About entanglement, ciphers, quanta and computers

Artur Ekert

Back in the early XX century…

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)

In a complete theory there is an element corresponding to each element of reality. A sufficient condition for the reality of a physical quantity is the possibility of predicting it with certainty, without disturbing the system. In quantum mechanics in the case of two physical quantities described by non-commuting operators, the knowledge of one precludes the knowledge of the other. Then either (1) the description of reality given by the wave function in quantum mechanics is not complete or (2) these two quantities cannot have simultaneous reality. Consideration of the problem of making predictions concerning a system on the basis of measurements made on another system that had previously interacted with it leads to the result that if (1) is false then (2) is also false. One is thus led to conclude that the description of reality as given by a wave function is not complete.

1.

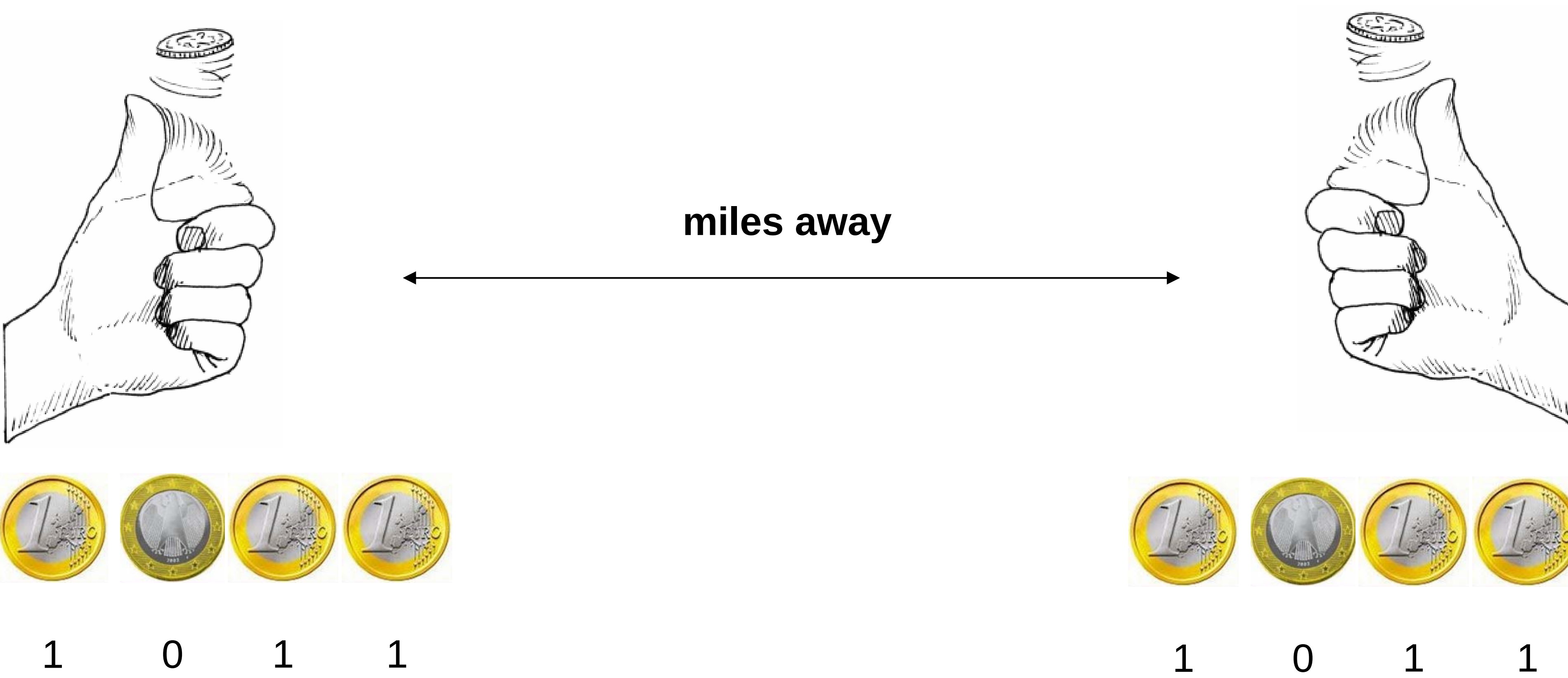
ANY serious consideration of a physical theory must take into account the distinction between the objective reality, which is independent of any theory, and the physical concepts with which the theory operates. These concepts are intended to correspond with the objective reality, and by means of these concepts we picture this reality to ourselves.

In attempting to judge the success of a physical theory, we may ask ourselves two questions: (1) "Is the theory correct?" and (2) "Is the description given by the theory complete?" It is only in the case in which positive answers may be given to both of these questions, that the concepts of the theory may be said to be satisfactory. The correctness of the theory is judged by the degree of agreement between the conclusions of the theory and human experience. This experience, which alone enables us to make inferences about reality, in physics takes the form of experiment and measurement. It is the second question that we wish to consider here, as applied to quantum mechanics.

Whatever the meaning assigned to the term *complete*, the following requirement for a complete theory seems to be a necessary one: *every element of the physical reality must have a counterpart in the physical theory*. We shall call this the condition of completeness. The second question is thus easily answered, as soon as we are able to decide what are the elements of the physical reality.

The elements of the physical reality cannot be determined by *a priori* philosophical considerations, but must be found by an appeal to results of experiments and measurements. A comprehensive definition of reality is, however, unnecessary for our purpose. We shall be satisfied with the following criterion, which we regard as reasonable. *If, without in any way disturbing a system, we can predict with certainty (i.e., with probability equal to unity) the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity.* It seems to us that this criterion, while far from exhausting all possible ways of recognizing a physical reality, at least provides us with one

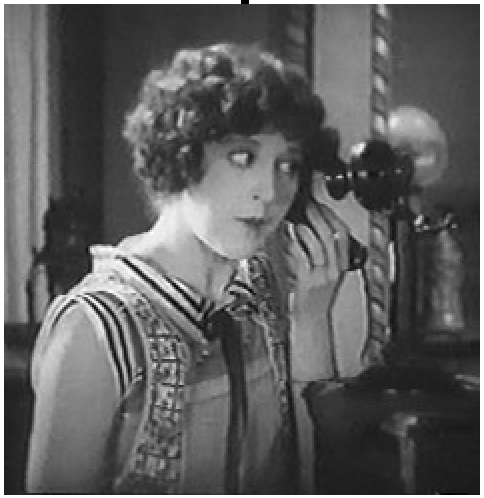
Spooky Action at a Distance



Scenario

Alice

Bob



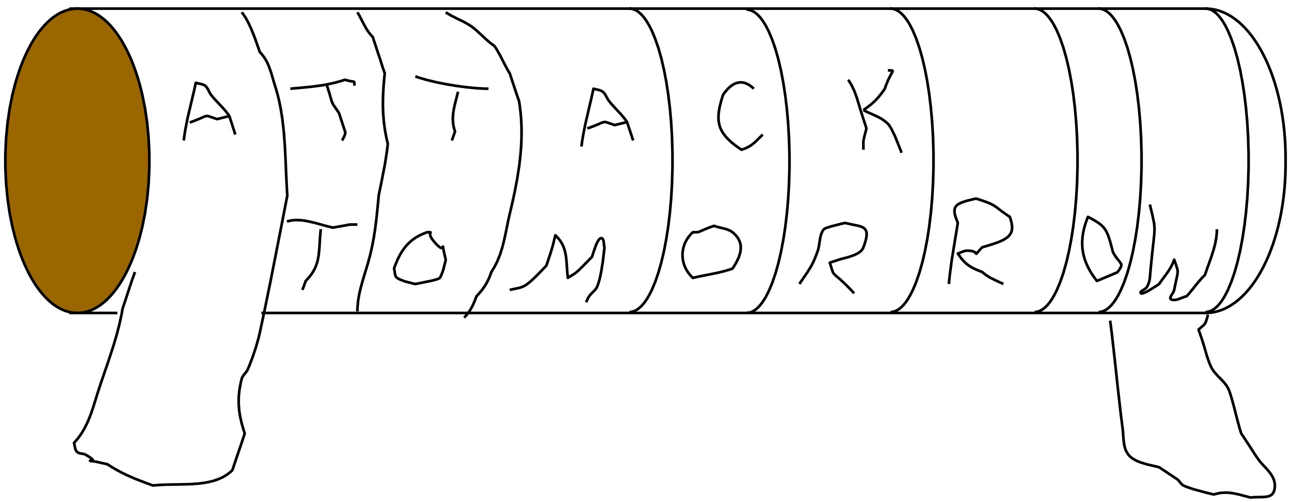
Eavesdropper

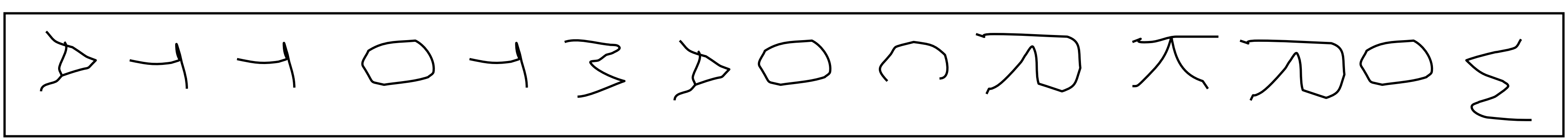
Typical techniques

- **PERMUTATIONS**
  - e.g. Scytale (400 BC)
- **SUBSTITUTIONS**
  - e.g. Caesar cipher (50 BC)
- **PERMUTATIONS + SUBSTITUTIONS**

Scytale

400 BC
SPARTA





Permutation of characters

Caesar ciphers

50 BC
ROME

ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ

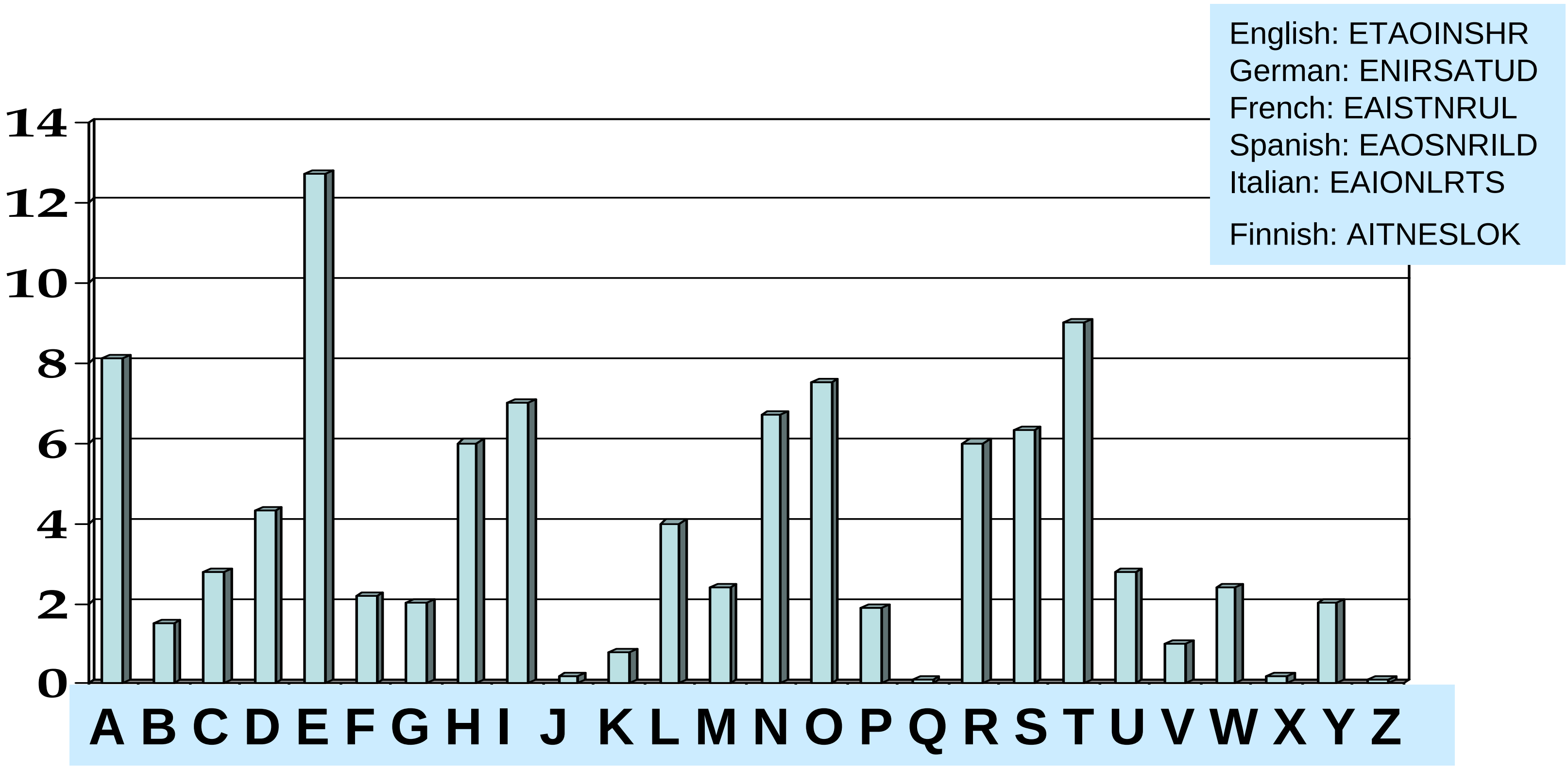
ABCDEFGHIJKLMNOPQRSTUVWXYZ
DEFGHIJKLMNOPQRSTUVWXYZABC

A T T A C K T O M O R R O W
DWWD F N WR P R U U R Z

Early cryptanalysis

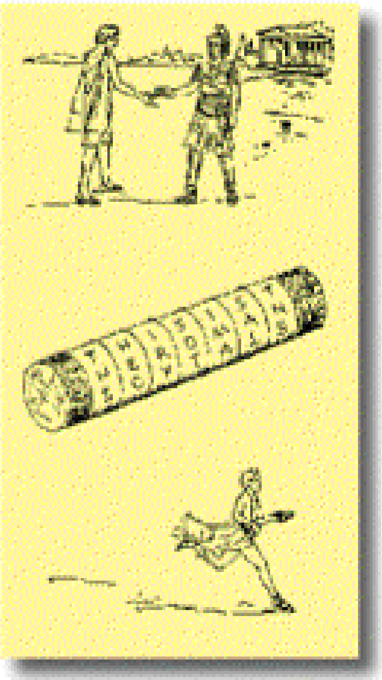
Baghdad, al-Kindi (800-873)

Frequency analysis

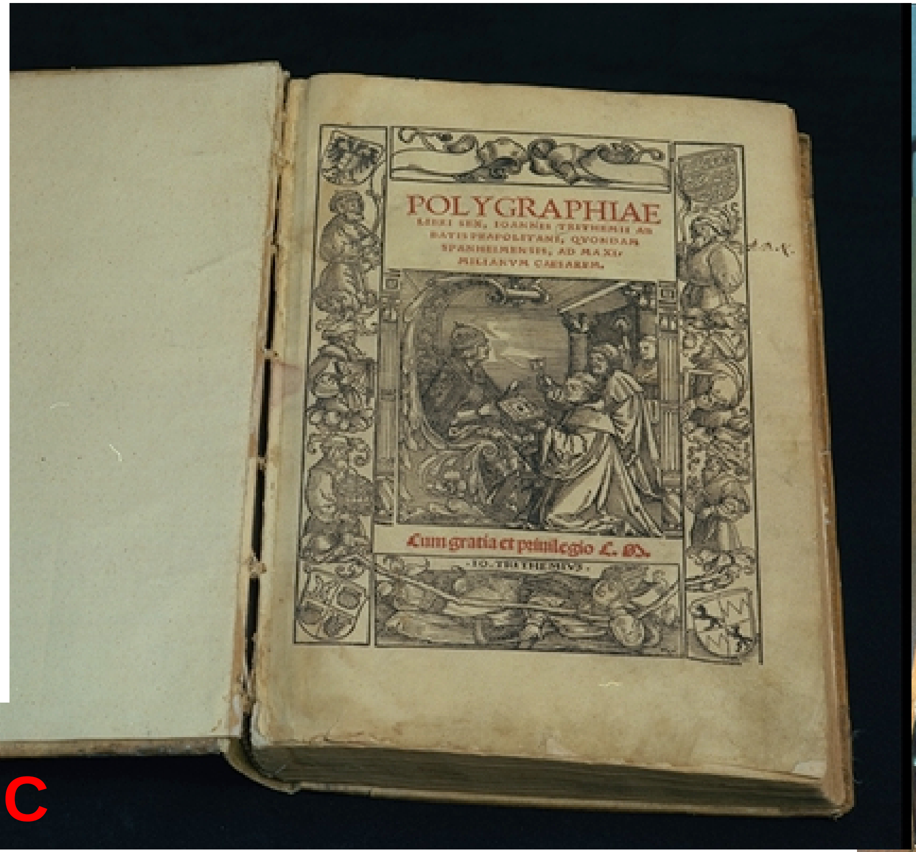


Frequency of letters in a typical English text

Is there a perfect cipher?



SCYTALE 400BC



POLYGRAPHIAE
1518

ENIGMA 1940

One-time pad

01011100	plaintext
11001010	KEY
10010110	cryptogram

1	0	0	1	0	1	1	0

cryptogram	10010110
KEY	11001010
plaintext	01011100

Key distribution problem

?

miles away

KEY	0	0	1	0	1	1	0

KEY	0	0	1	0	1	1	0

Quantum key distribution

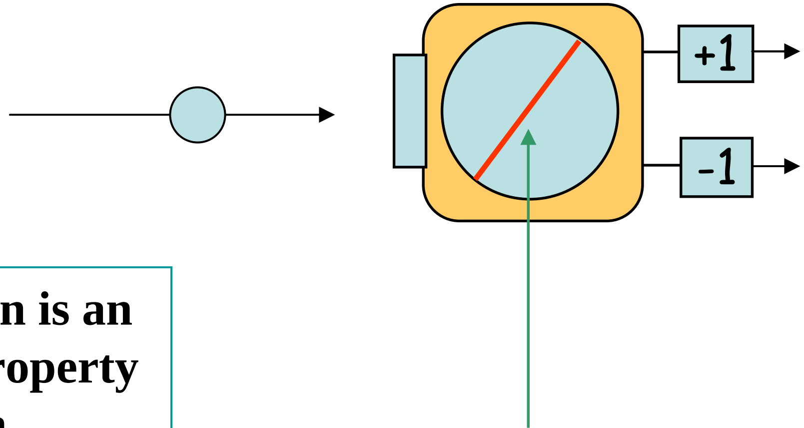
miles away

KEY	0	0	1	0	1	1	0

KEY	0	0	1	0	1	1	0

Spooky Action at a Distance

Polarization



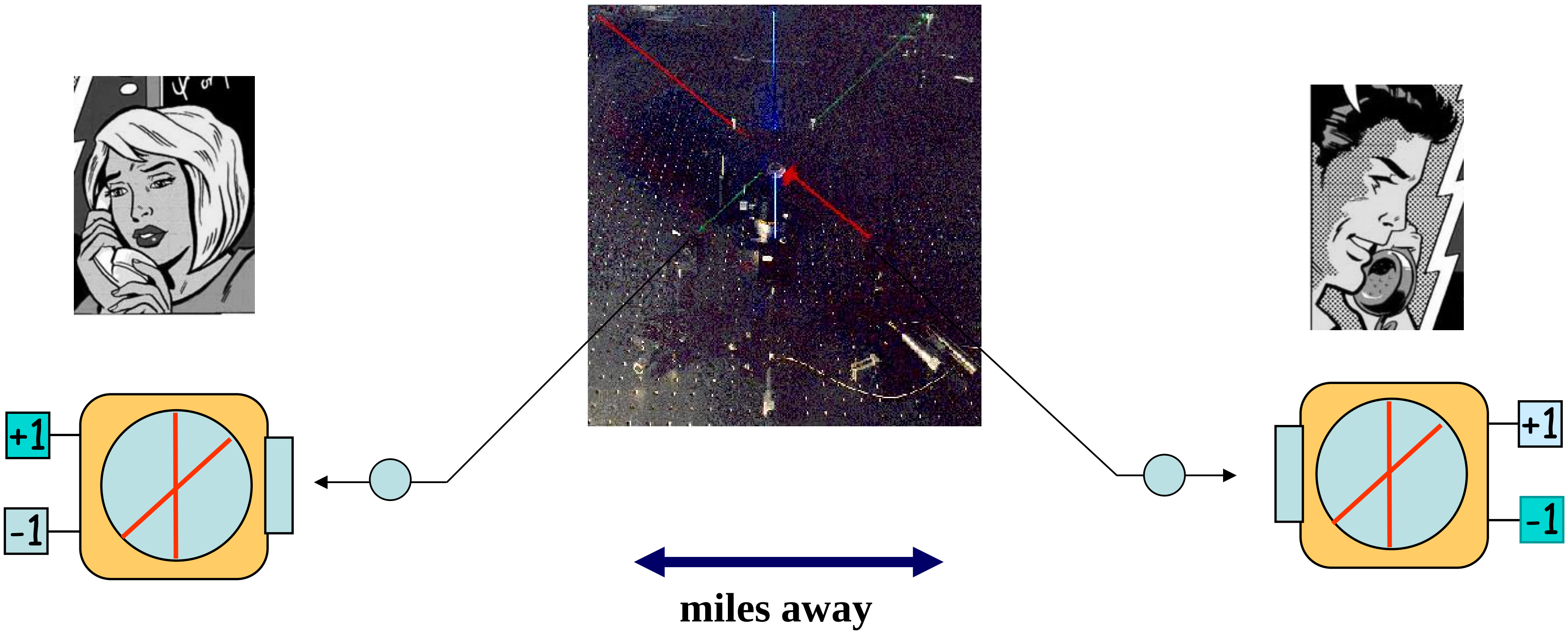
In any measurement we can get only two results: +1 or -1

(in units of $\hbar = 1.05 \times 10^{34}\,\mathrm{Js}$ **)**

Polarization is an intrinsic property of a photon

We cannot just "measure polarization". We can only measure polarization with respect to some specified direction

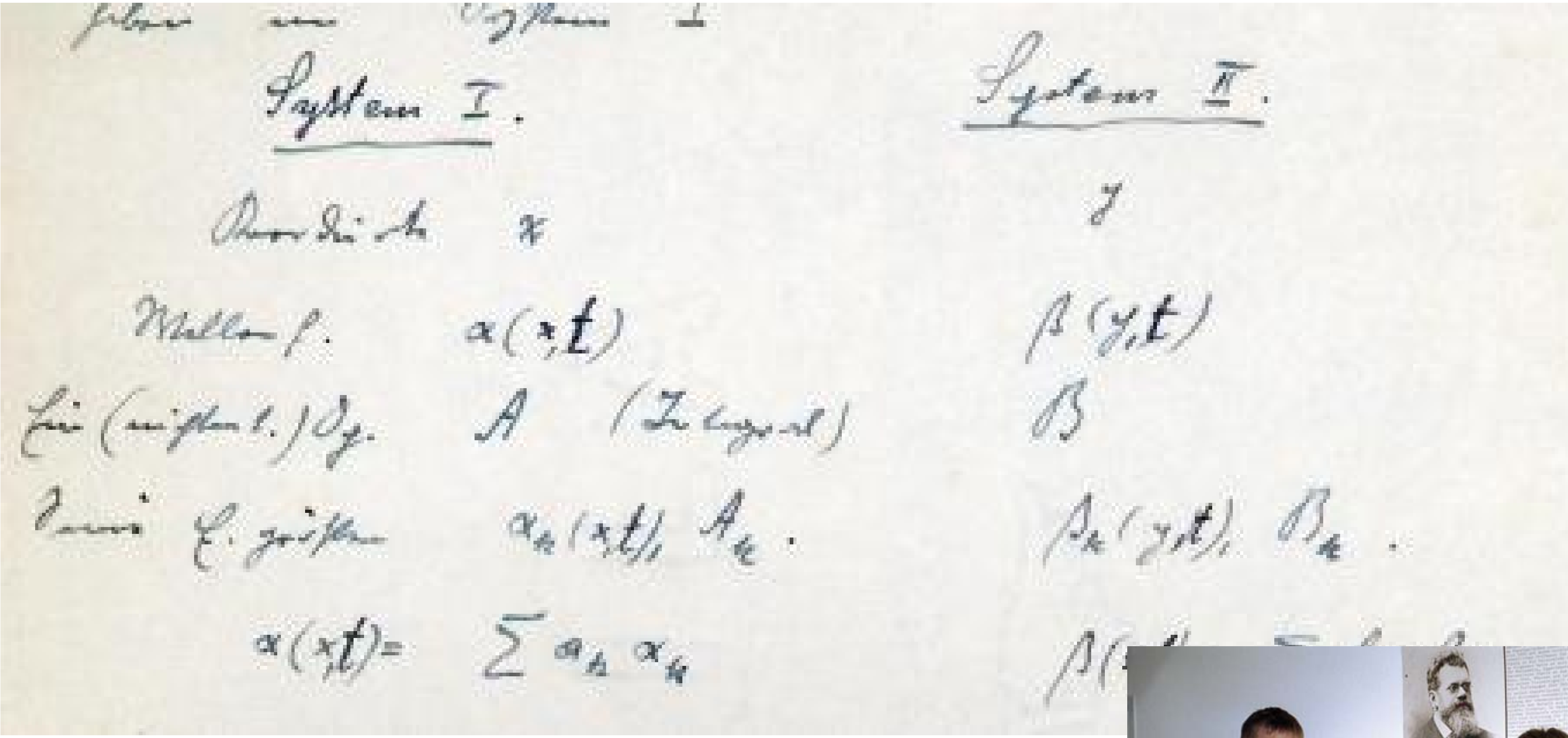
Enter entanglement



For $\oplus\oplus$ or $\otimes\otimes$ polarizations results are always opposite

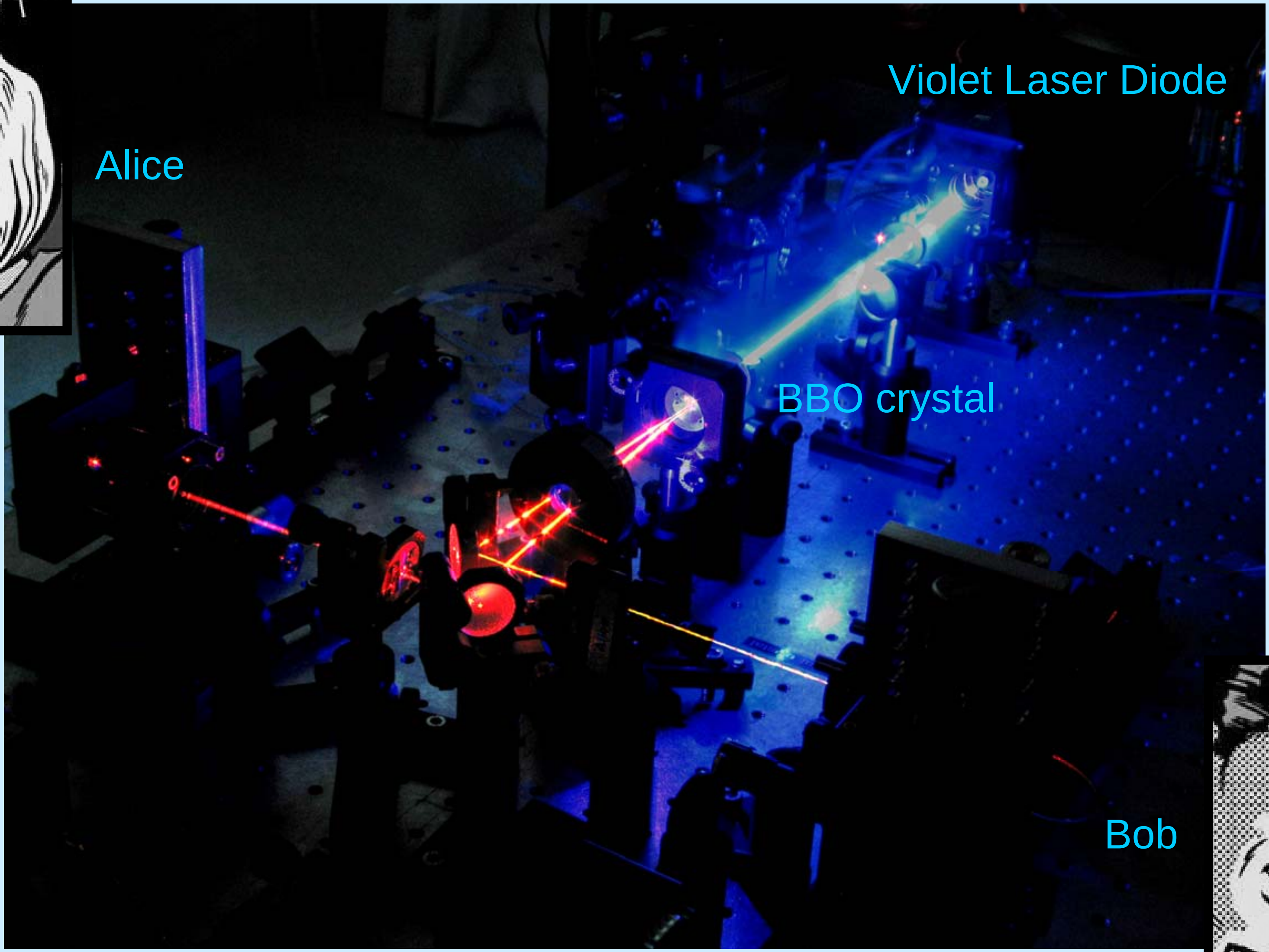
For $\oplus\otimes$ or $\oplus\otimes$ polarizations results are random

Schrödinger’s idea



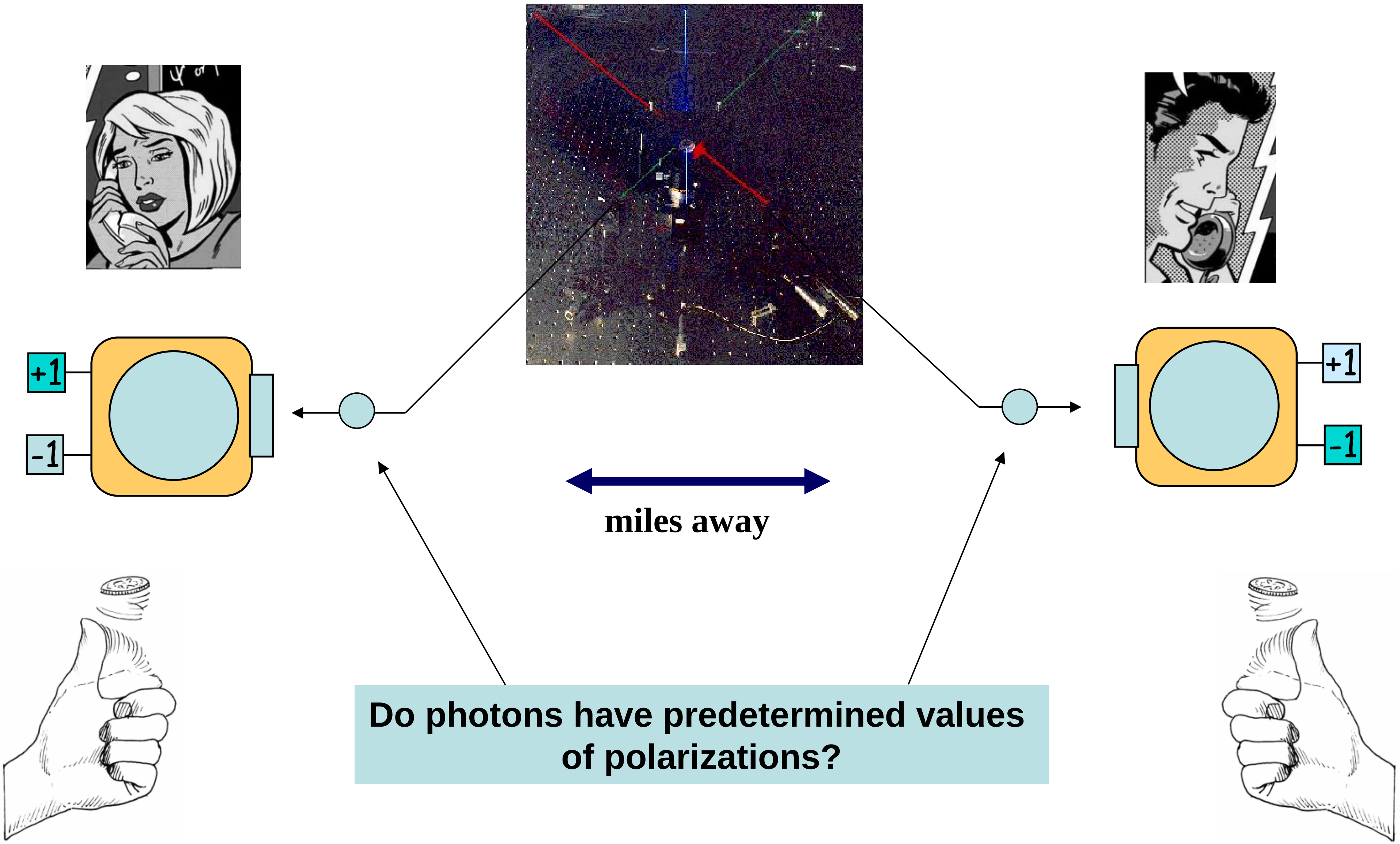
Manuscript by Schrödinger dated back to 1932 or 1933.
Discovered by Matthias Christandl and Lawrence Ioannou of Cambridge University in the Schrödinger archive in Vienna.

Entanglement @ NUS



Puzzling, eghhhh

Local realism



Suppose they have…

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)

In a complete theory there is an element corresponding to each element of reality. A sufficient condition for the reality of a physical quantity is the possibility of predicting it with certainty, without disturbing the system. In quantum mechanics in the case of two physical quantities described by non-commuting operators, the knowledge of one precludes the knowledge of the other. Then either (1) the description of reality given by the wave function in quantum mechanics is not complete or (2) these two quantities cannot have simultaneous reality. Consideration of the problem of making predictions concerning a system on the basis of measurements made on another system that had previously interacted with it leads to the result that if (1) is false then (2) is also false. One is thus led to conclude that the description of reality as given by a wave function is not complete.

1.

ANY serious consideration of a physical theory must take into account the distinction between the objective reality, which is independent of any theory, and the physical concepts with which the theory operates. These concepts are intended to correspond with the objective reality, and by means of these concepts we picture this reality to ourselves.

In attempting to judge the success of a physical theory, we may ask ourselves two questions: (1) "Is the theory correct?" and (2) "Is the description given by the theory complete?" It is only in the case in which positive answers may be given to both of these questions, that the concepts of the theory may be said to be satisfactory. The correctness of the theory is judged by the degree of agreement between the conclusions of the theory and human experience. This experience, which alone enables us to make inferences about reality, in physics takes the form of experiment and measurement. It is the second question that we wish to consider here, as applied to quantum mechanics.

Whatever the meaning assigned to the term *complete*, the following requirement for a complete theory seems to be a necessary one: *every element of the physical reality must have a counterpart in the physical theory*. We shall call this the condition of completeness. The second question is thus easily answered, as soon as we are able to decide what are the elements of the physical reality.

The elements of the physical reality cannot be determined by *a priori* philosophical considerations, but must be found by an appeal to results of experiments and measurements. A comprehensive definition of reality is, however, unnecessary for our purpose. We shall be satisfied with the following criterion, which we regard as reasonable. *If, without in any way disturbing a system, we can predict with certainty (i.e., with probability equal to unity) the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity.* It seems to us that this criterion, while far from exhausting all possible ways of recognizing a physical reality, at least provides us with one

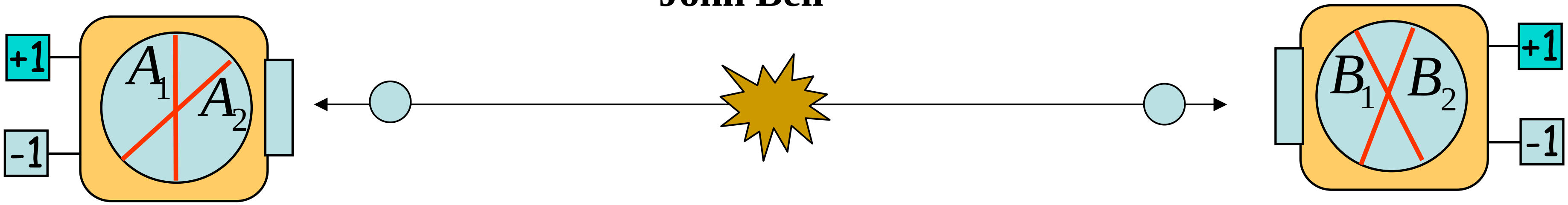
–"If, without in any way disturbing a system, we can predict with certainty… the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity"

LOCAL REALISM

PERFECT EAVESDROPPING!

Local realism is testable (1964)

John Bell



$$Q = A_1(B_1 - B_2) + A_2(B_1 + B_2)$$

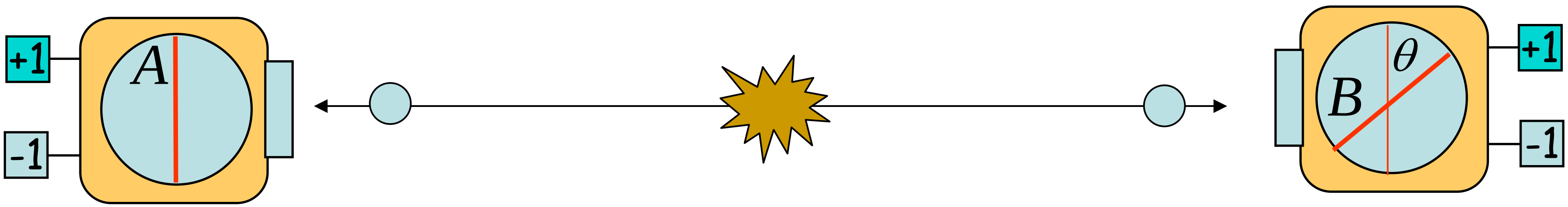
One of these terms is 0 and the other is ± 2

$$Q = \pm 2 \quad \text{hence} \quad -2 \leq \langle Q \rangle \leq 2$$

Quantum mechanical predictions

Experimental Fact

If A and B are θ degrees apart
Alice's and Bob's results agree
with the probability $\sin^2\theta$

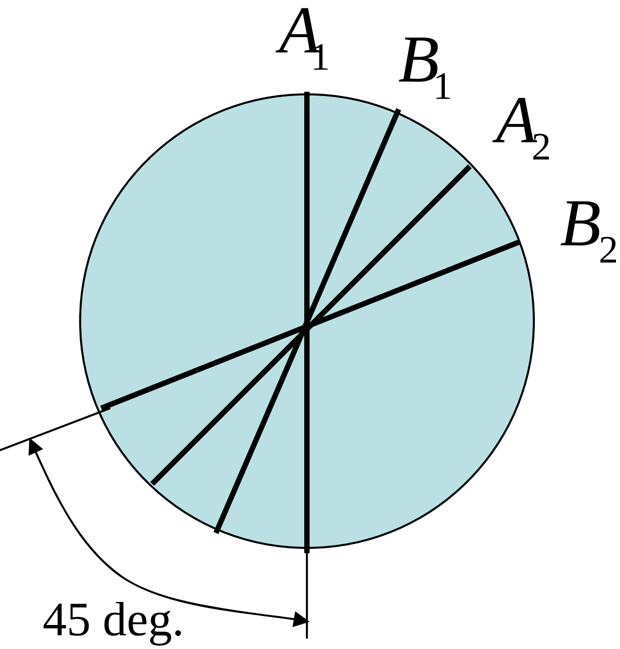


Results agree: $AB = 1$

Results disagree: $AB = -1$

$$\langle AB \rangle = \sin^2\theta - \cos^2\theta = -\cos 2\theta$$

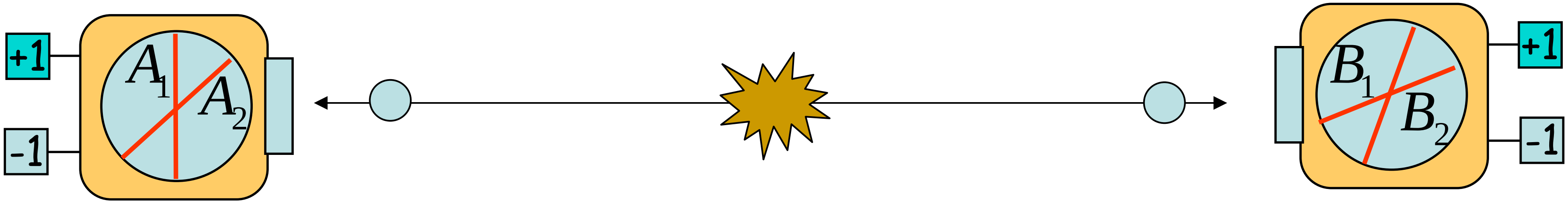
Quantum mechanics versus local realism



$$\langle A_1 B_1 \rangle = -\cos\frac{\pi}{4} = -\frac{1}{\sqrt{2}} \qquad \langle A_1 B_2 \rangle = -\cos\frac{3\pi}{4} = \frac{1}{\sqrt{2}}$$

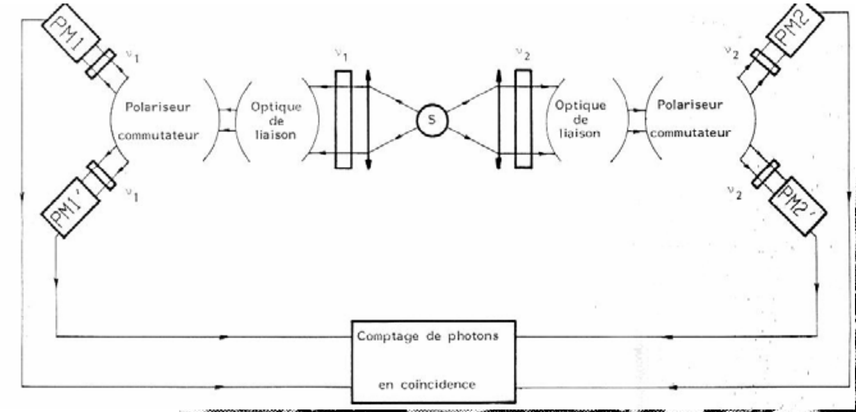
$$\langle A_2 B_1 \rangle = -\cos\frac{\pi}{4} = -\frac{1}{\sqrt{2}} \qquad \langle A_2 B_2 \rangle = -\cos\frac{\pi}{4} = -\frac{1}{\sqrt{2}}$$

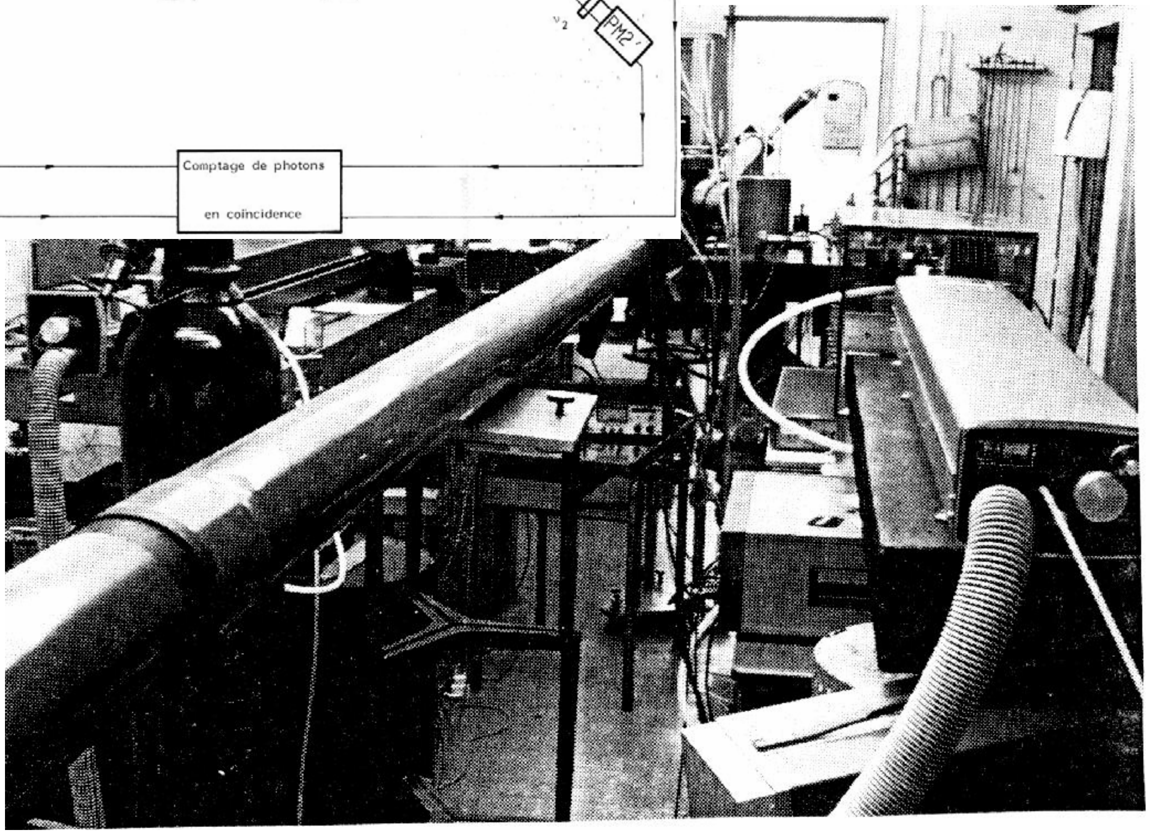
$$\langle Q \rangle = \langle A_1 B_1 \rangle - \langle A_1 B_2 \rangle + \langle A_2 B_1 \rangle + \langle A_2 B_2 \rangle$$
$$= -\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}} = -2\sqrt{2}$$



Local realism is refuted (early 1980s)

Alain Aspect





Entangled photons do not have predetermined values of polarization!

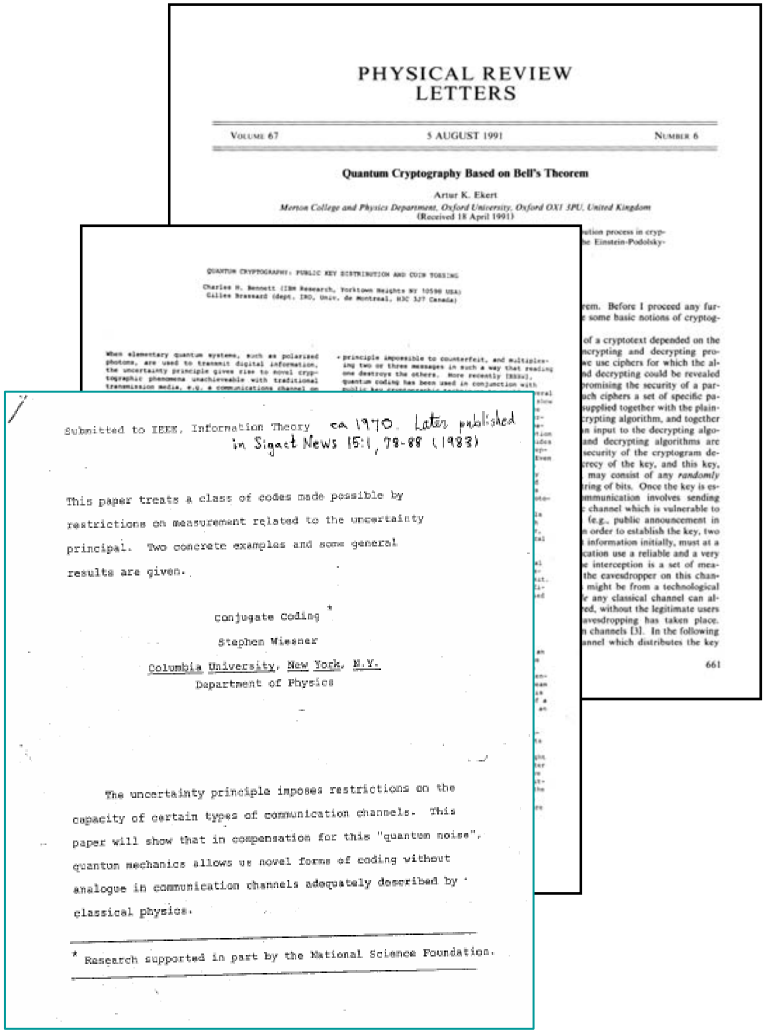
Institut d'Optique d'Orsay (1982)

What have we learned?

- Local realism is refuted by quantum theory
- Entangled photons do not have predetermined values of polarization…
- …so eavesdropper has nothing to measure
- Quantum mechanics allows eavesdropper free communication
- Any post-quantum theory that refutes local realism allows eavesdropper free communication.

Entanglement as a resource

QUANTUM CRYPTOGRAPHY


PHYSICAL REVIEW LETTERS

VOLUME 67 5 AUGUST 1991 NUMBER 6

Quantum Cryptography Based on Bell's Theorem

Artur K. Ekert

Merton College and Physics Department, Oxford University, Oxford OX1 3PU, United Kingdom
(Received 18 April 1991)

QUANTUM CRYPTOGRAPHY: PUBLIC KEY DISTRIBUTION AND COIN TOSSING

Charles H. Bennett (IBM Research, Yorktown Heights NY 10598 USA)
Gilles Brassard (dept. IRO, Univ. de Montreal, H3C 3J7 Canada)

Submitted to IEEE, Information Theory ca 1970. Later published in Sigact News 15:1, 78-88 (1983)

This paper treats a class of codes made possible by restrictions on measurement related to the uncertainty principal. Two concrete examples and some general results are given.

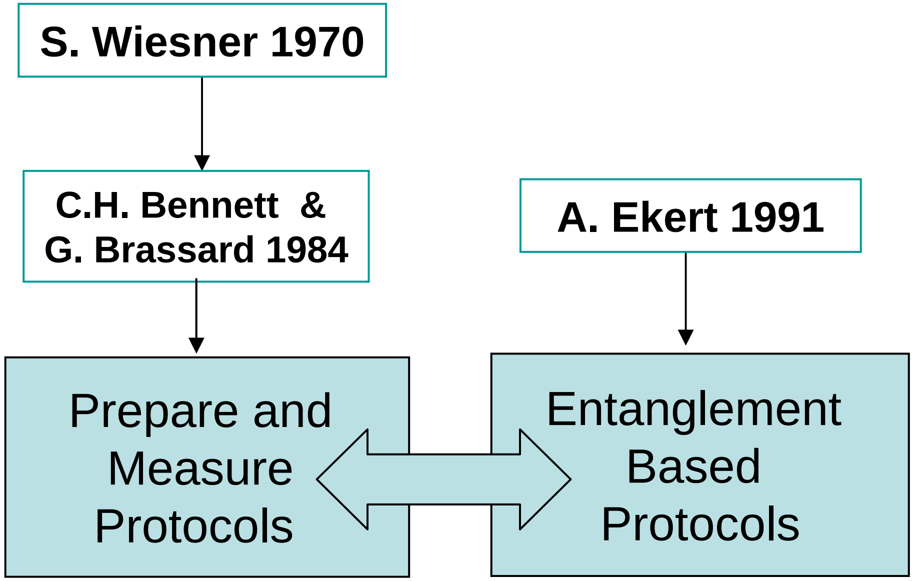
Conjugate Coding *

Stephen Wiesner

Columbia University, New York, N.Y.
Department of Physics

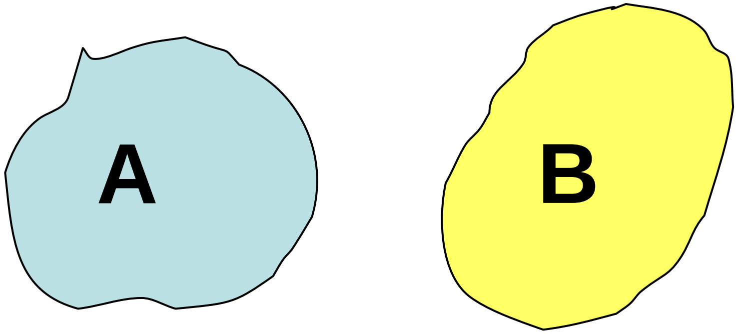
The uncertainty principle imposes restrictions on the capacity of certain types of communication channels. This paper will show that in compensation for this "quantum noise", quantum mechanics allows us novel forms of coding without analogue in communication channels adequately described by classical physics.

* Research supported in part by the National Science Foundation.



Entangled or separable ?

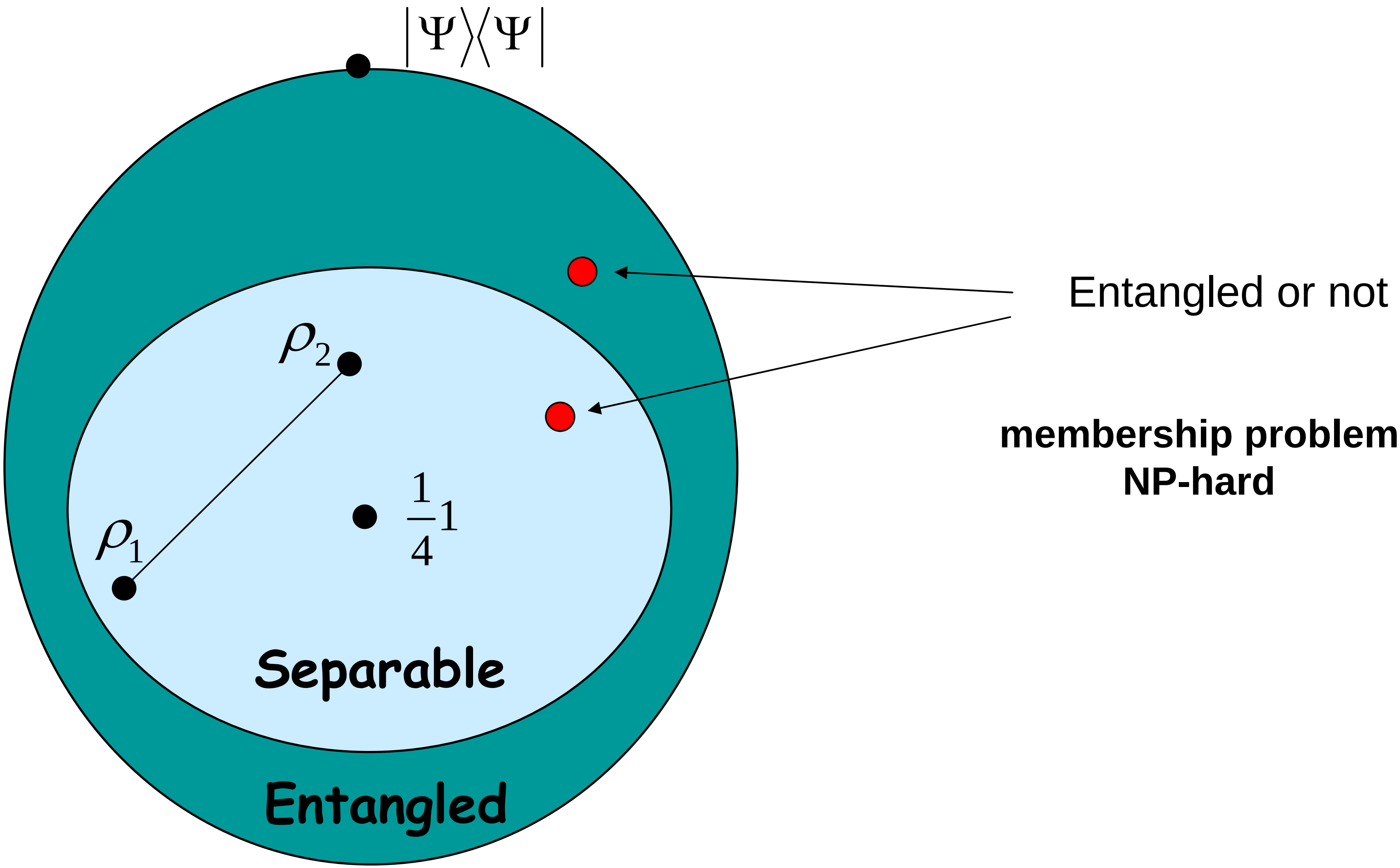
$|\Psi_a\rangle$ $|\Psi_b\rangle$



$$\rho = \sum_i p_i |a_i\rangle\langle a_i| \otimes |b_i\rangle\langle b_i|$$

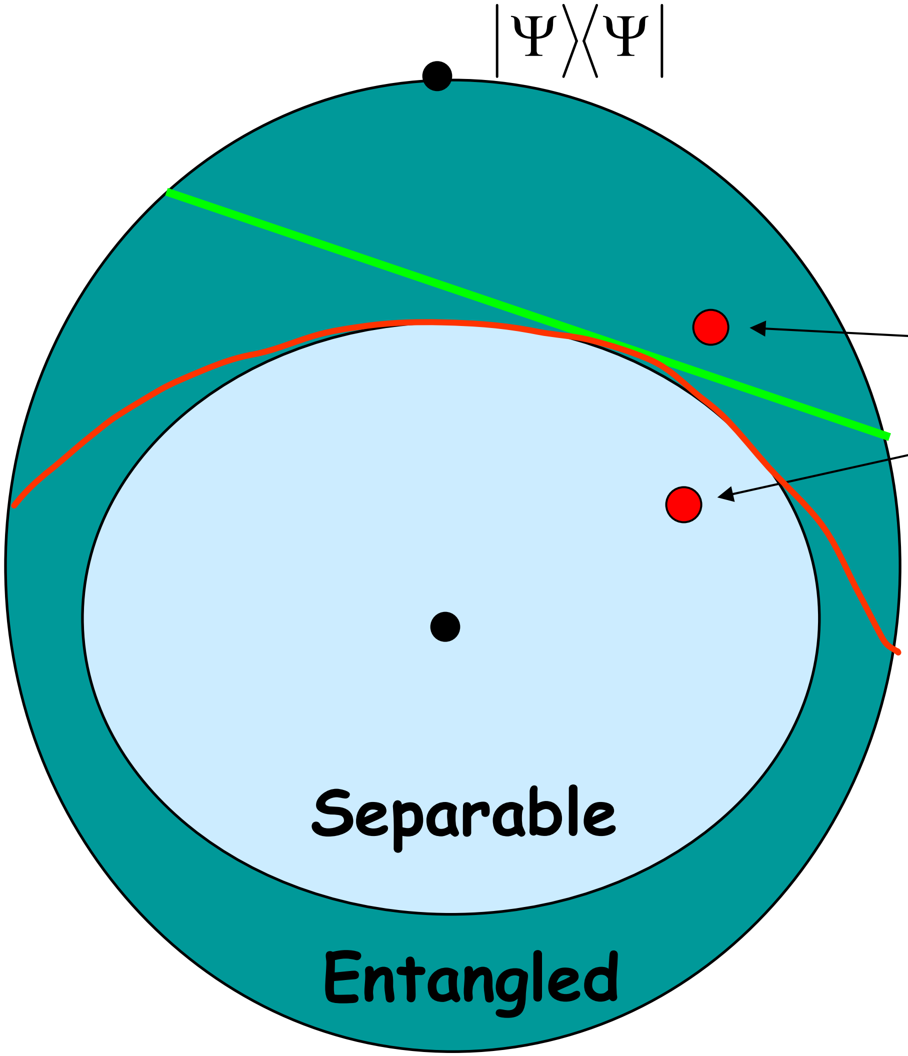
E.Schrödinger, Proc. Cam. Phil. Soc. 31, 555 (1935)
R.Werner, Phys. Rev. A 40, 4277 (1989)

Geometry of density operators



membership problem
NP-hard

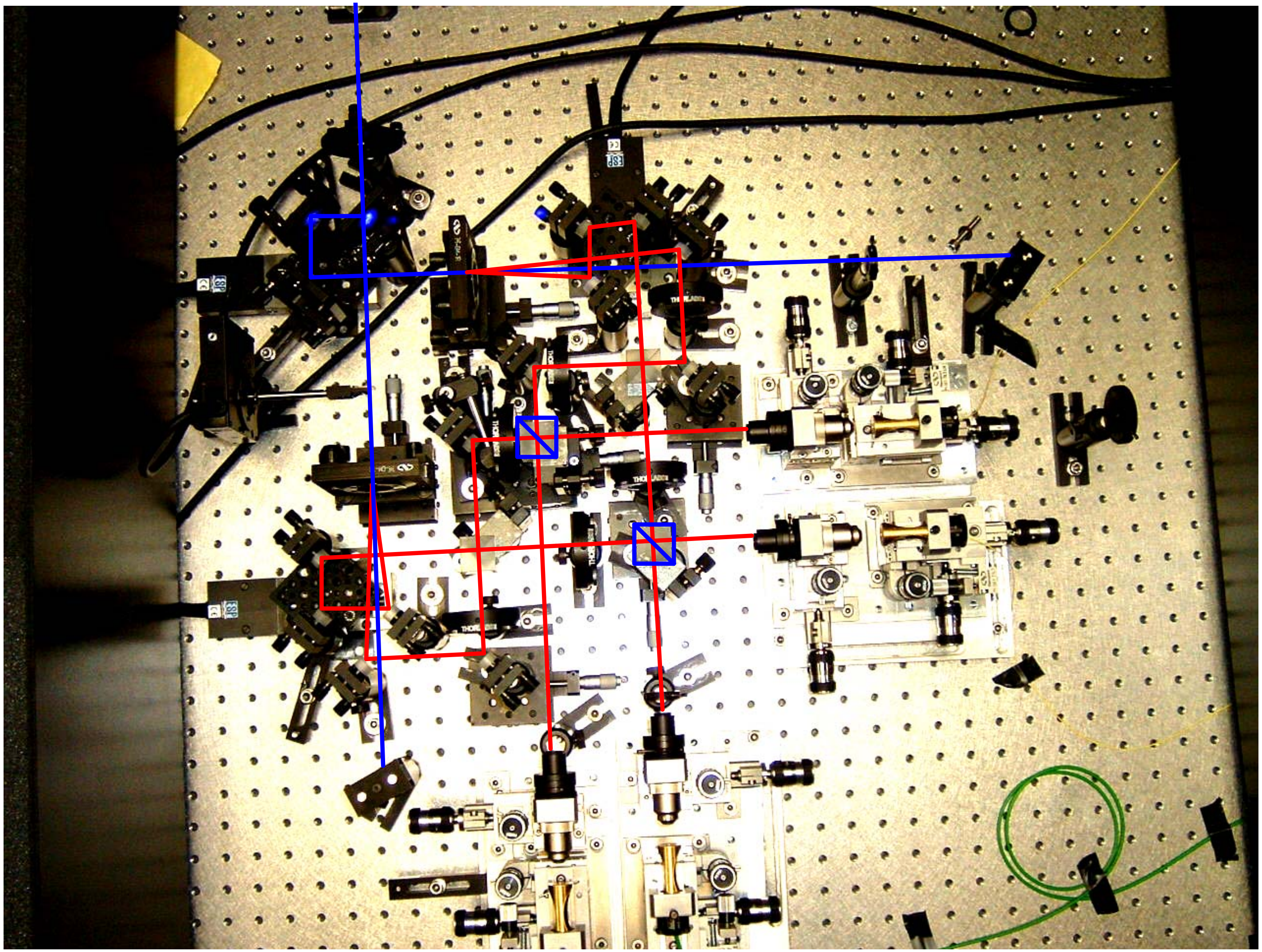
Entanglement witness



Entangled or not

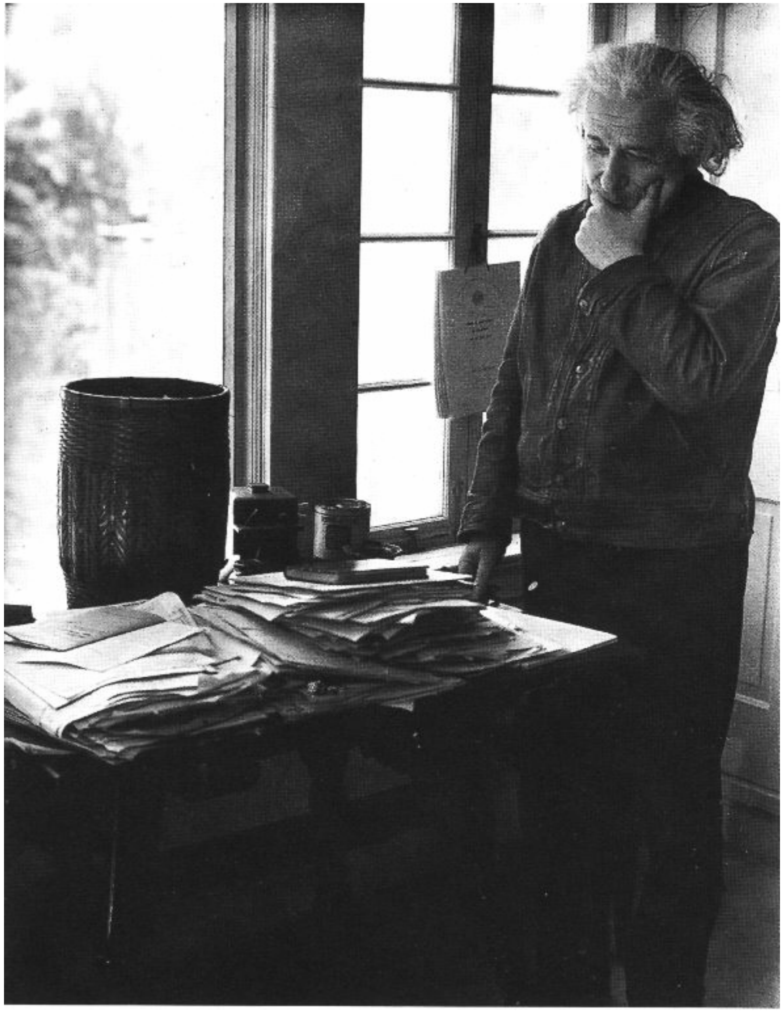
membership problem
NP-hard

Real stuff



There is even more to entanglement…

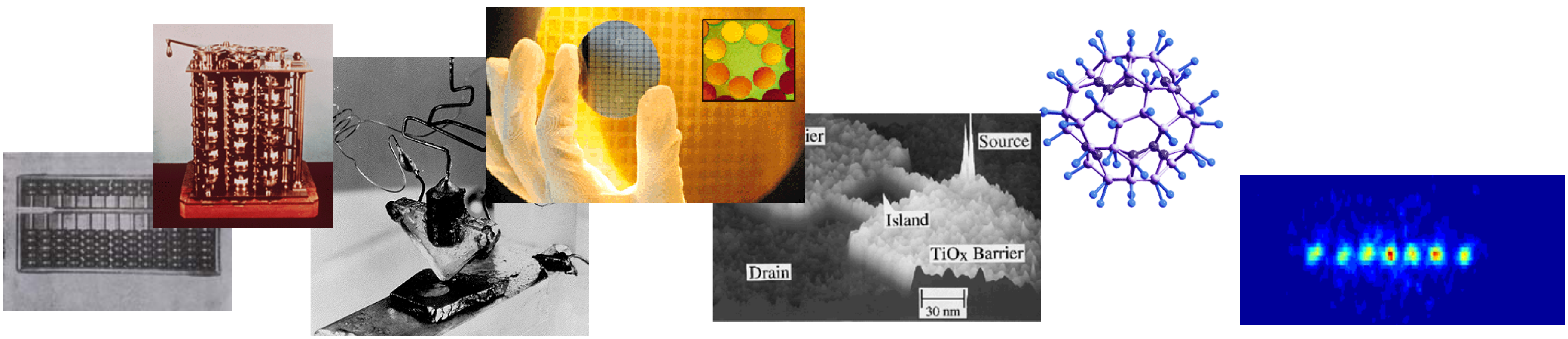
- **Quantum cryptography**
- **Quantum computation**
- **Quantum metrology**
- **Precise atomic clocks**
- **…**



Shrinking computer

CLASSICAL

QUANTUM



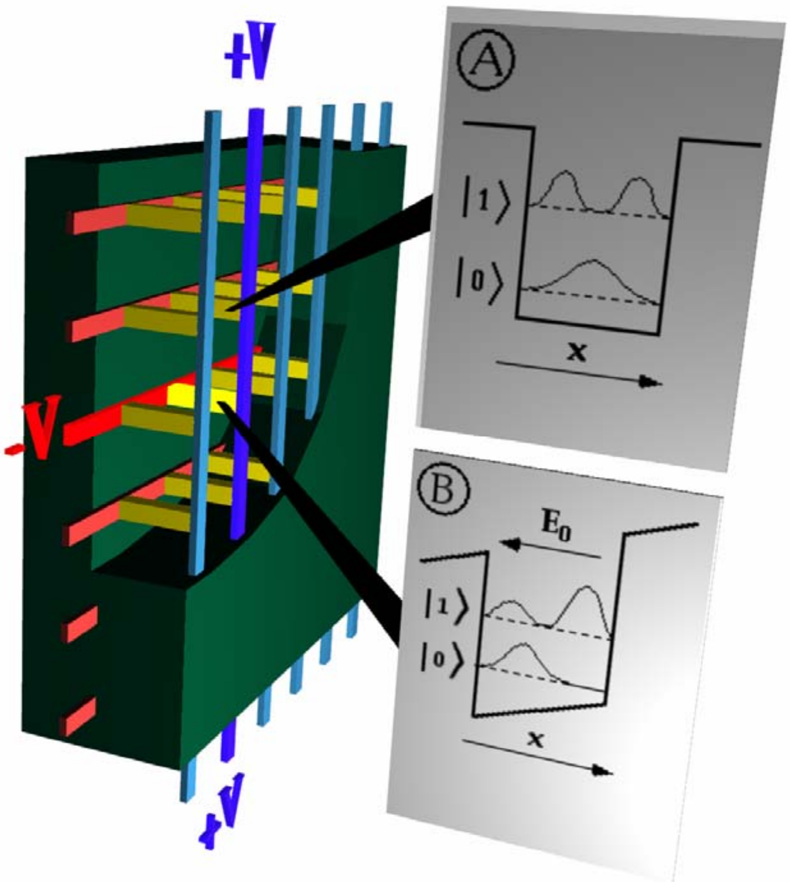
1 meter

0.000000001 meters

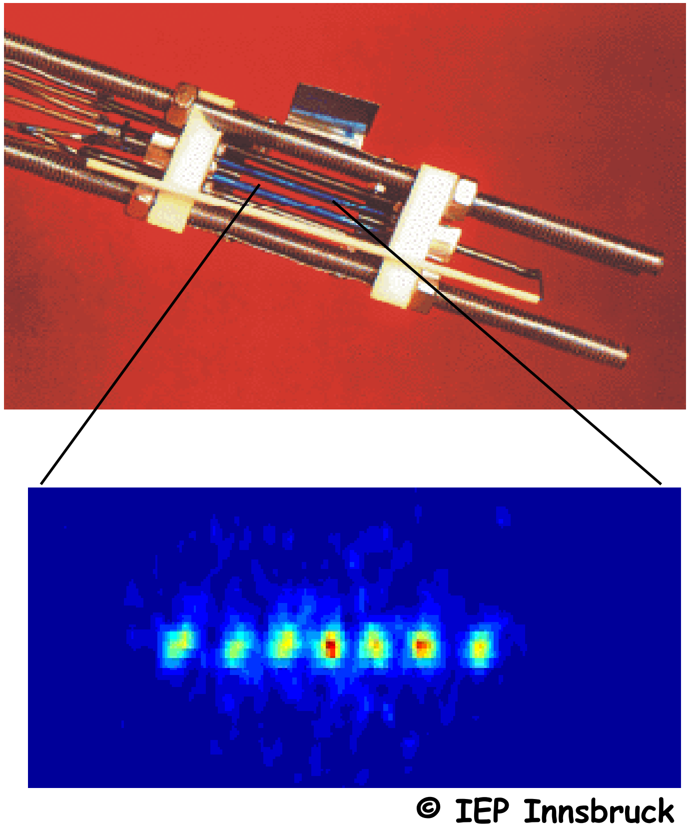
EVERY 18 MONTHS MICROPROCESSORS DOUBLE IN SPEED

How quantum computers will look like?

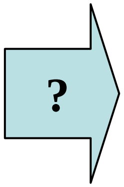
EVOLVING VISION…



1993 VISION (Barenco and Ekert)
array of single electron quantum dots



1994 VISION (Cirac and Zoller…)
ions in ion traps



Predictions are risky

"The Eniac has 18 000 vacuum tubes and weigh 30 tons, we envisage in the future of computers with 1000 tubes and of a weight of only 1 1/2 ton"

Popular Mechanics, 1949.

"I think there is a world market for about five computers"

Remark attributed to Thomas J. Watson
(Chairman of the Board of International Business Machines) 1943.