量子電腦與量子資訊

Goan, Hsi-Sheng

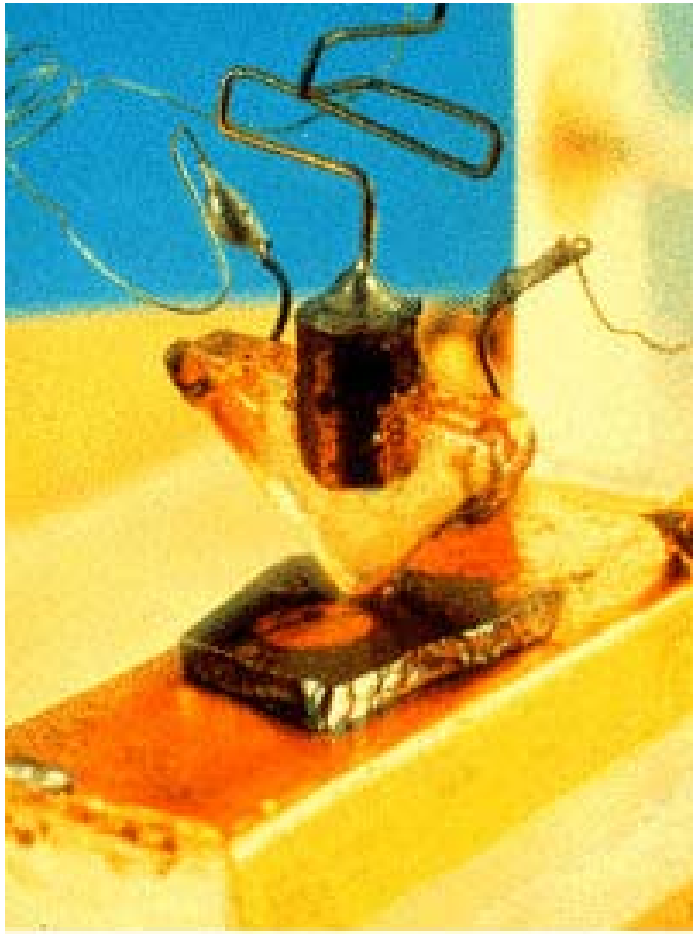
管　希　聖

Department of Physics
National Taiwan University

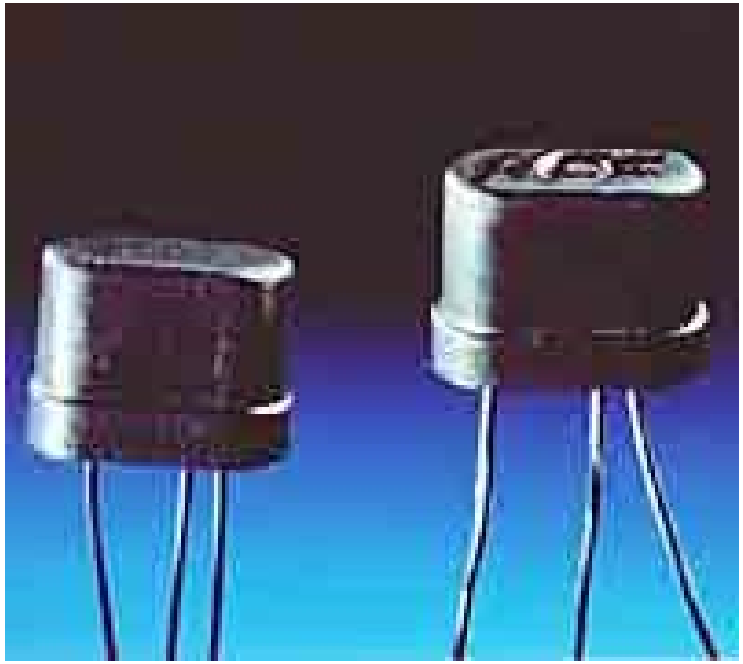
臺灣大學 物理系

E-mail: goan@phys.ntu.edu.tw

電晶體

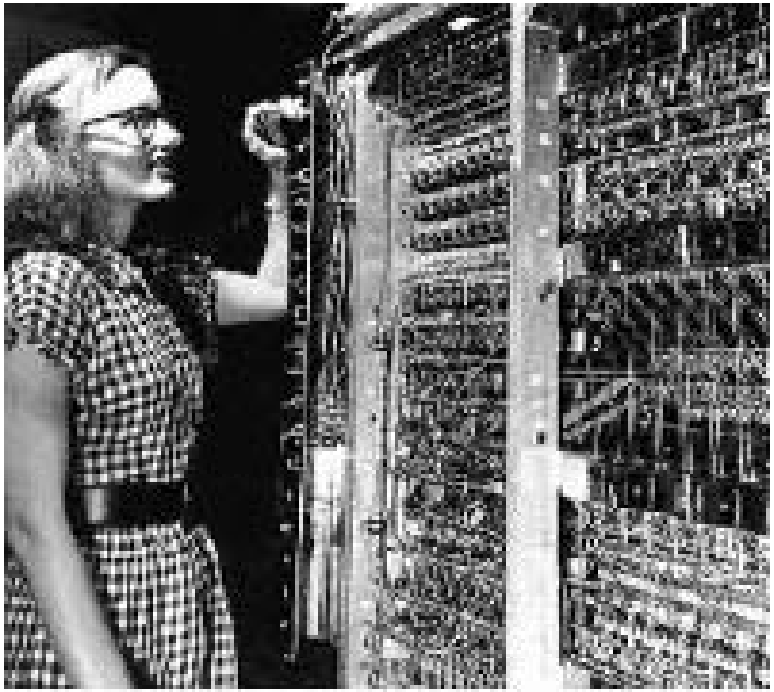


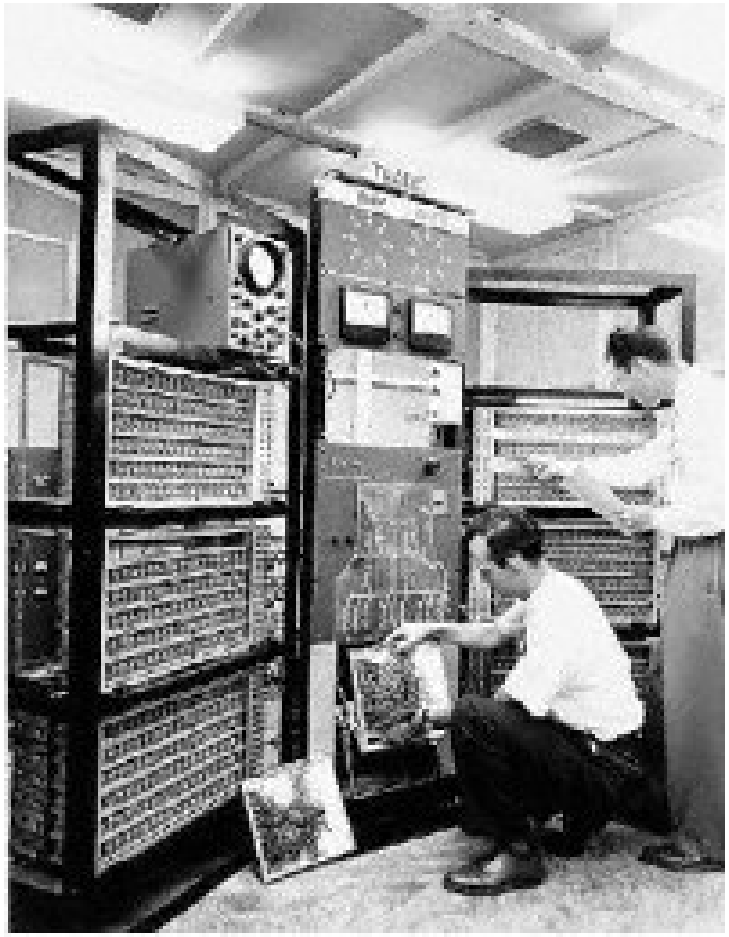
1947 年12月23日, W. Shockley, W. Brattain, and J. Bardeen 成功地測試這個點接觸電晶體(point-contact transistor), 開啟了半導體革命.



1954, 德州儀器公司 (Texas Instruments Inc.) 製成矽介面電晶體(silicon-based junction transistor), 每個造價 $2.50.

早期的電腦



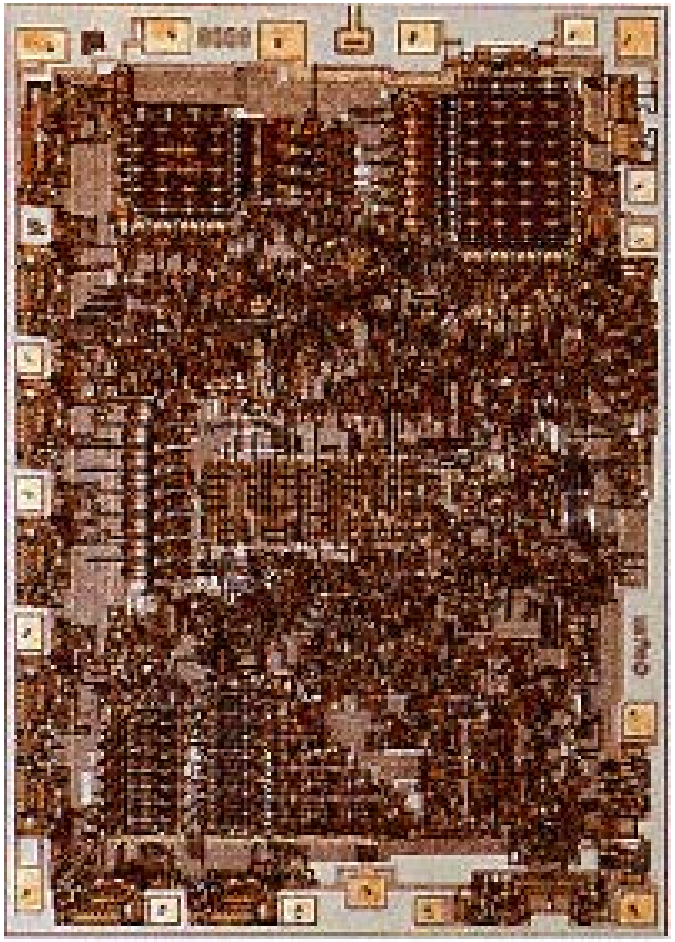


1951 “UNIVAC” 第一部商業化真空電腦耗資約一百萬美金

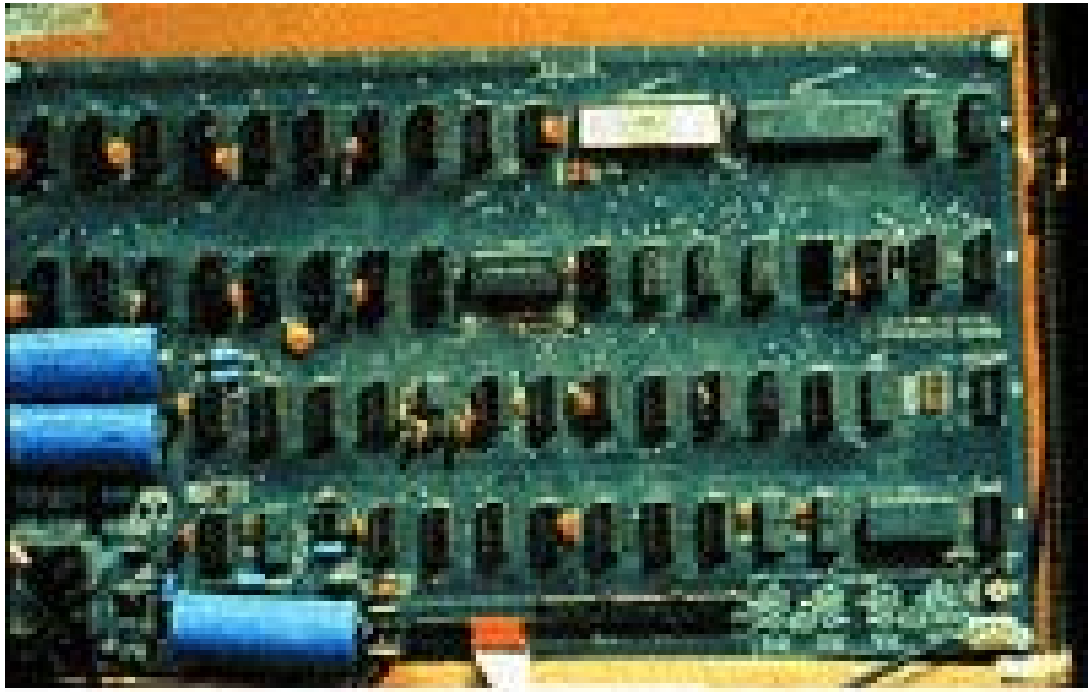
- 真空管電腦約需要 $750,000
- 高速印表機約需要 $185,000.

1955, AT&T 貝爾實驗室宣布第一部完全電晶體的電腦 “TRADIC”. 它包含約800個電晶體.

早期的微處理機與主機板

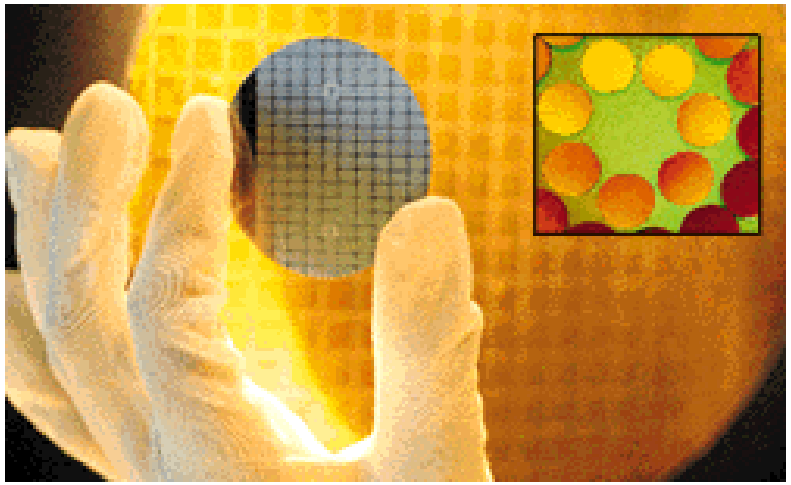


1972, Intel´s 8008微處理機
2500電晶體



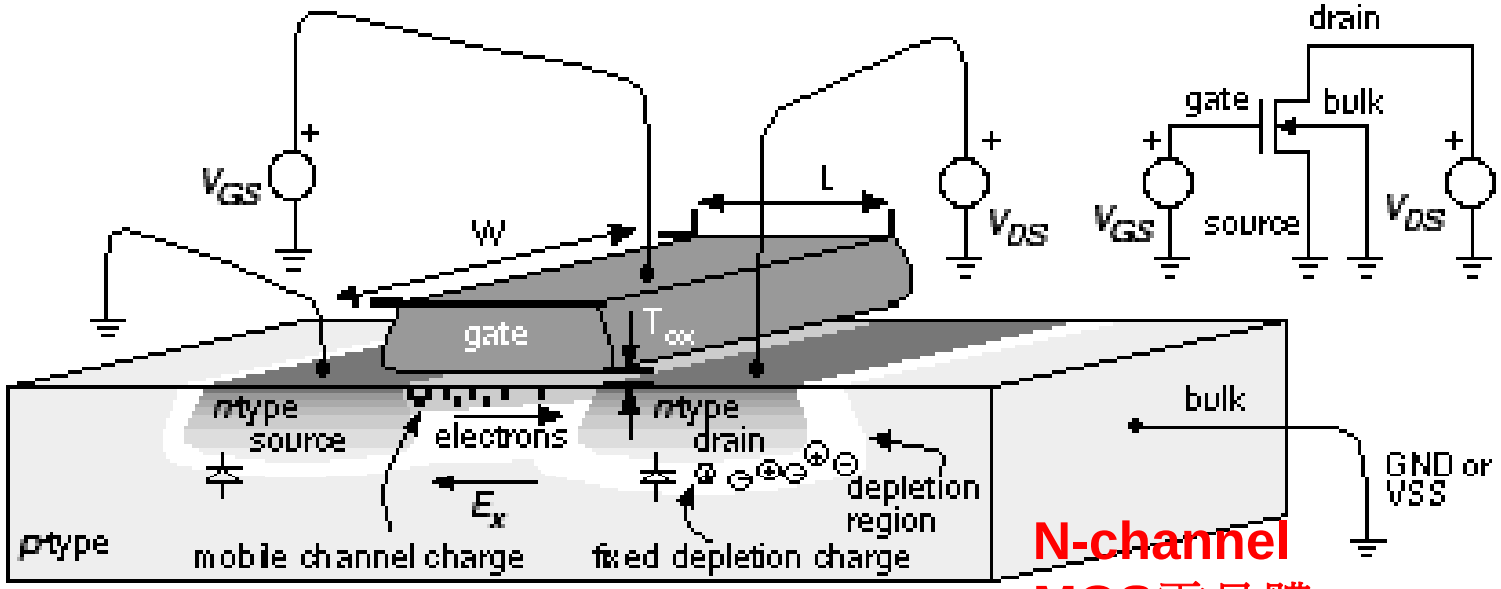
1976, Apple I 蘋果電腦主機板

從晶片到電晶體



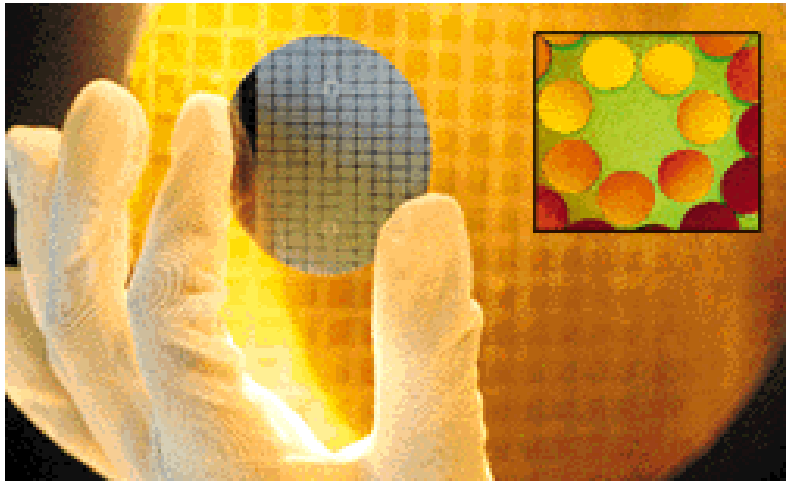
晶圓

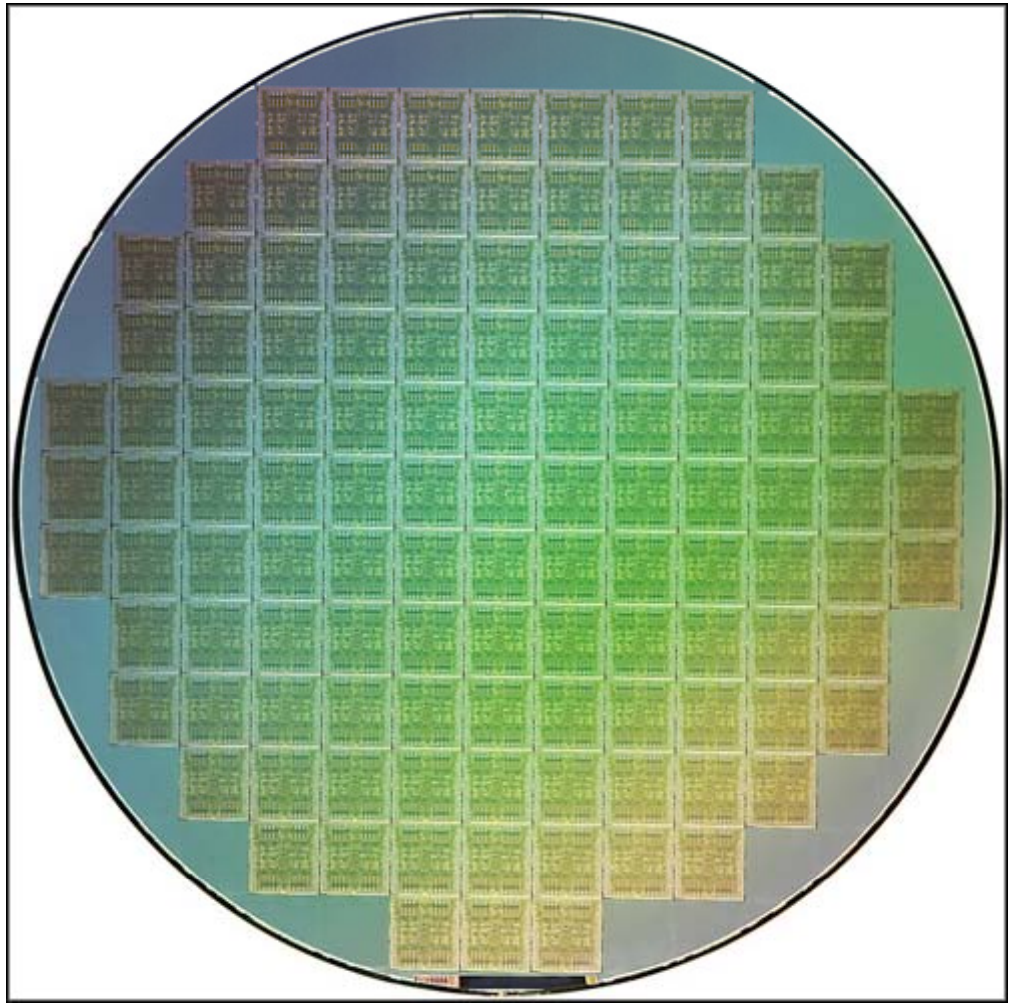
積體
電路



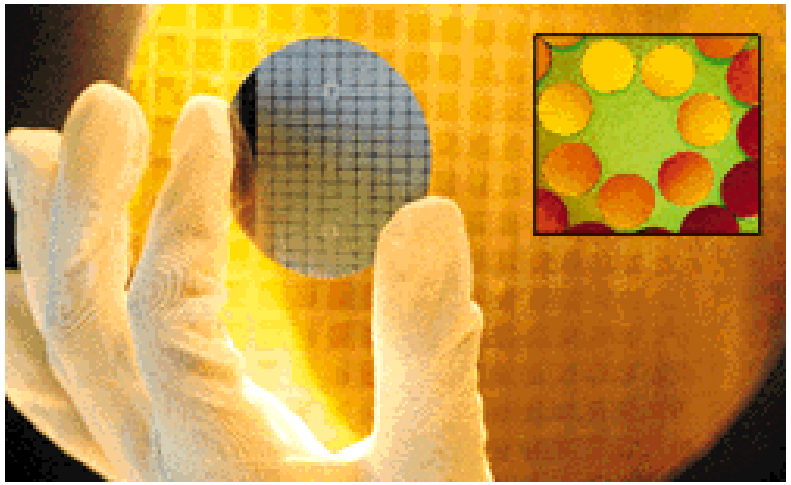
N-channel
MOS電晶體

晶圓



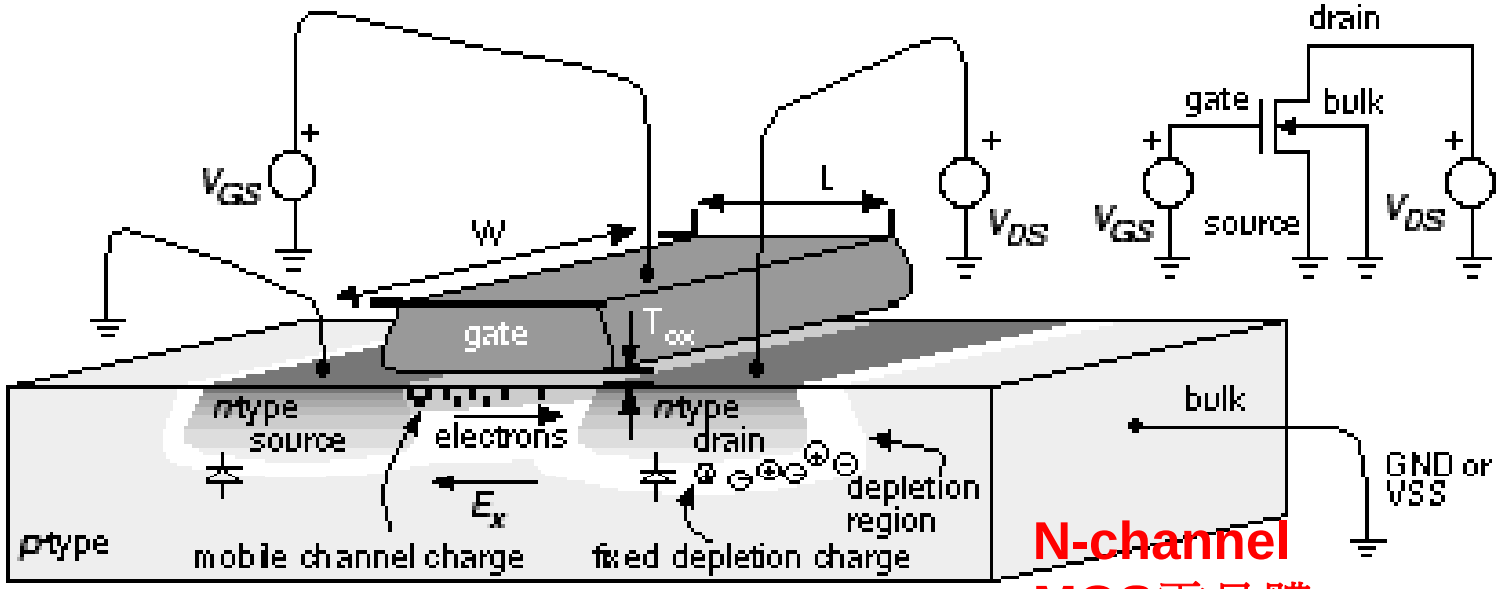


從晶片到電晶體



晶圓

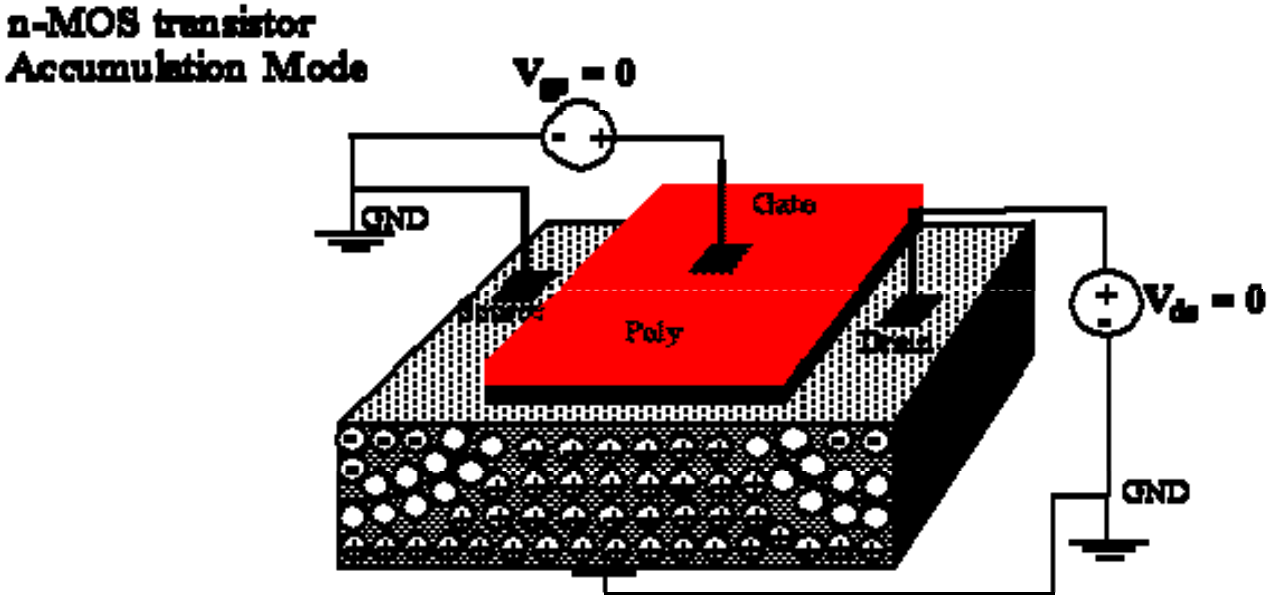
積體
電路



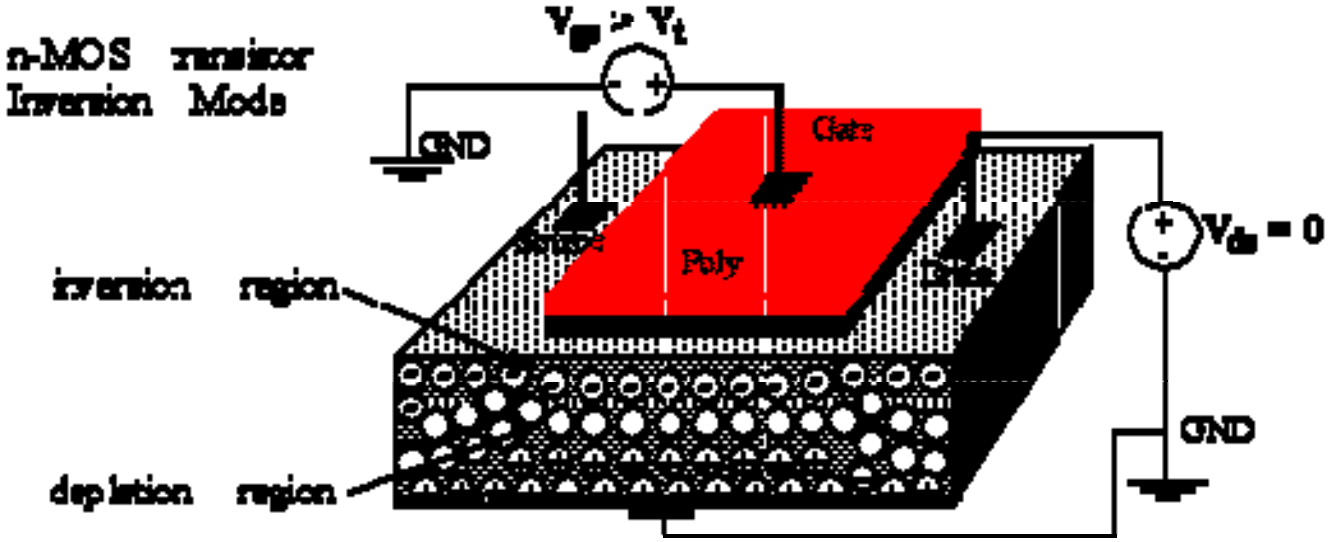
N-channel
MOS電晶體

N-channel MOS電晶體

不導通



導通



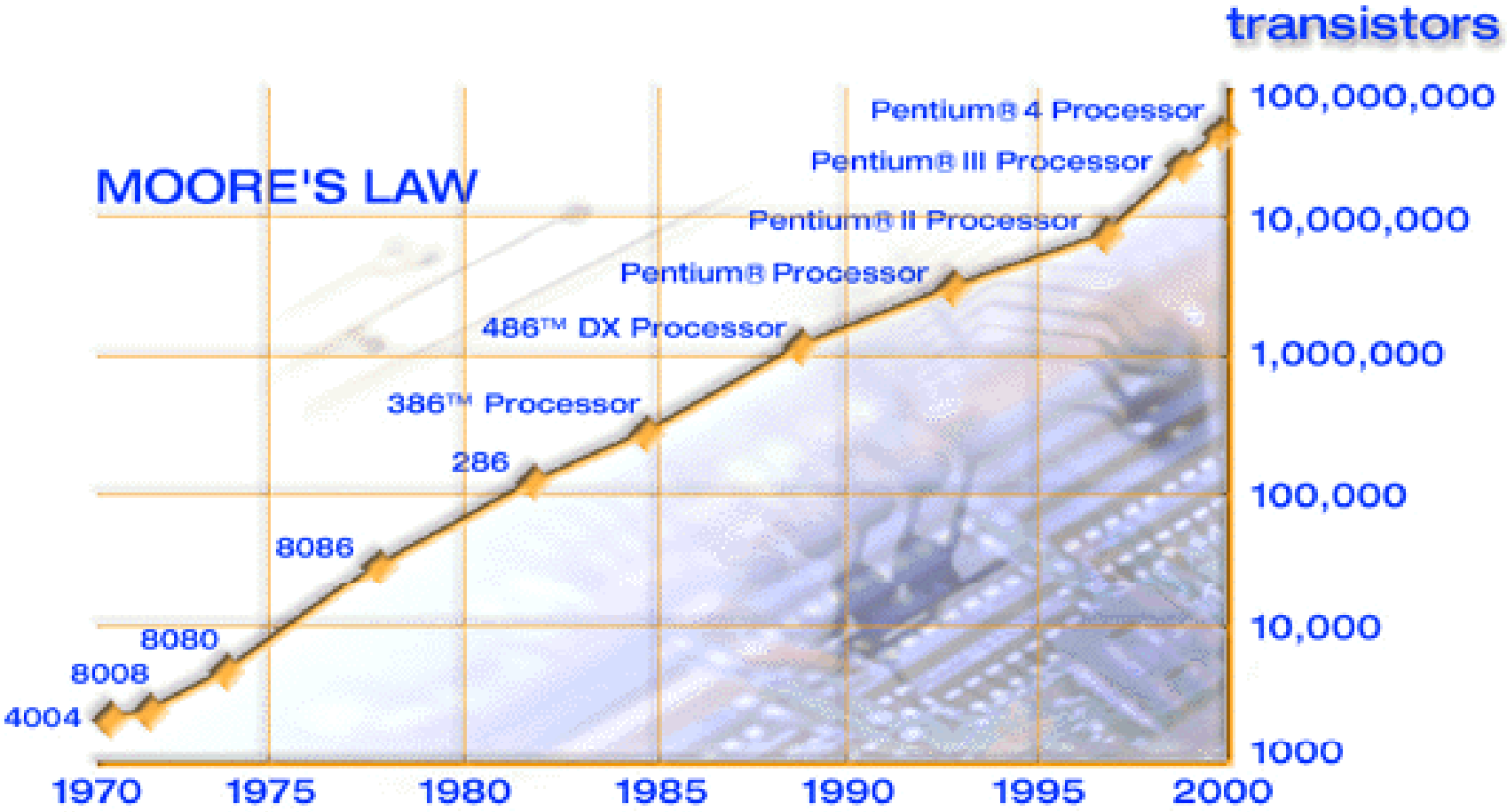
近代的電腦

積體電路

硬碟

桌上型電腦

Moore’s law (摩 爾 定律)



在積體電路中, 單位面積的電晶體數目隨時間成指數增長:

在晶片 中電晶體的數目每兩年成長一倍.

(http://www.intel.com/research/silicon/mooreslaw.htm)

晶片中電晶體的數目

	Year of introduction	Transistors
4004	1971	2,250
8008	1972	2,500
8080	1974	5,000
8086	1978	29,000
286	1982	120,000
386™ processor	1985	275,000
486™ DX processor	1989	1,180,000
Pentium® processor	1993	3,100,000
Pentium II processor	1997	7,500,000
Pentium III processor	1999	24,000,000
Pentium 4 processor	2000	42,000,000

2005年的筆記型電腦

ACER Aspire 3003LCi
全民超能無線達人機

鏡面**15**吋無線燒錄筆記電腦↘**19999**元

ASUS W5G760DD 新迅馳旗艦超可
筆記**12**吋鏡面寬螢幕視訊筆記電腦

intel inside
centrino™
MOBILE TECHNOLOGY

Dothan的電晶體大幅由7千7百萬大幅提升至1億4千萬。製程上已經由130奈米跳進90奈米。 65奈米

The New York Times
ON THE WEB

By JOHN MARKOFF
Published: February 20, 2006

I.B.M. Researchers Find a Way to Keep Moore's Law on Pace

SAN FRANCISCO, Feb. 19 — I.B.M. researchers plan to describe an advance in chip-making on Monday that could pave the way for new generations of superchips. The development, which comes from materials research in the design of advanced lenses and related technologies, **will make it possible to create semiconductors with wires thinner than 30 nanometers, one-third the width in today's industry-standard chips**. The researchers **have created the thinnest line patterns to date using deep ultraviolet lithography**, the laser technology used to print circuits on chips.

The key to pushing the technology further is a fluid immersion process for conducting the light onto the material that is etched to form the circuit pattern. The researchers discovered that **they could enhance the resolving power of the light source by shifting to a lens made from a crystalline quartz material and exotic immersion liquids that have better refraction properties than those currently used by the industry**.

台積電55奈米製程 進入量產

自由時報 電子報 2007年3月28日 星期三

台積電55奈米製程 進入量產

〔記者洪友芳／新竹報導〕台積電（2330）昨宣布，該公司的55奈米「半世代」製程技術進入量產，此一製程由65奈米製程技術直接微縮90%，所生產的晶片在相同運作速度下能節省耗電量達10%至20%，有助降低客戶的單顆晶粒成本。

台積電表示，目前已有許多客戶、元件資料庫與矽智財廠商使用台積電的55奈米製程，為了使更多客戶、矽智財及元件資料庫合作夥伴能以更具成本優勢的方式進行產品的試產及驗證工作，預計從今年5月起，每隔二個月將會提供55奈米製程的CyberShuttle服務。

台積電的55奈米製程由65奈米製程直接微縮，目前提供泛用型的GP（General Purpose）及消費性產品的GC（Consumer）55奈米邏輯製程，其中GP製程已於第一季開始量產，GC製程預計於今年稍後開始量產。

台積電企業發展副總經理陳俊聖表示，該公司首次推出的半世代製程技術是由0.35微米製程微縮而來，55奈米製程是公司的第六個半世代製程技術。「半世代」製程技術推出以來，一直相當成功，協助客戶在高度競爭的市場上獲得相當大的競爭優勢。

英特爾以色列研發新CPU 更小更快速省電

2007.11.13 中時電子報 www.chinatimes.com

- 製造電腦中央處理器（CPU） 全球知名的英特爾公司以色列研發中心宣布，發展出新型更小、更快速、且更省電的Penryn中央處理器，這個中央處理器只有四十五奈米大小。一奈米等於十億分之一米，約為頭髮寬度的十萬分之一。
- 英特爾總裁兼執行長歐特里尼表示，他恭賀以色列研發小組能夠發展出新型更有效、更省電、更快速、和更小的中央處理器；經由這種更好的中央處理器，將使消費者能使用到更輕便好用的電腦。「耶路撒冷郵報」今天報導指出，這種新型Penryn中央處理器是以新的電晶體方式，在減少大量浪費電能洩露的情況下，在明年這種Penryn中央處理器將使用鹵素元素製造。英特爾以色列製造中央處理器的工廠目前正在興建中，預計到明年底可以生產這種新型四十五奈米Penryn中央處理器。
- 四十五奈米的**Penryn**中央處理器電晶體的容量密度比原先的六十五奈米中央處理器要增加了近一倍的容量，在這小小的中央處理器內可以放置八億二千個電晶體。中央處理器是電子計算機的主要設備之一，它的功能主要是解釋計算機的指令、以及處理計算機軟件中的數據。

現代的筆記型電腦

ACER Aspire 2920Z【Intel 雙核心超可攜筆記】 輕鬆擁有！網路視訊、藍芽、杜比音效喇叭、杜比環繞音效、奈米瓷漆塗面

資訊展期間 爆低↘ **$19900元!**

ASUS U62PCT94DD(U6Vc) ，**Intel Centrino 2_45奈米2.53Ghz**《帶來GF9300M 高階獨立顯示卡▲再加320G大容量硬碟+指紋辨識及ASUS SmartLogon臉部辨識登入》12吋星鑽棕

採用Intel 最新**MONTEVINA平台**，採用**Core 2 Duo T9400雙核心45奈米行動處理器**, 相較於先前的intel Centrino Duo處理器更縮小了40%

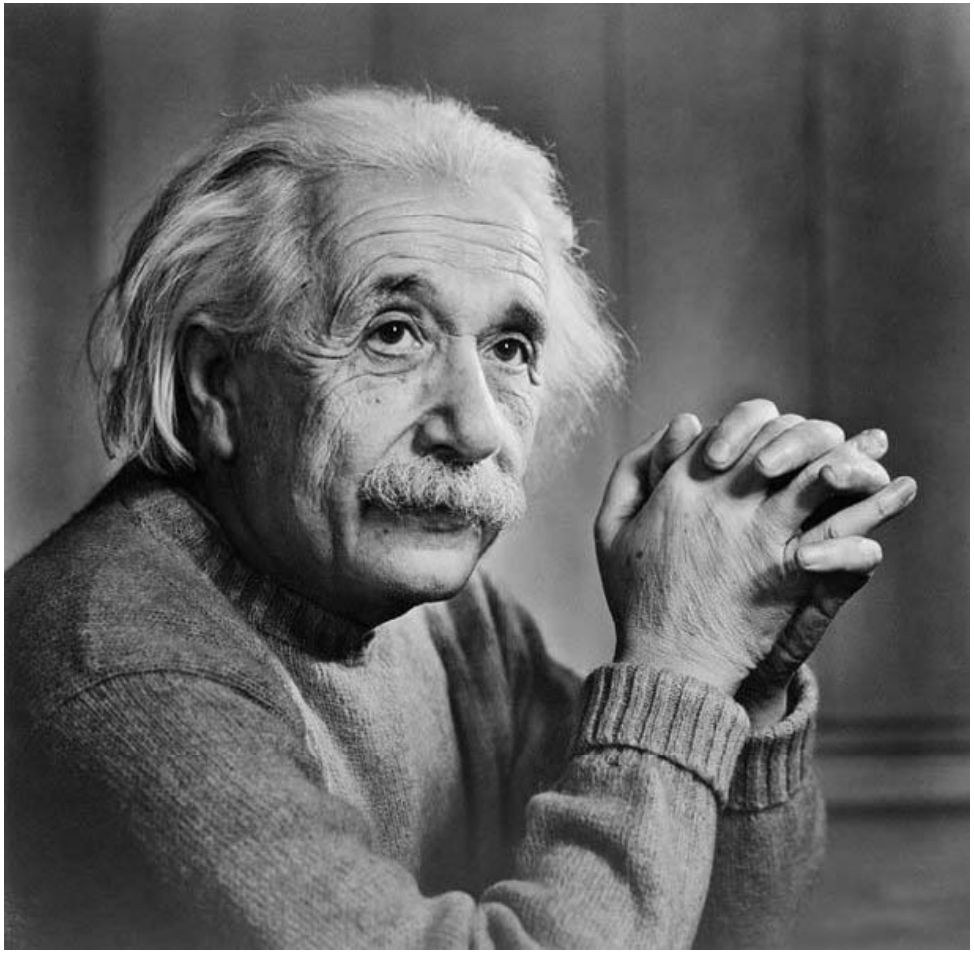
摩爾定律的影響和限制

- 達成摩爾定律的預測所造成的影響
  - Increase performance (運算表現變快)
  - Decrease costs (價格變低)
  - Smaller chips with greater functionality (晶片變小功能變多)
- 由於電晶體每年越做越小, 我們可能會見證到摩爾定律變成過時或不適用的一天的到來.
- 在2018年, 晶片在製程上有可能躍進到16奈米的技術. 如果再經過一次或二次的製造過程, 它會變得更小. 可是在這之後, 我們將會面臨到一些物理上的限制或極限.
  - 耗能和散熱問題
  - 電子直線運動
  - 量子穿隧效應 (quantum tunnelling effect)
- 替代方案: 分子電路學 (molecular electronics) …
- 元件變小 → 量子效應變得重要 (e.g. wave-particle duality 波-粒二象性).
- *量子計算* ***(quantum computation)***

量子年表

1900 年	卜朗克發現卜朗克常數
1905 年	愛因斯坦發表光量子說、特殊相對論、布朗運動
1906 年	愛因斯坦發表量子假說
1910 年	卜朗克接受量子假說
1911 年	拉塞福散射實驗
1913 年	波爾原子模型
1914 年	密立根實驗證實光電效應
1925 年	海森堡的矩陣力學
1924 年	迪．布羅意的物質波
1926 年	薛丁格的波動力學
1927 年	海森堡的測不準原理

愛因斯坦(Albert Einstein)



- 2005年已被物理界訂為國際物理年，旨在紀念愛因斯坦(Albert Einstein)於1905年，寫下近代物理史上最重要的一頁。
- 1905年,愛因斯坦在物理學三個不同領域中取得了歷史性成就，狹義相對論的建立和光量子論與布朗運動的提出，推動了物理學理論的革命。
- 愛因斯坦因在光電效應方面的研究，被授予1921年諾貝爾物理學獎

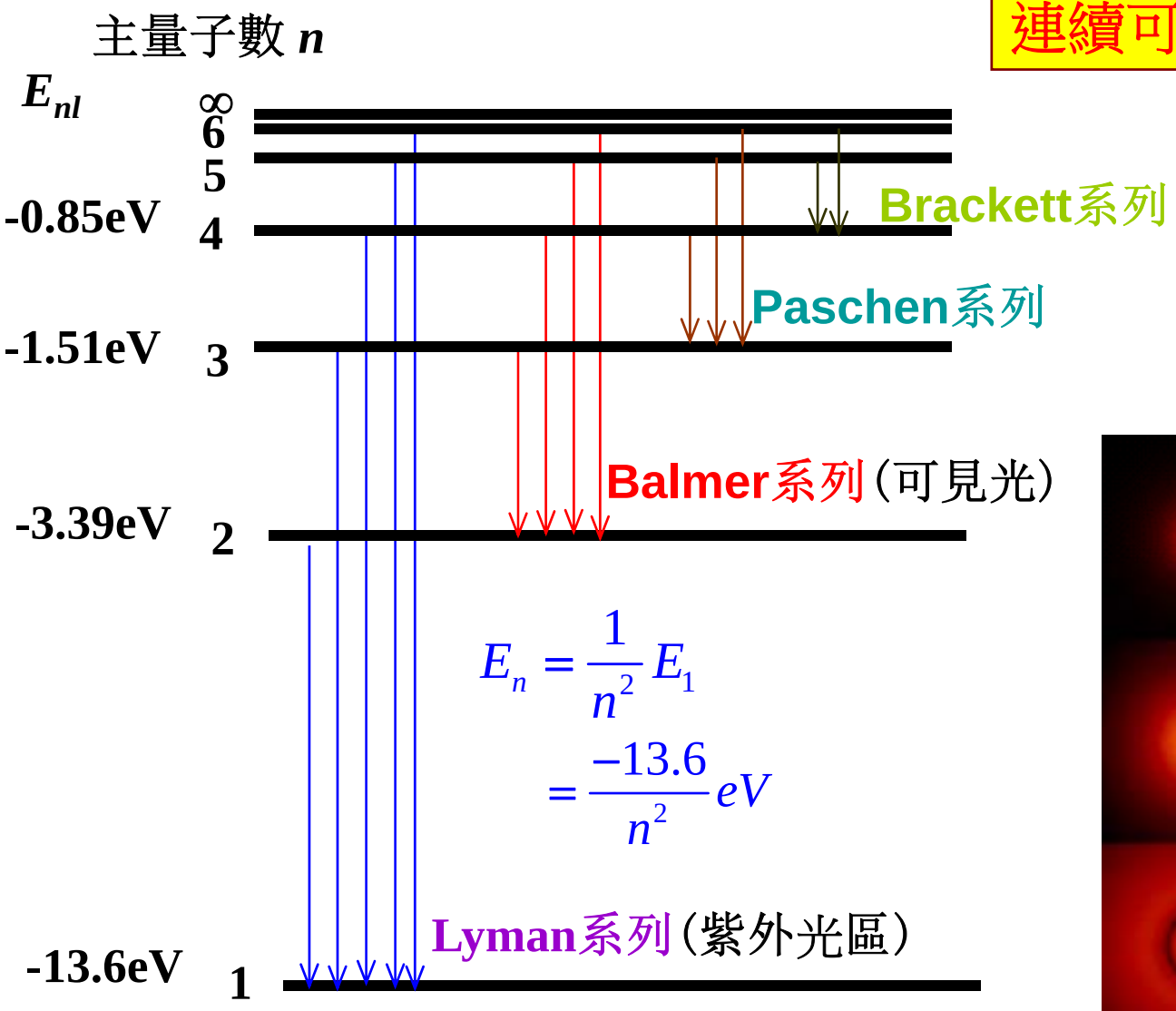
量子力學 (Quantum Mechanics)

- 二十世紀初期的量子理論與實驗進展提供了人們新的物理法則，也就是量子力學，去描述與了解物理現象和測量。
- 到目前為止所有觀測的物理現象都與量子力學的理論和解釋互相一致並無違背。
- **量子(quantum)是什麼? 其實量子的概念是把物質, 物理量不連續化, 不存在所謂之連續可分性。**
- **How successful is quantum mechanics?** **Damn Good!**

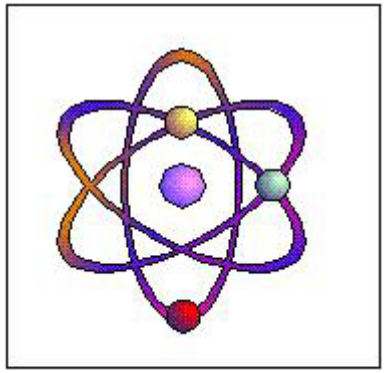
  It is ***unbelievably*** successful.
- 有些精確的實驗測量甚至與量子力學的預測吻合到令人驚歎的準確程度。"*g-2*"; quantum Hall effect: $\sigma_{xy}=n(e^2/h)$
- 量子力學理論和相對論理論是近代物理學的兩大基本支柱。古(經)典力學奠定了現代物理學的基礎，但對於高速運動的物體和微觀條件下的物體，牛頓定律不再適用。相對論解決了高速運動問題；量子力學解決了微觀, 原子尺度條件下的問題。
- 相對論雖然備受各方矚目，但卻不是近來吸引物理界興趣的主要論題，量子力學無疑佔據了這一地位。

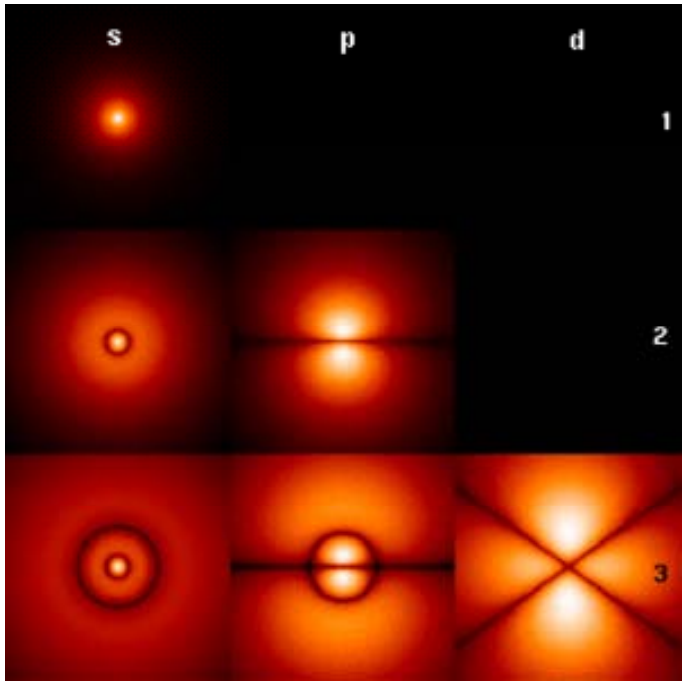
氫原子能階

•量子(quantum)是什麼?
量子的概念是把物質, 物理量不連續化, 不存在所謂之連續可分性。

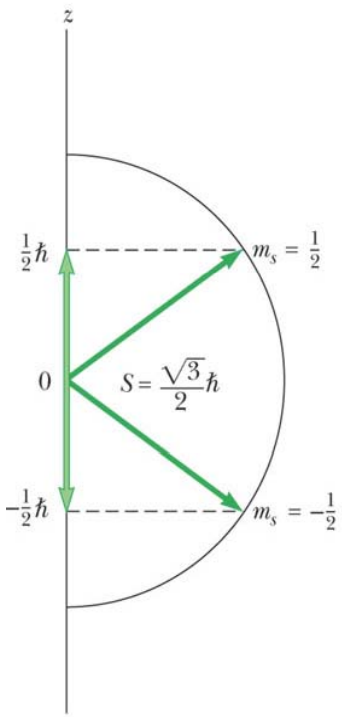


$$E_n = \frac{1}{n^2} E_1 = \frac{-13.6}{n^2} eV$$





Spin quantization



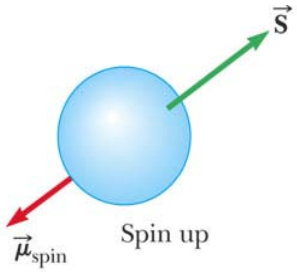
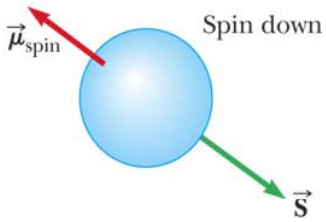
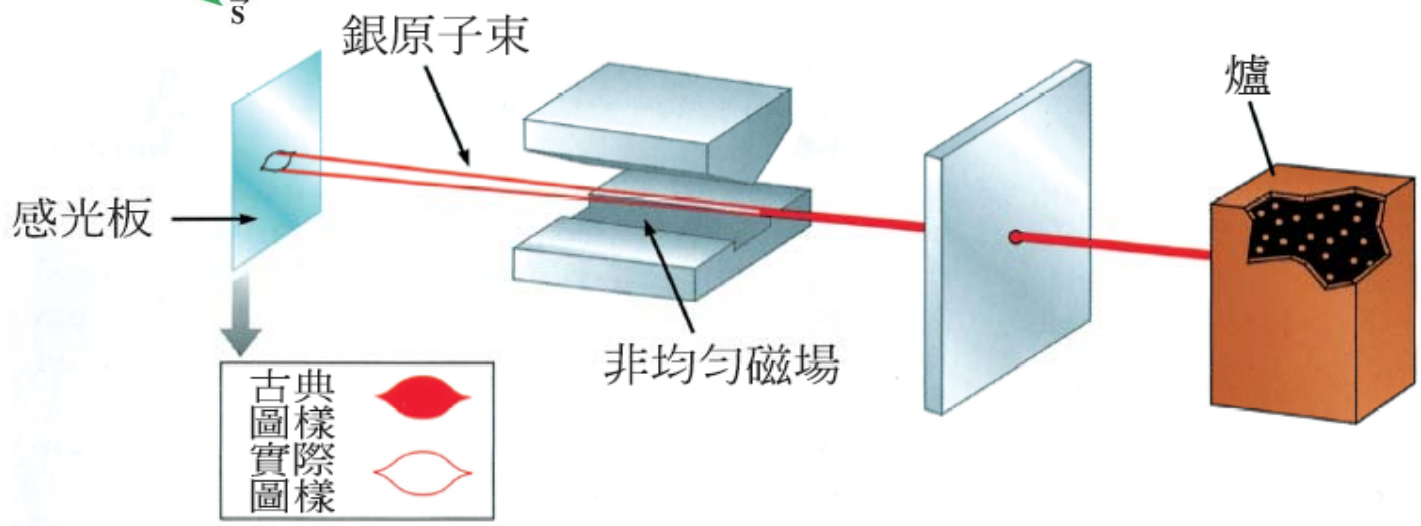


表 29.3 原子中允許的量子數到 $n = 3$

n	1	2				3								
ℓ	0	0	1			0	1			2				
m_ℓ	0	0	1	0	−1	0	1	0	−1	2	1	0	−1	−2
m_s	↑↓	↑↓	↑↓	↑↓	↑↓	↑↓	↑↓	↑↓	↑↓	↑↓	↑↓	↑↓	↑↓	↑↓





量子革命(Quantum revolution)

- 第一次量子革命(大約在19th 世紀末20th世紀初): 給了我們新的定律去描述真實物理性質與現象
  - 用量子力學 (quantum mechanics) 去了解已經存在的事物現象 (electron wavefunction 電子波函數, periodic table 週期表, how metals and semiconductor behaved 金屬和半導體, …).
  - 科學和技術上的突破: 電腦晶片(或半導體)工業和所謂的資訊時代 (Information Age)的來臨, 太陽電池 (solar cell), 雷射 (laser), …
- 量子科技工程的進展 (20th 世紀末之前到未來 …): 利用量子力學的原則去發展出新的科技.
  - 主動地去使用量子力學來轉化物理世界的量子面貌成為我們想設計出的高度非自然存在的量子狀態.
- 科技和科學的差別: 能夠去設計, 策劃, 改變, 建造我們周遭事物, 使它達成我們所想要達成的目地, 不是只是去解釋它而已.
- 把量子力學當作科學, 它可能已經成熟了.
- 量子科技現在正在以它自己的實力浮上檯面, 受人注目.

量子計算與量子資訊

- 量子計算與量子資訊是一門使用量子力學系統去達成資訊處理與計算工作的新興研究學門。
- 它是以量子力學準則為運算與工作基礎去研究、發現和進而設計出比古典更快速的或更有效的、或在古典上不可能的運算與資訊處理方法的新興且蓬勃發展的學門領域。

量子資訊科技
Quantum information science and technology

- Quantum algorithms and quantum computation (量子演算法和量子計算)
  - Shor's quantum factoring algorithm
  - Grover's search algorithm
- Quantum teleportation (量子傳動)
- Quantum cryptography (量子密碼學)
- Quantum information theory
  - Quantum channel capacity
  - Superdense coding and quantum data compression
  - Quantum error correction codes: protect against decoherence and noise
  - Entanglement measure
  - ……

RSA密碼學(cryptography)

- RSA密碼系統的基礎建構於去因式分解一個很大位數的半質數的困難度: 網際網路的標準編碼保密方法

  例如: 4633 = 41 x 113

- RSA systems 提供獎金給能夠因式分解他們所公布的很大整數的人 (例如下面整數的獎金為US $200K):

```
2519590847565789349402718324004839857142928212620 4
0320277771378360436620207075955562640185258807844 0
6918290641249515082189298559149176184502808489120 0
7284499268739280728777673597141834727026189637501 4
9718246911650776133798590957000973304597488084284 0
1797429100642458691817195118746121515172654632282 2
1686998754918242243363725908514186546204357679842 3
3871847744479207399342365848238242811981638150106 7
4810451660377306056201619676256133844143603833904 4
1495263443219011465754445417842402092461651572335 0
7787077498171257724679629263863563732899121548314 3
8167899885040445364023527381951378636564391212010 3
9712282212072035 7
```

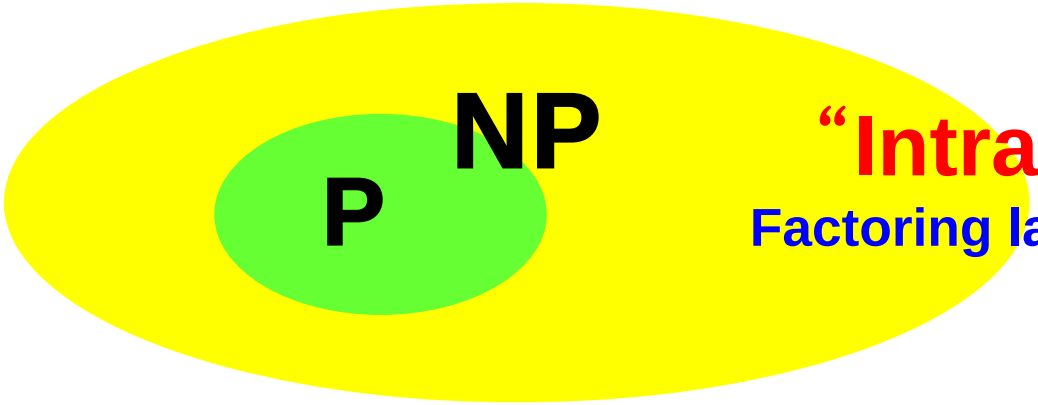
例如: 因式分解一個300位數的半質數; 最好的古典演算法需要10^{24} 步;
用 THz (10^{12} cycles/sec) 的電腦需要 150,000 years

Complexity(複雜度)

N= (# bits to describe the problem,
size of the problem)

(#steps to solve the problem) = Pol(N)
→ "P(polynomial;多項式的)"
: Tractable(易處理的), easy

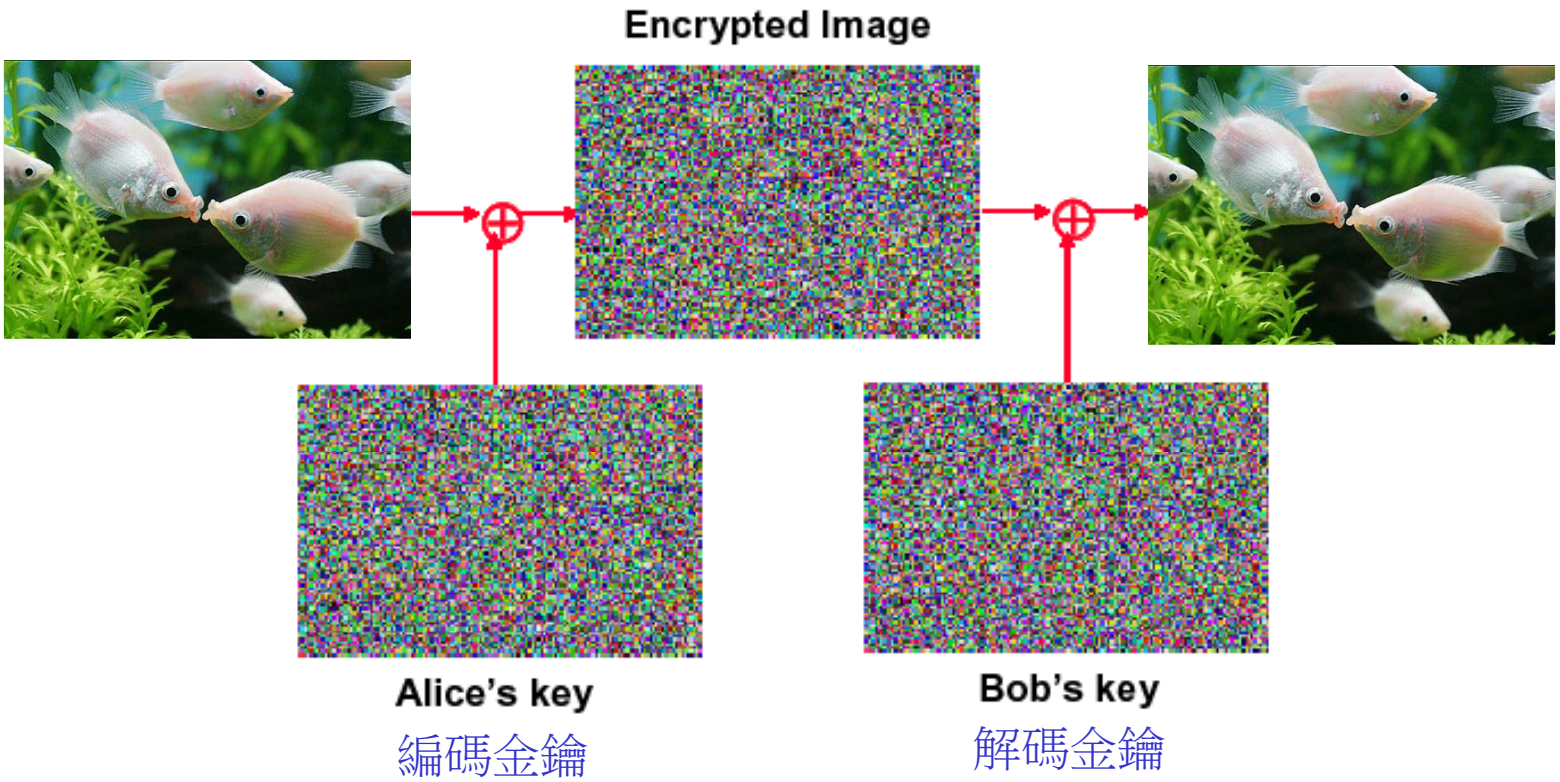
(#steps to verify the solution) = Pol(N)
→ "NP (nondeterministic polynomial;非確定性的多項式時間)"
: Intractable



"Intractable"

Factoring large integers?

編碼保密傳輸



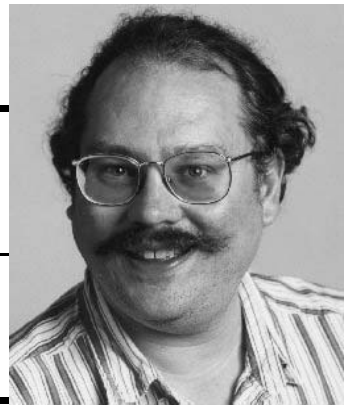
網路銀行 (internet banking): $N = p\,q$

- Public key: 公開的編碼金鑰 (N,e)
- Private key:不公開的解碼金鑰 (N, p,q)

量子演算法與運算加速

- 演算法(*algorithm*): 解決問題的詳細一步接一步的方法
- *電腦 (computer):* 可以執行任何演算法的普適性機器
- Quantum factoring(因式分解)algorithm : exponential speed-up (Shor's Algorithm) Example: factor a 300-digit number

Best classical algorithm: 10^{24} steps	Shor's quantum algorithm: 10^{10} steps
On classical THz computer: 150,000 years	On quantum THz computer: <1 second



Peter Shore

- Quantum search of an unsorted database: quadratic speed-up (Grover's Algorithm)
  - Example: name 姓名→ phone number 電話號碼 (easy 簡單)
  - phone number 電話號碼 → name 姓名 (hard 困難)
  - Classical: $O(n)$, Grover's: $O(\sqrt{n})$
- Simulation of quantum systems: up to exponential speed-up.

什麼是量子位元(quantum bit)?

- Classical bit: 0 or 1; 電晶體電壓的高或低
- **Quantum bit (qubit):** QM two-state system

  量子力學的兩種狀態的系統
- 一個量子位元有兩種可能的狀態 $|0\rangle$ or $|1\rangle$
- 一個量子位元狀態可以處在 $|0\rangle$ and $|1\rangle$ 的線性疊加態

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

α 和 β 可以是複數 (complex numbers) 並且 $|\alpha|^2 + |\beta|^2 = 1$

- 兩個量子位元的狀態可以處在此線性疊加態

$$|\psi\rangle = C_0|00\rangle + C_1|01\rangle + C_2|10\rangle + C_3|11\rangle \text{ 且 } \sum_{j=0}^{3}|C_j|^2 = 1$$

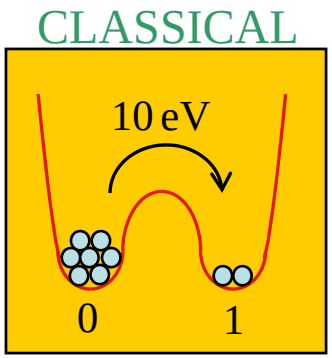
- 封閉的量子系統隨時間的演化是 Unitary: $|\psi'\rangle = U|\psi\rangle$

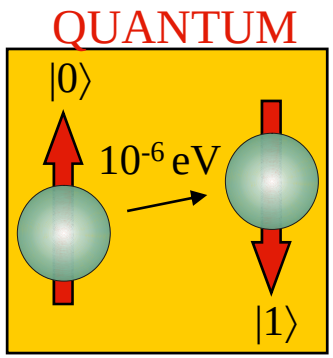
量子位元的物理表象

Quantum Bits

量子位元的物理表象

- Spin states;  $|0\rangle$ and $|1\rangle$
- Charge states; left or right 
- Flux states; L or R
- Energy states, ground or excited states
- Photon polarizations; H or V; L or R
- Photon number (Fock) states;
- More …





量子測量(quantum measurement)

- 量子測量是量子力學的幾個基本假設之一

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

$$= \frac{1}{\sqrt{2}}\left[(\alpha+\beta)|+\rangle + (\alpha-\beta)|-\rangle\right]$$

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

- 假如我們用 $|0\rangle$ 和 $|1\rangle$ 作為測量的基底(basis), 每次測量後的系統狀態 不是 $|0\rangle$ 就是 $|1\rangle$
  - 測量結果得到 $|0\rangle$ 的機率 $|\alpha|^2$
  - 測量結果得到 $|1\rangle$ 的機率 $|\beta|^2$
- 假如我們用 $|+\rangle$ 和 $|-\rangle$ 作為測量的基底(basis), 每次測量後的系統狀態 不是 $|+\rangle$ 就是 $|-\rangle$
  - 測量結果得到 $|+\rangle$ 的機率 $|\alpha+\beta|^2/2$
  - 測量結果得到 $|-\rangle$ 的機率 $|\alpha-\beta|^2/2$

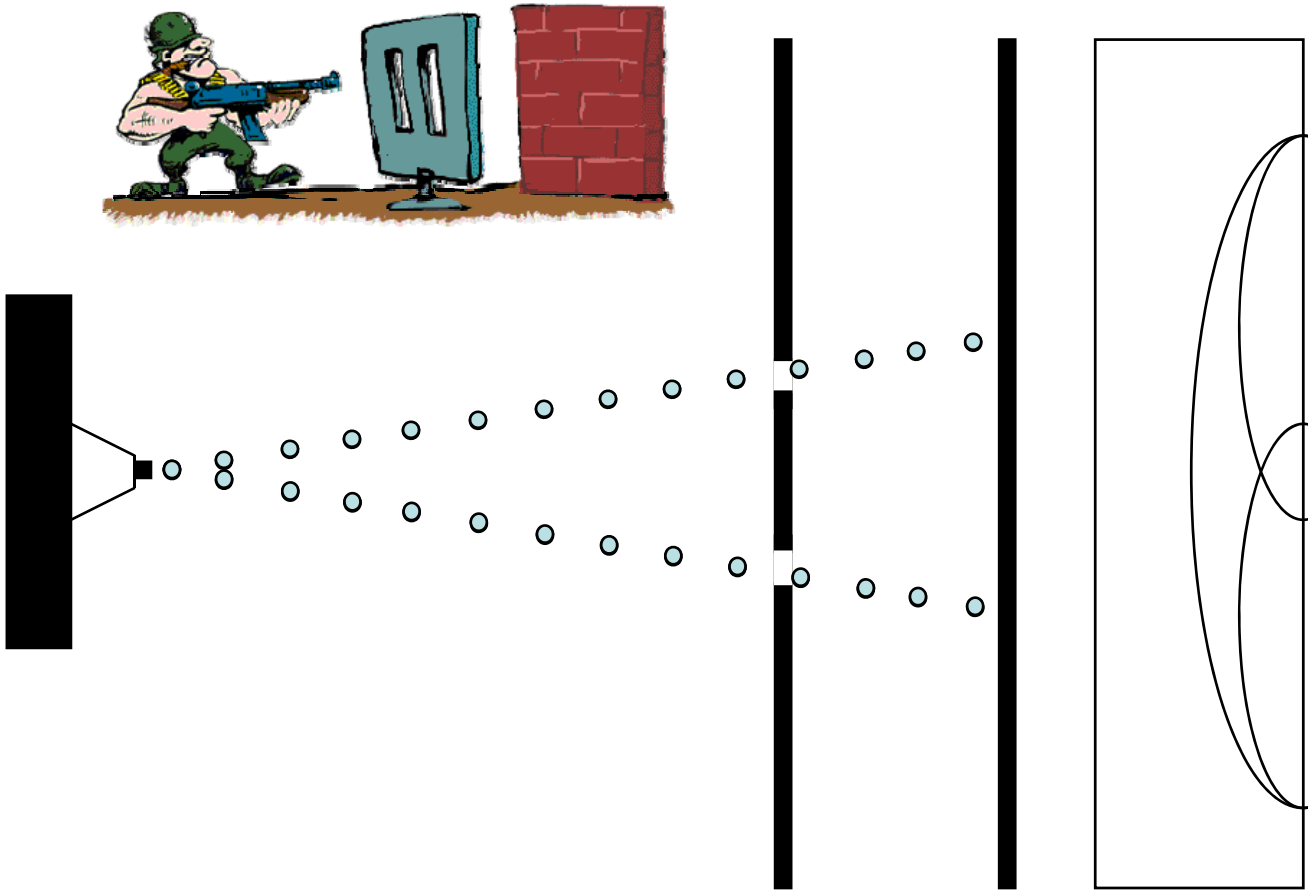
Does God play dice with the Universe?

- **Einstein** was one of the founders of quantum mechanics, yet he disliked **the randomness that lies at the heart of the theory** despite evidence suggesting so**. God does not, he famously said, play dice.**
- **However, quantum theory has survived a century of experimental tests.**

- **Einstein** suspected that there may be a 'hidden level' -- a mechanism which we are yet unable to detect -- that would give a deterministic explanation for apparently random processes at the quantum level.
- **Copenhagen School** believed that the behavior of the fundamental constituents of matter is not deterministic but indeterministic. In their view, events at the microphysical level occur **"randomly**", "**by pure chance**" - meaning that they aren't determined by any causes whatever. The way the universe itself behaves at the atomic level is **as if there were a god who was playing dice with it.**

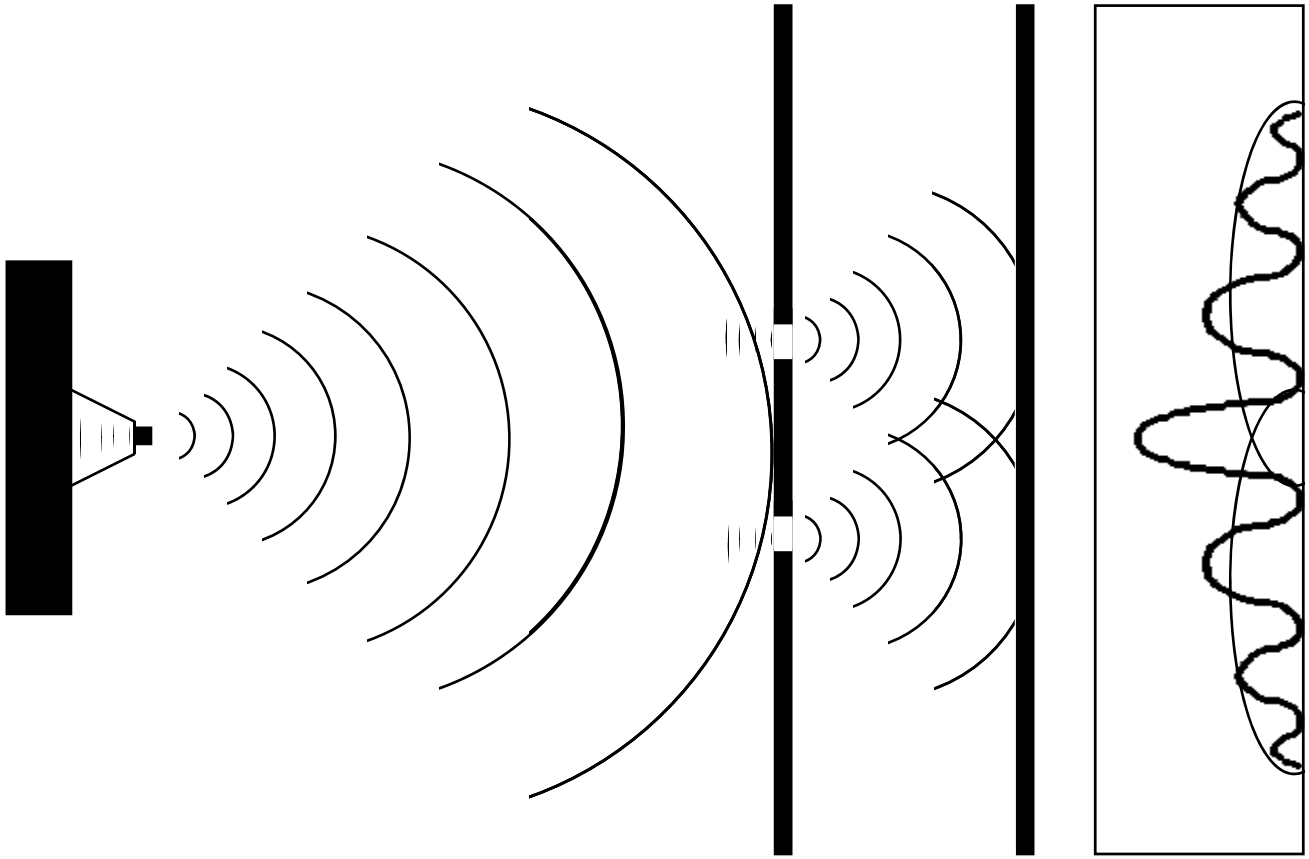
雙狹縫實驗
(Double-slit experiment)

子彈 (Bullets)



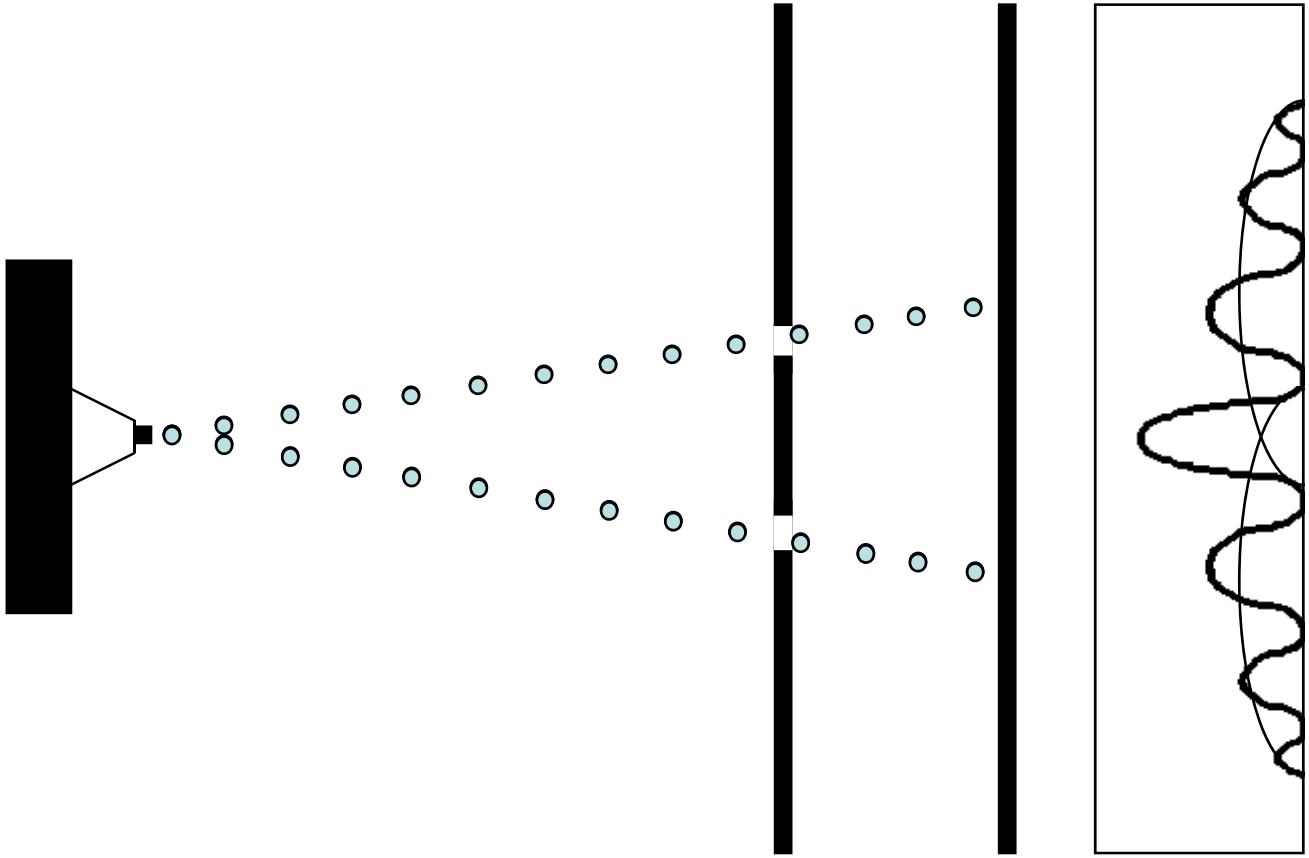
楊氏雙狹縫實驗
(Double-slit experiment)

聲波(Sound Waves)

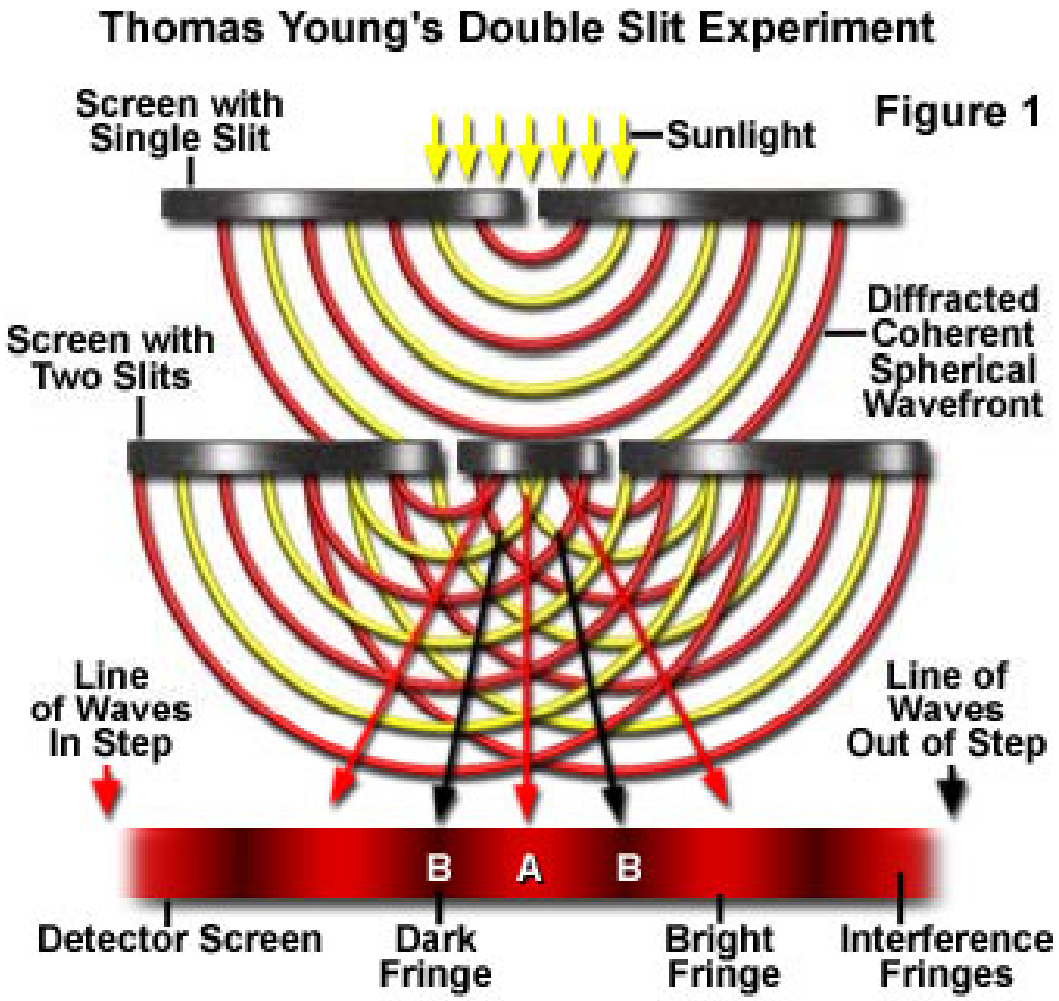


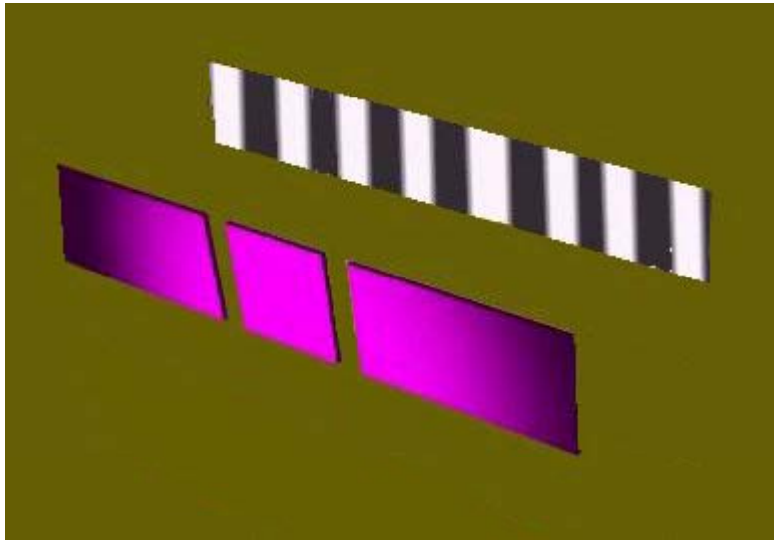
楊氏雙狹縫實驗
(Double-slit experiment)

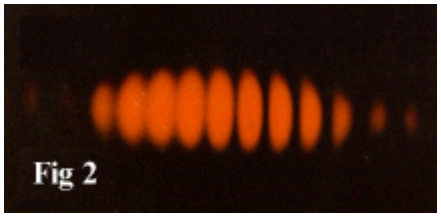
電子(Electrons)



楊氏雙狹縫實驗
(Double-slit experiment)

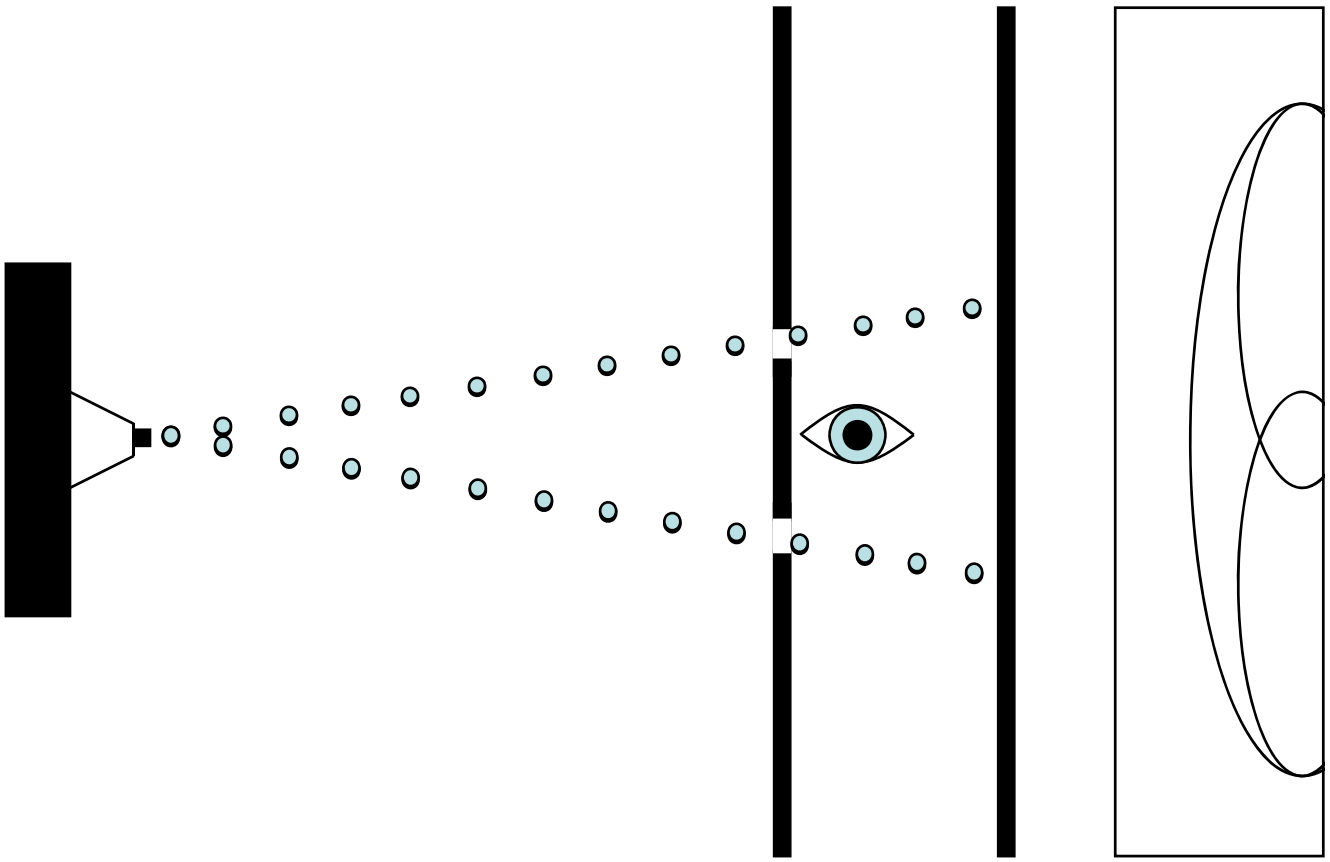




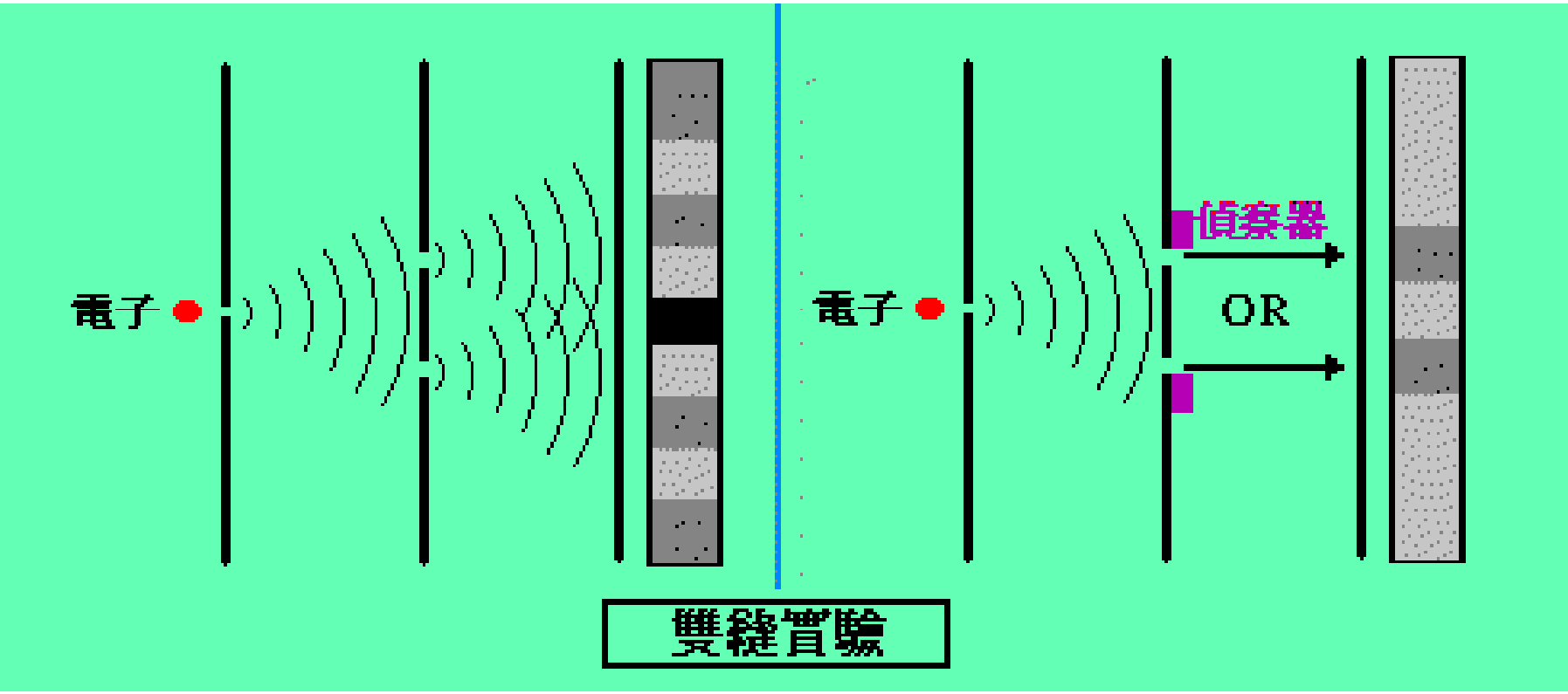


楊氏雙狹縫實驗
(Double-slit experiment)

觀測電子(Observing Electrons)



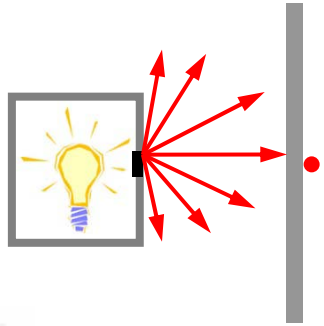
楊氏雙狹縫實驗
(Double-slit experiment)

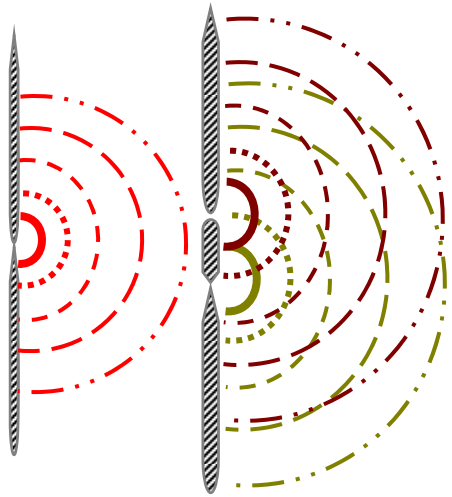


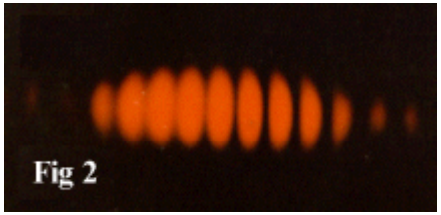
- 假如板上一個孔被蓋著,電子當然只會在剩餘的孔中穿過,而不發生干涉
- 假如我們在孔的兩邊各放一偵察器來探究竟電子穿過那一個孔,電子竟好似知你有心觀測它,竟然堆不出干涉條紋

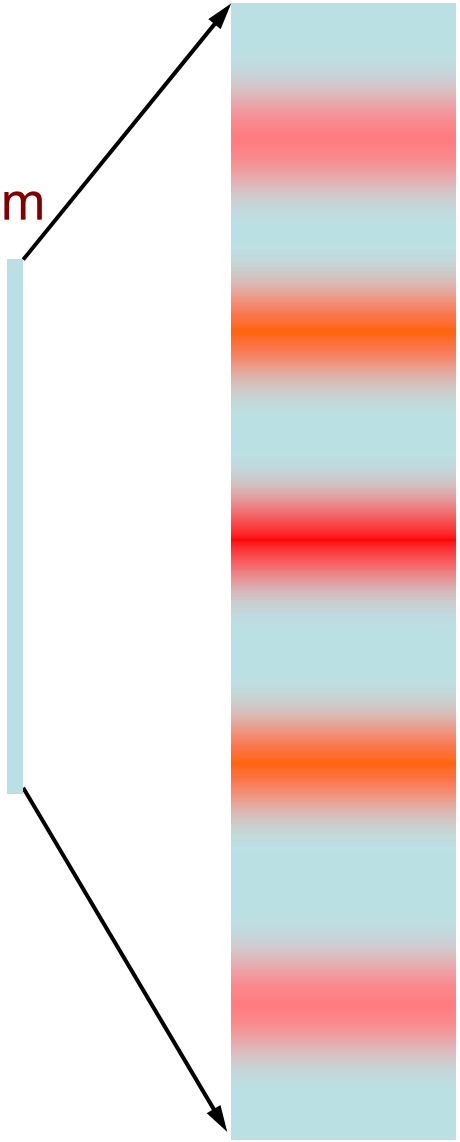
Pauli Dirac: The photon (electron) interferes with itself

No more than one photon can pass the slit each time.



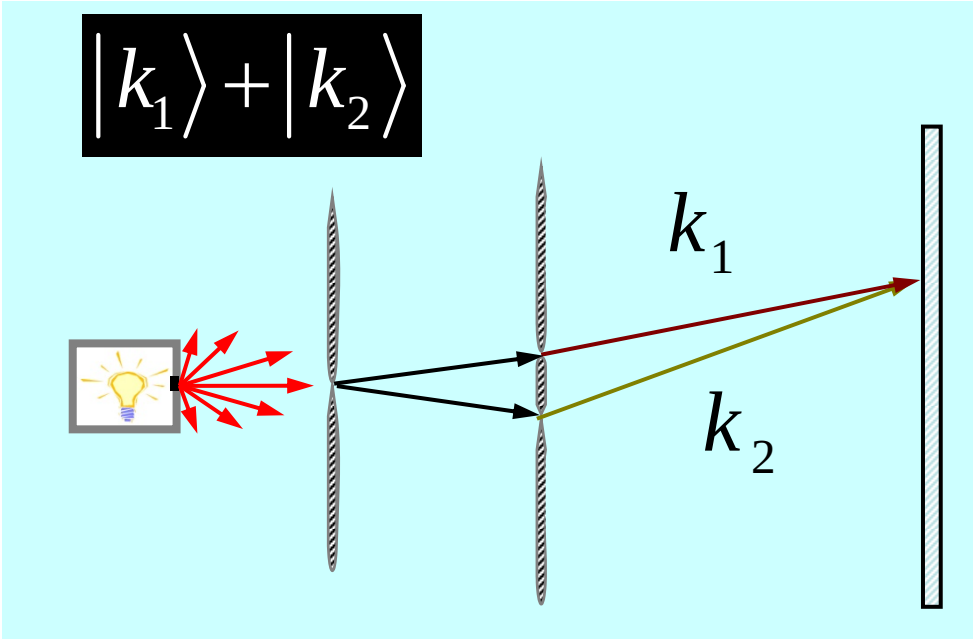






Courtesy of R.B. Liu

Superposition is not a mixture of two pathways

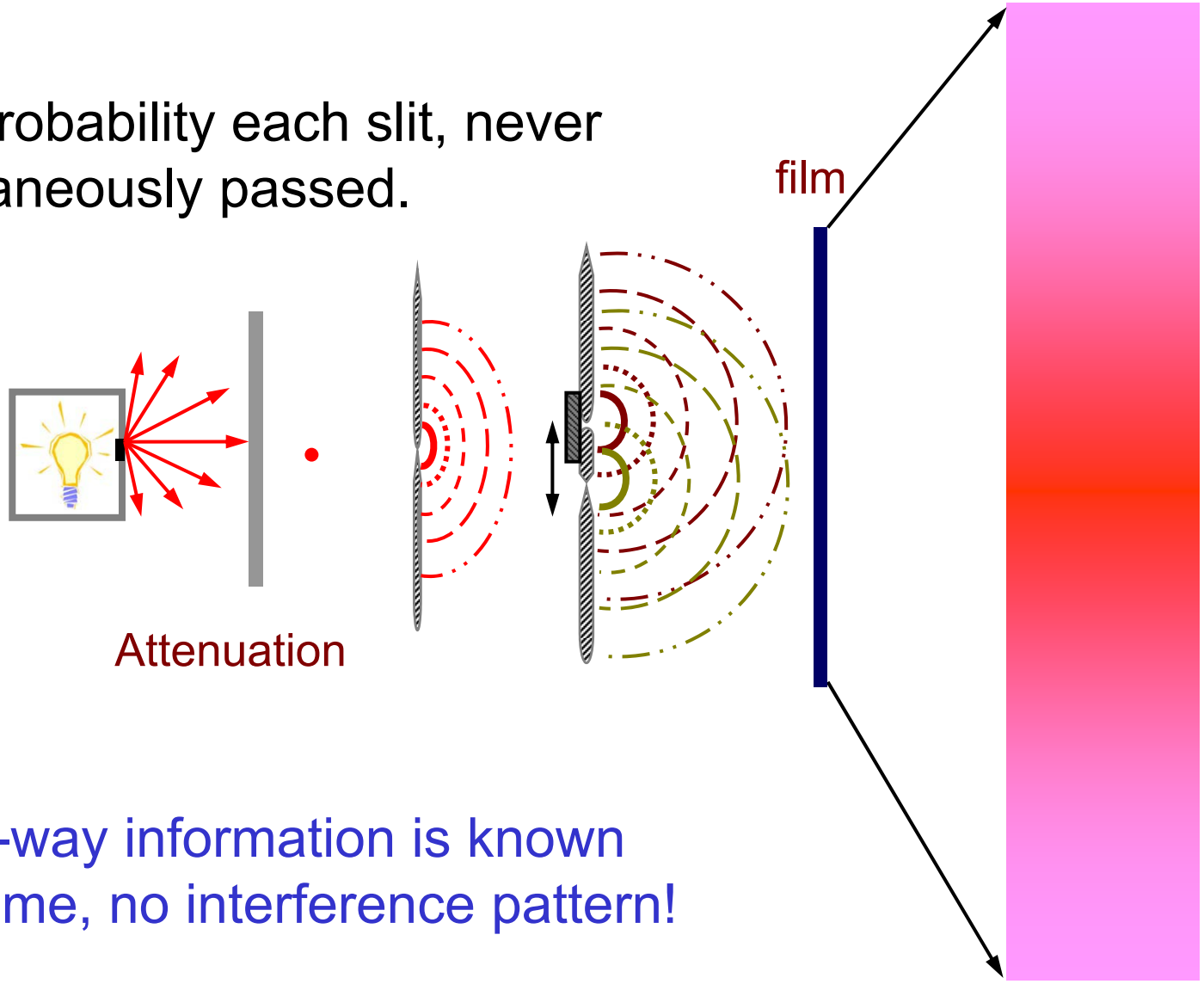


The photon passes two slits simultaneously. Or if which-way is known, no interference!

Courtesy of R.B. Liu

Decoherence I: Which-pathway pre-selected

50% probability each slit, never simultaneously passed.

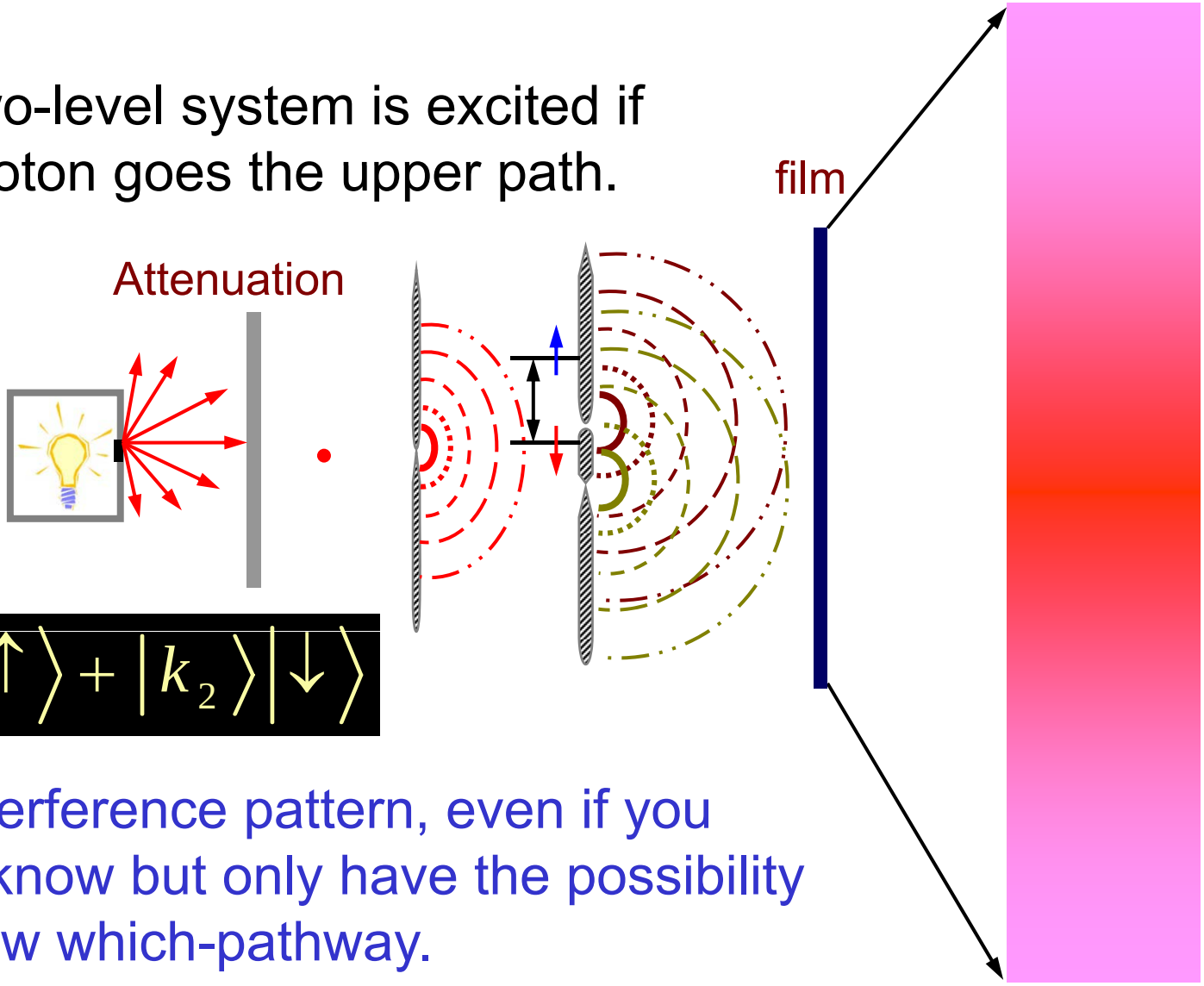


Which-way information is known each time, no interference pattern!

Courtesy of R.B. Liu

Decoherence II: Which-pathway recorded

The two-level system is excited if the photon goes the upper path.



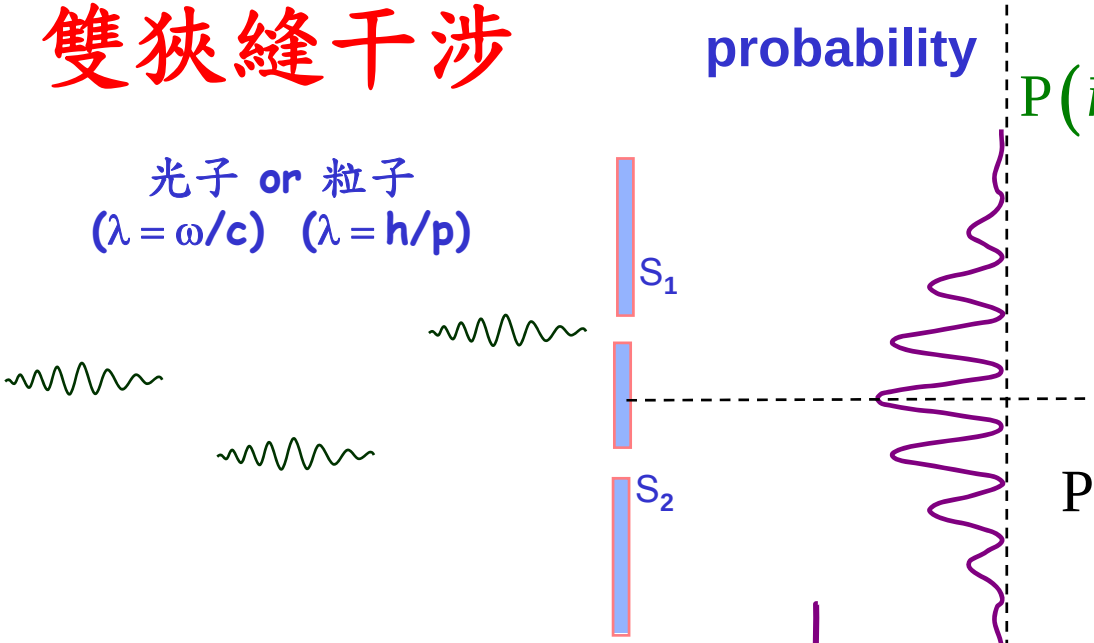
$$|k_1\rangle|\uparrow\rangle + |k_2\rangle|\downarrow\rangle$$

No interference pattern, even if you don't know but only have the possibility to know which-pathway.

Courtesy of R.B. Liu

雙狹縫干涉

光子 or 粒子
$(\lambda = \omega/c)$ $(\lambda = h/p)$

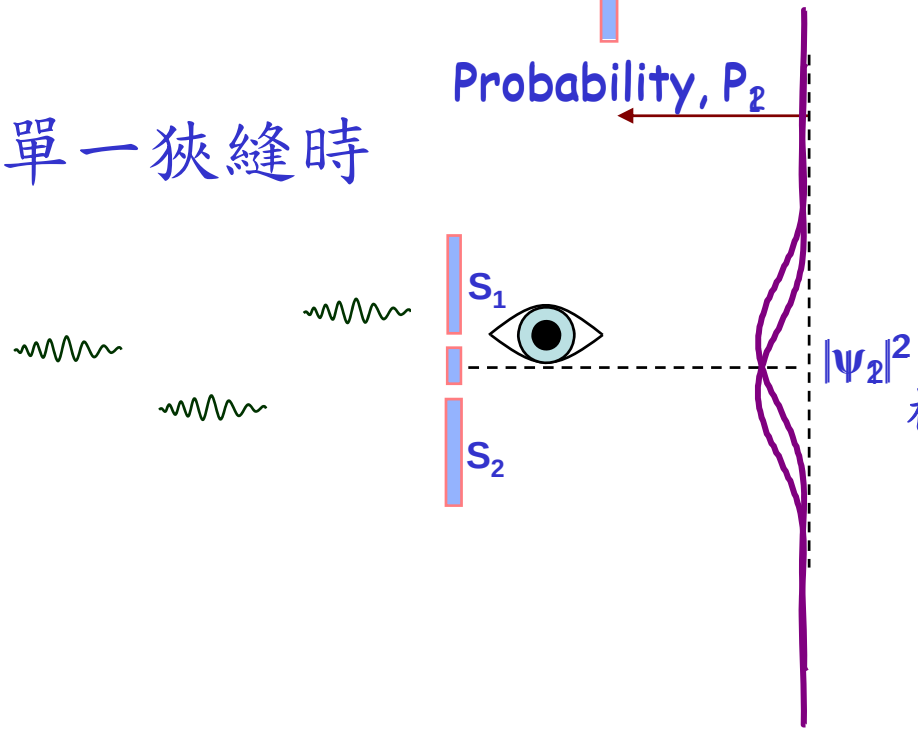


$$P(\vec{r}, t) \neq P_1 + P_2$$
$$\neq |\Psi_1(\vec{r}, t)|^2 + |\Psi_2(\vec{r}, t)|^2$$

$$P(\vec{r}, t) = |\Psi_1(\vec{r}, t) + \Psi_2(\vec{r}, t)|^2$$
$$= |\Psi(\vec{r}, t)|^2$$

物質波遵守波的合成原理

單一狹縫時



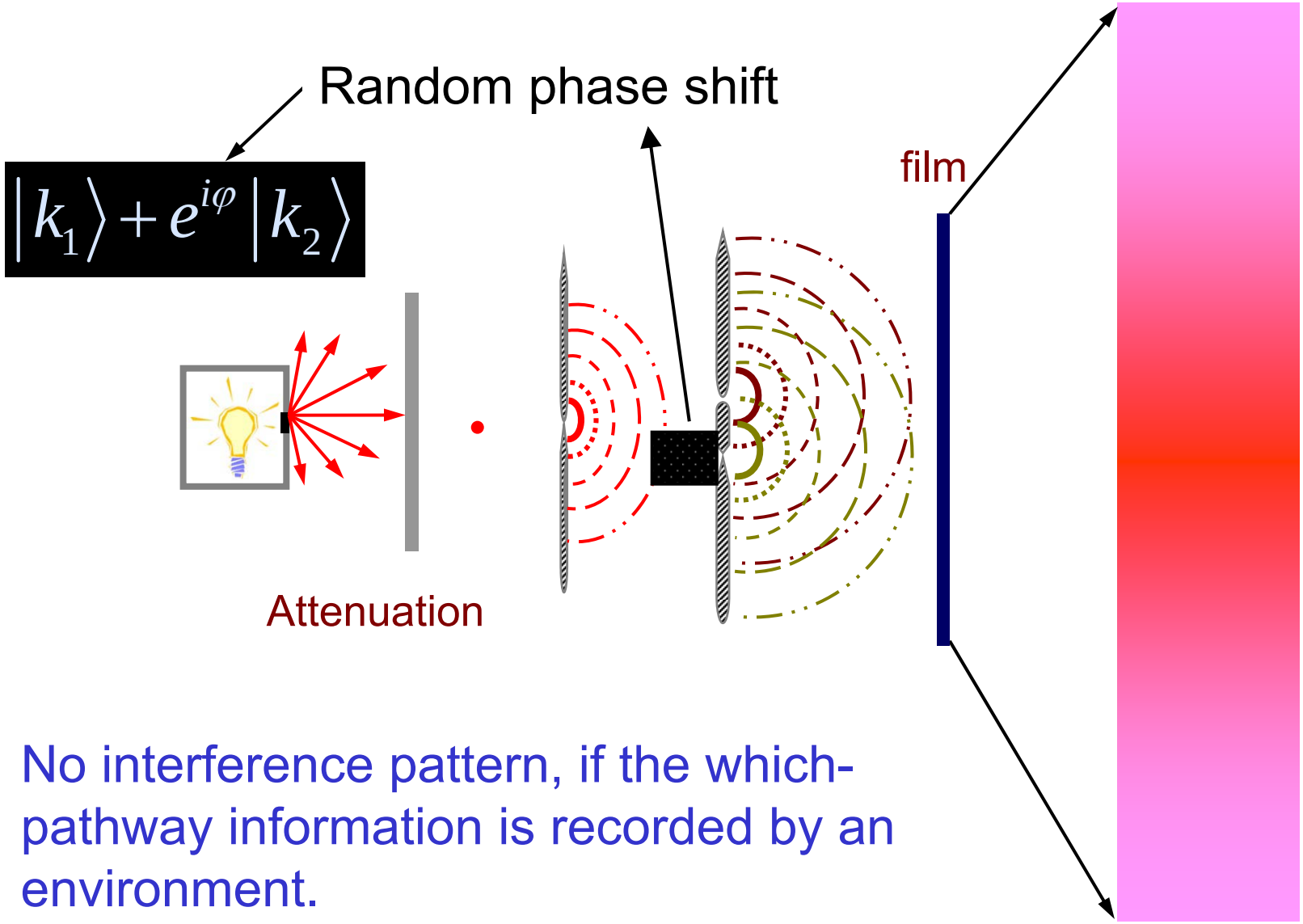
機率密度

機率密度振福

$$P(\vec{r}, t) = ?$$
$$\Psi(\vec{r}, t)$$

$$P(\vec{r}, t) = P_1 + P_2$$
$$= |\Psi_1(\vec{r}, t)|^2 + |\Psi_2(\vec{r}, t)|^2$$

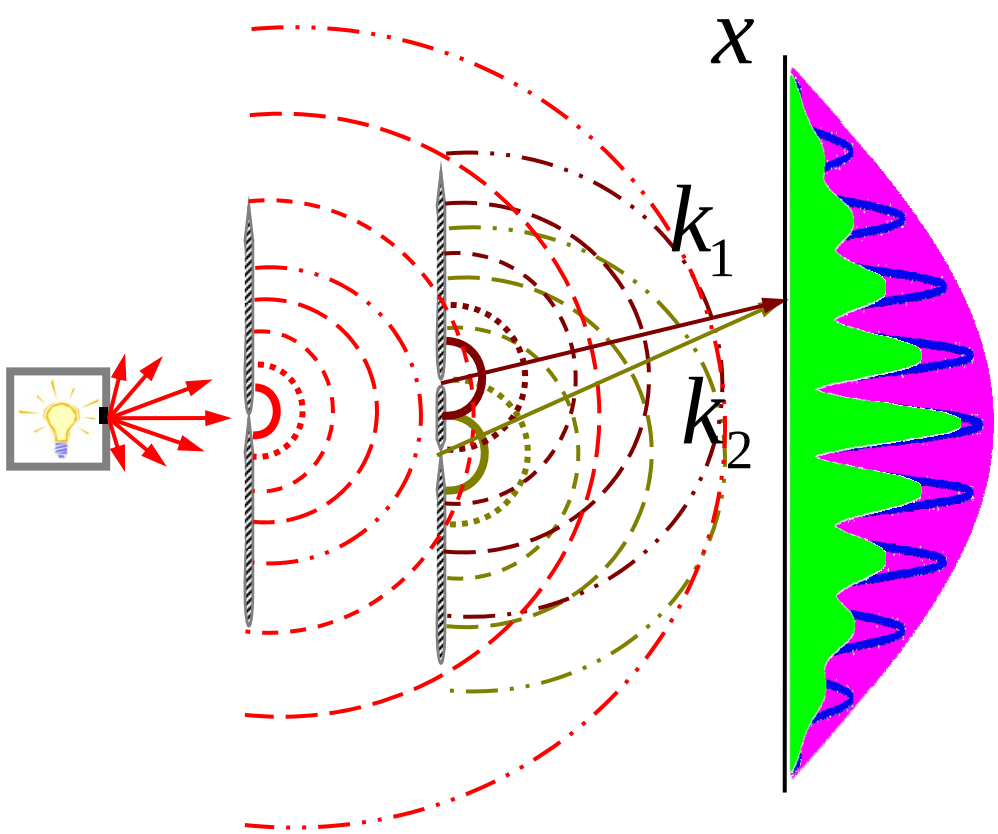
Decoherence III: Random phase

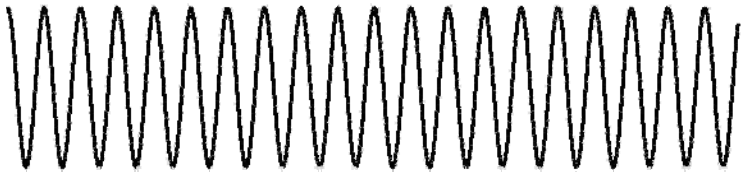


No interference pattern, if the which-pathway information is recorded by an environment.

Courtesy of R.B. Liu

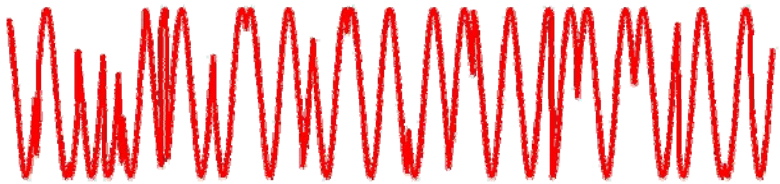
An example in Classical Physics





$$\left|\cos\left(k_1 x\right)+\cos\left(k_2 x\right)\right|^2$$

Random Phase



$$\left\langle\left|\cos\left(k_1 x\right)+\cos\left(k_2 x+\varphi_x\right)\right|^2\right\rangle$$

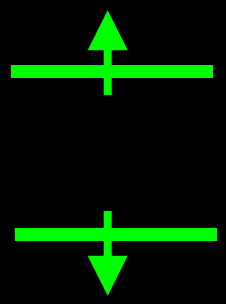
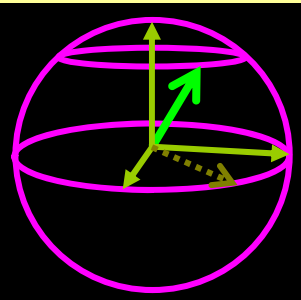
x_c Coherence memory length

How long the phase memorizes its history

$$1+\cos\left(\delta k\cdot x\right)\exp\left(-x/x_c\right)$$

Courtesy of R.B. Liu

Quantum information vs. Classical information

System	qubit	bit	Vector
Basis states			
Evolution		0 or 1	Continuous
Output	Quan.Meas.: digital	digital	analogous

- Quantum states are waves: Superposition
- Quantum states are particles: Digital output

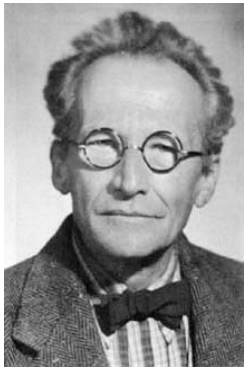
Entanglement

Alice

Bob

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

$$|\psi\rangle \neq |a\rangle|b\rangle$$



Schrödinger (1935): "I would not call [entanglement] *one* but rather *the* characteristic trait of quantum mechanics, the one that enforces its entire departure from classical lines of thought."

Entanglement and classicality

Bell (1964) and Aspect (1982): Entanglement can be used to show that no "locally realistic" (that is, classical) theory of the world is possible.

Further reading: Asher Peres, "Quantum theory: concepts and methods", Kluwer (1993).

是什麼使得量子電腦效力強大
（what makes quantum computer powerful)?

- Exponentiality(指數性質): computational state space is exponential in the physical size of the system (2^n).
- Quantum parallelism(量子平行性): by using superposition of quantum states, the computer is executing the algorithm on all possible inputs at once.

$$\text{e.g., } |\psi\rangle = (|00\rangle + |01\rangle + |10\rangle + |11\rangle)/2.$$

- Complex amplitudes or Interference(複數振幅或干涉)
- Quantum entanglement (composite systems) 量子糾纏

$$\text{Separable:} \frac{1}{\sqrt{2}}\left(|0\rangle_A |0\rangle_B + |0\rangle_A |1\rangle_B\right) = |0\rangle_A \otimes \frac{1}{\sqrt{2}}\left(|0\rangle_B + |1\rangle_B\right)$$

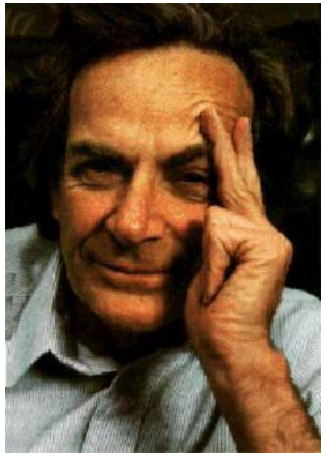
$$\text{Entangled:} \frac{1}{\sqrt{2}}\left(|0\rangle_A |1\rangle_B - |1\rangle_A |0\rangle_B\right) \neq |\psi\rangle_A \otimes |\phi\rangle_B$$

- More…

量子規則和更高階原則
Quantum rules and high-level principles

- Perhaps we don't really know what makes quantum systems more powerful than a classical computer
- Knowing the rules of the game (象棋, 西洋棋, 圍棋)
  $\neq$ Understanding the game
- Knowing the rules of Quantum Mechanics
  $\neq$ Understanding Quantum Mechanics
- ***Anybody who is not shocked by quantum theory has not understood it.***

  -Niels Bohr 波爾 Nobel Prize (1922)
- What high-level principles are implied by quantum mechanics?
- 費因曼 **(Richard Feynman,** Nobel Prize (1965)**):**
  "I think I can safely say that nobody understands the quantum theory."
  我想持平來說沒有人真正了解量子理論



Coherence, constant phase difference in two or more waves over time (Columbia Electronic Encyclopedia 2003)

Decoherence, some one is out of phase

Often because of entanglement with the environment

Recoherence, by a little control

Decoherence

- Process by which a quantum superposition state decays into a classical, statistical mixture of state.
- In system-environment models, decoherence is caused by interactions between the system and its environments.
- As the system and bath evolve under the total Hamiltonian, they become entangled.
- By tracing over the environmental degrees of freedom, the reduced density matrix of the system of interest at later times is no longer pure and the system is said to have decohered.

Superposition and entanglement

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

$$a|0\rangle + b|1\rangle e^{-i\omega_{10}t}$$

$$a|0\rangle + b|1\rangle e^{-i\omega_{10}t+i\varphi}$$

- Entanglement (composite systems)

$$\text{Separable: } |\varphi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A |0\rangle_B + |0\rangle_A |1\rangle_B\right) = |0\rangle_A \otimes \frac{1}{\sqrt{2}}\left(|0\rangle_B + |1\rangle_B\right)$$

$$\text{Entangled: } |\Psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A |1\rangle_B - |1\rangle_A |0\rangle_B\right) \neq |\psi\rangle_A \otimes |\phi\rangle_B$$

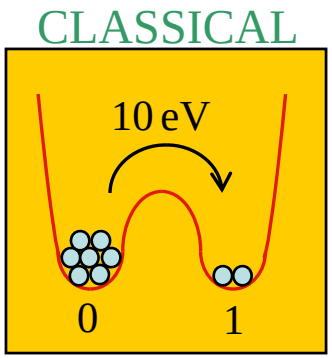
- Partial trace (composite systems)

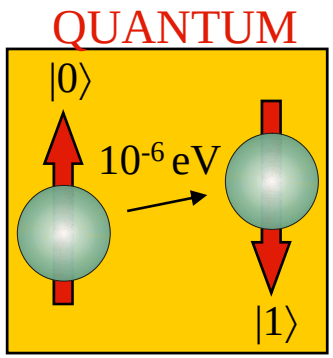
$$Tr_A\left[|\varphi\rangle\langle\varphi|\right] = \frac{1}{2}\left(|0\rangle + |1\rangle\right)\left(\langle 0| + \langle 1|\right)_B \quad \text{pure state}$$

$$Tr_A\left[|\Psi\rangle\langle\Psi|\right] = \frac{1}{2}\left(|0\rangle\langle 0| + |1\rangle\langle 1|\right)_B \quad \text{mixed state}$$

量子位元的物理表象

- Spin states;  $|0\rangle$ and $|1\rangle$
- Charge states; left or right 
- Flux states; L or R
- Energy states, ground or excited states
- Photon polarizations; H or V; L or R
- Photon number (Fock) states;
- More …





Requirements for physical implementation of quantum computation

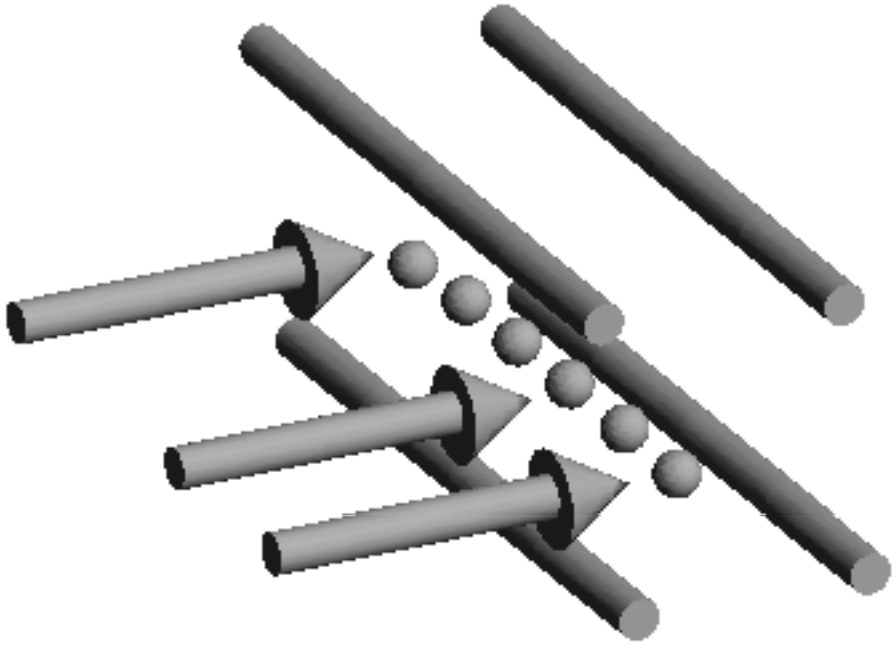
- A scalable physical system with well characterized qubits
- The ability to initialize the state of the qubits to a simple fiducial state, such as $|000\ldots\ldots\rangle$.
- Long relevant decoherence times, much longer than the gate operation time
- A universal set of quantum gates
- A qubit-specific measurement capability

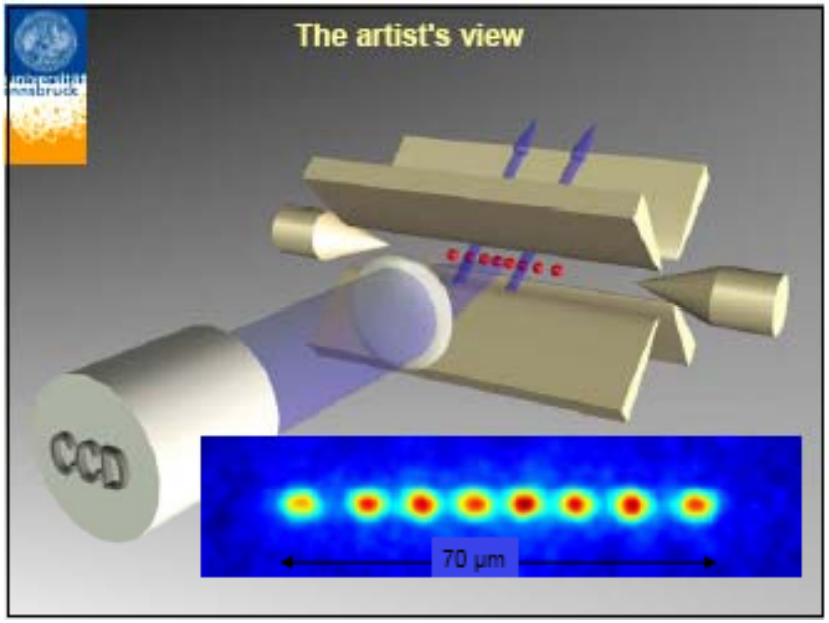
Physical systems actively considered for quantum computer implementation

- Liquid-state NMR
- NMR spin lattices
- Linear ion-trap spectroscopy
- Neutral-atom optical lattices
- Cavity QED + atoms
- Linear optics with single photons
- Nitrogen vacancies in diamond
- Electrons on liquid He
- Small Josephson junctions
  - “charge” qubits
  - “flux” qubits
- Impurity spins in semiconductors
- Coupled quantum dots
  - Qubits: spin,charge, excitons
  - Exchange coupled, cavity coupled

Ion Traps (離子阱)

- Ions are laser cooled using resolved sideband cooling, and the temperature of a ion's vibrational degree of freedom can be 10^{-3} K.
- Couple lowest centre-of-mass modes to internal electronic states of N ions by external lasers.

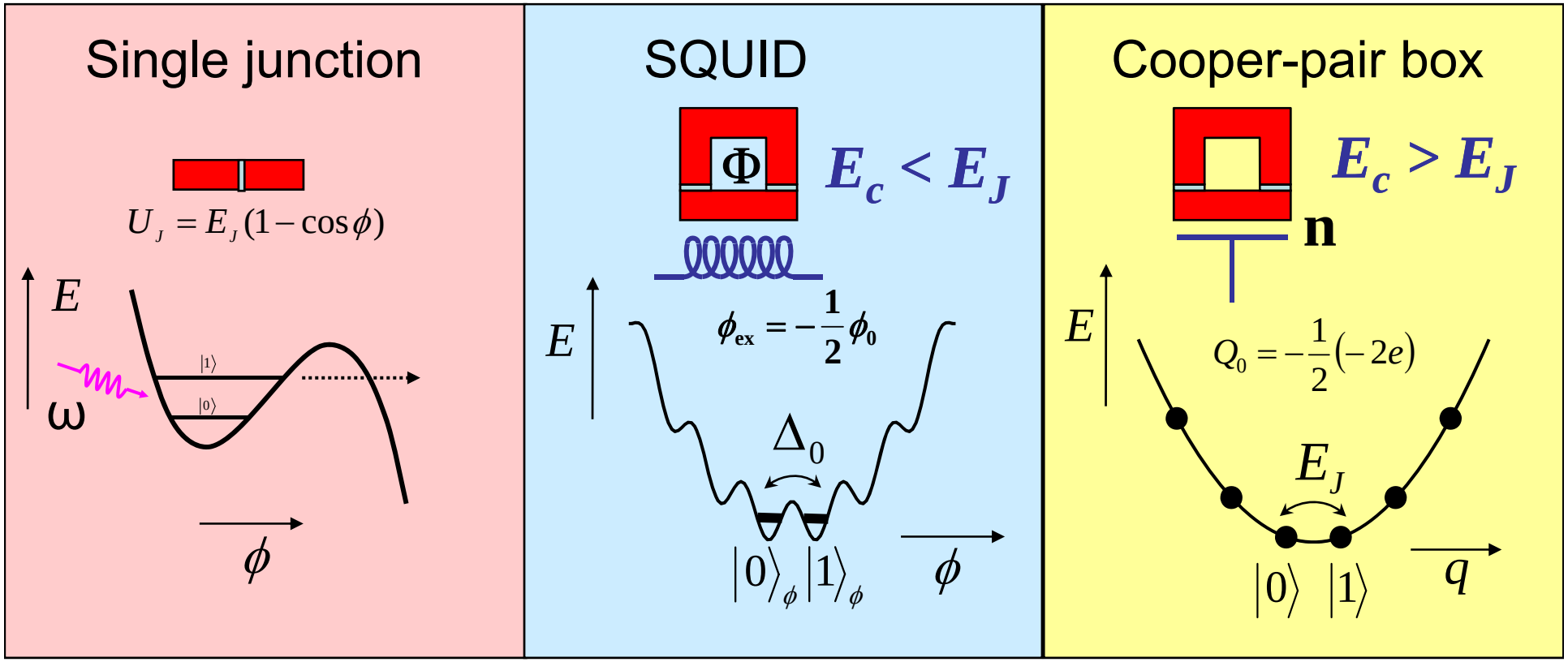




- Excellent optical readout achieved via fluorescence shelving in ion trap systems

超導體 Josephson-junction-based qubits

“ phase”	"flux"	“ charge”
Single junction	SQUID	Cooper-pair box

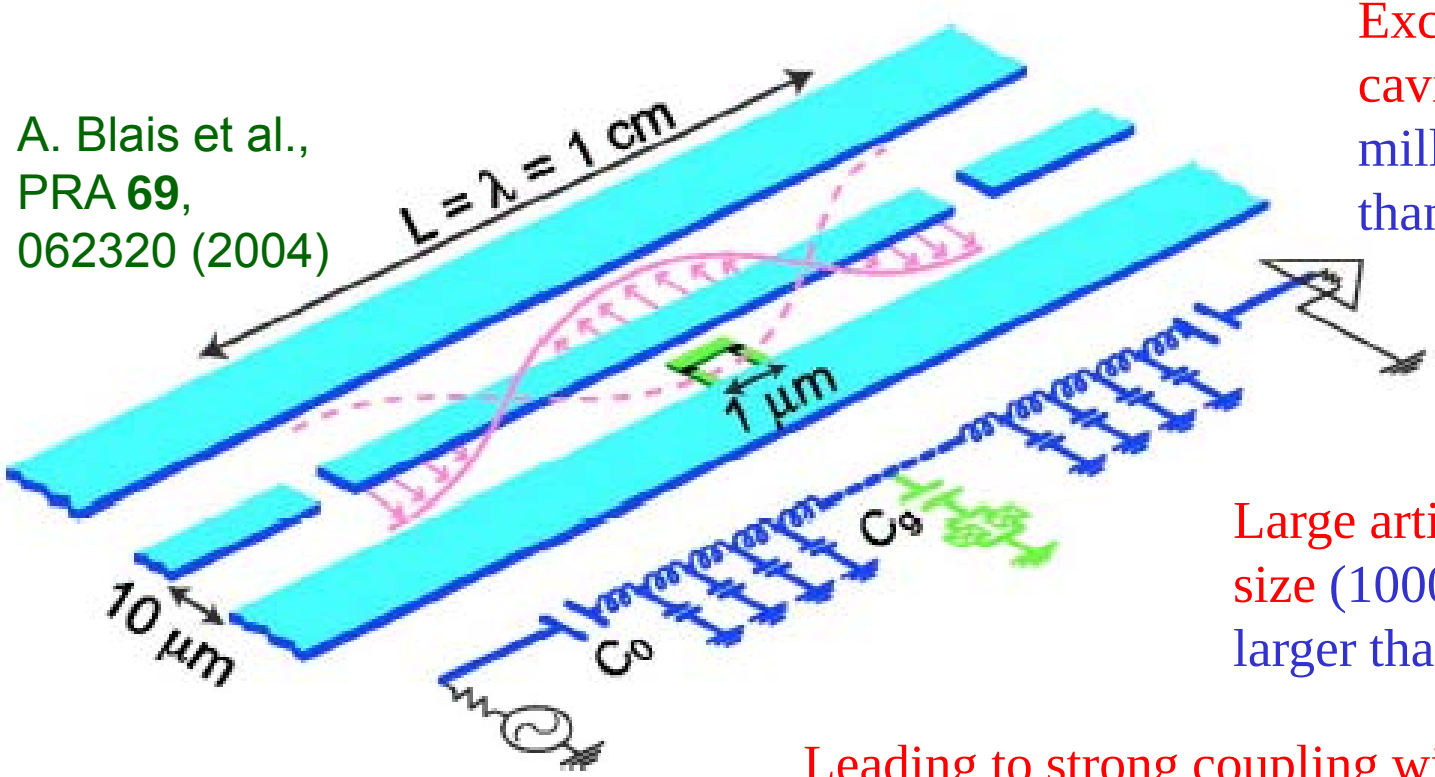


NIST	Delft	Saclay	NEC
Kansas	NTT		Chalmers
Maryland	Jena		Yale
UCSB			JPL

Circuit QED

- 1D trasmission line resonator consists of a full-wave section of superconducting coplanar wave quide.
- A Cooper-pair box qubit (an effective two-level atom) is placed between the superconducting lines and is capacitively coupled to the center trace at a maximum of the voltage standing wave, yielding a strong electric dipole interaction between the qubit and a single photon in the cavity.

A. Blais et al., PRA **69**, 062320 (2004)

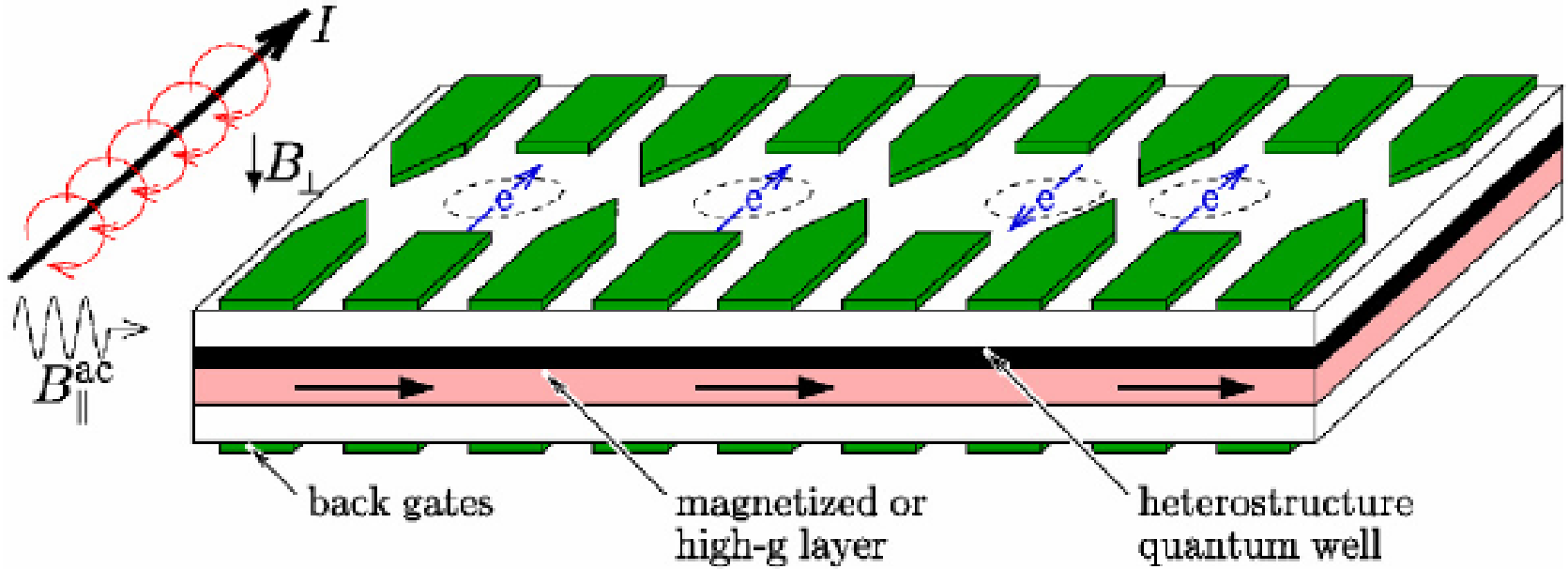


Exceptionally small cavity volume (one million times smaller than 3D cavities)

Large artificial atom size (10000 times larger than an atom)

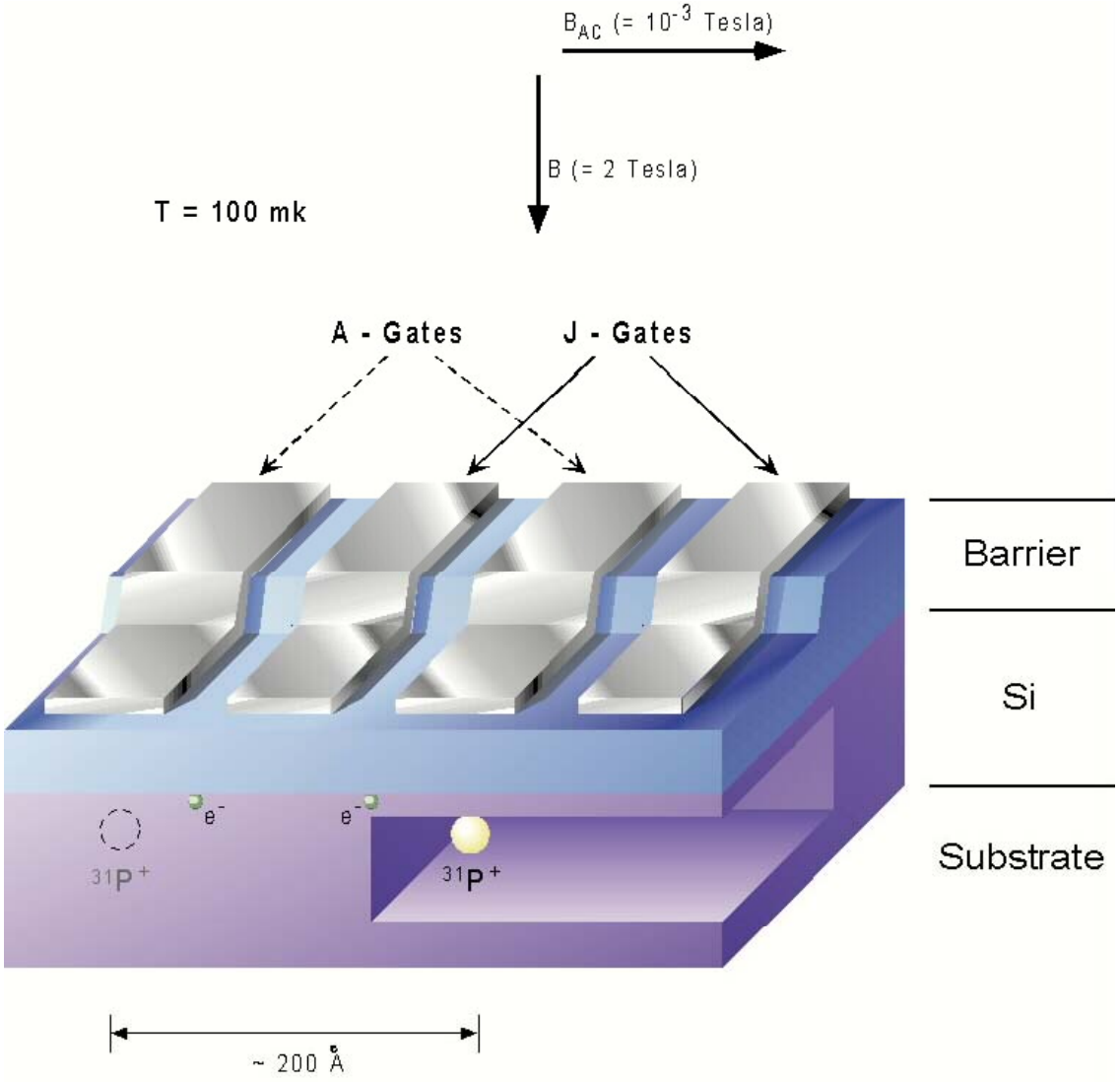
Leading to strong coupling with $g \gg \kappa, \gamma$

Electron spins in quantum dots



- Top electrical gates define quantum dots in 2DEG.
- Coulomb blockade confines excessive electron number at one per dot.
- Spins of electrons are qubits.
- Qubits can be addressed individually:
  - Back gates can move electrons into magnetized or high-g layer to produce locally different Zeeman splitting.
  - Or a current wire can produce magnetic field gradient.
- Exchange coupling is controlled by electrically lowing the tunnel barrier between dots

矽半導體的自旋量子電腦
Silicon-based spin quantum computer



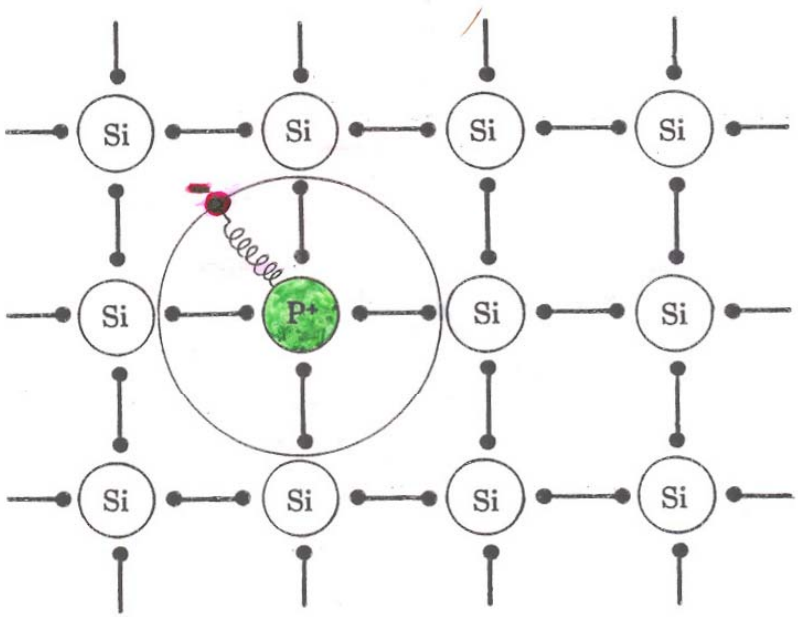
- Exploiting the existing strength of Si technology
- Regular array of P donors in pure silicon
- Low temperature:
  - Effective Hamiltonian involves only spins
  - Long spin coherence and relaxation times
- Magnetic field **B** to polarized electron spins
- Control with surface gates and NMR pulses
- Donor separation ~ 20nm
- Gate width < 10nm

元素週期表

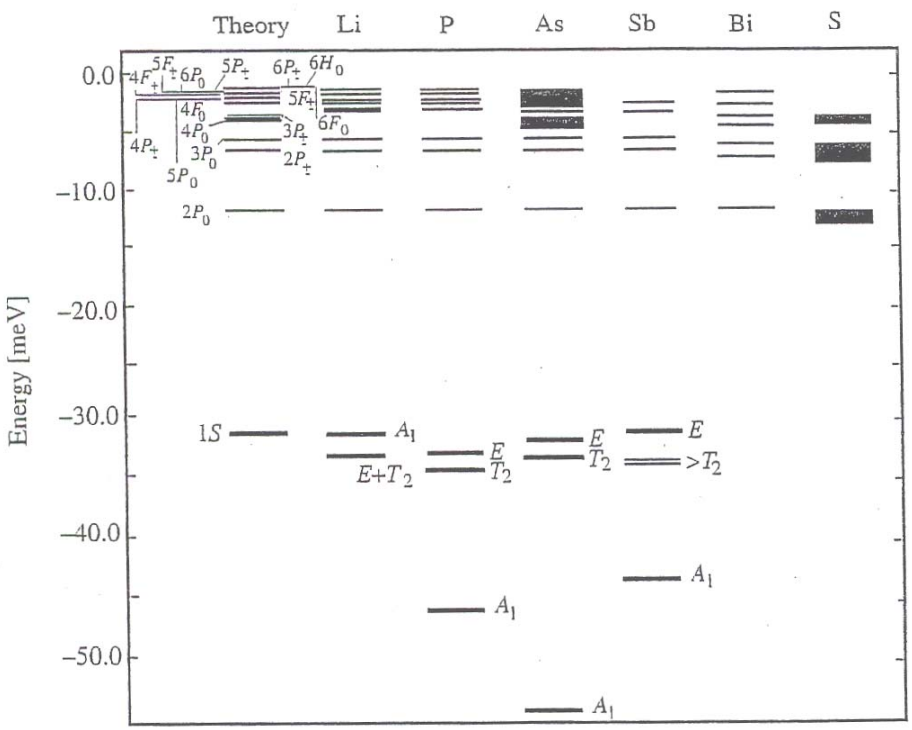
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1 H 氫																	鈍氣
鹼金屬	鹼土金屬															鹵素	2 He 氦
3 Li 鋰	4 Be 鈹											5 B 硼	6 C 碳	7 N 氮	8 O 氧	9 F 氟	10 Ne 氖
11 Na 鈉	12 Mg 鎂	---	---	---	---	過渡	金屬	---	---	---	---	13 Al 鋁	14 Si 矽	15 P 磷	16 S 硫	17 Cl 氯	18 Ar 氬
19 K 鉀	20 Ca 鈣	21 Sc 鈧	22 Ti 鈦	23 V 釩	24 Cr 鉻	25 Mn 錳	26 Fe 鐵	27 Co 鈷	28 Ni 鎳	29 Cu 銅	30 Zn 鋅	31 Ga 鎵	32 Ge 鍺	33 As 砷	34 Se 硒	35 Br 溴	36 Kr 氪
37 Rb 銣	38 Sr 鍶	39 Y 釔	40 Zr 鋯	41 Nb 鈮	42 Mo 鉬	43 Tc 鎝	44 Ru 釕	45 Rh 銠	46 Pd 鈀	47 Ag 銀	48 Cd 鎘	49 In 銦	50 Sn 錫	51 Sb 銻	52 Te 碲	53 I 碘	54 Xe 氙
55 Cs 銫	56 Ba 鋇	57 La 鑭	72 Hf 金 合	73 Ta 鉭	74 W 鎢	75 Re 錸	76 Os 鋨	77 Ir 銥	78 Pt 鉑	79 Au 金	80 Hg 汞	81 Tl 鉈	82 Pb 鉛	83 Bi 鉍	84 Po 釙	85 At 石 厄	86 Rn 氡
87 Fr 金 法	88 Ra 鐳	89 Ac 錒	104 Rf 金 鑪	105 Db	106 Sg	107 Bh	108 Hs	109 Mt	110 Uu n	111 Uu u	112 Uu b						

矽半導體中的磷施主
Phosphorus Donor in Si

P donor behaves effectively like a hydrogen-like atom embedded in Si

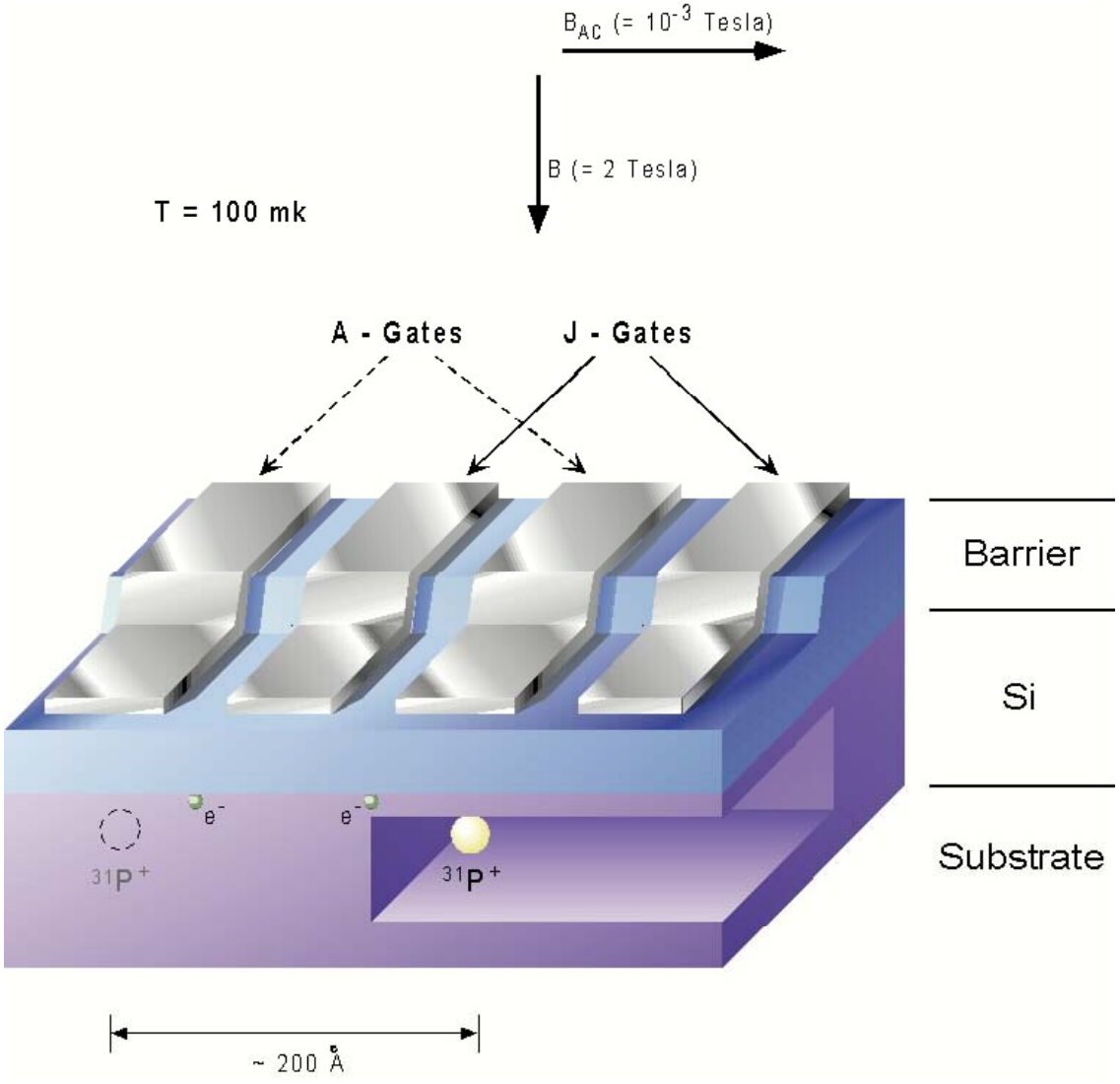


P shallow donor energy levels in Si



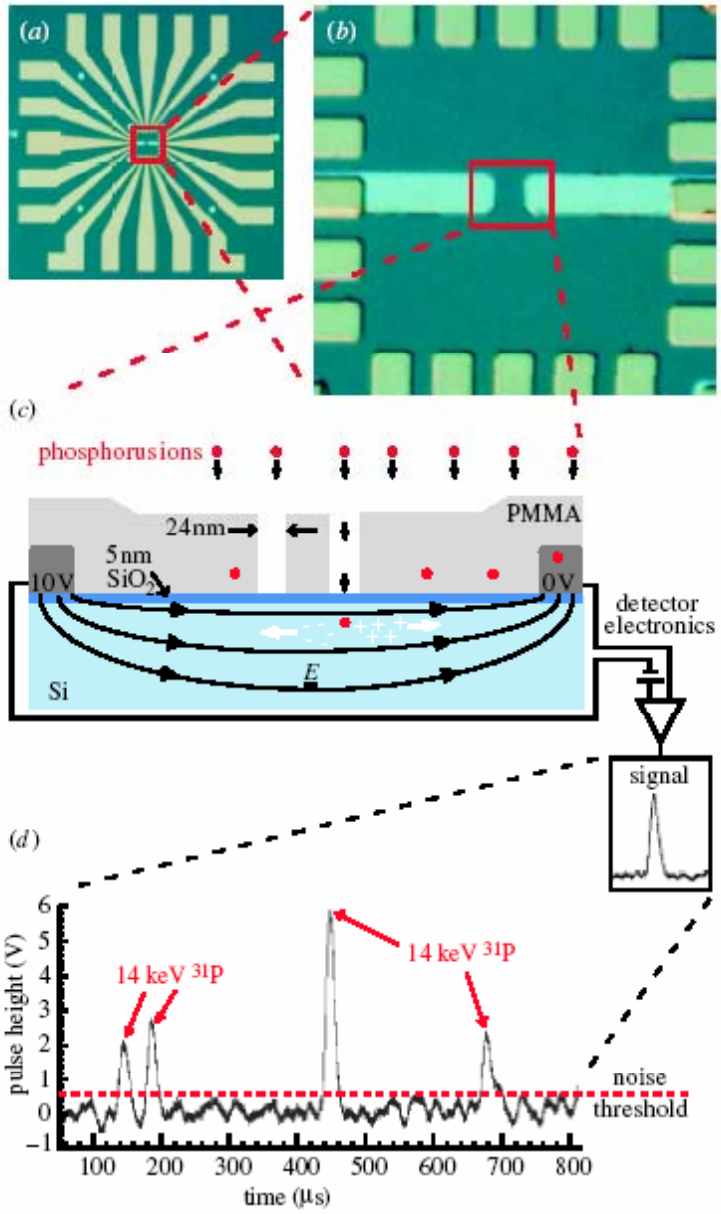
$$a_B^* = \varepsilon \frac{m_e}{m^*} a_B \ , \quad E_n = \frac{1}{\varepsilon^2} \frac{m^*}{m_e} E_n^H$$

矽半導體的自旋量子電腦
Silicon-based spin quantum computer



- Exploiting the existing strength of Si technology
- Regular array of P donors in pure silicon
- Low temperature:
  - Effective Hamiltonian involves only spins
  - Long spin coherence and relaxation times
- Magnetic field **B** to polarized electron spins
- Control with surface gates and NMR pulses
- Donor separation ~ 20nm
- Gate width < 10nm

Top-down approach for few qubit devices

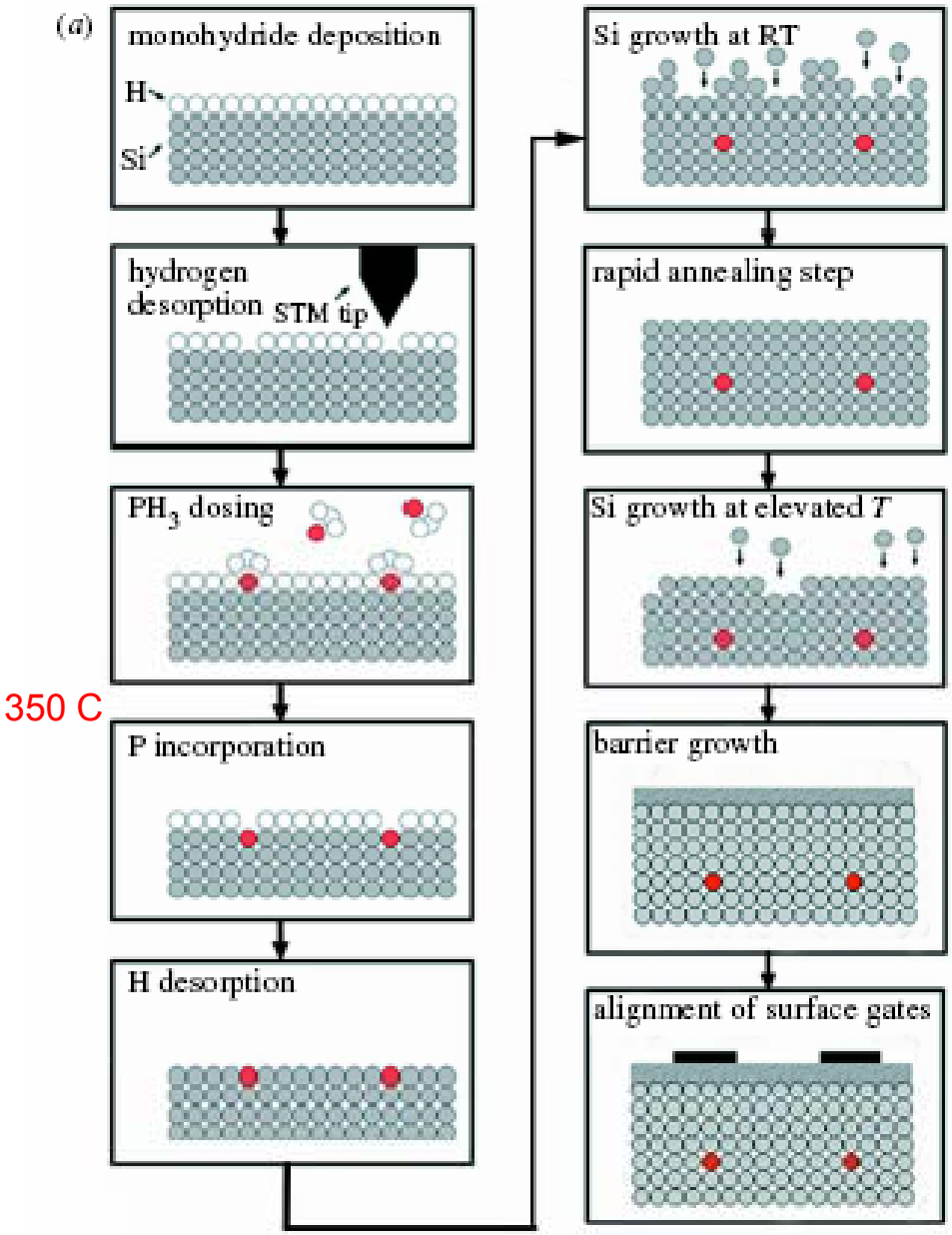


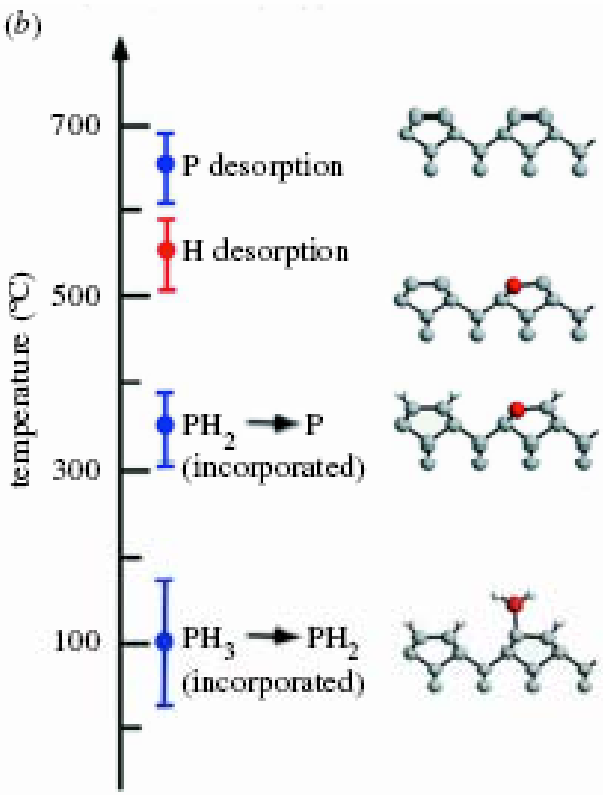
Controlled single-ion implantation

- 14 KeV P ion beam is used to implant P dopants to an average depth of 15nm below the Si-SiO2
- Ion-stopping resist defines the array sites
- Each ion entering the Si substrate produces e-hole pair that drift in an applied electric field
- Created single current pulse for each ion strike is detected by on-chip single ion detector circuit.

95% confidence in ion detection
50% confidence in each 2-donor device

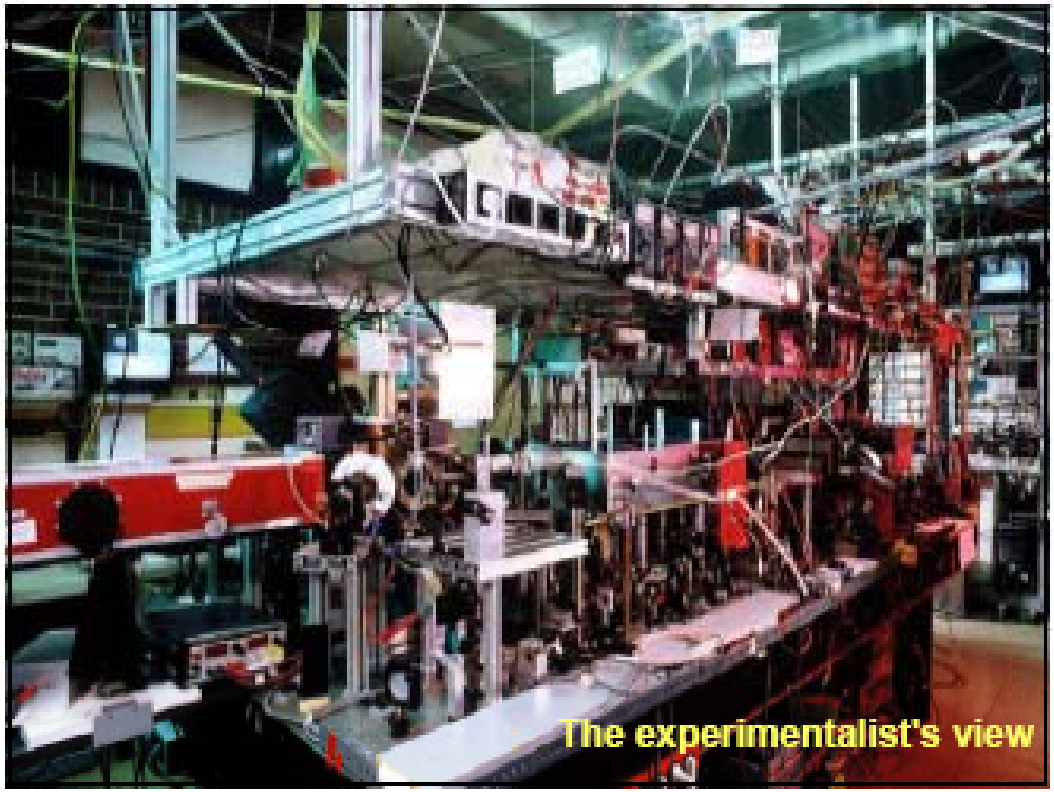
Bottom-up approach for large-scale qubit arrays



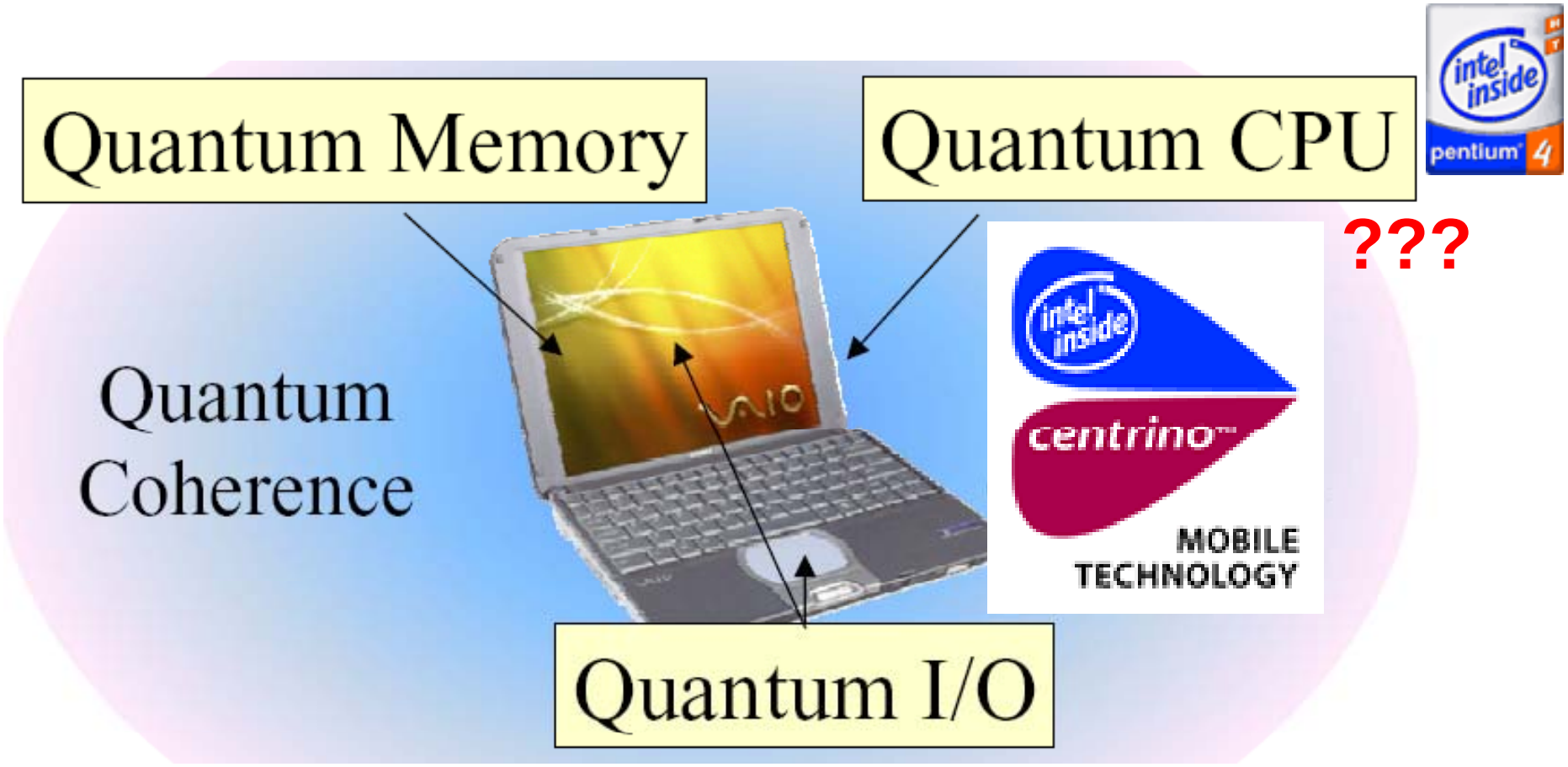


Using scanning tunnelling microscope lithography and epitaxial silicon overgrowth to construct devices at an atomic scale precision.

光學量子電腦實驗室



量子電腦???


Quantum Memory
Quantum CPU
???
Quantum Coherence
Quantum I/O
intel inside
pentium 4
intel inside
centrino
MOBILE TECHNOLOGY

量子電腦 周二在加誕生

- 中國時報 **2007.02.12**
  林上祚/台北報導
- 全球第一台量子電腦，即將於本周二由加拿大科技公司D-Wave，正式對外公佈，量子電腦是物理學家費曼(Richard Feynman)八〇年代所提出概念，儘管多數科學家認為，量子電腦廣泛商業化，還需二十年時間，不過D-Wave準備明年起正式量產。
- 量子電腦(quantum computer)，希望利用量子現象來增加計算的速度，最大特點是N個儲存位元可以同時儲存2N個資料。
- 根據英國衛報報導，加拿大科技公司D-Wave，已經成功說服多家創投基金，投資2000萬美元在量子電腦計劃，本周二第一台量子電腦原型機就將正式問世，並預估明年正式量產，未來除了可以用來破解蛋白質DNA的鍵結，還將可以運用在財務工程。
- 目前傳統電腦兩個位元的暫存器，在同一個時間上只能表示00、01、10和11中的一種狀態，但量子電腦兩個量子位元的暫存器，在一個時間上卻可以同時表示00、01、10和11四種狀態。
- 衛報報導，量子位元的狀態就像物理學家薛丁格（Schrodinger）比喻盒子裡亦死亦活的貓（Schrodinger’s cat），在盒子打開以前可以是任何一種狀態，三千個量子位元(qbits,quantum bits)，就能代表十的九十次方樣態，運算效能就能超越地球上所有電腦的總和。
- 不過量子電腦的最大問題是，只要受到任何些微干擾，例如過熱，馬上會當機，目前為止，量子電腦在實驗室中，只有成功運算了數千次，穩定度仍然不夠，D-Wave創辦人羅斯（Geordie Rose）目前設計的16量子位元電腦是用貴金屬鈮製成，並且須在零下273度（絕對零度）下運作，這麼苛刻的運作條件，讓它註定「用一次即當機」。

全球首臺量子計算機在加誕生 穩定度仍然不夠

- 全球首臺量子計算機在加誕生 穩定度仍然不夠 2007年02月17日 09:48:09　來源：科技日報

- 加拿大溫哥華D-Wave公司首席技術官基尼-羅斯宣佈，該公司已成功研製出一個具有16量子比特的“獵戶星座” (Orion)量子計算機。他透露，D-Wave公司將於2月13日和2月15日分別在美國加州和加拿大溫哥華展示他們的量子計算機。
- 量子計算機是物理學家費曼在19世紀80年代提出的概念。量子位可以同時表示1和0，因此能夠攜帶更多的資訊，更快地解決問題。量子計算機希望利用量子現象來增加計算的速度，最大特點是N個儲存位可以同時儲存2N個資料。不過量子計算機最大的問題是只要受到任何微干擾，例如過熱，馬上會關機。目前為止，量子計算機在實驗室中只能成功運算數千次，穩定度仍然不夠。D-Wave公司目前設計的16量子比特計算機是用貴金屬鈮製成，並且須在零下273K下運行。
- 有專家認為，D-Wave公司的嘗試只是一種原理性檢驗，雖很有必要，卻必須首先糾正量子計算中不可避免的錯誤，否則這個量子計算機將無法運行。許多科學家認為，量子計算機廣泛商業化還需20年時間。但羅斯認為，2008年他們將製成世界第一臺具有1000個量子比特的量子計算機。

加拿大公司展示量子電腦 速度與標準PC相當

加拿大公司展示量子電腦 速度與標準**PC**相當

2007-02-12 15:51:50　來源：CCIDNET.com

據reghardware網站報導稱，位於溫哥華的D-Wave表示，它已經開發了一台具有16個量子位元的量子電腦。

量子位可以同時表示1和0，因此能夠攜帶更多的資訊，更快地解決問題。

D-Wave的聲明受到了量子計算產業在實際和理論方面的懷疑。

由於只具有16個量子位，被稱為Orion的這款設備可能將沒有能力完成很大的數位的分解。量子電腦強大的數量處理能力已經引起安全廠商的擔憂，它們擔心，當具有數百個量子位元的量子電腦問世時，它們目前的加密技術會遭到淘汰。

據D-Wave的技術總監羅斯博士在其博客中稱，該公司計畫於2008年製造具有1000個量子位元的量子電腦。

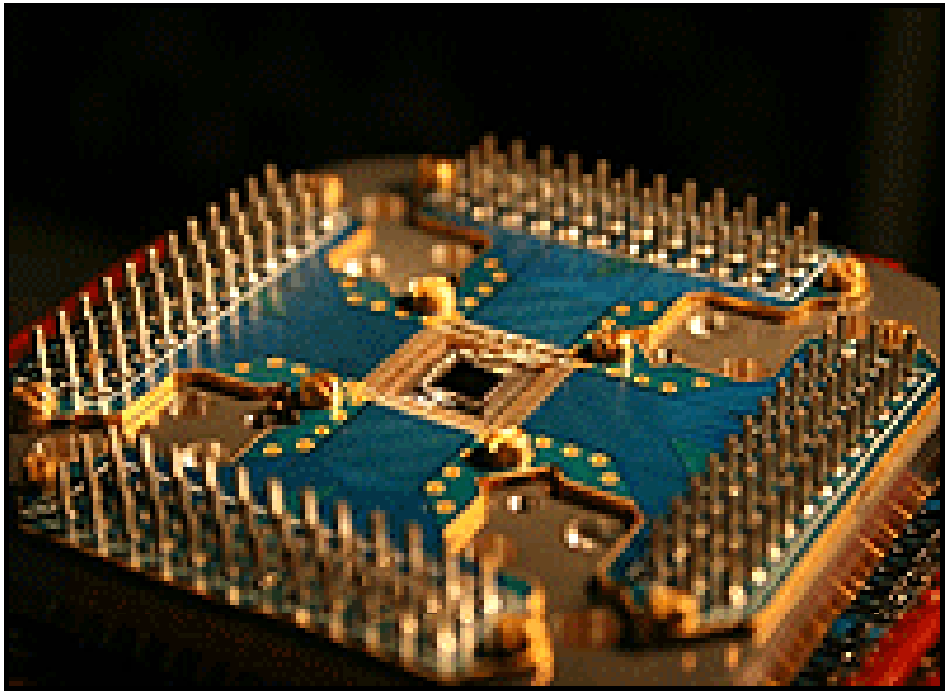
D-Wave將在其公司總部展示二款量子電腦的應用軟體，第一個是分子資料庫的模式匹配問題，第二個用於安排人們的席位。它們在16量子位元量子電腦上的運行速度與標準電腦相當。

First "Commercial" Quantum Computer Solves Sudoku Puzzles

- February 13, 2007 By JR Minkel
- A Canadian firm today unveiled what it called "the world's first commercially viable quantum computer." D-Wave Systems, Inc., "The Quantum Computing Company," during a much ballyhooed rollout at the Computer History Museum in Mountain View, Calif., hailed the new device as a big step toward the age of quantum computing, decades earlier than scheduled.
- For the demonstration, the quantum computer was given three problems to solve: searching for molecular structures that match a target molecule, creating a complicated seating plan, and filling in Sudoku (數獨) puzzles.
- But experts say the announcement may be a bit—er—premature. Even if the computer were to work as advertised, it still would be nearly 1,000 times too small to solve problems that stump ordinary computers. Moreover, researchers do not know whether it will work at bigger sizes.

COMPUTER OF TOMORROW? **D-Wave Systems, a Canadian company, has announced a new "commercially viable" quantum computing device (Orion) made of the superconducting element niobium.**

This is the core of a new quantum computer attached to Leiden Cryogenics dilution fridge, ready to begin a cool down to 0.005 degrees above absolute zero… about 500x colder than the coldest place in remote outer space.



The Orion chip in its package.

量子計算研究大躍進 量子電腦研發可期

中國時報　2007.09.27中央社

- 研究人員今天宣布，他們首度成功的在人造原子之間經由一段線纜傳輸數據，朝向超快量子計算科技新時代邁出重要一步。
- 美國兩組物理學家展示實驗過程，這或許能成為有朝一日大量生產量子電腦的基礎，而這種新型量子電腦的速度將遠快於當前最大的超級電腦。
- 科學家進行的實驗，是在兩個超導迴路「量子位元」間操縱單光子，所謂的單光子，是指個別的電磁能量團，沒有質量也沒有重量。 數據橫越一段奈米規模的迴路進行移動，這個迴路也就是所謂的「量子巴士」，是一段長二十毫米的線纜，置於超低溫中以避免產生電阻。
- 美國國家標準暨技術協會研究團隊在學者席蘭巴率領下設計出這種線纜，它也可以短暫儲存資料達十個奈米秒，這顯示資料儲存是可能的。耶魯大學學者梅吉率領團隊，則讓兩個量子位元間彼此產生交流。這兩項研究都刊登在英國「自然」期刊中。 梅吉說，這並不是科學家首次成功將一個量子位元與另一個連結。 但這是科學家首次利用等同於微型電腦晶片的物體，經由一段相對上的長距離完成這項實驗。
- 新型態的量子技術有數項特徵，能為未來大規模生產超強量子電腦鋪路。其一為可擴展性，也就是製造多重固態量子位元網的可能性，但這到目前還無法達成。

加拿大滑鐵盧大學量子計算研究所所長拉弗賴米在看過研究報告後評論說：「這些研究報告證實透過量子巴士可居中促成超導量子位元間的互動，而原則上這種量子巴士是可擴展的。」他說：「實驗顯示出加強量子對這些系統的掌控，而這攸關量子資訊處理器，更朝製造量子電腦邁出重要一步。」另一項優勢則在於利用現行的晶片科技，製造量子位元以及連結各位元的迴路。

相較於目前的科技，量子計算可說是在質方面的重大突破。相較於利用二進位法的零與一來保存資訊，量子計算則是根據量子力學的原則，而所謂量子力學控制了原子層級的狀態變化，又稱為「疊加現象」。以目前數位科技，量子位元可以用零或一來表示，但如果進行反直覺的繞彎，便能同時保有兩個數值，若能控制並評估量子位元，將能大幅增加同步計算的次數。

梅吉說，光子可以在原子層級上運送資料，要操控它就是一個很大的挑戰。

以光速行進的光子一閃即逝，一看見就消失了，因為它在接觸視網膜時即消耗掉存在所需的能量。光子可以電磁光譜中段的可見光形式呈現，也能呈現在光譜極端的X光與另一個極端的迦瑪射線。梅吉說，「我們必須控制每一個單光子相對的電訊號。」他並指出，一隻手機每秒釋放一千億乘以一兆個光子，也就是一的後面加上二十三個零。

其他專家都認為這些發現是重要的突破。拉弗賴米說：「他們確實是偉大的研究，這些技術令人印象深刻。」他們也提醒，要製造出量子筆記型電腦，還有一段很長的路要走，並指出實驗有兩項主要限制。

梅吉坦承，目前仍無法逐步形成量子位元彼此互動的網絡，「要製造真正的量子電腦，必須製造出更多成對的量子位元，沒有數千最少也要數百」。

另一個問題則在於溫度，為了讓實驗運作，線纜必須冷卻至攝氏零下兩百七十三點一三度。

No cloning theorem

An Unknown Quantum State Cannot Be Cloned.

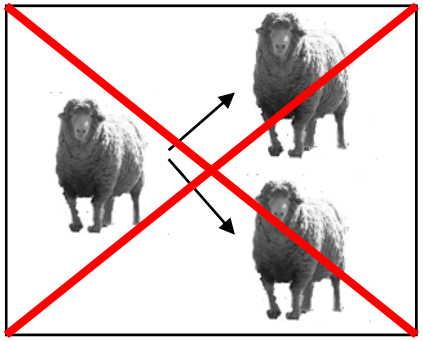
沒有一個可複製任意未知量子狀態的量子複印機存在

<Proof>

Zurek, Wootters (82)

$$U\left(|\alpha\rangle|0\rangle\right)=|\alpha\rangle|\alpha\rangle$$

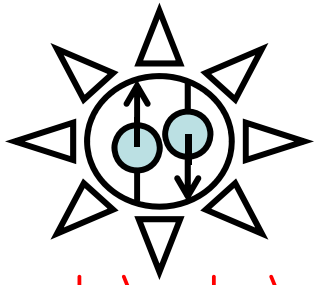
$$U\left(|\beta\rangle|0\rangle\right)=|\beta\rangle|\beta\rangle \qquad |\alpha\rangle\neq|\beta\rangle$$



Let $|\gamma\rangle=\frac{1}{\sqrt{2}}\left(|\alpha\rangle+|\beta\rangle\right).$

Then $U\left(|\gamma\rangle|0\rangle\right)=\frac{1}{\sqrt{2}}\left(|\alpha\rangle|\alpha\rangle+|\beta\rangle|\beta\rangle\right)\neq|\gamma\rangle|\gamma\rangle$

EPR pair and entanglement

Alice x ⇦  ⇨ y Bob

$$\frac{1}{\sqrt{2}}\left(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B\right) \neq |\psi\rangle_A \otimes |\phi\rangle_B$$

Reality principle (真實性) and locality principle (局域性)

→ Bell's Inequality

Classical physics: x and y are decided when picked up.
Quantum physics: x and y are decided when measured.

Aspect's Experiment → QM contradicts to Bell's inequality

愛因斯坦：

Does the moon exist only when you look at it ?

月亮是否只在你看著他的時候才存在？

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B\right)$$

$$= \frac{1}{\sqrt{2}}\left(|+\rangle_A|-\rangle_B - |-\rangle_A|+\rangle_B\right)$$

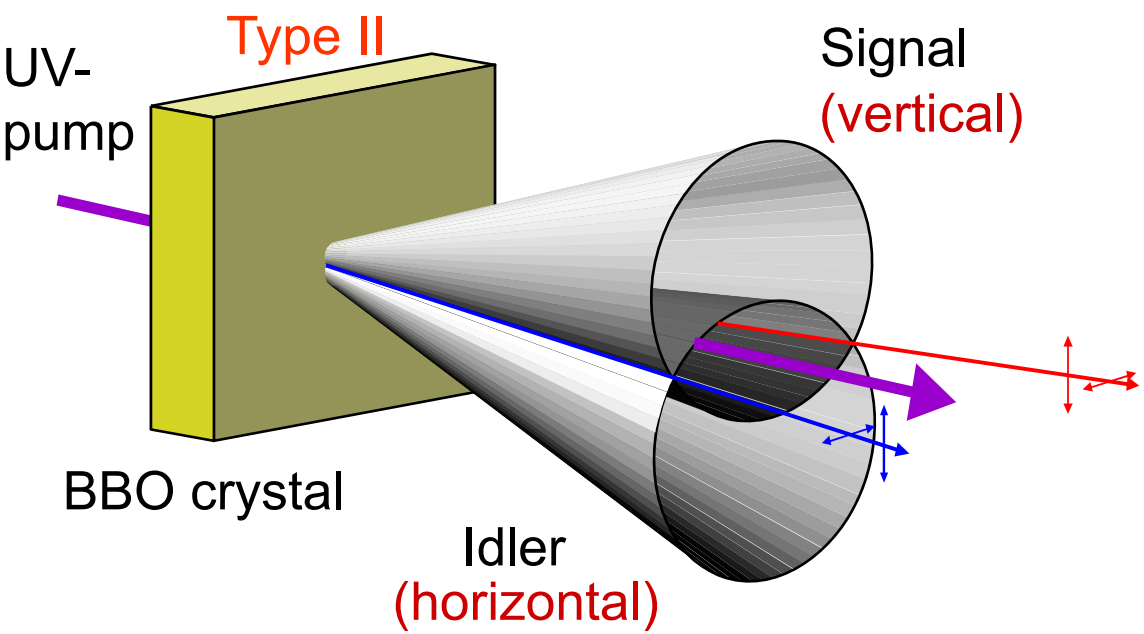
$$|+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right), \; |-\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$$

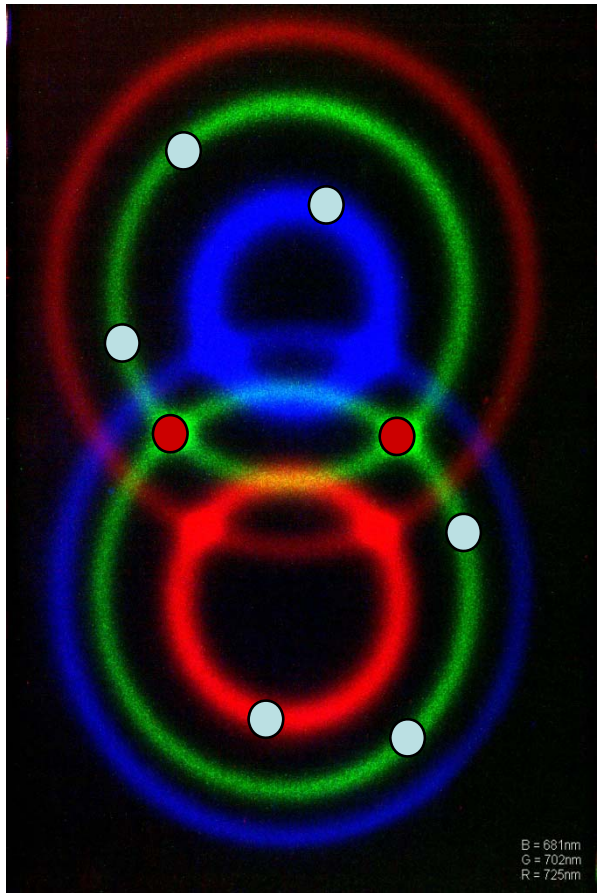
Entanglement Source - SPDC

Spontaneous parametric down conversion

$$\omega_{\text{pump}} = \omega_{\text{signal}} + \omega_{\text{idler}}$$

$$\vec{k}_{\text{pump}} \approx \vec{k}_{\text{signal}} + \vec{k}_{\text{idler}}$$

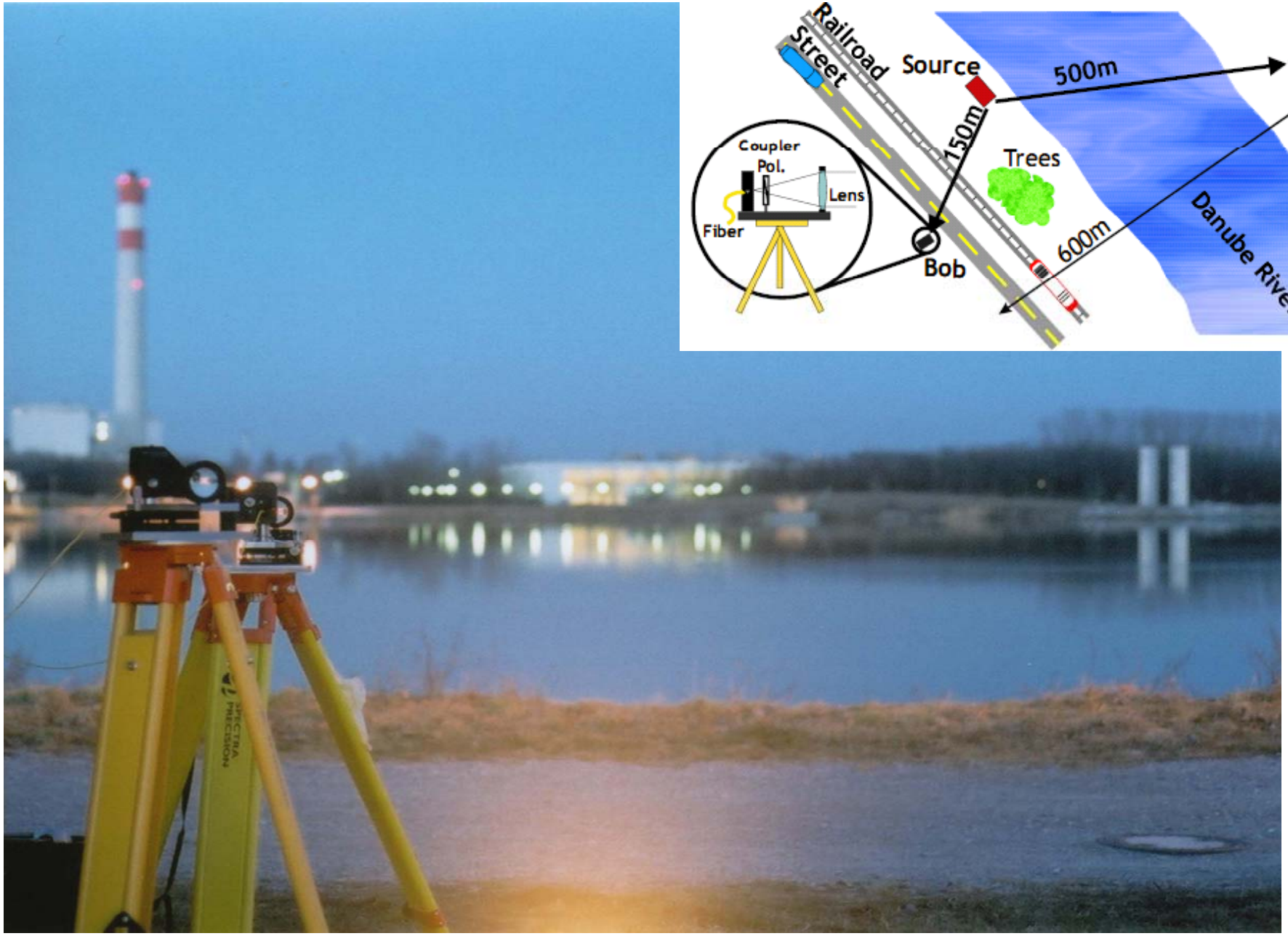


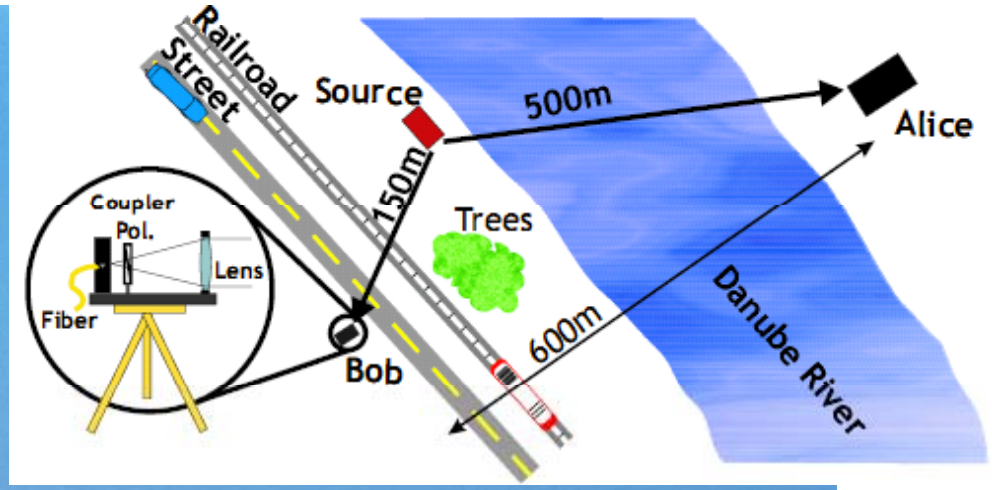


$$|\Psi\rangle_{12} = \frac{1}{\sqrt{2}}(|H\rangle_1|V\rangle_2 - |V\rangle_1|H\rangle_2)$$

Kwiat et al, PRL 75, 4337 (1995)

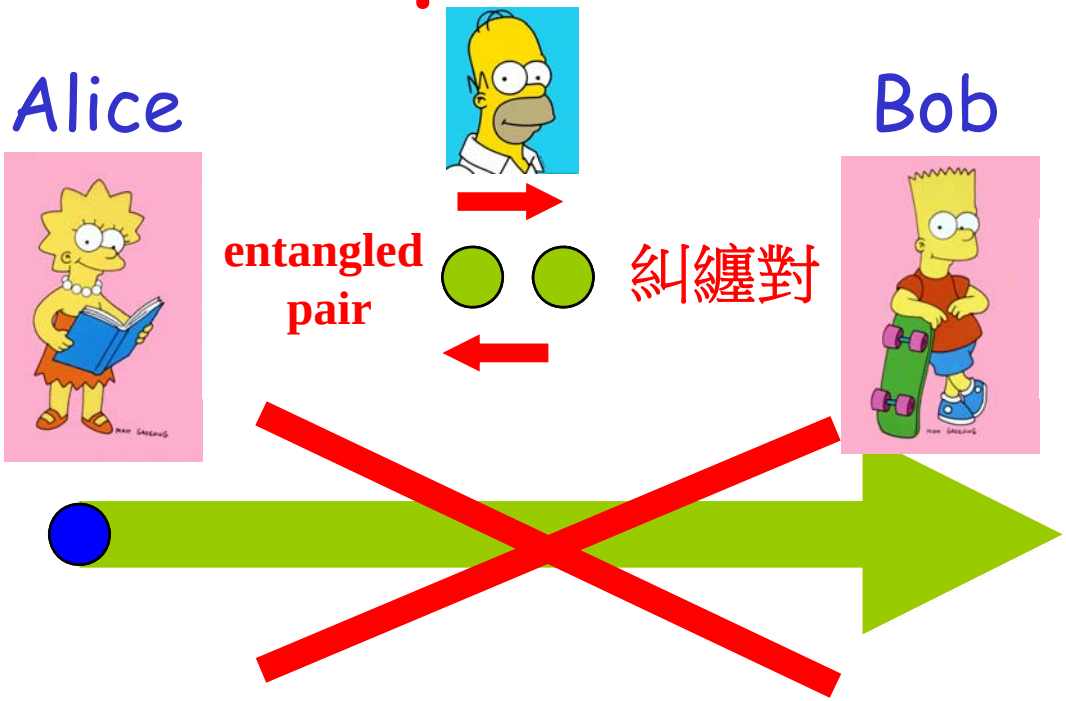
Entanglement is in the air…



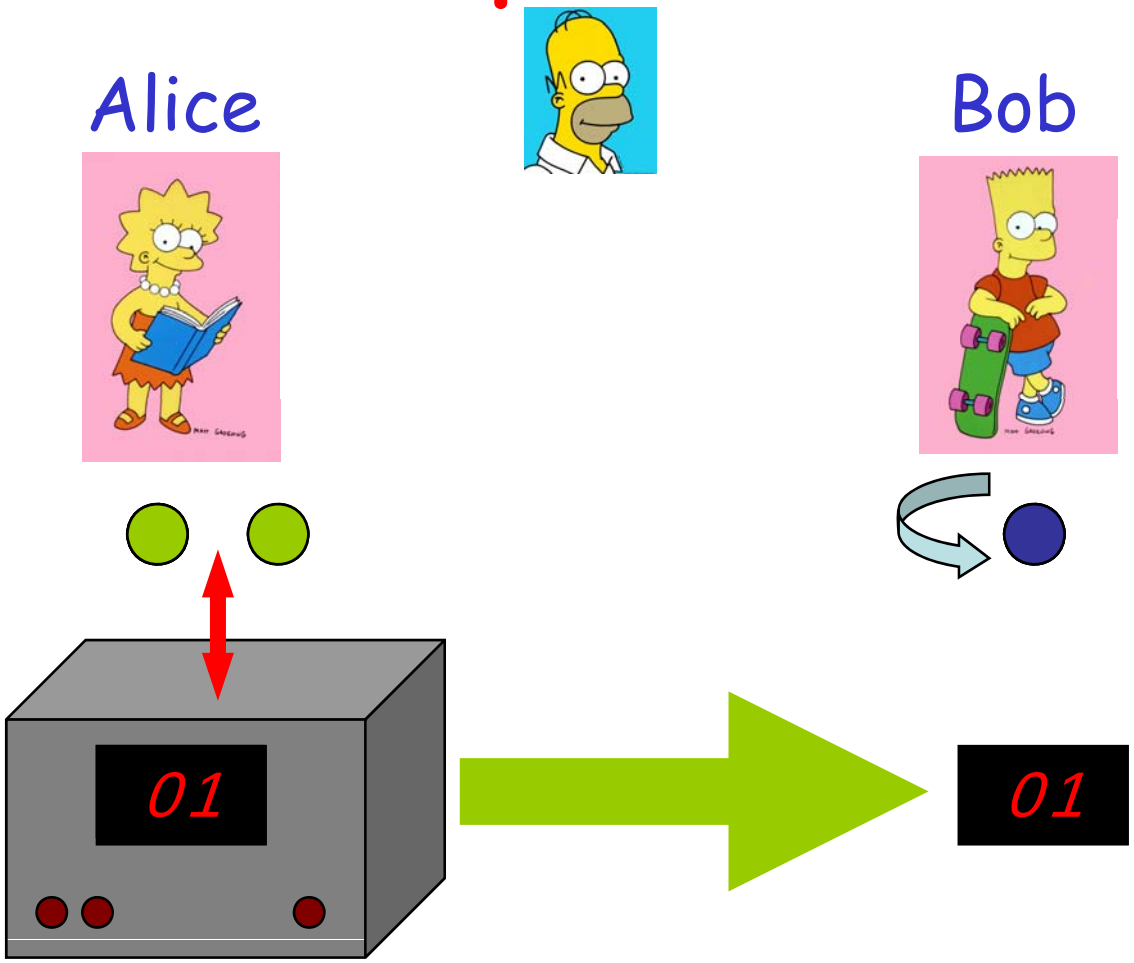


量子傳輸 (Quantum teleportation)

Teleportation

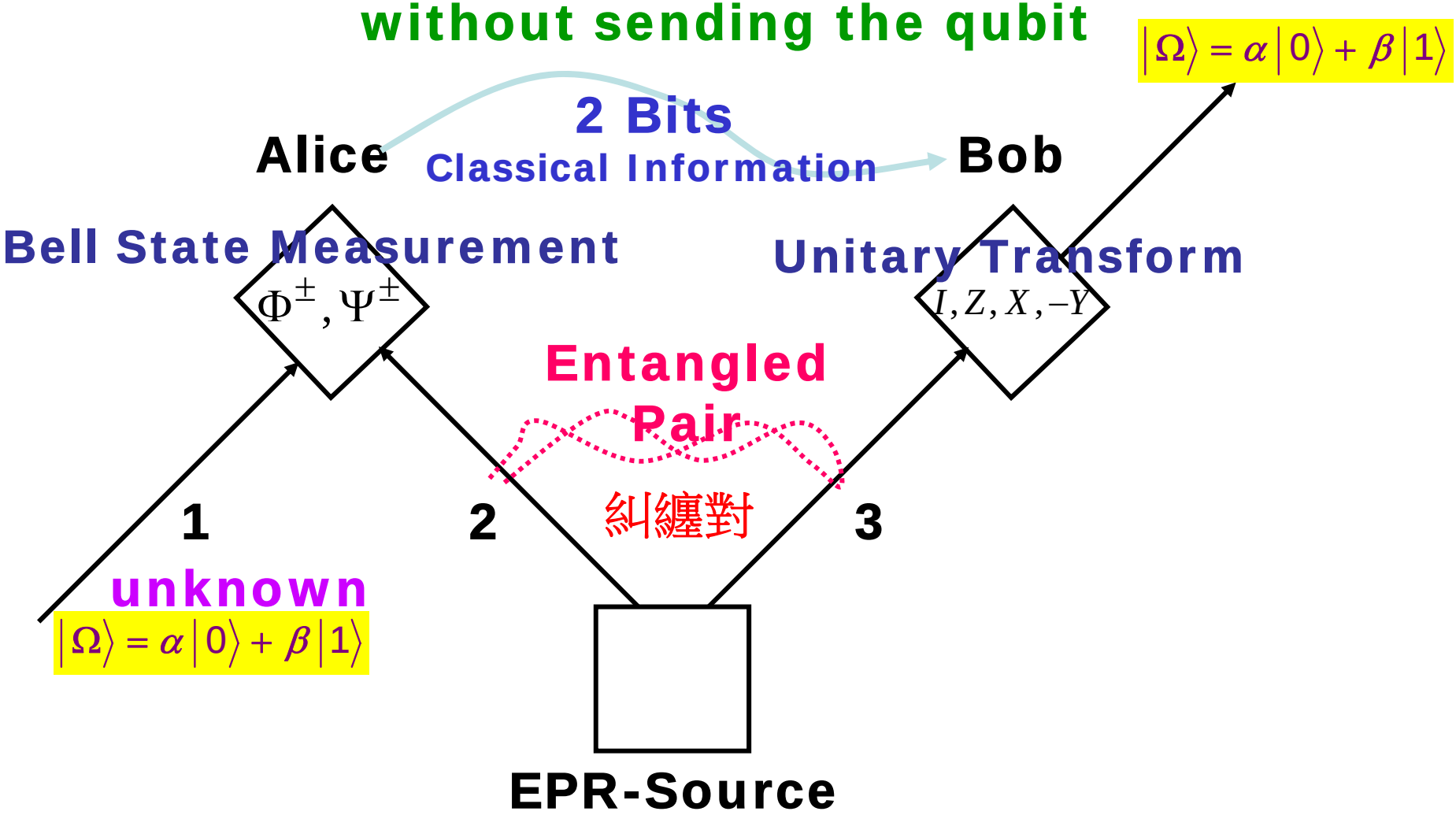


Teleportation

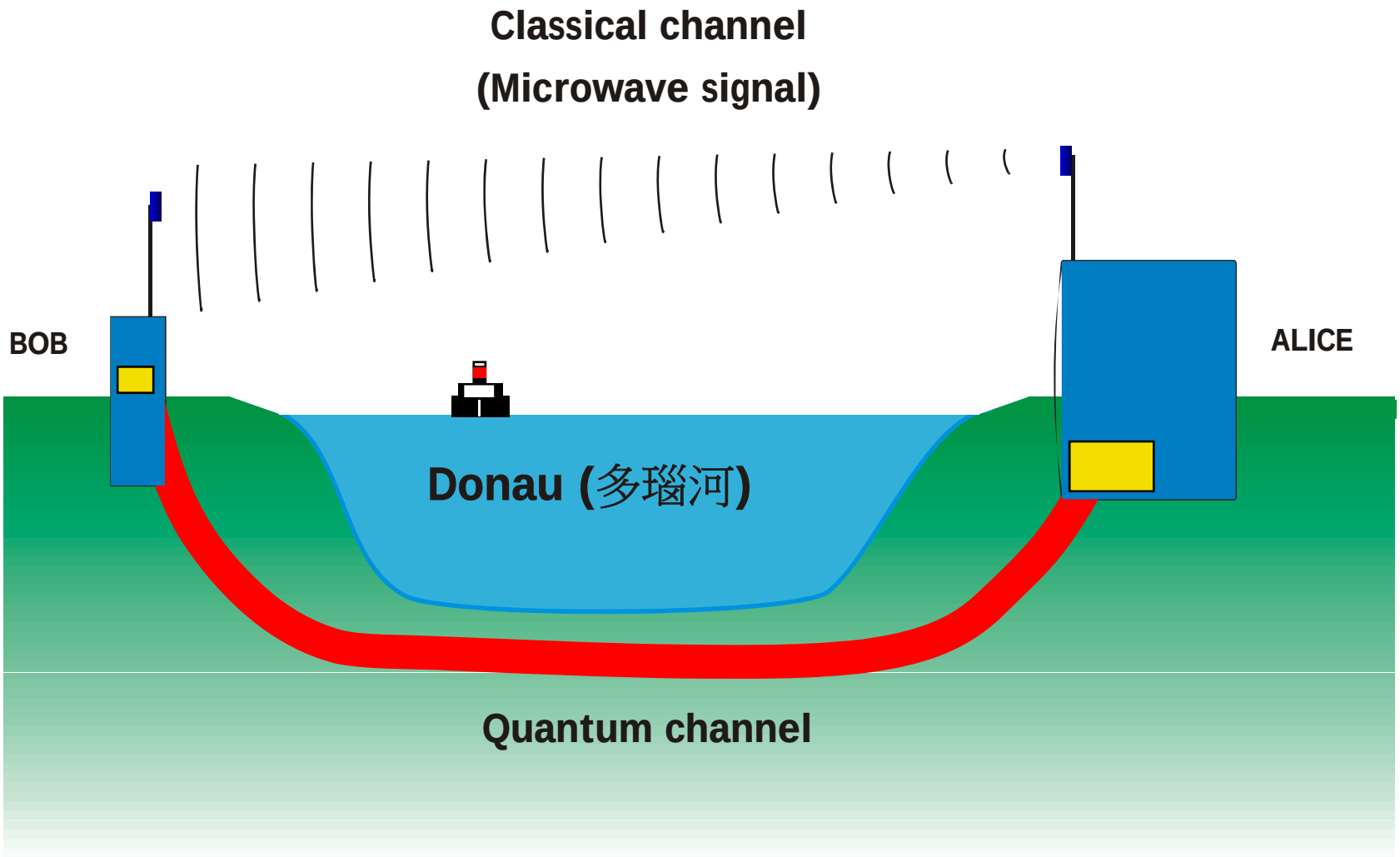


Quantum Teleportation

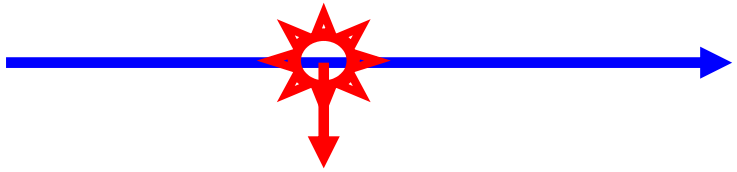
Transmit an unknown qubit state without sending the qubit



Long Distance Teleportation



量子密碼學
Quantum Cryptography



Quantum Mechanics provide a secure solution with quantum key distribution

No Cloning theorem & Heisenberg uncertainty principle + Irreversibility of quantum measurement

Need Single photon source and single photon detector to guarantee BB84 QKD absolutely secure and unbreakable.

BB84: 4 Polarizations

- Alice

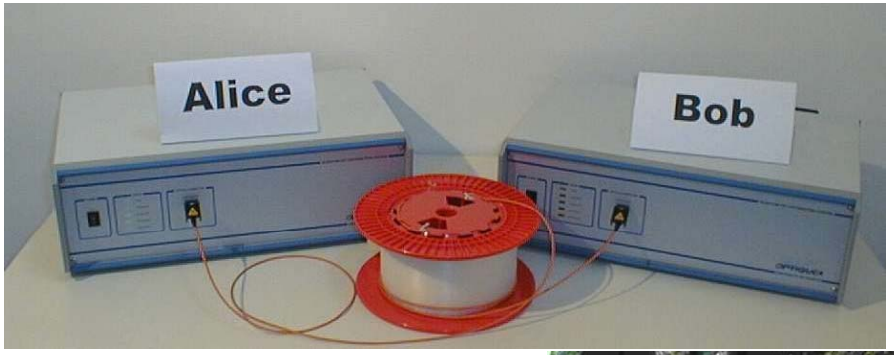
A1	=	0	1	1	0	0	1	0	0	0	0	1	1
A2	=	⊗	⊕	⊗	⊕	⊗	⊕	⊗	⊕	⊗	⊕	⊗	⊕
P	=	↗↙	↕	↖↘	★	↗↙	↕	↗↙	★	↗↙	★	↖↘	↕

- Bob

B	=	⊕	⊕	⊕	⊗	⊕	⊕	⊗	⊗	⊕	⊕	⊗	⊕
D	=	0	1	0	0	0	1	0	0	0	0	1	1
		1		1	1	1			1	1			

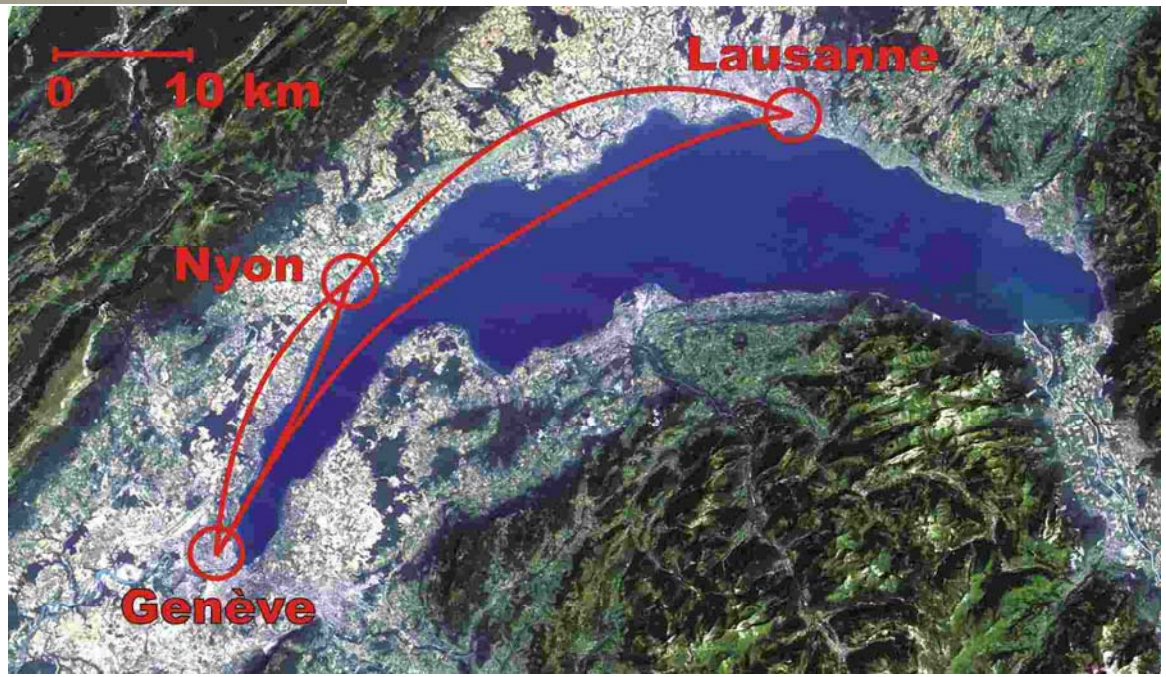
Distill secret key from raw key: **Information reconciliation and privacy amplification**

Quantum Key Distribution over 67 km with a plug&play system



Gisin, Zbinden, quant-ph/0203118

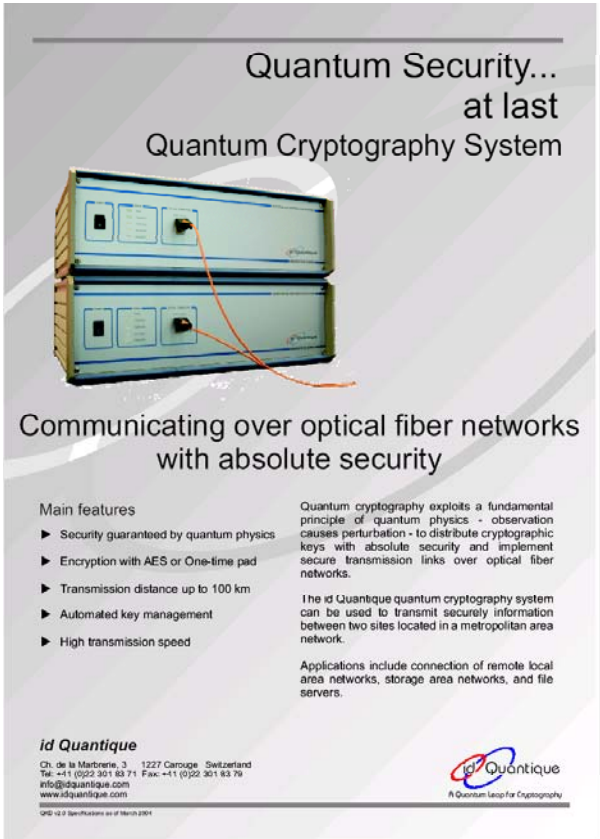
量子金鑰傳輸的商業化產品



MagiQ 100 km optical fiber commercial system; NEC 150 km (2004)

Commercial available!

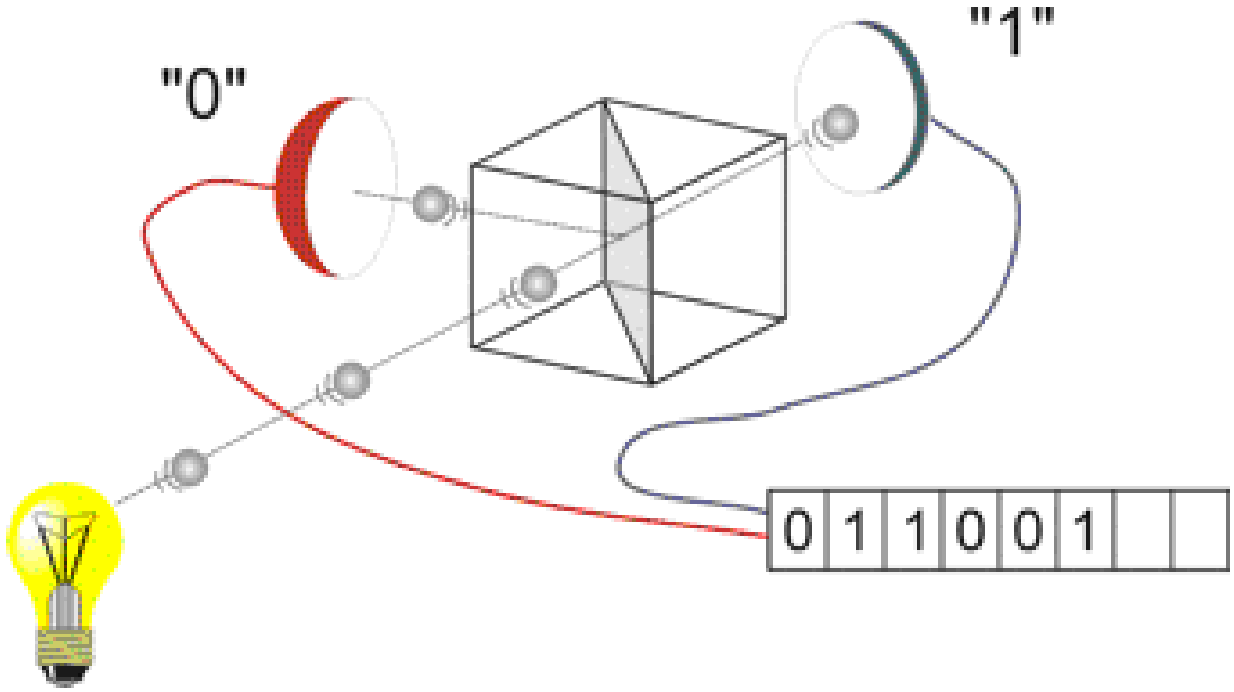
Quantum Cryptography is the most technicaly advanced application of quantum information – on the brink of commercialisation!



Quantum random number generators

- Being deterministic, computers are not capable of producing real random numbers.
- **Quantis** is a physical random number generator exploiting an elementary quantum optics process. Photons - light particles - are sent one by one onto a semi-transparent mirror and detected. The exclusive events (reflection - transmission) are associated to "0" - "1" bit values.

Quantis product line certified by Swiss Federal Office of Metrology



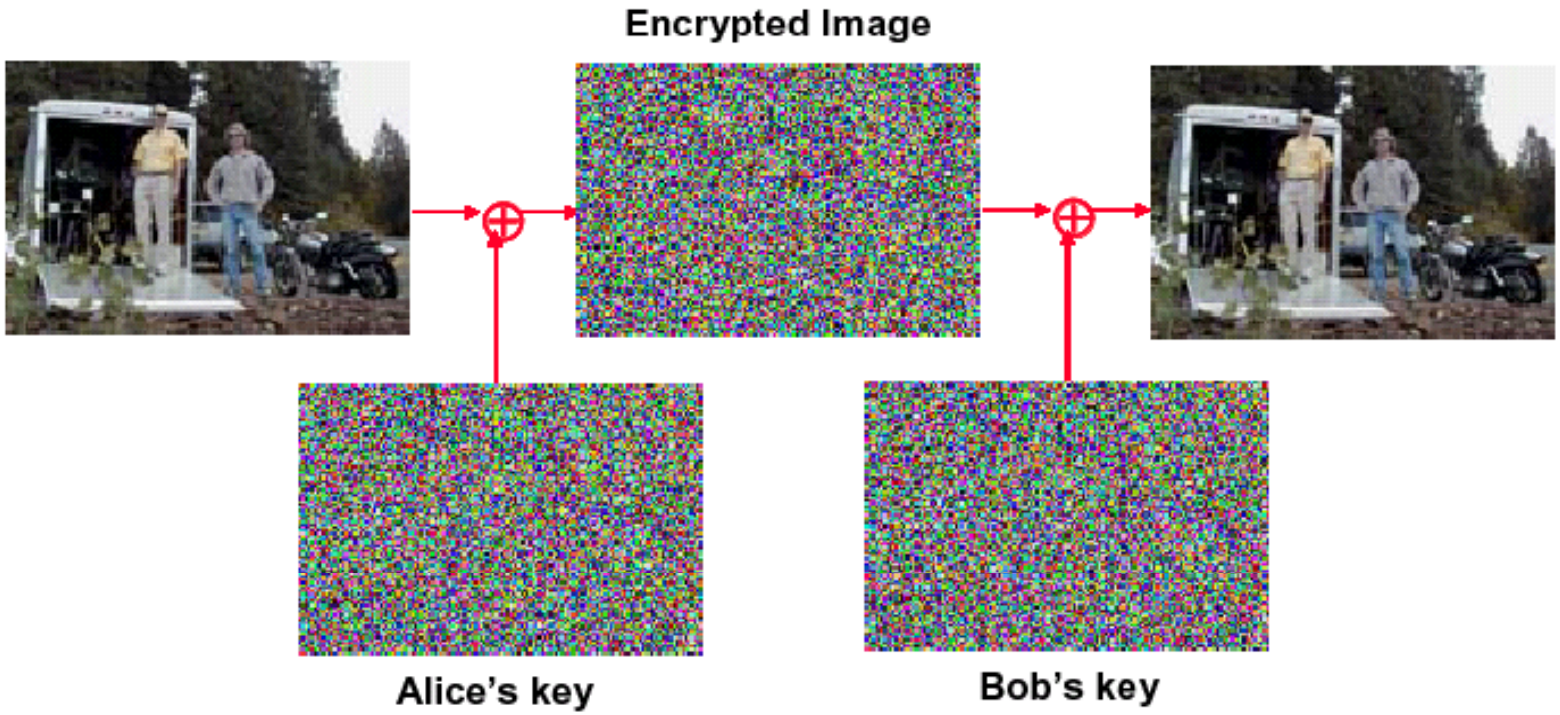
Practical free-space quantum key distribution over 10 km in daylight and at night

30km

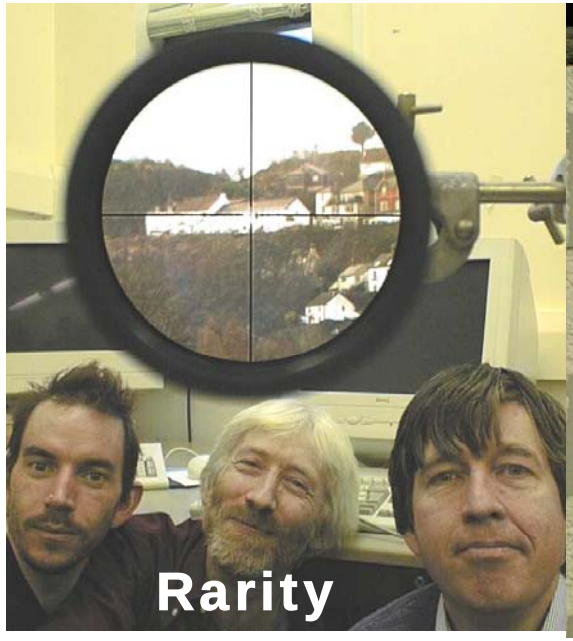
45km

開放空間的
量子金鑰傳輸

R. J. Hughes, J. E. Nordholt, D. Derkacs and C. G. Peterson **quant-ph/0206092**



23.4km Qinetiq-MPQ joint free space key exchange trial between Zugspitze and Karwendel

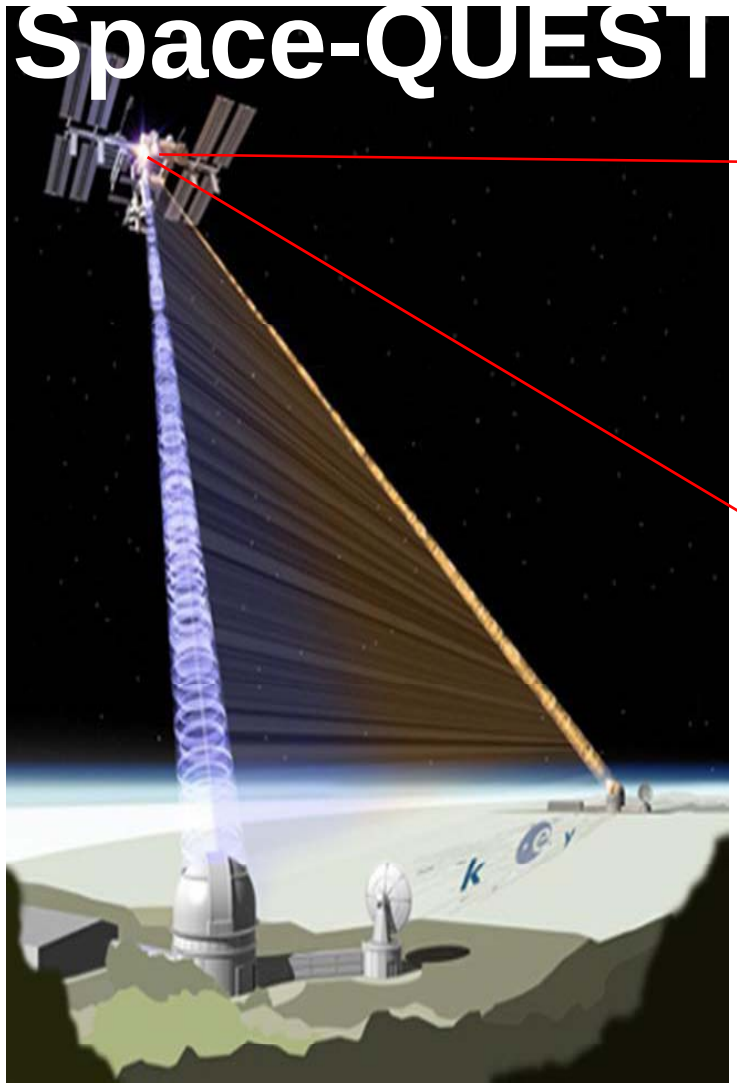


Autumn 2001

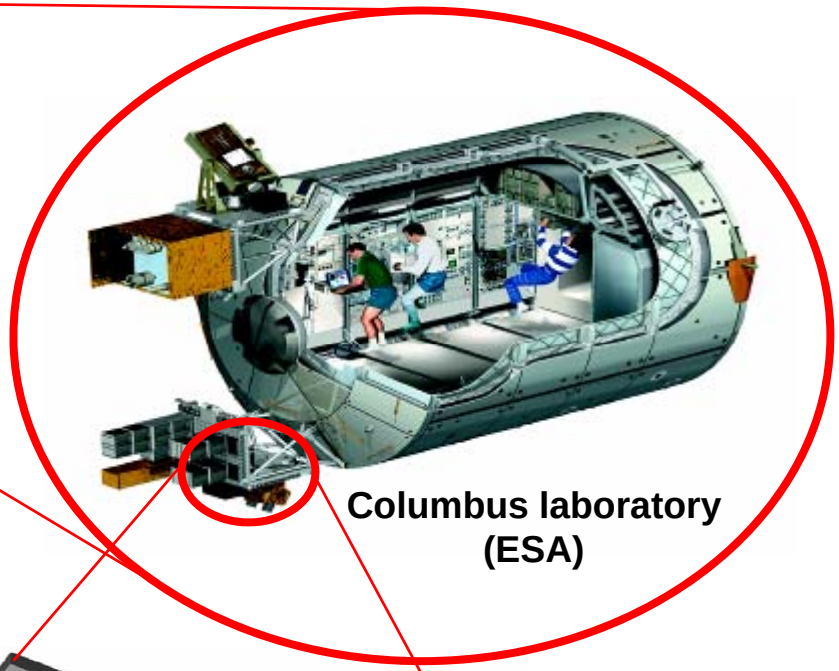
Autumn 2000: Key exchange over 1.9km between Qinetiq site and the local pub!

http://www.eqcspot.org/

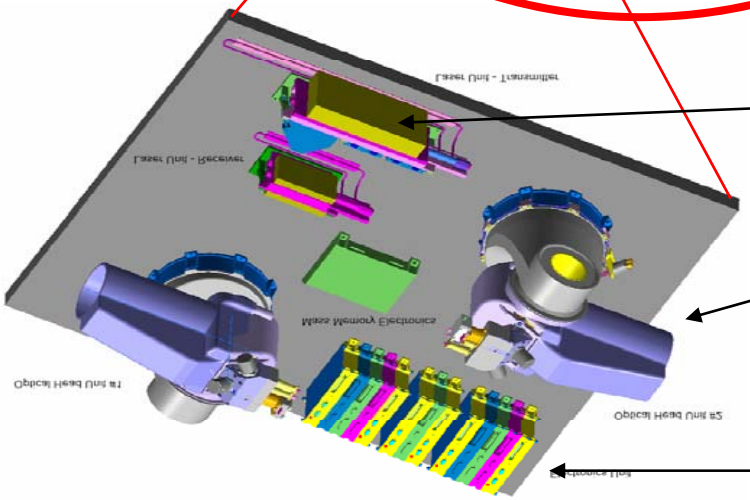
Space-QUEST



International Space Station (ISS)



Columbus laboratory (ESA)



Entangled photon source

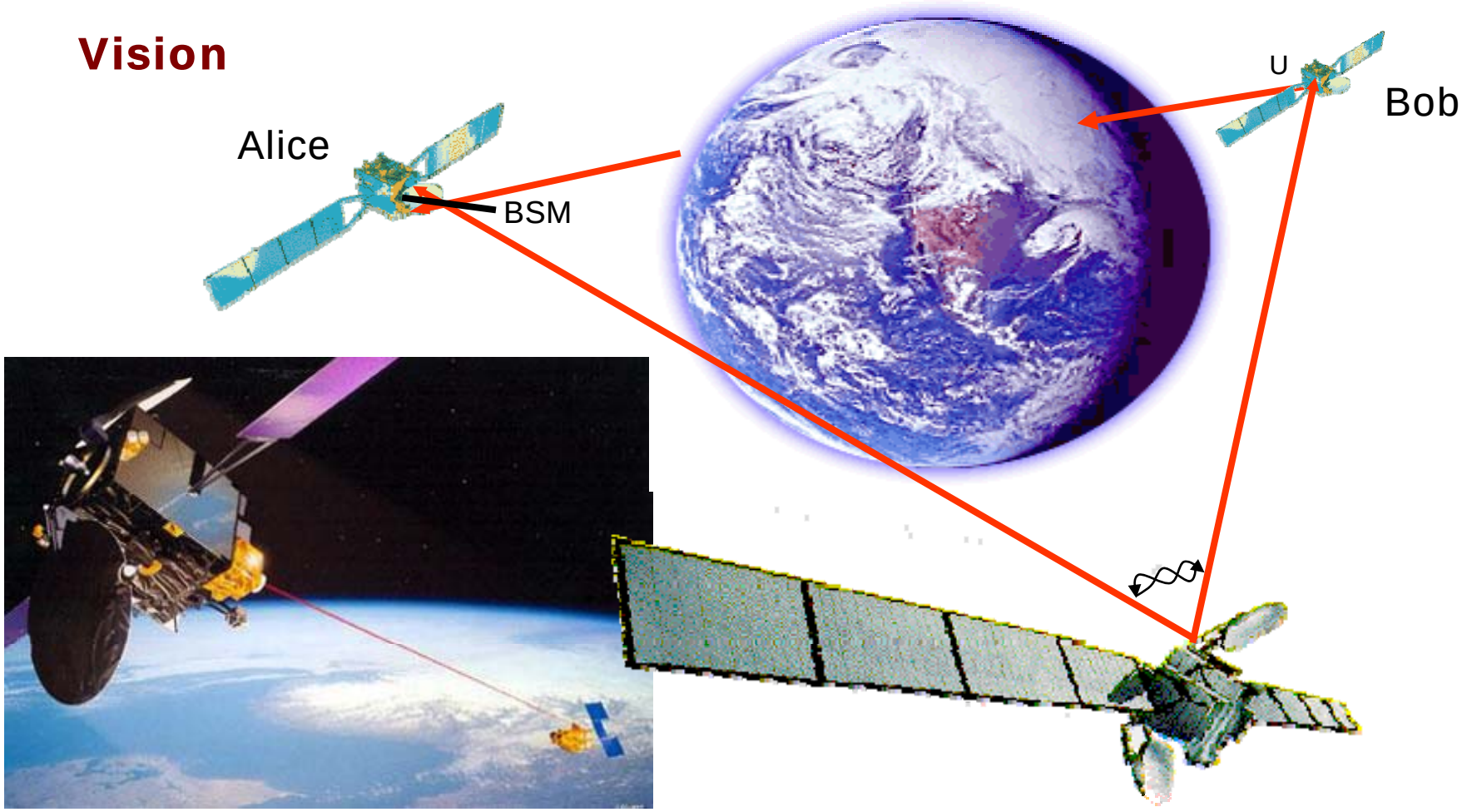
Two downlink telescops

Electronics

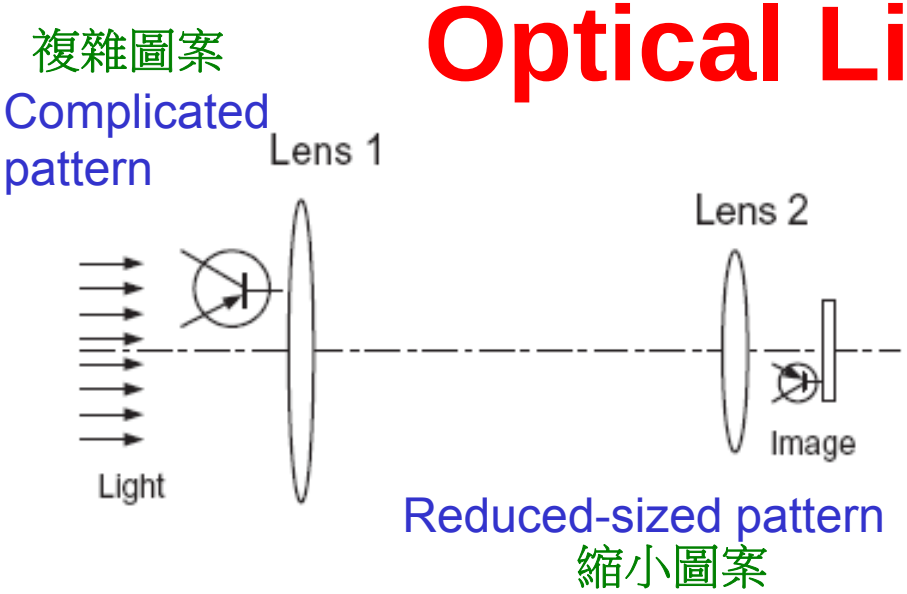
Aspelmeyer et al., quant-ph/0305105
Kaltenbaek et al., quant-ph/0308174
Pfennigbauer et al., JON 4, 549-560 (2005)

The Future of QKD(量子金鑰傳輸)?

Vision

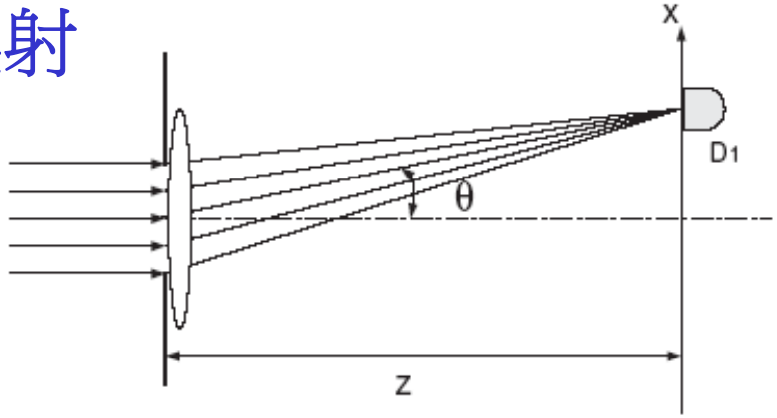


光學平版印刷術
Optical Lithography



- The resolution of the reduced image cannot be better than $\lambda/2$ due to the diffraction effect..
- No effective lenses working at very short wavelength in x-ray region
- Using ***N*-photon entangled state** to achieve a spatial resolution equivalent of using a light with wavelength λ/N.

繞射



$$\text{Diffraction} \propto \frac{\sin^2\beta}{\beta^2},$$

$$\beta = (\pi a/\lambda)\sin\theta.$$

Diffraction limit: minimum width at $\beta=\pi$.

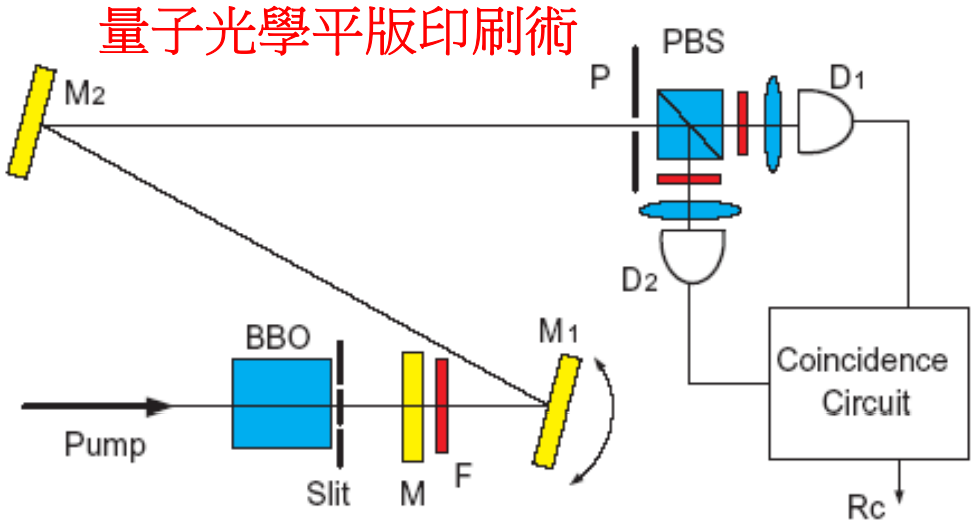
Quantum Interferometric Optical Lithography: Exploiting Entanglement to Beat the Diffraction Limit

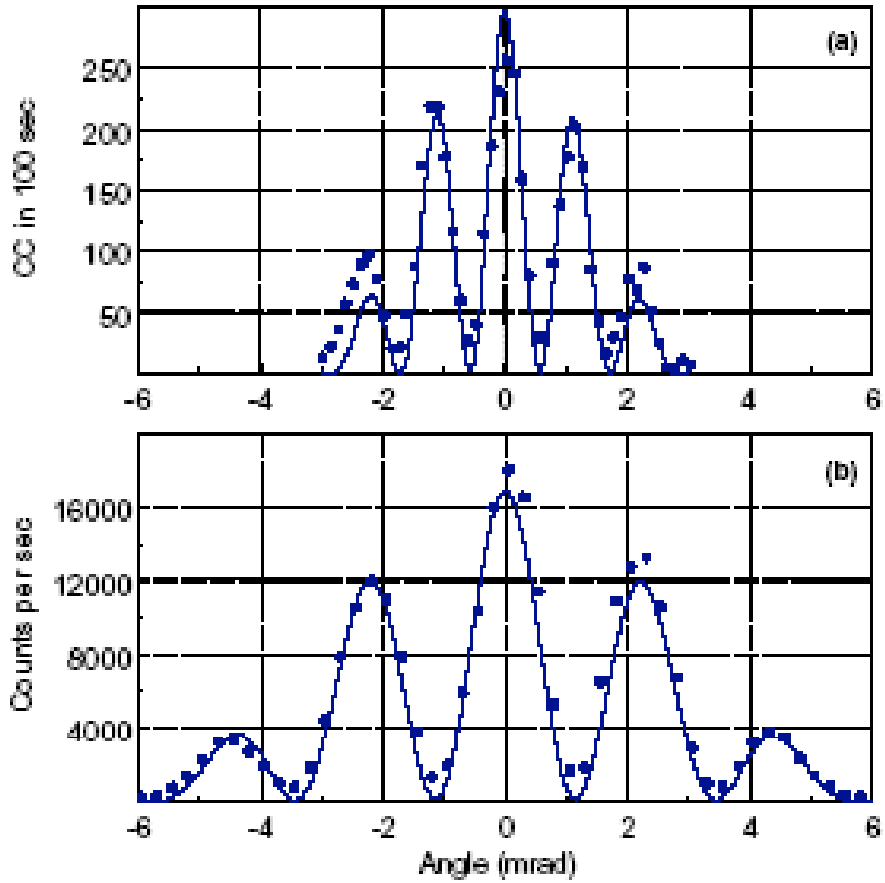
Agedi N. Boto,1 Pieter Kok,2 Daniel S. Abrams,1 Samuel L. Braunstein,2 Colin P. Williams,1 and Jonathan P. Dowling1,* **PRL 85, 2733 (2000)**

Two-Photon Diffraction and Quantum Lithography

Milena D'Angelo, Maria V. Chekhova,* and Yanhua Shih **PRL 87, 13602 (2001)**

量子光學平版印刷術





Two-photon pattern has a faster spatial interference modulation and a narrower diffraction pattern width by a factor of 2 than the classical case.

結語

- 量子計算與量子資訊是一門蓬勃發展的新興研究領域。它是以量子力學準則為運算與工作基礎去研究、發現和進而設計出更有效的或更快速的運算與資訊處理方法的新學門。
- 我們介紹了目前科學家們正嘗試去研究製造的幾個量子電腦的設計和最近在量子資訊與通訊上的新進展。
- 雖然大部份這些發展都還在基礎科學的研究階段，可是這些新穎應用的設計提案與實際的實驗努力已帶來令人印象深刻的初步成果。
- 它們在未來能否進而演變成一個嶄新實用的量子科技或量子資訊工程學門也是值得讓人深切期待的。
- 就像60多年前科學家發明電晶體後，不可能知道今天的科技，已可用大量電晶體，做出2萬元有找的筆記型電腦。科學家現在盡力研究量子電腦，同樣也沒人知道究竟會不會成功，即使後來發現實際可用的量子電腦無法被製造完成，但在研究過程中，勢必會發現更多新科技，對改善人類生活做出更多、更偉大的貢獻。