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
- Detailed presentation of BB84

Quantum computation with linear optics
- Notions (depending on time)
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3) Notion of trajectory is no longer valid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 $\Delta x \cdot \Delta p > \frac{\hbar}{2}$

**In quantum optics**:  
- Field quadratures are conjugate quantities  
  $X = \frac{(a + a^+)}{\sqrt{2}}$  
  $Y = \frac{(a - a^+)}{\sqrt{2}}$  
  $\Delta X \cdot \Delta Y > \frac{1}{2}$

- For intense beams:  
  Photon number $N$ and phase $\Phi$ are conjugate variables  
  $\Delta N \cdot \Delta \Phi > 1$
2) Measurement perturbs the system

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

$$|\psi\rangle = \sum c_i |\phi_i\rangle$$

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

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

A second measurement will give the result $a_i$ with probability 1, since the system is then already in state $|\phi_i\rangle$. 
3) Notion of trajectory is no longer valid

Young slit experiment:

\[ |\Psi\rangle = |\varphi_1\rangle + |\varphi_2\rangle \]

Superposition principle:

- Interference: \[ \|\Psi\|^2 = \|\varphi_1\|^2 + \|\varphi_2\|^2 + 2\langle \varphi_1 | \varphi_2 \rangle \]
- Entanglement: \[ |\Psi\rangle = |0\rangle_1 |1\rangle_2 + |1\rangle_1 |0\rangle_2 \]
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 $|x>$
  \[ U|x\rangle|s\rangle = |x\rangle|x\rangle \]  
  \[ \text{(a)} \]

- If particle 1 is in state $|y>$
  \[ U|y\rangle|s\rangle = |y\rangle|y\rangle \]  
  \[ \text{(b)} \]

- If particle 1 is in state $|\Phi>= (|x>+|y>)/\sqrt{2}$

  i) (a)+(b) -> \[ U|\Phi\rangle|s\rangle = (|x\rangle|x\rangle + |y\rangle|y\rangle)/\sqrt{2} \]  
  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.

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
Detailed presentation of BB84
Quantum computation with linear optics
Notions (depending on time)
Single photon sources

* **Attenuated laser**

\[ p(2) = \frac{p(1)^2}{2} \quad \text{for} \quad p(1) \ll 1 \]

* **Single photon sources**

- **Sub-Poissonian statistics**
  \[ p(2) = c_N(0) \frac{p(1)^2}{2} \]

**Molecule**

- 😞 Photobleaching

**Quantum dot**

- 😊 Narrow spectrum
- 😞 T = 4K

**Coloured center**

- 😞 Broad spectrum
- 😊 room temperature

**Nanocrystal**

- 😞 Blinking
- 😊 room temperature
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**, $g^{(2)}(\tau) = 1$
  - ![Poissonian light graph]

- **Bunched light**, $g^{(2)}(\tau) > 1$
  - ![Bunched light graph]

- **Antibunched light**, $g^{(2)}(\tau) < 1$
  - ![Antibunched light graph]

- **Single photons**, $g^{(2)}(\tau) < 1$
  - ![Single photon graph]
How to measure the autocorrelation function?

Confocal microscope

Laser excitation

Dichroic mirror

Filters

Pinhole

Sample

Photon correlation

Delay

50/50 beamsplitter

Avalanche photodiodes

Time-Amplitude Converter

$g^{(2)}(\tau)$
The ideal single photon source

Deterministic source with unity quantum efficiency*

One single photon per pulse: \( \frac{1}{T} \) 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 applications, see later.
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

Possibility of large quantum efficiency

30 nm

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)

$h(2\nu) \rightarrow h\nu + h\nu$
Continuous variables

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

Field quadrature components:

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

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

Good point: no photon counting required

References:
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
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
Ultrathin film (< 10 nm) of NbN, \( T < T_c = 10\, \text{K} \)

**Superconducting regime**

**Superconductivity is suppressed by the absorption of a photon**
(thermalisation time: 20 ps)
Characteristics of superconducting hot electron bolometers

- 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
<table>
<thead>
<tr>
<th>Detector</th>
<th>Qu. Eff. (%)</th>
<th>Temporal resolution (ps)</th>
<th>‘Dark cnt’/s</th>
<th>Temp.</th>
</tr>
</thead>
<tbody>
<tr>
<td>InGaAs APD/IR</td>
<td>10</td>
<td>500</td>
<td>10 000</td>
<td>Peltier</td>
</tr>
<tr>
<td>Si APD/Visible</td>
<td>50</td>
<td>300</td>
<td>25</td>
<td>Peltier</td>
</tr>
<tr>
<td>PM/Visible</td>
<td>20</td>
<td>25</td>
<td>2 000</td>
<td>-</td>
</tr>
<tr>
<td>PM/IR</td>
<td>0.5</td>
<td>150</td>
<td>16 000</td>
<td>-</td>
</tr>
<tr>
<td>STJ (supercond.)</td>
<td>40</td>
<td>10E6</td>
<td>-</td>
<td>He (0.3 K)</td>
</tr>
<tr>
<td>HEB (supercond.)</td>
<td>10</td>
<td>&lt; 30</td>
<td>&lt; 10</td>
<td>He (≈ 4 K)</td>
</tr>
</tbody>
</table>
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
  Detailed presentation of BB84
Quantum computation with linear optics
  Notions (depending on time)
Cryptography: the characters

Alice

Eve

Bob
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
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
Enable a key distribution whose confidentiality is based on the law of quantum physics.
**BB84 protocol**

0, 90° basis : 0° -> bit=0, 90°-> bit=1  
+/- 45° basis: -45°-> bit =0, 45°-> bit=1

<table>
<thead>
<tr>
<th>Alice</th>
<th>basis</th>
<th>0°</th>
<th>45°</th>
<th>45°</th>
<th>0°</th>
<th>45°</th>
<th>0°</th>
<th>45°</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Bob</th>
<th>basis</th>
<th>45°</th>
<th>45°</th>
<th>0°</th>
<th>0°</th>
<th>45°</th>
<th>0°</th>
<th>45°</th>
<th>0°</th>
</tr>
</thead>
<tbody>
<tr>
<td>Result</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

Communication of the basis via a classical channel

The key is :

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>1</th>
<th>0</th>
<th>0</th>
</tr>
</thead>
</table>
**Eavesdropper detection**

<table>
<thead>
<tr>
<th></th>
<th>Basis</th>
<th>0°</th>
<th>45°</th>
<th>45°</th>
<th>0°</th>
<th>45°</th>
<th>0°</th>
<th>45°</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>Value</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Eve</td>
<td>Basis</td>
<td>45°</td>
<td>0°</td>
<td>0°</td>
<td>45°</td>
<td>45°</td>
<td>0°</td>
<td>45°</td>
</tr>
<tr>
<td>Eve</td>
<td>Result</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Bob</td>
<td>Basis</td>
<td>45°</td>
<td>45°</td>
<td>0°</td>
<td>0°</td>
<td>45°</td>
<td>0°</td>
<td>45°</td>
</tr>
<tr>
<td>Bob</td>
<td>Result</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Error test</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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

Multiphoton pulses allow Eve to extract information

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

- $p(2) = p(1)^2 / 2$
- $p(3) = p(1)^3 / 6$

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:

$h\nu \rightarrow h\nu_1 + h\nu_2 \quad \text{with} \quad \nu = \nu_1 + \nu_2$

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

Alice: Polarization measurement and trigger

量子信道传给 Bob

触发信号传给 Bob

 высокоэффективность, лучший выбор длин волн
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 :
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
  Detailed presentation of BB84

Quantum computation with linear optics
  Notions (depending on time)
Quantum computation with photons

Qubit carried by a single photon.
For example, polarisation $H : |0\rangle$
$V : |1\rangle$

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

*Difficult points :
- 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):

Gate input

Qbit 1
Qbit 2

Auxiliary photons

Gate output

Auxiliary detectors

\[ \Psi_{in}^{Qbit} \otimes \Psi_{in}^{aux} \rightarrow \Psi_{out}^{Qbit}^{\text{(G)}} \Psi_{out}^{aux}^{\text{(G)}} + \sum_i \Psi_{out}^{Qbit}^{(i)} \Psi_{out}^{aux}^{(i)} \]

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.

Experimental conditions required

1) Indistinguishable photons.

2) Very efficient detectors, resolving the photon number.
Elementary physical effect: Two-photon interference

\[ \begin{align*} &+ \quad = 0 \\
\end{align*} \]

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 with two photons successively emitted by the same quantum dot:

\[ g^{(2)}(\delta t) \]

- Spectral width $\Delta \nu$ of a photon should be minimum, i.e., $\Delta \nu = 1/(2T_1)$, 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

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?

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

$\pi$ phase shift: qubit swapped
When control output and target output click in coincidence (probability 1/9), the CNOT gate is realized.

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.

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…