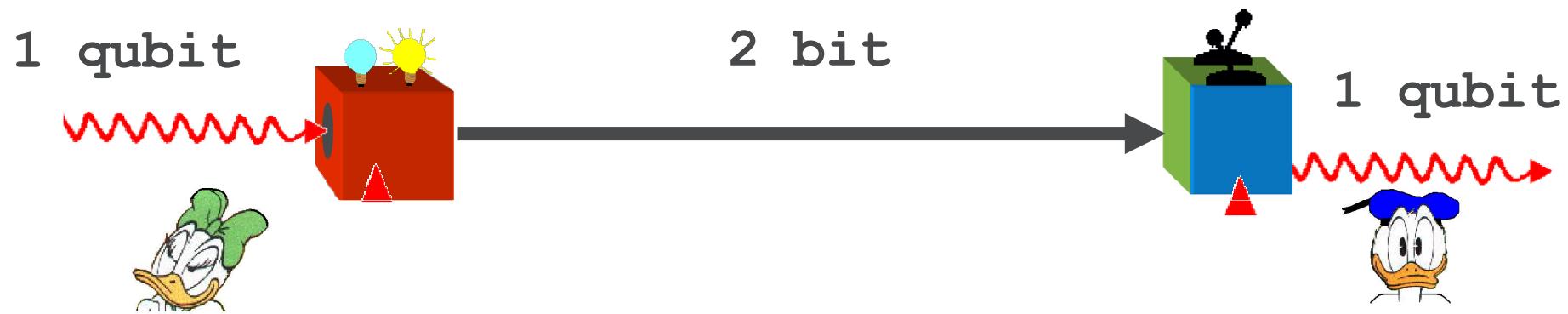
Alice和Bob的故事

- Alice刚刚办理了银行信用卡，密码是一组量子态。
- 这张卡是隐藏起来的Bob近期生活费的唯一来源。
- 现在Alice 只能通过告示板或广播单向地与Bob联系，她能把这个密码发给Bob吗？

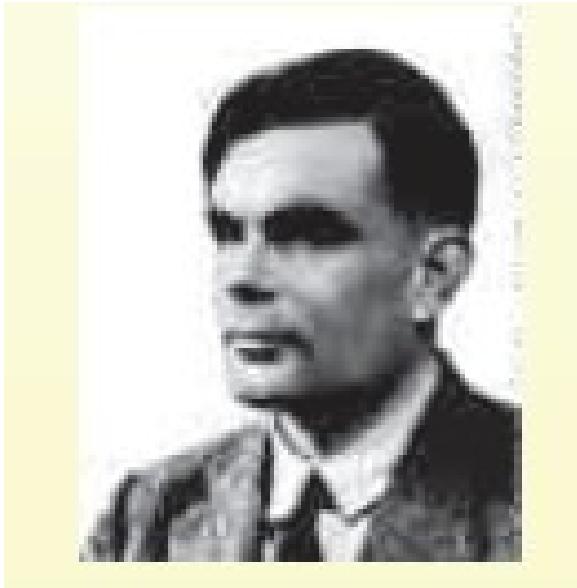
Entanglement enhanced
Teleportation



Entanglement enhanced
Teleportation



A. M. Turing

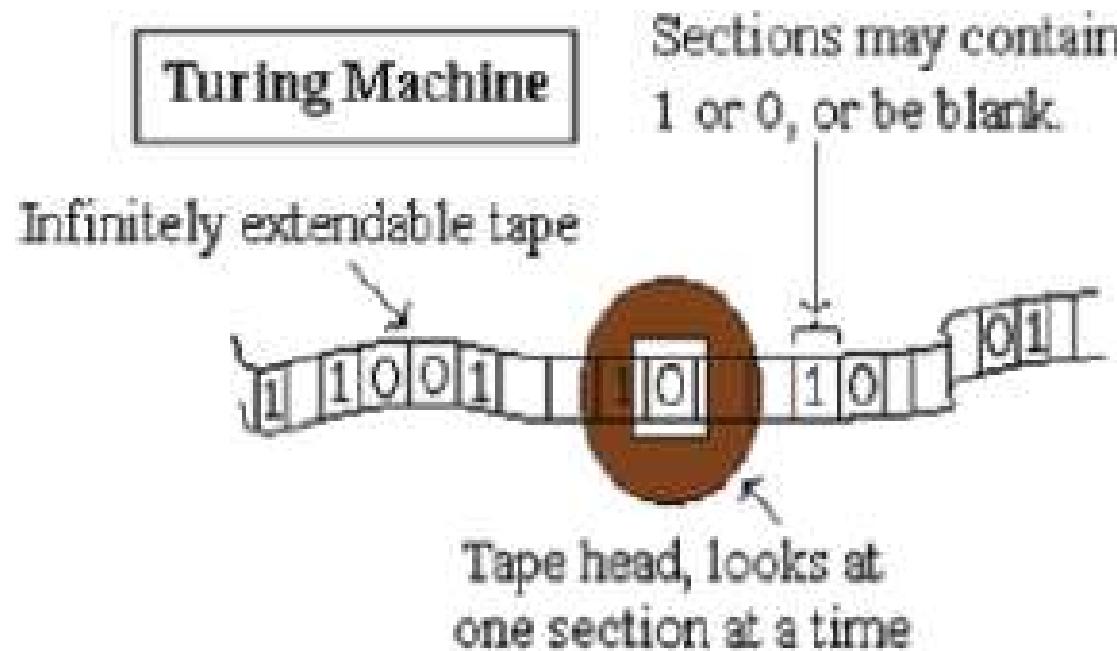


Alan Turing
(1912~1954)

A. M. Turing生于1912年，是英国一个上等家庭的次子。他幼年早熟，在剑桥大学读书时有过突出的贡献，毕业不久发表关于可计算性的革命性著作。二次世界大战中Turing参加破译德国密码一事直到近来才为众所周知。他的著作里有对数理逻辑和其他数学分支的重要贡献。他是关于计算机智力的可能性最早的论述者之一，他的著作至今仍被看作是重要的。1954年6月他因氰化物中毒而死，官方判定为自杀。

Turing机器

Turing 给出了通用Turing机的构造，为当代的计算机科学奠定了基础。



Church-Turing论题

○ Church论题：

算法可计算函数类=递归函数类

○ Turing论题：

算法可计算函数类=Turing机可计算函数类

定理 (Turing) : **递归函数类= Turing机可计算函数类**

因而Church 论题和 Turing 论题是等价的

合称为Church-Turing论题

Church-Turing论题

- Church-Turing论题是可计算理论的基础。从经典理论的观点看，机器与人有相同的计算数论函数的能力是Church-Turing论题的实质。
- 目前认为，量子计算理论没有对Church-Turing论题提出质疑，因为量子可计算与经典可计算的函数类是相同的。

量子计算的最初思想



Richard
Feynman

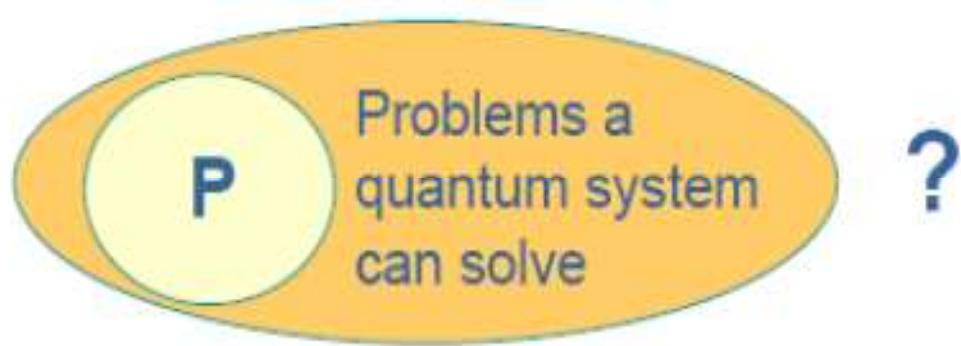
- Benniof: 提出了最早的量子图灵机。
(1970年代末)
- 1982年，Richard Feynman提出采用基于量子力学原理的计算装置求解量子系统有关问题可能会在本质上优于经典计算机。Feynman的观点引导了后来量子模拟的研究。
- David Deutsch: 提出了最早的量子算法。

量子Turing机

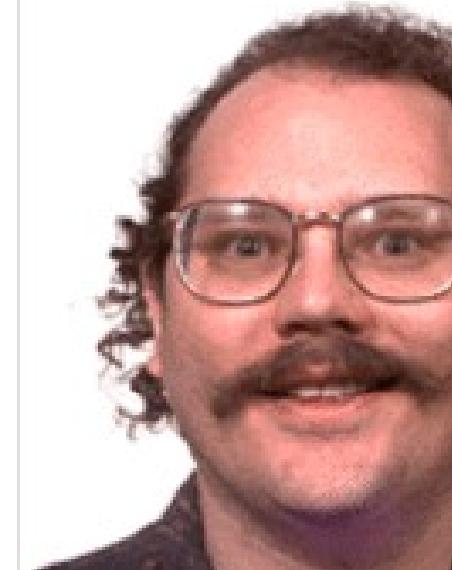


- 1985年，David Deutsch提出是否可以用物理定律导出更强的Church-Turing论题这一问题，并试图定义一种能有效模拟任意物理系统的计算装置，从而将Church-Turing论题置于当代物理学这一科学基础之上。Deutsch所提出的即是基于量子力学原理的Turing机，即量子Turing机。
- 1993-1997，量子图灵机理论有较大发展。

量子算法



量子计算机可以有效求解任何P类问题，但已知其不能有效求解PSPACE类以外的问题。量子计算机可有效求解的问题类在P类和PSPACE类之间的什么位置还不清楚。该问题的解决很可能导致PSPACE类是否等于P类这个计算机科学重要问题的解决。



Peter Shor

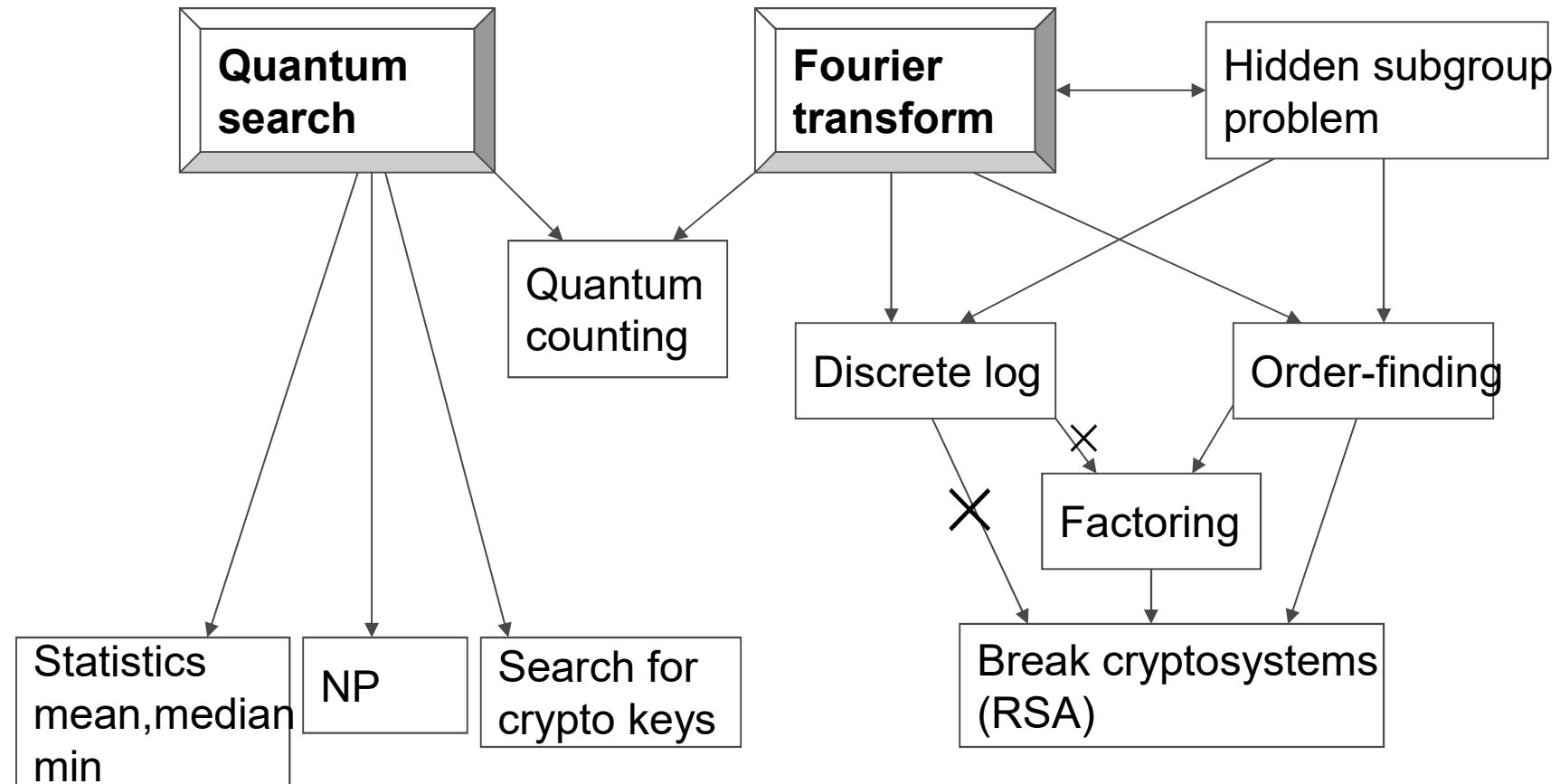
量子算法

- Deutsch给出了一个简单的例子，说明量子计算机确实在求解某些问题的能力上超过经典计算机。
- 1994年，Peter Shor 给出了大整数分解和求解有限域上的离散对数的有效量子算法。
- 1995年，Lov Grover给出了无序数据库搜索的快速量子算法。
- 构造新的量子算法是未来的挑战。

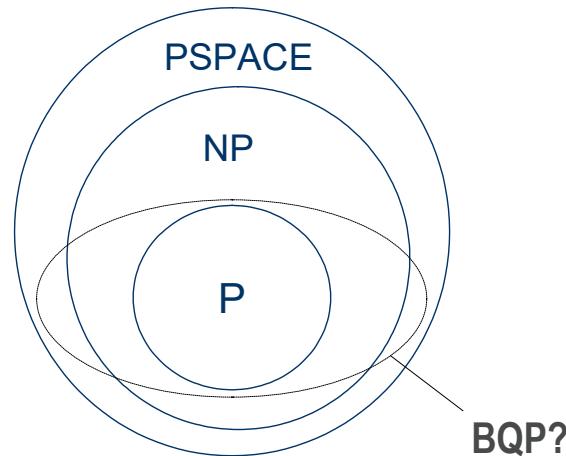


Lov Grover
Bell Labs

量子算法 (教材上的图, 有错误)



经典和量子复杂性类的关系



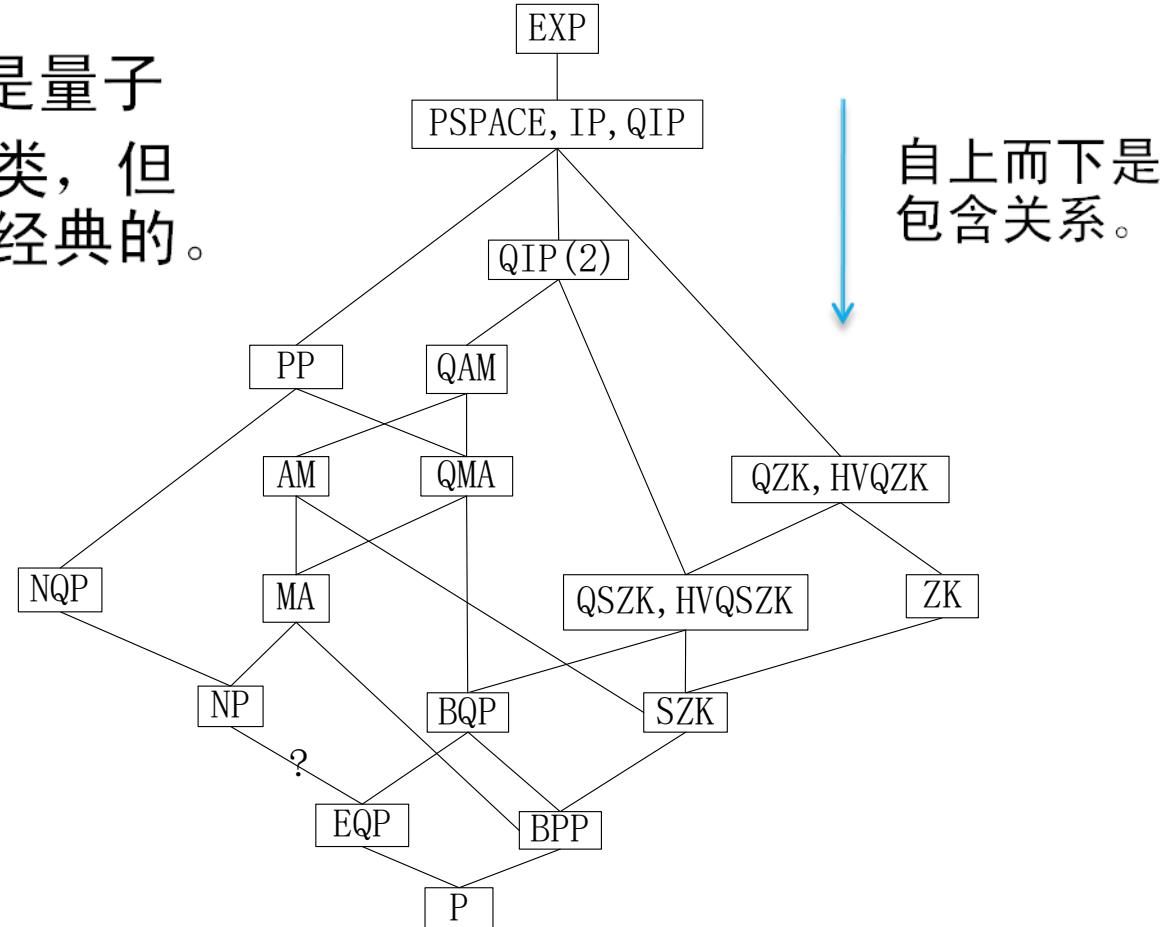
量子计算机可以有效求解任何P类问题，但已知其不能有效求解PSPACE类以外的问题。

量子计算机可有效求解的问题类在P类和PSPACE类之间的什么位置还不清楚。

该问题的解决很可能导致PSPACE类是否等于P类这个计算机科学重要问题的解决。

经典和量子复杂性类的关系 (2)

名称含Q的是量子计算复杂性类，但问题仍然是经典的。



量子算法设计的本质

- 可以认为量子并行计算与经典随机化方法很相近。差别在于：在经典概率计算机上，不同的概率分支总是相互排斥的，而在量子计算机上，不同的叠加分量却可能通过干涉而给出函数的某种全局性质。
- 许多量子算法设计的本质在于：精心选择函数和最终变换，以便有效地确定有关函数的有用的全局信息。这种全局信息在经典计算机上是不能有效得到的。

- 一般地，存储具有 n 个不同元素的量子系统的状态需要大概 c^n 比特经典计算机的内存，而量子计算机可以用 kn 量子比特进行模拟。
- 不过，即使量子计算机可以比经典计算机远为有效地模拟许多量子系统，这并不意味着快速模拟能得到关于量子系统的期望信息。

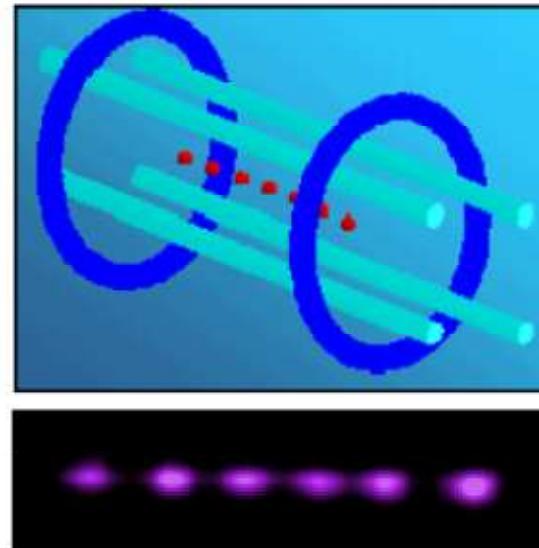
量子仿真 (2)

测量时，一个 kn 量子比特的模拟将坍缩为一个确定状态，只给出 kn 比特的信息，在波函数中的 c^n 比特的隐含信息不能全部访问。

因此，量子仿真的一个关键步骤是，研究有效抽取期望答案的系统化方法，但如何去做还不完全清楚。

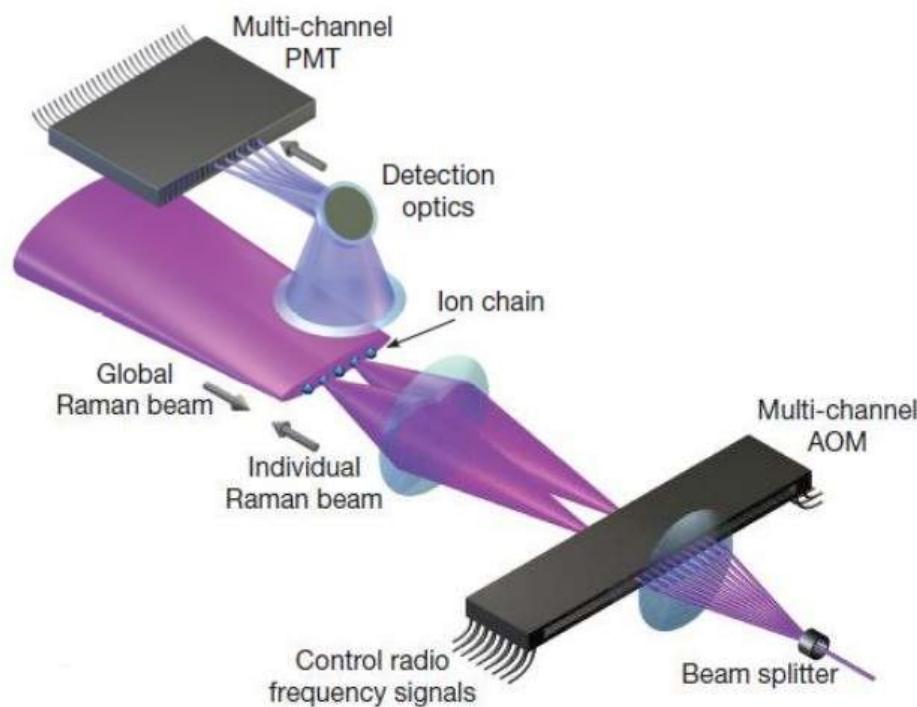
Ion traps

- Qubit: internal electronic state of atomic ion in a trap (ground and excited)
- Coupling: use quantised vibrational mode along linear axis (phonons)
- Single qubit gates: using laser



Cirac and Zoller, *Phys. Rev. Lett.* (1995)

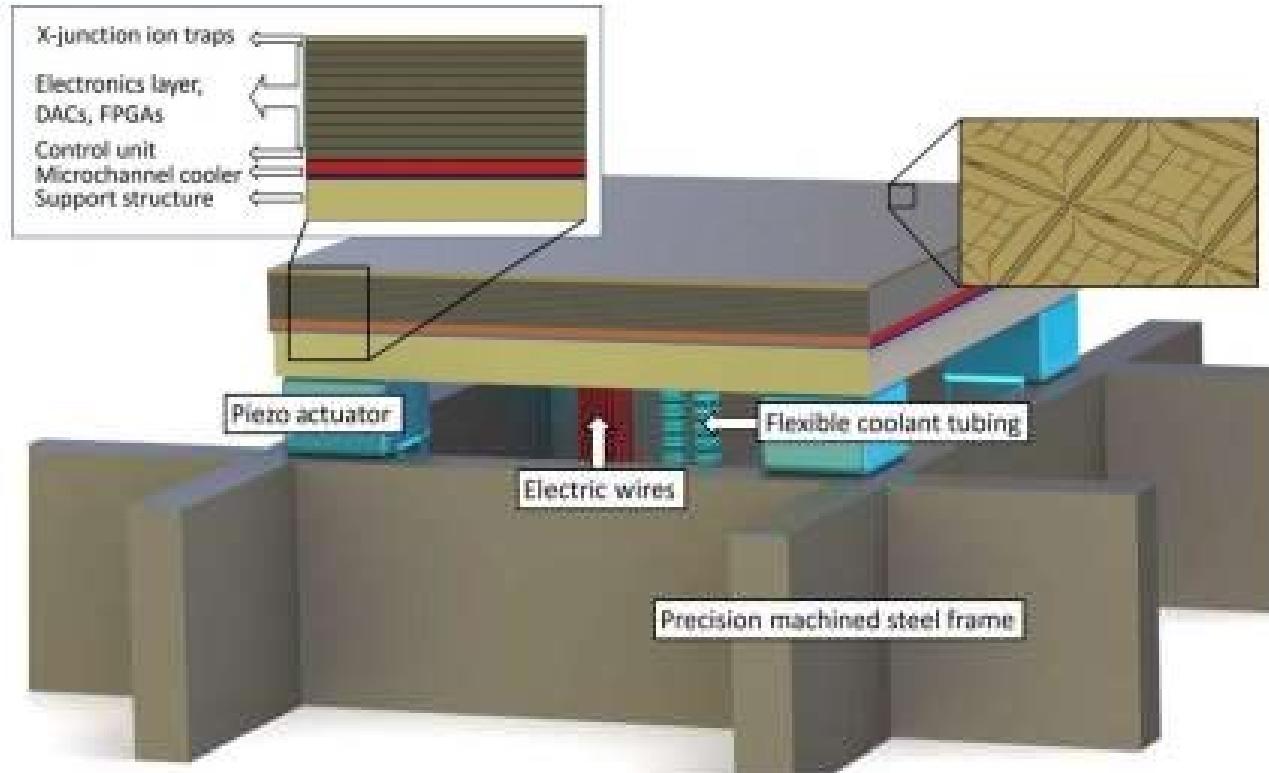
冷离子阱方案



图片展示了该计算机硬件结构，图片中间的离子量子比特排成一列，离子荧光发射被收集并映射至多道光电倍增管以进行测量，相向传输的拉曼光束完成门操作。衍射分光镜用于产生拉曼光束，以实现对特定离子的门操作。

2016年8月，马里兰大学牵头研制成功5个量子比特的可编程离子阱量子计算机，有关成果发表在Nature杂志上。

冷离子阱方案

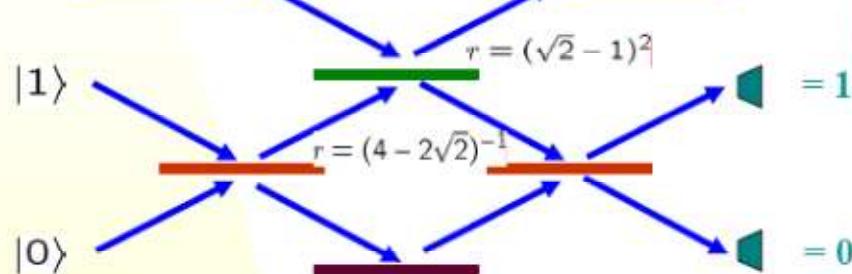


2017年，研究人员给出一个基于离子阱的，模块化的可扩展量子计算机设计，他们运用微波驱动量子门，利用阱间离子传送技术实现可扩展性。

Linear optics

- Qubit: polarisation of a single photon
- Coupling: via measurement
- Single-qubit gates: polarisation rotation

$$|\psi\rangle = \psi_0|0\rangle + \psi_1|1\rangle + \psi_2|2\rangle \quad |\psi'\rangle = \psi_0|0\rangle + \psi_1|1\rangle - \psi_2|2\rangle$$

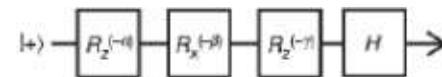
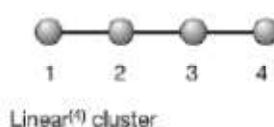


Knill, Laflamme,
Milburn, *Nature*
(2001)

The latest:

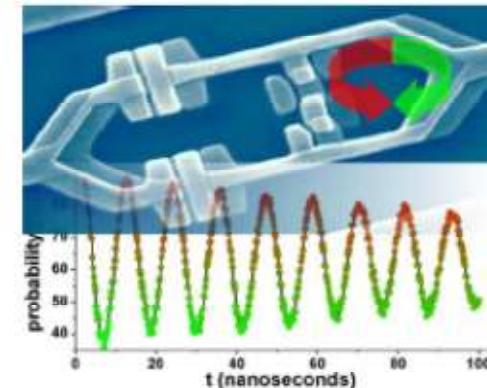
Zeilinger group – UVienna

“One-way” quantum
computing with four qubits



Superconducting Josephson junctions

- Qubit:
 - a) Magnetic flux trapped in loop
 - b) Cooper pair charge on metal box
 - c) Charge-phase
- Coupling: capacitive/inductive
- Single-qubit gates: flux bias, charge on gate, current through junction

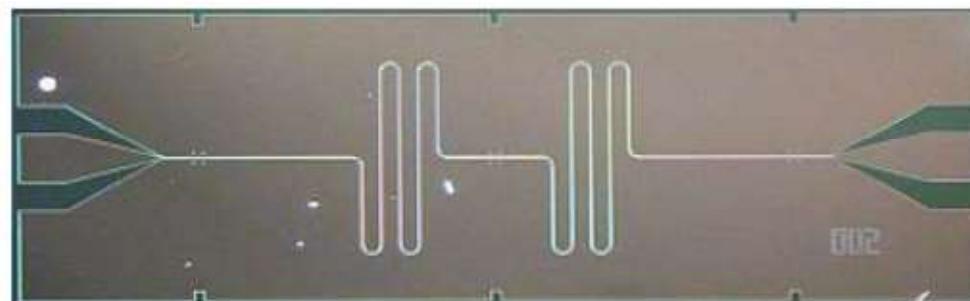


Nakamura, Pashkin,
Tsai, *Nature* (1999)

The latest:

Schoelkopf group – Yale

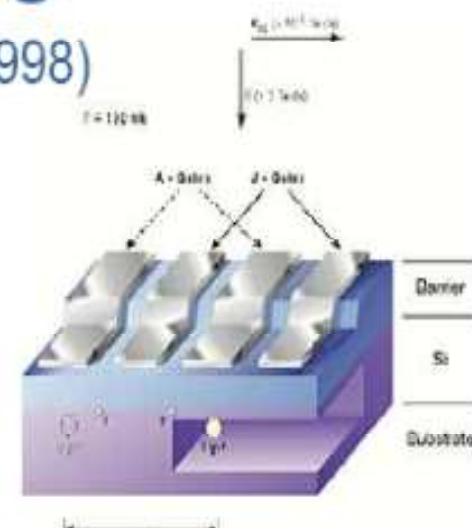
Coherent coupling of a
single photon to a
superconducting qubit
(Cooper pair box)



Silicon quantum computing

- Qubit:
 - ◆ Nuclear spin of single P donor
 - ◆ Electron spin of single donor
- Coupling: gate-controlled electron-electron interaction
- Single-qubit gates: NMR pulse; gate bias in

Kane, *Nature* (1998)



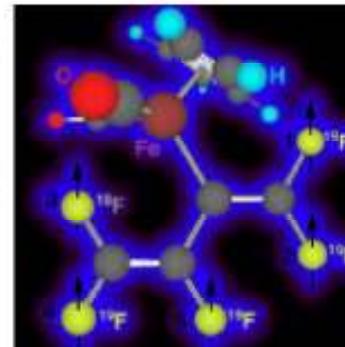
D-Wave2000Q



2017年初，D-Wave公司宣布推出具有2000个量子比特的D-Wave2000Q，可用于解决有关优化问题（不能运行Shor算法）

Nuclear magnetic resonance (NMR)

- Qubit: nuclear spins of atoms in a designer molecule
- Coupling and single-qubit gates: RF pulses tuned to NMR frequency



Gershenfeld and Chuang, *Science* (1997)

DiVincenzo criteria



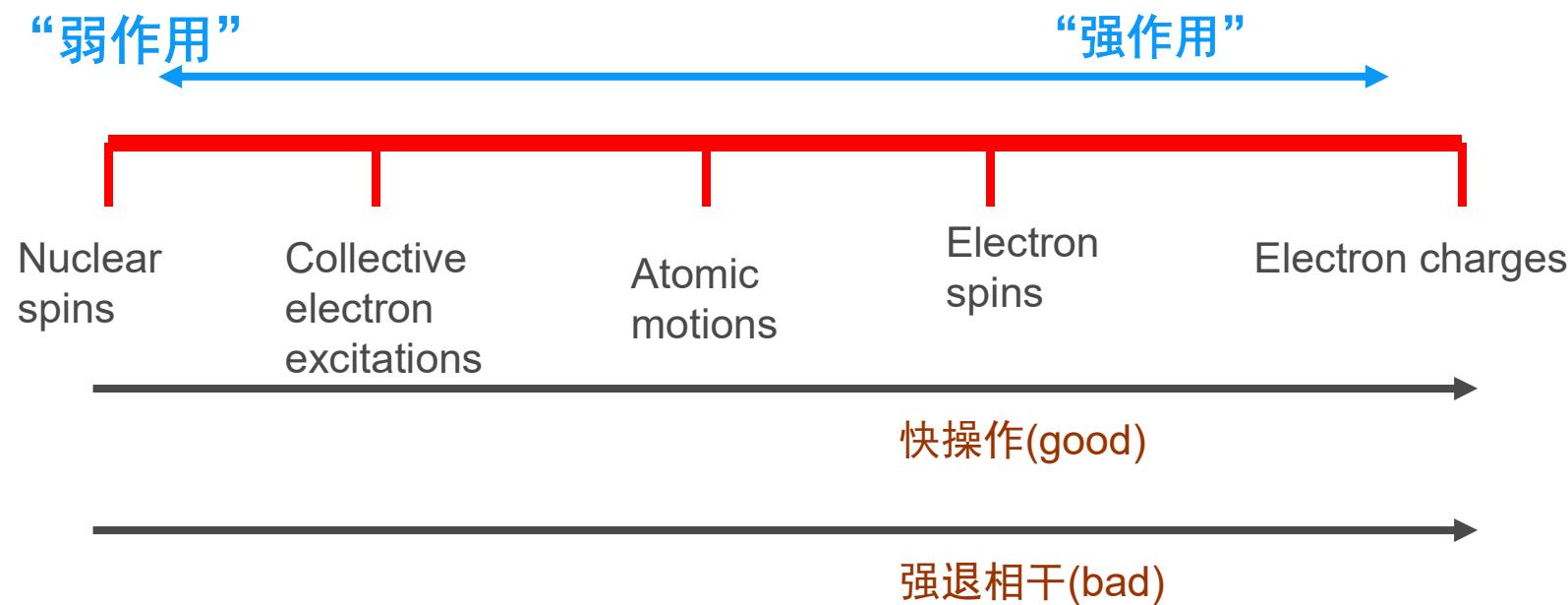
David DiVincenzo (IBM) – requirements for a quantum computer:

1. The machine must have a scalable collection of bits

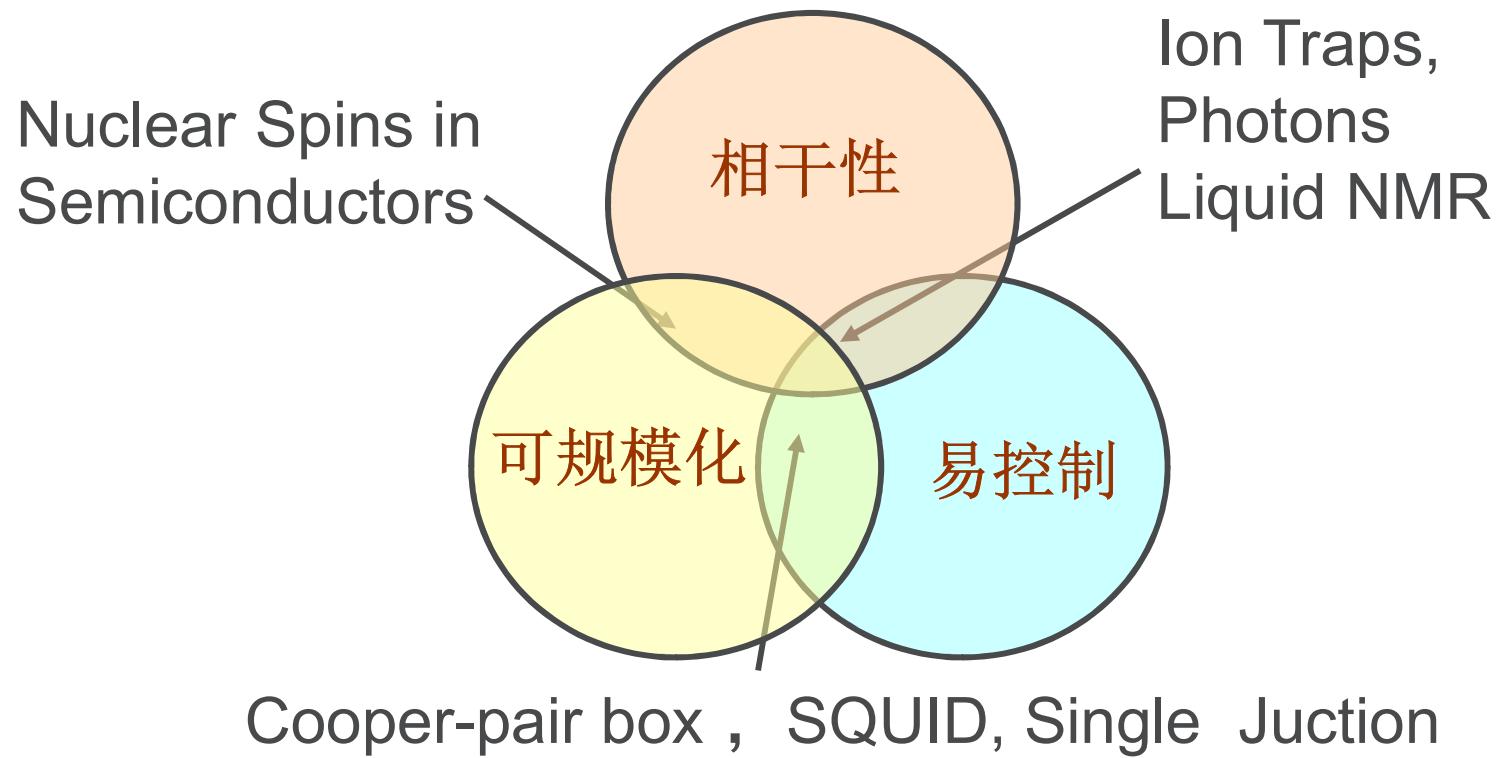
Each bit must be individually addressable, and it must be possible to scale up to a large number of bits
2. It must be possible to initiate all of the bits to zero
3. The error rate should be sufficiently low

Decoherence times must be much longer than the gate operation times
4. It must be possible to perform elementary logical operations between pairs of bits
5. Reliable readout of the final result must be possible

量子比特操作的时间标度

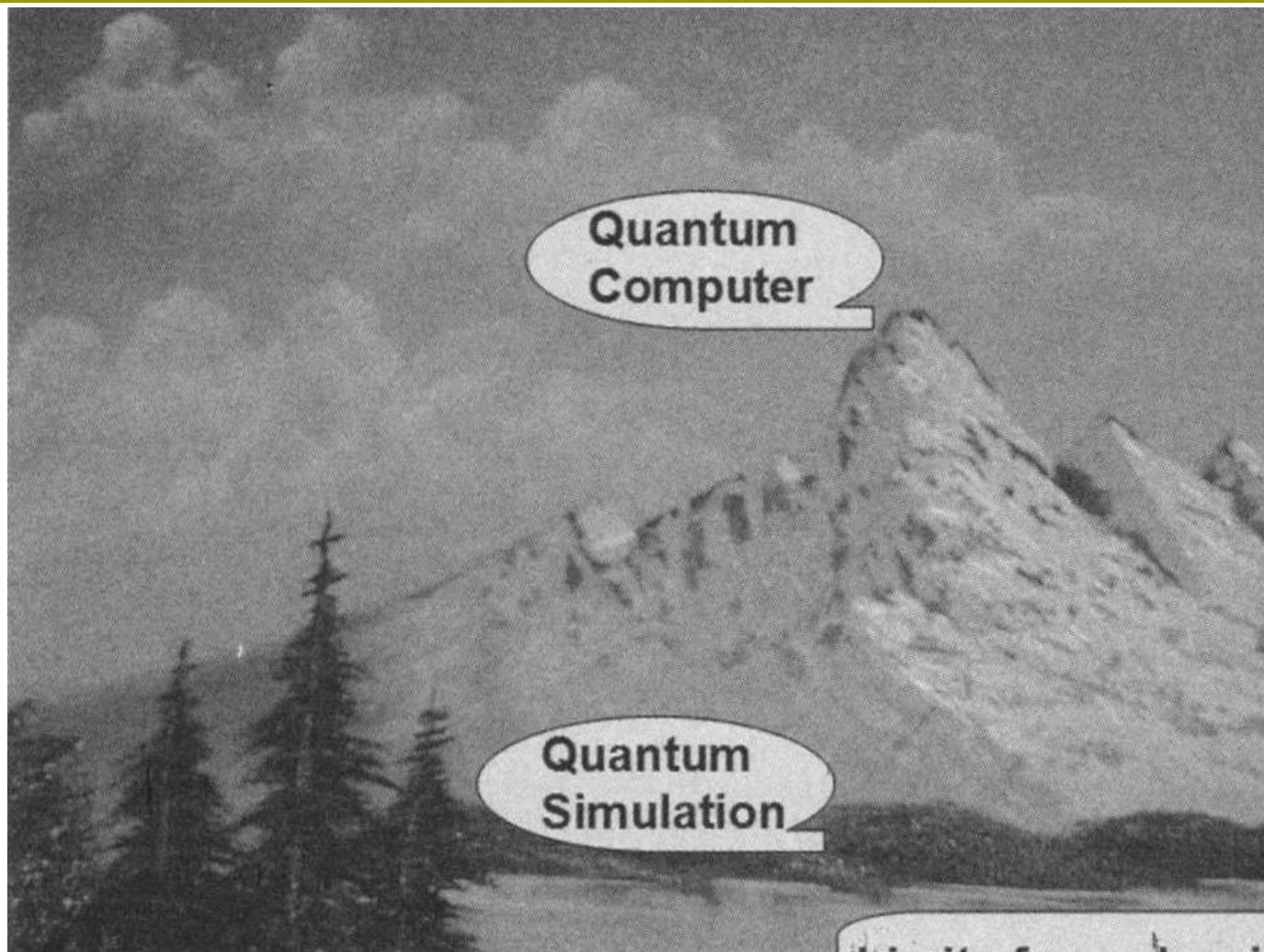


各类量子计算机物理实现方案比较



约瑟芬森结： 2002-2003年JJ Q-比特的相干性得到极大改进

量子计算



信息处理：经典vs量子

Property	Classical	Quantum
State—representation	string of bits $x \in \{0,1\}^n$	string of qubits $ \psi\rangle = \sum_x c_x x\rangle$
Computation primitives	deterministic or stochastic one-and two-bit operations	one-and two-qubit unitary transformations
Fault-tolerant computation	By classical fault-tolerant gate arrays	By quantum fault-tolerant gate arrays
Quantum computational speedups		Factoring: exponential speedup Search: quadratic speedup Black box iteration: no speedup

信息处理：经典vs量子 (2)

Communication primitives	Transmitting a classical bit	Transmitting a classical bit / a qubit Sharing an EPR pair
Source Entropy	$H = -\sum p(x) \log p(x)$	$S = -\text{Tr}(\rho \log \rho)$
Noiseless coding techniques	Classical data compression	Quantum data compression Entanglement concentration
Error-correction Techniques	Error-correcting codes	Quantum error-correcting codes Entanglement distillation
Noisy Channel Capacities	Classical capacity C_1 equals maximum mutual information through a single channel use	Classical capacity $C \geq C_1$; Unassisted quantum capacity $Q \leq C$; classically assisted quantum capacity $Q_2 \geq Q$
Entang.-Assisted Communication		Superdense Coding Quantum Teleportation
Communication complexity	Bit communication cost of distributed computation	Qubit cost, or entanglement-assisted bit cost , can be less

信息处理：经典vs量子 (3)

Secret crypto key agreement	Insecure against unlimited computing power , or if P=NP	Secure against general quantum attack and unlimited computing
2-Party Bit commitment		Insecure against attack by a quantum computer
Digital signatures		No known quantum realization

[第1次课] 绪论：量子信息简介

Q&A