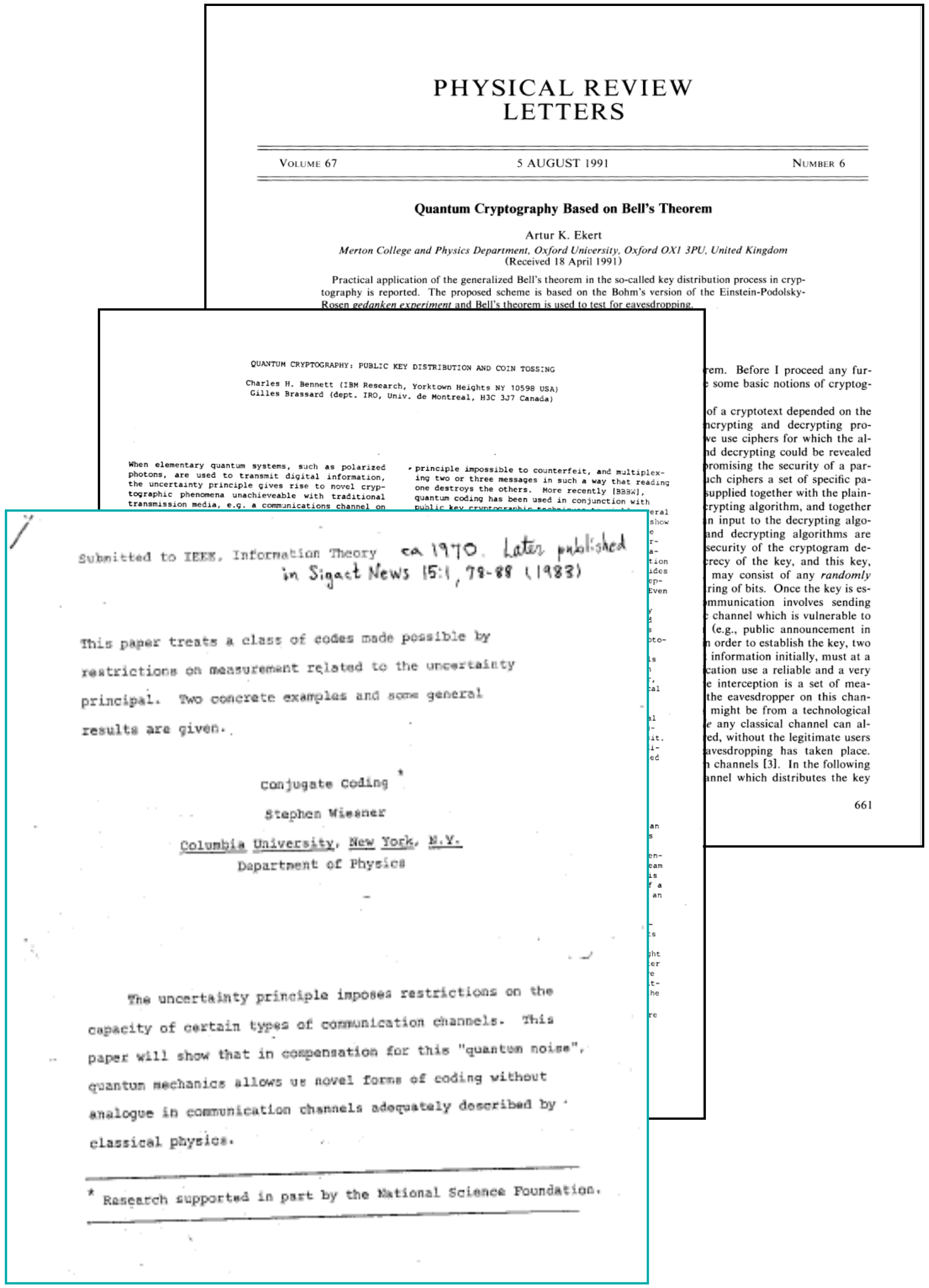
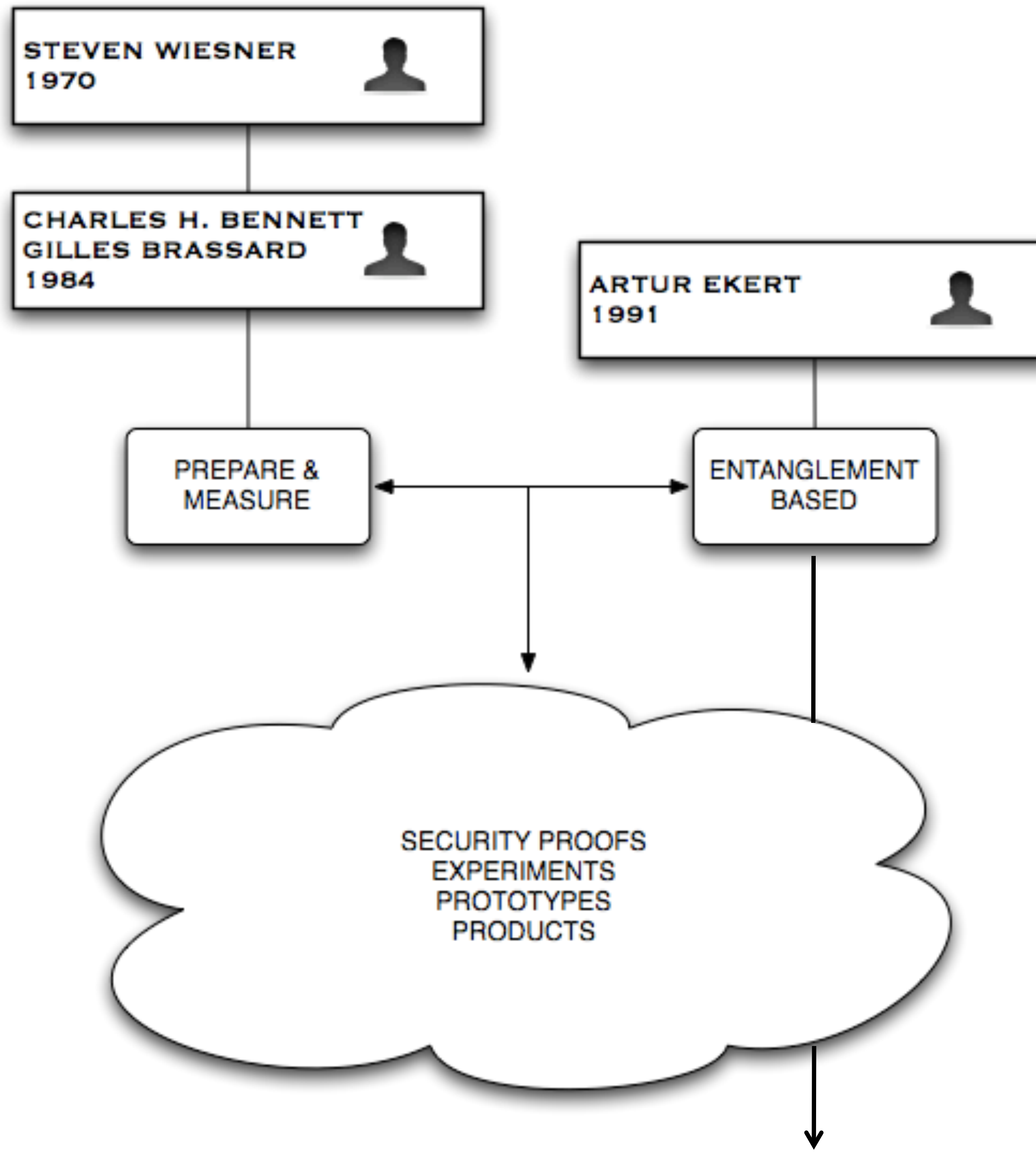
Quo Vadis
Quantum Cryptography

Artur Ekert

Origins





Device independence etc

Diverse and evolving field

QKD

OTHER PROTOCOLS

- oblivious transfer
- bit commitments
- authentication
- …

LIMITED RESOURCES

- bounded storage
- noisy memories
- …

IMPLEMENTATIONS

- detectors
- repeaters
- memories
- continuous variables
- decoy states
- hacking
- …

SECURITY PROOFS

- composable security
- de Finetti's theorems
- post-selection
- …

FOUNDATIONS

- uncertainty relations
- Bell's inequalities
- non-locality
- PR boxes
- device independence
- free will
- …

COMERCIALISATION

- design adaptation (plug and play)
- …

RELATED

- communication complexity
- privacy amplification
- error correction, hashing
- randomness extraction
- …

QUANTUM INFORMATION

- channel capacities
- …

How far can we send entangled photons?

Detection	Attenuation (optical fiber)		Attenuation (optical fiber)	Detection
η	$10^{-\frac{\alpha}{10}\frac{l}{2}}$	ν_S	$10^{-\frac{\alpha}{10}\frac{l}{2}}$	η

$$\boxed{R_1 = \nu_s \eta^2 10^{-\frac{\alpha}{10} l}}$$

l in km

$\alpha = 0.2$ dB/km telecom fiber $1.5\mu m$

$\eta = 0.5$

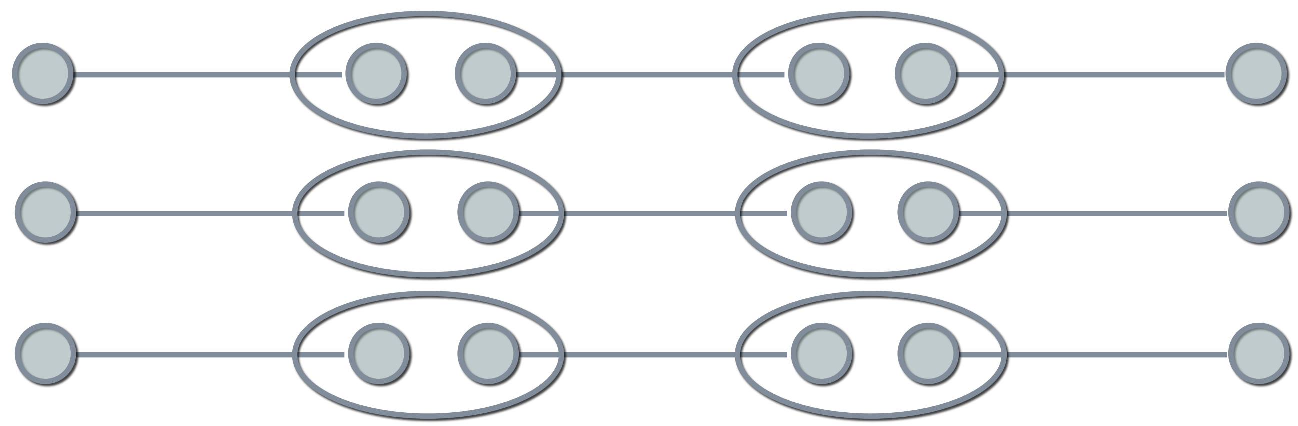
$\nu_s = 10$ GHz source of entangled photons

For l=1000 km we get one pair of entangled photons every 300 years

We can do better… (talk by Nicolas Gisin)

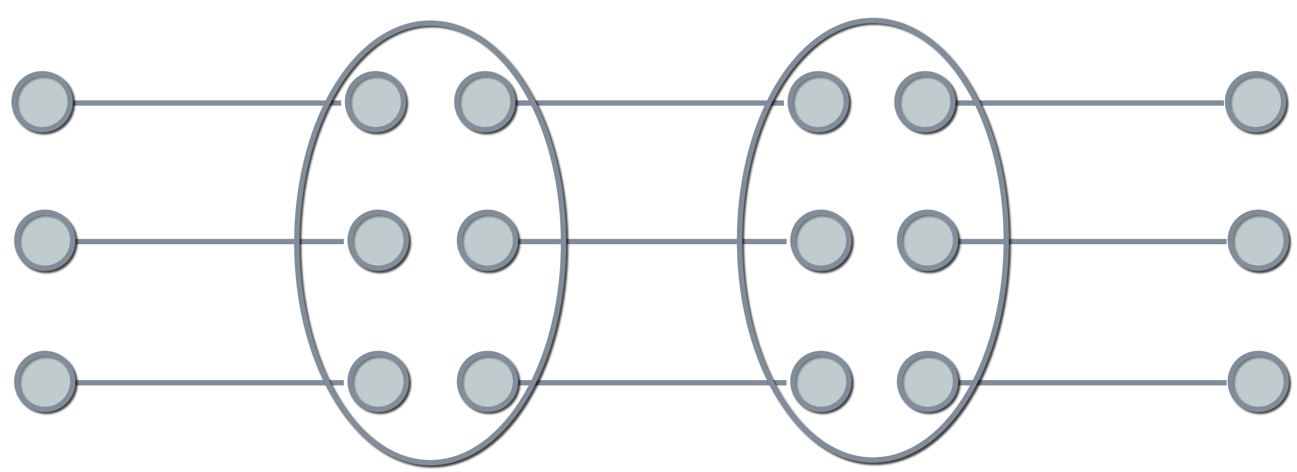
DIRECT

RELAYS



SIMULTANEOUS ENTANGLEMENT REQUIRED IN ALL LINKS
NO ADVANTAGE

REPEATERS

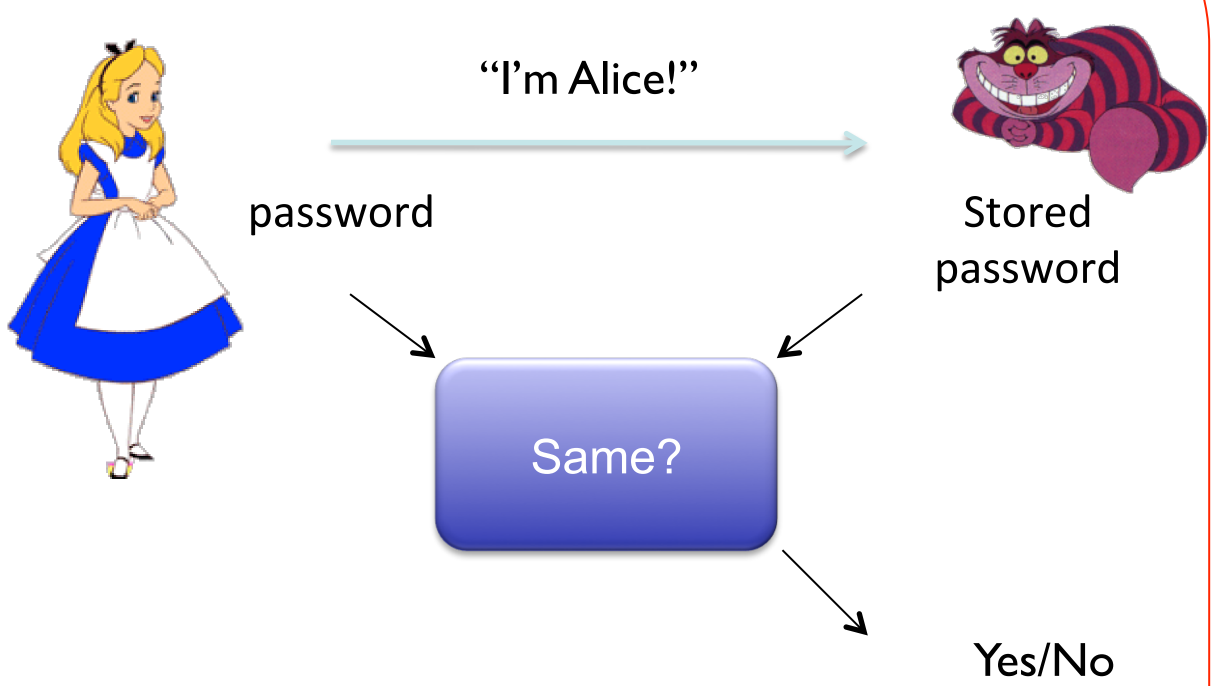


QUANTUM MEMORIES REQUIRED
BENEFITS OVER LONG DISTANCES

Cryptography from noisy storage

(talk by Stephanie Wehner)

Goal: Secure identification



Dishonest Alice:
Should not impersonate someone else.

Dishonest Bob:
Should not learn passwords of users he doesn't already know

Impossible without assumptions

Possible if cheating party's
- storage is small
(Bounded storage model)
- storage is large but noisy
(Noisy storage model)

Steady progress in analyzing more complex and sophisticated attacks. Security linked to adversary's ability to store quantum rather than classical information

Other restrictions?

Time, energy supply…

Understanding security

- Composibility issues: security criteria revisited

$$H(K) \geq n - \epsilon$$
$$I_{\mathrm{acc}}(K;E) \leq \epsilon$$

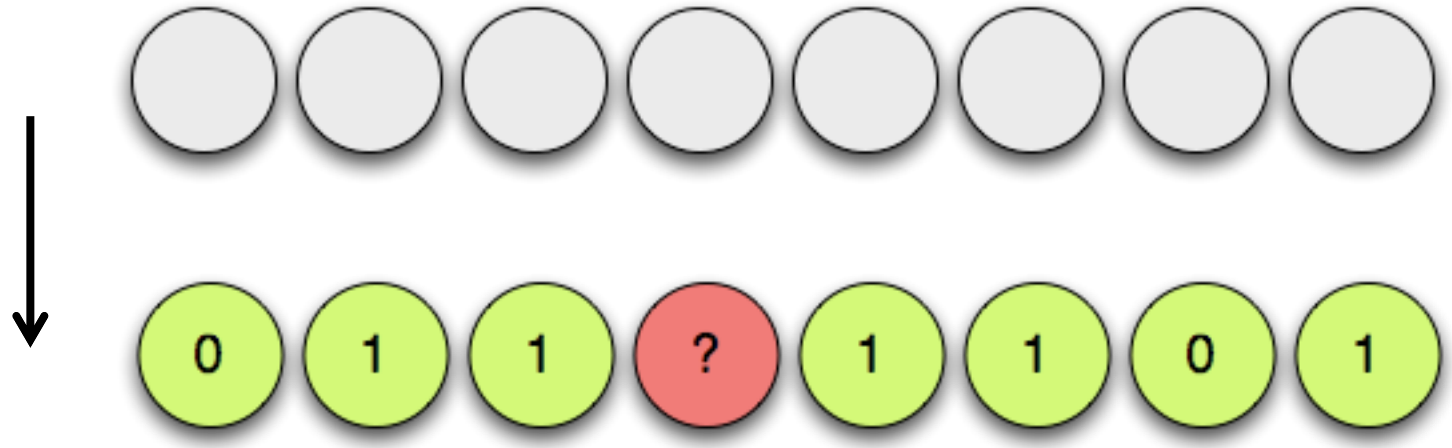
NO

$$||\rho_{KE} - \rho_U \otimes \rho_E|| \leq \epsilon$$

YES

- Simplification of security proofs: quantum de Finetti or post-selection

Locking



Information about the remaining bit may be unlocked!

$$H(K) \geq n - \epsilon$$

$$I_{\text{acc}}(K;E) \leq \epsilon$$

Small accessible information does not imply composable secrecy !

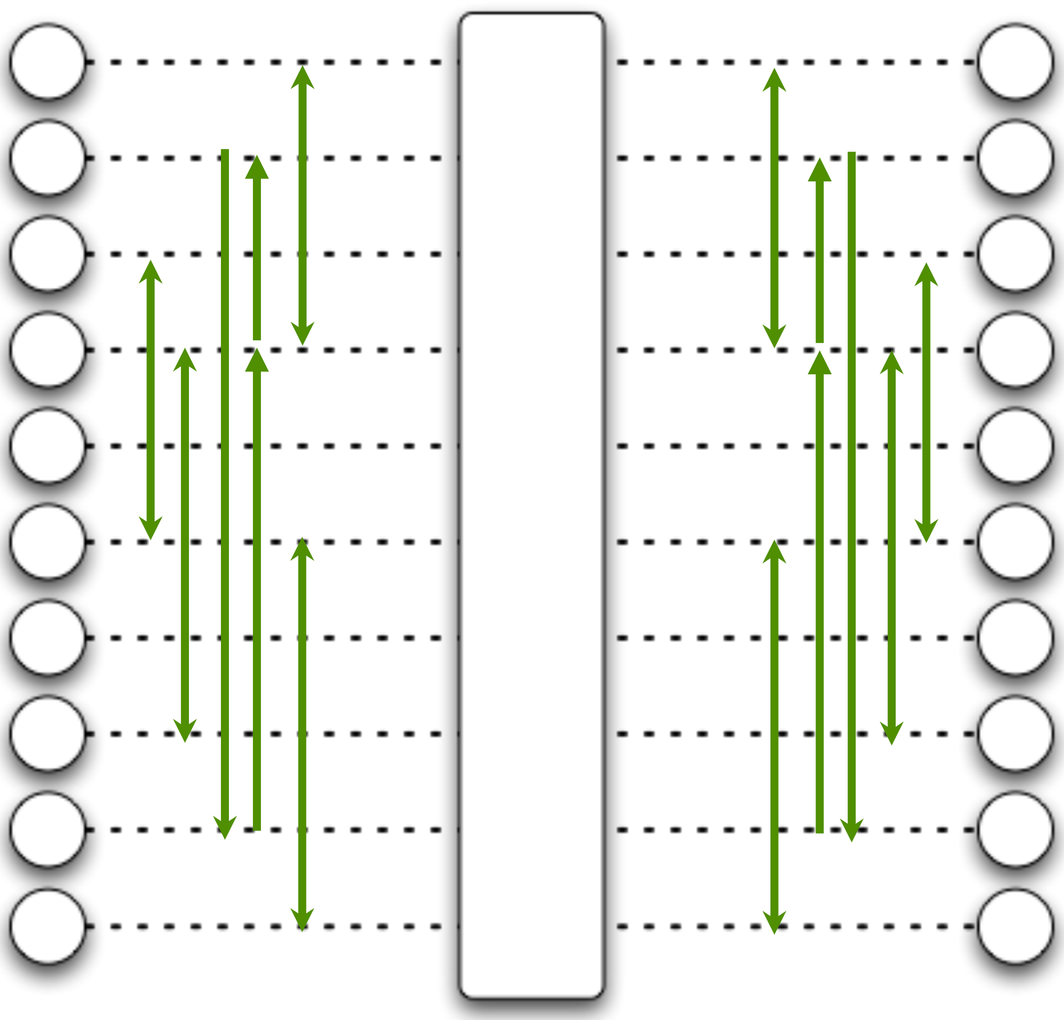
$$||\rho_{KE} - \rho_U \otimes \rho_E|| \leq \epsilon$$

which implies

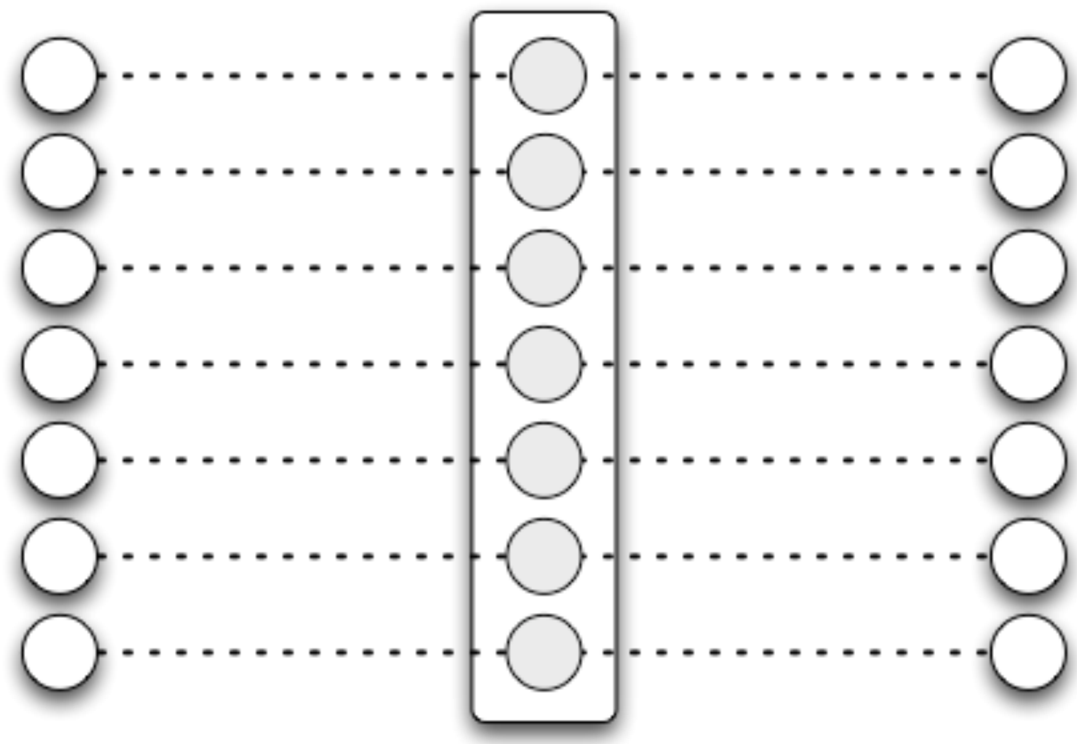
$$|P_{KE} - U_K P_E| \leq \epsilon$$

Power of random permutations

secure against collective attacks + permutations = secure against any attacks

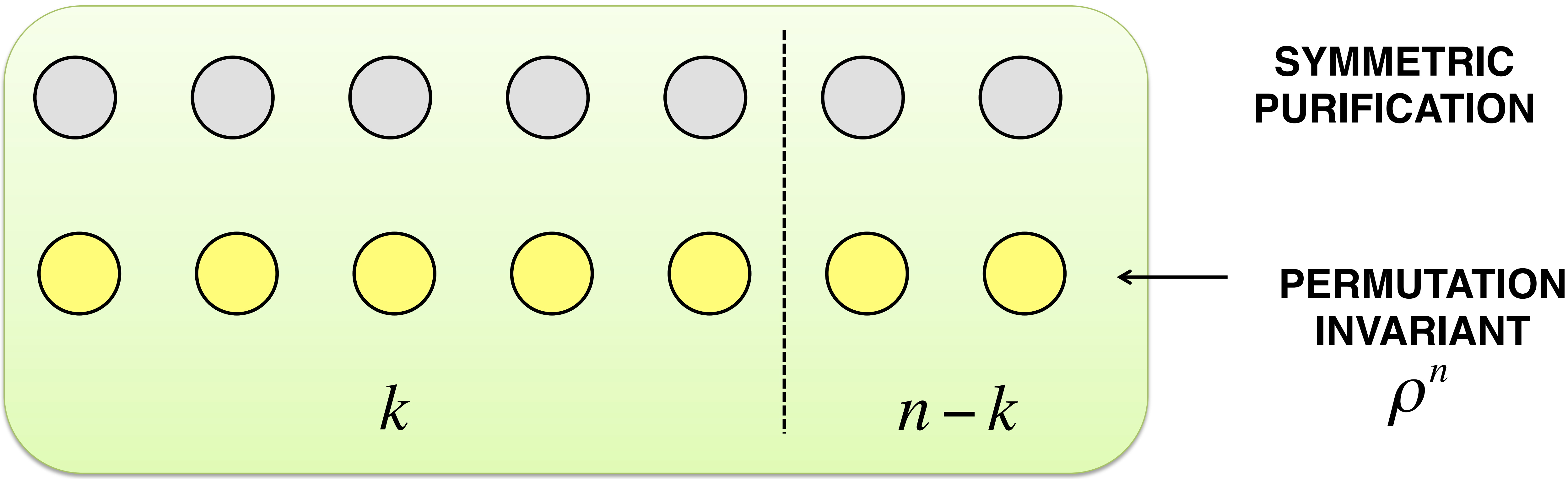


random permutation $\pi \in S_N$



$$\varrho^n \approx \sum_k \sigma_k^{\otimes n}$$

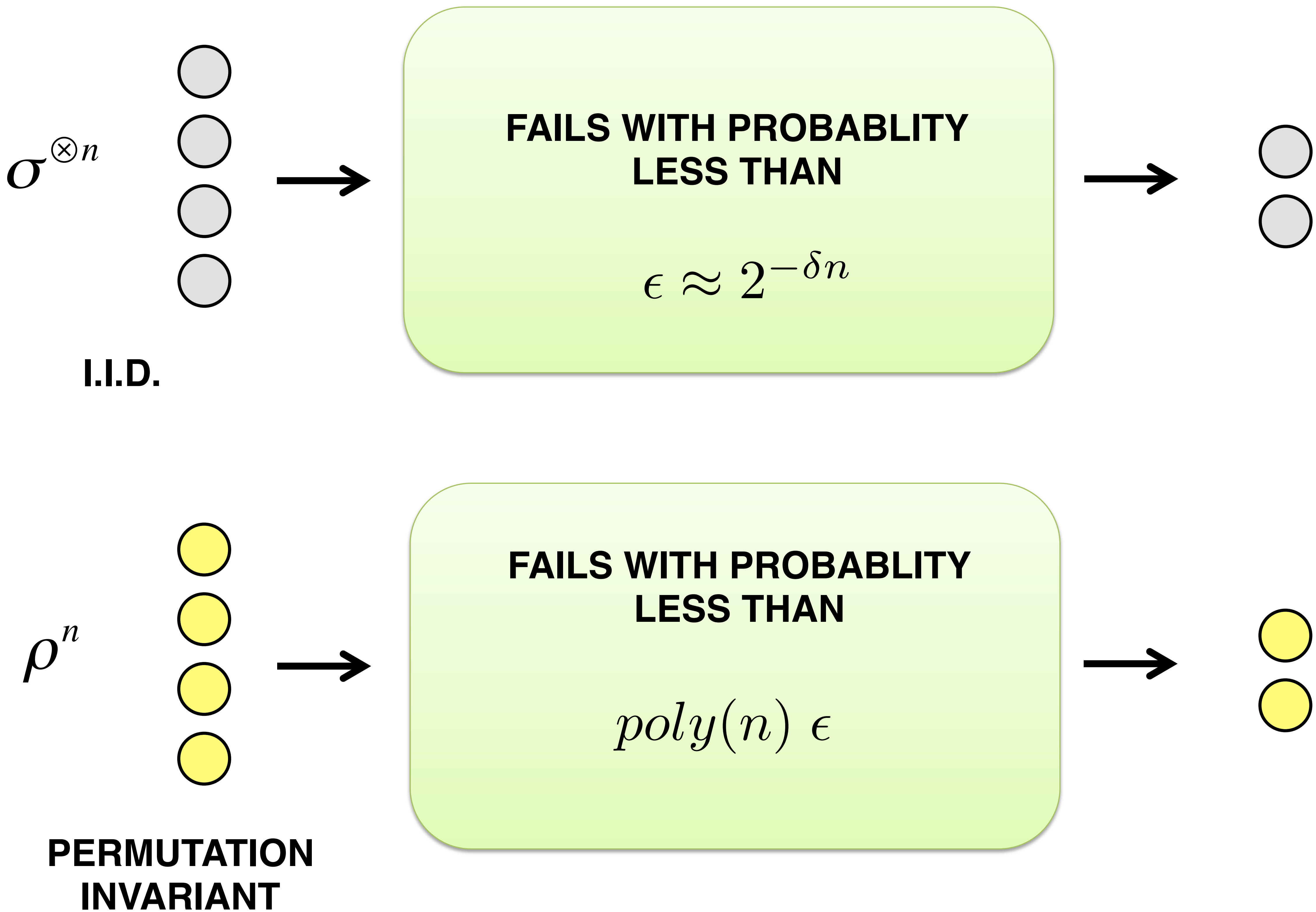
Quantum de Finetti



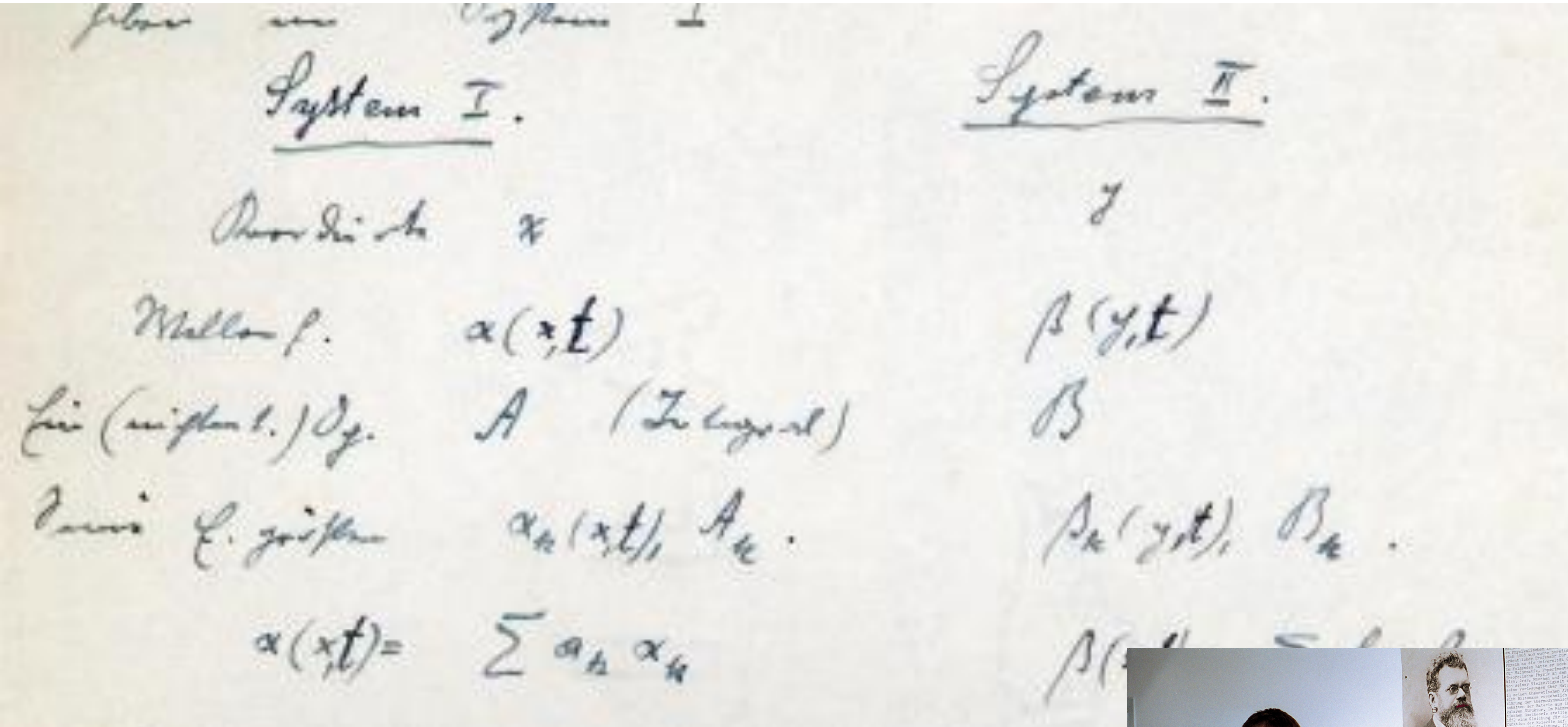
$$\left\| \rho^k - \sum_i p_i \sigma_i^{\otimes k} \right\| \leq 4d^2 \frac{k}{n}$$

- QKD application: k / n = deviation from perfect key = key rate, not good…
- Exponential version of quantum de Finetti, post-selection

Post-selection…



Entanglement after Schrödinger…


System I.

System II.

x

y

$\alpha(x,t)$

$\beta(y,t)$

A

B

$\alpha_k(x,t)$, A_k.

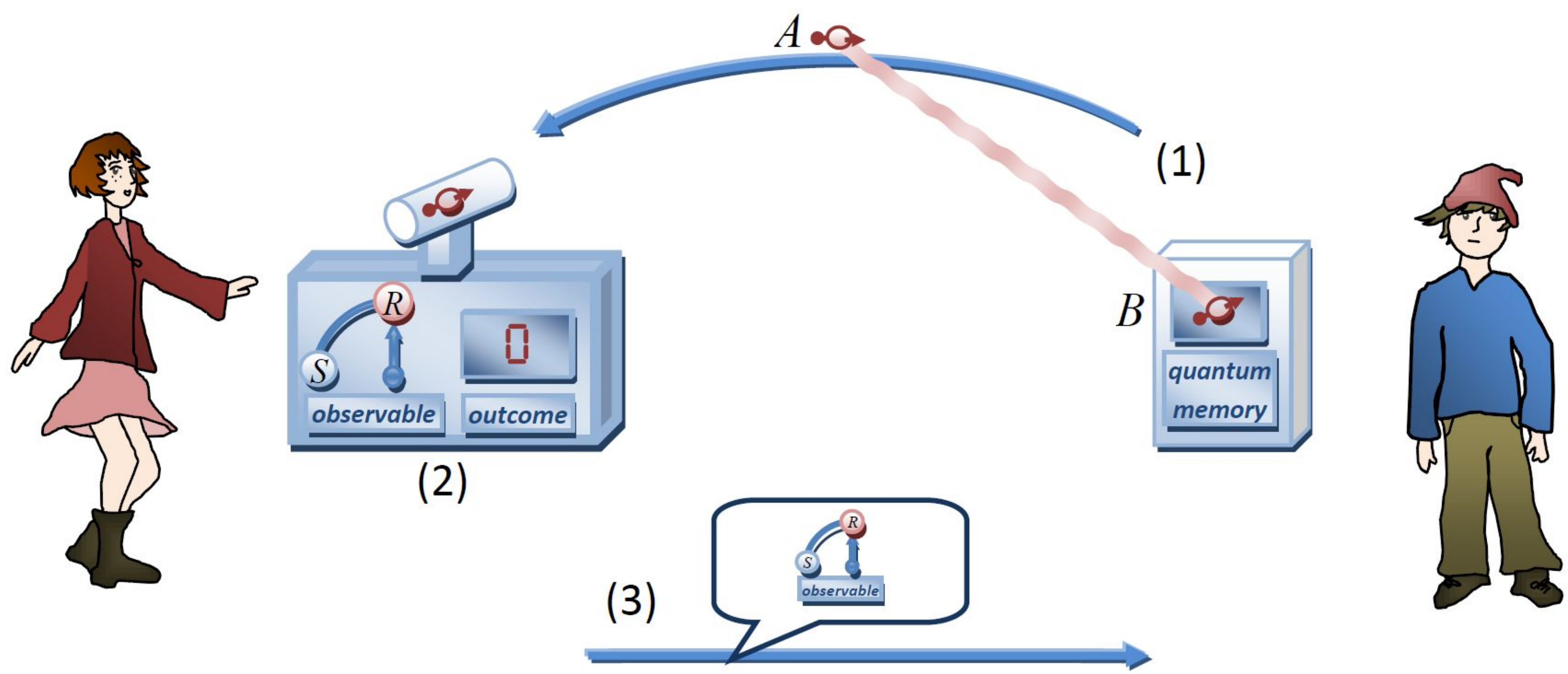
$\beta_k(y,t)$, B_k.

$\alpha(x,t) = \sum a_k \alpha_k$

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

Uncertainty after Heisenberg

(talk by Marco Tomamichel)

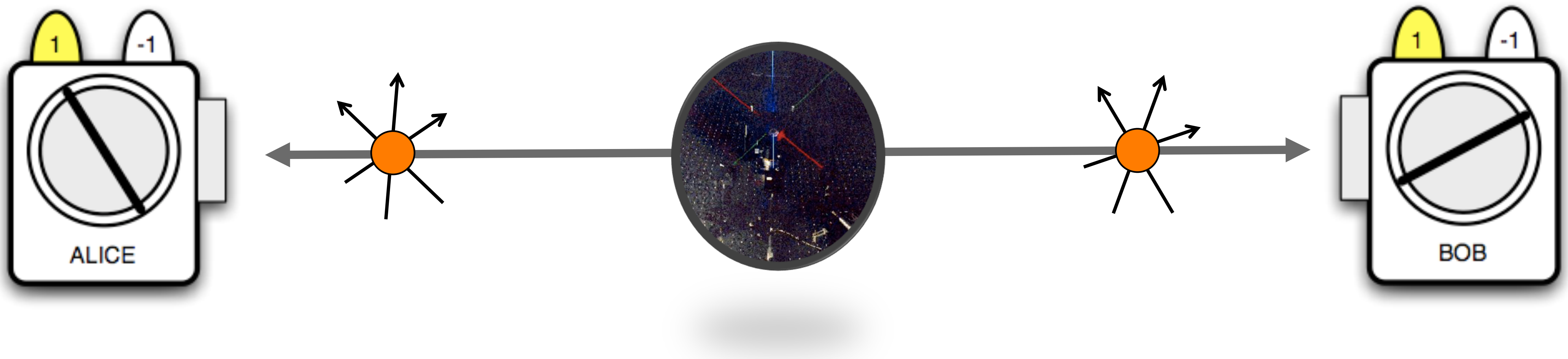


$$\Delta R \cdot \Delta S \geq \frac{1}{2}\langle [R,S] \rangle$$

$$H(R) + H(S) \geq \log_2 \frac{1}{c}$$

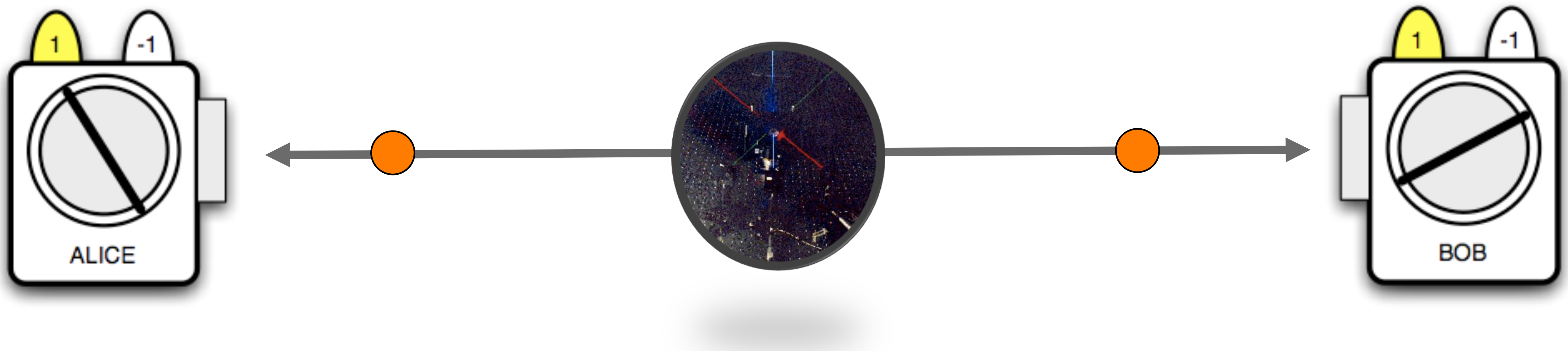
$$H(R|B) + H(S|B) \geq \log_2 \frac{1}{c} + H(A|B)$$

EPR: worry about reality



Do photons have predetermined values of polarizations?

Long mileage out of simple idea…



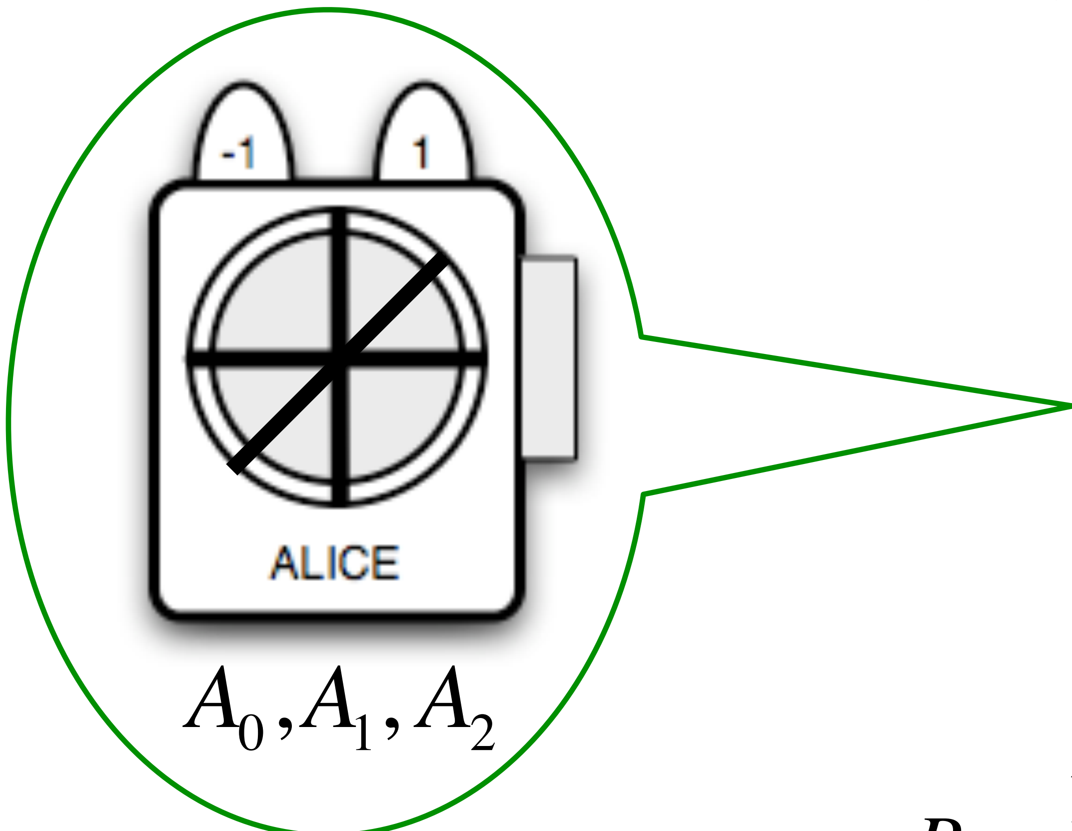
PHOTONS DO NOT CARRY PREDETERMINED VALUES OF POLARIZATIONS

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

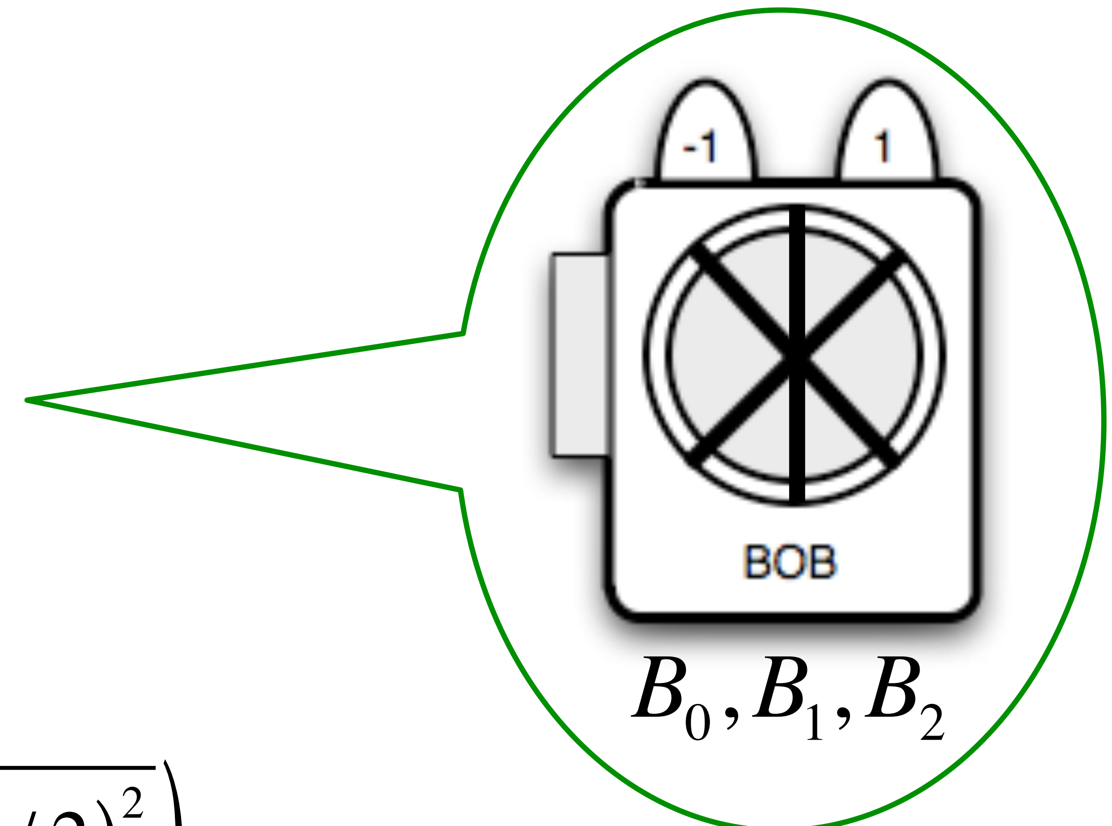
TESTING FOR THE VIOLATION OF BELL’S INEQUALITIES = TESTING FOR EAVESDROPPING

Device independent

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



EVE

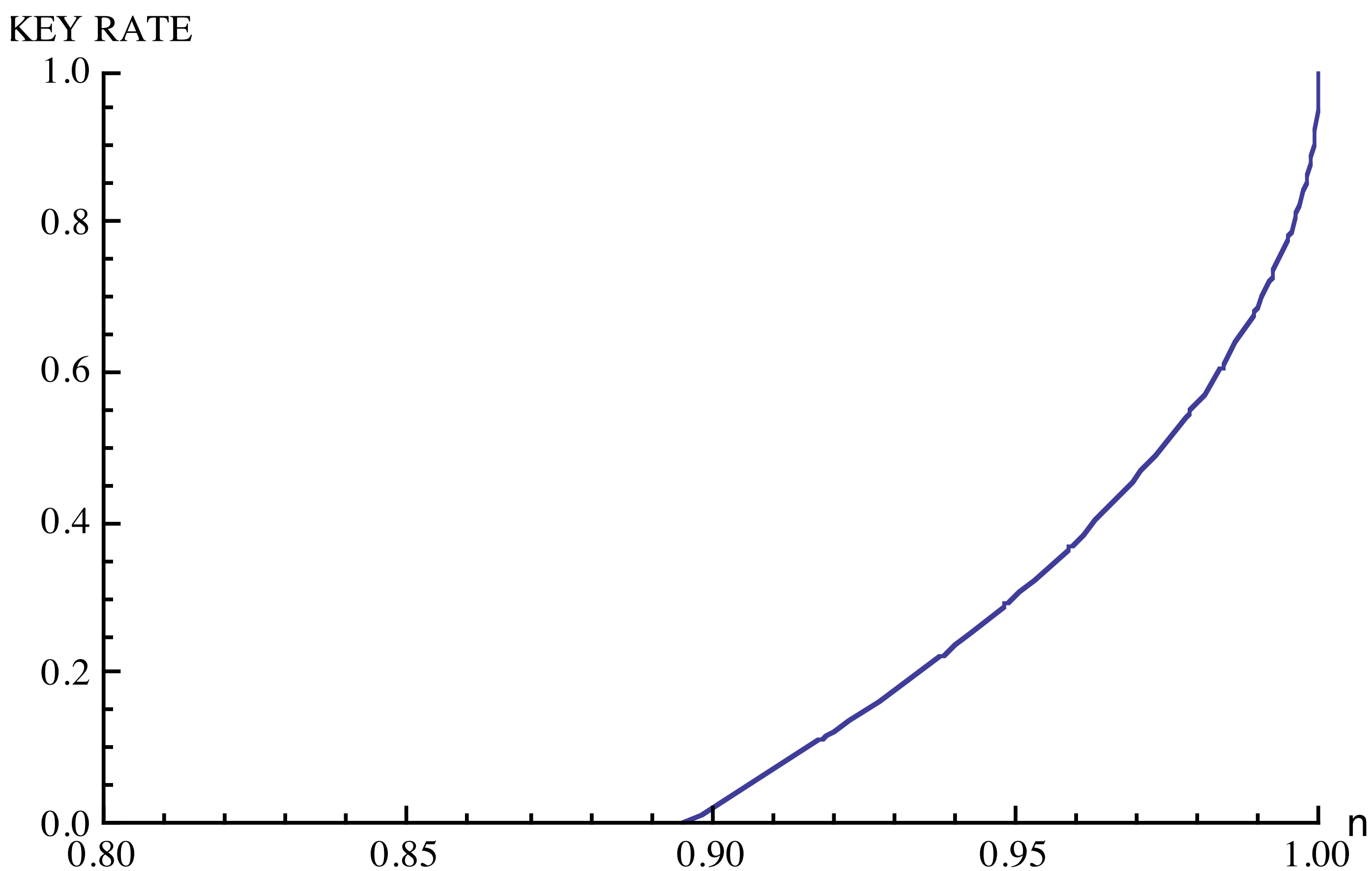


$$P_g \le \frac{1}{2}\left(1 + \sqrt{2 - (S/2)^2}\right)$$

$$\boxed{\text{key rate} = -\log P_g - h(A \mid B)}$$

Device independent

(talk by Toni Acin)



$$\nu = \frac{S}{2\sqrt{2}}$$

$$\boxed{\text{key rate} = -\log P_g - h(A\,|\,B)}$$

$$P_g \le \frac{1}{2}\left(1 + \sqrt{2 - (S/2)^2}\right)$$

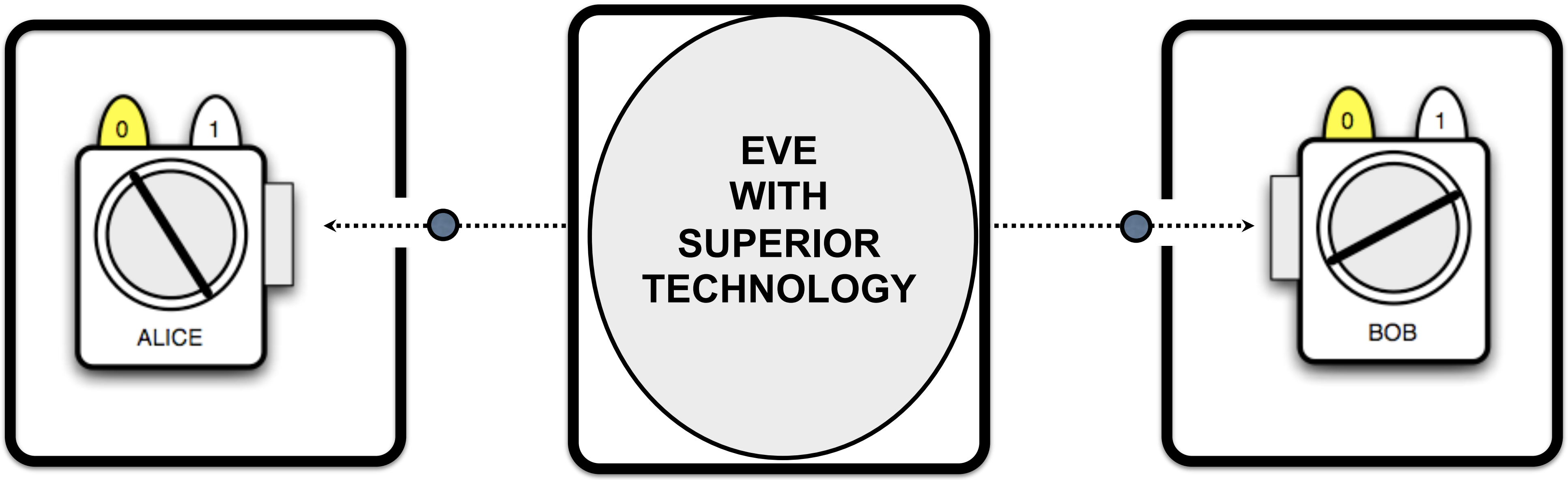
Detection efficiency issue

- Detection failures must not be ignored
- If detection fails assume outcome +1

$$\langle S \rangle = \eta^2 \underset{\underset{2\sqrt{2}}{\uparrow}}{S_2} + 2(1-\eta)\eta \underset{\underset{0}{\uparrow}}{S_1} + (1-\eta)^2 \underset{\underset{2}{\uparrow}}{S_0} \geq 2$$

$$\boxed{\eta \geq \frac{2}{1+\sqrt{2}} \approx 0.83}$$

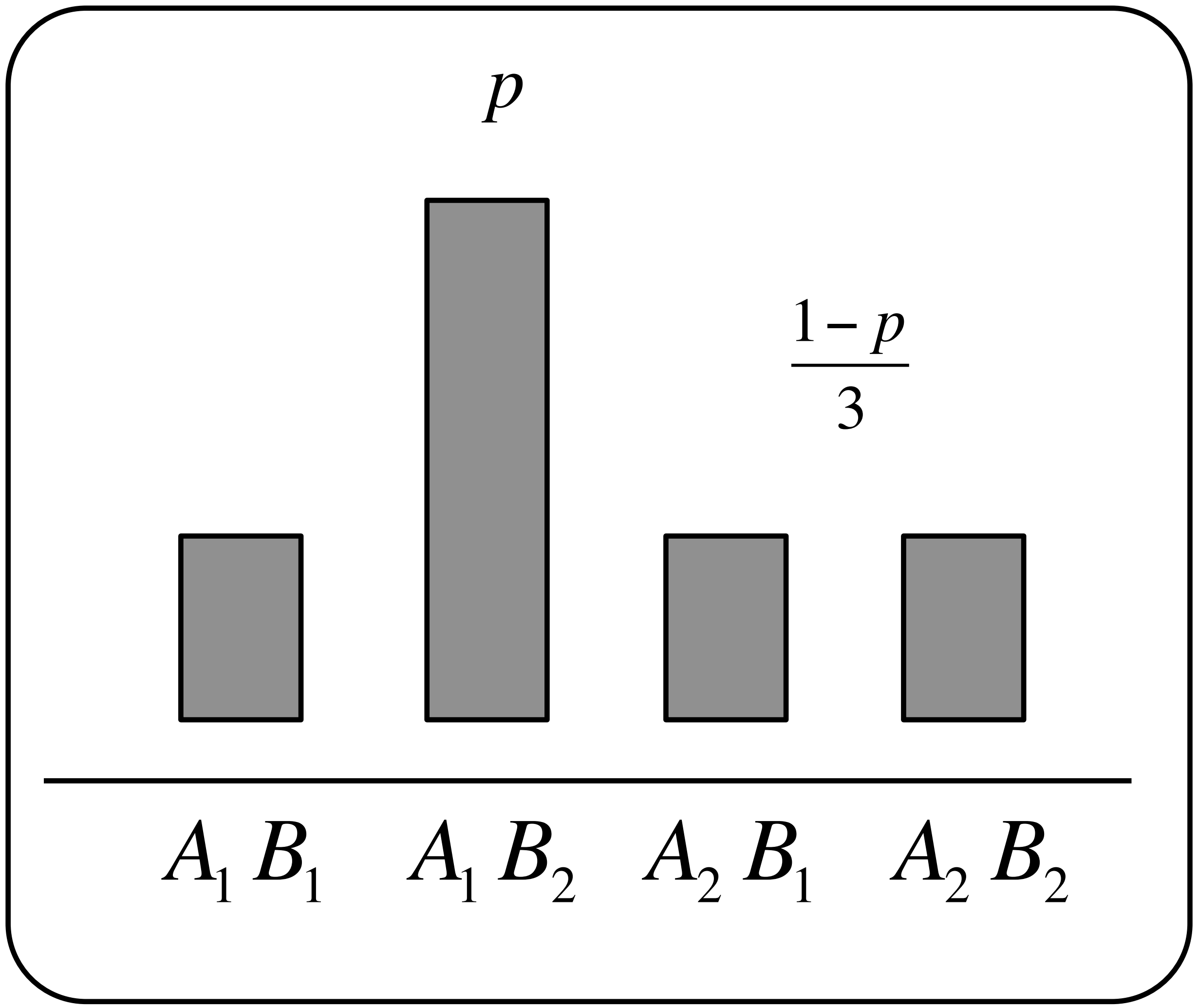
Assumptions

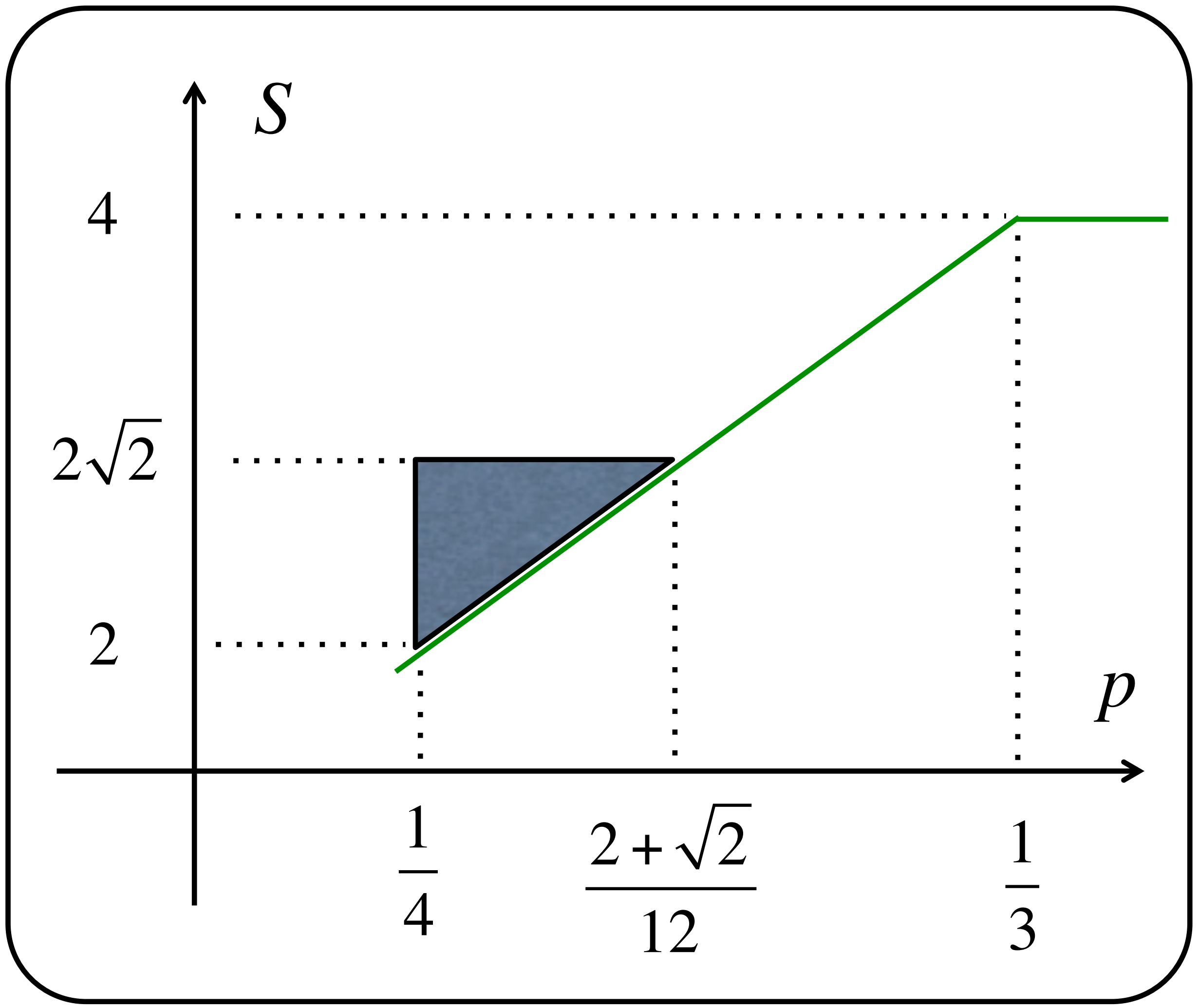


- Alice’s and Bob’s labs are secure - no information leaks
- Alice and Bob have free will and can **choose** their observables
- Alice and Bob control and trust devices in their labs
- Alice and Bob know the carriers, e.g. dimensionality of associated Hilbert space

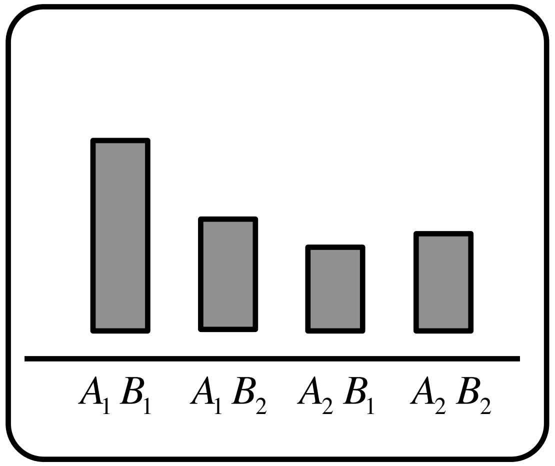
Let us get paranoid – “free will” issue…

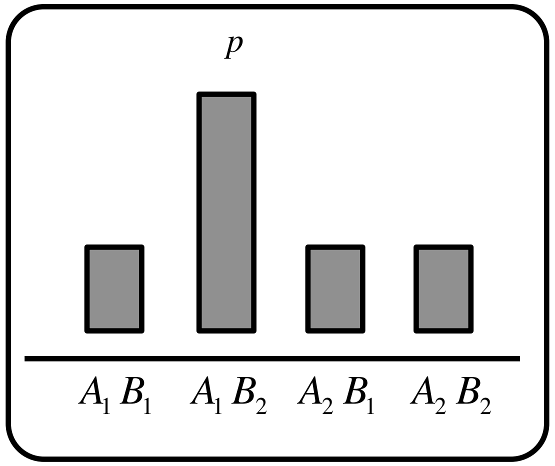
- Malicious Manipulator (MM) knows the settings

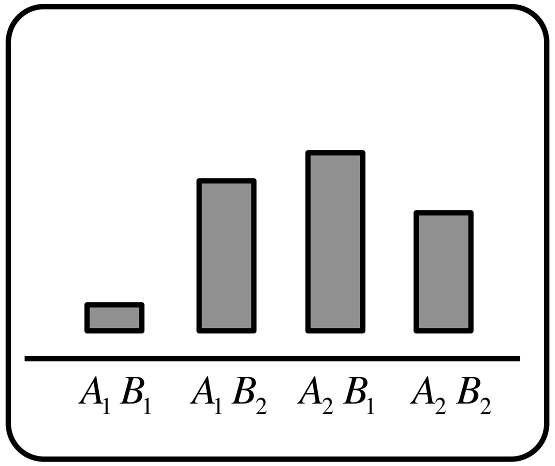


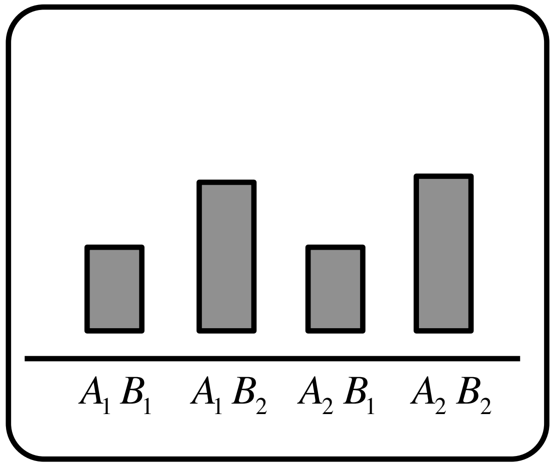


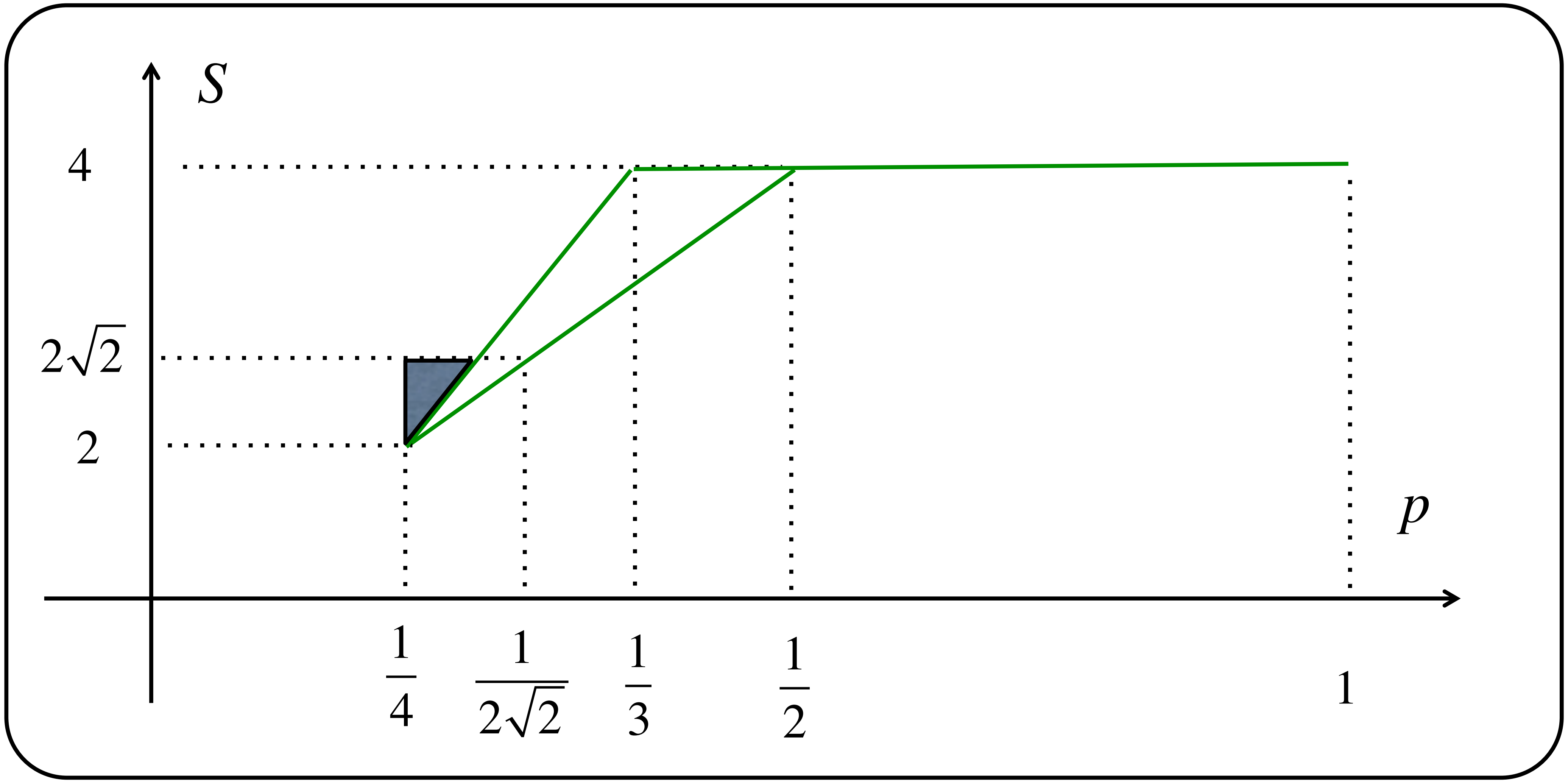
“Free will” issue…



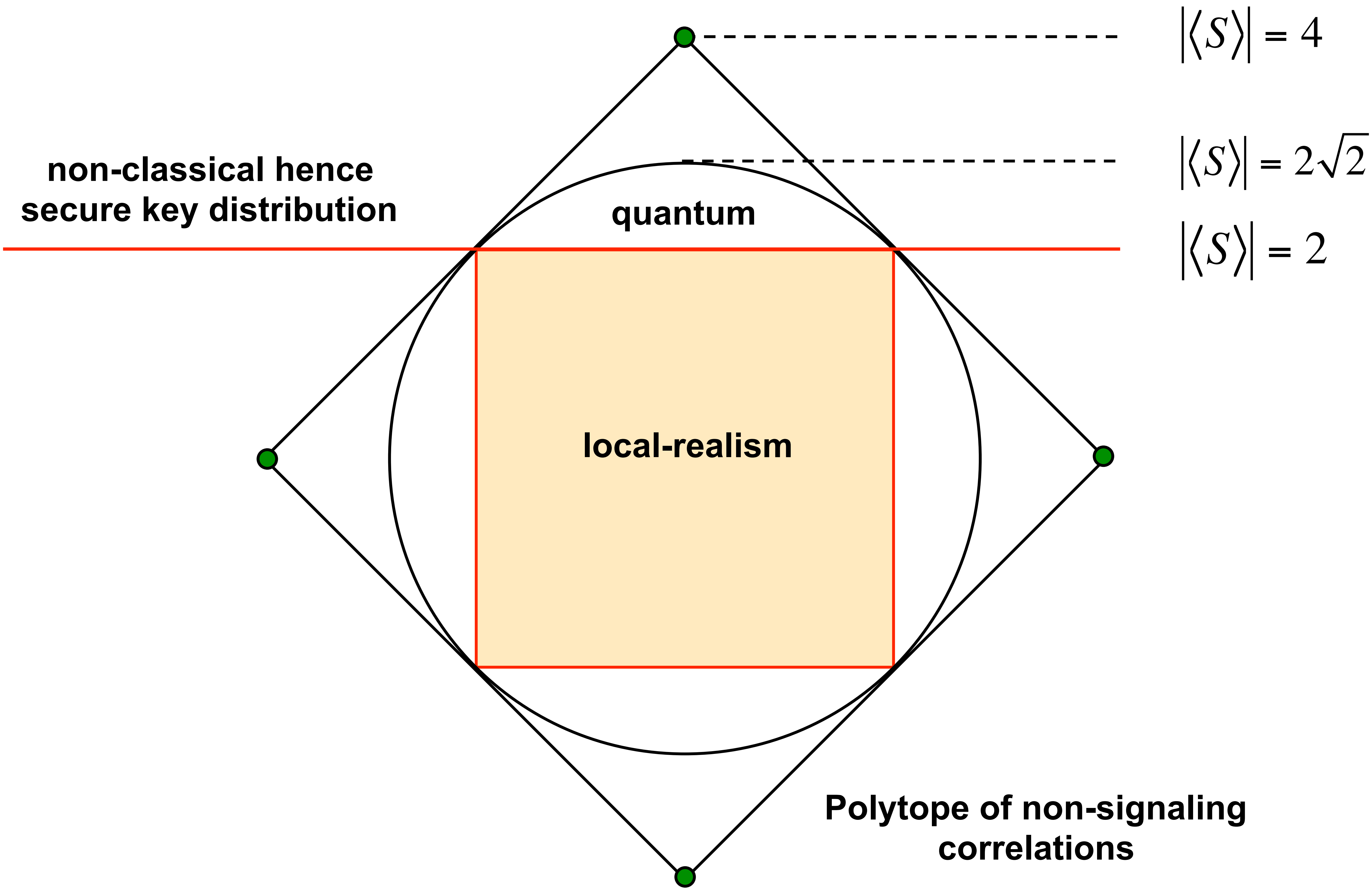








Beyond quantum…



To boldly go where no man has gone before…

4

WILDERNESS

$2\sqrt{2}$

QUANTUM WORLD

2

CLASSICAL WORLD

$|S| = 0$

Lets us get philosophical…

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.

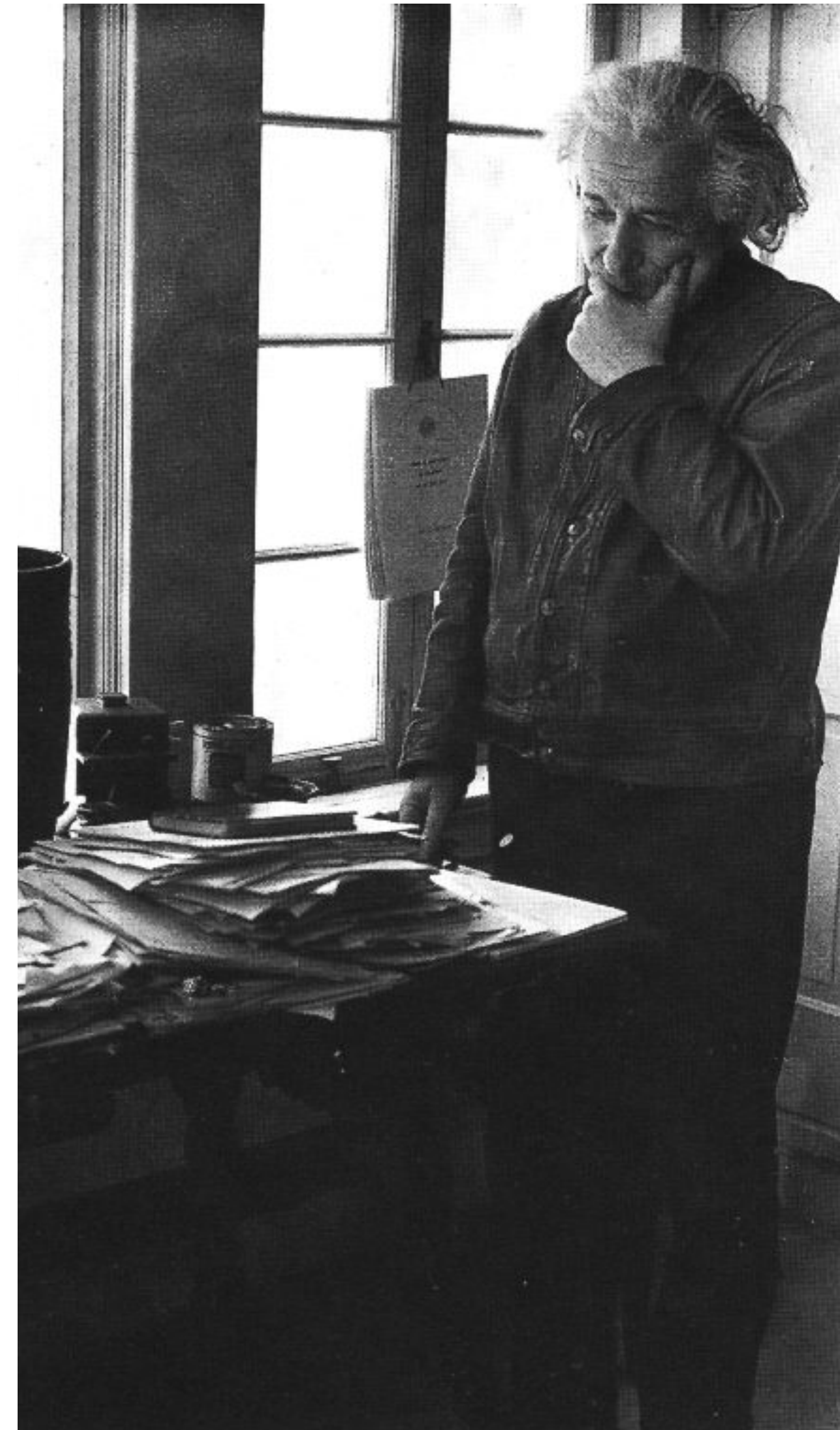
1.

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

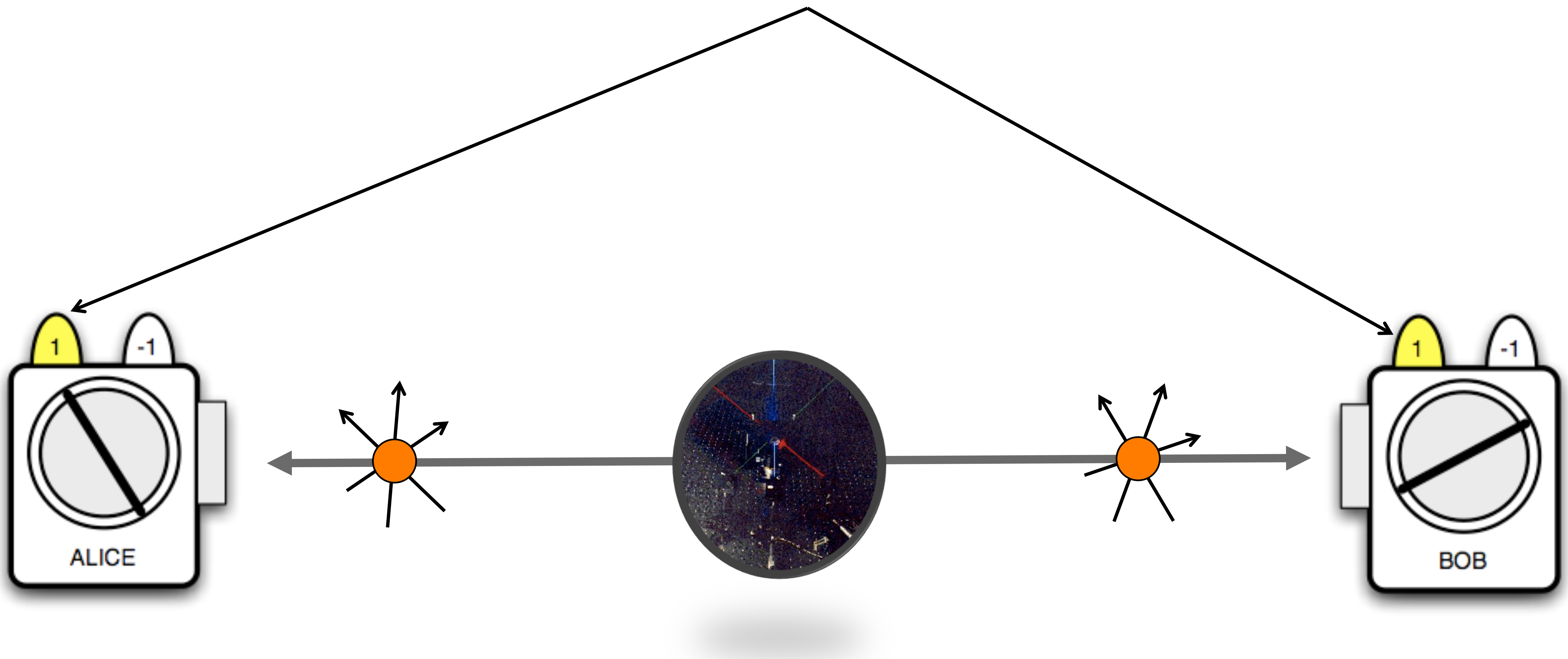


DEFINITION OF EAVESDROPPING

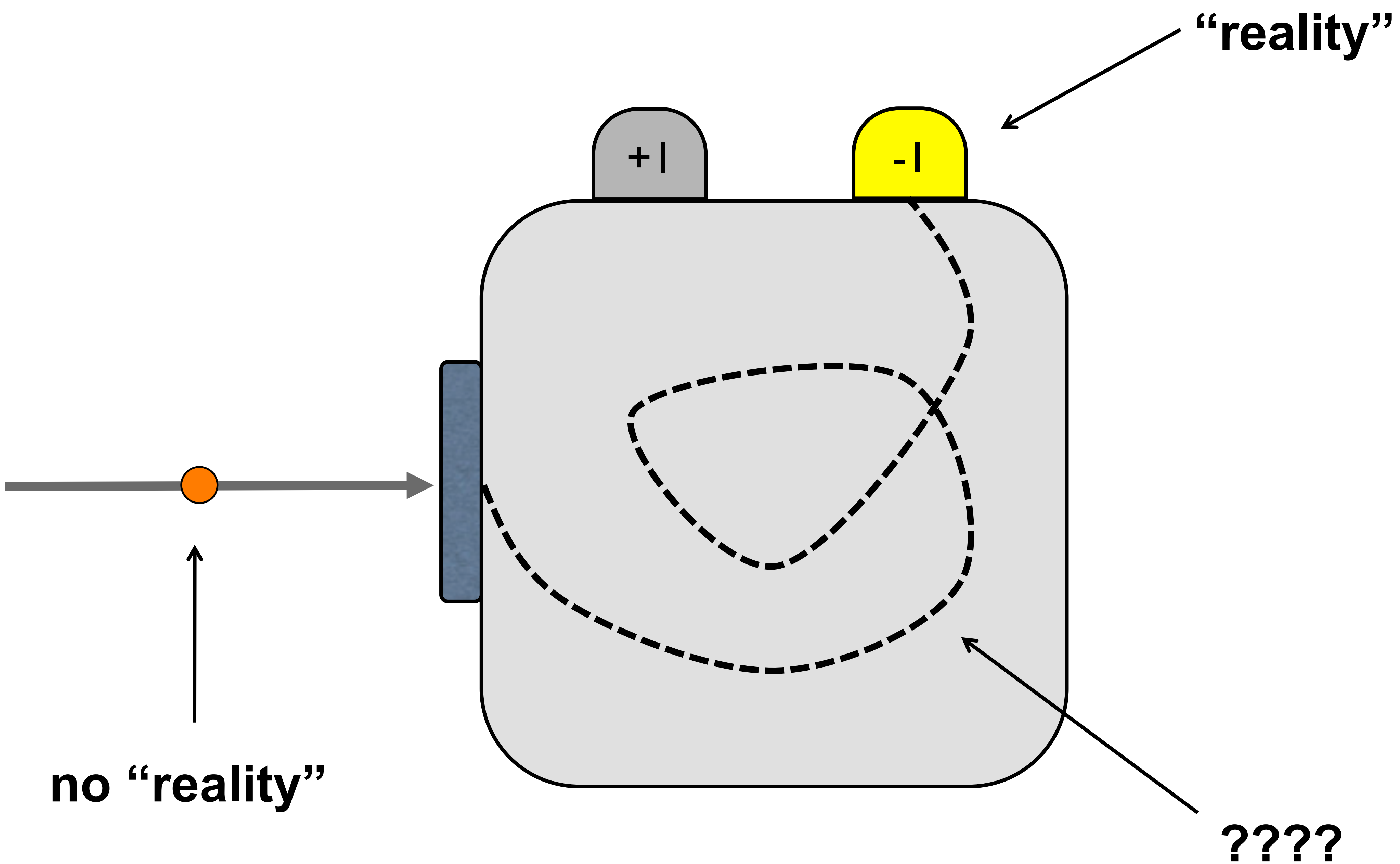
Some tacit assumptions

MEASUREMENT

Only one outcome



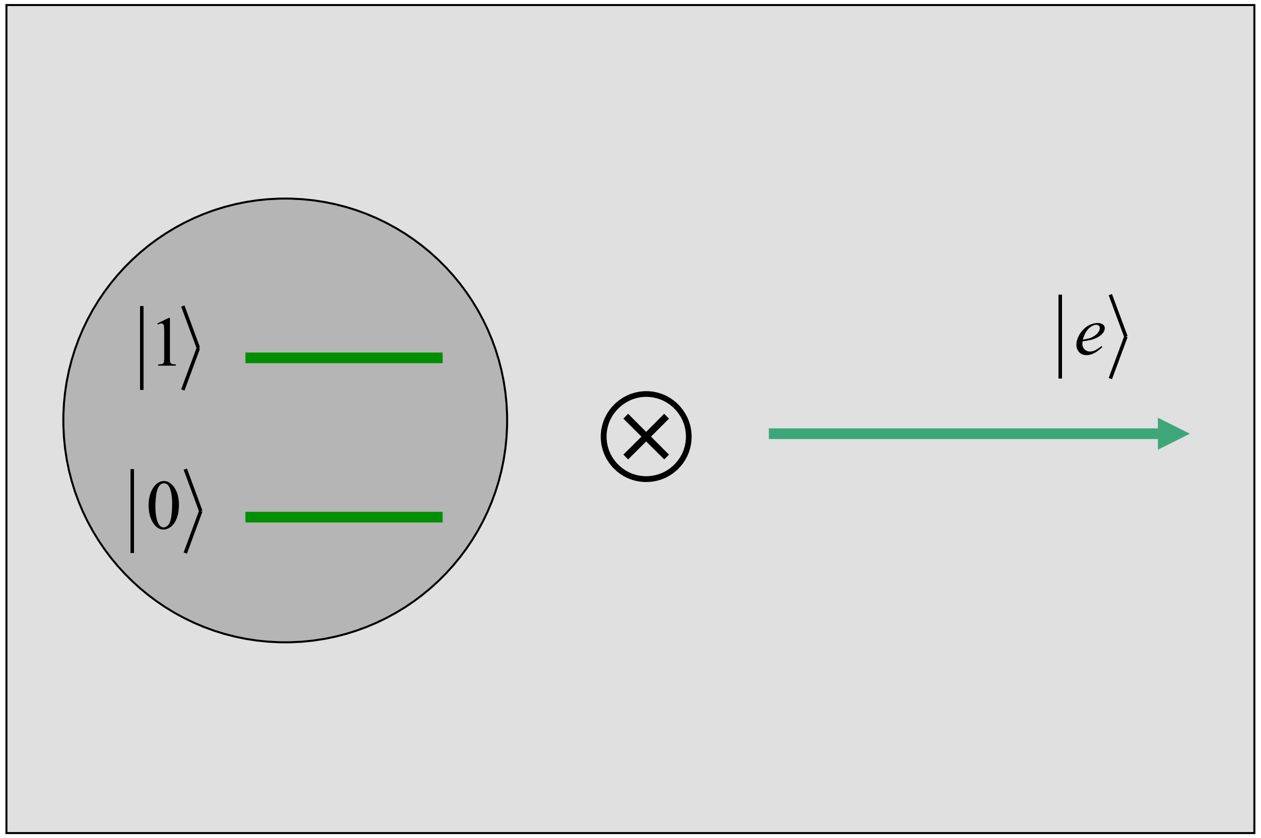
When “reality” happens and how?

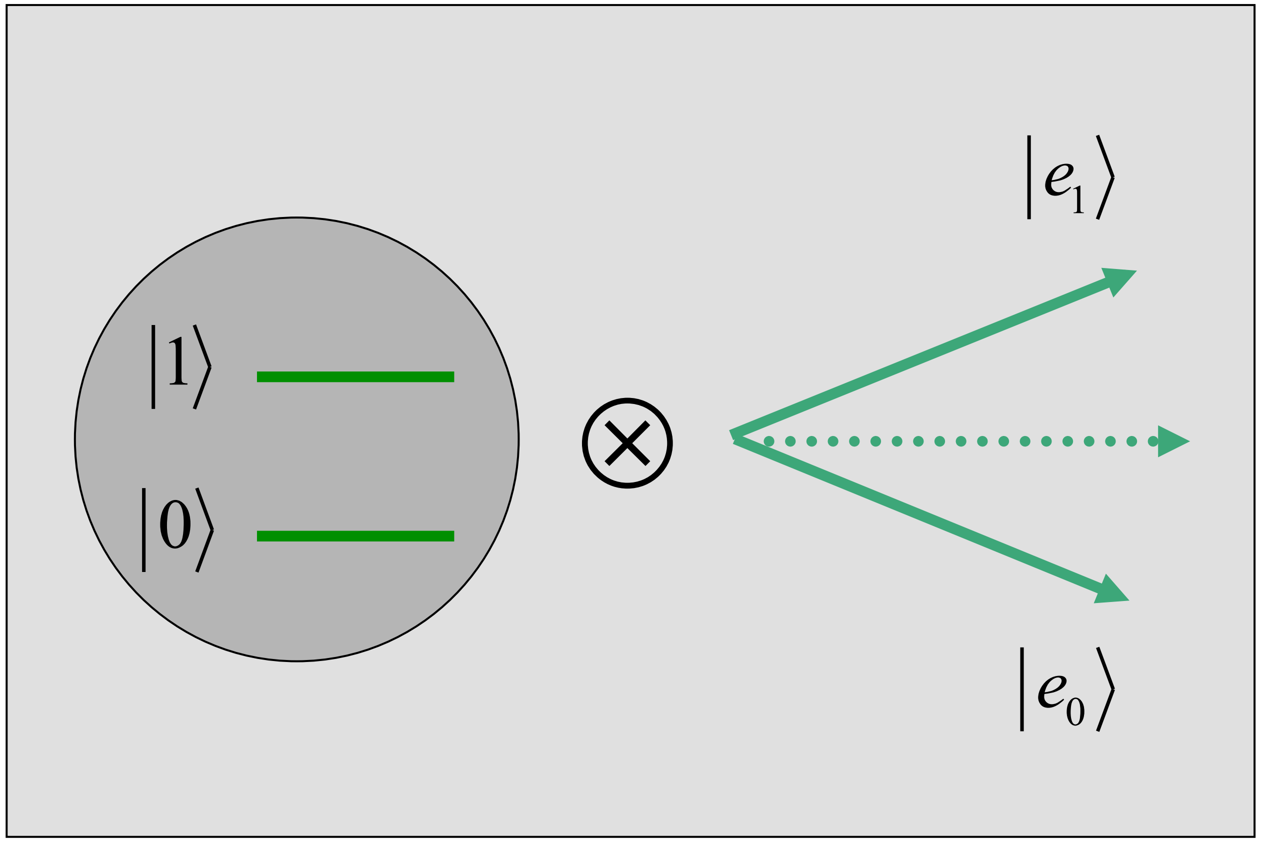


Keep it simple – Hugh Everett (1957)

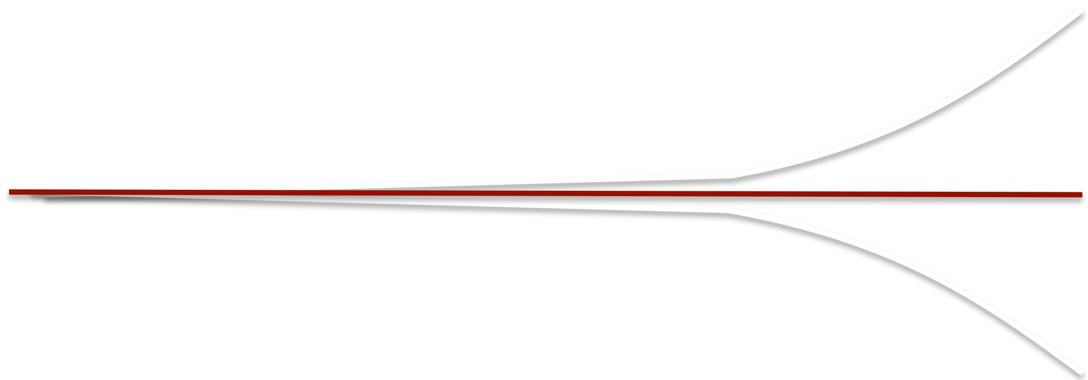
$$|a_k\rangle|e\rangle \rightarrow |a_k\rangle|e_k\rangle$$

MEASUREMENT = UNITARY EVOLUTION
NO NEED FOR PROJECTION POSTULATE





Everett's reality



$$|a_1\rangle|\text{apparatus}_1\rangle|\text{me}_1\rangle$$


$$|a_2\rangle|\text{apparatus}_2\rangle|\text{me}_2\rangle$$


$$|a_3\rangle|\text{apparatus}_3\rangle|\text{me}_3\rangle$$

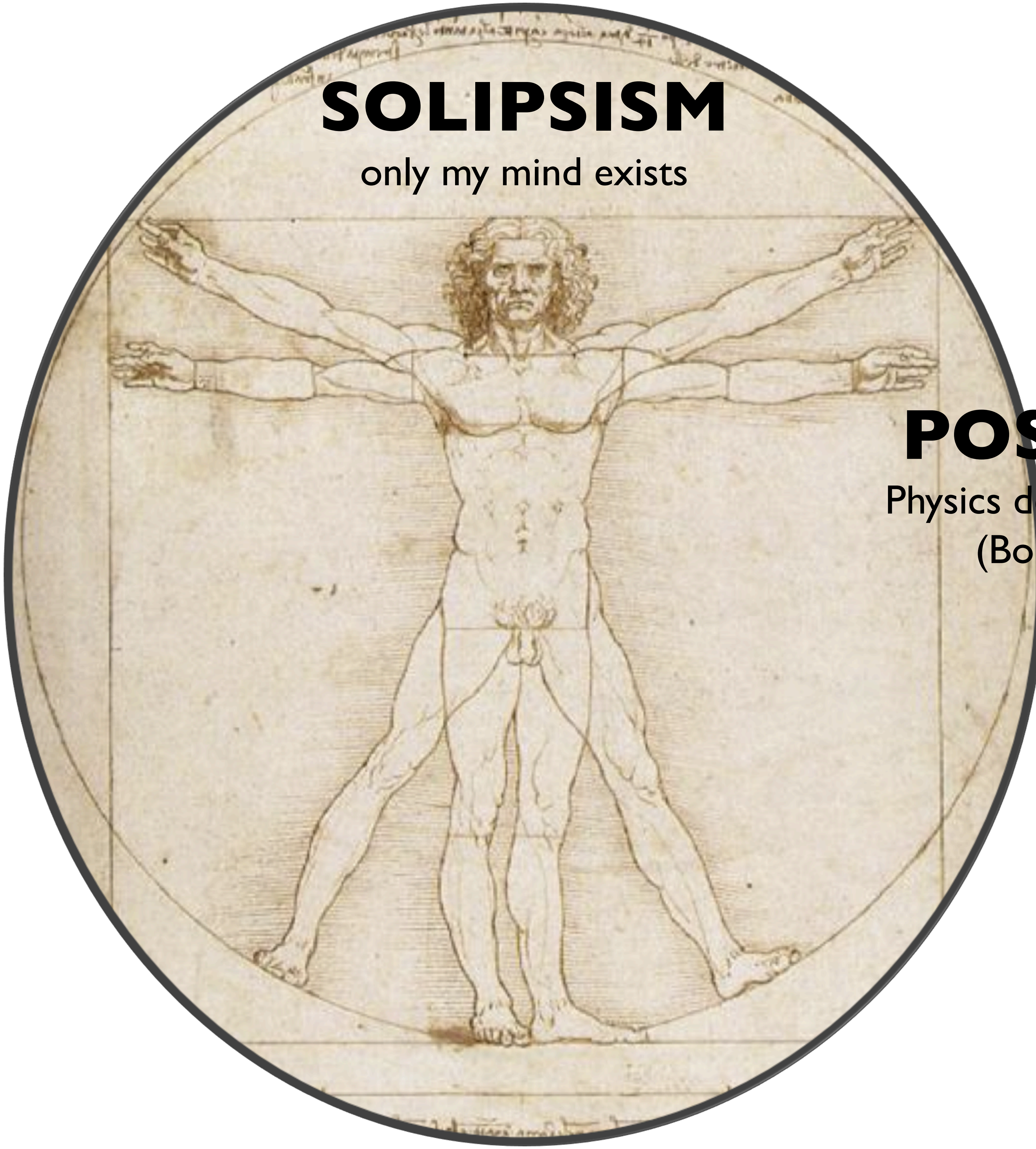

I PERCEIVE ONE OUTCOME BUT ALL OCCUR

NO SPECIAL STATUS TO OBSERVERS

NO MODIFICATION OF THE FORMALISM

NO PROJECTION POSTULATE

NO BELL'S THEOREM



SOLIPSISM

only my mind exists

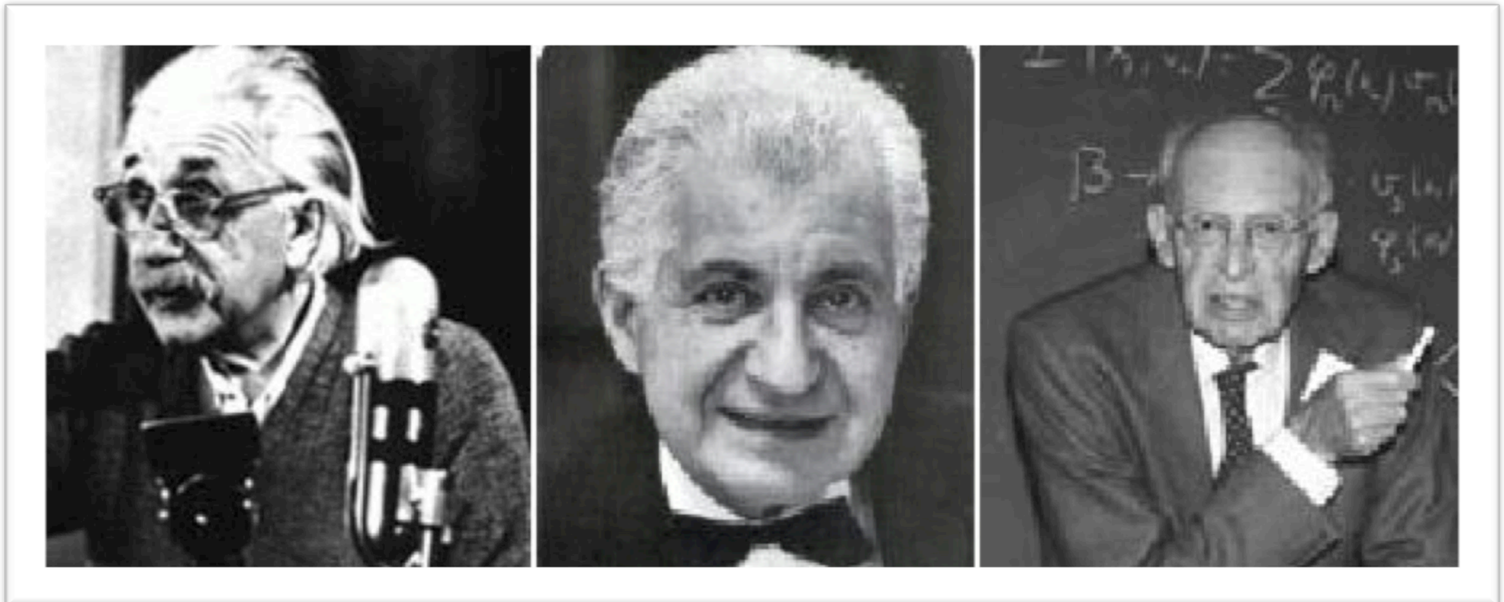
POSITIVISM

Physics describes perceptions
(Bohr, Heisenberg)

REALISM

Physics describes reality
(Einstein, Schrödinger)

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?