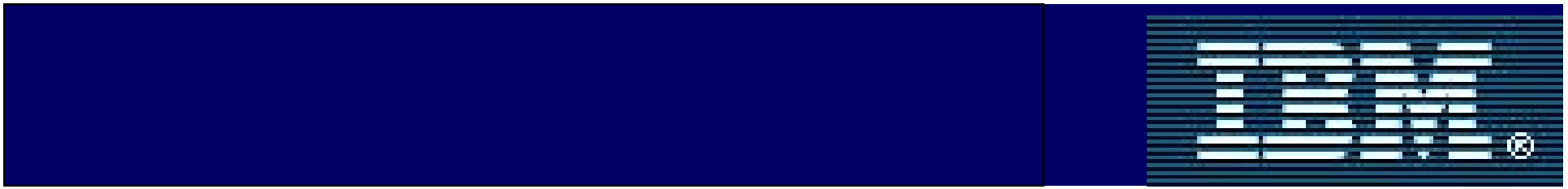
ARDA

Prospects for Quantum Computation

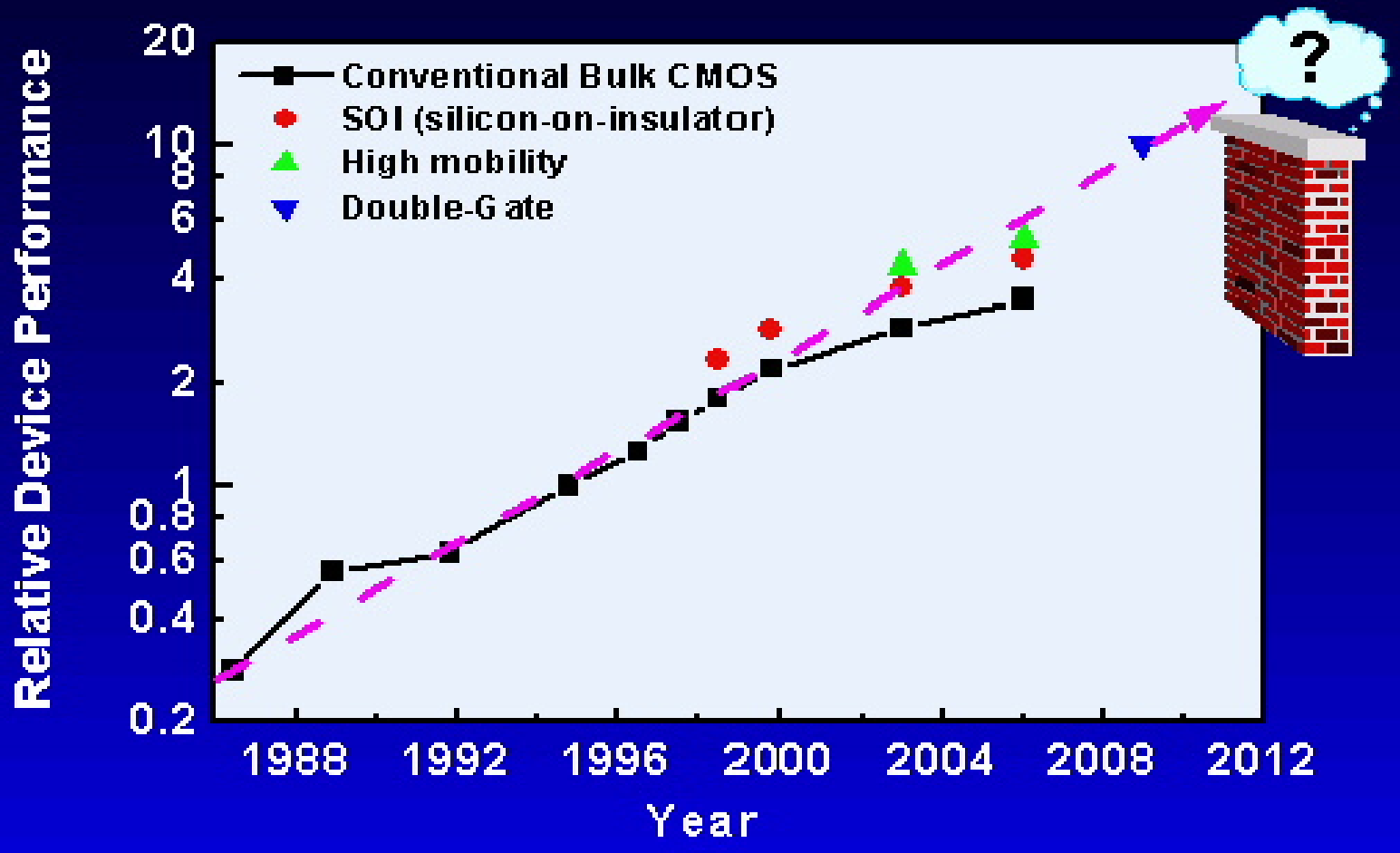
David DiVincenzo, IBM

Stony Brook, 5/2003



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**

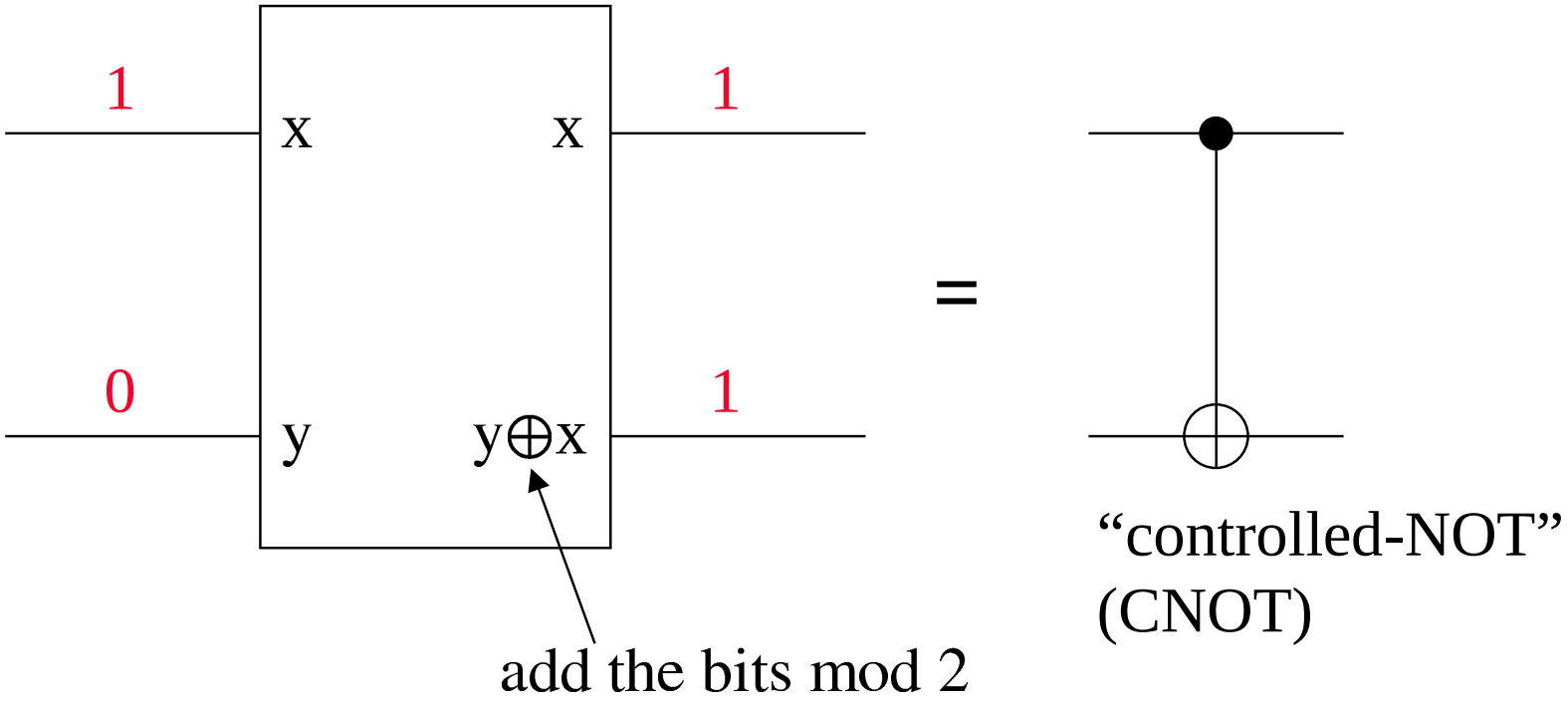
Possible qubit states: any **superposition** described by the **wavefunction**

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

Rules for quantum computing

D. Deutsch, Proc. R. Soc. A 400, 97 (1985)

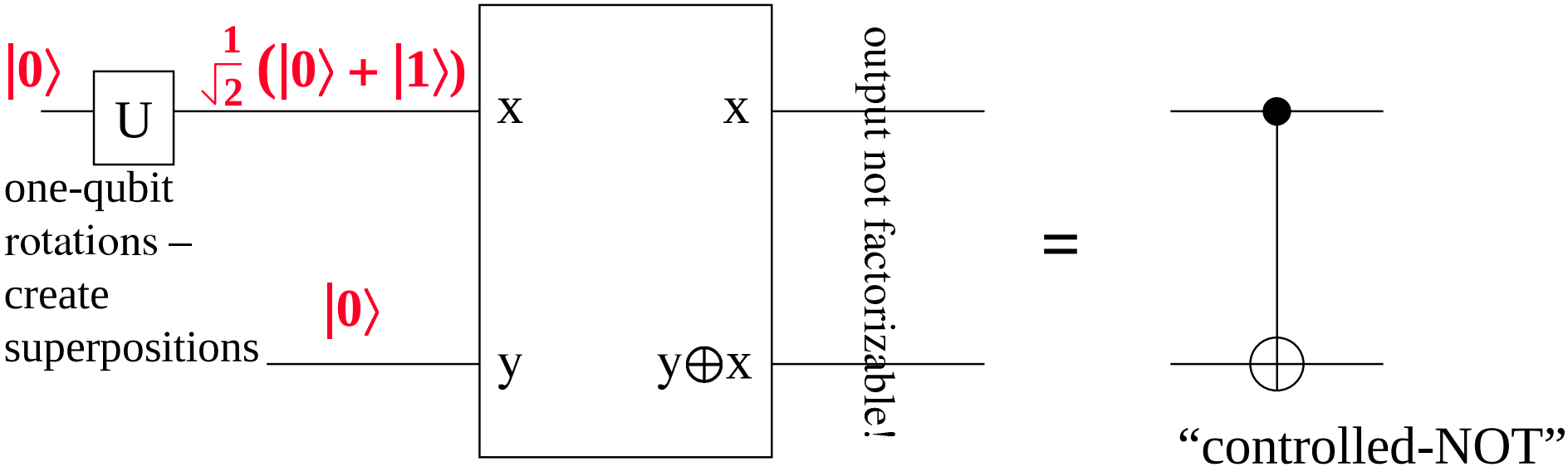
Consider this form of two-bit boolean logic gate:



Rules for quantum computing

D. Deutsch, Proc. R. Soc. A 400, 97 (1985)

Quantum rules of operation :



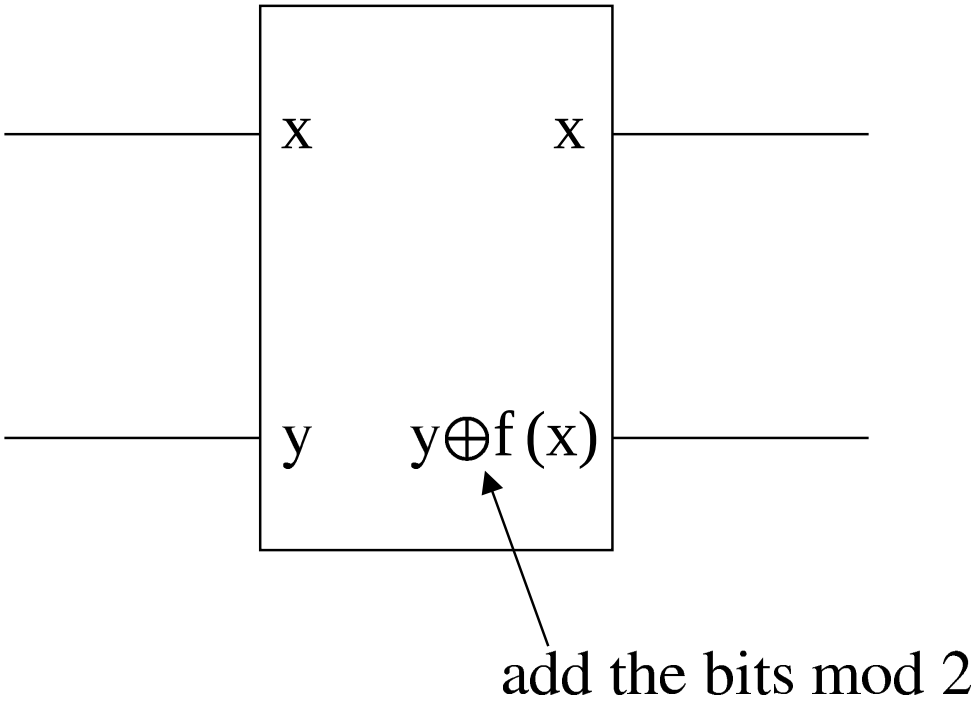
$$\psi_{in} = \frac{1}{\sqrt{2}}\left(|00\rangle + |10\rangle\right) \qquad \psi_{out} = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

Creation of entanglement

Exploiting superposition: the Deutsch algorithm

D. Deutsch, Proc. R. Soc. A 400, 97 (1985)

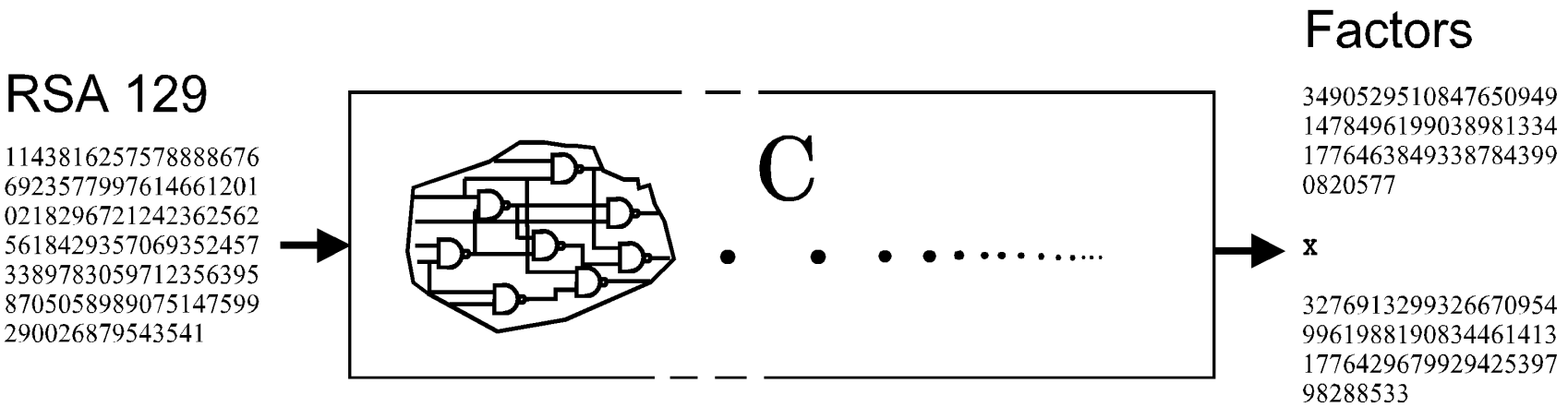
Consider this form of two-bit gate:



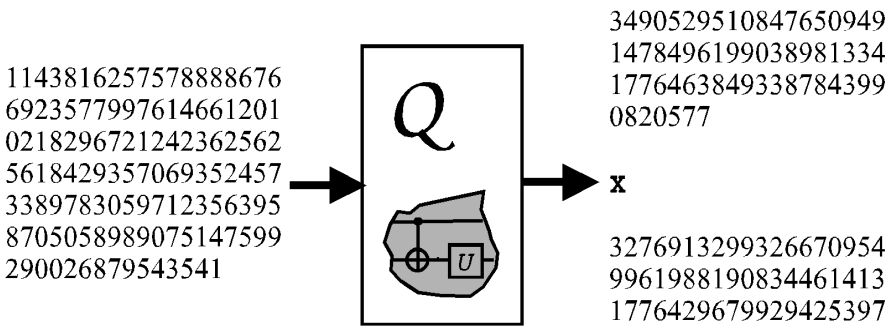
Fast Quantum Computation

P. Shor, AT&T, 1994

Classical factoring problem required 8 months on hundreds of computers



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



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) $x^2 - dy^2 = N$ $\exp\left(n^{1/2}\right) \rightarrow poly(n)$

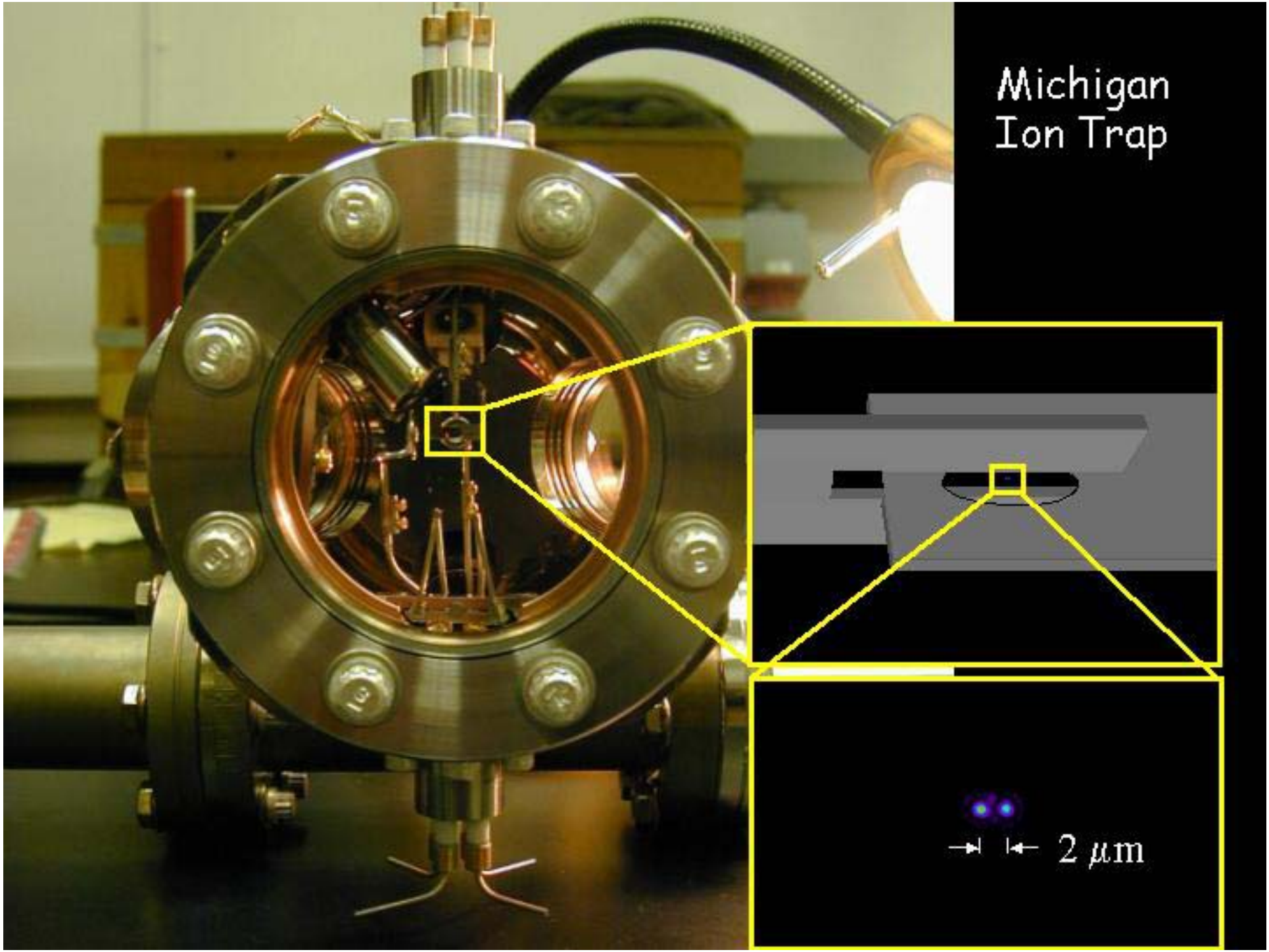
and also:

- 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

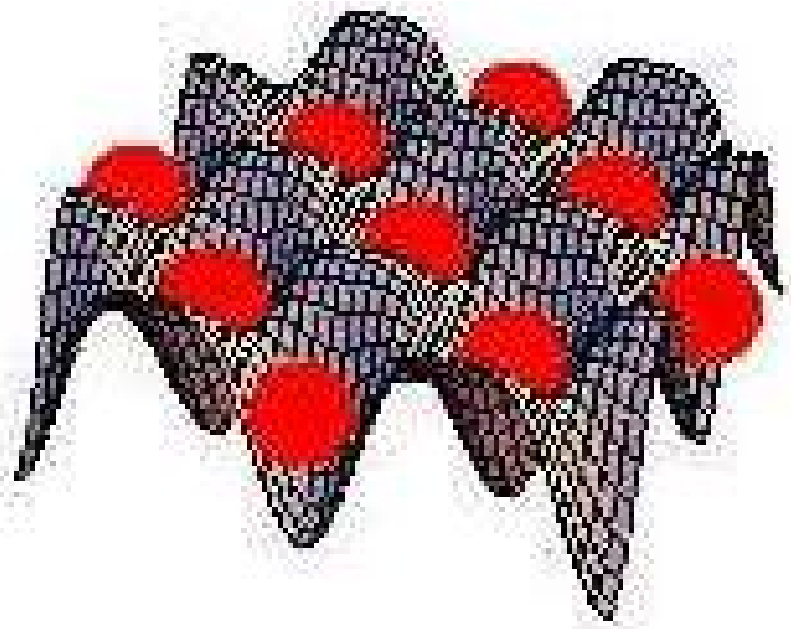
(BUT, some computations are not sped up at all!) See DiVincenzo & Loss, cond-mat/9901137

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
- Coupled quantum dots
  - Qubits: spin,charge,excitons
  - Exchange coupled, cavity coupled


Michigan
Ion Trap
2 μm

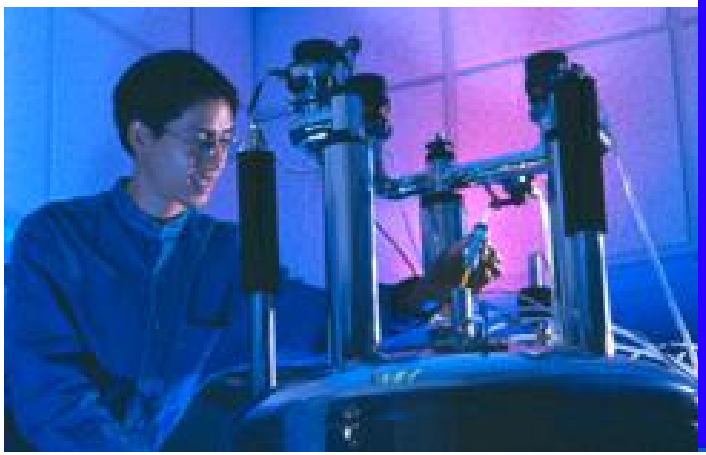
Proposed optical lattice quantum computer

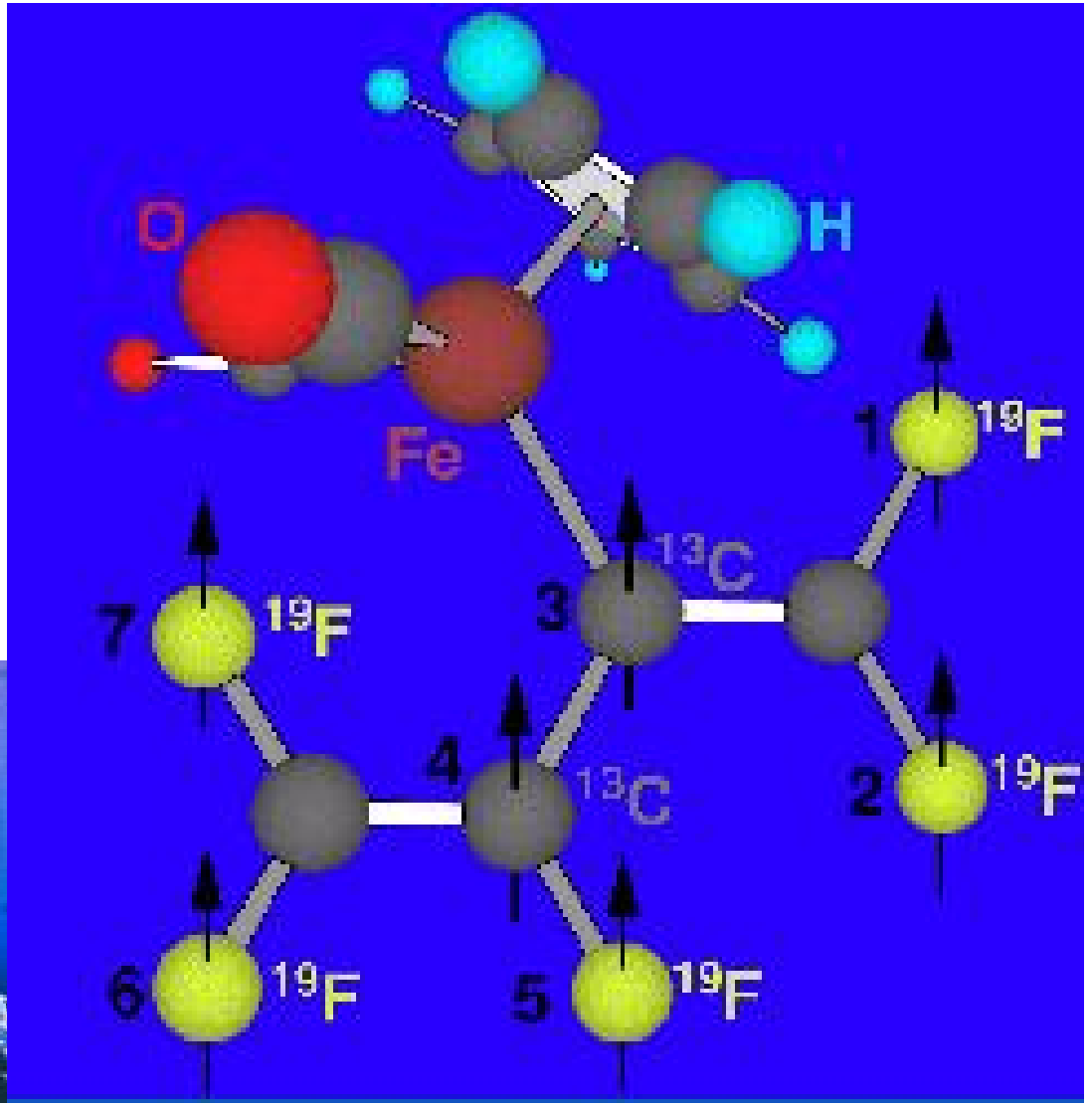


Ivan Deutsch/University of New Mexico

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

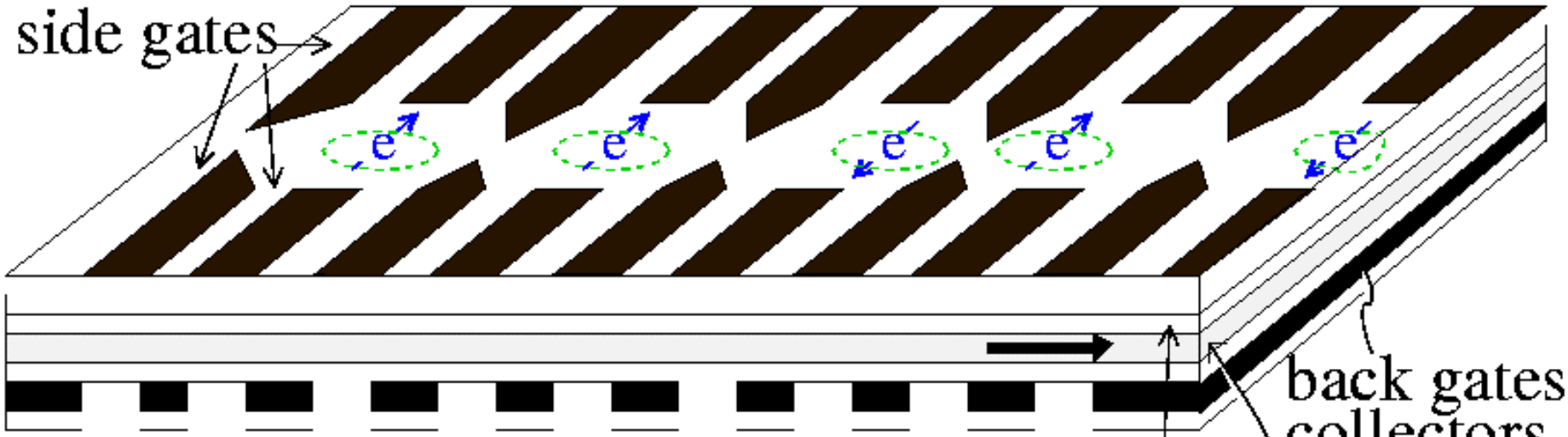
D. P. DiVincenzo, in Mesoscopic Electron Transport, eds. Sohn, Kowenhoven, Schoen (Kluwer 1997), p. 657, cond-mat/9612126; "The Physical Implementation of Quantum Computation," Fort. der Physik 48, 771 (2000), quant-ph/0002077.

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

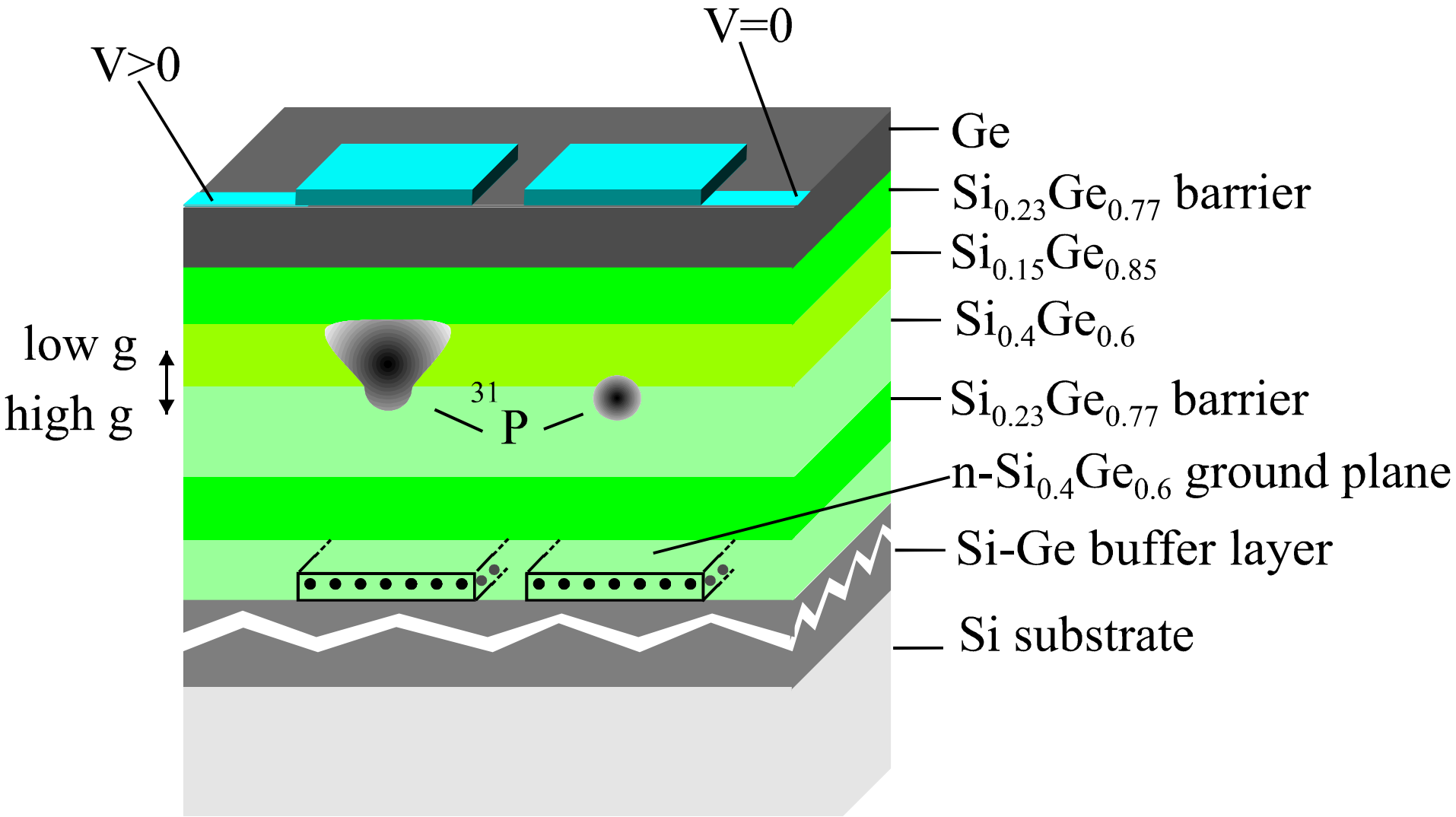
–readout by gatable magnetic barrier

/u/divince/tex/tevtex/nature2000/divloss4

Kane (1998) à

Concept device: spin-resonance transistor

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

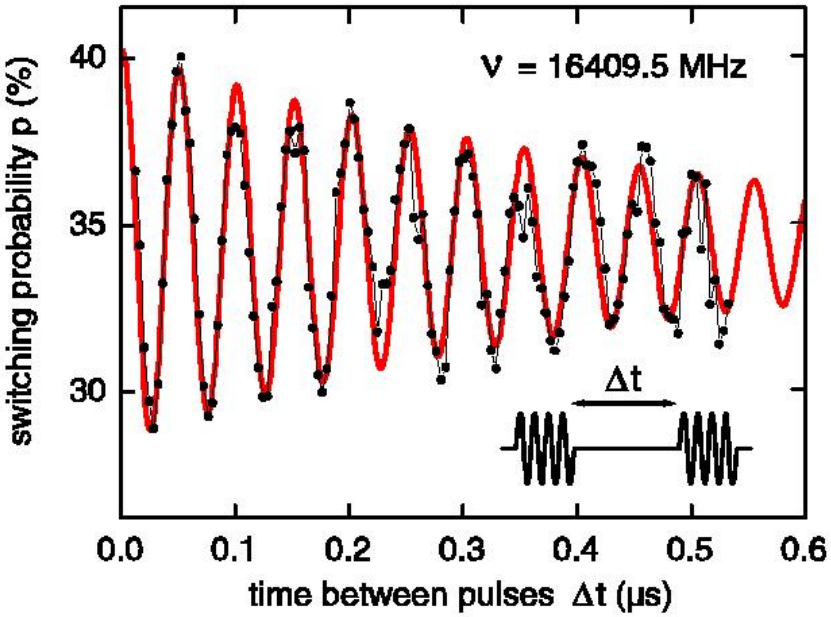


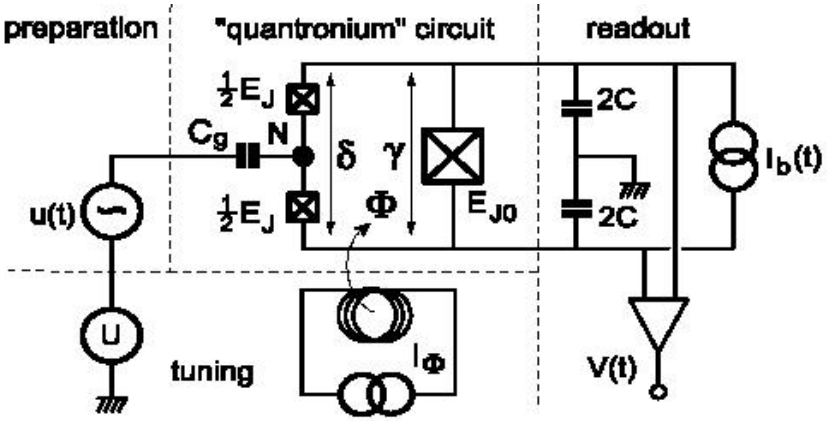
Recent progress – Josephson junction qubit

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





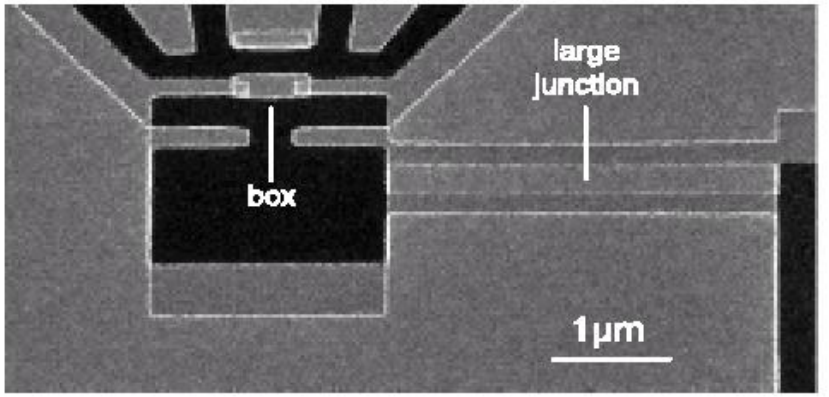


Figure 5: Ramsey fringes of the switching probability p (5×10^4 events) after two phase coherent microwave pulses separated by Δt. Dots: data at 15mK; The total acquisition time was 5 mn. Continuous line: fit by exponentially damped sinusoid with time constant $T_\varphi = 500 \pm 50$ ns. The

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
- artificial vs. natural collective effects – either is possible