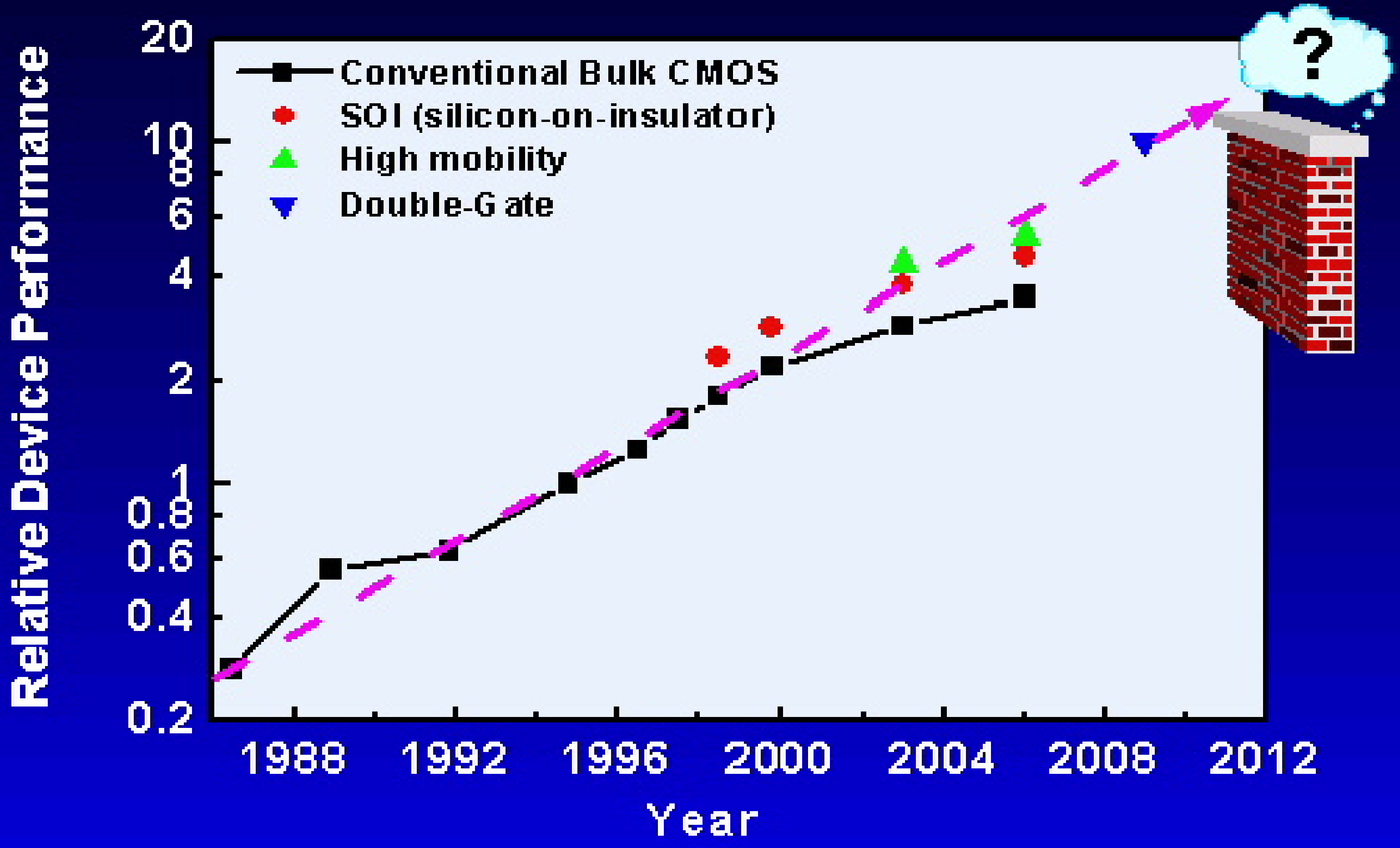
Prospects for Quantum Computation

David DiVincenzo, IBM

NIST, 4/2004

CMOS Device Performance

New device structures are needed to maintain performance…



Back to basics…

Fundamental carrier of information: the **bit**

Possible bit states:

“0” or **“1”**

Fundamental carrier of quantum information: the **qubit**

Possible qubit states: any **superposition** described by the **wavefunction**

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

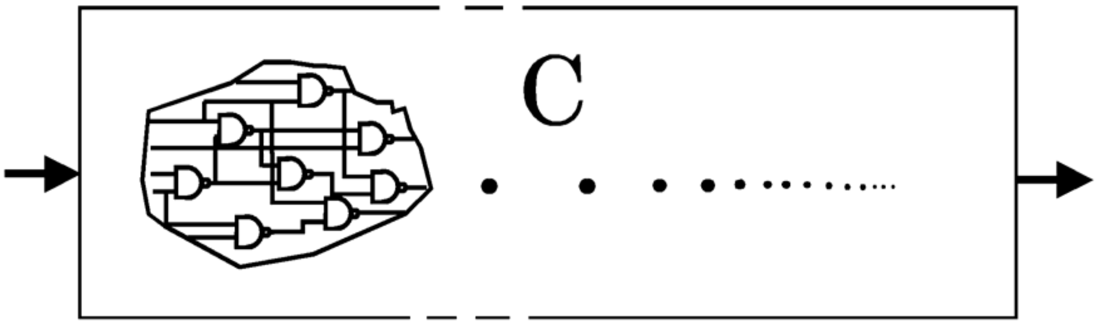
Fast Quantum Computation

P. Shor, AT&T, 1994

Classical factoring problem required 8 months on hundreds of computers

RSA 129

1143816257578888676
6923577997614661201
0218296721242362562
5618429357069352457
3389783059712356395
8705058989075147599
290026879543541



Factors

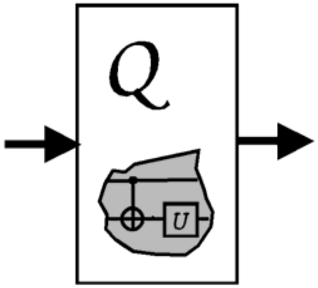
3490529510847650949
1478496199038981334
1776463849338784399
0820577

x

3276913299326670954
9961988190834461413
1776429679929425397
98288533

Same Input and Output, but Quantum processing of intermediate data gives

1143816257578888676
6923577997614661201
0218296721242362562
5618429357069352457
3389783059712356395
8705058989075147599
290026879543541



3490529510847650949
1478496199038981334
1776463849338784399
0820577

x

3276913299326670954
9961988190834461413
1776429679929425397
98288533

Exponential speedup
for Factoring

Quadratic speedup
for Search

Why we want quantum computing:

Prime factorization (Shor, 1994)	$p_1 p_2 = N$	$\exp\left(n^{1/3}\right) \rightarrow poly(n)$
Pell's equation (Hallgren, 2002)	$x^2 - dy^2 = N$	$\exp\left(n^{1/2}\right) \rightarrow poly(n)$

and also:

- Grover search – appointment scheduling
- period finding – group theory computations
- Gauss sums
- shifted Legendre symbol problem
- quantum simulation
- Raz algorithm – distributed simulation
- sampling complexity: disjoint subsets
- finite-round interactive proofs
- pseudo-telepathy (Bell inequalities, game playing)
- quantum cryptography
- quantum data hiding & secret sharing
- quantum digital signature

(BUT, some computations are not sped up at all!)

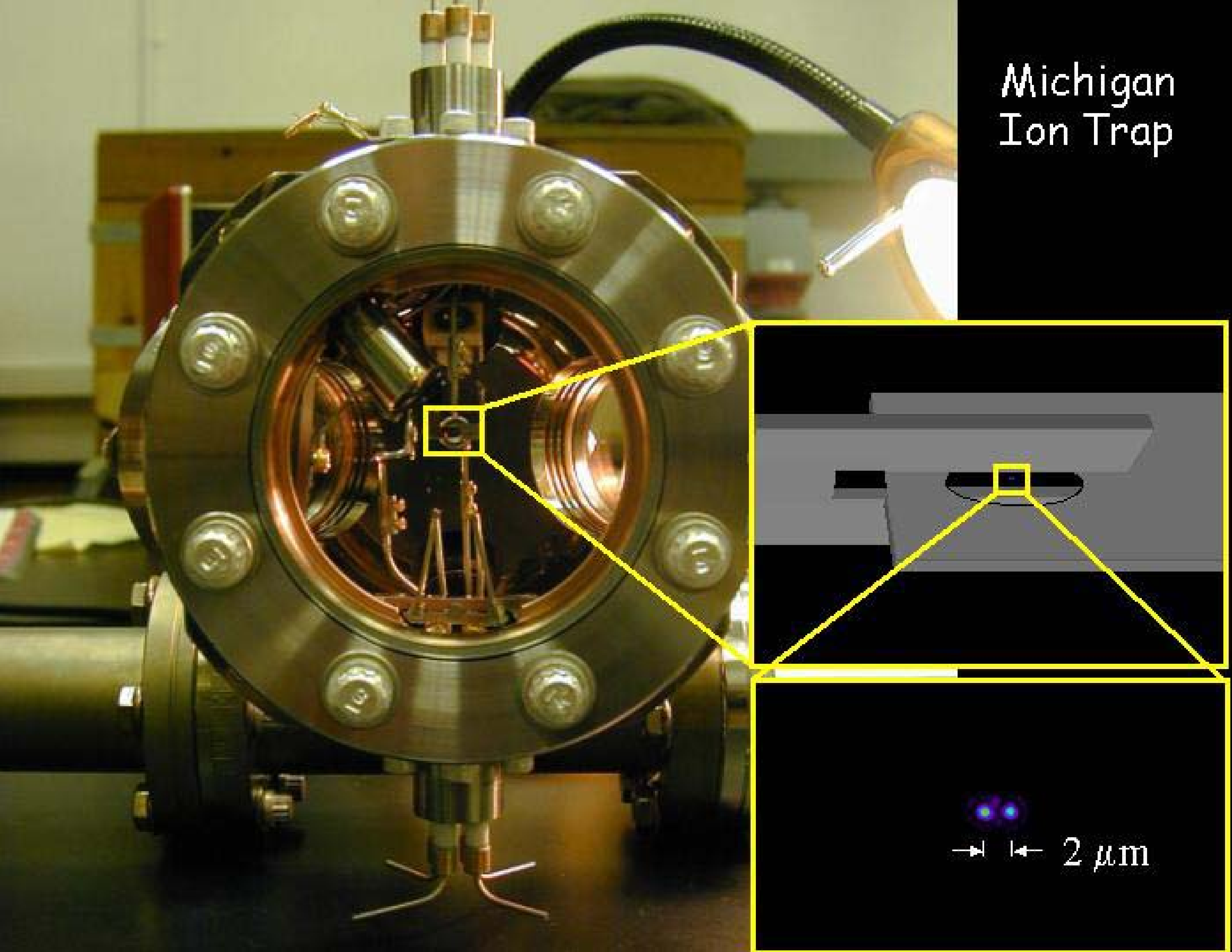
See DiVincenzo & Loss, cond-mat/9901137

(list almost unchanged for some years)

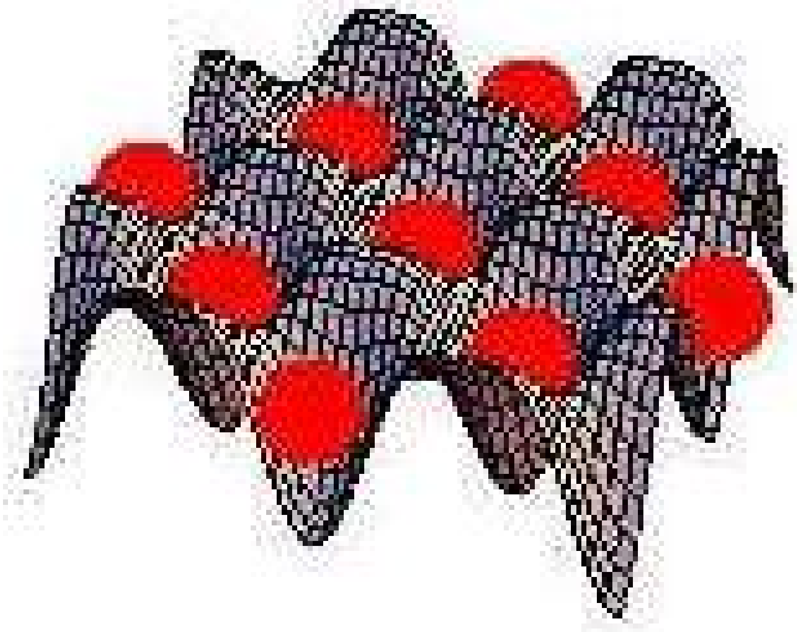
Physical systems actively considered for quantum computer implementation

- **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**
- **Spin spectroscopies, impurities in semiconductors & fullerines**
- **Coupled quantum dots**
  - **Qubits: spin,charge,excitons**
  - **Exchange coupled, cavity coupled**

Michigan Ion Trap

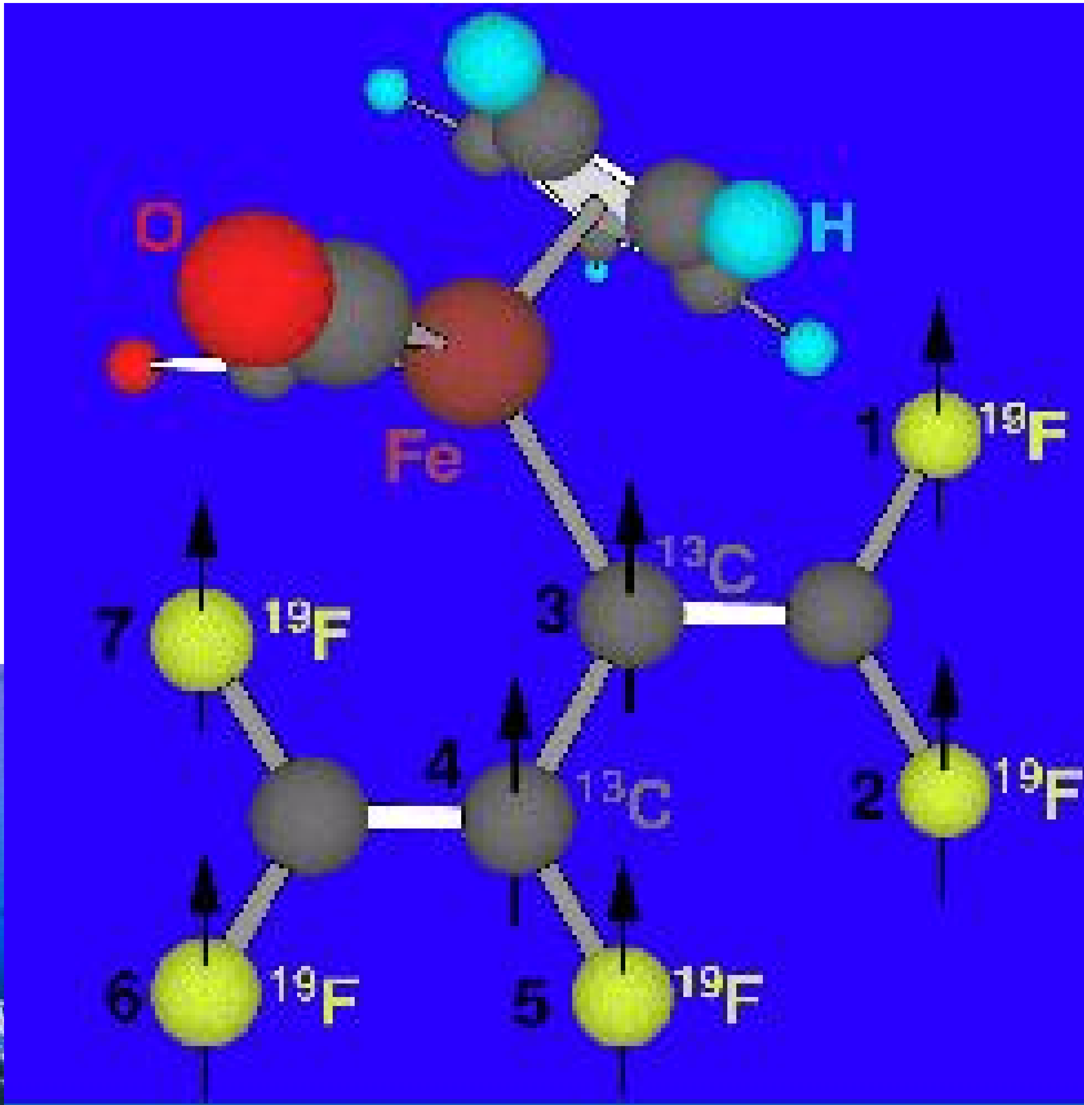


Proposed optical lattice quantum computer



- Ivan Deutsch/University of New Mexico
- **Laser egg carton.** Interfering laser beams can hold atoms in a precise array. In this arrangement, the atoms could form the basis for a quantum computer.

NMR quantum computer –
7 qubit operation



Five criteria for physical implementation of a quantum computer

1. Well defined extendible qubit array -stable memory
2. Preparable in the “000…” state
3. Long decoherence time (>10^4 operation time)
4. Universal set of gate operations
5. Single-quantum measurements

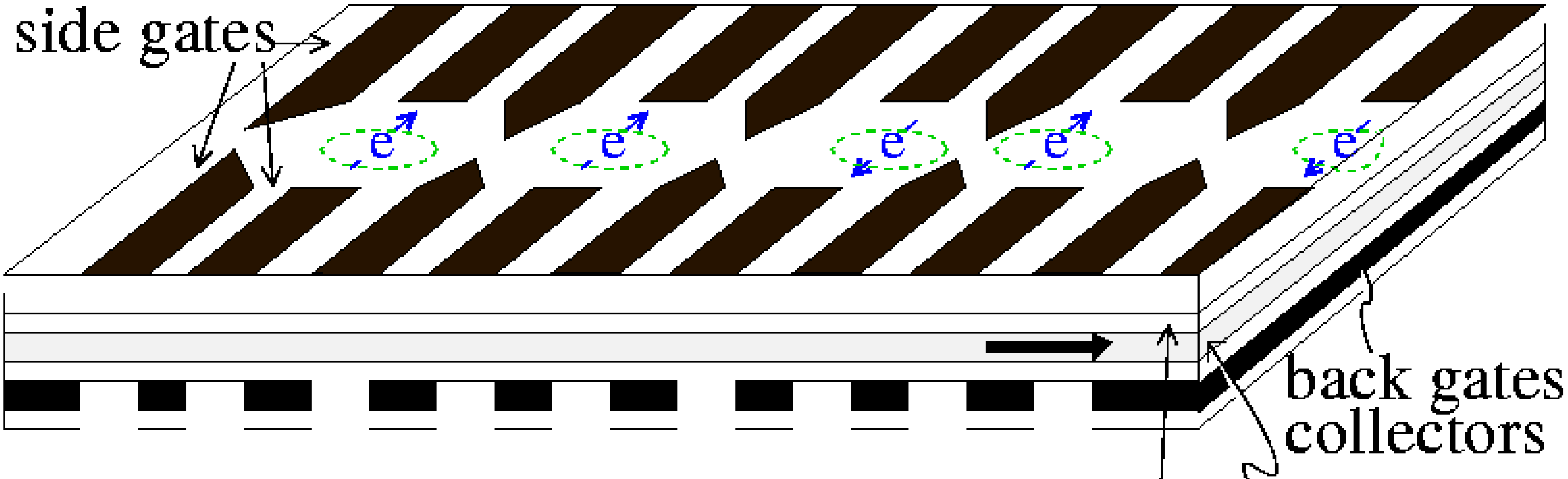
D. P. DiVincenzo, in Mesoscopic Electron Transport, eds. Sohn, Kowenhoven, Schoen (Kluwer 1997), p. 657, cond-mat/9612126; “The Physical Implementation of Quantum Computation,” Fort. der Physik 48, 771 (2000), quant-ph/0002077.

Five criteria for physical implementation of a quantum computer
& quantum communications

1. Well defined extendible qubit array -stable memory
2. Preparable in the “000…” state
3. Long decoherence time (>10^4 operation time)
4. Universal set of gate operations
5. Single-quantum measurements
6. Interconvert stationary and flying qubits
7. Transmit flying qubits from place to place

Quantum–dot array proposal:

Loss & DiVincenzo, Phys. Rev. A 57, 120 (1998).

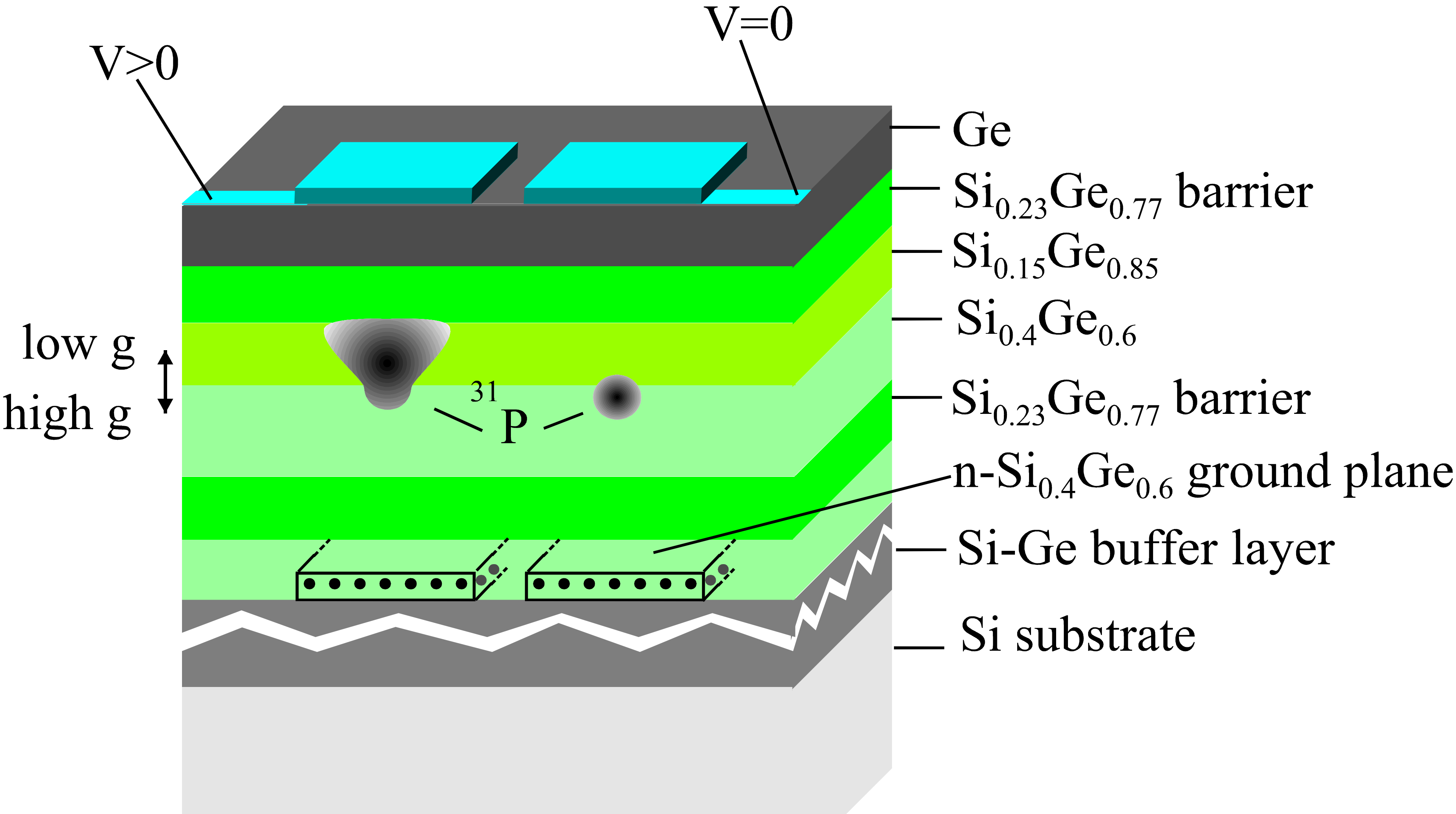


- –quantum dots defined in 2DEG by side gates
- –Coulomb blockade used to fix electron number at one per dot
- –spin of electron is qubit
- –gate operations: controllable coupling of dots by point–contact gate voltage
- –readout by gatable magnetic barrier

Kane (1998) →

Concept device: spin-resonance transistor

R. Vrijen et al, Phys. Rev. A 62, 012306 (2000)



5. Measurement requirement

- Ideal quantum measurement for quantum computing:

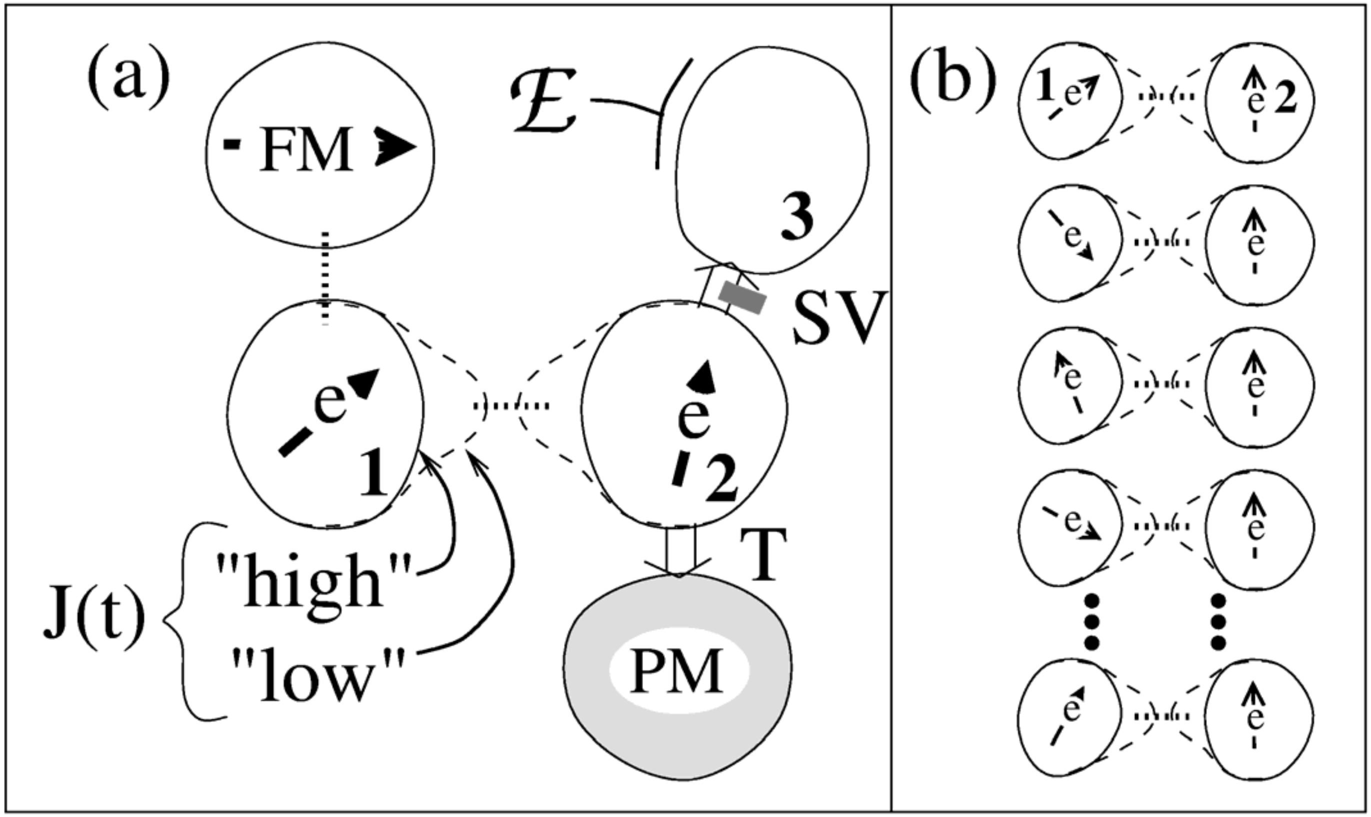
For the selected qubit:

if its state is $|0\rangle$, the classical outcome is always **"0"**

if its state is $|1\rangle$, the classical outcome is always **"1"**

(100% quantum efficiency)

- If quantum efficiency is not perfect but still large (●50%), desired measurement is achieved by "copying" (using cNOT gates) qubit into several others and measuring all.
- If q.e. is very low, quantum computing can still be accomplished using ensemble technique (cf. bulk NMR)
- Fast measurements (10^{-4} of decoherence time) permit easier error correction, but are not necessary



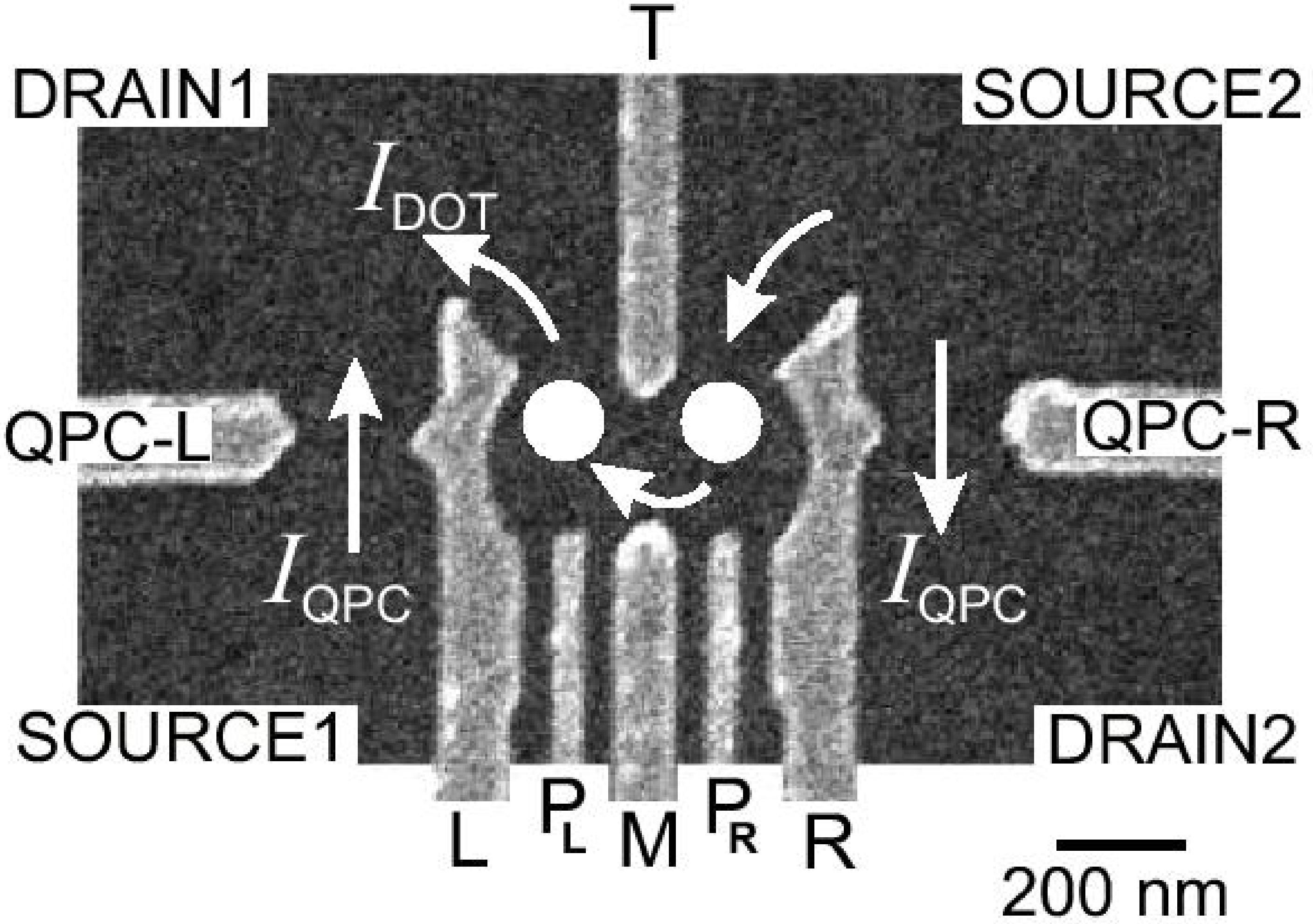
Loss & DiVincenzo
quant-ph/9701055

FIG. 1. a) Schematic top view of two coupled quantum dots labeled 1 and 2, each containing one single excess electron (e) with spin 1/2. The tunnel barrier between the dots can be raised or lowered by setting a gate voltage "high" (solid equipotential contour) or "low" (dashed equipotential contour). In the low state virtual tunneling (dotted line) produces a time-dependent Heisenberg exchange $J(t)$. Hopping to an auxiliary ferromagnetic dot (FM) provides one method of performing single-qubit operations. Tunneling (T) to the paramagnetic dot (PM) can be used as a POV read out with 75% reliability; spin-dependent tunneling (through "spin valve" SV) into dot 3 can lead to spin measurement via an electrometer $\mathcal{E}$. b) Proposed experimental setup for initial test of swap-gate operation in an array of many non-interacting quantum-dot pairs. Left column of dots is initially unpolarized while right one is polarized; this state can be reversed by a swap operation (see Eq. (31)).

Realizing few-electron quantum dots --- 2003, Delft

Few-Electron Quantum Dot Circuit with Integrated Charge Read-Out

J. M. Elzerman,[1] R. Hanson,[1] J. S. Greidanus,[1] L. H. Willems van Beveren,[1] S. De Franceschi,[1] L. M. K. Vandersypen,[1] S. Tarucha,[2,3] and L. P. Kouwenhoven[1]



- text

4. Universal Set of Quantum Gates

- Quantum algorithms are specified as sequences of unitary transformations U_1,U_2, U_3, each acting on a small number of qubits
- Each U is generated by a time-dependent Hamiltonian:

$$U_\alpha = \exp(i\int dt H_\alpha(t)/\hbar)$$

- Different Hamiltonians are needed to generate the desired quantum gates:

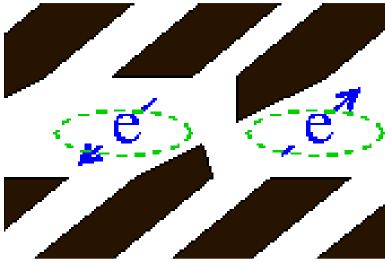
$$cNOT \Rightarrow H \propto \sigma_{zi}\sigma_{zj}$$

$$\text{1-bit gate} \Rightarrow H \propto \sigma_{xi}, \sigma_{yi}$$

- many different “repertoires” possible
- integrated strength of H should be very precise, 1 part in 10^{-4}, from current understanding of error correction

  (but, see topological quantum computing (Kitaev, 1997),
  or computing by teleportation (Knill 2004))

Gate operations with quantum dots (1):



--two-qubit gate:

Use the side gates to move electron positions horizontally, changing the wavefunction overlap

Pauli exclusion principle produces spin-spin interaction:

$$H = JS_1 \cdot S_2 = J(\sigma_{x1}\sigma_{x2} + \sigma_{y1}\sigma_{y2} + \sigma_{z1}\sigma_{z2})$$

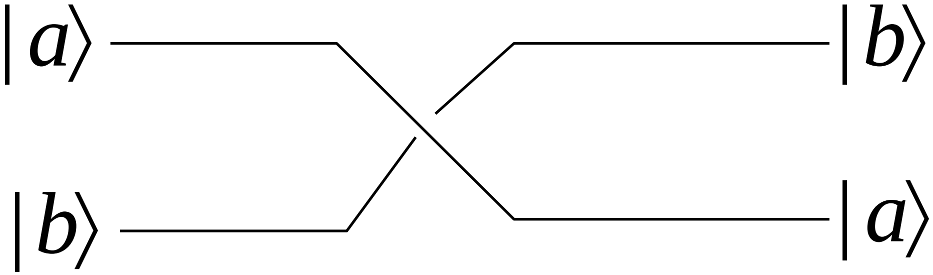
Model calculations (Burkard, Loss, DiVincenzo, PRB, 1999)
For small dots (40nm) give *J*✂*0.1meV*, giving a time for the "square root of swap" of

t✂*40 psec*

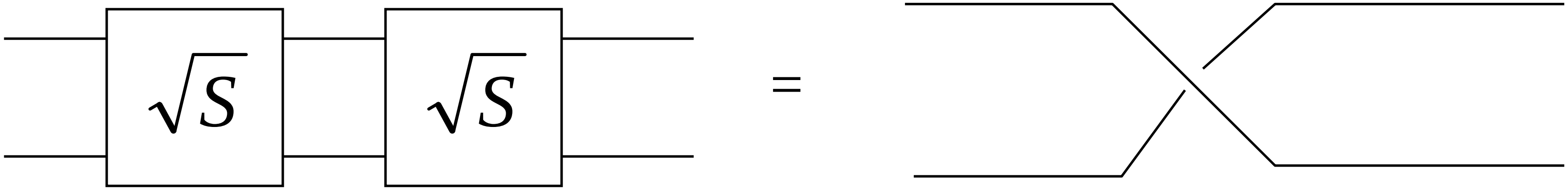
NB: interaction is very short ranged, off state is accurately *H=0*.

Making the CNOT from exchange:

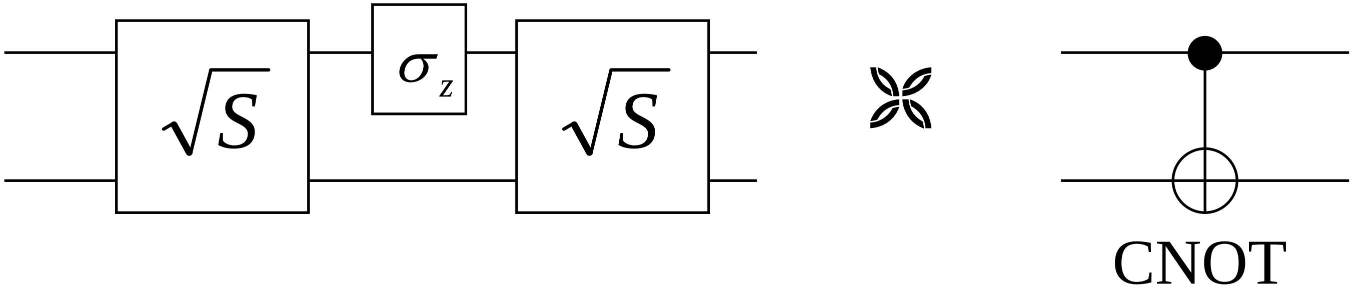
Exchange generates the “SWAP” operation:



More useful is the “square root of swap”, $\sqrt{S}$



Using SWAP:

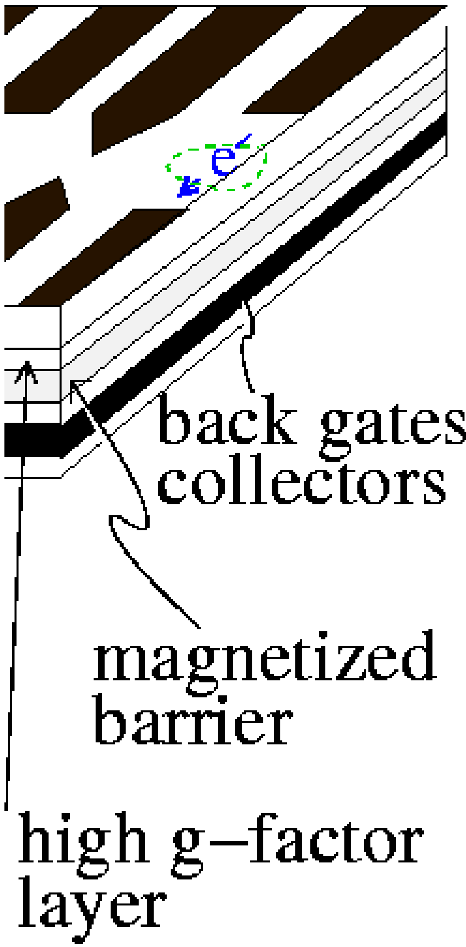


Gate operations with quantum dots (2):

--one-qubit gate:

Desired Hamiltonian is:

$$H = g\mu_B S \cdot B = g\mu_B (B_x\sigma_x + B_y\sigma_y + B_z\sigma_z)$$



One approach: use back gate to move electron vertically. Wavefunction overlap with magnetic or high g-factor layers produces desired Hamiltonian.

If B_{eff}= 1T, *t⌘160 psec*

If B_{eff}= 1mT, ***t⌘160 nsec***

Recent progress – Josephson junction qubit

Manipulating the quantum state of an electrical circuit

Science 296, 886 (2002)

D. Vion, A. Aassime, A. Cottet, P. Joyez, H. Pothier, C. Urbina, D. Esteve and M.H. Devoret

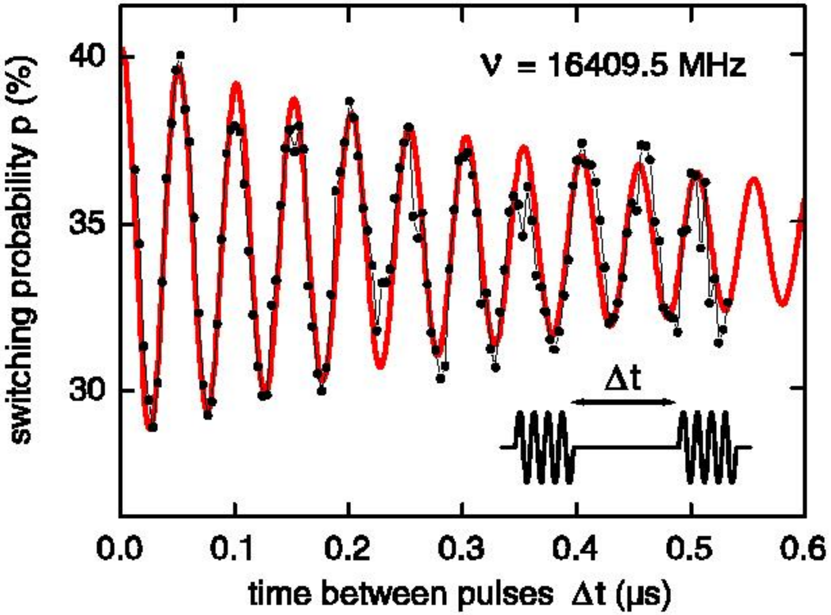
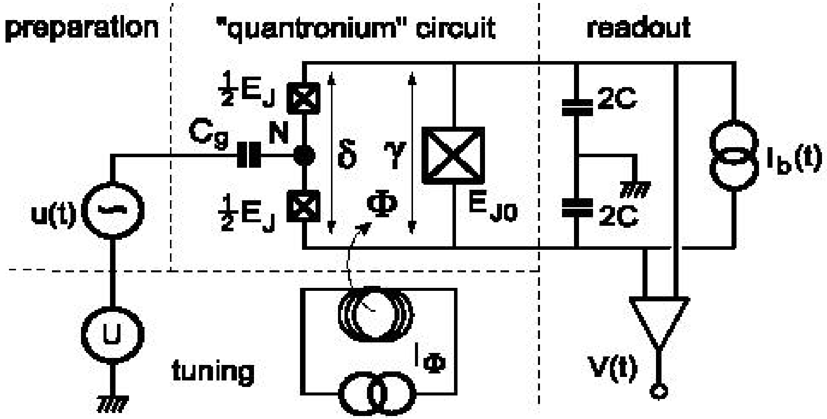
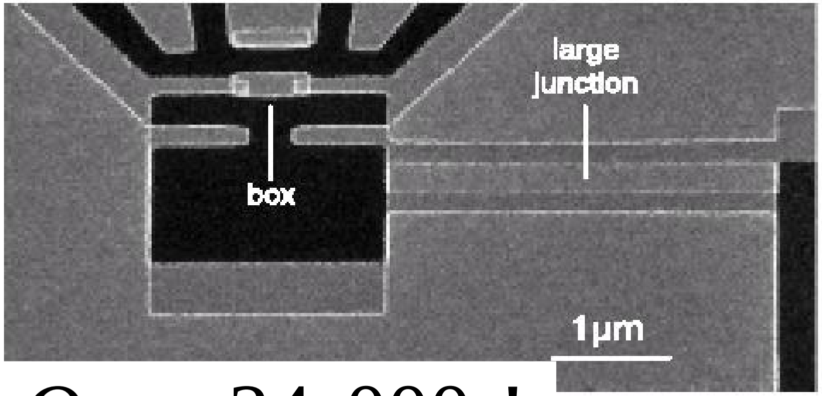


Figure 5: Ramsey fringes of the switching probability p (5×10^4 events) after two phase coherent microwave pulses separated by Δt. Dots: data at 15mK; The total acquisition time was 5 mn. Continuous line: fit by exponentially damped sinusoid with time constant $T_\varphi = 500 \pm 50$ ns. The





$$Q_\varphi \approx 24{,}000\ !$$

PROSPECTS??

- 1-2 qubits – several successes now & in coming years
- 10+ qubits in 10 years – crucial for field
- still many promising/possible approaches – AMO as well as solid state
- collective vs. elemental qubits – still up in the air
- Are we willing to pick a winner ???