

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

Dominique Spehner

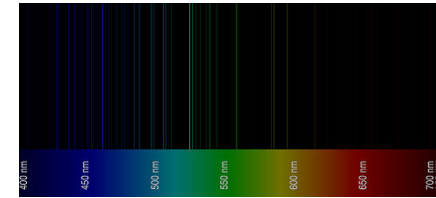
*Institut Fourier*

*et Laboratoire de Physique et Modélisation des Milieux Condensés*

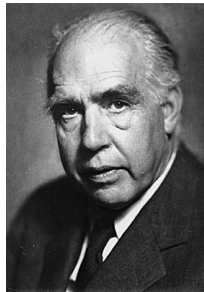
Université Joseph Fourier, Grenoble

## Physique du monde microscopique

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



*Raies d'émission du  
Cs*



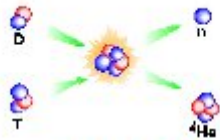
Library of Congress

Ses pères fondateurs sont :

M. Planck (1858-1947), N. Bohr (1885-1962),  
E. Schrödinger (1887-1961), W. Heisenberg (1901-1976),  
W. Pauli (1900-1958), P. Dirac (1902-1984),  
M. Born (1882-1970), P. Jordan (1902-1980)



## La physique quantique permet d'expliquer :



$10^{-15} M$

(noyaux, radioactivité  
Énergie nucléaire)



$10^{-10} M$

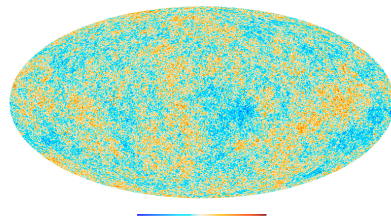
(atomes)



$10^{-8} M$

(molécules  
biologiques)

- 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)

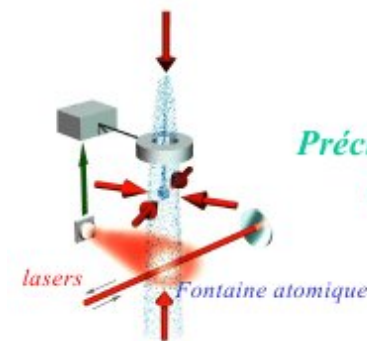
(rayonnement fossile de l'univers mesuré par Planck)

## 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*  
↪ *systèmes de navigation GPS*



*Précision d'une seconde  
sur 10 Millions  
d'années!*

*(Horloge atomique)*

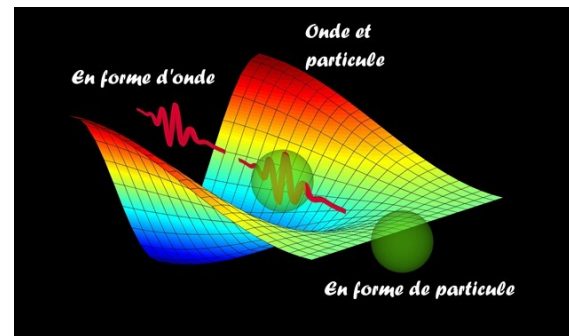
Qu'en sera-t-il au XXI-ième siècle ?

## 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.**

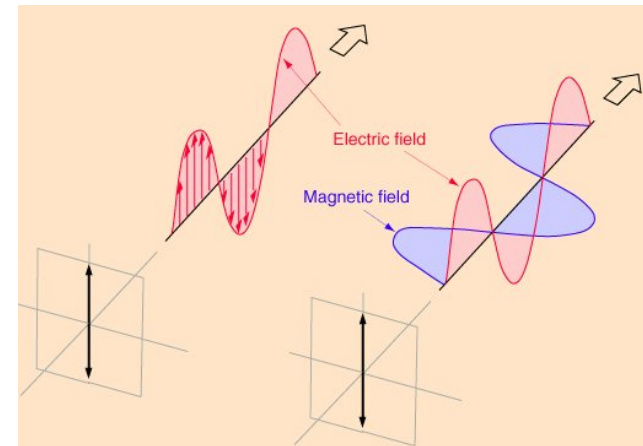
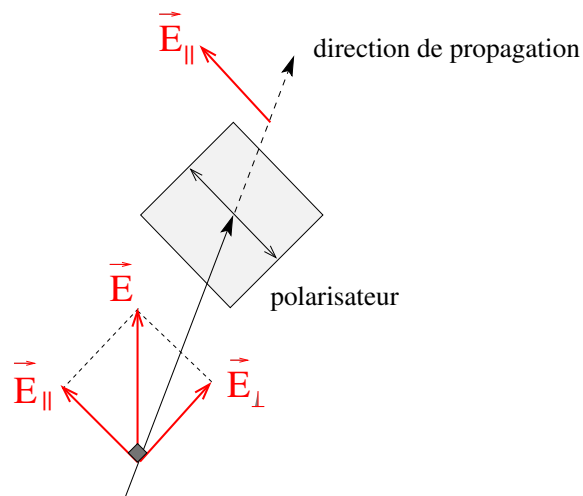


Nature ondulatoire de la matière : L. de Broglie (1892-1987)

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.

## 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”*

## 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.

*↔ 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  $O(\ln(N)^3)$ .

⇒ un ordinateur quantique pourrait décrypter facilement les messages cryptés par RSA !

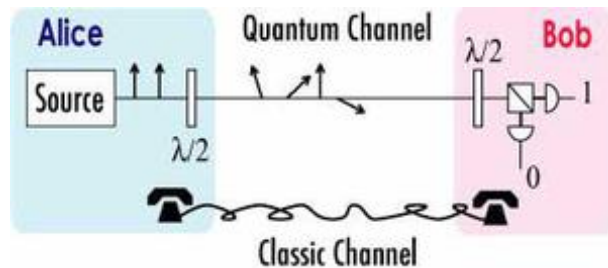


## Cryptographie quantique

► 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	×	+	×	+	+	×	×	+
Résultat Alice	0	0	1	0	1	1	1	0
Polarisateur Bob	+	×	×	+	+	+	×	×
Résultat Bob	0	1	1	0	1	1	1	0
<b>Clé secrète</b>			1	0	1		1	

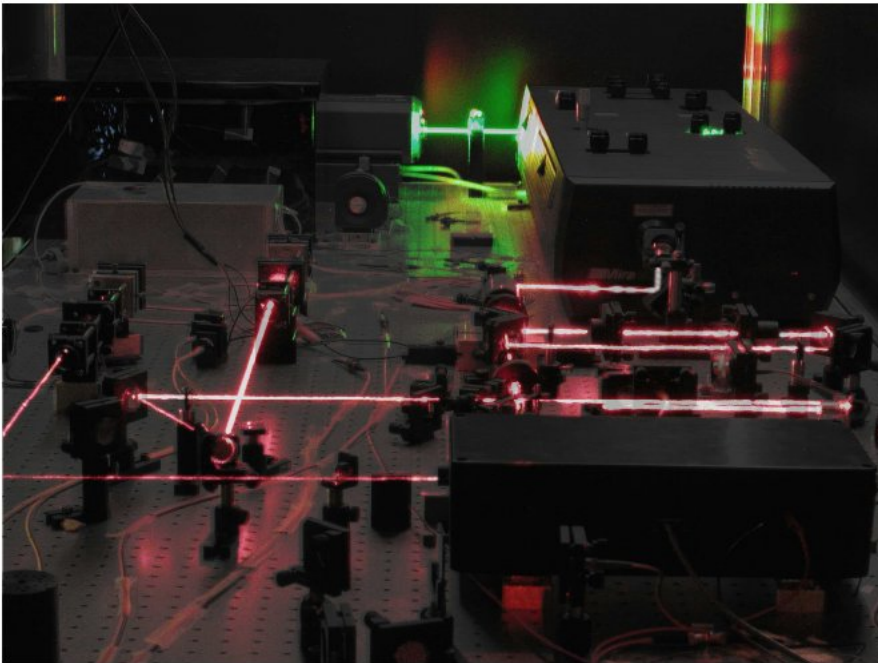
Si Eve mesure la polarisation dans la direction × et Alice et Bob dans la direction +, ces derniers obtiennent des résultats  $\neq$  avec proba  $1/2 \Rightarrow \exists$  espion!



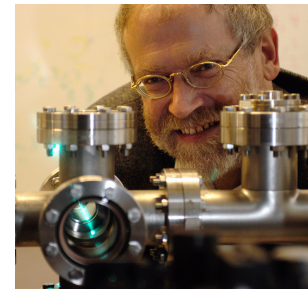
## Téléportation quantique

Elle permet de “faxer” un état quantique inconnu.

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

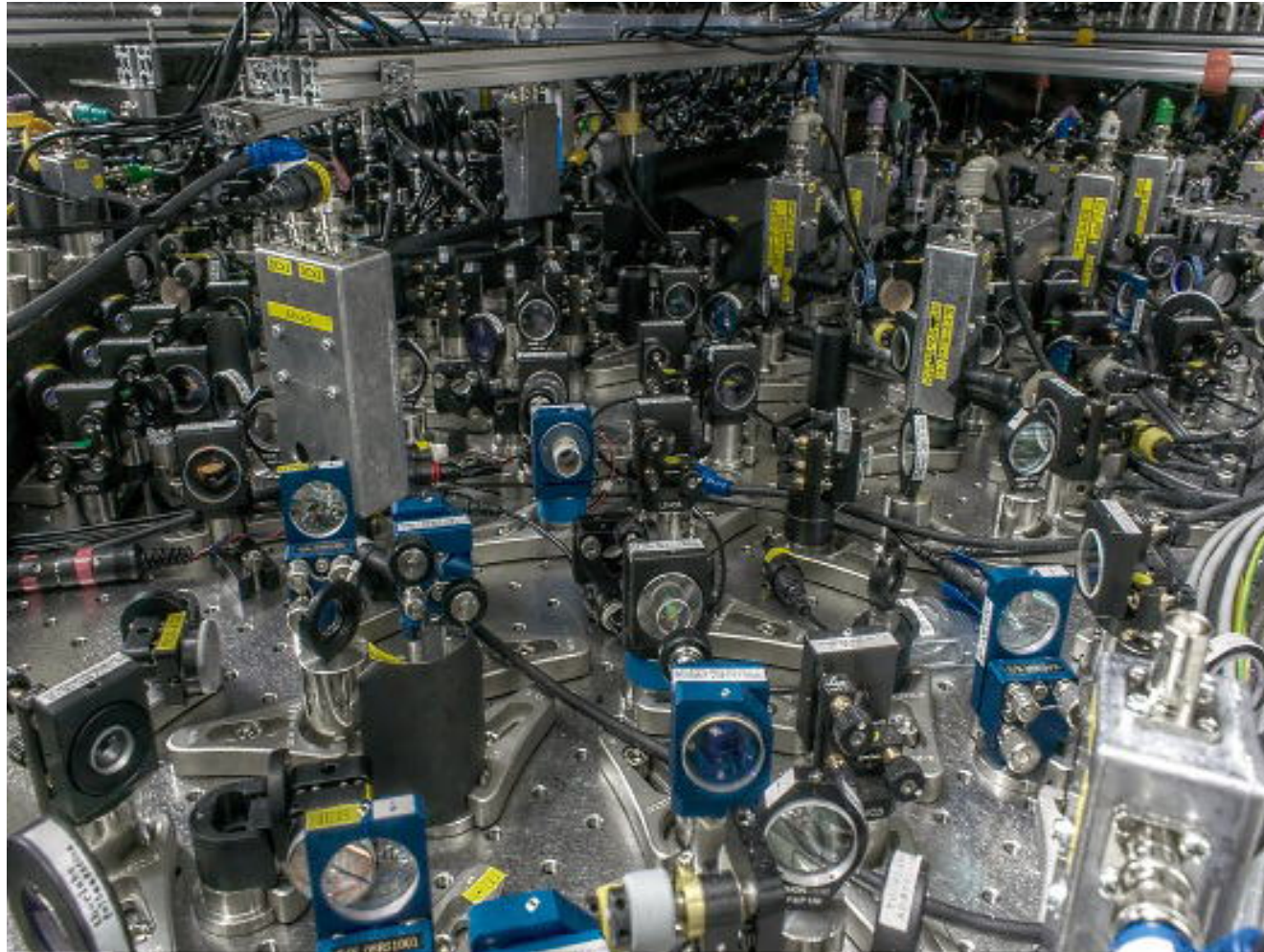


*Expérience de Genève (N. Gisin)*



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

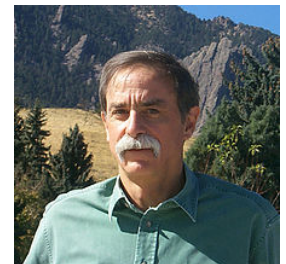
## Téléportation de “chats de Schrödinger”



*Expérience de Tokyo, School of engineering (A. Furusawa)*

## 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, défauts dans le diamant** (à Grenoble : groupes d'O. Buisson et d'O. Arcizet)



## 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 difficile 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**  
↔ *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 précisément
  - ▶ rôle important joué par la théorie de l'information.
- ✓ Certaines applications existent déjà, comme les communications cryptées quantiquement, mais il faudra encore attendre beaucoup de progrès techniques avant de voir un véritable ordinateur quantique...