

量子计算与量子通信

龙桂鲁

清华大学物理系, 北京100084

量子信息与测量重点实验室

gllong@tsinghua.edu.cn

2008年11月13日

计算机是我们今日生活所离不开的

电子教案

灯-电力-电网控制

计算机-计算器-电视-汽车-空调

几乎所有的电器

计算机带来的技术革命，改变了我们的社会、
我们的世界

计算机最早是为破译密码

- 英国最先制造出巨人计算机，资料至今保密
- 美国制造出二台计算机ENIAC

内容提要

- 量子力学
- 量子计算机
- Shor算法
- Grover算法
- 物理实现

计算机的发展迅速，远远超出先驱们的估计

- **Where a calculator on the Eniac is equipped with 18000 vacuum tubes and weighs 30 tons, computers in the future may have only 1000 tubes and weigh only 1 1/2 tons**
- **Popular Mechanics, March 1949**

量子力学很难理解

- **Anyone who is not shocked by quantum theory has not understood it.**

- **Niels Bohr**

- **I think I can safely say that no body understands quantum mechanics.**

- **Richard Feynman**

[Quantum]theory has, indeed, two powerful bodies of fact in its favour, and only one thing against it. First, in its favour are all the marvellous agreements that the theory has had with every experimental result to date. Second, and to me almost as important, it is a theory of astonishing and profound mathematical beauty. **The one thing that can be said against it is that it makes absolutely no sense!**

Roger Penrose

量子力学描写微观粒子的运动

- 量子力学的态
- 量子力学的力学量
- 量子力学的测量值 (量子化, 空间量子化)
- 量子力学测量的结果
- 量子力学态的演化

量子力学的态、力学量



原子核的自旋

核自旋由一个波函数表示 $|\Phi\rangle$

力学量由一个厄米算符表示（厄米矩阵）

$$S_x = \frac{\hbar}{2} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad S_y = \frac{\hbar}{2} \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad S_z = \frac{\hbar}{2} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

量子力学测量值只能是本征值=>固有的值

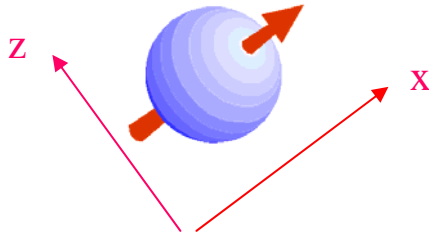
$$S_z = +\frac{\hbar}{2}, |S_z = +\frac{\hbar}{2}\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}; \quad S_z = -\frac{\hbar}{2}, |S_z = -\frac{\hbar}{2}\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix};$$

$$S_x = +\frac{\hbar}{2}, |S_x = +\frac{\hbar}{2}\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}; \quad S_x = -\frac{\hbar}{2}, |S_x = -\frac{\hbar}{2}\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix};$$

$$S_y = +\frac{\hbar}{2}, |S_y = +\frac{\hbar}{2}\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ i \\ \frac{1}{\sqrt{2}} \end{pmatrix}; \quad S_y = -\frac{\hbar}{2}, |S_y = -\frac{\hbar}{2}\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -i \\ \frac{1}{\sqrt{2}} \end{pmatrix};$$

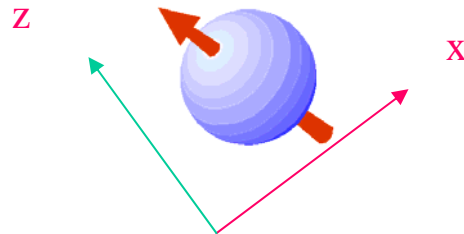
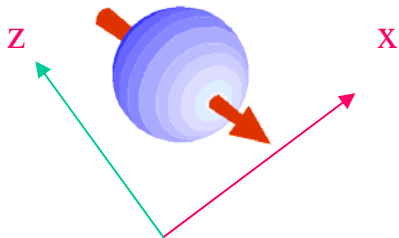
对自旋的三个分量进行测量得到的结果只能是 $\pm \frac{\hbar}{2}$

核自旋的状态可以是叠加态



$$|\Phi\rangle = |+\mathbf{x}\rangle = \sqrt{\frac{1}{2}} |+\mathbf{z}\rangle + \sqrt{\frac{1}{2}} |-\mathbf{z}\rangle$$

测量z分量，只能得到测量得到
 $\pm z$ ，其几率都是1/2



测量后体系的状态发生改变，塌缩到本征态

无论测量多么仔细，量子测量的结果使得体系的状态发生改变。只有在体系处在被测量量的本征态时，波函数才不会改变。

$$|\Phi\rangle \rightarrow |+z\rangle \quad \text{测量结果为} +z$$

量子体系的状态的时间演化遵从 Schroedinger方程

$$i\hbar \frac{\partial}{\partial t} |\Phi\rangle = H |\Phi\rangle$$

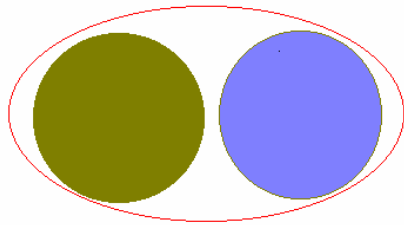
量子力学中的“牛顿方程”！

量子计算的过程是开启不同的**H**, 完成量子计算

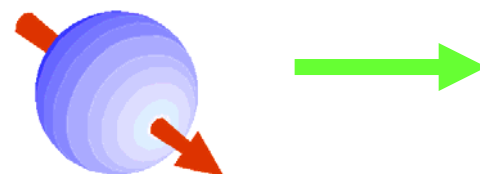
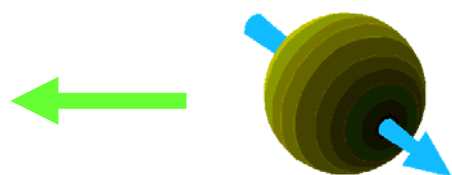
量子力学，难！之一：EPR佯谬

1935年 Einstein, Podolsky, Rosen. Bohm的简化表述

$$t = 0 \quad |\Phi^-\rangle = \left(|\uparrow_A \downarrow_B\rangle - |\downarrow_A \uparrow_B\rangle \right) \otimes \text{空间波函数}$$

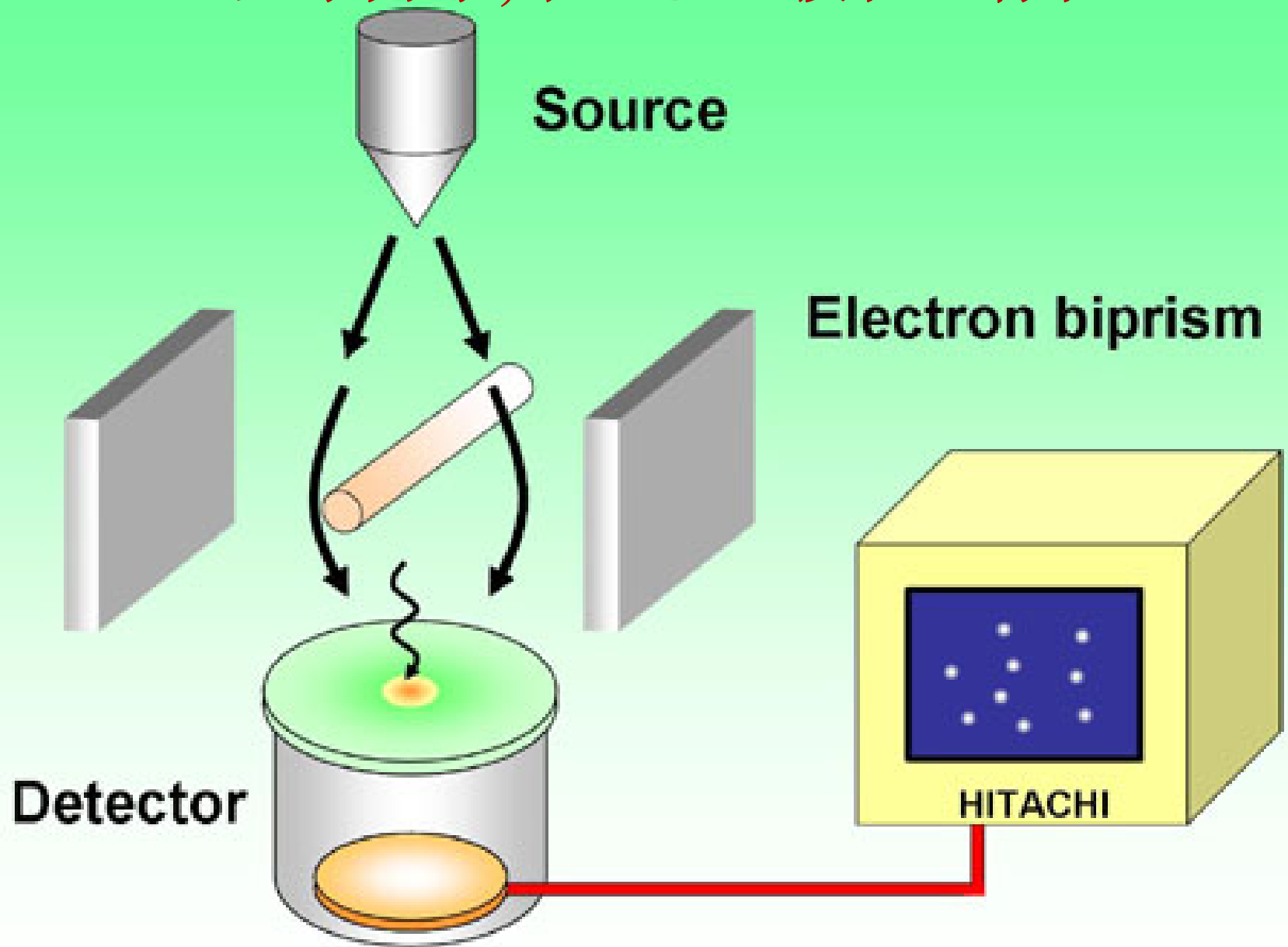


$t > T$

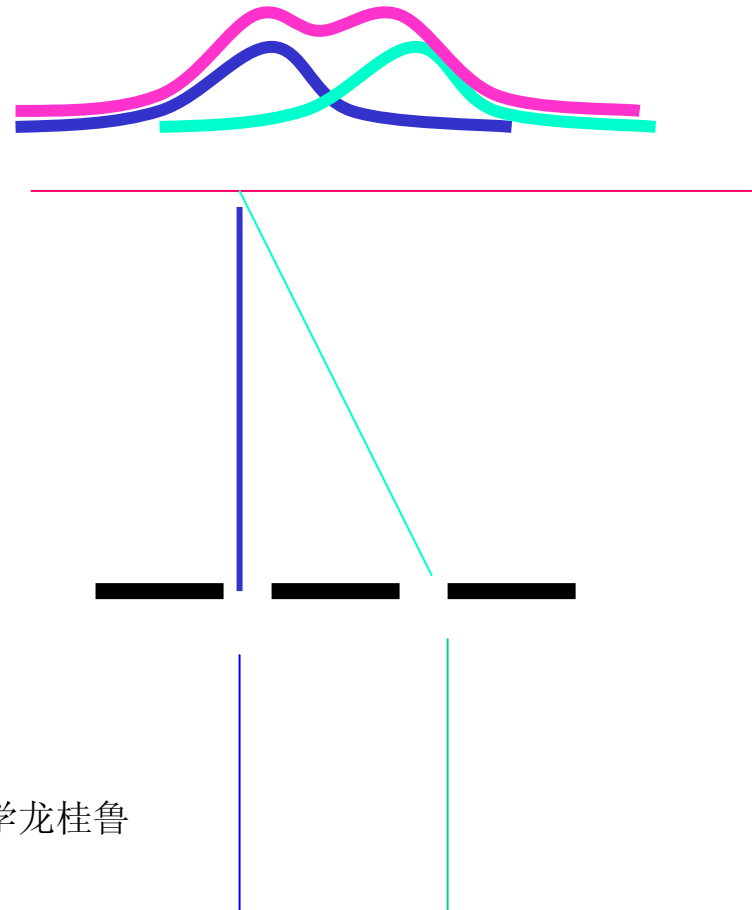
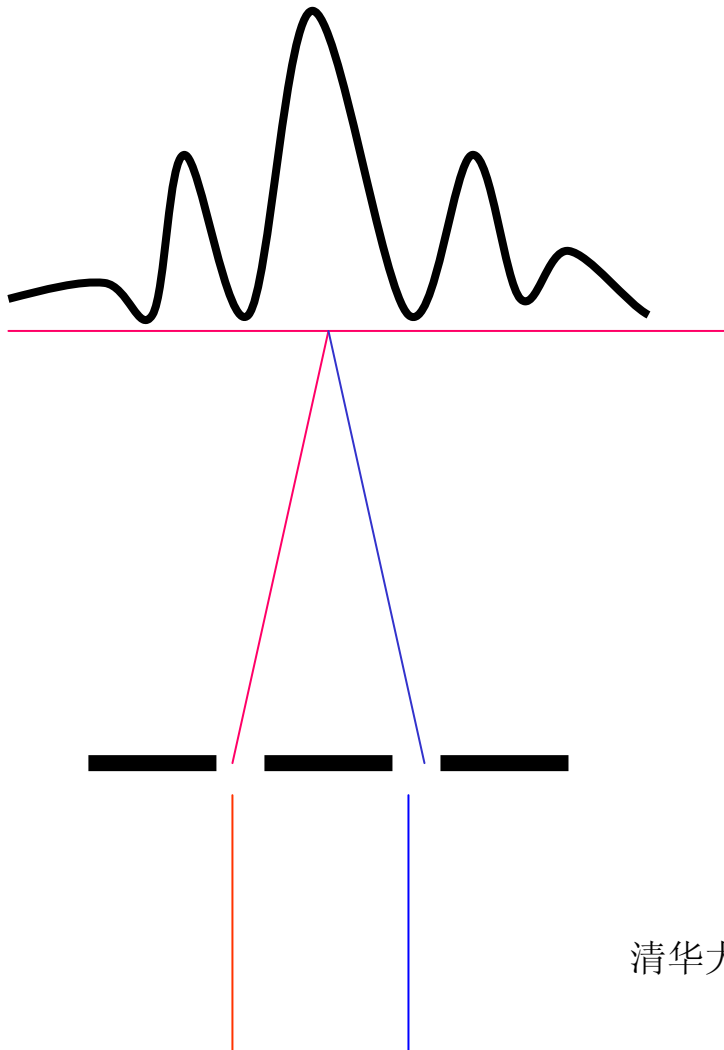


随着科学与技术的发展，这个理想实验被证实

量子力学,难! 之2: 波粒二像性



量子力学，难！之3： Which-way experiment



量子信息是量子力学（科学）与信息科学的结合

量子信息包含的内容

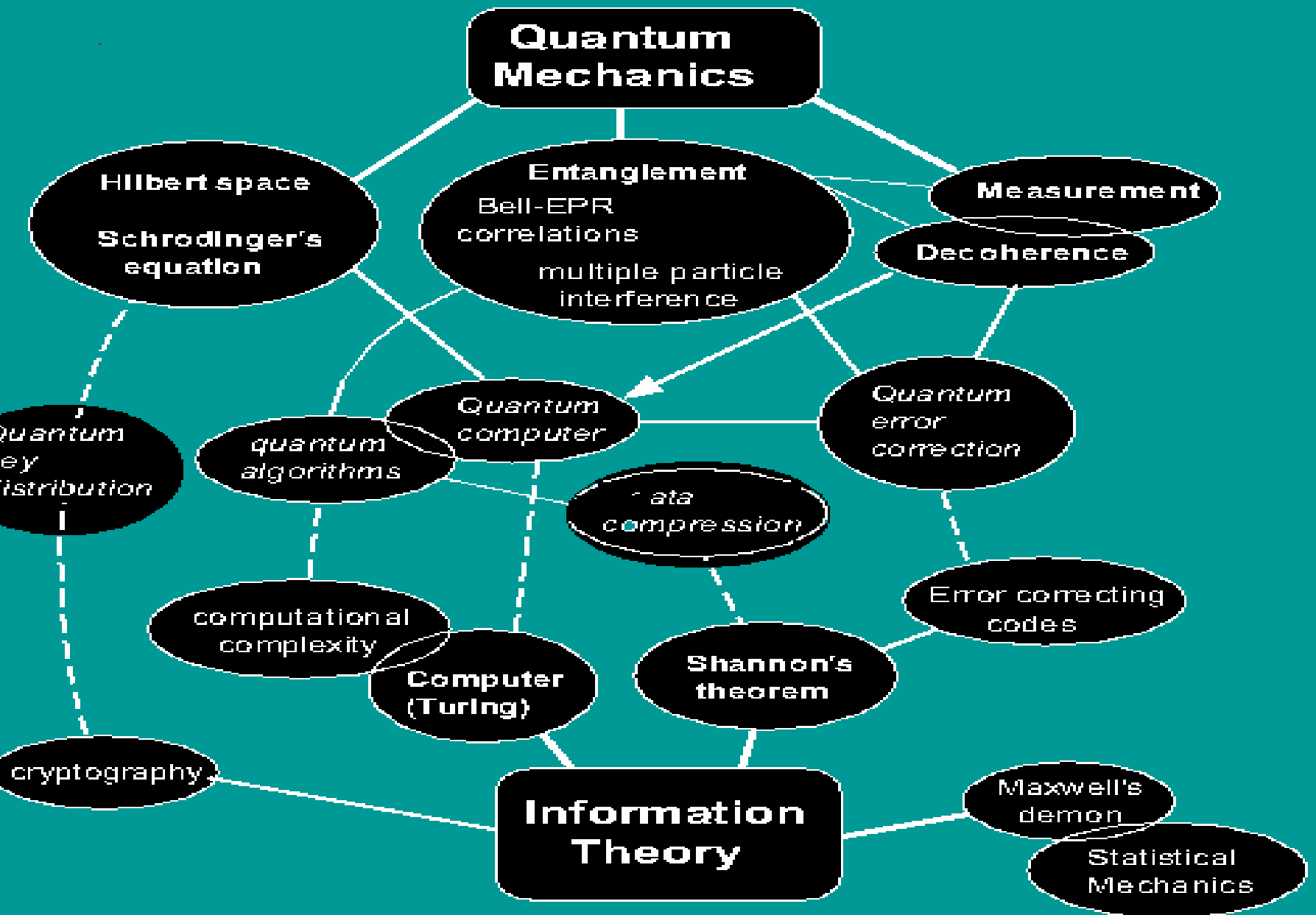
- **量子计算机**:以量子态进行计算的计算机

- **量子通讯**:

利用量子通道进行

经典信息生成与传递：**量子密钥分配**

量子信息的传递：**量子隐形传态**



量子计算

Reversible computer
Bennett 1973

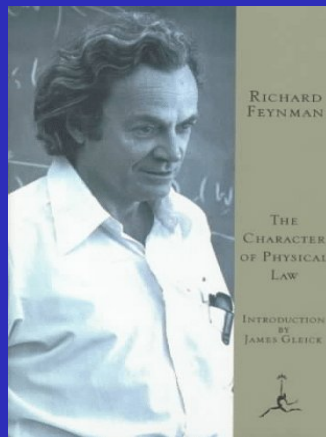


**Reversible Computer by
quantum mechanics**
P Benioff 1976



对量子体系的模拟需要使用量子计算机

Feynman 1982



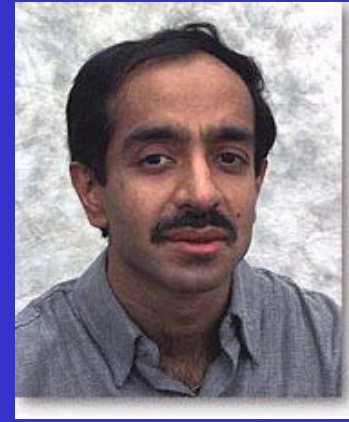
量子计算机具有普适性，量子平行性

Deutsch 1985





量子计算机快速分解大数算法
Shor, AT&T 1995



量子计算机可以快速进行数据搜索
Grover, Lucent 1996



J Jones, Oxford

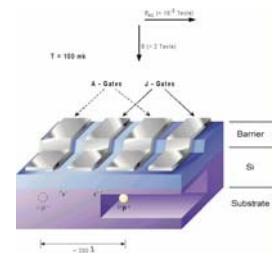
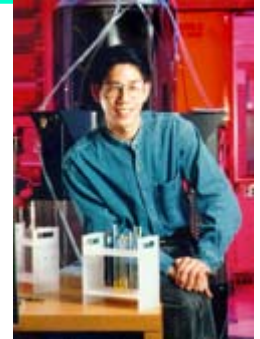
核磁共振量子计算算法演示1997



I Chuang, MIT

量子计算机 (2)

- 1997, 量子计算机的NMR实验方案
- 1998, NMR量子计算实验演示
- 1999, 各种实验方案的提出, 容错纠错码的提出 (Steane)
- 2000, NMR: 5个比特的算法演示 (IBM), 7个比特的量子态的制备; 固体硅基半导体NMR取得大的进展;
- 2001, 线性光学量子计算方案



2002: 固体超导量子计算 1个比特长寿命

2003: 2个固体超导量子比特的纠缠

2005: 量子计算的误差3%

清华大学:

2000—2002: 2—7个量子比特实验

2003: CORE, 2-Step QKD

2004: 实验量子密码通讯, QSS

直接安全量子通讯 Parallel QC

2005: 10比特QC, 新的计算模型

清华大学龙桂鲁

研究量子计算机的意义

- 量子体系的模拟必须使用以量子力学原理直接计算的计算机；300个量子比特体系的状态需要 $2^{300} \approx 10^{90}$ ，超过宇宙中的原子的总数：

量子计算机的建成会像计算机对科学研究产生巨大的影响。

量子计算机可以解决一些重要的数学问题:

Prime factorization
(Shor, 1994)

$$p_1 p_2 = N$$

$$\exp(n^{1/3}) \rightarrow \text{poly}(n)$$

Pell's equation
(Hallgren, 2002)

$$x^2 - dy^2 = N$$

$$\exp(n^{1/2}) \rightarrow \text{poly}(n)$$

**and
also:**

- Grover search – appointment scheduling
- period finding – group theory computations
- quantum simulation
- Raz algorithm – distributed simulation
- sampling complexity: disjoint subsets
- finite-round interactive proofs
- pseudo-telepathy (Bell inequalities, game playing)
- quantum cryptography
- quantum data hiding & secret sharing
- quantum digital signature

(BUT, some computations are not sped up at all!)
清华大学龙桂鲁

See DiVincenzo & Loss, cond-mat/9901137

Factorization: heart of encryption

RSA-129

$$221=13 \times 17$$

114381625757888867669235779976146612010

218296721242362562561842935706935245733

897830597123563958705058989075147599290

026879543541=? Factorized in 1994

3490529510847650949147849619903898133417

764638493387843990820577 **X**

327691329932667095499619881908344614131776

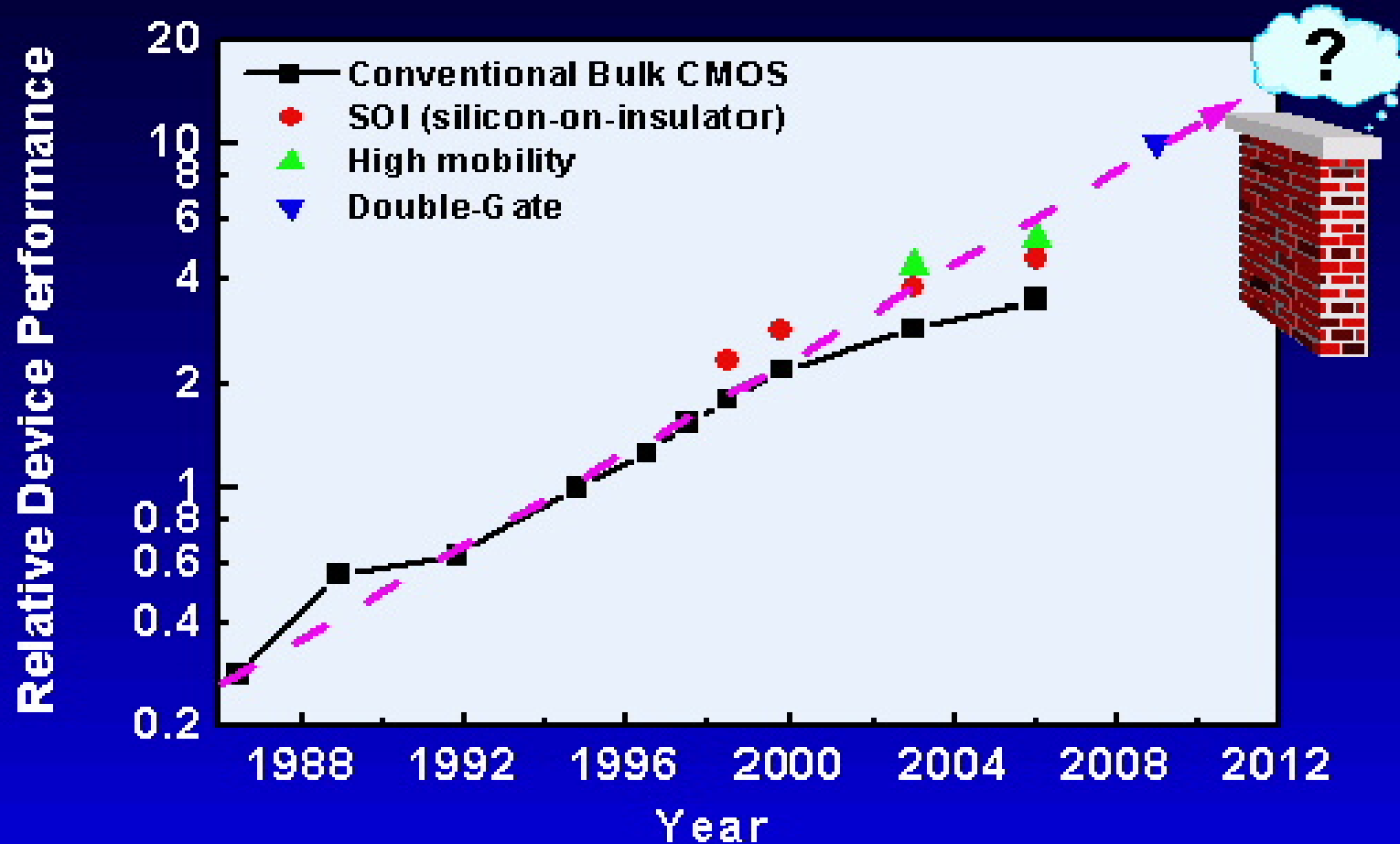
42967992942539798288533

- **Step1: 8 months /600 volunteers /20+ countries**
- **Step2: 45 hours (on a 16K MasPar MP-1 massively parallel computer).**
- **Bank of England uses a 155 digit number for its cryptography.**

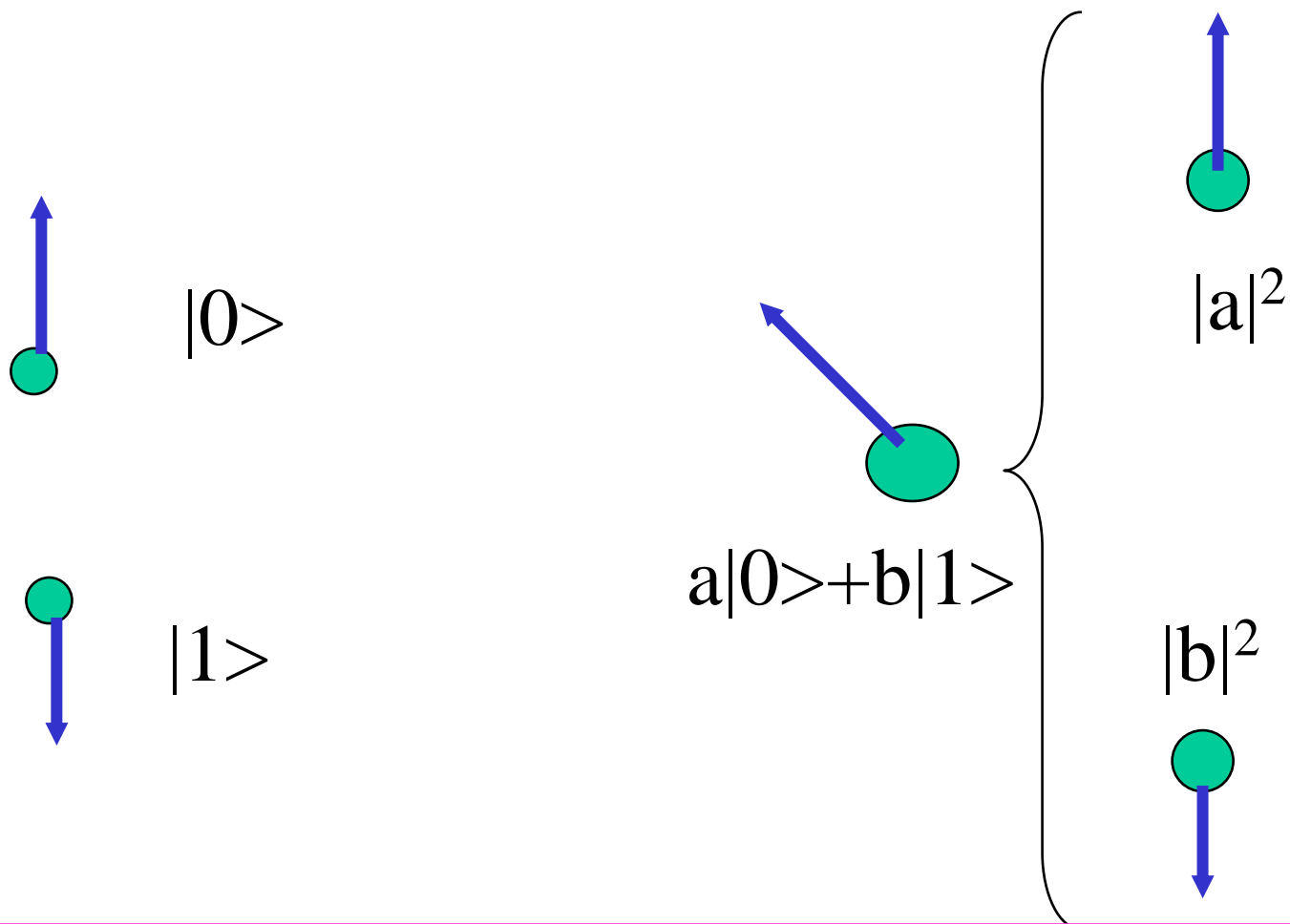
- 现在的计算机技术已经接近量子极限,量子计算机是一个新的发展方向

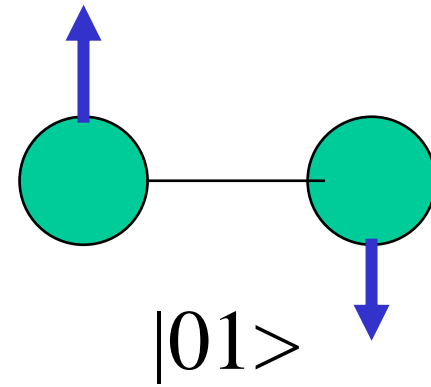
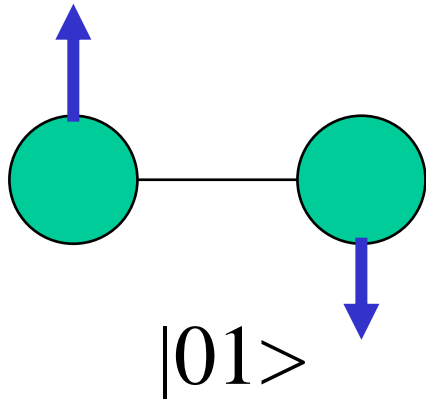
CMOS Device Performance

New device structures are needed to maintain performance...

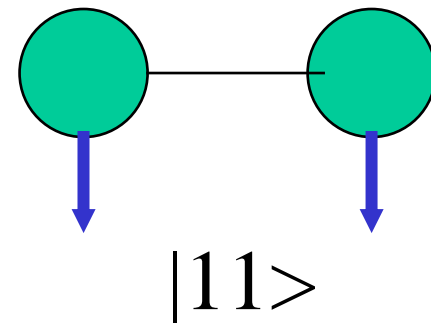
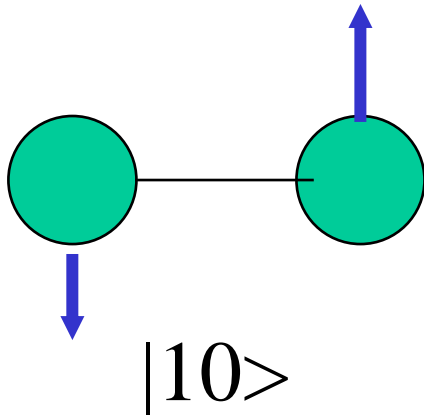


经典的比特与量子比特

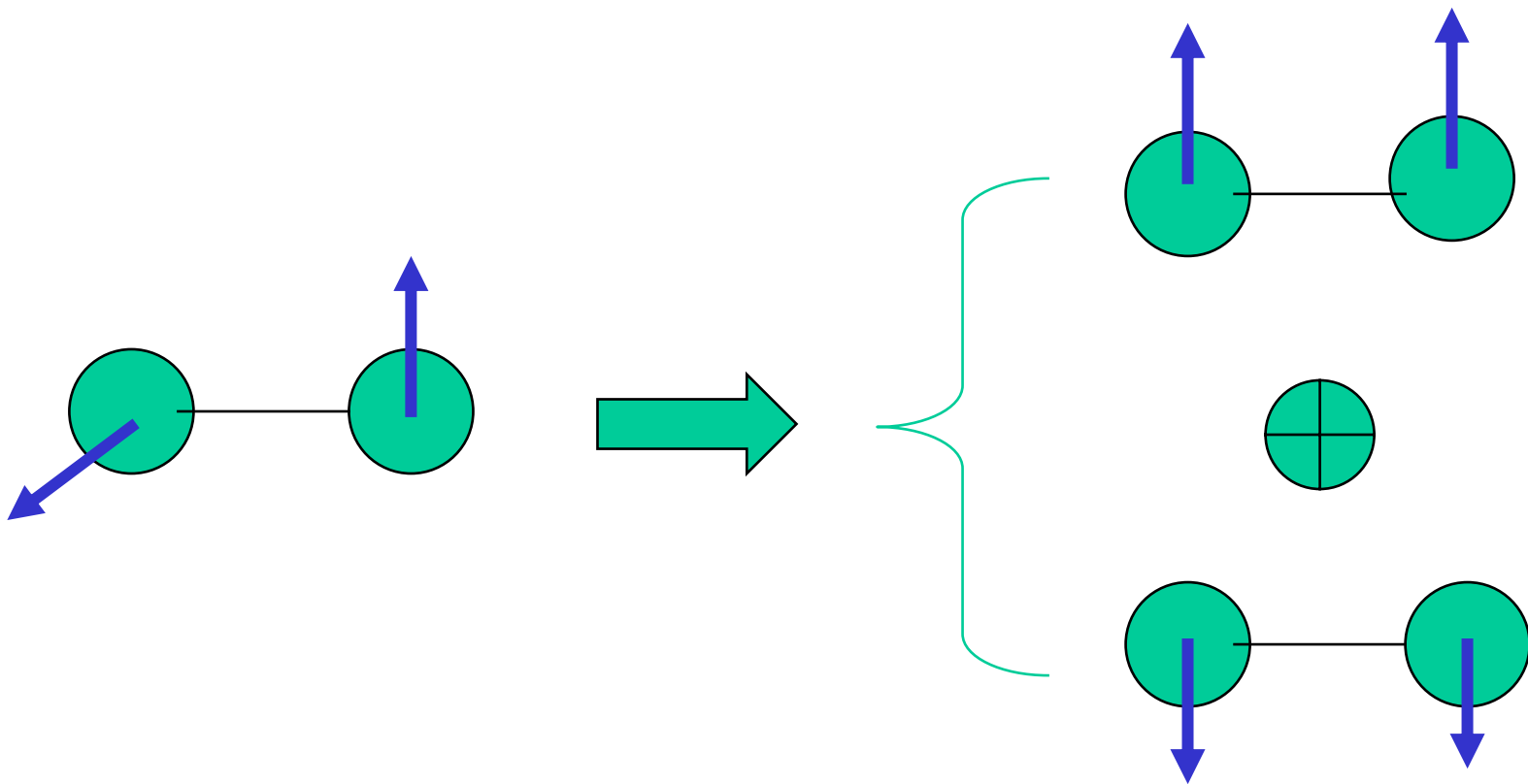




CNOT



$$\frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) |0\rangle \xrightarrow{CNOT} \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$$



量子计算机的特点

- 量子计算机具有巨大的信息携载量

在量子机和经典机中 n bits的都可以表示 $0, 1, 2, \dots, N-1, N=2^n$ 中的数。

但在某一时刻,经典计算机只能表示其中的一个, 而量子计算机可以同时表示所有的数的线性叠加。 比特数与等效内存

$10 \rightarrow 1\text{K}; 23 \rightarrow 1\text{M}; 30 \rightarrow 128\text{M}; 33 \rightarrow 1\text{G};$

$50 \rightarrow 131072\text{G};$ $500 \rightarrow 10^{467}\text{G}; 1000 \rightarrow 10^{967}\text{G};$
 $5000 \rightarrow 10^{4967}\text{G}。$

量子计算机的特点

- 巨大的量子并行功能

$$|\varphi\rangle = \frac{1}{\sqrt{N}} \{ |0\rangle + |1\rangle + |2\rangle + \dots + |N-1\rangle \}$$

$$U_f |\varphi\rangle = \frac{1}{\sqrt{N}} \{ |U_f(0)\rangle + |U_f(1)\rangle + \dots + |U_f(N-1)\rangle \}$$

CC requires N operations for the same task。 CC parallelism=线性增加
QC parallelism = 指数增加。

量子计算机的特点

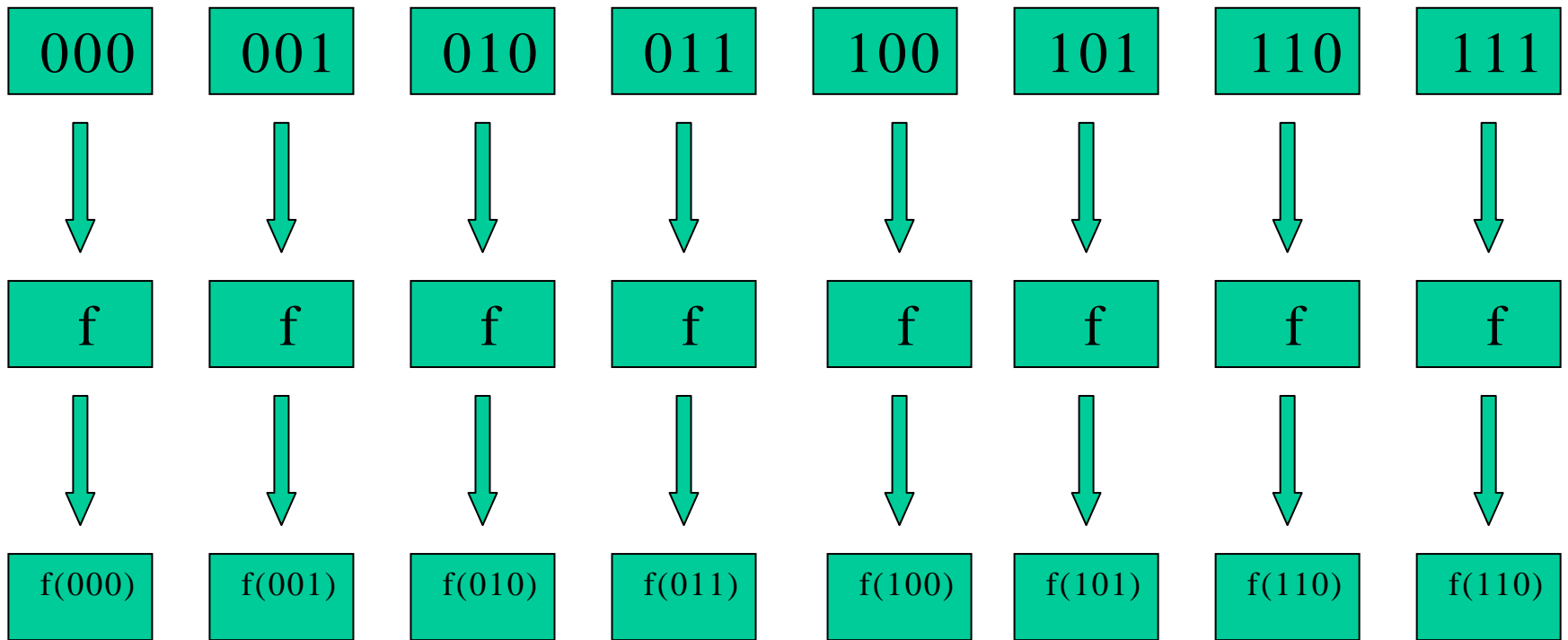
1、量子物理资源只需要经典计算机的对数多。

经典需要 N

量子需要 $\text{Log}_2(N)$

2、经典平行计算时，每个计算机都在作不同的计算，而量子计算机的一个相同操作完成了不同的计算任务。

经典计算



量子力学的叠加态与并行计算



量子算法—Shor大数因子化算法

- 可以证明，要分解一个大数 N ，等价于寻找函数 $f_{y,N}(x) = y^x \bmod N$ 的周期 r 。 y 为任意一个与 N 互质的自然数。一旦 r 找到，就可由 $(y^{r/2} \pm 1, N)$ 的最大公因子找出 N 的分解因子。
- 经典看来，要找出 r ，需要做的运算次数为 $e^{\log_2 N}$ 。
- 运用量子计算的并行性，运算次数为 $\log_2 N$ 的多项式。

一个简单的例子

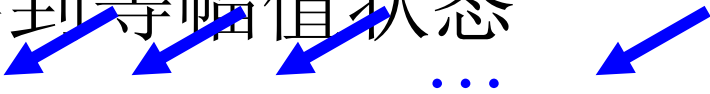
$f_{y,N}(x) = y^x \bmod N$ 的周期, $y=7, N=15$

x	0	1	2	3	4	5	6	7	8
7^x	1	7	49	343	...				
$7^x \bmod 15$	1	7	4	13	1	7	4	13	1

周期为 4 , $(7^{4/2}+1,15)=(50,15)=5,$

$(7^{4/2}-1,15)=(48,15)=3$

Shor大数因子化算法 (1)

- 一个大数 N , 两个存储器: 存储器1和存储器2。
- $q = 2^L$, $N^2 < q < 2N^2$, L 可以唯一地确定。
- 设置存储器1为 L 位存储器, 存储器2置空。
- 对存储器1的各个位进行局域变换 (Hadamard变换), 得到等幅值状态 $\frac{1}{\sqrt{q}} \sum_{x=0}^{q-1} |x\rangle$ 

Shor大数因子化算法 (2)

1. 选择一个任意的与 N 互质的数 y , 计算 $y^x \bmod N$, 并将计算结果存入存储器

$$\frac{1}{\sqrt{q}} \sum_{x=0}^{q-1} |x\rangle |y^x \bmod N\rangle$$

一步完成!

$$N=15, y=7, q=256, L=10$$

$$N = 15, y = 7$$

$$\begin{aligned} & \left(|0\rangle + |4\rangle + |8\rangle + \dots + |1020\rangle \right) |1\rangle \\ & + \left(|1\rangle + |5\rangle + |9\rangle + \dots + |1021\rangle \right) |7\rangle \\ & + \left(|2\rangle + |6\rangle + |10\rangle + \dots + |1022\rangle \right) |4\rangle \\ & + \left(|3\rangle + |7\rangle + |11\rangle + \dots + |1023\rangle \right) |13\rangle \end{aligned}$$

此时，直接对第一存储器测量，效率很低。

3. 测量第 2 个存储器后，显然 $x = x_0 + jr$ 对应的态在第一存储器保留下来， $j = 0, 1, 2, \dots, M$ ， M 代表循环的最大次数。存储器 1 的状态为

$$|\phi_{x_0}\rangle = \frac{1}{\sqrt{M+1}} \sum_{j=0}^M |x_0 + jr\rangle = \sum_{j=0}^{q/r-1} |x_0 + jr\rangle$$

对第 1 个存储器作量子Fourier变换,

$$U_{QFT} |x\rangle = \frac{1}{2^{L/2}} \sum_{y=0}^{2^L-1} e^{2\pi i xy/2^L} |y\rangle$$

则第 1 个存储器中的波函数变为

$$\sum_{y=0}^{2^L-1} C_y |y\rangle$$

其中系数 C_y 仅在一些特殊的值时不为零

此时，第一个存储器中系数不为零的态为

$$|0\rangle + |256\rangle + |512\rangle + |768\rangle$$

测量后得到了最小的差为256,反推得到

$$r = \frac{2^{10}}{256} = 4$$

经典搜索与量子搜索

- 从没有排序的 N 个数据中搜索一个特定的数据，经典计算机的做法是按照这些数据依次寻找，直到找到为止。平均需要 $N/2$ 次运算，最不幸的情况是要做 N 次运算。
- 量子搜索算法(L.K.Grover)通过一次次并行计算，将所要寻找的信息的几率逐步放大，直到所需数据项的几率几乎为1。运算次数为 $O(\sqrt{N})$ 。

量子搜索

- 我们拿着电话号码本，上面以很小的字体写着很多电话号码。先不打开它，对所有号码进行若干次操作，然后打开电话本，发现里面写着一个大大的号码，就是我们所寻找的信息。

Quantum mechanics helps in searching a needle in a haystack, PRL 79(1997) 325.

Grover算法的要点

相干叠加数据库:

$$|\psi\rangle = \frac{1}{\sqrt{N}} \{ |0\rangle + |1\rangle + |2\rangle + \dots + |\tau\rangle + \dots + |N-2\rangle + |N-1\rangle \} = H|0\rangle$$

搜索过程将标记态的系数不断放大

1、对标记态的系数取反:

$$I_{\tau} = 1 - 2|\tau\rangle\langle\tau|$$

2、对所有的系数平均取反

$$D_{ij} = \begin{cases} \frac{2}{N}, & i \neq j \\ \frac{2}{N} - 1, & i = j \end{cases}$$

对平均取反运算是由三步组成：

- **Hadmard-Walsch**变换
- 对 $|0\rangle$ 态系数取反
- **Hadmard-Walsch**变换

$$I_0 = 1 - 2|0\rangle\langle 0|$$

Hadmard-Walsch变换W:

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

$$|\psi\rangle_0 = \frac{1}{\sqrt{8}} \{ |0\rangle + |1\rangle + |2\rangle + |3\rangle + |4\rangle + |5\rangle + |6\rangle + |7\rangle \}$$

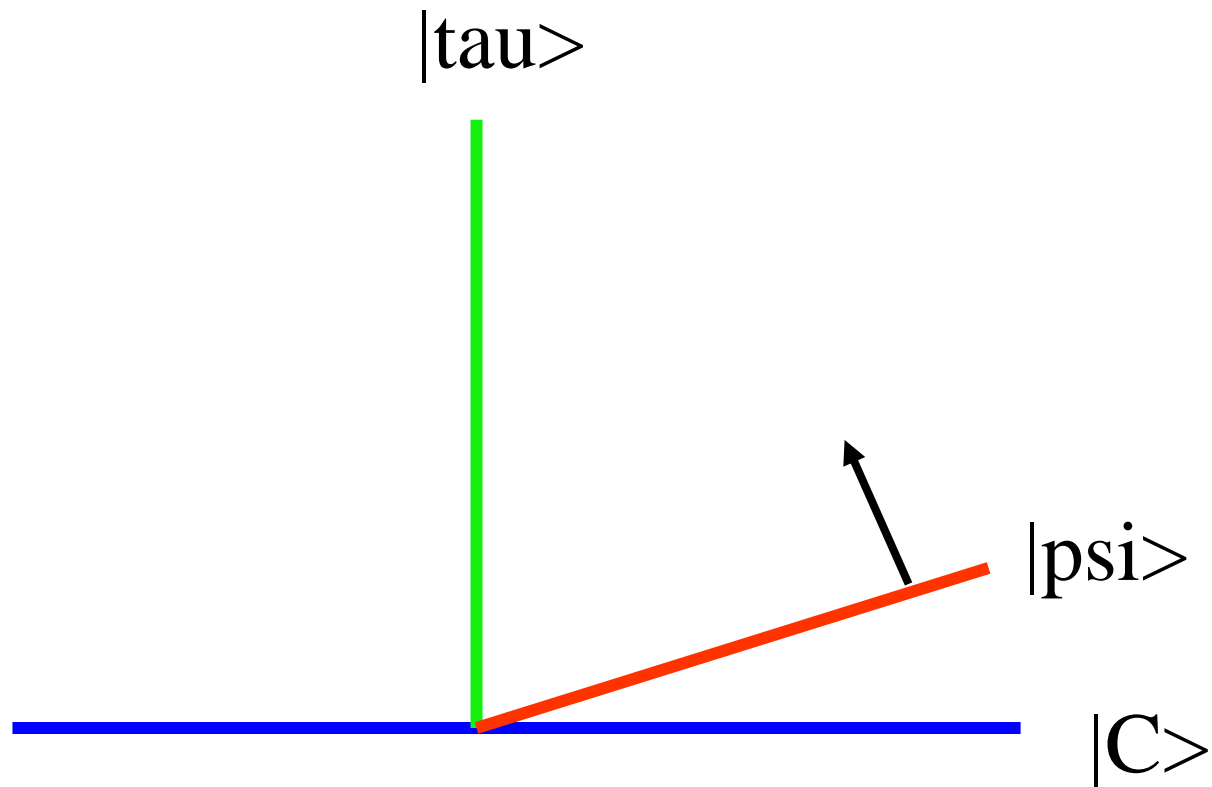
P=0.125

$$|\psi\rangle_1 = \frac{1}{2\sqrt{8}} \{ |0\rangle + |1\rangle + |2\rangle + 5|3\rangle + |4\rangle + |5\rangle + |6\rangle + |7\rangle \}$$

P=0.781

$$|\psi\rangle_2 = \frac{1}{4\sqrt{8}} \{ -|0\rangle - |1\rangle - |2\rangle + 11|3\rangle - |4\rangle - |5\rangle - |6\rangle - |7\rangle \}$$

P=0.945



- 一次迭代相当于旋转 2θ 的角度，经过 j 次连续迭代，态矢成为：

$$|\varphi_j\rangle = \cos[(2j+1)\theta]|c\rangle + \sin[(2j+1)\theta]|\tau\rangle$$

- 找到 $|\tau\rangle$ 的几率最大 (为1)满足下面的条件:

$$\sin(2j+1)\theta = 1$$

$$(2j+1)\theta = \frac{\pi}{2}$$

$$\therefore j_c = \frac{\pi}{4\theta} - \frac{1}{2} \approx \frac{\pi}{4} \sqrt{N}$$

量子计算与经典计算的关键不同

- 1、对资源的需求是指数量级的少
- 2、量子平行使得能力指数的增加
- 3、测量的限制，使得量子计算并非都能指数加快

同样：量子计算的物理实现困难也是巨大的
但是理论上已经没有了困难

量子搜索中的相位匹配

龙-算法

其中有两个态系数取反: $|0\rangle$, $|\tau\rangle$: 推广: 一般的相位旋转

Zalka: 旋转 $|\tau\rangle \rightarrow 0 \rightarrow \pi$: **By continuity, it is now clear that we can adjust the absolute value of the amplitude of the marked states to any value between these extremes. . . .**

Grover: “The above derivation easily extends to the case when the amplitudes in states of , **instead of being inverted by I_γ and I_τ , are rotated by arbitrary phases.** However, the number of operations required to reach τ will be greater. Given a choice, it would be clearly better to use the inversion rather than a different phase rotation. . . .”

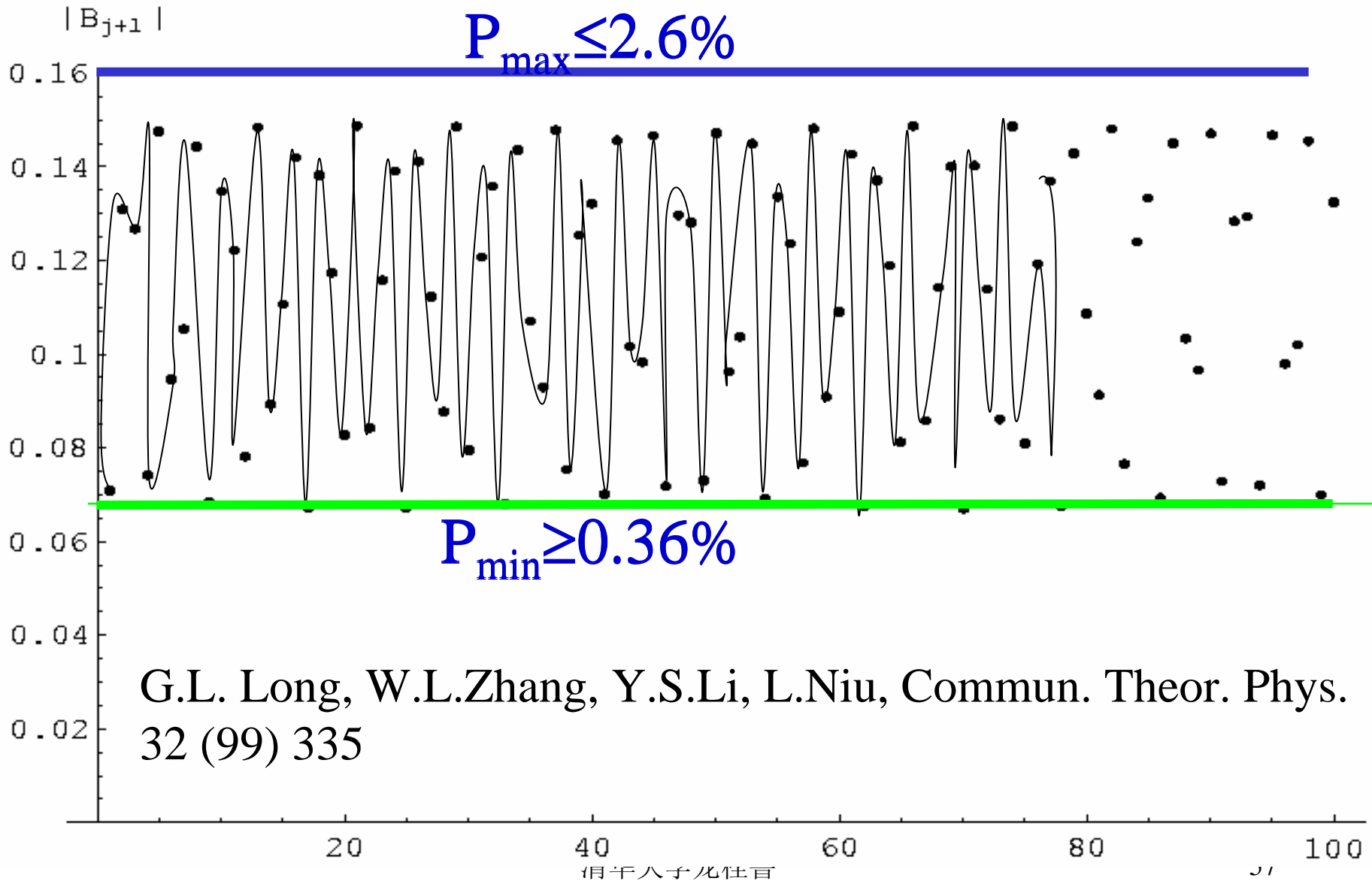
Replacing the phase inversion of the marked state

$$|\psi_j\rangle = A_j |c\rangle + B_j |\tau\rangle$$

$$\begin{pmatrix} A_{j+1} \\ B_{j+1} \end{pmatrix} = \begin{pmatrix} -e^{i\theta} \frac{N-2}{N} & \frac{2\sqrt{N-1}}{N} \\ e^{i\theta} \frac{2\sqrt{N-1}}{N} & \frac{N-2}{N} \end{pmatrix} \begin{pmatrix} A_j \\ B_j \end{pmatrix} = \begin{pmatrix} -e^{-i\theta} \cos 2\beta & \sin 2\beta \\ e^{i\theta} \sin 2\beta & \cos 2\beta \end{pmatrix} \begin{pmatrix} A_j \\ B_j \end{pmatrix}$$

Using direct calculation, we found that the algorithm did not search in the way as expected: it fails totally!

$$\theta = \pi/4$$



G.L. Long, W.L.Zhang, Y.S.Li, L.Niu, Commun. Theor. Phys.
32 (99) 335

量子搜索的相位匹配

$$I_0 = I + (e^{i\phi} - 1) |0\rangle\langle 0|;$$

$$I_\tau = I + (e^{i\theta} - 1) |\tau\rangle\langle \tau|$$

It fails in general unless if the phase rotations satisfy the phase matching condition:

$$\theta = \phi$$

相位匹配条件在2个比特核磁共振实验验证:

Experimental NMR realization of a generalized quantum search algorithm, G L Long, H Y Yan, Y S Li et al, Phys Lett A286(2001)121

在光学实现中部分验证，并提出对多比特（20）量子搜索检验相位匹配：**Bhattacharya, van Linden, Spreuw, PRL88 (2002) 137901**

- **Analysis of generalized Grover quantum search algorithms using recursion equations**

以色列、德国、美国Eli Biham, Ofer Biron, Markus Grassl, D A Lidar and Daniel Shapira, Phys. Rev. A63 (2001)012310 :

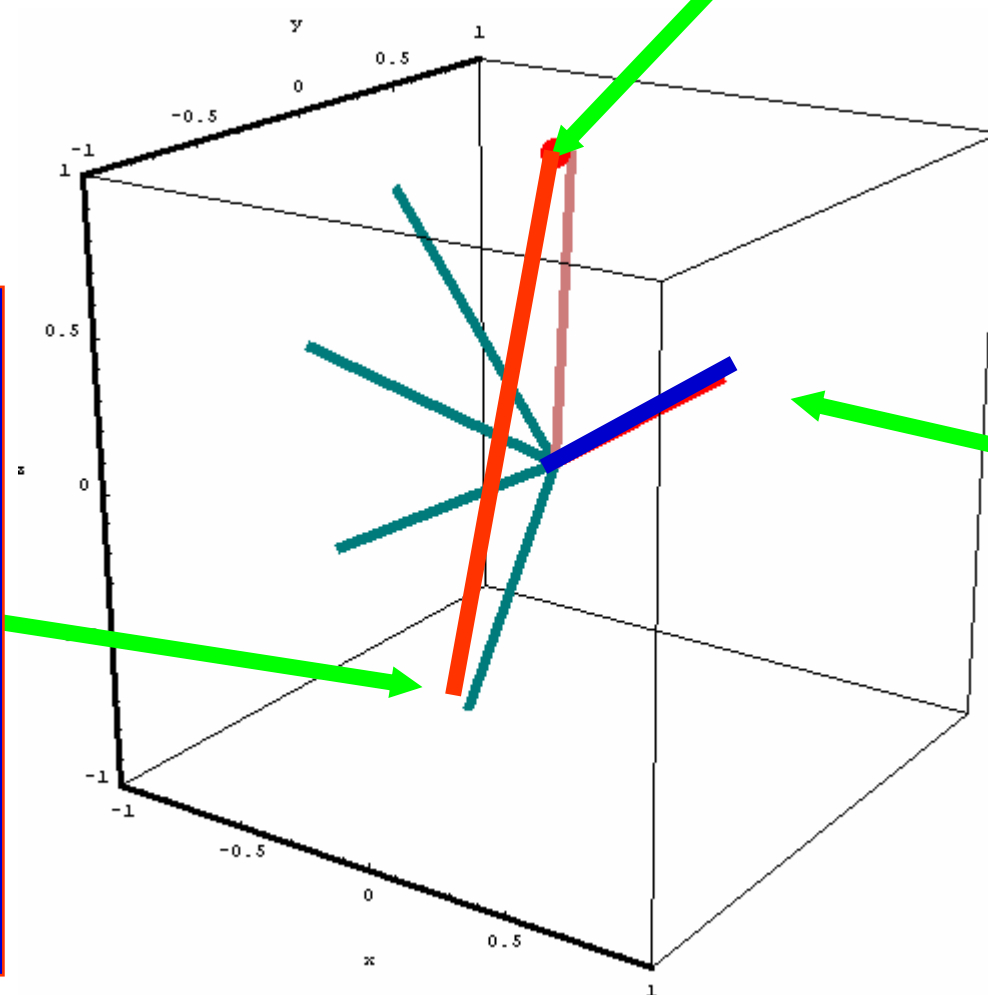
“Moreover, it was found that in order for the algorithm to apply the two rotation angles must be equal, namely, $\beta=\gamma$ ”

- **Peter Hoyer, Arbitrary phases in quantum amplitude amplification, Physical Review A62 (2000) 052304**
- In particular, the effects of using arbitrary phases in amplitude amplification have been studied in a sequence of papers by Long et al. [2--5]
- Our results complement the results of Long et al. who are primarily interested in the question of how large phase errors we can tolerate and still obtain a quantum algorithm for searching that succeeds with high probability. We are primarily interested in the question of what restrictions we need to put on the two angles used in amplitude amplification and still obtain quantum algorithms that succeed with certainty. .

$$(\mathbf{r}_f - \mathbf{r}_o) \cdot \mathbf{l}_n = 0$$

The marked state \mathbf{r}_f

The initial state \mathbf{r}_o



Rotational axis \mathbf{l}_n

Using the geometric picture of the quantum search algorithm, it is derived that the phase matching condition is

$$\tan\left(\frac{\theta}{2}\right)\left[\cos(2\beta) + \tan\theta_0 \cos\delta \sin 2\beta\right]$$

||

$$\tan\left(\frac{\phi}{2}\right)\left[1 - \tan\theta_0 \sin\delta \sin 2\beta \tan\left(\frac{\theta}{2}\right)\right]$$

龙-算法(Long Algorithm)

改进的量子搜索算法

**G L Long, Phys. Rev. A 64 (2001) 022307,
Grover algorithm with zero theoretical failure
rate,**

Long Algorithm

标准的Grover算法是粗糙的，成功率不是100%

准确的量子搜索中，相位不是取反，而是略微小于180度的转动

The maximum probability for finding the marked state in Grover algorithm is not exactly 100%.

n	1	2	3	≈ 7	≈ 10	≈ 13	≈ 20
N	2	4	8	100	1000	10⁴	10⁶
P_{max}	0.5	1.0	0.95	0.998	0.9996	1-10⁻⁶	1-10⁻⁶

We have improved this by replacing the phase inversions with smaller phase rotations.

$$\theta = \phi = 2 \arcsin \left(\frac{\sin \left(\frac{\pi}{4J + 6} \right)}{\sin \beta} \right)$$

特例:

TABLE II. Examples of $j_{op} + 1$ and ϕ .

$N =$	2	4	8	16	100	1000	10^4	10^6	10^8	10^{10}
$j_{op} + 1$	1	1	2	3	8	25	79	785	7854	78540
$\frac{\phi}{\pi}$	$\frac{1}{2}$	1	0.677007	0.698709	0.748018	0.854022	0.90089	0.989752	0.992688	0.9973

量子计算机的物理实现

DiVincenzo criteria



- David DiVincenzo (IBM) – requirements for a scalable quantum computer:
 1. The machine must have a 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 should be possible

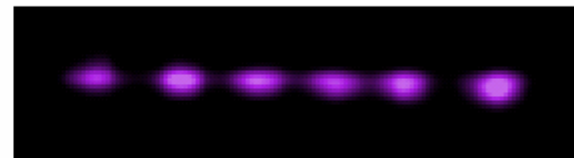
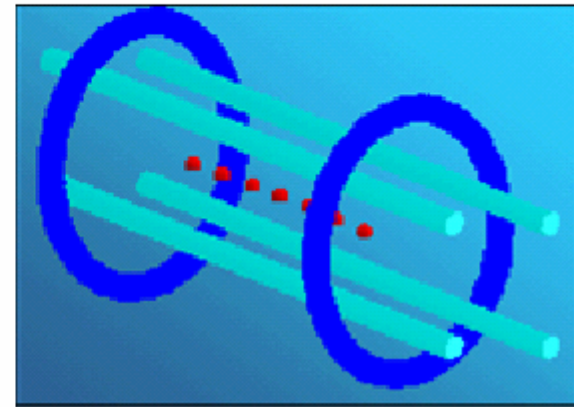
Physical implementations

Many sub-fields of physics have proposals for QC

- Liquid-state NMR
- NMR spin lattices
- Linear ion-trap spectroscopy
- Neutral-atom optical lattices
- Cavity QED + atom
- Linear optics
- Nitrogen vacancies in diamond
- Electrons in liquid He
- Superconducting Josephson junctions
 - ◆ charge qubits
 - ◆ flux qubits
 - ◆ phase qubits
- Quantum Hall qubits
- Coupled quantum dots
 - ◆ spin, charge, excitons
- Spin spectroscopies, impurities in semiconductors

Ion traps

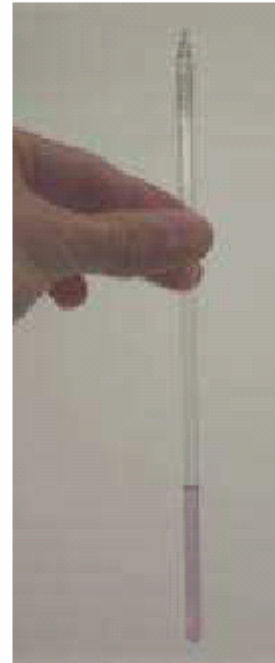
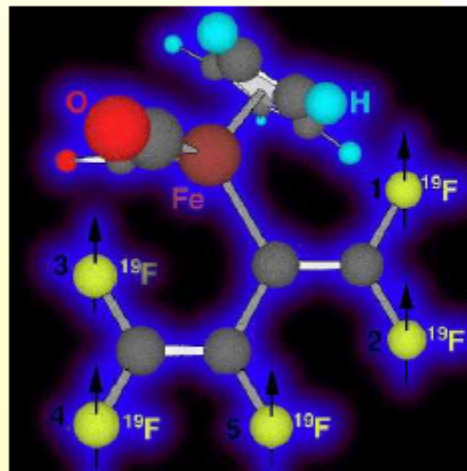
- Qubit: internal electronic state of atomic ion in a trap (ground and excited)
- Coupling: use quantised vibrational mode along linear axis (phonons)
- Single qubit gates: using laser



Cirac and Zoller¹, *Phys. Rev. Lett.* (1995)

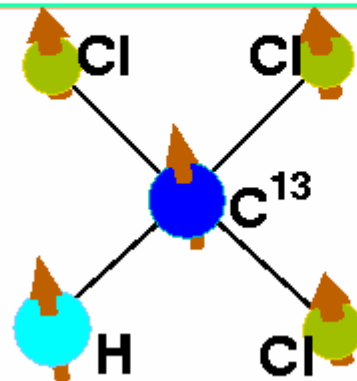
Nuclear magnetic resonance (NMR)

- 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)

An Example: Labeled Chloroform at Room Temperature



Chlorine (3/2) spins interact very weakly with carbon¹³ (1/2) and proton (1/2) spins

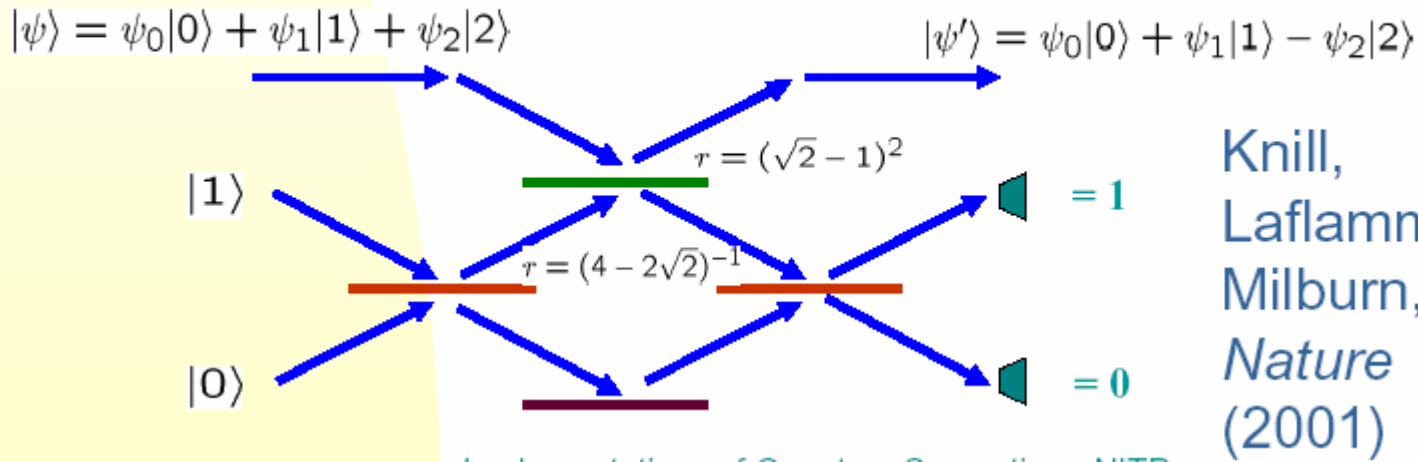
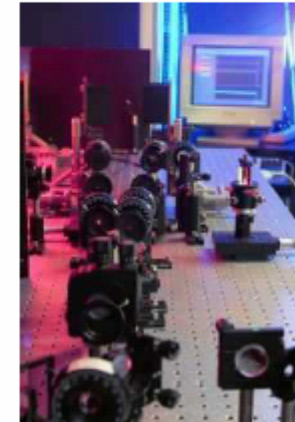
- Hamiltonian for the proton and carbon¹³ spins in a strong magnetic field along z :

$$H = \omega_H \sigma_z^{(H)} / 2 + \omega_C \sigma_z^{(C)} / 2 + J \sigma_z^{(H)} \sigma_z^{(C)} / 4 + H_{RF} + H_{rest}$$

At 11.4T: $\omega_H \approx 500\text{MHz}$ $J \approx 215\text{Hz}$ $|H_{rest}| \lesssim 2\text{Hz}$
 $\omega_C \approx 125\text{MHz}$

Linear optics

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

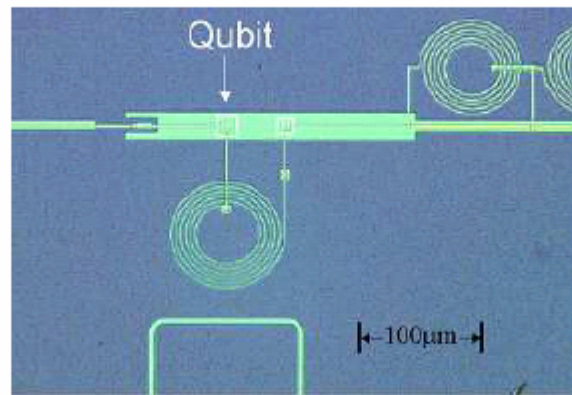


Knill,
Laflamme,
Milburn,
Nature
(2001)

Superconducting Josephson junctions

Qubit: a) Magnetic flux trapped in loop
b) Cooper pair charge on metal box
c) Charge-phase

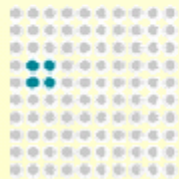
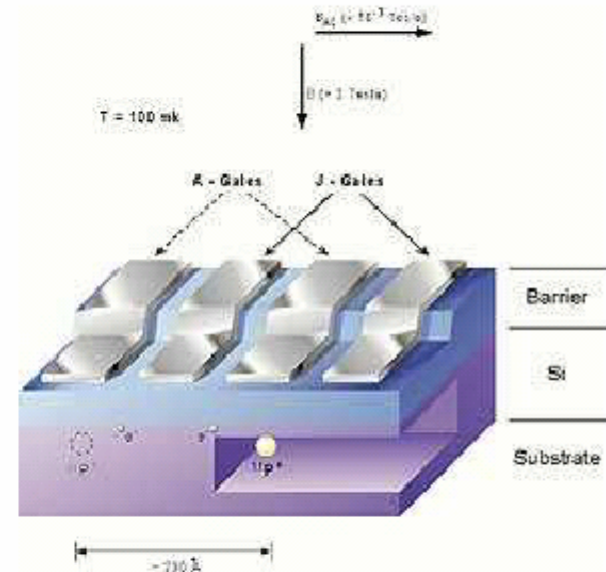
- ◆ Coupling: capacitive/inductive
- ◆ Single-qubit gates: flux bias, charge on gate, current through junction



Nakamura,
Pashkin, Tsai,
Nature (1999)

Silicon quantum computing

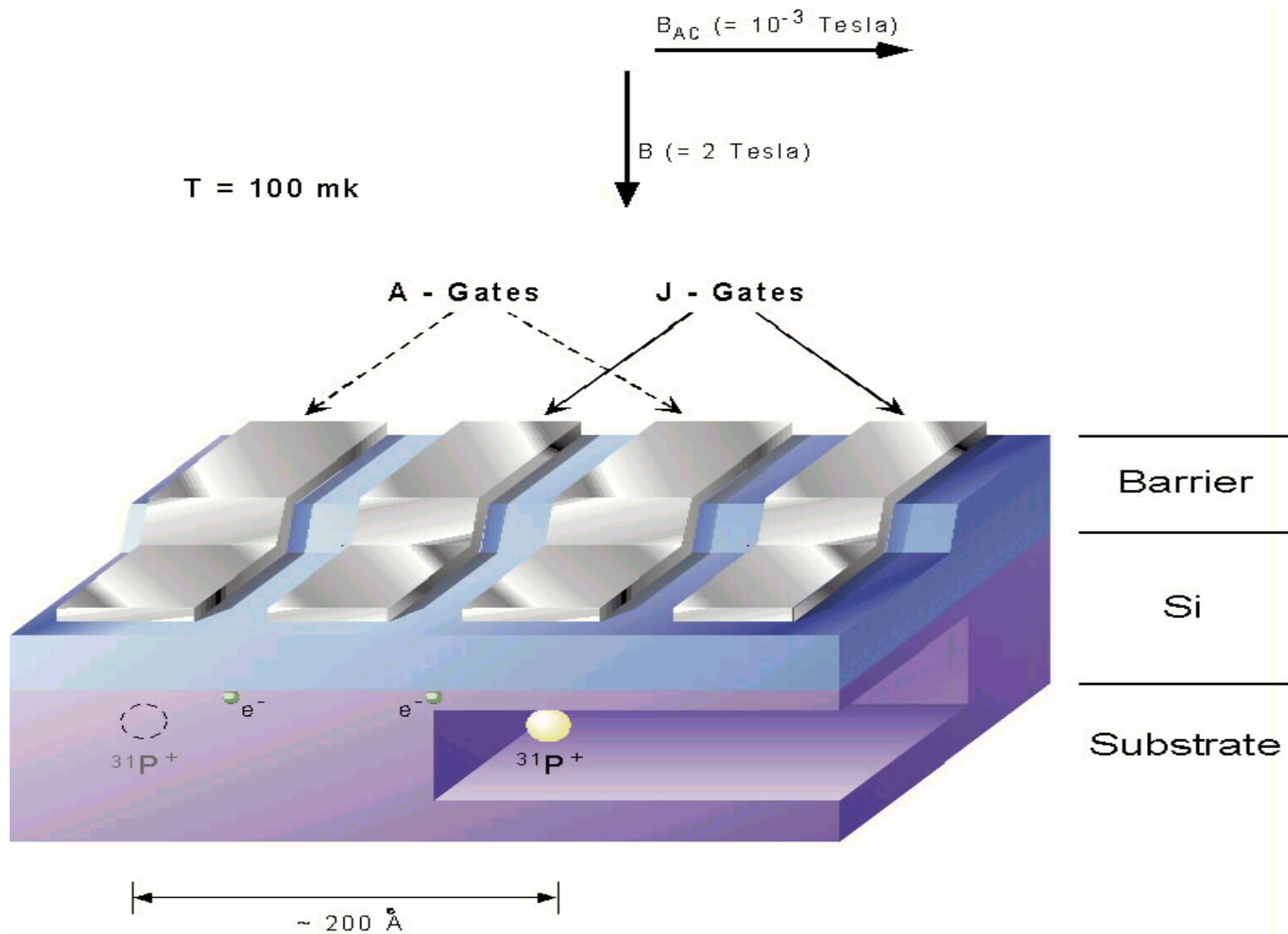
- Qubit:
 - ◆ Nuclear spin of single P donor
 - ◆ Electron spin of single donor
 - ◆ Electron charge
- Coupling: gate-controlled electron-electron interaction
- Single-qubit gates: NMR pulse; gate bias in magnetic material; charge on gate



CENTRE FOR
QUANTUM COMPUTER
TECHNOLOGY

AUSTRALIAN RESEARCH COUNCIL SPECIAL RESEARCH CENTRE

Kane, *Nature* (1998)



前途光明的实现方案

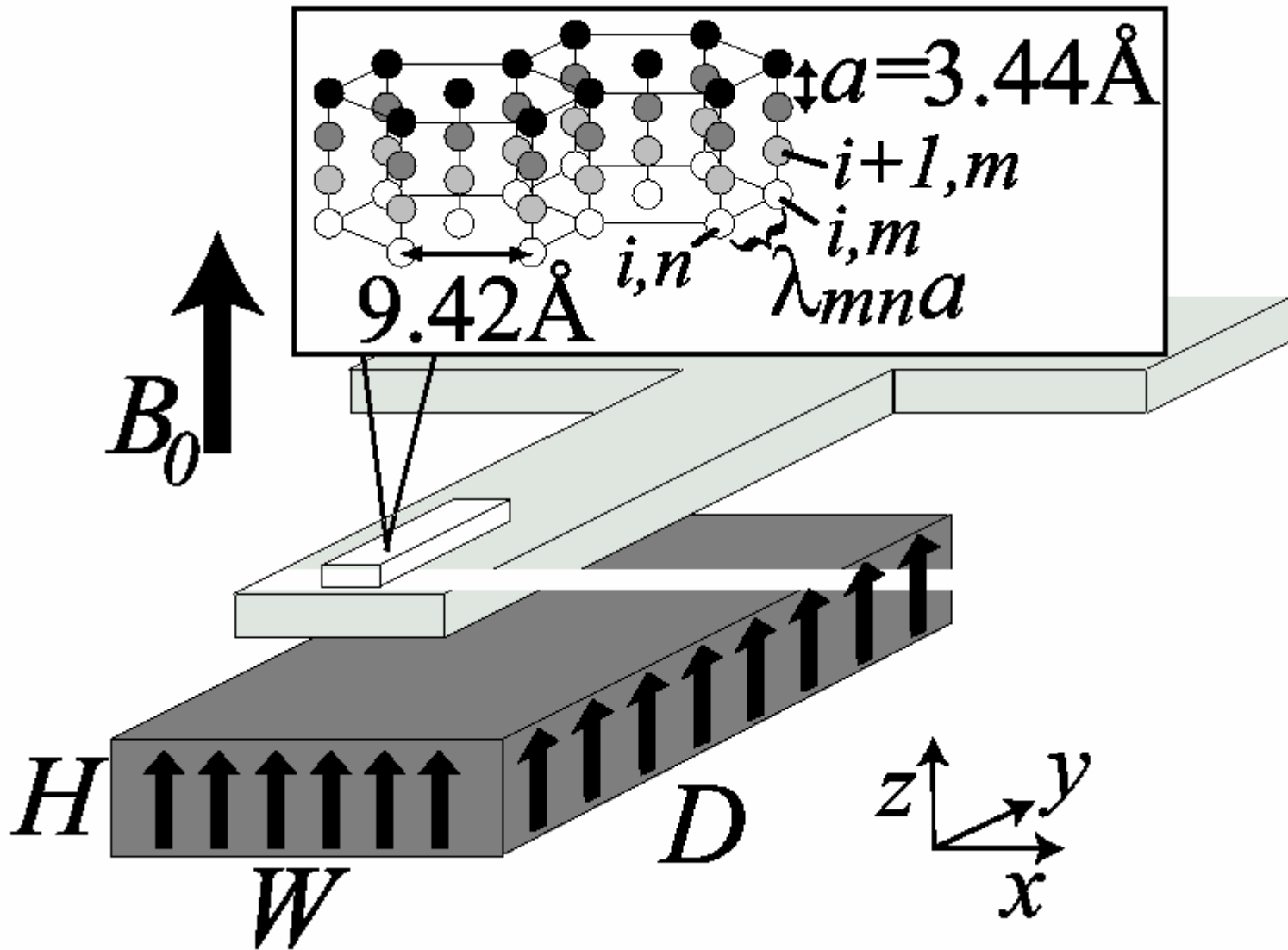



















































Table 4.0-1

The Mid-Level Quantum Computation Roadmap: Promise Criteria

QC Approach	The DiVincenzo Criteria							
	Quantum Computation						QC Networkability	
	#1	#2	#3	#4	#5		#6	#7
NMR								
Trapped Ion								
Neutral Atom								
Cavity QED								
Optical								
Solid State								
Superconducting								
Unique Qubits	This field is so diverse that it is not feasible to label the criteria with "Promise" symbols.							



Entanglement and Squeezing in Solid State Circuits

Entanglement and squeezing in solid-state circuits, W Y Huo and GLL, *New Journal of Physics* 10 (2008) 013026

**Generation of squeezed states of nanomechanical resonator
using three-wave mixing, WY Huo and GLL, *APL*, 92, 133102 2008**



Strong Coupling in Circuit QED system:

A. Blais, et al. Phys. Rev. A, 69: 062320 (2004),

A. Wallraff, et al. Nature, 431: 162–167 (2004),

Sun, Wei, Liu and Nori, PRB 2006

Proposals for generation squeezed states in solid state circuits:

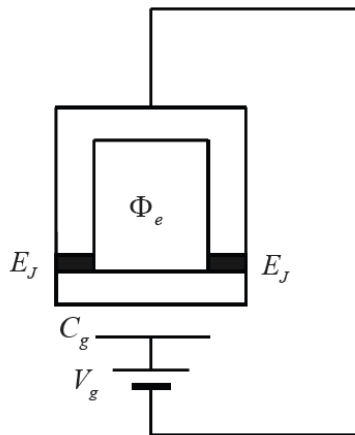
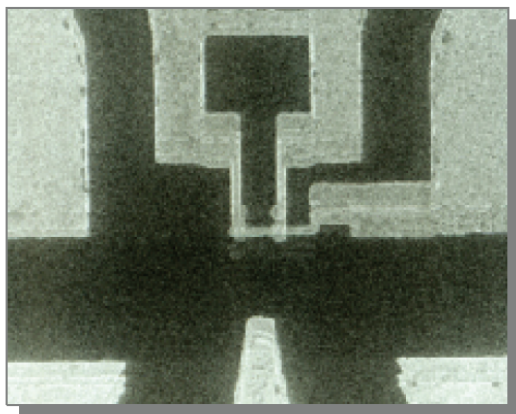
K. Moon, S. M. Girvin, PRL, 95: 140504 (2005)

Zhou X X, A. Mizel, PRL, 97, 267201 (2006)

P. Rabl, et al, PRB, 70, 205304 (2004)

R. Ruskov, et al, PRB, 71, 235407 (2005)

T. Ojanen, J. Salo, PRB, 75, 184508 (2007)



Superconducting Charge qubit

$$H = -\frac{E_c}{2}(1 - 2n_g)\sigma_z - E_J \cos\left(\frac{\pi\Phi_e}{\Phi_0}\right)\sigma_x$$

$$E_c = \frac{(2e)^2}{2C_\Sigma}$$

$$n_g = \frac{C_g V_g}{2e}$$

$$|n=1\rangle = |\downarrow\rangle_z$$

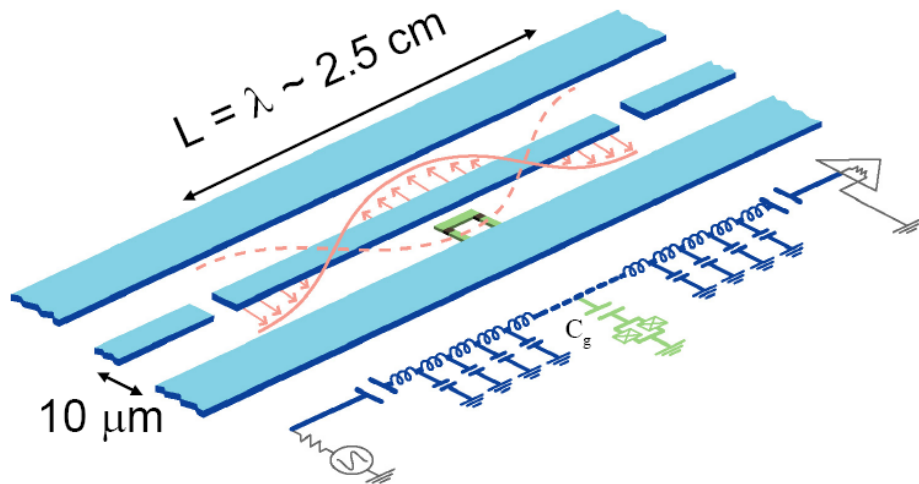
$$|n=0\rangle = |\uparrow\rangle_z$$

V_g Gate voltage

Φ_e External flux



A. Blais, et al. Phys. Rev. A, 69: 062320 (2004)

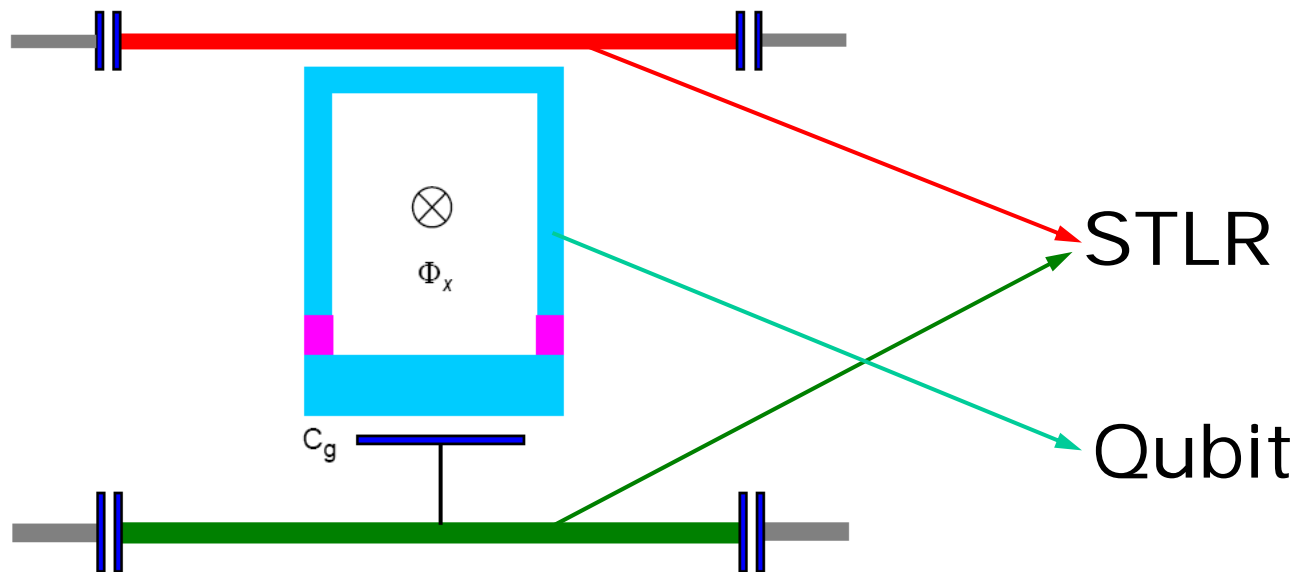


One voltage mode
is coupled to the
charge qubit

$$H = \hbar\omega\left(a^\dagger a + \frac{1}{2}\right) - \frac{E_c}{2}(1 - 2n_g)\sigma_z - E_J \cos\left(\frac{\pi\Phi_e}{\Phi_0}\right)\sigma_x$$

$$n_g = \frac{C_g(V_{DC} + V_q)}{2e}$$

$$V_q = V_0(a^\dagger + a)$$



$$H = \hbar\omega_a a^\dagger a + \hbar\omega_b b^\dagger b - \frac{1}{2}E_c(1 - 2n_g)\sigma_z - E_J \cos \frac{\pi(\Phi_e + \Phi_q)}{\Phi_0} \sigma_x + \frac{eC_g V_0}{C_\Sigma} (a^\dagger + a)\sigma_z$$



Expanding the effective Josephson coupling to the first order in Φ_q/Φ_0

$$H = \hbar\omega_a a^\dagger a + \hbar\omega_b b^\dagger b - \frac{1}{2}E_c(1 - 2n_g)\sigma_z - E_J \cos \frac{\pi\Phi_e}{\Phi_0} \sigma_x \\ + \hbar\lambda'_a(a^\dagger + a)\sigma_z - i\hbar\lambda'_b(b^\dagger - b)\sigma_x$$

In the eigenspace of the qubit

$$H = \hbar\omega_a a^\dagger a + \hbar\omega_b b^\dagger b - \frac{1}{2}\hbar\Omega\rho_z + \hbar\lambda_a(a^\dagger\rho_- + a\rho_+) \\ + i\hbar\lambda_b(b^\dagger\rho_- - b\rho_+)$$



Low temperature, Resonating

$$H = \hbar\Omega a^\dagger a + \hbar\Omega b^\dagger b - \frac{1}{2}\hbar\Omega\rho_z + \hbar\lambda_a(a^\dagger\rho_- + a\rho_+) + i\hbar\lambda_b(b^\dagger\rho_- - b\rho_+)$$

Initial State $|0\rangle|0\rangle|e\rangle$

State at time t

$$|\psi(t)\rangle = e^{-i\frac{\Omega t}{2}} \left[\cos \Lambda t |0\rangle|0\rangle|e\rangle + \sin \Lambda t (\sin \alpha |0\rangle|1\rangle|g\rangle - i \cos \alpha |1\rangle|0\rangle|g\rangle) \right]$$

$$\Lambda = \sqrt{\lambda_a^2 + \lambda_b^2} \quad \cos \alpha = \lambda_a/\Lambda \quad \sin \alpha = \lambda_b/\Lambda$$



When $\Delta t = \pi/2$

The entangled state of the two STLRs,
also the single-photon entangled state

$$|\Psi\rangle = \sin \alpha |0\rangle |1\rangle - i \cos \alpha |1\rangle |0\rangle$$



External biased flux $\Phi_e = 0$

$$H = \hbar\omega_a a^\dagger a + \hbar\omega_b b^\dagger b - \frac{1}{2}E_c(1 - 2n_g)\sigma_z - E_J \cos \frac{\pi(\Phi_e + \Phi_q)}{\Phi_0} \sigma_x \\ + \frac{eC_g V_0}{C_\Sigma} (a^\dagger + a)\sigma_z$$

Expanding the effective Josephson coupling to the second order in Φ_q/Φ_0

$$H_N = \hbar\omega_a a^\dagger a + \hbar\omega_b b^\dagger b - \frac{1}{2}\hbar\Omega\rho_z + \hbar g_a (a^\dagger \rho_- + a \rho_+) \\ + \hbar g_b (b^{\dagger 2} \rho_- + b^2 \rho_+)$$

three-body nonlinear interaction Hamiltonian



$$H_N = \hbar\omega_a a^\dagger a + \hbar\omega_b b^\dagger b - \frac{1}{2}\hbar\Omega\rho_z + \hbar g_a (a^\dagger \rho_- + a \rho_+) + \hbar g_b (b^{\dagger 2} \rho_- + b^2 \rho_+)$$

Large detuning

$$\begin{aligned} |\Delta_a| &= |\Omega - \omega_a| \gg G \\ |\Delta_b| &= |\Omega - 2\omega_b| \gg G \end{aligned} \quad G = \sqrt{g_a^2 + g_b^2}$$

Qubit: nonlinear media

Canonical Transformation $H_S = e^{-S} H e^S$

$$S = \frac{g_a}{\Delta_a} (a^\dagger \rho_- - a \rho_+) + \frac{g_b}{\Delta_b} (b^{\dagger 2} \rho_- - b^2 \rho_+)$$



Keeping the qubit in the ground state, the effective Hamiltonian of the two STLRs reads

$$H_S = \hbar\omega_a a^\dagger a + \hbar\omega_b b^\dagger b - \frac{1}{2}\hbar g_a g_b \left(\frac{1}{\Delta_a} + \frac{1}{\Delta_b} \right) (b^{\dagger 2} a + a^\dagger b^2)$$

If $\omega_a = 2\omega_b = 2\omega$

In the interaction picture

$$H_I = \hbar\kappa (b^{\dagger 2} a + a^\dagger b^2)$$

$\kappa = -g_a g_b / \Delta$ Depends on the frequency and is tunable



In the parametric approximation

$$H_I = \hbar\kappa\beta (b^{\dagger 2}e^{-i\phi} + e^{i\phi}b^2)$$

β : Amplitude of the pump field

ϕ : phase of the pump field

Evolution operator $U(t) = e^{-i\kappa\beta t(b^{\dagger 2}e^{-i\phi} + e^{i\phi}b^2)}$



Squeezing operator $S(\xi) = e^{-i\frac{\xi}{2}(b^{\dagger 2}e^{-i\phi} + b^2e^{i\phi})}$



Setting the phase $\phi = \pi/2$

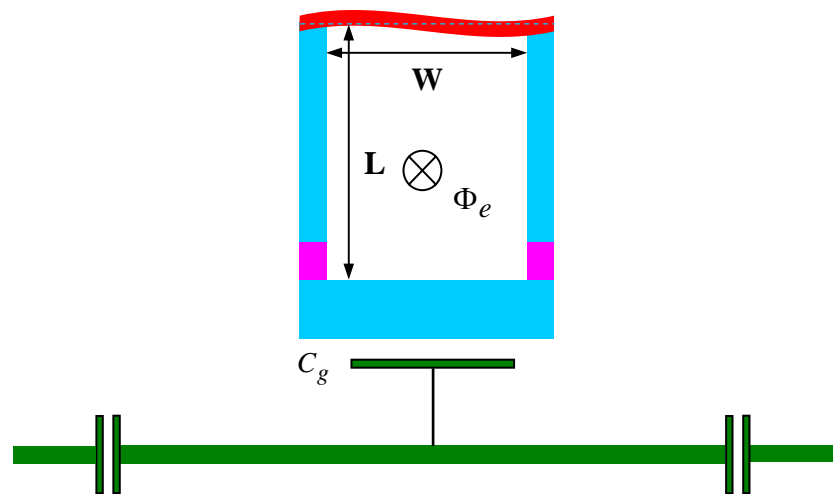
The two conjugate operators

$$X_1 = \frac{1}{2} (b + b^\dagger), X_2 = \frac{1}{2i} (b - b^\dagger)$$

The variances of the two operators become

$$\Delta X_1 = \sqrt{\langle X_1^2 \rangle - \langle X_1 \rangle^2} = \frac{e^{-\xi}}{2}$$

$$\Delta X_2 = \sqrt{\langle X_2^2 \rangle - \langle X_2 \rangle^2} = \frac{e^{\xi}}{2}$$



A nanomechanical resonator is fabricated as one part of the SQUID. The effective area of the SQUID is

$$S = W(L + x)$$

$x = \sqrt{\hbar/(2M\omega_b)}(b^\dagger + b)$ is the displacement operator

The effective flux threading the SQUID becomes

$$\Phi_e = \Phi_e^0 + BWx$$

Generation of squeezed states of nanomechanical resonator using three-wave mixing, WY Huo and GLL, APL, 92, 133102 2008



The Hamiltonian of the system

$$H = \hbar\omega_a a^\dagger a + \hbar\omega_b b^\dagger b - \frac{1}{2}E_c(1 - 2n_g)\sigma_z - E_J \cos \frac{\pi(\Phi_e^0 + BWx)}{\Phi_0} \sigma_x + \frac{eC_g V_0}{C_\Sigma} (a + a^\dagger) \sigma_z$$

Following the above derivation.....

In interaction picture

$$H_I(t) = \hbar\kappa\beta(b^{\dagger 2}e^{-i\phi} + b^2e^{i\phi})$$



Squeezing operator

$$S(\xi) = e^{-i\frac{\xi}{2}(b^{\dagger 2}e^{-i\phi} + b^2e^{i\phi})} = e^{-i\kappa\beta t(b^{\dagger 2}e^{-i\phi} + b^2e^{i\phi})}$$

$$\phi = \pi/2 \quad \Delta x = \sqrt{\langle x^2 \rangle - (\langle x \rangle)^2} = x_0 e^{-\xi}$$
$$\Delta p = \sqrt{\langle p^2 \rangle - (\langle p \rangle)^2} = p_0 e^{\xi}$$

Considering the influence of fluctuation

$$\Delta x = x_0 \sqrt{e^{-2\xi} + \left(\frac{\gamma t}{2}\right) e^{2\xi}}$$

γ is the linewidth, ξ is the squeezing parameter



Choosing the following experimental parameters

$$E_J/2\pi = 4 \text{ GHz}, \Omega/2\pi = 10 \text{ GHz},$$

$$\omega_a/2\pi = 2\omega_b/2\pi = 3 \text{ GHz},$$

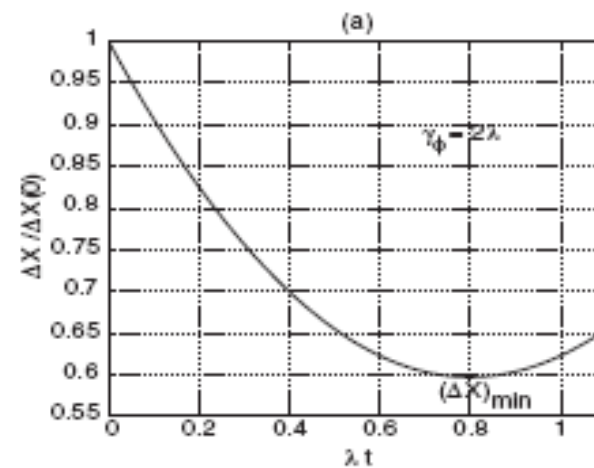
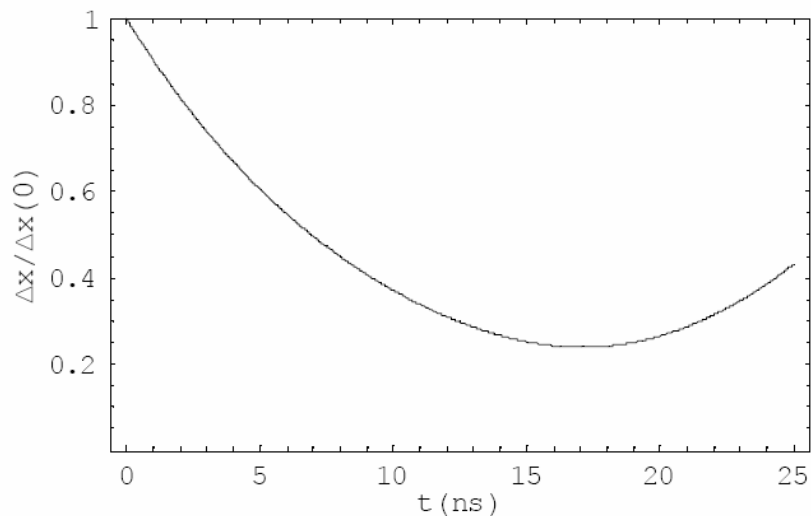
$$C_g/C_\Sigma = 0.1, B = 0.2 \text{ T}, W = 5 \text{ } \mu\text{m},$$

$$V_0 = 2 \text{ } \mu\text{V}, x_0 = 5 \times 10^{-13} \text{ m},$$

$$Q = 10^5, P = 8 \text{ W}, \tau = 0.1 \text{ ns}$$

nonlinear coupling constant $\kappa/2\pi \approx 4 \text{ Hz}$

Effective Rabi frequency $\Omega_p/2\pi \approx 16 \text{ MHz}$



$\Delta x / \Delta x(0)$ minimum $\sim 24\%$

XX ZHou et
al PRL, 97,
267201(2006)

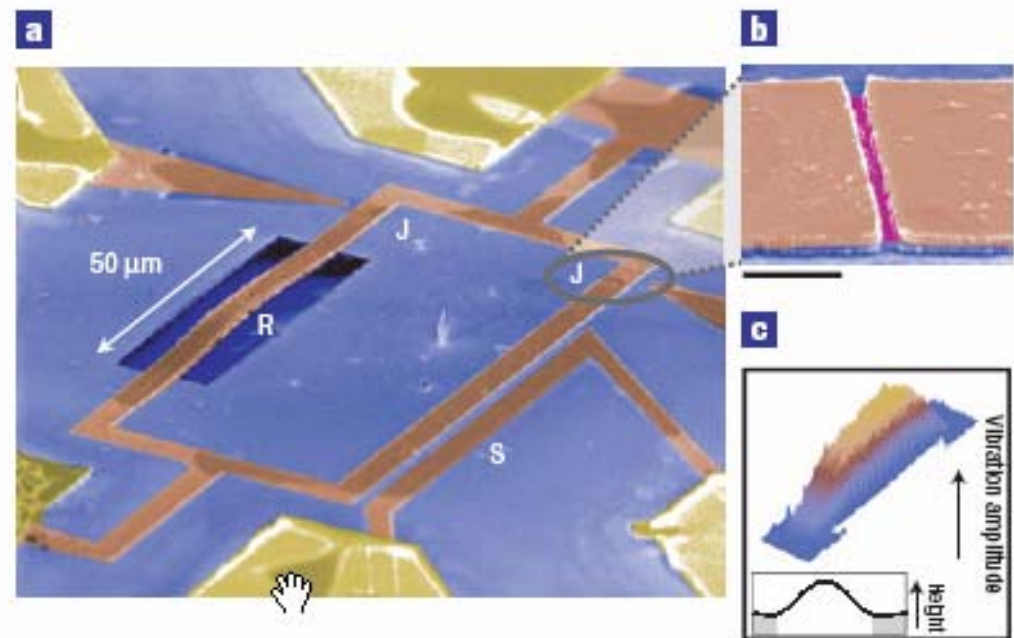
Motion detection of a micromechanical resonator embedded in a d.c. SQUID

S. ETAKI^{1,2*}, M. POOT¹, I. MAHBOOB², K. ONOMITSU², H. YAMAGUCHI² AND H. S. J. VAN DER ZANT^{1*}

¹Kavli Institute of Nanoscience, Delft University of Technology, Post Office Box 5046, 2600 GA Delft, Netherlands

²NTT Basic Research Laboratories, NTT Corporation, Atsugi-shi, Kanagawa 243-0198, Japan

*e-mail: s.etaki@tudelft.nl; h.s.j.vanderzant@tudelft.nl

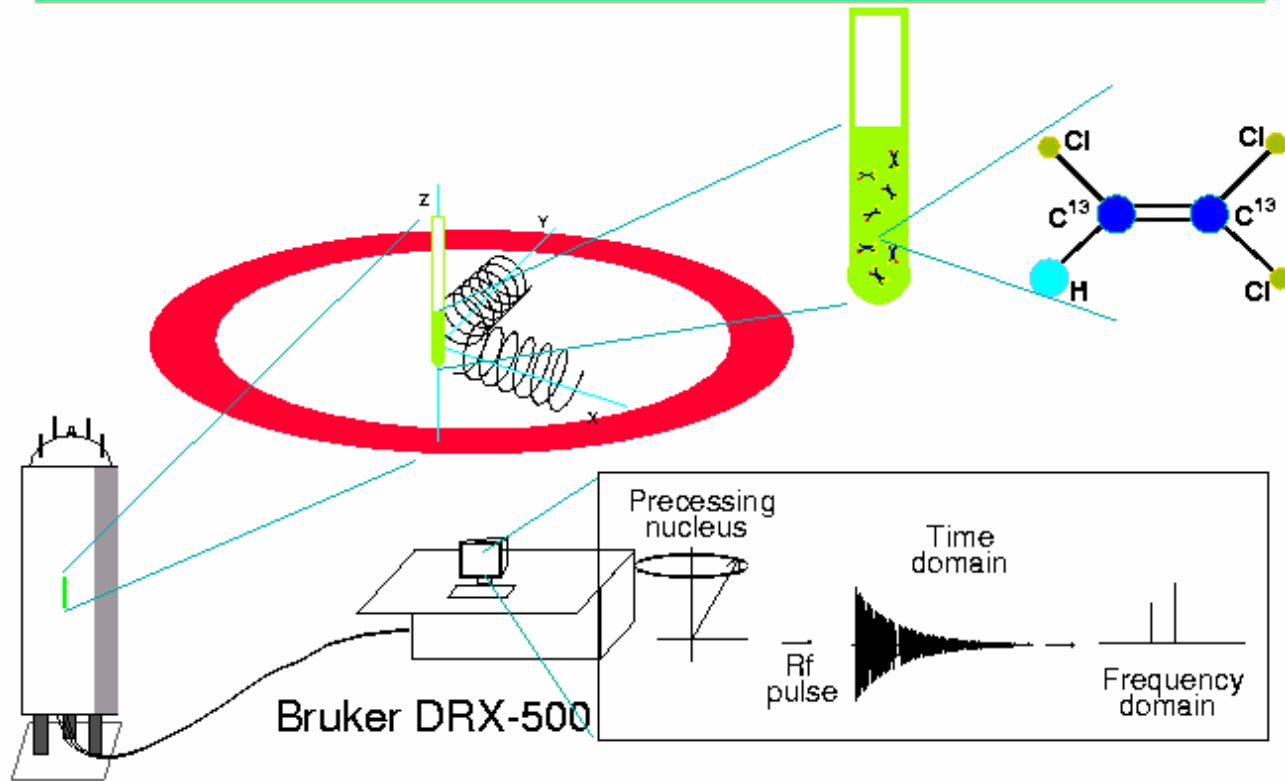


达到比量子极限低**36**倍的位置
探测

核磁共振量子计算

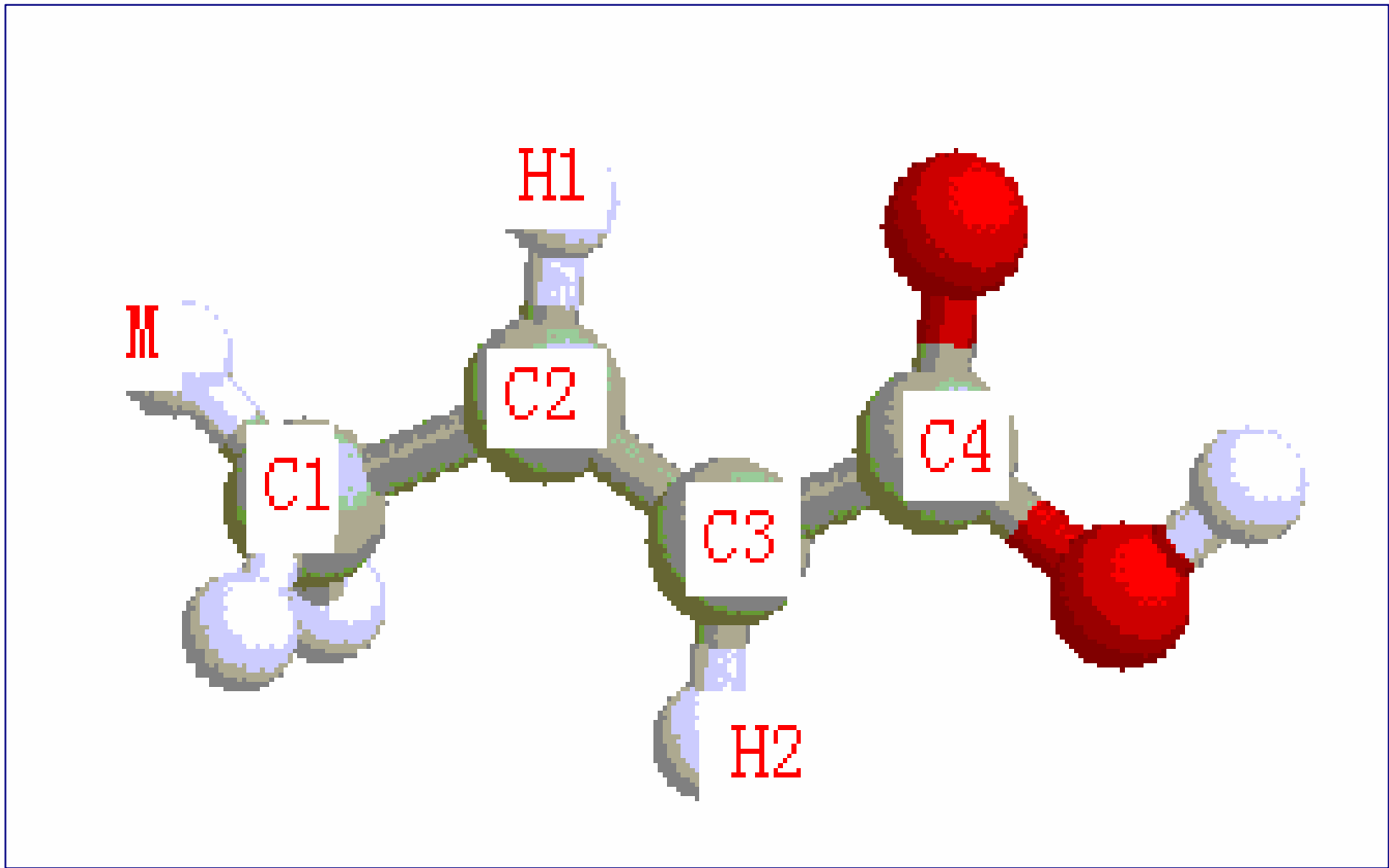
量子计算机的硬件---NMR实验

NMR System Overview



Experimental realization in a 7 qubit NMR QC

(G.L. Long and L. Xiao, J Chem Phys 2003)



^{13}C labeled crotonic acid, 7 qubits system.

An algorithmic benchmark for quantum information processing

E. Knill^{*}, R. Laflamme^{*}, R. Martinez^{*} & C.-H. Tseng[†]

^{*} *Los Alamos National Laboratory, MS B265, Los Alamos, New Mexico 87545, USA*

[†] *Department of Nuclear Engineering, MIT, Cambridge, Massachusetts 02139, USA*

Nature, 404, 368 (2000)

Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance

Lieven M. K. Vandersypen^{*†}, Matthias Steffen^{*†}, Gregory Breyta^{*}, Costantino S. Yannoni^{*}, Mark H. Sherwood^{*} & Isaac L. Chuang^{*†}

^{*} *IBM Almaden Research Center, San Jose, California 95120, USA*

[†] *Solid State and Photonics Laboratory, Stanford University, Stanford, California 94305-4075, USA*

Nature, 414, 883 (2001)

NMR experimental realization of seventh-order coupling transformations and the seven-qubit modified Deutsch-Jozsa algorithm

Daxiu Wei, Jun Luo, Xiaodong Yang, Xianping Sun, Xizhi Zeng, Maili Liu, Shangwu Ding, and Mingsheng Zhan

武汉物理数学所组
Quant-ph/0301041,
2003

量子计算与量子通信

龙桂鲁

清华大学物理系, 北京100084

量子信息与测量重点实验室

gllong@tsinghua.edu.cn

2008年11月13日

内容提要

- 量子密码通讯
- 量子纠错
- 量子密集编码
- 量子秘密共享

量子密码通讯

密码学:

中国:公元前11世纪周武王使用阴符

大胜克敌 破军擒将 降城得邑 失利丧土

长一尺 长九寸 长八寸 长三寸

密钥不能重复使用:

德国人的教训: 1918年第一次世界大战中

棋盘密钥, 德国人6月3日使用了6月1日的密钥。挽救了巴黎。

量子密码通讯的提出

1979年，美国的Wiesner提出设想。

1984年，Bennett, Brassard, BB84协议。

1992年，Bennett, B92协议。

1991年，Ekert, EPR协议。

现有几十种量子密钥传递方案。

经典密码通讯

M : 信息明文; G_k : 数据变换; C : 密文;

K : 参数, 密钥。

$$G_K(M) = C$$

$$G_K^{-1}(C) = M$$

经典密码方案面临的问题

- 对称密码必须经常更换和传送密钥，增加了被窃听的危险。
- 日益增强的计算机使很复杂的密码也不断被破译。
- **Shor**大数因子化算法（1995年）严重威胁**RSA**公钥密码体制。

Vernam一次性便笺密码

- 唯一安全的经典密码
- 一套随机的0,1的系列
- 密钥和明文一样长
- 一次性便笺式密码较长，经常生成、传送和保存数量庞大的数据库作为密码本。

Example of (Quantum) Cryptography

- **Alice** and **Bob** generate shared key material (**random numbers**) using **single photon transmissions** of quantum cryptography over 14 km of optical fiber
- e.g. use of key for **“one-time pad” encryption/decryption of short messages**:

Sample of key material

B	00001010	01111111	01010111	01011010	00010011
A	00001010	01111111	01010111	01011010	00010001
B	00000011	11100111	11011111	00000100	00001100
A	00000011	11100111	11011111	00000100	00001100
B	10110100	11101110	01110000	10100101	11111001
A	10110100	11101110	01110000	10100101	11111001
B	00110100	01001000	10000000	10111111	01010101
A	00110100	01001000	10000000	10111111	01010101
B	10111111	00000000	00100010	01011000	11011010
A	10111011	01000000	00100010	01011000	11011010

Alice encrypts

Secure communications are becoming more and more important, not only in their traditional arenas, but in everyday life.

plaintext = “m”

ASCII = 10110110
 \oplus key = 10010010
 00100100

Eve (enemy cryptanalyst) sees

☐>%o²,ŪC_@☐{ĚöOsu”Ā*i{ĂùG”
 ÇcwŪú÷Éj☐×.☐·w0Q!-ókâwörŠĀj
 óR☐ÆbÀOđšçt‘v☐Ø☐»☐f+±âÉ9☐
 ĀšÑ·¹+Ī4,,Īa3ĪĚbeEQù☐+|•☐GáŪ
 X̄J,-☐(ĒÍ☐IH^

ciphertext = “\$”

Bob decrypts

Secure communications are becoming more and more important, not only in their traditional arenas, but in everyday life.

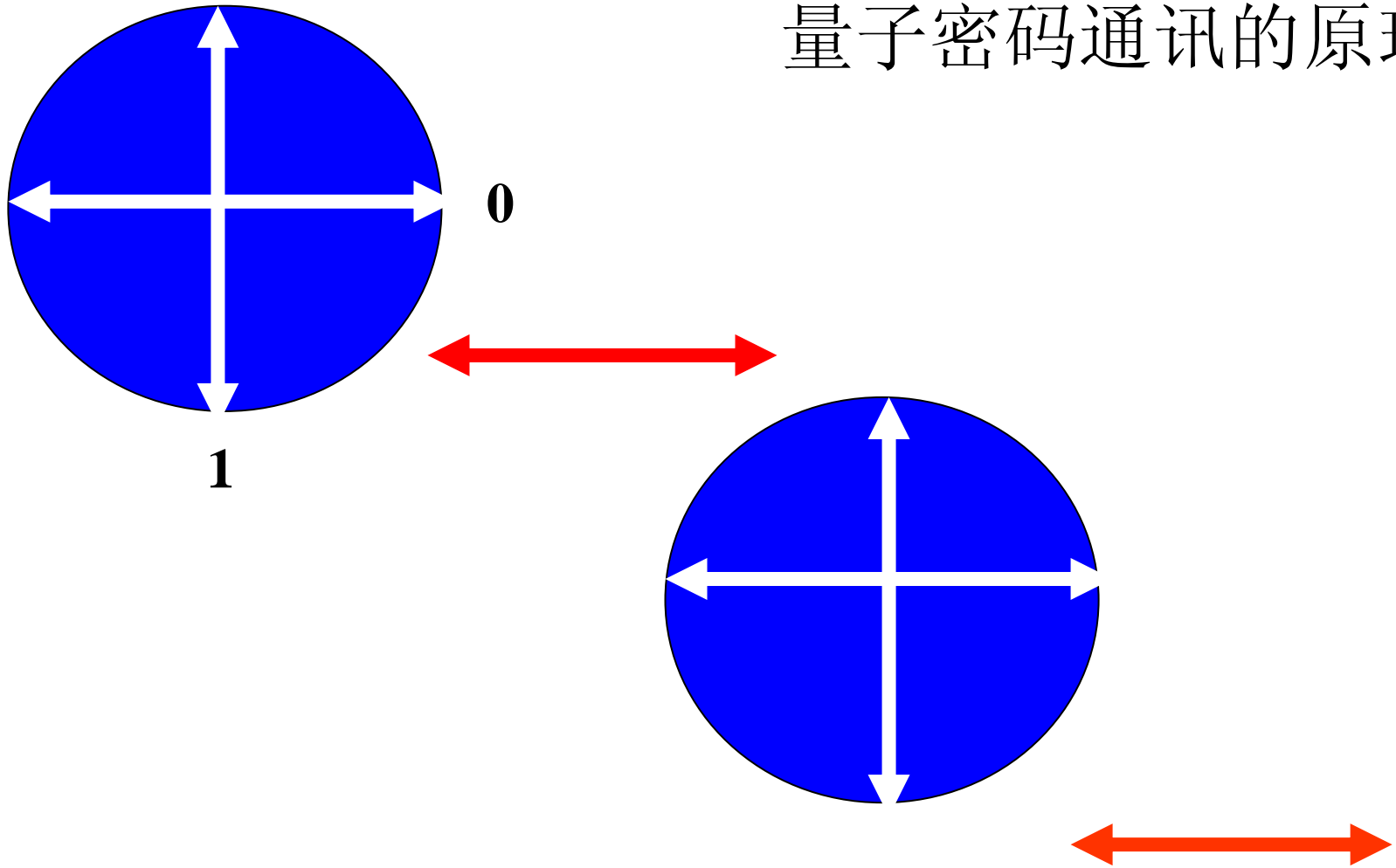
ASCII = 01000100
 \oplus key = 10010010
 10110110

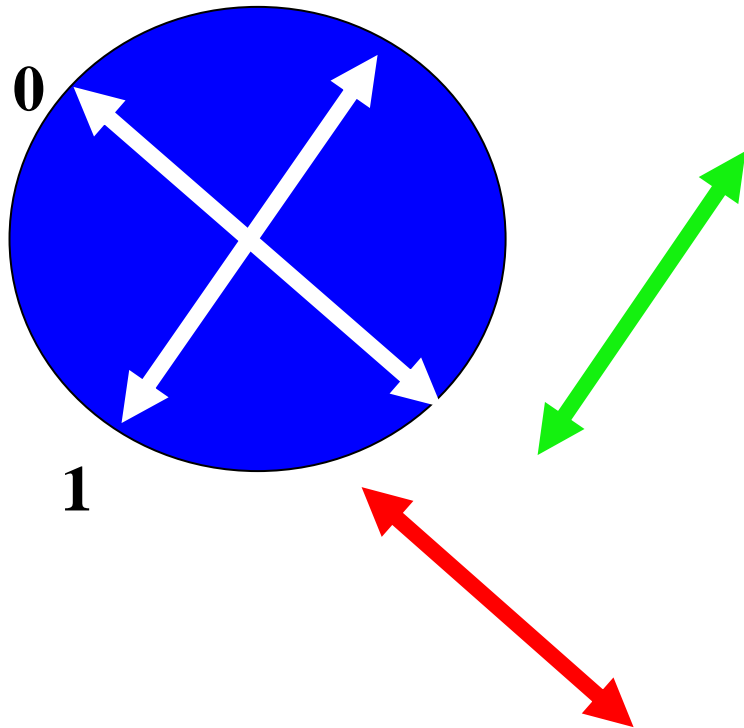
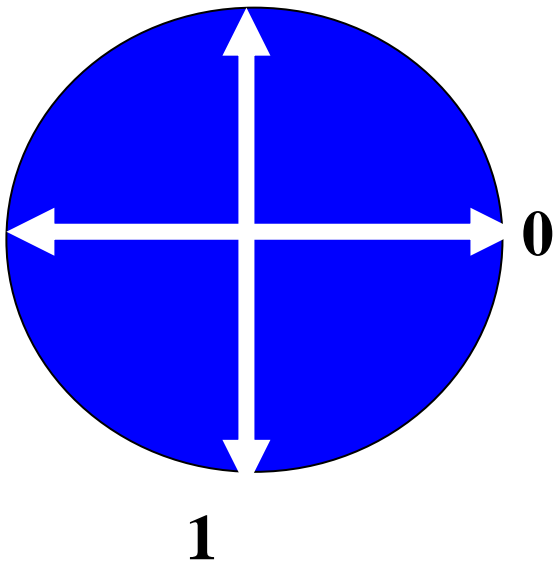
decrypted = “m”

-
- 利用量子力学的测量原理产生和传递密钥
 1. 安全性很高，任何窃听的企图都会被合法用户发现；
 2. 可以直接用作一次性便笺密钥；
 3. 如果可以确定密钥的绝对安全性，可以利用这些密钥产生更长的密钥。

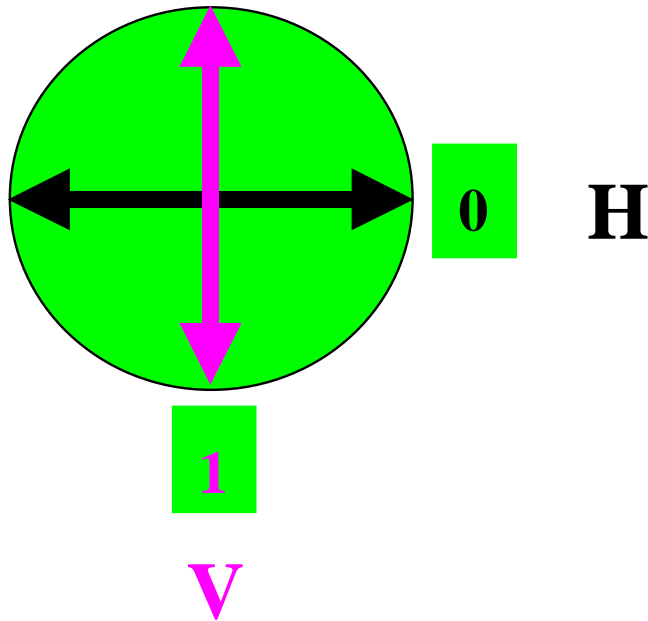
单光子编码

量子密码通讯的原理



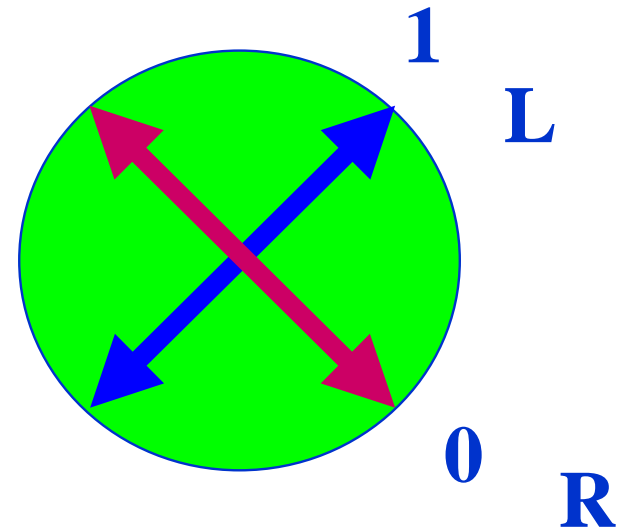
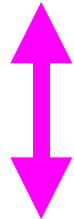


Bennett-Brassard 1984 protocol (BB84)



$$|H\rangle = |0\rangle$$

$$|V\rangle = |1\rangle$$

































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

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



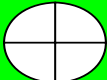
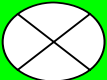
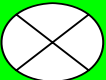
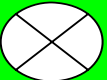
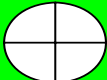
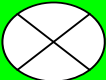
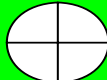
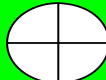
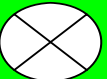
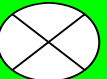
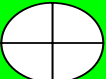
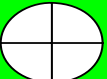
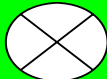
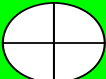
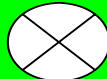
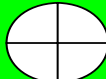
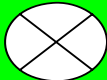
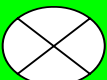
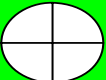
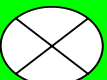
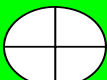
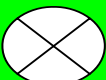
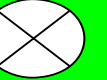
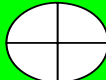
BB84 protocol without Eve present

Alice	         
	         
	1 0 0 1 1 0 0 1 0 1

Bob	         
	1 0 1 1 1 0 0 0 0 0

Raw Key	0 1 1 0 0 0
---------	-------------

BB84 Protocol With Eve Present

Alice								
	↓	↖	↖	↗	→	↗	↓	→
	1	0	0	1	1	0	1	0
Eve								
	1	0	1	0	1	1	0	0
Bob								
	1	<u>0</u>	0	<u>1</u>	1	<u>1</u>	0	<u>0</u>

channel and a classical public channel. Normally single photons are being used to carry the information and the quantum

of their key by an eavesdropper would be a reduction of the correlation between the values of their bits. Let us suppose,

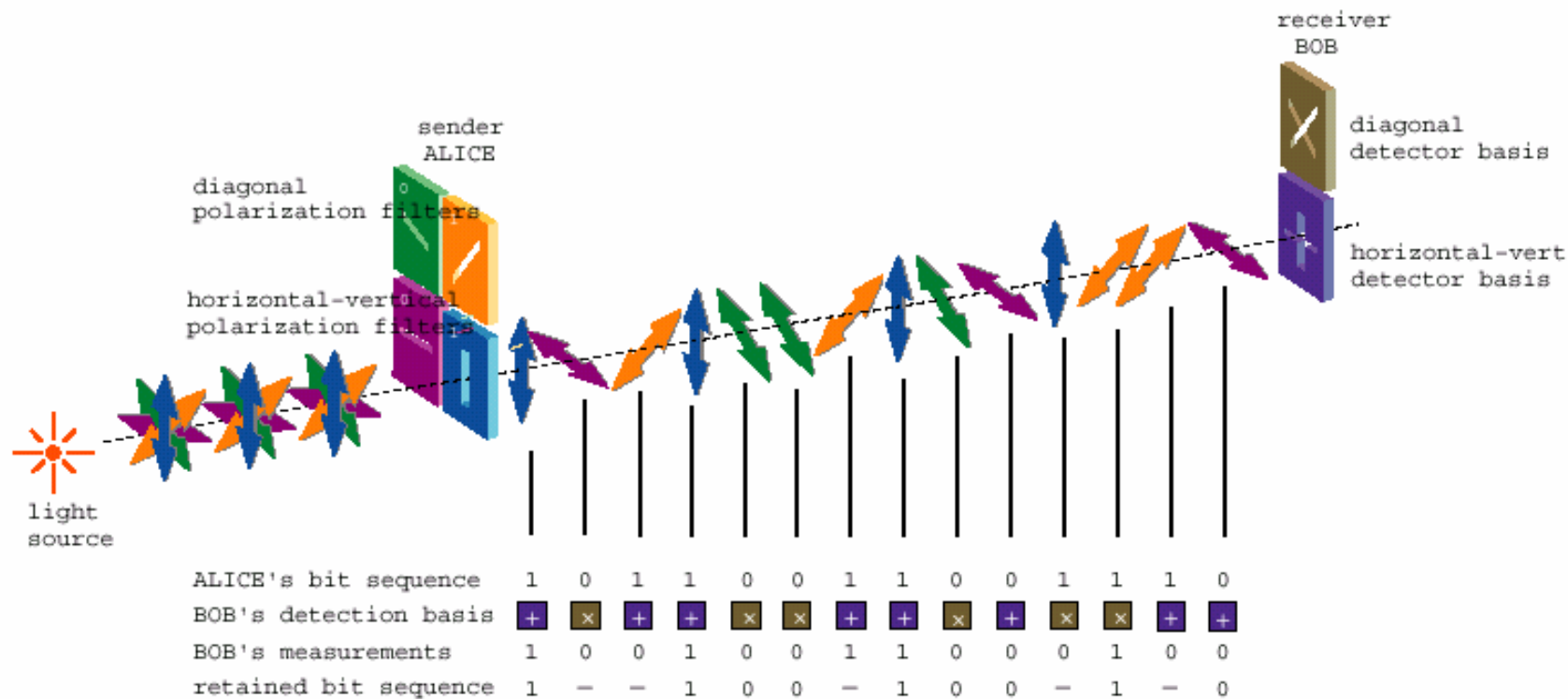
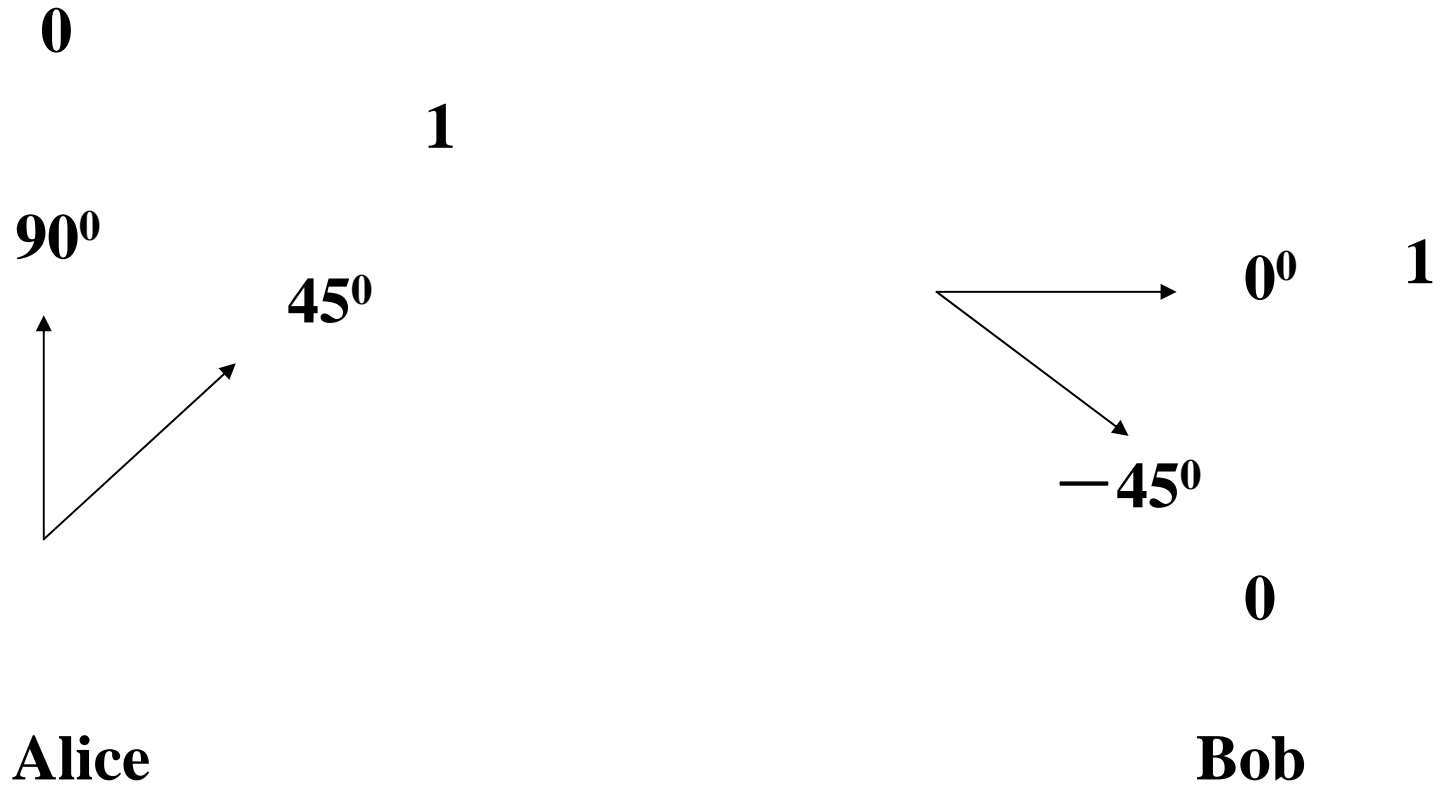


Fig. 1. The principle of QC according to the BB84 protocol. Alice sends down an optical fiber photons polarized randomly either horizontally, vertically, at $+45^\circ$, or at -45° (row 1), Bob randomly chooses one of his analyzer basis (row 2) and records his result (row 3). Then they compare the used basis and retain all results with compatible basis (row 4)

BB84 方案

B92 protocol



C. H. Bennett, Phys. Rev. Lett. 68, 3121 (1992)

Hwang-Koh-Han 1998 protocol

	N_k								N_k										
控制码	0	...	1	0	1	1	0	0	1	0	...	1	0	1	1	0	0	1	...
MB	\otimes	...	\oplus	\otimes	\oplus	\oplus	\otimes	\otimes	\oplus	\otimes	...	\oplus	\otimes	\oplus	\oplus	\otimes	\otimes	\oplus	...
Alice	
Bob	

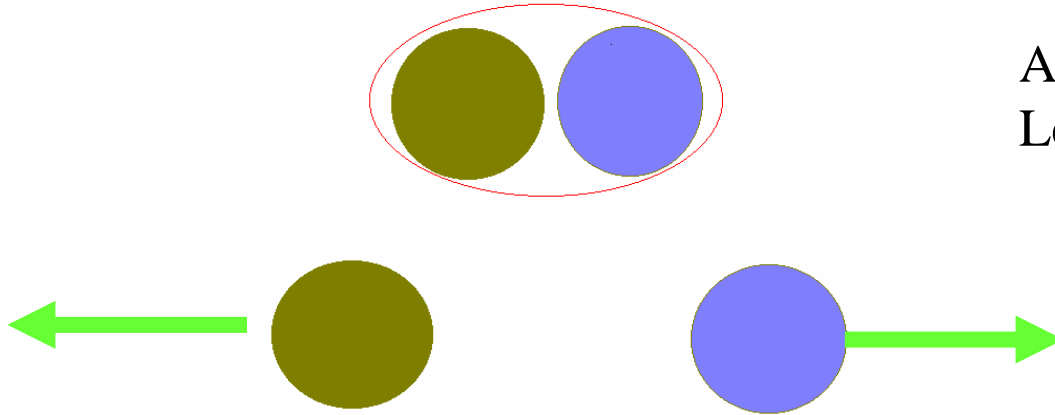
W.Y. Hwang, I.G. Koh and Y.D. Han,

Phys. Lett. A 244, 489 - 494 (1998)

清华大学龙桂鲁

Ekert 1991 protocol (Ekert 91)

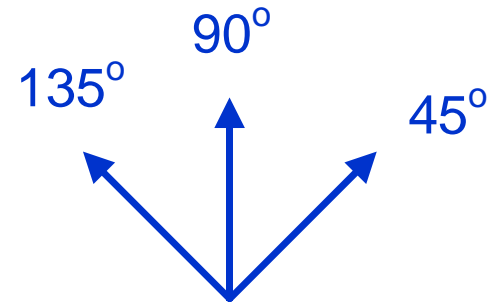
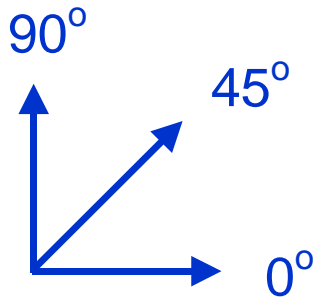
A.K. Ekert, Phys. Rev. Lett. 67, 661-663 (1991)



$$|\Phi^-\rangle_{AB} = \left(|\uparrow_A \downarrow_B\rangle - |\downarrow_A \uparrow_B\rangle \right)$$

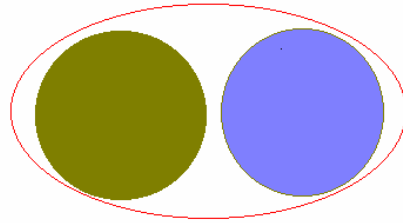
Alice

Bob



Bennett-Brassard-Mermin 1992 protocol (BBM92)

C.H. Bennett et al., Phys.
Rev. Lett. 68, 557-559 (1992)



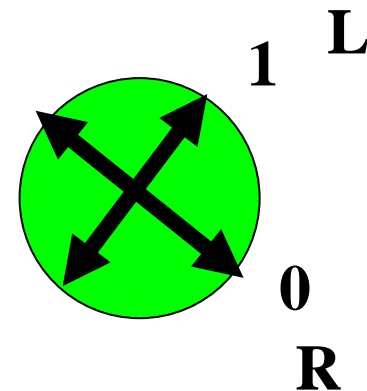
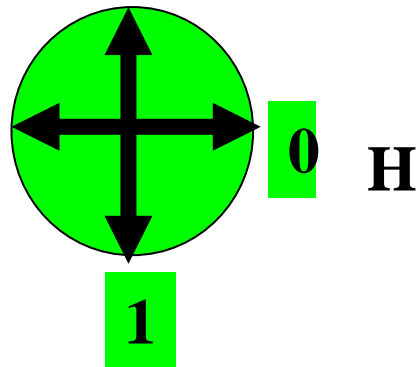
Alice



Bob

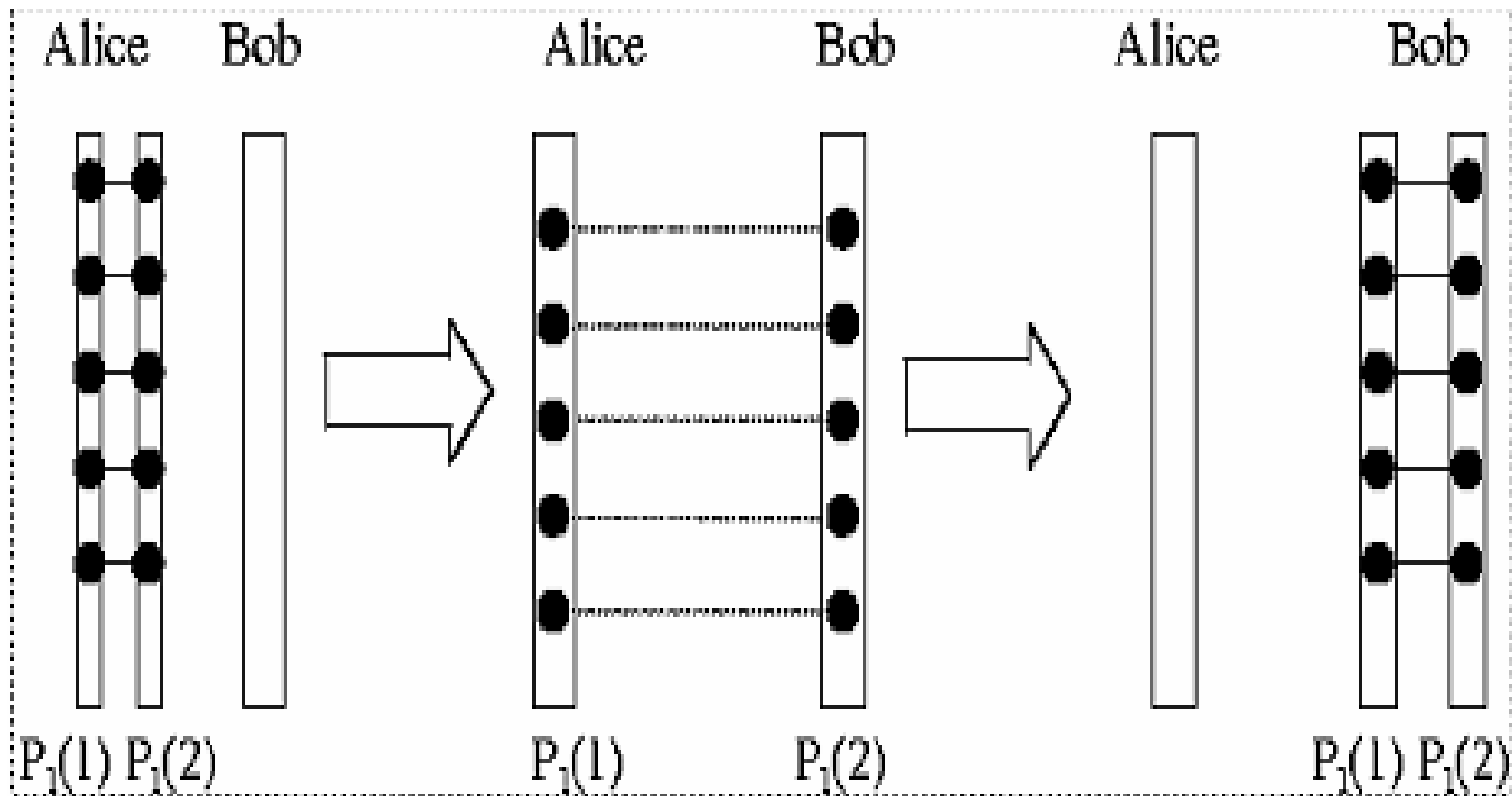
$$|\Phi^-\rangle_{AB} = \left(|\uparrow_A \downarrow_B\rangle - |\downarrow_A \uparrow_B\rangle \right)$$

Like BB84,
choose
randomly two
MBs



Long-Liu 2002 protocol

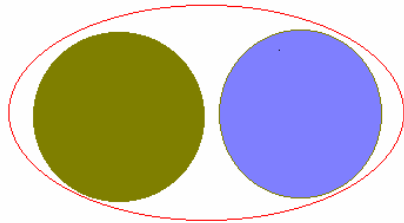
G L Long, X S Liu, Phys. Rev. A 65, 032302 (2002)



Deng-Long 2003 protocol (CORE)

Controlled **O**rder **R**earrangement **E**ncryption for quantum key distribution

F G Deng and G L Long, Phys. Rev. A 68, 042315 (2003).



EPR pair

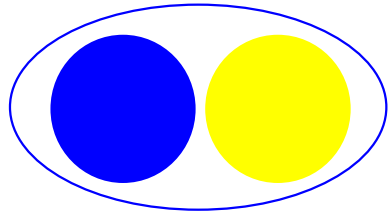
$$|\psi^-\rangle_{AB} = \frac{1}{\sqrt{2}} (|0\rangle_A |1\rangle_B - |1\rangle_A |0\rangle_B)$$

$$|\psi^+\rangle_{AB} = \frac{1}{\sqrt{2}} (|0\rangle_A |1\rangle_B + |1\rangle_A |0\rangle_B)$$

$$|\phi^-\rangle_{AB} = \frac{1}{\sqrt{2}} (|0\rangle_A |0\rangle_B - |1\rangle_A |1\rangle_B)$$

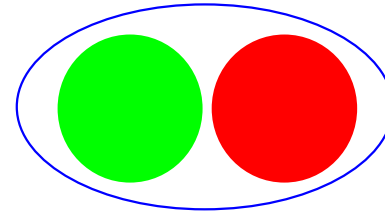
$$|\phi^+\rangle_{AB} = \frac{1}{\sqrt{2}} (|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B)$$

CORE c-1



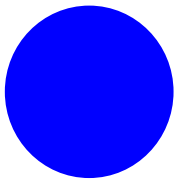
A_1 B_1

Pair A_1B_1

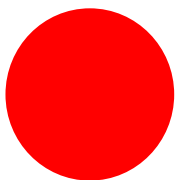


A_2 B_2

Pair A_2B_2



A_1



B_2

A_1 and B_2 from different pairs

$$\rho_{A_1B_2} = \bar{\rho}_{A_1} \otimes \bar{\rho}_{B_2} = \frac{1}{4} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

CORE 续-3

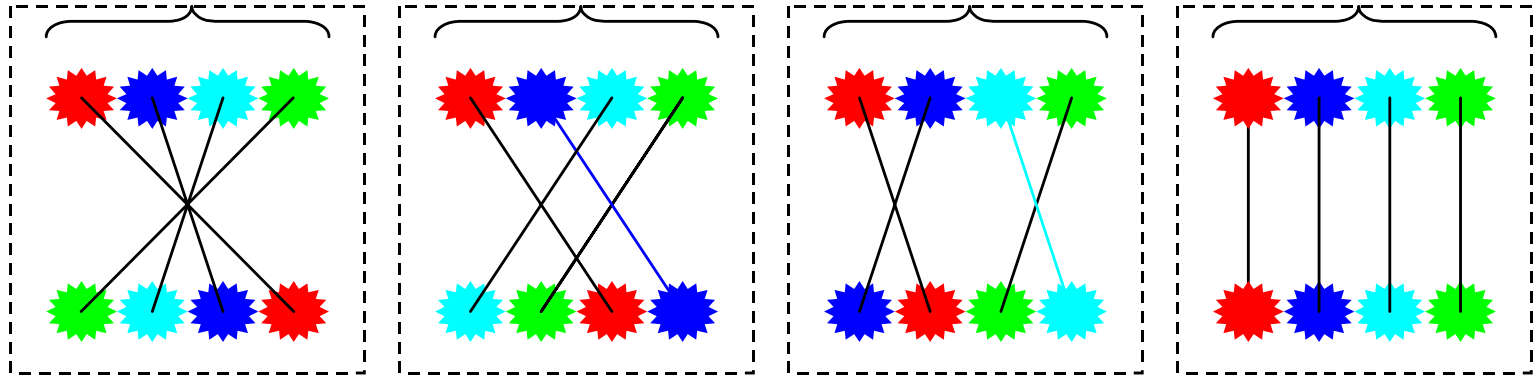
控制码:

11

10

01

00



顺序重排加密方式: E_3

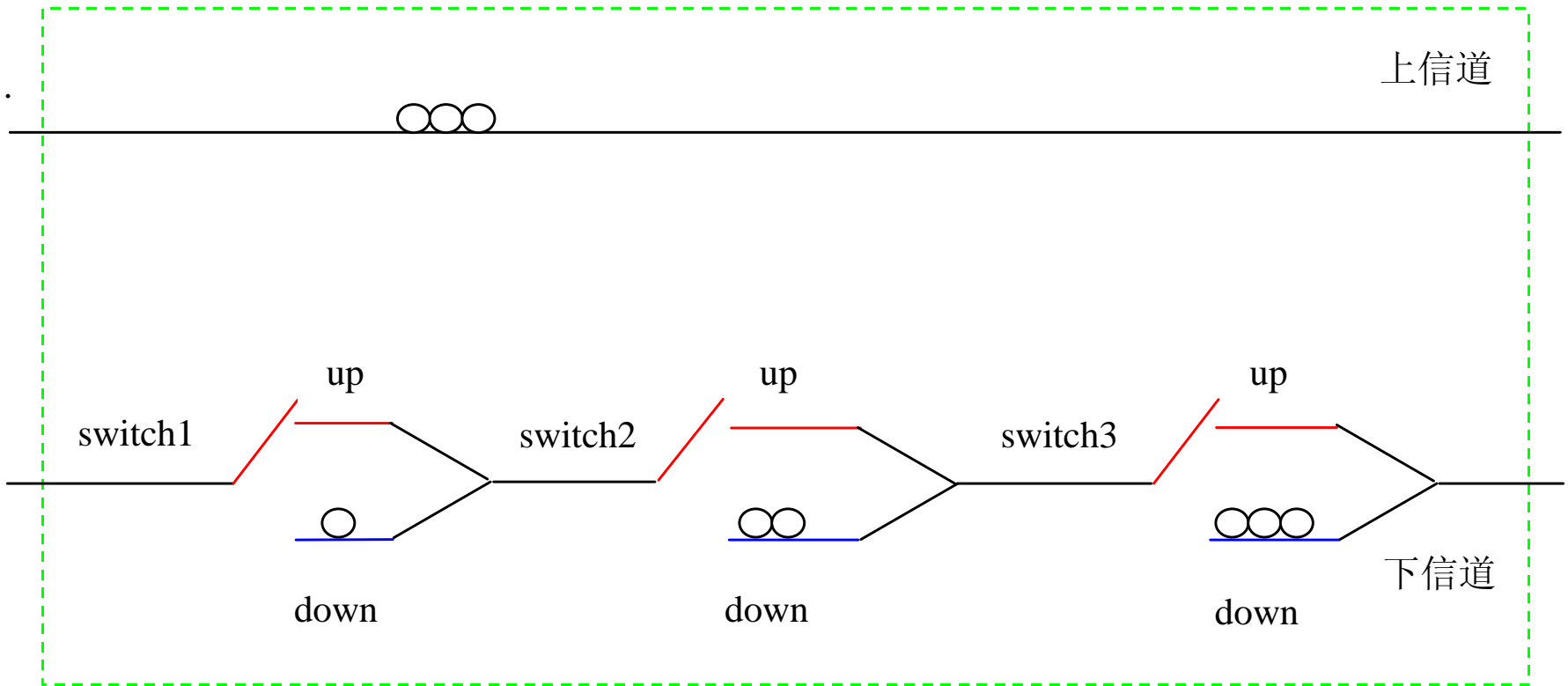
E_2

E_1

E_0

illustration of **CORE with 4 pairs** (order encryption/decryption)

CORE 续-4



Realization of CORE using optical delays

Quantum Secure Direct Communication

- Two requirements:
- Alice and Bob can exchange secret information directly without first establishing a key and then send the information through a classical channel using the one-time-pad.
- The secret information can not be leaked even though Eve can intercept.

Quantum secure direct communication

Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block

F G Deng, G L Long and X S Liu, Phys. Rev. A 68, 042317 (2003).

初态: $|\psi^-\rangle_{AB} = \frac{1}{\sqrt{2}} (|0\rangle_A |1\rangle_B - |1\rangle_A |0\rangle_B)$

coding

operation

00 $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$|\psi^-\rangle_{AB} = \frac{1}{\sqrt{2}} (|0\rangle_A |1\rangle_B - |1\rangle_A |0\rangle_B)$

01 $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

$|\psi^+\rangle_{AB} = \frac{1}{\sqrt{2}} (|0\rangle_A |1\rangle_B + |1\rangle_A |0\rangle_B)$

10 $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

$|\phi^-\rangle_{AB} = \frac{1}{\sqrt{2}} (|0\rangle_A |0\rangle_B - |1\rangle_A |1\rangle_B)$

11 $i\sigma_y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$

清华大学 $|\phi^+\rangle_{AB} = \frac{1}{\sqrt{2}} (|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B)$

Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block

Fu-Guo Deng,^{1,2} Gui Lu Long,^{1,2,3,4} and Xiao-Shu Liu^{1,2}

¹*Department of Physics, Tsinghua University, Beijing 100084, People's Republic of China*

²*Key Laboratory For Quantum Information and Measurements, Beijing 100084, People's Republic of China*

³*Center for Atomic and Molecular NanoSciences, Tsinghua University, Beijing 100084, People's Republic of China*

⁴*Institute of Theoretical Physics, Chinese Academy of Sciences, Beijing 100080, People's Republic of China*

(Received 18 June 2003)

A protocol for quantum secure direct communication using blocks of Einstein-Podolsky-Rosen (EPR) pairs is proposed. A set of ordered N EPR pairs is used as a data block for sending secret message directly. The ordered N EPR set is divided into two particle sequences, a checking sequence and a message-coding sequence. After transmitting the checking sequence, the two parties of communication check eavesdropping by measuring a fraction of particles randomly chosen, with random choice of two sets of measuring bases. After insuring the security of the quantum channel, the sender Alice encodes the secret message directly on the message-coding sequence and sends them to Bob. By combining the checking and message-coding sequences together, Bob is able to read out the encoded messages directly. The scheme is secure because an eavesdropper cannot get both sequences simultaneously. We also discuss issues in a noisy channel.

DOI: 10.1103/PhysRevA.68.0423XX

PACS number(s): 03.67.Hk, 03.65.Ud, 03.67.Dd, 03.65.Ta

TWO-STEP QUANTUM DIRECT COMMUNICATION . . .

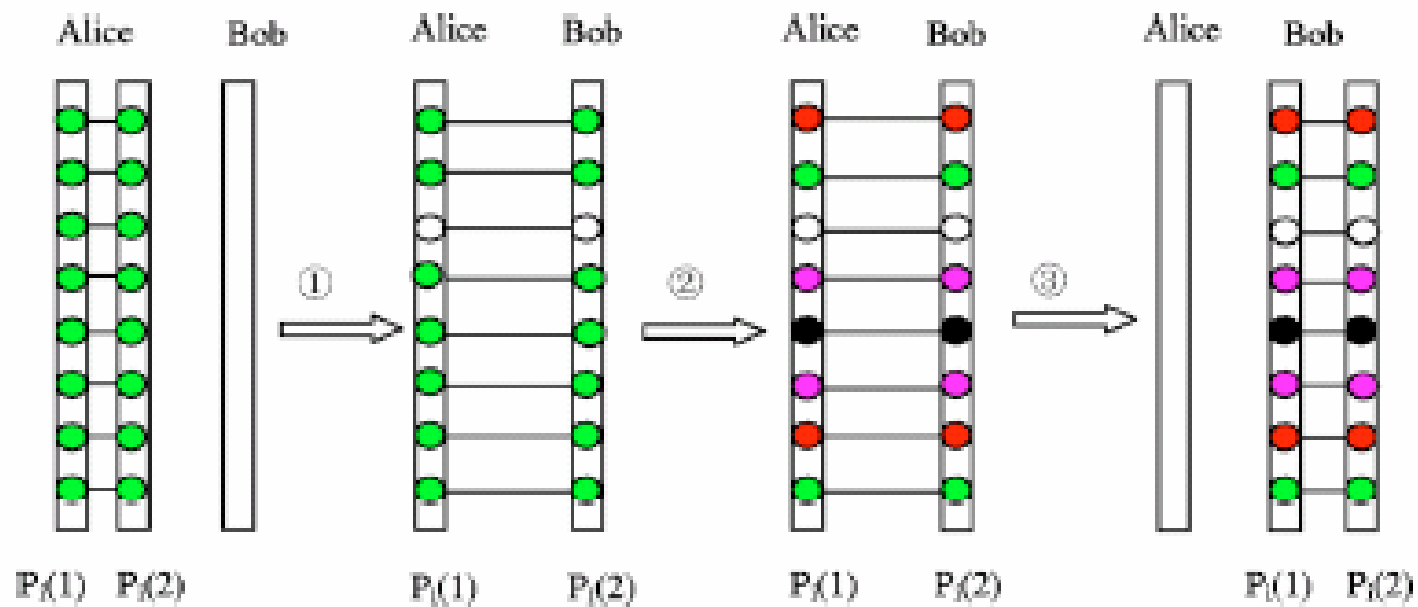


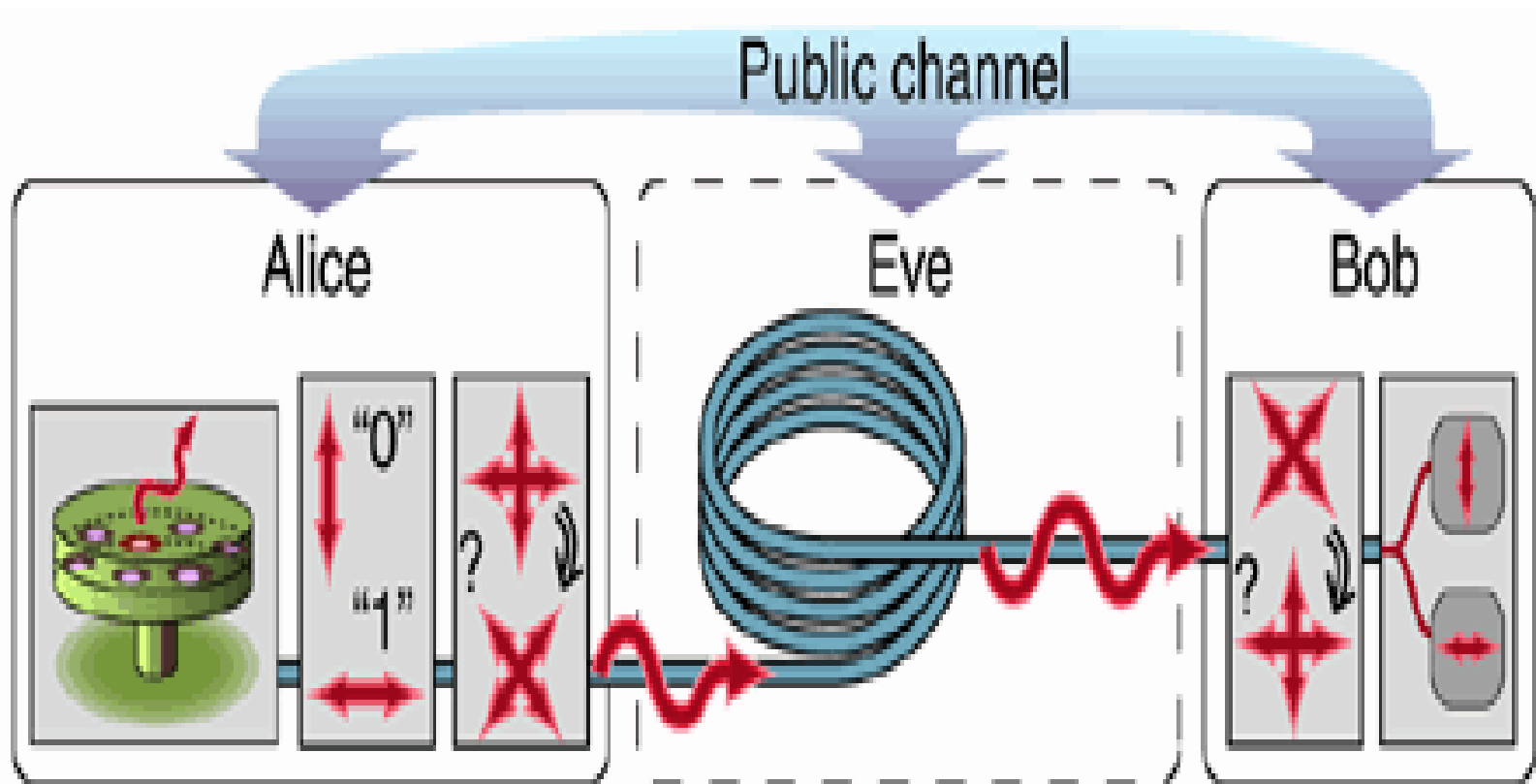
FIG. 1. Illustration of the QSDC protocol. Alice prepares the ordered N EPR pair in the same quantum states and divides them into two partner-particle sequences. She first sends one sequence to Bob for checking eavesdropping by choosing a fraction of particles to measure with randomly chosen measuring basis. If the quantum line is secure, Alice encodes the partner EPR pairs, using four unitary operations, the secret messages and sends the second sequence to Bob.

最新的几个量子通讯方案:

Efficient multiparty quantum-secret-sharing schemes, Li Xiao, Gui Lu Long, Fu-Guo Deng, and Jian-Wei Pan, PHYSICAL REVIEW A 69, 052307 (2004)

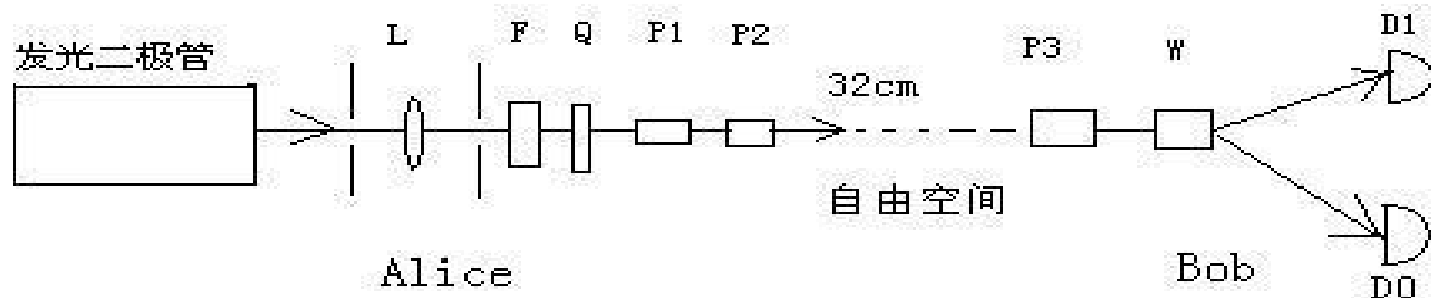
Secure direct communication with a quantum one-time pad, Fu-Guo Deng and Gui Lu Long, Physical Review A 69, 052319 (2004)

Bidirectional quantum key distribution protocol with practical faint laser pulses, F G Deng and G L Long, Phys. Rev. A70, 012311(2004)



第一次量子密钥分发实验

- 1989年，Bennett 和 Brassard:



量子密码通讯的实验进展

- 1) 1993, 英国国防部最早使用光纤进行了量子密钥实验。脉冲 半导体激光器, 光子波长 1.3micro-m , 光纤传输 10km 。探测器为低温冷却的锗雪崩二极管。
- 2) 1995, 英国通讯实验室, 光纤传输 10km (误码率为 1.5%), 30km (4%)。有效比特传输率分别为每秒 700 和 260 。
- 3) 1993, 瑞士日内瓦大学在 1.1km 长的光纤中传输 1.3 micro-m 波长光子, 误码率仅为 0.54% 。

量子密码通讯的实验进展 (续)

- 4) 1995, 在日内瓦湖底铺设底23km长民用光通信光缆中进行了表演, 误码率为3.4%。
- 5) Johns Hopkins: 1995, 1km光纤, 0.4%; 1996, 200m自由空间, 2%, 每秒发送比特数1k。
- 6) LANL:
1995, 1.3微米, B92协议, 205m自由空间;
2000, 500m自由空间, 48km光纤;
2000, 1.6km自由空间。
- 7) 西方国家的目标是在近5年之内实现量子密码实用化。
目前的技术极限是光纤传输70km。

Daylight Quantum Key Distribution over 1.6 km

W. T. Buttler, R. J. Hughes, S. K. Lamoreaux, G. L. Morgan, J. E. Nordholt, and C. G. Peterson

University of California, Los Alamos National Laboratory, Los Alamos, New Mexico 87545

(Received 14 January 2000)

Quantum key distribution (QKD) has been demonstrated over a point-to-point 1.6-km atmospheric optical path in full daylight. This record transmission distance brings QKD a step closer to surface-to-satellite and other long-distance applications.

PACS numbers: 03.67.Dd, 03.65.Bz, 42.50.Ar, 42.79.Sz

Quantum cryptography was introduced in the mid-1980s [1] as a new method for generating the shared, secret random number sequences, known as cryptographic keys, that are used in crypto-systems to provide communications security (for a review, see [2]). The appeal of quantum cryptography (or more accurately, quantum key distribution, QKD) is that its security is based on laws of nature and information-theoretically secure techniques, in contrast to existing methods of key distribution that derive their security from the perceived intractability of certain problems in number theory, or from the physical security of the distribution process.

Several groups have demonstrated QKD over multikilometer distances of optical fiber [3], but there are many key distribution problems for which QKD over line-of-sight atmospheric paths would be advantageous (for example, it is impractical to send a courier to a satellite). Free-space

bit in the sequence, Alice prepares and transmits a single photon to the recipient, "Bob," who measures each arriving photon and attempts to identify the bit value Alice has transmitted. Alice's photon state preparations and Bob's measurements are chosen from sets of nonorthogonal possibilities. For example, using the B92 protocol [11] Alice agrees with Bob (through public discussion) that she will transmit a 45° polarized photon state $|45\rangle$, for each "0" in her sequence, and a vertical polarized photon state $|v\rangle$, for each "1" in her sequence. Bob agrees with Alice to randomly test the polarization of each arriving photon with -45° polarization, $| -45\rangle$, to reveal "1s," or horizontal polarization, $|h\rangle$, to reveal "0s." In this scheme Bob will never detect a photon for which he and Alice have used a preparation/measurement pair that corresponds to different bit values, such as $|h\rangle$ and $|v\rangle$, which happens for 50% of the bits in Alice's sequence. However, for the other

BS output ports is used to monitor the average photon number \bar{n} of the dim pulses as follows: (1) a calibration photon-number measurement is made from the rate at which a calibrated single-photon counting module (SPCM) [20] fires at the transmitter's SM transmission-fiber output with a given input, (2) next the transmitter's SPD count rate is calibrated to the SPCM firing rate with the same input to determine the SPD efficiency, which is then (3) used with the experimental SPD count rates to measure the transmitted \bar{n} in key generation mode.

At the QKD receiver (Bob) light pulses are collected by a 8.9-cm diameter Cassegrain telescope and directed

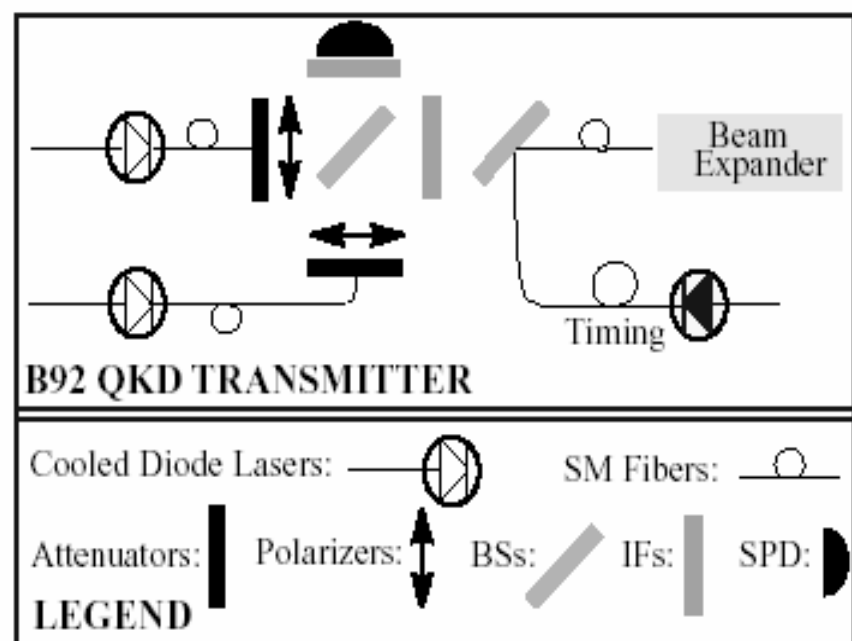


FIG. 1. Free-Space QKD Transmitter (Alice): The legend describes the basic components; cooled data lasers (on left) are pulsed 5 ns prior to the timing laser. See text for details.

(LS1) under cloudless New Mexico skies. By 11:30 LS1 turbulence induced beam-spreading hindered our ability to efficiently acquire data at low bit-error rates (BER), ϵ (where BER, ϵ , is defined as the ratio of the number of bits received in error to the total number of bits received). The system efficiency, η_{sys} , which accounts for losses between the transmitter and MM fibers at the receiver, and the receiver's SPDs efficiencies had an average value of $\langle \eta_{\text{sys}} \rangle \sim 0.13$ with a standard deviation of $\sigma = 0.04$. Fluctuations in η_{sys} were caused by turbulence induced beam spreading and beam wander; the typical beam

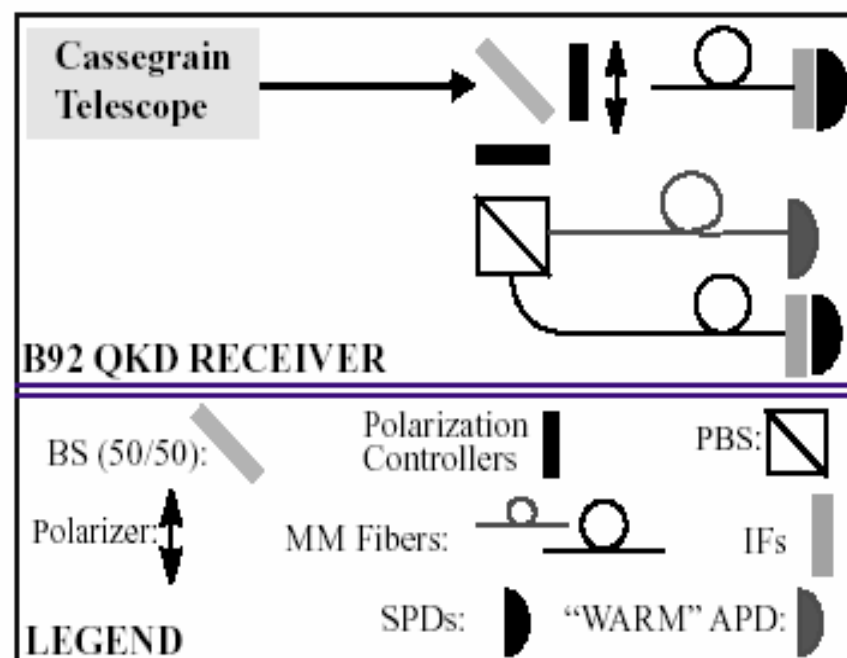
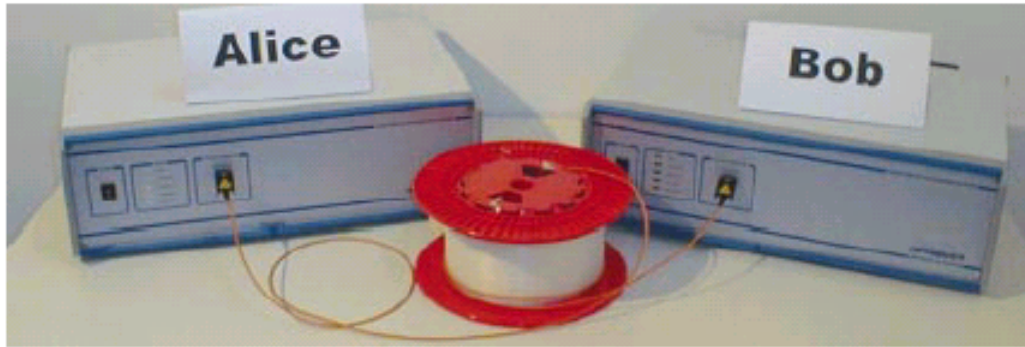
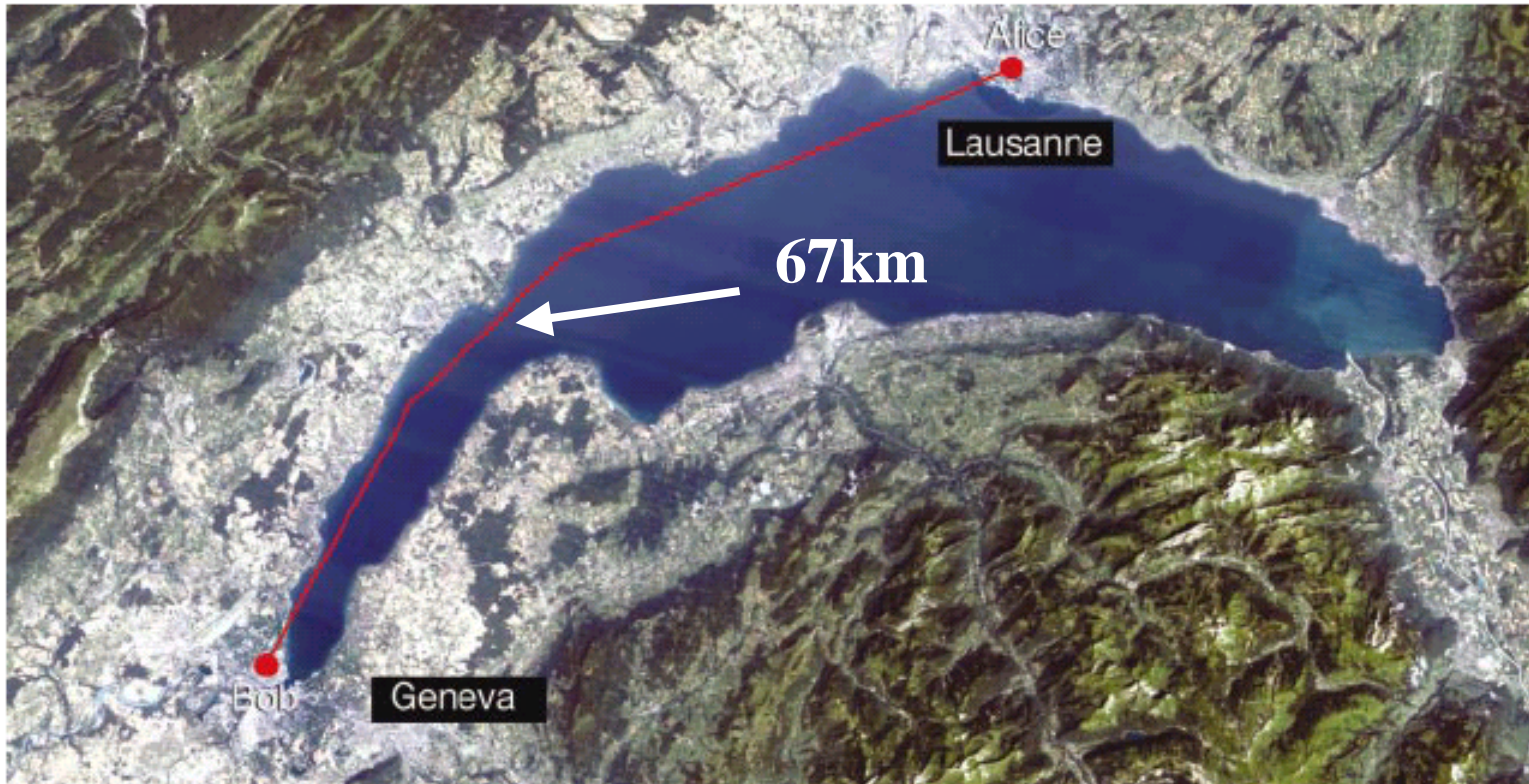


FIG. 2. Free-Space QKD Receiver (Bob): The legend describes the basic components; SPD MM-fibers are longer than the "warm" APD MM-fiber to delay the dim pulse 10 ns relative to the bright timing-pulse. See text for details.



Light work: keys encoded using polarized photons have been sent between Alice and Bob (left) through 67 km of fibre-optic cable under Lake Geneva.



key and check it over the public channel for errors. If Eve has been assessing the polarization of the photons en route between Alice

hope to predict the outcome of this algorithm.

In 1989, a team led by Bennett and Brassard built a working device, and sent

量子纠错

直观的推测:

量子计算机无法纠错

因此无法实现量子计算机

我是这一观点的受害者

Shor的天才

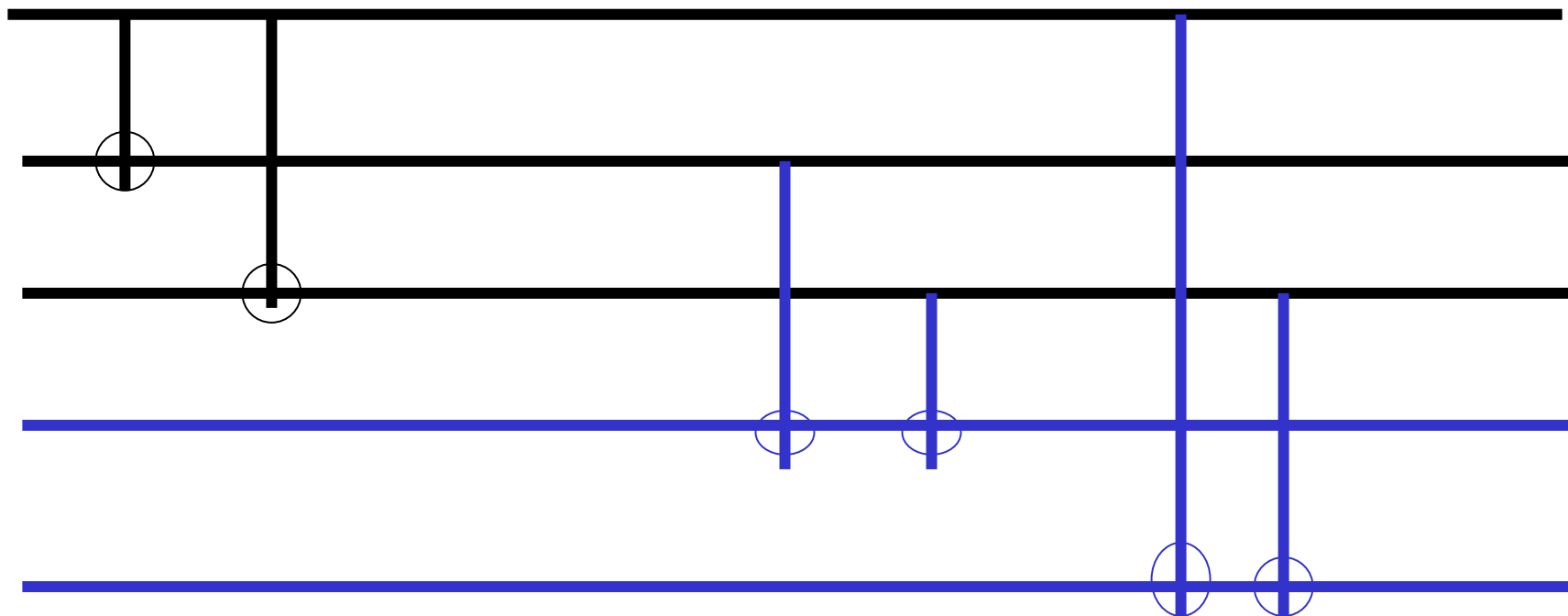
$$(a | 000\rangle + b | 111\rangle) | 00\rangle \rightarrow (a | 000\rangle + b | 111\rangle) | 00\rangle$$

$$(a | 001\rangle + b | 110\rangle) | 00\rangle \rightarrow (a | 001\rangle + b | 110\rangle) | 01\rangle$$

$$(a | 010\rangle + b | 101\rangle) | 00\rangle \rightarrow (a | 010\rangle + b | 101\rangle) | 10\rangle$$

$$(a | 100\rangle + b | 011\rangle) | 00\rangle \rightarrow (a | 100\rangle + b | 011\rangle) | 11\rangle$$

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



$$(a |000\rangle + b |111\rangle) |00\rangle + \varepsilon (a |001\rangle + b |110\rangle) |00\rangle$$



$$(a |000\rangle + b |111\rangle) |00\rangle + \varepsilon (a |001\rangle + b |110\rangle) |01\rangle$$

For small error, with large probability to obtain (0,0) and small probability to obtain (0,1)

几个比较大的进展

- 1、Shor证明可以纠错
- 2、Bennett, Preskill等人：误差要小于 10^{-6}
- 3、Knill: 2005.3.3 小于3%就可以了

目前的误差

10%左右：核磁共振，超导

离子阱：<1%

Quantum Teleportation

中文翻译

量子隐形传态

量子离物传态

Bell States

- For a 2 qubit system there are 4 Bell states
- The 4 states are orthogonal \rightarrow They can be represented as a Unitary Transform.
- The Property that makes BELL STATES so remarkable is that we can transform from one state to another by only changing 1 qubit.

$$\begin{aligned} |\psi^+\rangle_{12} &= \frac{1}{\sqrt{2}} (|0\rangle_1 |1\rangle_2 + |1\rangle_1 |0\rangle_2) \\ |\psi^-\rangle_{12} &= \frac{1}{\sqrt{2}} (|0\rangle_1 |1\rangle_2 - |1\rangle_1 |0\rangle_2) \end{aligned}$$

$$\begin{aligned} |\phi^+\rangle_{12} &= \frac{1}{\sqrt{2}} (|0\rangle_1 |0\rangle_2 + |1\rangle_1 |1\rangle_2) \\ |\phi^-\rangle_{12} &= \frac{1}{\sqrt{2}} (|0\rangle_1 |0\rangle_2 - |1\rangle_1 |1\rangle_2) \end{aligned}$$

Teleportation

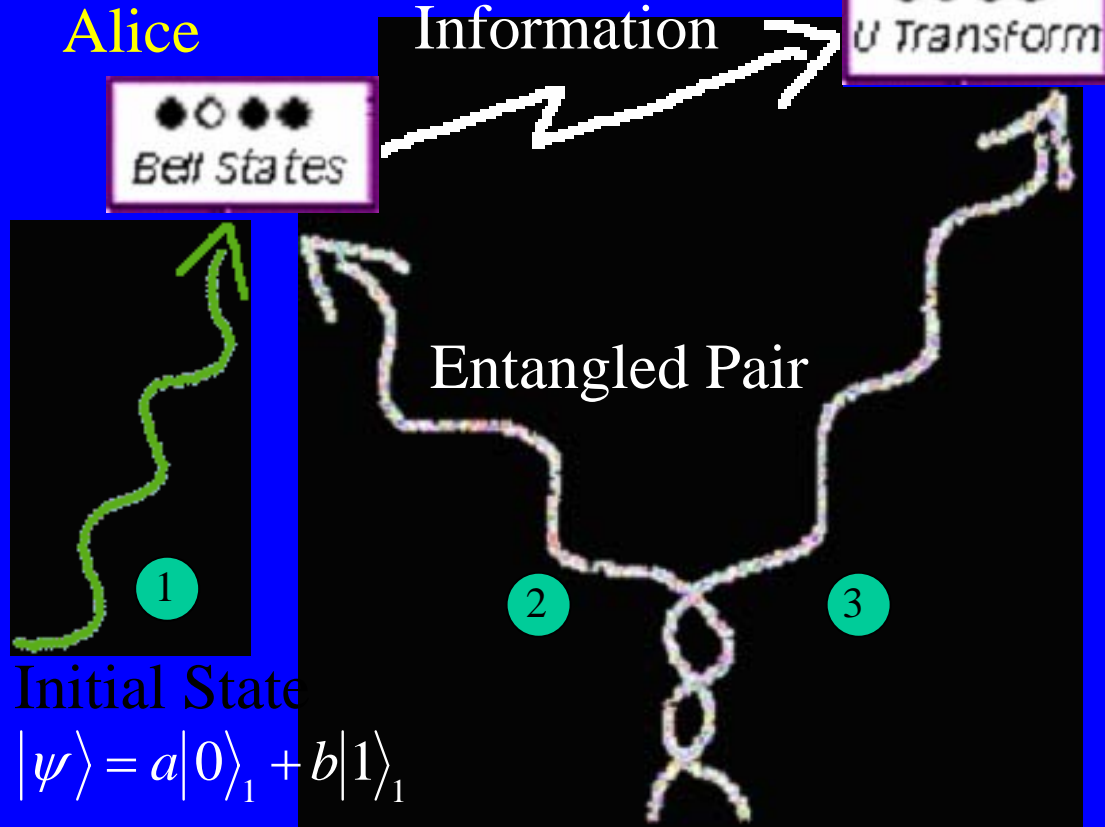
Of One qubit \rightarrow $|0\rangle$ Or $|1\rangle$

Entangled State

$$|\psi\rangle_{23} |\psi\rangle_{12} = \frac{1}{\sqrt{2}} (|0\rangle_2 |0\rangle_3 \otimes |1\rangle_1 |1\rangle_2 + |1\rangle_2 |1\rangle_3 \otimes |0\rangle_1 |0\rangle_2)$$

Bell States

$$\begin{aligned} |\psi^+\rangle_{12} &= \frac{1}{\sqrt{2}} (|0\rangle_1 |0\rangle_2 + |1\rangle_1 |1\rangle_2) \\ |\psi^-\rangle_{12} &= \frac{1}{\sqrt{2}} (|0\rangle_1 |0\rangle_2 - |1\rangle_1 |1\rangle_2) \\ |\phi^-\rangle_{12} &= \frac{1}{\sqrt{2}} (|0\rangle_1 |1\rangle_2 - |1\rangle_1 |0\rangle_2) \\ |\phi^+\rangle_{12} &= \frac{1}{\sqrt{2}} (|0\rangle_1 |1\rangle_2 + |1\rangle_1 |0\rangle_2) \end{aligned}$$



Superdense Coding

Super Dense Coding

- Alice & Bob have the long distance feeling
- Goal: to transmit some CLASSICAL information from Alice to Bob.
- Alice is in possession of two classical bits of information which she wishes to send to Bob but can only send one qubit to Bob.
- Can she achieve her goal?

Super Dense Coding

- Super Dense Coding says YES!
 - They both initially share a pair of qubits in the entangled state.

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

- Alice initially has the first qubit and Bob has the second qubit.
 - Note the qubit is prepared ahead of time by a third party who then sends one to Alice and one to Bob
 - By sending a single qubit to Bob, Alice can communicate two bits of classical information

Super Dense Coding

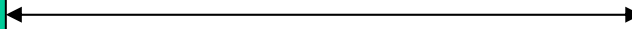
$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

Alice
00: I 01: Z
10: X 11: iY

1 qubit

1 qubit

Bob



Super Dense Coding

- Procedure:
 - If Alice wants to send...

00	She does nothing
01	She applies the phase flip Z to her qubit
10	She applies quantum NOT gate X
11	She applies the iY gate
- Then Bob applies an appropriate measurement operator

Super Dense Coding

- Four Resulting States

$$\begin{aligned} 00: |\psi\rangle &\rightarrow \frac{|00\rangle + |11\rangle}{\sqrt{2}} \\ 01: |\psi\rangle &\rightarrow \frac{|00\rangle - |11\rangle}{\sqrt{2}} \\ 10: |\psi\rangle &\rightarrow \frac{|10\rangle + |01\rangle}{\sqrt{2}} \\ 11: |\psi\rangle &\rightarrow \frac{|01\rangle - |10\rangle}{\sqrt{2}} \end{aligned}$$

Bell States

Super Dense Coding

- Notice that the Bell States...

Form an orthonormal basis

eg:

$$\begin{aligned} & \left(\frac{\langle 00| + \langle 11|}{\sqrt{2}} \right) \left(\frac{|00\rangle + |11\rangle}{\sqrt{2}} \right) \\ &= \frac{1}{2} (\langle 00|00\rangle + \langle 00|11\rangle + \langle 11|00\rangle + \langle 11|11\rangle) \\ &= \frac{1}{2} (2) = 1 \end{aligned}$$

...therefore can be distinguished by an appropriate quantum measurement. Example:

$$P_{ij} = |b_{ij}\rangle \langle b_{ij}|$$

General scheme for superdense coding between multiparties

X. S. Liu,^{1,2} G. L. Long,^{1,2,3,4,5} D. M. Tong,² and Feng Li⁶

¹*Department of Physics, Tsinghua University, Beijing 100084, China*

²*Department of Physics, Shandong Normal University, Jinan 250014, China*

³*Key Laboratory for Quantum Information and Measurement, Beijing 100084, China*

⁴*Institute of Theoretical Physics, Chinese Academy of Sciences, Beijing 100080, People's Republic of China*

⁵*Center for Atomic, Molecular and NanoSciences, Tsinghua University, Beijing 100084, People's Republic of China*

⁶*Basic Education Section, Capital University of Economics and Business, Beijing 100026, People's Republic of China*

(Received 25 July 2001; published 4 January 2002)

Dense coding or superdense coding in the case of high-dimension quantum states between two parties and multiparties is studied in this paper. We construct explicitly the measurement basis and the forms of the single-body unitary operations corresponding to the basis chosen, and the rules for selecting the one-body unitary operations in a multiparty case.

DOI: 10.1103/PhysRevA.65.022304

PACS number(s): 03.67.-a, 89.70.+c

Quantum dense coding or superdense coding [1] is one of the important branches of quantum-information theory. It has been widely studied both in theory and in experiment [1,2]. The basic idea of quantum dense coding is that quantum mechanics allows one to encode information in the quantum states that is denser than classical coding. Bell-basis states

$$|\Psi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2},$$

$$|\Psi^-\rangle = (|00\rangle - |11\rangle)/\sqrt{2},$$

To present our scheme more clearly, let us first begin with dense coding between two parties in three dimensions. The general Bell basis of the Hilbert space of two particles with three dimensions is [5,6]:

$$|\Psi_{nm}\rangle = \sum_j e^{2\pi i j n/3} |j\rangle \otimes |j+m \bmod 3\rangle / \sqrt{3}, \quad (2)$$

where $n, m, j = 0, 1, 2$. Explicitly,

$$|\Psi_{00}\rangle = (|00\rangle + |11\rangle + |22\rangle) / \sqrt{3},$$

三方量子超密编码的核磁共振实验实现

魏达秀 杨晓冬 罗军 孙献平 曾锡之 刘买利

(中国科学院武汉物理与数学研究所波谱与原子分子物理国家重点实验室, 武汉 430071. E-mail: dxwei@wipm.ac.cn)

摘要 报道了使用液相核磁共振(NMR)实验技术, 利用三个量子位实现三方量子超密编码的实验过程. 实验表明: 根据龙桂鲁等人和 Crudka 等人提出的多方量子超密编码的方案, 三量子位的量子超密编码只需要传送两个量子位便可以完成传送三个经典位信息的任务. 因此, 量子超密编码具有比经典通信更强大的信息传递能力.

关键词 量子通信 量子超密编码 核磁共振



近年来, 量子信息处理(quantum information processing, QIP)^[1,2]已经吸引了越来越多的注意, 并得到了蓬勃的发展. 其原因在于量子信息处理比经典方法具有更快的速度和更高的效率^[3~9].

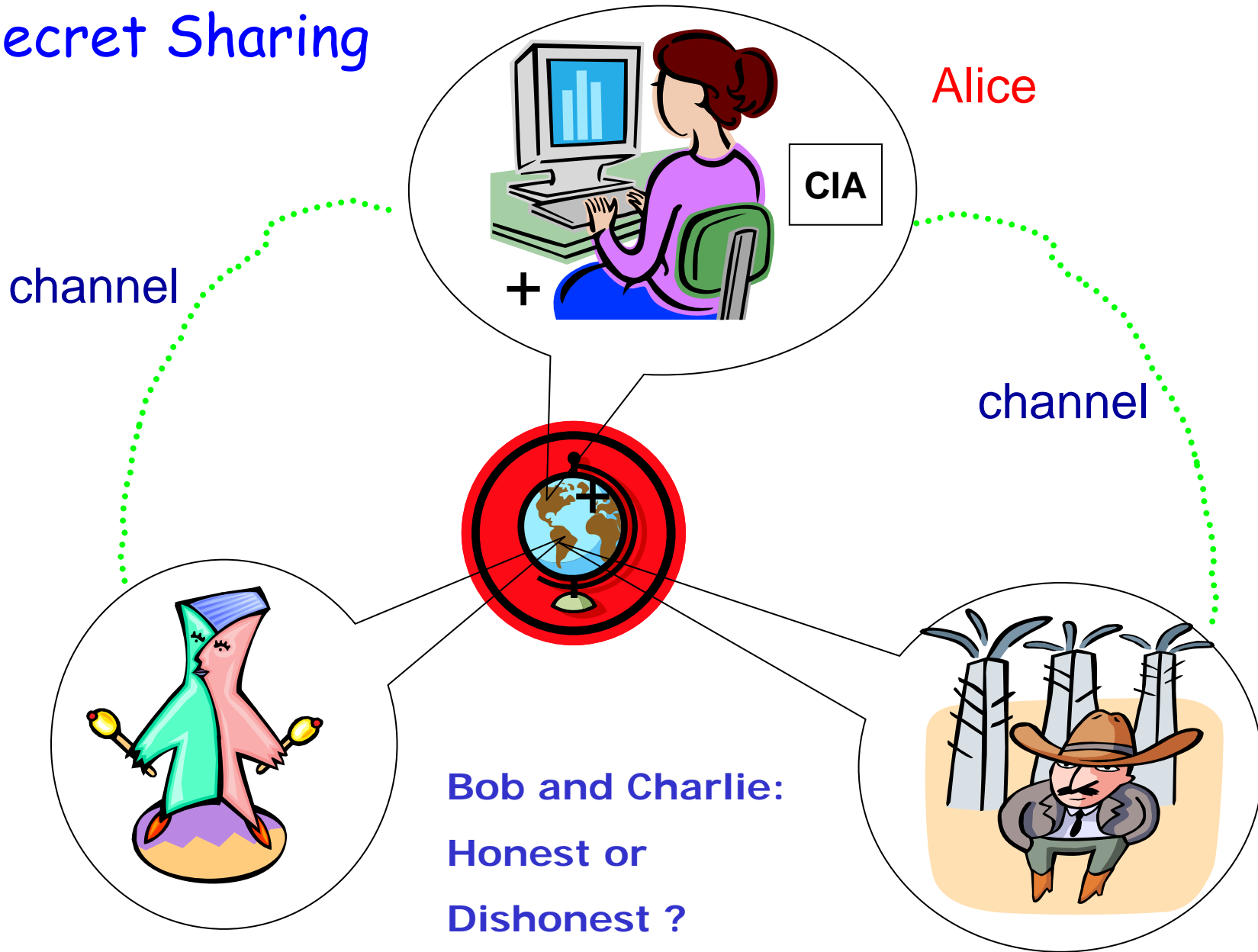
量子超密编码(quantum superdense coding, QSDC)是量子信息处理研究的领域之一, 它在 1993 年由 Bennett 和 Wiesner^[6]首次提出. 最近量子超密编码又一次引起了人们的关注, 因为我国的龙桂鲁小组^[10]和波兰的 Crudka 小组^[11]分别将 Bennett 和 Wiener 提出的原始的两维和两方的量子超密编码方

对于两方的量子超密编码, 只传送 1 个量子位即可完成传送 2 个经典位信息的任务. 上述简单情形的量子超密编码过程已由 Mattle 等人^[12]和方细明等人^[13]分别在量子光学体系和核自旋体系中实现.

核磁共振(nuclear magnetic resonance, NMR)实验是实现量子信息处理过程的重要实验方法之一^[14,15]. 本文报道了使用液相核磁共振(NMR)实验实现三方量子超密编码的过程. 结果表明: 3 量子位的量子超密编码只需传递 2 个量子位便可以实现 8 种不同的编码, 即 3 个经典位的信息, 比经典通信具有更

Quantum Secret Sharing

Secret Sharing



Agent Bob

Agent Charlie

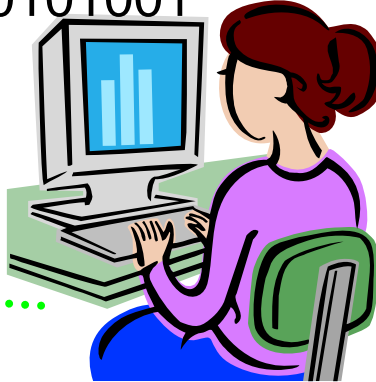
Message: Key: 0101001 Alice

\oplus Secret key :1011010 Bob

Coded:1110011 Charlie

Message: Key: 0101001

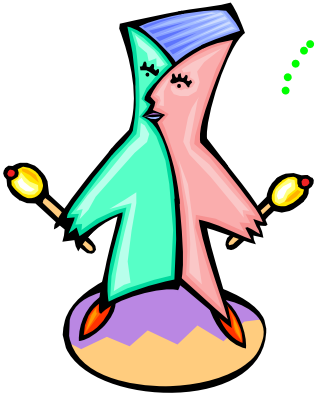
Alice



Coded:1110011



Secret key :1011010

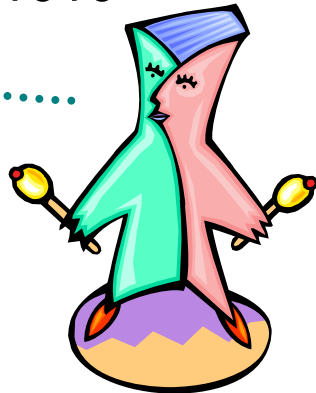
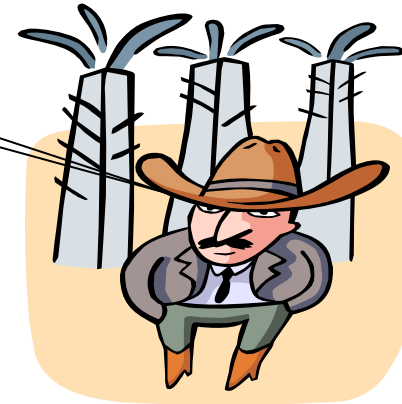
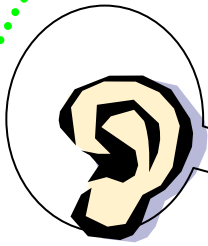


Agent Bob

Agent Charlie



The **DISHONEST**
agent can eavesdrop
without awareness!



Agent Bob 清华大学龙桂鲁 Agent Charlie

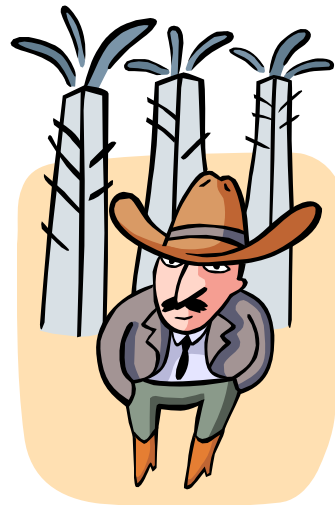
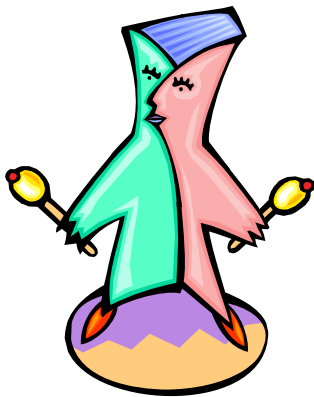
Secret key :1011010

“fake” Secret key :011010

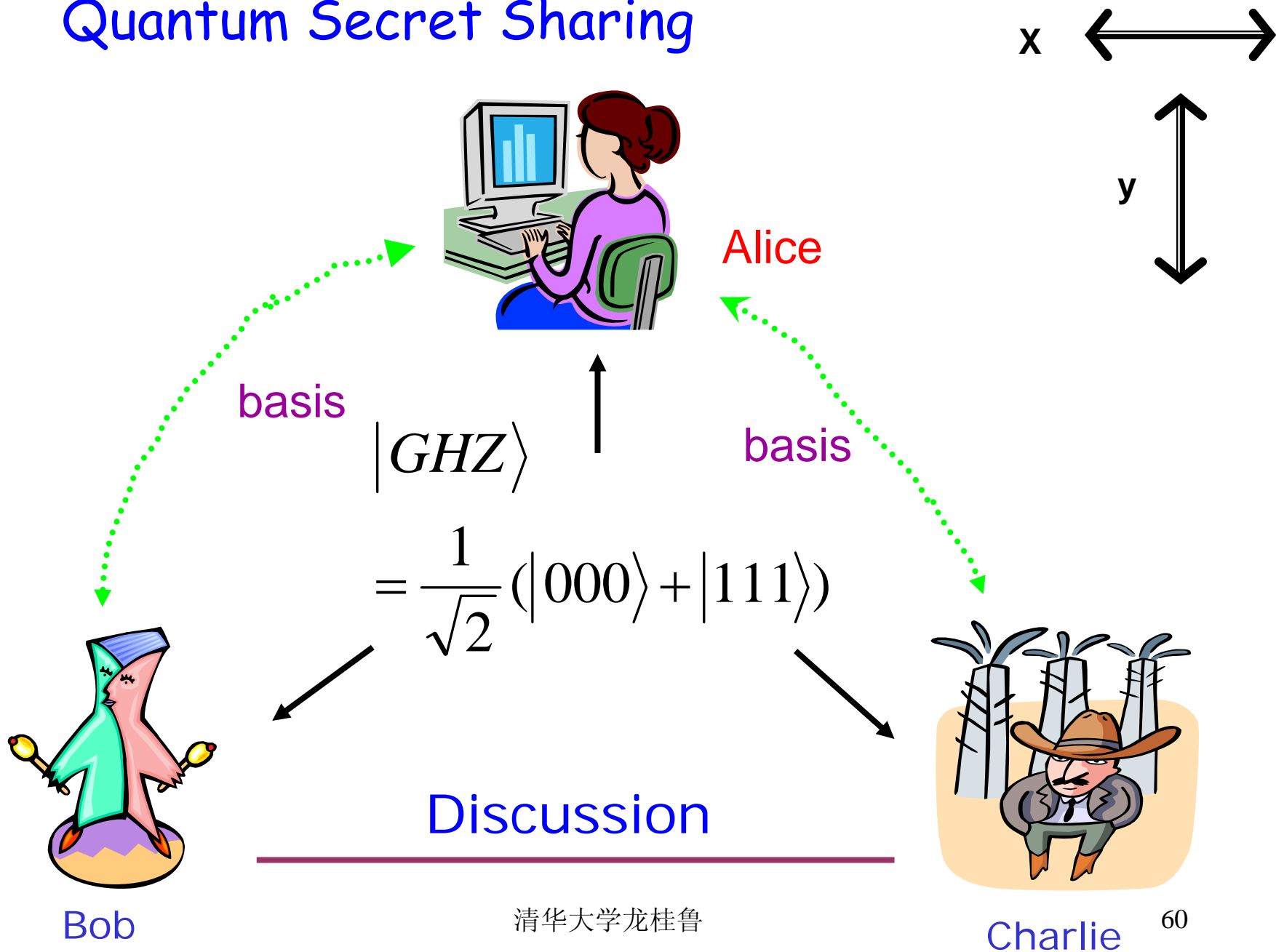
Secret Sharing Rules:

1. There may be one --and at most one-- dishonest agent.

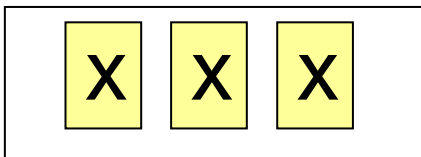
2. If these two agents carry it out together, the honest agent will prevent the dishonest one from obstruction.



Quantum Secret Sharing



Alice



+X -x +y -y

+X

Bob

-x

+y

-y

+x	-x	-y	+y
-x	+x	+y	-y
-y	+y	-x	+x
+y	-y	+x	-x

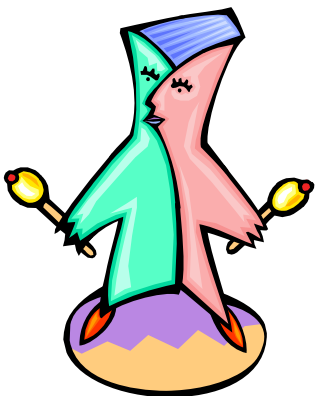
Entry : Charlie

X

$$\pm x = \frac{1}{\sqrt{2}} (|0\rangle \pm |1\rangle) \quad \pm y = \frac{1}{\sqrt{2}} (|0\rangle \pm i|1\rangle)$$

Entanglement Attack

$$\begin{aligned} & |GHZ\rangle \\ &= \frac{1}{\sqrt{2}} (|000\rangle + |111\rangle) \\ &= \frac{1}{\sqrt{2}} \underbrace{|+x\rangle}_{\text{red underline}} \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) \\ &\quad + \frac{1}{\sqrt{2}} \underbrace{|-x\rangle}_{\text{red underline}} \frac{1}{\sqrt{2}} (|00\rangle - |11\rangle) \\ &= \frac{1}{\sqrt{2}} \underbrace{|+y\rangle}_{\text{red underline}} \frac{1}{\sqrt{2}} (|00\rangle - i|11\rangle) \\ &\quad + \frac{1}{\sqrt{2}} \underbrace{|-y\rangle}_{\text{red underline}} \frac{1}{\sqrt{2}} (|00\rangle + i|11\rangle) \end{aligned}$$



$$\frac{1}{\sqrt{2}} (|00\rangle \pm |11\rangle)$$

$$\frac{1}{\sqrt{2}} (|00\rangle \pm i|11\rangle)$$

Measurement Basis

$$\begin{aligned}
 |GHZ\rangle &= \frac{1}{\sqrt{2}} (|000\rangle + |111\rangle) \\
 &= \frac{1}{\sqrt{2}} |+\ x\rangle \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) + \frac{1}{\sqrt{2}} |-\ x\rangle \frac{1}{\sqrt{2}} (|00\rangle - |11\rangle)
 \end{aligned}$$

$$\begin{aligned}
 &= \frac{1}{\sqrt{2}} (|+\ y\rangle + |-\ y\rangle) \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) \\
 &+ \frac{-i}{\sqrt{2}} (|+\ y\rangle - |-\ y\rangle) \frac{1}{\sqrt{2}} (|00\rangle - |11\rangle)
 \end{aligned}$$

$$\begin{aligned}
 &\frac{1}{2} [e^{-\frac{i\pi}{4}} (|+\ x\rangle |+\ y\rangle + |-\ x\rangle |-\ y\rangle) \\
 &+ e^{\frac{i\pi}{4}} (|+\ x\rangle |-\ y\rangle + |-\ x\rangle |+\ y\rangle)]
 \end{aligned}$$

清华大学龙桂鲁

Alice	
Bob	+y
+X	-y
-X	+y
+y	-x
-y	+x
Charlie	

1946年2月14日，在美国诞生了第一台计算机

ENIAC

2007年2月13日，D-wave公司在美国的计算机
博物馆宣布研制成第一台量

子计算机ORION

D-wave计划

2007年底 32 量子比特

2008年中期 1024 量子比特

消息公布后，在全世界引起轰动；

1. 大量的媒体进行了报道

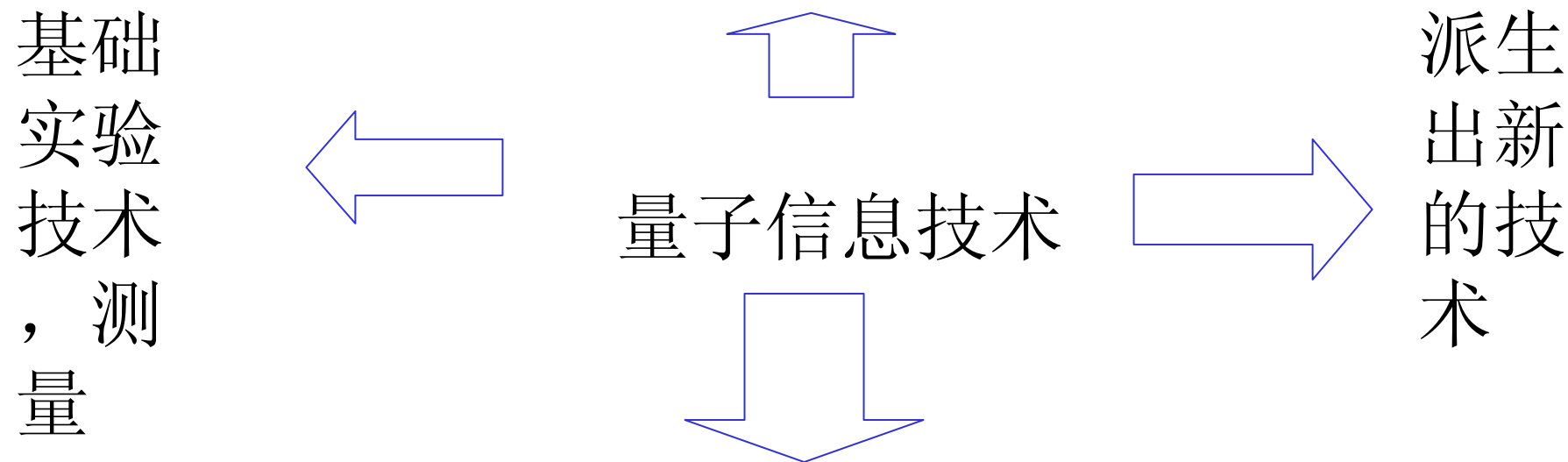
2. 震惊，不可思议

3. 怀疑

4. 为什么？如何看待这件事情？

量子信息是一个诱人的学科

新的计算机技术，通讯技术，信息技术



量子力学的基本问题，各种物理机制

一个只赢不输的投入，一个朝阳学科，一个充满困难和挑战，清华大学九桂馨一个充满机会的学科

感谢大家！