Quantum Information Processing

12/08/2005

Quantum Computation - a very quick intro

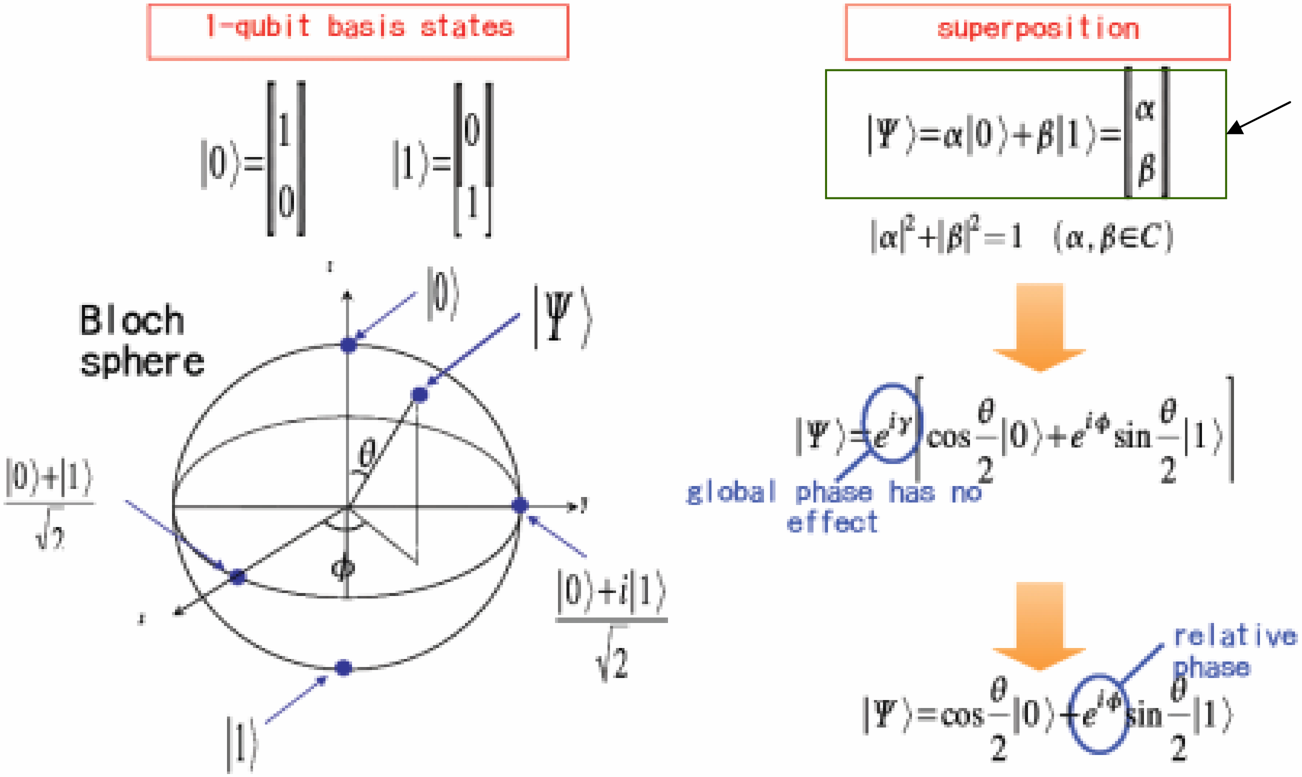
A prime motivation for manipulation of spins in semiconductors is to perform quantum information processsing.

What is quantum computation?

Using the quantum properties of quantum-bits (qubits) to perform calculations more rapidly (in principle) than is possible with classical computers.

http://qist.lanl.gov/ = New Roadmap for QIP.

Superposition and qubits



$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

$|0\rangle$ $|\Psi\rangle$ θ ϕ $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ $\frac{|0\rangle+i|1\rangle}{\sqrt{2}}$ $|1\rangle$

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

$$|\alpha|^2 + |\beta|^2 = 1 \quad (\alpha, \beta \in C)$$

$$|\Psi\rangle = e^{i\gamma}\left[\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle\right]$$

$$|\Psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$$

Quantum bit
qubit

A superposition of the two states (a qubit) can be represented by a point on the Bloch sphere.

A two-level quantum system can be used in practice as a qubit if

1. It can be prepared in a well-defined state, such as |0>, the reference state.

2. Any state of the qubit can be transformed into any other state. Such transformations are carried out by means of unitary transformations.

3. The qubit state can be measured in the computational basis {|0>, |1>}. (α, β can be determined).

A unitary transformation (matrix) $U^H U = U U^H = I$

$U^{-1}=U^H$, ie, unitary transformation is always reversible and no information is lost (information lost to the environment -> decoherence).

example

A generic unitary operator:

$$U_\theta \equiv \begin{pmatrix} \cos(\theta/2) & \sin(\theta/2) \\ -\sin(\theta/2) & \cos(\theta/2) \end{pmatrix}$$

U_π inverts a qubit (up to a phase):

$$U_\pi \equiv \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

$$U_\pi|0\rangle \equiv \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |1\rangle \qquad U_\pi|1\rangle \equiv \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = -\begin{pmatrix} 0 \\ 1 \end{pmatrix} = -|0\rangle$$

$U_{\pi/2}$ produces a superposition:

$$U_{\pi/2}|0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$$

What can this do for us?

Imagine a string of *N* qubits, starting out in |0000…>.

Use the state of each qubit to represent a binary number, a_i.

Now apply the linear operator $U_{\theta i}$ to each qubit in this state.
Result:

$$\frac{1}{\sqrt{2^N}}\sum_{i=0}^{N-1}\left|a_i\right\rangle$$

We've now prepared the qubits in a *superposition* of all their possible values!

From a *linear* number of operations *N*, we've produced a superposition with an *exponentially* large number of terms, 2^N.

What can this do for us?

Now suppose we had two such strings.
Suppose we had an operator ***O*** that, when operating on a string *a* returned a particular function *f*(*a*).
That is,

$$\mathrm{O}\left|a;0\right\rangle \rightarrow \left|a; f(a)\right\rangle$$

Consider applying this operator to our big superposition:

$$\mathrm{O}\frac{1}{\sqrt{2^N}}\sum_{i=0}^{N-1}\left|a_i;0\right\rangle \rightarrow \frac{1}{\sqrt{2^N}}\sum_{i=0}^{N-1}\left|a; f(a_i)\right\rangle$$

Now with a *single* operation we've computed *f*(*a*) for all possible states of the N qubits.

That's the crux of quantum computation! Because of this kind of "quantum parallelism", it's possible to do certain computations much faster than with classical computers.

Universal gates

Universal classical computation:
Any function can be constructed from the elementary gates AND, OR, NOT, and FANOUT, which constitute a universal set of gates for classical computation.

Universal quantum computation:
Each unitary transformation acting on a many-qubit system can be decomposed into gates acting on a single qubit and a single gate acting on two qubits, eg, CNOT gate.

Controlled-NOT

$$\left|x\right\rangle\left|y\right\rangle \to \left|x\right\rangle\left|x\oplus y\right\rangle$$

x, y = 1,0
$\oplus$ addition modulo 2 (XOR)

x=0, y=y
X=1, y=1-y

What kinds of applications?

There are already quantum algorithms (well-defined series of operations) for:

- Factoring large numbers (Peter Schor) exponential speedup compared to classical computers.
(O(n^2log$n$log$n$) vs. exp(O($n^{1/3}$(log$n$)$^{2/3}$))

- Searching databases (Lov Grover). Quadratic speedup compared to classical computers
$O(\sqrt{N})$ vs. O(N)

We need 50-1000 qubits to perform tasks inaccessible to the classical computer.

What kinds of applications?

Dissipationless.
Unitary transformation is reversible.
In contrary, each classical operation will dissipate at least an amount of energy k_BTln2 (actual computers consumes orders of magnitudes more).

(secure) transmission of information.
Entanglement provides operations *inaccessible* to classical means. Quantum cryptography and teleportation.

Why is it hard to make a quantum computer?

- One needs to be able to go in and couple qubits together great precision, almost arbitrarily.

- How can one manipulate one particular qubit without accidentally decohering the entire system?

- System must be isolated from the environment so that coherence times are long compared to operation times.

- One really wants to do this in a way that’s *scaleable*.

DiVincenzo, 2001

General requirements for a quantum computer

1. a scalable system of well-defined qubits
2. a method to reliably initialize the quantum system
3. long coherence times
4. existence of universal gates
5. an efficient measurement scheme

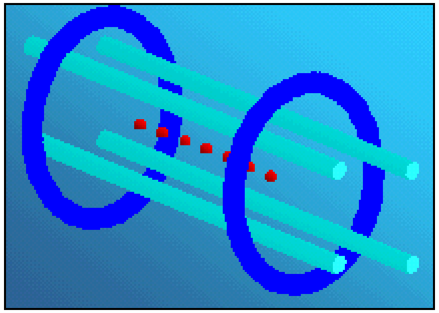
How are people trying to implement QIP?

Several approaches:

- Optical trapping / manipulation of atoms and ions
- NMR (liquid, solids)
- Superconducting qubits
- Optical systems
- Quantum dots

Everyone would love to do this in the solid state, because it would scale well and interface with existing technology….

Ion traps

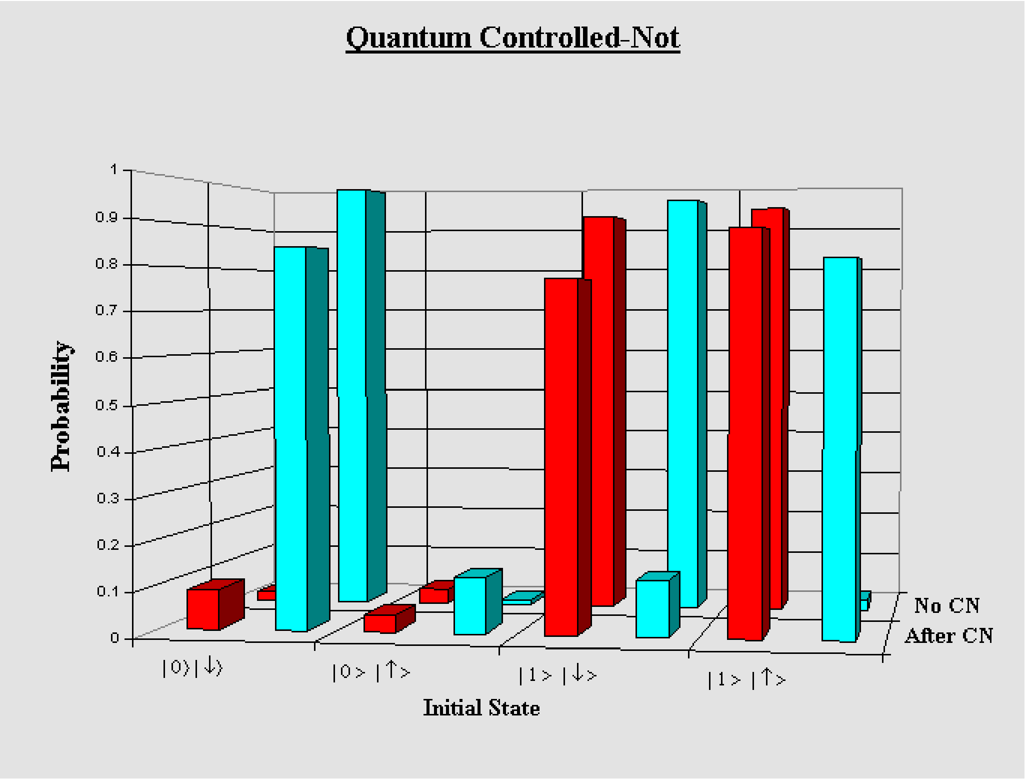


Ions trapped by linear and oscillating electric fields

Qubits:

1) Two ground state hyperfine levels (these are called "hyperfine qubits")
2) A ground state level and an excited level (these are called the "optical qubits")

Qubit preparation through obsorption rules of EM signals.



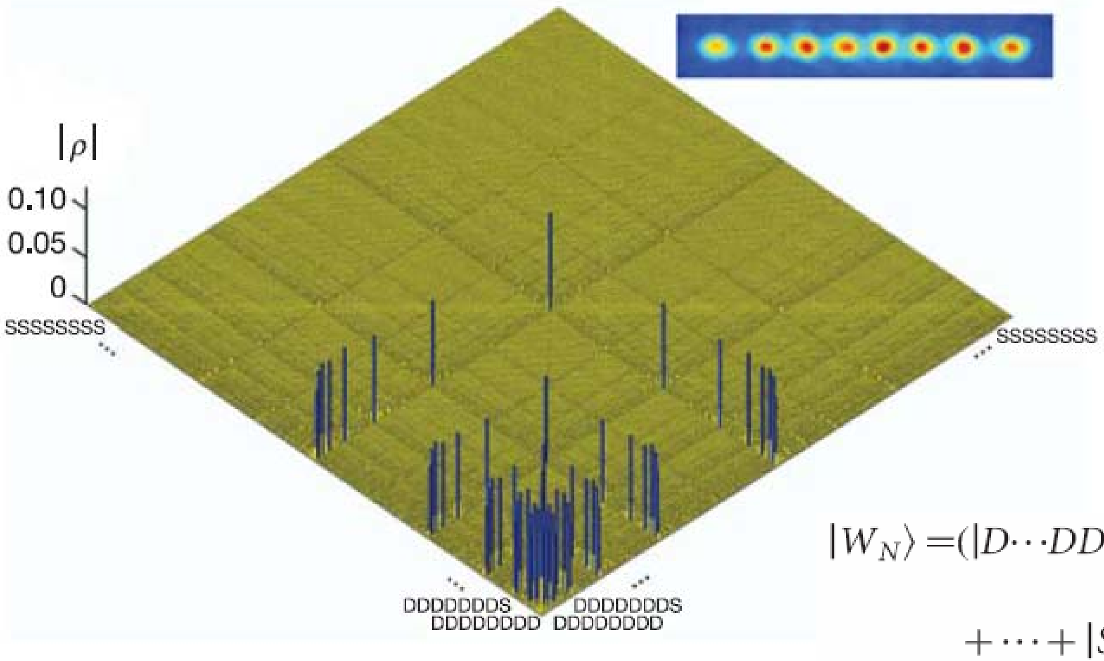
Qubit coupling through excitement of collective motion of the ions with laser beam
Communication via “head” ions

Monroe group, U-M Department of Physics and the FOCUS Ultrafast Optics Center
NIST

Ion trap qubits

Haffner *et al.*, Nature **438**, 643 (2005)

Recent advances suggest that ion traps may work very well!
Should have no fundamental limits, but still very technically challenging.



$$|W_N\rangle = (|D\cdots DDS\rangle + |D\cdots DSD\rangle + |D\cdots DSDD\rangle + \cdots + |SD\cdots D\rangle)/\sqrt{N}$$

NMR

Qubits: nuclear spins
Two qubit operation: indirect exchange mediated by carriers.

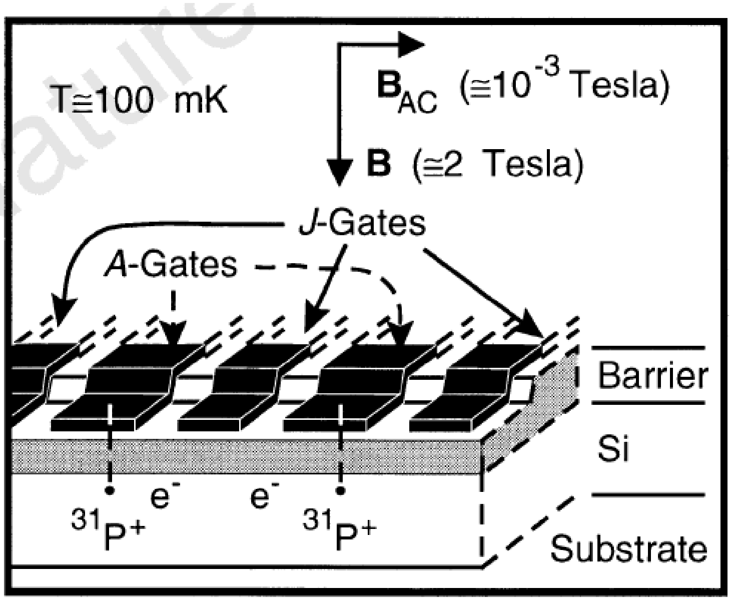
Problem: you don’t really have pure quantum states.
Solution: with 10^{22} qubits, you can fudge things and have *effective* pure states.
Larmor frequency for each qubit will be different due to screening of the environment.

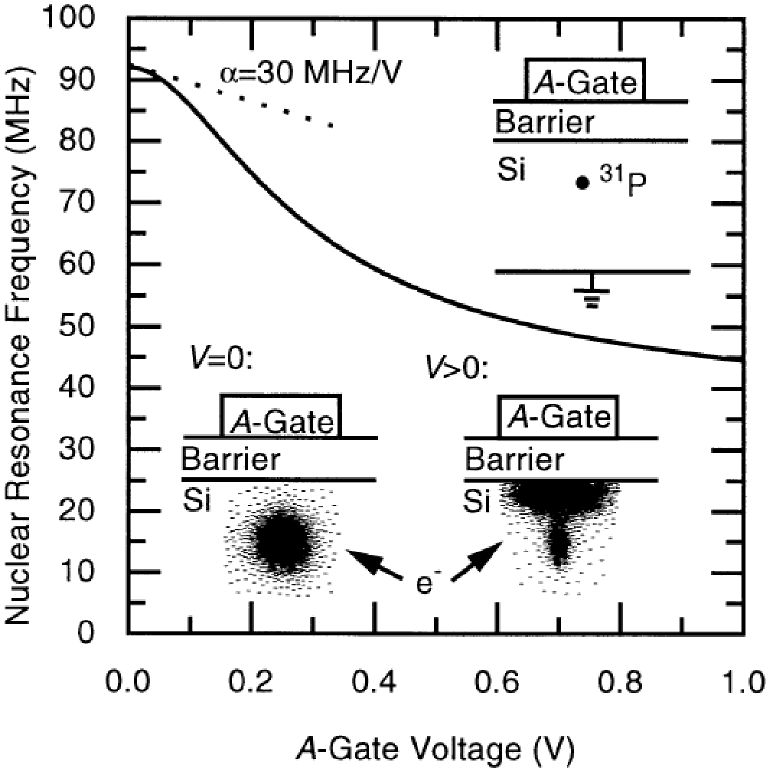
Ex: investigators at MIT have used 13 nuclear spins in a molecule to factor the number 15 = 5 x 3.

NMR in molecules does *not* scale well:
Individual chemical shifts of NMR frequencies are too limited -
can’t individually flip 8456th spin out of 10000, for example.

NMR hybrid - solid state possibility

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



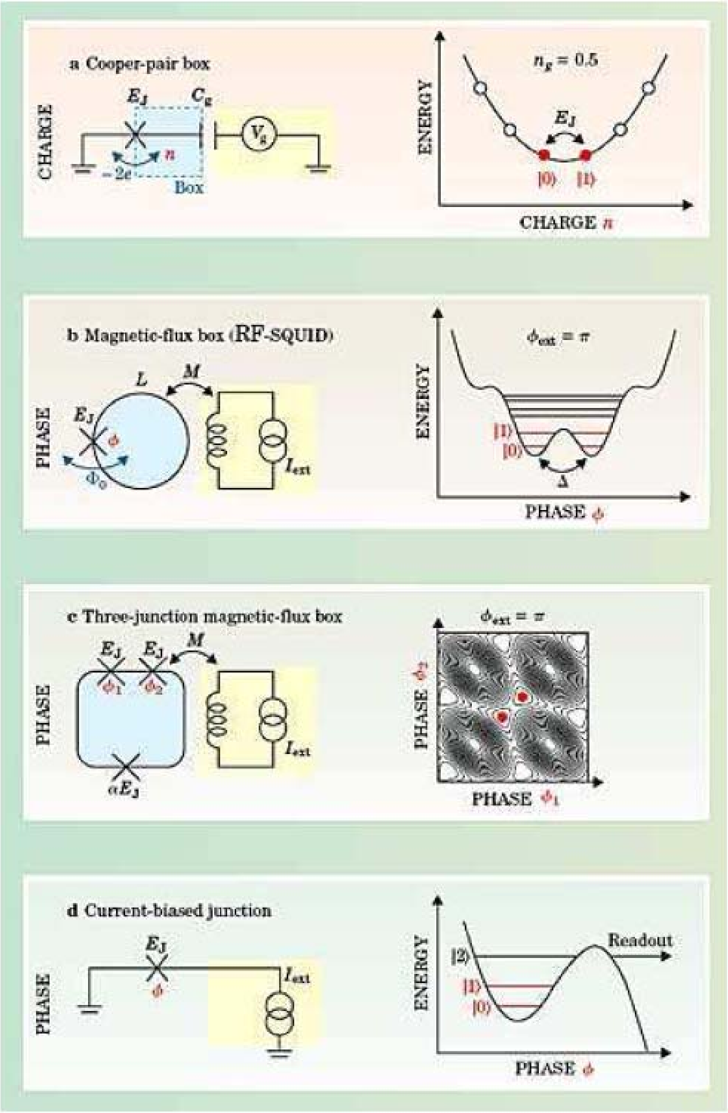


- Use P dopants in **Si** as qubits.
- Big hyperfine + Stark effects = dialable NMR frequencies (controlled by A gates) to address individual qubits.
- Exchange coupling controlled by J gates.
- Could be read out electrostatically….

Challenge: Uniformly place and locate individual dopants, fabrication.

Superconducting qubits

Physics Today, November 2005



Several groups trying to use superconducting structures as qubits.

Possible qubits include charge based (“Cooper pair box”), fluxbased, and Josephson phase based.

Readout, manipulation all use nanofab. SQUIDs and SETs….

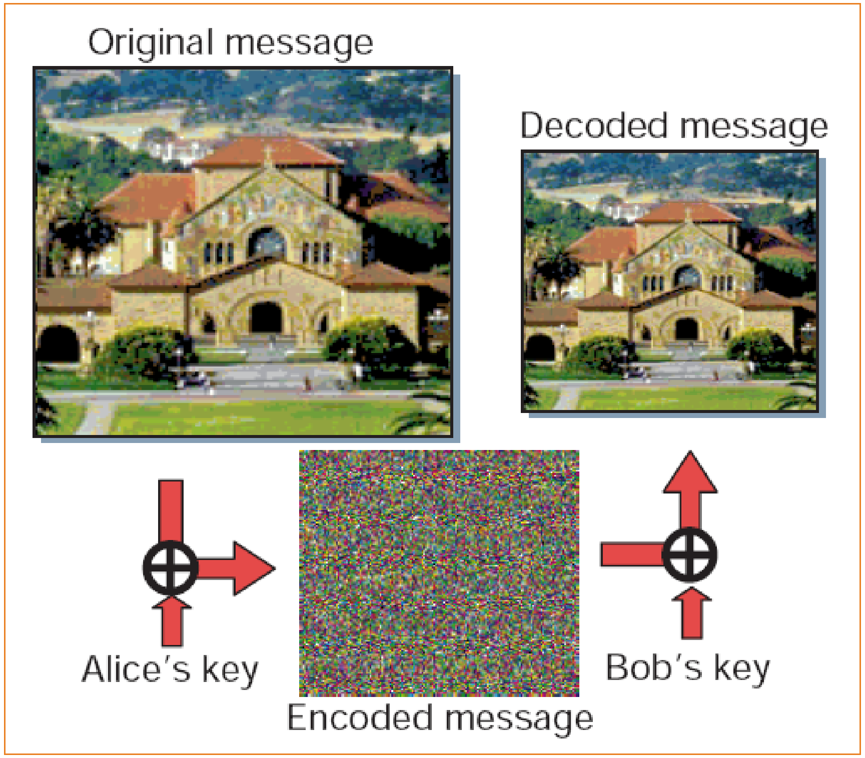
Optical systems:

Yamamoto group, Stanford

Wakes, *Nature* **420**, 762 (2002)

Qubits: two optical modes of a single photon (single photon sources needed)

Two qubit operation: normally mediated by atoms in a non-linear medium, difficult.

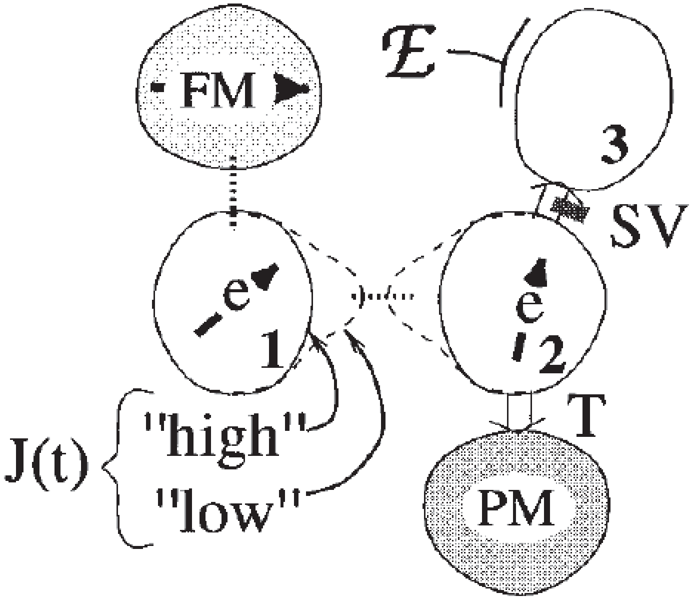


Useful in quantum communication. Long distance communication possible via commercial channels, eg, free space, satellites can in principle transmit secure information everywhere in the world.

Quantum dots

Idea of Divincenzo and Loss:

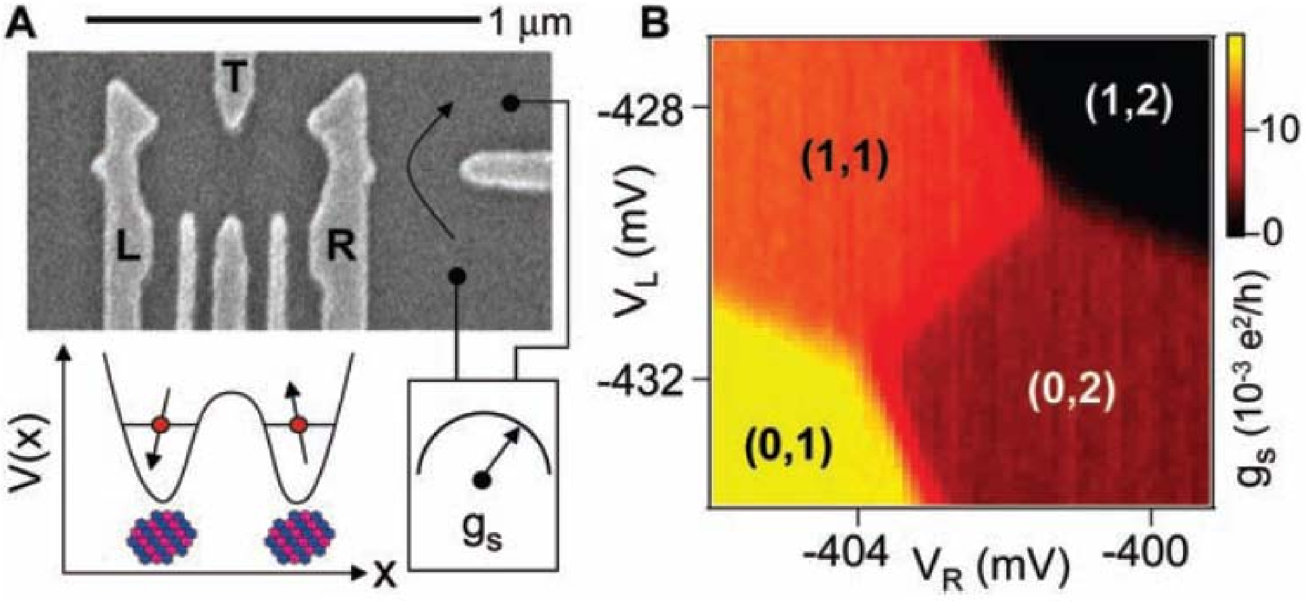
- Qubits: electron spins in individual dots
- Two-qubit operation obtained by exchange coupling between neighboring dots, which is controlled by pulses on the gates to control the barrier height and duration.
- Spin-charge conversion and readout with an SET or QPC.



D. Loss and D. P. DiVincenzo, Phys. Rev. A **57**, 120 (1998).

Petta *et al*., Science **309**, 2180 (2005)

Quantum dots



- gate voltage pulses control charge states of the dots.
- Charge state can be readout with a QPC detector.

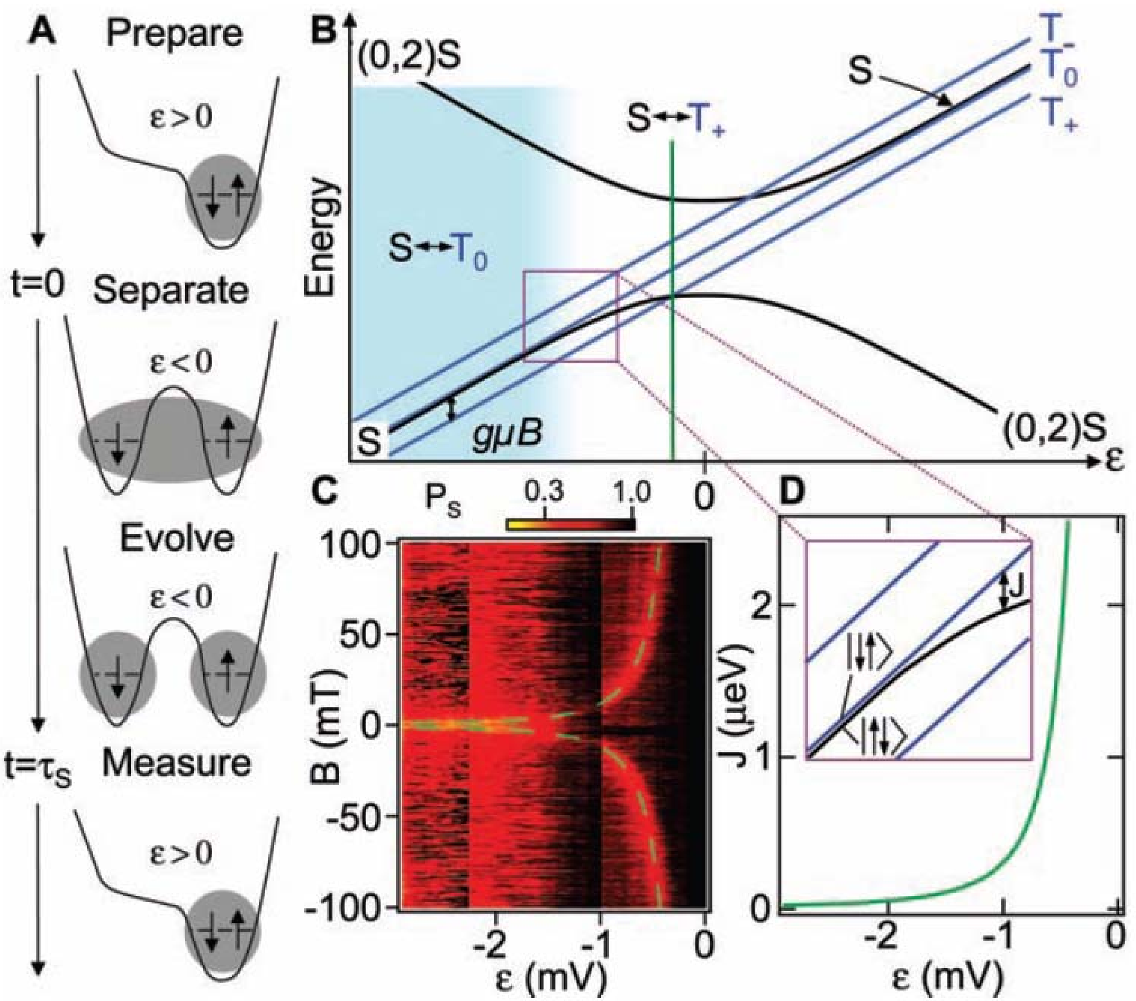
Quantum dots

Petta *et al*., Science **309**, 2180 (2005)

Qubit: (1,1)’s singlet state S and T_0 of the triplet state.

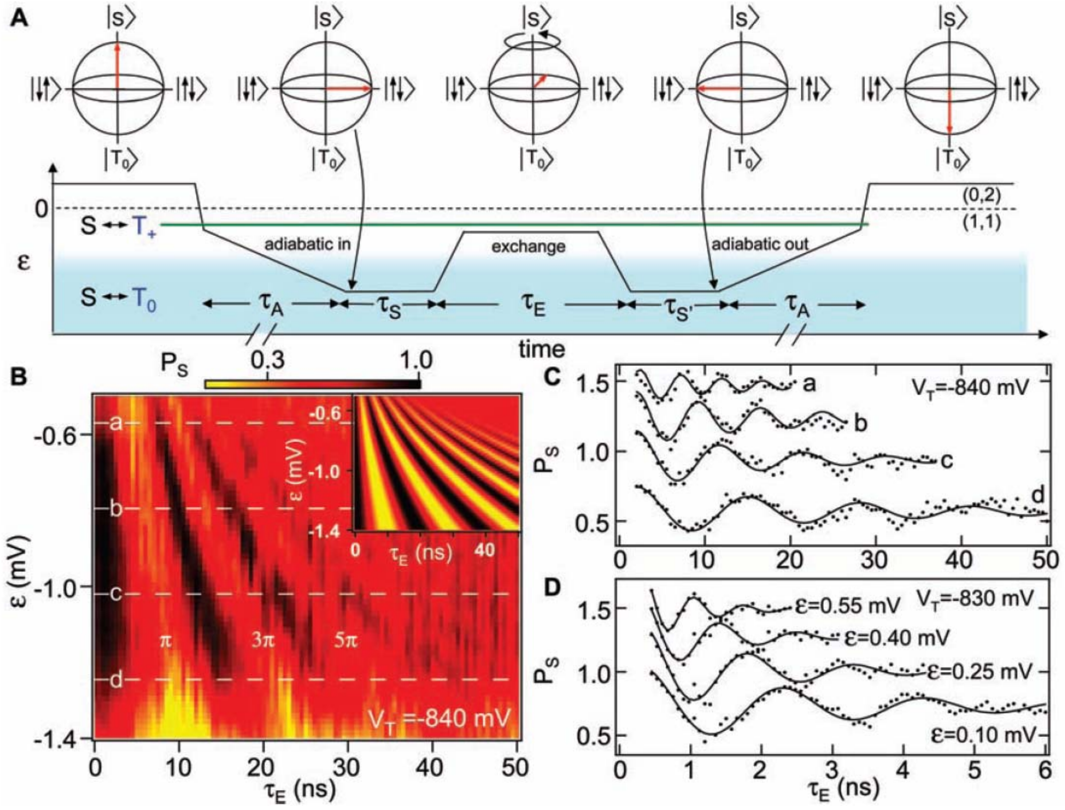
Single qubit operation obtained by controlling the interaction of the two dots.

Final state readout by measuring the (0,2) singlet state, which can only be obtained from the (1,1) singlet state.



Quantum dots

Petta *et al*., Science **309**, 2180 (2005)



- unitary operation of a single qubit
- T_2*~10ns, T_2~1μs

Entanglement and quantum communication

Entangled particles are non-interacting but are described by a common wavefunction; consequently, individual particles are not independent of each other and their quantum properties are inextricably interwoven

EPR paradox (Einstein, Podolsky and Rosen, 1935)

Entangled qubits violates special relativity?

Consider spin singlet state $|\psi\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right)$

Alice measures one particle and obtains S_z=-1, then the other particle Bob measures must have S_z=+1, even though A and B can be arbitrarily far apart.

A classical communication must occur for A and B to exchange information, hence special relativity is not violated.

Quantum cryptography

Classical communication can be breached since information can be copied without changing the original message.

Eavesdropping of quantum communication changes the quantum states and will be detected and keyed accordingly.

Quantum teleportation

Quantum information can be sent from Alice to Bob through exchange of classical information and a pair of entangled qubits. (the original copy is destroyed in the process, ie, no cloning is not allowed).
Necessary for communication between different units of a quantum computer.

QIP summary:

- Very intriguing ideas
- Number of possible technologies, technically challenging, not clear if any of them will work well in a practical manner.
- Progress has been much more rapid than people had imagined, particularly in the superconducting qubits and semiconductor quantum dot approaches.
- Many implementations would depend critically on nanofabrication and nanotechnology.

Concluding remarks:

In depth discussion in EECS521

Moor’s law: alive and well until 2015-2020?

Si technology: scaling rules, high-k, metal gate, strain Si

III-V materials. Lighter effective mass -> higher mobility
Quantum wells structure to further enhance mobility and speed.

Ballistic transistors. Dissipationless inside the channel.
Quantum contact resistance. Current saturation due to
velocity saturation.

Single electron devices: Coulomb blockade phenomena.
high density, low power devices.

Concluding remarks:

Nanotube devices: small size, 1d system, ballistic transistor,

Nanowire devices: small, clean system,
special applications, sensors, solar cells, hybrid devices?

Molecular electronics: smallest size, enormous parallel production potential

Spin based electronics: extra degree of freedom to carry informatipon,
pure spin current - no power dissipation,

Quantum computation: parallelism, dissipationless
tasks inaccessible to classical computers:
large number factoring, database searching
Quantum communication.