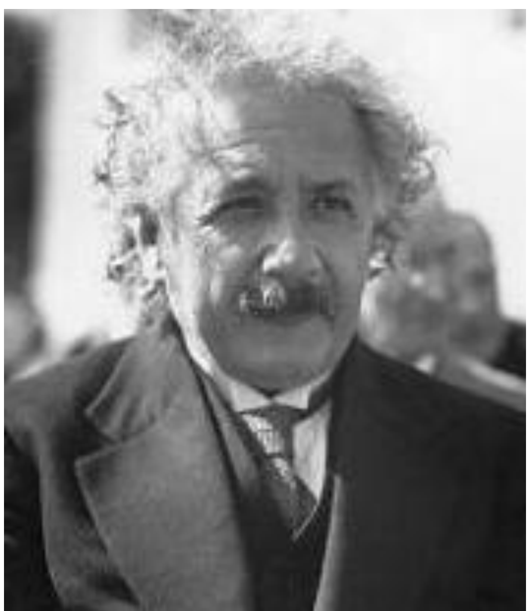
# From Einstein's doubts to quantum information: a new quantum revolution

Alain ASPECT - Institut d'Optique - Palaiseau



Enrico Fermi Lecture

Roma

06 02 2014

# Quantum information
# a flourishing field

**Quantum Information**
www.vjquantuminfo.org/ - Traduire cette page
Virtual Journal of **Quantum Information**, a multijournal compilation, contains articles that focus on **quantum information**, including quantum computing, ...

MAY 15, 1935 PHYSICAL REVIEW VOLUME 47

**Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?**

A. EINSTEIN, B. PODOLSKY AND N. ROSEN, *Institute for Advanced Study, Princeton, New Jersey*
(Received March 25, 1935)

age
new era of

OCTOBER 15, 1935 PHYSICAL REVIEW VOLUME 48

**Can Quantum-Mechanical Description of Physical Reality be Considered Complete?**

N. BOHR, *Institute for Theoretical Physics, University, Copenhagen*
(Received July 13, 1935)

nced readers

Proceedings of the Cambridge Philosophical Society, 1935 - hep.princeton.edu

DISCUSSION OF PROBABILITY RELATIONS BETWEEN SEPARATED SYSTEMS

BY E. SCHRÖDINGER

[Communicated by Mr M. BORN]

Physics Vol. 1, No. 3, pp. 195–200, 1964 Physics Publishing Co. Printed in the United Stat

ON THE EINSTEIN PODOLSKY ROSEN PARADOX*

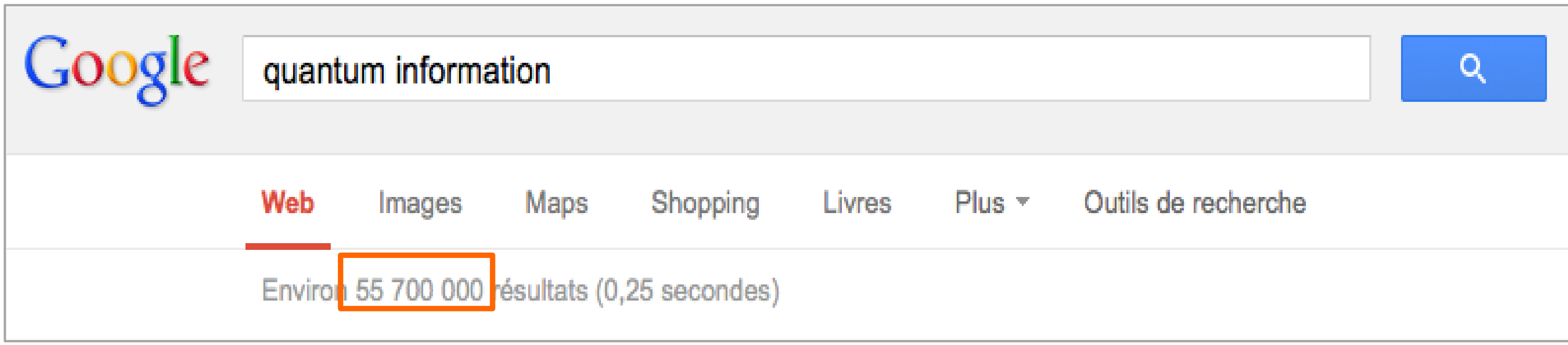
J. S. BELL†
*Department of Physics, University of Wisconsin, Madison, Wisconsin*
†On leave of absence from SLAC and CERN

ons: Homepage

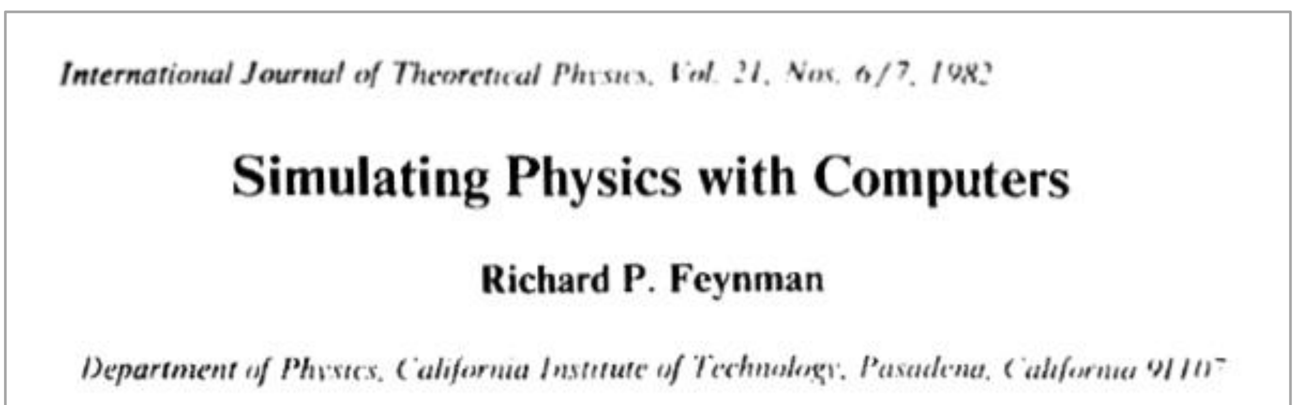
The Centre for **Quantum Information** and Foundations (formerly the Centre for Quantum Computation), part of the University of Cambridge, and based within the ...

Entanglement is different!

# Quantum information
# a flourishing field




How did it emerge?


*International Journal of Theoretical Physics, Vol. 21, Nos. 6/7, 1982*

**Simulating Physics with Computers**

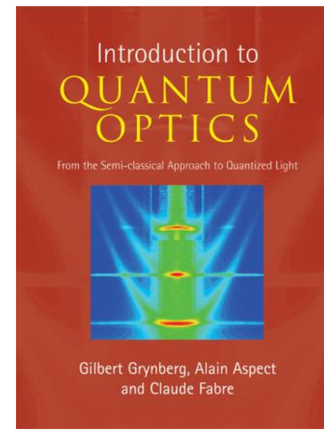
**Richard P. Feynman**

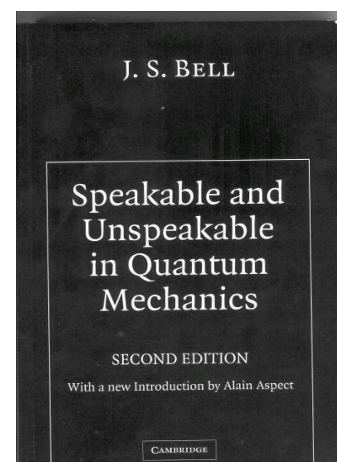
*Department of Physics, California Institute of Technology, Pasadena, California 91107*

Entanglement is more!

# From Einstein's doubts to quantum information

1. From Einstein-Podolsky -Rosen to Bell
2. Experimental tests of Bell's inequalities with correlated photons
3. A new quantum age

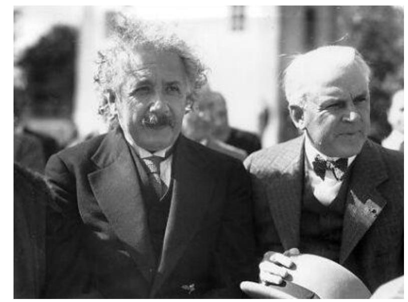


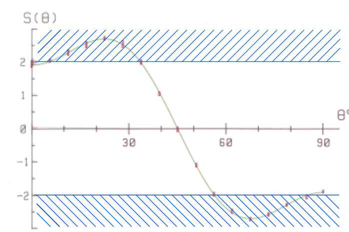



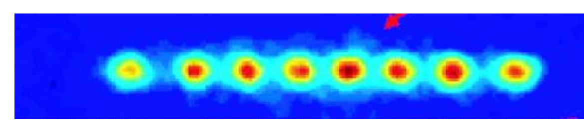

http://www.lcf.institutoptique.fr/Alain-Aspect-homepage

# From Einstein’s doubts to quantum information

1. From Einstein-Podolsky -Rosen to Bell:
   entanglement is different
2. Experimental tests of Bell’s inequalities with correlated photons
3. A new quantum age?







# Einstein and quantum physics

## A founding contribution (1905)

Light is made of quanta, later named photons, which have well defined energy and momentum. Nobel 1922.

## A fruitful objection (1935): entanglement

Einstein, Podolsky, Rosen (EPR): The quantum formalism allows one to envisage amazing situations (pairs of entangled particles): the formalism must be completed.

Objection underestimated for a long time (except Bohr's answer, 1935) until Bell's theorem (1964) and the acknowledgement of its importance (1970-82).

## Entanglement at the core of quantum information (198x-20??)

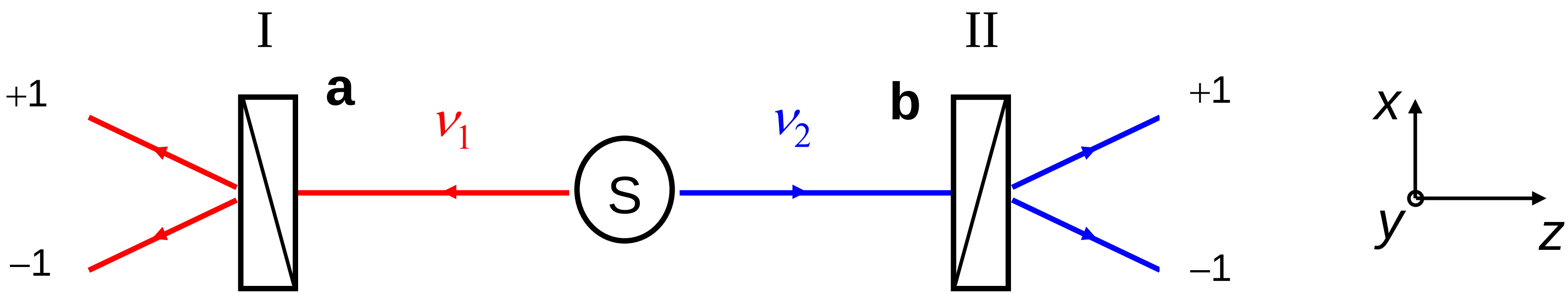
# The EPR question

Is it possible (necessary) to explain the probabilistic character of quantum predictions by invoking a supplementary underlying level of description (supplementary parameters, hidden variables) ?

A positive answer was the conclusion of the Einstein-Podolsky-Rosen reasoning (1935). Bohr strongly opposed this conclusion.

Bell’s theorem (1964) has allowed us to settle the debate.

# The EPR GedankenExperiment with photons correlated in polarization

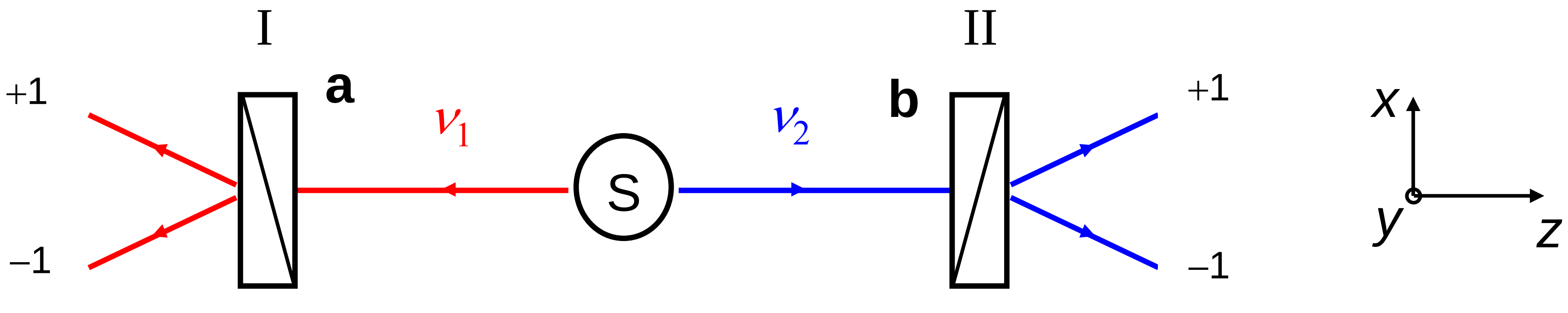



Measurement of the polarization of $\nu_1$ along orientation **a** and and of polarization of $\nu_2$ along orientation **b** : results +1 or –1

- Probabilities to find +1 ou –1 for $\nu_1$ (measured along **a**) and +1 or –1 for $\nu_2$ (measured along **b**).

| Single probabilities | Joint probabilities |
|---|---|
| $P_+(\mathbf{a})\ ,\ P_-(\mathbf{a})$ | $P_{++}(\mathbf{a},\mathbf{b})\ ,\ P_{+-}(\mathbf{a},\mathbf{b})$ |
| $P_+(\mathbf{b})\ ,\ P_-(\mathbf{b})$ | $P_{-+}(\mathbf{a},\mathbf{b})\ ,\ P_{--}(\mathbf{a},\mathbf{b})$ |

# The EPR GedankenExperiment with photons correlated in polarization




For the entangled EPR state… $|\Psi(\nu_1,\nu_2)\rangle = \frac{1}{\sqrt{2}}\{|x,x\rangle + |y,y\rangle\}$

Quantum mechanics predicts
results separately random …

$$P_+(\mathbf{a}) = P_-(\mathbf{a}) = \frac{1}{2} \;;\; P_+(\mathbf{b}) = P_-(\mathbf{b}) = \frac{1}{2}$$

but strongly correlated:

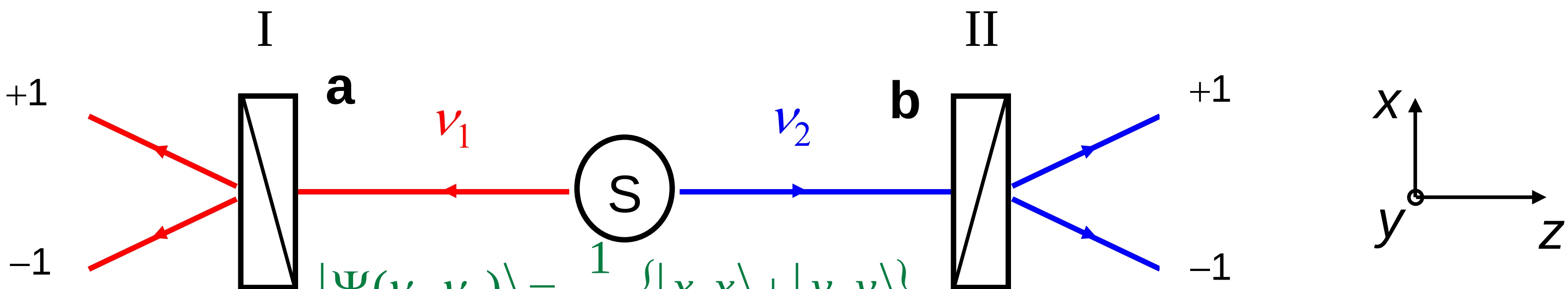
$$P_{++}(\mathbf{a},\mathbf{b}) = P_{--}(\mathbf{a},\mathbf{b}) = \frac{1}{2}\cos^2(\mathbf{a},\mathbf{b})$$

$$P_{+-}(\mathbf{a},\mathbf{b}) = P_{-+}(\mathbf{a},\mathbf{b}) = \frac{1}{2}\sin^2(\mathbf{a},\mathbf{b})$$

$$P_{++}(0) = P_{--}(0) = \frac{1}{2}$$

$$P_{+-}(0) = P_{-+}(0) = 0$$

# Coefficient of correlation of polarization (EPR state)




$$|\Psi(\nu_1,\nu_2)\rangle = \frac{1}{\sqrt{2}}\{|x,x\rangle + |y,y\rangle\}$$

Quantitative expression of the correlations between results of measurements in I et II: coefficient:

$$E = P_{++} + P_{--} - P_{+-} - P_{-+} = P(\text{résultats id°}) - P(\text{résultats ¹ })$$

QM predicts, for parallel polarizers (a,b) = 0

$$P_{++} = P_{--} = \frac{1}{2} \quad \Rightarrow \quad E_{\mathrm{MQ}} = 1$$

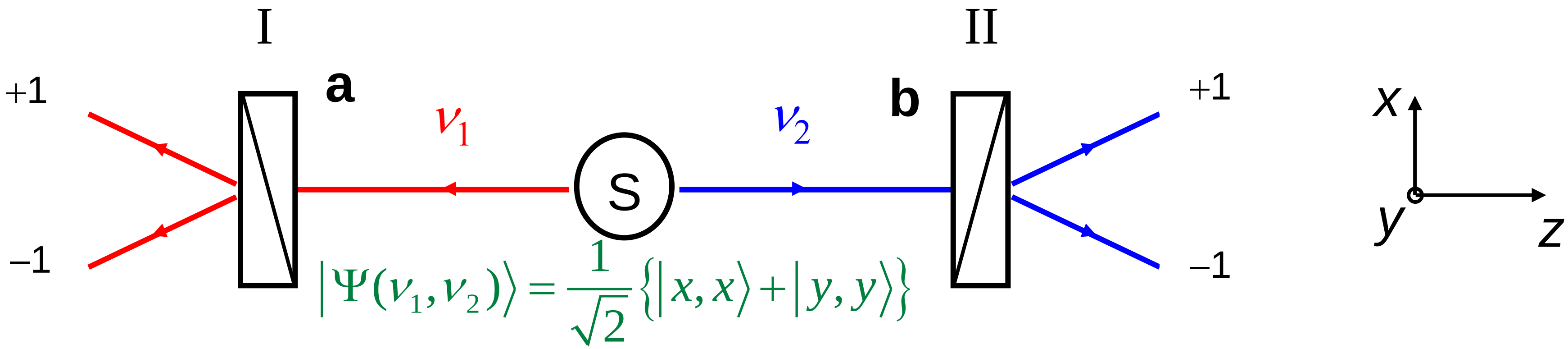
$$P_{+-} = P_{-+} = 0$$

Total correlation

More generally, for an arbitrary angle (a,b) between polarizers

$$E_{\mathrm{MQ}}(\mathbf{a},\mathbf{b}) = \cos 2(\mathbf{a},\mathbf{b})$$

# How to “understand” the EPR correlations predicted by quantum mechanics?




$$E_{\mathrm{MQ}}(\mathbf{a},\mathbf{b}) = \cos 2(\mathbf{a},\mathbf{b})$$

Can we derive an image from the QM calculation?

# How to "understand" the EPR correlations predicted by quantum mechanics?

## Can we derive an image from the QM calculation?

The direct calculation $P_{++}(\mathbf{a},\mathbf{b}) = \left|\langle +_{\mathbf{a}}, +_{\mathbf{b}} | \Psi(\nu_1,\nu_2)\rangle\right|^2 = \frac{1}{2}\cos^2(\mathbf{a},\mathbf{b})$ is done in an abstract space, where the two particles are described globally: impossible to extract an image in real space where the two photons are separated.

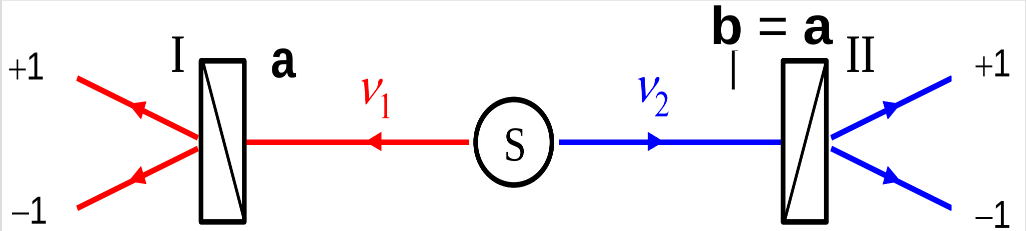
Related to the non factorability of the entangled state:

$$|\Psi(\nu_1,\nu_2)\rangle = \frac{1}{\sqrt{2}}\left\{|x,x\rangle + |y,y\rangle\right\} \neq |\phi(\nu_1)\rangle \cdot |\chi(\nu_2)\rangle$$

One cannot identify properties attached to each photon separately

"Quantum phenomena do not occur in a Hilbert space, they occur in a laboratory" (A. Peres) $\Rightarrow$ An image in real space?

# A real space image of the EPR correlations derived from a quantum calculation




$$|\Psi(\nu_1,\nu_2)\rangle = \frac{1}{\sqrt{2}}\{|x,x\rangle + |y,y\rangle\} = \frac{1}{\sqrt{2}}\{|+_{\mathbf{a}},+_{\mathbf{a}}\rangle + |-_{\mathbf{a}},-_{\mathbf{a}}\rangle\}$$

2 step calculation (standard QM)

1) Measure on $\nu_1$ by I (along **a**)

$\Rightarrow$ result $+1$ $|+_{\mathbf{a}}\rangle$

or

$\Rightarrow$ result $-1$ $|-_{\mathbf{a}}\rangle$

Just after the measure, “collapse of the state vector”: projection onto the eigenspace associated to the result

$|+_{\mathbf{a}},+_{\mathbf{a}}\rangle$

or

$|-_{\mathbf{a}},-_{\mathbf{a}}\rangle$

2) Measure on $\nu_2$ by II (along **b** = **a** )

- If one has found $+1$ for $\nu_1$ then the state of $\nu_2$ is $|+_{\mathbf{a}}\rangle$ and the measurement along **b** = **a** yields $+1$;
- If one has found $-1$ for $\nu_1$ then the state of $\nu_2$ is $|-_{\mathbf{a}}\rangle$ and the measurement along **b** = **a** yields $-1$;

Easily generalized to **b** ≠ **a** (Malus law)

The measurement on $\nu_1$ seems to influence instantaneously at a distance the state of $\nu_2$ : unacceptable for Einstein (relativistic causality).

# A classical image for the correlations at a distance (suggested by the EPR reasoning)

- The two photons of the same pair bear from their very emission an identical property ($\lambda$) , that will determine the results of polarization measurements.
- The property $\lambda$ differs from one pair to another.

exemple

$\lambda = +_a$

ou

$\lambda = -_a$

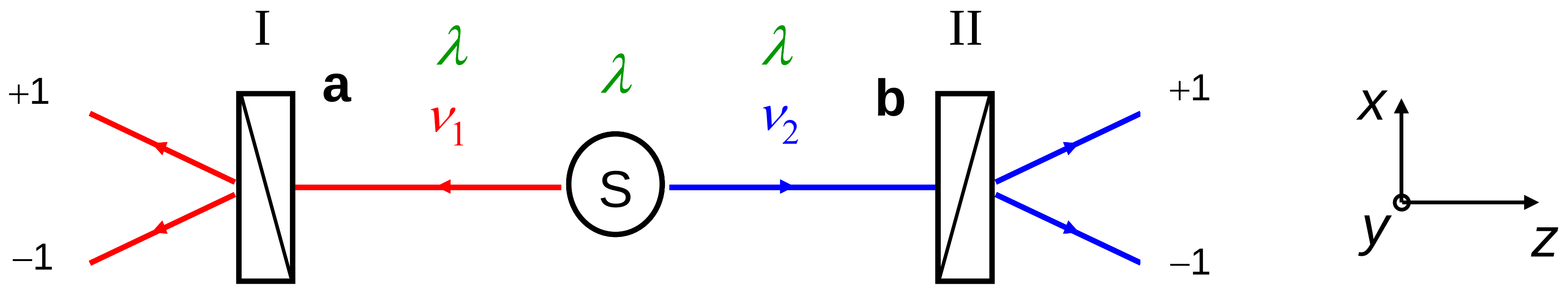



Image simple and convincing (analogue of identical chromosomes for twin brothers), but……amounts to completing quantum formalism: $\lambda$ = supplementary parameter, "hidden variable".

⇨ Bohr disagreed: QM description is complete, you cannot add anything to it

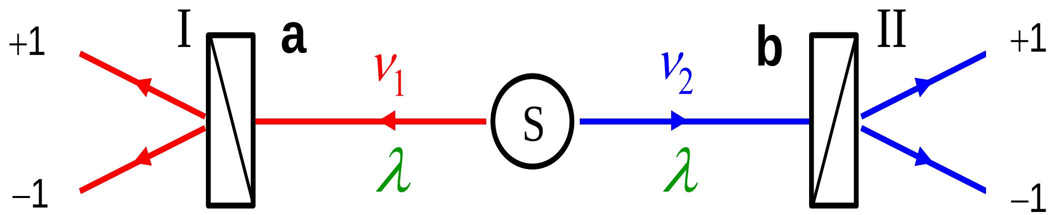
# A debate for many decades

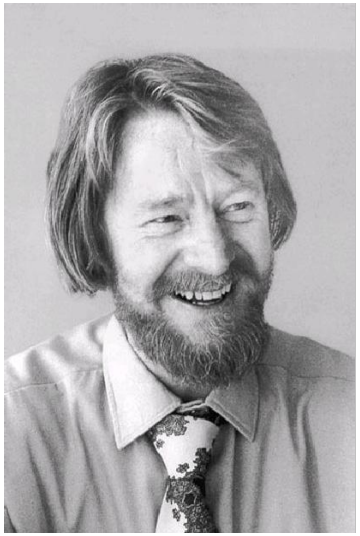
Intense debate between Bohr and Einstein…

… without much attention from a majority of physicists

- Quantum mechanics accumulates success:
  - Understanding nature: structure and properties of matter, light, and their interaction (atoms, molecules, absorption, spontaneous emission, solid properties, superconductivity, superfluidity, elementary particles …)
  - New concepts leading to revolutionary inventions: transistor (later: laser, integrated circuits…)
- No disagreement on the validity of quantum predictions, only on its interpretation.

# 1964: Bell's formalism



Consider local supplementary parameters theories (in the spirit of Einstein's ideas on EPR correlations):

- The two photons of a same pair have a common property $\lambda$ (sup. param.) determined at the joint emission

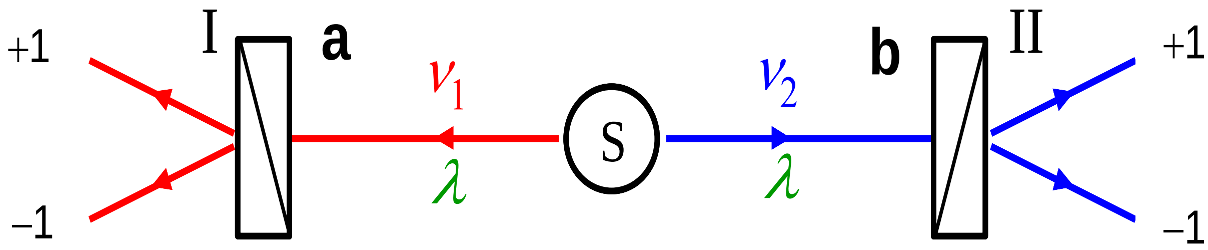
- The supplementary parameter $\lambda$ determines the results of measurements at I and II $\Leftrightarrow$ $A(\lambda, \mathbf{a}) = +1 \text{ or } -1$ at polarizer I

  $B(\lambda, \mathbf{b}) = +1 \text{ or } -1$ at polarizer II

- The supplementary parameter $\lambda$ is randomly distributed among pairs $\Leftrightarrow$ $\rho(\lambda) \geq 0$ and $\int \rho(\lambda)\, d\lambda = 1$ at source S

$$E(\mathbf{a}, \mathbf{b}) = \int \mathrm{d}\lambda\, \rho(\lambda)\, A(\lambda, \mathbf{a})\, B(\lambda, \mathbf{b})$$

# 1964: Bell's formalism to explain correlations



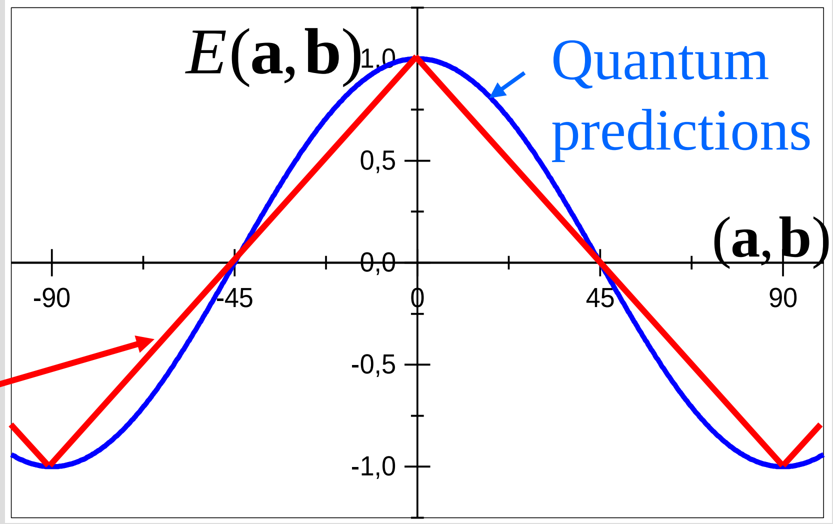

## An example

- Common polarisation $\lambda$, randomly distributed among pairs $\rho(\lambda) = 1/2\pi$
- Result (±1) depends on the angle between $\lambda$ and polarizer orientation (**a** or **b**)

$$A(\lambda, \mathbf{a}) = \text{sign}\{\cos 2(\theta_{\mathbf{a}} - \lambda)\}$$

$$B(\lambda, \mathbf{b}) = \text{sign}\{\cos 2(\theta_{\mathbf{b}} - \lambda)\}$$

Resulting correlation




Not bad, but no exact agreement

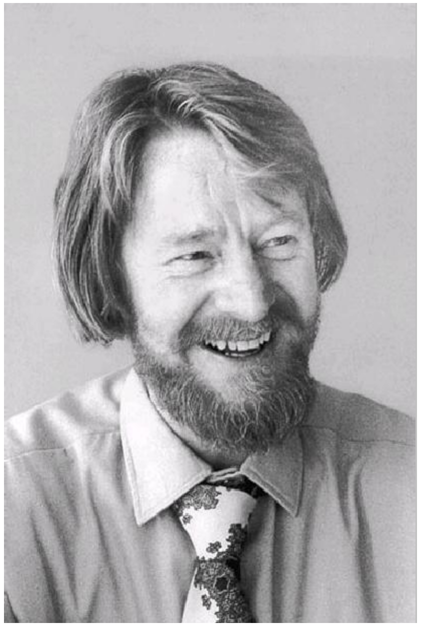
Is there a better model, agreeing with QM predictions at all orientations?

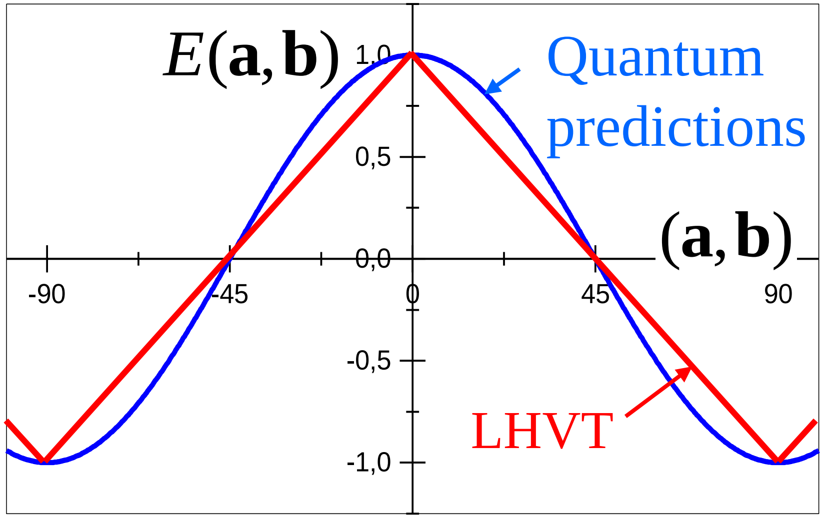
Bell's theorem gives the answer

# Bell's theorem

# No!

No local hidden variable theory (in the spirit of Einstein's ideas) can reproduce quantum mechanical predictions for EPR correlations at all the orientations of polarizers.






Impossible to cancel the difference everywhere

Impossible to have quantum predictions exactly reproduced at *all* orientations, by any model à la Einstein

# Bell's inequalities are violated by certain quantum predictions

Any local hidden variables theory $\Rightarrow$ Bell's inequalities

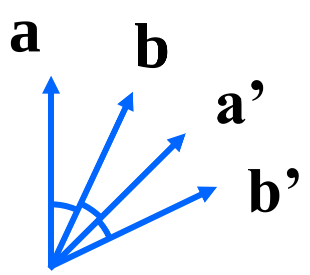
$-2 \leq S \leq 2$ avec $S = E(\mathbf{a},\mathbf{b}) - E(\mathbf{a},\mathbf{b}') + E(\mathbf{a}',\mathbf{b}) + E(\mathbf{a}',\mathbf{b}')$

CHSH inequ. (Clauser, Horne, Shimony, Holt, 1969)

Quantum mechanics $E_{\text{MQ}}(\mathbf{a},\mathbf{b}) = \cos 2(\mathbf{a},\mathbf{b})$

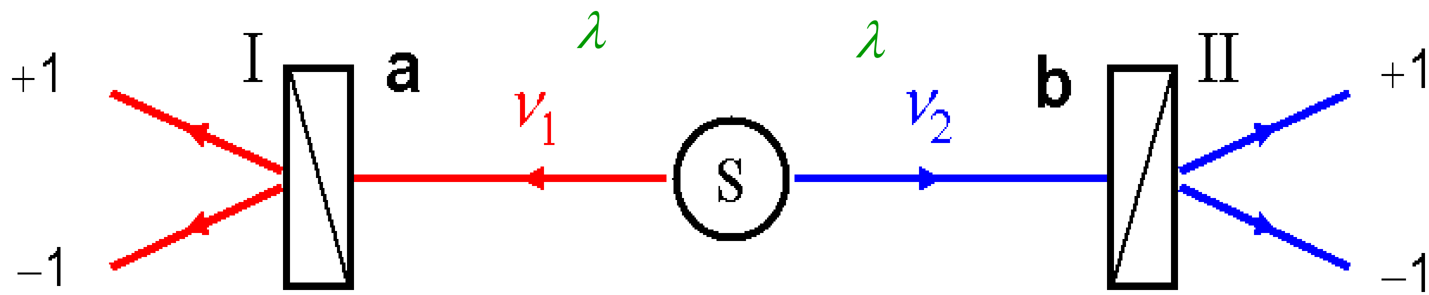
For orientations $(\mathbf{a},\mathbf{b}) = (\mathbf{b},\mathbf{a}') = (\mathbf{a}',\mathbf{b}) = \dfrac{\pi}{8}$

$S_{\text{QM}} = 2\sqrt{2} = 2.828... > 2$




CONFLICT ! The possibility to complete quantum mechanics according to Einstein ideas is no longer a matter of taste (of interpretation). It has turned into an experimental question.

# Conditions for a conflict
# (⇒ hypotheses for Bell's inequalities)

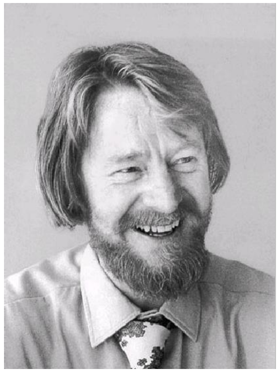



Supplementary parameters λ carried along by each particle.
Explanation of correlations « à la Einstein » attributing individual properties to each separated particle: local realist world view.

**Bell's locality condition**

- The result $A(\lambda, \mathbf{a})$ of the measurement on $\nu_1$ by I does not depend on the orientation **b** of distant polarizer II (and conv.)
- The distribution $\rho(\lambda)$ of supplementary parameters over the pairs does not depend on the orientations **a** and **b**.

# Bell’s locality condition

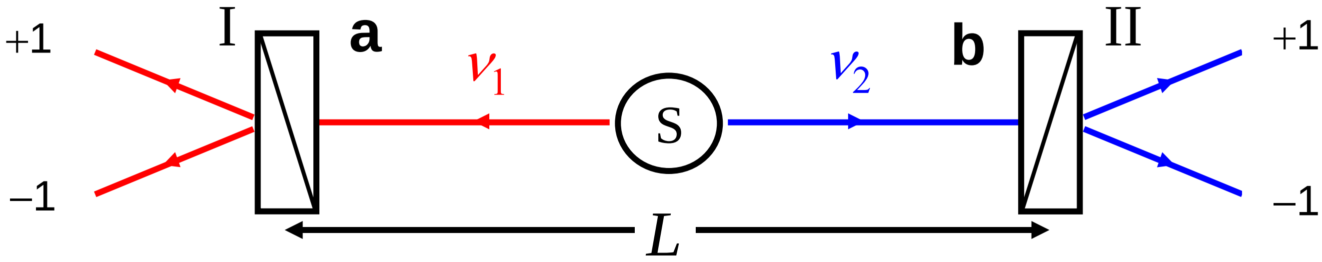


$$A(\lambda,\mathbf{a},\cancel{\mathbf{b}}) \qquad B(\lambda,\cancel{\mathbf{a}},\mathbf{b}) \qquad \rho(\lambda,\cancel{\mathbf{a}},\cancel{\mathbf{b}})$$

can be stated as a reasonable hypothesis, but…

…in an experiment with variable polarizers (orientations modified faster than the propagation time $L/c$ of light between polarizers) Bell’s locality condition becomes a consequence of Einstein’s relativistic causality (no faster than light influence)

*cf. Bohm & Aharonov, Physical Review, 1957*




Conflict between quantum mechanics and Einstein’s world view (local realism based on relativity).

# From epistemology debates to experimental tests

Bell's theorem demonstrates a quantitative incompatibility between the local realist world view (à la Einstein) –which is constrained by Bell's inequalities, and quantum predictions for pairs of entangled particles –which violate Bell's inequalities.

An experimental test is possible.

When Bell's paper was written (1964), there was no experimental result available to be tested against Bell's inequalities:

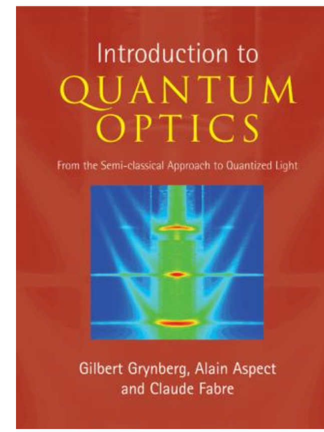
- Bell's inequalities apply to all correlations that can be described within classical physics (mechanics, electrodynamics).
- B I apply to most of the situations which are described within quantum physics (except EPR correlations)

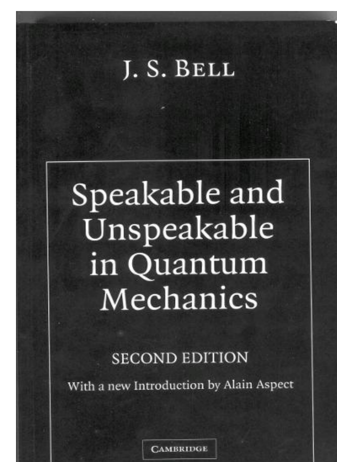
One must find a situation where the test is possible:

CHSH proposal (1969)

# From Einstein's doubts to quantum information

1. From Einstein-Podolsky -Rosen to Bell
2. Experimental tests of Bell's inequalities with correlated photons: entanglement demonstrated
3. A new quantum age



# Three generations of experiments

Pioneers (1972-76): Berkeley, Harvard, Texas A&M

- First results contradictory (Clauser = QM; Pipkin ≠ QM)
- Clear trend in favour of Quantum mechanics (Clauser, Fry)
- Experiments significantly different from the ideal scheme

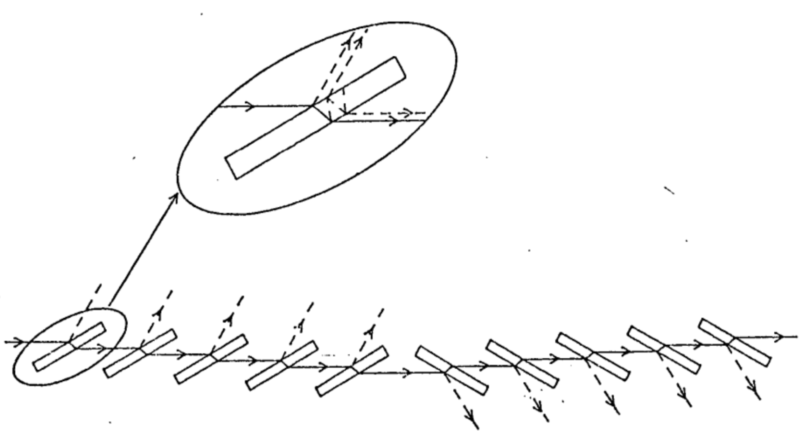
Institut d'optique experiments (1975-82)

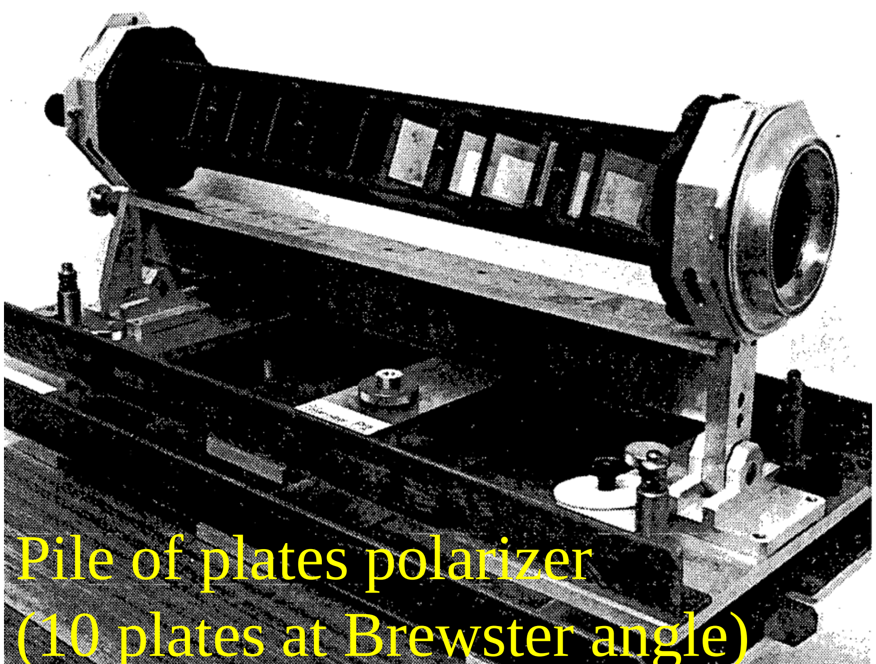
- A source of entangled photons of unprecedented efficiency
- Schemes closer and closer to the ideal GedankenExperiment
- Test of quantum non locality (relativistic separation)

Third generation experiments (1988-): Maryland, Rochester, Malvern, Genève, Innsbruck, Los Alamos, Boulder, Urbana Champaign…

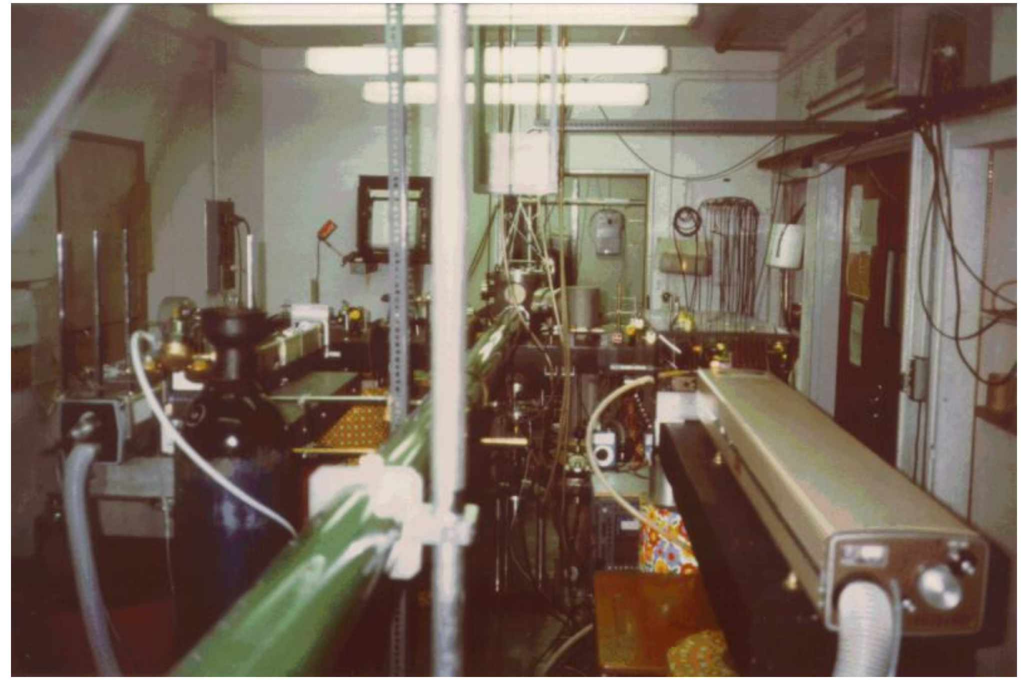
- New sources of entangled pairs
- Closure of the last loopholes
- Entanglement at very large distance
- Entanglement on demand

# Orsay's source of pairs of entangled photons (1981)





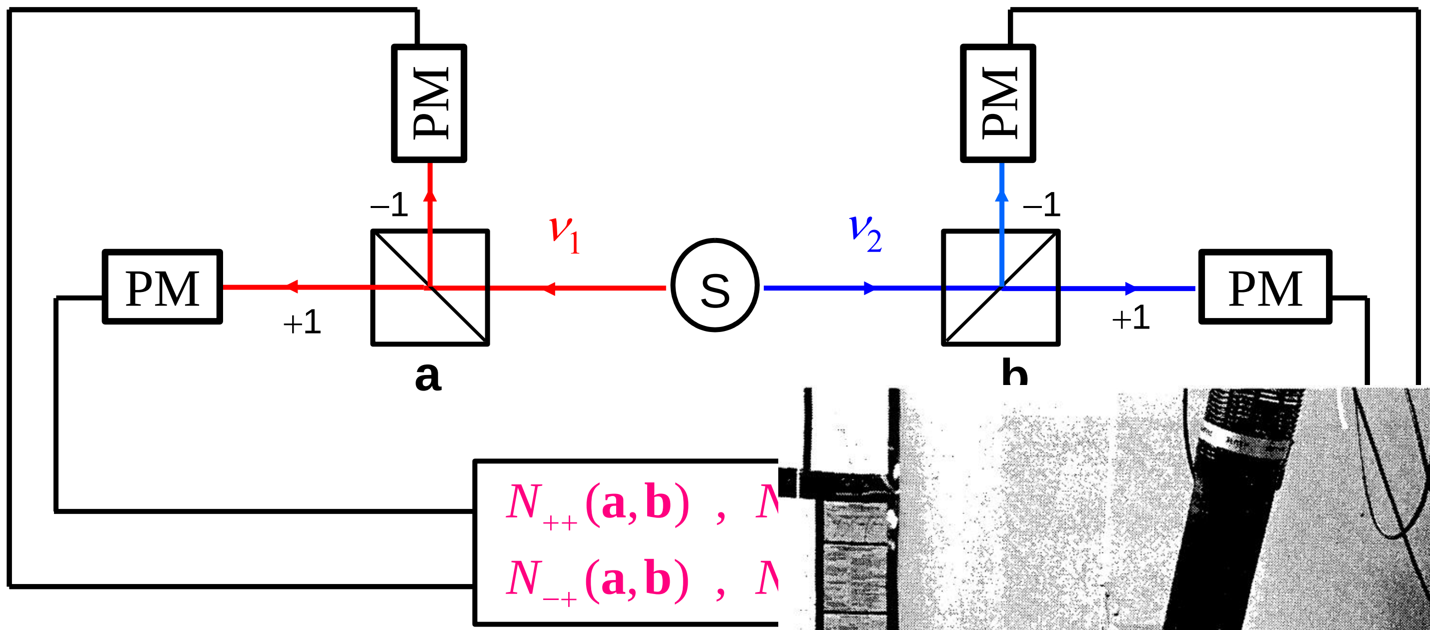
Pile of plates polarizer
(10 plates at Brewster angle)

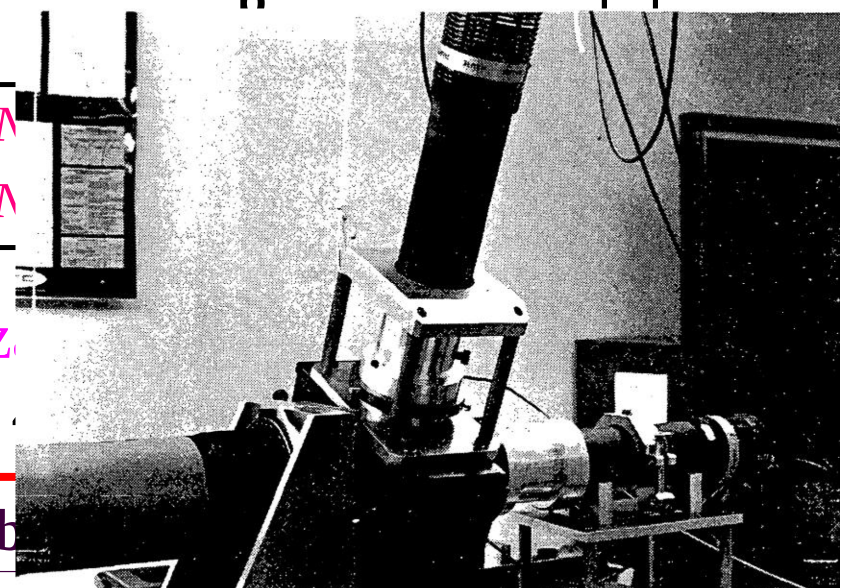


☺ 100 coincidences per second
1% precision for 100 s counting

Polarizers at 6 m from the source:
violation of Bell's inequalities,
entanglement survives "large" distance

# Experiment with 2-channel polarizers (AA, P. Grangier, G. Roger, 1982)



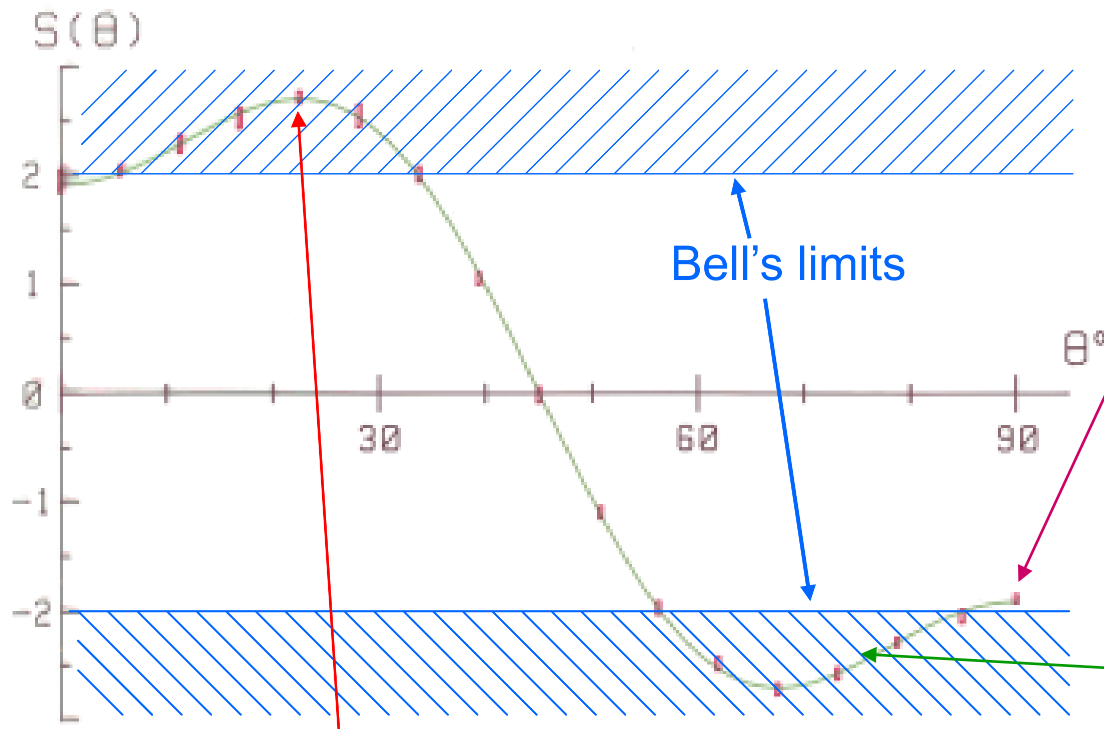



Direct measurement of the polariz

simultaneous measurement of the

$$E(\mathbf{a},\mathbf{b}) = \frac{N_{++}(\mathbf{a},\mathbf{b}) - N_{+-}(\mathbf{a},\mathbf{b}\ldots}{N_{++}(\mathbf{a},\mathbf{b}) + N_{+-}(\mathbf{a},\mathbf{b}) + N_{-+}(\mathbf{a},\mathbf{b}) + N_{--}(\mathbf{a},\mathbf{b})}$$

# Experiment with 2-channel polarizers (AA, P. Grangier, G. Roger, 1982)




▯ Measured value ± 2 standard dev.

— Quantum mechanical prediction (including imperfections of real experiment)

For $\theta = (\mathbf{a},\mathbf{b}) = (\mathbf{b},\mathbf{a}') = (\mathbf{a}',\mathbf{b}) = 22.5°$ $S_{exp}(\theta) = 2.697 \pm 0.015$

Violation of Bell's inequalities $S \leq 2$ by more than $40\ \sigma$

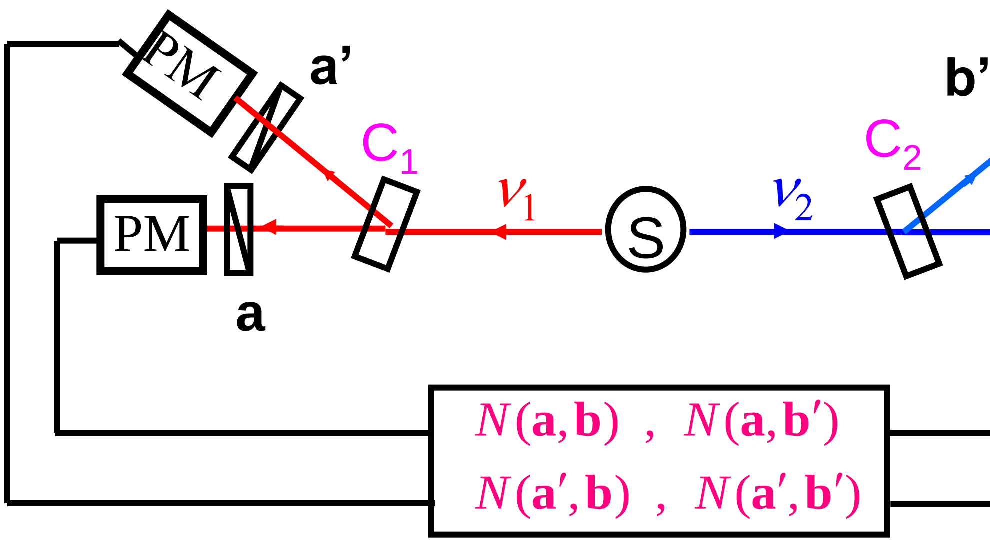
Excellent agreement with quantum predictions $S_{MQ} = 2.70$

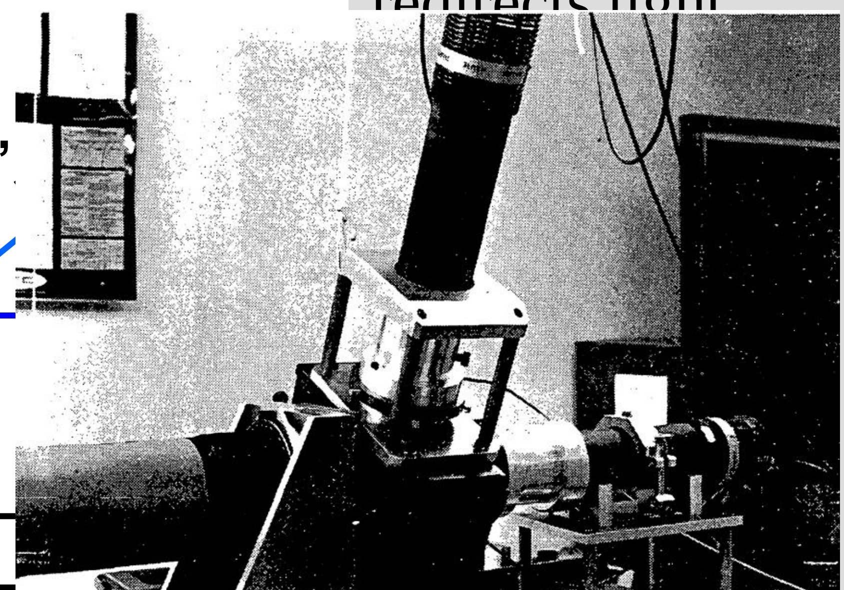
# Experiment with variable polarizers AA, J. Dalibard, G. Roger, PRL 1982

Impose locality as a consequence of relativistic causality: change of polarizer orientations faster than the time of propagation of light between the two polarizers (40 nanoseconds for $L$ = 12 m)

☹ Not realist with massive polarizer

☺ Possible with optical switch



Switch $C_1$ redirects light

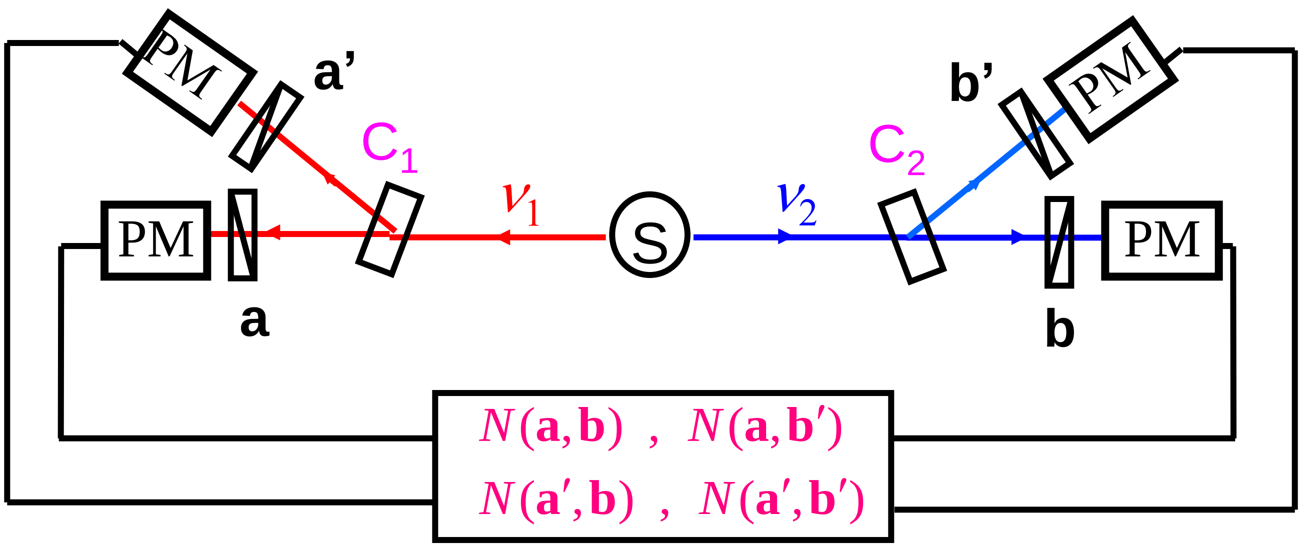
**a** and **a'**

Idem $C_2$ for **b** and **b'**

Between two switching: $10 \text{ ns} < L/c \approx 40 \text{ ns}$

# Experiment with variable polarizers: results AA, J. Dalibard, G. Roger, PRL 1982

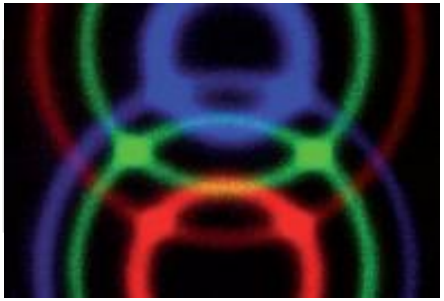
Acousto optical switch: change every 10 ns. Faster than propagation of light between polarizers (40 ns) and even than time of flight of photons between the source S and each switch (20 ns).




Difficult experiment: reduced signal; data taking for several hours; switching not fully random

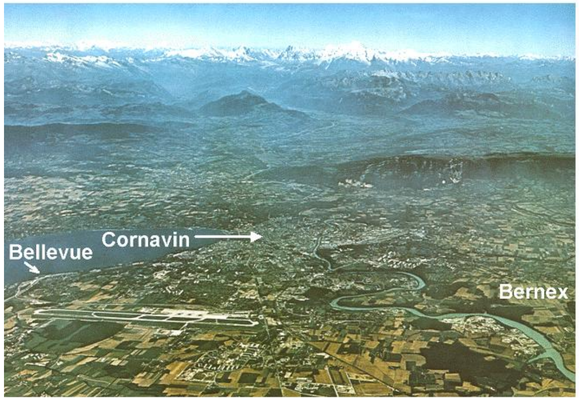
Convincing result: Bell's inequalities violated by par 6 standard deviations. Each measurement space-like separated from setting of distant polarizer: Einstein's causality enforced

# Third generation experiments



Entangled photon pairs by parametric down conversion, well defined directions: injected into optical fibers.

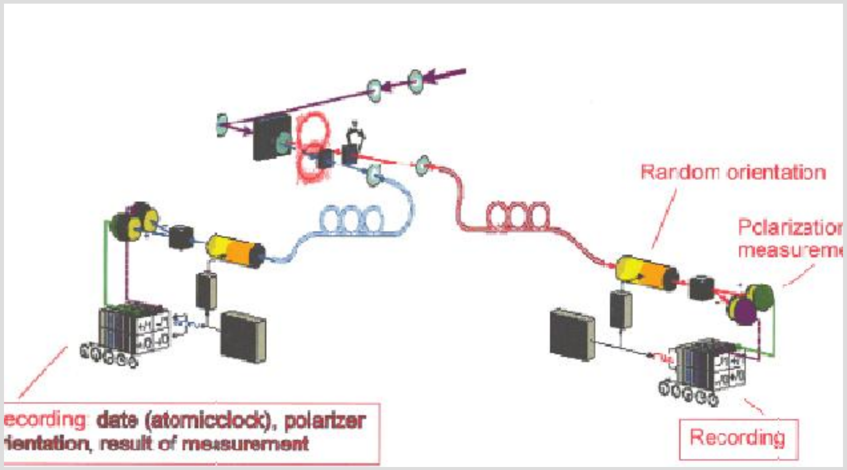
Entanglement at a very large distance




Geneva experiment (1998):

- Optical fibers of the commercial telecom network
- Measurements separated by 30 km

Agreement with QM.




Innsbruck experiment (1998):

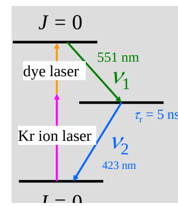
variable polarizers with orientation chosen by a random generator during the propagation of photons (several hundreds meters).

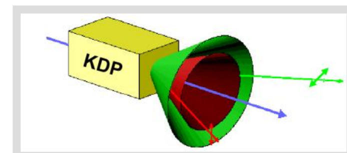
Agreement with QM.

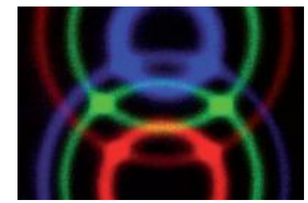
# Bell's inequalities have been violated in almost ideal experiments

Results in agreement with quantum mechanics in experiments closer and closer to the GedankenExperiment:

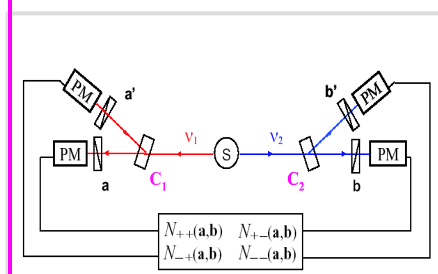
- Sources of entangled photons more and more efficient

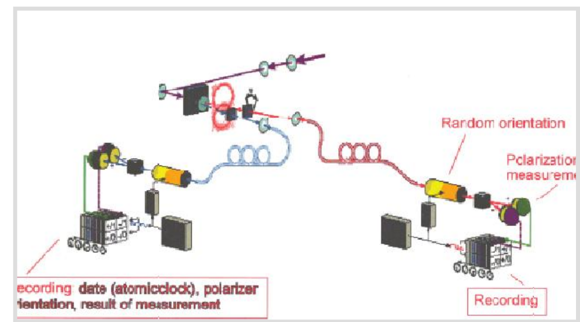


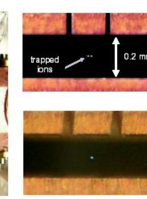



- Relativistic separation of measurements with variable polarizers (Orsay 1982, Innsbruck 1998); closure of locality loophole




- Experiment with trapped ions (Boulder 2000): closure of the "sensitivity loophole" (recent experiments with photons in Vienna, Urbana Champaign).




**Einstein's local realism is untenable**

# The failure of local realism

Einstein had considered (in order to reject it by *reductio ad absurdum*) the consequences of the failure of the EPR reasoning: [If quantum mechanics could not be completed, one would have to]

- either drop the need of the independence of the physical realities present in different parts of space
- or accept that the measurement of $S_1$ changes (instantaneously) the real situation of $S_2$

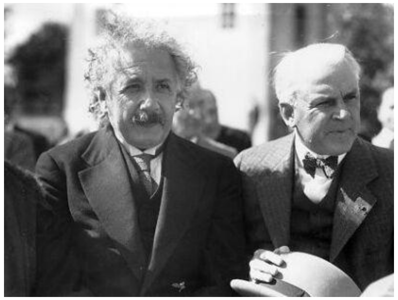
## Quantum non locality – Quantum holism

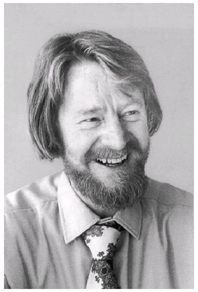
The properties of a pair of entangled particles are more than the addition of the individual properties of the constituents of the pairs (even space like separated). Entanglement = global property.

NB: no faster than light transmission of a “utilizable” signal (ask!)

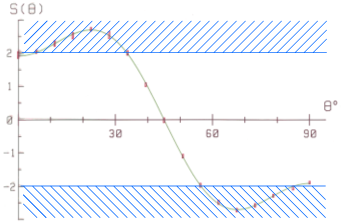
# From Einstein's doubts to quantum information

1. From Einstein-Podolsky -Rosen to Bell

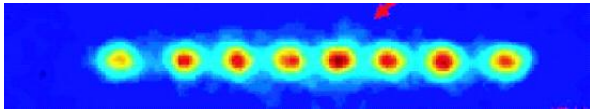




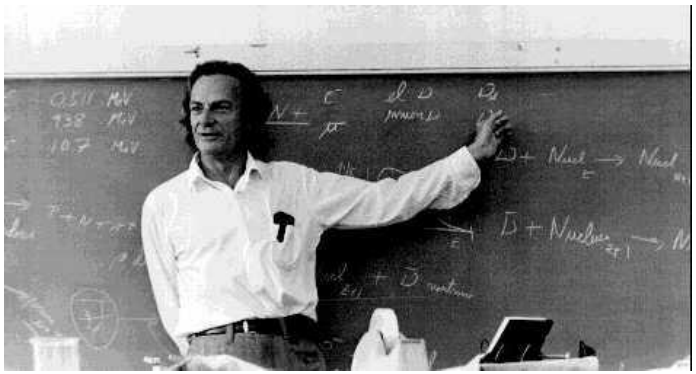
2. Experimental tests of Bell's inequalities with correlated photons

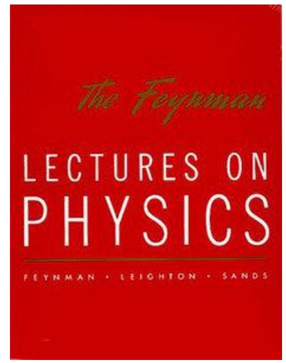


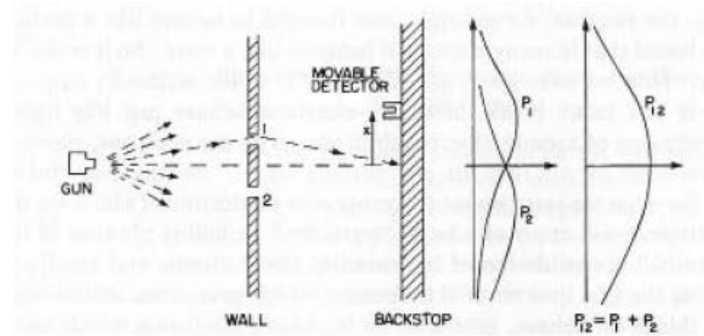

3. A new quantum age: entanglement is more



# It took a long time for entanglement to be recognized as a revolutionary concept






## Wave particle duality for a single particle: the only mystery (1960)

*In this chapter we shall tackle immediately the basic element of the mysterious behavior in its most strange form. We choose to examine a phenomenon which is impossible, absolutely impossible, to explain in any classical way, and which has in it the heart of quantum mechanics. In reality it contains the only mystery.*

*This point was never accepted by Einstein… It became known as the Einstein-Podolsky-Rosen paradox. But when the situation is described as we have done it here, there doesn't seem to be any paradox at all…*

# It took a long time for entanglement to be recognized as a revolutionary concept

> **Simulating Physics with Computers**
>
> **Richard P. Feynman** 1982

*we always have had (secret, secret, close the doors!) we always have had a great deal of difficulty in understanding the world view that quantum mechanics represents. At least I do*

*I've entertained myself always by squeezing the difficulty of quantum mechanics into a smaller and smaller place, so as to get more and more worried about this particular item.*

*It seems to be almost ridiculous that you can squeeze it to a numerical question that one thing is bigger than another. But there you are-it is bigger than any logical argument can produce*

a second mystery, and then…

# Entanglement: a resource for quantum information

The understanding of the extraordinary properties of entanglement has triggered a new research field: quantum information

Hardware based on different physical principles allows emergence of new concepts in information processing and transport:

- Quantum computing (R. Feynman 1982, D. Deutsch 1985 )
- Quantum cryptography (Bennett Brassard 84, Ekert 1991)
- Quantum teleportation (BB&al., 1993; Innsbruck, Roma 1997)
- Quantum simulation (Feynman 1982, Hänsch and col. 2002)

**Entanglement is at the root of most of the schemes for quantum information**

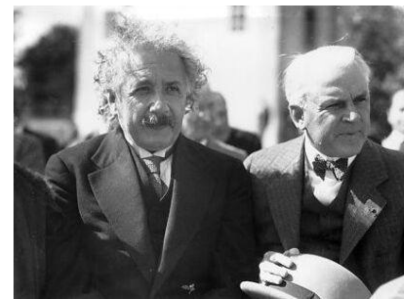
# Entanglement: a resource for quantum information

The understanding of the extraordinary properties of entanglement and its generalization to more than two particles (GHZ) has triggered a new research field: quantum information

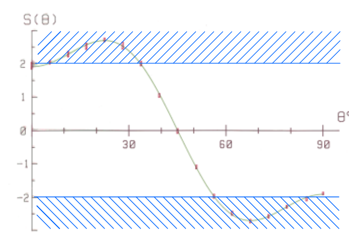
Hardware based on different physical principles allows emergence of new concepts in information science, realized experimentally with ions, photons, atoms, Josephson junctions, RF circuits:

- Quantum computing (R. Feynman 1982, D. Deutsch 1985;… Boulder, Innsbruck, Paris, Roma, Palaiseau, Munich, Saclay, Yale, Santa Barbara, Zurich, … )
- Quantum cryptography (Bennett Brassard 84, Ekert 1991;… Geneva, Singapore, Palaiseau, …)
- Quantum teleportation (BB&al., 1993; Roma, Innsbruck 1997)
- Quantum simulation (Feynman, Cirac and Zoller;… Munich, Innsbruck, Zurich, Palaiseau, Paris, Roma … )

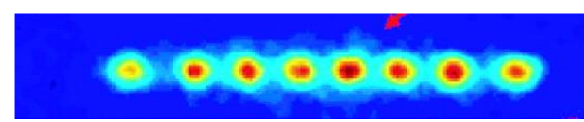
# From Einstein's doubts to quantum information



1. From Einstein-Podolsky -Rosen to Bell




2. Experimental tests
3. A new quantum age:
   Quantum information
   Quantum cryptography



# Mathematically proven safe cryptography: sharing two identical copies of a secret key

The goal: distribute to two partners (Alice et Bob) two identical secret keys (a random sequence of 1 and 0), with absolute certainty that no spy (Eve) has been able to get a copy of the key.

Using that key, Alice and Bob can exchange (publicly) a coded message with a mathematically proven safety (Shannon theorem) (provided the message is not longer than the key)

Eve

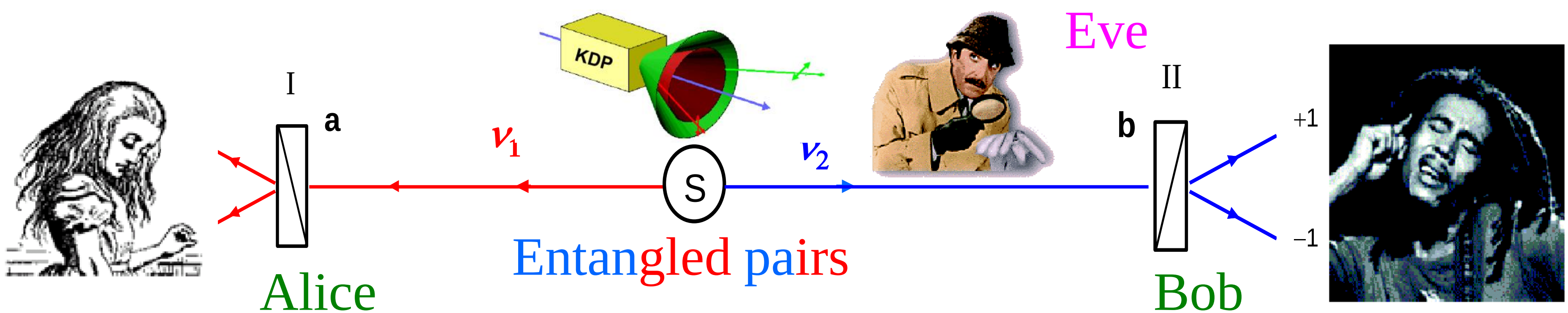
110100101 110100101

Alice Bob

**Quantum optics provides means of safe key distribution**

# Quantum Key Distribution with entangled photons (Ekert)

Alice and Bob select their analysis directions **a** et **b** randomly among 2, make measurements, then send publicly the list of all selected directions



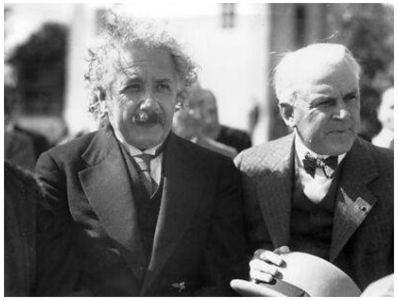

**Cases of a** et **b** identical : identical results ⇒ 2 identical keys

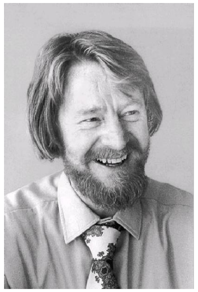
There is nothing to spy on the entangled flying photons: the key is created at the moment of the measurement.

If Eve chooses a particular direction of analysis, makes a measurement, and reemits a photon according to her result, his maneuver leaves a trace that can be detected by doing a Bell’s inequalities test.

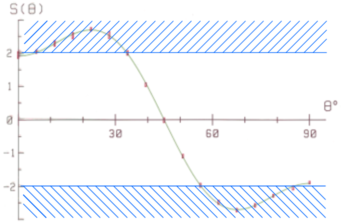
QKD at large distance, from space, on the agenda

# From Einstein's doubts to quantum information

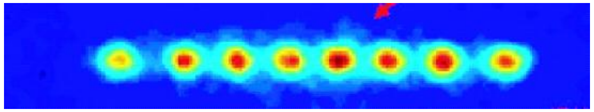




1. From Einstein-Podolsky -Rosen to Bell




2. Experimental tests
3. A new quantum age:
   Quantum information
   Quantum computing



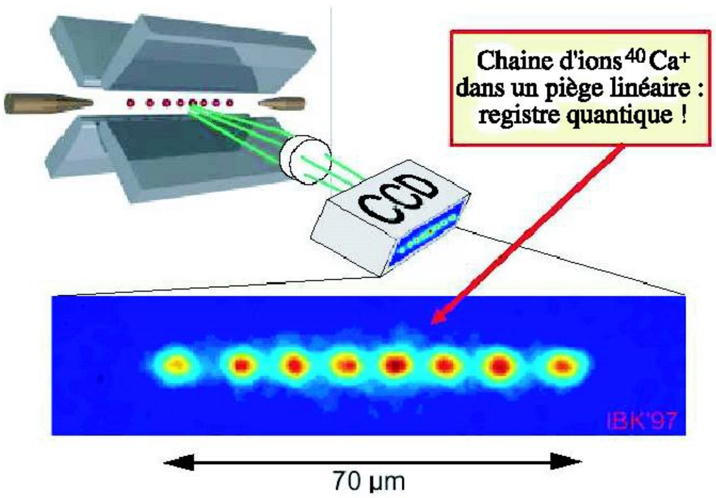
# Quantum computing

A quantum computer could operate new types of algorithms able to make calculations exponentially faster than classical computers. Example: Shor's algorithm for factorization of numbers: the RSA encryption method would no longer be safe.

Fundamentally different hardware: fundamentally different software.

What would be a quantum computer?

An ensemble of interconnected quantum gates, processing strings of entangled quantum bits (qubit: 2 level system)



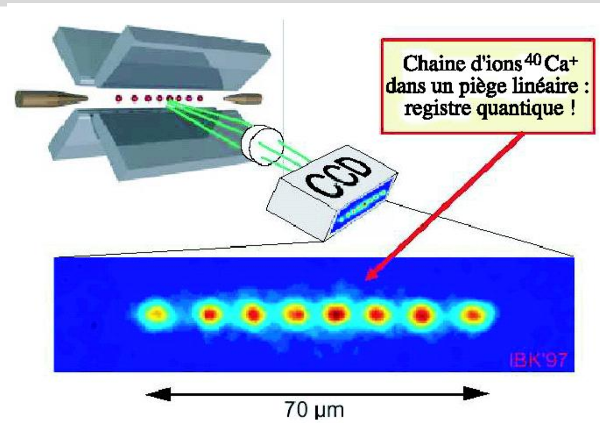

Entanglement ⇒ massive parallelism

The Hilbert space to describe N entangled qubits has dimension $2^N$ !
(most of that space consists of entangled states)

# Quantum computing???

A quantum computer could operate new types of algorithms able to make calculations exponentially faster than classical computers.
Example: Shor's algorithm for factorization of numbers: the RSA encryption method would no longer be safe.

What would be a quantum computer?
An ensemble of entangled quantum bits
(qubit: 2 level system)
Entanglement ⇒ massive information $2^N$

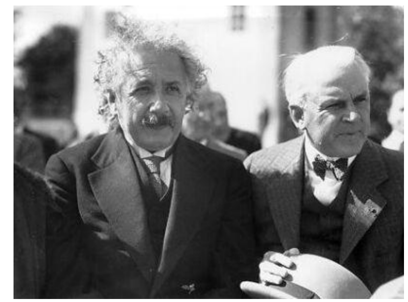



A dramatic problem: decoherence: hard to increase the number of entangled qubits
Nobody knows if such a quantum computer will ever work:

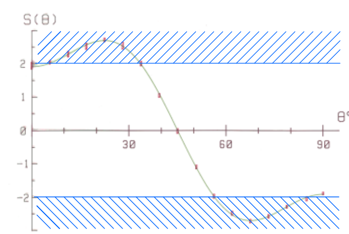
- Needed: $10^5$ = 100 000 entangled qubits
- Record: 14 entangled qubits (R. Blatt)

Would be a kind of Schrödinger cat

# From Einstein's doubts to quantum information

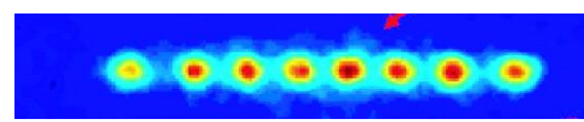


1. From Einstein-Podolsky -Rosen to Bell



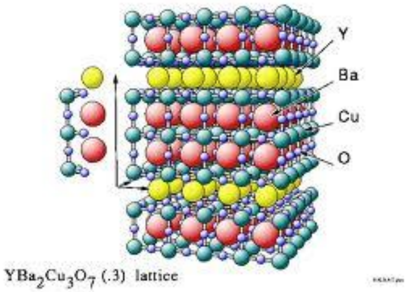

2. Experimental tests

3. A new quantum age:
   Quantum information
   Quantum simulation



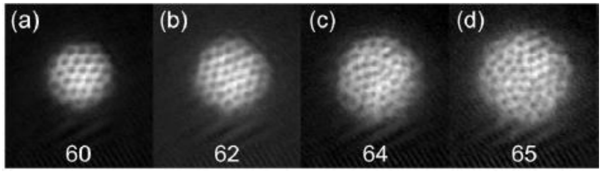
# Quantum simulation

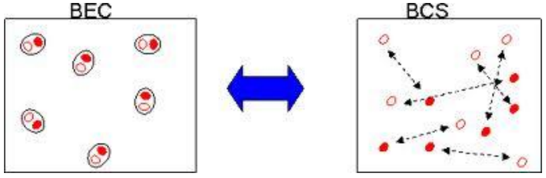
Goal: understand a system of many entangled particles, absolutely impossible to describe, least to study, on a classical computer (Feynman 1982)
Example: electrons in solids (certain materials still not understood, e.g. high $T_C$ supraconductors)



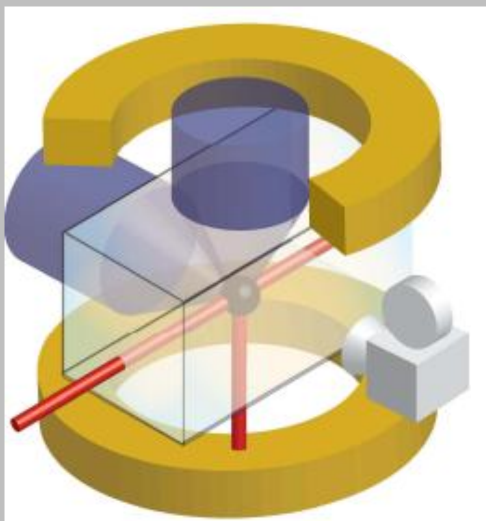

Quantum simulation: mimick the system to study with other quantum particles "easy" to manipulate, observe, with parameters "easy" to modify
Example: ultracold atoms in synthetic potentials created with laser beams

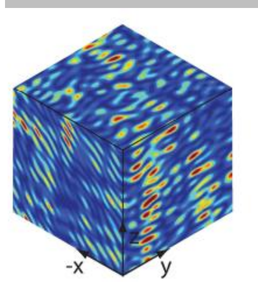
- Can change density, potential parameters
- Many observation tools: position or velocity distributions, correlations…

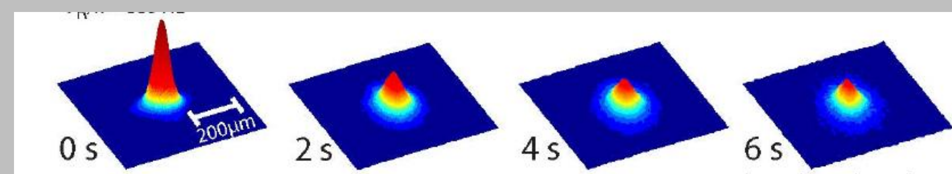


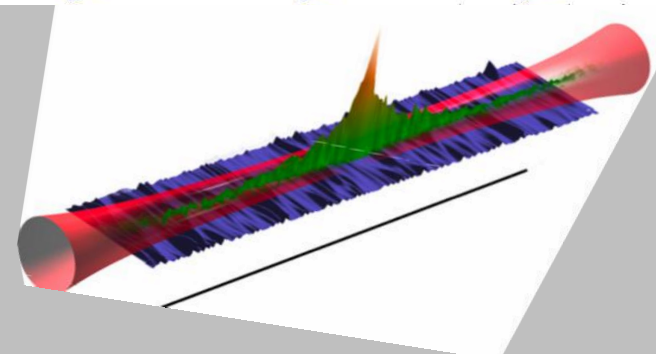



# Quantum simulator of the Anderson transition in a disordered potential





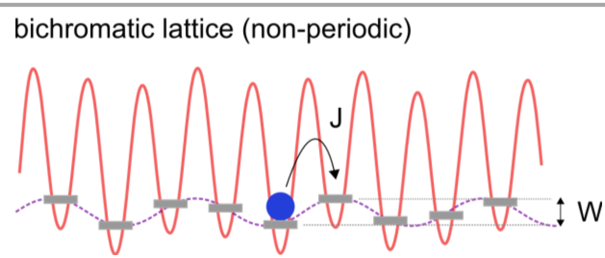



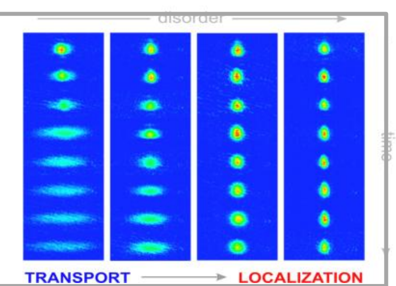



Atoms suspended, released in the disordered potential created with lasers. Absorption images

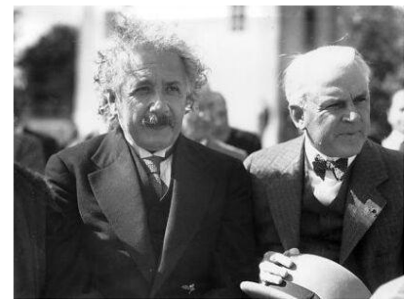
Direct observation of a localized component, with an exponential profile (localized wave function)

Similar experiments in Florence (Inguscio's group)

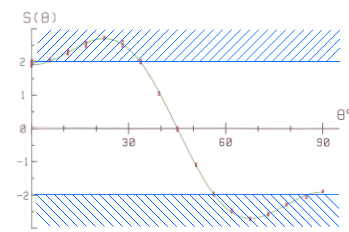


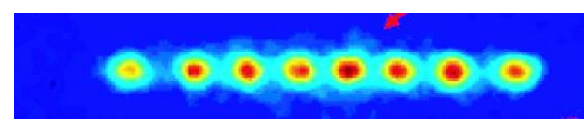
# From Einstein's doubts to quantum information



1. From Einstein-Podolsky -Rosen to Bell




2. Experimental tests of Bell's inequalities with correlated photons



3. A new quantum age: entanglement is more

# A new quantum revolution?

## Two concepts at the root of a new quantum era

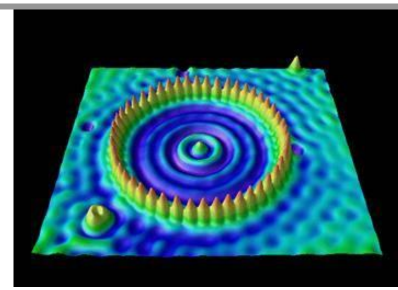
### Entanglement

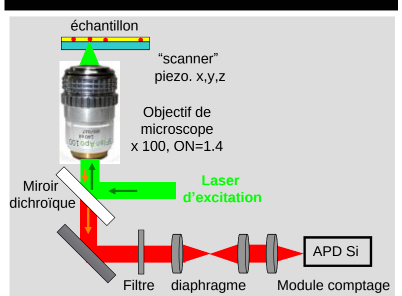
- A revolutionary concept, as guessed by Einstein and Bohr, strikingly demonstrated by Bell, put to use by Feynman et al.
- Drastically different from concepts underlying the first quantum revolution (wave particle duality).

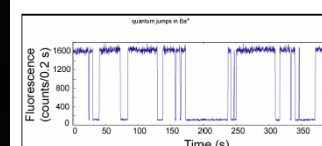
### Individual quantum objects

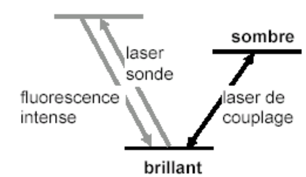
- experimental control
- theoretical description (quantum Monte-Carlo)

Examples: electrons, atoms, ions, single photons, photons pairs





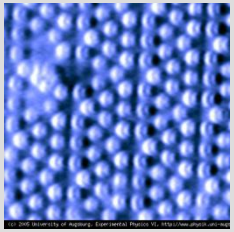



# What was the first quantum revolution?

A revolutionary concept: Wave particle duality

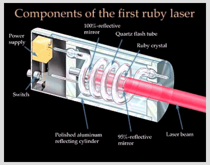
- Understanding the structure of matter, its properties, its interaction with light
  - Electrical, mechanical properties

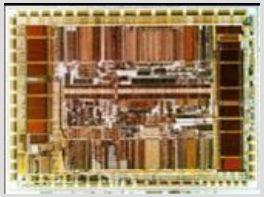


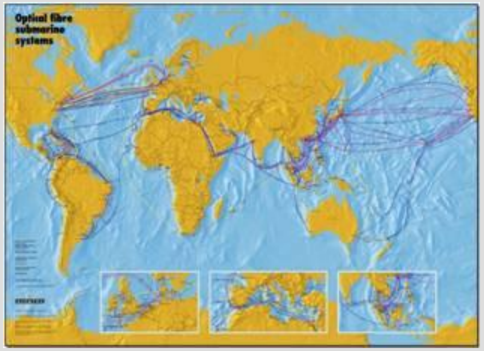
- Understanding "exotic properties"
  - Superfluidity, supraconductivity, Bose Einstein Condensate

Revolutionary applications

- Inventing new devices
  - Laser, transistor, integrated circuits





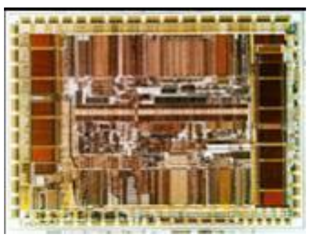

- Information and communication society

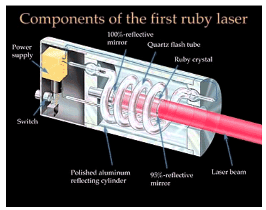
As revolutionary as the invention of heat engine (change society)

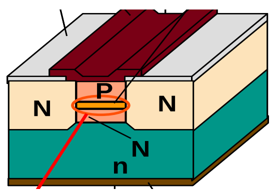
Not only conceptual, also technological

# Towards a new technological revolution?

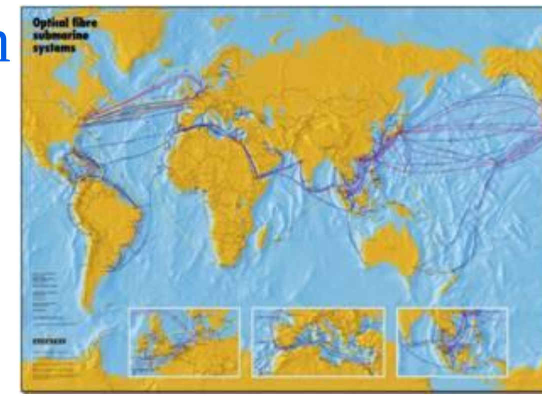
Will the new conceptual revolution (entanglement + individual quantum systems) give birth to a new technological revolution?






First quantum revolution (wave particle duality): lasers, transistors, integrated circuits ⇒ "information society"



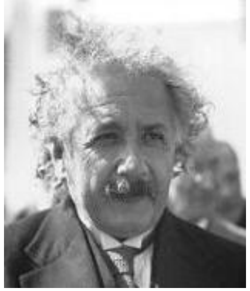

Will quantum computing and quantum communication systems lead to the "quantum information society"?

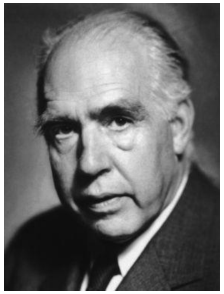
The most likely roadmap (as usual): from proofs of principle with well defined elementary microscopic objects (photons, atoms, ions, molecules…) to solid state devices (and continuous variables?) …

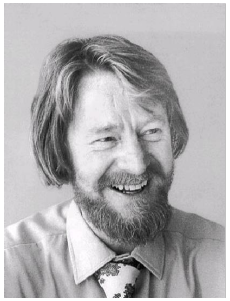
A fascinating issue… we live exciting times!

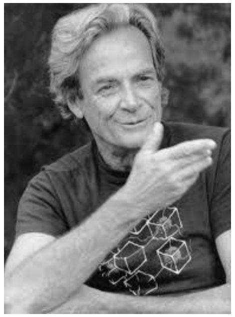
# Visionary fathers of the second quantum revolution

- Einstein discovered a new quantum feature, entanglement, different in nature from wave-particle duality for a single particle
- Schrödinger realized that entanglement is definitely different
- Bohr had the intuition that interpreting entanglement according to Einstein's views was incompatible with Quantum Mechanics
- Bell found a proof of Bohr's intuition
- Feynman realized that entanglement could be used for a new way to process information









We stand on the shoulders of giants!

# Standing on shoulders of giants

The best-known use of this phrase was by Isaac Newton in a letter to his rival Robert Hooke, in 1676:

> "What Descartes did was a good step. You have added much several ways, and especially in taking the colours of thin plates into philosophical consideration. If I have seen a little further it is by standing on the shoulders of Giants."

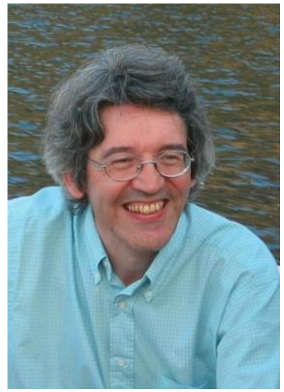
Newton didn't originate it though. The 12th century theologian and author John of Salisbury used a version of the phrase in a treatise on logic called *Metalogicon*, written in Latin in 1159. Translations of this difficult book are quite variable but the gist of what Salisbury said is:

> "We are like dwarfs sitting on the shoulders of giants. We see more, and things that are more distant, than they did, not because our sight is superior or because we are taller than they, but because they raise us up, and by their great stature add to ours."

# We need the contribution of many people

Thanks to the 1982 team

Jean Dalibard



Philippe Grangier

Gérard Roger

André Villing

and to the atom optics group, who makes quantum simulation an experimental reality

# Bell's inequalities at the lab classes of the Institut d'Optique Graduate School

L'Institut d'Optique

Rech

Actualités • Accueil • Médiathèque • Annuaire • Liens • Contac

Qui sommes nous ? | Formation | Apprentissage | Laboratoire | IOTech | Inc

**Formation> Moyens pédagogiques (TP,...)**

**Moyens pédagogiques (TP, ...)**

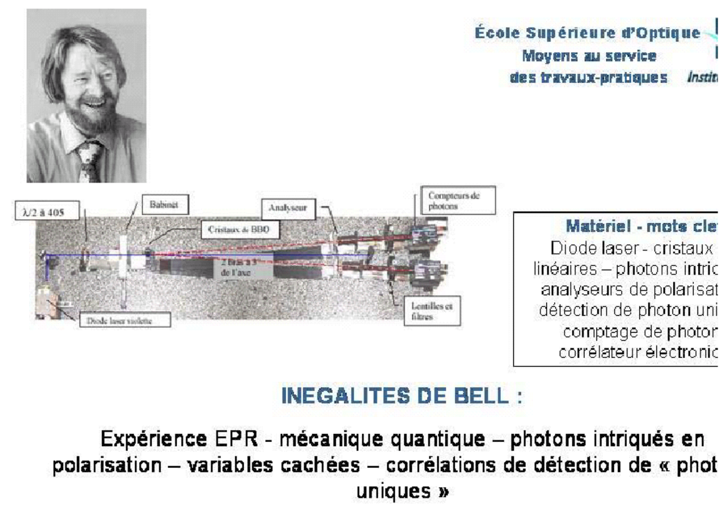
Les **moyens pédagogiques** sont ceux de l'École Supérieure d'Optique et so
- des **ressources propres** du service des TP
- des **ressources du laboratoire** Charles Fabry de l'Institut d'Optique
- des **ressources des industriels partenaires** (à travers l'ASERFO, l'assoc de soutien à l'enseignement et la formation en optique, ou au travers de dc nature ") et collectivités territoriales (région, département) qui soutienne d'ingénieurs.

Les TP se renouvellent ainsi régulièrement, également grâce à **l'apport par eux-mêmes** lors des projets systèmes de 2ème année et projets de 3ème a

Ce qui suit est un *échantillon* des nombreux TP d'optique et d'électronique s d'enseignement . Vous pouvez pour chaque TP:
- cliquer sur l'imagette pour avoir un agrandi et quelques informations succir
- cliquer sur "télécharger le dossier" , constitué de documents pédagogique les enseignants ou les étudiants : textes, affiches, diaporamas, films, etc.

Contact : Lionel JACUBOWIEZ, responsable du service des TP.

*Gyromètre à fibre* présentation (1,3Mo)
*Caméra bolométrique* poster (1,7Mo)
*Analyse de fronts d'onde aberrants avec un HASO* présentation (1,3Mo)
*Op*
*TP de microprocesseur* article (380Ko)
*Transmission numérique sur fibre optique en VHDL* article (1,5Mo)
*Étude de vibromètres laser* présentation .pdf (2,5Mo)
*Bruits*
*Microscopie*
*Inégalités de Bell*
*Effet raman dans une fibre*
*Transm*

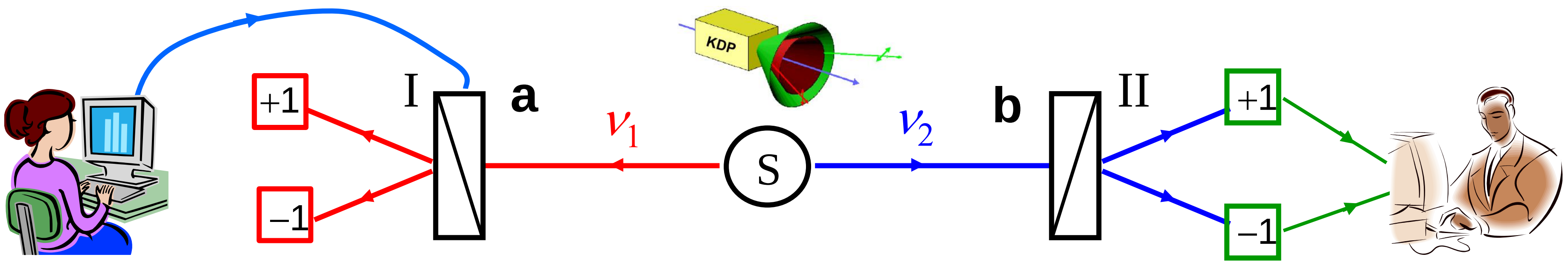



http://www.institutoptique.fr/telechargement/inegalites_Bell.pdf

# Appendix

## No faster than light signaling with EPR pairs

# No faster than light signaling with EPR entangled pairs




Alice changes the setting of polarizer I from **a** to **a'**: can Bob instantaneously observe a change on its measurements at II ?

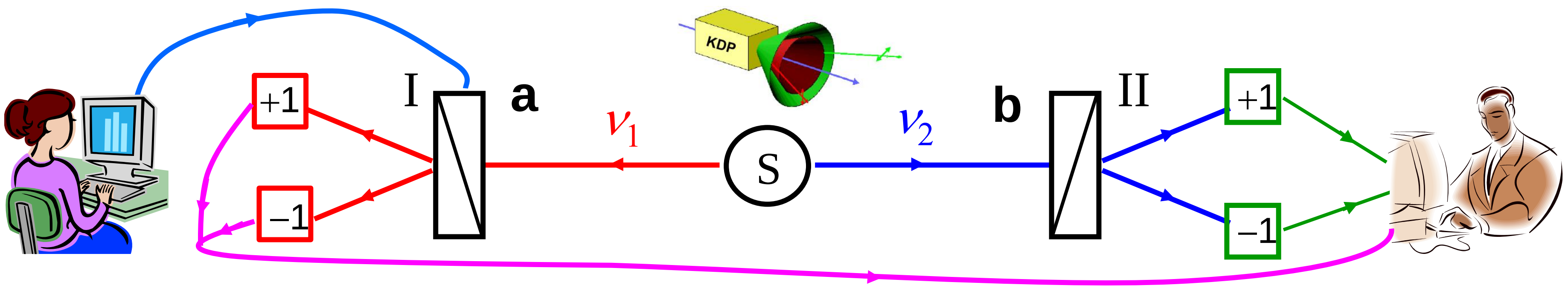
Single detections: $P_+(\mathbf{b}) = P_-(\mathbf{b}) = 1/2$ No information about **a**

Joint detections: $P_{++}(\mathbf{a},\mathbf{b}) = P_{--}(\mathbf{a},\mathbf{b}) = \frac{1}{2}\cos^2(\mathbf{a},\mathbf{b})$ etc.

Instantaneous change !

Faster than light signaling ?

# No faster than light signaling with EPR entangled pairs




Alice changes the setting of polarizer I from **a** to **a'**: can Bob instantaneously observe a change on its measurements at II ?

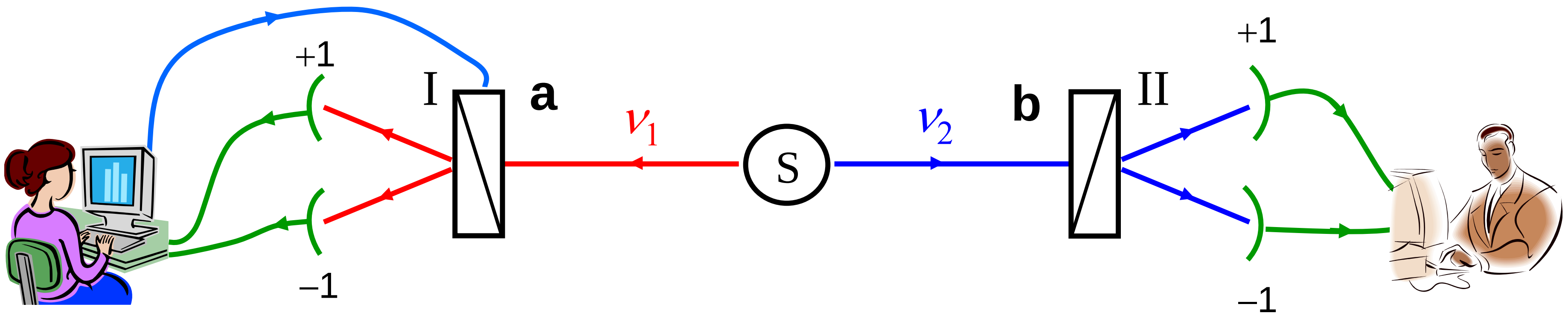
Joint detections: $P_{++}(\mathbf{a},\mathbf{b}) = P_{--}(\mathbf{a},\mathbf{b}) = \frac{1}{2}\cos^2(\mathbf{a},\mathbf{b})$ etc.

Instantaneous change ! Faster than light signaling ?

To measure $P_{++}(\mathbf{a},\mathbf{b})$ Bob must compare his results to the results at I: the transmission of these results from I to Bob is done on a classical channel, not faster than light.

*cf.* role of classical channel in quantum teleportation.

# So there is no problem ?




View *a posteriori* onto the experiment:

During the runs, Alice and Bob carefully record the time and result of each measurement.

After completion of the experiment, they meet and compare their data…

… and they find that $P_{++}(\mathbf{a},\mathbf{b})$ had changed instantaneously when Arthur had changed his polarizers orientation…

Non locality still there, but cannot be used for « practical telegraphy »

# Is it a real problem ?

« It has not yet become obvious to me that there is no real problem. I cannot define the real problem, therefore I suspect there's no real problem, but I am not sure there is no real problem. So that's why I like to investigate things. »*

R. Feynman: *Simulating Physics with Computers*, Int. Journ. of Theoret. Phys. 21, 467 (1982)**

* This sentence was written about EPR correlations

** A founding paper on quantum computers

# It took a long time for entanglement to be recognized as a revolutionary concept

In this chapter we shall tackle immediately the basic element of the mysterious behavior in its most strange form. We choose to examine a phenomenon which is impossible, *absolutely* impossible, to explain in any classical way, and which has in it the heart of quantum mechanics. In reality, it contains the *only* mystery.

*"This point was never accepted by Einstein... it became known as the "Einstein-Podolsky-Rosen paradox". But when the situation is described as we have done it here, there doesn't seem to be any parado[x at all."]*

R.P. Feynmann (1960) Lectures on Physics

*"We always have had a great deal of difficulty in understanding the world view that quantum mechanics represents... It has not yet become obvious to me that there is no real problem...*

*I've entertained myself always by squeezing the difficulty of quantum mechanics into a smaller and smaller place, so as to get more and more worried about this particular item. It seems to be almost ridiculous that you can squeeze it to a numerical question that one thing is bigger than another. But there you are - it is bigger..."* R.P. F (1982) Simulating Physics with computers

# Mathematically proven safe cryptography: sharing two identical copies of a secret key

The goal: distribute to two partners (Alice et Bob) two identical secret keys (a random sequence of 1 and 0), with absolute certainty that no spy (Eve) has been able to get a copy of the key.

Using that key, Alice and Bob can exchange (publicly) a coded message with a mathematically proven safety (Shannon theorem) (provided the message is not longer than the key)

Eve

110100101 110100101

Alice Bob

Quantum optics provides means of safe key distribution (QKD)