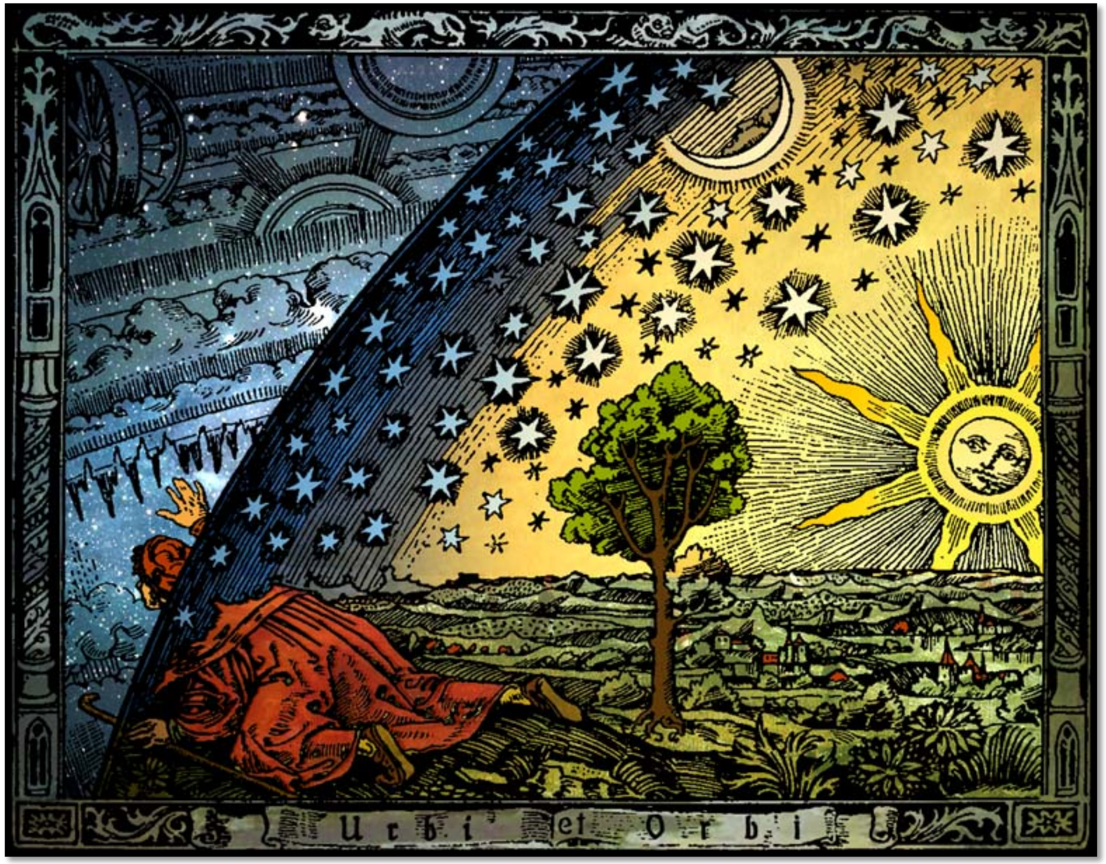


LESS REALITY MORE SECURITY

Artur Ekert
Mathematical Institute
University of Oxford

The story of worry…

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.

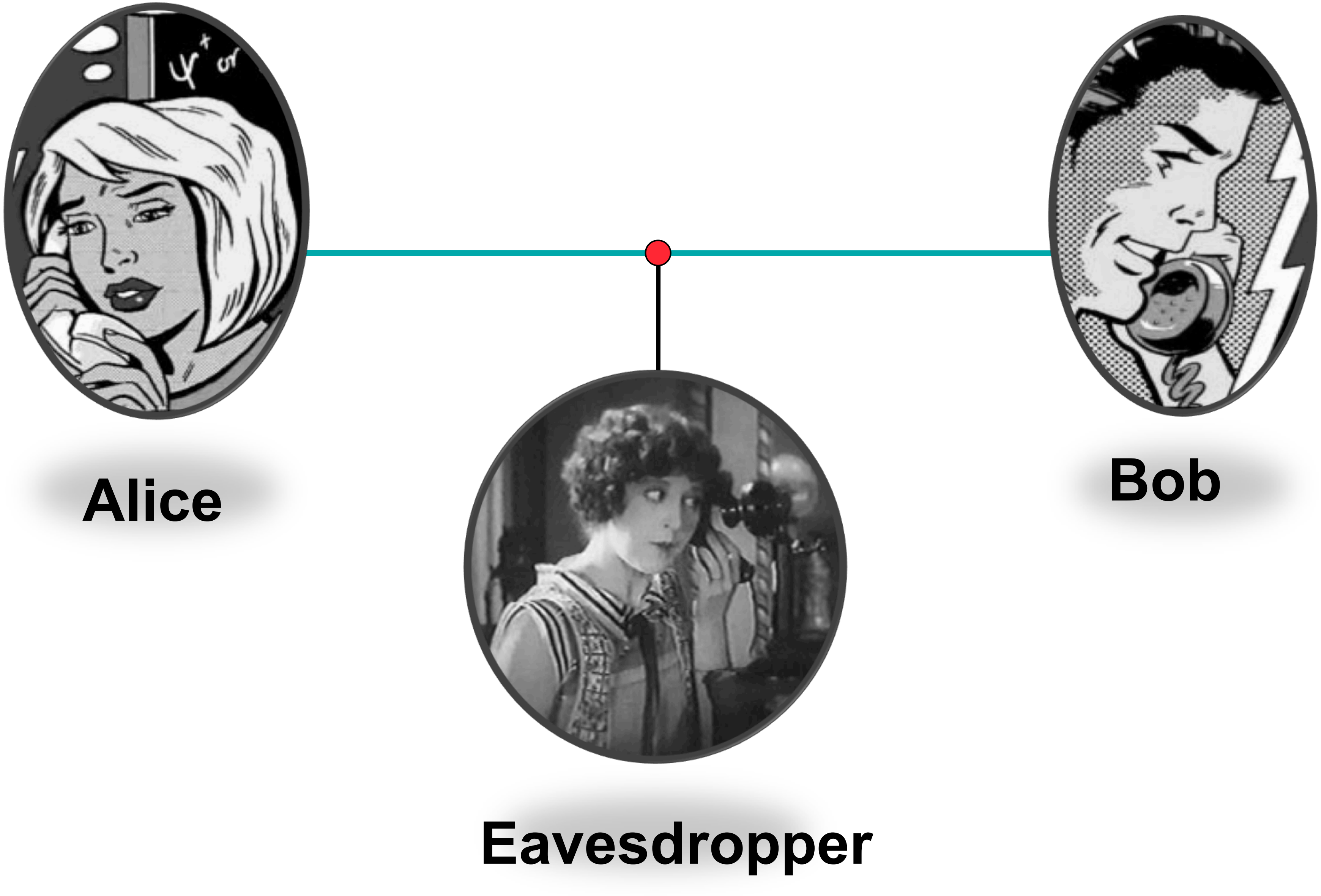
ANY serious consideration of a physical theory must take into account the distinction between the objective reality, which is independent of any theory, and the physical concepts with which the theory operates. These concepts are intended to correspond with the objective reality, and by means of these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

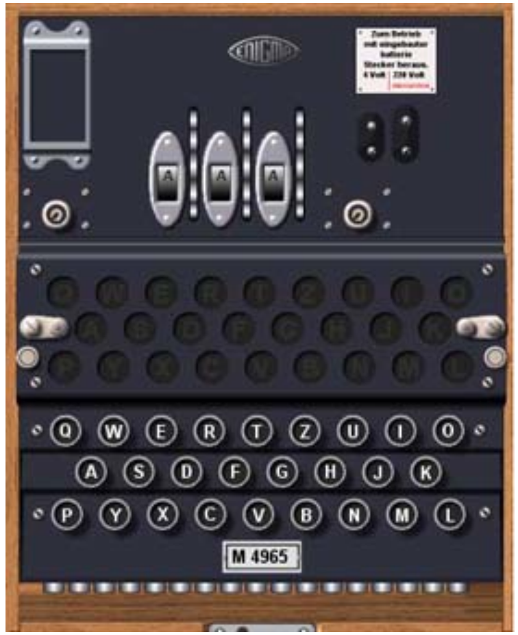
The story of secrecy…



Is there a perfect cipher ?

SCYTALE 400BC

ALBERTI'S DISC 1450



ENIGMA 1940

One-time pad

1011100	plaintext
11001010	KEY
10010110	cryptogram

1	0	0	1	0	1	1	0

cryptogram	10010110
KEY	11001010
plaintext	1011100

Key distribution problem

?

miles away

KEY	0	0	1	0	1	1	0

KEY	0	0	1	0	1	1	0

Possible solutions

PUBLIC KEY CRYPTOGRAPHY

SECURITY BASED ON COMPUTATIONAL COMPLEXITY

CAN BE BROKEN BY QUANTUM COMPUTERS

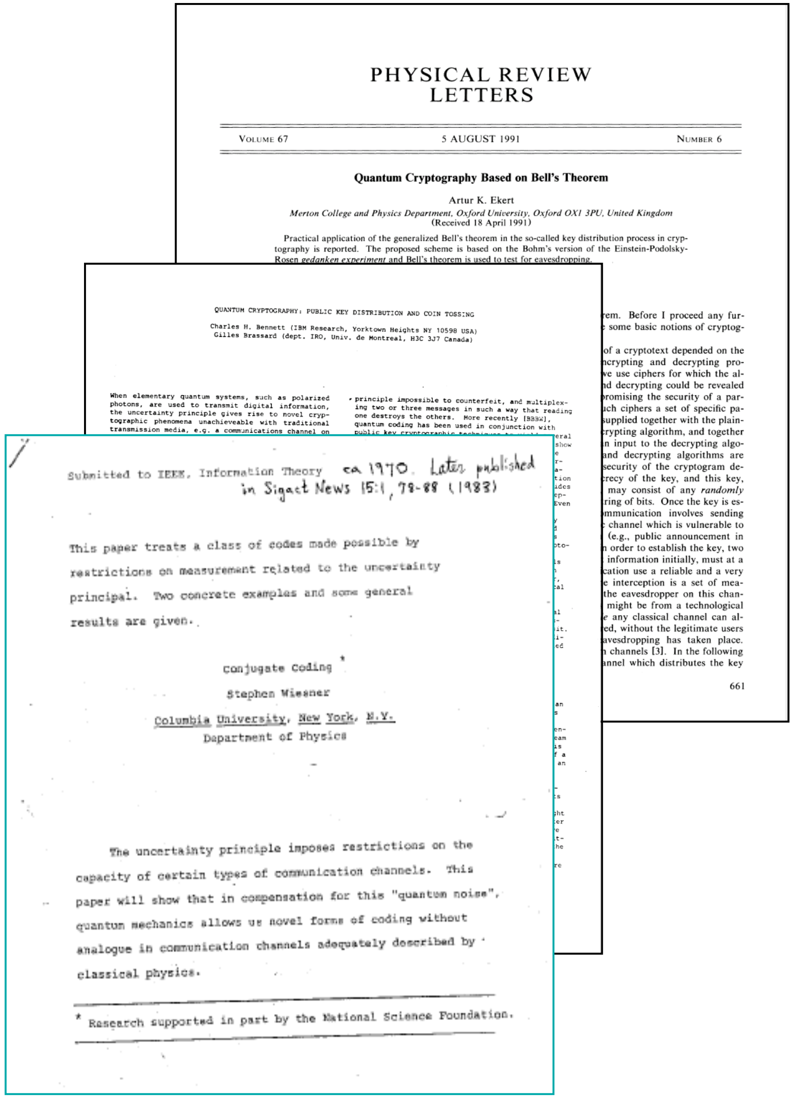
QUANTUM CRYPTOGRAPHY

SECURITY BASED ON QUANTUM PHENOMENA

POST-QUANTUM CRYPTOGRAPHY

SECURITY BASED ON NON-LOCALITY

Origins of 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)

Practical application of the generalized Bell's theorem in the so-called key distribution process in cryptography is reported. The proposed scheme is based on the Bohm's version of the Einstein-Podolsky-Rosen *gedanken experiment* and Bell's theorem is used to test for eavesdropping.

661

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 *

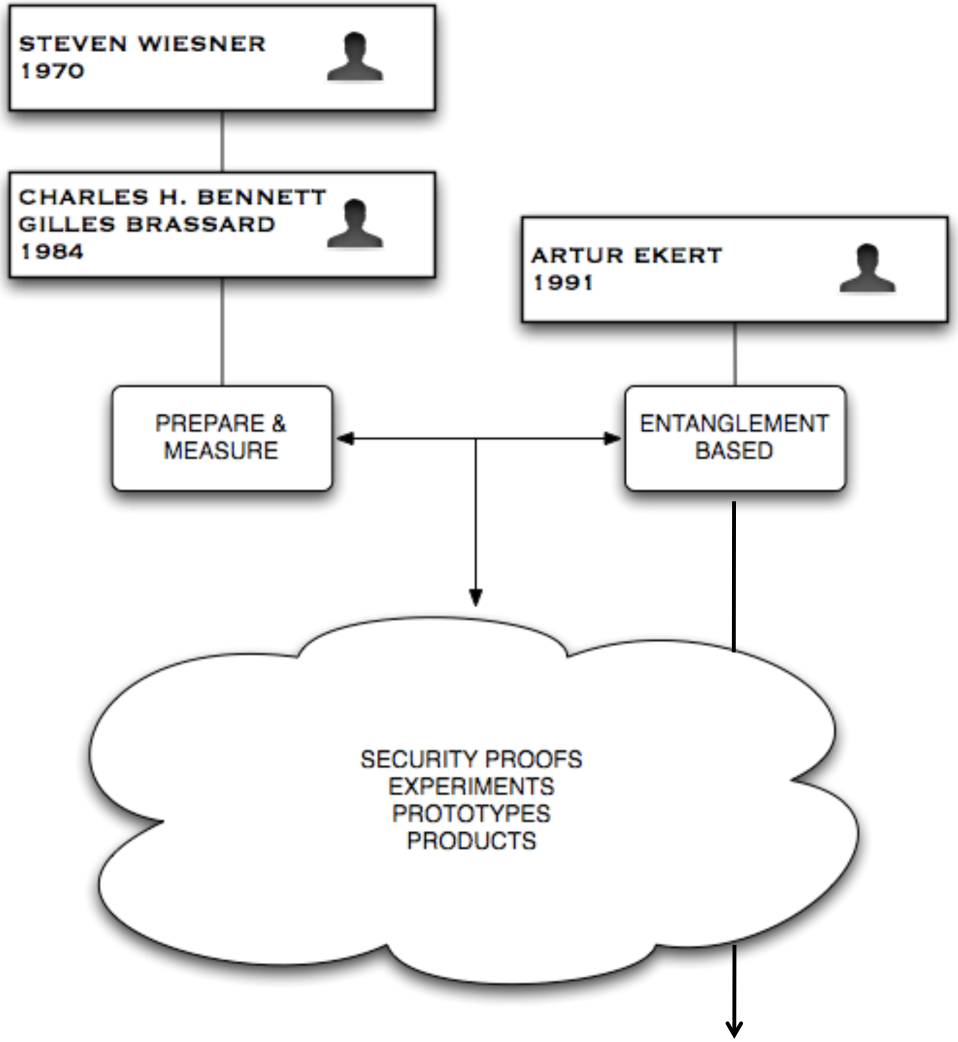
Stephen Wiesner

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.



Device independence etc

Connections

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.

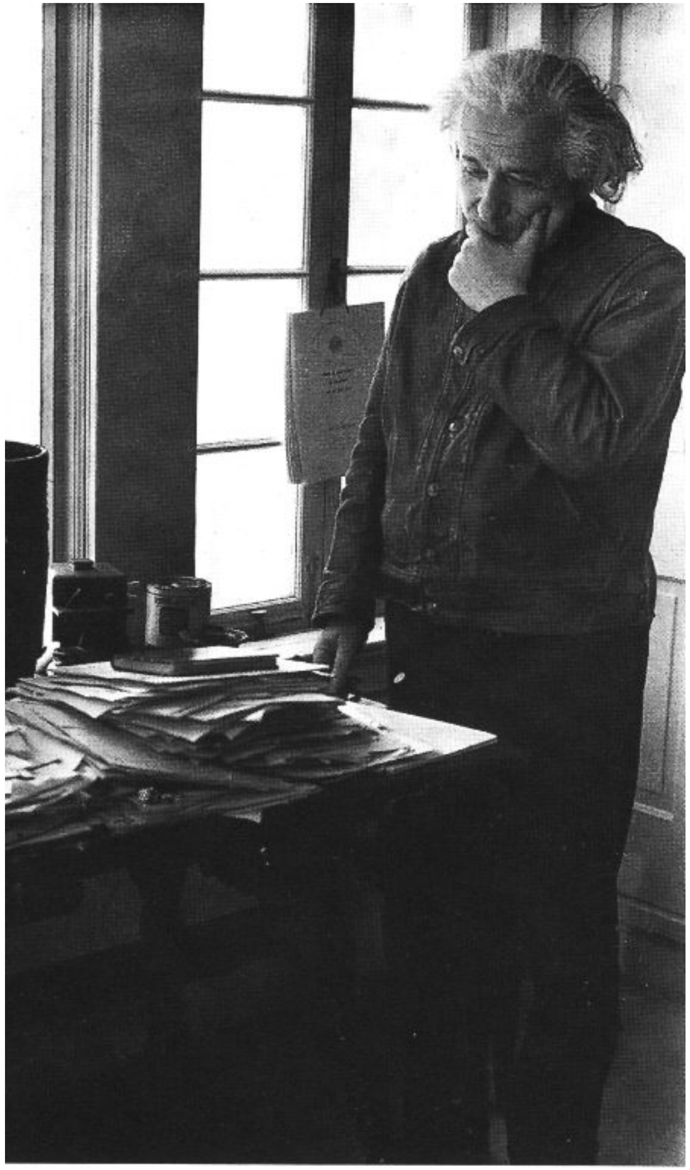
1.

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.

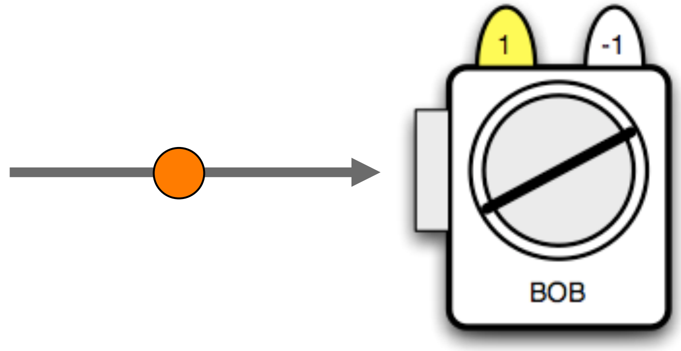
Whatever the meaning assigned to the term *complete*, the following requirement for a complete theory seems to be a necessary one: *every element of the physical reality must have a counterpart in the physical theory*. We shall call this the condition of completeness. The second question is thus easily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



DEFINITION OF EAVESDROPPING

Polarization

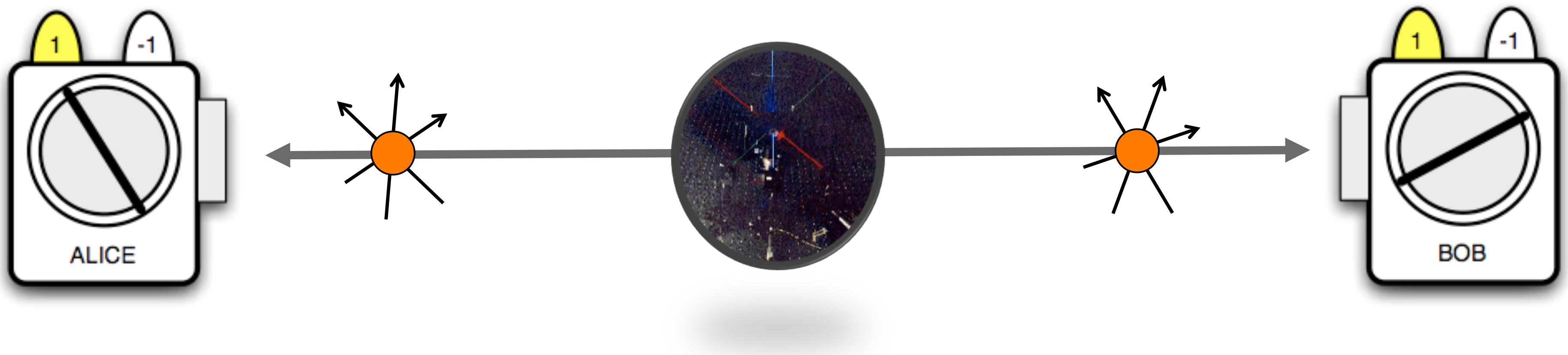


POLARIZATION IS AN INTRINSIC PROPERTY OF A PHOTON

WE CANNOT JUST "MEASURE POLARIZATION" - WE CAN ONLY MEASURE POLARIZATION WITH RESPECT TO SOME SPECIFIED DIRECTION

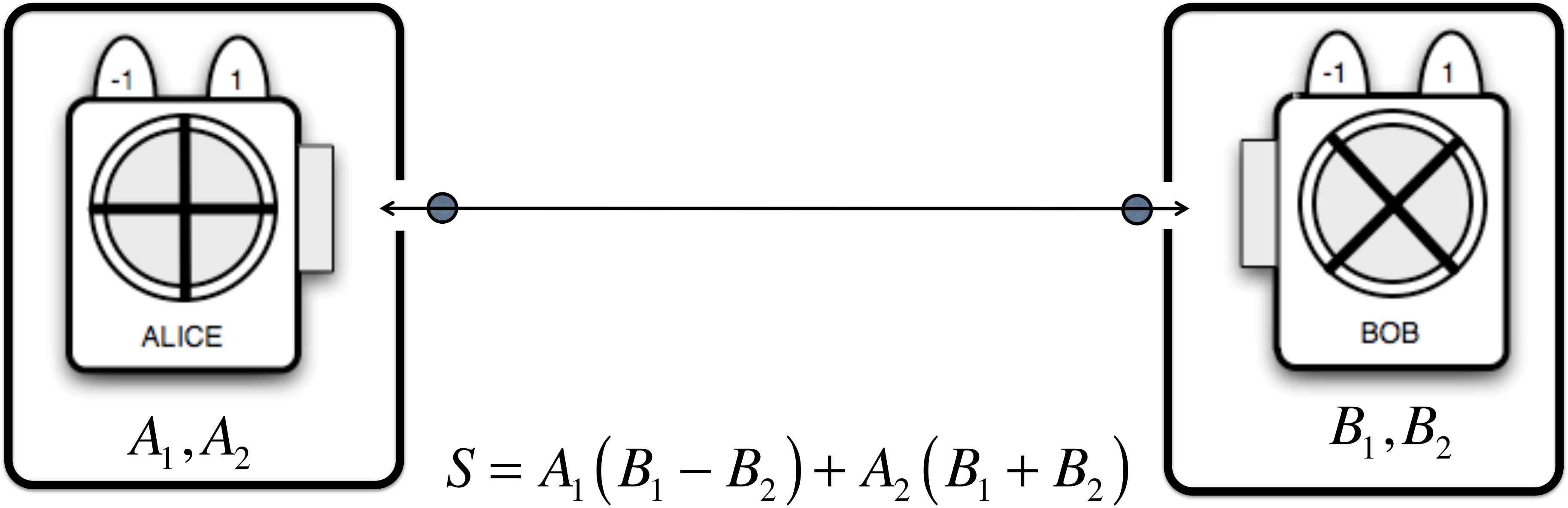
IN ANY MEASUREMENT WE CAN GET ONLY TWO RESULTS: +1 OR -1

Local realism



Do photons have predetermined values of polarizations?

Local realism is testable

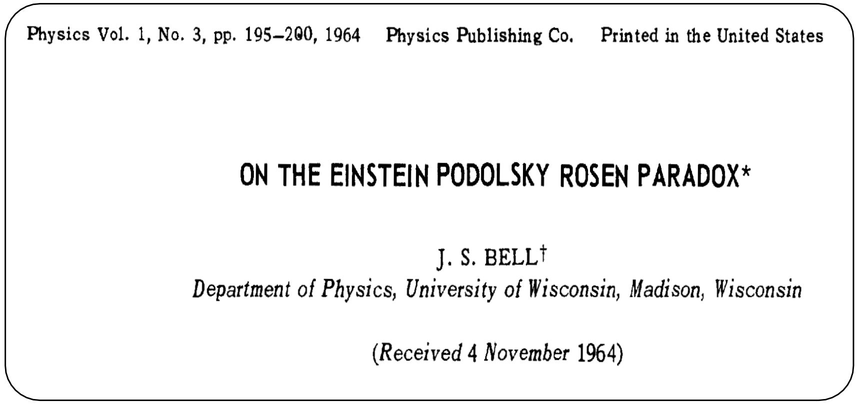


$$S = A_1\left(B_1 - B_2\right) + A_2\left(B_1 + B_2\right)$$

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

$S = \pm 2$ **hence** $-2 \leq \langle S \rangle \leq 2$

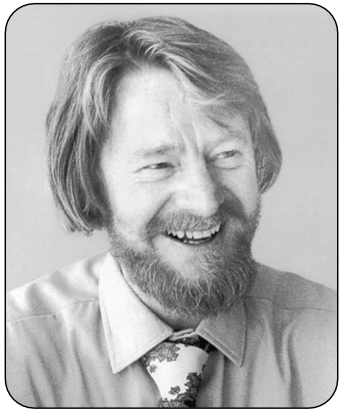
Quantum theory versus local realism


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

ON THE EINSTEIN PODOLSKY ROSEN PARADOX*

J. S. BELL†
Department of Physics, University of Wisconsin, Madison, Wisconsin

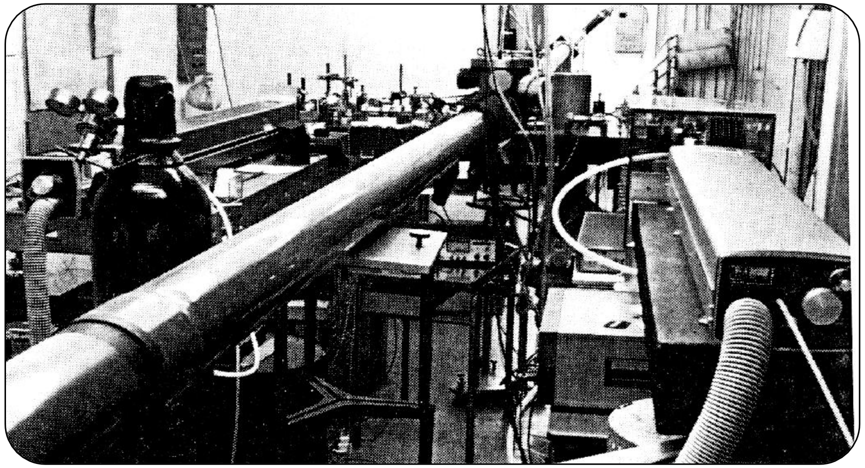
(*Received* 4 *November* 1964)



John S. Bell

<u>LOCAL REALISM IS TESTABLE</u>

1964



Institut d’Optique d’Orsay (1982)

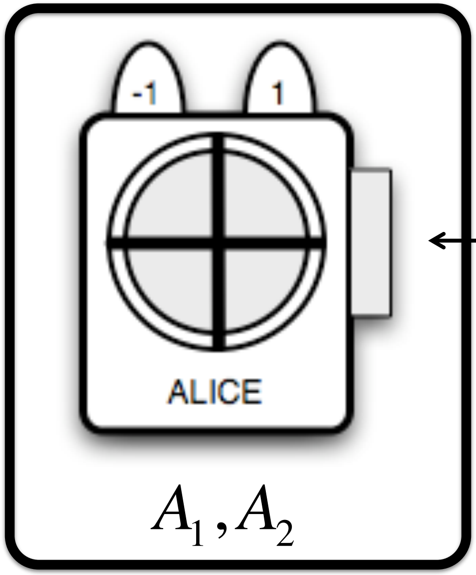
Alain Aspect

<u>LOCAL REALISM IS REFUTED</u>

**J.F. Clauser, S.J. Freedman,
E.S. Fry, A. Aspect, P. Grangier,
G. Roger…**

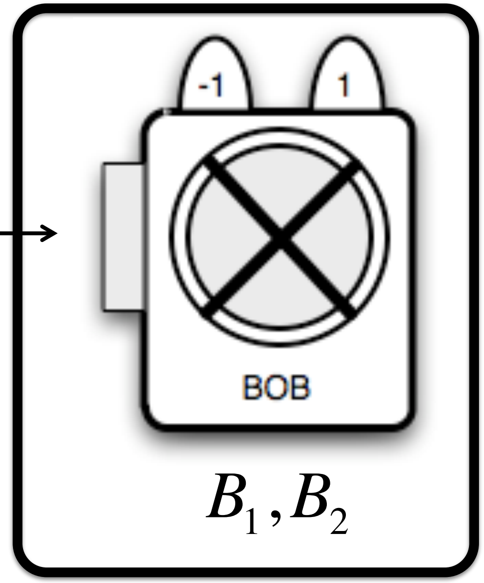
1972-1982

Local realism is refuted



Experimental fact

If A and B are θ degrees apart Alice's and Bob's results agree with the probability $\sin^2\left(\frac{\theta}{2}\right)$



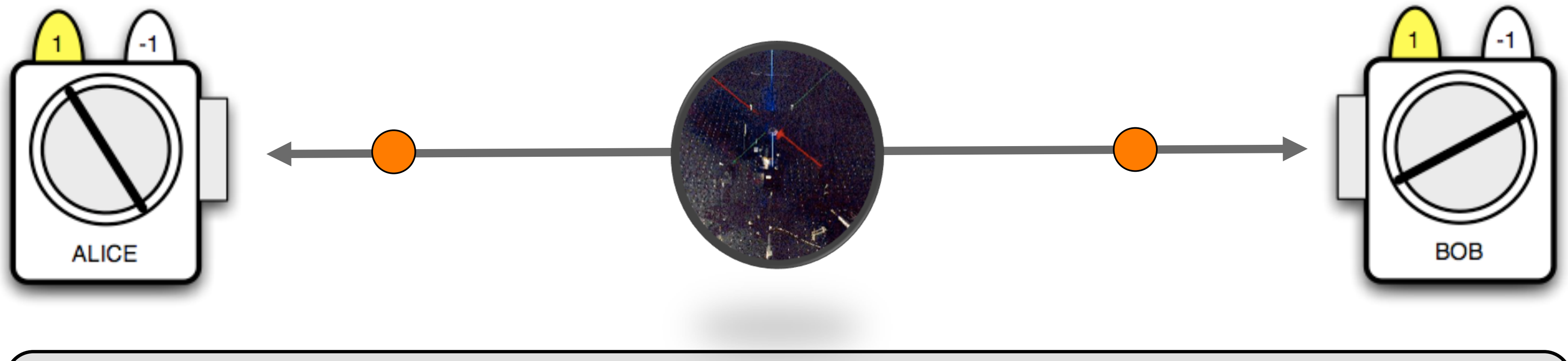
Results agree: $AB = 1$

Results disagree: $AB = -1$

$$\langle AB \rangle = \sin^2\left(\frac{\theta}{2}\right) - \cos^2\left(\frac{\theta}{2}\right) = -\cos\theta$$

$$-2\sqrt{2} \le \langle A_1B_1 \rangle - \langle A_1B_2 \rangle + \langle A_2B_1 \rangle + \langle A_2B_2 \rangle \le 2\sqrt{2}$$

Less reality more security



PHOTONS DO NOT CARRY PREDETERMINED VALUES OF POLARIZATIONS

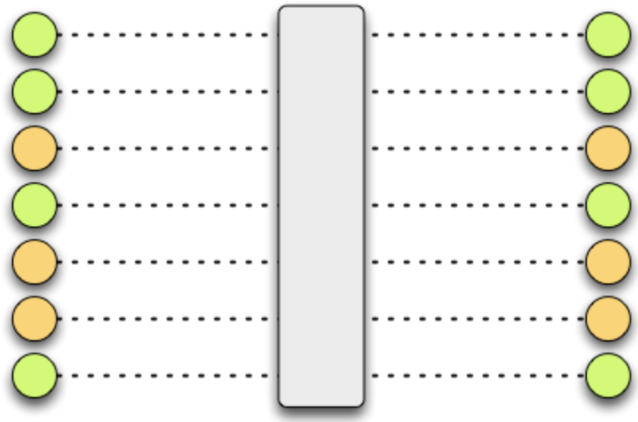
IF THE VALUES DID NOT EXIST PRIOR TO MEASUREMENTS THEY WERE NOT AVAILABLE TO ANYBODY INCLUDING EAVESDROPPERS

TESTING FOR THE VIOLATION OF BELL'S INEQUALITIES = TESTING FOR EAVESDROPPING

A. Ekert 1991

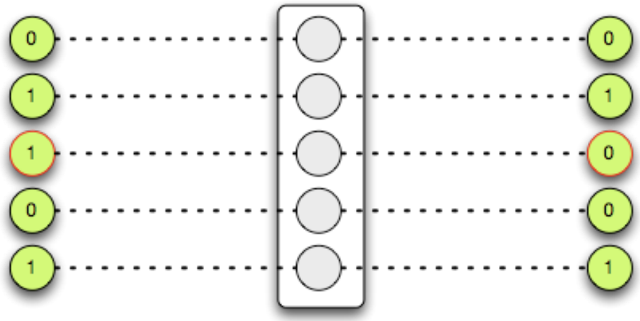
Quantum Key Distribution

Alice and Bob hold N bipartite quantum subsystems e.g. pairs of entangled qubits that can be provided by Eve



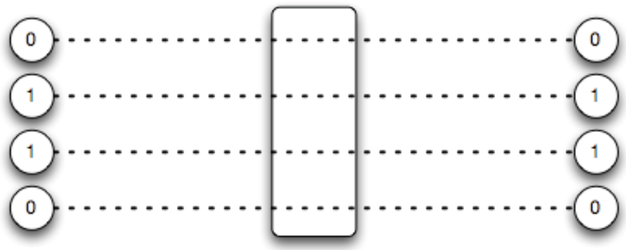
Parameter estimation bounds Eve's information

Alice and Bob measure qubits in a prescribed basis and obtain two partially correlated strings X and Y



Error correction and privacy amplification

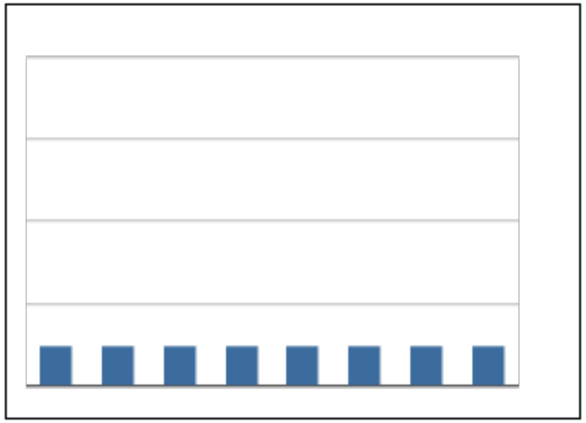
THE KEY



Security defined

$$P_{KE} \stackrel{?}{=} U_K P_E$$

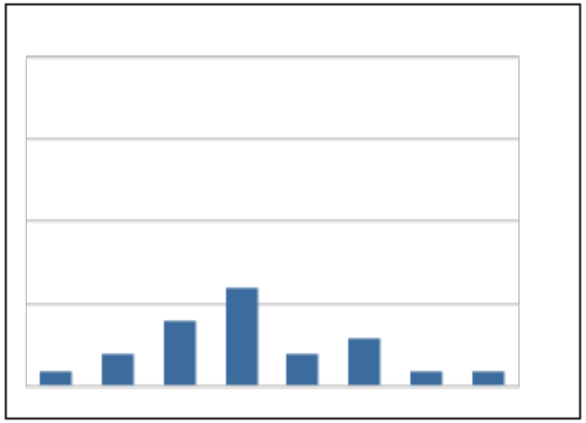
U_K



2^n equally probable keys

$K \in \{0,1\}^n$

P_E

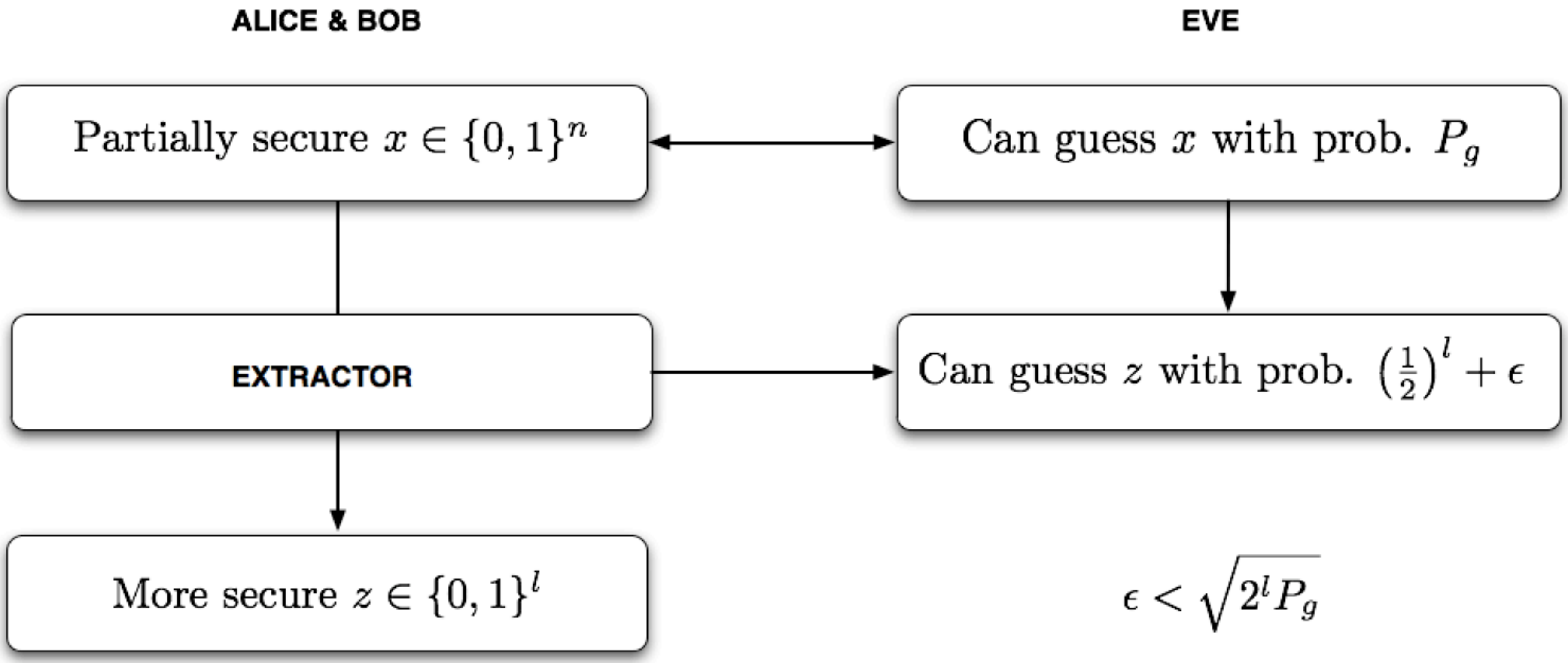


Eve's information

$$|P_{KE} - U_K P_E| \leq \epsilon$$

secret and uniformly distributed

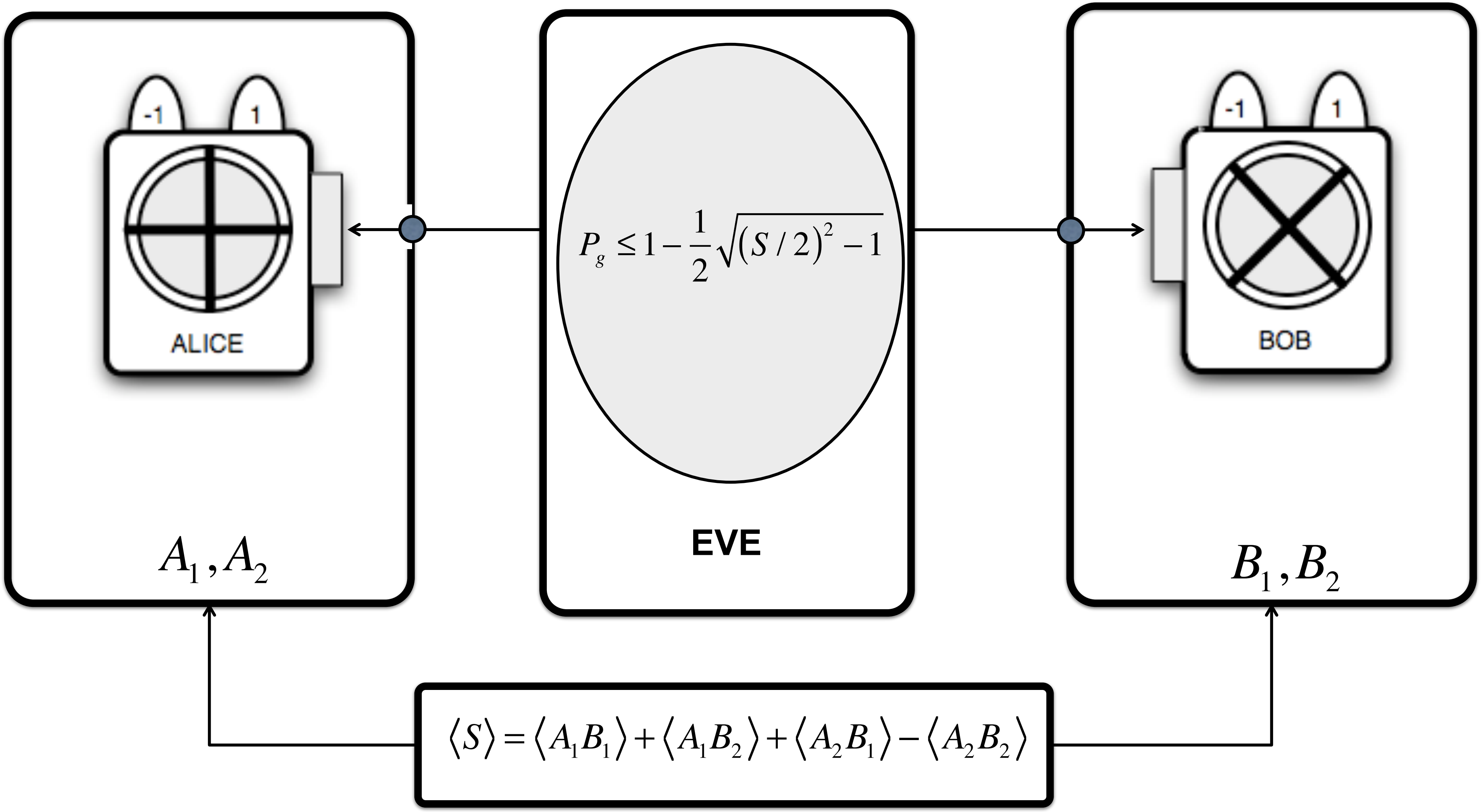
Intuition quantified



$$\epsilon < \sqrt{2^l P_g}$$

$$\epsilon \leq \sqrt{\left(\frac{1}{2}\right)^{k-l}} \qquad P_g = \left(\frac{1}{2}\right)^k$$

Bell inequalities and security



Bell's inequality & security revisited

$$\langle S \rangle = \langle A_1 B_1 \rangle + \langle A_1 B_2 \rangle + \langle A_2 B_1 \rangle - \langle A_2 B_2 \rangle$$

$+1 \quad +1 \quad +1 \quad -1$

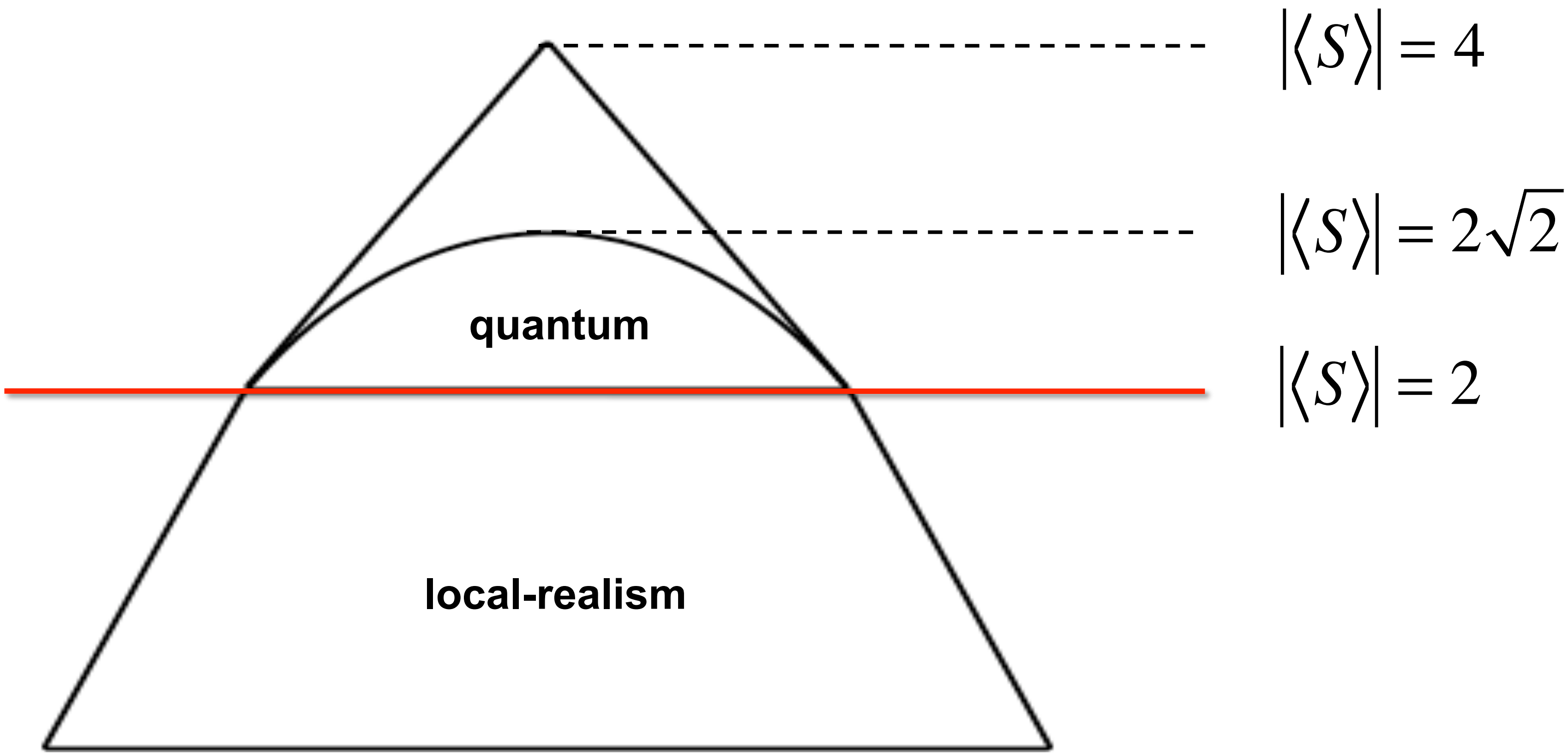
Does nature allow such correlations?

No spooky action at a distance

$$\sum_y P(x,y \mid A,B) = P(x \mid A,\cancel{B})$$

$$\sum_x P(x,y \mid A,B) = P(y \mid \cancel{A},B)$$

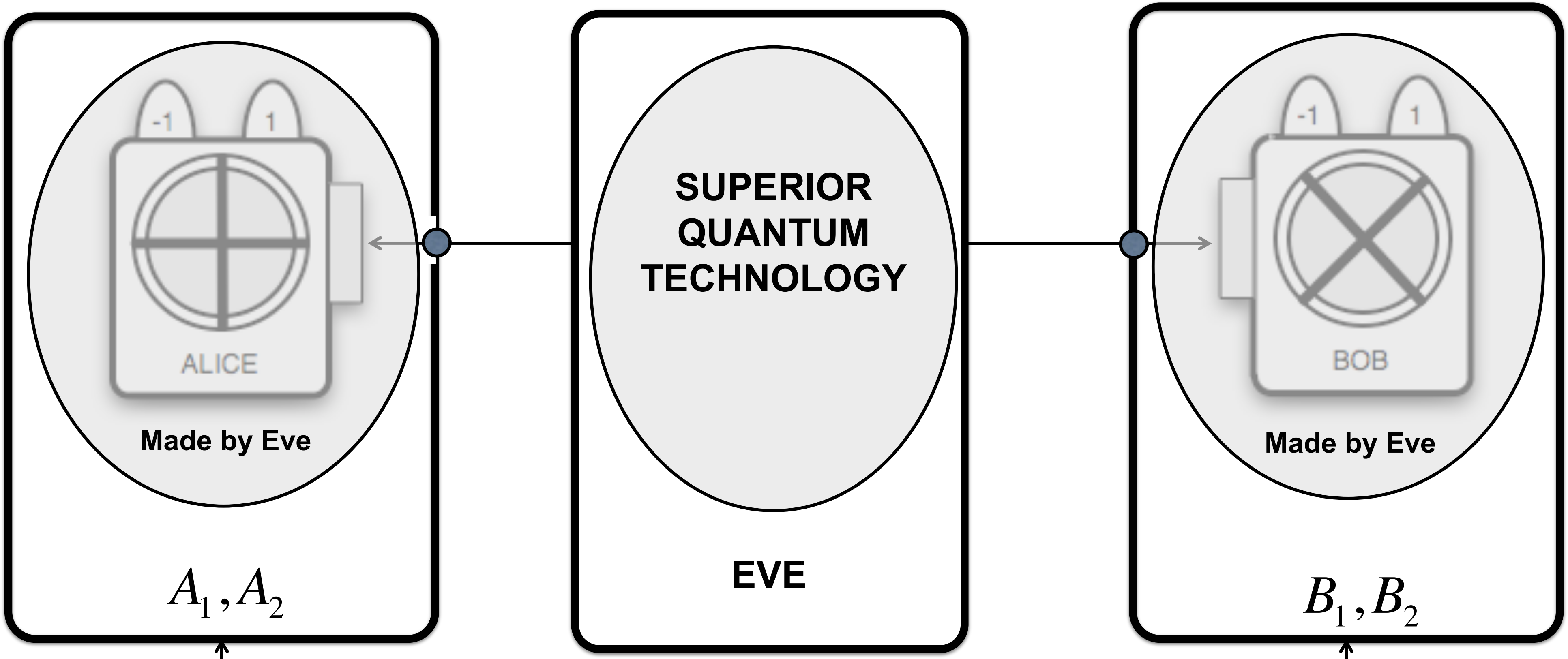
Correlations galore



Convex set of non-signaling correlations

$$S = \langle A_1 B_1 \rangle + \langle A_1 B_2 \rangle + \langle A_2 B_1 \rangle - \langle A_2 B_2 \rangle$$

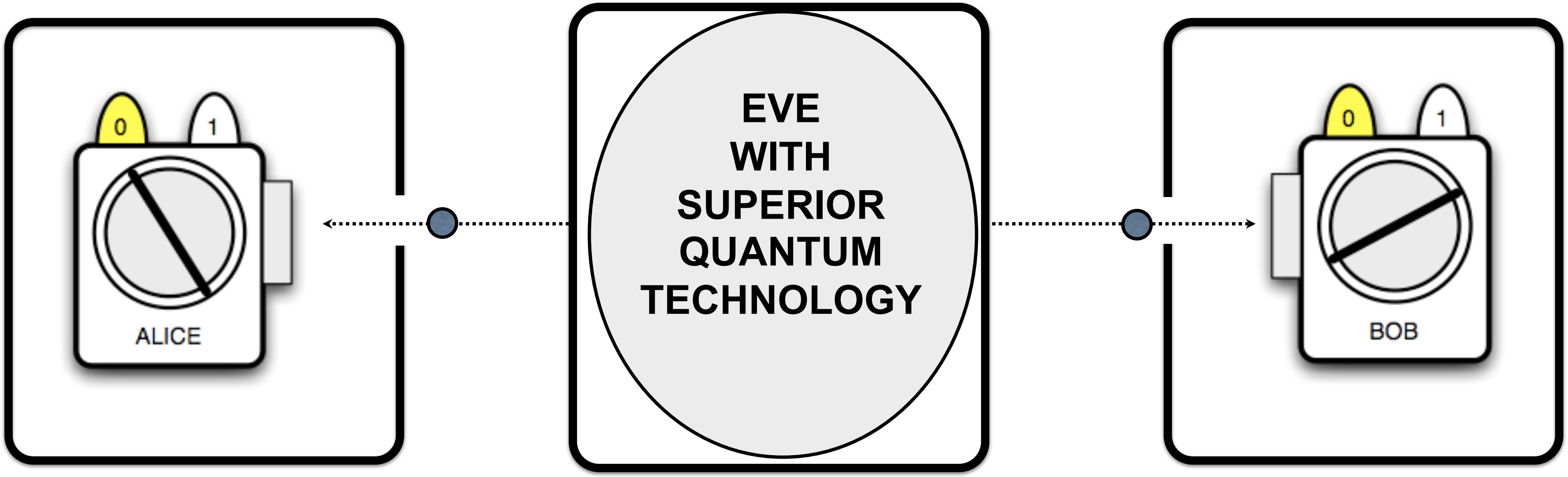
Device independent



$$\langle S \rangle = \langle A_1 B_1 \rangle + \langle A_1 B_2 \rangle + \langle A_2 B_1 \rangle - \langle A_2 B_2 \rangle$$

LOOPHOLE FREE VIOLATION OF BELL'S INEQUALITY ESSENTIAL

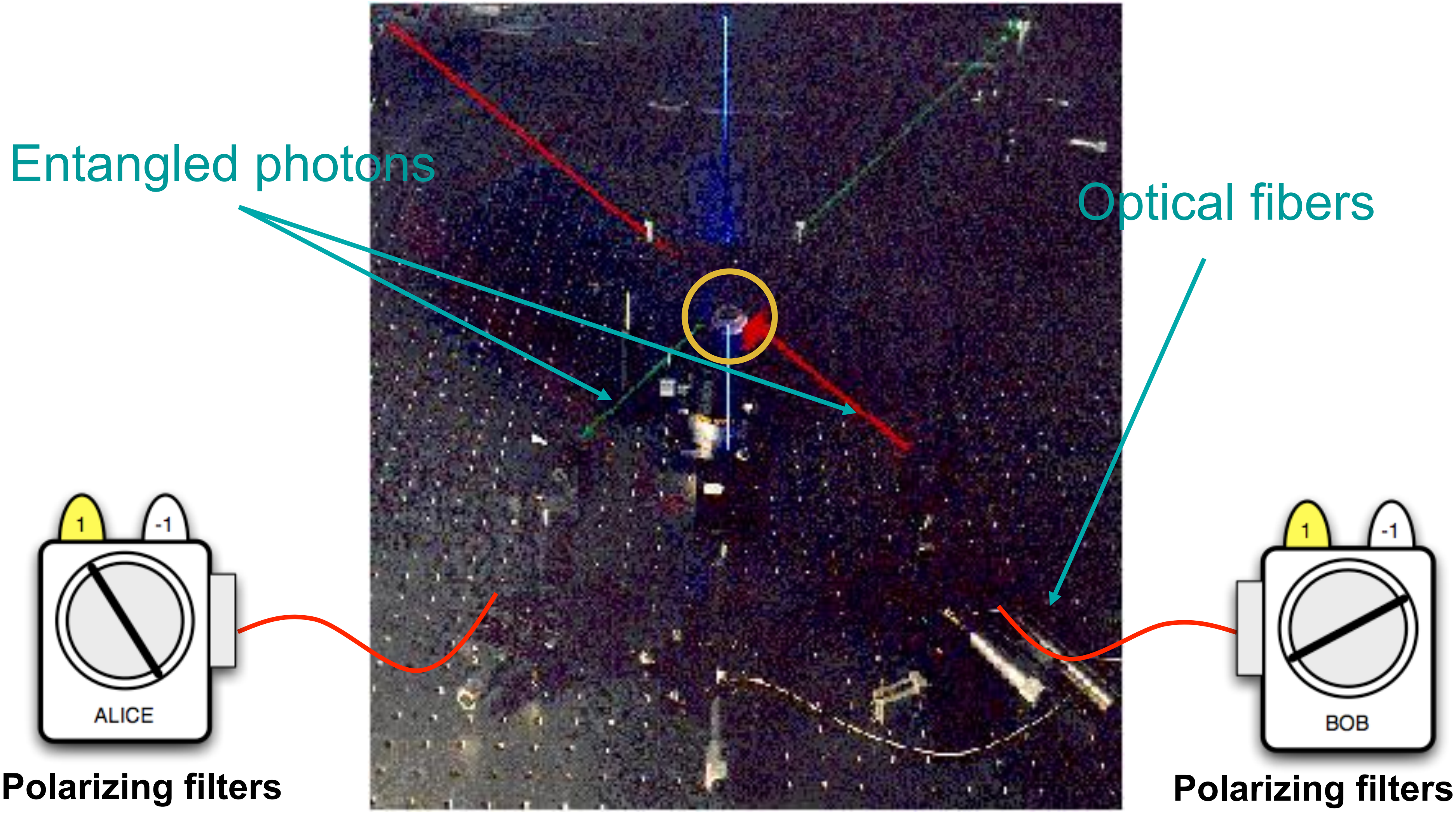
Assumptions



- Alice's and Bob's labs are secure - no information leaks
- Alice and Bob have free will and can **choose** their observables
- Alice and Bob control and trust devices in their labs
- Alice and Bob know the carriers, e.g. dimensionality of associated Hilbert space

Early days: DRA Malvern – Oxford 1990

Parametric down conversion

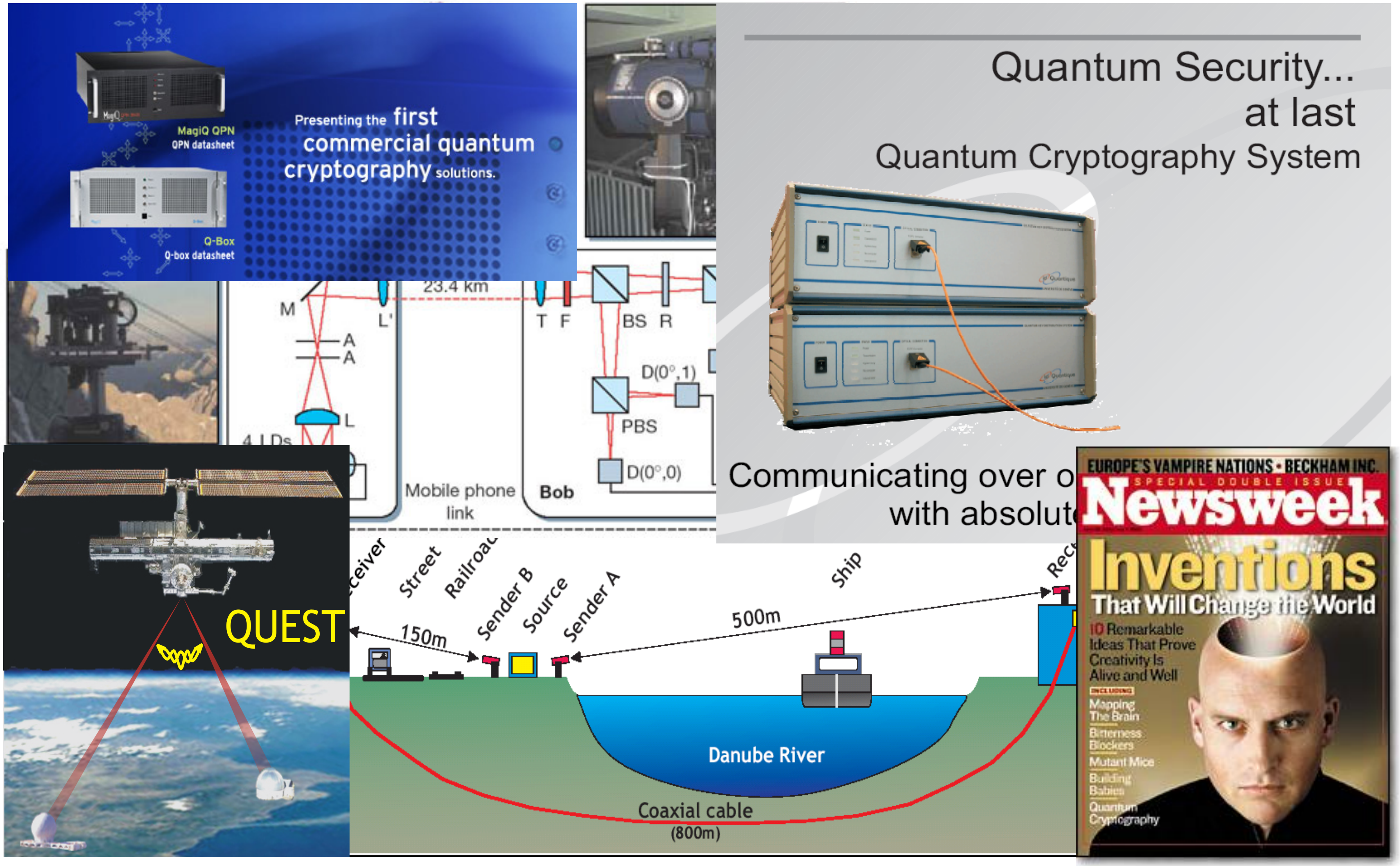


Polarizing filters & photodetectors

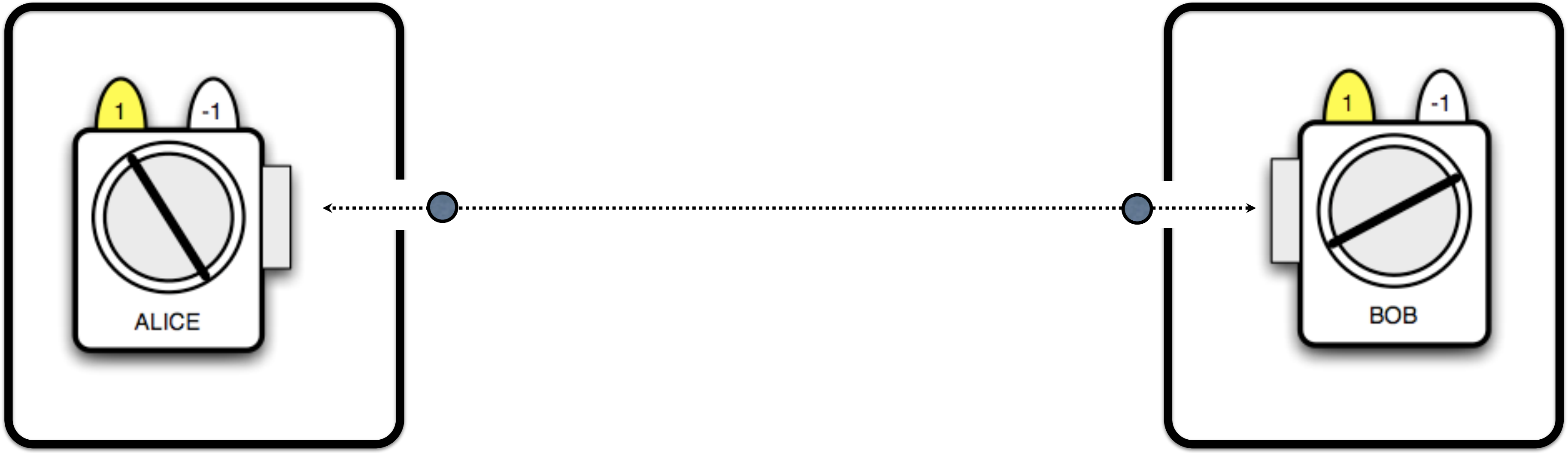
John Rarity, Paul Tapster & A.E.

Polarizing filters & photodetectors

Quantum cryptography today…

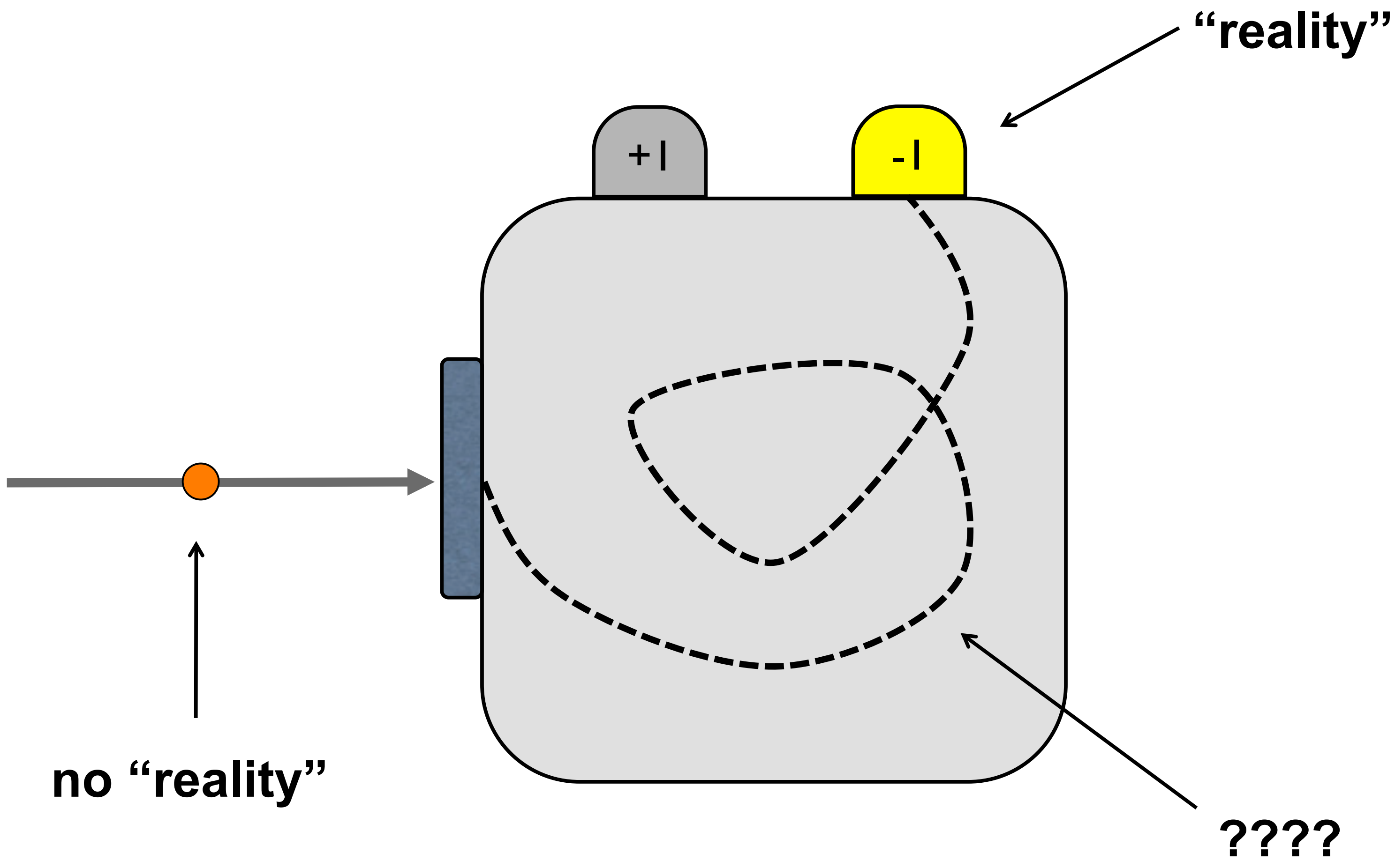


Post-quantum crypto tomorrow

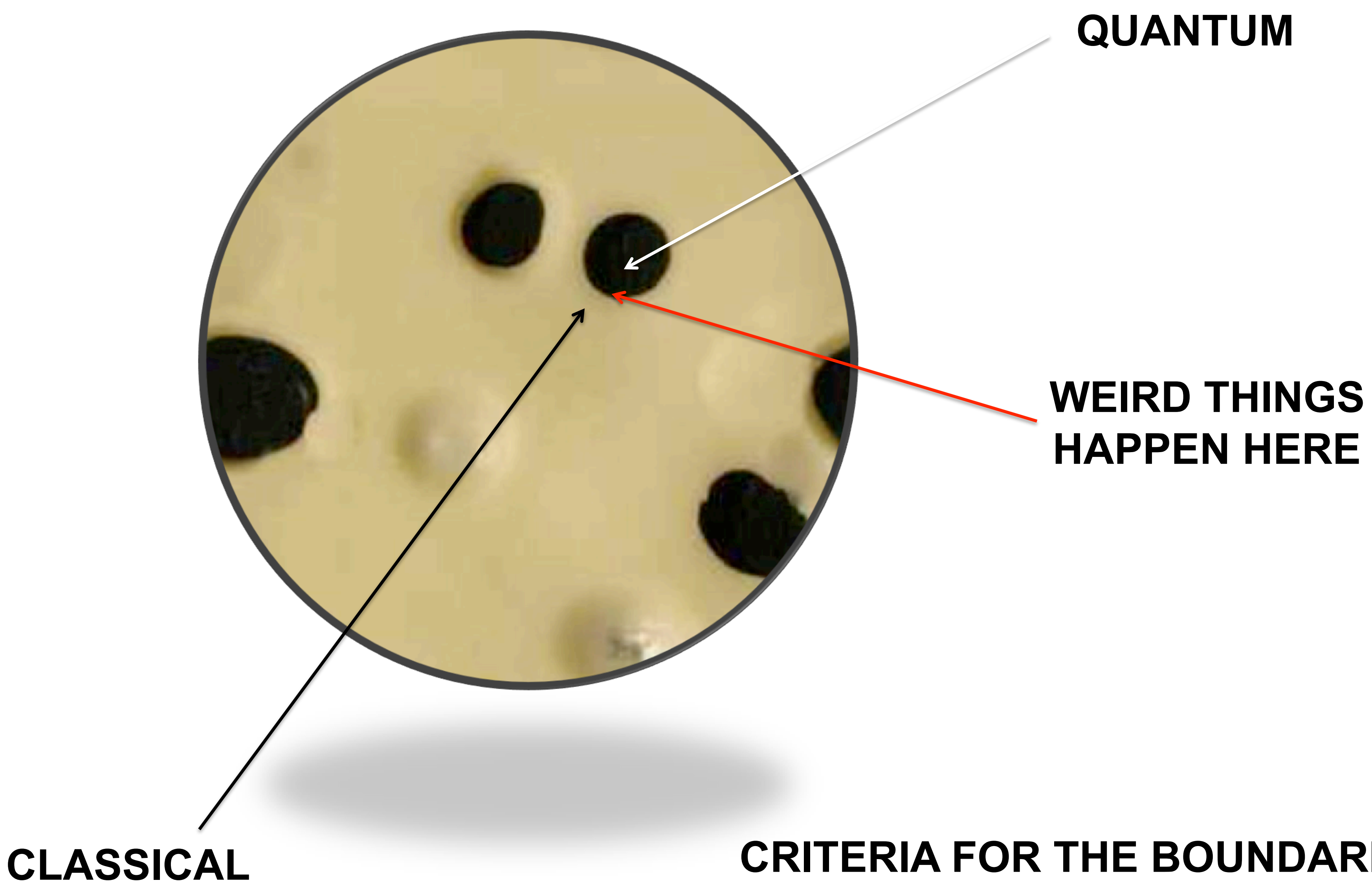


loop-hole free violation of Bell inequalities

When “reality” happens and how?

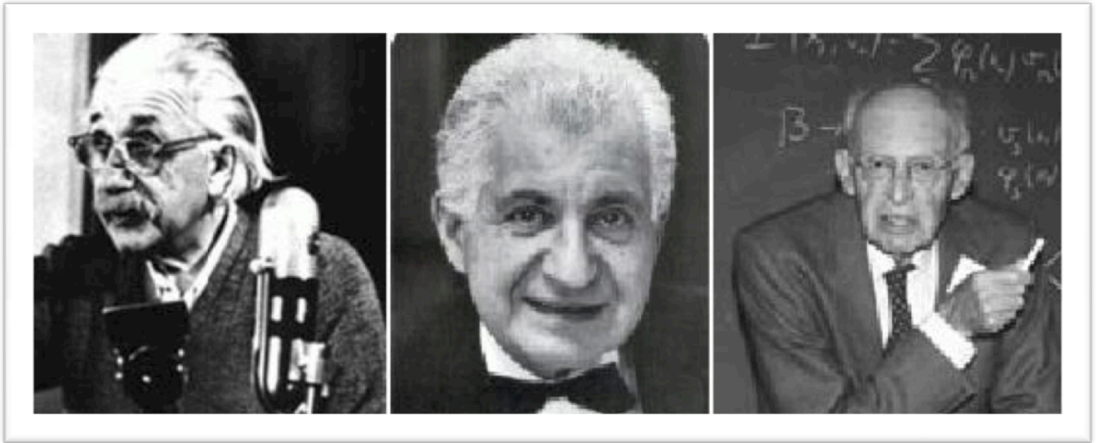


Swiss cheese reality

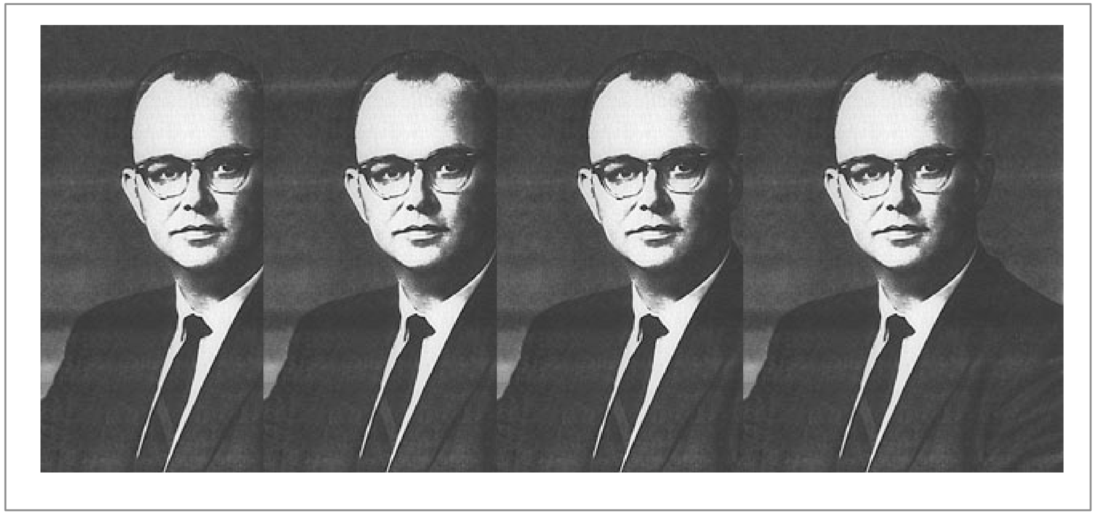


CRITERIA FOR THE BOUNDARIES ?

So what is the story with this reality?



EPR VISION OF REALITY IS TOO SIMPLISTIC



IS EVERETT'S MULTIVERSE A GOOD SUBSTITUTE?

IMPACT ON SECURITY?

To boldly go where no man has gone before…

— 4 —

WILDERNESS

— $2\sqrt{2}$ —

QUANTUM WORLD

— 2 —

CLASSICAL WORLD

$|S| = 0$