GRENOBLE I
UNIVERSITE JOSEPH FOURIER
SCIENCES. TECHNOLOGIE. MEDECINE

exposé UE SCI, Valence

Qu'est-ce qu'un ordinateur quantique et à quoi pourrait-il servir ?

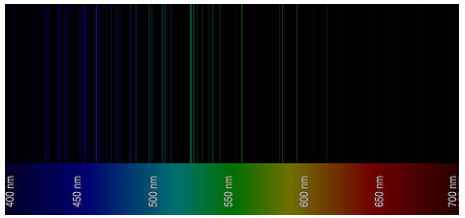
Dominique Spehner

Institut Fourier
et Laboratoire de Physique et Modélisation des Milieux Condensés

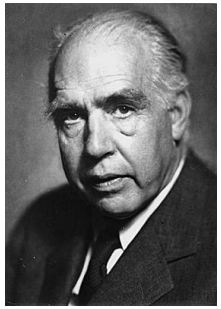
Université Joseph Fourier, Grenoble

Physique du monde microscopique

La mécanique quantique décrit la physique à l'échelle des molécules, atomes et des particules élémentaires (quarks, photon, neutrinos, boson de Higgs ?, etc...)



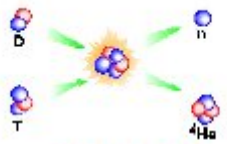
Raies d'émission du Cs

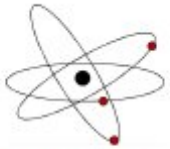

Ses pères fondateurs sont :

M. Planck (1858-1947), N. Bohr (1885-1962), W. Heisenberg (1901-1976), E. Schrödinger (1887-1961) et P. Dirac (1902-1984)

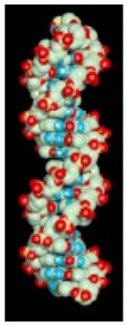
La physique quantique permet d'expliquer :



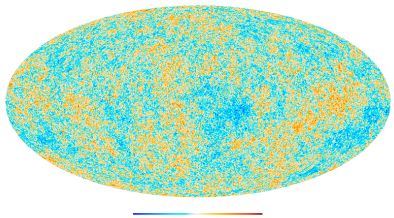
10^{-15} M
(noyaux, radioactivité
Énergie nucléaire)



10^{-10} M
(atomes)



10^{-8} M
(molécules
biologiques)



(rayonnement fossile de l'univers mesuré par Planck)

- → les collisions à haute énergie au CERN
- → les réactions nucléaires
- → la structure de la matière (molécules, solides, liquides et gaz)
- → les propriétés de conduction des matériaux
- → le magnétisme (aimants,...)
- → les réactions chimiques
- → ...
- → la photosynthèse ?
- → ...
- → les origines de l'univers (Big Bang)

Un siècle de physique quantique

Les prédictions de la théorie quantique n'ont jamais jusqu'ici été mises en défaut ! Certaines prédictions sont vérifiées expérimentalement avec une précision supérieure à 10^{-10} *(moment magnétique de l'électron).*

La mécanique quantique a permis des avancées technologiques considérables au XX-ième siècle, par exemple :

- *transistors, diodes, circuits intégrés*
- *lasers*
- *Imagerie par Résonance Magnétique*
- *mesure précise du temps*
  $\hookrightarrow$ *systèmes de navigation GPS*

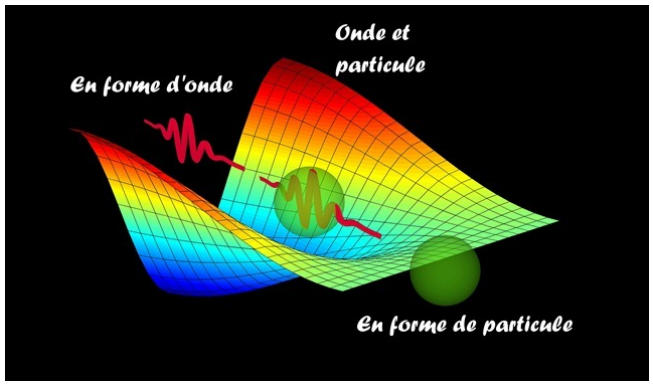
(Horloge atomique)

Qu'en sera-t-il au XXI-ième siècle ?

Une théorie très précise mais bien étrange...

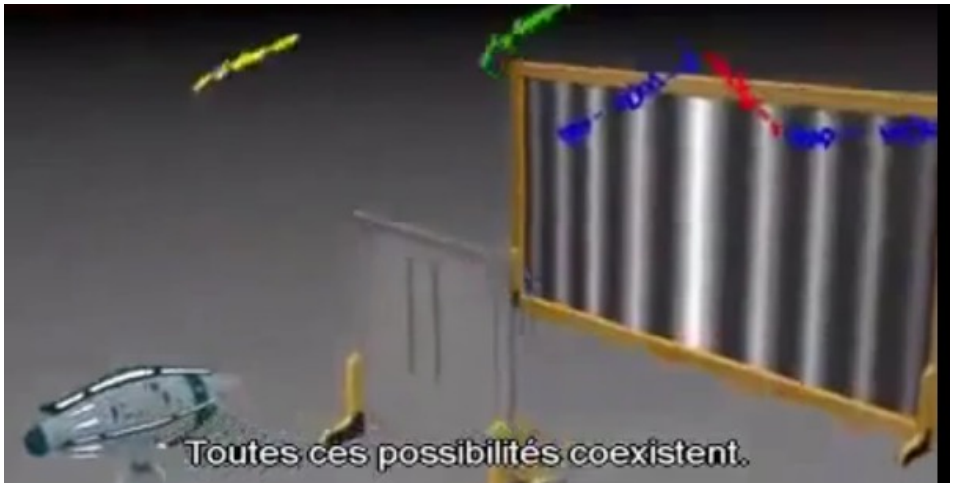
"Ceux qui prétendent avoir compris la mécanique quantique manifestent ainsi que ce n'est pas le cas" (R. Feynman).

Un corpuscule quantique (photon, électron, molécule,...) est **en même temps une onde et une particule**.



La notion de trajectoire n'a pas de sens : si la particule a une position bien définie alors sa vitesse n'est pas définie (elle est totalement aléatoire) et vice versa.

Expérience des fentes d'Young



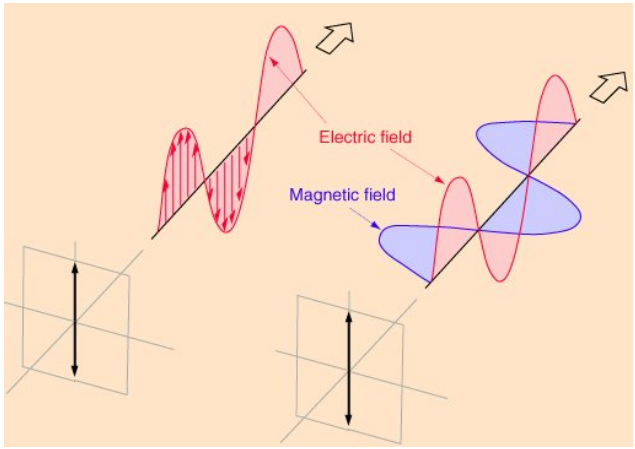
(source: "Dr Quantum" sur YouTube)

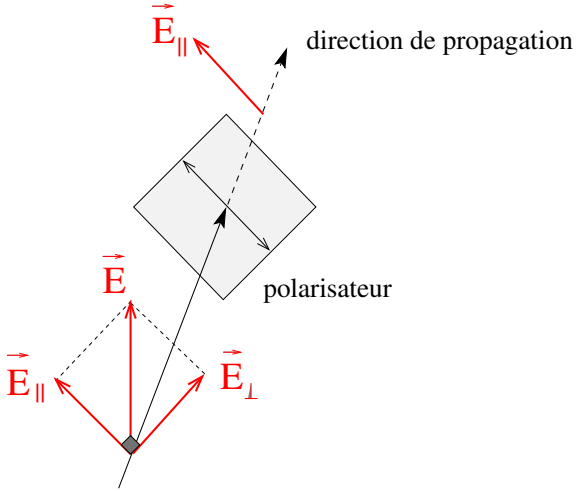
↪ Expérience réalisée avec des **électrons envoyés un par un** à Tokyo en 1989 (A. Tonomura *et al.*).

↪ Observation de figures d'interférences pour des **molécules** C_{60} à Vienne en 1999 (A. Arndt *et al.*),

Polarisation du photon

Un polarisateur transmet uniquement le champ électrique $\vec{E}$ selon son axe
$\hookrightarrow$ *lumière linéairement polarisée.*





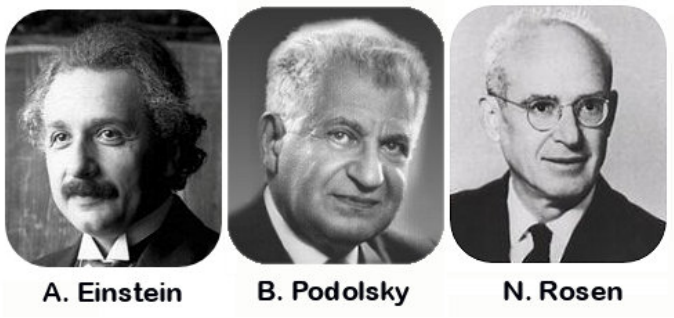
Le photon (quanta de lumière) est transmis/absorbé avec une probabilité $1/2$.

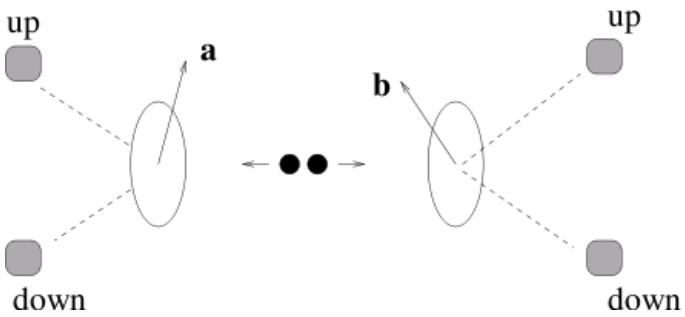
$\Rightarrow$ il est impossible de savoir à l'avance le résultat de la mesure !

Seule la **probabilité** du résultat de mesure de polarisation peut être prédite. *"Le vieux joue aux dés"*

Le "paradoxe" EPR : non-localité

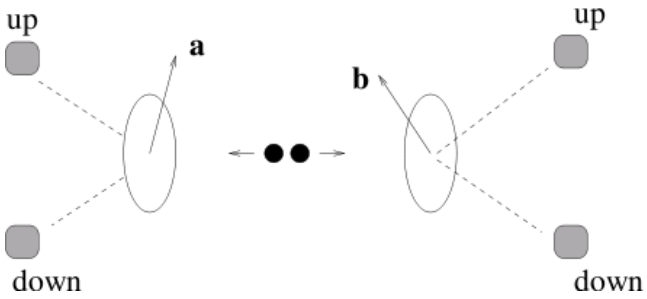
En 1935, Einstein, Podolsky et Rosen proposent une expérience de pensée montrant que soit la théorie quantique est incomplète, soit elle est non locale : une mesure a une *action instantanée à distance*





Dans un cristal non-linéaire un atome peut émettre une paire de photons (*photons jumeaux*) tq si le 1er photon est transmis par un polarisateur d'axe $\vec{a}$, alors le 2nd photon est instantanément polarisé $\perp \vec{a}$.

Violation de l'inégalité de Bell



$$\langle ab\rangle+\langle a'b\rangle+\langle a'b'\rangle-\langle ab'\rangle \leqslant 2$$

corrélations classiques

corrélations quantiques

↪ Expérience réalisée en 1982 par L. Aspect à Paris, puis dans d'autres laboratoires ⇒ l'inégalité de Bell est violée.

Principe de superposition

- L'*état d'une particule* est décrit par un *vecteur de* $\mathbb{C}^N$.

  ★ **Ex. 1 :** état de polarisation d'1 photon :

$$|\psi\rangle = c_0|\uparrow\rangle + c_1|\rightarrow\rangle \quad \in \mathbb{C}^2$$

  $|\uparrow\rangle$ ($|\rightarrow\rangle$) représente une polarisation verticale (horizontale)
  $c_{0,1}$ sont les composantes complexes vérifiant $|c_0|^2 + |c_1|^2 = 1$

  ★ **Ex. 2 :** état de polarisation de 2 photons jumeaux :

$$|\psi_{\mathrm{EPR}}\rangle = \frac{1}{\sqrt{2}}(|\uparrow,\rightarrow\rangle - |\rightarrow,\uparrow\rangle) \quad \in \mathbb{C}^4$$

- Une *observable (polarisation selon $\vec{a}$, énergie,...)* est décrite par une *matrice A auto-adjointe*. Ses valeurs sont quantifiées et données par les valeurs propres $\lambda_1, \cdots, \lambda_N$ de A.

Chat de Schrödinger et décohérence

E. Schrödinger a imaginé en 1935 un dispositif conduisant à une superposition d'un chat vivant et d'un chat mort :

$$|CHAT\rangle = \frac{1}{\sqrt{2}}(|\text{vivant}\rangle + |\text{mort}\rangle)$$

De telles superpositions ne peuvent exister que sur des temps ridiculement courts à cause de la **décohérence**, qui **transforme les états quantiques en états classiques.**

Un ordinateur quantique pour simuler... des systèmes quantiques

Les ordinateurs usuels ne peuvent simuler la dynamique d'un grand nb de particules quantiques. Un ordinateur fonctionnant selon les principes quantiques serait bien plus efficace *(R. Feynman 1982)*.

▷ Un ordinateur classique utilise des **bits dans les états** $0, 1$ pour représenter les nbs et effectuer les opérations logiques

▷ Un ordinateur quantique utilise des **"qubits"** dont les états sont des **combinaisons linéaires de** $|0\rangle$ **et** $|1\rangle$ **:**

$$|\psi\rangle = c_0|0\rangle + c_1|1\rangle \text{ avec } c_{0,1} \in \mathbb{C},\ |c_0|^2 + |c_1|^2 = 1.$$

→ Un tel ordinateur avec 150 qubits serait plus "puissant" que tous les super-ordinateurs du monde réunis !

Factoriser en nombres premiers

$$N = p_1^{n_1} \times p_2^{n_2} \times \dots$$

- Il est très difficile de factoriser en nombres premiers un grand entier N : les algorithmes connus nécessitent un temps $\approx O(N)$ exponentiel dans le nombre de bits codant N.
- Par contre, l'opération inverse (développer) est très simple.

  $\hookrightarrow$ *algorithme RSA utilisé pour crypter des messages grâce à* $N = p_1 p_2$, *pour décrypter il faut connaître* p_1 *et* p_2.

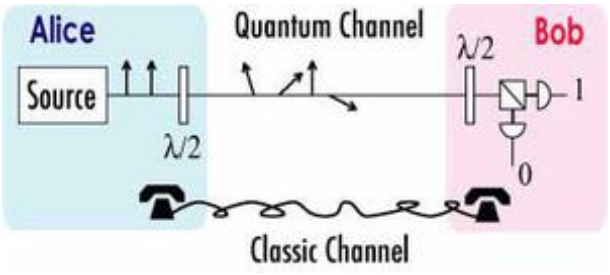
- En 1994, P. Schor découvre un "algorithme quantique" permettant de factoriser un entier N en facteurs premiers en un temps $O(\ln(N)^3)$.

  $\Rightarrow$ un ordinateur quantique pourrait décrypter facilement les messages cryptés par RSA !

Cryptographie quantique

- Comment distribuer à Alice et Bob une clé secrète leur permettant de décrypter un message public, de sorte qu'ils puissent s'apercevoir si un espion a intercepté la clé ?


- C'est impossible classiquement, mais C. Bennett et G. Brassard ont proposé en 1984 d'utiliser des photons polarisés :



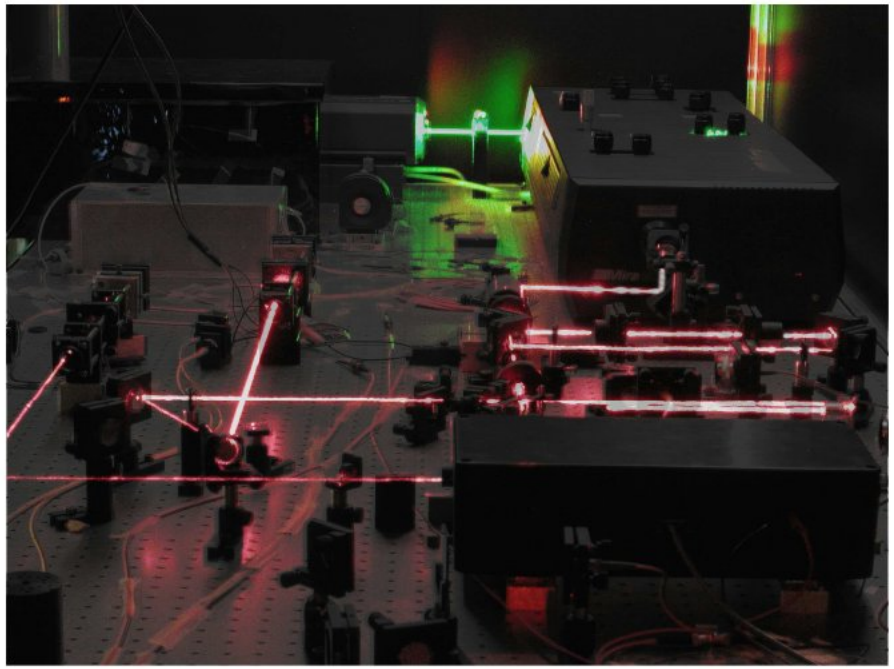
Polarisateur Alice	$\times$	$+$	$\times$	$+$	$+$	$\times$	$\times$	$+$
Résultat Alice	0	0	1	0	1	1	1	0
Polarisateur Bob	$+$	$\times$	$\times$	$+$	$+$	$+$	$\times$	$\times$
Résultat Bob	0	1	1	0	1	1	1	0
Clé secrète			1	0	1		1	

Si Eve mesure la polarisation dans la direction $\times$ et Alice et Bob dans la direction $+$, ces derniers obtiennent des résultats $\neq$ avec proba $1/2 \Rightarrow \exists$ espion!

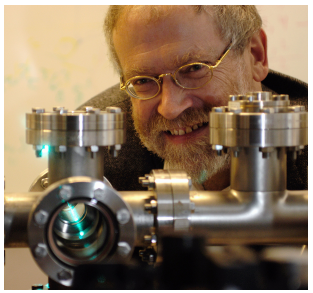
Téléportation quantique

Elle permet de "faxer" un état quantique $|\psi\rangle$ inconnu.

L'envoyeur et le receveur doivent **partager une paire EPR** (photons jumeaux) + échanger des informations classiquement



Expérience de Genève (N. Gisin)



$\hookrightarrow$ expérience réalisée pour la 1ère fois en 1997 à Innsbruck dans le groupe de A. Zeilinger.

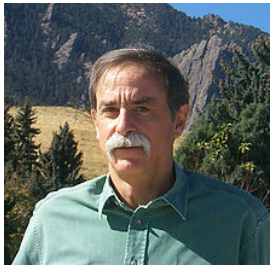
Les réalisations expérimentales

★ Moment magnétique de spin en Résonance Magnétique Nucléaire : factorisation $15 = 3 \times 5$ avec 7 qubits (IBM, Stanford University)

★ Ions piégés : téléportation, réalisation de portes quantiques, (R. Blatt, Innsbruck)

★ Photons dans une cavité : chats de Schrödinger, mesures quantiques (S. Haroche, Paris, prix Nobel 2012)

★ atomes froids manipulés par lasers (D. Wineland, Colorado, prix Nobel 2012)



★ Circuits supraconducteurs (à Grenoble : groupe d'O. Buisson)

Les difficultés...

→ il faut pouvoir contrôler et “manipuler” le système quantique (atomes, photons, spin,...)

→ la décohérence transforme rapidement un ordinateur quantique en ordinateur classique
⇒ effectuer les calculs sur un temps très court

→ les qubits doivent interagir entre eux pour créer des corrélations quantiques (difficile pour les photons).

Conclusion : il semble impossible à l'heure actuelle de réaliser un ordinateur avec plus d'une dizaine de qubits...

Conclusions

- ✓ L'information quantique est un domaine à cheval sur la **physique, l'informatique, et les mathématiques**
  $\hookrightarrow$ *force les scientifiques à travailler ensemble !*

- ✓ Une meilleure compréhension du monde quantique émerge grâce à :
  - ► des expériences avec des systèmes à peu de particules (photons, atomes) bien contrôlées et mesurées précisemment
  - ► rôle important joué par la théorie de l'information.

- ✓ Certaines applications existent déjà, comme les communications cryptées quantiquement, mais il faudra attendre longtemps avant de voir un véritable calculateur quantique...