An Introduction to Quantum Information Technologies:

From "You Can Buy it Now" to "Can It Ever Be Done?"

Michael E. Flatté
Optical Science and Technology Center
Department of Physics and Astronomy
University of Iowa

Supported by DARPA, ARO, and NSF

Quantum Information Devices

Quantum Key Distribution (Quantum Cryptography)

- *Why?*
- *Relies on entanglement and quantum measurement*
- *Commercially available (ID Quantique)*
- *Future development: quantum repeaters*

Quantum Computation

- *Why?*
- *Demonstration calculations with*
  - ensemble liquid NMR
  - cold ions in traps
- *Demonstration qubits in solid state systems*
  - superconducting qubits
  - semiconductor spin qubits

Quantum Key Distribution

"Alice" wishes to send a message to "Bob"
without meeting in advance to set a key

Large amounts of information

Requires large amounts of key

One current strategy (internet):

- *Bob provides Alice publicly with the required information to encrypt (public key)*
- *the information required to decode is retained in a secret key that only Bob knows*
- *relies on "nearly irreversible" process, such as factoring large numbers into primes*

Would prefer:

theoretically unbreakable codes

public generation of a secret key shared by Alice and Bob

Entangled States

Two two-state systems created in a coherent superposition of states... such as:

two photons

L R + R L

2γ generated in radioactive decay

2γ generated via coherent nonlinear process in a nonlinear material (χ_2)

two electrons

up down − down up

(singlet state, total spin=0)

Measurement on entangled states

two detectors separated by an arbitrary distance

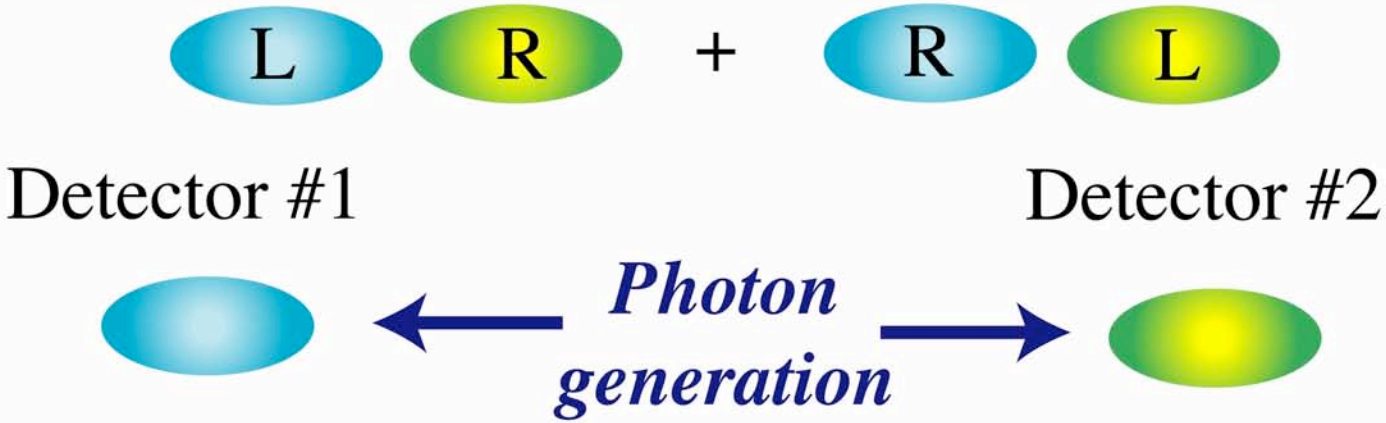
Results: detector #1 measures L, #2 measures R

or

detector #1 measures R, #2 measures L

and no other outcomes

Key generation via entangled states



If #1 measures L and #2 measures R, bit is 1

If #1 measures R and #2 measures L, bit is 0

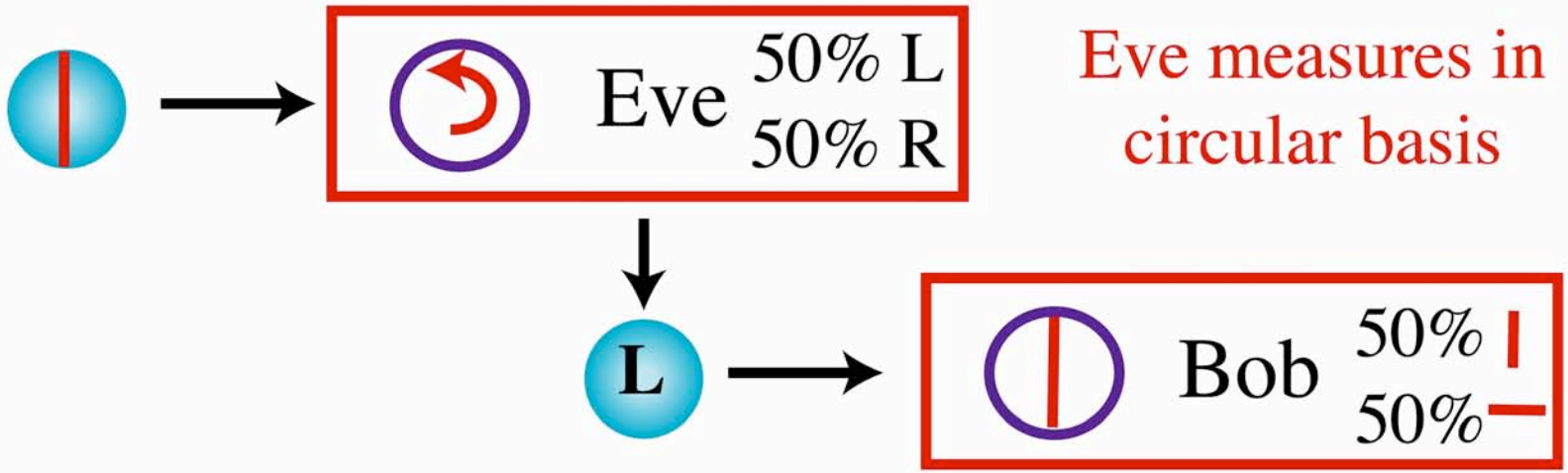
Were photons detected?

public communication to check

What about eavesdropping ("Eve")?

Eavesdropping

Statistical elimination of eavesdropping (nonclonability)



Eve measures in circular basis

Bob measures in linear basis

Eavesdropping has an identical effect to noise

Public generation of secret key

Decoherence from noise or eavesdropping can be measured (statistically)

However, sufficient levels of noise or eavesdropping will cause public generation of a secret key to fail

Public Key Generation

(Alice) sends bits with one of 4 non-orthogonal polarizations

photons with two linear and two circular polarizations

(Bob) measures with random polarization orientation

In public, classical channel Alice and Bob check the polarization choices

they discard measurements with different bases

They also check a subset of the measurements.

this provides an upper bound on noise

and eavesdropping

Remaining ***processed*** bits form the key for the message.

One-pad cryptography

classically unbreakable

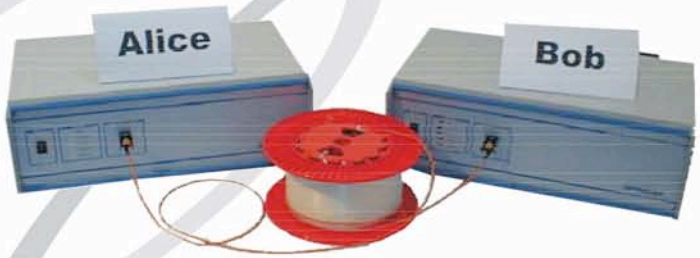
very key intensive

Key	*00010100010*
Message	*01010010011*
Send XOR	*01000110001*

QKD - Commercial

Quantum Security... at last

Quantum Key Distribution System



Key distribution over optical fiber with absolute security

Main features

- First quantum cryptography system
- Security guaranteed by quantum physics
- Point-to point key distribution
- Standard optical fiber
- Distances up to 70 km
- Key rate up to 1000 bits/s
- Compact and reliable

Key distribution is a central problem in cryptography. Currently, public key cryptography is commonly used to solve it. However, these algorithms are vulnerable to increasing computer power. In addition, their security has never been formally proven.

Quantum cryptography exploits a fundamental principle of quantum physics - observation causes perturbation - to distribute cryptographic keys with absolute security.

id Quantique is introducing the first quantum key distribution system. It consists of an emitter and a receiver, which can be connected to PC's through the USB port.

id Quantique

10, rue Cingria 1205 GenÊve Switzerland
Tel: +41 (0)22 379 69 29 Fax: +41 (0)22 781 09 80
email: info@ idquantique.com
web: http://www.idquantique.com

id Quantique
A Quantum Leap for Cryptography

Performance

			Units
Key exchange rate[1] over	10 km	4000	Bits/s
	20 km	1500	
	50 km	100	

Notes

[1]: The key exchange rate depends on the actual fiber attenuation.

Interface

Platform	Windows 98 2nd ed, 2000, ME, XP
Interface	USB version 1.0, 12 Mbit/s Plug & Play connection

General information

	Emitter	Receiver	
Optical connector[2]	FC/PC		
Operating temperature	+10 to +30		C
Dimension (L W H)	32 x 46 x 16		cm
Weight	13	7	kg
Power supply	110 - 230		VAC

Notes

[2]: Other connector type available upon request

Sales Contact

For further information on this or other products, please contact id Quantique by phone: +41 (0)22 379 69 29 or email: info@ idquantique.com

Disclaimer

The information and specification set forth above are subject to change at any time by id Quantique without prior notice. June 2003.

QKD - Limitations

Only one photon at a time

Otherwise Eve can split off one and measure it without being detected

Single photon sources are inefficient

Attenuate light source to reduce 2-photon emission, so 2-photon << 1-photon, but 1-photon << 0-photon

Future approaches:

quantum error correction -

extends effective attenuation length

efficient single-photon emitters

quantum repeaters -

generate correlations between entangled pairs over long distances - not information transfer, so fidelity can depend polynomially on distance

L.-M. Duan, et al., Nature 414, 413 (2001).

Algorithms for quantum computers

Many problems are "hard" for traditional computers

Factoring large numbers into prime factors

Finding specific entries in an unordered list

Travelling salesman

Fermionic sign problem in quantum Monte Carlo

Known quantum algorithms which are much faster than classical ones

Shor (1994): factoring a large number into primes

requires polynominal, not exponential time!

see Rev. Mod. Phys. 68, 733 (1996)

Grover (1997): looking for an entry in an unordered list

"Quantum mechanics helps in searching for a needle in a haystack"

Phys. Rev. Lett. 79, 325 (1997)

(more to come)

Quantum vs Classical Information

Bennett and DiVincenzo Nature 404, 247 (2000)

	Classical	Quantum
the bit	0 or 1	two-state system $\|0\rangle$ and $\|1\rangle$ $\cos\theta \, \|0\rangle + \exp(i\phi)\sin\theta \, \|1\rangle$
copyable?	yes	no! (quantum money)
communicable?	yes	yes (quantum teleportation)
fault-tolerant?	yes	yes! Shor, PRA 52, 2493 (1995) Preskill, Proc. R. Soc. Lond. A 454, 385 (1998)

Quantum Error Correction (w/o Redundancy)

Shor, PRA 52, 2493 (1995)

classical $0 \longrightarrow 000, \qquad 1 \longrightarrow 111$

But we cannot copy quantum bits... instead we entangle them

quantum $a|0\rangle+b|1\rangle \longrightarrow a|000\rangle+b|111\rangle$

Single bit-flip error

$$|000\rangle \longrightarrow |100\rangle$$

XOR $\longrightarrow$ Flip bit

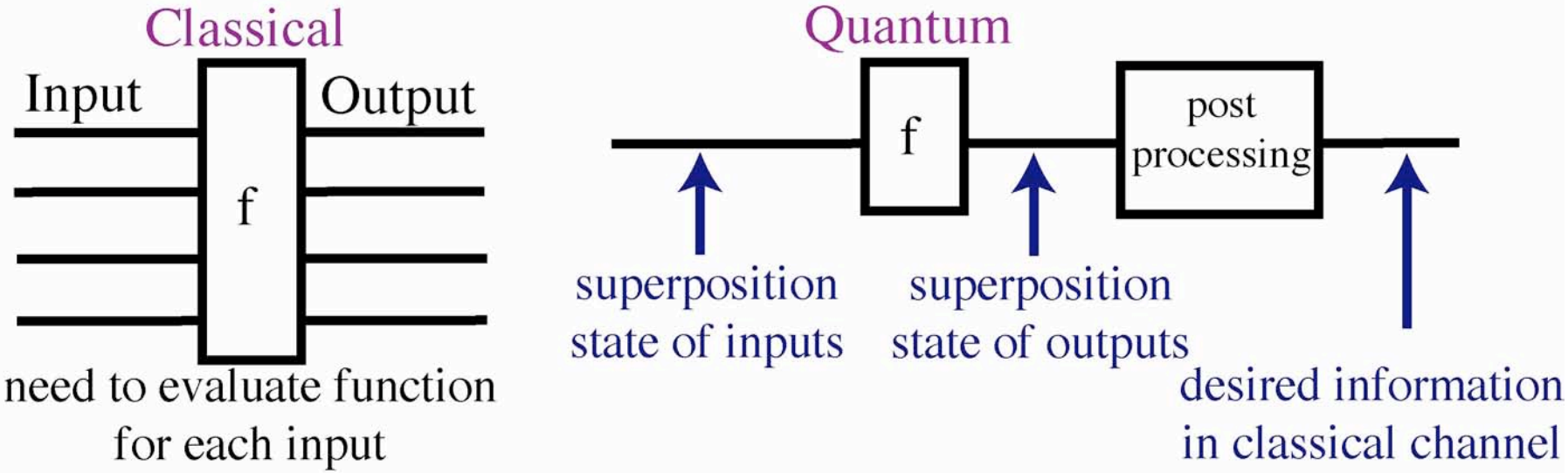
Phase error

$$|000\rangle+|111\rangle \longrightarrow |000\rangle - |111\rangle$$

Three entangled versions of the phase....

error correct with quantum XOR on the phases

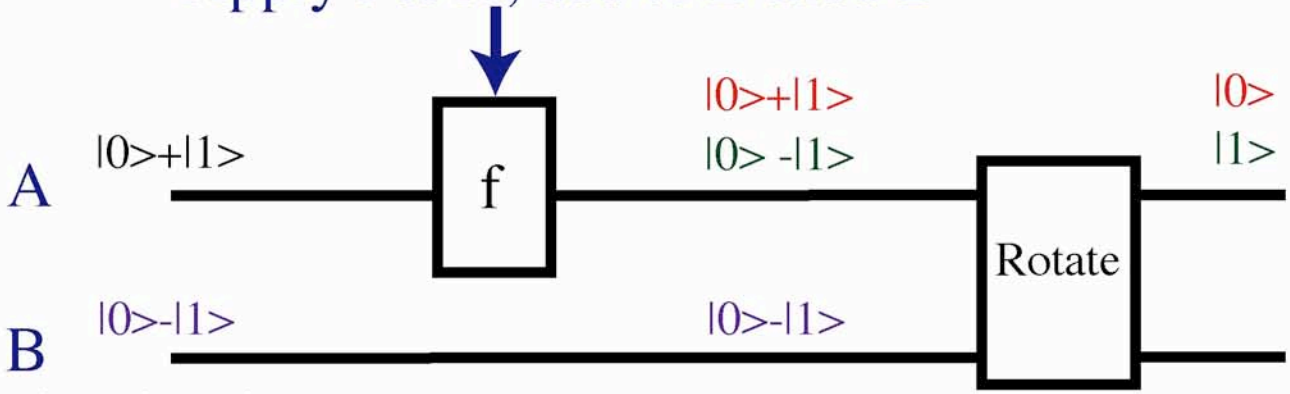
Quantum Parallelism



Deutsch - Jozsa algorithm

Proc. R. Soc. Lond. A **439,** 553 (1992).

Apply f to A, add to B mod 2



$|x\rangle(|0\rangle-|1\rangle)$ $\quad$ $|x\rangle(|0+f(x)\rangle-|1+f(x)\rangle)$

$= (-1)^{f(x)}|x\rangle(|0\rangle-|1\rangle)$

constant function

$f(0)=f(1)=0$

$f(0)=f(1)=1$

balanced function

$f(x) = x$

$f(x) = -x$

Superposition: Classical vs. Quantum

Classical Superposition of n two-mode systems

state variable of one system $\phi(x) = b_0 f_0(x) + b_1 f_1(x)$

where $f_0(x)$ *and* $f_1(x)$ *describe the modes*

superposition: $\phi_0(x_0)+\phi_1(x_1)+\phi_2(x_1)+\ldots$

described by 2n numbers

Quantum Superposition of n two-state systems

state of one system $|\phi\rangle = b_0 |0\rangle + b_1|1\rangle$

state of n systems:

$$|\psi\rangle = \sum_{i_1,\ldots i_n} b_{i_1,i_2,i_3,\ldots i_n} |i_1\rangle|i_2\rangle|i_3\rangle\ldots|i_n\rangle$$

described by 2^n *numbers*

larger working space is a direct consequence of entanglement

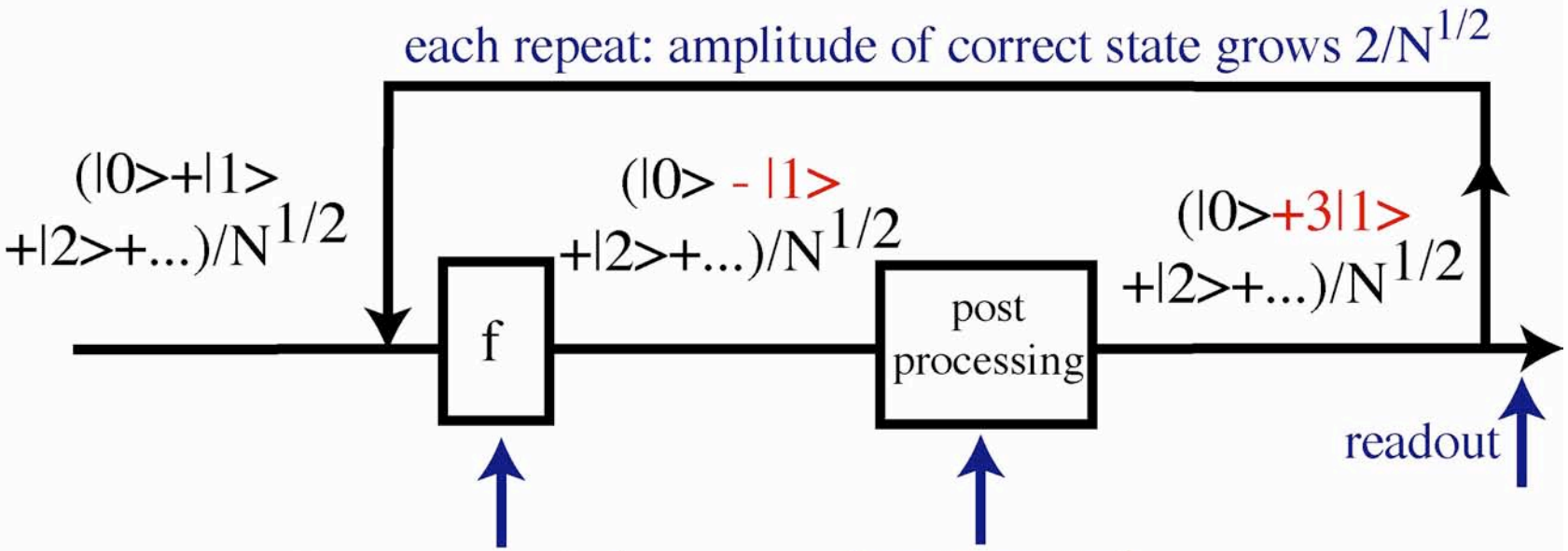
Grover Algorithm

PRL 79, 325 (1997).

Find an entry in an unordered list of N entries:

Classical: on average, examine N/2 entries

Quantum: on average, $N^{(1/2)}$ operations



Input state is $|x\rangle$

Ouput state is $(-1)^{f(x)}|x\rangle$

invert around average

$f(x) = 1$ for correct entry

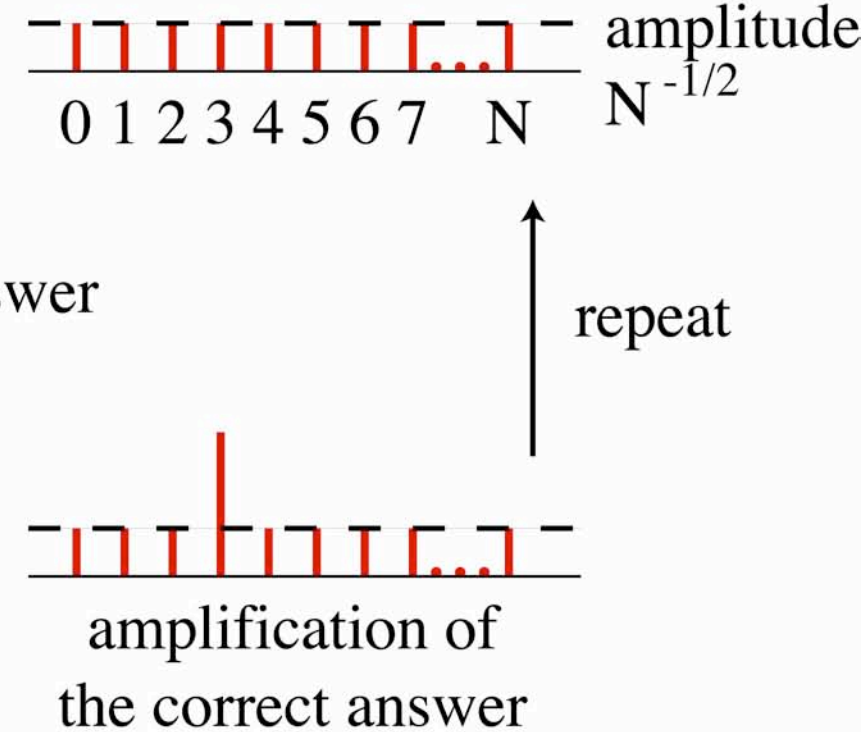
$f(x) = 0$ for all other entries...

Grover Algorithm

PRL 79, 325 (1997).

bit 1 bit 2 bit n $N=2^n$

$$\frac{(|0\rangle+|1\rangle)(|0\rangle+|1\rangle)\ldots(|0\rangle+|1\rangle)}{N^{1/2}}$$



This algorithm breaks the DES (Data Encryption Standard) used in internet commerce

Quantum Factoring (Shor's Algorithm)

2 registers of qubits, |x> and |y>.

(1) initial state |x.y> = |0,0>

(2) put |x> in linear superposition of all (w) qubits, so |x> is a linear superposition of values from 1 to Q=2^w, $Q^{-1/2}\sum_x |x,0\rangle$

(3) put |y> into an entangled state with |x> such that f(x) is correlated with x, so the state is

$$Q^{-1/2}\sum_x |x, f(x)\rangle$$

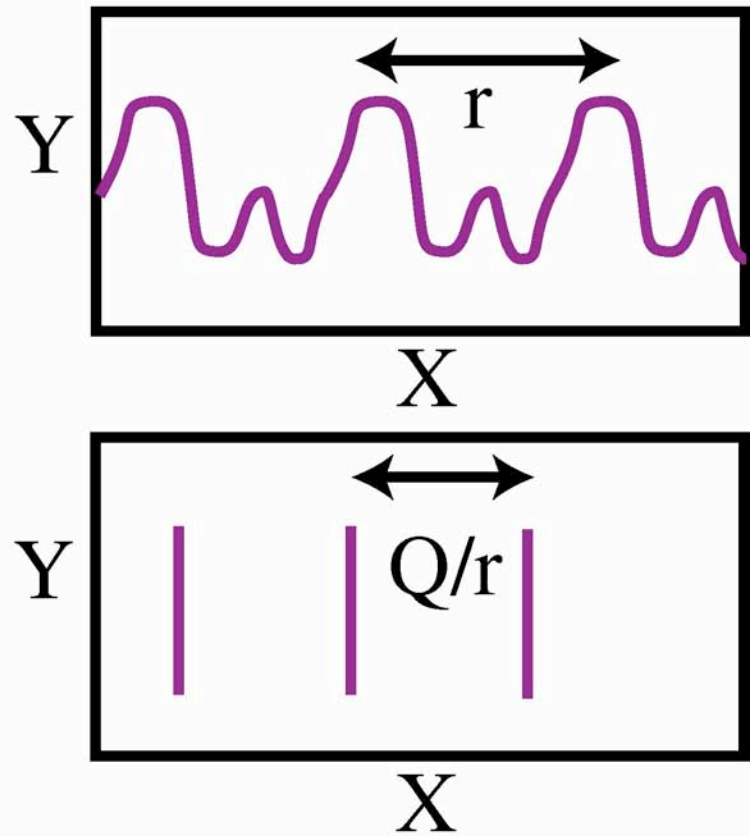
Quantum Factoring (Shor's Algorithm)

$$Q^{-1/2}\sum_{x}|x, f(x)\rangle$$

(4) Fourier transform the X register to yield

$$Q^{-1}\sum_{x,k} e^{2\pi i k x/Q}|k, f(x)\rangle$$

(5) Observe value of X register ~ Q/r



Quantum Computing Algorithm Primatives

Barenco, *et al.* PRA 52, 3457 (1995)

1-bit operation

$$A|0\rangle + Be^{i\theta}|1\rangle \rightarrow C|0\rangle + De^{i\psi}|1\rangle$$

2-bit Quantum XOR

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

A B XOR B

Unitary operations

All algorithms can be decomposed into these two

Milestones

NMR ensemble liquid quantum computation

1993: Theoretical proposal: Science 261, 1569
1998: Deutsch-Jozsa algorithm: Nature 393, 144
1998: Grover algorithm: PRL 80, 3408
2001: Shor algorithm: Nature 414, 883

ion trap quantum computation

1995: Theoretical proposal: PRL 74, 4091
1999: Demonstration of qubit: PRL 83, 4713
2003: Deutsch-Jozsa algorithm: Nature 421, 48
2003: 2-qubit gate: Nature 422, 412

superconducting quantum computation

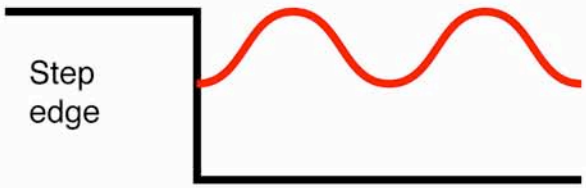
1999: Theoretical proposal: Nature 398, 305
2002: Demonstration of qubit: PRL 89, 117901; Science 296, 889
2003: Demonstration 2-qubit coupling: Nature 421, 823

semiconductor spin quantum computation

1998: Theoretical proposal: PRA 57, 120
2003: Demonstration of qubit: cond-mat/0309079

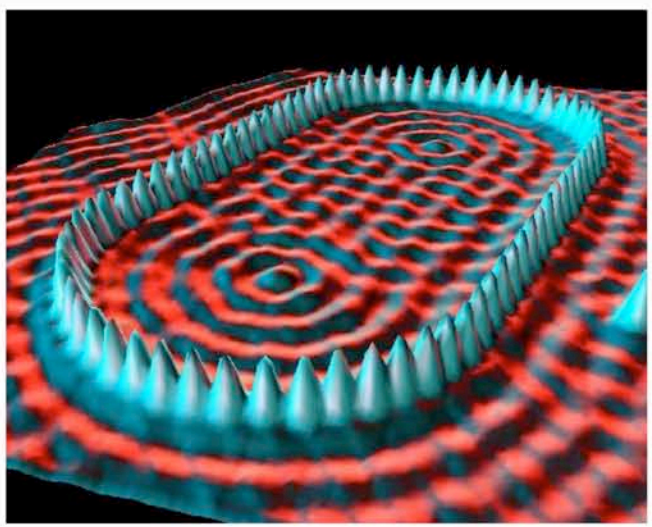
Orbital coherence in Transport

Coherence between
exp(ikx) and exp(-ikx)



Quantum Corrals

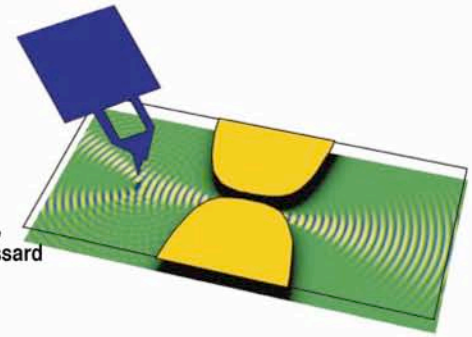
M. Crommie, C. P. Lutz, and D. Eigler



Coherent branched flow in a two-dimensional electron gas

M. A. Topinka, B. J. LeRoy, R. M. Westervelt, S. E. J. Shaw, R. Fleischmann, E. J. Heller, K. D. Maranowski & A. .C. Gossard

Nature 410, 183 (2001).



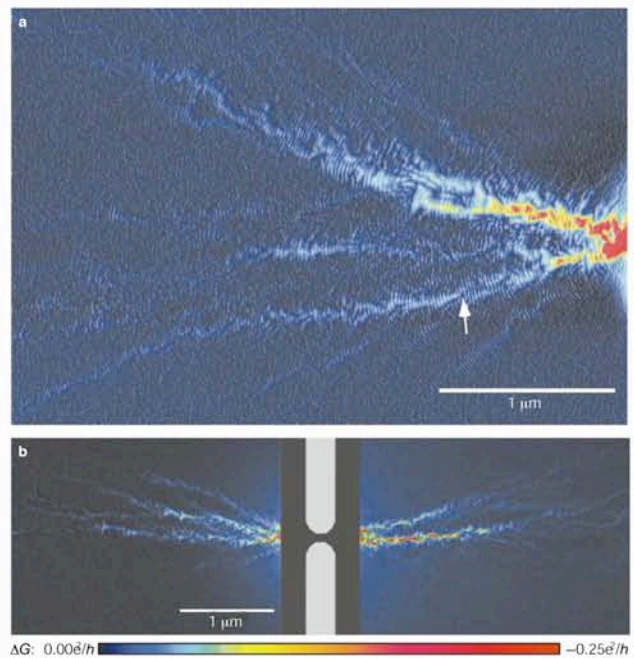


Figure 2 Experimental images of electron flow. **a**, Image of electron flow from one side of a QPC at $T = 1.7$ K, biased on the $G = 2e^2/h$ conductance step. Dark regions correspond to areas where the tip had little effect on QPC conductance, and hence are areas of low electron flow. The colour varies and the height in the scan increases with increasing electron flow. Narrow branching channels of electron flow are visible, and fringes spaced by $\lambda_F/2$, half the Fermi wavelength, are seen to persist across the entire scan. **b**, Images of electron flow from both sides of a different QPC, again biased on the $G = 2e^2/h$ conductance step. The gated region in the centre was not scanned. Strong channelling and branching are again clearly visible. The white arrow points out one example of the formation of a cusp downstream from a dip in the potential.

Quantum Computer: Physical Requirements

Requirements

DiVincenzo quant-ph/0002077

1. A scalable physical system with well-characterized qubits

2. The ability to initialize the state of the qubits (|00...000>)

3. Long relevant decoherence times (compared to gate times)

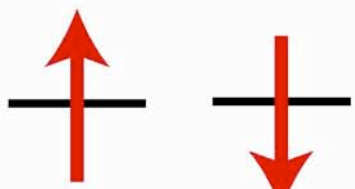
4. A "universal" set of quantum gates

5. The ability to measure specific qubits.

Spin 1/2 as a Physical Realization of a Qubit

Hilbert space has two states: up and down

Single particle in the space

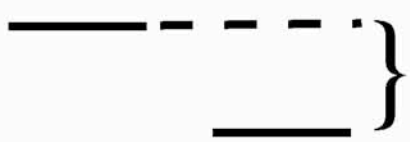


$|0\rangle \quad |1\rangle$

$$\frac{|0\rangle + e^{i\vartheta}|1\rangle}{\sqrt{2}}$$

Single-bit operations...

Magnetic field + time (precession)



$\Delta E = g\mu B/2$

$$\longrightarrow \quad \frac{|0\rangle + e^{i\Delta E t/\hbar}|1\rangle}{\sqrt{2}}$$

$|0\rangle \quad |1\rangle$

AC field (NMR) allows frequency specific precession

Spin 1/2 as a Physical Realization of a Qubit

Quantum XOR between two Qubits

Spin-spin coupling

$$H_s(t) = J(t)\vec{S}_1 \bullet \vec{S}_2$$

Time evolution of the two qubits from this Hamiltonian

$$U_s(t) = Te^{-i\int_0^t H_s(t')dt'} \qquad \int dt J(t) = J_o\tau_s = \pi(\mathrm{mod}\, 2\pi)$$

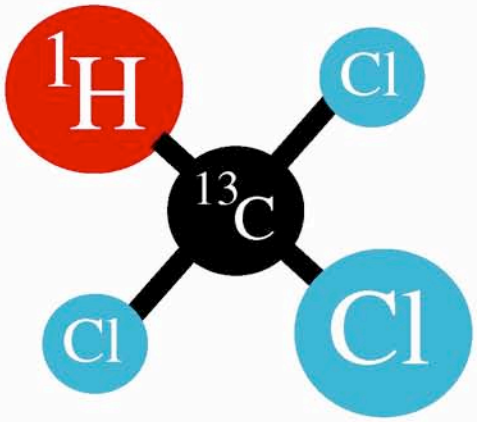
$$U_s(J_o\tau_s = \pi) = U_{swap} \qquad U_{swap}|ij\rangle = |ji\rangle$$

Similarly can generate U_{XOR}

Preferably... controllable J(t)

NMR Quantum Computation

I. L. Chuang, et al., Nature 393, 143 (1998)



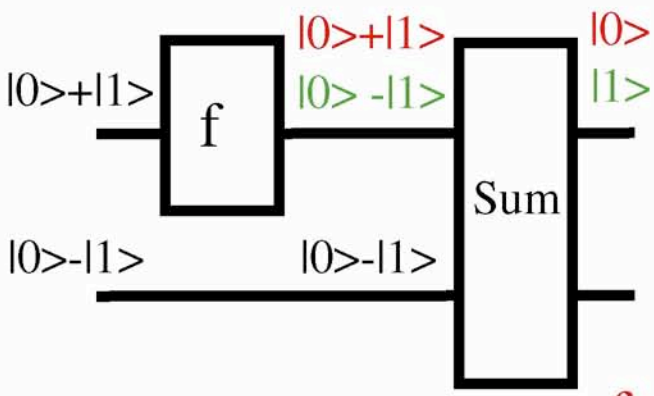
Two distinguishable qubits
1 - nuclear spin of H
2 - nuclear spin of C

precession frequency of one spin depends on orientation of the other
→ 2-qubit gate

$T_2 \sim 300$ ms, $T_{exp} \sim 7$ms

each molecule is one quantum computer
→ ensemble averaging

Deutsch - Jozsa algorithm

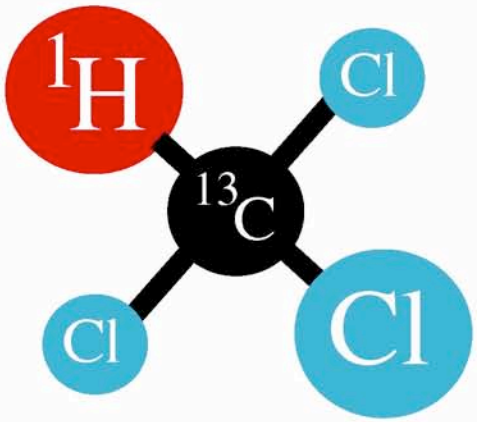


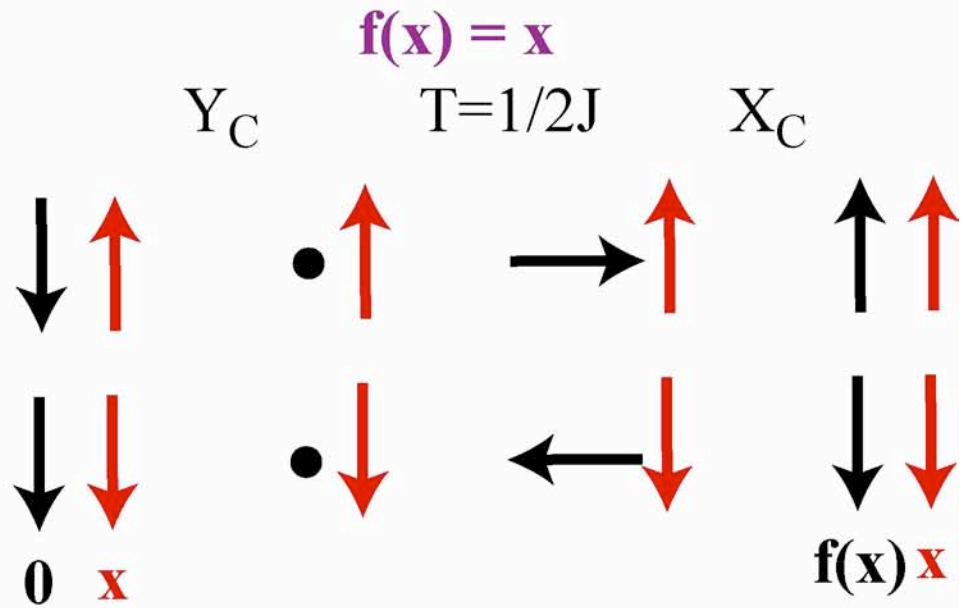
$f|x\rangle = \exp[i\pi f(x)]|x\rangle$

f = constant function f(0)=f(1)=0 or f(0)=f(1)=1
f = balanced function f(x) = x or f(x) = -x

NMR Quantum Computation

I. L. Chuang, et al., Nature 393, 143 (1998)





Full description: Y_C T=1/2J $(-Y)_C X_C (-Y)_A (-X)_A Y_A$

Measurement of spin eigenstate - $\pi/2$ pulse and measure transverse magnetization

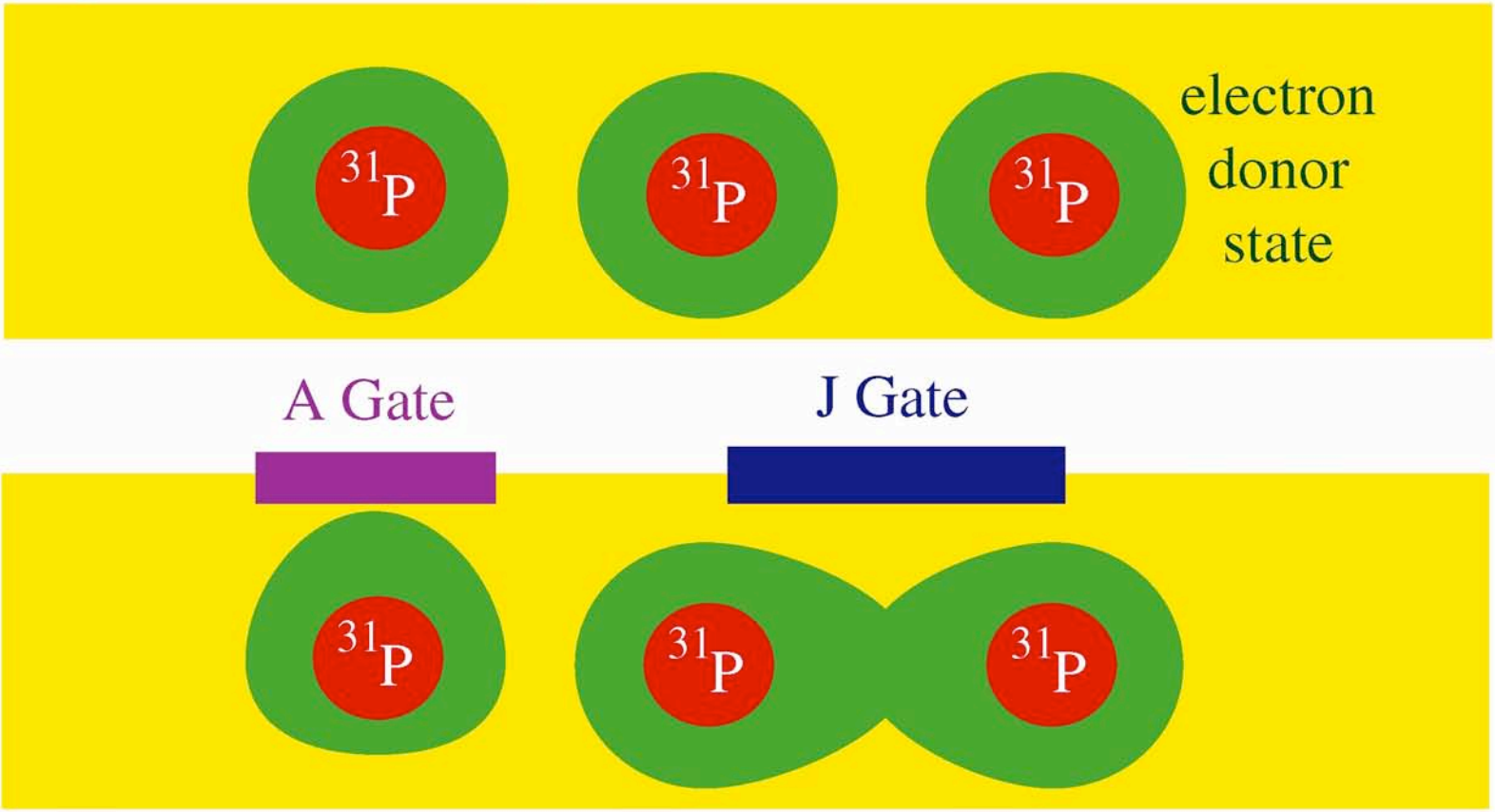
Quantum Computer: Physical Requirements

Requirements	Ensemble NMR
DiVincenzo quant-ph/0002077	
1. A scalable physical system with well-characterized qubits	spins of atoms in different environments have different ω
2. The ability to initialize the state of the qubits (|00...000>)	number of molecules in ground state scales as exp(-#qubits)
3. Long relevant decoherence times (compared to gate times)	often seconds
4. A "universal" set of quantum gates	pulse-shaping techniques
5. The ability to measure specific qubits.	ensemble measurement of many, many molecules

P in Si Quantum Computation

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

qubits are nuclear spins of P in Si matrix



1 (A) and 2 (J) qubit gates influence nuclear spins
through (1) distorting donor states
(2) hyperfine (spin) interaction between electrons and nuclei

Quantum Computer: Physical Requirements

Requirements	P in Si
DiVincenzo quant-ph/0002077	
1. A scalable physical system with well-characterized qubits	P nuclear spins in Si host (regular, 100 nm separation!)
2. The ability to initialize the state of the qubits (|00...000>)	hyperfine interaction with electrons (much higher Zeeman energy)
3. Long relevant decoherence times (compared to gate times)	long decoherence times in Si (I=0, weak spin-orbit coupling)
4. A "universal" set of quantum gates	A and J gates
5. The ability to measure specific qubits.	spin-sensitive single-electron transistors

Rabi Oscillations for Single Ion

Roos, et al., PRL 83, 4713 (1999)

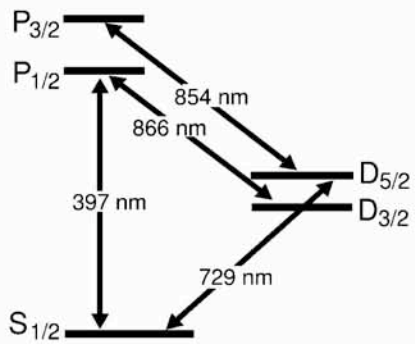


FIG. 1. Relevant energy levels of Ca and the corresponding transition wavelengths.

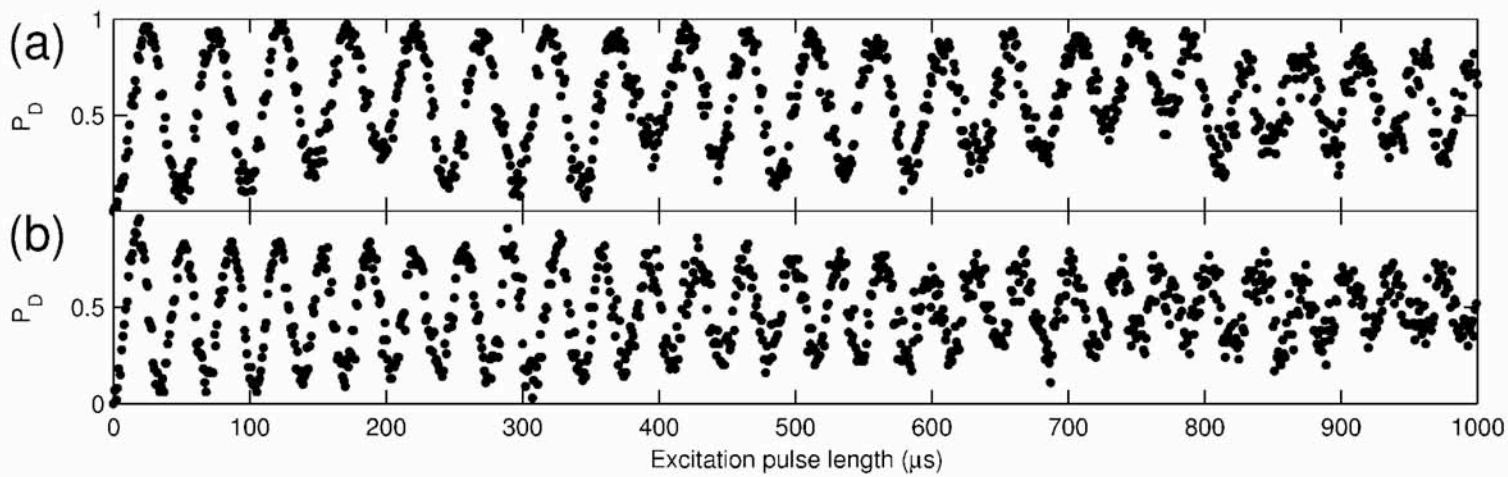


FIG. 4. (a) Rabi oscillations on the blue sideband for the initial state . Coherence is maintained for up to 1 ms. (b) Rabi oscillations as in (a), but for an initial vibrational Fock state .

Quantum Computer: Physical Requirements

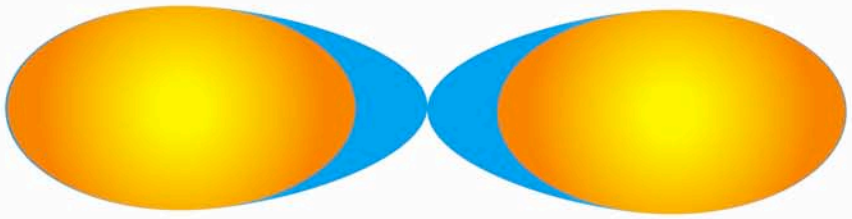
Requirements	Ion Trap
DiVincenzo quant-ph/0002077	
1. A scalable physical system with well-characterized qubits	internal spin states of ions in a linear trap
2. The ability to initialize the state of the qubits (|00...000>)	laser cooling of ions to ground state motion in trap
3. Long relevant decoherence times (compared to gate times)	weak coupling of ions to environment in trap
4. A "universal" set of quantum gates	coupling of internal spin state of ions to vibrations of ions
5. The ability to measure specific qubits.	visible fluorescence from single ions (quantum-jump spectroscopy)

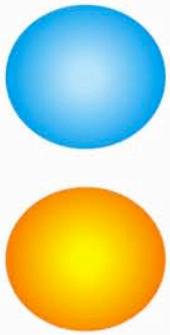
Quantum dot gating to control exchange J

Loss and DiVincenzo, PRA 57, 120 (1998).

Quantum XOR between two Qubits

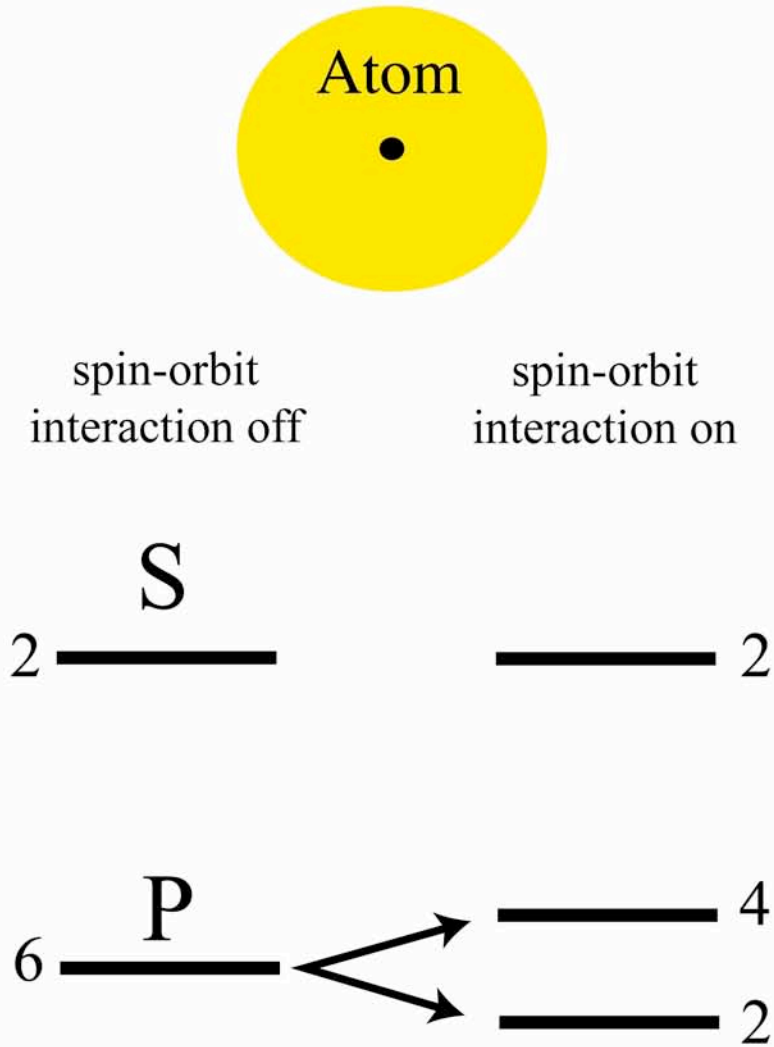
Coupling between quantum dots mediated by an electric gate



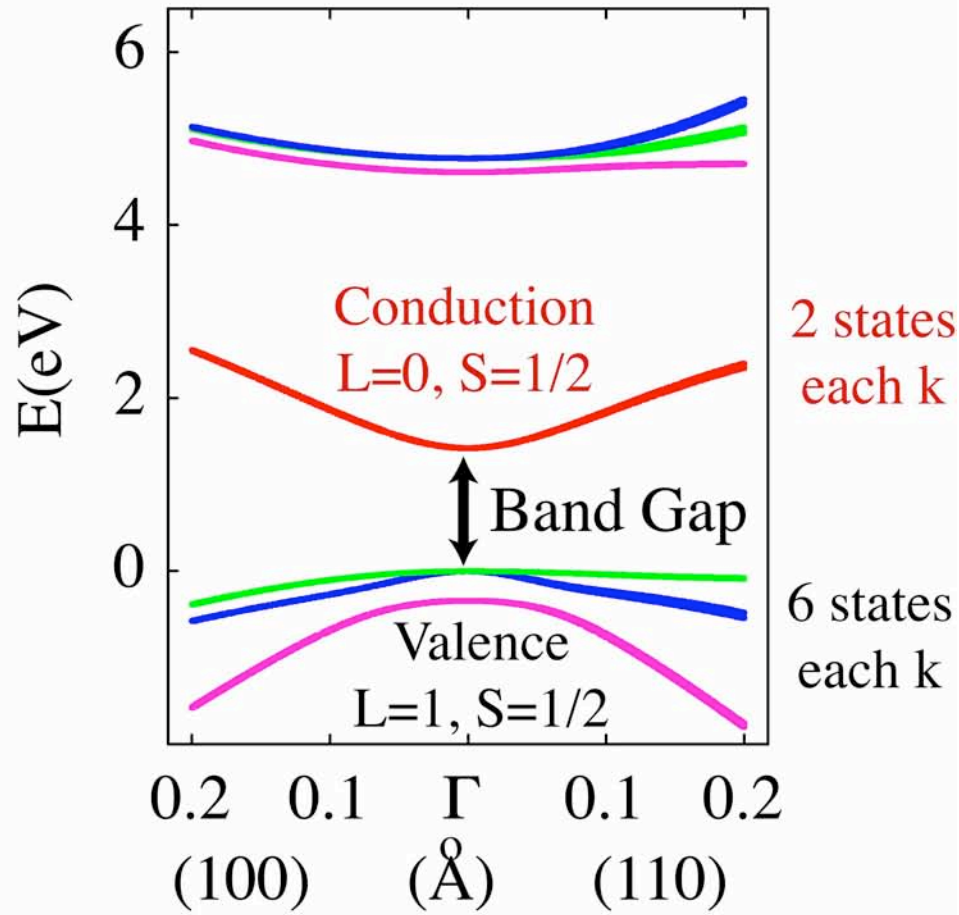


$$H_s(t) = J(t)\,\vec{S}_1 \bullet \vec{S}_2$$

Optically creating spin-polarized carriers

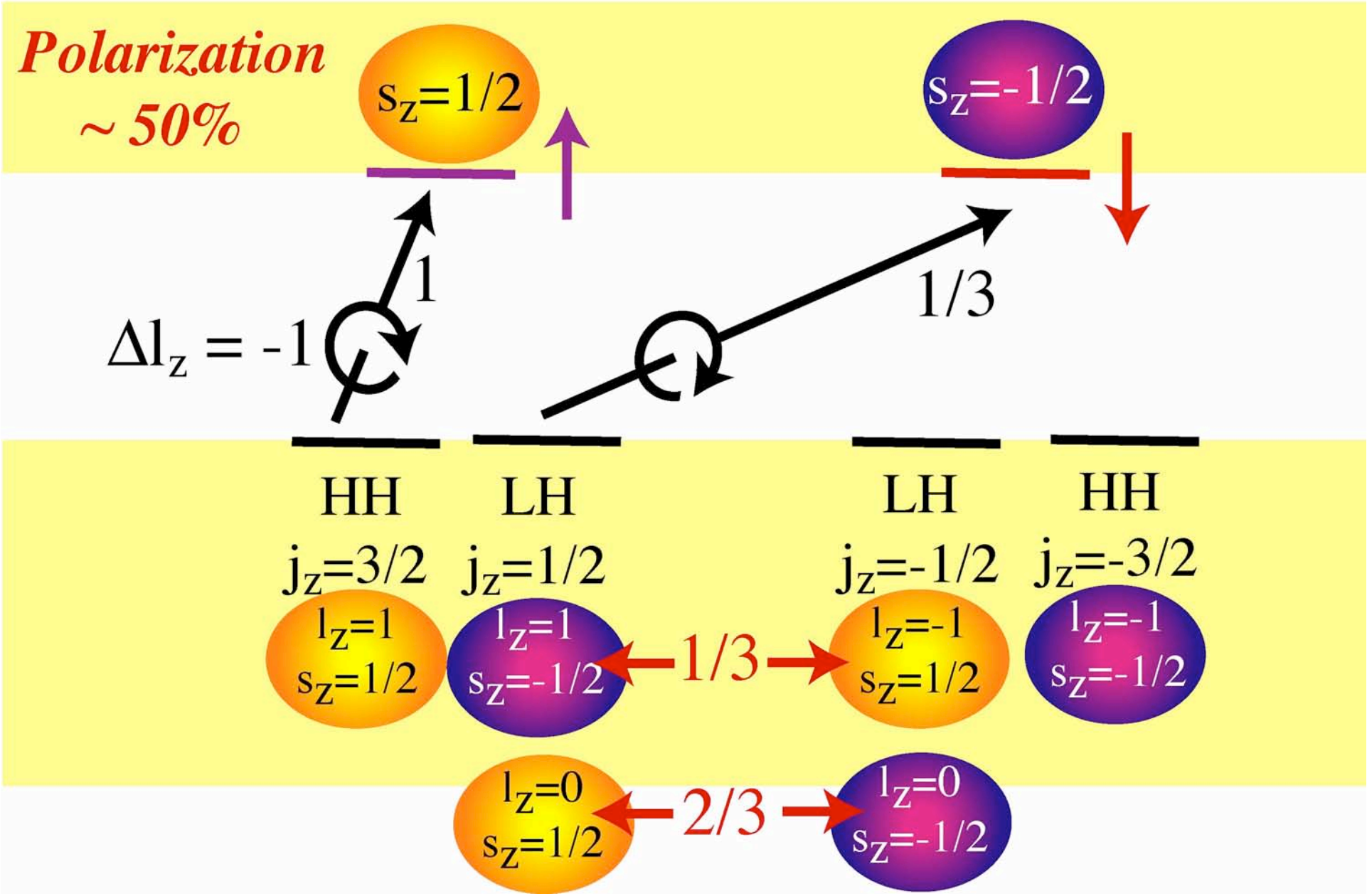


Electronic structure of GaAs

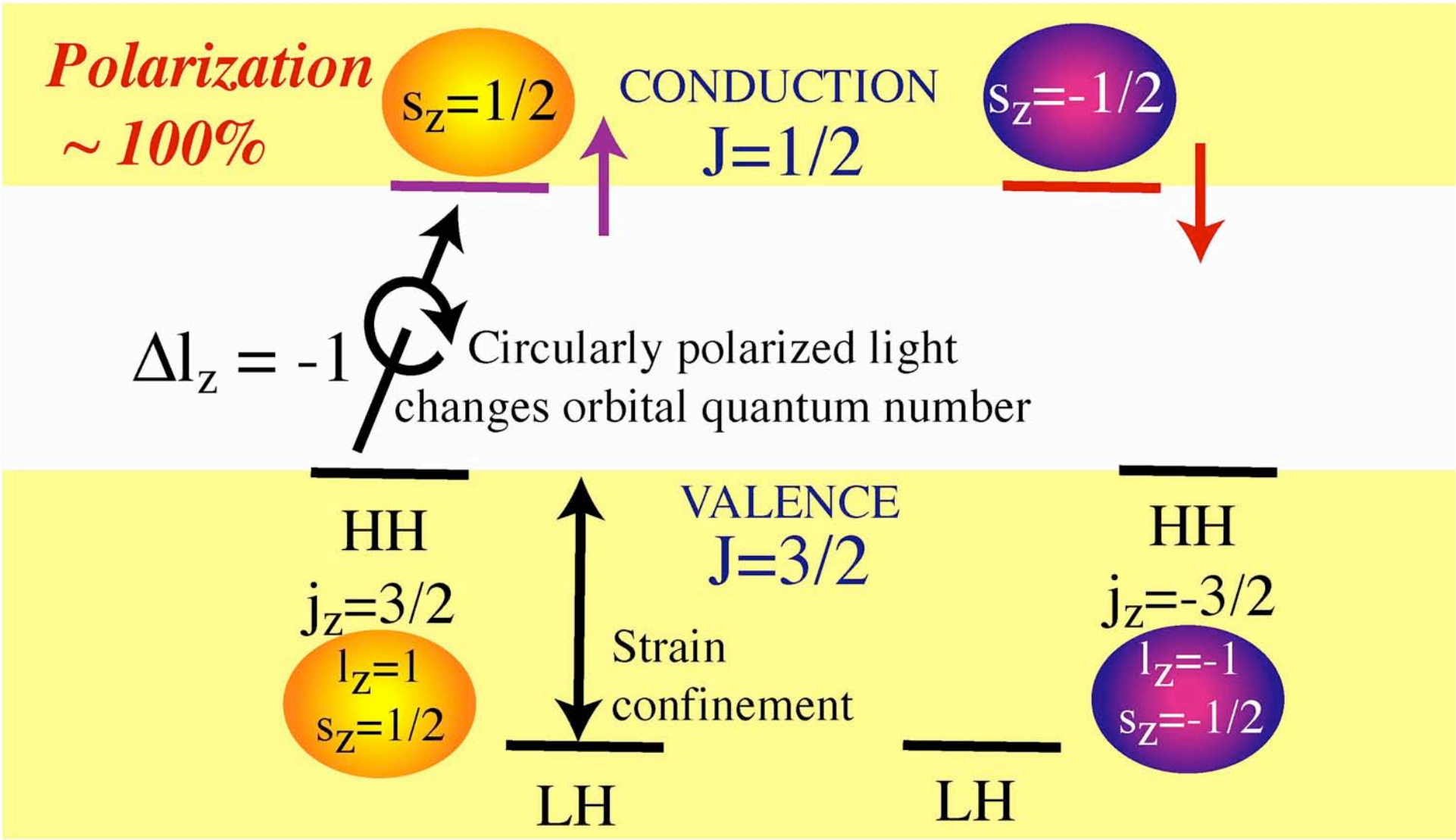


Optical transitions are vertical

Optical excitation of spin-polarized distributions

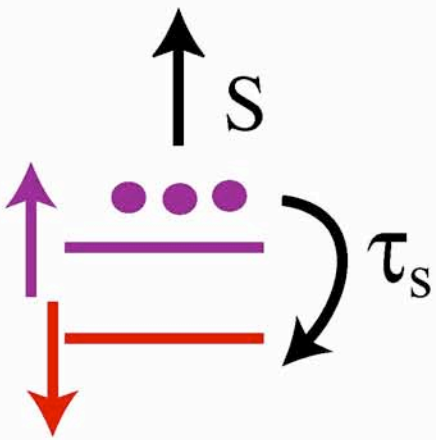


Optical excitation of spin-polarized distributions

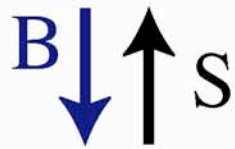


Low-dimensional structures (e.g. quantum wells)

Longitudinal and Transverse Spin Coherence

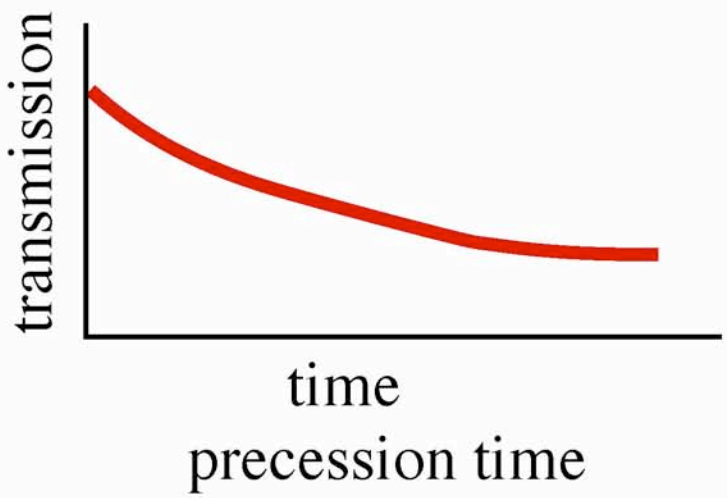


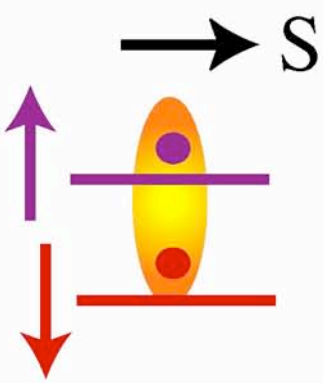
Incoherent state



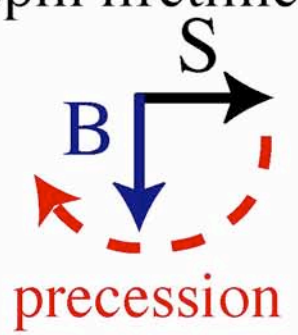
$T_1 = \tau_s/2$

T_1: Decay of S
(spin lifetime)

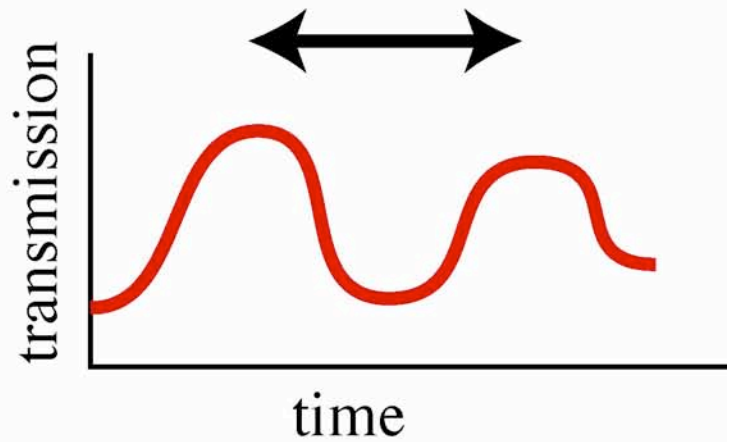




Coherent state

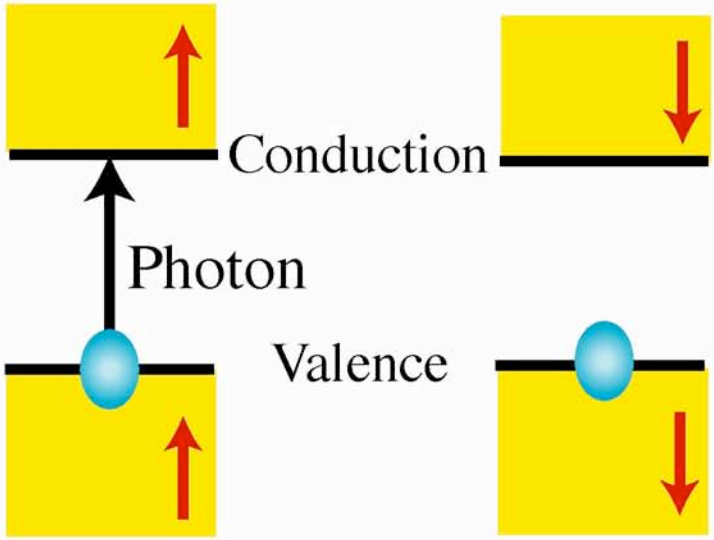


T_2: Decay of S
(spin decoherence)

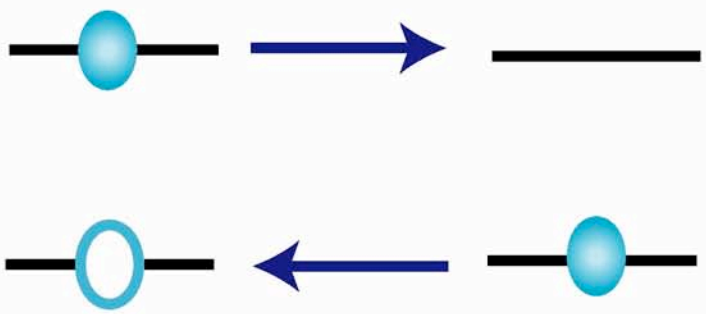


100 ns and 100 μm

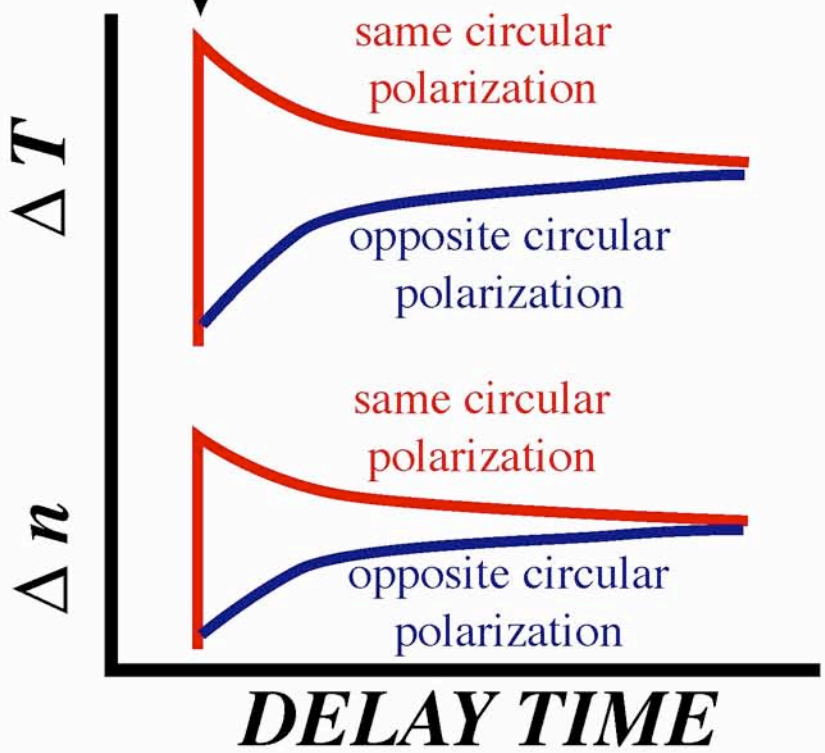
Polarized Differential Transmission



decay of spin polarization

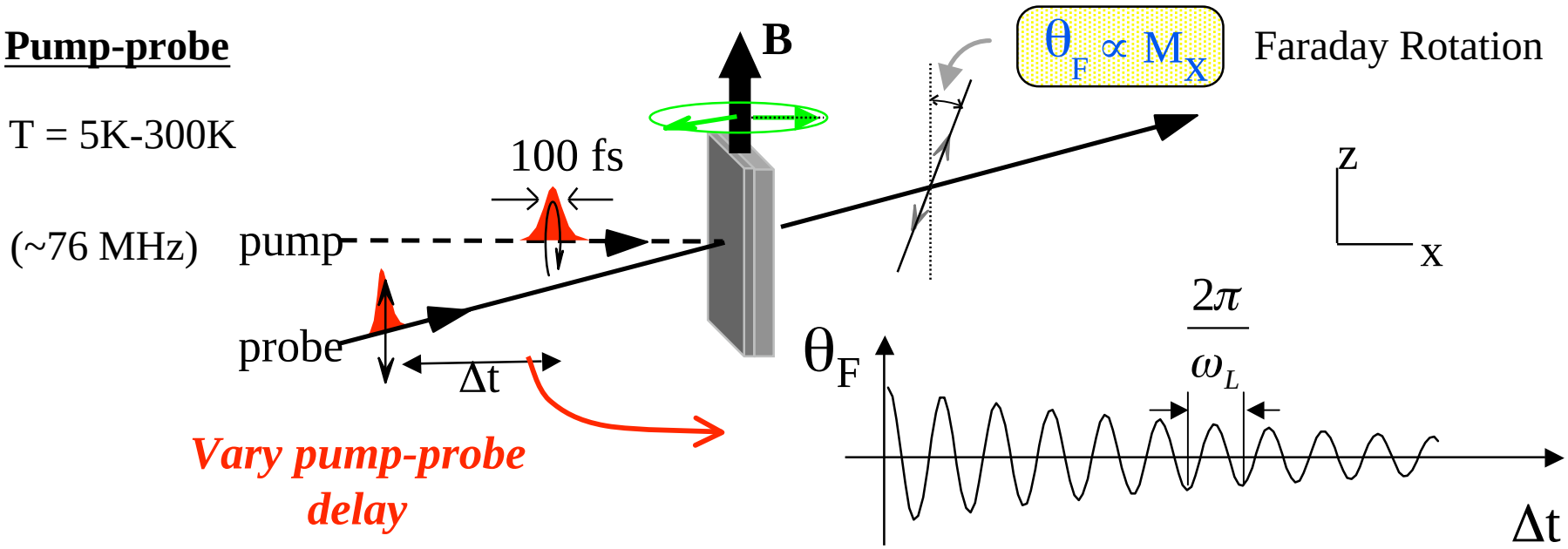


Spin polarized distribution is created with polarized light



Probe with polarized light to detect the decay of the spin polarized distribution

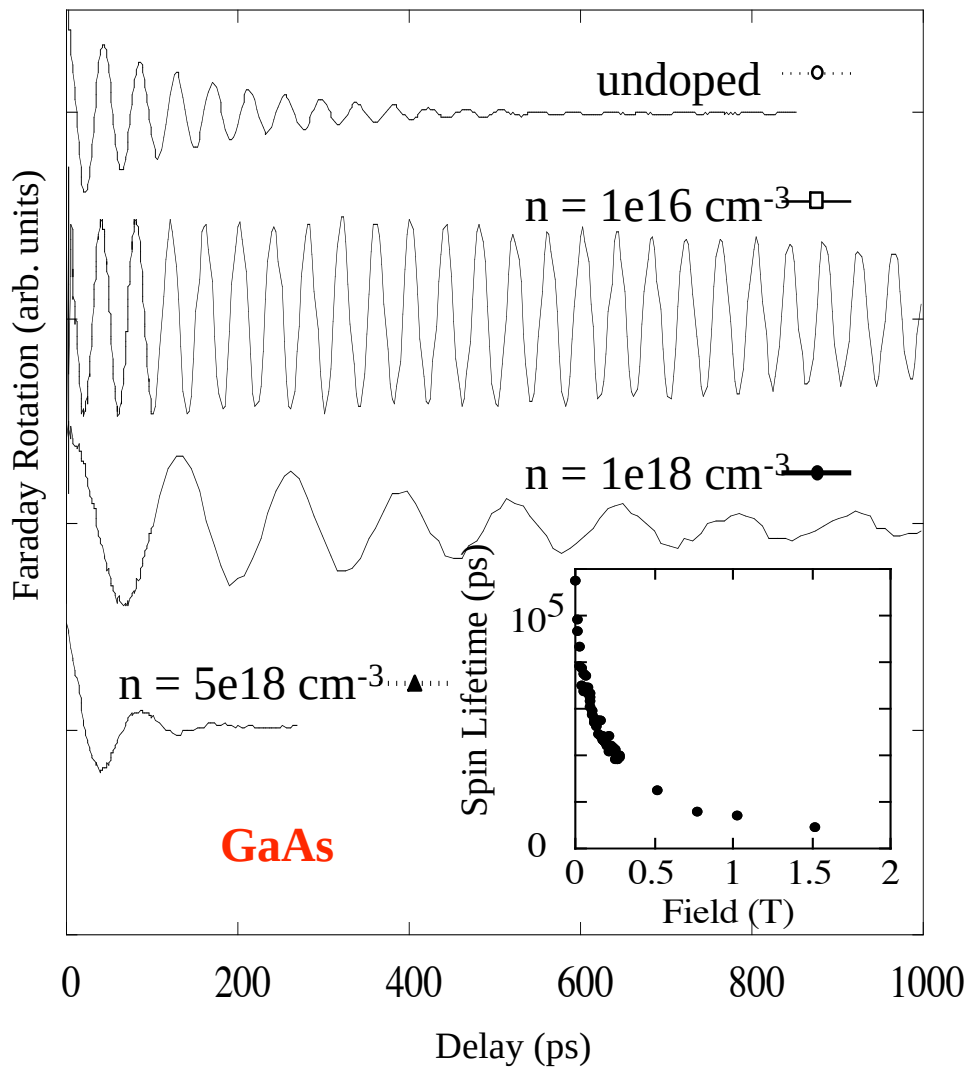
Faraday Rotation



Crooker, et al., PRL 77, 2814 (1996).

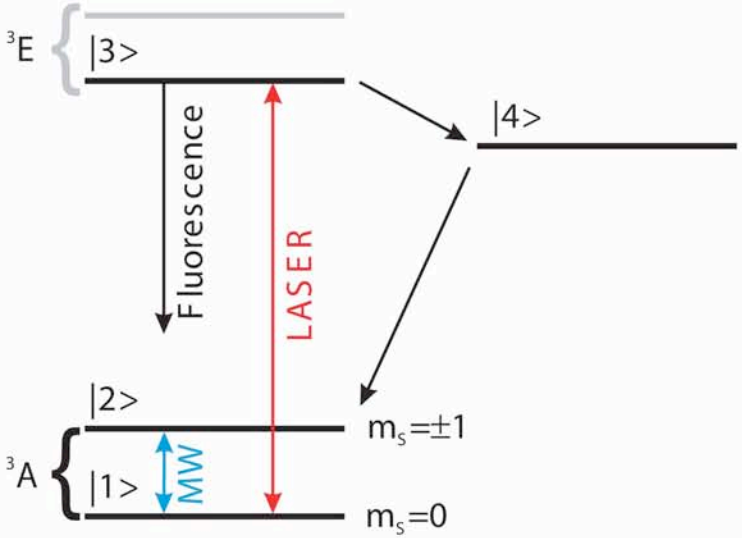
Bulk GaAs

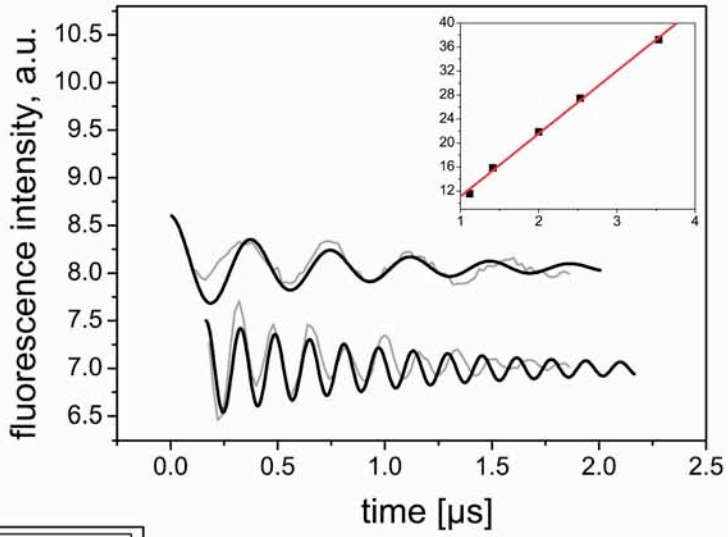
Kikkawa and Awschalom, PRL 80, 4313 (1998).

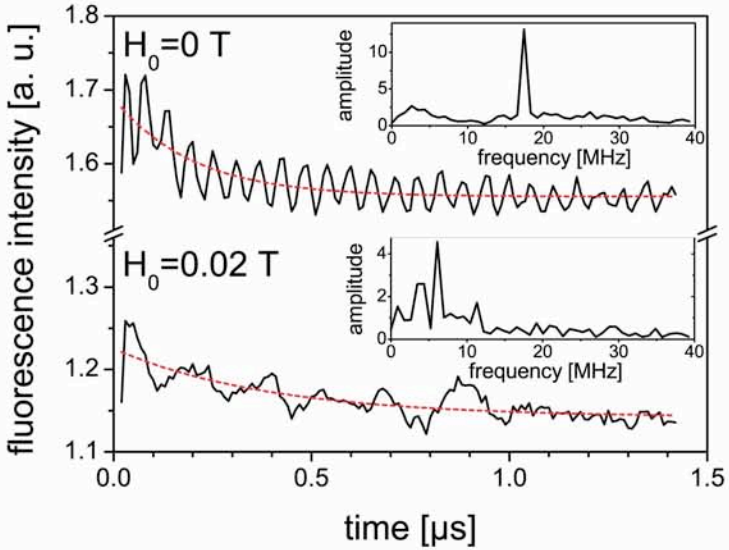


Rabi Oscillations in Single Spin

NV center in diamond: Jelezko, et al., cond-mat/0309079







Quantum Information Devices are Real

Quantum Key Distribution (Quantum Cryptography)

- *demonstrated and commercially available*
- *much room for improvement:*
  - *more efficient single-photon sources*
  - *quantum repeaters*
  - *error correction*

Quantum Computation

- *demonstration calculations have been done*
- *several techniques have been explored*
- *many pessimists have already been proven wrong*
- *the ability to manipulate quantum coherence is*
  - *not unique to any particular physical system*
- *the challenge ahead should not be underestimated*
- *the payoffs are unpredictable, but may be huge*