Quantum Information Processing

Jonathan Jones

http://nmr.physics.ox.ac.uk/teaching

The Information Age

Communication

Shannon

Computation

Turing

Current approaches are essentially classical

which is wrong "…because Nature isn't classical dammit!" (Feynman)

Classical Information

- Classical information is made up of bits, which can be in either of two states, 0 and 1

- Bits can (in principle) be measured perfectly
- Bits can be measured without disturbance
- Bits can be copied without restriction
- Local manipulations cannot affect other distant bits

Qubits

- Bits can be mapped to the eigenstates $|0\rangle$ and $|1\rangle$ of a two state quantum system (a qubit)
- If a qubit is confined to its eigenstates then it behaves much like a classical bit
- But qubits are not confined to eigenstates: they can exist in superpositions of these states opening up entirely new forms of information processing!

Quantum Information

- Qubits can be superpositions of two different states at the same time
- Qubits cannot be measured perfectly
- Qubits cannot be measured without disturbance
- Qubits cannot be copied
- Local manipulations on one qubit can affect other distant qubits

Quantum “technologies”

- Quantum Communication: quantum dense coding, quantum cryptography, quantum teleportation (Hilary)
- Quantum Computing: surpassing the classical limits (Trinity)
- Quantum Mechanics: insights into the foundations of quantum theory

Qubits & quantum registers

Classical Bit

0 or 1

Quantum Bit

0 or 1 or 0 1

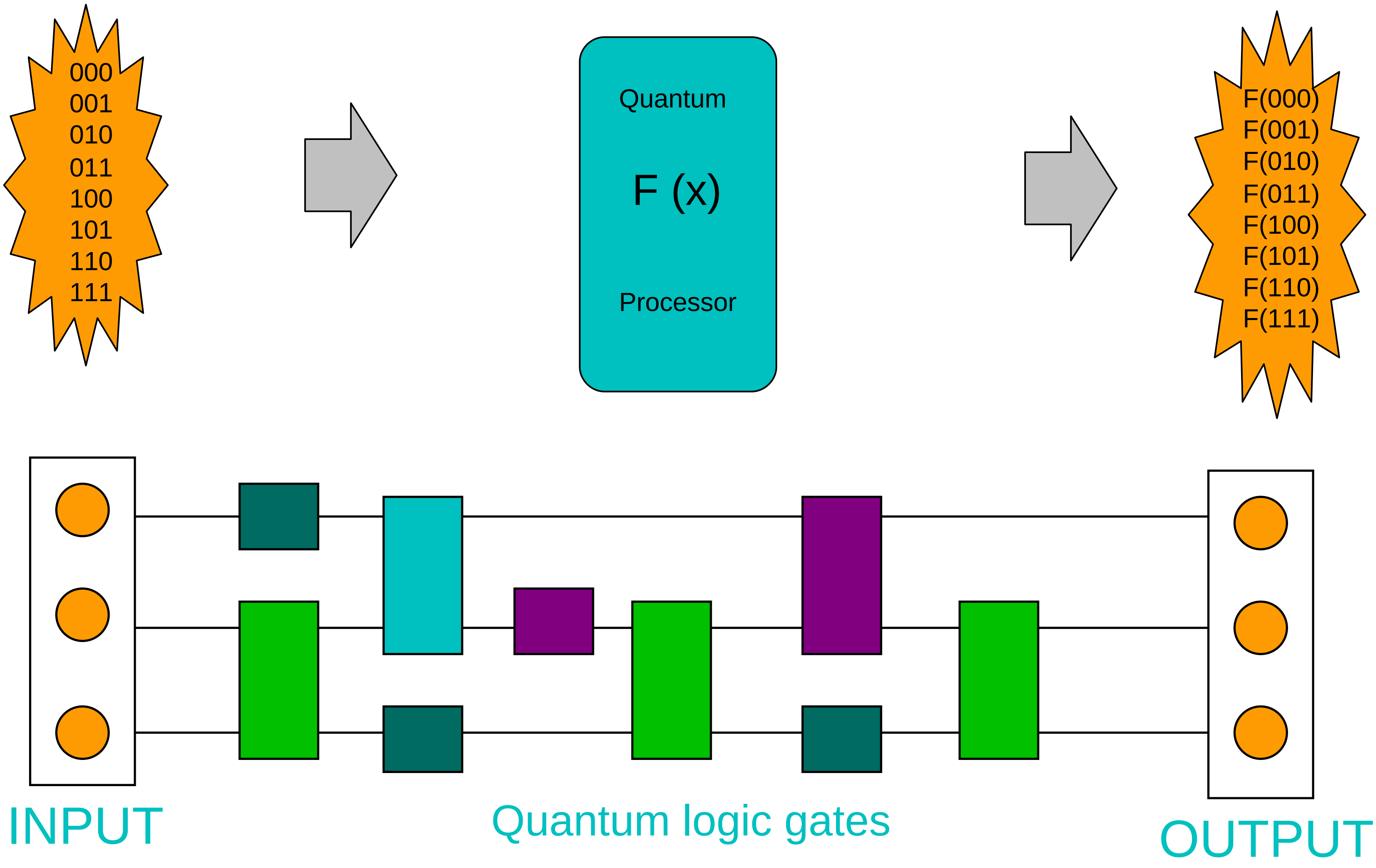
Classical register

101

Quantum register

000 001 010 011
100 101 110 111

Quantum parallel processing



000
001
010
011
100
101
110
111

Quantum

F (x)

Processor

F(000)
F(001)
F(010)
F(011)
F(100)
F(101)
F(110)
F(111)

INPUT

Quantum logic gates

OUTPUT

Exponential power

Qubits	Computations
1	2
2	4
4	16
8	256
16	65536
32	4.29×10^{9}
64	1.84×10^{19}
128	3.40×10^{38}

Power of quantum computing

- A quantum computer with 400 qubits could in principle perform more calculations in one step than could have been performed by a classical computer made from the entire visible universe
- In practice you need to use extra qubits to make the calculations work properly
  - A quantum computer with 4000 qubits could easily outperform *any conceivable* classical computer
  - These speed gains are only achievable for *some* calculations

Getting the answer out…

- Quantum computers could perform vast numbers of computations in parallel
- But we can’t access all that power directly! At the end of the day we can only read out a single result
- Quantum algorithms are all about extracting small pieces of useful information which are hard to compute in other ways

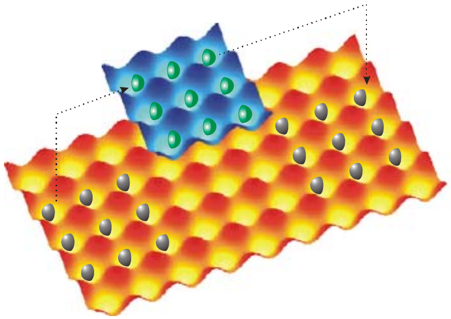
What could we do with one?

- Simulate quantum mechanics in complex systems: from astrophysics to zoology
- Factorise big numbers with Shor’s algorithm: the end of classical cryptography?
- Speed up searches: Grover’s algorithm
- Quantum computing is not the answer to everything

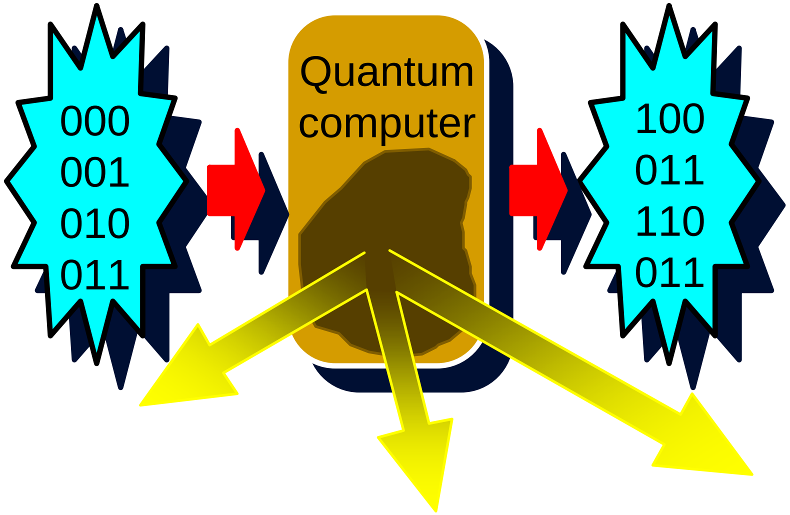
How might we build one?

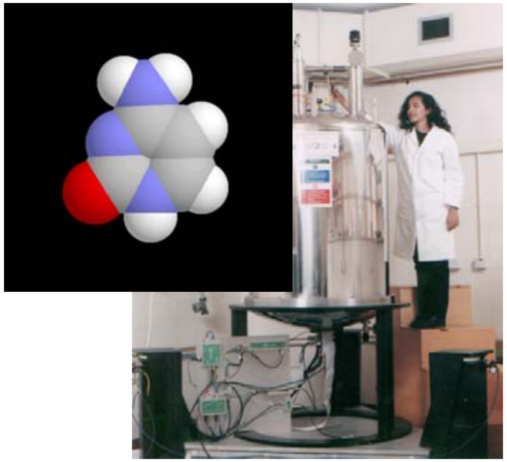
- To build a quantum computer you need
- Quantum objects (to act as qubits),
- Interacting strongly with one another (to build logic gates),
- Isolated from the environment (stable), but
- Accessible from the outside world for input, output and control
- Small quantum computers (2–7 qubits) already exist!

Technologies

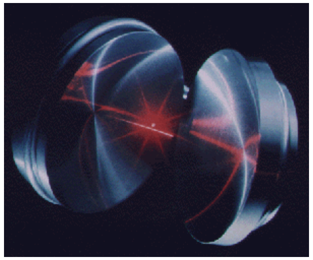


optical lattices

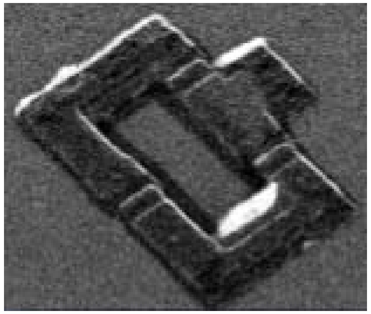




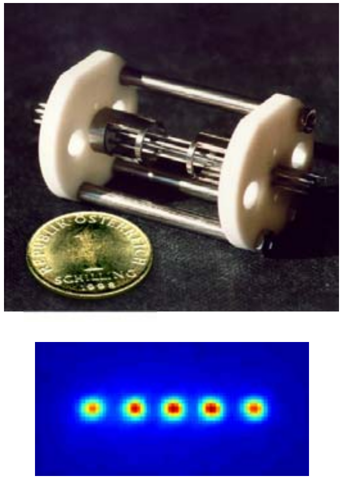
NMR



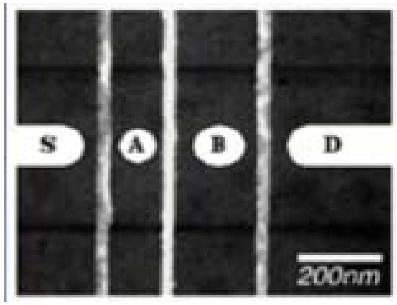
cavity QED



superconductors



ion traps



quantum dots

ARDA Roadmap 2004

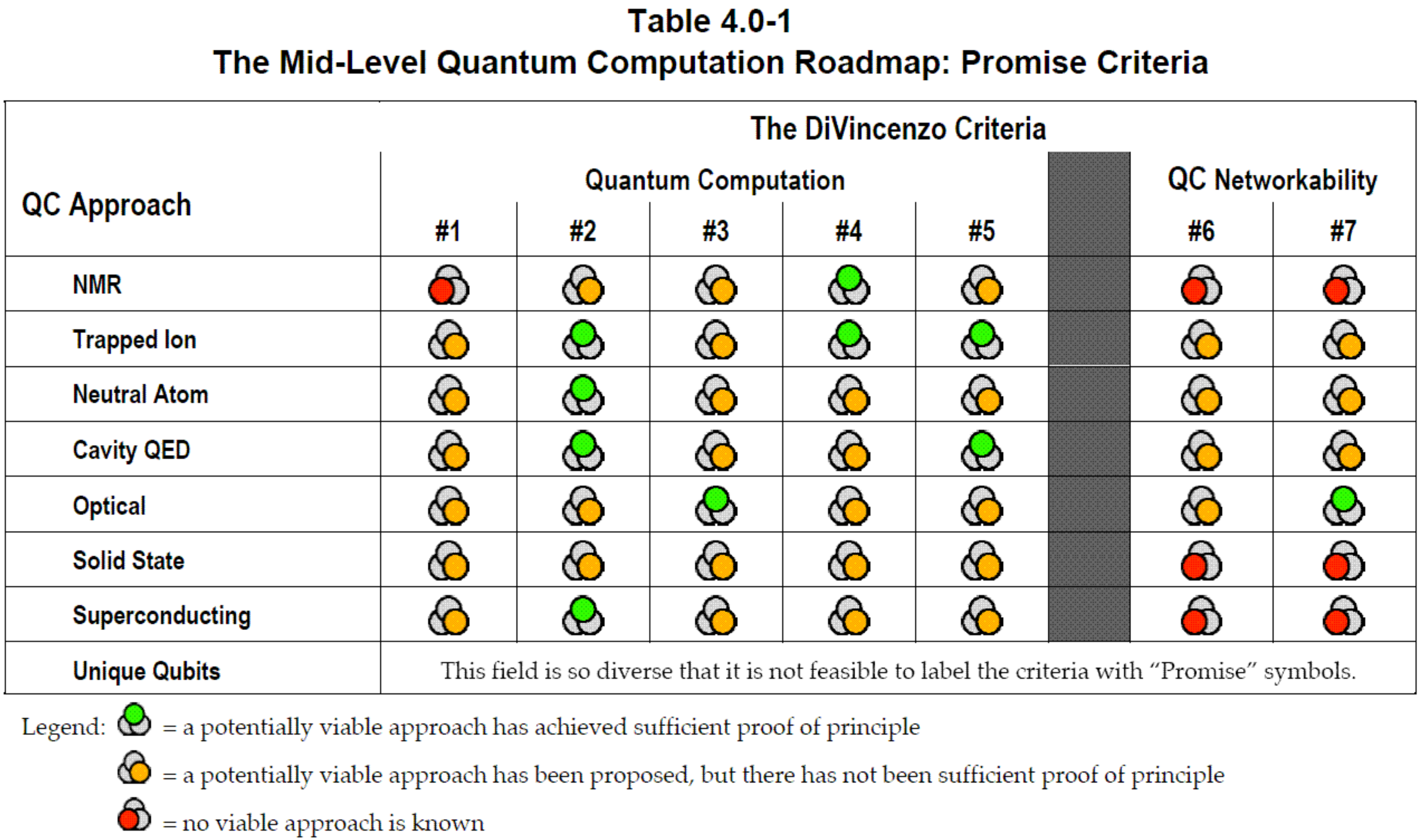


Table 4.0-1

The Mid-Level Quantum Computation Roadmap: Promise Criteria

QC Approach	The DiVincenzo Criteria							
	Quantum Computation						QC Networkability	
	#1	#2	#3	#4	#5		#6	#7
NMR	🔴	🟠	🟠	🟢	🟠		🔴	🔴
Trapped Ion	🟠	🟢	🟠	🟢	🟢		🟠	🟠
Neutral Atom	🟠	🟢	🟠	🟠	🟠		🟠	🟠
Cavity QED	🟠	🟢	🟠	🟠	🟢		🟠	🟠
Optical	🟠	🟠	🟢	🟠	🟠		🟠	🟢
Solid State	🟠	🟠	🟠	🟠	🟠		🔴	🔴
Superconducting	🟠	🟢	🟠	🟠	🟠		🔴	🔴
Unique Qubits	This field is so diverse that it is not feasible to label the criteria with "Promise" symbols.							

Legend: 🟢 = a potentially viable approach has achieved sufficient proof of principle

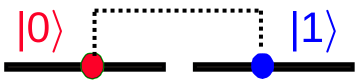
🟠 = a potentially viable approach has been proposed, but there has not been sufficient proof of principle

🔴 = no viable approach is known

NMR experiments

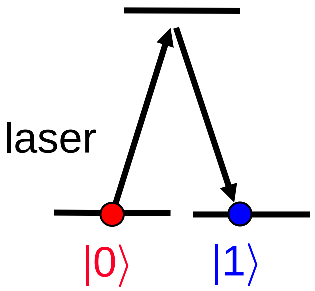
Trapped atom/ion methods

1. **quantum memory**: single atoms

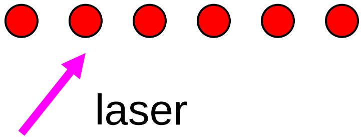


qubit in *long lived* internal states

2. **single qubit gate**



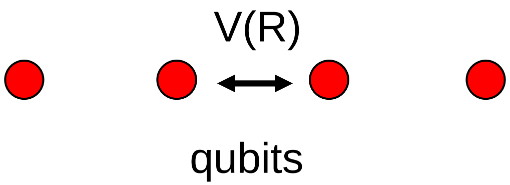
addressing a single qubit



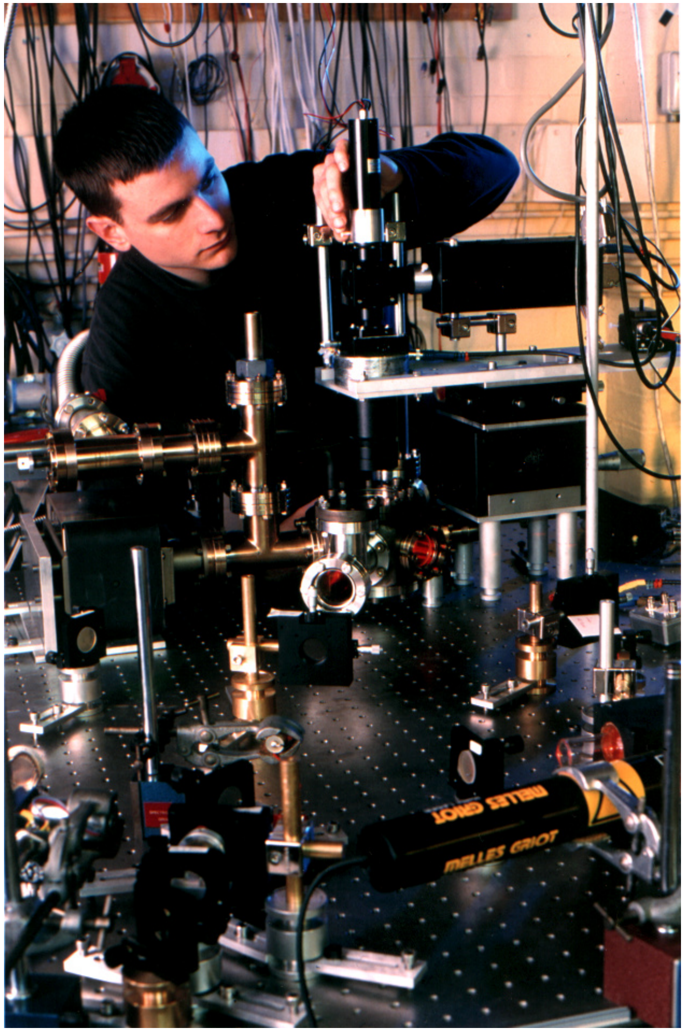
3. **two qubit gate**

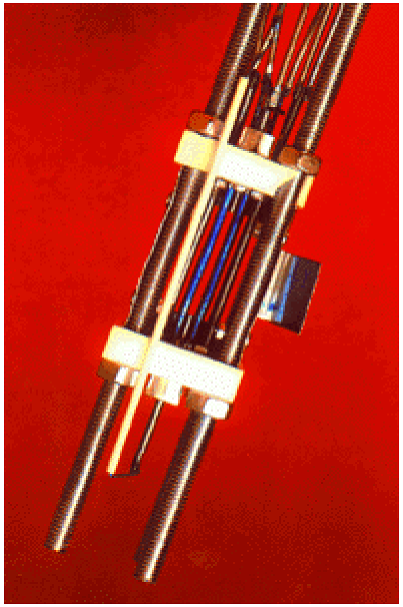
Concepts:

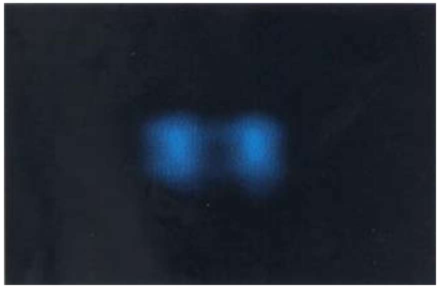
- controlled interactions based on the Coulomb force between ions
- use a collective mode as data bus (ion traps)

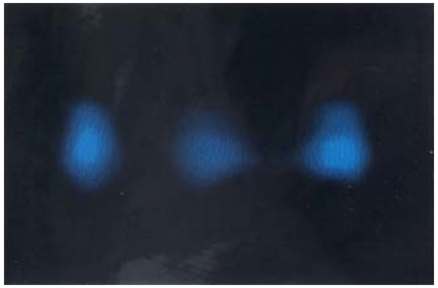


Ion experiments

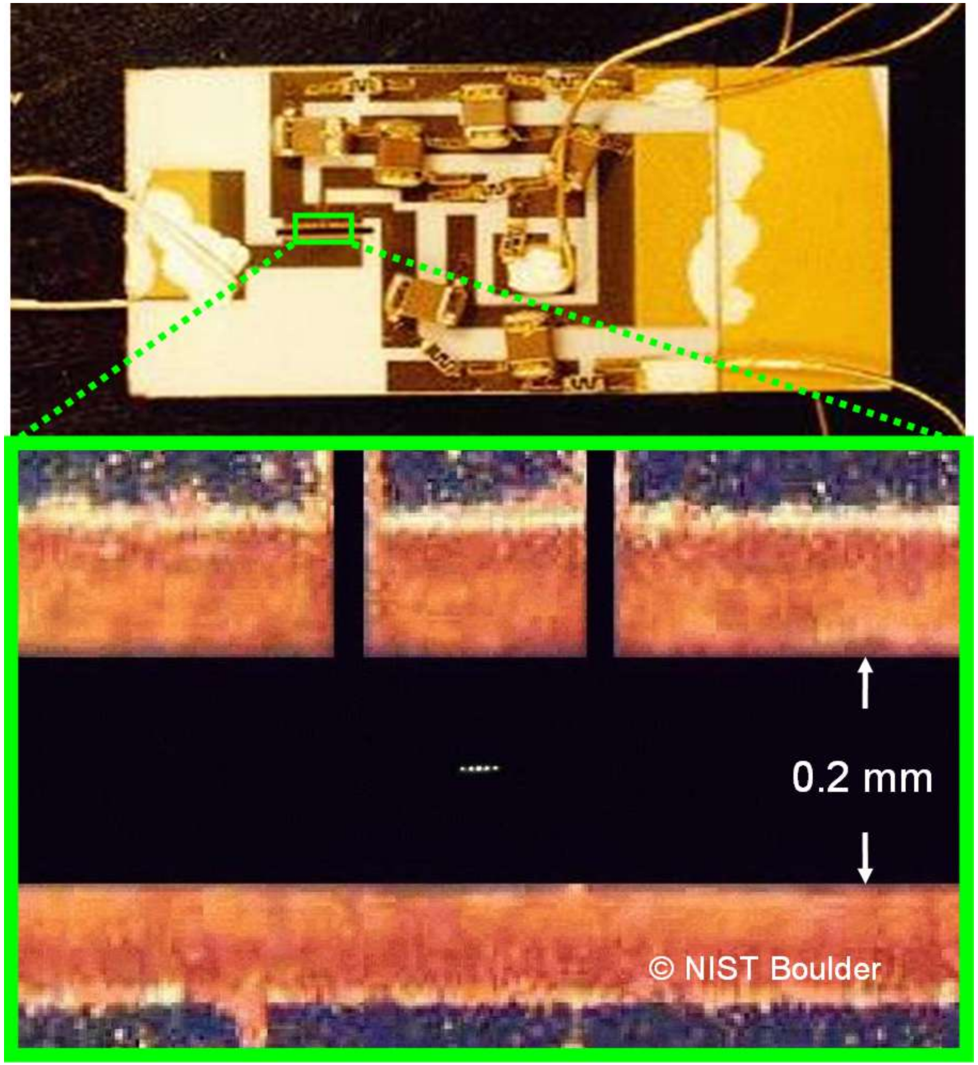








The NIST trap

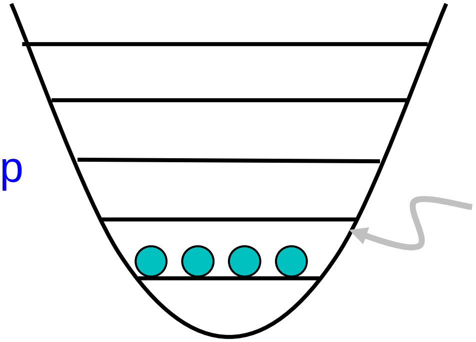


small trap electrode dimensions

pros:
-tight confinement
-better for scaling up

cons:
- surface quality essential
  impurities lead to ion heating

Bose-Einstein condensates



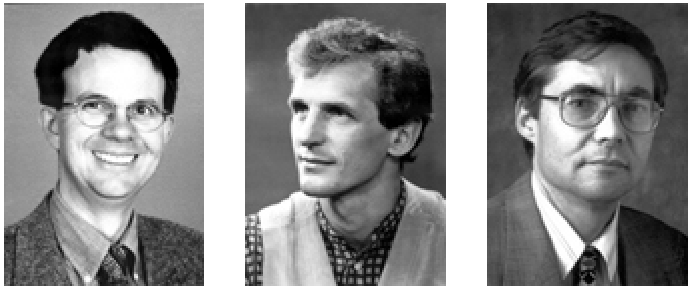
trap

ultra cold atoms

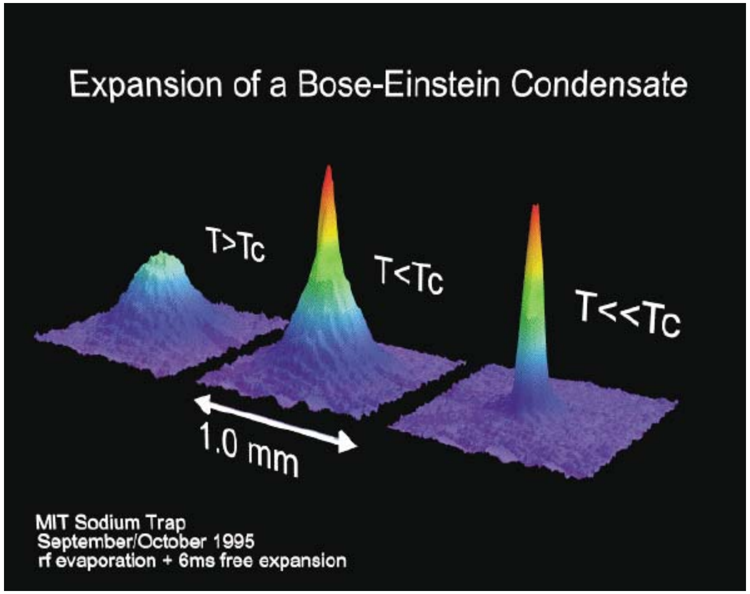
Bose Einstein condensate (BEC):

A macroscopic number of particles occupy the same one particle state, i.e.,T≈0

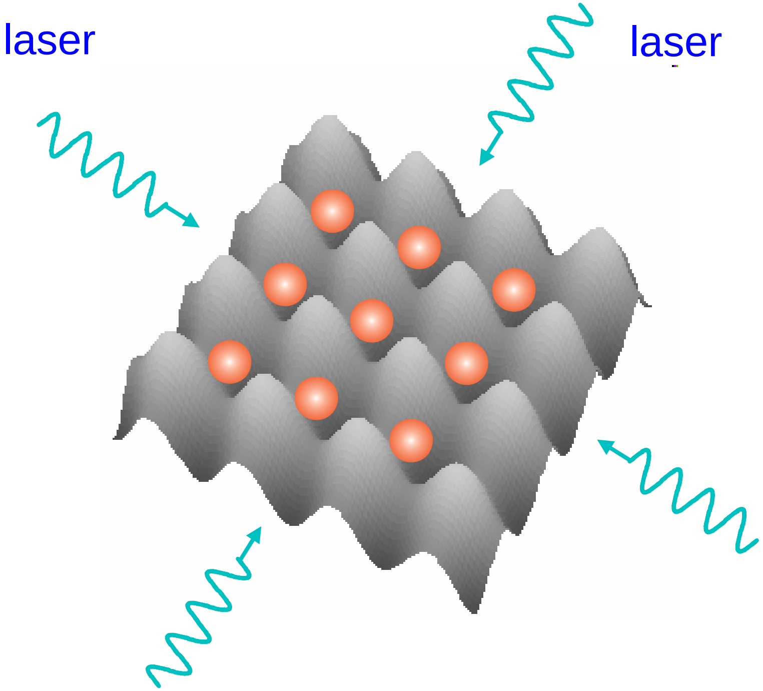
Source of ultra cold atoms
Quantum control over these atoms



Nobel prize 2001:
Cornell, Ketterle and Wieman



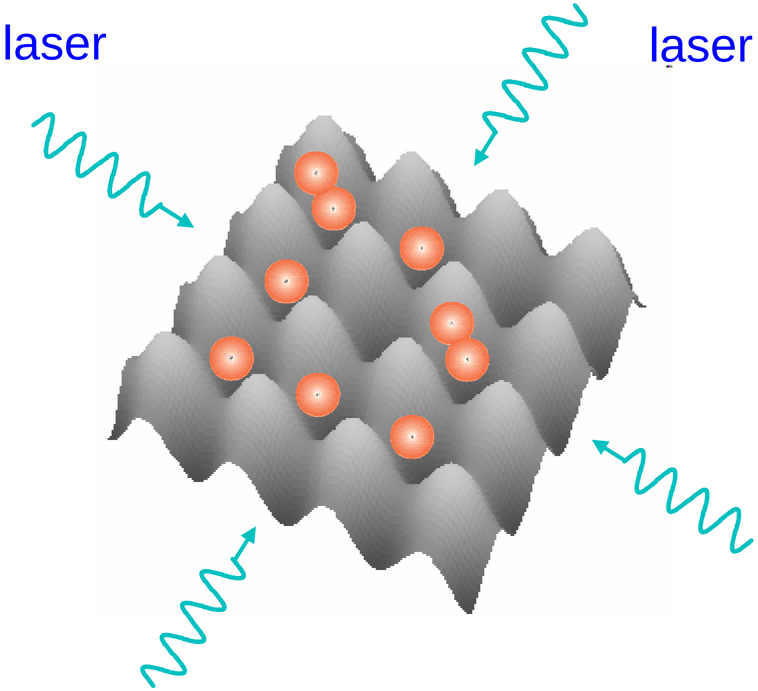
Cold neutral atoms



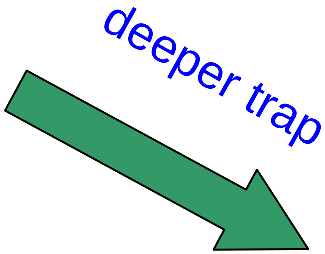
optical lattice as micro trap array

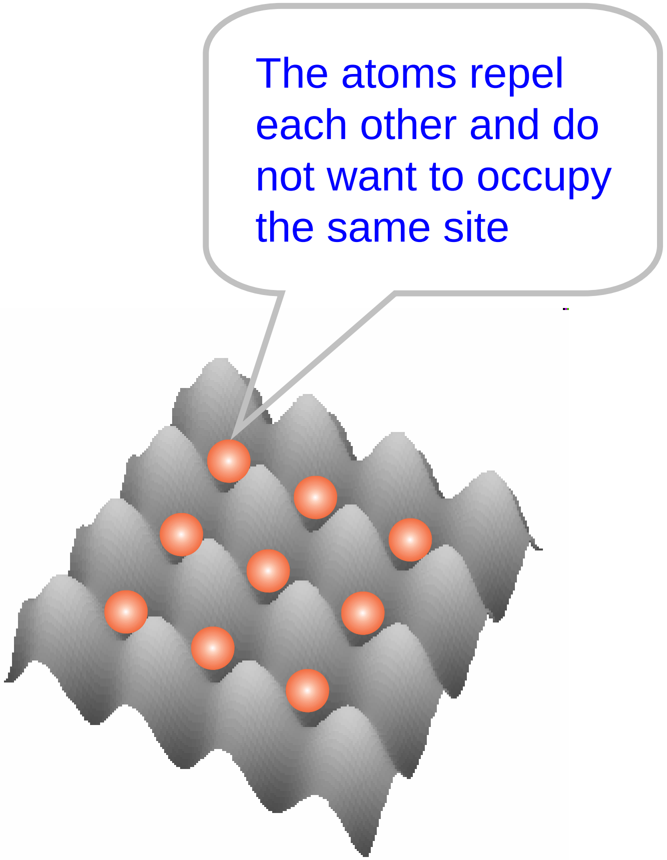
(egg box for atoms!)

Theory: Innsbruck
Experiment: München, NIST



random filling after loading with a BEC

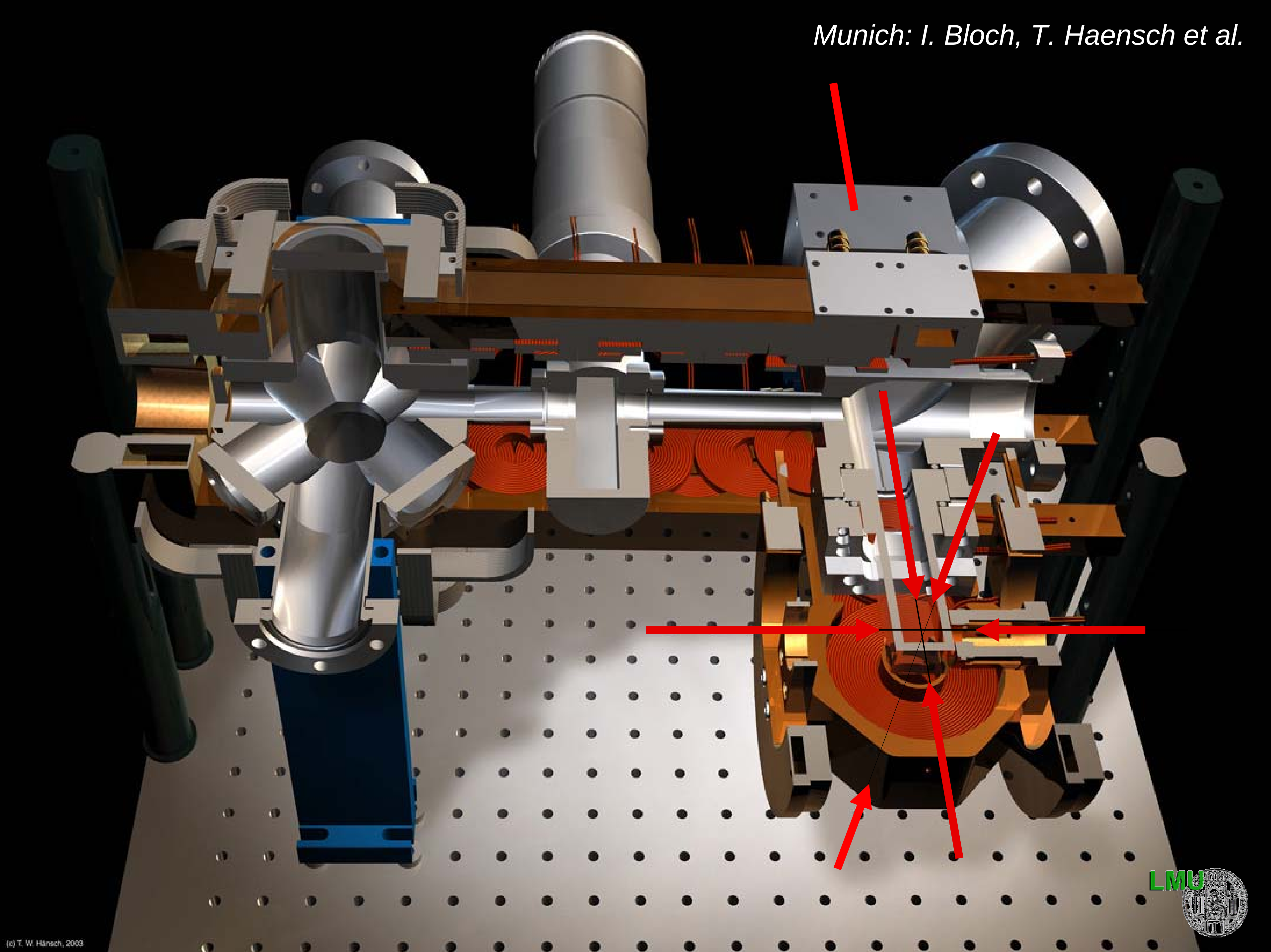




The atoms repel each other and do not want to occupy the same site

Regular filling by increasing the interaction in a deep trap

Munich: I. Bloch, T. Haensch et al.



(c) T. W. Hänsch, 2003

The EPR paradox

- Generate a pair of spin-1/2 particles in a singlet state (no total angular momentum)
  - » Generate a pair of photons by parametric down conversion
- Measure the spin of each particle along some randomly chosen basis
  - » If the measurement bases are the same for the two particles then the measurement results will be perfectly anti-correlated

Bell & Aspect

- Bell analysed this problem and showed that the predictions of quantum mechanics were inconsistent with any *local realistic* model
- Aspect *et al.* have performed a range of experiments which show that reality appears to agree with quantum mechanics
  - Nuts to Einstein, Podolsky & Rosen!
- Effects used in quantum communication

EPR cryptography 1

- Alice generates many EPR pairs and sends one half of each pair to Bob
- Alice and Bob measure their own particles along randomly chosen bases
- Alice and Bob announce the bases they used (but *not* the results they got)
- For those measurements where they used the same basis they know each others result!

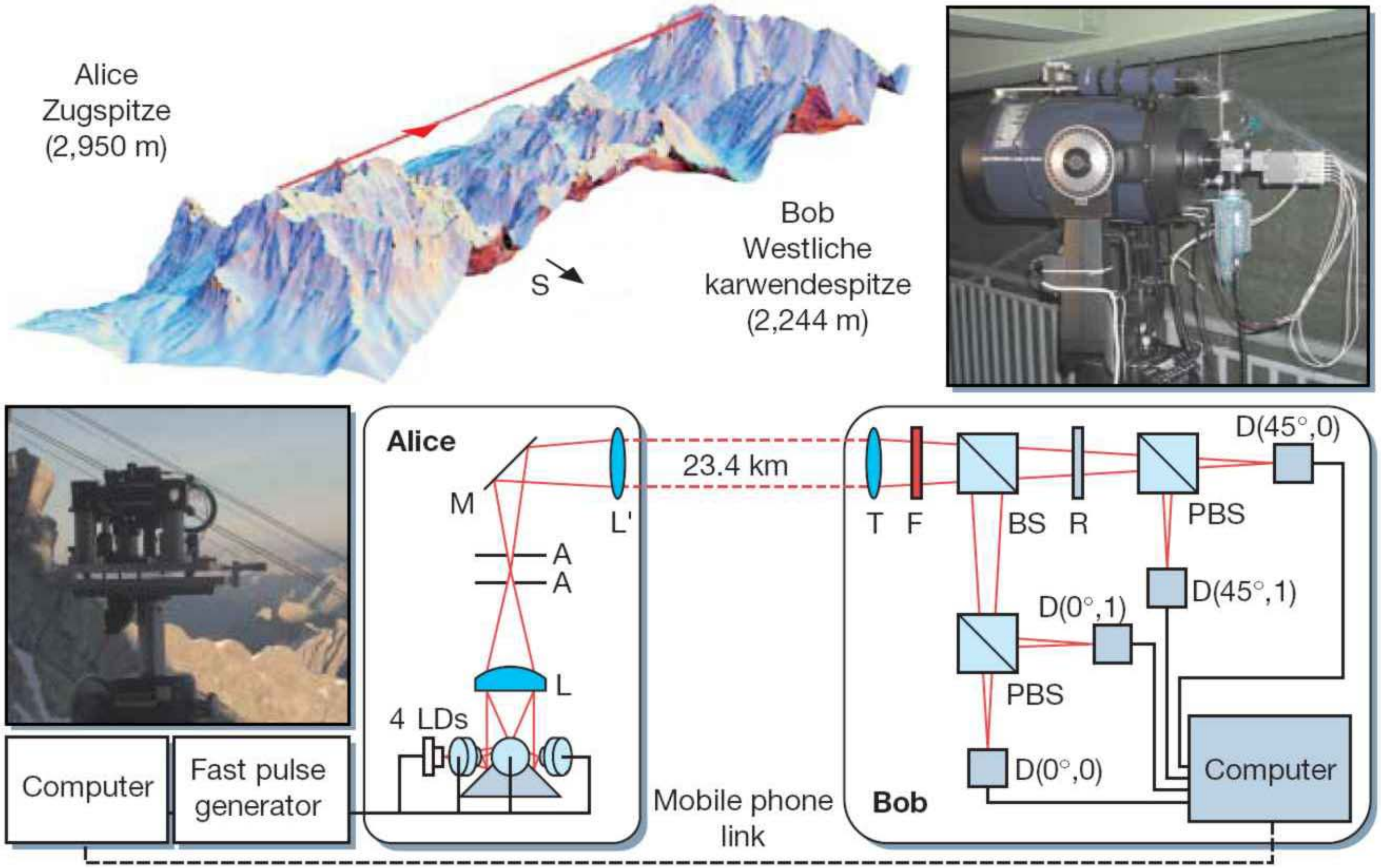
EPR cryptography 2

- Alice and Bob can use their own local results to create a *random number* which can be used as a cryptography key
- Because they built this number using EPR correlations they both have the *same* number
- Because they never announced any of their results, nobody else can know it
- A shared secret!

EPR cryptography 3

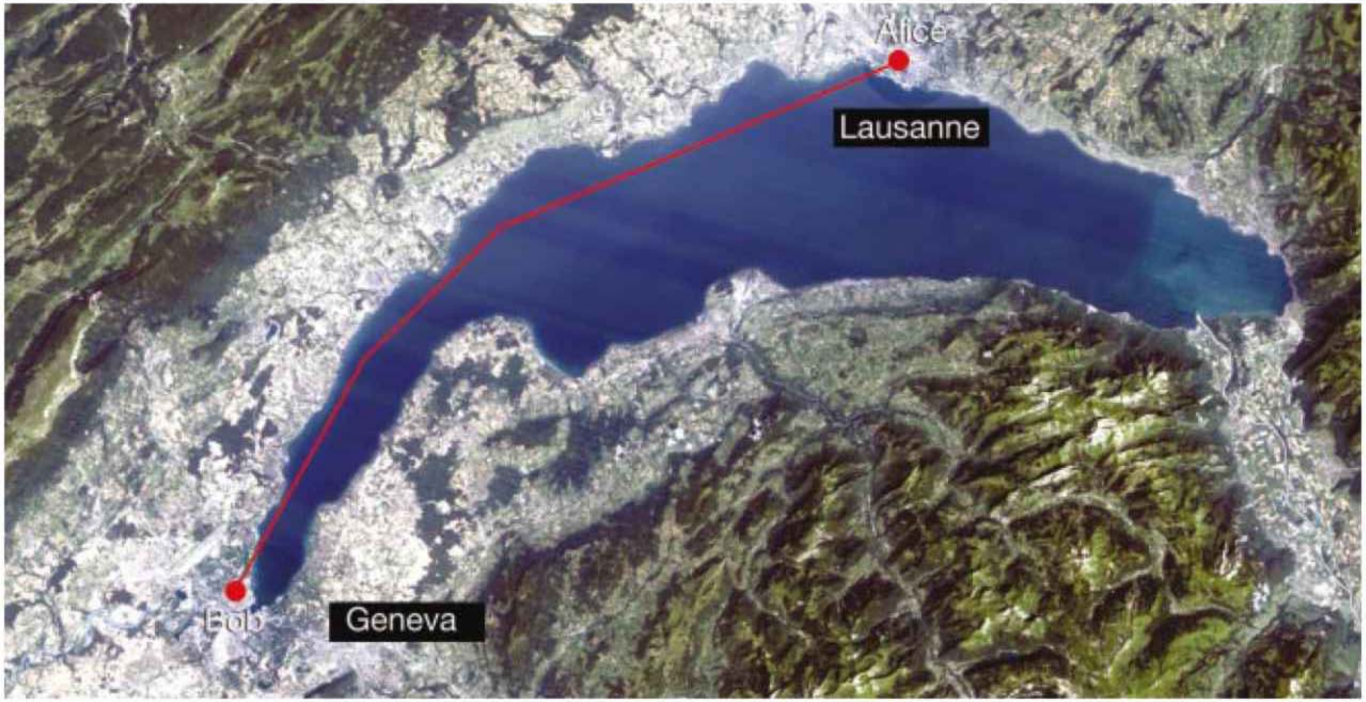
- What’s to stop an eavesdropper (Eve) from intercepting the particles which Alice sent to Bob?
- If Eve doesn’t measure the particles she doesn’t learn anything
- If Eve does measure the particles she irreparably alters their state
- Alice and Bob can always detect this

Photon experiments

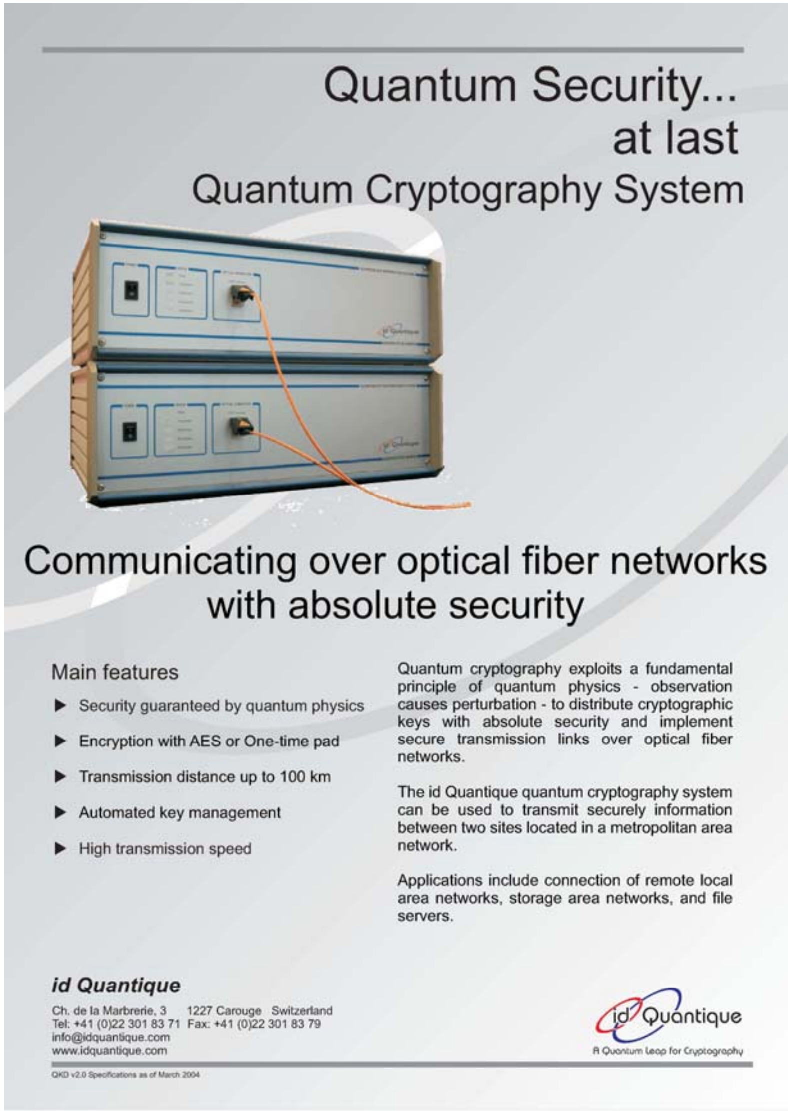


Photon experiments

Light work: keys encoded using polarized photons have been sent between Alice and Bob (left) through 67 km of fibre-optic cable under Lake Geneva.



An ideal gift…



Quantum Security...
at last

Quantum Cryptography System

Communicating over optical fiber networks with absolute security

Main features

- Security guaranteed by quantum physics
- Encryption with AES or One-time pad
- Transmission distance up to 100 km
- Automated key management
- High transmission speed

Quantum cryptography exploits a fundamental principle of quantum physics - observation causes perturbation - to distribute cryptographic keys with absolute security and implement secure transmission links over optical fiber networks.

The id Quantique quantum cryptography system can be used to transmit securely information between two sites located in a metropolitan area network.

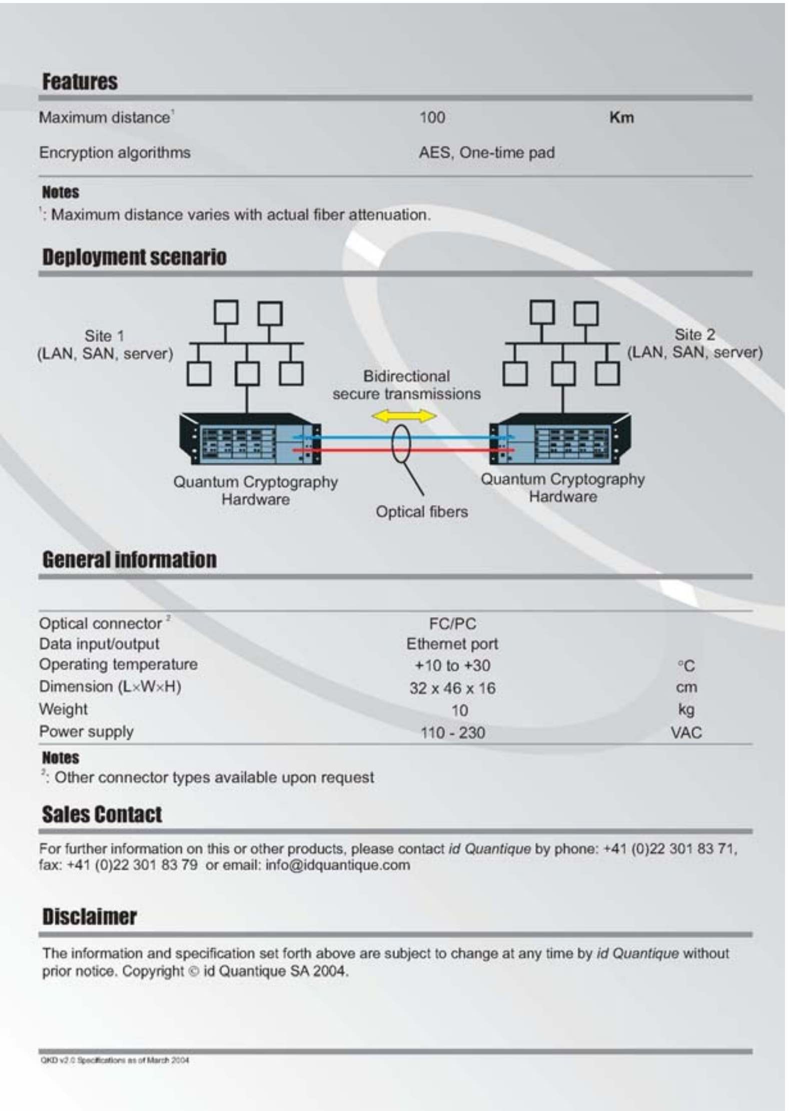
Applications include connection of remote local area networks, storage area networks, and file servers.

id Quantique

Ch. de la Marbrerie, 3 1227 Carouge Switzerland
Tel: +41 (0)22 301 83 71 Fax: +41 (0)22 301 83 79
info@idquantique.com
www.idquantique.com

id Quantique
A Quantum Leap for Cryptography

QKD v2.0 Specifications as of March 2004



Features

Maximum distance[1]	100	Km
Encryption algorithms	AES, One-time pad	

Notes

[1]: Maximum distance varies with actual fiber attenuation.

Deployment scenario

Site 1
(LAN, SAN, server)

Bidirectional
secure transmissions

Site 2
(LAN, SAN, server)

Quantum Cryptography
Hardware

Optical fibers

Quantum Cryptography
Hardware

General information

Optical connector[2]	FC/PC	
Data input/output	Ethernet port	
Operating temperature	+10 to +30	°C
Dimension (L×W×H)	32 x 46 x 16	cm
Weight	10	kg
Power supply	110 - 230	VAC

Notes

[2]: Other connector types available upon request

Sales Contact

For further information on this or other products, please contact *id Quantique* by phone: +41 (0)22 301 83 71, fax: +41 (0)22 301 83 79 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. Copyright © id Quantique SA 2004.

QKD v2.0 Specifications as of March 2004

Summary

- Quantum mechanics gives an entirely new way of looking at information (technologies)
- Quantum computers could transform much of science
  - » Assuming we ever manage to build them…
- Quantum cryptography for ultimate security
  - » Commercially available!
- Lots of lovely physics!