Quantum information in a nutshell (簡介)

Quantum mechanics + information science
= quantum information science
= quantum information transfer
+ quantum algorithm (software)
+ quantum computer (hardware)
+ quantum simulation
+…
= a field rapidly growing in the last 10 years

師範大學物理系 張明哲

Brief histroy

- 1982 A. Aspect: verified Bell inequality experimentally
- R. Feynman: proposed quantum computation, and gave lectures
- 1984 C.H. Bennett and G. Brassard: quantum cryptography (密碼)
- 1985 D. Deutsch: “Quantum theory, the Church-Turing principle, and the universal quantum computer”
- 1993 C.H. Bennett et al: quantum teleportation (遠傳)
- 1994 P.W. Shor: algorithm (算則) for finding prime factors of an integer
- 1996 A. Steane and P. Shor: quantum error correction
- 1997 L.K. Grover: algorithm for database searching
- 1997 A. Zeilinger’s group: teleportation of photon
- ...
- 2001 I. Chuang’s group: quantum computer with 7-qubit can factor integer 15

Recommended references

- General
  - *The code book (碼書)*, by S. Singh
  - The ghost in the atom (*原子中的幽靈*), edited by P. Davis and J. Brown
  - Schrodinger's kittens (*薛汀格的貓*), by J. Gribbin
  - *The Feynman processor (費曼處理器)*, by G. Milburn
  - *Feynman lectures on computation*, by R. Feynman
- Lecture notes
  - D. Mermin's on-line lecture note (Cornell)
  - J. Preskill's on-line lecture note (Caltech)
- Books
  - *Quantum computation and quantum information*, by M. Nielsen and I. Chuang
  - *The physics of quantum information*, by D. Bouwmeester, A. Ekert and A. Zeilinger
- ITP's on-line conferences on quantum information
  - http://online.itp.ucsb.edu/online/qinfo_c01/ and /qinfo01/
- LANL /quant-ph preprint archive

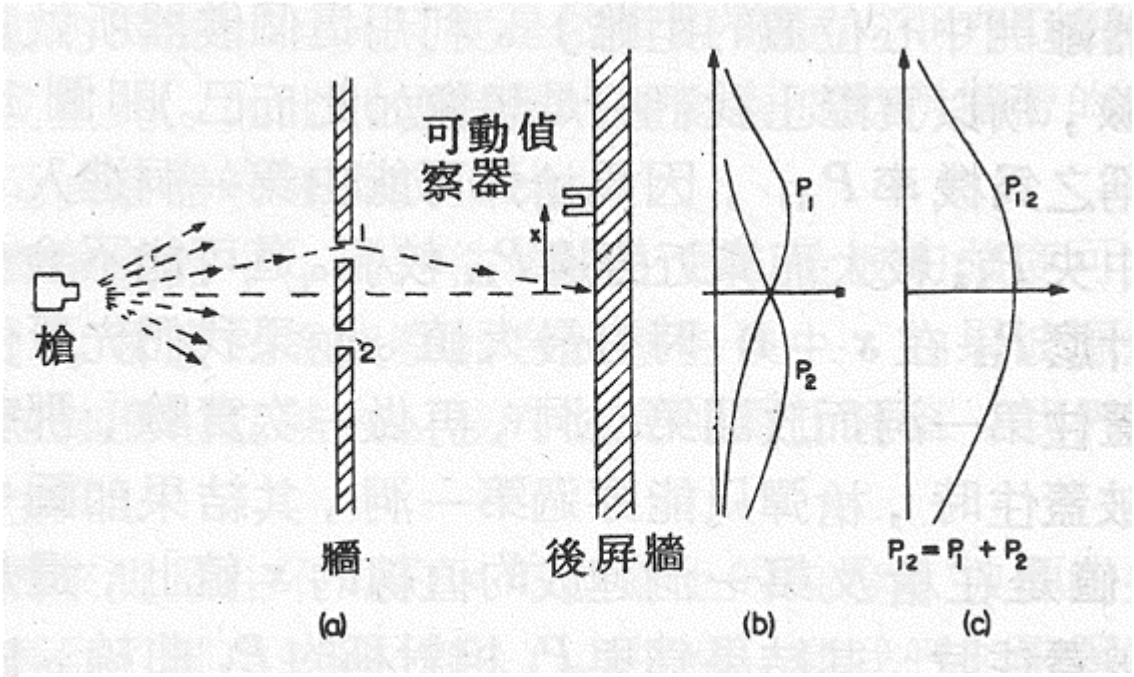
A partial list of journal articles

- Quantum-Mechanical Computers, by S. Lloyd, Sci. Am. Oct. (1995).
- Quantum computation and Shor's factoring algorithm, by A. Ekert and R. Jozsa, Rev. Mod. Phys. **68**, 733 (1996).
- Special issue on quantum information in Phys. World, Mar. (1998).
- J. Bell and the most profound discovery of science, by A. Whitaker, Phys. World, Dec. (1999).
- Experiment and the foundation of quantum mechanics, by A. Zeilinger, Rev. Mod. Phys. **71**, S288 (1999).
- Quantum theory: weird and wonderful, by T. Leggett, Phys. World, Dec. (1999).
- Quantum teleportation, by A. Zeilinger, Sci. Am. Apr. (2000).
- !00 years of quantum mysteries, by M. Tegmark and J.A. Wheeler, Sci. Am. Feb. (2001).
- Quantum-state engineering with Josephson-junction devices, by Y. Makhlin et al, Rev. Mod. Phys. **73**, 357 (2001).
- Quantum cryptography, by N. Gisin et al, Rev. Mod. Phys. **74**, 145 (2002).
- Rules for a complex quantum world, by M. Nielsen, Sci. Am. Oct. (2002).
  - 量子計算的遊戲規則,科學人,2003年一月號
- Single photons on demand, by P. Grangier and I. Abram, Phys. World, Feb (2003).

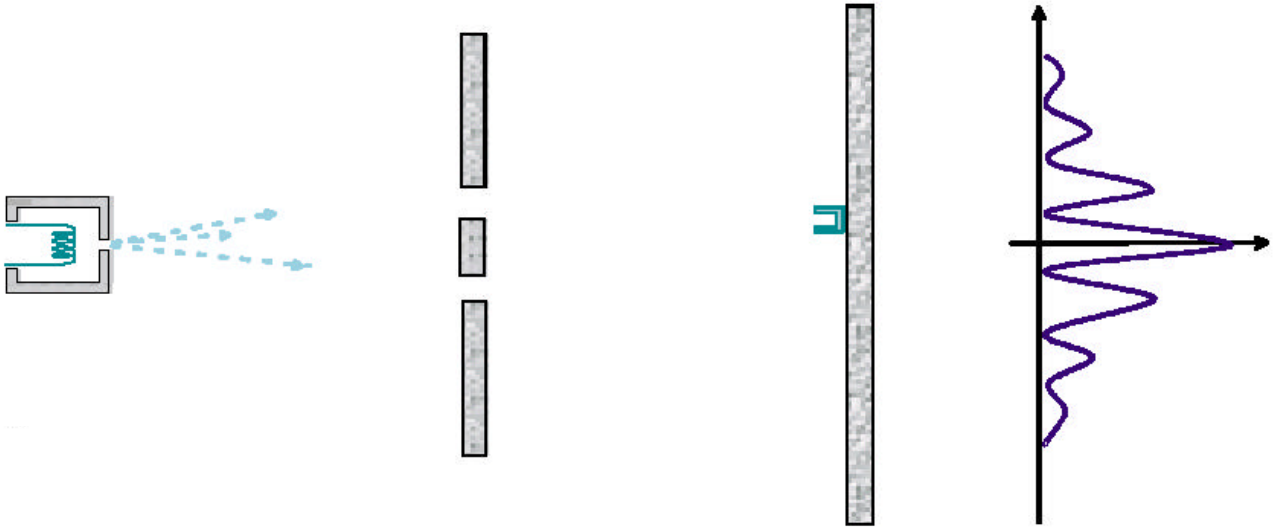
Articles in Physics Today

- Is the moon there when nobody looks? by D. Mermin, Apr. (1985).
- What's wrong with these elements of reality? By D. Mermin, June (1990).
- Information is physical, by R. Landauer, May (1991).
- Decoherence and the transition from quantum to classical, by W.H. Zurek, Oct. (1991); also see the Letters Column in Apr. (1993) for responses.
- Quantum cryptography defies eavesdropping, by, G.P. Collins, Nov. (1992).
- Multiparticle interferometry and the the superposition principle, by D.M. Greenberger, M.A. Horne, and A. Zeilinger, Aug (1993).
- Quantum information and computation, by C. Bennett, Oct. (1995).
- Quantum computing: dream or nightmare? by S. Haroche and J.M. Raimond, Aug. (1996).
- Ehaustive searching is less tiring with a bit of quantum magic, by G.P. Collins, Oct. (1997).
- Quantum teleportation channels opened in Rome and Innsbruck, Feb. (1998).
- Entanglement, decoherence, and the quantum/classical boundary, by S. Haroche, July (1998).
- Battling decoherence: the fault-tolerant quantum computer, by J. Preskill, June (1999).
- Single microwave photons can be measured nondestructively, by R. Fitzgerald, Oct. (1999)
- What really gives a QC its power?, by R. Fitzgerald, Jan. (2000).
- Physicists triumph at guess my number, by A.M. Steane and W. van Dam, Feb. (2000).
- From quantum cheating to quantum security, by D. Gottesman and H.K. Lo, Nov. (2000).
- Two realization schemes raise hopes for SC quantum bits, by R. Fitzgerald, June (2002).
- Quantum entanglement: a modern perspective, by B. Terhal et al, Apr (2003).

2-slit experiment using bullets

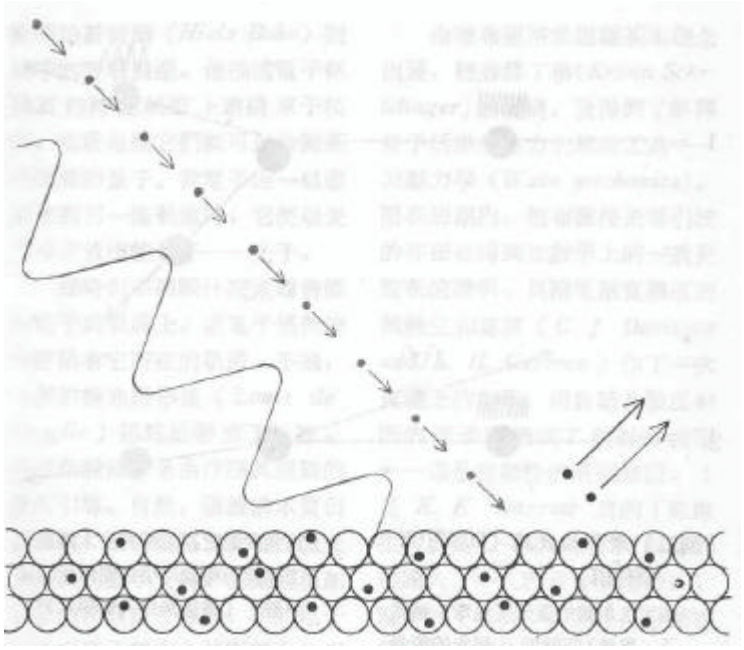


2-slit interference of light (Young, 1801)



Light behaves like water waves

Photo-electric effect (Einstein, 1905)



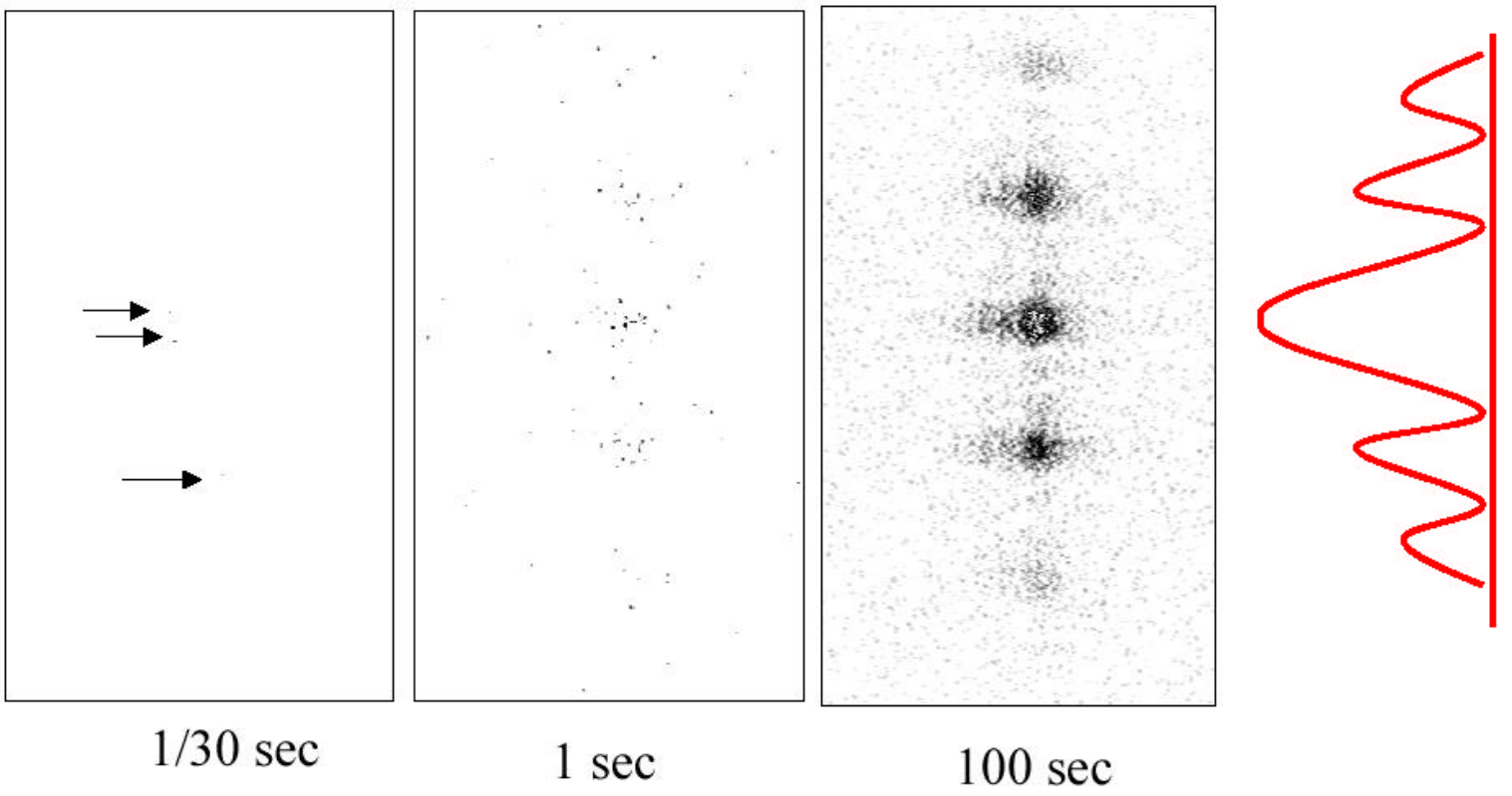
Light behaves like particles

- higher intensity, more emitted electrons, but with the same kinetic energy
- kinetic energy of electrons depends on light frequency
- below a critical frequency, no electrons emitted

$\rightarrow \quad E = h\nu$

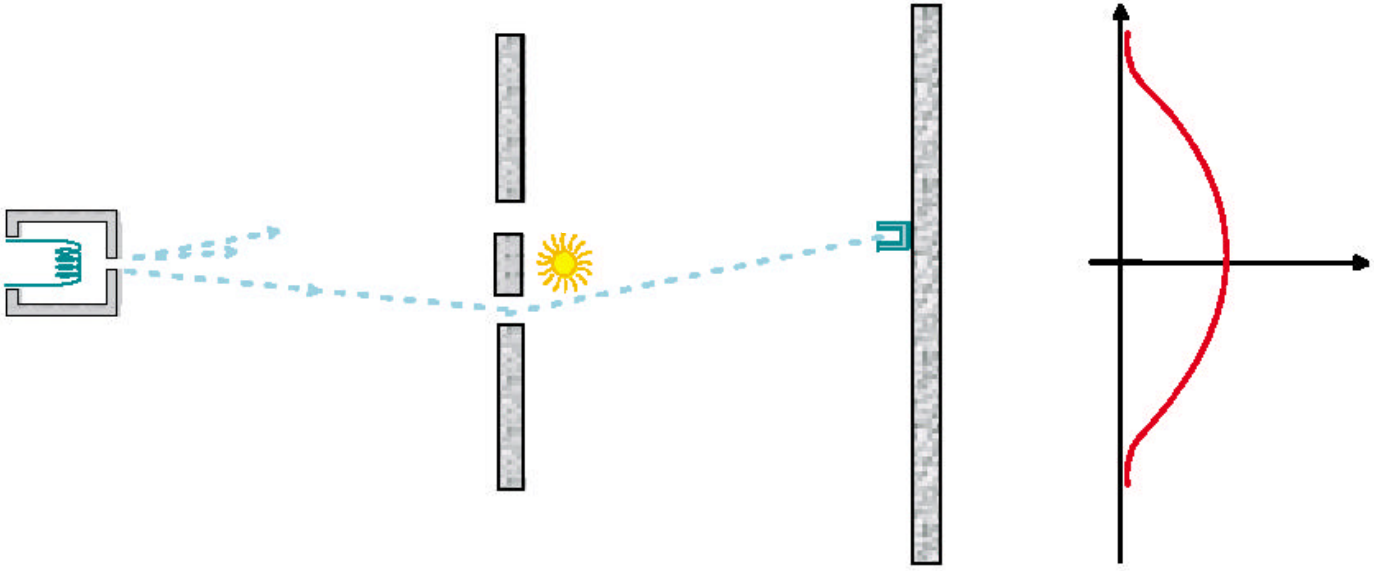
$(h/2\pi = 10^{-27}$ erg-sec)

2-slit experiment: single photon interference



Light behaves like both wave and particles

Which-way measurement



- if they are particles, then they cannot interfere

What's special about the microscopic world?

Classical	Quantum
~~wave or particle~~	wave and particle (Einstein 1905, de Broglie 1923)
~~position and velocity (x,v)~~	wave function $\psi(x,t)$
~~Newton's eq of motion~~	Schrodinger's wave eq.(1925)
$m\frac{d^2\vec{x}}{dt^2} = \vec{F}(\vec{x},t)$	$i\hbar\frac{\partial y(\vec{x},t)}{\partial t} = \left[-\frac{\hbar^2}{2m}\frac{d^2}{d\vec{x}^2} + V(\vec{x})\right] y(\vec{x},t)$
~~deterministic~~	probabilistic for a single event, deterministic for a collection of events (Bohr, Heisenberg...)

Measurement process in quantum mechanics

Take 2-slit experiment as an example

- Before the photon hits the detector, it is a superposition of up-hole (0) and down-hole (1) states

$$|\Psi>= a|0>+b|1> \quad \text{(Dirac's notation)}$$

- Upon “measurement”, it “collapses” (縮併) to a particular state

$$|\Psi> \rightarrow |0> \text{ with probability } |a|^2, \quad \text{(Born's rule, 1926)}$$
$$\rightarrow |1> \text{ with probability } |b|^2, \quad |a|^2+|b|^2=1$$

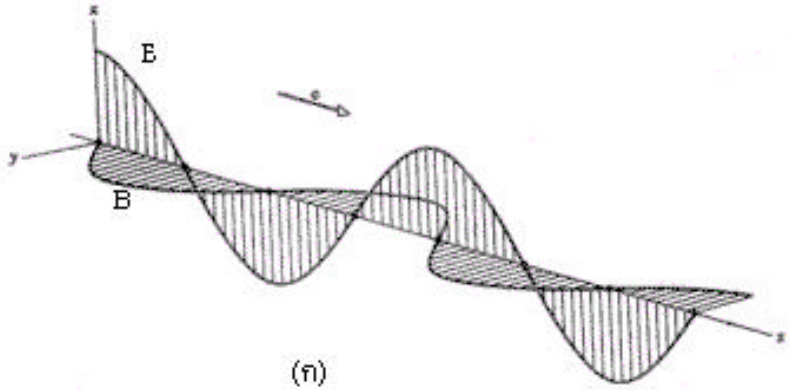
- The collapse is irreversible and cannot be avoided

How to build a quantum bit?

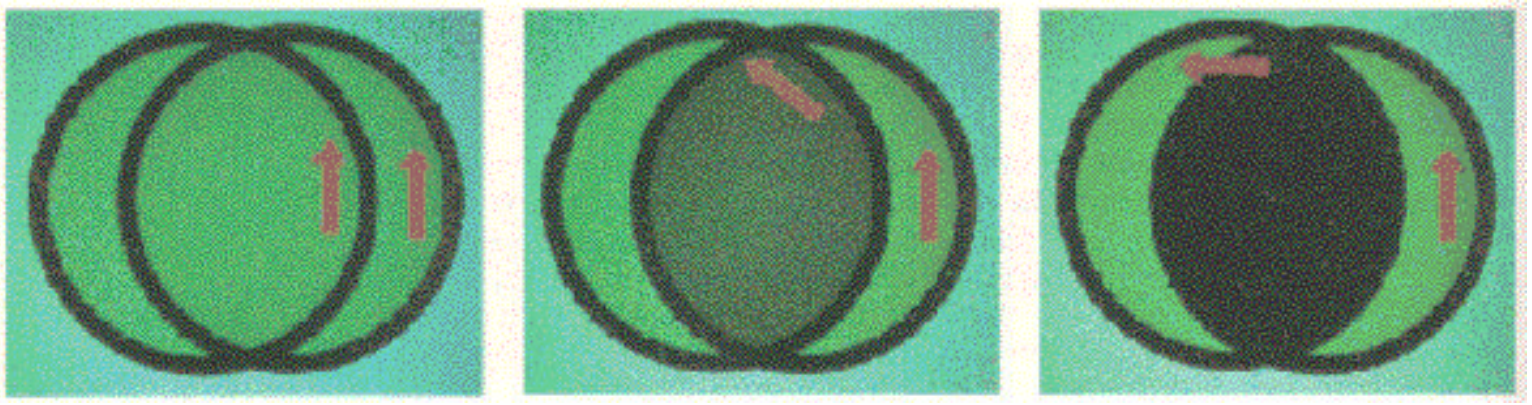
- Any 2-state system can be a qubit:
  - photon (two polarizations)
  - electron, nucleus…(spin-1/2)
  - linear ions in a trap (GS and the lowest vibrational mode)
  - Bose-Einstein condensate (spinning state of the atoms...)
  - Josephson junction (two opposite circulations)
  - …

- Before you read it, a qubit can be 0 and 1 at the same time
- When you read it, it is either 0 or 1

Polarization of light

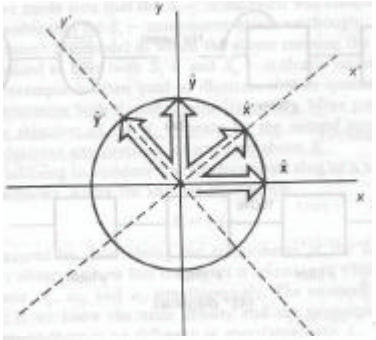


(ก)



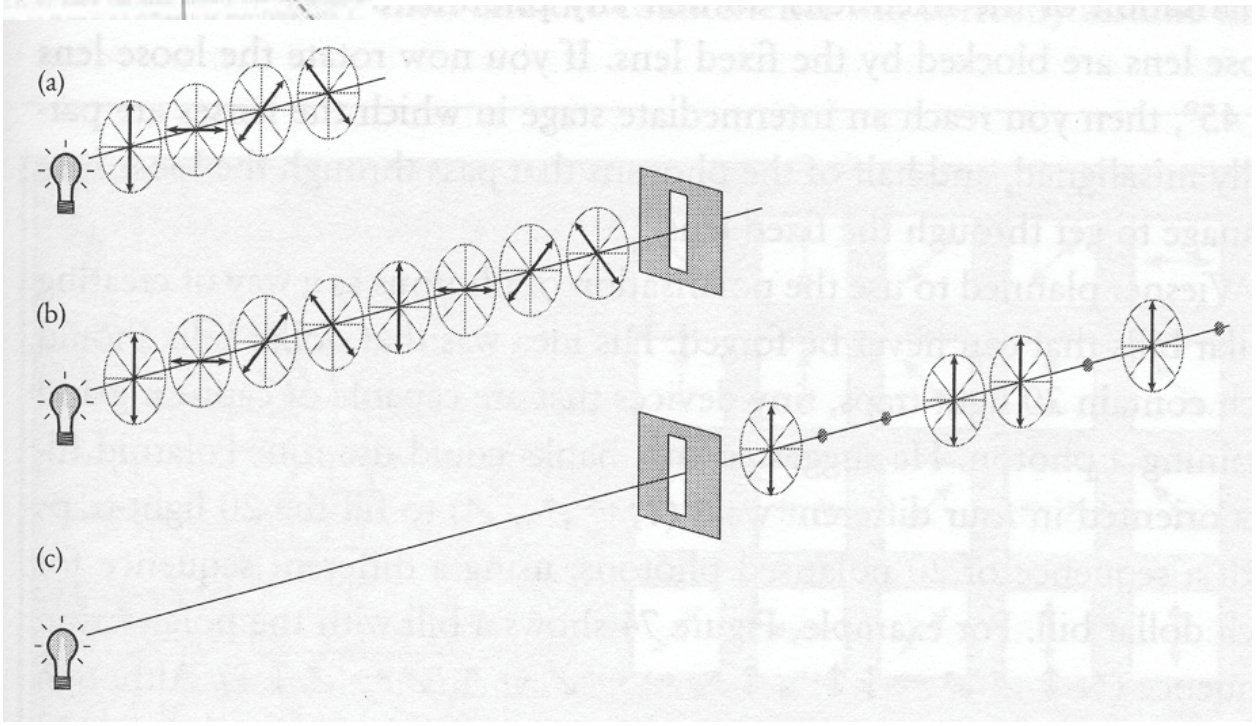
$$I(q) = I_0 \cos^2 q$$ (Marlus law)

State of a single photon

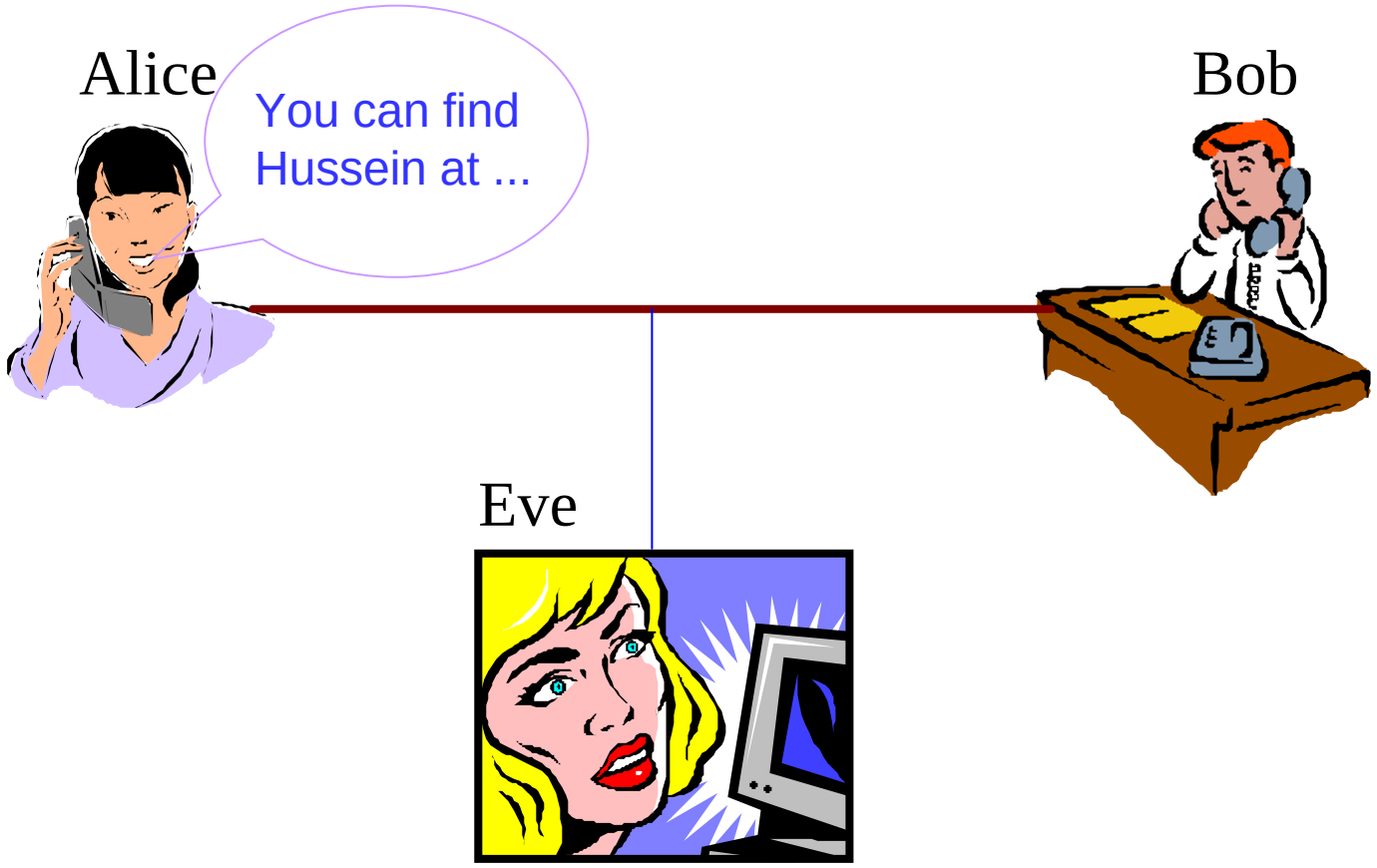


$$|x'\rangle = \frac{1}{\sqrt{2}}|x\rangle + \frac{1}{\sqrt{2}}|y\rangle, \quad (50\%\ |x\rangle + 50\%|y\rangle)$$

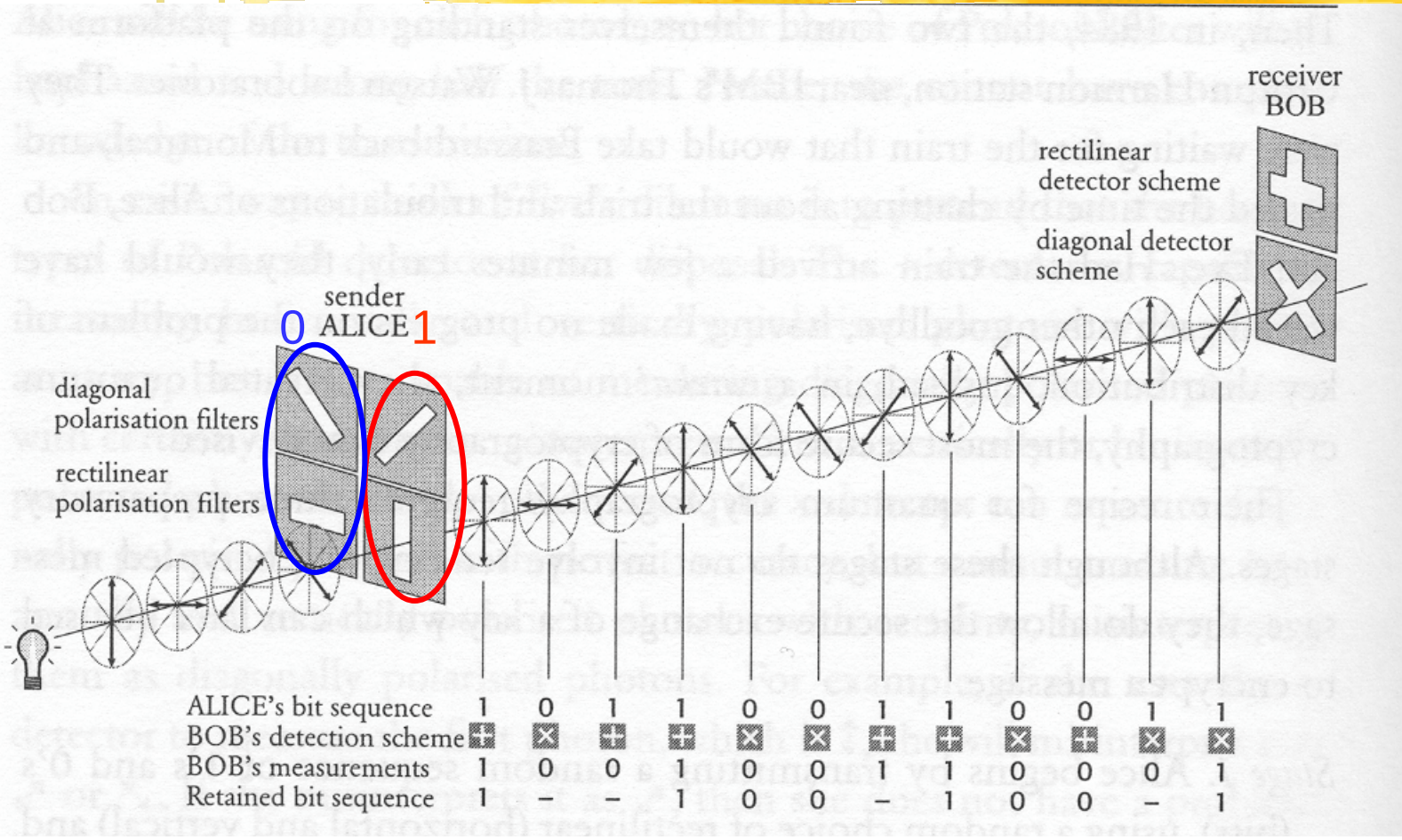
$$|y'\rangle = -\frac{1}{\sqrt{2}}|x\rangle + \frac{1}{\sqrt{2}}|y\rangle \quad (50\%\ |x\rangle + 50\%|y\rangle)$$



How can we detect eavesdroppers

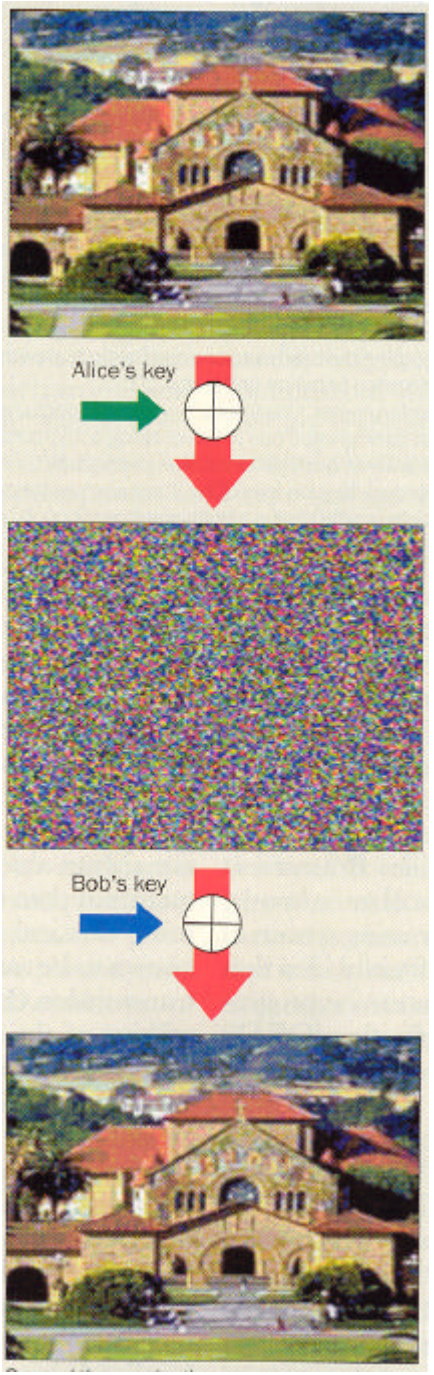


Quantum key distribution (Bennett and Brassard, 1984)



From p.342 of *The code book*, by S. Singh

Quantum key distribution



- Current status (July, 2003):
100 km via cable; 23 km via open air.
- Transmission rate: a few kbit/sec
- Commercial product: id Quantique
A quantum leap for cryptography

What's the use of quantum information ?

- transfer of information
  - distribution of "public key" (公開鑰匙) in cryptography
  - "superdense coding" (超密編碼) in data transmission
  - "quantum teleportation" (量子遠傳) of states
- computation (質因數分解)
  - factorizing large integers (to break RSA encryption)
  - searching a large data base (資料庫搜尋)
  - Solving NP-complete problems (travelling salesman...)
- more exotic applications...

Table 4.1. Milestones in the development of quantum computer technology

Type of hardware	No. of qubits needed	No. of steps before decoherence	Status
Quantum Cryptography	1	1	implemented
Entanglement based quantum cryptography	2	1	demonstrated
Quantum C-NOT gate	2	1	demonstrated
Composition of gates	2	2	demonstrated
Deutsch's algorithm	2	3	demonstrated
Channel capacity doubling	2	2	imminent
Teleportation	3	2	demonstrated
Entanglement swapping	4	1	demonstrated
Repeating station for quantum cryptography	a few	a few	theory still incomplete
Quantum simulations	a few	a few	simple demos
Grover's algorithm with toy data	3+	6+	demonstrated with NMR
Ultra-precise frequency standards	a few	a few	foreseeable
Entanglement purification	a few	a few	foreseeable
Shor's algorithm with toy data ...	16+ ...	hundreds + ...	
Quantum factoring engine	hundreds	hundreds	
Universal quantum computer	thousands +	thousands +	

From p.102 of *The physics of quantum information*

Superposition of multiple-qubit states

Quantum entanglement 量子糾纏

Separable states: eg., $|0>_A|0>_B$, $|1>_A|1>_B$

Entangled states: eg., $\frac{1}{\sqrt{2}}\left(|0>_A|1>_B - |1>_A|0>_B\right)$

- It is non-local in nature, aka “spooky action at a distance”
- Stimulated the invention of EPR paradox, Bell inequality...
- Before “recording”, neither qubit value pops into existence!

See D. Mermin in

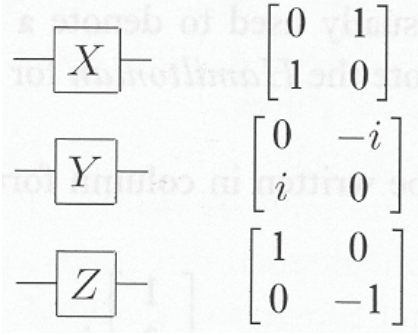
Physics Today, Apr. 1985: *Is the moon there when nobody looks?*

Qubit states and Pauli gates

1-qubit states: $|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}, |1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$

2-qubit states: $|00\rangle = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}, |01\rangle = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}, |10\rangle = \begin{pmatrix}0\\0\\1\\0\end{pmatrix}, |11\rangle = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}$

1-qubit Pauli gates:



For example, X|0>=|1>, X|1>=|0>

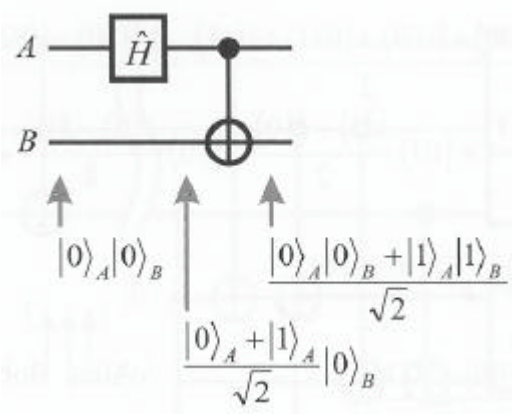
Hadamard gate and CNOT (aka XOR) gate 受控非閘

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

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

Matrix representation

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

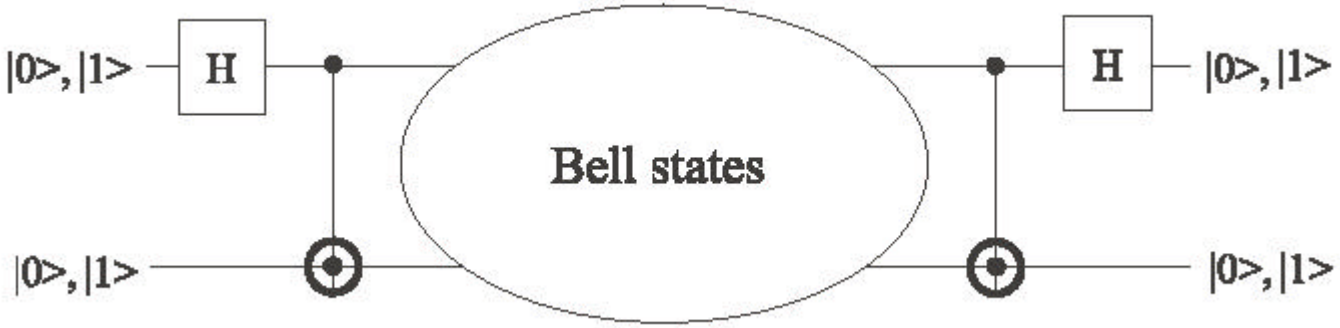


$$C_X|00\rangle = |00\rangle, \quad C_X|01\rangle = |01\rangle,$$
$$C_X|10\rangle = |11\rangle, \quad C_X|11\rangle = |10\rangle.$$

$$C_X = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

All possible quantum logic gates can be built by using only 1-qubit unitary gate (SU_2 rotation) and CNOT gate

Bell states



$$C_X H|0>|0> = \frac{1}{\sqrt{2}}\left(|0>|0> + |1>|1>\right) \equiv |f^+>,$$

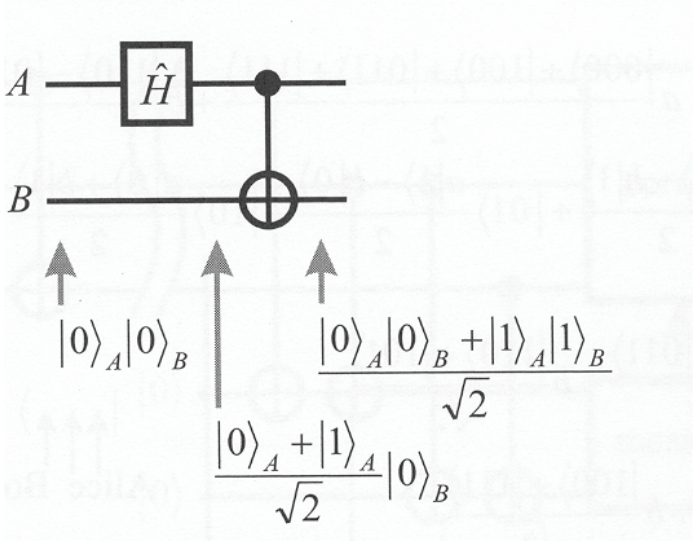
$$C_X H|0>|1> = \frac{1}{\sqrt{2}}\left(|0>|1> + |1>|0>\right) \equiv |y^+>,$$

$$C_X H|1>|0> = \frac{1}{\sqrt{2}}\left(|0>|0> - |1>|1>\right) \equiv |f^->,$$

$$C_X H|1>|1> = \frac{1}{\sqrt{2}}\left(|0>|1> - |1>|0>\right) \equiv |y^->.$$

Quantum superdense coding (Bennett and Wiesner, 1992)

First make an entangled state:



Alice and Bob shares this EPR state:

$$|\Psi_{EPR}\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$$

Quantum superdense coding

Alice prepares and sends one of the 4 Bell states

Bob performs CNOT and H operations to get 2 bits of information!

$$1_a|\Psi_{EPR}>=\frac{1}{\sqrt{2}}(|0>|0>+|1>|1>)$$

$$X_a|\Psi_{EPR}>=\frac{1}{\sqrt{2}}(|1>|0>+|0>|1>)$$

$$Z_a|\Psi_{EPR}>=\frac{1}{\sqrt{2}}(|0>|0>-|1>|1>)$$

$$Z_aX_a|\Psi_{EPR}>=\frac{1}{\sqrt{2}}(|0>|1>-|1>|0>)$$

$$H_aCN_{ab}(1_a|\Psi_{EPR}>)=|0>|0>$$

$$H_aCN_{ab}(X_a|\Psi_{EPR}>)=|0>|1>$$

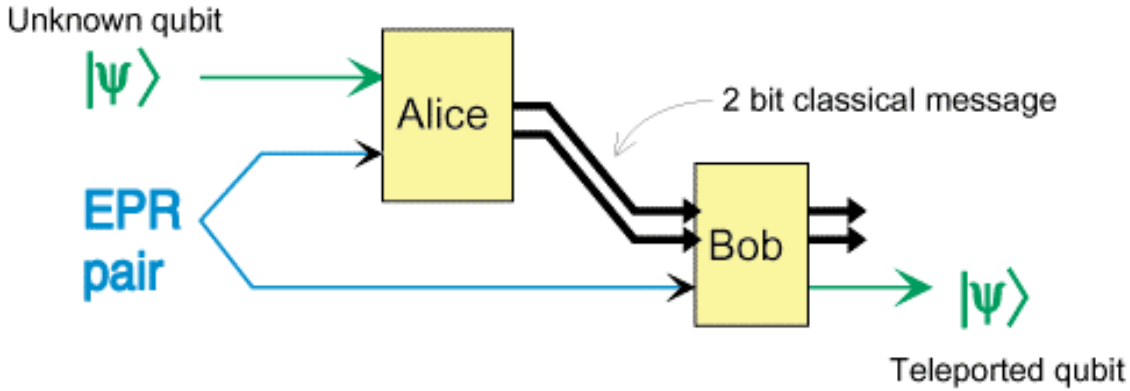
$$H_aCN_{ab}(Z_a|\Psi_{EPR}>)=|1>|0>$$

$$H_aCN_{ab}(Z_aX_a|\Psi_{EPR}>)=|1>|1>$$

Manipulation of quantum entanglement

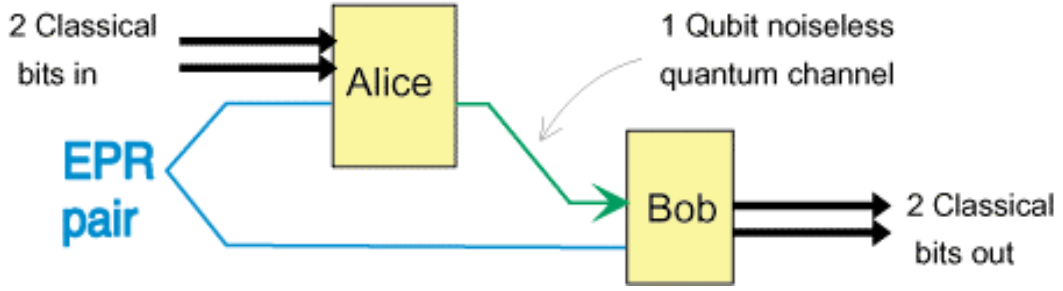
Quantum Teleportation

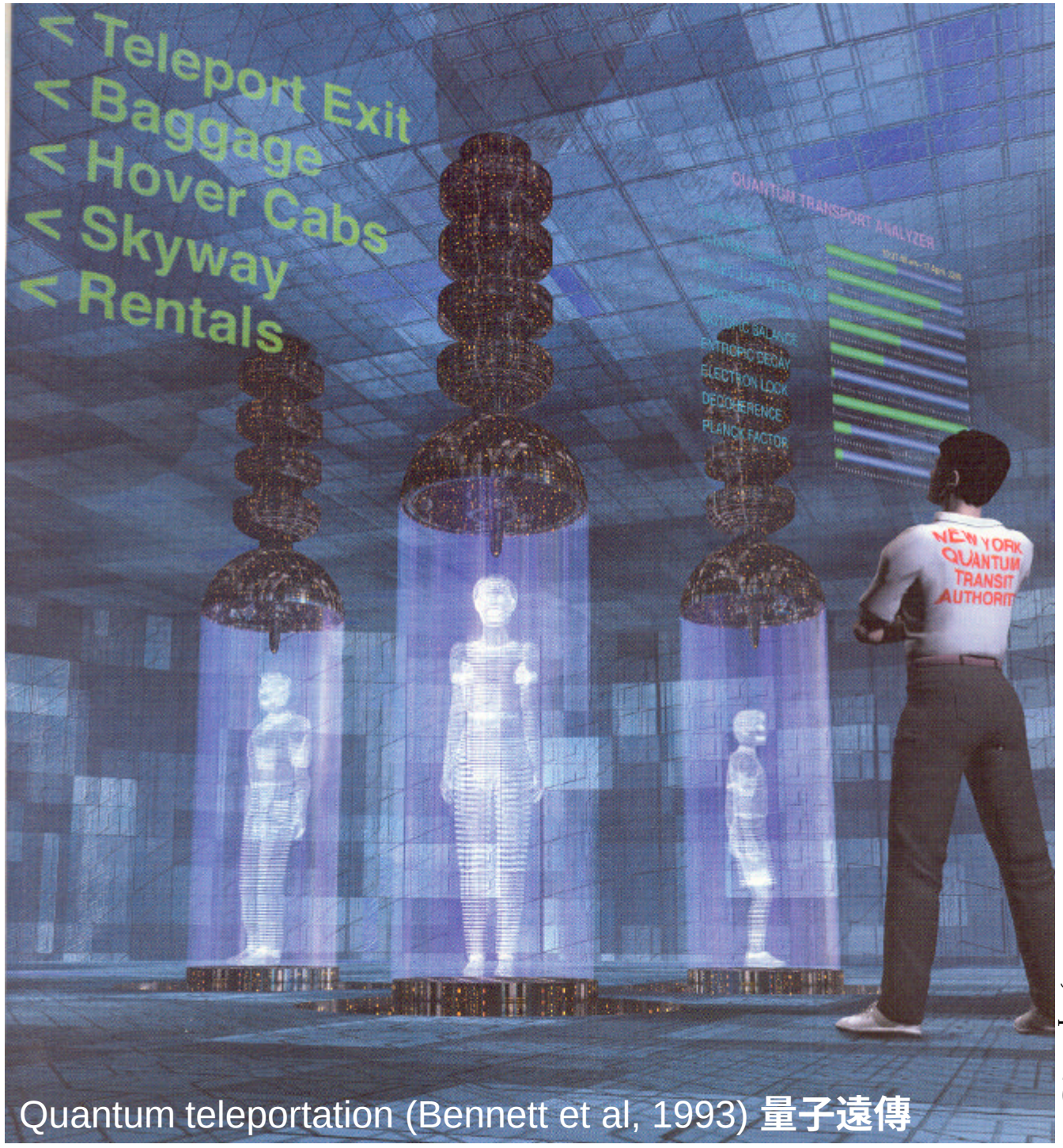
uses 2 classical bits to send 1 qubit



Quantum Superdense Coding

uses 1 qubit to send 2 classical bits





Quantum teleportation (Bennett et al, 1993) **量子遠傳**

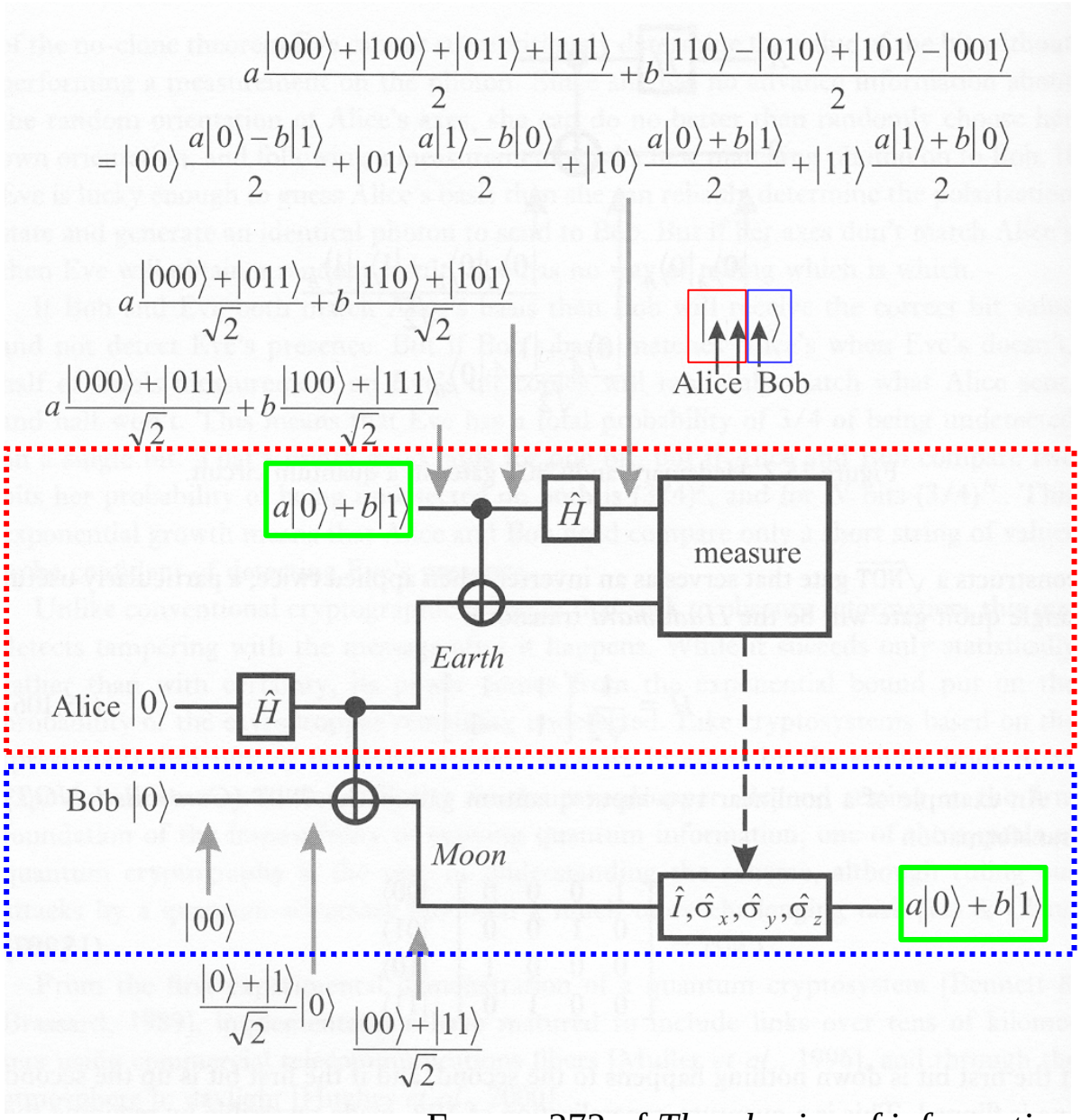
Scientific American, Apr. 2000

Quantum teleportation

(Bennet, Brassard, Crepeau, Jozsa, Peres, and Wootters, 1993)

- QT is not faster than light.
- QT is not quantum “faxing”.
- **Neither** matter **nor** energy is transferred.
- Can teleport a state to a stabler system (Q memory)
- Current status (July, 2003)
  - 10 km via optical fiber, 600 m via air
- For historical notes on QT, see
  - quant-ph/0304158, by Peres
  - quant-ph/0305088, by Mermin

Circuit diagram of quantum teleportation



$$|00\rangle \rightarrow \quad s_Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$|01\rangle \rightarrow is_Y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

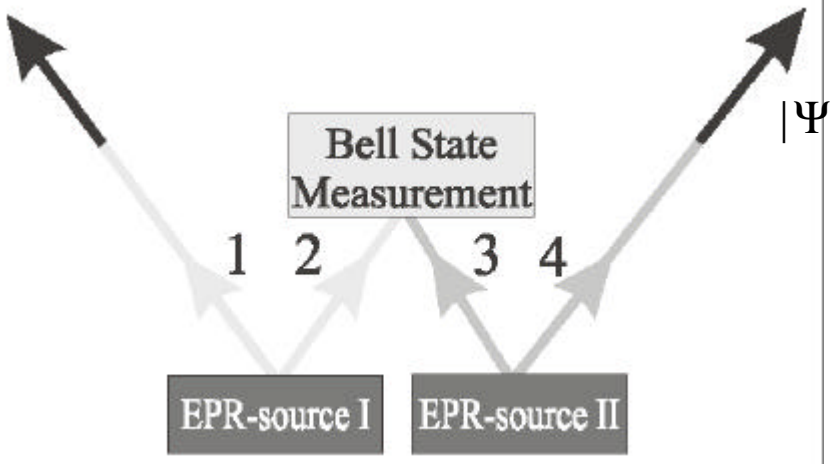
$$|10\rangle \rightarrow \quad I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$|11\rangle \rightarrow \quad s_X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

From p.272 of *The physics of information technology*, by N. Gershenfeld

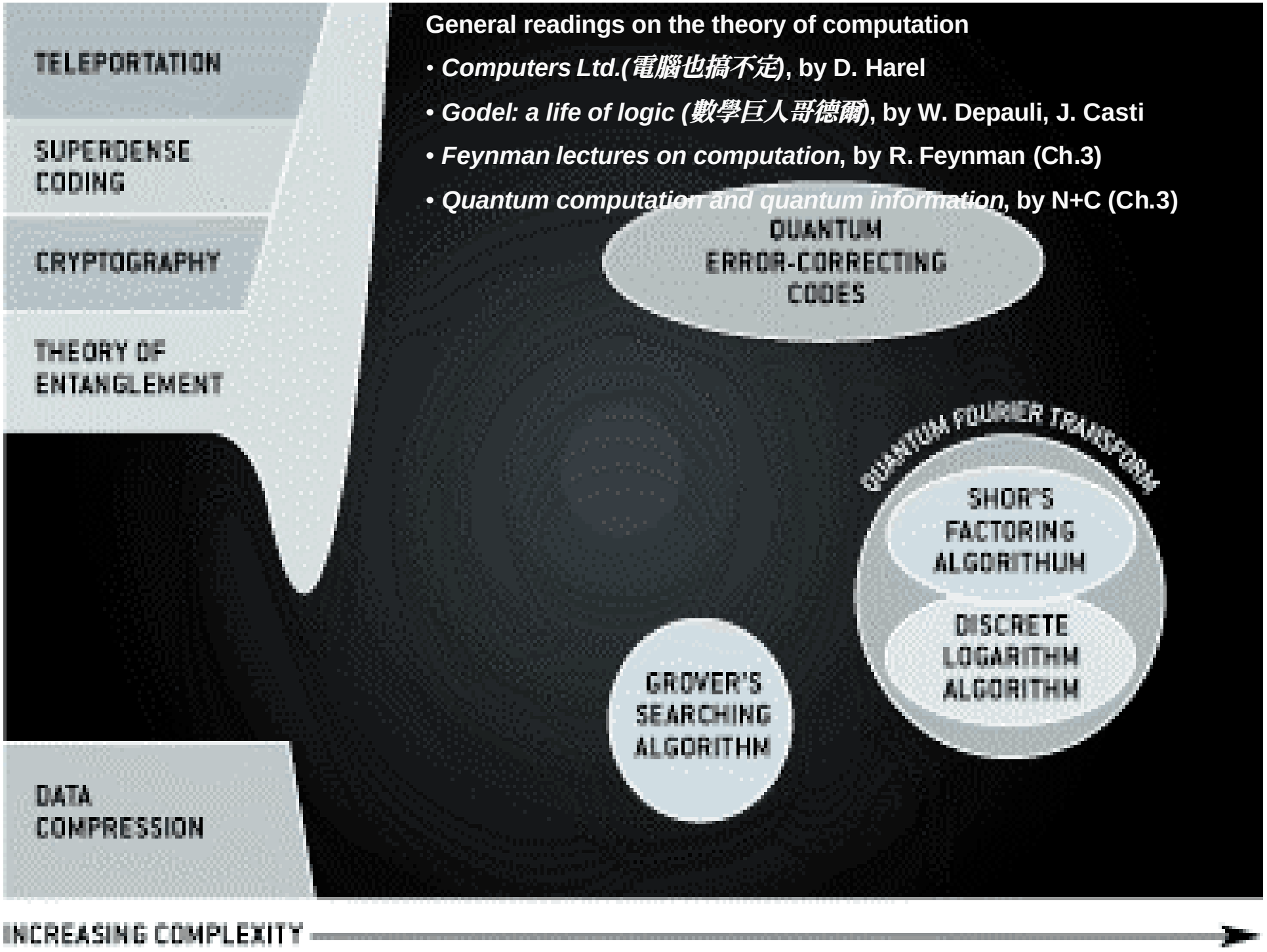
Entanglement swapping (Zukowski et al 1993)

Teleportation of entanglement



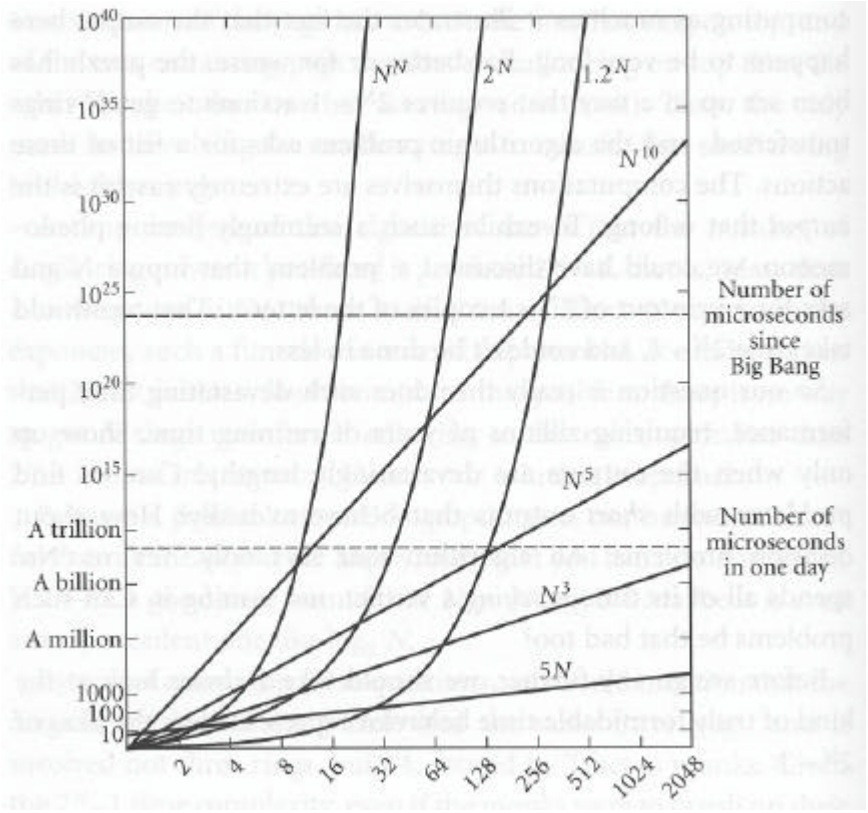
$$|\Psi>_{1234} = \frac{1}{2}\left(|H>_1|V>_2 - |V>_1|H>_2\right)$$
$$\times\left(|H>_3|V>_4 - |V>_3|H>_4\right)$$
$$= \frac{1}{2}(|y^+>_{14}|y^+>_{23} - |y^->_{14}|y^->_{23}$$
$$- |f^+>_{14}|f^+>_{23} + |f^->_{14}|f^->_{23})$$

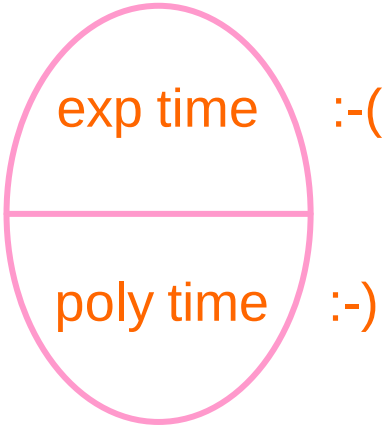
- Before: no entanglement between 1-2 pair and 3-4 pair
- After: 1 and 4 are entangled even though they never interacted!


TELEPORTATION
SUPERDENSE CODING
CRYPTOGRAPHY
THEORY OF ENTANGLEMENT
DATA COMPRESSION
General readings on the theory of computation
• Computers Ltd.(電腦也搞不定), by D. Harel
• Godel: a life of logic (數學巨人哥德爾), by W. Depauli, J. Casti
• Feynman lectures on computation, by R. Feynman (Ch.3)
• Quantum computation and quantum information, by N+C (Ch.3)
QUANTUM ERROR-CORRECTING CODES
QUANTUM FOURIER TRANSFORM
SHOR'S FACTORING ALGORITHUM
DISCRETE LOGARITHM ALGORITHM
GROVER'S SEARCHING ALGORITHM
INCREASING COMPLEXITY

Complexity of computation

Polynomial time vs exponential time (using a Turing machine)



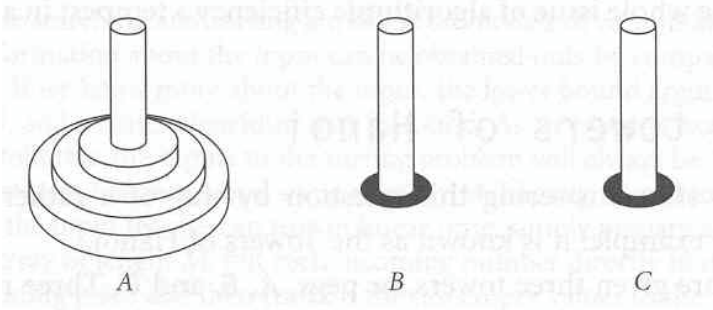


Tractable problems (polynomial time) 易解

- Find the eigenvalues of an M×M symmetric matrix
- # of steps $\propto M^3$
- Find the Fourier transform of a sequence of M values
- # of steps $\propto M (\ln M)$
- ...

Intractable problems (exponential time or worse) **難解**

Hanoi tower



Number of moves = 2^N-1

Tibetan monks have to tackle N=64.

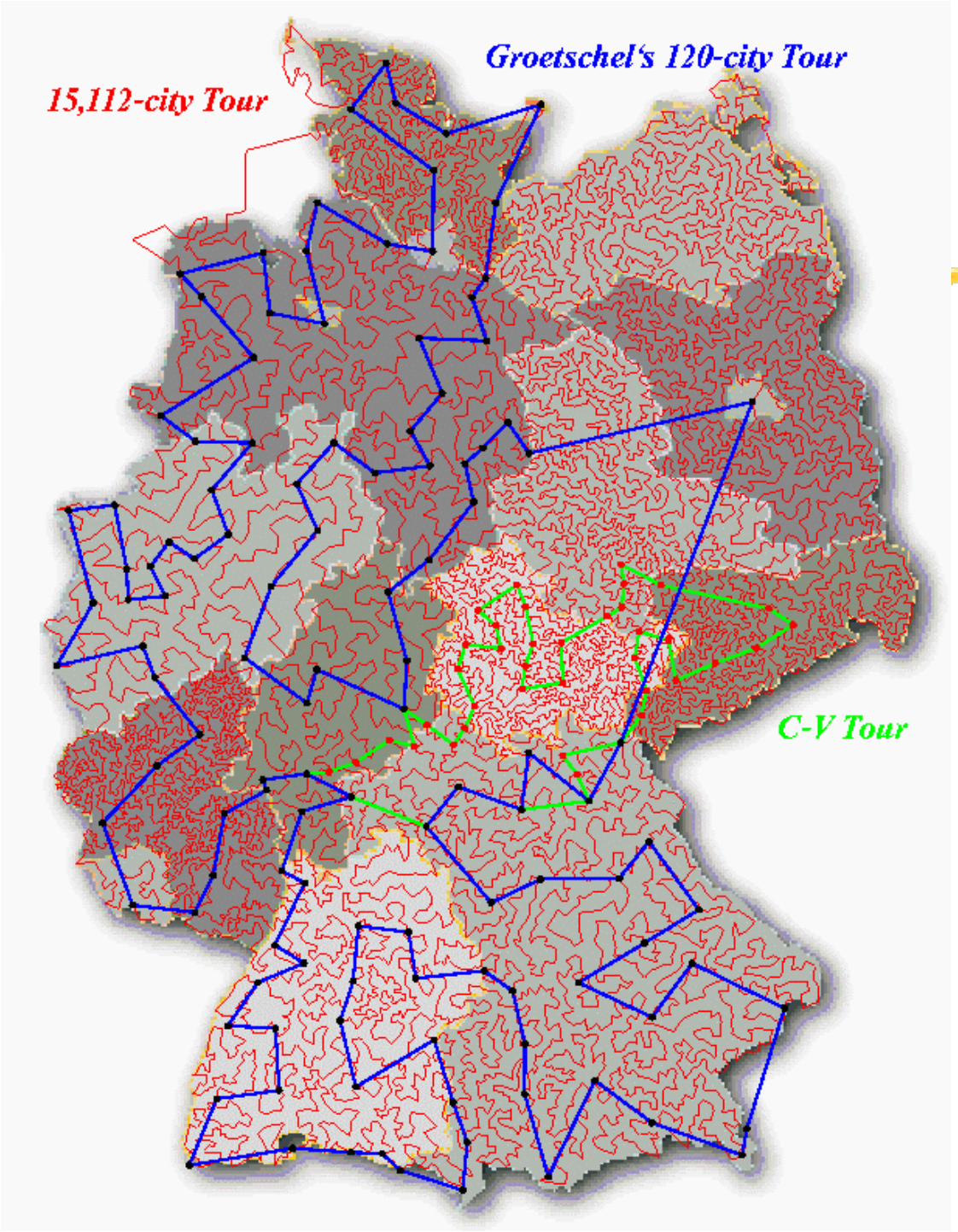
Even if they can move 1 million rings every sec,

it still requires more than half a million years!

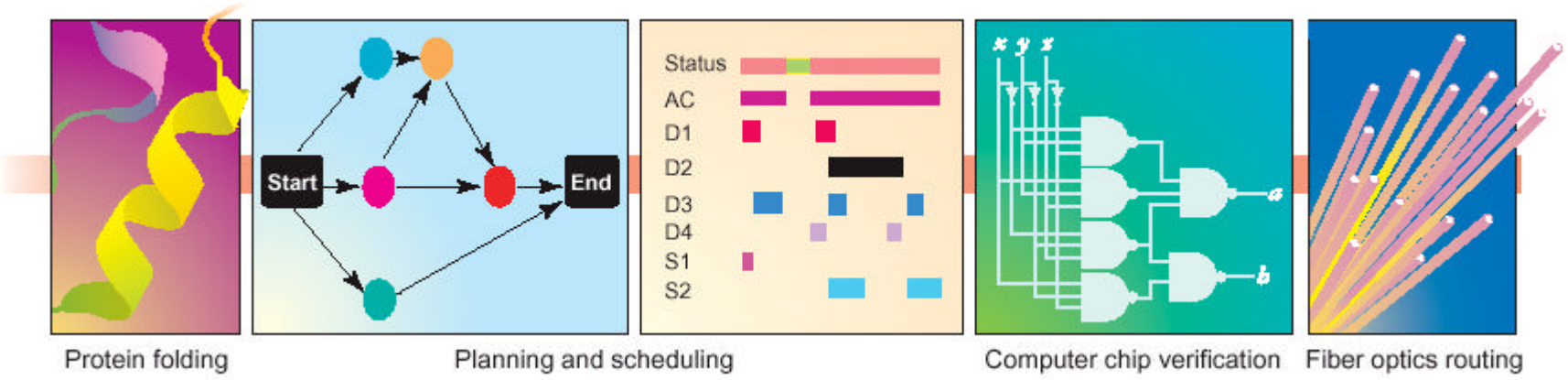
Between tractable and intractable: Travelling salesman problem

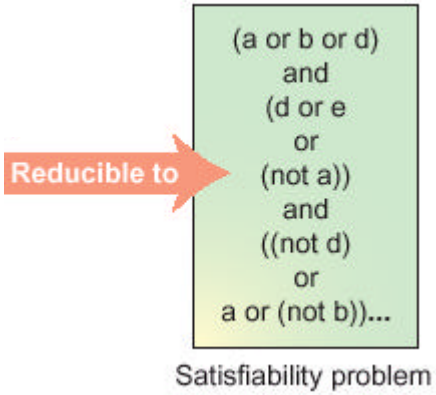
This is the largest TSP instance that has been solved to date (July, 2001), exceeding the 13,509-city tour through the United States that was solved in 1998. The computation was carried out on a network of 110 processors located at Rice University and at Princeton University. The total computer time used in the computation was 22.6 years, scaled to a Compaq EV6 Alpha processor running at 500 MHz. The optimal length of the tour is approximately 66,000 km.

See http://www.math.princeton.edu/tsp/



NP-complete problems and SAT problem





- Still don't know if these problems are tractable or intractable. See www.claymath.org/Millennium_Prize_Problems
- If one of them is tractable/intractable, then all of them are tractable/intractable! (Cook and Levin, 1971)
- Can be reduced to P-time by parallel computation!

From Science **297**, 784 (2002)

Quantum computation

- State preparation (superposition)
- Unitary evolution (don’t peep!)
  - thus is reversible (no place for AND/OR gates, which are irreversible)
  - thus essentially costs no energy! (Landauer principle, 1961)
- Readout (measurement)

A QC is nothing but a giant interference machine!

Quantum computation is parallel in nature

A N-qubit state:

$$|\Psi_{in}\rangle = \frac{1}{2^{n/2}}\left(|11\cdots11\rangle + \cdots + |00\cdots11\rangle + |00\cdots10\rangle + |00\cdots01\rangle + |00\cdots00\rangle\right)$$

$$= \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle_n$$

assume $U_f |x\rangle_n |0\rangle_m = |x\rangle_n |f(x)\rangle_m$

then $U_f |\Psi_{in}\rangle |0\rangle = \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle |f(x)\rangle$

Can get f(x) for all $N=2^n$ x-values in one run! :-)

This does not mean that one run yields multiple results,
since when we “read the tape”, there is only one result! :-(

Basis of *public key* cryptography (RSA, 1977)

4 220 851 x 2 594 209 → **10 949 769 651 859**

ALWAYS EASY
(50 microseconds on a PC)

prime factors

10 949 769 651 859 → **4 220 851 x 2 594 209**

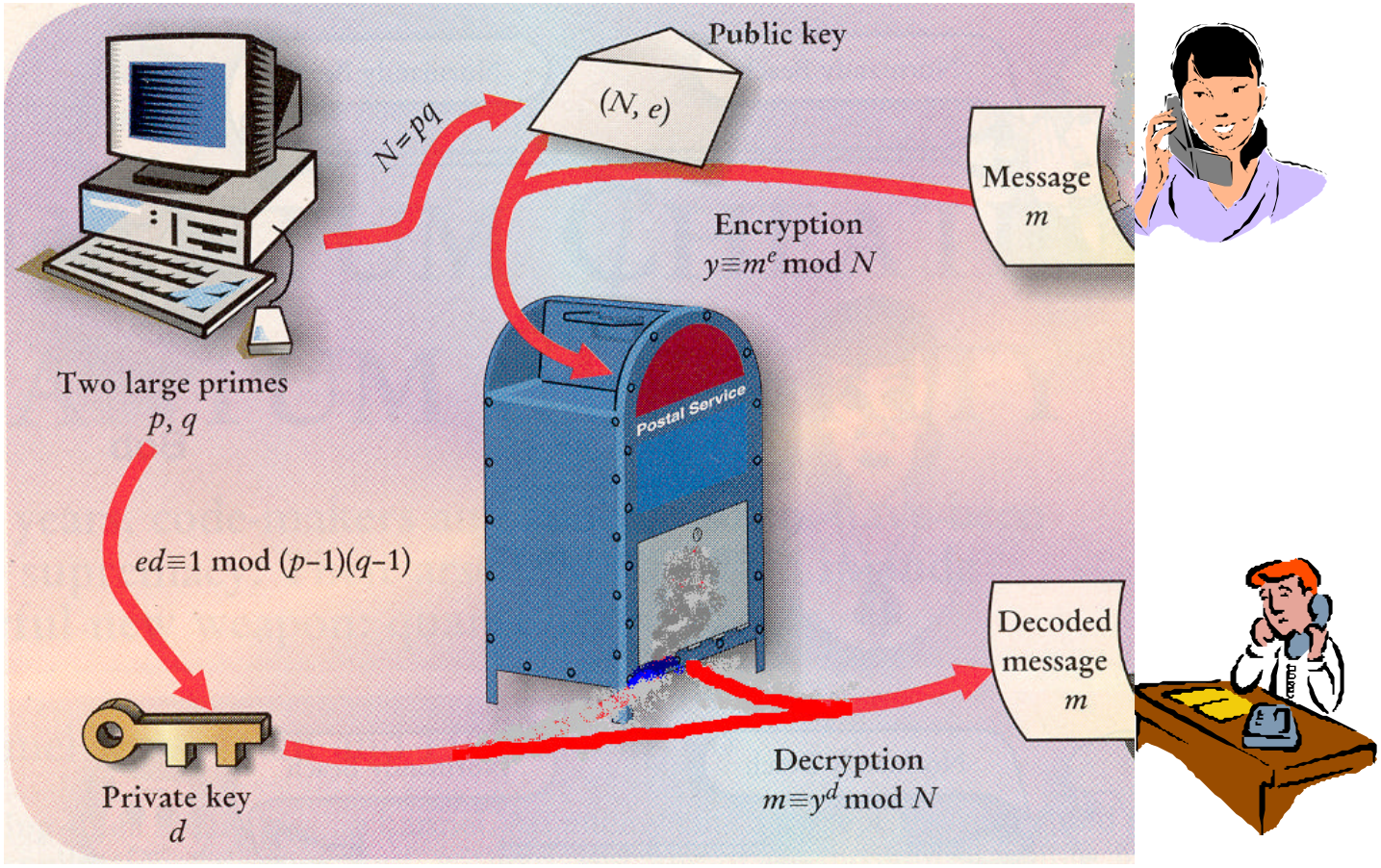
HARD ON A CLASSICAL COMPUTER
(1 second on a PC)

For 250 digits, a million years!

EASY ON A QUANTUM COMPUTER
~ 100 000 qubits, ~ a few hours

From S. Girvin's talk

RSA encryption 加密



To know the math behind this magic, see Mermin's note.

Breaking the code without knowing p and q

How would Eve decode the message?

1. Intercept the encoded message y.
2. Find out a "r" that satisfies $y^r=1 \bmod N$

   (r is called the "order" of y)
3. After r is known, calculate a d' that satisfies $ed'=1 \bmod r$.

   (instead of $ed=1 \bmod (p-1)(q-1)$!)
4. Finally, the message can be decode using

$$y^{d'}=m \bmod N$$

(for details, again consult Mermin's note.)

Best classical algorithm for finding r requires $\exp[n^{1/3}(\log n)^{2/3}]$ steps

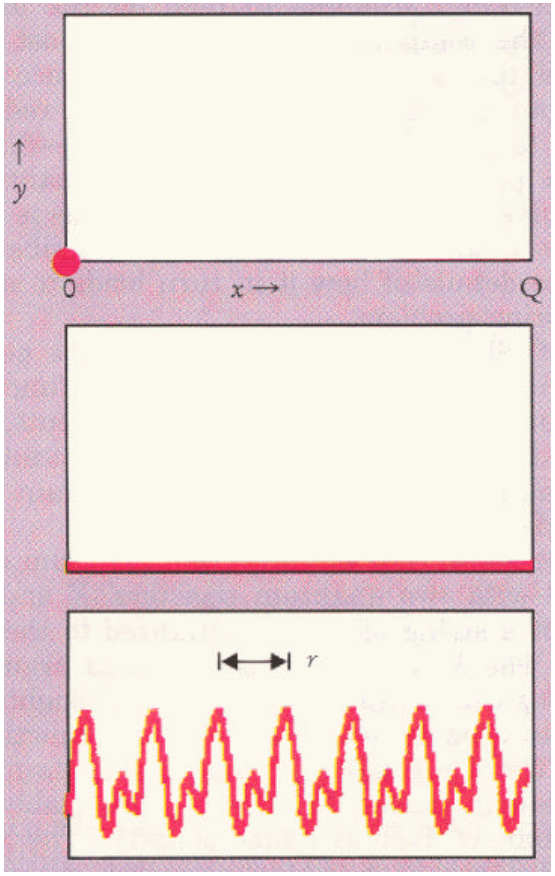
Shor's algorithm (1994)

1. Initialize state $|0,0>$

2. Create superposition $\sum_{0 \le x \le Q} |x,0>$

3. Calculate modular exponentiation

$$\sum_{0 \le x \le Q} |x, y^x \bmod \mathrm{N}>$$



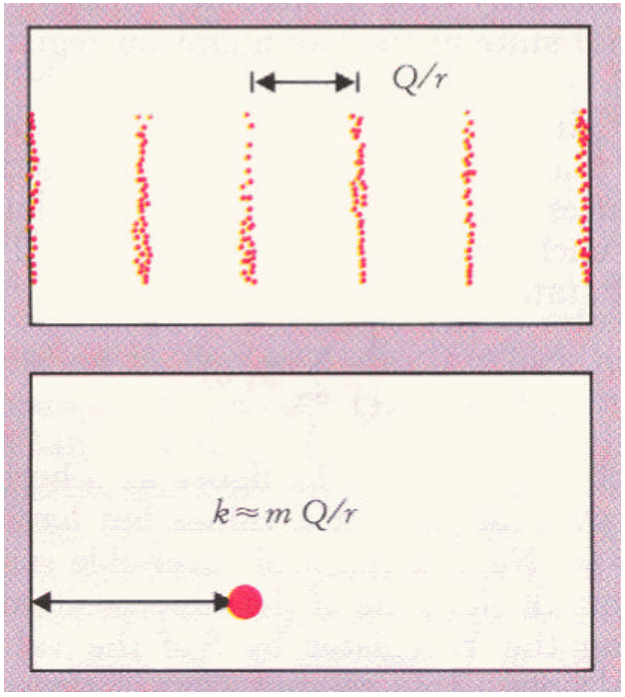
(to be continued)

Shor's algorithm

4. Measure the 2nd label

$$\sum_{0 \le k \le Q/r} |x_0 + kr, y^{x_0} \bmod \mathrm{N} >$$

(partially collapse the state)



5. Perform QFT and measure the 1st label

$$\sum_{0 \le z \le Q} e^{2\pi i x_0 z/Q} \left(\sum_{0 \le k \le Q/r} e^{2\pi i k r z/Q} \right) |z, y^{x_0} \bmod \mathrm{N} >$$

$$p(z) \propto \left| \sum_{0 \le k \le Q/r} e^{2\pi i k r z/Q} \right|^2 \text{ is large when } z \approx mQ/r!$$

The difficulty of finding the order r grows with n^3

Use r to get p and q

1. Pick a random y < N that is coprime with N

2. Find the order r of y mod N

3. Find the gcd of $y^{r/2} \pm 1$ and N

This method fails if (1): r is odd, or (2): r is even but $y^{r/2} = 1$ or -1 mod N. This happens with a chance < 1/2.

4. If fails, pick another y and try it again!

For details, see Ekert and Jozsa, RMP68, 733 (1996)

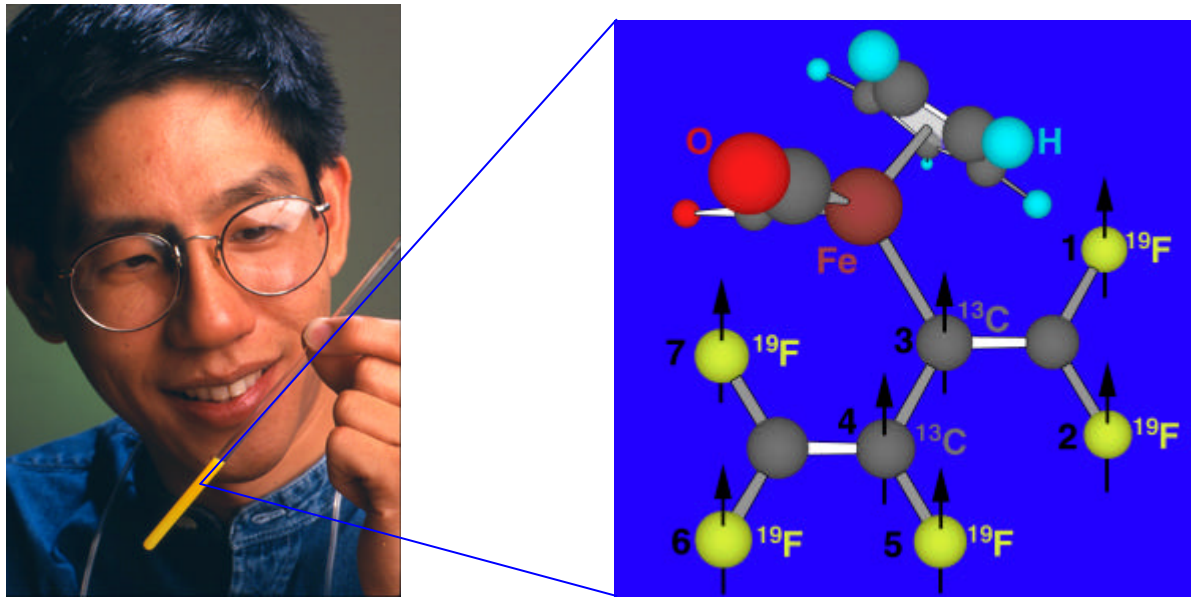
Example: N=15

pick y=7

$7^4=1 \bmod 15$, $\therefore r=4$

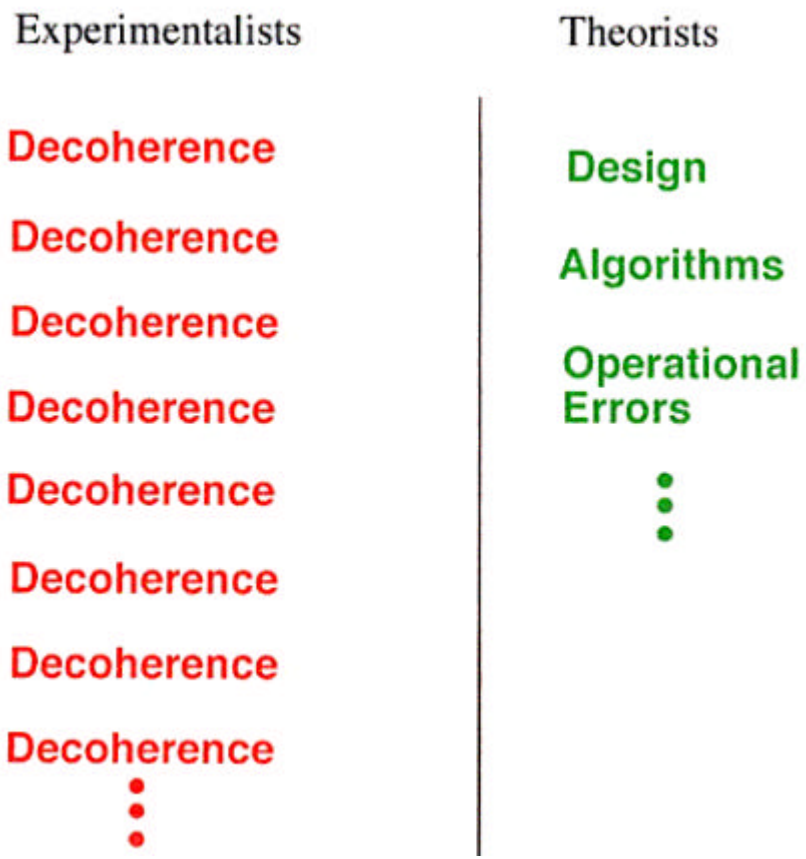
gcd(49+1,15)=5; gcd(49-1,15)=3, and 15=3x5!

IBM’s quantum computer (2001)



7-qubit QC solves 15=3x5 using Shor’s algorithm.

Difficulties of quantum computer



Need to shield the environment from peeking the calculation.

No cloning theorem (Wotters and Zurek, 1982)

You cannot clone an unknown qubit!

- **Assume an amplifier operator:**

$$\hat{A}|\psi\rangle = |\psi\rangle|\psi\rangle$$

- **Must be linear:**

$$\hat{A}(\alpha|0\rangle + \beta|1\rangle) = \alpha\hat{A}|0\rangle + \beta\hat{A}|1\rangle = \alpha|0\rangle|0\rangle + \beta|1\rangle|1\rangle$$

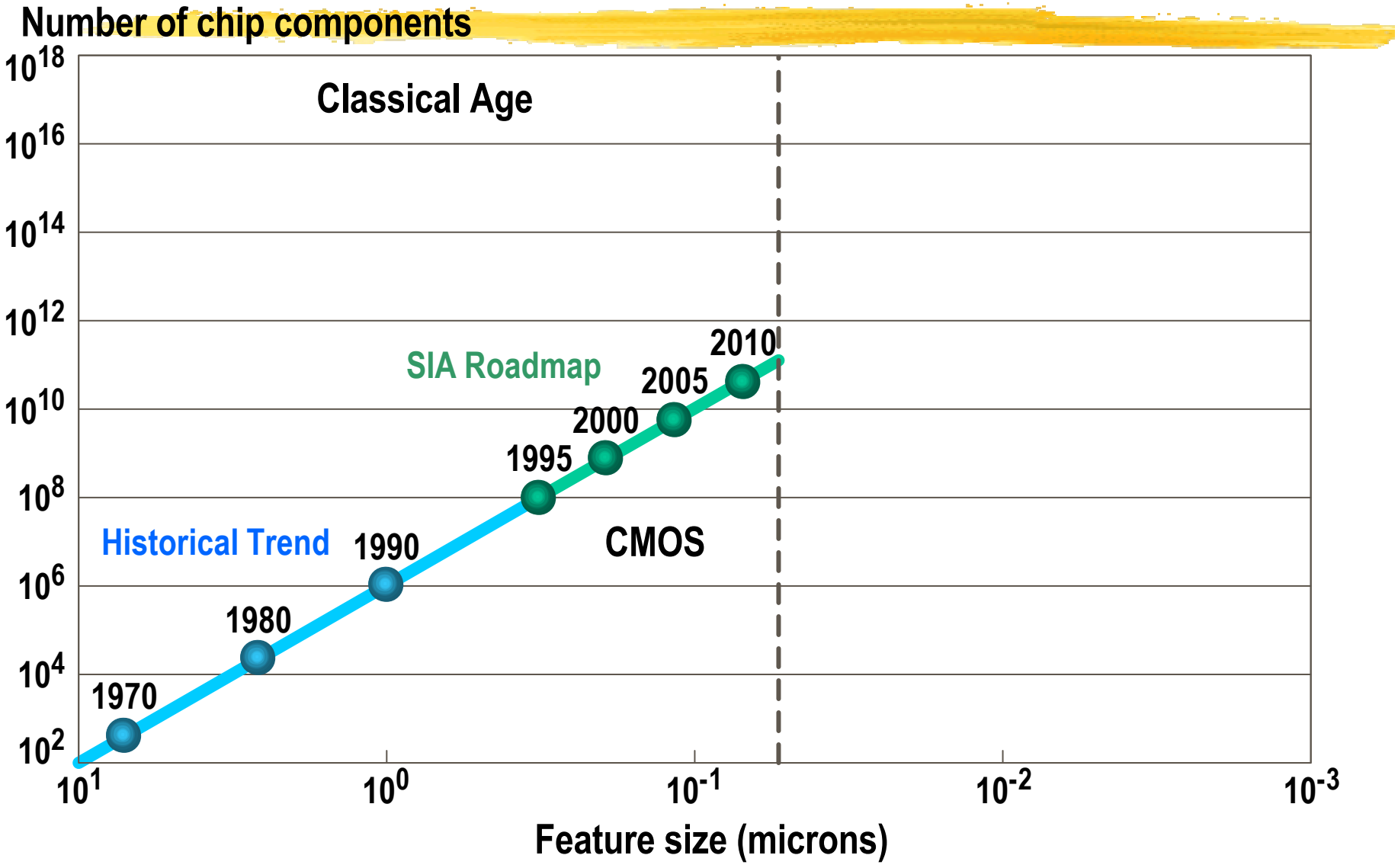
- **Apply to superposition:**

$$\hat{A}(\alpha|0\rangle + \beta|1\rangle) = (\alpha|0\rangle + \beta|1\rangle)(\alpha|0\rangle + \beta|1\rangle)$$
$$= \alpha^2|0\rangle|0\rangle + \beta^2|1\rangle|1\rangle + \alpha\beta|0\rangle|1\rangle + \alpha\beta|1\rangle|0\rangle$$

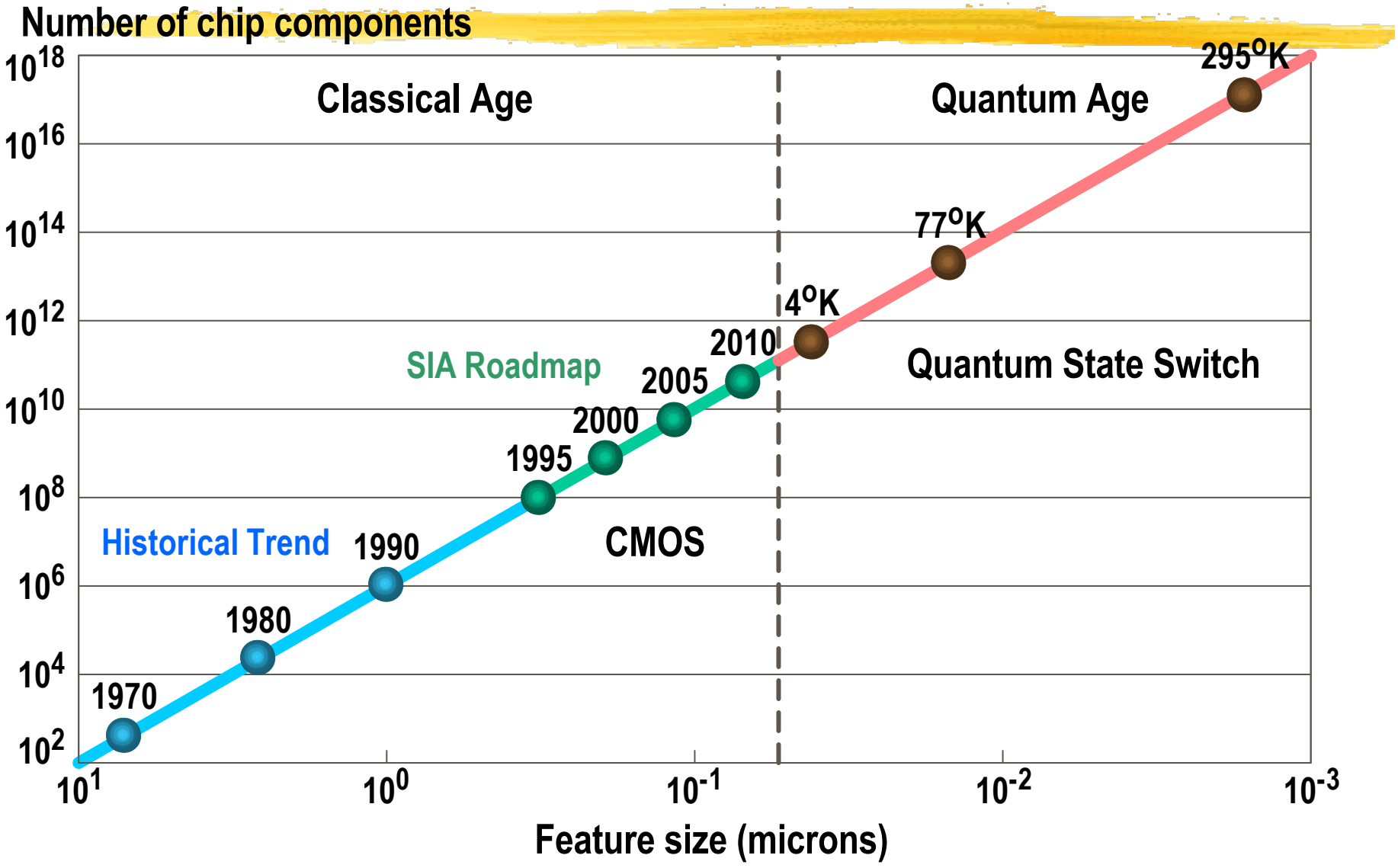
contradiction!

From N. Gershenfeld's talk

Scaling of electronic devices



Scaling of electronic devices



Perspective

- Future
  - Another optical computer or Josephson-junction computer?
  - The 10th question Mermin would like to ask his colleagues in the year 2100 if he awoke from a 100-year sleep (Phys. Today, Feb. 2001):

    Has anybody built a QC that can factor a 1000-bit integer? What else is it used for? Do most homes have one?

- Past
  - I think there is a world market for maybe 5 computers
    -- Thomas Watson, chairman of IBM, 1943
  - Computers in the future may weigh no more than 1.5 tons
    -- Popular Mechanics, 1949