From quantum optics to quantum communication

Jean-Philippe Poizat
Jean-Philippe.Poizat@ujf-grenoble.fr
Laboratoire de Spectrométrie Physique
Equipe mixte CEA/CNRS/UJF
Nanophysique et Semiconducteurs
Grenoble, France

From quantum optics to quantum communication

Outlook :

Important results in quantum mechanics

Quantum optics : the tools

Single photons

Entangled photons (See M. Zukowski)

Continuous variables

Detectors

Quantum cryptography

Detailled presentation of BB84

Quantum computation with linear optics

Notions (depending on time)

Impossibilities of quantum mechanics

1) Position and momentum can not be known simultaneously

2) Measurements perturb the system

3) Notion of trajectory is no longer valid

4) Unknown quantum states can not be duplicated

5) Polarisation of a single photon can not be known

⇒ **These impossibilities can be turned into advantages...**

1) Position and momentum can not be known simultaneously

Heisenberg inequality $\Delta x \, . \, \Delta p > \hbar/2$

In quantum optics :

- Field quadratures are conjugate quantities

$X=(a+a^{+}) / 2^{1/2}$

$Y=(a- a^{+}) / 2^{1/2}$ $\Delta X \, . \, \Delta Y > 1/2$

- For intense beams :

Photon number N and phase Φ are conjugate variables

$\Delta N \, . \, \Delta \Phi > 1$

2) Measurement perturbs the system

State $|\psi>$, observable A.
$|\psi>$ is expanded on the $|\phi_i>$ basis of the A eigenvectors.

$$|\psi> = \Sigma\, c_i|\phi_i>$$

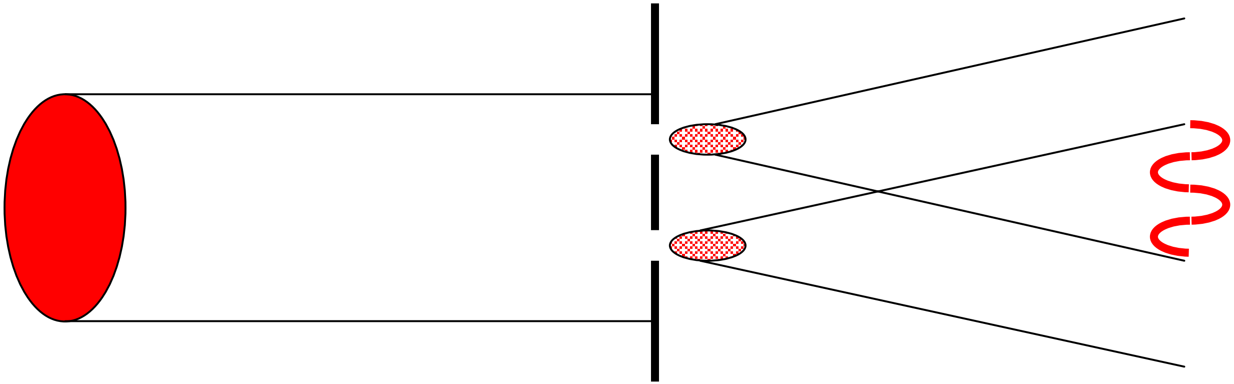
* Eigenvalue a_i corresponding to eigenvector $|\phi_i>$ is obtained with probability $P(a_i)=|c_i|^2$.
* After having obtained the result a_i, the system is projected in state $|\phi_i>$.

$\rightarrow$ The measurement has changed the state of the system from $|\psi>$ to $|\phi_i>$.

A second measurement will give the result a_i with probability 1, since the system is then already in state $|\phi_i>$.

3) Notion of trajectory is no longer valid

Young slit experiment :



$$\left|\Psi\right\rangle = \left|\varphi_1\right\rangle + \left|\varphi_2\right\rangle$$

Superposition principle :

→ **Interference** $$\left\|\Psi\right\|^2 = \left\|\varphi_1\right\|^2 + \left\|\varphi_2\right\|^2 + 2\left\langle\varphi_1\middle|\varphi_2\right\rangle$$

→ **Entanglement** $$\left|\Psi\right\rangle = \left|0\right\rangle_1\left|1\right\rangle_2 + \left|1\right\rangle_1\left|0\right\rangle_2$$

4) No-cloning theorem

One wishes to clone the state of particle 1 over to particle 2. Particle 2 is initially in state |s>.

Suppose that U is the cloning operator

- If particle 1 is in state |x>

$$U|x\rangle|s\rangle = |x\rangle|x\rangle \qquad \text{(a)}$$

- If particle 1 is in state |y>

$$U|y\rangle|s\rangle = |y\rangle|y\rangle \qquad \text{(b)}$$

- If particle 1 is in state |Φ>=(|x>+|y>)/√2

i) (a)+(b) -> $U|\Phi\rangle|s\rangle = \left(|x\rangle|x\rangle + |y\rangle|y\rangle\right)/\sqrt{2}$

ii) $U|\Phi\rangle|s\rangle = |\Phi\rangle|\Phi\rangle$

$$= (|x\rangle|x\rangle + |y\rangle|y\rangle + |x\rangle|y\rangle + |y\rangle|x\rangle)/2$$

i) et ii) do not give the same result !

5) Polarisation of a single photon can not be known

How to obtain information on the unknown linear polarization of a single incoming photon ?

Only solution : put a polarizing cube in a given orientation and see where the photon comes out.

$\longrightarrow$ The complete information can not be known for a single photon

From quantum optics
to quantum communication

Outlook :

Important results in quantum mechanics

Quantum optics : the tools

- Single photons
- *Entangled photons (See M. Zukowski)*
- *Continuous variables*
- Detectors

Quantum cryptography

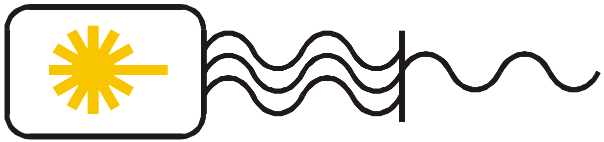
- Detailled presentation of BB84

Quantum computation with linear optics

- Notions (depending on time)

Single photon sources

* Attenuated laser

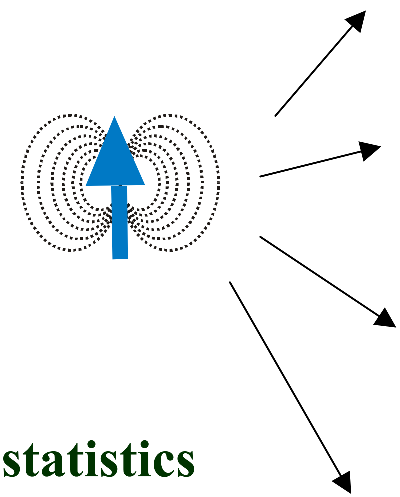


☹ **Poissonian statistics**

$$p(2) = \frac{p(1)^2}{2} \quad \text{for} \quad p(1) << 1$$

* Single photon sources

Single emitter



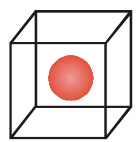
Molecule

☹ **Photobleaching**

Quantum dot

☺ **Narrow spectrum**

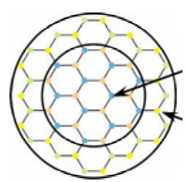
☹ **T = 4K**



Coloured center

☹ **Broad spectrum**

☺ **room temperature**



Nanocrystal

☹**Blinking**

☺ **room temperature**

☺ **Sub-Poissonian statistics**

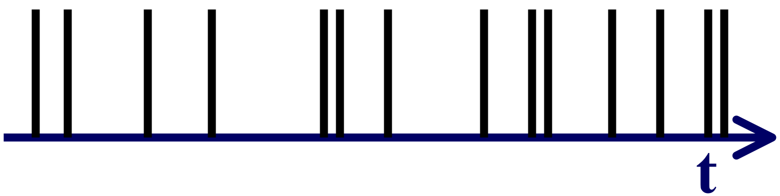
$$p(2) = c_N(0)\frac{p(1)^2}{2}$$

How to characterize a single photon source ?

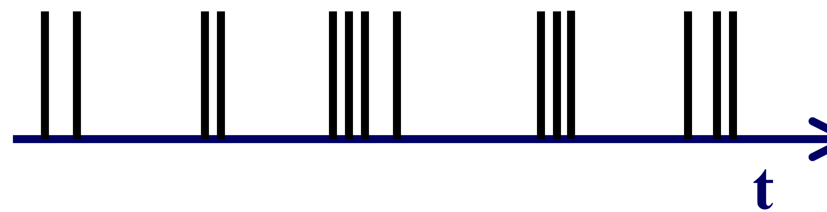
Measure the autocorrelation function

$$g^{(2)}(\tau) = \frac{\langle I(t+\tau)I(t)\rangle}{\langle I(t)\rangle^2}$$

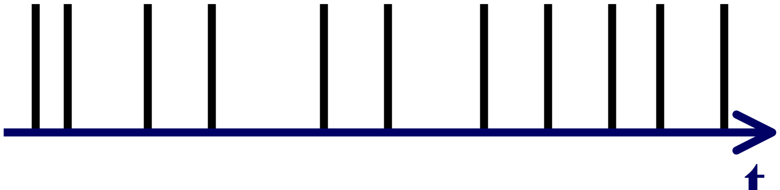
Poissonian light, $g^{(2)}(\tau) = 1$



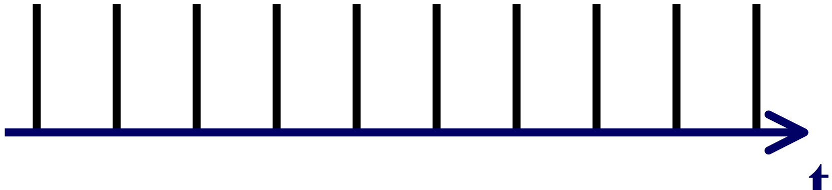
* **Bunched light**, $g^{(2)}(\tau) > 1$



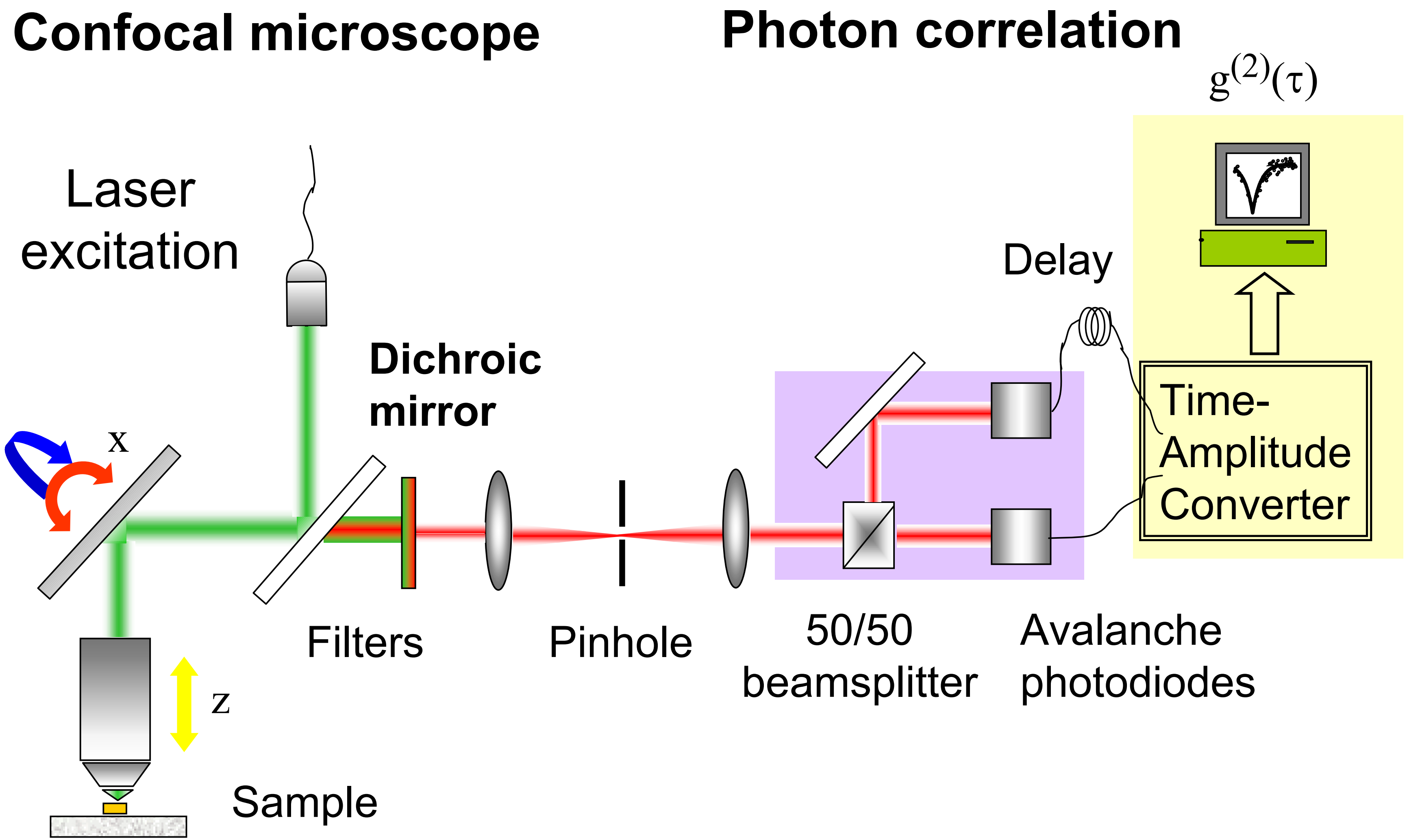
Antibunched light, $g^{(2)}(\tau) < 1$



* **Single photons**, $g^{(2)}(\tau) < 1$

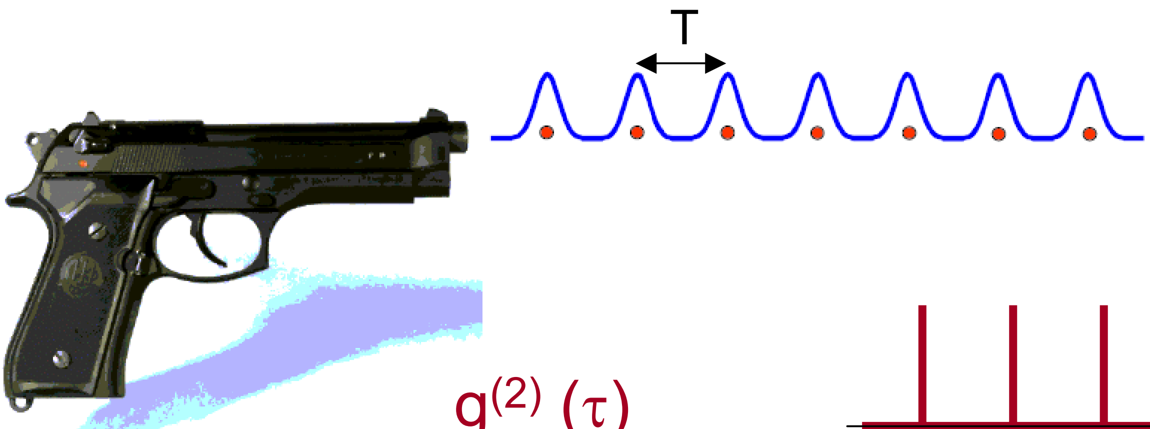


How to measure the autocorrelation function ?

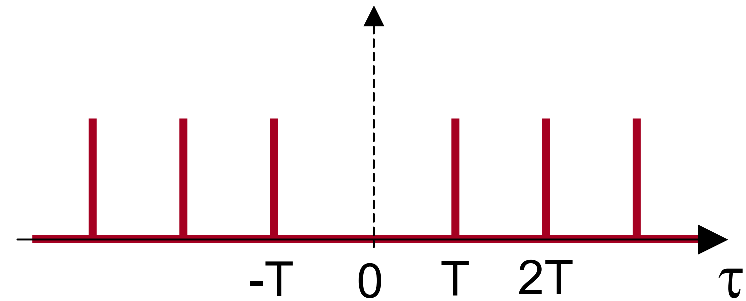


The ideal single photon source

Deterministic source with unity quantum efficiency*



$g^{(2)}(\tau)$

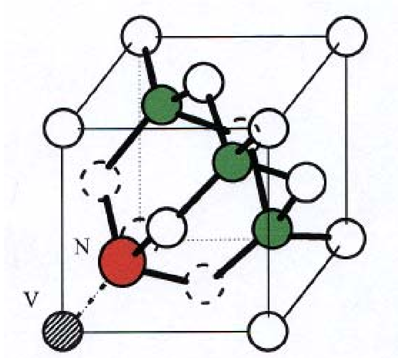


One single photon per pulse : 1/T photons per second

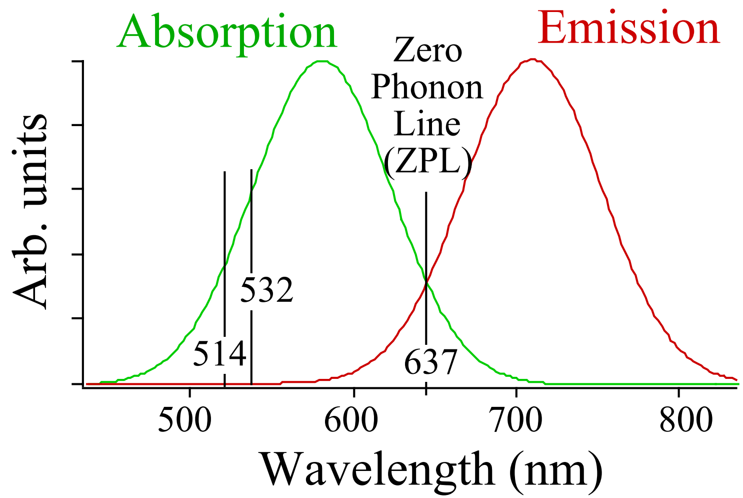
Experimentally : excite the single dipole with a pulsed laser

* Ideal for quantum cryptography or metrology. Other properties such as spectrum can be important for other application, see later

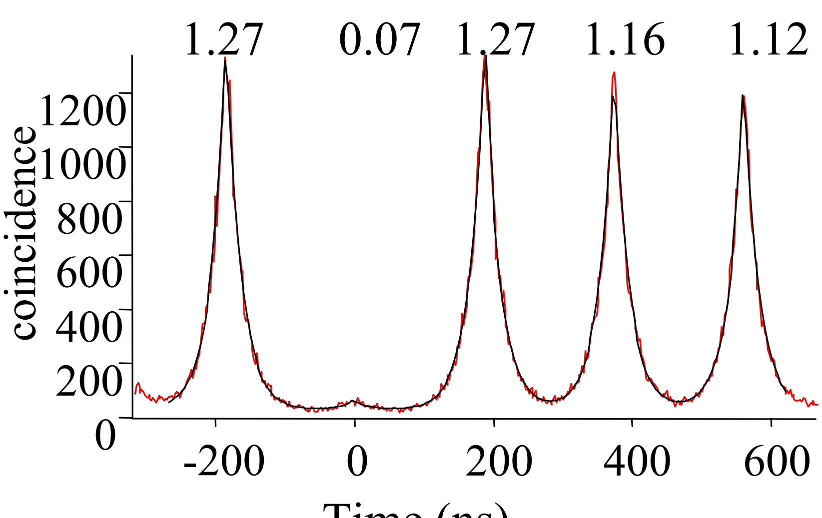
NV centers in diamond



NV centers



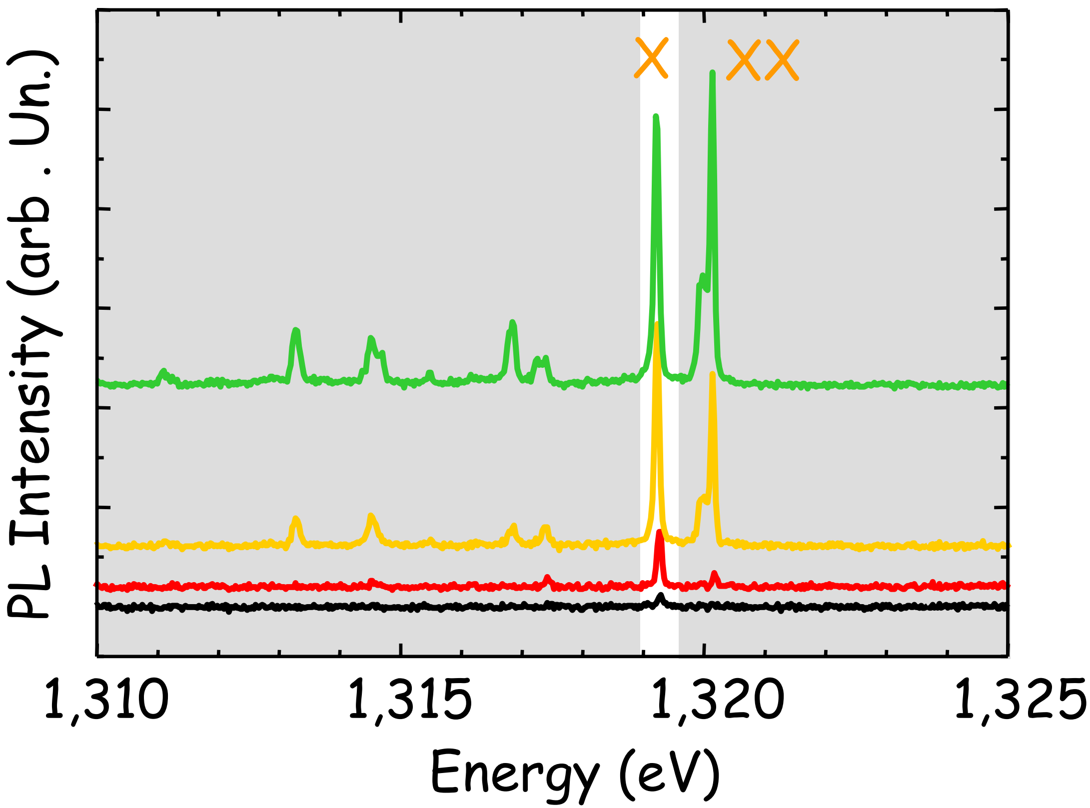
Diamond nanocrystals Φ=50 nm containing a single NV center

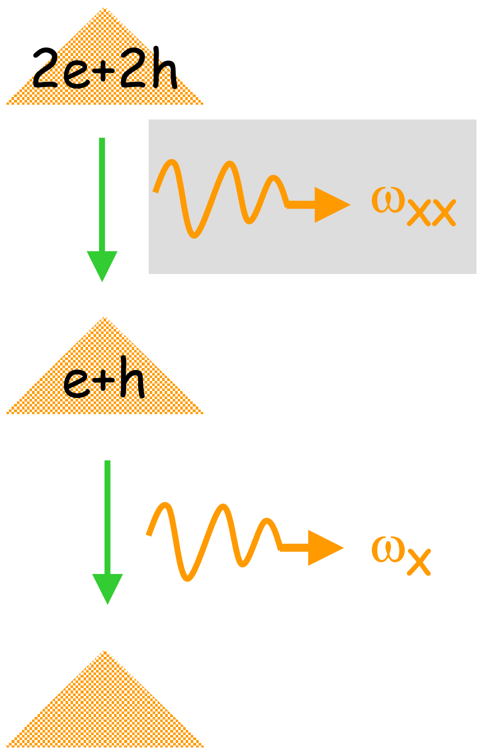


- **Repetition rate 5.3 MHz**
- **Rate of polarized single photons : 116 kcps**
- **Total efficiency : 2.2 %**

$1/g^{(2)}(0)=14.2$

Optical properties of a single quantum dot

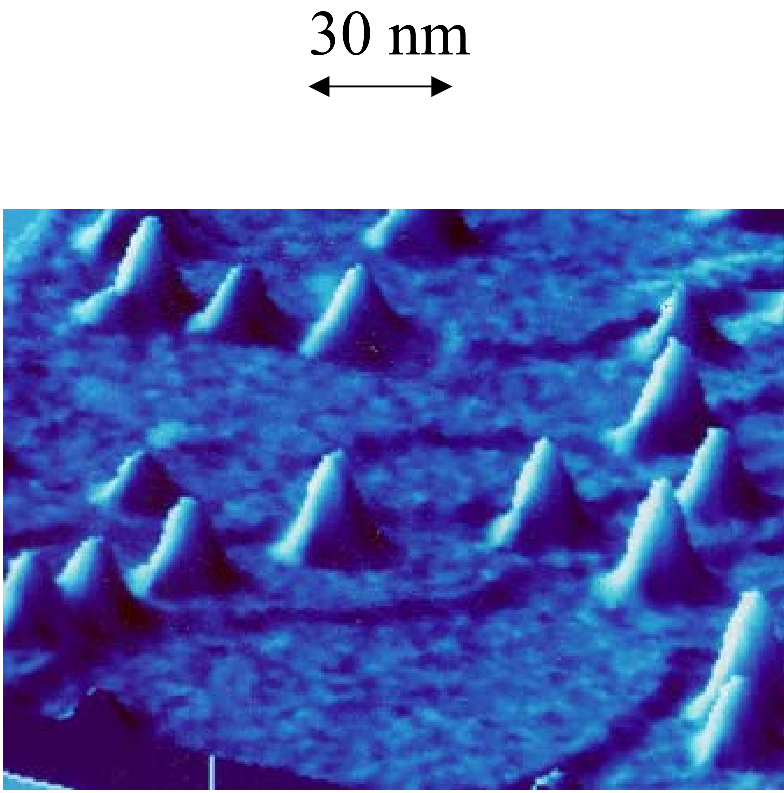


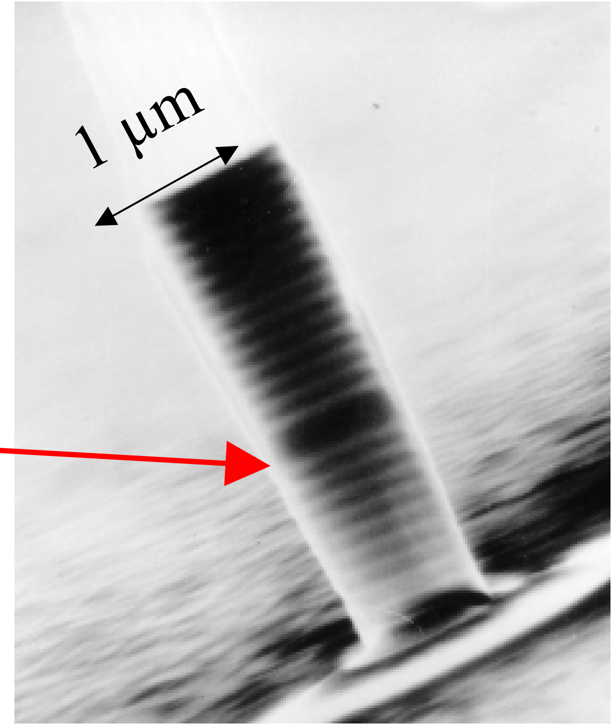


- Non-resonant pumping : more than one e-h pair injected
- Spectral filtering of X line

J.M. Gérard et B. Gayral, J. Lightwave Technol. 17, 2089 (1999)

Possibility of large quantum efficiency





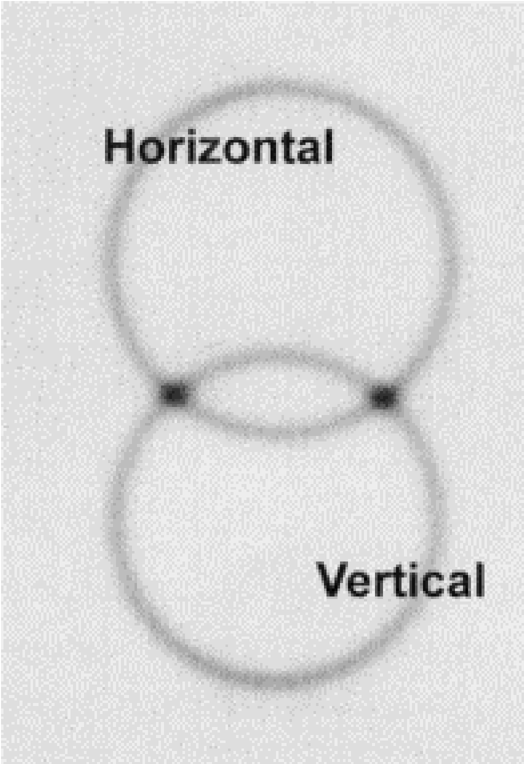
Quantum dots + **3D microcavities**

=> Efficient single photon source

Entangled pairs of photons
(see M. Zukowski presentation)

$\chi^{(2)}$ non-linear crystal
Kwiat et al (95)

$h(2\nu) \longrightarrow h\nu + h\nu$



Continuous variables

Quantum cryptography and quantum teleportation can be performed using continuous variables (ie with many photons):

Field quadrature components :

$$X = (a + a^{+})/2^{1/2}$$
$$Y = (a - a^{+})/2^{1/2}$$
With $[X,Y]=i$

These quadratures are measured with a local oscillator used as a phase reference.

Good point : no photon counting required

<u>References :</u>

Quantum teleportation : Furusawa et al, Science **282**, 706 (1998)
Quantum cryptography : Grosshans et al, Nature **421**, 238 (2003)

Detectors

Efficient photonic systems need

- good photon sources

- good detectors

Detector requirements for quantum cryptography

Photon counter with:

- Low dark count rate
- Large quantum efficiency
- High repetition rate
- Wavelengths : 1.3 or 1.55 μm

oratoire de Spectrométrie Physique

Detector requirements for photonic quantum gates

Very efficient detectors (>99%) with photon number resolution.

Candidates :

- Avalanche photodiodes (88% @ 694 nm), (Yamamoto et al)

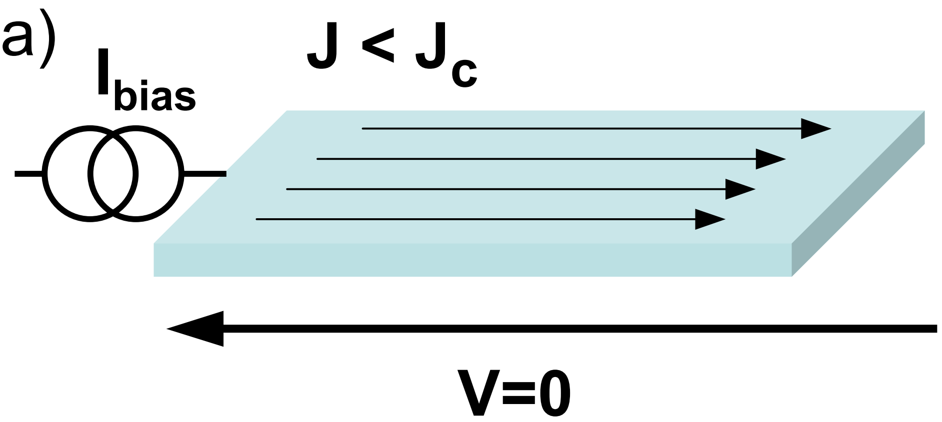
- Proposals with atomic vapors (>99%), (Kwiat, Imamoglu)

- Superconducting detectors

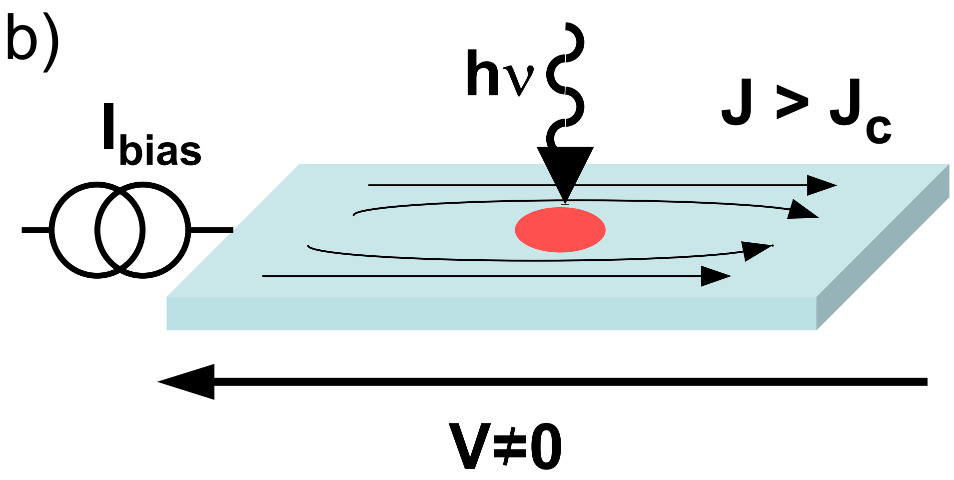
oratoire de Spectrométrie Physique

Principle of superconducting hot electron bolometer

Ultrathin film (< 10 nm) of NbN, $T<T_c=10K$



Superconducting regime



Superconductivity is suppressed by the absorption of a photon (thermalisation time: 20 ps

Characterics of superconducting hot electron bolometers

oratoire de Spectrométrie Physique

- Photon counting regime, ultra-low noise.

- Ultra-fast detector (20 ps) without dead time :
  * Optical testing of large scale integrated devices

- Wavelength range :
  visible and near-IR (especially 1.3 et 1.55 μm)
  * **Astrophysics**
  * **Quantum cryotography**

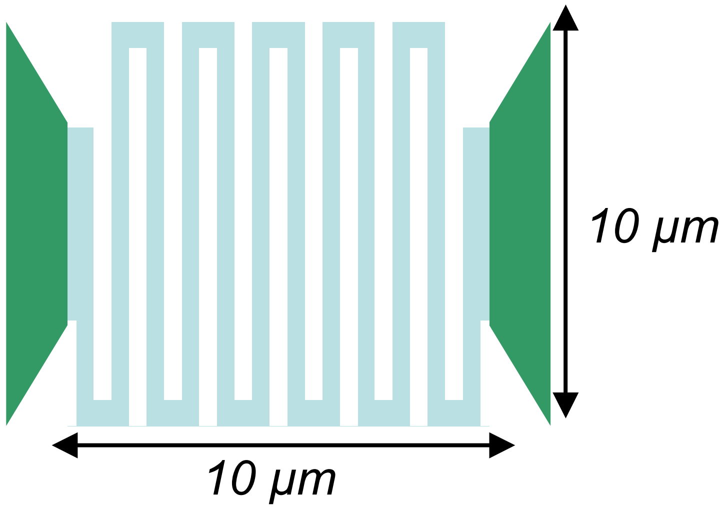
- Many photon effects :
  * **Non-linear detection**
  * **Photon number resolution**

Comparison with other photon counters

Detector	Qu. Eff. *(%)*	Temporal resolution *(ps)*	'Dark cnt'/s	Temp.
InGaAs APD/IR	10	500	10 000	Peltier
Si APD/Visible	50	300	25	Peltier
PM/Visible	20	25	2 000	-
PM/IR	0.5	150	16 000	-
STJ (supercond.)	40	10E6	-	He *(0,3 K)*
HEB (supercond.)	10	< 30	< 10	He *(≈ 4 K)*

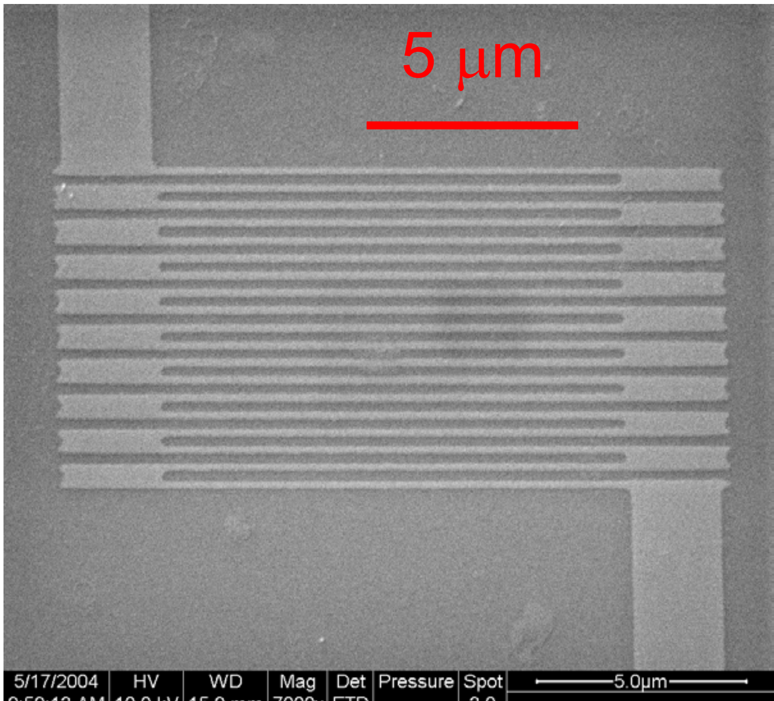
Laboratoire de Spectrométrie Physique

Device structure



Collaboration CEA/DRFMC, Grenoble
B. Delaet, J.C. Villegier

SEM image



From quantum optics to quantum communication

Outlook :

Important results in quantum mechanics

Quantum optics : the tools

- Single photons
- *Entangled photons (See M. Zukowski)*
- *Continuous variables*
- Detectors

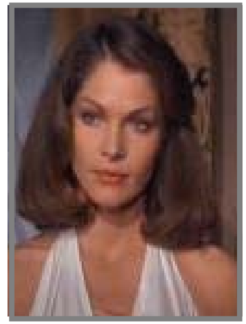
Quantum cryptography

- **Detailled presentation of BB84**

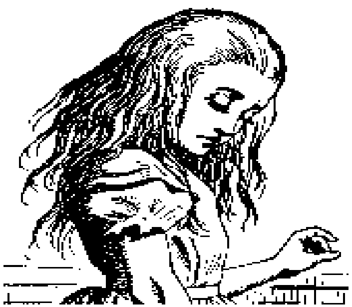
Quantum computation with linear optics

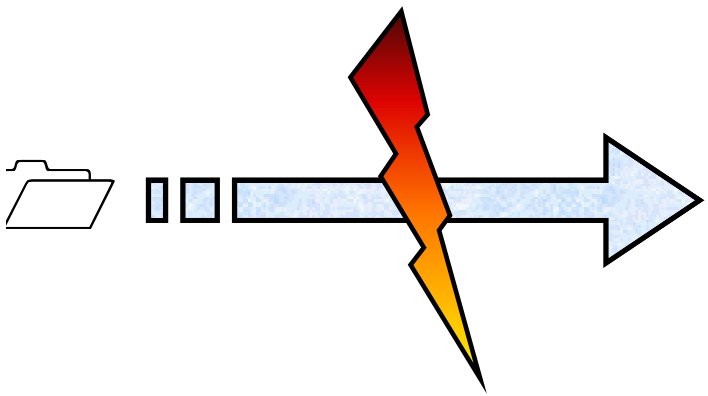
- Notions (depending on time)

Cryptography : the characters



Eve

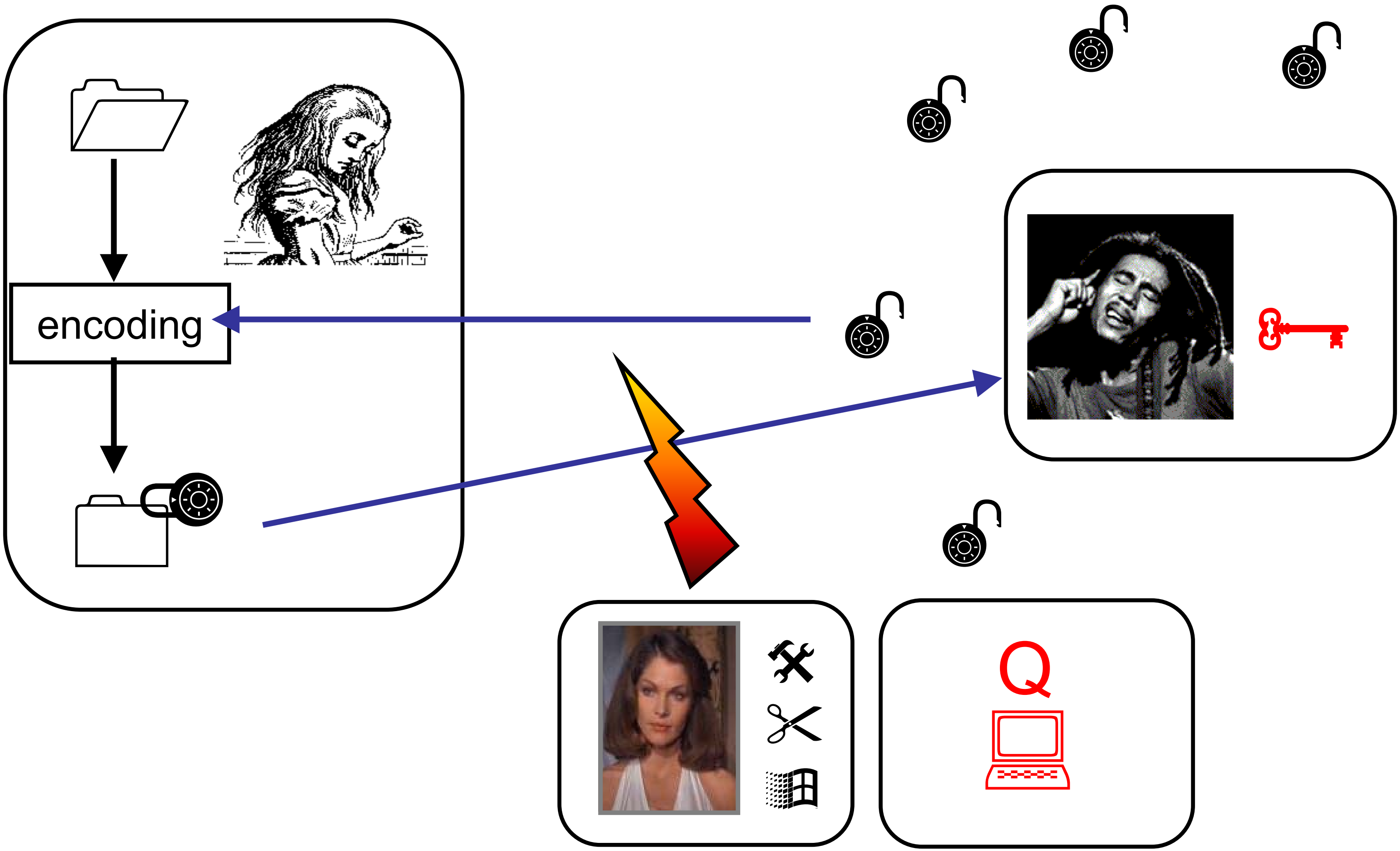




Bob

Alice

Public key cryptosystems (1970)



Symmetrical encryption (secret key)
One time pad (1917)

Alice

Message (M1) :	1 0 1 1 0 1 0 0	0 0 0 0 0 0 0 0
Key (K) :	0 1 1 0 1 0 0 0	1 1 1 0 1 0 1 0
Encrypted message (B1=M1+K):	1 1 0 1 1 1 0 0	1 1 1 0 1 0 1 0

Bob

Encrypted message (B1=M1+K):	1 1 0 1 1 1 0 0	1 1 1 0 1 0 1 0
Key (K):	0 1 1 0 1 0 0 0	1 1 1 0 1 0 1 0
Message (M1=B1-K):	1 0 1 1 0 1 0 0	0 0 0 0 0 0 0 0

For total security the key must be secret, as long as the message and used only once:

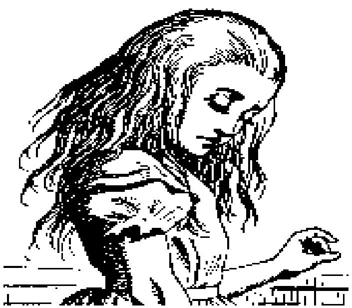
Message (M2):	0 0 0 0 0 0 0 0	0 1 1 0 0 1 1 0
Key (K) :	0 1 1 0 1 0 0 0	1 1 1 0 1 0 1 0
Encrypted message (B2=M2+K):	0 1 1 0 1 0 0 0	1 0 0 0 1 1 0 0
Decrypted message M2+M1 :	1 0 1 1 0 1 0 0	0 1 1 0 0 1 1 1

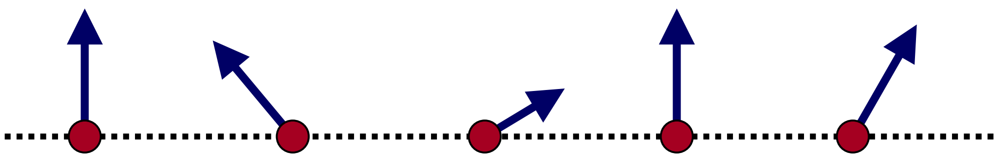
BB84 protocol (Bennett, Brassard 1984)

Enable a key distribution whose confidentiality is based on the law of quantum physics.

Classical channel :
phone, internet...

Alice





Bob

Quantum channel
Polarized single photons -45°,0°,45°,90°

BB84 protocol

0, 90° basis : 0° -> bit=0, 90°-> bit=1

+/- 45° basis: -45°-> bit =0, 45°-> bit=1

Alice	basis	0°	45°	45°	0°	45°	0°	0°	45°
	Value	1	1	0	1	0	0	1	0
Bob	basis	45°	45°	0°	0°	45°	0°	45°	0°
	Result	0	1	1	1	0	0	1	0
Communication of the basis via a classical channel			OK		OK	OK	OK		
The key is :			1		1	0	0		

Eavesdropper detection

Alice	Basis	0°	45°	45°	0°	45°	0°	0°	45°
	Value	1	1	0	1	0	0	1	0
Eve	Basis	45°	0°	0°	45°	45°	0°	0°	45°
	Result	0	1	1	1	0	0	1	0
Bob	Basis	45°	45°	0°	0°	45°	0°	45°	0°
	Result	0	0	1	1	0	0	1	0
Error test			No		Yes	Yes	Yes		

Eve will introduce errors :

→ Alice and Bob use up good photons to test the quantum bit error rate

Error rate introduced by Eve

Eve can not duplicate the photon (no-cloning theorem)

Good strategy for Eve (intercept and resend):

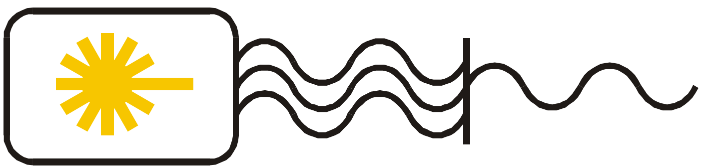
Eve chooses randomly a measurement basis and send a photon corresponding to the result of her measurement.

* *For a correct choice of the basis (50 % chance) :*
  → Eve does not introduce any errors
* *For a wrong choice of the basis (50 % chance) :*
  → She sends a photon in the wrong basis, and if Bob chooses the correct basis, he has only 50% chance of obtaining the correct result.

→ **This leads to an error rate of 25 % between Alice et Bob.**

Single photon vs attenuated laser

Usual QKD : Pulsed
Attenuated Laser



☹ Poissonian Statistics
with $p(1) \ll 1$:

$$\mathbf{p(2) = p(1)^2 / 2}$$
$$\mathbf{p(3) = p(1)^3 / 6}$$

→ **Multiphoton pulses allow Eve to extract information**

For attenuated laser pulse, the line is not longer secure :

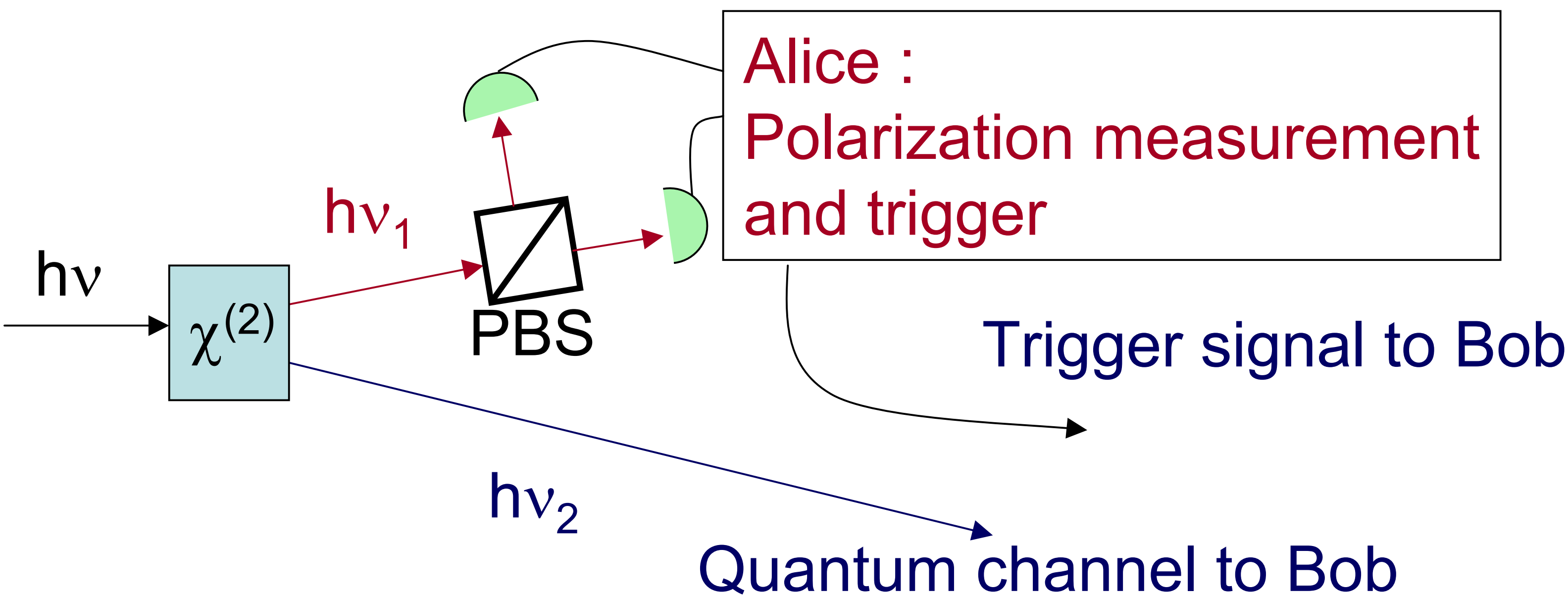
- if $p(2)/p(1) > \eta$, with unlimited technology,
- if $p(3)/p(1) > \eta$, in any cases.

Other way of producing single photons

Use entangled photon pairs produced by $\chi^{(2)}$ parametric down conversion :

$$h\nu \;\; \text{->} \;\; h\nu_1 + h\nu_2 \quad \text{with} \quad \nu=\nu_1+\nu_2$$

Polarization entangled state $|\Phi\rangle = |H_1V_2\rangle + |V_1H_2\rangle$



☺ High efficiency, better choice of wavelengths

Experimental difficulties

* **Sources** :
Have a good single photon source :
Attenuated laser, photon pistol, photon pairs...

* **Transmission** :
Polarization dispersion in fibers, losses…

* **Detection** :
Photon counting at 1.3 ou 1.55 μm is not very efficient.

Review article on quantum cryptography :
N. Gisin et al, Rev. Mod. Phys. **74**, 145 (2002).

From quantum optics
to quantum communication

<u>Outlook</u> :

Important results in quantum mechanics

Quantum optics : the tools

Single photons

Entangled photons (See M. Zukowski)

Continuous variables

Detectors

Quantum cryptography

Detailled presentation of BB84

Quantum computation with linear optics

Notions (depending on time)

oratoire de Spectrométrie Physique

Quantum computation with photons

Qubit carried by a single photon.

For example, polarisation H : I0>

V : I1>

<u>* Good points :</u>

- Single qubit operation are trivial
- Relatively good detection
- Propagation is natural
- Photons are relatively immune to decoherence

<u>*Difficult points :</u>

- Photon can not be stored
- Two qubit quantum gate :
  - Non-linear optics : very difficult
  - **All-optical conditionnal quantum gate**

Two qubits photonic quantum gate

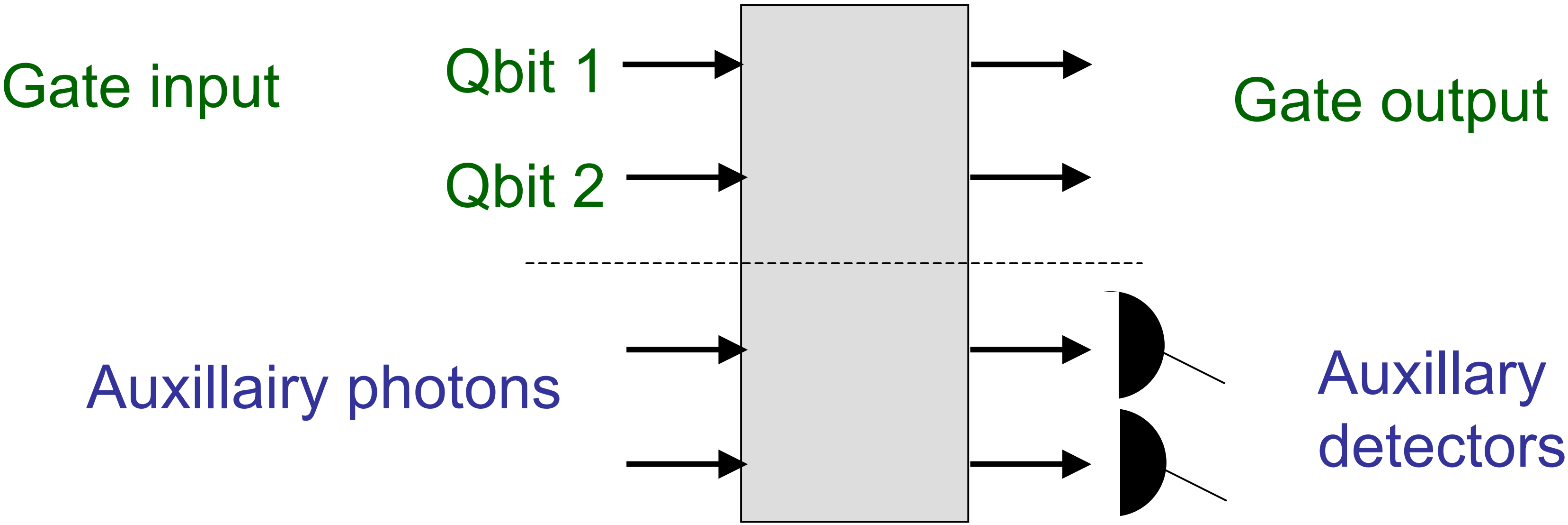
Challenge : A single photon should change the state of another single photon.

* **With non-linear optics :**
  Requires extremely high non-linearity (perhaps achievable in Cavity QED).

* **All-optical conditionnal quantum gate :**
  Knill, Laflamme, Milburn proposal.

All-optical quantum gates

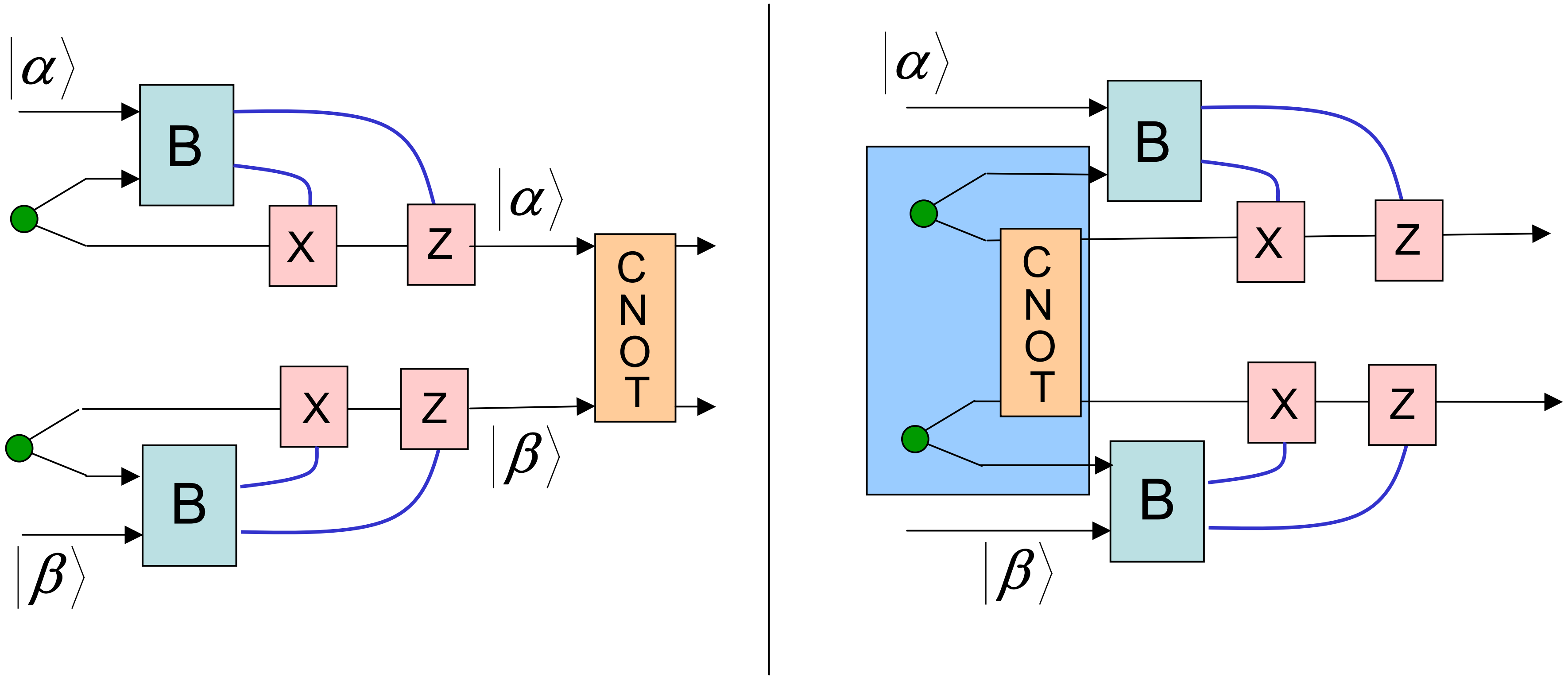
Principle (Knill et al, Nature **409**, 46 2001):



$$\left|\Psi^{in}_{Qbit}\right\rangle \otimes \left|\Psi^{in}_{aux}\right\rangle \longrightarrow \left|\Psi^{out}_{Qbit}\right\rangle^{(G)} \left|\Psi^{out}_{aux}\right\rangle^{(G)} + \sum_{i} \left|\Psi^{out}_{Qbit}\right\rangle^{(i)} \left|\Psi^{out}_{aux}\right\rangle^{(i)}$$

Conditionnal gate !

How to build a computer with conditionnal gates ?



These two systems are equivalent :

- A known state is prepared in advance using a conditionnal all-optical gate. It is stored in the blue box.
- It is then used when the real data $|\alpha\rangle$ and $|\beta\rangle$ come along.

Gottesman et Chuang, Nature 402, 390, (1998)

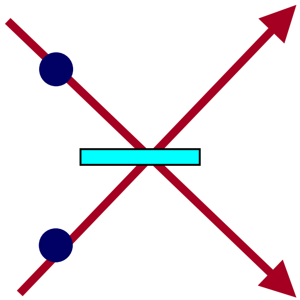
Experimental conditions required

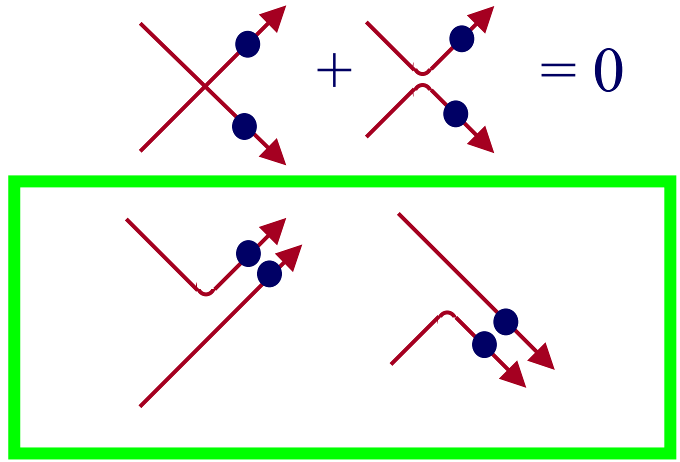
1) Indistinguishable photons.

2) Very efficient detectors,
resolving the photon number.

oratoire de Spectrométrie Physique

Elementary physical effect : Two-photon interference





The two photons must be indistinguishable :

i) Arrive simultaneously

ii) have the same polarization

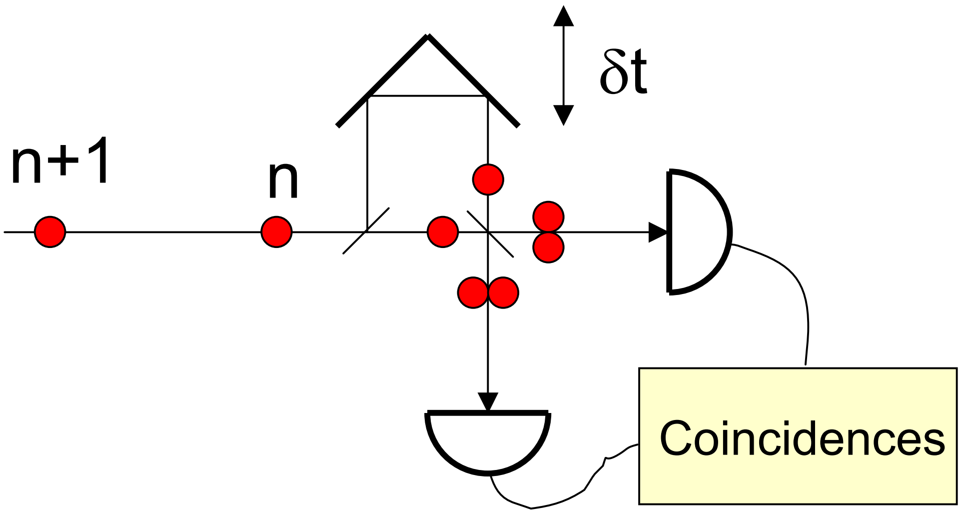
iii) have the same spectrum

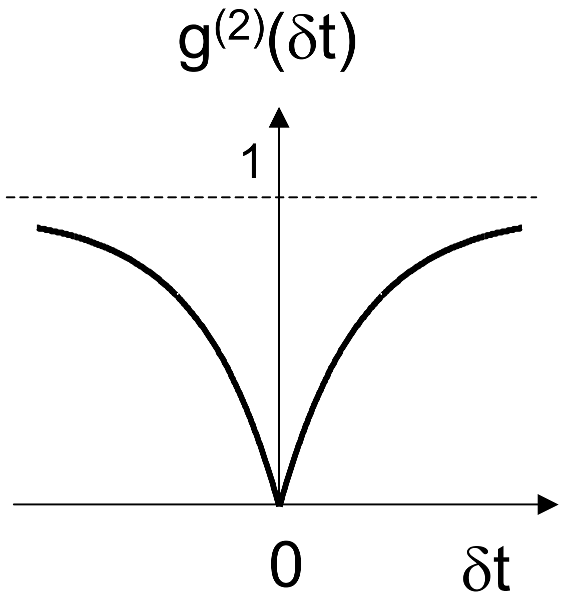
iv) come out in the same spatial modes

→ **Requires a single-mode single-photon source**

Two-photon interference : Photon coalescence

Two-photon interference with two photons successively emitted by the same quantum dot :





C. Santori et al, Nature **419**, 594 (2002)

Indistinguishability : Spectral conditions

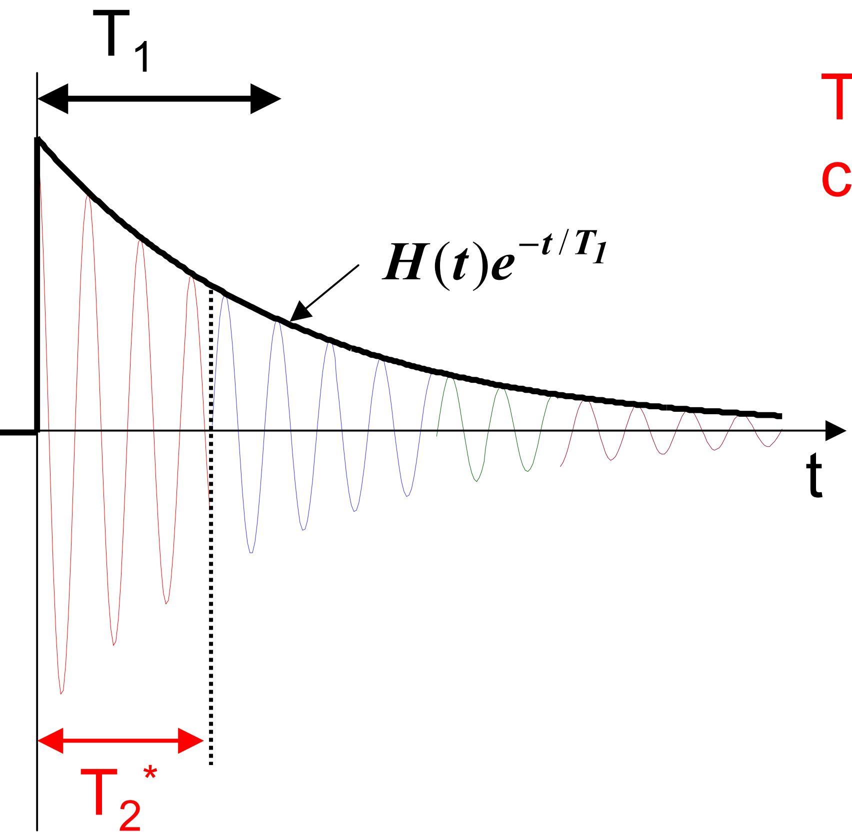
- Spectral width $\Delta\nu$ of a photon should be minimum,
ie $\Delta\nu=1/(2T_1)$, where T_1 is the emitter lifetime.
The goal is $T_2=2T_1$.

-Two successive photons should have the same frequency (charge fluctuations may perturb).

Lifetime limited linewidth of single photons

oratoire de Spectrométrie Physique

Photon wave packet : $$\Psi(t) = H(t)e^{-t/T_1}e^{-i(\omega t+\varphi(t))}$$



T_2^* is the dephasing time corresponding to the fluctuating $\varphi(t$

Linewidth is :

$$\Delta\nu \propto \frac{1}{T_2} = \frac{1}{2T_1} + \frac{1}{T_2^*}$$

T_1 : emitter's lifetime
T_2 : coherence time

How to obtain a quantum dot with a lifetime limited linewidth ?

oratoire de Spectrométrie Physique

Linewidth is $$\Delta\nu \propto \frac{1}{T_2} = \frac{1}{2T_1} + \frac{1}{T_2^*}$$

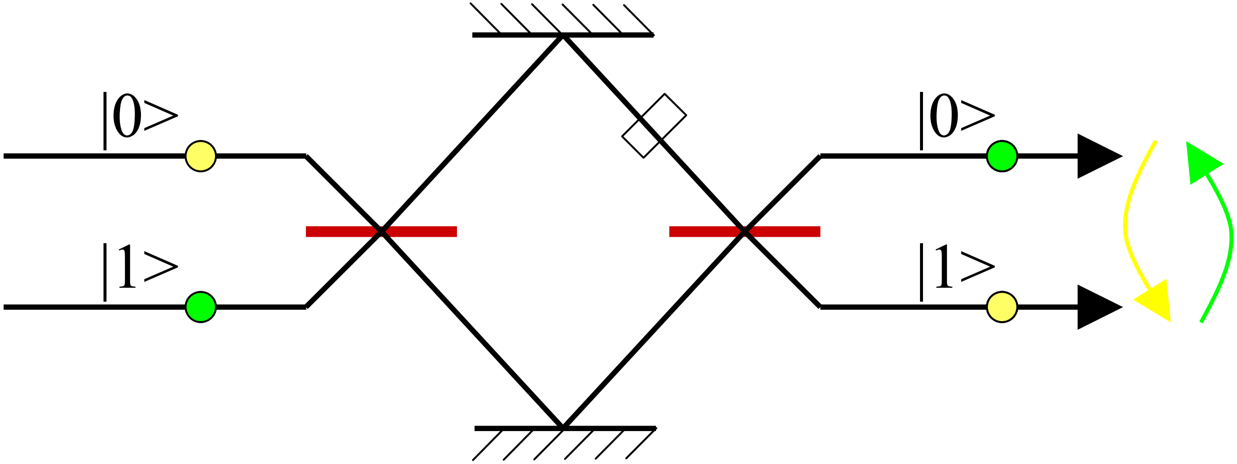
- Low temperature (2K) to reduce the phonon-induced dephasing rate (ie, enlarge T_2^*).

- Reduce lifetime T_1 :
    - Well-chosen quantum dots,
    - Microcavity : Purcell effect.

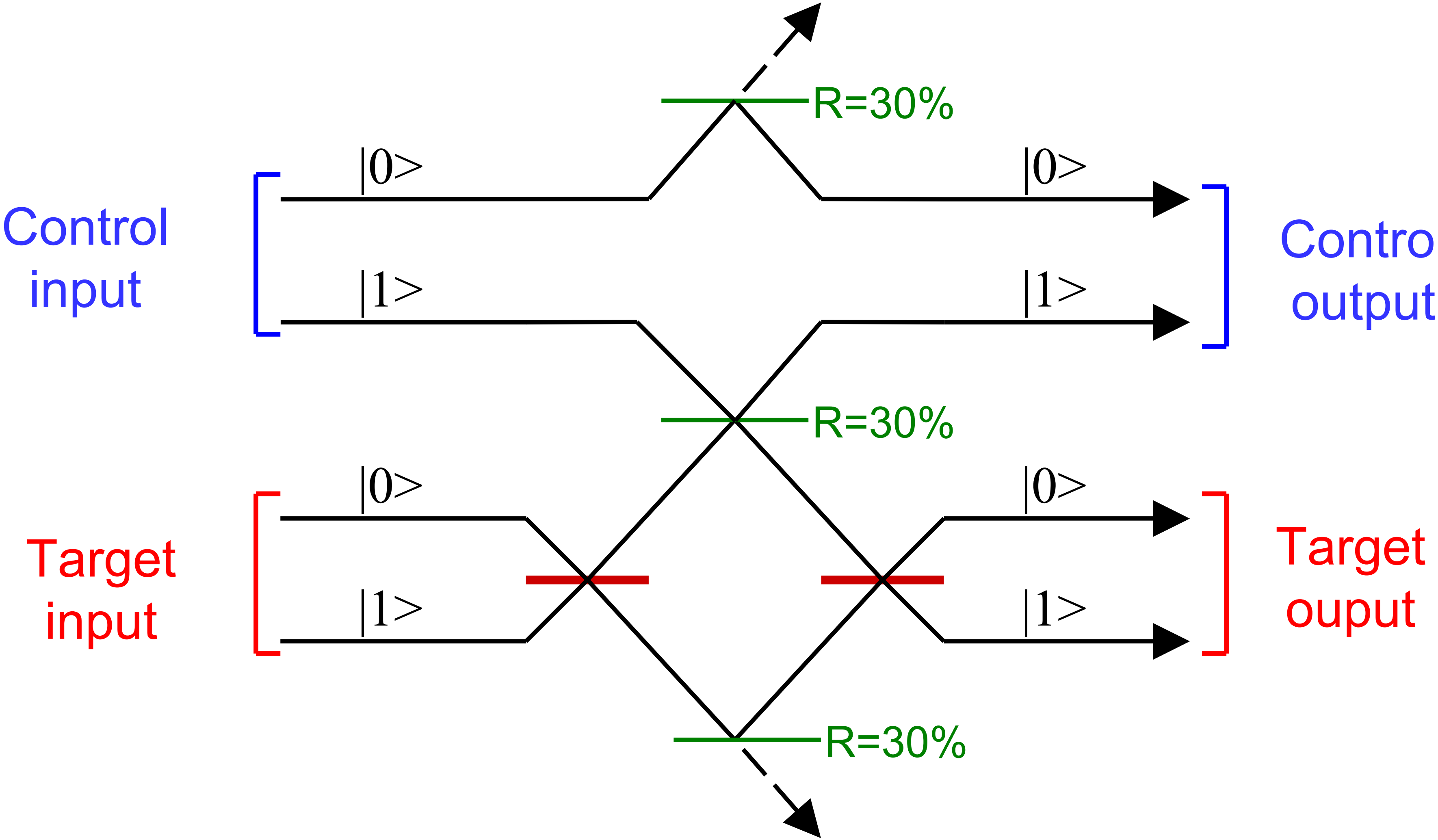
- High quality epitaxial growth.

Photonic quantum gate : an example

π phase shift : qubit swapped



Photonic quantum gate : an example



When control output and target ouput clic in coincidence (probability 1/9), the CNOT gate is realized.

O'Brien et al., Nature **426**, 264 (2003)

Photonic quantum gates

In the latter scheme the qubits are no longer available for further computing since they have to be detected.

Other schemes* exist that uses auxiliary photons and leave the qubits available for further computation.

*Proposal : Pittman et al PRA **68**, 032316 (2003)
Experiment : Gasparoni et al, quant-ph 0404107

Conclusions and perspectives

Current status of photonic quantum information :

* Photonic is the best for communication :
   - Quantum cryptography is mature
     (2 start up, over 100 km in telecom fibers)
   - Quantum teleportation over large distance is under way

* Photonic quantum computation is in the race…