Nobel Prize in Physics 2022:

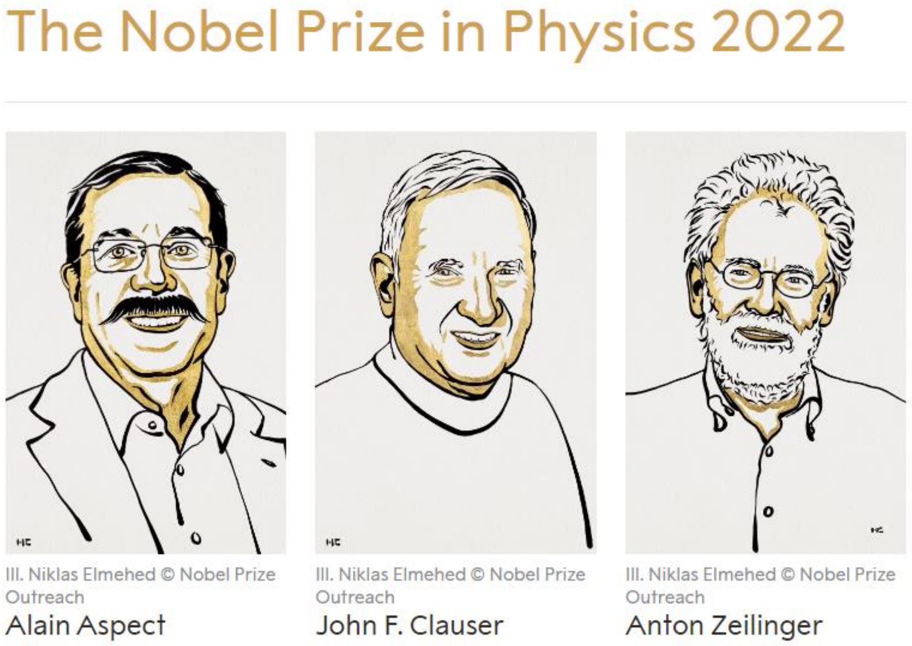
From the Foundations of Quantum Mechanics to Quantum Information Science

Helena Vieira Alberto

Physics Department, University of Coimbra

Coffee with Physics
9 November, 2022

Coffee first, than physics

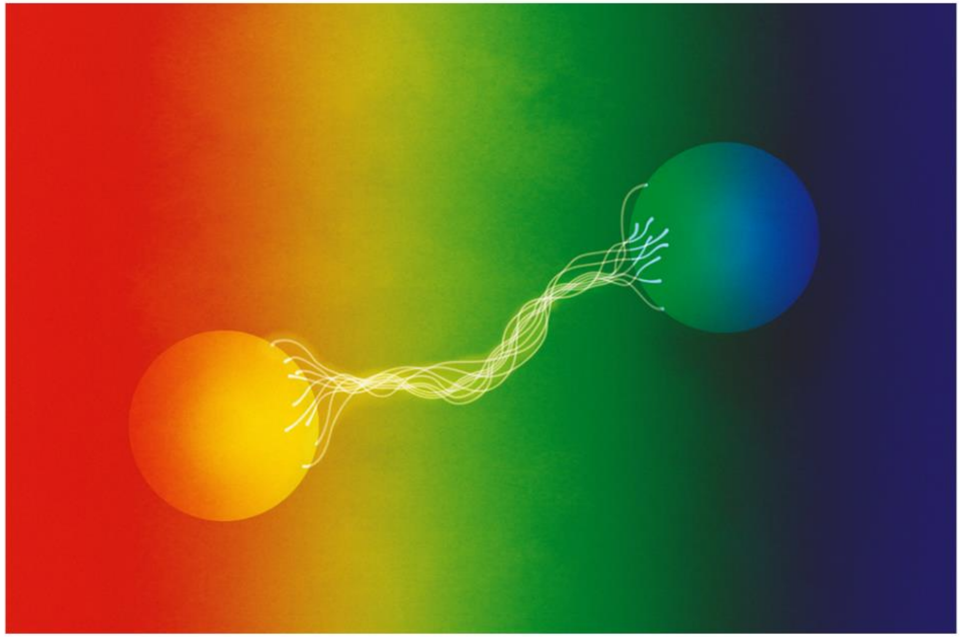


The Nobel Prize in Physics 2022

Ill. Niklas Elmehed © Nobel Prize Outreach
Alain Aspect

Ill. Niklas Elmehed © Nobel Prize Outreach
John F. Clauser

Ill. Niklas Elmehed © Nobel Prize Outreach
Anton Zeilinger

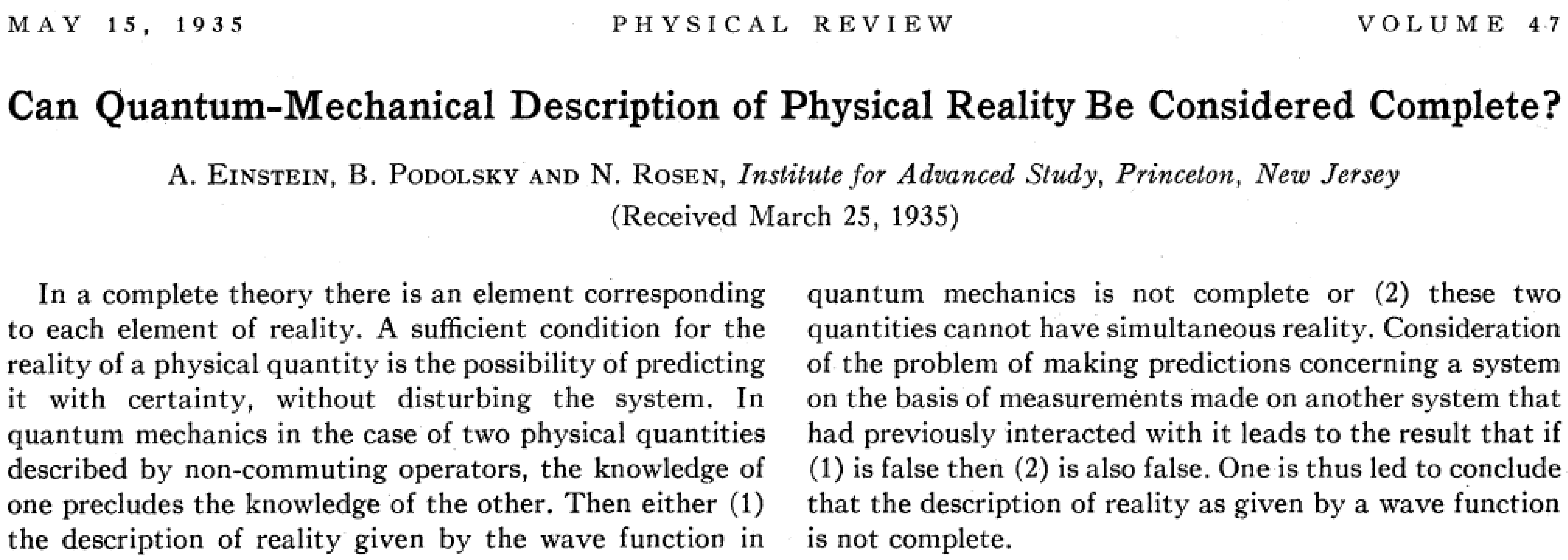


© Johan Jarnestad/The Royal Swedish Academy of Sciences

1935-1982

The Foundations of Quantum Mechanics

1935 – EPR paper



MAY 15, 1935 PHYSICAL REVIEW VOLUME 47

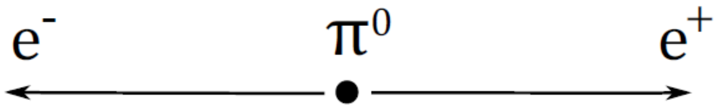
Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?

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.

EPR-Bohm paradox



$$\frac{1}{\sqrt{2}}\left(|\uparrow_-\downarrow_+\rangle - |\downarrow_-\uparrow_+\rangle \right)$$

EPR (Einstein, Podolsky, Rosen) assumed valid

the principle of locality , i.e, the result of a measurement of a system cannot influence the result of a measurement of a second system occurring simultaneously.

in order to conclude

the principle of realism , i.e., the values of a physical quantity have a physical reality which is independent of its measurement.

Einstein's (EPR's) Claim: the description of reality given by the wave function in quantum mechanics is not complete.

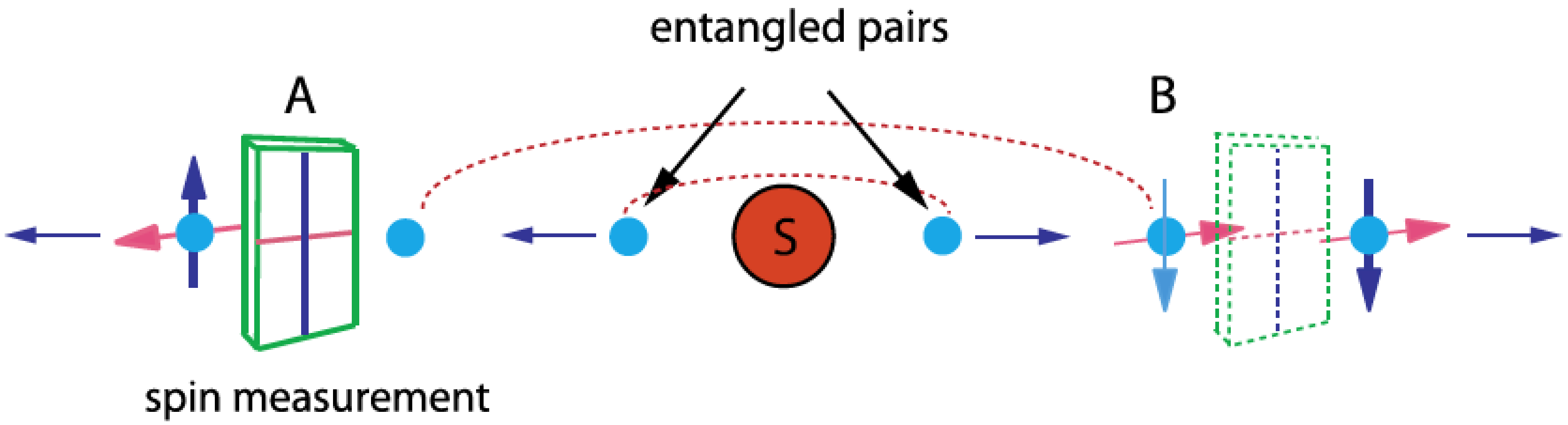
The state of a physical system is represented by a vector $|\Psi\rangle$

A physical quantity is represented by an operator

Pauli Operators

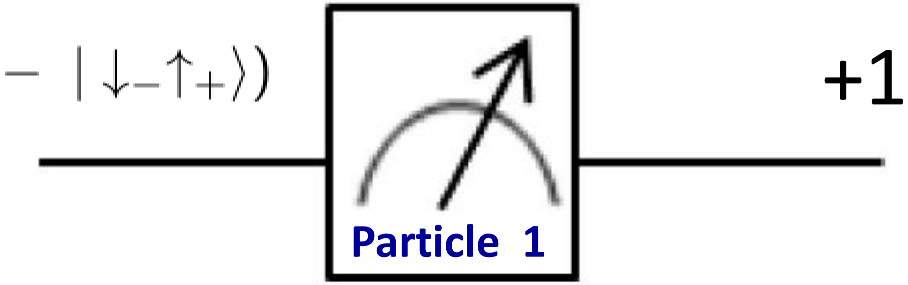
$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

matrix	eigenvalue	eigenvector
σ_x	$+1$	$\lvert\uparrow_x\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}$
	-1	$\lvert\downarrow_x\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix}$
σ_y	$+1$	$\lvert\uparrow_y\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ i \end{pmatrix}$
	-1	$\lvert\downarrow_y\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -i \end{pmatrix}$
σ_z	$+1$	$\lvert\uparrow_z\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$
	-1	$\lvert\downarrow_z\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$


entangled pairs
A
B
S
spin measurement

Measurement of particle 1 of a Bell state in a z basis

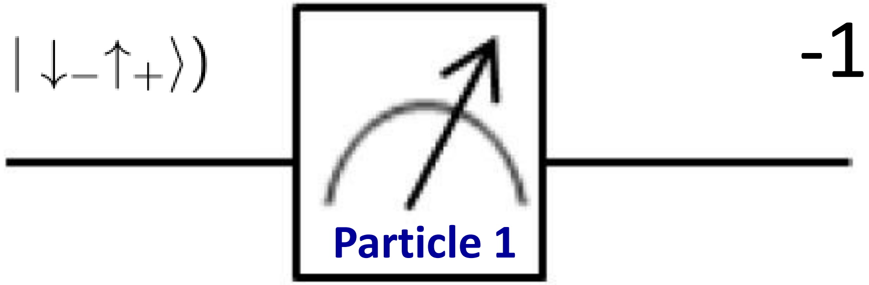
$$\frac{1}{\sqrt{2}}(|\uparrow_-\downarrow_+\rangle - |\downarrow_-\uparrow_+\rangle)$$



+1 , 50% probability

or

$$\frac{1}{\sqrt{2}}(|\uparrow_-\downarrow_+\rangle - |\downarrow_-\uparrow_+\rangle)$$



-1, 50% probability

In the end, I know the state of particle 2 although I did not measured it!

EPR-Bohm paradox

$\sigma_z^{(A)}$	$\sigma_z^{(B)}$	$\sigma_z^{(A)}\,\sigma_z^{(B)}$
+1	-1	-1
+1	-1	-1
-1	+1	-1
-1	+1	-1
+1	-1	-1
.	.	.
.	.	.
.	.	.

$$\langle \sigma_z^{(A)} \rangle = 0 \quad \langle \sigma_z^{(B)} \rangle = 0 \qquad \langle \sigma_z^{(A)}\,\sigma_z^{(B)} \rangle = -1$$

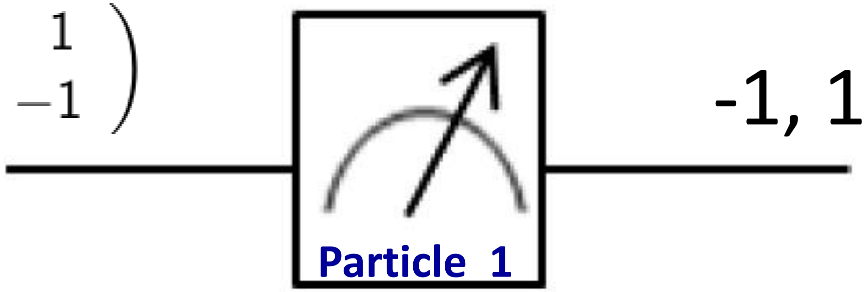
Let us assume particles are independent, each one has a physical reality which is independent of the other as Einstein states .

If I measure particle 1 in x basis I always get the same result !

It makes no sense!

The result should not depend on the direction of measurement!

$$|\downarrow_x\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

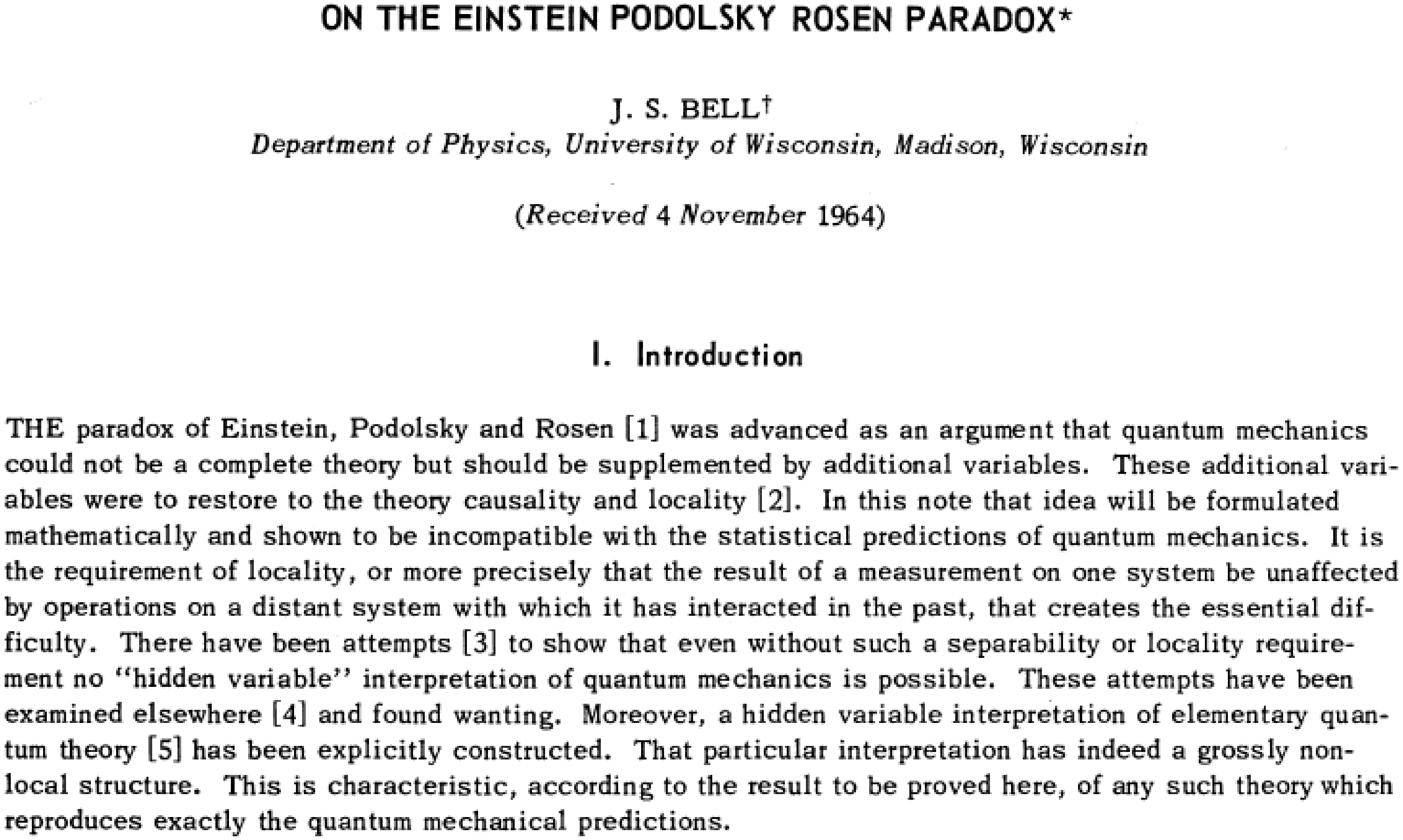


-1, 100% probability

X basis

1964 - Bell paper

“All attempts to construct a local realist model of quantum mechanics are doomed to fail”



ON THE EINSTEIN PODOLSKY ROSEN PARADOX*

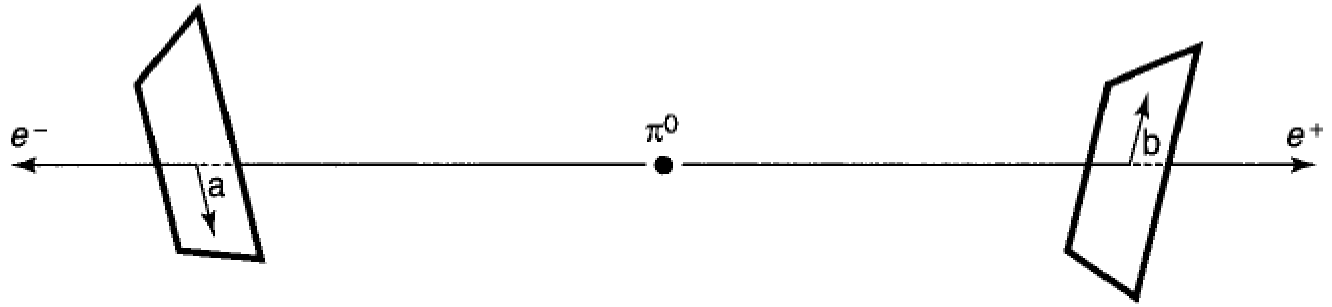
J. S. BELL†
Department of Physics, University of Wisconsin, Madison, Wisconsin

(*Received* 4 *November* 1964)

I. Introduction

THE paradox of Einstein, Podolsky and Rosen [1] was advanced as an argument that quantum mechanics could not be a complete theory but should be supplemented by additional variables. These additional variables were to restore to the theory causality and locality [2]. In this note that idea will be formulated mathematically and shown to be incompatible with the statistical predictions of quantum mechanics. It is the requirement of locality, or more precisely that the result of a measurement on one system be unaffected by operations on a distant system with which it has interacted in the past, that creates the essential difficulty. There have been attempts [3] to show that even without such a separability or locality requirement no “hidden variable” interpretation of quantum mechanics is possible. These attempts have been examined elsewhere [4] and found wanting. Moreover, a hidden variable interpretation of elementary quantum theory [5] has been explicitly constructed. That particular interpretation has indeed a grossly non-local structure. This is characteristic, according to the result to be proved here, of any such theory which reproduces exactly the quantum mechanical predictions.

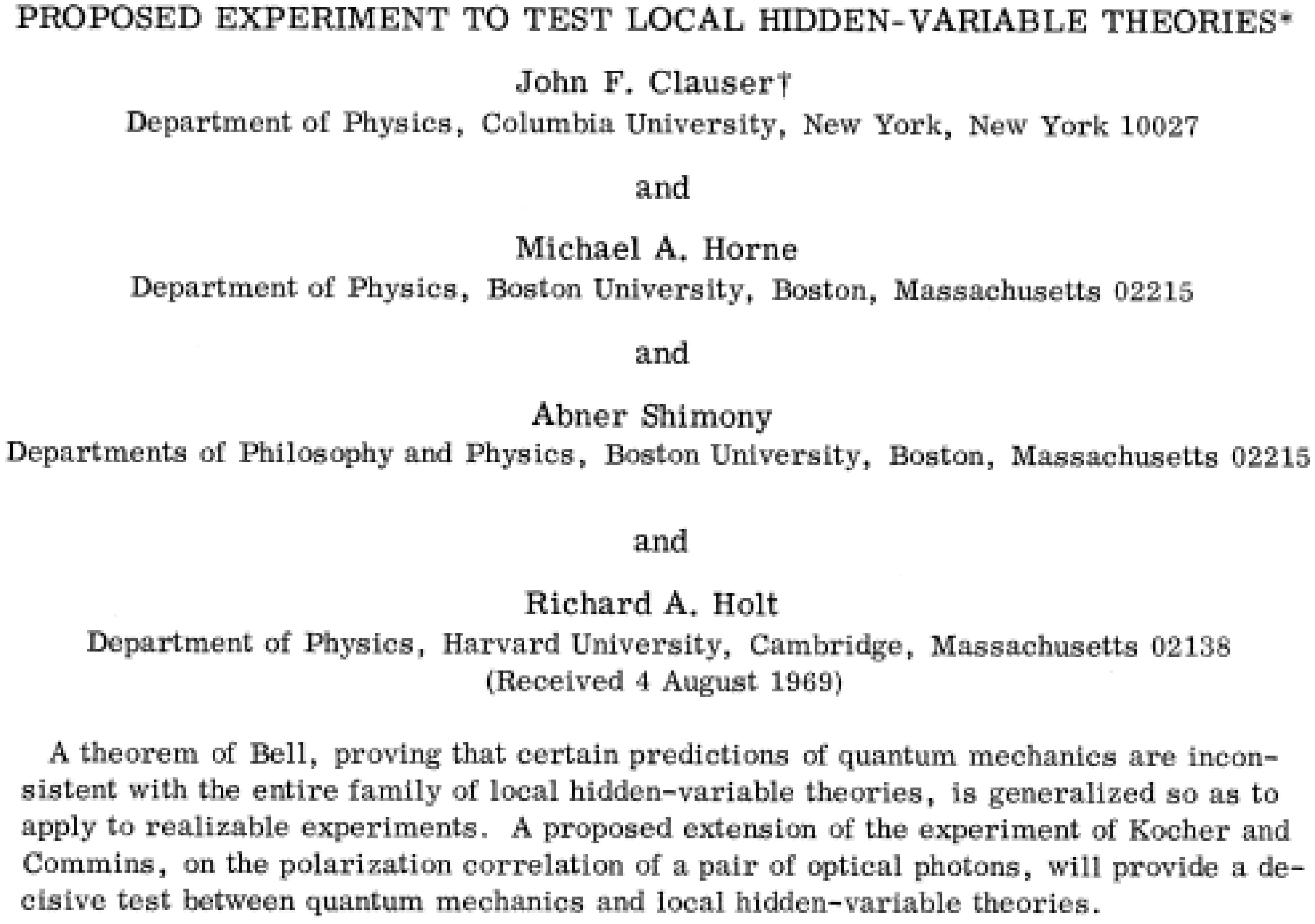
Bell version of EPR/Bohm experiment



Instead of measuring both in z direction

- Lab A measures in direction a (or a’)
- Lab B measures in direction b (oru b’)

1969 – Clauser, Horne, Shimony, Holt inequality



PROPOSED EXPERIMENT TO TEST LOCAL HIDDEN-VARIABLE THEORIES*

John F. Clauser†
Department of Physics, Columbia University, New York, New York 10027

and

Michael A. Horne
Department of Physics, Boston University, Boston, Massachusetts 02215

and

Abner Shimony
Departments of Philosophy and Physics, Boston University, Boston, Massachusetts 02215

and

Richard A. Holt
Department of Physics, Harvard University, Cambridge, Massachusetts 02138

(Received 4 August 1969)

A theorem of Bell, proving that certain predictions of quantum mechanics are inconsistent with the entire family of local hidden-variable theories, is generalized so as to apply to realizable experiments. A proposed extension of the experiment of Kocher and Commins, on the polarization correlation of a pair of optical photons, will provide a decisive test between quantum mechanics and local hidden-variable theories.

Bell Experiment

Bell test with fixed directions **a** and **b** :

$\sigma_a^{(A)}$	$\sigma_b^{(B)}$	$\sigma_a^{(A)}\,\sigma_b^{(B)}$
+1	-1	-1
+1	+1	+1
-1	+1	-1
+1	-1	-1
-1	-1	+1
.	.	.
.	.	.
.	.	.

Final result :

$$P_{a\,b} = \langle \sigma_a^{(A)}\,\sigma_b^{(B)} \rangle$$

Quantum Mechanics predicts

$$P_{a\,b} = \langle \sigma_a^{(A)}\,\sigma_b^{(B)} \rangle = -\hat{a}\cdot\hat{b} = -\cos\theta$$

Students of Quantum Optics and Quantum Information + Students of Quantum Technologies

(Home problem !)

Problem

1. Show that

$$P(\mathbf{a},\mathbf{b}) = \langle \sigma_a^{(A)} \sigma_b^{(B)} \rangle = -\cos\theta = -\hat{a}\cdot\hat{b}$$

2. Complete the table 1 with the values of $P(\mathbf{a},\mathbf{b})$ corresponding to each pair of directions and show that the value of S predicted by Quantum Mechanics for this set of directions is $S = 2\sqrt{2}$.

3. According to the paper, for $a = b = 1$, box A performs a measurement $\sigma_x^{(A)}$ and box B performs a measurement $\sigma_d^{(B)}$, where the direction d is defined by $\hat{e}_d = \frac{1}{\sqrt{2}}(-\hat{e}_x - \hat{e}_z)$.

   (a) Consider the box B.

   i. Prove that the operator

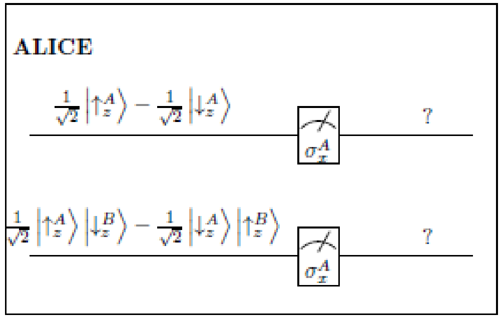
$$\sigma_d^{(B)} = \vec{\sigma}^{(B)}\cdot\hat{e}_d \ = (\sigma_x\cdot\hat{e}_x + \sigma_y\cdot\hat{e}_y + \sigma_z\cdot\hat{e}_z)^{(B)}\cdot\hat{e}_d$$

   is given by

$$\sigma_d^{(B)} = \frac{1}{\sqrt{2}}\begin{pmatrix} -1 & -1 \\ -1 & 1 \end{pmatrix}$$

   ii. What are the possible results for a measurement of $\sigma_d^{(B)}$? Justify your answer.

   (b) Let us now consider the box A, with a=1, that is, a box where measurements of σ_x of electron A are performed, that is, of $\sigma_x^{(A)}$.


ALICE
$\frac{1}{\sqrt{2}}|\uparrow_z^A\rangle - \frac{1}{\sqrt{2}}|\downarrow_z^A\rangle$
σ_x^A
?
$\frac{1}{\sqrt{2}}|\uparrow_z^A\rangle|\downarrow_z^B\rangle - \frac{1}{\sqrt{2}}|\downarrow_z^A\rangle|\uparrow_z^B\rangle$
σ_x^A
?

   Start by considering box A in a situation where the experimental team could not perform the entanglement between spins A and B. In this case, the spin state A-B is factorizable: $|\Psi\rangle = |\Psi\rangle^A \otimes |\Psi\rangle^B$. Thus, spin A is described simply by the function $|\Psi^A\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow_z^A\rangle - |\downarrow_z^A\rangle\right)$.

   i. Prove that $|\Psi^A\rangle$ é an eigenvector of $\sigma_x^{(A)}$.

   ii. What are the probabilities of getting +1 and −1 in a measurement in this case?

   iii. Predict the average value of a list of measurements under these conditions.

   (c) Now consider box A in a situation where there is entanglement, i.e. spin A is described by $|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow_z^A\rangle|\downarrow_z^B\rangle - |\downarrow_z^A\rangle|\uparrow_z^B\rangle\right)$. Under these conditions, a set of measurement of $\sigma_x^{(A)}$ is performed.

Consider the following choice of directions **a**, **a**$'$ e **b**, **b**$'$:

$\hat{a}$	$\hat{b}$	$P_{a\,b} = -\hat{a}\cdot\hat{b}$
$\hat{e}_z$	$\frac{1}{\sqrt{2}}(\hat{e}_x - \hat{e}_z)$	$P_{ab} = +\frac{1}{\sqrt{2}}$
$\hat{e}_z$	$\frac{1}{\sqrt{2}}(-\hat{e}_x - \hat{e}_z)$	$P_{ab'} = +\frac{1}{\sqrt{2}}$
$-\hat{e}_x$	$\frac{1}{\sqrt{2}}(+\hat{e}_x - \hat{e}_z)$	$P_{a'b} = +\frac{1}{\sqrt{2}}$
$-\hat{e}_x$	$\frac{1}{\sqrt{2}}(-\hat{e}_x - \hat{e}_z)$	$P_{a'b'} = -\frac{1}{\sqrt{2}}$

Quantum Mechanics predicts

$$S = |P_{ab} + P_{ab'} + P_{a'b} - P_{a'b'}| = 2\sqrt{2}$$

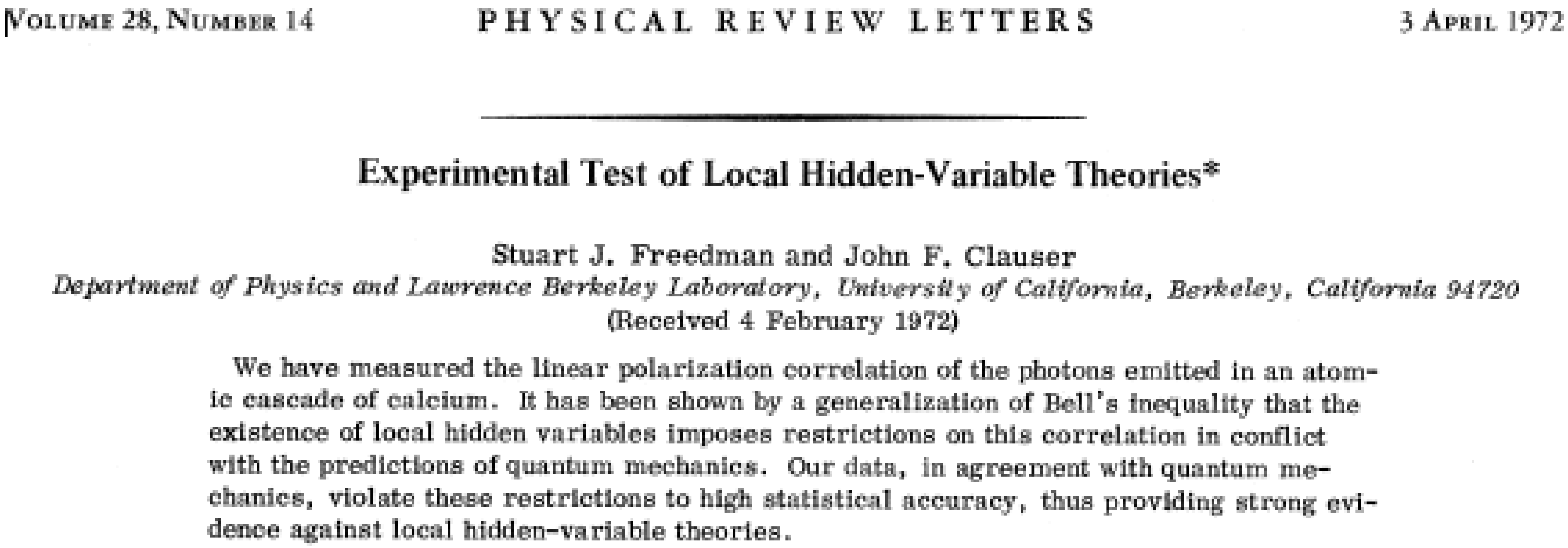
In conditions of **local realism**, we have

$$S = |P_{ab} + P_{ab'} + P_{a'b} - P_{a'b'}| \leq 2$$

which is named

CHHS-Bell (Clauser-Holt-Horne-Shimony) inequality

1972 – Freedman-Clauser experiment



VOLUME 28, NUMBER 14 PHYSICAL REVIEW LETTERS 3 APRIL 1972

Experimental Test of Local Hidden-Variable Theories*

Stuart J. Freedman and John F. Clauser
Department of Physics and Lawrence Berkeley Laboratory, University of California, Berkeley, California 94720

(Received 4 February 1972)

We have measured the linear polarization correlation of the photons emitted in an atomic cascade of calcium. It has been shown by a generalization of Bell's inequality that the existence of local hidden variables imposes restrictions on this correlation in conflict with the predictions of quantum mechanics. Our data, in agreement with quantum mechanics, violate these restrictions to high statistical accuracy, thus providing strong evidence against local hidden-variable theories.

The concept of Hauser experiment

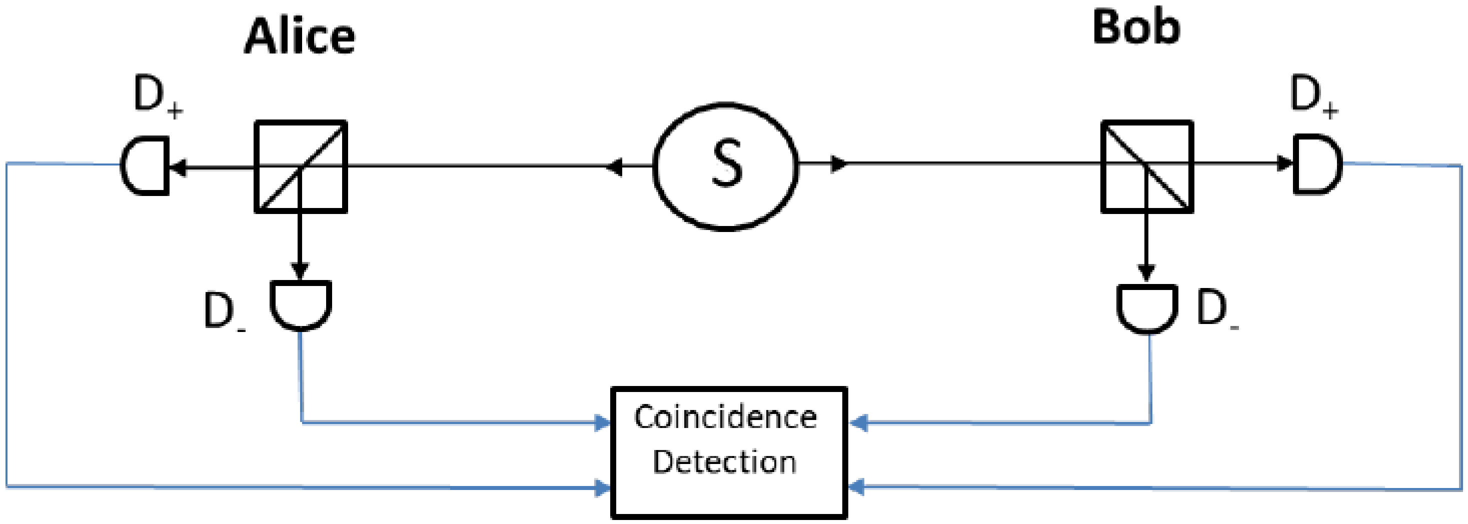


Figure 2. *The source S produces pairs of entangled photons, sent in opposite directions. Each photon encounters a two-channel polarizer whose orientation can be set by the Alice and Bob . Emerging signals from each channel are detected by single photon detector D_+ and D_- and coincidences counted by the coincidence unit. The correlation* $E(a,b) = (N_{++} - N_{+-} - N_{-+} + N_{--})/(N_{++} + N_{+-} + N_{-+} + N_{--})$ *where* N_{++}, N_{+-}, N_{-+}, *and* N_{--} *are the number of coincidence events recorded corresponding to the simultaneous detection at Alice's and Bob's detectors* D_+ *and* D_+ , D_+ *and* D_-, D_- *and* D_+ , *and* D_- *and* D_- , *respectively.*

1972 – Freedman-Clauser experiment

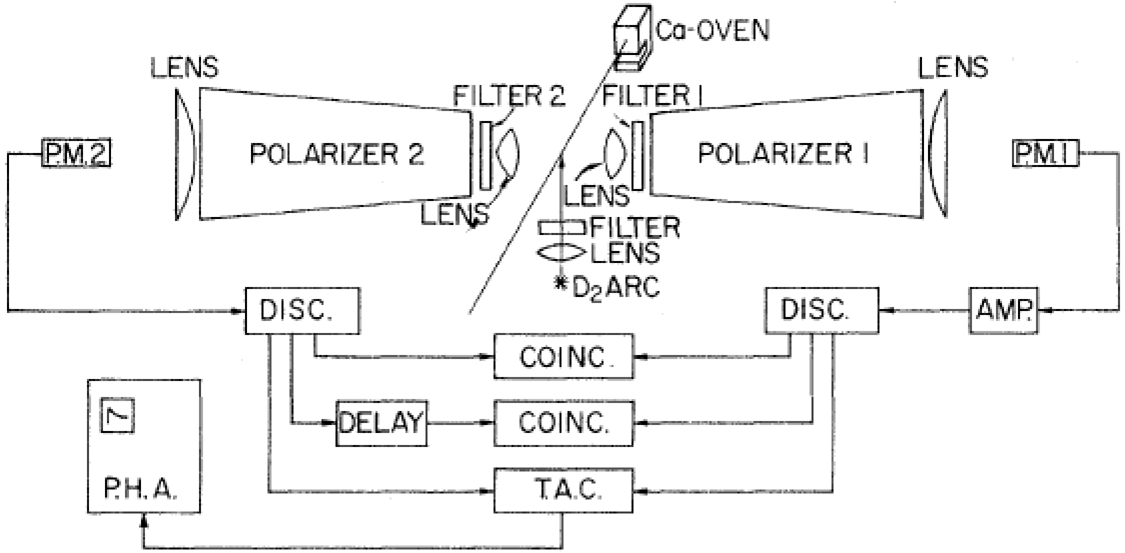
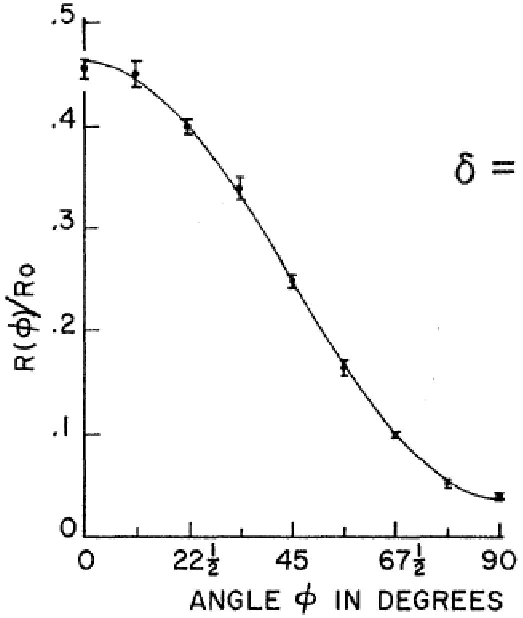


FIG. 1. Schematic diagram of apparatus and associated electronics. Scalers (not shown) monitored the outputs of the discriminators and coincidence circuits during each 100-sec count period. The contents of the scalers and the experimental configuration were recorded on paper tape and analyzed on an IBM 1620-II computer.

1972 – Freedman-Clauser experiment

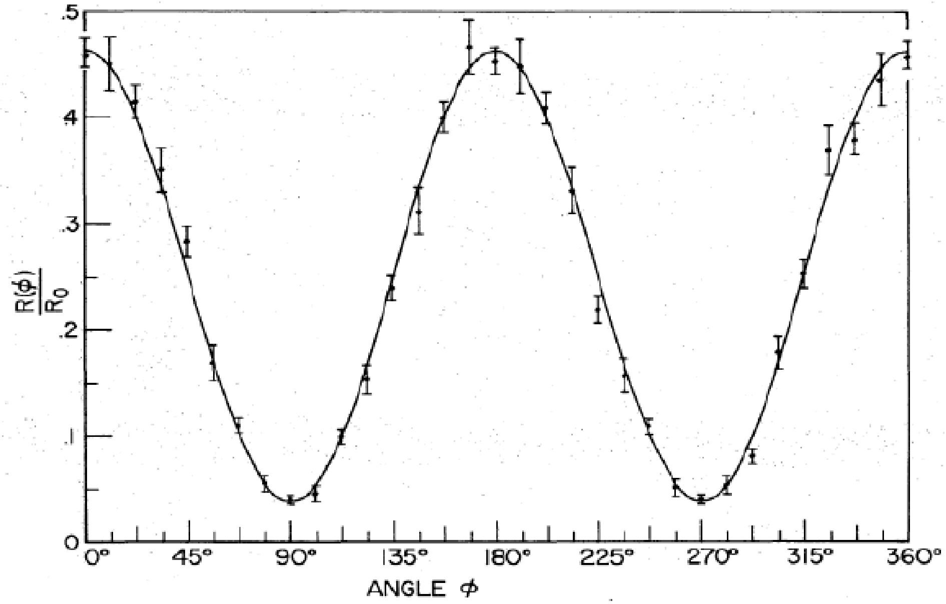
$$\delta = \left| R(22\tfrac{1}{2}^\circ)/R_0 - R(67\tfrac{1}{2}^\circ)/R_0 \right| - \tfrac{1}{4} \leqslant 0,$$

Maximum violation of Bell inequality , expressed using coincidence rates at the angles between the polarizers, occurs for 22,5 deg and 67.5 deg



$\delta = 0.050 \pm 0.008$

FIG. 3. Coincidence rate with angle φ between the polarizers, divided by the rate with both polarizers removed, plotted versus the angle φ. The solid line is the prediction by quantum mechanics, calculated using the measured efficiencies of the polarizers and solid angles of the experiment.



The experimentally measured ratio R(ϕ)/R₀ as a function of the angle ϕ between the axes of the polarizers. The solid line is not a fit to the data points but the polarization correlation predicted by quantum mechanics. (From Freedman's PhD thesis, Experimental Test of Local Hidden-Variable Theories, Lawrence Berkeley National Laboratory, 1972.)

Problem: Alice can send the information on the direction of measurement to Bob and vice versa; no information should be sent, according to Bell.

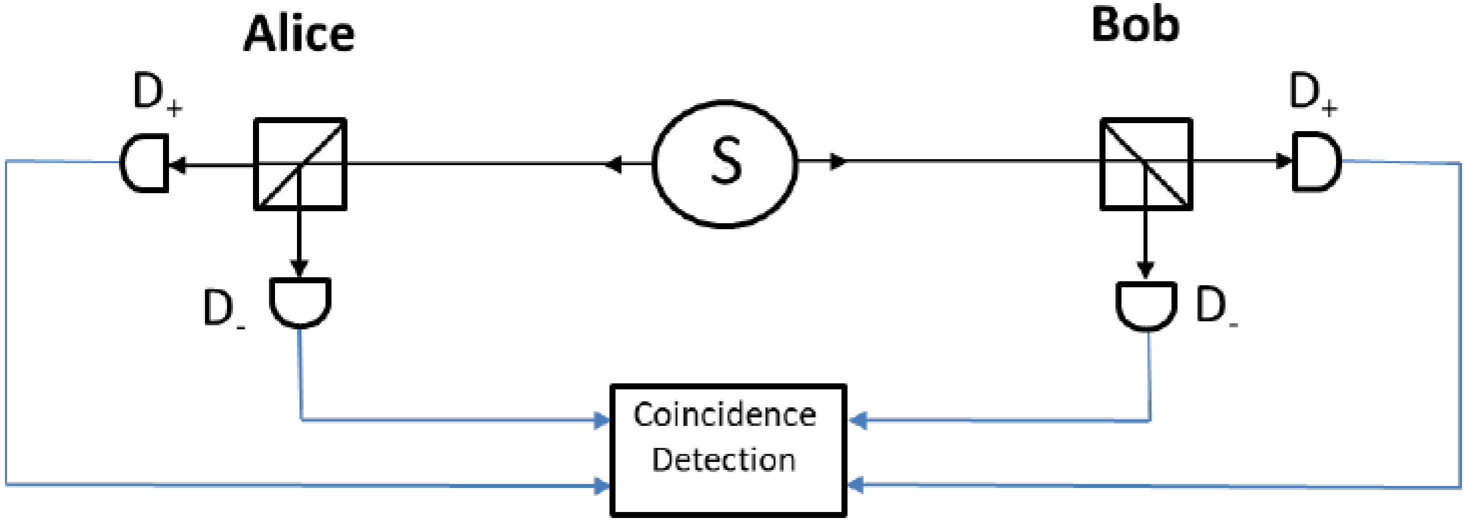


Figure 2. *The source S produces pairs of entangled photons, sent in opposite directions. Each photon encounters a two-channel polarizer whose orientation can be set by the Alice and Bob . Emerging signals from each channel are detected by single photon detector D_+ and D_- and coincidences counted by the coincidence unit. The correlation* $E(a,b) = (N_{++} - N_{+-} - N_{-+} + N_{--})/(N_{++} + N_{+-} + N_{-+} + N_{--})$ *where N_{++}, N_{+-}, N_{-+}, and N_{--} are the number of coincidence events recorded corresponding to the simultaneous detection at Alice's and Bob's detectors D_+ and D_+ , D_+ and D_-, D_- and D_+ , and D_- and D_- , respectively.*

1976-1982 Aspect Experiments

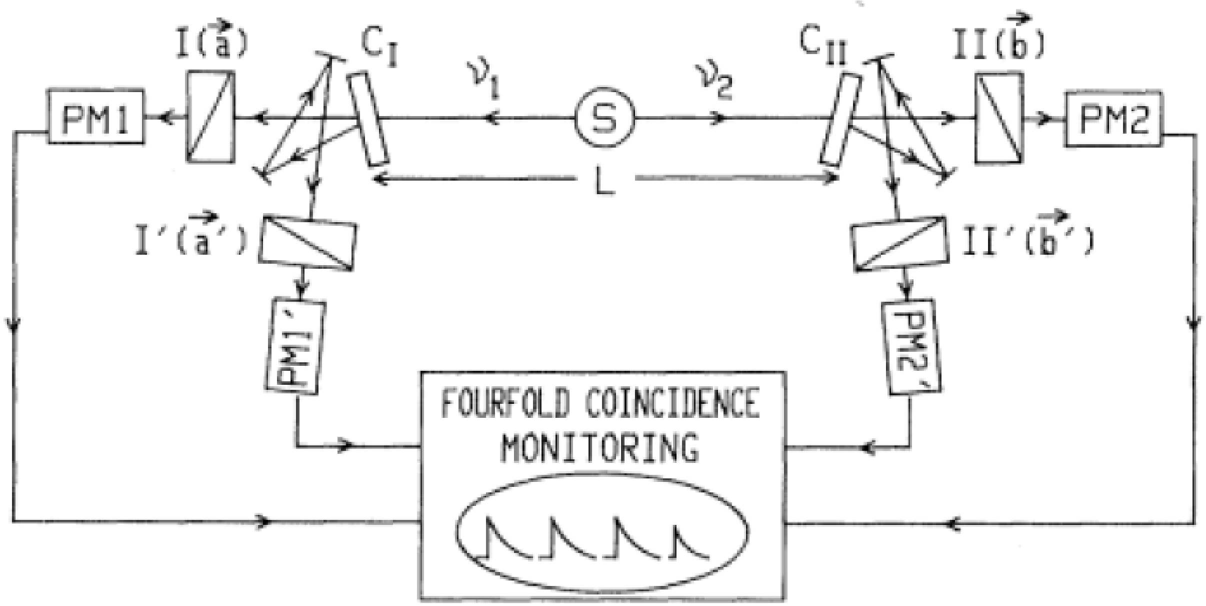
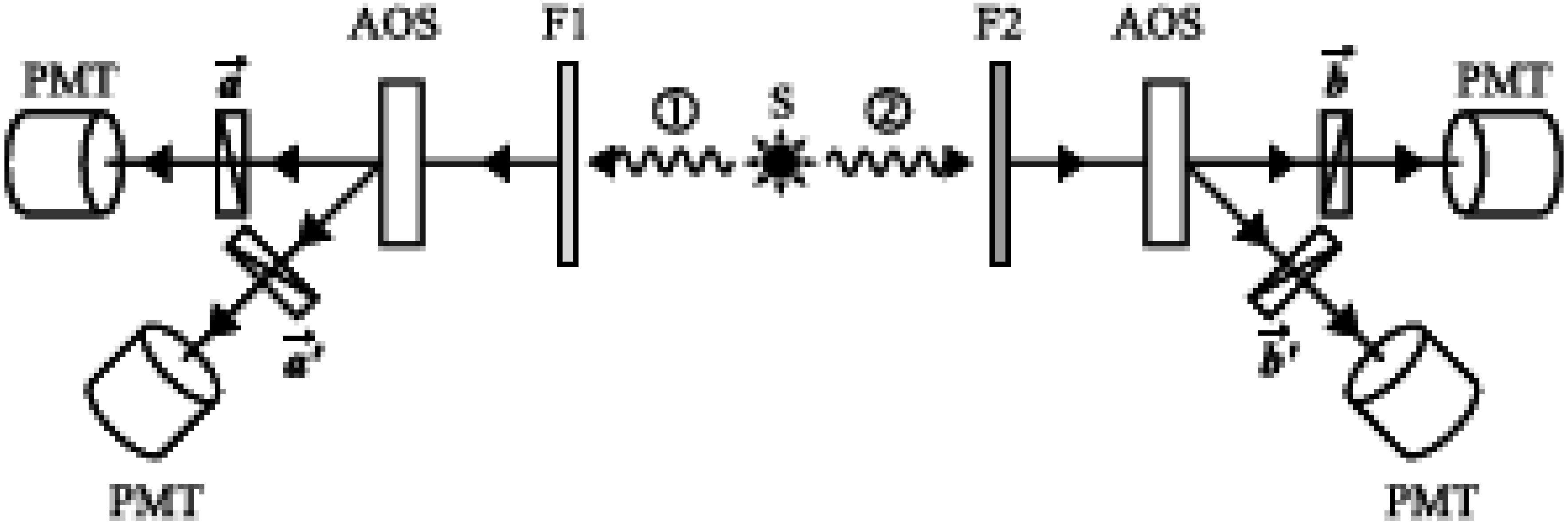


Figure 6. *Schematic of the experiment proposed by Aspect in 1976 [15] and performed with collaborators in 1982 [14]. The photons emitted by the calcium cascade source first meet the optical switches $C_I$and C_{II}, where they can either be transmitted to polarizers and detectors PM1 and PM2, or be reflected to another set of polarizers and detectors PM1' and PM2'. Switching between the two channels occurs approximately every 10 ns. The distance between the polarizers was 12 m. The optical switches are ultrasonic standing waves resulting from interference between counter-propagating acoustic waves produced by two electro-acoustical transducers.*

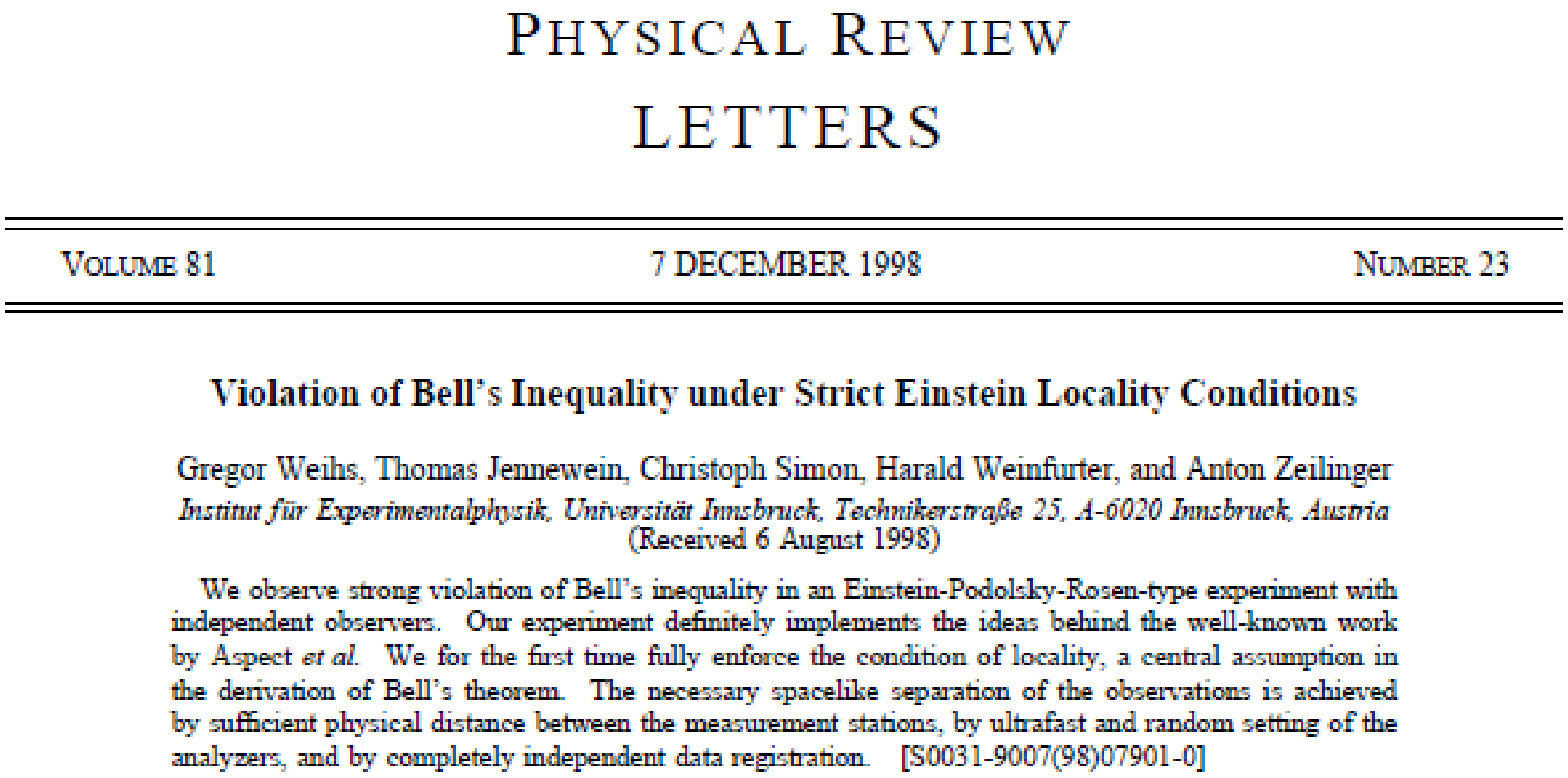
Pictorial view of Aspect Experiment in 1982



AOS – fast acousto-optical switch with switching time

t< L/c

1998 – Zeilinger experiment



PHYSICAL REVIEW LETTERS

VOLUME 81 7 DECEMBER 1998 NUMBER 23

Violation of Bell's Inequality under Strict Einstein Locality Conditions

Gregor Weihs, Thomas Jennewein, Christoph Simon, Harald Weinfurter, and Anton Zeilinger
Institut für Experimentalphysik, Universität Innsbruck, Technikerstraße 25, A-6020 Innsbruck, Austria

(Received 6 August 1998)

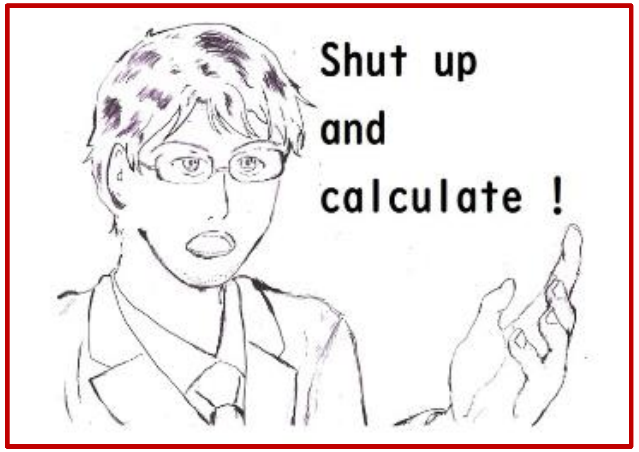
We observe strong violation of Bell's inequality in an Einstein-Podolsky-Rosen-type experiment with independent observers. Our experiment definitely implements the ideas behind the well-known work by Aspect *et al.* We for the first time fully enforce the condition of locality, a central assumption in the derivation of Bell's theorem. The necessary spacelike separation of the observations is achieved by sufficient physical distance between the measurement stations, by ultrafast and random setting of the analyzers, and by completely independent data registration. [S0031-9007(98)07901-0]

Argument of locality loop-hole: "Aspect et al. used periodic sinusoidal switching, which is predictable into the future. "
Solution: electro-optic modulator is driven by a random-number generator
Argument of detection loop-hole : "the efficiency of photon detection is low"; Bell inequality is proven only for a subset of the photons – solved in 2025 only!

Quantum Mechanics

- Two very different approaches

1. the standard approach :



(*a motto of Richard Feynman*)

i.e. use main experimental results to define postulates of Quantum Mechanics and derived everything from there.

Arguments:

- Quantum Mechanics works and it is extremely successful.
- We should use it to make predictions and explain Nature.
- We should not waste time trying to prove something we know it is true since almost a century ago.

Quantum Mechanics

- Two very different approaches

2. Zeilinger approach :

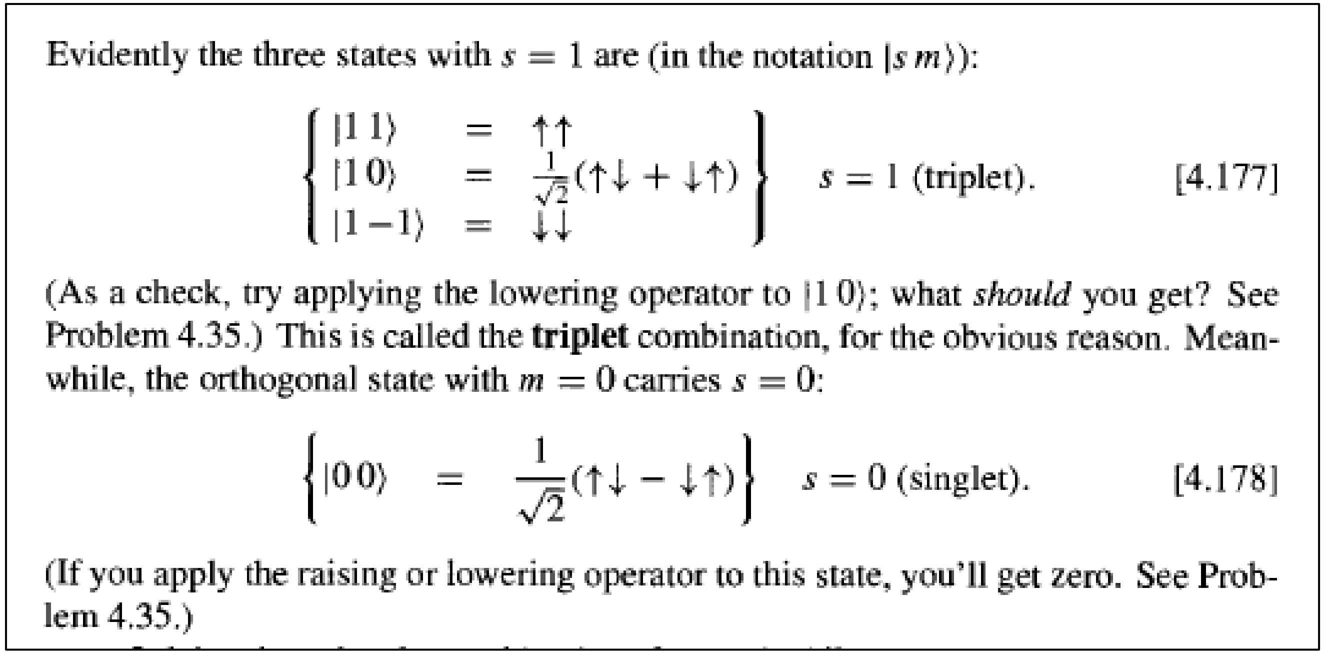
Fundamental research on entanglement of photons and Bell pairs deepens our understanding of quantum mechanics and of quantum information .

Side effects: applications such as

- quantum cryptography in ultra-secure transmission of information
- quantum teleportation for quantum internet
- Quantum computation : quantum supremacy as been proven in a proof of principle experiment with quantum optics

Example: the description of the coupling of two spin ½ particles

- The approach of a book in Quantum Mechanics



Evidently the three states with $s = 1$ are (in the notation $|s\,m\rangle$):

$$\left\{\begin{array}{lcl} |1\,1\rangle & = & \uparrow\uparrow \\ |1\,0\rangle & = & \frac{1}{\sqrt{2}}(\uparrow\downarrow + \downarrow\uparrow) \\ |1\,{-1}\rangle & = & \downarrow\downarrow \end{array}\right\} \quad s = 1 \text{ (triplet).} \qquad [4.177]$$

(As a check, try applying the lowering operator to $|1\,0\rangle$; what *should* you get? See Problem 4.35.) This is called the **triplet** combination, for the obvious reason. Meanwhile, the orthogonal state with $m = 0$ carries $s = 0$:

$$\left\{|0\,0\rangle \;=\; \frac{1}{\sqrt{2}}(\uparrow\downarrow - \downarrow\uparrow)\right\} \quad s = 0 \text{ (singlet).} \qquad [4.178]$$

(If you apply the raising or lowering operator to this state, you'll get zero. See Problem 4.35.)

Griffiths – Introduction of Quantum Mechanics, page 166

The approach of Quantum Information

Let's look at each state separately.

- What information can we get for each particle?

$$\begin{array}{lclcl}
|\uparrow\uparrow\rangle & = & |\uparrow\rangle\ |\uparrow\rangle & \Rightarrow & \text{states are factorizable} & \Rightarrow & \text{independent particles} \\
|\downarrow\downarrow\rangle & = & |\downarrow\rangle\ |\downarrow\rangle & \Rightarrow & \text{states are factorizable} & \Rightarrow & \text{independent particles}
\end{array}$$

$$\begin{aligned}
\frac{1}{\sqrt{2}}\left(|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle\right) \quad & \neq \quad \frac{1}{\sqrt{2}}\left(|\uparrow\rangle + |\downarrow\rangle\right)\ \frac{1}{\sqrt{2}}\left(|\uparrow\rangle + |\downarrow\rangle\right) \\
& \neq \quad |\psi_1\rangle\ \ |\psi_2\rangle \\
& \Rightarrow \quad \text{states are } \textit{not} \text{ factorizable} \\
& \Rightarrow \quad \textit{entangled} \text{ particles} \\
\frac{1}{\sqrt{2}}\left(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle\right) \quad & \neq \quad \frac{1}{\sqrt{2}}\left(|\uparrow\rangle - |\downarrow\rangle\right)\ \frac{1}{\sqrt{2}}\left(|\uparrow\rangle - |\downarrow\rangle\right) \\
& \neq \quad |\psi_1\rangle\ \ |\psi_2\rangle \\
& \Rightarrow \quad \text{states are } \textit{not} \text{ factorizable} \\
& \Rightarrow \quad \textit{entangled} \text{ particles}
\end{aligned}$$

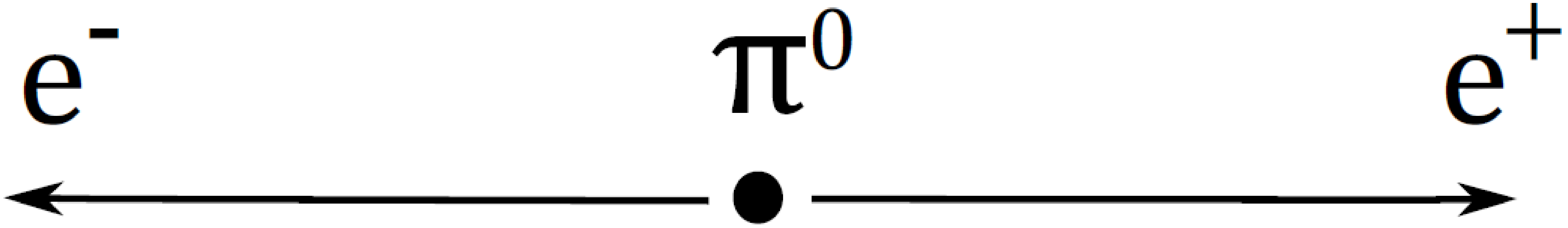
The approach of Quantum Information

- Where does entanglement come from?

Answer:
Entanglement comes from birth; just look at state preparation.

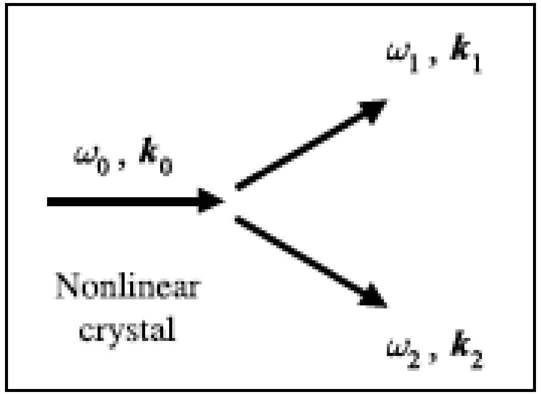
- How can I prepare a state of independent particles ?
- How can I prepare a state of entangled particles ?

producing entangled spins



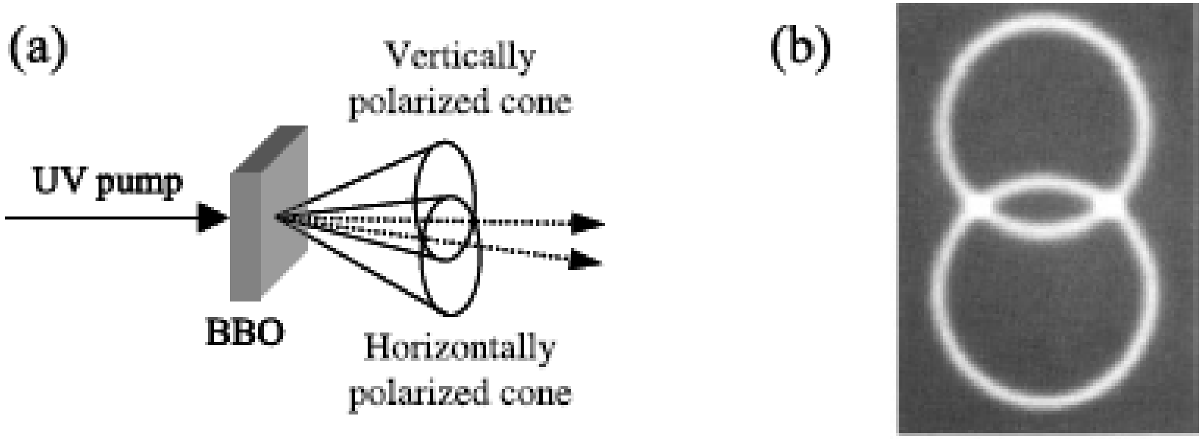
$$\vec{S}_{e^-} + \vec{S}_{e^+} = 0$$

producing entangled photons


ω_1 , $\boldsymbol{k}_1$
ω_0 , $\boldsymbol{k}_0$
Nonlinear crystal
ω_2 , $\boldsymbol{k}_2$

$$\omega_0 = \omega_1 + \omega_2,$$

$$\boldsymbol{k}_0 = \boldsymbol{k}_1 + \boldsymbol{k}_2,$$



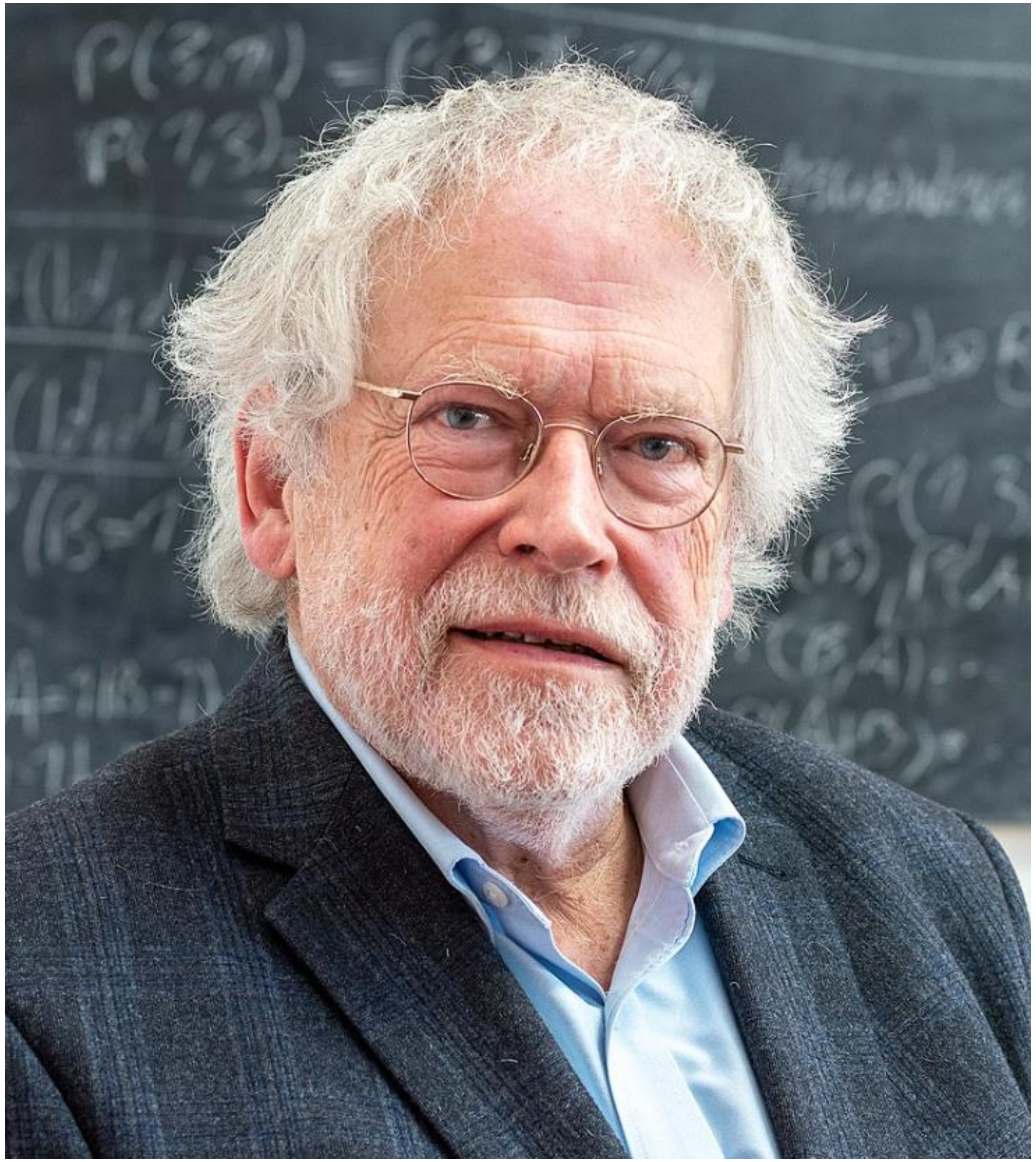
$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|\leftrightarrow_1, \updownarrow_2\rangle + \mathrm{e}^{\mathrm{i}\phi}|\updownarrow_1, \leftrightarrow_2\rangle\right)$$

BBO: beta-barium borate crystal used in type-II phase matching
(the down-converted photons have orthogonal polarizations)

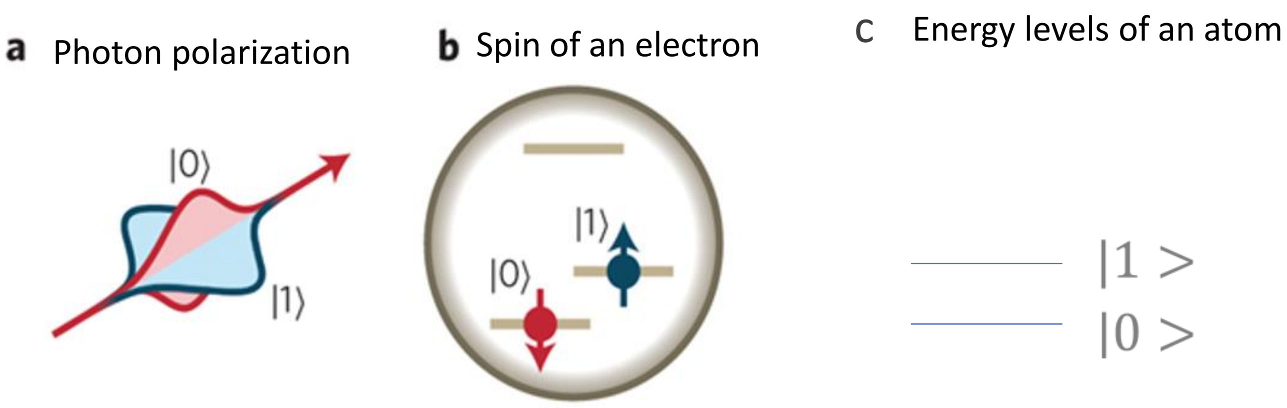
1990-2022 and beyond

Anton Zeilinger:
Quantum communication with photons as part of Quantum Information Science

Part I - Entanglement



Individual Quantum systems



a Photon polarization

b Spin of an electron

c Energy levels of an atom

Qubit: $|\psi\rangle = c_1 \, |0\rangle + c_2 \, |1\rangle$

Testing Entanglement in a 2 qubit system

Clauser-Holt-Horne-Shimony (CHSH) polynomial is defined as

$$\begin{aligned} B_{\mathrm{CHSH}} &= ab + ab' + a'b - a'b' & (2) \\ &= a(b + b') + a'(b - b') & (3) \end{aligned}$$

The principle of local realism (LR, initials of *Local Realism*) assumes that

- the result of a measurement in one system cannot instantly influence the result of a measurement in a second system.
- the values of physical quantities have a physical reality independently of being measured or not.
- one of the terms of the expression (3) is null and the other is ±2, thus $\langle B_{\mathrm{CHSH}} \rangle^{\mathrm{LR}} = 2$.

Testing Entanglement in a 2 qubit system

In Quantum Mechanics the quantities a,a', b and b' are Pauli spin operators, with eigenvalues ± 1 and such that

$$a^2 = a'^2 = b^2 = b'^2 = \mathbb{1}\ . \tag{4}$$

Bell operator is written as

$$B_{\mathrm{CHSH}} = a \otimes b + a \otimes b' + a \otimes' b - a' \otimes b' \tag{5}$$

Combining (4) and (5) we get

$$B^2_{\mathrm{CHSH}} = 4\mathbb{1}_a \otimes \mathbb{1}_b - [a, a'] \otimes [b, b'] \tag{6}$$

Assuming local realism, all observables commute, thus

$$\langle B_{\mathrm{CHSH}} \rangle^{\mathrm{LR}} = \sqrt{\langle B^2_{\mathrm{CHSH}} \rangle^{\mathrm{LR}}} = \sqrt{4} = 2\ .$$

Testing Entanglement in a 2 qubit system

- In Quantum Mechanics, the a, a' and b, b' observables do not commute.
- The observables a, a' and b, b' are represented by Pauli operators obeying the relations $[\sigma_j, \sigma_k] = 2\, i\, \epsilon_{jkl}\, \sigma_l$.
- σ_l has eigenvalues ± 1, the absolute maximum value of the commutators eigenvalues is 2.
- The maximum value of $\langle B_{\mathrm{CHSH}} \rangle$ predicted by Quantum Mechanics is

$$\langle B_{\mathrm{CHSH}} \rangle^{\mathrm{QM}} = \sqrt{\langle B^2_{\mathrm{CHSH}} \rangle^{\mathrm{QM}}} = \sqrt{8} = 2\sqrt{2}\ .$$

- Local realism leads to inequality $\langle B_{\mathrm{CHSH}} \rangle \leq 2$, whose violation is demonstrated experimentally choosing a two-qubit state for which Quantum Mechanics predicts $\langle B_{\mathrm{CHSH}} \rangle = 2\sqrt{2}$.

Measurement of non-locality and entanglement

- The violation of a Bell inequality can be characterized by the ratio $R(B)$ associated with a Bell polynomial:

$$R(B) = \frac{\langle B \rangle^{\mathrm{QM}}}{\langle B \rangle^{\mathrm{LR}}}$$

- The value of $R(B)$ is a measure of non-locality because if $R(B) > 1$ the state cannot be described by local realism.

1990 - Mermim inequalities

- In 1990 Mermin showed, that, for an odd number of qubits, the quantity R is maximized using so-called Mermin inequalities.
- For n qubits, inequalities are defined for the observables $a_1, a_2, \cdots, a_n$, all of which have eigenvalues ± 1.
- Mermim's polynomials, M_n, can be obtained by defining $M_1 \equiv 1$ and constructing M_n recursively from M_{n-1}.
- Mermim's M_2 polynomial is the B_{CHSH} polynomial.
- For $n = 3$ qubits we have

$$M_3 = (a_1 a_2 a_3' + a_1 a_2' a_3 + a_1' a_2 a_3) - (a_1' a_2' a_3') \qquad (7)$$

whose square is

$$\begin{aligned} M_3^2 = \quad & 4 \quad \mathbb{1}_1 \otimes \mathbb{1}_2 \otimes \mathbb{1}_3 - ([a_1, a_1'] \otimes [a_2, a_2'] \otimes \mathbb{1}_3 + \\ & + \quad [a_1, a_1'] \otimes \mathbb{1}_2 \otimes [a_3, a_3'] + \mathbb{1}_1 \otimes [a_2, a_2'] \otimes [a_3, a_3']) \end{aligned}$$

Testing Entanglement in a 3 qubit system

- Assuming local realism, all variables commute, thus $\langle M_3 \rangle^{\mathrm{LR}} = \sqrt{4} = 2$.
- The maximum value of $\langle M_3 \rangle^{\mathrm{QM}}$ is $\langle M_3 \rangle^{\mathrm{QM}} = \sqrt{4 + 4 \times 3} = 4$.
- The maximum value of R for $n = 3$ is $R(M_3) = \frac{\langle M_3 \rangle^{\mathrm{QM}}}{\langle M_3 \rangle^{\mathrm{LR}}} = \frac{4}{2} = 2$.
- In general, for n qubits, a state of type GHZ

  $$|\Psi_{\mathrm{GHZ}}\rangle = \frac{1}{\sqrt{2}} \left(|00 \cdots 0\rangle + e^{i\phi} |11 \cdots 1\rangle \right)$$

  produces the maximum violation of the Mermim inequality.
- The cases $n = 2$ and $n = 3$ also correspond to states where the entanglement is maximum.
- However, the same is not true for $n \geq 4$.

GHZ paradox (Greenberger, Horne, Zeilinger; 1989)

$$|\chi\rangle = \frac{1}{\sqrt{2}}\Big(\,|\uparrow^A\uparrow^B\uparrow^C\rangle - |\downarrow^A\downarrow^B\downarrow^C\rangle \Big)$$

Prepare four identical states $|\chi\rangle$ and perform the measurements:

$$\begin{array}{lccccr}
1 & \sigma_x^{(A)} & \sigma_y^{(B)} & \sigma_y^{(C)} & & \langle\sigma_x^{(A)}\,\sigma_y^{(B)}\sigma_y^{(C)}\rangle = +1 \\
2 & \sigma_y^{(A)} & \sigma_x^{(B)} & \sigma_y^{(C)} & & \langle\sigma_y^{(A)}\,\sigma_x^{(B)}\sigma_y^{(C)}\rangle = +1 \\
3 & \sigma_y^{(A)} & \sigma_y^{(B)} & \sigma_x^{(C)} & & \langle\sigma_y^{(A)}\,\sigma_y^{(B)}\sigma_x^{(C)}\rangle = +1 \\
4 & \sigma_x^{(A)} & \sigma_x^{(B)} & \sigma_x^{(C)} & & \langle\sigma_x^{(A)}\,\sigma_x^{(B)}\sigma_x^{(C)}\rangle = -1 \\
\hline
\end{array}$$

local realism: $+1$ MQ: -1

Experimental Test: Pan, Zeilinger et al, Nature 403, 515 (2000)

Winner : Quantum Mechanics !

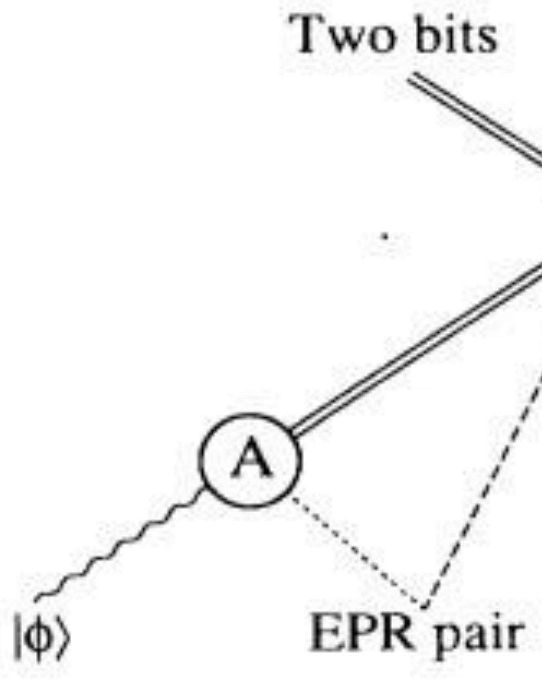
- Conclusion of Bell and GHZ experiments: **Nature does not obey simultaneously to locality and realism.**

- What does it mean not obeying to locality?
  Means that the result of a measurement can be influenced instantaneously by a distant event; however, such influences, if they exist, cannot propagate at a speed larger that the speed of light in vaccum, cannot transport energy or information. The influence corresponds solely to a correlation of data.

- What does it mean not obeying to realism?
  Means that the physical properties are not defined prior to observation and independently of observation.

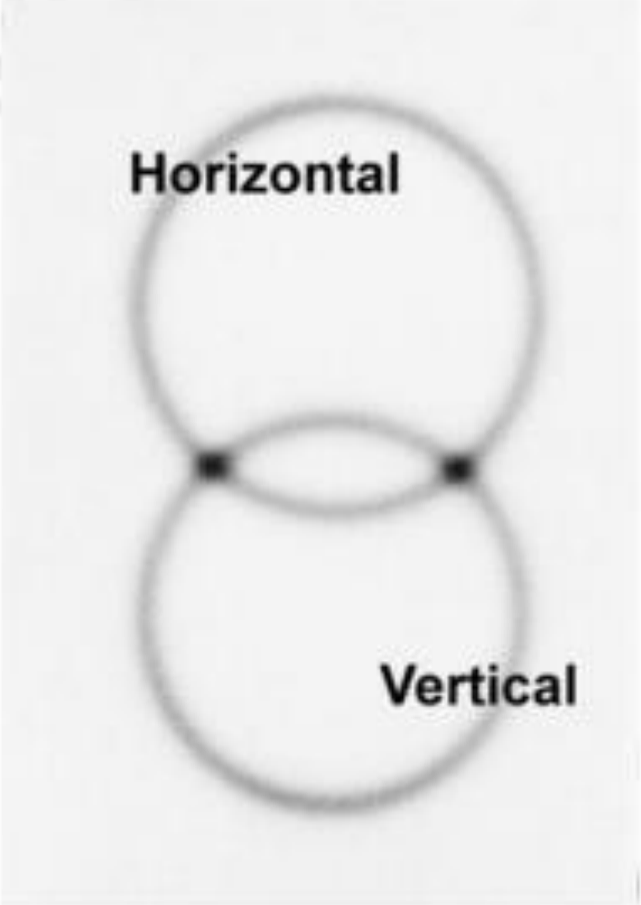
Aplications: quantum teleportation, superdense coding, quantum encriptation

1993 – Bennet: proposal for Quantum teleportation

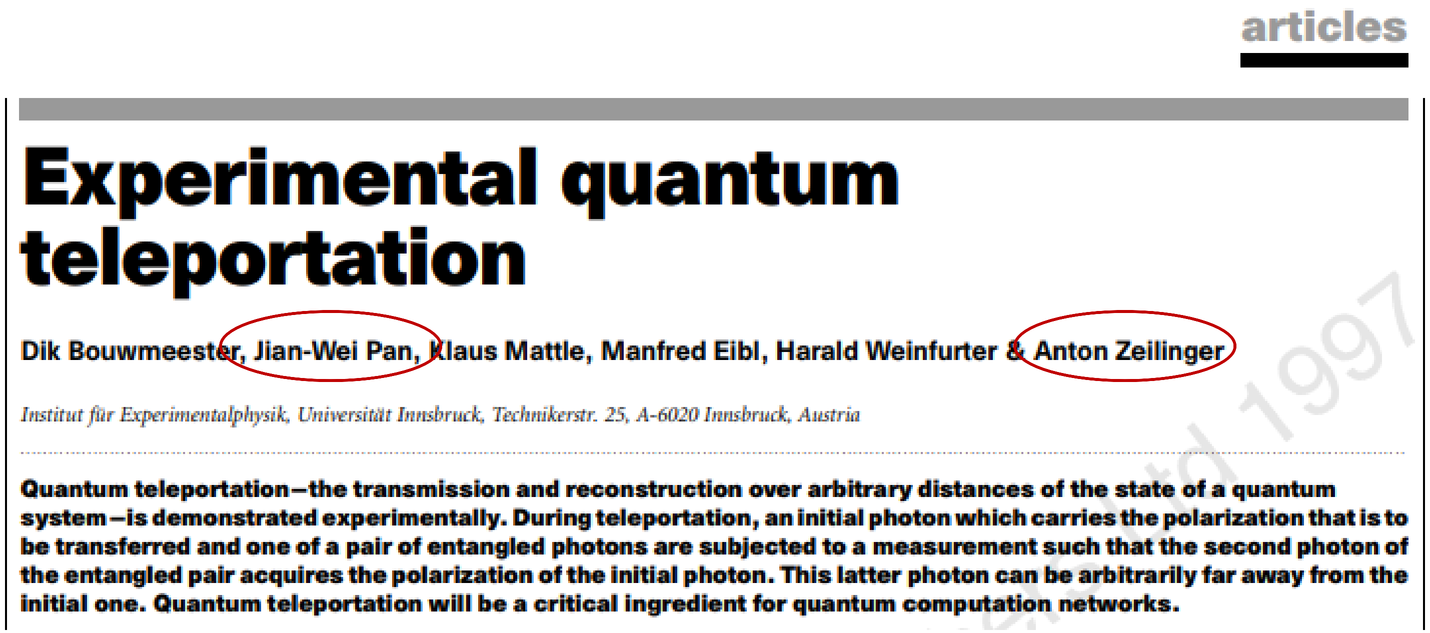


The solid lines represent a classical pair of bits, the dashed lines an EPR pair of particles, and the wavy line a quantum particle in an unknown state I Φ). Alice (A) performs a quantum measurement, and Bob (B) a unitary operation.

1997 - First Quantum Teleportation experiment



Photons emerging from type II down-conversion (see text). Phc
rpendicular to the propagation direction. Photons are produced
n on the top circle is horizontally polarized while its exactly
n the bottom circle is vertically polarized. At the intersection po
ions are undefined; all that is known is that they have to be
sults in entanglement.



articles

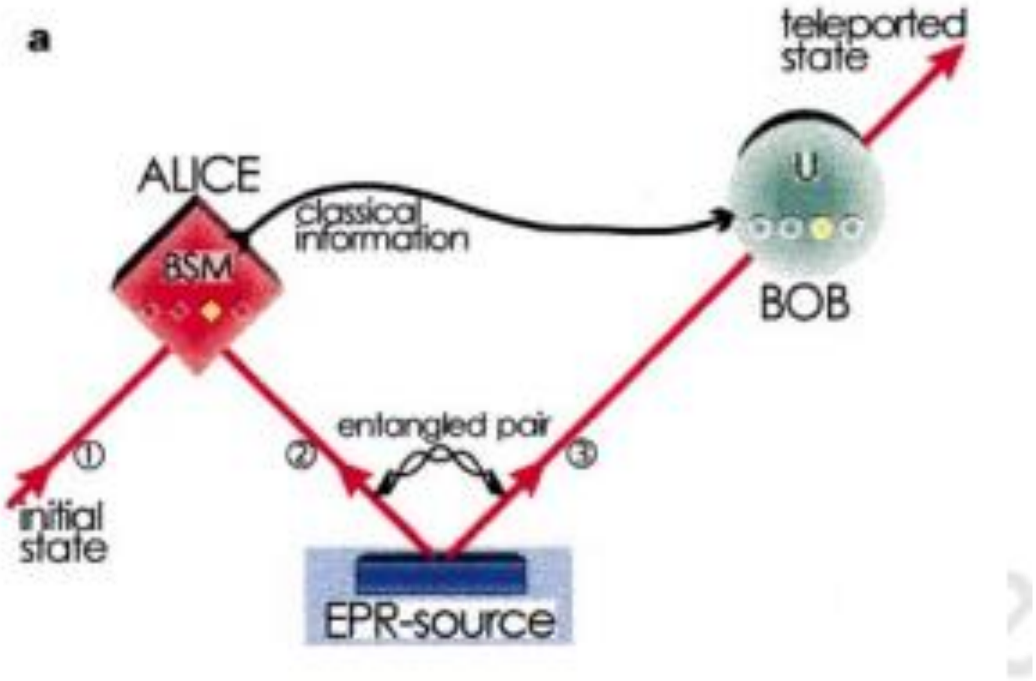
Experimental quantum teleportation

Dik Bouwmeester, Jian-Wei Pan, Klaus Mattle, Manfred Eibl, Harald Weinfurter & Anton Zeilinger

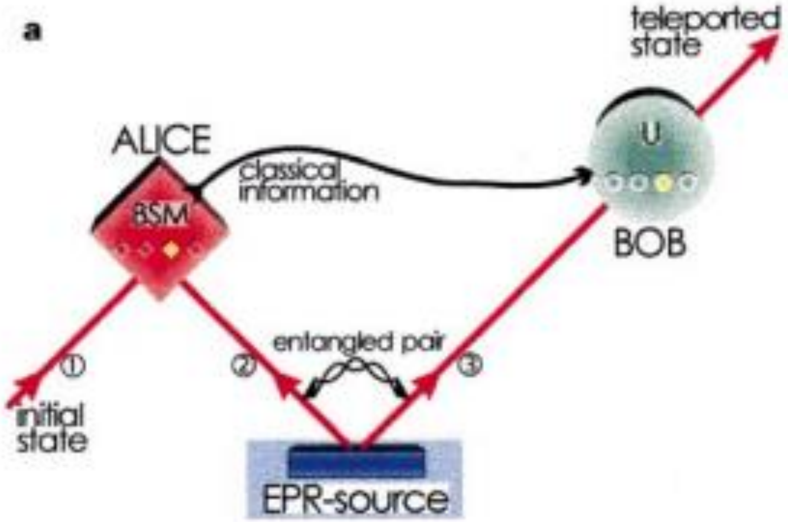
Institut für Experimentalphysik, Universität Innsbruck, Technikerstr. 25, A-6020 Innsbruck, Austria

Quantum teleportation—the transmission and reconstruction over arbitrary distances of the state of a quantum system—is demonstrated experimentally. During teleportation, an initial photon which carries the polarization that is to be transferred and one of a pair of entangled photons are subjected to a measurement such that the second photon of the entangled pair acquires the polarization of the initial photon. This latter photon can be arbitrarily far away from the initial one. Quantum teleportation will be a critical ingredient for quantum computation networks.

1997 - First Quantum Teleportation experiment



Quantum Teleportation



BSM : Bell State Measurement

$$
\begin{aligned}
|\psi_0\rangle &= |\psi\rangle_c \, |\beta_{00}\rangle_{ab} \\
&= \tfrac{1}{2}|\beta_{00}\rangle_{ca} \otimes (\alpha|0\rangle_b + \beta|1\rangle_b) + \\
&\quad \tfrac{1}{2}|\beta_{01}\rangle_{ca} \otimes (\beta|0\rangle_b + \alpha|1\rangle_b) + \\
&\quad \tfrac{1}{2}|\beta_{10}\rangle_{ca} \otimes (\alpha|0\rangle_b + \beta|1\rangle_b) + \\
&\quad \tfrac{1}{2}|\beta_{11}\rangle_{ca} \otimes (-\beta|0\rangle_b + \alpha|1\rangle_b)
\end{aligned}
$$

Alice		Bob
M_1 M_2		
0 0	$\mapsto$	$\alpha|0\rangle + \beta|1\rangle$
0 1	$\mapsto$	$\beta|0\rangle + \alpha|1\rangle$
1 0	$\mapsto$	$\alpha|0\rangle - \beta|1\rangle$
1 1	$\mapsto$	$-\beta|0\rangle + \alpha|1\rangle$

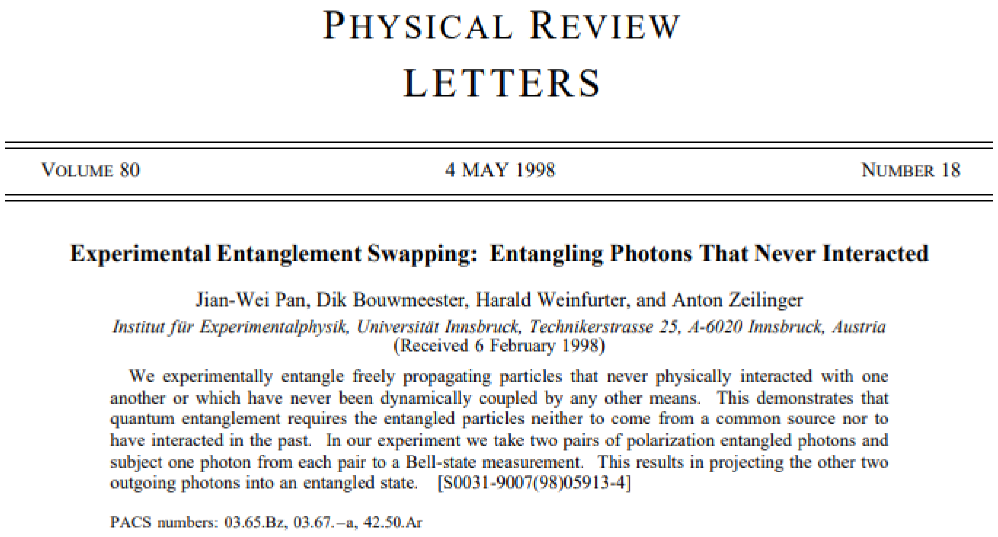
Quantum Teleportation

- Allows the transmission of a state without a physical transport of the particle.

- Transmission of information is not instantaneous! It requires sending classic bits.

- The transmission of the state is not a copy. The original qubit becomes a bit at the end.

1998 – first demonstration of entanglement swapping (Jian-Wei Pan, H. Weinfurter and Zeilinger)



PHYSICAL REVIEW LETTERS

VOLUME 80 | 4 MAY 1998 | NUMBER 18

Experimental Entanglement Swapping: Entangling Photons That Never Interacted

Jian-Wei Pan, Dik Bouwmeester, Harald Weinfurter, and Anton Zeilinger

Institut für Experimentalphysik, Universität Innsbruck, Technikerstrasse 25, A-6020 Innsbruck, Austria

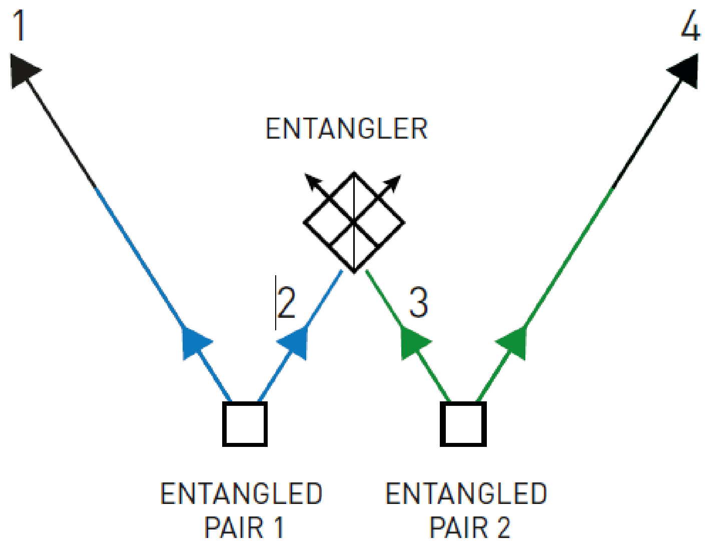
(Received 6 February 1998)

We experimentally entangle freely propagating particles that never physically interacted with one another or which have never been dynamically coupled by any other means. This demonstrates that quantum entanglement requires the entangled particles neither to come from a common source nor to have interacted in the past. In our experiment we take two pairs of polarization entangled photons and subject one photon from each pair to a Bell-state measurement. This results in projecting the other two outgoing photons into an entangled state. [S0031-9007(98)05913-4]

PACS numbers: 03.65.Bz, 03.67.–a, 42.50.Ar

Entangled particles that never met

Two pairs of entangled particles are emitted from different sources. One particle from each pair is brought together in a special way that entangles them. The two other particles (1 and 4 in the diagram) are then also entangled. In this way, two particles that have never been in contact can become entangled.



2015-2017 Loop-hole free Bell tests

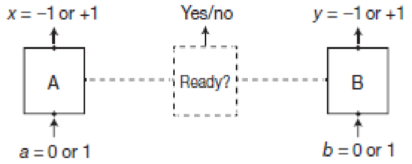
682 | NATURE | VOL 526 | 29 OCTOBER 2015

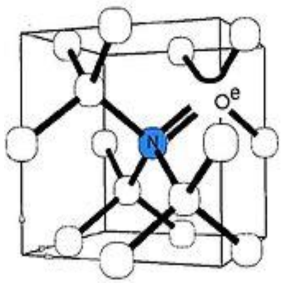
LETTER

doi:10.1038/nature15759

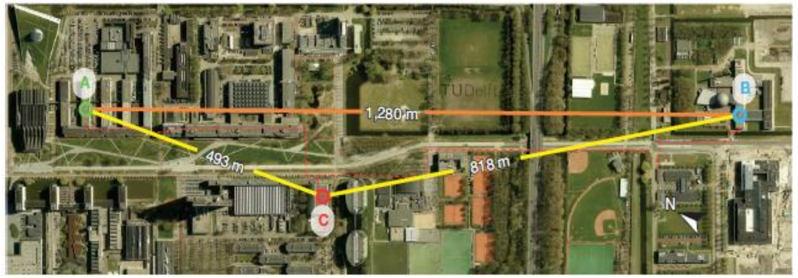
Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres

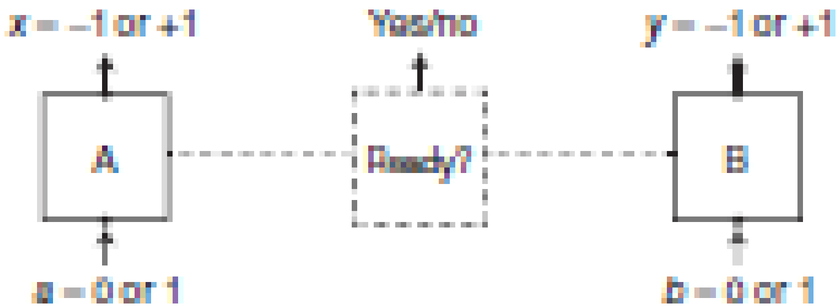
B. Hensen[1,2], H. Bernien[1,2]†, A. E. Dréau[1,2], A. Reiserer[1,2], N. Kalb[1,2], M. S. Blok[1,2], J. Ruitenberg[1,2], R. F. L. Vermeulen[1,2], R. N. Schouten[1,2], C. Abellán[3], W. Amaya[3], V. Pruneri[3,4], M. W. Mitchell[3,4], M. Markham[5], D. J. Twitchen[5], D. Elkouss[1], S. Wehner[1], T. H. Taminiau[1,2] & R. Hanson[1,2]





Nitrogen-vacancy center





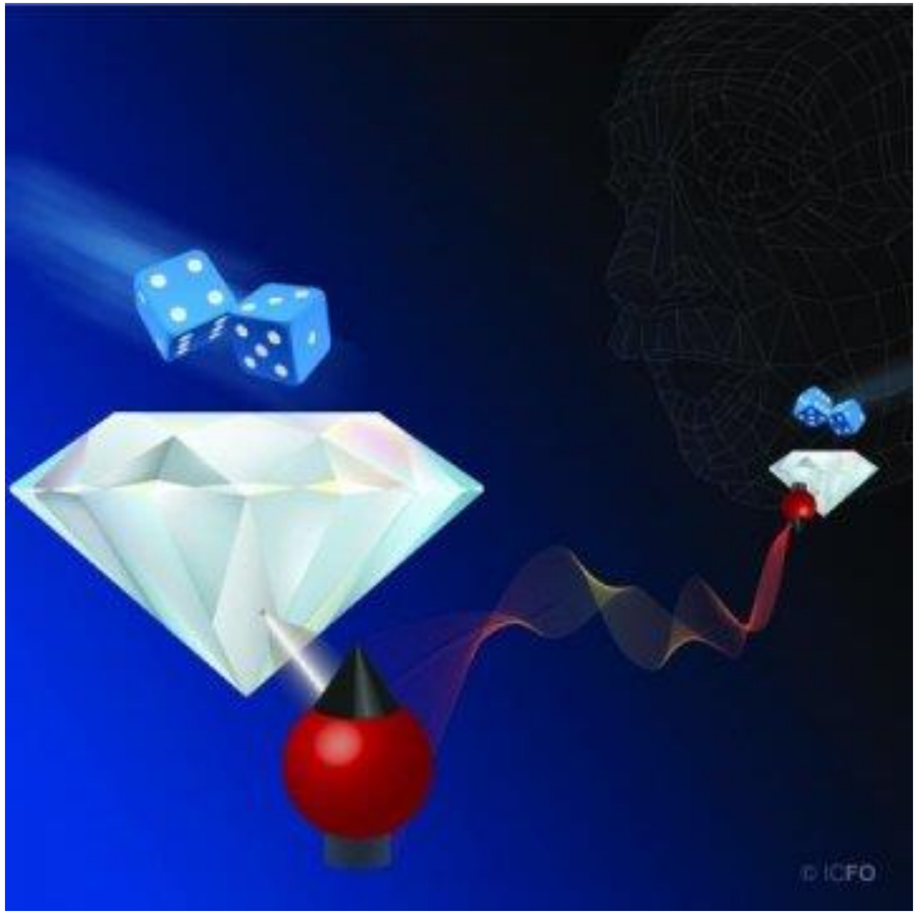
BOX A – random bit a
a=0 : spin measured along Z direction
a=1: spin measured along X direction

BOX B - random bit b
b=0 : spin measured along (-Z+X)/$\sqrt{2}$ direction
B=1: spin measured along (Z+X)$\sqrt{2}$ direction

If nature obeys both locality and realism:

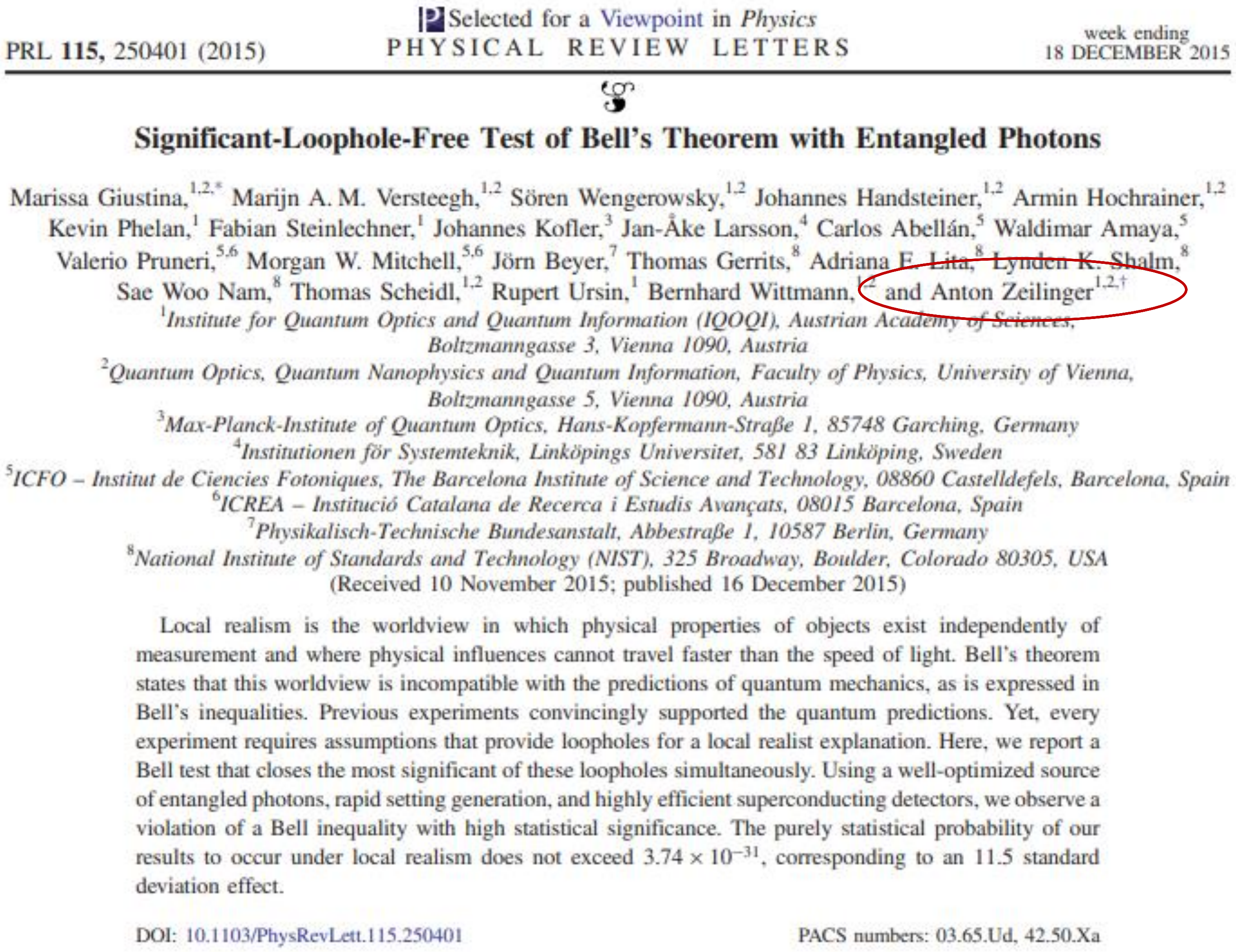
$$S = |P_{00} - P_{01} + P_{10} + P_{11}| \leq 2.$$

Experiment result: S=2.42±0.20 with 245 trials



$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow^{(1)}\rangle|\downarrow^{(2)}\rangle - |\downarrow^{(1)}\rangle|\uparrow^{(2)}\rangle\right)$$

Electronic spin associated with a single nitrogen-vacancy defect centre in diamond



Selected for a Viewpoint in *Physics*

PRL **115,** 250401 (2015) PHYSICAL REVIEW LETTERS week ending 18 DECEMBER 2015

Significant-Loophole-Free Test of Bell's Theorem with Entangled Photons

Marissa Giustina,[1,2,*] Marijn A. M. Versteegh,[1,2] Sören Wengerowsky,[1,2] Johannes Handsteiner,[1,2] Armin Hochrainer,[1,2] Kevin Phelan,[1] Fabian Steinlechner,[1] Johannes Kofler,[3] Jan-Åke Larsson,[4] Carlos Abellán,[5] Waldimar Amaya,[5] Valerio Pruneri,[5,6] Morgan W. Mitchell,[5,6] Jörn Beyer,[7] Thomas Gerrits,[8] Adriana E. Lita,[8] Lynden K. Shalm,[8] Sae Woo Nam,[8] Thomas Scheidl,[1,2] Rupert Ursin,[1] Bernhard Wittmann,[1,2] and Anton Zeilinger[1,2,†]

[1]*Institute for Quantum Optics and Quantum Information (IQOQI), Austrian Academy of Sciences, Boltzmanngasse 3, Vienna 1090, Austria*

[2]*Quantum Optics, Quantum Nanophysics and Quantum Information, Faculty of Physics, University of Vienna, Boltzmanngasse 5, Vienna 1090, Austria*

[3]*Max-Planck-Institute of Quantum Optics, Hans-Kopfermann-Straße 1, 85748 Garching, Germany*

[4]*Institutionen för Systemteknik, Linköpings Universitet, 581 83 Linköping, Sweden*

[5]*ICFO – Institut de Ciencies Fotoniques, The Barcelona Institute of Science and Technology, 08860 Castelldefels, Barcelona, Spain*

[6]*ICREA – Institució Catalana de Recerca i Estudis Avançats, 08015 Barcelona, Spain*

[7]*Physikalisch-Technische Bundesanstalt, Abbestraße 1, 10587 Berlin, Germany*

[8]*National Institute of Standards and Technology (NIST), 325 Broadway, Boulder, Colorado 80305, USA*

(Received 10 November 2015; published 16 December 2015)

Local realism is the worldview in which physical properties of objects exist independently of measurement and where physical influences cannot travel faster than the speed of light. Bell's theorem states that this worldview is incompatible with the predictions of quantum mechanics, as is expressed in Bell's inequalities. Previous experiments convincingly supported the quantum predictions. Yet, every experiment requires assumptions that provide loopholes for a local realist explanation. Here, we report a Bell test that closes the most significant of these loopholes simultaneously. Using a well-optimized source of entangled photons, rapid setting generation, and highly efficient superconducting detectors, we observe a violation of a Bell inequality with high statistical significance. The purely statistical probability of our results to occur under local realism does not exceed 3.74×10^{-31}, corresponding to an 11.5 standard deviation effect.

DOI: 10.1103/PhysRevLett.115.250401 PACS numbers: 03.65.Ud, 42.50.Xa

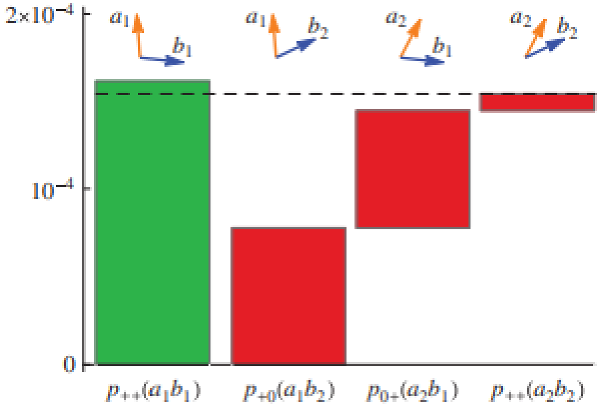
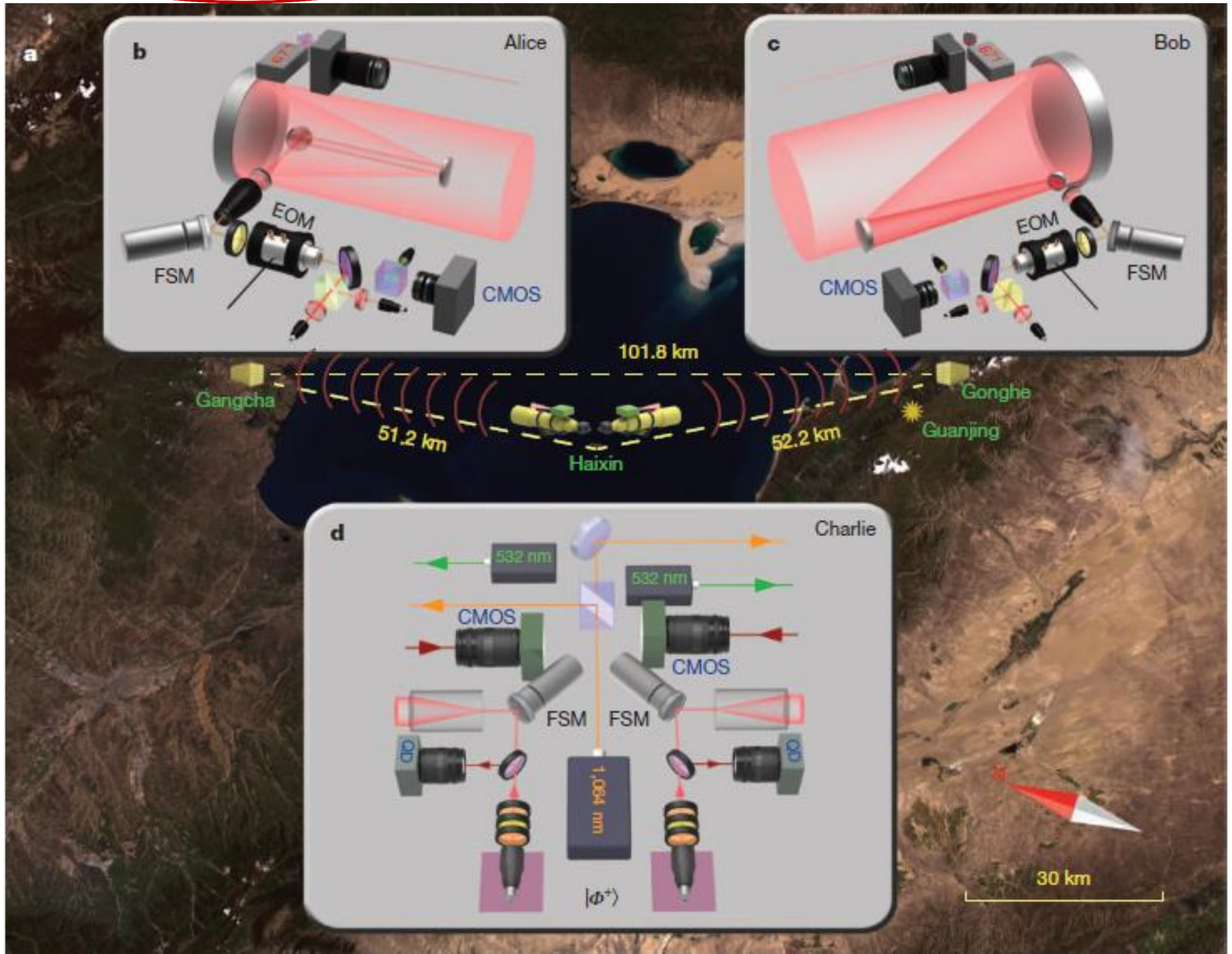


FIG. 3 (color). Bar chart of the four joint probabilities entering the Bell inequality (1). Since the green bar representing $p_{++}(a_1b_1)$ outweighs the sum of the other three red bars, the J value is positive and the CH-Eberhard inequality is violated.

Quantum teleportation and entanglement distribution over 100-kilometre free-space channels

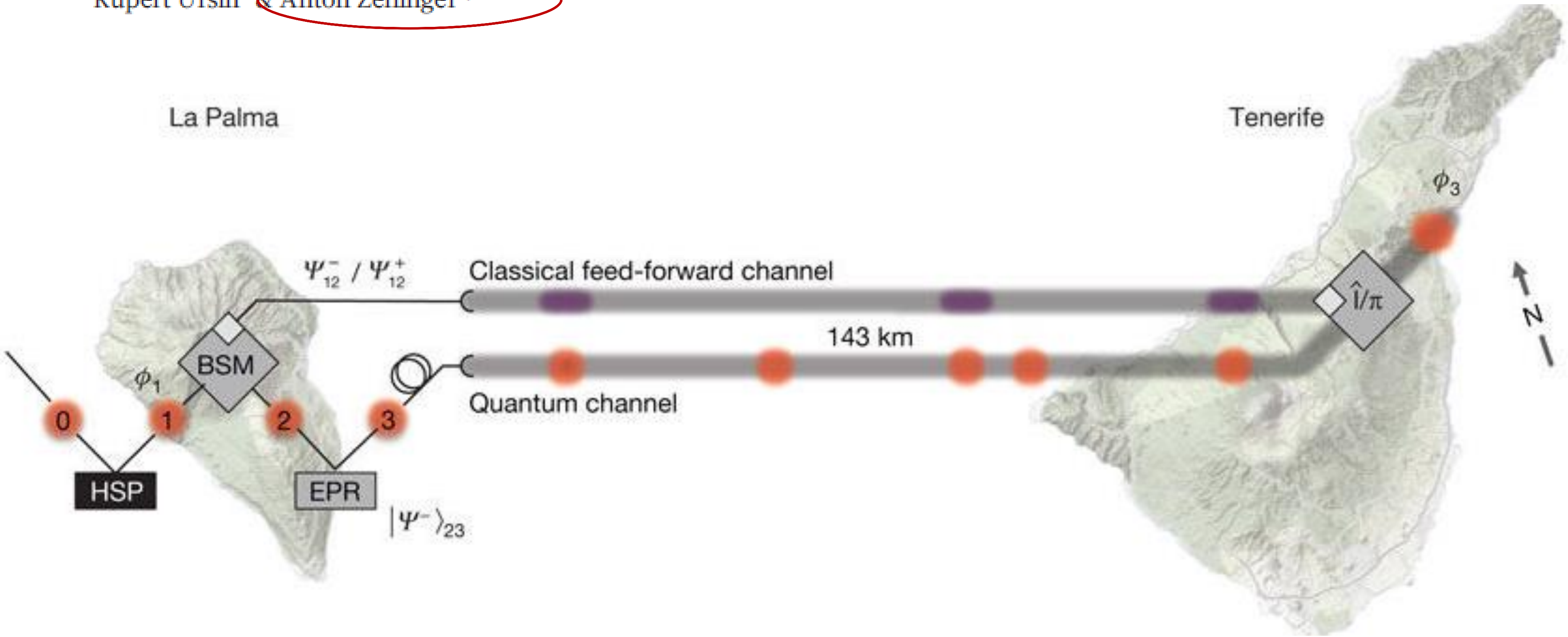
Juan Yin[1]*, Ji-Gang Ren[1]*, He Lu[1]*, Yuan Cao[1], Hai-Lin Yong[1], Yu-Ping Wu[1], Chang Liu[1], Sheng-Kai Liao[1], Fei Zhou[1], Yan Jiang[1], Xin-Dong Cai[1], Ping Xu[1], Ge-Sheng Pan[1], Jian-Jun Jia[2], Yong-Mei Huang[3], Hao Yin[1], Jian-Yu Wang[2], Yu-Ao Chen[1], Cheng-Zhi Peng[1] & Jian-Wei Pan[1]



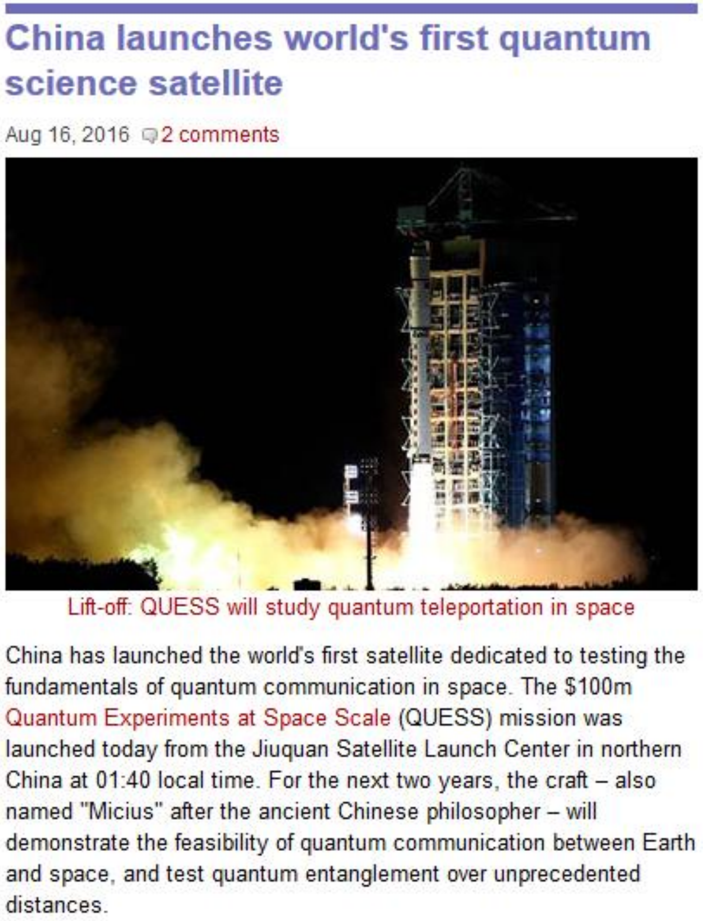
Nature **489**, 269–273 (13 September 2012)

Quantum teleportation over 143 kilometres using active feed-forward

Xiao-Song Ma[1,2]†, Thomas Herbst[1,2], Thomas Scheidl[1], Daqing Wang[1], Sebastian Kropatschek[1], William Naylor[1], Bernhard Wittmann[1,2], Alexandra Mech[1,2], Johannes Kofler[1,3], Elena Anisimova[4], Vadim Makarov[4], Thomas Jennewein[1,4], Rupert Ursin[1] & Anton Zeilinger[1,2]



2016 – First Quantum communication satellite

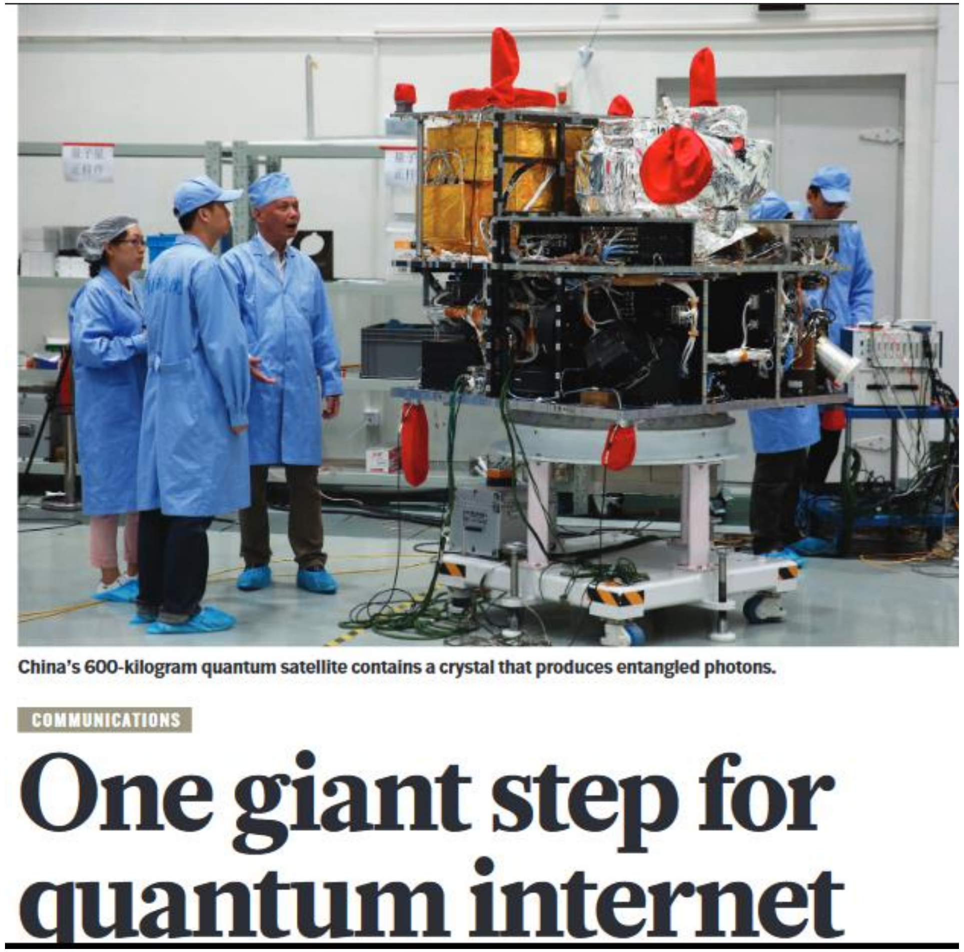


China launches world's first quantum science satellite

Aug 16, 2016 2 comments

Lift-off: QUESS will study quantum teleportation in space

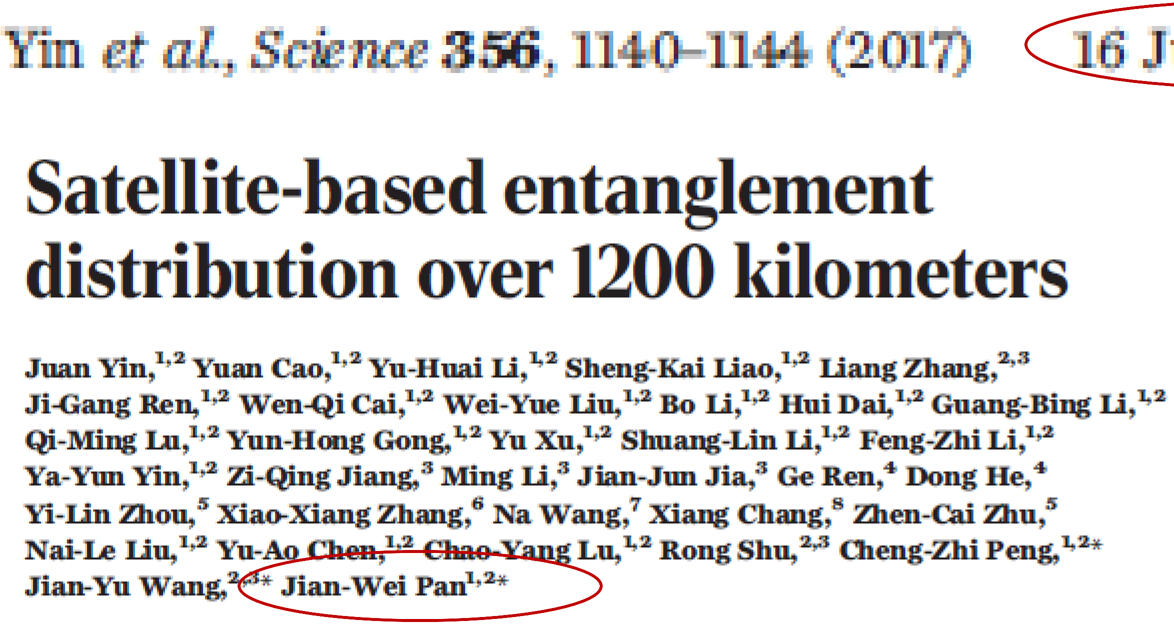
China has launched the world's first satellite dedicated to testing the fundamentals of quantum communication in space. The $100m Quantum Experiments at Space Scale (QUESS) mission was launched today from the Jiuquan Satellite Launch Center in northern China at 01:40 local time. For the next two years, the craft – also named "Micius" after the ancient Chinese philosopher – will demonstrate the feasibility of quantum communication between Earth and space, and test quantum entanglement over unprecedented distances.



China's 600-kilogram quantum satellite contains a crystal that produces entangled photons.

COMMUNICATIONS

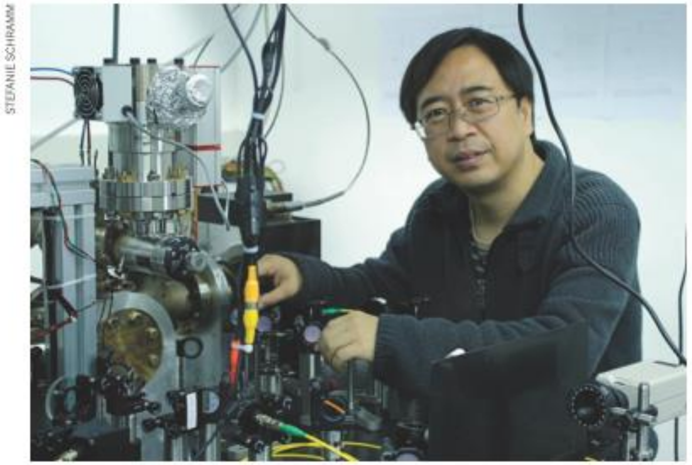
One giant step for quantum internet



Yin *et al.*, *Science* **356**, 1140–1144 (2017) 16 June 2017

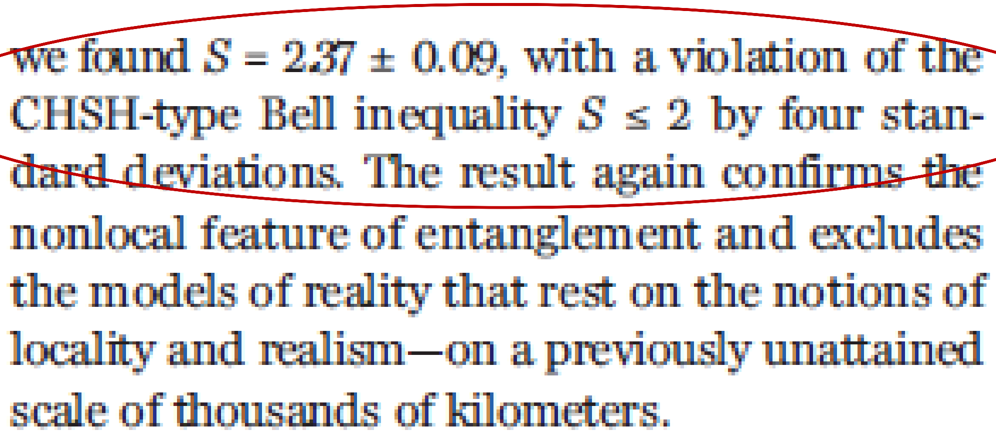
Satellite-based entanglement distribution over 1200 kilometers

Juan Yin,[1,2] Yuan Cao,[1,2] Yu-Huai Li,[1,2] Sheng-Kai Liao,[1,2] Liang Zhang,[2,3] Ji-Gang Ren,[1,2] Wen-Qi Cai,[1,2] Wei-Yue Liu,[1,2] Bo Li,[1,2] Hui Dai,[1,2] Guang-Bing Li,[1,2] Qi-Ming Lu,[1,2] Yun-Hong Gong,[1,2] Yu Xu,[1,2] Shuang-Lin Li,[1,2] Feng-Zhi Li,[1,2] Ya-Yun Yin,[1,2] Zi-Qing Jiang,[3] Ming Li,[3] Jian-Jun Jia,[3] Ge Ren,[4] Dong He,[4] Yi-Lin Zhou,[5] Xiao-Xiang Zhang,[6] Na Wang,[7] Xiang Chang,[8] Zhen-Cai Zhu,[5] Nai-Le Liu,[1,2] Yu-Ao Chen,[1,2] Chao-Yang Lu,[1,2] Rong Shu,[2,3] Cheng-Zhi Peng,[1,2]* Jian-Yu Wang,[2,3]* Jian-Wei Pan[1,2]*



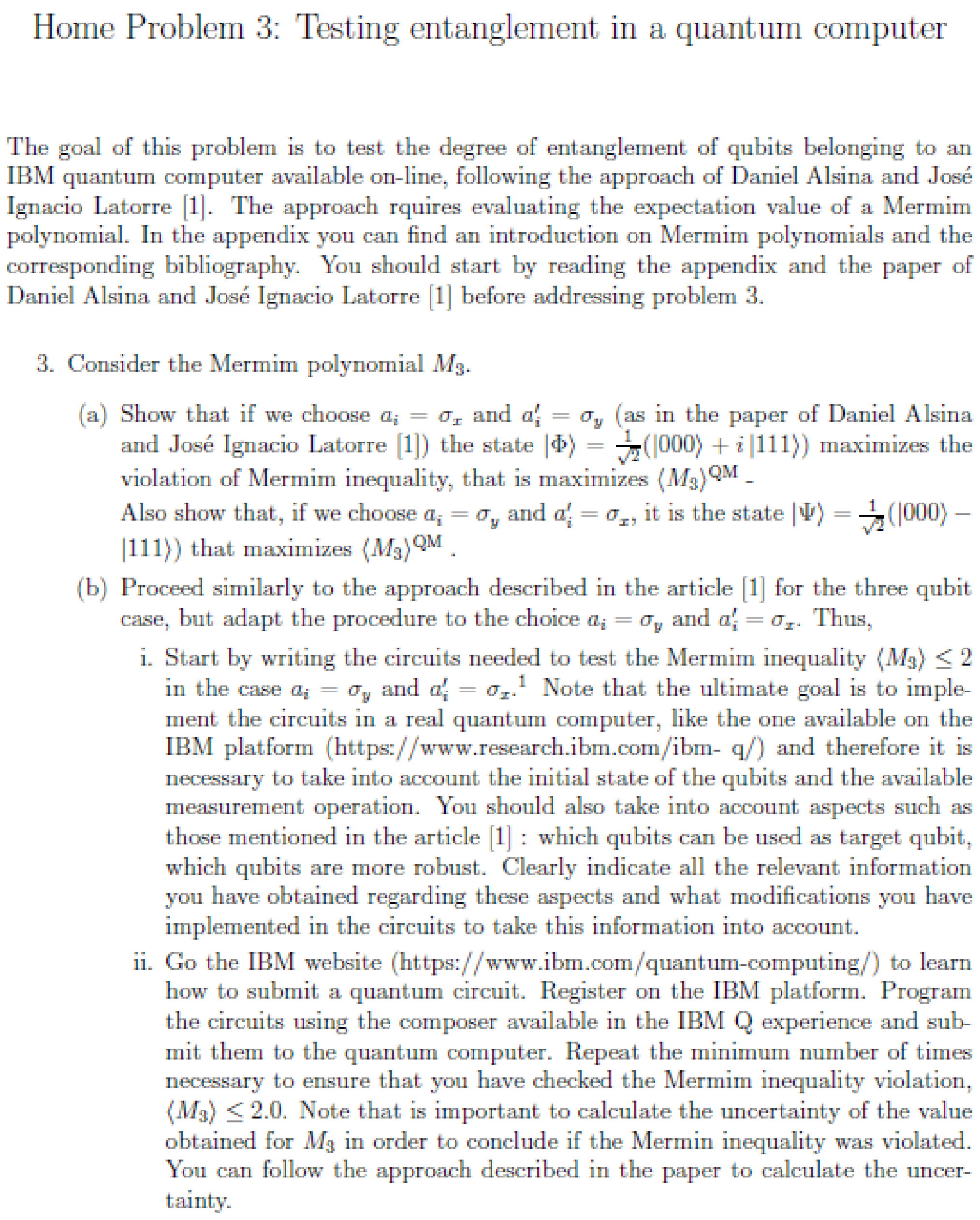
STEFANIE SCHRAMM

Jian Wei Pan



we found $S = 2.37 \pm 0.09$, with a violation of the CHSH-type Bell inequality $S \leq 2$ by four standard deviations. The result again confirms the nonlocal feature of entanglement and excludes the models of reality that rest on the notions of locality and realism—on a previously unattained scale of thousands of kilometers.

Violation of Bell inequality or Mermim inequality became a standard test for entanglement



Home Problem 3: Testing entanglement in a quantum computer

The goal of this problem is to test the degree of entanglement of qubits belonging to an IBM quantum computer available on-line, following the approach of Daniel Alsina and José Ignacio Latorre [1]. The approach rquires evaluating the expectation value of a Mermim polynomial. In the appendix you can find an introduction on Mermim polynomials and the corresponding bibliography. You should start by reading the appendix and the paper of Daniel Alsina and José Ignacio Latorre [1] before addressing problem 3.

3. Consider the Mermim polynomial M_3.

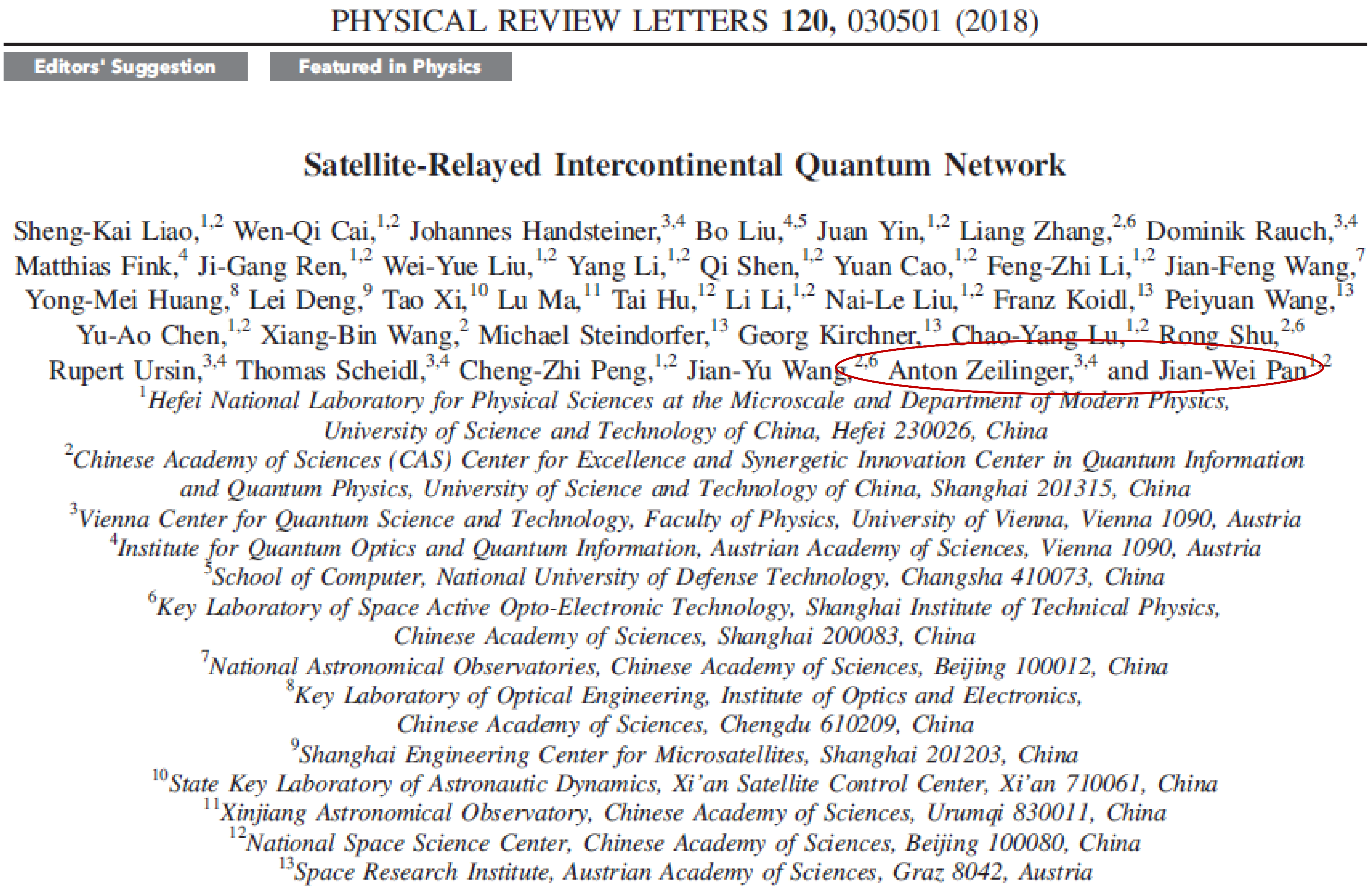
   (a) Show that if we choose $a_i = \sigma_x$ and $a'_i = \sigma_y$ (as in the paper of Daniel Alsina and José Ignacio Latorre [1]) the state $|\Phi\rangle = \frac{1}{\sqrt{2}}(|000\rangle + i\,|111\rangle)$ maximizes the violation of Mermim inequality, that is maximizes $\langle M_3 \rangle^{\mathrm{QM}}$.
   Also show that, if we choose $a_i = \sigma_y$ and $a'_i = \sigma_x$, it is the state $|\Psi\rangle = \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)$ that maximizes $\langle M_3 \rangle^{\mathrm{QM}}$.

   (b) Proceed similarly to the approach described in the article [1] for the three qubit case, but adapt the procedure to the choice $a_i = \sigma_y$ and $a'_i = \sigma_x$. Thus,

      i. Start by writing the circuits needed to test the Mermim inequality $\langle M_3 \rangle \leq 2$ in the case $a_i = \sigma_y$ and $a'_i = \sigma_x$.[1] Note that the ultimate goal is to implement the circuits in a real quantum computer, like the one available on the IBM platform (https://www.research.ibm.com/ibm- q/) and therefore it is necessary to take into account the initial state of the qubits and the available measurement operation. You should also take into account aspects such as those mentioned in the article [1] : which qubits can be used as target qubit, which qubits are more robust. Clearly indicate all the relevant information you have obtained regarding these aspects and what modifications you have implemented in the circuits to take this information into account.

      ii. Go the IBM website (https://www.ibm.com/quantum-computing/) to learn how to submit a quantum circuit. Register on the IBM platform. Program the circuits using the composer available in the IBM Q experience and submit them to the quantum computer. Repeat the minimum number of times necessary to ensure that you have checked the Mermim inequality violation, $\langle M_3 \rangle \leq 2.0$. Note that is important to calculate the uncertainty of the value obtained for M_3 in order to conclude if the Mermin inequality was violated. You can follow the approach described in the paper to calculate the uncertainty.

Main first goal of quantum internet: ultra-secure communications



PHYSICAL REVIEW LETTERS **120,** 030501 (2018)

Editors' Suggestion **Featured in Physics**

Satellite-Relayed Intercontinental Quantum Network

Sheng-Kai Liao,[1,2] Wen-Qi Cai,[1,2] Johannes Handsteiner,[3,4] Bo Liu,[4,5] Juan Yin,[1,2] Liang Zhang,[2,6] Dominik Rauch,[3,4] Matthias Fink,[4] Ji-Gang Ren,[1,2] Wei-Yue Liu,[1,2] Yang Li,[1,2] Qi Shen,[1,2] Yuan Cao,[1,2] Feng-Zhi Li,[1,2] Jian-Feng Wang,[7] Yong-Mei Huang,[8] Lei Deng,[9] Tao Xi,[10] Lu Ma,[11] Tai Hu,[12] Li Li,[1,2] Nai-Le Liu,[1,2] Franz Koidl,[13] Peiyuan Wang,[13] Yu-Ao Chen,[1,2] Xiang-Bin Wang,[2] Michael Steindorfer,[13] Georg Kirchner,[13] Chao-Yang Lu,[1,2] Rong Shu,[2,6] Rupert Ursin,[3,4] Thomas Scheidl,[3,4] Cheng-Zhi Peng,[1,2] Jian-Yu Wang,[2,6] Anton Zeilinger,[3,4] and Jian-Wei Pan[1,2]

[1]*Hefei National Laboratory for Physical Sciences at the Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei 230026, China*

[2]*Chinese Academy of Sciences (CAS) Center for Excellence and Synergetic Innovation Center in Quantum Information and Quantum Physics, University of Science and Technology of China, Shanghai 201315, China*

[3]*Vienna Center for Quantum Science and Technology, Faculty of Physics, University of Vienna, Vienna 1090, Austria*

[4]*Institute for Quantum Optics and Quantum Information, Austrian Academy of Sciences, Vienna 1090, Austria*

[5]*School of Computer, National University of Defense Technology, Changsha 410073, China*

[6]*Key Laboratory of Space Active Opto-Electronic Technology, Shanghai Institute of Technical Physics, Chinese Academy of Sciences, Shanghai 200083, China*

[7]*National Astronomical Observatories, Chinese Academy of Sciences, Beijing 100012, China*

[8]*Key Laboratory of Optical Engineering, Institute of Optics and Electronics, Chinese Academy of Sciences, Chengdu 610209, China*

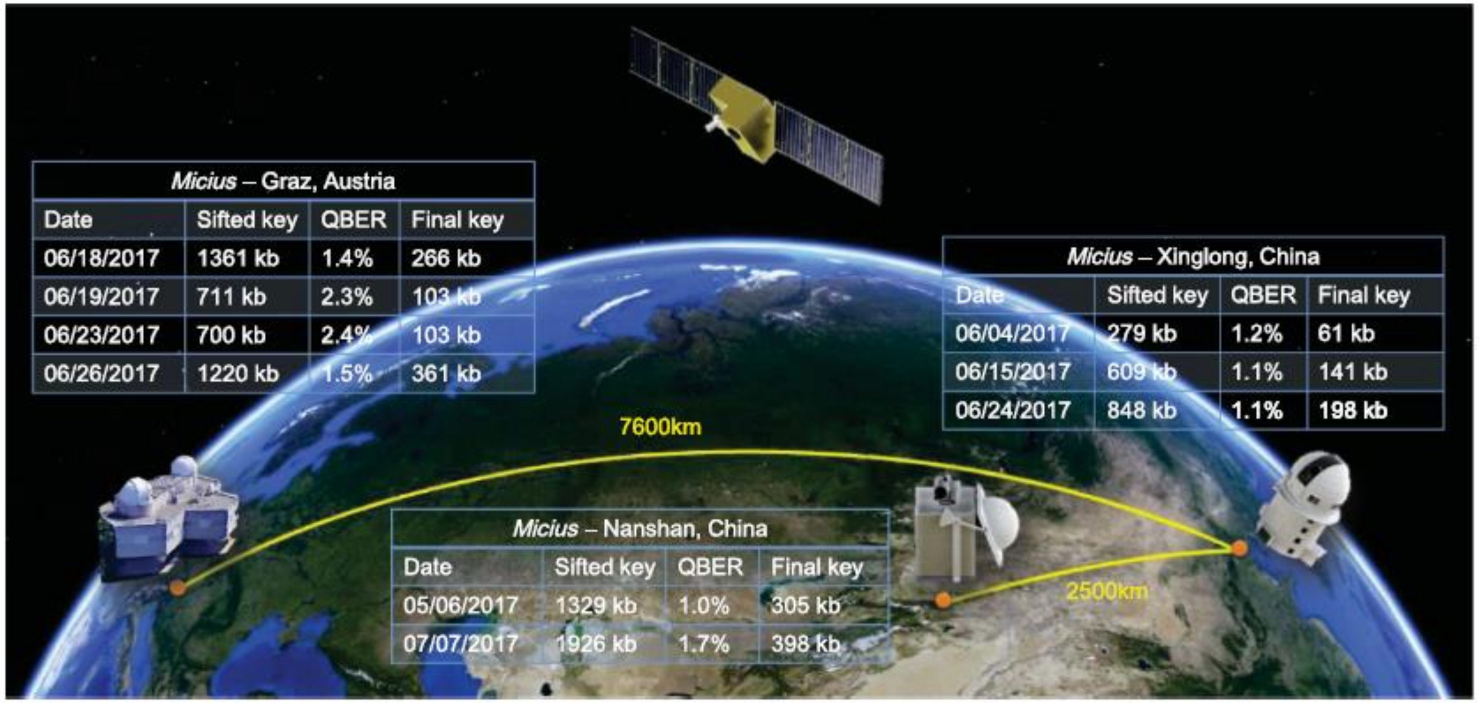
[9]*Shanghai Engineering Center for Microsatellites, Shanghai 201203, China*

[10]*State Key Laboratory of Astronautic Dynamics, Xi'an Satellite Control Center, Xi'an 710061, China*

[11]*Xinjiang Astronomical Observatory, Chinese Academy of Sciences, Urumqi 830011, China*

[12]*National Space Science Center, Chinese Academy of Sciences, Beijing 100080, China*

[13]*Space Research Institute, Austrian Academy of Sciences, Graz 8042, Austria*



Micius – Graz, Austria

Date	Sifted key	QBER	Final key
06/18/2017	1361 kb	1.4%	266 kb
06/19/2017	711 kb	2.3%	103 kb
06/23/2017	700 kb	2.4%	103 kb
06/26/2017	1220 kb	1.5%	361 kb

Micius – Xinglong, China

Date	Sifted key	QBER	Final key
06/04/2017	279 kb	1.2%	61 kb
06/15/2017	609 kb	1.1%	141 kb
06/24/2017	848 kb	1.1%	198 kb

Micius – Nanshan, China

Date	Sifted key	QBER	Final key
05/06/2017	1329 kb	1.0%	305 kb
07/07/2017	1926 kb	1.7%	398 kb

FIG. 1. Illustration of the three cooperating ground stations (Graz, Nanshan, and Xinglong). Listed are all paths used for key generation and the corresponding final key length.

On Sep. 29, 2017, an intercontinental video conference was held between the Chinese Academy of Sciences and the Austria Academy of Sciences. The satellite-based QKD network is combined with fiber-based metropolitan quantum networks, in which fibers are used to efficiently and conveniently connect many users inside a city with a distance scale of within 100 km. The Xinglong ground station is connected to the conference venue, Zhongguancun Software Park in Beijing, via a 280-km optical fiber link involving six trusted relays [19,20]. We employed the Advanced Encryption Standard (AES)-128 protocol that refreshed the 128-bit seed keys every second. The video conference lasted for 75 min with a total data transmission of ~2 GB, which consumed

In summary, using the *Micius* satellite as a trusted relay, we have demonstrated intercontinental quantum communication among multiple locations on Earth with a maximal separation of 7600 km. Our work already constitutes a simple prototype for a global quantum communications network. To increase the time and area coverage for a more efficient QKD network, we plan to launch higher-orbit satellites and implement daytime operation using telecommunication wavelength photons and tighter spatial and spectral filtering [21]. One limitation of the current implementation of the QKD protocol is that we have to trust the satellite itself, which can be overcome in the future using entanglement-based systems [22–24]. Other future developments will include multiparty connections from satellites to various ground stations in parallel, and the connection to large ground networks [20], at first in China and Europe and then on a global scale.

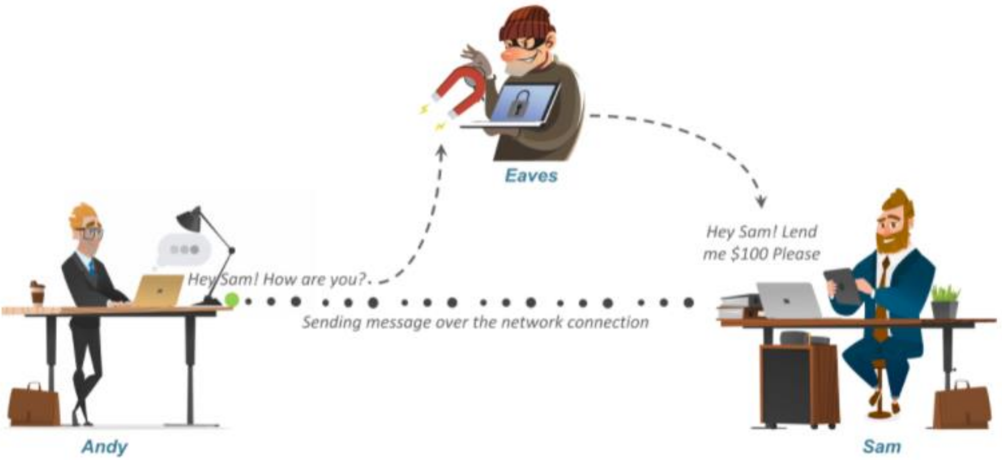
What is ultra-secure communications ?

Answer : Encrypted Communications using Vernan cypher (or one time pad) which is theoretically unbreakable if

- It uses blocks of perfectly random data equal in length to the message to encode
- each key is known only by the two partners
- each key is used only once

Problems:

- *Having a perfect random generator*
- *Detecting intrusion during the key distribution process*

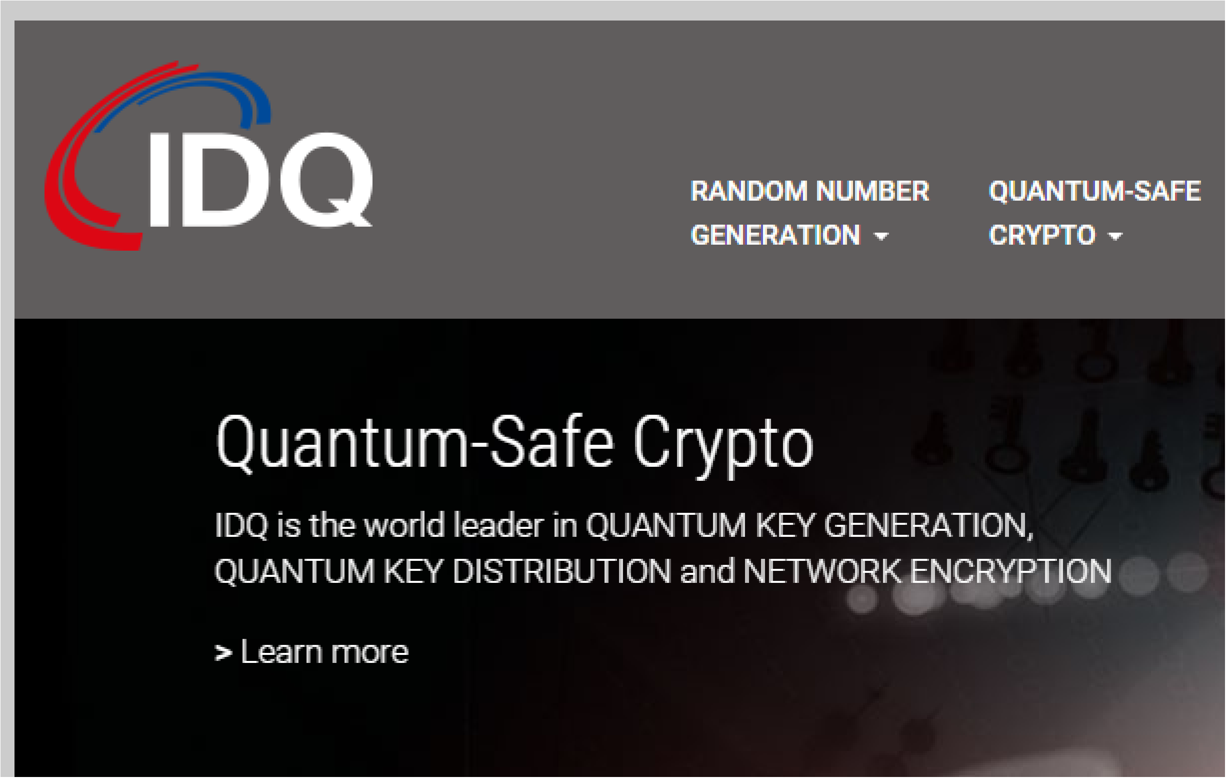

Eaves
Hey Sam! How are you?
Sending message over the network connection
Hey Sam! Lend me $100 Please
Andy
Sam

Solutions:

Both problems are solved using the properties of quantum information:

- random generator based on a quantum process, intrinsically random
- Quantum Key Distribution : due to the properties of quantum information, if an intruder is present he will be detected and the generated key will be rejected without being used

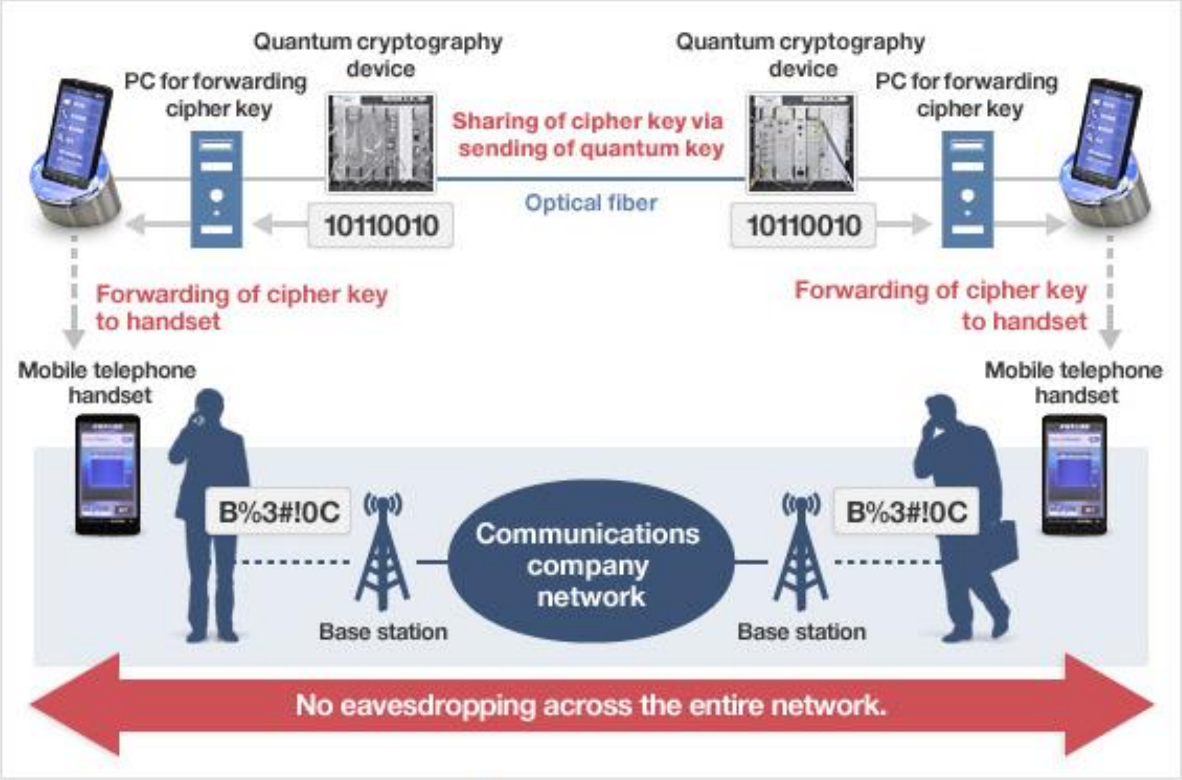
Quantum cryptography is in the market:



Quantum-Safe Crypto

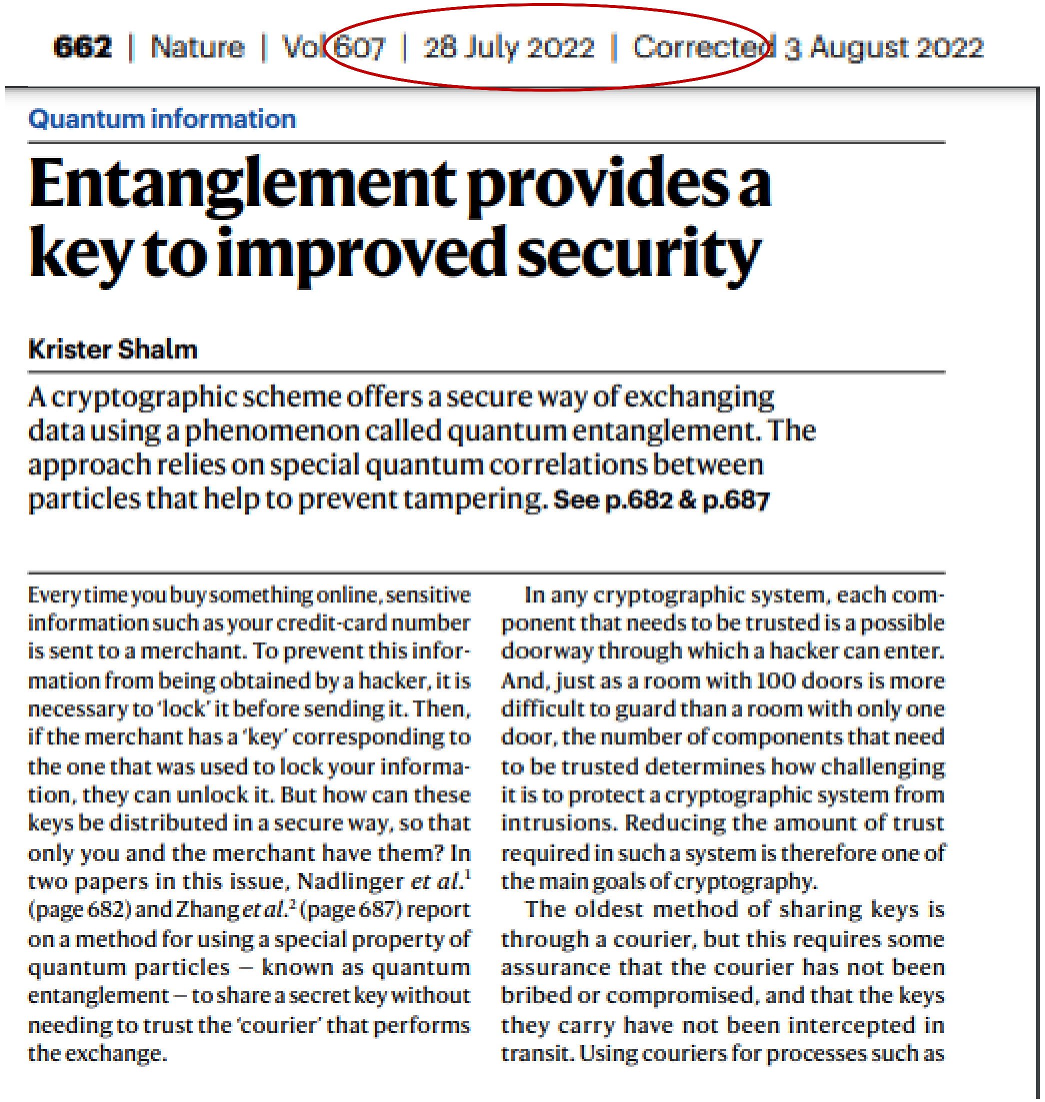
IDQ is the world leader in QUANTUM KEY GENERATION, QUANTUM KEY DISTRIBUTION and NETWORK ENCRYPTION

MITSUBISHI ELECTRIC
Changes for the Better


Quantum cryptography device
Quantum cryptography device
PC for forwarding cipher key
PC for forwarding cipher key
Sharing of cipher key via sending of quantum key
Optical fiber
10110010
10110010
Forwarding of cipher key to handset
Forwarding of cipher key to handset
Mobile telephone handset
Mobile telephone handset
B%3#!0C
B%3#!0C
Communications company network
Base station
Base station
No eavesdropping across the entire network.

Functioning of one-time pad mobile telephone software

2022 – Device independent QKD protocols using loop-hole free Bell tests



662 | Nature | Vol 607 | 28 July 2022 | Corrected 3 August 2022

Quantum information

Entanglement provides a key to improved security

Krister Shalm

A cryptographic scheme offers a secure way of exchanging data using a phenomenon called quantum entanglement. The approach relies on special quantum correlations between particles that help to prevent tampering. **See p.682 & p.687**

Every time you buy something online, sensitive information such as your credit-card number is sent to a merchant. To prevent this information from being obtained by a hacker, it is necessary to 'lock' it before sending it. Then, if the merchant has a 'key' corresponding to the one that was used to lock your information, they can unlock it. But how can these keys be distributed in a secure way, so that only you and the merchant have them? In two papers in this issue, Nadlinger *et al.*[1] (page 682) and Zhang *et al.*[2] (page 687) report on a method for using a special property of quantum particles – known as quantum entanglement – to share a secret key without needing to trust the 'courier' that performs the exchange.

In any cryptographic system, each component that needs to be trusted is a possible doorway through which a hacker can enter. And, just as a room with 100 doors is more difficult to guard than a room with only one door, the number of components that need to be trusted determines how challenging it is to protect a cryptographic system from intrusions. Reducing the amount of trust required in such a system is therefore one of the main goals of cryptography.

The oldest method of sharing keys is through a courier, but this requires some assurance that the courier has not been bribed or compromised, and that the keys they carry have not been intercepted in transit. Using couriers for processes such as

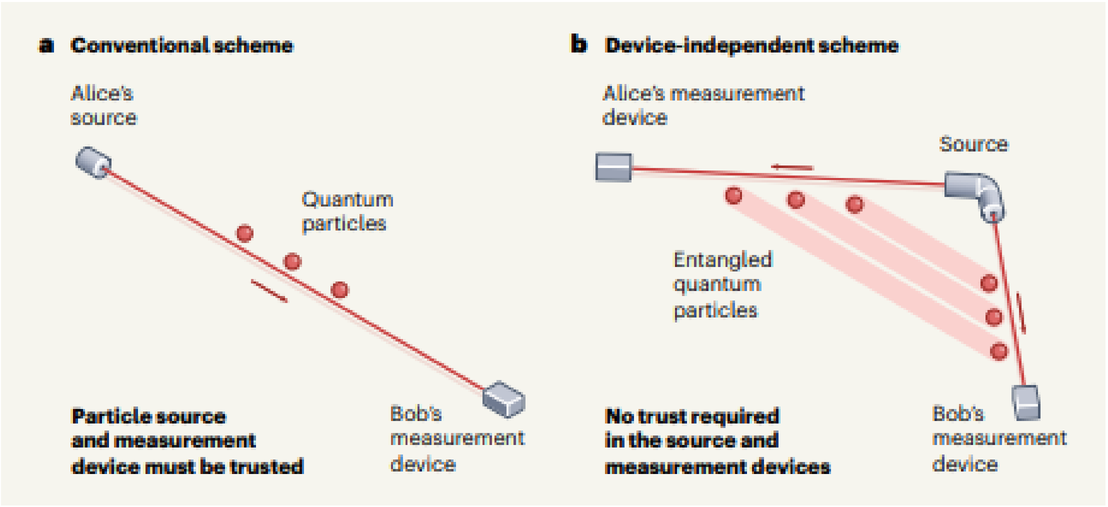
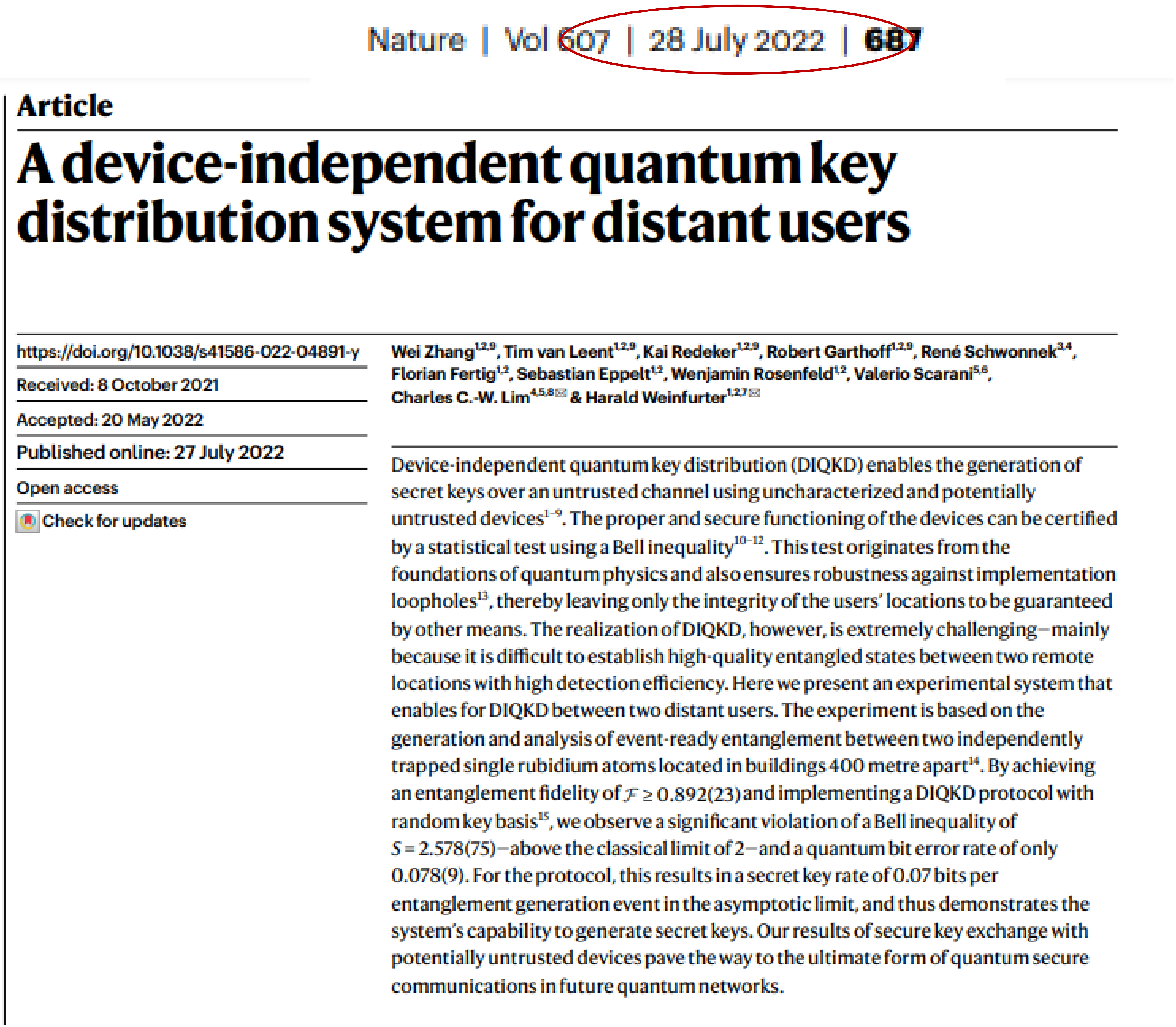

a Conventional scheme
Alice's source
Quantum particles
Particle source and measurement device must be trusted
Bob's measurement device
b Device-independent scheme
Alice's measurement device
Source
Entangled quantum particles
No trust required in the source and measurement devices
Bob's measurement device

Figure 1 | Schemes for distributing secret keys using quantum mechanics. Quantum particles can be used to deliver a key for encrypting sensitive information, because quantum mechanics dictates that anyone who intercepts the particles will inadvertently disturb them in a way that can be detected. **a**, In conventional schemes, two parties (labelled Alice and Bob) can create a key to encrypt and decrypt secret messages, but this method assumes that the particle source and measurement devices have not been compromised. **b**, Nadlinger *et al.*[1] and Zhang *et al.*[2] used quantum entanglement – through which pairs of quantum particles are correlated over long distances – to implement a scheme that does not require a trustworthy source or measurement devices. Alice and Bob can perform a test on their entangled particles under a strict set of conditions to detect whether the source has been compromised, so they need only safeguard their measurement results by sealing their laboratories.



Nature | Vol 607 | 28 July 2022 | 687

Article

A device-independent quantum key distribution system for distant users

https://doi.org/10.1038/s41586-022-04891-y

Received: 8 October 2021

Accepted: 20 May 2022

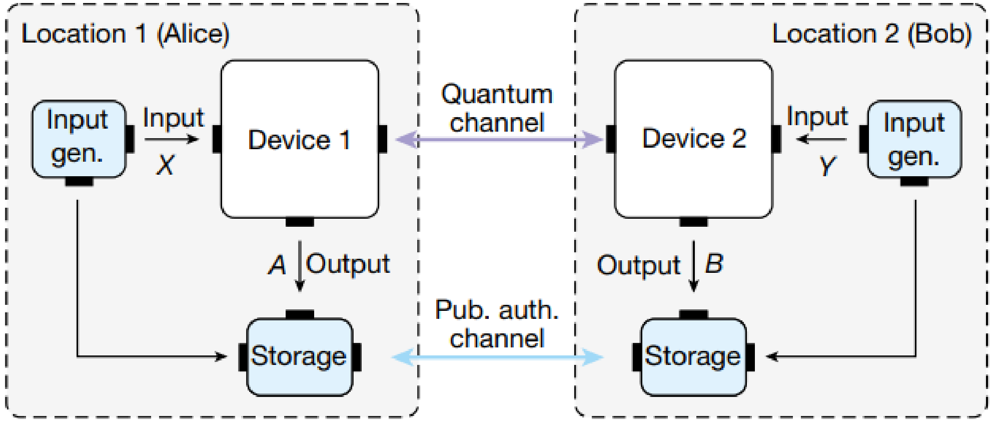
Published online: 27 July 2022

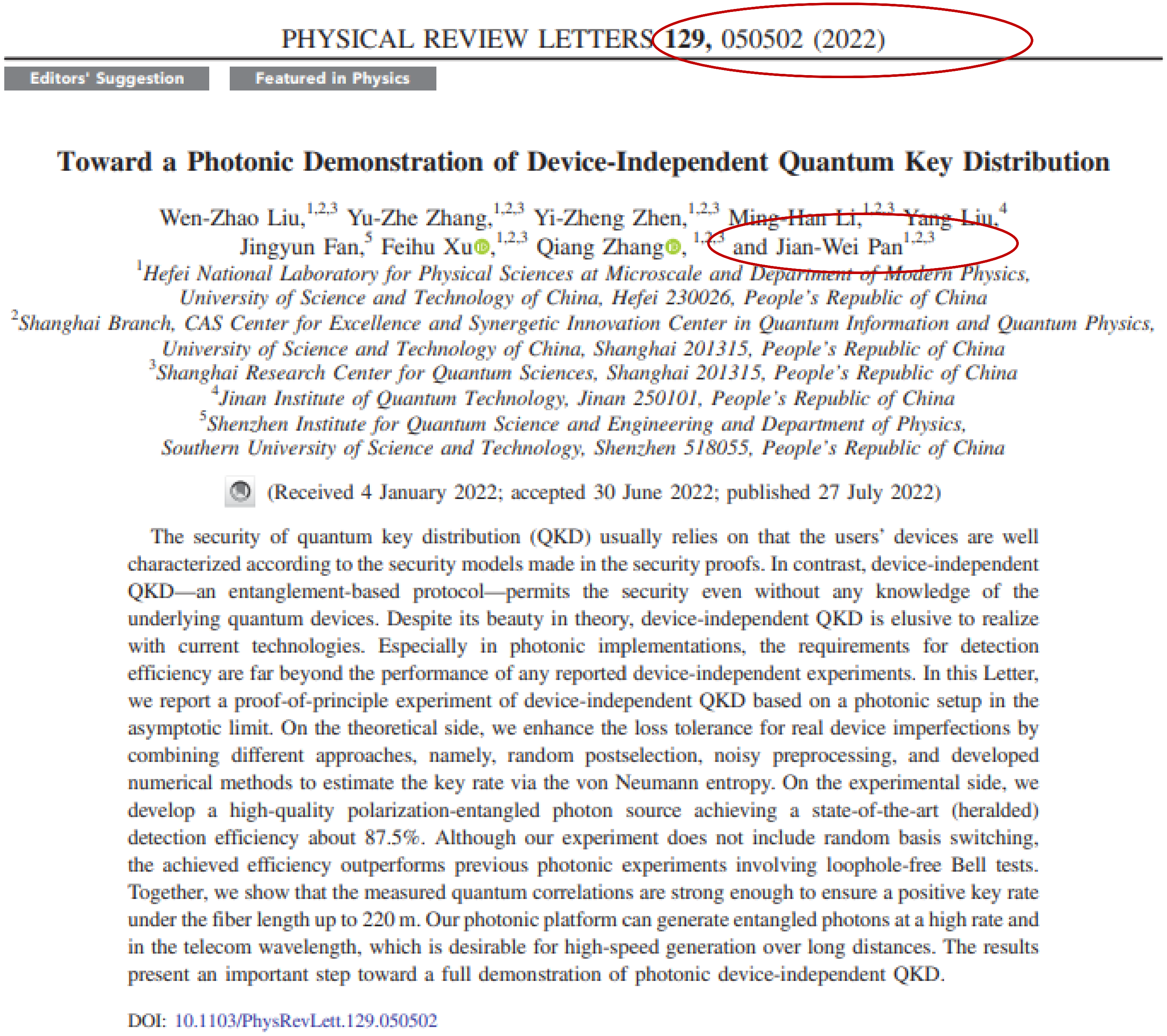
Open access

Check for updates

Wei Zhang[1,2,9], Tim van Leent[1,2,9], Kai Redeker[1,2,9], Robert Garthoff[1,2,9], René Schwonnek[3,4], Florian Fertig[1,2], Sebastian Eppelt[1,2], Wenjamin Rosenfeld[1,2], Valerio Scarani[5,6], Charles C.-W. Lim[4,5,8]✉ & Harald Weinfurter[1,2,7]✉

Device-independent quantum key distribution (DIQKD) enables the generation of secret keys over an untrusted channel using uncharacterized and potentially untrusted devices[1–9]. The proper and secure functioning of the devices can be certified by a statistical test using a Bell inequality[10–12]. This test originates from the foundations of quantum physics and also ensures robustness against implementation loopholes[13], thereby leaving only the integrity of the users' locations to be guaranteed by other means. The realization of DIQKD, however, is extremely challenging—mainly because it is difficult to establish high-quality entangled states between two remote locations with high detection efficiency. Here we present an experimental system that enables for DIQKD between two distant users. The experiment is based on the generation and analysis of event-ready entanglement between two independently trapped single rubidium atoms located in buildings 400 metre apart[14]. By achieving an entanglement fidelity of $\mathcal{F} \geq 0.892(23)$ and implementing a DIQKD protocol with random key basis[15], we observe a significant violation of a Bell inequality of $S = 2.578(75)$—above the classical limit of 2—and a quantum bit error rate of only 0.078(9). For the protocol, this results in a secret key rate of 0.07 bits per entanglement generation event in the asymptotic limit, and thus demonstrates the system's capability to generate secret keys. Our results of secure key exchange with potentially untrusted devices pave the way to the ultimate form of quantum secure communications in future quantum networks.





PHYSICAL REVIEW LETTERS **129,** 050502 (2022)

Editors' Suggestion

Featured in Physics

Toward a Photonic Demonstration of Device-Independent Quantum Key Distribution

Wen-Zhao Liu,[1,2,3] Yu-Zhe Zhang,[1,2,3] Yi-Zheng Zhen,[1,2,3] Ming-Han Li,[1,2,3] Yang Liu,[4]
Jingyun Fan,[5] Feihu Xu,[1,2,3] Qiang Zhang,[1,2,3] and Jian-Wei Pan[1,2,3]

[1]*Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics,*
University of Science and Technology of China, Hefei 230026, People's Republic of China

[2]*Shanghai Branch, CAS Center for Excellence and Synergetic Innovation Center in Quantum Information and Quantum Physics,*
University of Science and Technology of China, Shanghai 201315, People's Republic of China

[3]*Shanghai Research Center for Quantum Sciences, Shanghai 201315, People's Republic of China*

[4]*Jinan Institute of Quantum Technology, Jinan 250101, People's Republic of China*

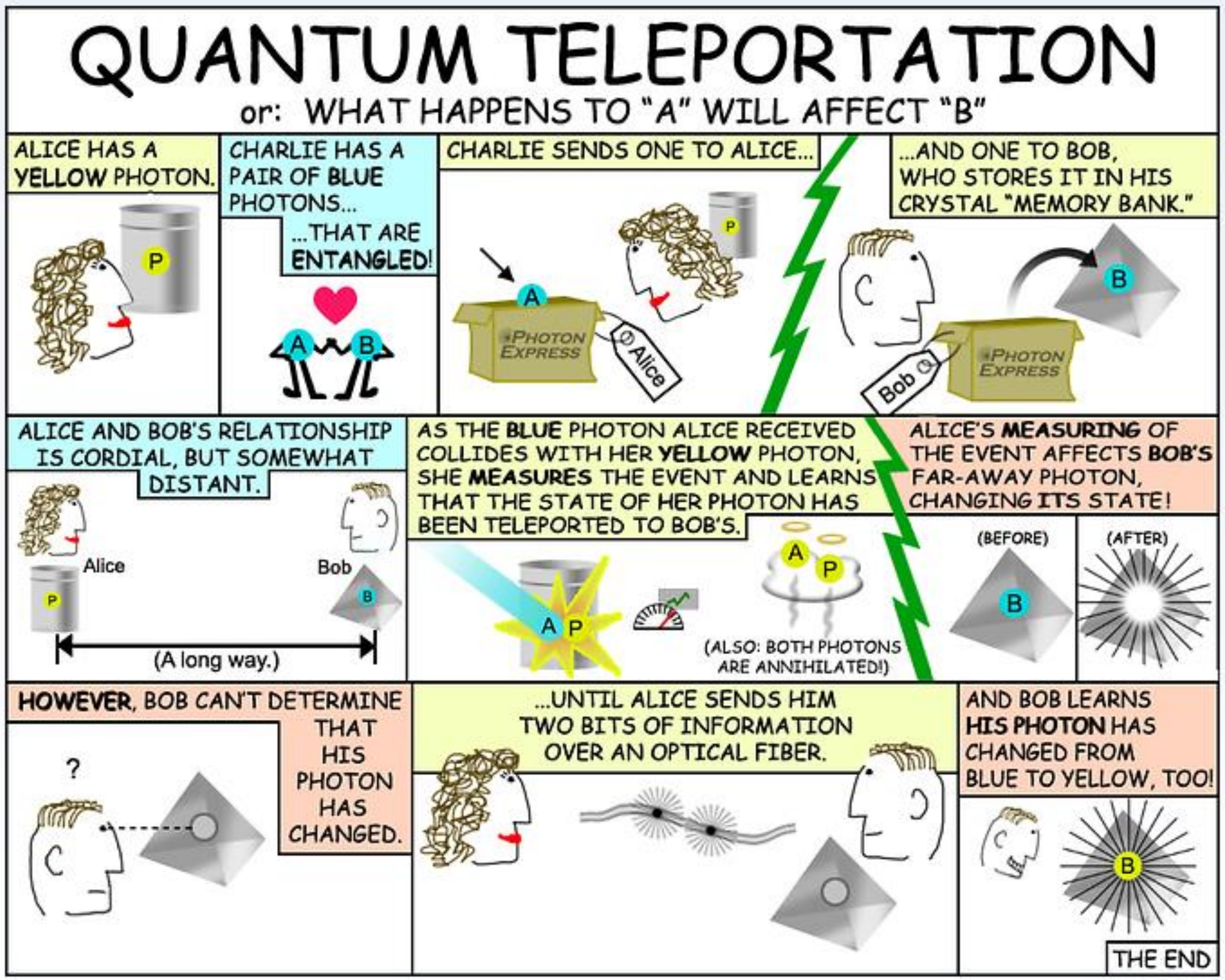
[5]*Shenzhen Institute for Quantum Science and Engineering and Department of Physics,*
Southern University of Science and Technology, Shenzhen 518055, People's Republic of China

(Received 4 January 2022; accepted 30 June 2022; published 27 July 2022)

The security of quantum key distribution (QKD) usually relies on that the users' devices are well characterized according to the security models made in the security proofs. In contrast, device-independent QKD—an entanglement-based protocol—permits the security even without any knowledge of the underlying quantum devices. Despite its beauty in theory, device-independent QKD is elusive to realize with current technologies. Especially in photonic implementations, the requirements for detection efficiency are far beyond the performance of any reported device-independent experiments. In this Letter, we report a proof-of-principle experiment of device-independent QKD based on a photonic setup in the asymptotic limit. On the theoretical side, we enhance the loss tolerance for real device imperfections by combining different approaches, namely, random postselection, noisy preprocessing, and developed numerical methods to estimate the key rate via the von Neumann entropy. On the experimental side, we develop a high-quality polarization-entangled photon source achieving a state-of-the-art (heralded) detection efficiency about 87.5%. Although our experiment does not include random basis switching, the achieved efficiency outperforms previous photonic experiments involving loophole-free Bell tests. Together, we show that the measured quantum correlations are strong enough to ensure a positive key rate under the fiber length up to 220 m. Our photonic platform can generate entangled photons at a high rate and in the telecom wavelength, which is desirable for high-speed generation over long distances. The results present an important step toward a full demonstration of photonic device-independent QKD.

DOI: 10.1103/PhysRevLett.129.050502

Questions that can be anticipated and possible answers, including some that can be found in the web


QUANTUM TELEPORTATION
or: WHAT HAPPENS TO "A" WILL AFFECT "B"
ALICE HAS A YELLOW PHOTON.
P
CHARLIE HAS A PAIR OF BLUE PHOTONS...
...THAT ARE ENTANGLED!
A
B
CHARLIE SENDS ONE TO ALICE...
PHOTON EXPRESS
Alice
...AND ONE TO BOB, WHO STORES IT IN HIS CRYSTAL "MEMORY BANK."
Bob
ALICE AND BOB'S RELATIONSHIP IS CORDIAL, BUT SOMEWHAT DISTANT.
Alice
Bob
(A long way.)
AS THE BLUE PHOTON ALICE RECEIVED COLLIDES WITH HER YELLOW PHOTON, SHE MEASURES THE EVENT AND LEARNS THAT THE STATE OF HER PHOTON HAS BEEN TELEPORTED TO BOB'S.
(ALSO: BOTH PHOTONS ARE ANNIHILATED!)
ALICE'S MEASURING OF THE EVENT AFFECTS BOB'S FAR-AWAY PHOTON, CHANGING ITS STATE!
(BEFORE)
(AFTER)
HOWEVER, BOB CAN'T DETERMINE THAT HIS PHOTON HAS CHANGED.
?
...UNTIL ALICE SENDS HIM TWO BITS OF INFORMATION OVER AN OPTICAL FIBER.
AND BOB LEARNS HIS PHOTON HAS CHANGED FROM BLUE TO YELLOW, TOO!
THE END

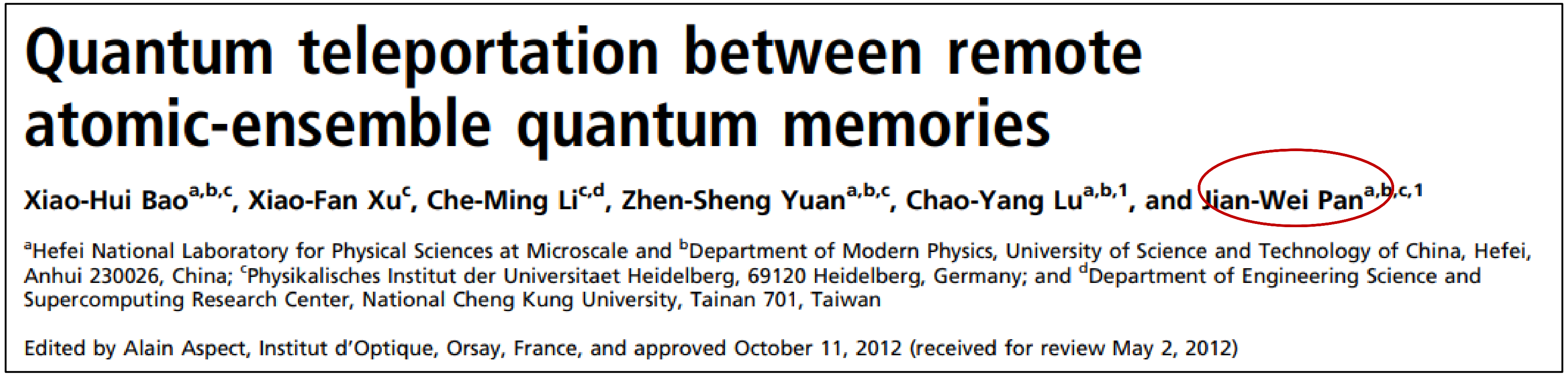
Quantum mechanics can be confusing. This cartoon helps explain recent research by NASA Jet Propulsion Laboratory, University of Geneva and NIST.

Can quantum teleportation be done with macroscopic objects?

- *There is no physic law defining a limit between the quantum world and the classic one. At present all we can say is that*

scientists do not teleport Kirk, but can teleport photons and even atoms.

- *One can push the limits, some scientists work really hard to do it, but nature will beat you at some point.*
- *Nevertheless, In 2012, a landmark was achieved when Chinese researchers were able to teleport the quantum states of the first macroscopic object — a group of 100 million rubidium atoms.*



Quantum teleportation between remote atomic-ensemble quantum memories

Xiao-Hui Bao[a,b,c], Xiao-Fan Xu[c], Che-Ming Li[c,d], Zhen-Sheng Yuan[a,b,c], Chao-Yang Lu[a,b,1], and Jian-Wei Pan[a,b,c,1]

[a]Hefei National Laboratory for Physical Sciences at Microscale and [b]Department of Modern Physics, University of Science and Technology of China, Hefei, Anhui 230026, China; [c]Physikalisches Institut der Universitaet Heidelberg, 69120 Heidelberg, Germany; and [d]Department of Engineering Science and Supercomputing Research Center, National Cheng Kung University, Tainan 701, Taiwan

Edited by Alain Aspect, Institut d'Optique, Orsay, France, and approved October 11, 2012 (received for review May 2, 2012)

Proceedings of the National Academy of Sciences, 109(50), 20347–20351. doi:10.1073/pnas.1207329109

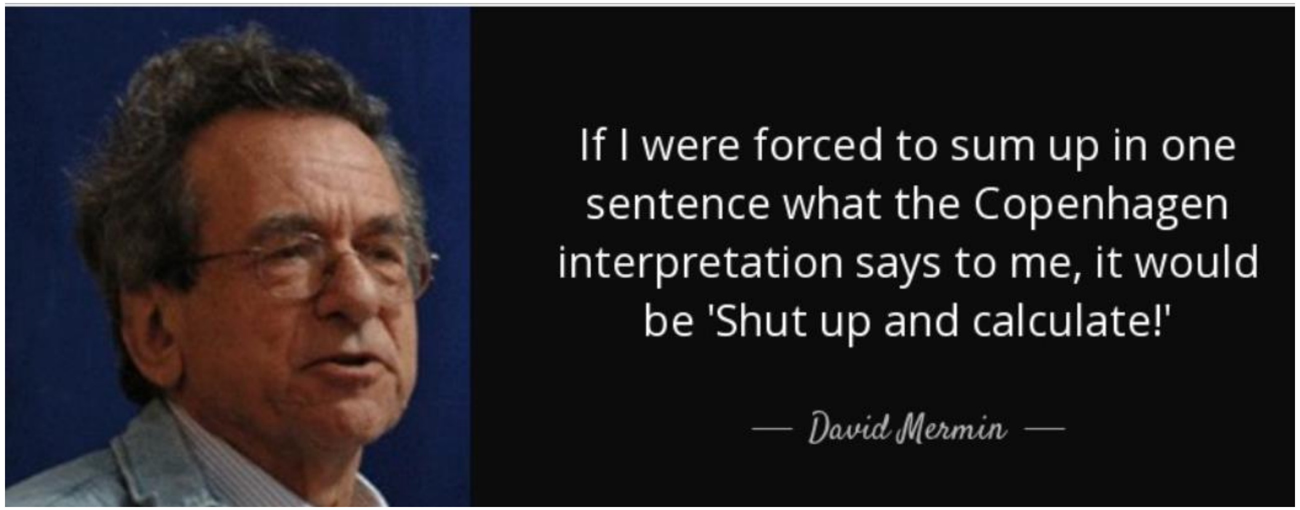
- Is there any other interpretation of Quantum Mechanics besides Copenhagen interpretation?

Yes, there are quite a few interpretations of quantum mechanics *other than the Copenhagen interpretation. They are all counter-intuitive in one way or another. And so it must be, since* Bell's theorem *proves that local realism is incompatible with quantum theory.*

- Is the Copenhagen interpretation still the most widely accepted position?

Yes, but If you find the quantum world confusing you're not alone. A recent survey shows that physicists disagree over the picture of reality that quantum mechanics describes – and that many of them don't even care.

Some related quotes from Mermin:



If I were forced to sum up in one sentence what the Copenhagen interpretation says to me, it would be 'Shut up and calculate!'

— David Mermin —

An extrapolation of its present rate of growth reveals that in the not too distant future Physical Review will fill bookshelves at a speed exceeding that of light. This is not forbidden by general relativity since no information is being conveyed.

David Mermim