Usage of Quantum State

電子通過1=>|0>
通過2=>|1>
} bit

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

≈ 同時通過1與2

≠analog (0.8, 0.2455..)

Due to superposition, get more information!

➡ **Quantum Information Science**

Quantum Cryptography

不管是那種密碼(如聖經密碼,…)

➔需要所謂的密碼鑰匙(key)

1 1 0 0 1 0

0 1 1 0 1 0

XOR 1 1 0 0 1 0

1 0 1 0 0 0

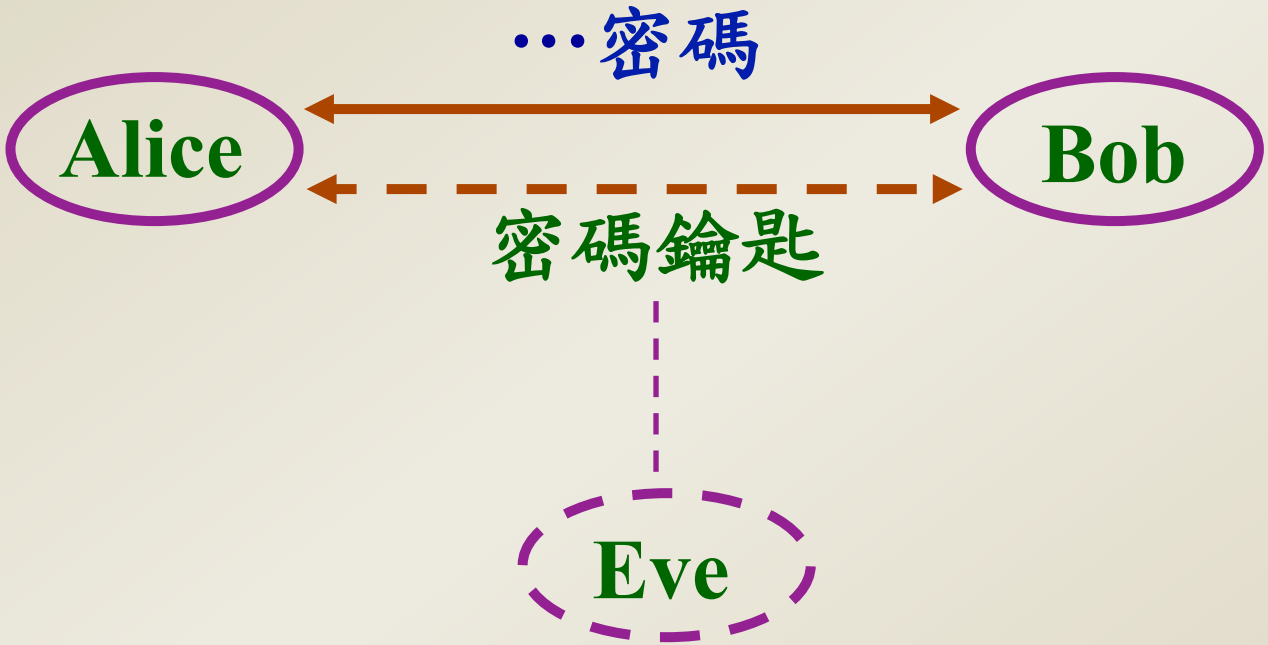
transmission

1 0 1 0 0 0

XOR 1 1 0 0 1 0

0 1 1 0 1 0

如何安全傳達密碼鑰匙呢?



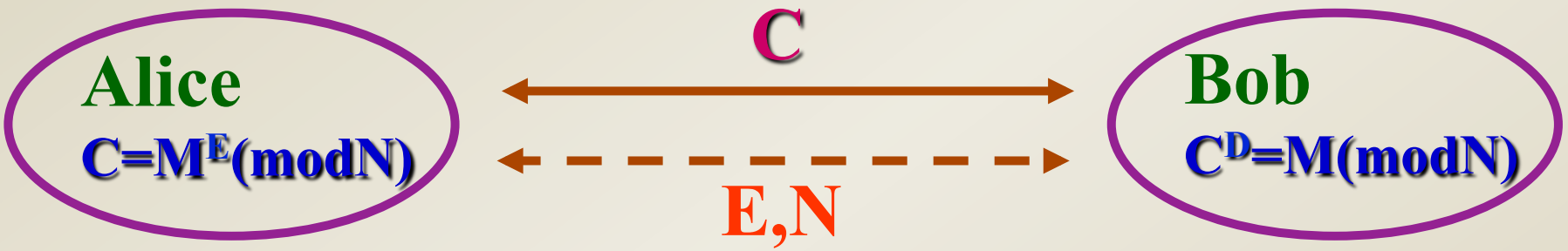
典型的古典方法:

由公告的密碼鑰匙找密碼必須會作非常大的數之因式分解才行

The RSA algorithm

Ron Rivest, Adi Shamir, and Leonard Adleman, 1978

MESSAGE: M



(1) Bob選兩個質數: P與Q, 得 N=PQ
並找E(奇數, 加密)與(P-1)(Q-1)(偶數)互質, 公布E與N讓Alice知道

(2) Bob找D使得ED-1可以被(P-1)(Q-1)整除
即 ED=1mod((P-1)(Q-1))

Example

Alice 先告訴 Bob有資料要傳給他
Bob 說好, 先讓我算一下
Bob 選了P=47與Q=71, 計算N=3337
(P-1)(Q-1)=3220
試E=79

D=(Z*3220+1)/79, Z=1,2,3,...
發現Z=25時, D為整數, 且D=1019
所以Bob只公布E=79與N=3337 讓 Alice知道

一旦知道E與N, Alice可傳送其資料如下:

例如要傳送 Dr Dobbs
可先轉為 6882326879666683 (decimal ASCII)
再分割為 688 232 687 966 668 3

$$1570 = 688^{79} \pmod{3337} \qquad 2756 = 232^{79} \pmod{3337}$$

$$2091 = 687^{79} \pmod{3337} \qquad 2276 = 966^{79} \pmod{3337}$$

$$2423 = 668^{79} \pmod{3337} \qquad 158 = 3^{79} \pmod{3337}$$

最後Alice將1570 2756 2091 2276 2423 158
傳給Bob

Bob收到資料後, 可還原資料如下:

D=1019

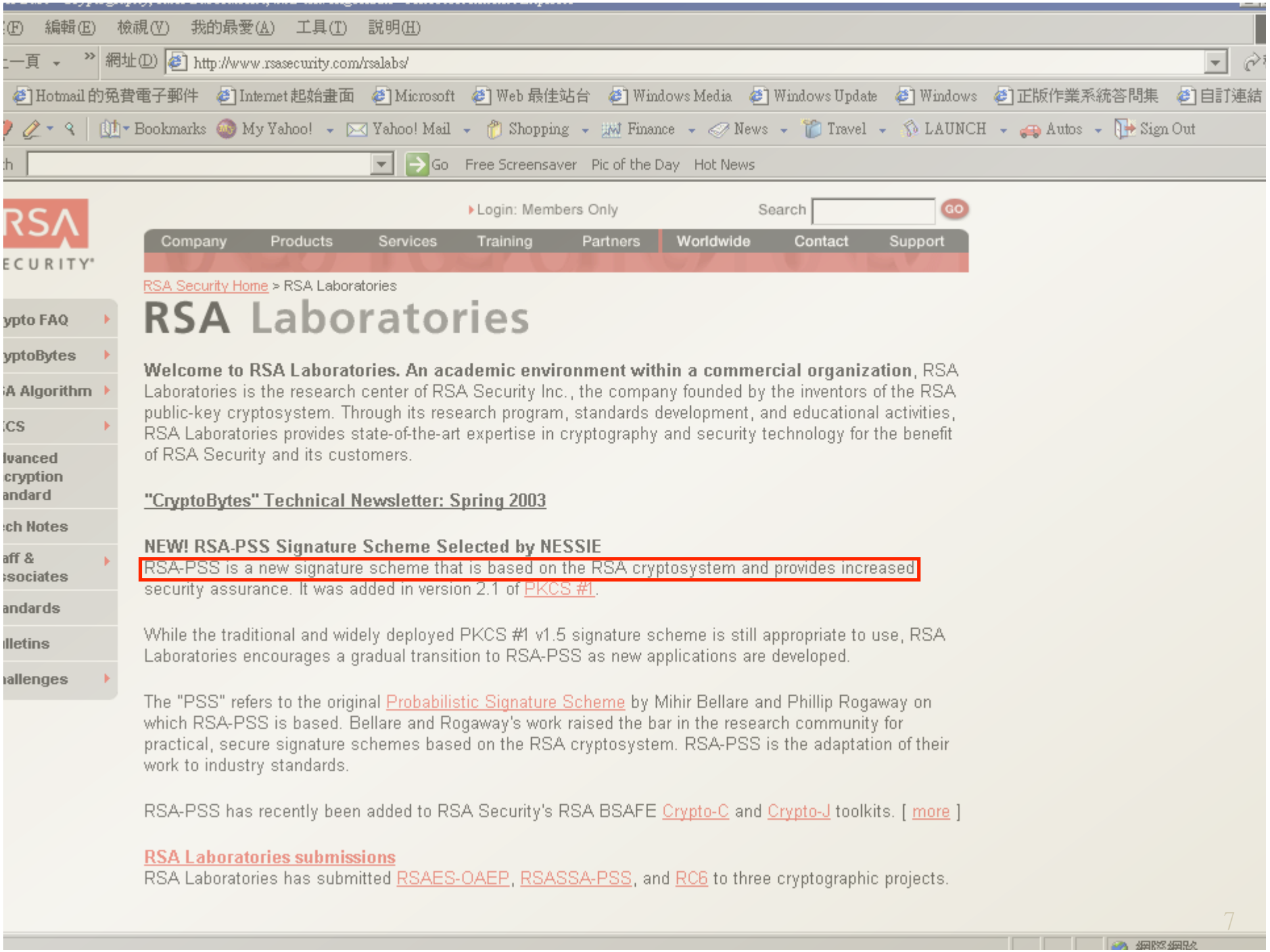
$$1570^{1019} = 688 (\mathrm{mod}\, 3337) \quad 2756^{1019} = 232 (\mathrm{mod}\, 3337)$$

$$2091^{1019} = 687 (\mathrm{mod}\, 3337) \quad 2276^{1019} = 966 (\mathrm{mod}\, 3337)$$

$$2423^{1019} = 668 (\mathrm{mod}\, 3337) \quad 158^{1019} = 3 (\mathrm{mod}\, 3337)$$

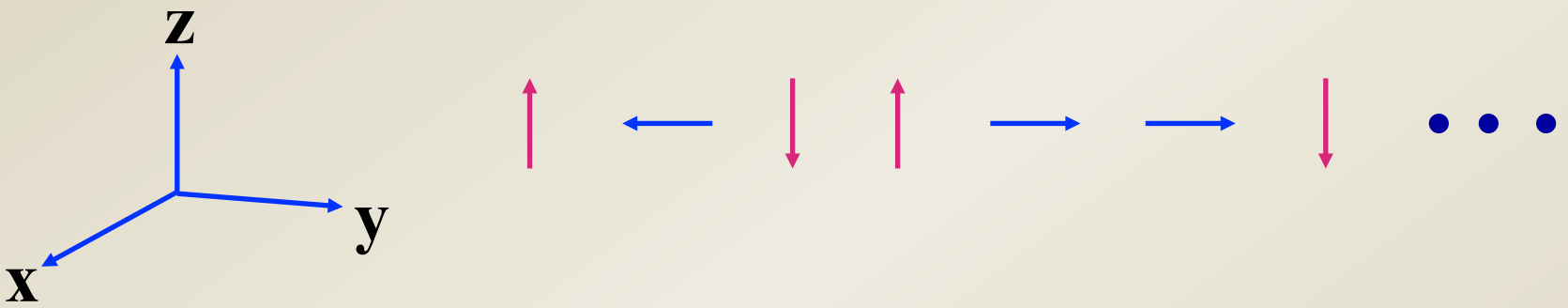
因而還原688 232 687 966 668 3**即Dr Dobbs**

由於D一直都在Bob手中, 無外洩可能, 所以除非竊聽者會計算D, 否則這是非常安全的方式

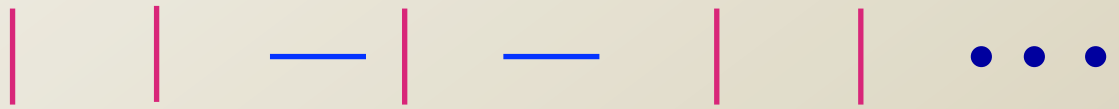

(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
網址(D) http://www.rsasecurity.com/rsalabs/
Hotmail 的免費電子郵件 Internet 起始畫面 Microsoft Web 最佳站台 Windows Media Windows Update Windows 正版作業系統答問集 自訂連結
Bookmarks My Yahoo! Yahoo! Mail Shopping Finance News Travel LAUNCH Autos Sign Out
Go Free Screensaver Pic of the Day Hot News
Login: Members Only
Search
GO
Company Products Services Training Partners Worldwide Contact Support
RSA Security Home > RSA Laboratories
RSA Laboratories
ypto FAQ
yptoBytes
A Algorithm
CS
lvanced cryption andard
ch Notes
aff & ssociates
andards
lletins
allenges
Welcome to RSA Laboratories. An academic environment within a commercial organization, RSA Laboratories is the research center of RSA Security Inc., the company founded by the inventors of the RSA public-key cryptosystem. Through its research program, standards development, and educational activities, RSA Laboratories provides state-of-the-art expertise in cryptography and security technology for the benefit of RSA Security and its customers.
"CryptoBytes" Technical Newsletter: Spring 2003
NEW! RSA-PSS Signature Scheme Selected by NESSIE
RSA-PSS is a new signature scheme that is based on the RSA cryptosystem and provides increased security assurance. It was added in version 2.1 of PKCS #1.
While the traditional and widely deployed PKCS #1 v1.5 signature scheme is still appropriate to use, RSA Laboratories encourages a gradual transition to RSA-PSS as new applications are developed.
The "PSS" refers to the original Probabilistic Signature Scheme by Mihir Bellare and Phillip Rogaway on which RSA-PSS is based. Bellare and Rogaway's work raised the bar in the research community for practical, secure signature schemes based on the RSA cryptosystem. RSA-PSS is the adaptation of their work to industry standards.
RSA-PSS has recently been added to RSA Security's RSA BSAFE Crypto-C and Crypto-J toolkits. [more]
RSA Laboratories submissions
RSA Laboratories has submitted RSAES-OAEP, RSASSA-PSS, and RC6 to three cryptographic projects.

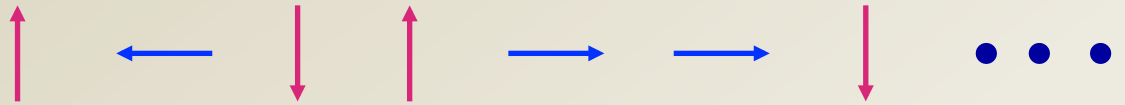
量子密碼鑰匙傳達六部曲(BB84)

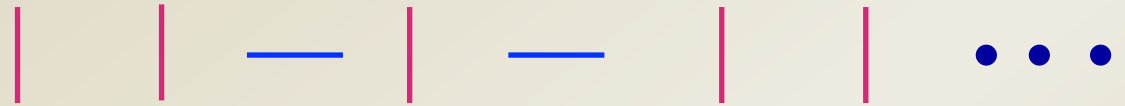
步驟一:Alice用SG磁鐵準備具以下自旋的電子



步驟二:Bob任意選SG磁鐵軸測電子的自旋



Alice 

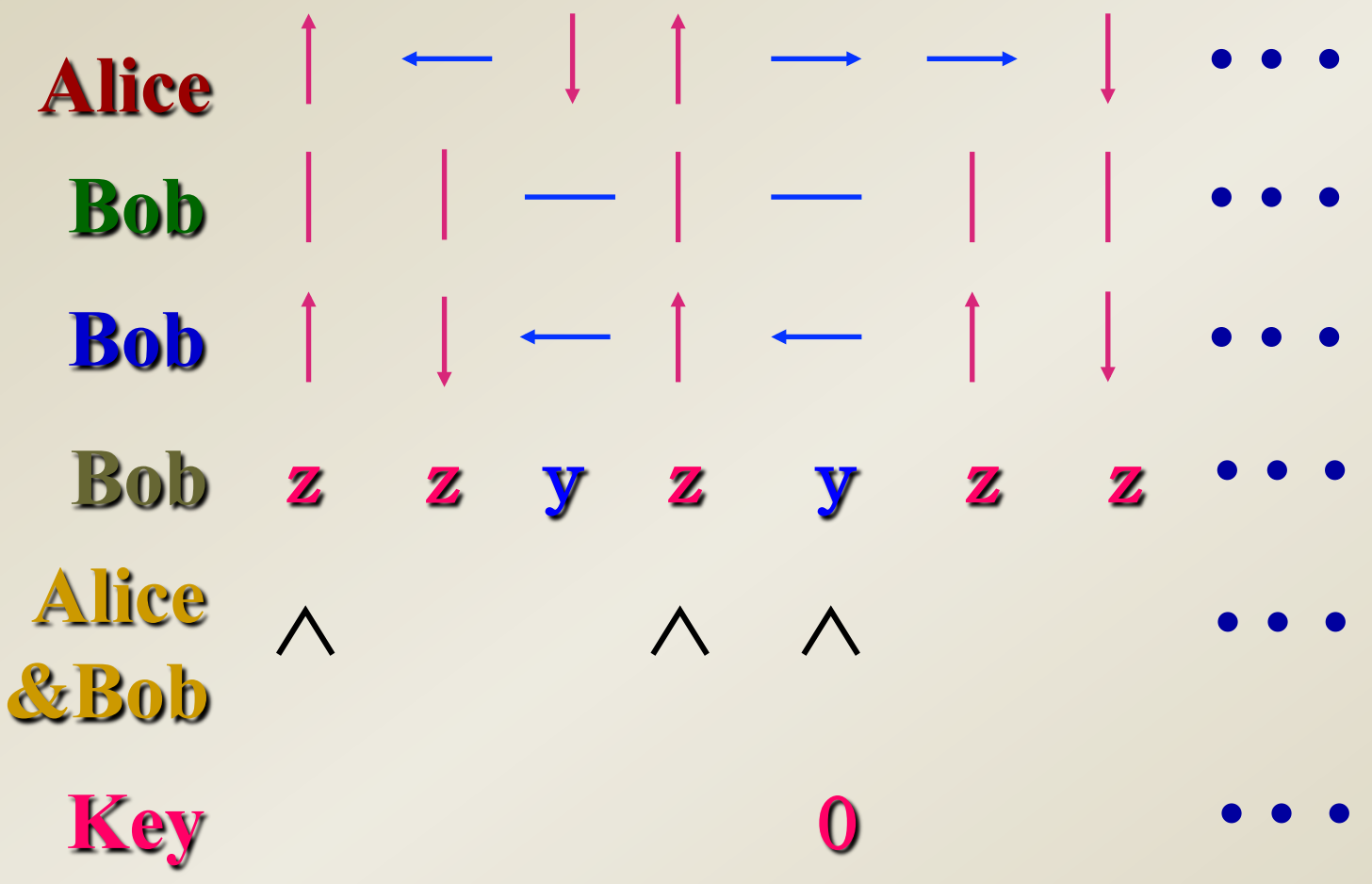
Bob 

步驟三:Bob記錄他所測得電子自旋的方向

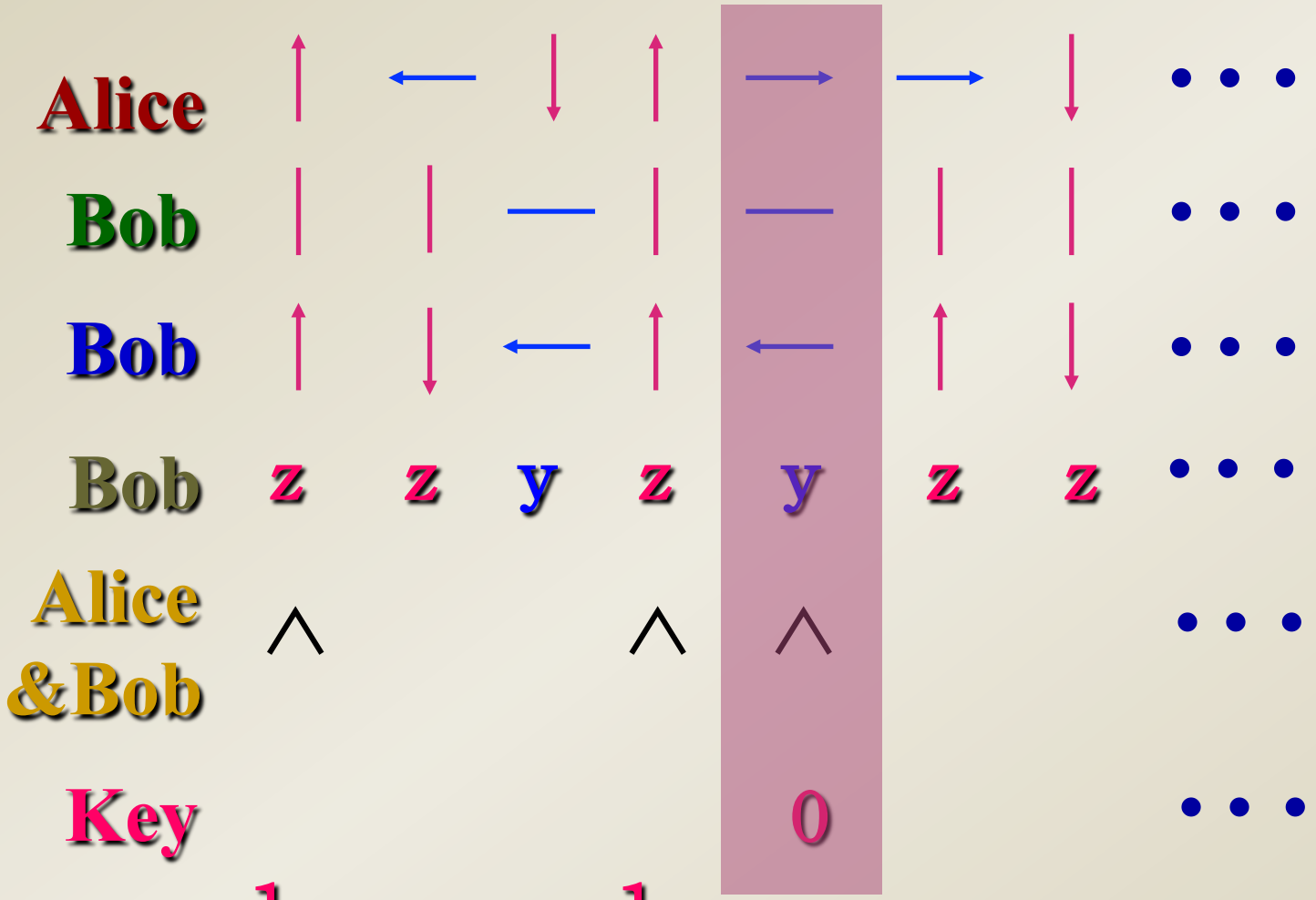
Bob 

步驟四:Bob公布他所用的軸

Bob z z y z y z z • • •



步驟五:Alice告訴Bob那些軸是對的, 所對應的電子自旋方向即為可作為共同的密碼鑰匙

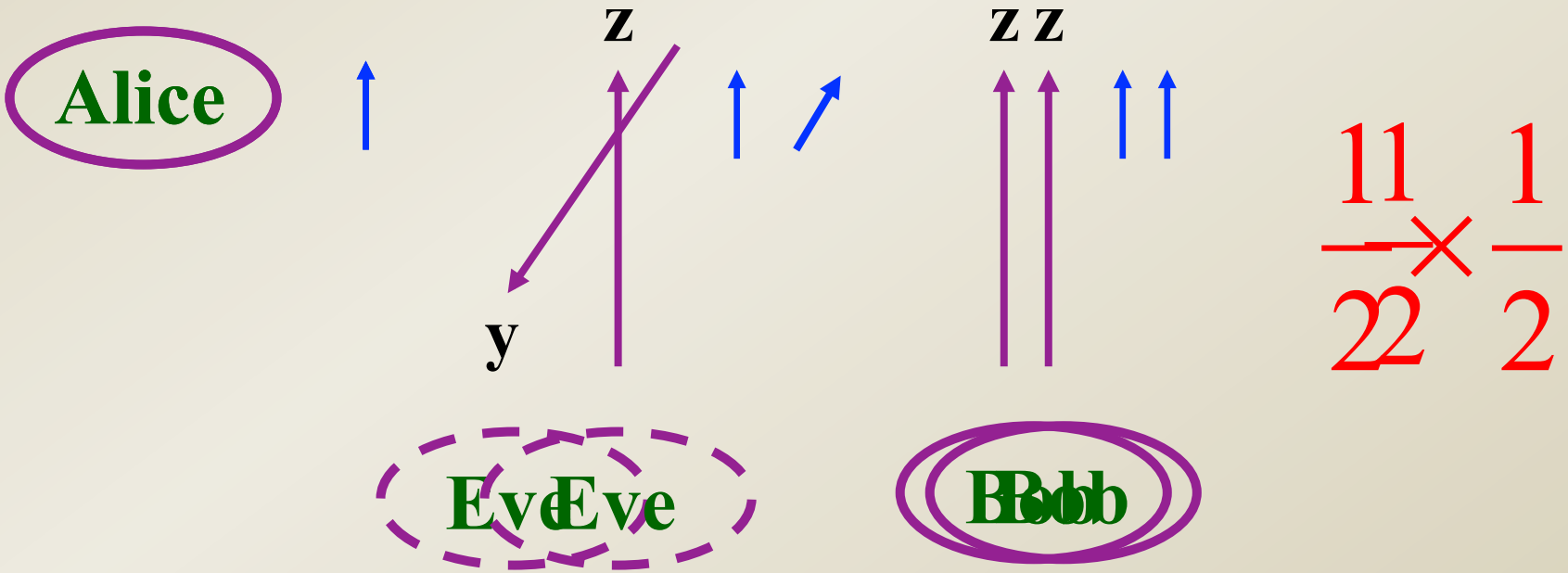


步驟六:Alice與Bob隨意取一部分key公步檢查有無錯誤, 被竊聽(eavesdropped)

被竊聽不被發現的機會

竊聽者(Eve)要先猜選SG軸

將通過SG軸的電子繼續送給Bob



一個qubit不被發現被竊聽的機會 = 1/2+1/4 = 3/4

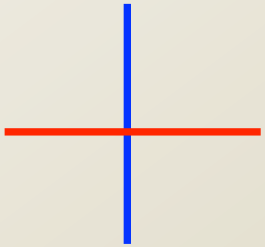
若拿出公布檢查的有m個qubit, 不被發現被竊聽的機會 = $(3/4)^m$ ➔0

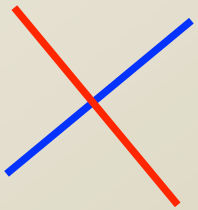
實際的實驗以光子進行

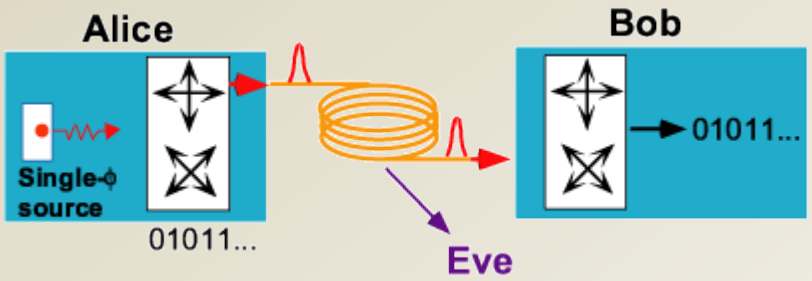
光子的偏振方向 v.s. 電子的自旋

電子

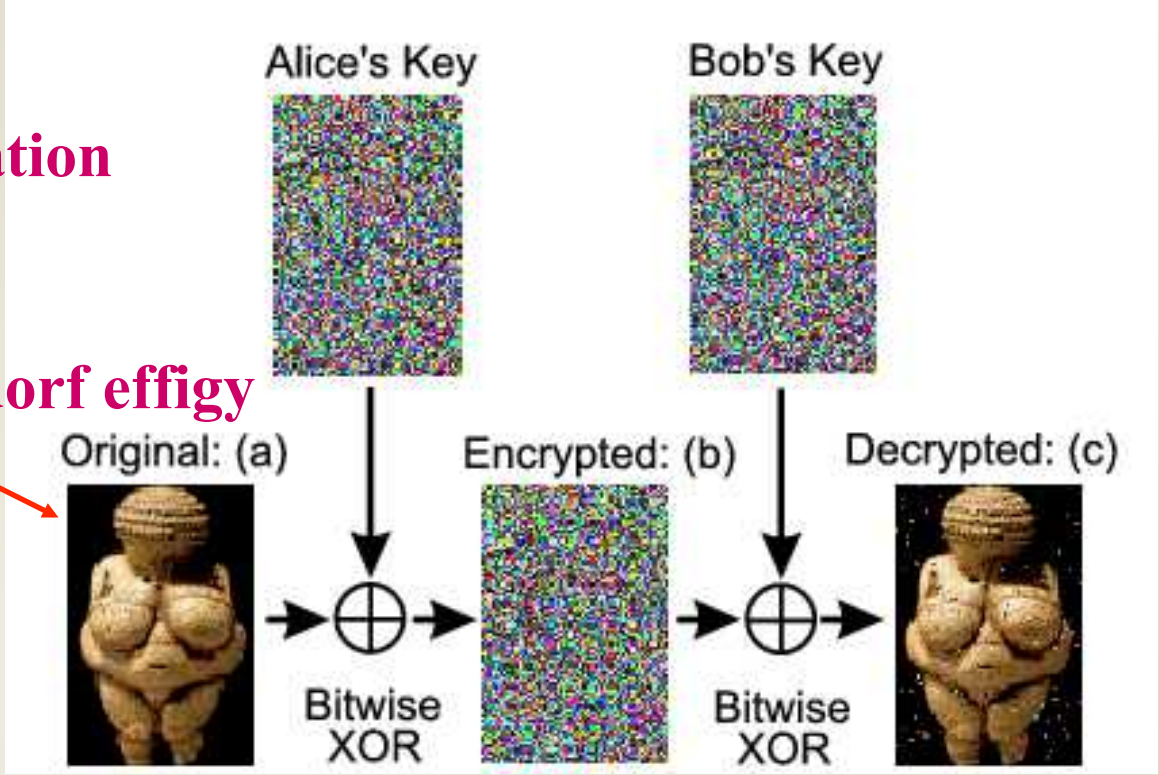
光子







60x90 pixels
8 bit color information
per pixel + header
= 49984bits
Venus von Willendorf effigy



Phys. Rev. Lett. 84, 4729-4732 (2000)

(Ekert scheme, using entangled photons)

Usage of many qubits

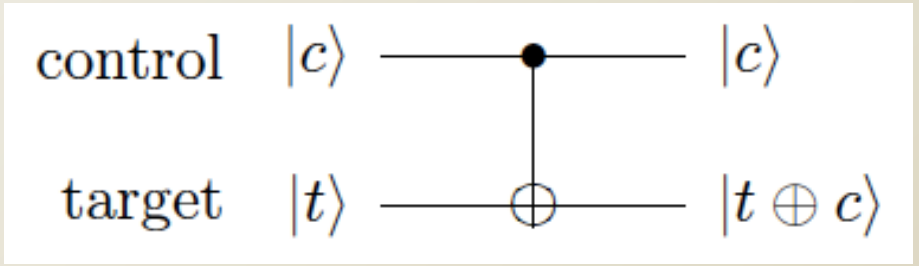
Quantum Logic Gates :

Unitary transformation of qubit (rotation..)

$$\text{example} \left| \right. = \frac{|1\rangle + |0\rangle}{\sqrt{2}}$$

$$\begin{pmatrix} a & b \\ b^* & a \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

Controlled operation



$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & x_{00} & x_{10} \\ 0 & 0 & x_{01} & x_{11} \end{bmatrix}$$

$$x_{00}|10\rangle\langle 10| + x_{01}|01\rangle\langle 11|$$

$$+x_{10}|11\rangle\langle 10| + x_{11}|11\rangle\langle 11|$$

Universal Quantum Gates

Classical : AND, OR, NOT can construct any classical function

Quantum: any U ($UU^{\dagger}=1$) can be decomposed into ..

$$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \text{(Hadamard)}$$

$$\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \text{(phase)}$$

$$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix} (\pi/8)$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \text{(control-not)}$$

$|00\rangle \rightarrow |00\rangle \quad |01\rangle \rightarrow |01\rangle$

$|10\rangle \rightarrow |11\rangle \quad |11\rangle \rightarrow |10\rangle$

牽一髮動全身的量子平行處理

古典平行化: 產生 $0,1,2,3,\ldots,N=2^m-1$

m 位元

0000…..000

0000…..001

0000…..010

.

.

1111…..111

⇨ 需N個步驟

⇨ 共需m×N個位元

量子平行化：只需m個步驟與m個位元

$$\left| \right\rangle = \frac{|1\rangle + |0\rangle}{\sqrt{2}} \quad \text{(or using B to rotate)}$$

m個步驟

$$\frac{|1\rangle + |0\rangle}{\sqrt{2}} \times \frac{|1\rangle + |0\rangle}{\sqrt{2}} \times \frac{|1\rangle + |0\rangle}{\sqrt{2}} \times \cdots \frac{|1\rangle + |0\rangle}{\sqrt{2}} \times \frac{|1\rangle + |0\rangle}{\sqrt{2}}$$

$$= \frac{1}{2^{m/2}} \left[|000\ldots000\rangle + |000\ldots001\rangle + |000\ldots010\rangle + \cdots + |111\ldots111\rangle \right]$$

$0,1,2,3,\ldots,N=2^m-1$

量子平行處理：可集體處理0,1,2,3,…,N=2^m-1

$$Q=\frac{1}{2^{m/2}}\left[|000\ldots000\rangle+|000\ldots001\rangle+|000\ldots010\rangle+\cdots+|111\ldots111\rangle\right]$$

$$=\frac{1}{2^{m/2}}\left[|0\rangle+|1\rangle+|2\rangle+\cdots+|N\rangle\right]$$

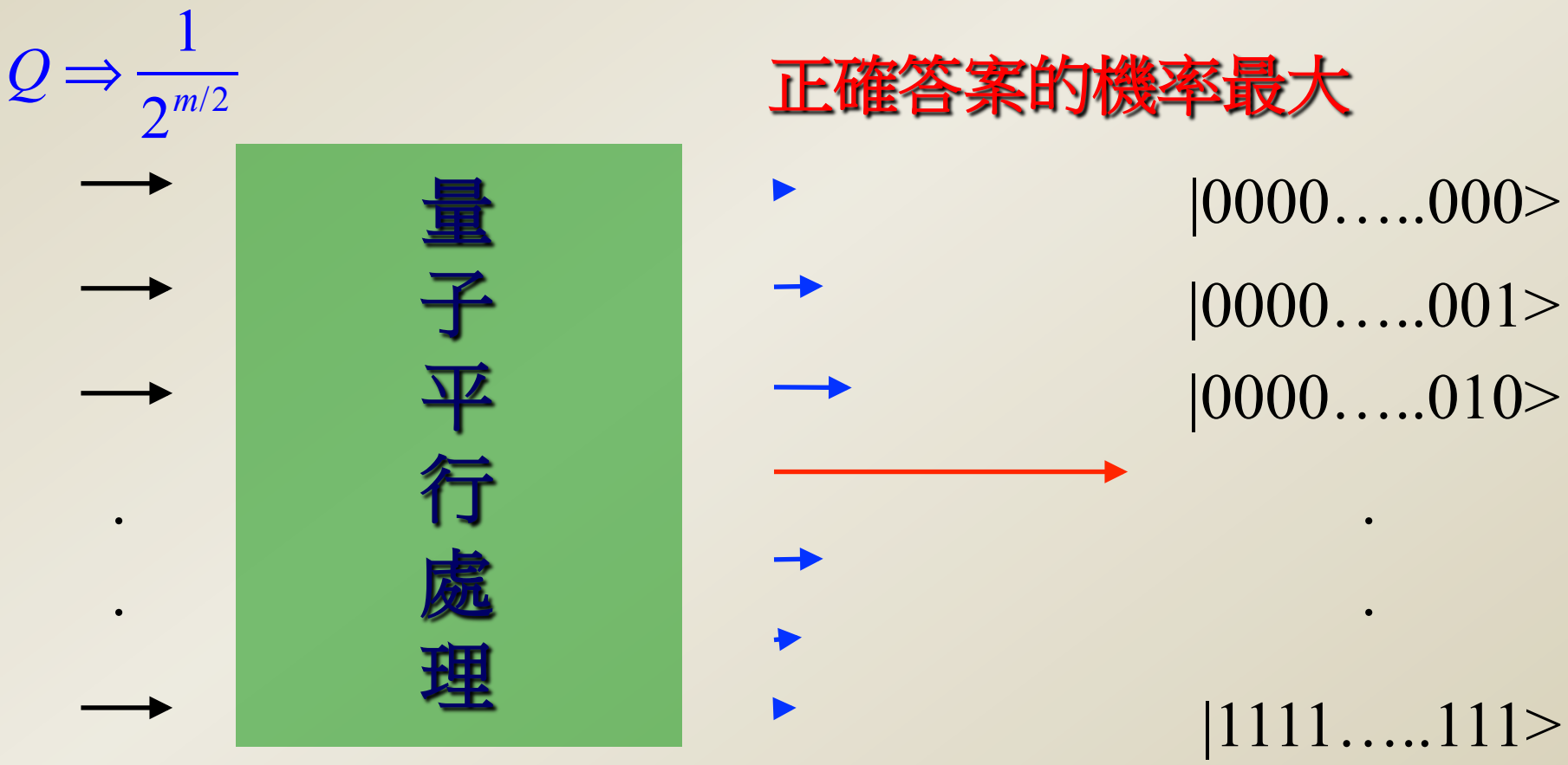
第一位元 $|0\rangle \Rightarrow$ $\Big|$ $=\dfrac{|1\rangle+|0\rangle}{\sqrt{2}}$ $\Rightarrow$ 牽一髮動全身!

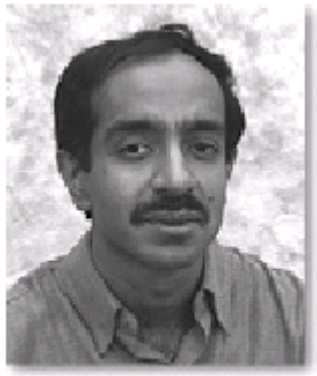
$$Q\Rightarrow \frac{1}{2^{m/2}}\left[\frac{1}{\sqrt{2}}|0\rangle+\frac{1}{\sqrt{2}}|1\rangle+\frac{1}{\sqrt{2}}|2\rangle+\cdots+\left(1+\frac{1}{\sqrt{2}}\right)|N\rangle\right]$$

量子演算法較有效率!

量子演算法 (quantum computation)

=量子平行處理+機率





Lov K. Grover

例：量子搜索術 (Grover algorithm)

如在x=0,1,2,3,…,N(如電話簿)中找出所要的資料
清華大學總機電話號碼 …..

Oracle:

找尋的條件=> 可以檢驗找到的是否正確之

function f(x) 或device

=>即給定x在不做完整搜尋下可檢驗x是否為解

設所要的資料可以f(x) = 1標示, 其他的資料則滿足 f(x) = 0

$$|Q\rangle = \frac{1}{2^{m/2}}\left[|0\rangle + |1\rangle + |2\rangle + \cdots + |N\rangle\right]$$

$\Rightarrow$ (controlled operation, oracle operator $\hat{O}$)

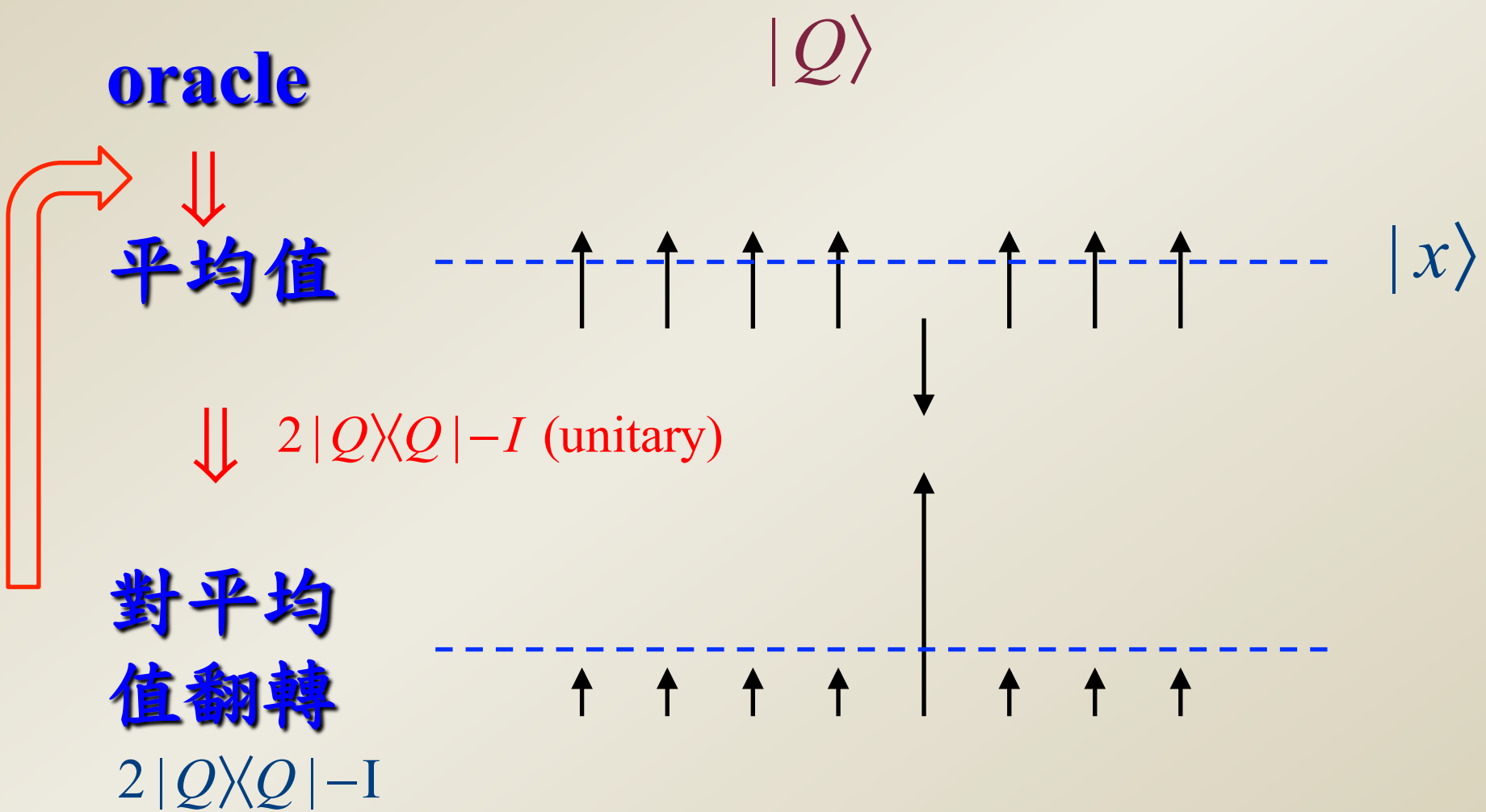
$$|x\rangle = \frac{1}{2^{m/2}}\left[(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle + (-1)^{f(2)}|2\rangle + \cdots + (-1)^{f(N)}|N\rangle\right]$$

古典一個一個搜查：$O(N)$

量子搜查：可集體處理0,1,2,3,…,N

$$\Rightarrow O(\sqrt{N}) \quad \sqrt{10000} = 100$$

量子搜查策略


$|Q\rangle$
oracle
平均值
$|x\rangle$
$2|Q\rangle\langle Q|-I$ (unitary)
對平均值翻轉
$2|Q\rangle\langle Q|-\mathrm{I}$

Example:

$$|Q\rangle = \frac{1}{2\sqrt{2}}|000\rangle + \frac{1}{2\sqrt{2}}|001\rangle + ... + \frac{1}{2\sqrt{2}}|111\rangle$$

$$|x\rangle = \frac{1}{2\sqrt{2}}|000\rangle + \frac{1}{2\sqrt{2}}|001\rangle + \frac{1}{2\sqrt{2}}|010\rangle - \frac{1}{2\sqrt{2}}|011\rangle + ... + \frac{1}{2\sqrt{2}}|111\rangle$$

$$= |\mathrm{Q}\rangle - \frac{1}{\sqrt{2}}|011\rangle$$

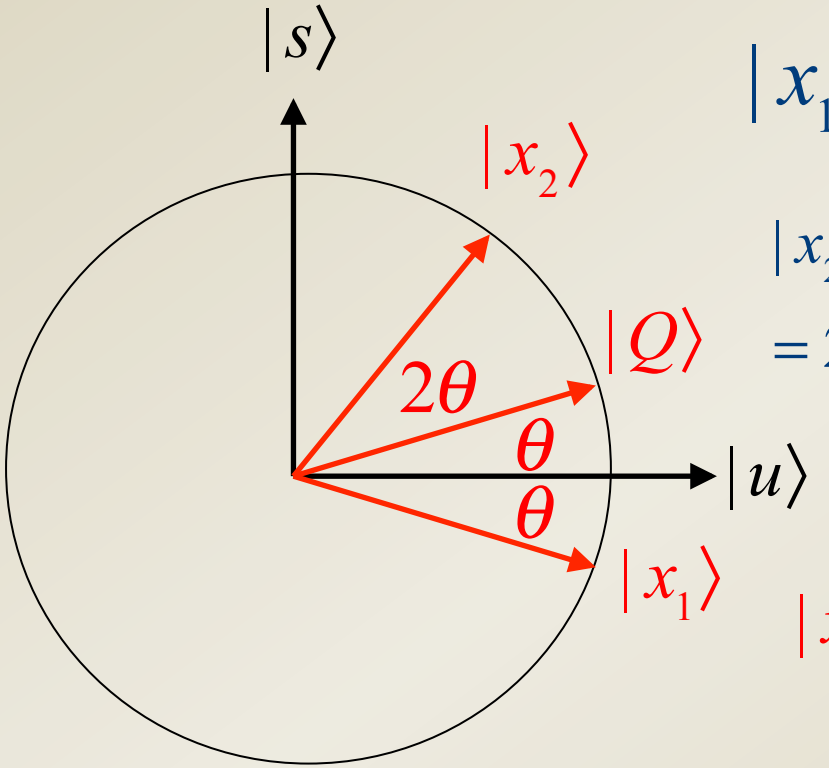
$$(2|Q\rangle\langle Q| - I)|x\rangle = \left(2|Q\rangle\langle Q| - I\right)\left[|Q\rangle - \frac{1}{\sqrt{2}}|011\rangle\right]$$

$$= |Q\rangle - \frac{2}{\sqrt{2}}|Q\rangle\langle Q|011\rangle + \frac{1}{\sqrt{2}}|011\rangle = |Q\rangle - \frac{1}{2}|Q\rangle + \frac{1}{\sqrt{2}}|011\rangle$$

$$= \frac{1}{4\sqrt{2}}|000\rangle + \frac{1}{4\sqrt{2}}|001\rangle + \frac{1}{4\sqrt{2}}|010\rangle + \frac{5}{4\sqrt{2}}|011\rangle + ... + \frac{1}{4\sqrt{2}}|111\rangle$$

Geometry picture & number of steps

$$|Q\rangle = \frac{1}{\sqrt{N}}\left[|0\rangle + |1\rangle + |2\rangle + \cdots + |N\rangle\right] \qquad \frac{1}{\sqrt{N}} = \sin\theta \approx \theta$$



$$|x_1\rangle = \hat{O}|Q\rangle \Rightarrow \theta \rightarrow -\theta$$

$$|x_2\rangle = \left(2|Q\rangle\langle Q| - I\right)|x_1\rangle = 2|Q\rangle\langle Q|x_1\rangle - |x_1\rangle$$
$$= 2\cos 2\theta\,|Q\rangle - |x_1\rangle$$

$$\langle Q|x_2\rangle = 2\cos 2\theta - \cos 2\theta = \cos 2\theta$$

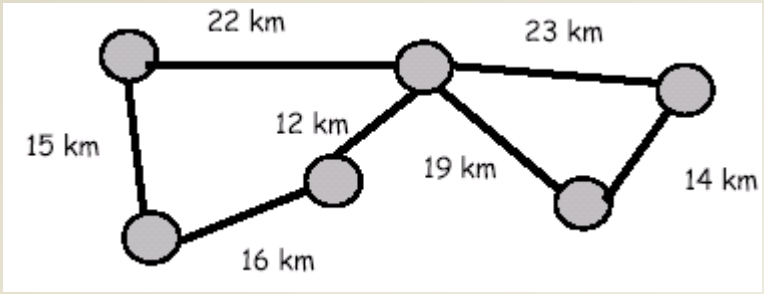
$$|x_n\rangle = \cos(2n+1)\theta\,|u\rangle + \sin(2n+1)\theta\,|s\rangle$$

$$(2n+1)\theta \approx \frac{\pi}{2} \Rightarrow n \approx \frac{\pi}{4\theta} \approx \frac{\pi}{4}\sqrt{N}$$

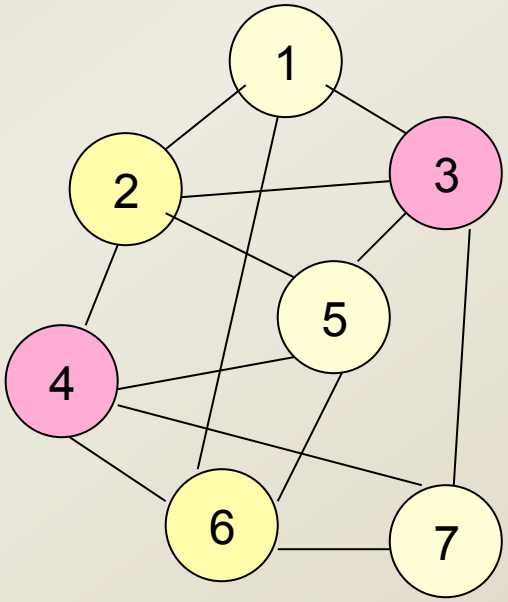
還有許多可能的應用...

只要能有oracle即可以量子搜尋處理

推銷員的旅程問題（Traveling Salesperson Problem)



圖色問題



量子計算：大質數問題

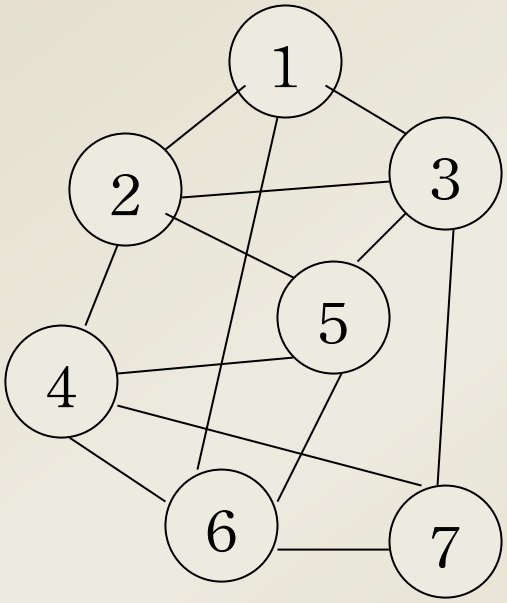
給定一著色=> x =>
存在f(x) = 1 or 0

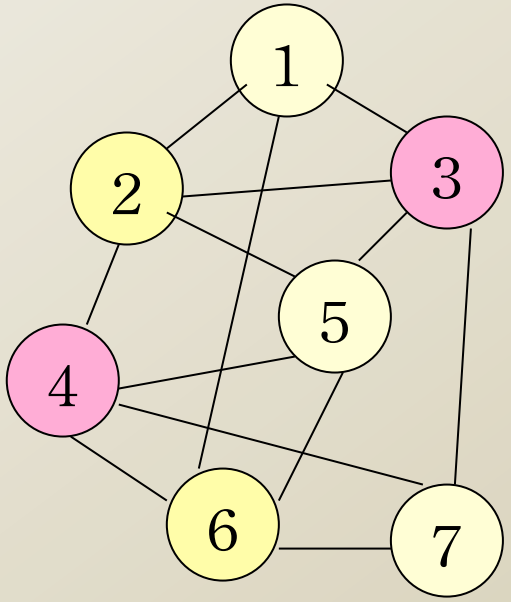
圖色問題

將每一節點塗上一個顏色

任一邊長的兩端節點之顏色必不相同

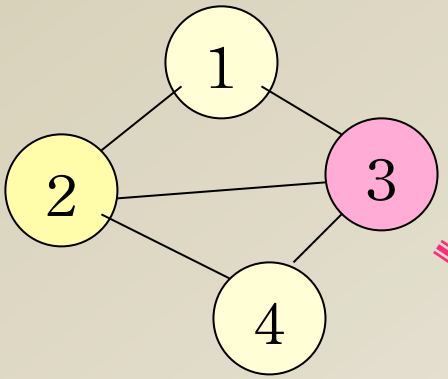
使用的總顏色數最小





此圖可以三色圖滿

Quantum Oracle



We need to give all possible colors here

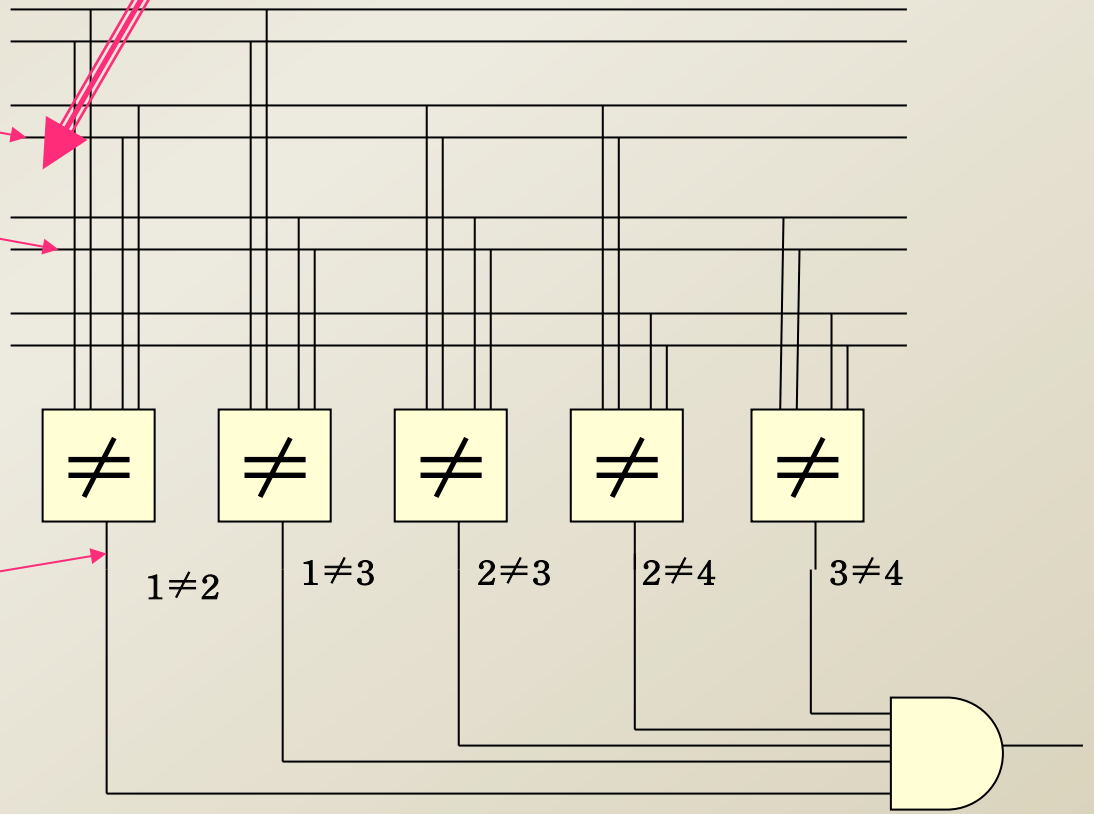
Two wires for color of node 1

Two wires for color of node 2

Two wires for color of node 3

Two wires for color of node 4

Gives "1" when nodes 1 and 2 have different colors



Value 1 for good coloring