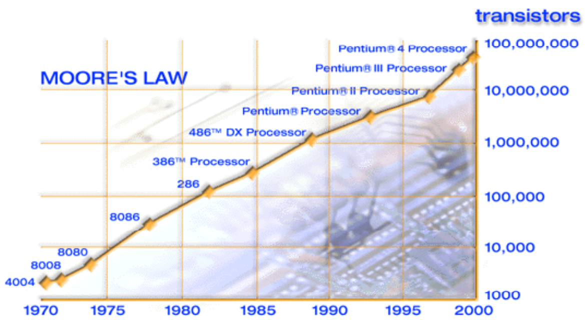
Quantum Technology and Spin Quantum Computation
量子科技與自旋量子計算

Goan, Hsi-Sheng
管 希 聖
Department of Physics,
Center for Theoretical Sciences, and
Center for Quantum Science and Engineering,
National Taiwan University

Development of modern Computing and Networking

- Computer speed doubles every 2 years (Moore's Law).
- Data storage density doubles every 12 months.
- Network speed doubles every 9 months.

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 新迅馳旗艦超可攜筆記12吋鏡面寬螢幕視訊筆記電腦

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

2010年的筆記型電腦

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%

台積電直攻20奈米製程 2年後投產

2010/4/14 上午 10:05:00

CNA 即時新聞 NEWS

- 晶圓代工龍頭台積電將跳過22奈米製程，直接發展20奈米製程技術；預計2012年下半年開始導入生產。晶圓代工龍頭廠台積電今天宣佈，將跳過22奈米製程，直接發展20奈米製程技術；預計20奈米製程在2012年下半年開始導入生產。

  台積電於美西時間13日在加州聖荷西舉行技術研討會，有多達1500位客戶及合作廠商代表參加；台積電研究發展資深副總經理蔣尚義於會中表示，在先進製程技術開發上，台積電已面臨一個關鍵時刻。

  蔣尚義指出，台積電需跳脫單純考慮技術層面的思維模式，主動積極考量投資報酬率；透過與客戶密切合作及在資源整合與最佳化的創新，解決技術及經濟層面的挑戰。

  由於台積電20奈米製程將比22奈米製程擁有更佳的閘密度及晶片效能／成本比，蔣尚義說，基於為客戶創造價值的決定，台積電將跳過22奈米製程，直接發展20奈米製程。

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。

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.

Some basic quantum principles

- Quantization (quantum size effect): discrete allowed energies.
- Uncertainty principle: non-commuting quantum measurement observables
- Quantum superposition: indistinguishable ways; quantum parallelism.
- Quantum Interference: complex amplitudes
- Tunnelling: in classical forbidden spatial region.
- Entanglement: non-separable state, non-local correlation.
- Decoherence: environmental degradation effects on delicate quantum system.

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)

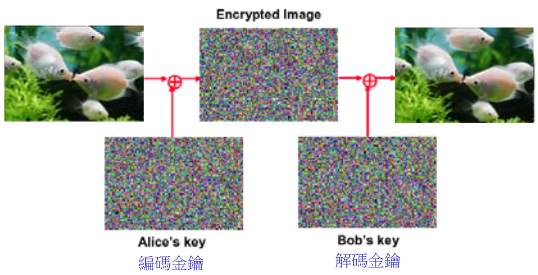
- RSA密碼系統的基礎建構於去因式分解一個很大位數的半質數的困難度: 網際網路的標準編碼保密方法

  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):

25195908475657893494027183240048398571429282126204
03202777713783604366202070759555626401852588078440
69182906412495150821892985591491761845028084891200
72844992687392807287776735971418347270261896375014
97182469116507761337985909570009733045974880842840
17974291006424586918171951187461215151726546322822
16869987549182422433637259085141865462043576798423
38718477444792073993423658482382428119816381501067
48104516603773060562016196762561338441436038339044
14952634432190114657544454178424020924616515723350
77870774981712577246796292638635637328991215483143
81678998850404453640235273819513786365643912120103
97122822120720357

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

編碼保密傳輸

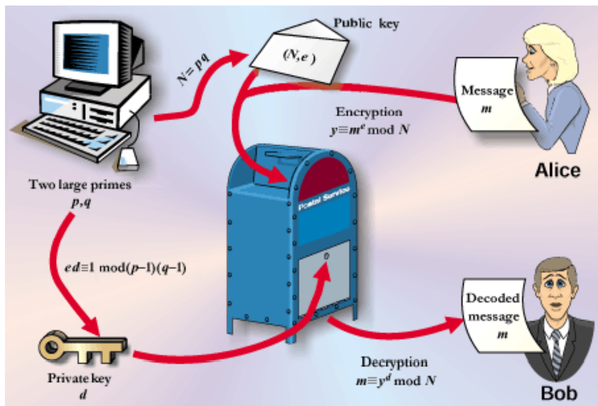


網路銀行 (internet banking): $N = p\ q$

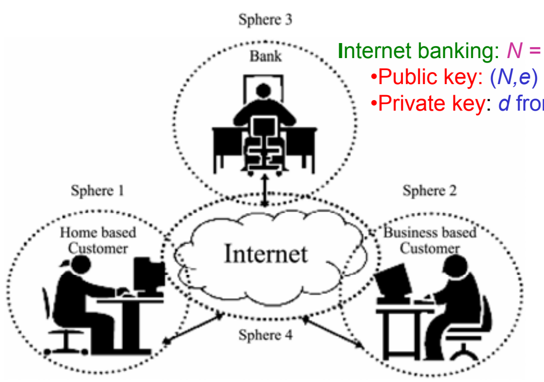
•Public key: 公開的編碼金鑰 (N,e)

•Private key:不公開的解碼金鑰 (N, p,q)

RSA public-key cryptography



Internet Banking

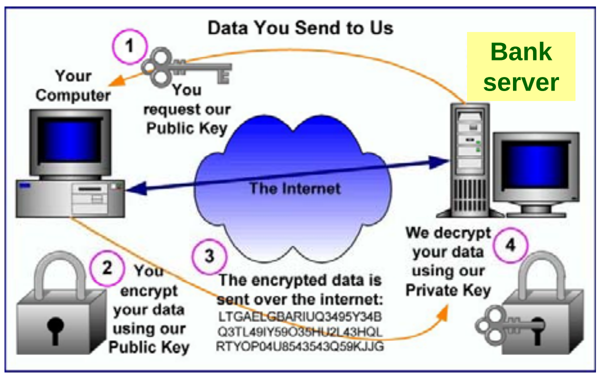


Internet banking: $N = p\ q$

•Public key: (N,e)

•Private key: d from p,q

Internet Banking cryptosystem

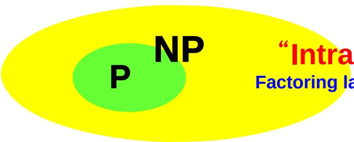


Complexity(複雜度)

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

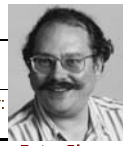


"Intractable"
Factoring large integers?

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

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

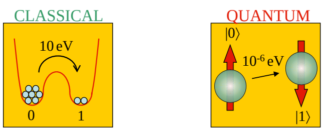
- 封閉的量子系統隨時間的演化是 Unitary: $|\psi'\rangle = U|\psi\rangle$

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.**

Entanglement

Alice 

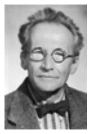
$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

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

Bob 

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

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



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.

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

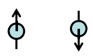
- Complex amplitudes or Interference(複數振幅或干涉)
- Quantum entanglement (composite systems) 量子糾纏

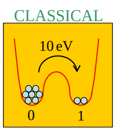
$$\text{Separable:}\ \frac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B + |0\rangle_A|1\rangle_B\right) = |0\rangle_A \otimes \frac{1}{\sqrt{2}}\left(|0\rangle_B + |1\rangle_B\right)$$

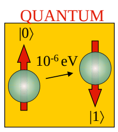
$$\text{Entangled:}\ \frac{1}{\sqrt{2}}\left(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B\right) \neq |\psi\rangle_A \otimes |\phi\rangle_B$$

- 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

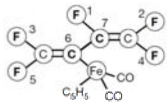
- A scalable physical system with well characterized qubits
- The ability to initialize the state of the qubits to a simple fiducial state, such as $|000\ldots\ldots\rangle$.
- Long relevant decoherence times, much longer than the gate operation time
- A universal set of quantum gates
- A qubit-specific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

NATURE | VOL 414 | 20/27 DECEMBER 2001 | 883

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

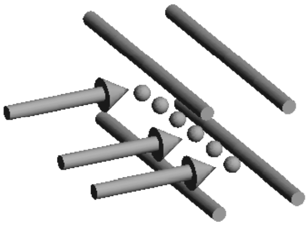


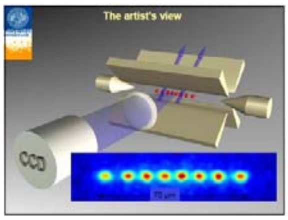
Lieven M. K. Vandersypen*†, Matthias Steffen*†, Gregory Breyta*, Costantino S. Yannoni*, Mark H. Sherwood* & Isaac L. Chuang*†

- Currently the fastest computers in existence, or supercomputers, could factor a number that is 130 digits long in about a month. But they wouldn't be able to factor a 200-digit number.
- The molecule used consists primarily of fluorine and carbon atoms and can be regarded as 7-qubit QC.
- A vial of liquid containing quadrillions of the molecules was placed inside a machine called a nuclear magnetic resonance spectrometer
- By bombarding the molecules with a precise sequence of

Ion Traps (離子阱)

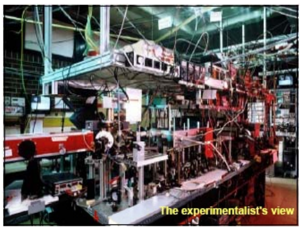
- Ions are laser cooled using resolved sideband cooling, and the temperature of a ion's vibrational degree of freedom can be 10^{-3} K.
- Couple lowest centre-of-mass modes to internal electronic states of N ions by external lasers.





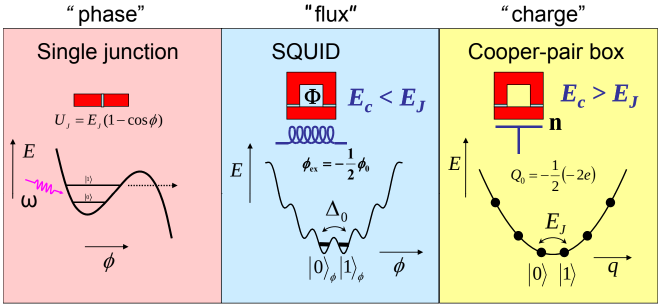
- Excellent optical readout achieved via fluorescence shelving in ion trap systems

光學量子電腦計算



超導體 Josephson-junction-based qubits

"phase" "flux" "charge"



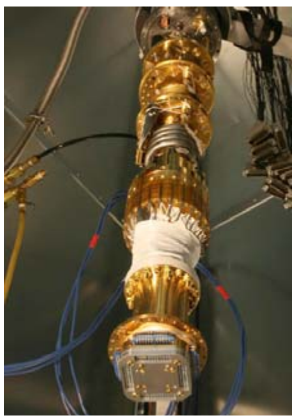
NIST
Kansas
Maryland
UCSB

Delft
NTT
Jena

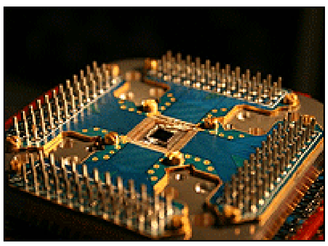
Saclay

NEC
Chalmers
Yale
JPL

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.

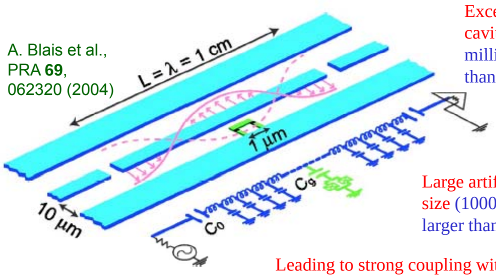


The Orion chip in its package.

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)

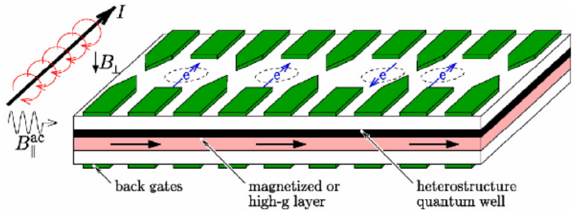


Exceptionally small cavity volume (one million times smaller than 3D cavities)

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

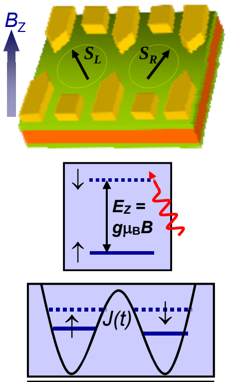
Leading to strong coupling with $g \gg \kappa, \gamma$

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

Quantum dot spin qubits



$H_s(t) = J(t)\, \mathbf{S}_L \cdot \mathbf{S}_R$

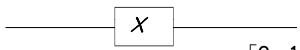
Loss & DiVincenzo, PRA 57, 120 (1998)

- Qubit defined by Zeeman-split levels of *single electron* in quantum dot
- 1-qubit control:
  - magnetic (ESR-field)
  - electric (modulate effective g-factor)
- 2-qubit coupling: electric (exchange interaction between dots)
- Read-out

Hanson et al. (Delf)

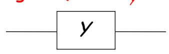
Pauli gates

X gate (AKA σ_x or σ_1)



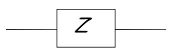
$X|0\rangle = |1\rangle; \quad X|1\rangle = |0\rangle; \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

Y gate (AKA σ_y or σ_2)



$Y|0\rangle = i|1\rangle; \quad Y|1\rangle = -i|0\rangle; \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$

Z gate (AKA σ_z or σ_3)



$Z|0\rangle = |0\rangle; \quad Z|1\rangle = -|1\rangle; \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

Notation: $\sigma_0 \equiv I$

Universal and CNOT gate

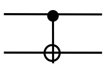
- CNOT + single qubit rotations are universal for quantum computation.
- Any gate can be constructed using CNOT and single qubit rotations.

$$\text{CNOT} + \; R_X(\alpha),\; R_Y(\beta),\; R_Z(\gamma)$$

- What is the CNOT (Controlled-Not) gate:

$|00\rangle \to |00\rangle$
$|01\rangle \to |01\rangle$
$|10\rangle \to |11\rangle$
$|11\rangle \to |10\rangle$

$$\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$



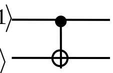
CNOT gate

- Task is to demonstrate that the CNOT gate and single qubit rotations may be constructed.

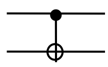
Bell States / EPR States / EPR Pairs

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

$|0\rangle$



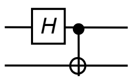
$a|00\rangle + b|11\rangle$



CNOT gate

$|x\rangle$

$|y\rangle$



$|\beta_{xy}\rangle$

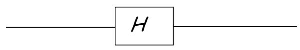
$|00\rangle \quad |\Phi^+\rangle = |\beta_{00}\rangle = \dfrac{|00\rangle + |11\rangle}{\sqrt{2}}$

$|01\rangle \quad |\Psi^+\rangle = |\beta_{01}\rangle = \dfrac{|01\rangle + |10\rangle}{\sqrt{2}}$

$|10\rangle \quad |\Phi^-\rangle = |\beta_{10}\rangle = \dfrac{|00\rangle - |11\rangle}{\sqrt{2}}$

$|11\rangle \quad |\Psi^-\rangle = |\beta_{11}\rangle = \dfrac{|01\rangle - |10\rangle}{\sqrt{2}}$

Hadamard gate



$H|0\rangle = \dfrac{|0\rangle + |1\rangle}{\sqrt{2}}; \quad H|1\rangle = \dfrac{|0\rangle - |1\rangle}{\sqrt{2}};$

$H = \dfrac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$

Effective qubit Hamiltonian

$$H(t) = \sum_i \mu_B g_i(t) \boldsymbol{B}_i(t) \cdot \boldsymbol{S}_i + \sum_{i<j} J_{ij}(t) \boldsymbol{S}_i \cdot \boldsymbol{S}_j$$

- Single qubit operations:
  - Z-rotations: electric (modulate effective g-factor or produce locally different magnetic field)
  - X and Y rotations: ESR (electron spin resonance)

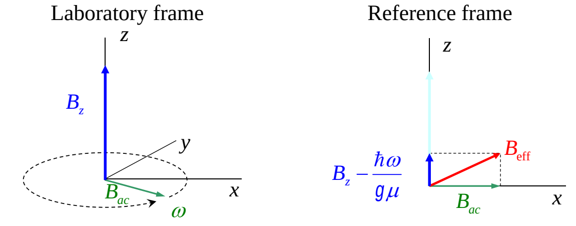
Notations: $\sigma_x = X;\ \sigma_y = Y;\ \sigma_z = Z.$

- Two-qubit operation: $U(t) = T\ \exp\left(\frac{i}{\hbar}\int_0^t \frac{J_{ij}}{4} \boldsymbol{\sigma}_i \cdot \boldsymbol{\sigma}_j\right)$
- Swap gate: when $\frac{1}{\hbar}\int J(\tau)d\tau = \pi (\mathrm{mod}\ 2\pi);\quad U_{sw}|nm\rangle = e^{i\frac{\pi}{4}}|mn\rangle$

$|00\rangle \to |00\rangle$
$|01\rangle \to |10\rangle$
$|10\rangle \to |01\rangle$
$|11\rangle \to |11\rangle$

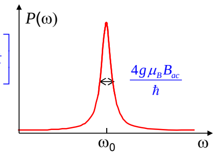
$$\mathrm{SWAP} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Single qubit rotations



$$P_{|1\rangle}(t) = \frac{(g\mu_B B_{ac}/\hbar)^2}{(\frac{g\mu_B B_{ac}}{\hbar})^2 + (\frac{\omega-\omega_0}{2})^2} \sin\left[\sqrt{(\frac{g\mu_B B_{ac}}{\hbar})^2 + (\frac{\omega-\omega_0}{2})^2}\ t\right]$$

with an initial $|0\rangle$ state; $\quad \omega_0 = g\mu_B B_z/\hbar$



Constructing CNOT gate from the controlled Z Gate

Hadamard gate:

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},\quad H = R_Z(\frac{\pi}{2}) R_X(\frac{\pi}{2}) R_Z(\frac{\pi}{2})$$

Controlled-Z gate,

$$\Lambda_1 Z = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

$$\Lambda_1 Z = e^{i\pi(\frac{I-Z}{2}\otimes\frac{I-Z}{2})} = (e^{-i\frac{\pi}{4}Z} \otimes I)\ (I \otimes e^{-i\frac{\pi}{4}Z})\ e^{i\frac{\pi}{4}Z\otimes Z}$$

Controlled-Not gate:

$$\mathrm{CNOT} = (I \otimes H)\ \Lambda_1 Z\ (I \otimes H)$$

Construction of two-qubit gates

- *Any* two-qubit gate may be expressed in the following way:

$$V = (W_1 \otimes W_2)\ e^{i\theta_X X\otimes X + i\theta_Y Y\otimes Y + i\theta_Z Z\otimes Z}\ (W_3 \otimes W_4)$$

where W_1, W_2, W_3 and W_4 are local operations. We can perform these operations using single-qubit rotations.

- The only challenge is to perform the entangling part of the gate.
- What we have: $U(\theta) = e^{i\theta(X\otimes X + Y\otimes Y + Z\otimes Z)}$
- What we want: $T = e^{i\frac{\pi}{4}Z\otimes Z}$
- Isolate the Z-Z term:

$$(Z\otimes I)\ U(\frac{\pi}{8})\ (Z\otimes I)\ U(\frac{\pi}{8}) = e^{i\frac{\pi}{8}(-X\otimes X - Y\otimes Y + Z\otimes Z)}\ e^{i\frac{\pi}{8}(X\otimes X + Y\otimes Y + Z\otimes Z)}$$

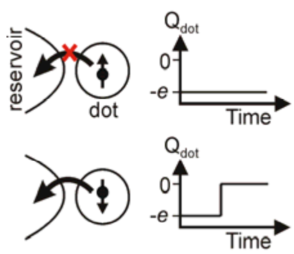
$$= e^{i\frac{\pi}{4}Z\otimes Z}$$

Read-out concept

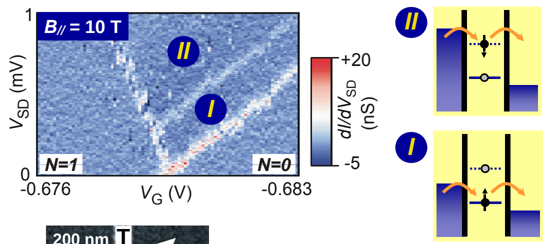
- Spin magnetic moment: $\mu_B = 9.27\times10^{-23}$ A m^2 very small!
- Use spin to charge conversion with fast charge read-out
- Apply magnetic field to split the spin up and down by the Zeeman energy with appropriate dot potential.

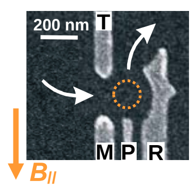
Step 1: Convert spin to charge

Step 2: Measure charge



Step 1: Convert spin to charge

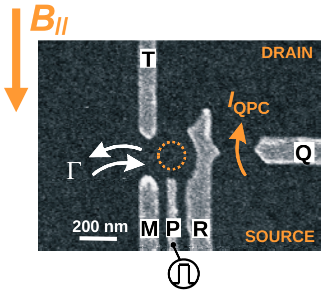


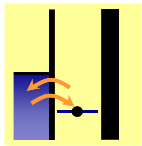


- We can convert spin to charge using Zeeman energy
- Relaxation time T_1 > 50 µs

Hanson *et al.*, PRL **91**, 196802 ('03)
Hanson *et al.*, cond-mat/0311414

Step 2: measure charge within T_1

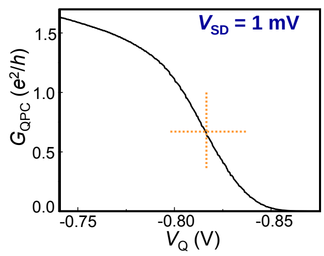


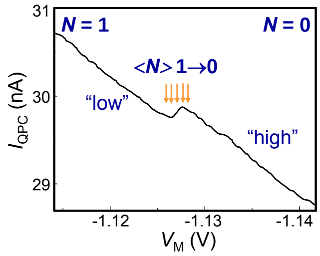


- Tunnel barrier to QPC-channel closed completely
- QD weakly connected to reservoir
- Detect individual tunnel events

- Fast IV-converter (100 kHz, 0.8nV/Hz$^{1/2}$)
- Fast ISO-amp (300 kHz)
- Low-pass filter (40 kHz)
- Fast data acquisition (0.45 µs / point)

QPC average charge detection (dc)

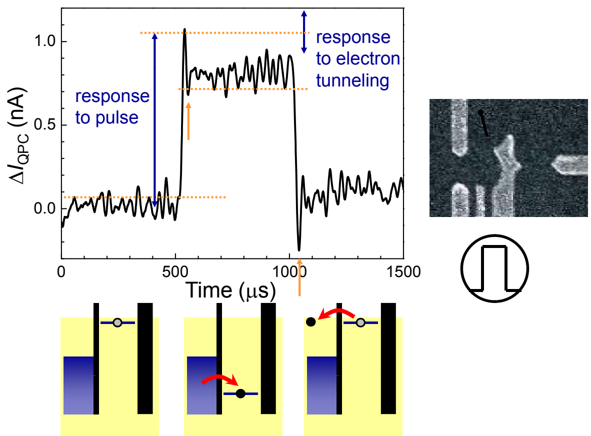




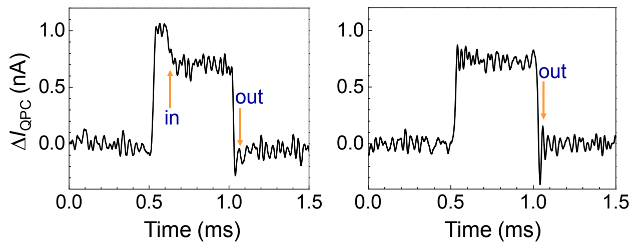
- V_{SD} = 1 mV
- G_{QPC} ~ 0.5 – 1.0 e^2/h
- I_{QPC} ≈ 30 nA

- Sweep dot-gate (V_M)
- I_{QPC} increases (~1%) when <N> from 1 to 0

Tunneling induced by pulse



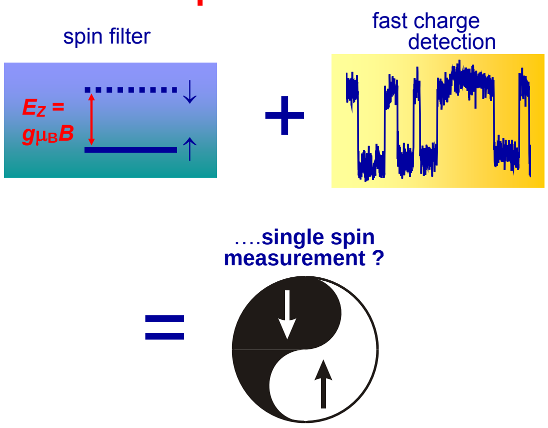
Tunnel-time is stochastic



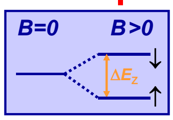
- Tunnel-in event visible
- Tunnel-out event very fast

- Tunnel-in event too fast
- Tunnel-out event visible

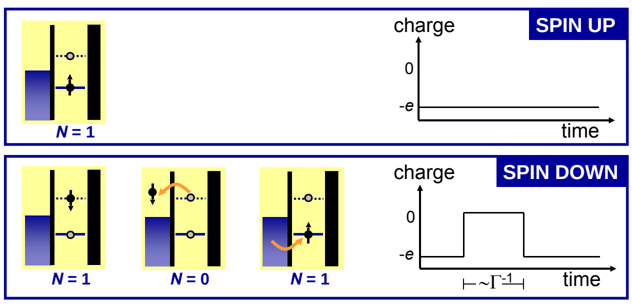
Spin readout



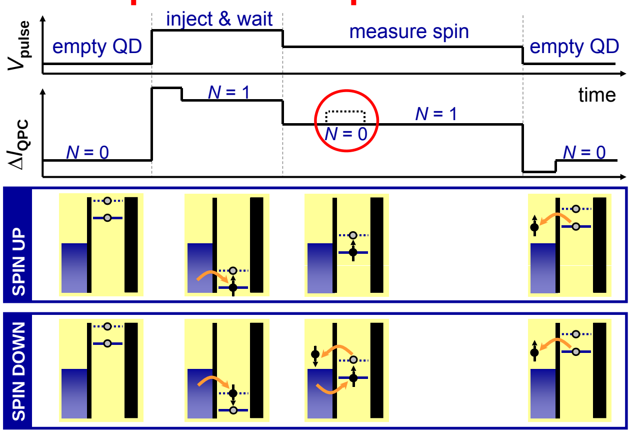
Spin-to-charge conversion



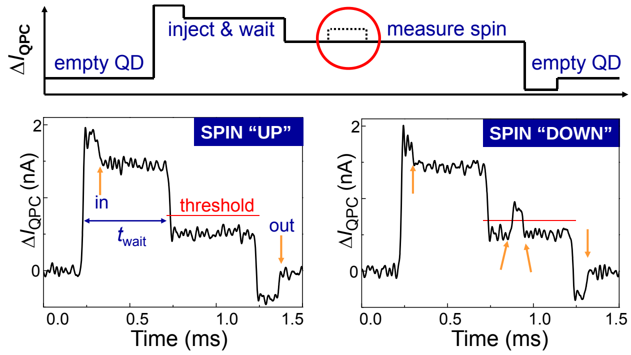
Use Zeeman splitting $\Delta E_Z = g\mu_B B$



Spin read-out procedure



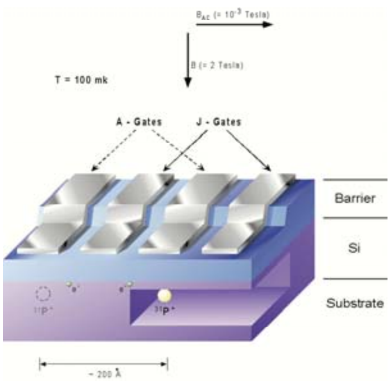
Single-shot spin read-out results



Flat signal in read-out region
⇒ spin is “up”

Step during read-out region
⇒ spin is “down”

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

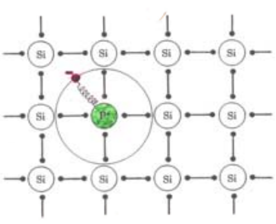


- Exploiting the existing strength of Si technology
- Regular array of P donors in pure silicon
- Low temperature:
  - Effective Hamiltonian involves only spins
  - Long spin coherence and relaxation times
- Magnetic field **B** to polarized electron spins
- Control with surface gates and NMR pulses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

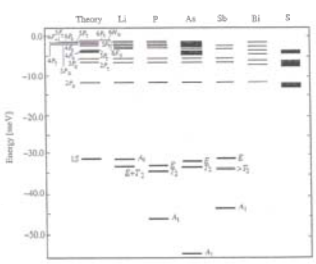
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1 H 氫					元素週期表												鈍氣
鹼金屬	鹼土金屬															鹵素	2 He 氦
3 Li 鋰	4 Be 鈹											5 B 硼	6 C 碳	7 N 氮	8 O 氧	9 F 氟	10 Ne 氖
11 Na 鈉	12 Mg 鎂	---	---	---	---	過渡	金屬	---	---	---	---	13 Al 鋁	14 Si 矽	15 P 磷	16 S 硫	17 Cl 氯	18 Ar 氬
19 K 鉀	20 Ca 鈣	21 Sc 鈧	22 Ti 鈦	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 金需	105 Db	106 Sg	107 Bh	108 Hs	109 Mt	110 Uun	111 Uuu	112 Uub						

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

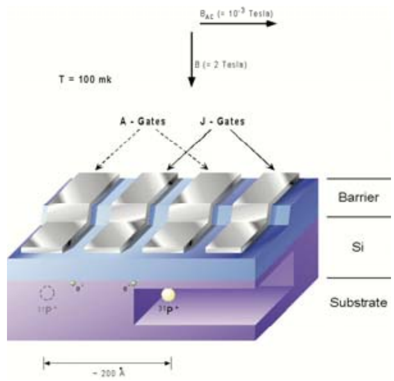


P shallow donor energy levels in Si



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

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

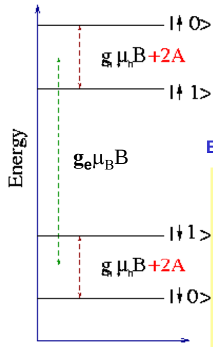


- Exploiting the existing strength of Si technology
- Regular array of P donors in pure silicon
- Low temperature:
  - Effective Hamiltonian involves only spins
  - Long spin coherence and relaxation times
- Magnetic field **B** to polarized electron spins
- Control with surface gates and NMR pulses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

Silicon-based quantum bits

- Donor nuclear spins [Kane, Nature (1998)]
- Donor electron spins
  - Si-Ge hetero-structures [Vrijen et al., PRA (2000)]
  - Dipolar coupling [de Sousa et al., PRA (2004)]
  - Surface gate and global control [Hill et al., PRB (2005)]
- Donor electron-nuclear spin pairs
  - Digital Approach [Skinner et al., PRL (2003)]
- Donor electron charges
  - P/P+ charge qubit [Hollenberg et al., (2004)]
- Electron spins in silicon-based quantum dots [Friesen et al., PRB (2002)]
- …….

Single-qubit system



Effective low-energy low-temperature Hamiltonian:

$$H_B + H_A = g_e\mu_e B\frac{Z_e}{2} - g_n\mu_n B\frac{Z_n}{2} + A\boldsymbol{\sigma}_e\cdot\boldsymbol{\sigma}_n$$

where $A = (2\pi/3)g_e\mu_e g_n\mu_n\,|\Psi(0)|^2$

Notations: $\sigma_x = X;\ \sigma_y = Y;\ \sigma_z = Z.$

Energy separation:

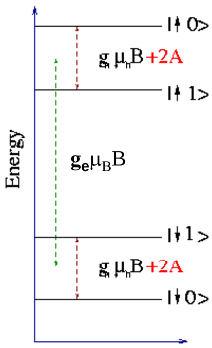
$$E^{(2)}_{|\uparrow 0\rangle} = g_e\mu_B B/2 - g_n\mu_n B/2 + A$$

$$E^{(2)}_{|\uparrow 1\rangle} = g_e\mu_B B/2 + g_n\mu_n B/2 - A + \frac{2A^2}{(g_e\mu_B B/2 + g_n\mu_n B/2)}$$

$$E^{(2)}_{|\downarrow 1\rangle} = -g_e\mu_B B/2 + g_n\mu_n B/2 + A$$

$$E^{(2)}_{|\downarrow 0\rangle} = -g_e\mu_B B/2 - g_n\mu_n B/2 - A - \frac{2A^2}{(g_e\mu_B B/2 + g_n\mu_n B/2)}$$

Effective single-qubit Hamiltonian



Qubit energy separation (if nuclear spins is initialized in spin-up state):

$$\Delta E = E^{(2)}_{|\uparrow 0\rangle} - E^{(2)}_{|\downarrow 0\rangle}$$

$$= g_e\mu_B B + 2A + \frac{2A^2}{(g_e\mu_B B/2 + g_n\mu_n B/2)}$$

Effective single-qubit Hamiltonian:

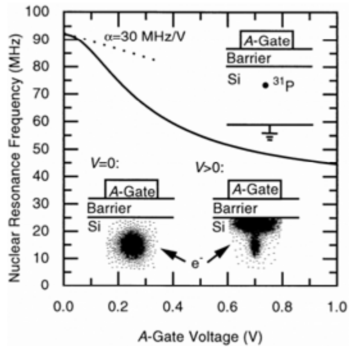
$$H_{eff} = \frac{\hbar}{2}\omega(A)Z_e$$

$$\hbar\omega(A) = g_e\mu_B B + 2A + \frac{4A^2}{(g_e\mu_B + g_n\mu_n)B}$$

Hamiltonian in a Bac field:

$$H_{ac} = g_e\mu_e B_{ac}[X_e\cos(\omega_{ac}t) + Y_e\sin(\omega_{ac}t)]$$

Single-qubit control



B. Kane, Nature **393**, 133 (1998)

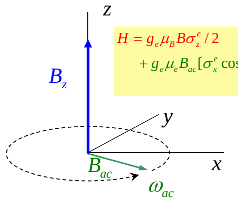
Having control over hyperfine interaction by applying voltage to A gate would allow us to:

- Change the resonant frequency of a particular qubit.
- Perform X and Y rotations on a specific qubit using a resonant magnetic field
- Perform a Z on a specific qubit (much faster than X and Y rotations)

These three operations allow us to do any single qubit rotation on the nuclear spins.

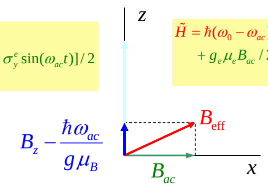
Single qubit rotations

Laboratory frame



$$H = g_e\mu_B B\sigma^e_z/2 + g_e\mu_e B_{ac}[\sigma^e_x\cos(\omega_{ac}t) + \sigma^e_y\sin(\omega_{ac}t)]/2$$

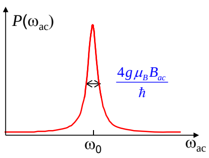
Reference frame



$$\tilde{H} = \hbar(\omega_0 - \omega_{ac})\sigma^e_z/2 + g_e\mu_e B_{ac}/2$$

$$P_{|\downarrow\rangle}(t) = \frac{(g\mu_B B_{ac}/\hbar)^2}{(\frac{g\mu_B B_{ac}}{\hbar})^2 + (\frac{\omega_0 - \omega_{ac}}{2})^2}\sin\left[\sqrt{(\frac{g\mu_B B_{ac}}{\hbar})^2 + (\frac{\omega_0 - \omega_{ac}}{2})^2}\ t\right]$$

with an initial $|\uparrow\rangle$ state; $\omega_0 = g\mu_B B_z/\hbar$



Two-qubit Hamiltonian

- Effective e-spin Hamiltonian in the rotating frame

$$H_{eff} = \frac{\hbar}{2}\Delta\omega_1\sigma^{1e}_z + \frac{\hbar}{2}\Delta\omega_1\sigma^{2e}_z + \frac{1}{2}g_e\mu_B B_{ac}(\sigma^{1e}_x + \sigma^{2e}_x) + J\boldsymbol{\sigma}^{1e}\cdot\boldsymbol{\sigma}^{2e},$$

where $\Delta\omega_i = \omega(A_i) - \omega_{ac}$,

$$\hbar\omega(A) = g_e\mu_B B_0 + 2A + \frac{4A^2}{(g_e\mu_B + g_n\mu_n)B}$$

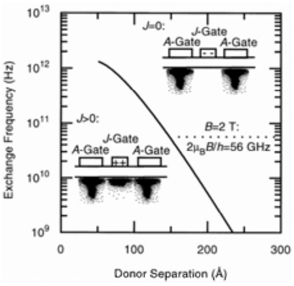
- Full Hamiltonian in the Lab. frame

$$\begin{aligned} H = \ & \tfrac{1}{2}g_e\mu_B B_0\left(\sigma^{1e}_z + \sigma^{2e}_z\right) - \tfrac{1}{2}g_n\mu_n B_0\left(\sigma^{1n}_z + \sigma^{2n}_z\right) \\ & + \tfrac{1}{2}g_e\mu_B B_{ac}\left(\cos\omega_{ac}t(\sigma^{1e}_x + \sigma^{2e}_x) + \sin\omega_{ac}t(\sigma^{1e}_y + \sigma^{2e}_y)\right) \\ & - \tfrac{1}{2}g_n\mu_n B_{ac}\left(\cos\omega_{ac}t(\sigma^{1n}_x + \sigma^{2n}_x) + \sin\omega_{ac}t(\sigma^{1n}_y + \sigma^{2n}_y)\right) \\ & + A_1\boldsymbol{\sigma}^{1e}\cdot\boldsymbol{\sigma}^{1n} + A_2\boldsymbol{\sigma}^{2e}\cdot\boldsymbol{\sigma}^{2n} + J\boldsymbol{\sigma}^{1e}\cdot\boldsymbol{\sigma}^{2e}\,. \end{aligned}$$

Two-qubit control

- Two qubit Hamiltonian:

$$H_{2q} = \sum_{i=1}^{2} H_B + H_A + H_{ac} + H_J$$



$$H_J = J\boldsymbol{\sigma}_{e1} \cdot \boldsymbol{\sigma}_{e2}$$

The magnitude of the exchange interaction, J, depends on the degrees of overlap of electronic wave functions and can be controlled by the surface J-Gate.

B. Kane, Nature **393**, 133 (1998)

Universal and CNOT gate

- CNOT + single qubit rotations are universal for quantum computation.
- Any gate can be constructed using CNOT and single qubit rotations.

$$\text{CNOT} + R_X(\alpha),\ R_Y(\beta),\ R_Z(\gamma)$$

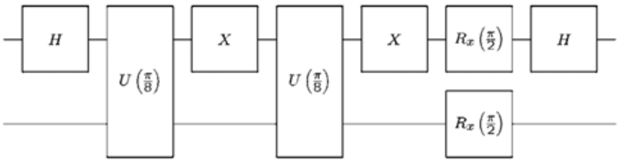
- What is the CNOT (Controlled-Not) gate:

$$|00\rangle \to |00\rangle$$
$$|01\rangle \to |01\rangle$$
$$|10\rangle \to |11\rangle$$
$$|11\rangle \to |10\rangle$$

$$\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

- Task is to demonstrate that the CNOT gate and single qubit rotations may be constructed.

Canonical decomposition of CNOT gate for global control e-spin QC



$$U\left(\frac{\pi}{8}\right) = \exp\left[i\frac{\pi}{8}\boldsymbol{\sigma}^{1e} \cdot \boldsymbol{\sigma}^{2e}\right]$$

CNOT gate operation time: 297ns

J/h=10.2 GHz

C. D. Hill, L. C. L. Hollenberg, A. G. Fowler, C. J. Wellard, A. D. Greentree, and H.-S. Goan, *"Global control and fast solid-state donor electron spin quantum computing"*, Phys. Rev. B **72**, 045350 (2005).

PHYSICAL REVIEW B **72**, 045350 (2005)

Global control and fast solid-state donor electron spin quantum computing

C. D. Hill,[1,*] L. C. L. Hollenberg,[2] A. G. Fowler,[2] C. J. Wellard,[2] A. D. Greentree,[2] and H.-S. Goan[3]

We propose a scheme for quantum information processing based on donor electron spins in semiconductors, with an architecture complementary to the original Kane proposal. We show that a naïve implementation of electron spin qubits provides only modest improvement over the Kane scheme, however through the introduction of global gate control we are able to take full advantage of the fast electron evolution timescales. We estimate that the latent clock speed is 100–1000 times that of the nuclear spin quantum computer with the ratio T_2/T_{ops} approaching the 10^6 level.

- Simulation of electron exchange mediated two-qubit gates in the Kane donor nuclear spin scheme showed that the gate fidelity is limited primary by the electron coherence when the electron dephasing timescale is close to the typical gate operation time of O(μs).
- Experimental indication: P donor electron spin T_2 > 60 ms at 4K in purified silicon [Tyryshkin, Lyon et al., PRB (2003)].
- Features of e-spin based QC:
  - **Fast gate speed (16.0 μs → 297ns) ,**
  - **Comparatively simpler readout**

Optimal control

- One of the important criteria for physical implementation of a practical quantum computer is to have a universal set of quantum gates with operation times much faster than the relevant decoherence time of the quantum computer.
- High-fidelity quantum gates to meet the error threshold of about 10^{-4} (10^{-3}) are also desired for fault-tolerant quantum computation (FTQC).
- Thus the goal of optimal control is to find fast and high-fidelity quantum gates.

Error threshold: P. Aliferis and J. Preskill, Phys. Rev. A **79**, 012332 (2009).

Quantum error correction and fault-tolerant quantum computation

- Quantum error correction: to protect quantum information from errors due to decoherence and other quantum noise.
- The key result in the theory of QEC is the **threshold theorem for FTQC**: if a quantum computer has an intrinsic error rate per gate which is less than a certain threshold (currently estimated to be $10^{-4} \sim 10^{-3}$), it is possible by means of error correcting codes to make the total error probability arbitrarily low.
- That is, the overall probability of error for the whole computation can be made less than ε for any value of ε> 0; and the overhead for doing so scales like O(polylog(1/ε)).
- This means that once it is possible to build Q-bits and Q-gates with sufficiently low decoherence, quantum computations of unlimited size are possible!

Error threshold: P. Aliferis and J. Preskill, Phys. Rev. A **79**, 012332 (2009).

GRadient Ascent Pulse Engineering (GRAPE)

- N. Khaneja et al., J. Magn. Reson. **172**, 296 (2005).
- A. Sporl et al., Phys. Rev. A **75**, 012302 (2007)

- Propagator during time step j ($\Delta t=T/N$)

$$U_j(\Delta t)=\exp\left[-\frac{i}{\hbar}\Delta t\left(H_0+\sum_{k=1}^{m}u_{kj}H_k\right)\right]$$

- Propagator at final time T

$$U_F=U_N\cdots U_1$$

See also: Montangero et al., PRL **99**, 170501 (2007) and Carlini et al., PRL **96**, 060503 (2006);PRA **75**, 042308 (2007)

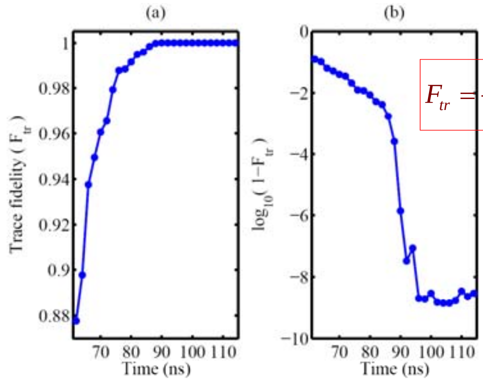
- Performance function (fidelity)

$$\Phi=\frac{1}{N_d}\left|\mathrm{Tr}\left\{U_D^{\dagger}U_F\right\}\right|^2,\ \text{where } U_D:\text{desired op.}$$

Nielsen et al., Science; PRA (2006)

- Optimize the performance function (fidelity) w.r.t. the control amplitudes u_{kj} in a given time T.
- The minimum time sequence that meets the required fidelity is the **near** time-optimal control sequence.

Trace Fidelity versus gate time



$$F_{tr}=\frac{1}{2^n}\left|\mathrm{Tr}\left\{U_D^{\dagger}U_F\right\}\right|$$

Optimizer: spectral projected gradient method

Stopping criteria of the error threshold : 10^{-9}

30 piecewise constant steps is sufficient

Choice of the value of B_{ac}

- While the target electron spin qubit will perform a particular unitary operation within time t, every spectator qubit will rotate around the x-axis with an angle of

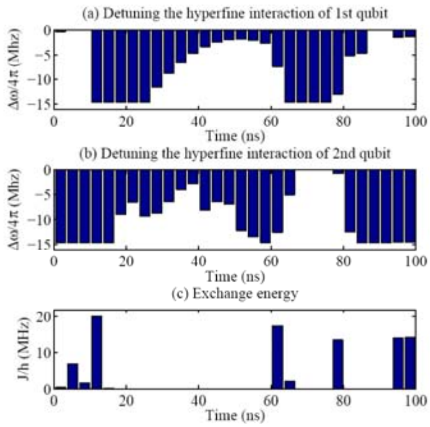
$$\theta_x=\frac{g_e\mu_B B_{ac}}{\hbar}t$$

- If θ_x does not equal to $2n\pi$, where n is an integer, another correction step will be required for the spectator qubits. Therefore, it will be more convenient to choose the operation time,

$$t=\frac{2n\pi\hbar}{g_e\mu_B B_{ac}}$$

- For $t=100\text{ns}$ and $n=1$, $B_{ac}=3.56\times10^{-4}\text{T}$.

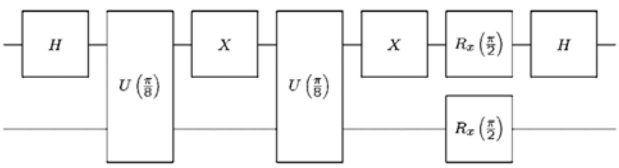
Near time-optimal control sequence



30 steps in 100ns with an error of 1.11×10^{-16}

Calculations performed using the effective e-spin Hamiltonian

Canonical decomposition of CNOT gate for global control e-spin QC



$$U\left(\frac{\pi}{8}\right)=\exp\left[i\frac{\pi}{8}\boldsymbol{\sigma}^{1e}\cdot\boldsymbol{\sigma}^{2e}\right]$$

CNOT gate operation time: 297ns

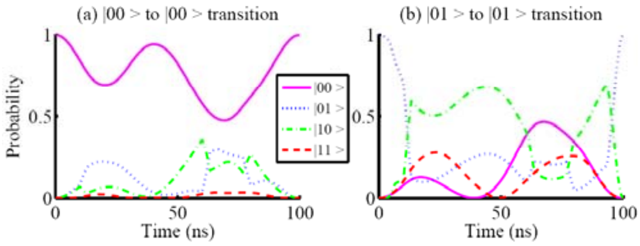
J/h=10.2 GHz

C. D. Hill, L. C. L. Hollenberg, A. G. Fowler, C. J. Wellard, A. D. Greentree, and H.-S. Goan, *"Global control and fast solid-state donor electron spin quantum computing"*, Phys. Rev. B **72**, 045350 (2005).

Parallel quantum computing

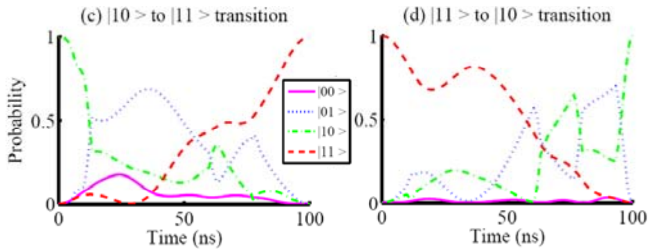
- Traditional decomposition method that decomposes general gate operations into several single-qubit and some interaction (two-qubit) operations in series as the CNOT gate in the globally controlled electron spin scheme. So the single-qubit operations and two-qubit (interaction) operations do not act on the same qubits at the same time.
- The GRAPE optimal control approach is in a sense more like parallel computing as single-qubit (A1 and A2 both on) and two-qubit (J on) operations can be performed simultaneously on the same qubits in parallel.
- As a result, the more complex gate operation it is applied, the more time one may save, especially for those multiple-qubit gates that may not be simply decomposed by using the traditional method.

Time evolution of the near time-optimal CNOT gate with input states |00> and |01>



Simulations performed using the full Hamiltonian

Time evolution of the near time-optimal CNOT gate with input states of |10> and |11>



Simulations performed using the full Hamiltonian

Conclusions

- A great advantage of the optimal control gate sequence is that the maximum exchange interaction is about 500 times smaller than the typical exchange interaction of J/h=10.2 GHz in the Kane's original proposal and yet the CNOT gate operation time is still 3 times faster than that in the globally controlled electron spin scheme.
- This small exchange interaction relaxes significantly the stringent distance constraint of two neighboring donor atoms of 10-20nm as reported in the original Kane's proposal to about 30nm. To fabricate surface gates within such a distance is within reach of current fabrication technology.
- Each step of the control sequence is about 3.3ns which may be achievable with modern electronics.

Conclusions

- The CNOT gate sequence we found has high fidelity, above the fidelity threshold required for fault-tolerant quantum computation.
- The fidelity of the gate sequence is shown, by using realistic (device) parameters, to be robust against control voltage fluctuations, electron spin decoherence and dipole-dipole interaction.
- The GRAPE time-optimal control approach is in a sense more like parallel computing. The more complex gate operation it is applied, the more time one may save, especially for those multiple-qubit gates that may not be simply decomposed by using the traditional method.
- The GRAPE optimization technique may prove useful in implementing (complex) quantum gate operations.
- Ref: D.-B. Tsai, P.-W. Chen and H.-S. Goan, Phys. Rev. A 79, 060306 (Rapid Communication) (2009).

Single-spin detection and quantum state readout by magnetic resonance force microscopy

Goan, Hsi-Sheng
管 希 聖
Department of Physics
Center for Theoretical Sciences, and
Center for Quantum Science and Engineering,
臺灣大學

Collaborators: Shesha Raghunathan and Todd A. Brun
at the University of Southern California

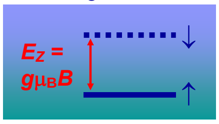
Single-spin detection

- Single-spin measurement is an extremely important challenge, and necessary for the future successful development of several recent spin-based proposals for quantum information processing.
- There are both direct and indirect single-spin measurement proposals:
  - Direct proposals: SQUID, MRFM,…
  - Indirect proposals: Spin-dependent charge transport, spin-dependent optical transition (fluorescence) ,….
- The idea behind some indirect proposals is to transform the problem of detecting a single spin into the task of measuring charge transport since the ability to detect a single charge is now available.
- Magnetic resonance force microscopy (MRFM) has been suggested as a promising technique for single-spin detection [Sidles ('92), Berman et.al.('02)].
- To date, MRFM technique has demonstrated with

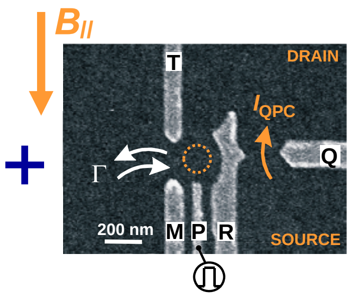
single-spin sensitivity ! D. Rugar's group ('04)

Single spin readout

spin to charge conversion + fast charge detection

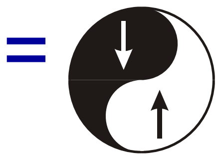


+



....single spin measurement ?

=



letters to nature

Single-shot read-out of an individual electron spin in a quantum dot

J. M. Elzerman, R. Hanson, L. H. Willems van Beveren, B. Witkamp, L. M. K. Vandersypen & L. P. Kouwenhoven

Kavli Institute of Nanoscience Delft and ERATO Mesoscopic Correlation Project, Delft University of Technology, PO Box 5046, 2600 GA Delft, The Netherlands

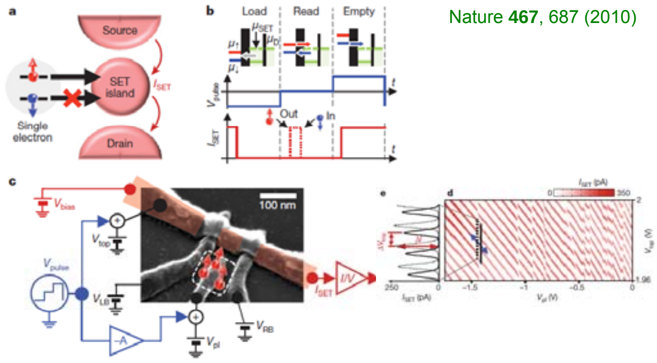
NATURE | VOL 430 | 22 JULY 2004 | www.nature.com/nature

LETTER

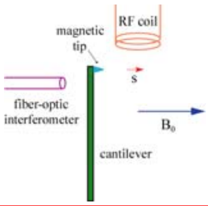
doi:10.1038/nature09392

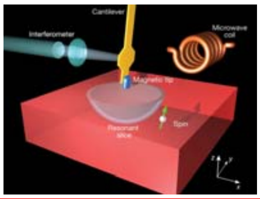
Single-shot readout of an electron spin in silicon

Nature **467**, 687 (2010)



Single spin detection by magnetic resonance force microscopy





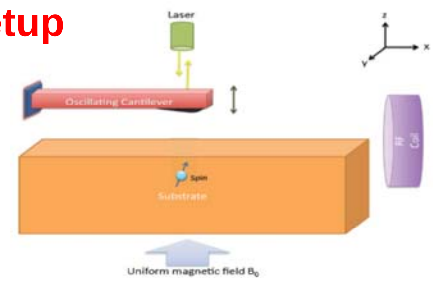
D. Rugar *et al.*, *Nature* **430**, 329 (2004):

- T.A. Brun and **H.-S. Goan**, "*Realistic simulations of single-spin nondemolition measurement by magnetic resonance force microscopy*", Physical Review A **68**, 032301 (2003).
- G.P. Berman, F. Borgonovi, **H.-S. Goan**, S.A. Gurvitz, and V.I. Tsifrinovich, "*Single-spin measurement and decoherence in magnetic resonance force microscopy*", Physical Review B **67**, 094425 (2003).
- **H.-S. Goan**, and T.A. Brun, "*Single spin measurement by magnetic resonance force microscopy: Effect of measurement device, thermal noise and spin relaxation*", Proceedings of **SPIE**, **5276**, 250-261 (2004).
- T. A. Brun and **H.-S. Goan,** "*Realistic simulations of single-spin measurement via magnetic resonance force microscopy*", International Journal of Quantum Information **3**, 1-9 Suppl. (2005).

Magnetic resonance imaging

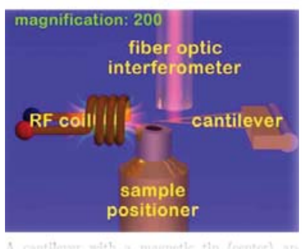
- Magnetic Resonance Imaging (MRI) principle: if the precessing frequency of magnetic moments in a uniform magnetic field is driven on resonance by an external ac magnetic field, the resulting signal reveals something about the spin state of the magnetic moments and the external magnetic environment in which they are placed.
- At least approximate amount of 10^{12} nuclear spins or 10^{9} electron spins is required to generate a measurable MRI signal (via conventional inductive detection techniques).
- Compared to MRI, MRFM technique provides considerable improvements in sensitivity (minimum force detectable) and spatial resolution.

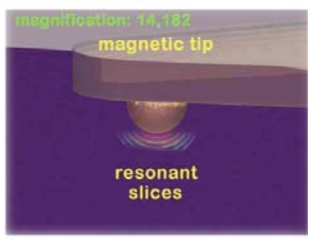
MRFM setup



- A uniform magnetic field in the z-direction.
- A ferromagnetic particle (small magnetic material) mounted on the cantilever tip producing a magnetic field gradient on the single spin.
- As a result, a reactive force (interaction) acts back on the magnetic cantilever tip in the z-direction from the single spin.

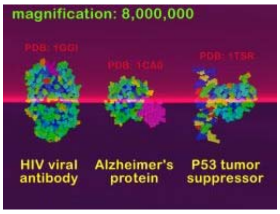
Schematic illustration of MRFM





(John Sidles's group at UW, Seattle, USA)

What is the use of MRFM?



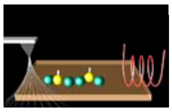
MRFM combines four different technologies to serve as a sensing and imaging device:

- 3-dimensional non-destructive magnetic resonance imaging,
- atomic-level resolution atomic force microscopy,
- mobile scanning probe microscopy allowing in-situ and direct observation,
- continuous observation or readout technique.

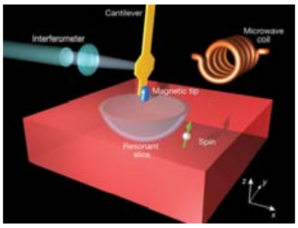
- the direct observation of individual molecules (or other nanoscale devices or materials),
- *in situ*, in their native forms and native environments,
- with three-dimensional atomic-scale resolution,
- by a nondestructive observation process.

MRFM animation

http://www.almaden.ibm.com/vis/models/models.html#mrfm



Single-spin detection by MRFM

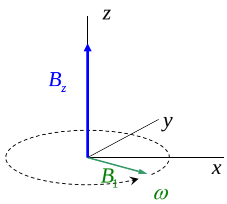


D. Rugar *et al.*, *Nature* **430**, 329 (2004): demonstrated to achieve a detection sensitivity of a single electron spin using the **oscillating cantilever-driven adiabatic reversals (OSCAR)** protocol .

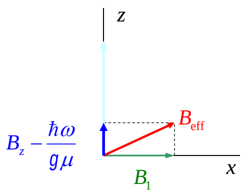
- But the required averaging time is still too long to achieve the real-time readout of the single electron spin quantum state.
- The ability to accomplish the single spin magnetic resonance detection at a spatially resolved location would fulfil an important requirement for many quantum computation schemes.
- Moreover, the ability to detect a single *nuclear* spin would have tremendous impacts on the fields of quantum information processing, quantum computation, data storage, nanometre-scale electronics, materials sciences, biology, biomedicine, and etc.

Laboratory frame and rotating reference frame

Laboratory frame



Reference frame



Spin-cantilever Hamiltonian

In the reference frame rotating with the frequency of the RF (MW) field,

$$\hat{H}_{sz}(t) = \hat{H}_z - \hbar[\omega_L - \omega]\hat{S}_z + \hbar\omega_1\hat{S}_x - g\mu\left(\frac{\partial B_z}{\partial Z}\right)\hat{Z}\hat{S}_z,$$

$$\hat{H}_C = \hat{P}^2/(2m) + m\omega_m\hat{Z}^2/2 + f(t)\hat{Z},$$

$$\omega_L = g\mu B_z/\hbar, \quad \text{Lamor frequency}$$

$$\omega_1 = g\mu B_1/\hbar, \quad \text{Rabi frequency.}$$

For $\omega = \omega_L$, $\hat{H}_{SC}(t) = \hat{H}_C + \varepsilon\hat{S}_x - \eta\hat{Z}\hat{S}_z$,

where $f(t)$: the positive-gain-controlled feedback mechanism,

$$\eta = g\mu(\partial B_Z/\partial Z)_0,$$

$$\varepsilon = \hbar\omega_1.$$

Principle of single-spin measurement I. : oscillating cantilever-driven adiabatic reversals (OSCAR)

- The time scale of cantilever motion is much slower than the time scale of spin precession, i.e., $|dZ/dt| \ll (\varepsilon/\eta)^2$, then the spin Hamiltonian changes with time adiabatically.
- In the case when the adiabatic approximation is exact, the instantaneous eigenstates of the spin Hamiltonian in the rotating reference frame of the RF (MW) field are the spin states parallel or antiparallel to the direction of the effective magnetic field $\mathbf{B}^{\mathrm{eff}} = (\varepsilon, 0, -\eta Z)$,

 denoted as $|v_\pm(t)\rangle$, respectively.

- We define an operator $\hat{S}'_z$ for the component of spin along this axis.

Principle of single-spin measurement II.

- Starting at a general initial spin state in the $\hat{S}_z$ basis

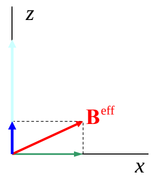
$$\chi(0) = a|\uparrow\rangle + b|\downarrow\rangle$$

- In the basis of the instantaneous $\hat{S}'_z$ eigenstates:

$$\chi(0) = a_{eff}\,|v_+(0)\rangle + b_{eff}\,|v_-(0)\rangle,$$

where $a_{eff} = a\cos(\theta_0/2) + b\sin(\theta_0/2),$

$a_{eff} = -a\sin(\theta_0/2) + b\cos(\theta_0/2),$



$\theta_0 = \theta(0)$ initial angle between $\mathbf{B}^{eff}(0)$ and z-axis direction

$$\tan[\theta(t)] = \frac{B_x^{eff}(t)}{B_z^{eff}(t)} = -\frac{\varepsilon}{\eta Z}$$

Principle of single-spin measurement III.

- Following from the adiabatic theorem:

$$\chi(t) = a_{eff}\,|v_+(t)\rangle \exp(-i\int_0^t \lambda_+(t')dt')$$
$$+ b_{eff}\,|v_-(t)\rangle \exp(-i\int_0^t \lambda_-(t')dt'),$$

where $\lambda_\pm(t) = \pm\sqrt{\varepsilon^2 + \eta^2 Z^2}$ are instantaneous eigenvalues.

- Probabilities $|a_{eff}|^2$ and $|b_{eff}|^2$ remain the same at all times.

- This provides us with an opportunity to measure the initial spin state probabilities at later times.

How do we measure these spin state probabilities?

- The idea is to transfer the information of the spin state to the frequency shift of the driven cantilever by keeping the amplitude of the cantilever vibrations at a fixed preset value by feedback control (OSCAR).
- In the interaction picture in which the state is rotating with the instantaneous eigenstates of the spin Hamiltonian, the spin-cantilever Hamiltonian can be written as:

$$[\hat{H}_C + \hat{H}_S][|\psi_z\rangle \otimes |v_\pm\rangle] = [\hat{H}_C + \lambda_\pm][|\psi_z\rangle \otimes |v_\pm\rangle]$$

$$\lambda_\pm = \pm\sqrt{\varepsilon^2 + \eta^2 Z^2} \approx \pm\varepsilon[1 + (\eta Z/\varepsilon)^2/2]$$

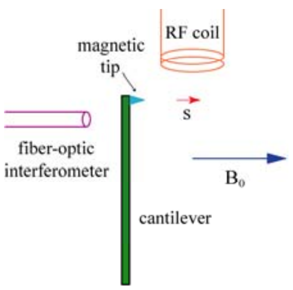
effective Hamiltonian: $H' = (\eta^2/2\varepsilon)\hat{Z}^2\hat{\sigma}'_z$

- The frequency of the driven cantilever vibrations depends on the orientation of the spin states of $\hat{\sigma}'_z$.

Measurement scheme and device

- The cleaved end of the fiber and the vibrating cantilever form a cavity. As the cantilever moves, the resonant frequency of the cavity changes.
- Because the time scale of the cantilever's motion is very long compared to the optical time scale, we can treat the effects of this in the adiabatic limit.
- The cavity mode is also subject to driving by an external laser, and has a very high loss rate.
- In the bad cavity limit, the dynamics of field quadrature (x) adiabatically follows that of cantilever position.
- The continuous monitoring of the cantilever motion at a fixed amplitude is done by fiber-optic interferometer : homodyne measurement on the light escaping the cavity
  - ⇒ frequency shift of the cantilever vibrations.
  - ⇒ state of the single spin.

MRFM setup

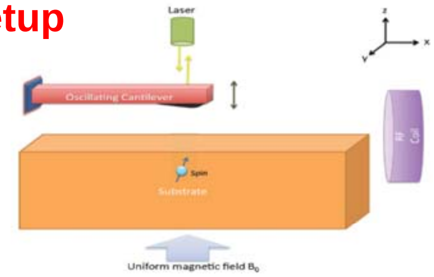


- A uniform magnetic field in the z-direction.
- A ferromagnetic particle (small magnetic material) mounted on the cantilever tip producing a magnetic field gradient on the single spin.
- As a result, a reactive force (interaction) acts back on the magnetic cantilever tip in the z-direction from the single spin.

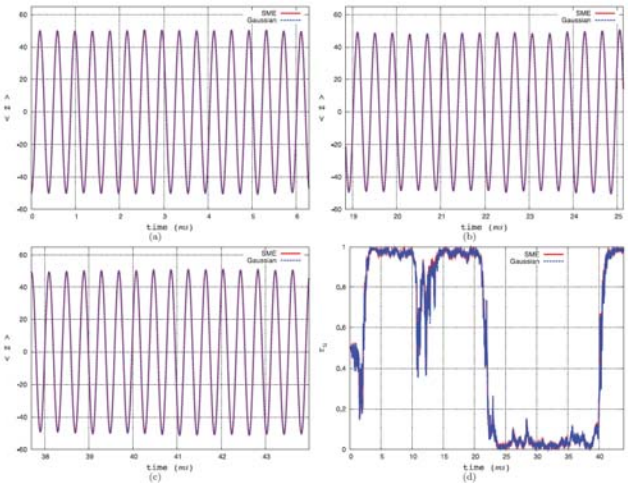
Stochastic master equation approach

- Consider various relevant sources of noise:
  - cantilever in a thermal bath and interacting with the cavity mode
  - cavity mode subject to driving by an external laser and its decay form the cavity
  - ``back-action'' noise and shot noise of detected photocurrent
  - spin noise due to magnetic source
- Develop a continuous measurement model taking into account a positive gain-controlled feedback mechanism that maintains the amplitude of the cantilever at a predetermined constant, leading to a change in cantilever frequency.
- A stochastic master equation represents the evolution of the state conditioned on the photocurrent measurement record.
- We simplify the description of the cantilever-spin system by approximating the cantilever wave function as a Gaussian wave packet and show that the resulting Gaussian approximation closely matches the full quantum behavior.

MRFM setup



- A uniform magnetic field in the z-direction.
- A ferromagnetic particle (small magnetic material) mounted on the cantilever tip producing a magnetic field gradient on the single spin.
- As a result, a reactive force (interaction) acts back on the magnetic cantilever tip in the z-direction from the single spin.



Parameters

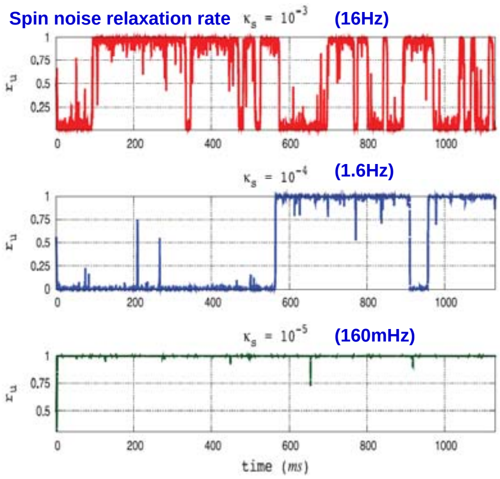
In physical units:

$$\omega = 10^5\,\mathrm{s}^{-1},\ m = 10^{-12}\,\mathrm{kg},\ Q = 10^5,\ \varepsilon / g\mu_B = 3\times10^{-2}\,\mathrm{T},$$

$$\eta / g\mu_B = (\partial \mathrm{B}_z / \partial Z) = 10^7\,\mathrm{T/m},\ k_B T = 10\,\mathrm{mK},$$

$$\omega_c = 1.4\times10^{15}\,\mathrm{s}^{-1},\ Q_c = 100,\ P_L = 1\,\mu\mathrm{W},\ e_d = 0.85,$$

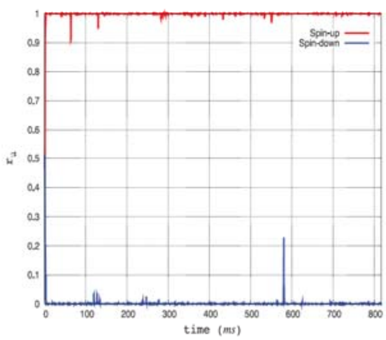
$$k_S = 16\,\mathrm{Hz},\ \mathcal{A} = 32\,\mathrm{nm}.$$



Time evolution of the spin-up probability r_u for different k_S values

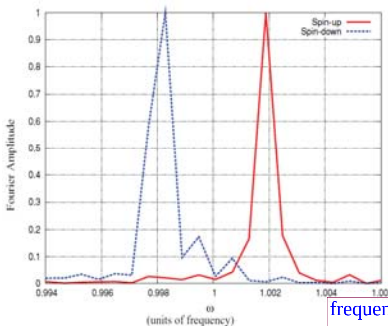
The number of spin flips decreases as κ_s is reduced.

Time evolution of the spin-up probability r_u for the two trajectories



In the red trajectory, the spin relaxes to its up state, while in the blue trajectory, it relaxes to its down state.

Frequency shift in the OSCAR MRFM protocol for two trajectories



- Fourier amplitude (in arbitrary units) as a function of cantilever frequency ω corresponding to the two trajectories in previous slide.
- The Fourier amplitude is calculated using a standard FFT algorithm; the number of samples is $N = 2^{19}$, and the sample spacing is $\Delta t = 0.02$.

frequency resolution $\le$ frequency shift

$$\Delta f \approx \frac{1}{N\Delta t} \approx \frac{1}{T_{\mathrm{sampling}}} \le \frac{(\eta^2/2\varepsilon)}{2\pi}$$

Summary

- In physical units:

  If we take $f^{\text{phys}} = \omega^{\text{phys}} / 2\pi \approx 16\text{kHz}$,

  $T_{\text{sampling}}^{\text{phys}} = T_{\text{sampling}} / f^{\text{phys}} \approx 656\text{ms}$.

  Requiring $k_S^{-1} > T_{\text{sampling}}^{\text{phys}}$, we take $k_S = 160\text{mHz}$

  Cantilever frequency shift $= (\eta^2 / 2\varepsilon)\omega^{phys} \approx 29\text{Hz}$
- In our simulation, it takes ~ 650 ms for the OSCAR protocol to determine a shift of ~ 30 Hz in cantilever frequency and, consequently, to ascertain the orientation of the spin.
- The time scale of the spin noise must be longer than the sampling duration to use OSCAR MRFM as a single-spin measurement device.
- Steady improvement in these techniques should make single-spin measurement more efficient and effective.
- Ref: S. Raghunathan, T. A. Brun, H.-S.Goan, PRA **82**, 052319 (2010).

Recent experiments on MRFM

letters to nature

Single spin detection by magnetic resonance force microscopy

D. Rugar, R. Budakian, H. J. Mamin & B. W. Chui

IBM Research Division, Almaden Research Center, 650 Harry Rd, San Jose, California 95120, USA

NATURE | VOL 430 | 15 JULY 2004 | www.nature.com/nature 329

REPORTS 21 JANUARY 2005 VOL 307 SCIENCE 408

Creating Order from Random Fluctuations in Small Spin Ensembles

R. Budakian,* H. J. Mamin, B. W. Chui, D. Rugar

We demonstrate the ability to create spin order by using a magnetic resonance force microscope to harness the naturally occurring statistical fluctuations in small ensembles of electron spins. In one method, we hyperpolarized the spin system by selectively capturing the transient spin order created by the statistical fluctuations. In a second method, we took a more active approach and rectified the spin fluctuations by applying real-time feedback to the entire spin ensemble. The created spin order can be stored in the laboratory frame for a period on the order of the longitudinal relaxation time of 30 seconds and then read out.

Improvements in detection signal-to-noise ratio should allow real-time quantum state detection and feedback control of individual electron spins

Nanoscale magnetic resonance imaging

C. L. Degen[a], M. Poggio[a,b], H. J. Mamin[a], C. T. Rettner[a], and D. Rugar[a,1]

Proc. Natl Acad. Sci. USA ***106*** **,**1313 (2009).

Abstract:

We have combined ultrasensitive magnetic resonance force microscopy (MRFM) with 3D image reconstruction to achieve magnetic resonance imaging (MRI) with resolution <10 nm. The image reconstruction converts measured magnetic force data into a 3D map of nuclear spin density, taking advantage of the unique characteristics of the "resonant slice" that is projected outward from a nanoscale magnetic tip. The basic principles are demonstrated by imaging the 1H spin density within individual tobacco mosaic virus particles sitting on a nanometer-thick layer of adsorbed hydrocarbons. This result, which represents a 100 millionfold improvement in volume resolution over conventional MRI, demonstrates the potential of MRFM as a tool for 3D, elementally selective imaging on the nanometer scale.

Review article: M. Poggio and C. L. Degen, "Force-detected nuclear magnetic resonance: recent advances and future challenges", Nanotechnology **21**, 342001 (2010).

Future directions

- Optimal control in open quantum systems.
- Quantum error correction for continuously detected errors in circuit cavity QED systems.
- Quantum measurements by superconducting bifurcation Josephson amplifier.
- Non-Markovian electron transport properties in nano-structures (quantum dots, superconducting devices)
- Two-time correlation functions of system operators in non-Markovian open systems.
- Conditional counting statistics in interacting nano-structure devices.
- Device modeling for quantum computing architectures
- ….

No cloning theorem

An Unknown Quantum State Cannot Be Cloned.

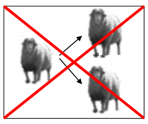
沒有一個可複製任意未知量子狀態的量子複印機存在

<Proof> **Zurek, Wootters (82)**

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

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

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



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

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

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

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

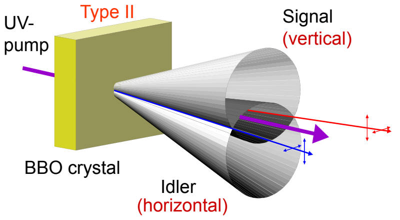
$$|+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right),\ |-\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$$

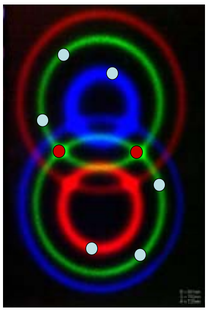
Entanglement Source - SPDC

Spontaneous parametric down conversion

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

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



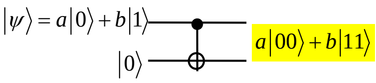


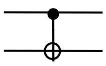
$$|\Psi\rangle_{12} = \frac{1}{\sqrt{2}}(|H\rangle_1|V\rangle_2 - |V\rangle_1|H\rangle_2)$$

Kwiat et al, PRL 75, 4337 (1995)

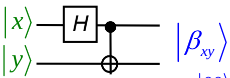
Entanglement is in the air…

Bell States / EPR States / EPR Pairs





CNOT gate



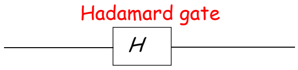
$|00\rangle$ $\quad |\Phi^+\rangle = |\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$

$|01\rangle$ $\quad |\Psi^+\rangle = |\beta_{01}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$

$|10\rangle$ $\quad |\Phi^-\rangle = |\beta_{10}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$

$|11\rangle$ $\quad |\Psi^-\rangle = |\beta_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$

Hadamard gate

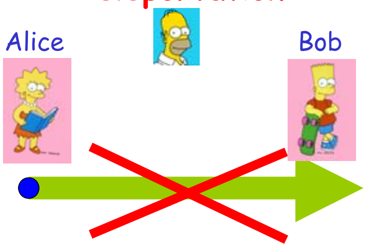


$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}; \quad H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}};$$

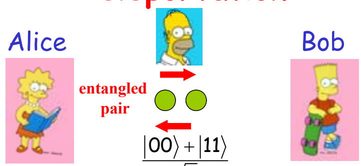
$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Quantum teleportation

Teleportation

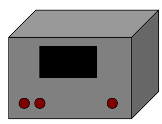


Teleportation



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

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

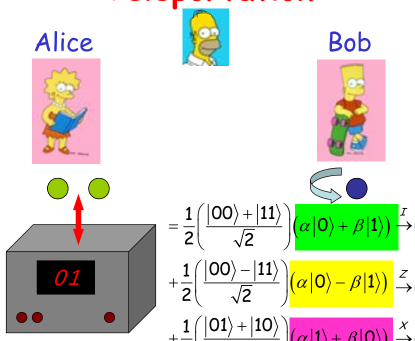


$$(\alpha|0\rangle + \beta|1\rangle)\left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right) = \frac{\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle}{\sqrt{2}}$$

$$|00\rangle = \frac{1}{\sqrt{2}}\left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right) + \frac{1}{\sqrt{2}}\left(\frac{|00\rangle - |11\rangle}{\sqrt{2}}\right) \qquad |10\rangle = \frac{1}{\sqrt{2}}\left(\frac{|01\rangle + |10\rangle}{\sqrt{2}}\right) - \frac{1}{\sqrt{2}}\left(\frac{|01\rangle - |10\rangle}{\sqrt{2}}\right)$$

$$|01\rangle = \frac{1}{\sqrt{2}}\left(\frac{|01\rangle + |10\rangle}{\sqrt{2}}\right) + \frac{1}{\sqrt{2}}\left(\frac{|01\rangle - |10\rangle}{\sqrt{2}}\right) \qquad |11\rangle = \frac{1}{\sqrt{2}}\left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right) - \frac{1}{\sqrt{2}}\left(\frac{|00\rangle - |11\rangle}{\sqrt{2}}\right)$$

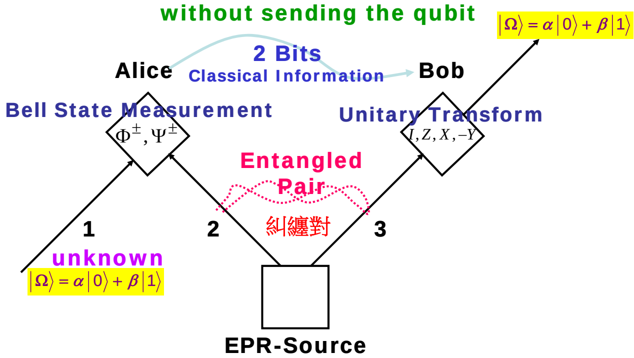
Teleportation



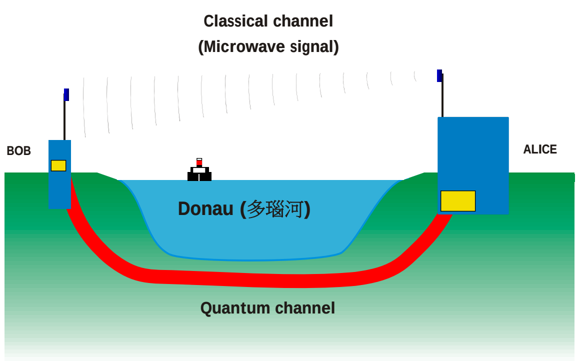
$$= \frac{1}{2}\left(\frac{|00\rangle+|11\rangle}{\sqrt{2}}\right)(\alpha|0\rangle+\beta|1\rangle) \xrightarrow{I} (\alpha|0\rangle+\beta|1\rangle)$$
$$+\frac{1}{2}\left(\frac{|00\rangle-|11\rangle}{\sqrt{2}}\right)(\alpha|0\rangle-\beta|1\rangle) \xrightarrow{Z} (\alpha|0\rangle+\beta|1\rangle)$$
$$+\frac{1}{2}\left(\frac{|01\rangle+|10\rangle}{\sqrt{2}}\right)(\alpha|1\rangle+\beta|0\rangle) \xrightarrow{X} (\alpha|0\rangle+\beta|1\rangle)$$
$$+\frac{1}{2}\left(\frac{|01\rangle-|10\rangle}{\sqrt{2}}\right)(\alpha|1\rangle-\beta|0\rangle) \xrightarrow{ZX} (\alpha|0\rangle+\beta|1\rangle)$$

Quantum Teleportation

Transmit an unknown qubit state without sending the qubit



Long Distance Teleportation



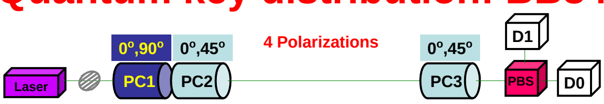
量子密碼學
Quantum Cryptography

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.

Quantum key distribution: BB84



- Alice

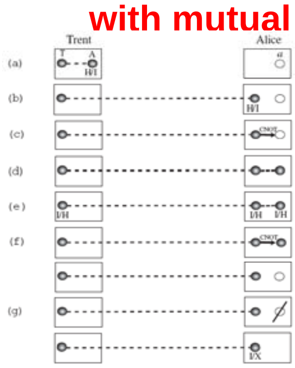
A1	=	0	1	1	0	0	1	0	0	0	0	1	1
A2	=	⊗	⊕	⊗	⊕	⊗	⊕	⊗	⊕	⊗	⊕	⊗	⊕
P	=	↗	↕	↘	↔	↗	↕	↗	↔	↗	↔	↘	↕

- 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 direct communication with mutual authentication



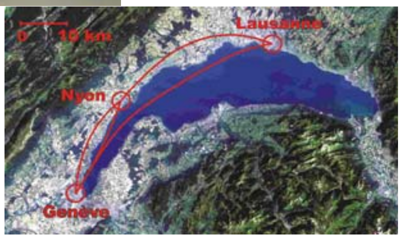
- We propose a new protocol that is capable of achieving secure quantum direct communication with authentication.
- Our quantum protocol introduces a mutual authentication procedure, uses the quantum Bell states, and applies unitary transformations in the authentication process.
- Then it exploits and utilizes the entanglement swapping and local unitary operations in the communication processes.
- Our protocol does not require a direct quantum link between any two users, who want to communicate with each other. This may also be an appealing advantage in the implementation of a practical quantum communication network.

- C.-A. Yen, S.-J. Horng, H.-S. Goan, T.-W. Kao, Y.-H. Chou, Quantum Information and Computation **9**, 0376 (2009).
- C.-A. Yen, S.-J. Horng, H.-S. Goan, T.-W. Kao, Opt. Commun. **283,** 3202 (2010).

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

Gisin, Zbinden, quant-ph/0203118

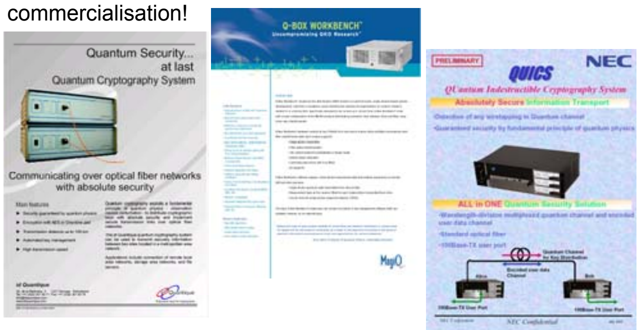
量子金鑰傳輸的商業化產品



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

Commercial available!

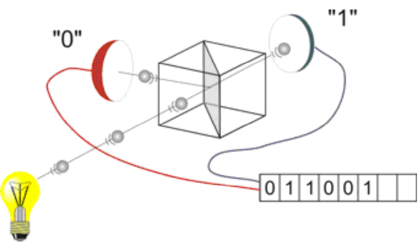
Quantum Cryptography is the most technicaly advanced application of quantum information – on the brink of commercialisation!



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

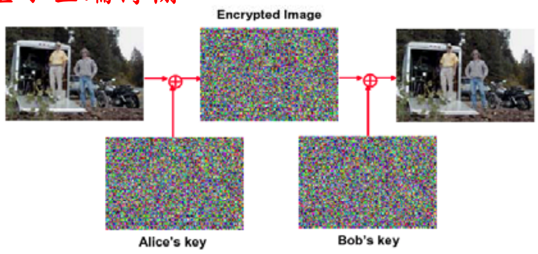


Practical free-space quantum key distribution over 10 km in daylight and at night

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**

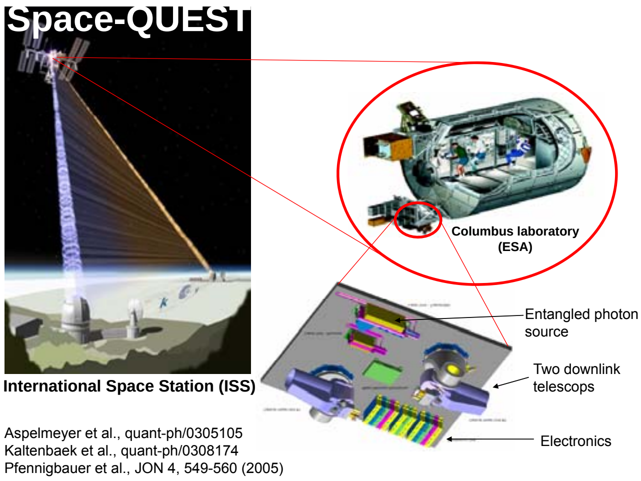


23.4km Qinetiq-MPQ joint free space key exchange trial between Zugspitze and Karwendel

Autumn 2001

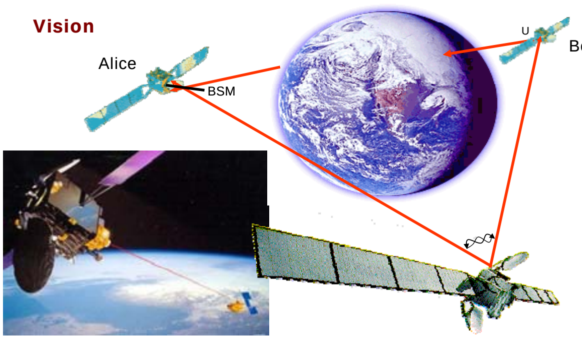
Autumn 2000: Key exchange over 1.9km between Qinetiq site and the local pub!

http://www.eqcspot.org/



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

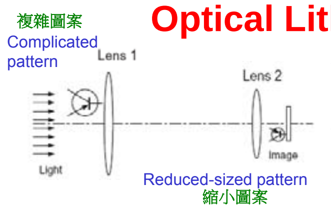
The Future of QKD(量子金鑰傳輸)?



結語

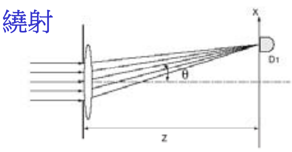
- 量子計算與量子資訊是一門蓬勃發展的新興研究領域。它是以量子力學準則為運算與工作基礎去研究、發現和進而設計出更有效的或更快速的運算與資訊處理方法的新學門。
- 我們介紹了目前科學家們正嘗試去研究製造的幾個量子電腦的設計和最近在量子資訊與通訊上的新進展。
- 雖然大部份這些發展都還在基礎科學的研究階段，可是這些新穎應用的設計提案與實際的實驗努力已帶來令人印象深刻的初步成果。
- 它們在未來能否進而演變成一個嶄新實用的量子科技或量子資訊工程學門也是值得讓人深切期待的。
- 就像60多年前科學家發明電晶體後，不可能知道今天的科技，已可用大量電晶體，做出2萬元有找的筆記型電腦。科學家現在盡力研究量子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

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



Diffraction $\propto \dfrac{\sin^2\beta}{\beta^2}$,

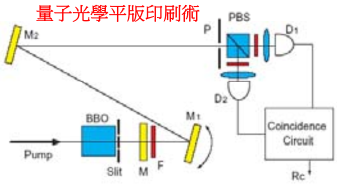
$\beta = (\pi a/\lambda)\sin\theta$.

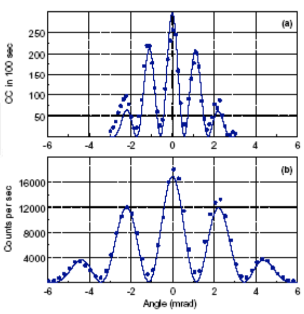
Diffraction limit: minimum width at $\beta = \pi$.

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



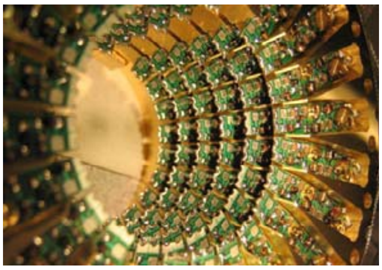


Two-photon pattern has a faster spatial interference modulation and a narrower diffraction pattern width by a factor of 2 than the classical case.

State of the Art

Quantum Algorithms

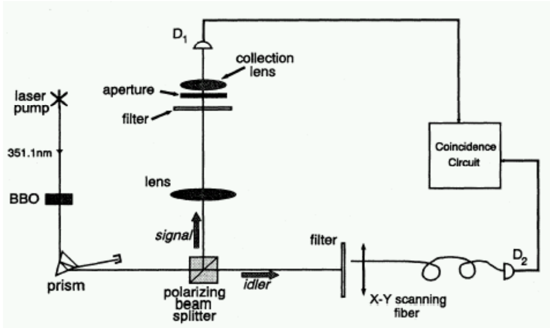
- Factoring, discrete log [Shor 94]
- Unstructured search [Grover 96]
- Various hidden subgroup problems [Long List]
- Pell's equation [Hallgren 02]
- Hidden shift problems [van Dam, Hallgren, Ip 03]
- Graph traversal [CCDFGS 03]
- Spatial search [AA 03, CG 03/04, AKR 04]
- Element distinctness [Ambainis 03]
- Various graph problems [DHHM 04, MSS 03,…]
- Testing matrix multiplication [Buhrman,Špalek 04]
- …



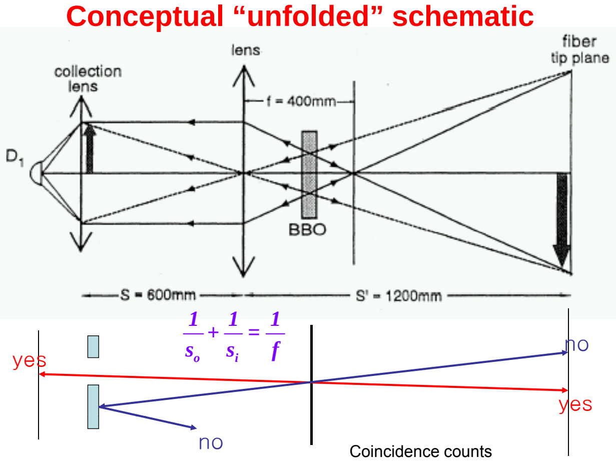
A filter ensures that noise and extraneous signals don't affect the operation of the processor. In Orion, electrical currents come down loops of wire. This creates magnetic fields, which change the behavior of niobium inside the processor. By recording the changes, you get answers to complex computer problems.

"Ghost" imaging by two-photon entanglement

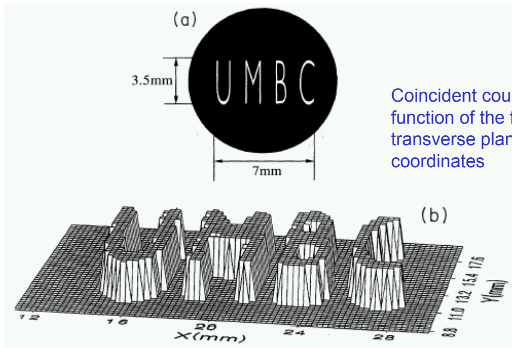
Shih *et al*., PRA52, R3429 (1995).



Conceptual "unfolded" schematic



Quantum imaging



Coincident counts as a function of the fiber tip's transverse plan coordinates

The Measurement of a spatial observable of one photon determines the spatial observable of the other photon with unit probability.

100 Years of the Quantum

M. Tegmark and J.A. Wheeler

Scientific American, Feb., 68 (2001)