QUANTUM LIGHT :

A BRIEF INTRODUCTION

Philippe Grangier
Laboratoire Charles Fabry de l'Institut d'Optique,
UMR 8501 du CNRS, 91127 Palaiseau, France

Quantum Physics

* « Quantum Mechanics » elaborated at the end of the 1920's (1925 - 1927 : Schrödinger, Heisenberg, Dirac, Bohr, Born…)
« Greatest intellectual adventure of the 20th century » ?

*** Theory at the basis of our understanding of physical world :** stability and structure of matter, nature of light, interactions between matter and light...

*** Perfectly coherent formalism, huge success, incredible number of applications :** transistor (electronics and computers), laser (telecommunications and internet, medecine, biology…)

*** But... keeps a « mysterious » character :** non-deterministic theory, non-locality (in a subtle way...), no simple correspondance between « quantum objects » and the usual (macroscopic) world.

Quantum Physics

During the last 30 years, a **« second quantum revolution »*** is taking place, characterized by :

- a direct access to the « world of atoms »
(dynamics of individual quantum objects, and not only of statistical ensembles)

- a better understanding of the role of « paradoxical » quantum properties (linear superpositions, entanglement…)

The goal of this presentation is to illustrate these new ideas by using a few examples, that will exploit a lot the light quanta (« photons ») introduced by Einstein in 1905.

* Alain Aspect, in « Demain la physique », Ed. Odile Jacob, 2004

Is light made of waves or particles ?

Ancient Egypt : Light is a stream of flowers...

17th century : particles (Descartes) or waves (Huygens) ?

18th century : particles (Newton) ! ?

19th century : waves !
interferences
diffraction :
electromagnetism
Problem solved ?

20th century :
unexpected
comeback of
particles !
"Photons"

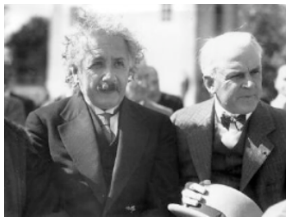
Stele Isaac Newton

Max Planck (1900) Albert Einstein (1905)

Is light made of waves or particles ?

The concept of photon was extremely difficult to admit for physicists, unti unambiguous experiments were done (Millikan, 1915)

1921 : Nobel Prize for Einstein
1923 : Nobel Prize for Millikan



At the end of the 1920's it was admitted that
all microphysics entities (photons, electrons...) have
« complementary » wave/particles properties
-> **Only possible description : Quantum Physics**

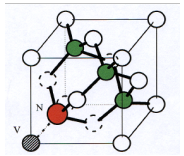
But in 1952, Erwin Schrödinger wrote :
« we never experiment with a single electron or atom or molecule… this invariably entails ridiculous consequences ».

Single Photon Sources

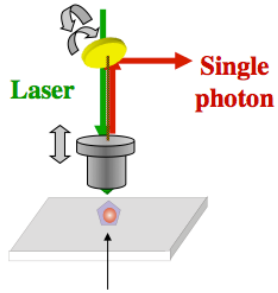
« Photon gun » ?

A usual light source emits
10^{20} photons per second

How to get only one at a time ?

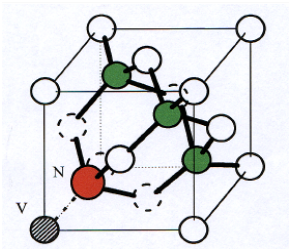


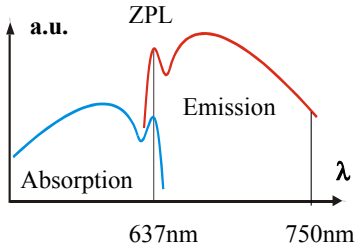
NV center :
Single nitrogen atom embedded in diamond



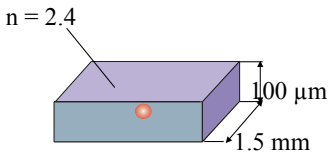
A single emitting atom !

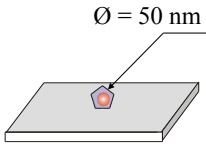
NV-Centers in diamond





Bulk or Nanocrystals

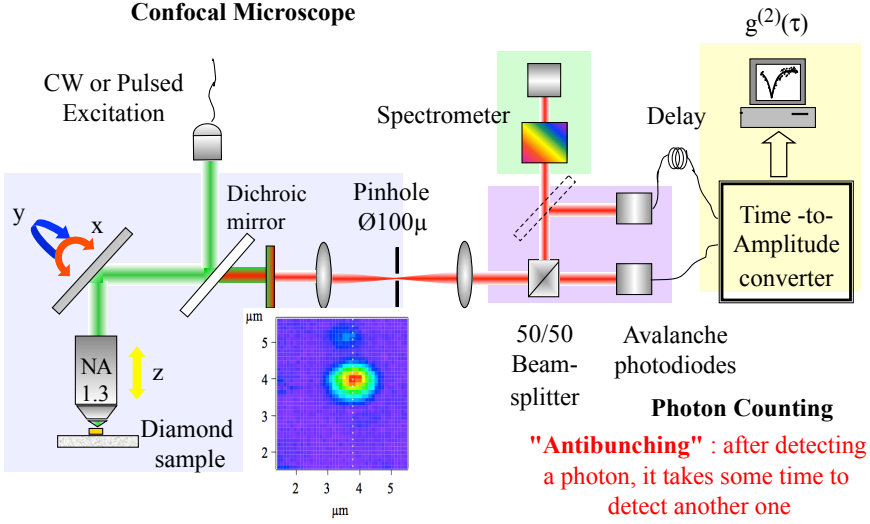




Advantages :
Less background
Better collection
Easier to handle

Experimental Setup

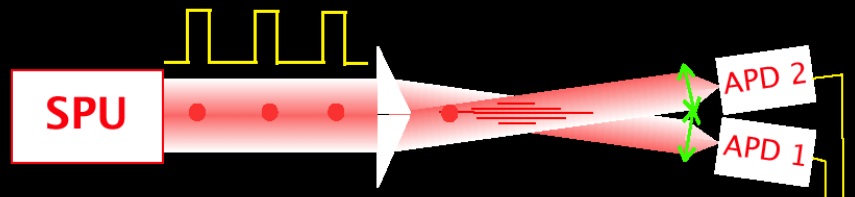
Confocal Microscope



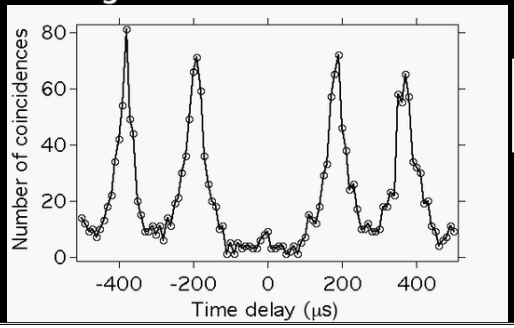
Photon Counting

"Antibunching" : after detecting a photon, it takes some time to detect another one

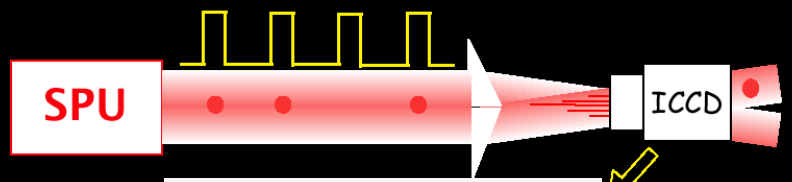
Checking that there is one photon only



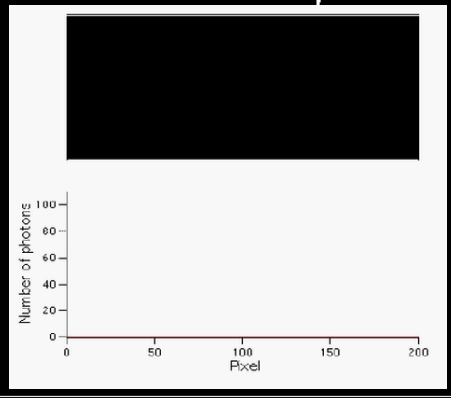
Histogramme des coïncidences



Single Photon Interferences



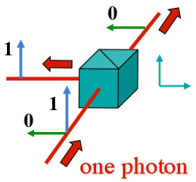
Single Photon Source : NV centers in diamond nanocrystals. Pulsed excitation: "train of single photon pulses"



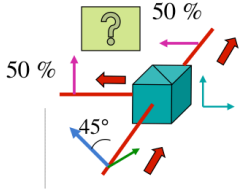
Experiment done at ENS Cachan : V. Jacques, E Wu, T. Toury, F. Treussart, J.-F. Roch.

Polarization of a Single Photon

Coding a bit (0 or 1) on the polarization of one photon

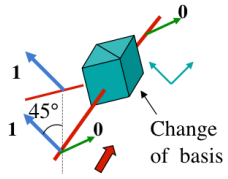


Deterministic result



Random result

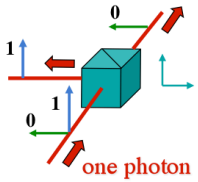
A useful information is extracted if and only if the basis used by the emitter (coding) and by the receiver (detecting) are the same !



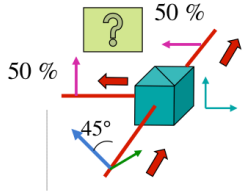
Deterministic result

Polarization of a Single Photon

Coding a bit (0 or 1) on the polarization of one photon



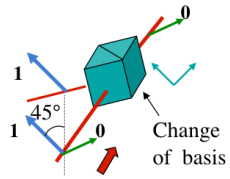
Deterministic result



Random result

The polarization of a single photon carries a "quantum bit" or "qubit"

$$|45°\rangle = (|h\rangle + |v\rangle)/\sqrt{2}$$
$$|135°\rangle = (|h\rangle - |v\rangle)/\sqrt{2}$$



Deterministic result

Quantum Information

New point of view at the end of the 20th century (1984-1994) :
Is it possible to use the photon (and quantum objects in general) to transmit or process information more efficiently ?

« Quantum Information Processing and Communications »

Two main applications, actively studied :

1. Quantum cryptography
quantum key distribution (Bennett Brassard 1984).

2. Quantum computing
exponential acceleration of
some algorithms (factorization : Shor 1994).

Main topics

1. The light, wave and/or particle ?

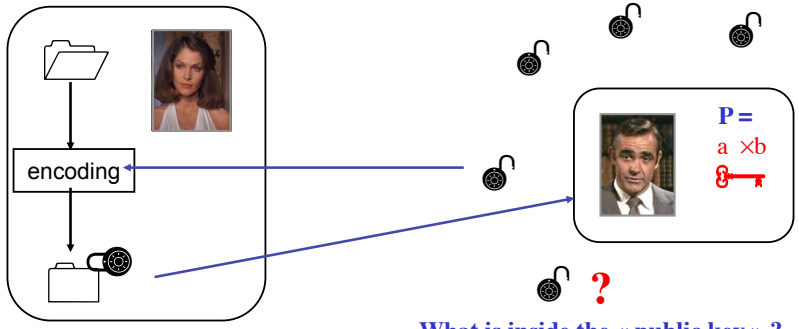
2. Quantum cryptography :
from principles to experimental implementations

3. Entangled qubits and quantum computing

The characters

Public key cryptosystems

Rivest, Shamir et Adelman (RSA, 1978)



What is inside the « public key » ?
the product P of two large numbers :
factorization very difficult to perform !

Factorising RSA 155 (512 bits - summer 1999)

« Challenge » proposed the RSA company (www.rsa.com)
Previous record : RSA140 (465 bits), february 1999

RSA155 = 109417386415705274218097073220403576120037329454492\
059909138421314763499842889347847179972578912673324976257528\
997818337970765372440271467435315933543338 97;

RSA155 is not a prime ! ("probabilistic" algorithm, very fast)

Factorization ? **Preparation :** 9 weeks over 10 workstations.
Sieve : 3.5 months over 300 PCs , 6 countries
Result : **3.7 Go, stored in Amsterdam**
Processing : 9.5 days on Cray C916, Amsterdam
Factorization: 39.4 hours on 4 workstations

f1 = 102639592829741105772054196573991675\
900716567808038066803341933521790711307779;
f2 = 106603488380168454820927220360012878\
679207958575989291522270608237193062808643;
f1 and f2 are primes, and f1 * f2 = RSA155 (immediate onPC)

« Challenges » proposed by the company RSA

number	digits	date completed	sieving time	algorithm
C116	116	1990	275 MIPS years	mpqs
RSA-120	120	June, 1993	830 MIPS years	mpqs
RSA-129	129	April, 1994	5000 MIPS years	mpqs
RSA-130	130	April, 1996	1000 MIPS years	gnfs
RSA-140	140	February, 1999	2000 MIPS years	gnfs
RSA-155	155	August, 1999	8000 MIPS years	gnfs
C158	158	January, 2002	3.4 Pentium 1GHz CPU years	gnfs
RSA-160	160	March, 2003	2.7 Pentium 1GHz CPU years	gnfs
RSA-576	174	December, 2003	13.2 Pentium 1GHz CPU years	gnfs
C176	176	May, 2005	48.6 Pentium 1GHz CPU years	gnfs
RSA-200	200	May, 2005	121 Pentium 1GHz CPU years [*]	gnfs

Improvement by two orders of magnitude between 1999 and 2005...

PUBLIC KEY CRYPTOSYSTEMS

- Problems :

- Mathematical demonstrations about PKC have a statistical character (the factorisation may be found easily for "unfortunate choices" of a, b)
--> "recommendations" for the choice of the prime numbers a and b

- **No absolute demonstration for security** -> better computers, better algorithms (obviously kept secret) ?

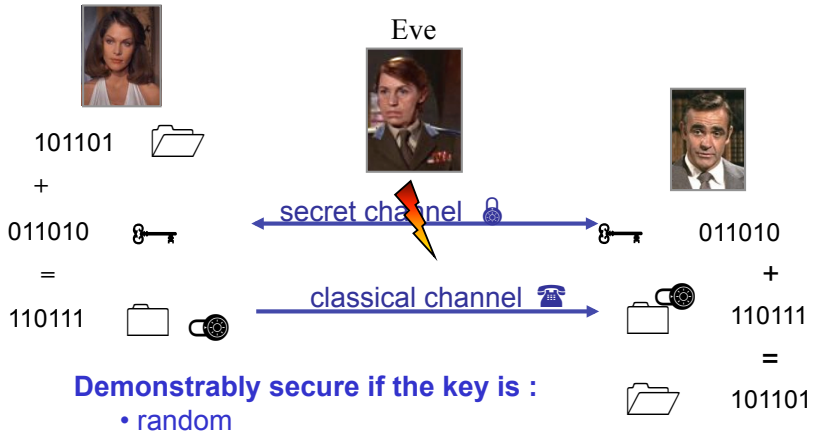
- Article by Peter Shor (1994) :

a "quantum computer" might be able to factorize the product of two prime numbers in a "polynomial" time ! *lot of reactions !*

Best classical algorithm (number field sieve) :
nfs[n] = Exp[1.9 Log[n]$^{1/3}$ Log[Log[n]]$^{2/3}$] **nfs[2^{1024}] / nfs[2^{512}] = 6.2 10^6**

Shor algorithm : shor[n] = Log[n]^3 **shor[2^{1024}] / shor[2^{512}] = 8**

Secret key cryptosystem : one-time pad (G. Vernam, 1917)



Demonstrably secure if the key is :
- random
- as long as the message
- used only once (Shannon)

Quantum Secret Key Cryptosystem : Bennett-Brassard (1984)

101101 + 011010 = 110111

quantum channel

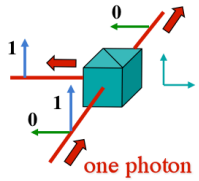
classical channel

011010 + 110111 = 101101

Demonstrably secure if the key is :

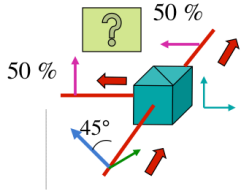
- random
- as long as the message
- used only once (Shannon)
- **unknown by Eve : Quantum laws !**

Polarization of a Single Photon



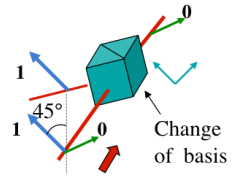
Coding a bit (0 or 1) on the polarization of one photon

Deterministic result



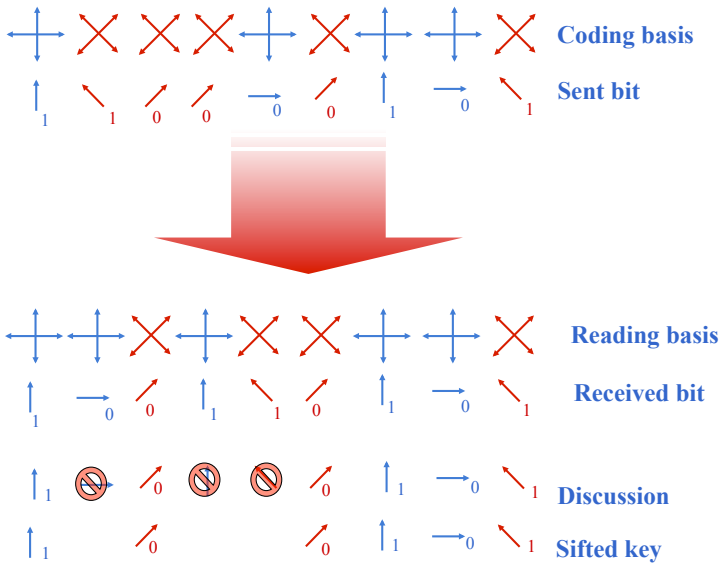
Random result

A useful information is extracted if and only if the basis used by the emitter (coding) and by the receiver (detecting) are the same !

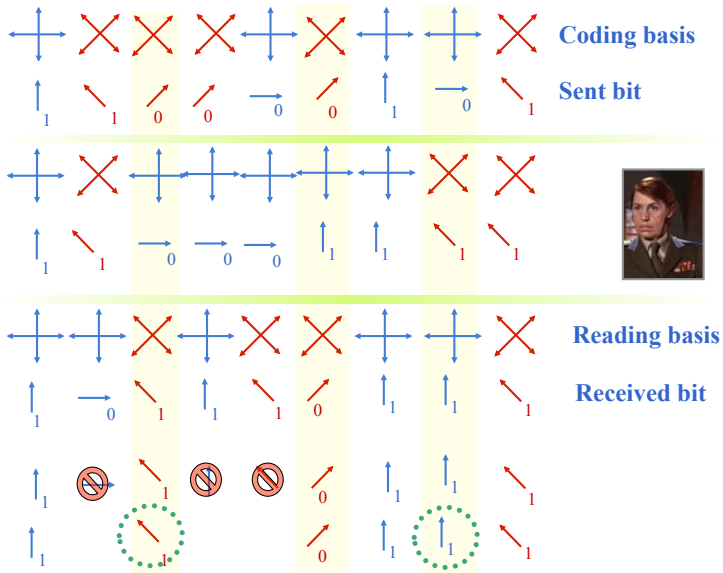


Deterministic result

« BB84 » Protocol (Bennett and Brassard, 1984)



« BB84 » Protocol (Bennett and Brassard, 1984)



Institut d'Optique

QUANTUM CRYPTOGRAPHY : PRINCIPLE
(C. Bennett and G. Brassard, 1984)

QIPC / S4P

Eve has to make a measurement without knowing the basis used by Alice
(this information comes too late for her !)

- intercept / resend using either the + or x basis
- intercept / resend using an optimized basis (22.5°)
- use quantum non-demolition measurements…
- duplicate (clone) photons and keep one aside…

All such measurements will create errors in the transmission
(the more Eve knows, the more errors !)

*** Evaluation of errors :**

After the initial exchange between Alice and Bob
measure the error rate by comparing publicly a part of the raw key:
-> evaluation of the amount of information (maybe) available to Eve.

*** Classical post-processing (essential for security !)**

Requires a public authenticated channel

*** Alice and Bob have a totally secure and errorless secret key**
(non-zero size if initial QBER < 11%)

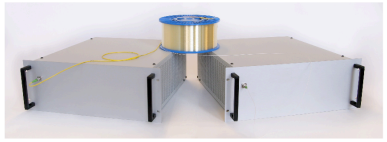
Industrial Perspectives ?

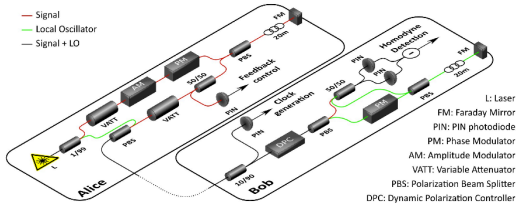
*** Several startups worldwide are selling QKD systems** (optical fibers, 50 km)

IdQuantique
(Genève)

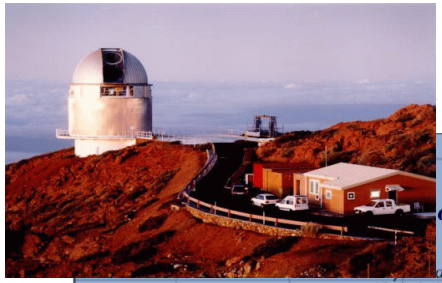
MagiQ Technologies
(New York)

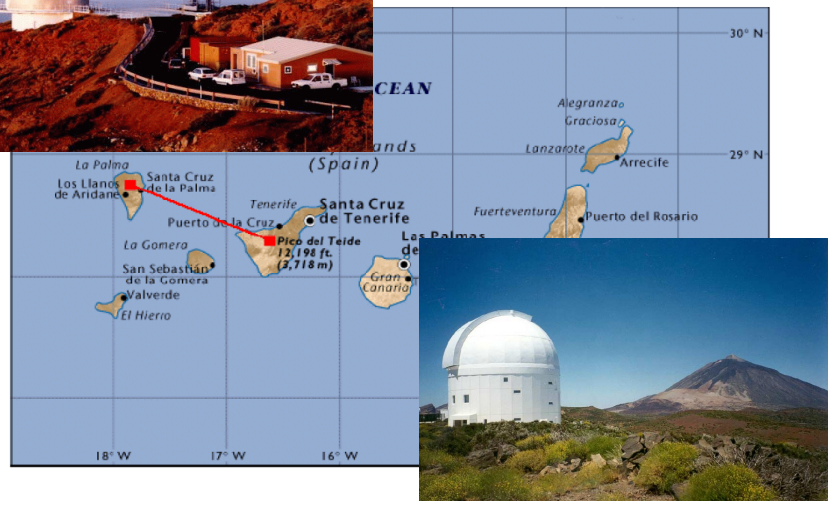
SEQURENET
A QUANTUM KEY TO NETWORK SECURITY



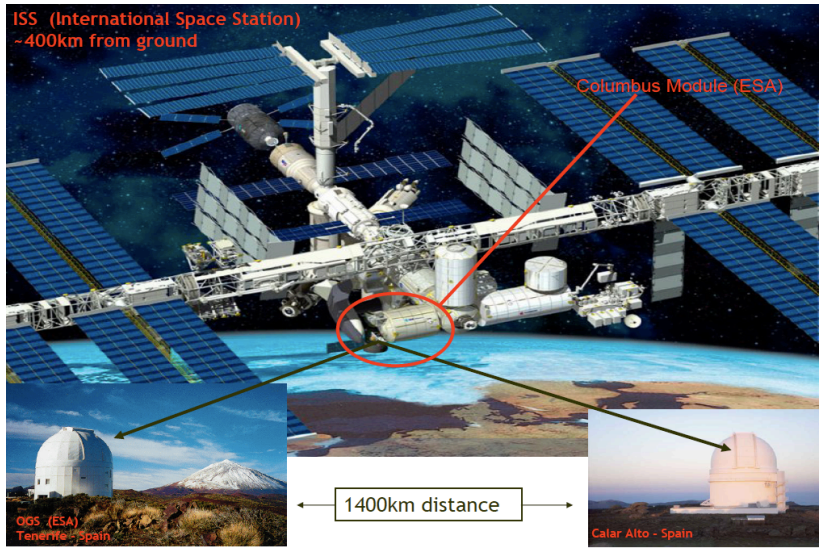


LaPalma and Tenerife





Quantum cryptography with satellites



Main topics

1. The light, wave and/or particle ?

2. Quantum cryptography :
   from principles to experimental implementations

3. Entangled qubits and quantum computing

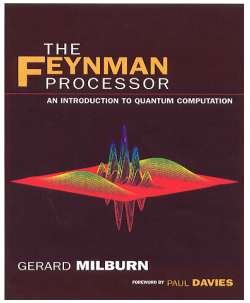
Next steps...

* Quantum cryptography has been making nice progress

  - commercial systems are available

  - present challenges : network opertation, certification, market

* What about quantum computing ?



QUBITS

Classical bit : 2 states 0 and 1

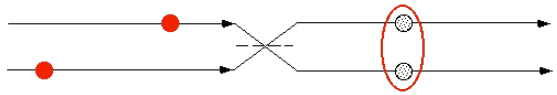
Quantum bit : 2 states $|0\rangle$ and $|1\rangle$, plus arbitrary superpositions :

$$|\psi\rangle = \cos(\theta)\, e^{i\varphi} |0\rangle + \sin(\theta)\, e^{-i\varphi} |1\rangle$$

Simple exemples :

Polarised photon

"Split photon"



-> very useful for quantum cryptography

QUANTUM COMPUTING : REGISTERS

"Analog" classical computing ? (continuous values) : no

N bits with possible values 0 and 1

Register : | ε(1) | ε(2) | ε(3) | ε(4) | .... | ε(N) | (ε=0 ou 1)

State of a classical analog computer : N continuous variables ε(i)

Possible state of the computer : $|\varepsilon(1), \varepsilon(2), \varepsilon(3), \varepsilon(4) .... \varepsilon(N)\rangle$ (ε=0 or 1)

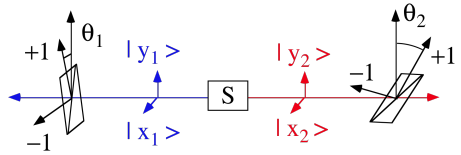
General state of the computer : $\sum c_x \; |\varepsilon(1), \varepsilon(2), \varepsilon(3), \varepsilon(4) .... \varepsilon(N)\rangle$

State of a quantum computer : 2^N continuous (complex) variables c_x !!!

The computer states live in a huge 2^N-dimensional Hilbert space

Most of these states are "entangled" (individual qubits have no state)

Einstein, Podolsky and Rosen « paradox » (EPR-Bohm version)



Source S emitting pairs of photons "1" and "2" in the quantum state : (| x1 x2 > + | y1 y2 >)/√2 Entangled state !

- The result is random for each photon, but measuring one polarization allows one to know the polarization of the other photon with probability unity.

- The measured polarization can be chosen arbitrarily, while the two photons are very far apart : what is « really » the polarization of the second photon ?

Einstein, Podolsky and Rosen « paradox » (1935)

Bell 's inequalities

« Hidden variables » or « supplementary parameters » denoted λ,

with a normalized statistical distribution ρ(λ) : $\int d\lambda\, \rho(\lambda) = 1$

$\varepsilon_1(\lambda,\theta_1) = \pm 1,\ \varepsilon_2(\lambda,\theta_2) = \pm 1,\quad E(\theta_1,\theta_2) = \int d\lambda\, \rho(\lambda)\, \varepsilon_1(\lambda,\theta_1)\, \varepsilon_2(\lambda,\theta_2)$

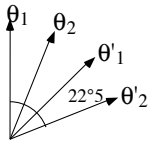
locality !

locality / freedom of choice

then : $-2 \le S \le 2$ with :

$$S = E(\theta_1,\theta_2) + E(\theta'_1,\theta_2) + E(\theta'_1,\theta'_2) - E(\theta_1,\theta'_2)$$

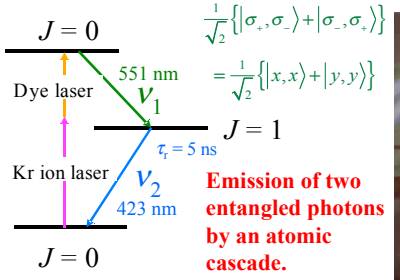
Demonstration : $\varepsilon_1(\lambda,\theta_1)\,\varepsilon_2(\lambda,\theta_2) + \varepsilon_1(\lambda,\theta'_1)\,\varepsilon_2(\lambda,\theta_2) + \varepsilon_1(\lambda,\theta'_1)\,\varepsilon_2(\lambda,\theta'_2) - \varepsilon_1(\lambda,\theta_1)\,\varepsilon_2(\lambda,\theta'_2) = \pm 2$



For the indicated angles one has $S_{QM} = 2\sqrt{2}$

Conflict ! Experimental result ?

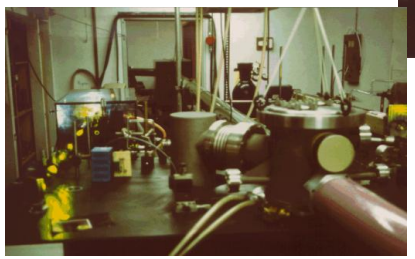
Orsay's source of pairs of entangled photons (1980-82)



$\frac{1}{\sqrt{2}}\{|\sigma_+,\sigma_-\rangle + |\sigma_-,\sigma_+\rangle\}$

$= \frac{1}{\sqrt{2}}\{|x,x\rangle + |y,y\rangle\}$

Emission of two entangled photons by an atomic cascade.



* Laser-induced two-photon excitation of a cascade in a Calcium 40 atomic beam.

☺ 100 detected pairs per second

1% precision for 100 s counting

*** Random switching of polarizers !**

Experimental tests of Bell's inequalities

Experiments with an active fast change in the polarizers orientations (initially proposed by Alain Aspect in 1976 to close the « locality loophole »)

Orsay 1982 : A. Aspect et al, Phys. Rev. Lett. 49, 1804 (1982).
- * distance between polarizers : 15 m -> L/c = 50 ns
- * measurement switching time : 20 ns (ok)
- * violation of Bell's inegalities by 6 standard deviations (15 h counting time)

Innsbruck 1998 : G. Weihs et al, Phys. Rev. Lett. 81, 5039 (1998).
- * distance between polarizers : 400 m (optical fibers) -> L/c = 1.3 μs
- * truly random and independant switching time
- * violation of Bell's inegalities by 30 standard deviations (10 s counting time).

La Palma-Tenerife 2010 : T. Scheidl et al, Proc. Natl. Acad. Sci. 107, 19708 (2010).
- * distance between polarizers :144 km (free space) -> L/c = 480 μs
- * truly random and independant switching time + ρ(λ) independant of θ1 and θ2
- * violation of Bell's inegalities by 16 standard deviations (600 s counting time).

Conclusion : Bell 's hypothesis are untenable – entangled states do exist !

QUANTUM COMPUTING : REGISTERS

General state of the computer : $\Sigma\ c_x\ |\ \varepsilon(1), \varepsilon(2), \varepsilon(3), \varepsilon(4) \ldots . \varepsilon(N)\ \rangle$

(linear superposition of all possible register states)

- During the computer evolution, all 2^N states $|\varepsilon(1) \ldots . \varepsilon(N)\ \rangle$ are involved

-> **"quantum parallelism"**

- When the state of the computer is "measured", **a single binary state** is detected (the probabilities for all other ones cancel out)

-> one keeps all the **advantages of a binary calculation.**

Very peculiar mixture of analog and binary ingredients !

"Doors can be open and closed at the same time"

QUANTUM COMPUTING

A quantum computer can implement some algorithms very efficiently :

- **factoring algorithm (Shor 1994) : exponential gain**
- **sorting algorithm (Grover 1996) : quadratic gain**

... but it is extremely difficult to realize :

- quantum states like $\Sigma\ c_i\ |\ \varepsilon(1), \varepsilon(2), \varepsilon(3), \ldots \varepsilon(N) >$ with a large N are very sensitive to all uncontrolled interactions with the environment : **"decoherence"**
- the interactions of the qubits between themselves and with the external world must be extremely well controlled, in order to simultaneously carry out the calculation, and avoid decoherence

A few encouraging results... :

- **any calculation can be carried out from 1 and 2 qubits quantum gates**
- **it it possible to design quantum error correcting codes**

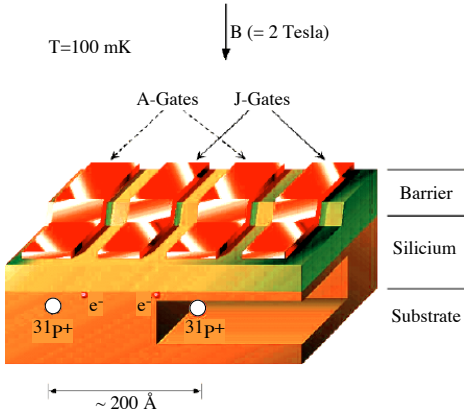
QUANTUM COMPUTER IN SILICON

Qubit : magnetic moment of phosphorus atoms individually implanted below electrodes

"A" : 1 qubit gates
"J" : 2 qubits gates

*** Technically possible**

*** Decoherence ???**

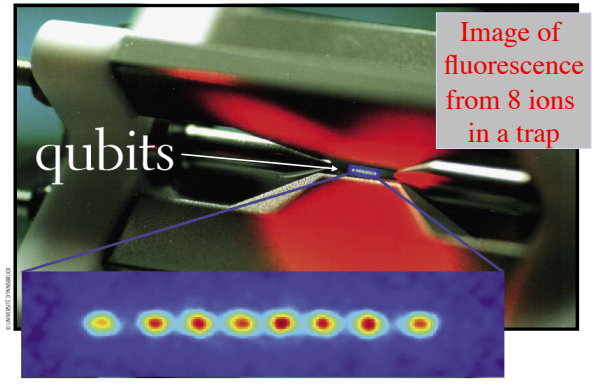


B. E. Kane, "A silicon-based nuclear spin quantum computer", Nature, Vol. 393, p. 133, 1998

LINEAR ION TRAPS

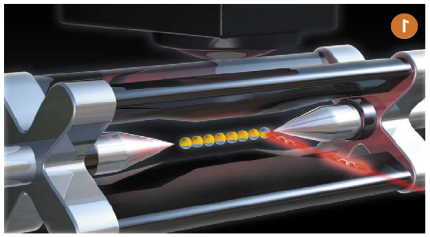
* Confinement using electromagnetic fields : « chain » of trapped ions

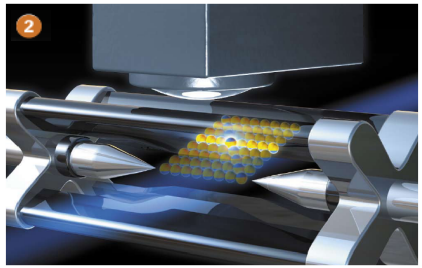
* Laser cooling : ions in the ground state of the harmonic trap



Isolated ions in vacuum : decoherence much smaller than in a solid...

« Quantum Byte » (Innsbruck, 2005)





Quantum register with 8 qubits

Control of the « calculation» using a sequence of laser pulses

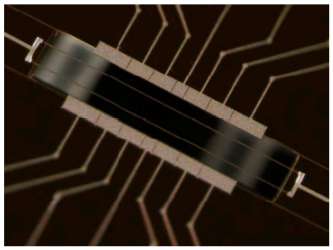
Preparation and read out:

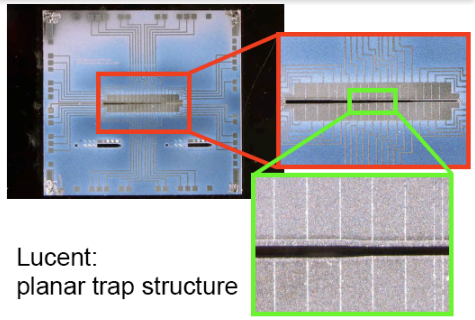
$$|\psi\rangle = \frac{1}{\sqrt{8}}\big(\ |10000000\rangle + |01000000\rangle + |00100000\rangle + |00010000\rangle + |00001000\rangle + |00000100\rangle + |00000010\rangle + |00000001\rangle\ \big)$$

… Difficult to draw !

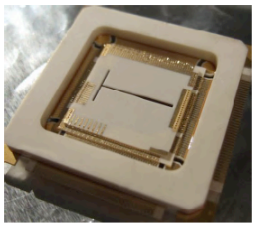
For example: Chip traps for ions (2006/2007)

Sandia: planar trap structure



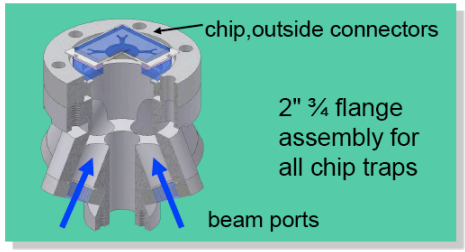


Lucent:
planar trap structure



Innsbruck design

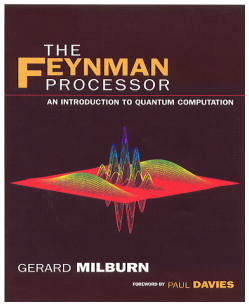
IOF
T - trap



As a conclusion...

* Quantum cryptography is making steady progress
  - full systems are availa
  - present challenges : n

* Quantum computing is making progress too !



The Nobel Prize in Physics 2012
Serge Haroche, David J. Wineland

The Nobel Prize in Physics 2012
Serge Haroche
David J. Wineland


Photo: © CNRS Photothèque/Christophe Lebedinsky

Serge Haroche

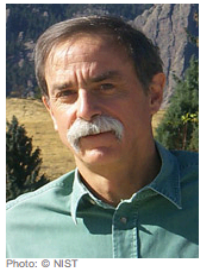


Photo: © NIST

David J. Wineland

The Nobel Prize in Physics 2012 was awarded jointly to Serge Haroche and David J. Wineland *"for ground-breaking experimental methods that enable measuring and manipulation of individual quantum systems"*