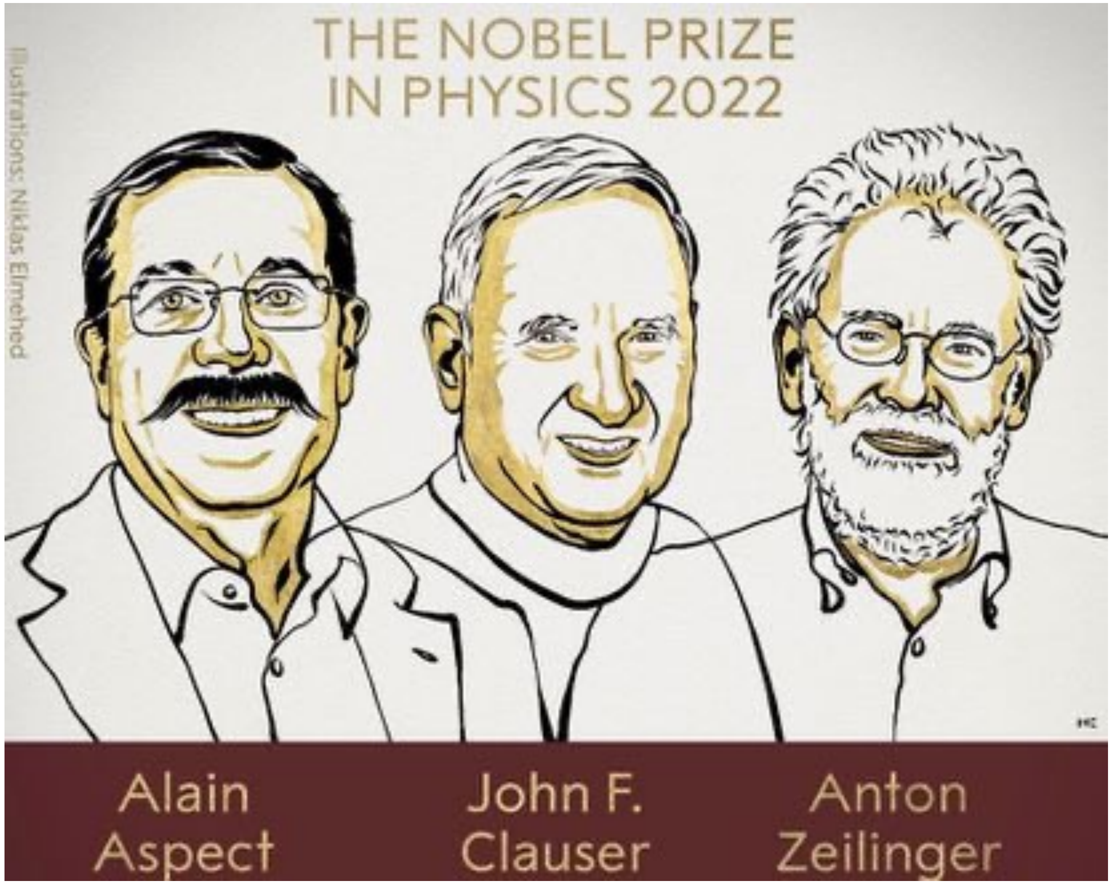
El teorema de Bell i els protocols de informació quàntica independents dels dispositius

Antonio Acín
Professor ICREA a l'ICFO-Institut de Ciències Fotòniques, Castelldefels

Institut d'Estudis Catalans, 23 de maig de 2023, Barcelona



Entangled states – from theory to technology

Alain Aspect, John Clauser and Anton Zeilinger have each conducted groundbreaking experiments using entangled quantum states, where two particles behave like a single unit even when they are separated. Their results have cleared the way for new technology based upon quantum information.

Bell’s Theorem: a bit of history

Bell’s theorem solves the question of whether classical models like those introduced by Einstein-Podolsky-Rosen (EPR) can account for quantum predictions.

Bell's Theorem: a bit of history

Bell's theorem solves the question of whether classical models like those introduced by Einstein-Podolsky-Rosen (EPR) can account for quantum predictions.

THE NEW YORK TIMES, SATURDAY, MAY 4, 1935.

EINSTEIN ATTACKS QUANTUM THEORY

Scientist and Two Colleagues Find It Is Not 'Complete' Even Though 'Correct.'

SEE FULLER ONE POSSIBLE

Believe a Whole Description of 'the Physical Reality' Can Be Provided Eventually.

PRINCETON, N. J., May 3.—Professor Albert Einstein will attack science's important theory of quantum mechanics, a theory of which he was a sort of grandfather. He concludes that while it is "correct" it is not "complete."

With two colleagues at the Institute for Advanced Study here, the noted scientist is about to report to the American Physical Society what is wrong with the theory of quantum mechanics, it has been learned exclusively by Science Service.

The quantum theory, with which science predicts with some success inter-atomic happenings, does not meet the requirements for a satisfactory physical theory, Professor Einstein will report in a joint paper with Dr. Boris Podolsky and Dr. N. Rosen.

In the quantum theory as now used, the latest Einstein paper will point out that where two physical quantities such as the position of a particle and its velocity interact, a knowledge of one quantity precludes knowledge about the other. This is the famous principle of uncertainty put forward by Professor Werner Heisenberg and incorporated in the quantum theory. This very fact, Professor Einstein feels, makes the quantum theory fail in the requirements necessary for a satisfactory physical theory.

Two Requirements Listed.

These two requirements are:

1. The theory should make possible a calculation of the facts of nature and predict results which can be accurately checked by experiment; the theory should be, in other words, correct.

2. Moreover, a satisfactory theory should, as a good image of the objective world, contain a counterpart for things found in the objective world; that is, it must be a complete theory.

Quantum theory, Professor Einstein and his colleagues will report, fulfills the correctness requirement but fails in the completeness requirement.

While proving that present quantum theory does not give a complete description of physical reality, Professor Einstein believes some later, still undeveloped, theory will make this possible. His conclusion is:

"While we have thus shown that the wave function [of quantum theory] does not provide a complete description of the physical reality, we left open the question of whether or not such a description exists. We believe, however, that such a theory is possible."

The development of quantum mechanics has proved very useful in exploring the atom. Six Nobel Prizes in physics, including one to Einstein, have been awarded for various phases of the researches leading up to quantum mechanics. The names of Planck, Bohr, de Broglie, Heisenberg, Dirac and Schroedinger, as well as Einstein, are linked with quantum mechanics.

The exact title of the Einstein-Podolsky-Rosen paper is: "Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?"

Explanation by Podolsky.

In explaining the latest view of the physical world as revealed in their researches Dr. Podolsky, one of the authors, said:

"Physicists believe that there exist real material things independent of our minds and our theories. We construct theories and invent words (such as electron, positron, &c.) in an attempt to explain to ourselves what we know about our external world and to help us to obtain further knowledge of it. Before a theory can be considered to be satisfactory it must pass two very severe tests. First, the theory must enable us to calculate facts of nature, and these calculations must agree very accurately with observations and experiments. Second, we expect a satisfactory theory, as a good image of objective reality, to contain a counterpart for every element of the physical world. A theory satisfying the first requirement may be called a correct theory while, if it satisfies the second requirement, it may be called a complete theory.

"Hundreds of thousands of experiments and measurements have shown that, at least in cases when matter moves much slower than light, the theory of Planck, Einstein, Bohr Heisenberg and Schroedinger known as quantum mechanics is a correct theory. Einstein, Podolsky and Rosen now discuss the question of the completeness of quantum mechanics. They arrive at the conclusion that quantum mechanics, in its present form, is not complete.

"In quantum mechanics the condition of any physical system, such as an electron, an atom, &c., is supposed to be completely described by a formula known as a 'wave function.' Suppose that we know the wave function for each of two physical systems, and that these two systems come together, interact, and again separate (as when two particles collide and move apart). Quantum mechanics, although giving us considerable information about such a process, does not enable us to calculate the wave function of each physical system after the separation. This fact is made use of in showing that the wave function does not give a complete description of physical reality. Since, however, description of physical systems by wave functions is an essential step of quantum mechanics, this means that quantum mechanics is not a complete theory."

Raises Point of Doubt.

Special to THE NEW YORK TIMES.

PRINCETON, N. J., May 3.—Asked to comment on the new ideas of Professor Einstein and his collaborators, Professor Edward U. Condon, mathematical physicist of Princeton University, said tonight:

"Of course, a great deal of the argument hinges on just what meaning is to be attached to the word 'reality' in connection with physics. They have certainly discussed an interesting point in connection with the theory. Dr. Einstein has never been satisfied with the statistical causality which in the new theories replaces the strict causality of the old physics.

"It is reported that when he first learned of the work of Schroedinger and Dirac, he said, 'Der lieber Gott wuerfelt nicht, [the good Lord does not throw dice]. For the last five years he has subjected the quantum mechanical theories to very searching criticism from this standpoint. But I am afraid that thus far the statistical theories have withstood criticism."

Bell's Theorem: a bit of history

Bell's theorem solves the question of whether classical models like those introduced by Einstein-Podolsky-Rosen (EPR) can account for quantum predictions.

THE NEW YORK TIMES, SATURDAY, MAY 4, 1935.

EINSTEIN ATTACKS QUANTUM THEORY

Scientist and Two Colleagues Find It Is Not 'Complete' Even Though 'Correct.'

SEE FULLER ONE POSSIBLE

Believe a Whole Description of 'the Physical Reality' Can Be Provided Eventually.

Copyright 1935 by Science Service.

PRINCETON, N. J., May 3.—Professor Albert Einstein will attack science's important theory of quantum mechanics, a theory of which he was a sort of grandfather. He concludes that while it is "correct" it is not "complete."

With two colleagues at the Institute for Advanced Study here, the noted scientist is about to report to the American Physical Society what is wrong with the theory of quantum mechanics, it has been learned exclusively by Science Service.

The quantum theory, with which science predicts with some success inter-atomic happenings, does not meet the requirements for a satisfactory physical theory, Professor Einstein will report in a joint paper with Dr. Boris Podolsky and Dr. N. Rosen.

In the quantum theory as now used, the latest Einstein paper will point out that where two physical quantities such as the position of a particle and its velocity interact, a knowledge of one quantity precludes knowledge about the other. This is the famous principle of uncertainty put forward by Professor Werner Heisenberg and incorporated in the quantum theory. This very fact, Professor Einstein feels, makes the quantum theory fail in the requirements necessary for a satisfactory physical theory.

Two Requirements Listed.

These two requirements are:

1. The theory should make possible a calculation of the facts of nature and predict results which can be accurately checked by experiment; the theory should be, in other words, correct.

2. Moreover, a satisfactory theory should, as a good image of the objective world, contain a counterpart for things found in the objective world; that is, it must be a complete theory.

Quantum theory, Professor Einstein and his colleagues will report, fulfills the correctness requirement but fails in the completeness requirement.

While proving that present quantum theory does not give a complete description of physical reality, Professor Einstein believes some later, still undeveloped, theory will make this possible. His conclusion is:

"While we have thus shown that the wave function [of quantum theory] does not provide a complete description of the physical reality, we left open the question of whether or not such a description exists. We believe, however, that such a theory is possible."

The development of quantum mechanics has proved very useful in exploring the atom. Six Nobel Prizes in physics, including one to Einstein, have been awarded for various phases of the researches leading up to quantum mechanics. The names of Planck, Bohr, de Broglie, Heisenberg, Dirac and Schroedinger, as well as Einstein, are linked with quantum mechanics.

The exact title of the Einstein-Podolsky-Rosen paper is: "Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?"

Explanation by Podolsky.

In explaining the latest view of the physical world as revealed in their researches Dr. Podolsky, one of the authors, said:

"Physicists believe that there exist real material things independent of our minds and our theories. We construct theories and invent words (such as electron, positron, &c.) in an attempt to explain to ourselves what we know about our external world and to help us to obtain further knowledge of it. Before a theory can be considered to be satisfactory it must pass two very severe tests. First, the theory must enable us to calculate facts of nature, and these calculations must agree very accurately with observations and experiments. Second, we expect a satisfactory theory, as a good image of objective reality, to contain a counterpart for every element of the physical world. A theory satisfying the first requirement may be called a correct theory while, if it satisfies the second requirement, it may be called a complete theory.

"Hundreds of thousands of experiments and measurements have shown that, at least in cases when matter moves much slower than light, the theory of Planck, Einstein, Bohr Heisenberg and Schroedinger known as quantum mechanics is a correct theory. Einstein, Podolsky and Rosen now discuss the question of the completeness of quantum mechanics. They arrive at the conclusion that quantum mechanics, in its present form, is not complete.

"In quantum mechanics the condition of any physical system, such as an electron, an atom, &c., is supposed to be completely described by a formula known as a 'wave function.' Suppose that we know the wave function for each of two physical systems, and that these two systems come together, interact, and again separate (as when two particles collide and move apart). Quantum mechanics, although giving us considerable information about such a process, does not enable us to calculate the wave function of each physical system after the separation. This fact is made use of in showing that the wave function does not give a complete description of physical reality. Since, however, description of physical systems by wave functions is an essential step of quantum mechanics, this means that quantum mechanics is not a complete theory."

Raises Point of Doubt.

Special to THE NEW YORK TIMES.

PRINCETON, N. J., May 3.—Asked to comment on the new ideas of Professor Einstein and his collaborators, Professor Edward U. Condon, mathematical physicist of Princeton University, said tonight:

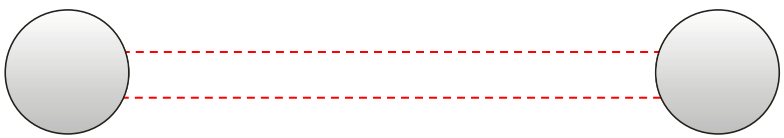
"Of course, a great deal of the argument hinges on just what meaning is to be attached to the word 'reality' in connection with physics. They have certainly discussed an interesting point in connection with the theory. Dr. Einstein has never been satisfied with the statistical causality which in the new theories replaces the strict causality of the old physics.

"It is reported that when he first learned of the work of Schroedinger and Dirac, he said, 'Der lieber Gott wuerfelt nicht, [the good Lord does not throw dice]. For the last five years he has subjected the quantum mechanical theories to very searching criticism from this standpoint. But I am afraid that thus far the statistical theories have withstood criticism."

While we have thus shown that the wave function does not provide a complete description of the physical reality, we left open the question of whether or not such a description exists. We believe, however, that such a theory is possible.

Quantum entanglement

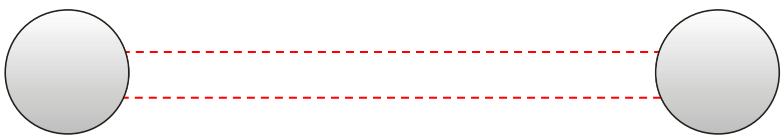
Quantum entanglement: quantum particles can be correlated in ways that do not have a classical analogue.



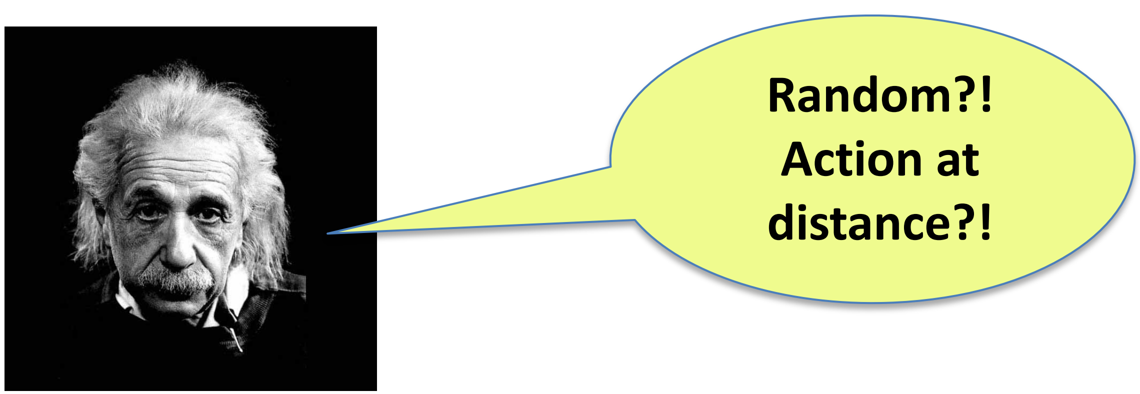
1. Outcomes of measurements performed on two distant entangled particles are random.
2. Nevertheless, the coincide, no matter the distance between the two particles.

Quantum entanglement

Quantum entanglement: quantum particles can be correlated in ways that do not have a classical analogue.

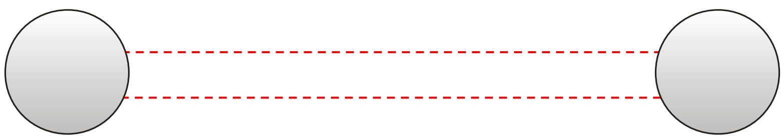


1. Outcomes of measurements performed on two distant entangled particles are random.
2. Nevertheless, the coincide, no matter the distance between the two particles.

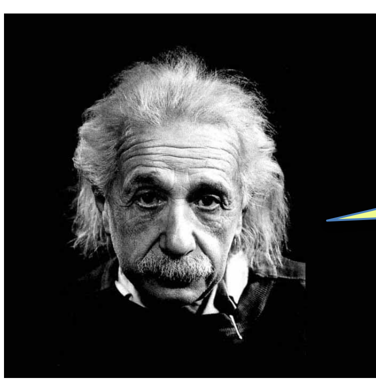


Quantum entanglement

Quantum entanglement: quantum particles can be correlated in ways that do not have a classical analogue.



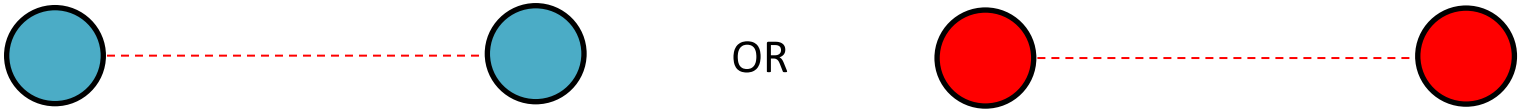
1. Outcomes of measurements performed on two distant entangled particles are random.
2. Nevertheless, the coincide, no matter the distance between the two particles.



Random?!
Action at distance?!

The ping-pong ball test

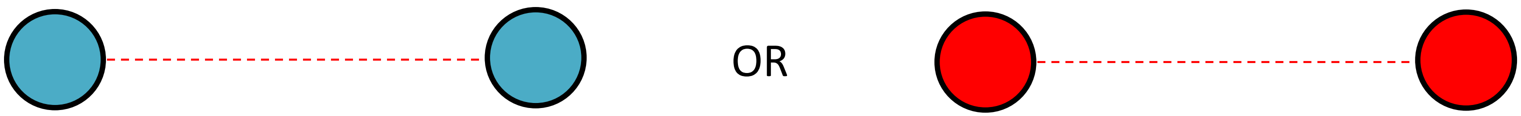
If a “quantum” effect can be explained with ping-pong balls, then the effect is no quantum.



If one observer knows the colour of the ball, the colour of the other ball is immediately determined.

The ping-pong ball test

If a “quantum” effect can be explained with ping-pong balls, then the effect is no quantum.



If one observer knows the colour of the ball, the colour of the other ball is immediately determined.

The main difference is that in quantum theory the properties (colours) of the particles are not predetermined, the theory does not explain the experiment as a combination of situations with deterministic assignments.

Bell's Theorem: a bit of history

The EPR article suggested that quantum physics was an incomplete theory: it proposed the existence of a "better", more complete theory making the same predictions as quantum physics.

Bell’s Theorem: a bit of history

The EPR article suggested that quantum physics was an incomplete theory: it proposed the existence of a “better”, more complete theory making the same predictions as quantum physics.

This theory must satisfy the principles of “locality” and “realism”, which are expected to be satisfied by any reasonable physical theory.

Bell's Theorem: a bit of history

The EPR article suggested that quantum physics was an incomplete theory: it proposed the existence of a "better", more complete theory making the same predictions as quantum physics.

This theory must satisfy the principles of "locality" and "realism", which are expected to be satisfied by any reasonable physical theory.

Bell's Theorem implies that an EPR model is unable to reproduce all the correlations observed when measuring (entangled) quantum particles. That is, it proves the incompatibility between EPR models satisfying locality and realism and quantum physics.

Bell’s Theorem: a bit of history

The EPR article suggested that quantum physics was an incomplete theory: it proposed the existence of a “better”, more complete theory making the same predictions as quantum physics.

This theory must satisfy the principles of “locality” and “realism”, which are expected to be satisfied by any reasonable physical theory.

Bell’s Theorem implies that an EPR model is unable to reproduce all the correlations observed when measuring (entangled) quantum particles. That is, it proves the incompatibility between EPR models satisfying locality and realism and quantum physics.

The experimental demonstration of Bell’s Theorem proved that EPR models cannot explain all correlations observed in nature.

However, this is not a talk on History of Physics…

It is a talk on the current understanding of Bell’s Theorem.

Let’s start by some basic ideas.

However, this is not a talk on History of Physics…

It is a talk on ~~the~~ my current understanding of Bell’s Theorem.

Let’s start by some basic ideas.

Correlations and causality

It can be argued that the main scientific question in any scientific discipline is to understand which causes are behind some observed correlations:

Correlations and causality

It can be argued that the main scientific question in any scientific discipline is to understand which causes are behind some observed correlations:

if an observer performs an action in a given location at a given moment in time, how will this affect actions in another point in space-time?

Correlations and causality

Causality is the main concept behind this idea: correlations cry out for explanations!

Correlations and causality

Causality is the main concept behind this idea: correlations cry out for explanations!

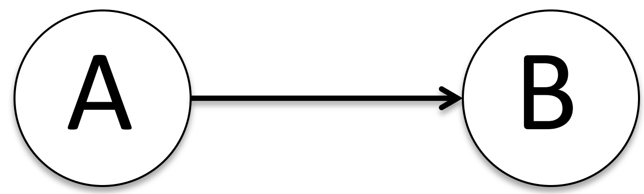
If one observes correlations between two events, *A* and *B*, there are two possible explanations:

Correlations and causality

Causality is the main concept behind this idea: correlations cry out for explanations!

If one observes correlations between two events, *A* and *B*, there are two possible explanations:

1. One event caused the other:

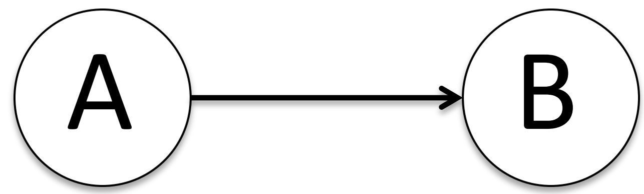


Correlations and causality

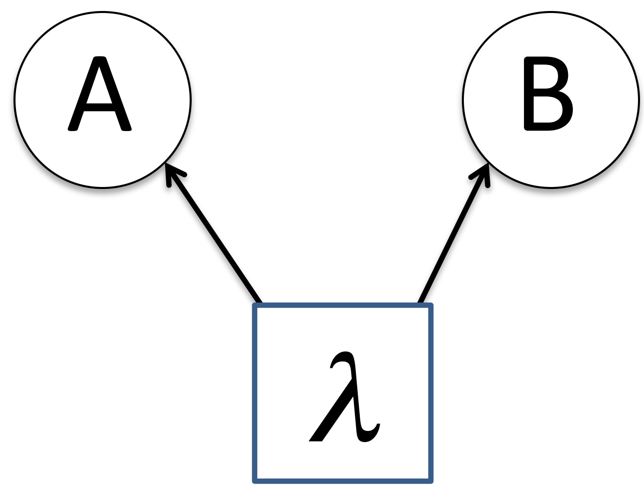
Causality is the main concept behind this idea: correlations cry out for explanations!

If one observes correlations between two events, *A* and *B*, there are two possible explanations:

1. One event caused the other:



2. The correlations have a common cause:

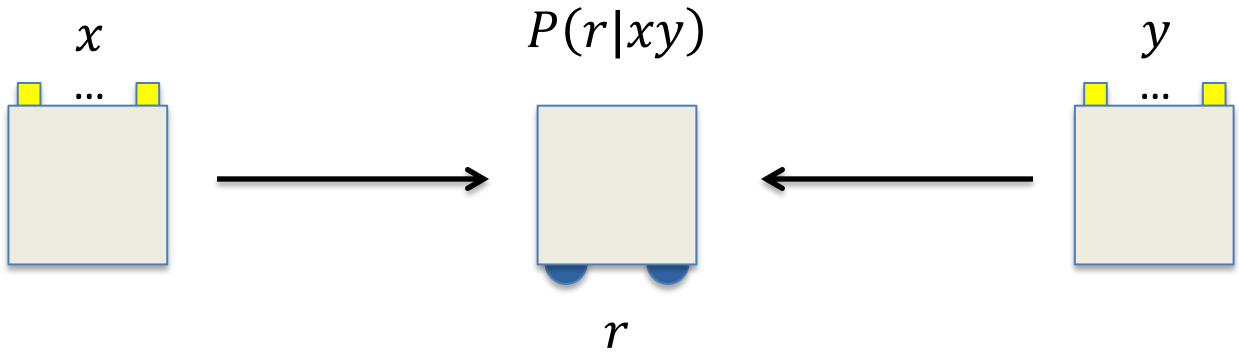


Causal networks

Natural language to represent physical experiments.

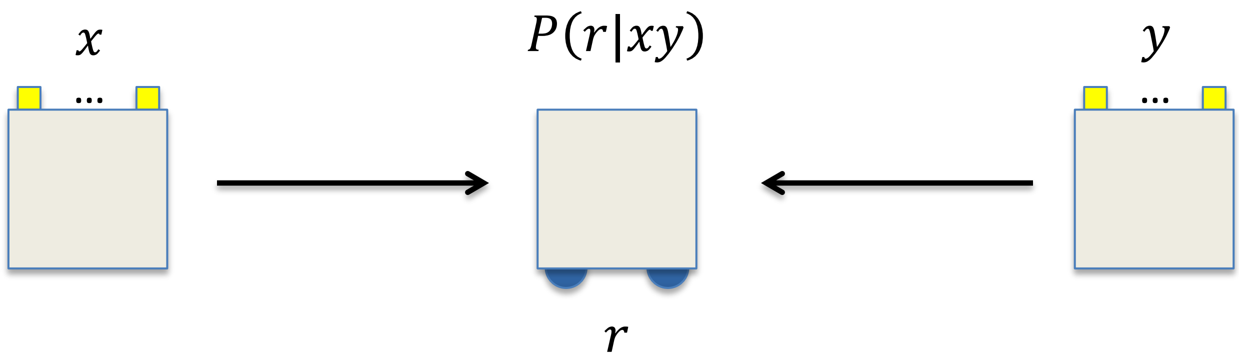
Causal networks

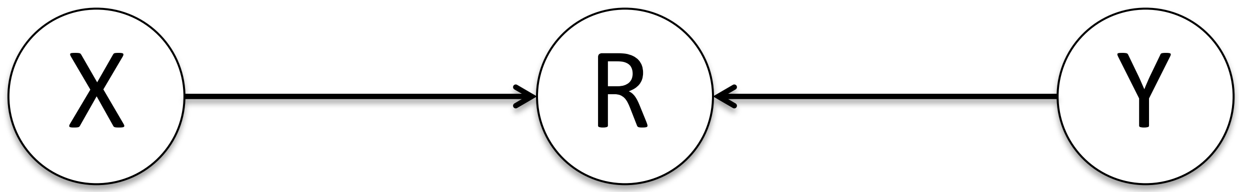
Natural language to represent physical experiments.



Causal networks

Natural language to represent physical experiments.





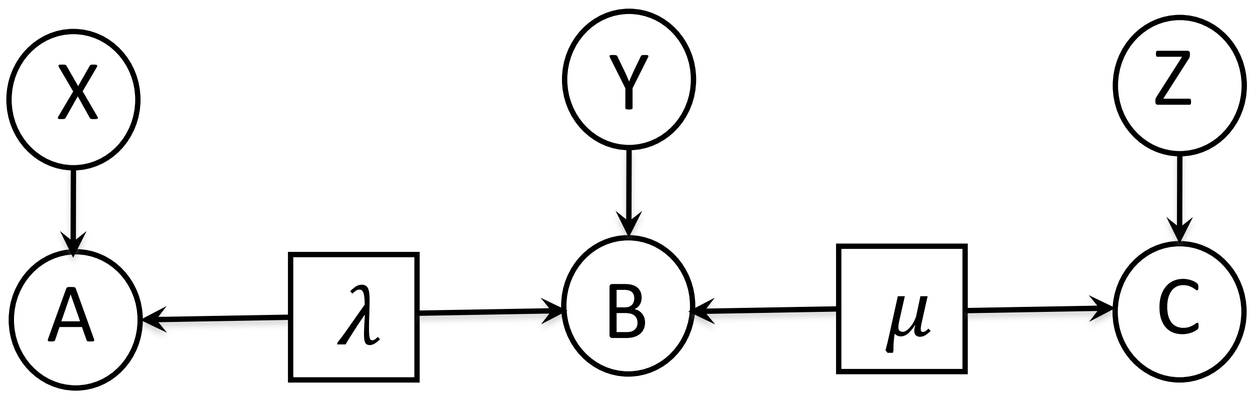
Causality constraints

The causal connections impose constraints on the observed statistics.

Causality constraints

The causal connections impose constraints on the observed statistics. Example:

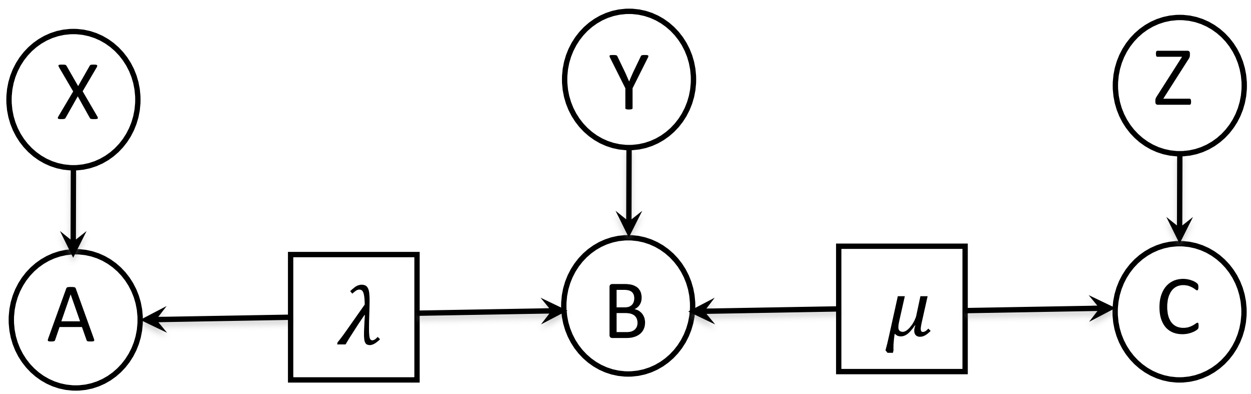
$$P(a, b, c|x, y, z)$$



Causality constraints

The causal connections impose constraints on the observed statistics. Example:

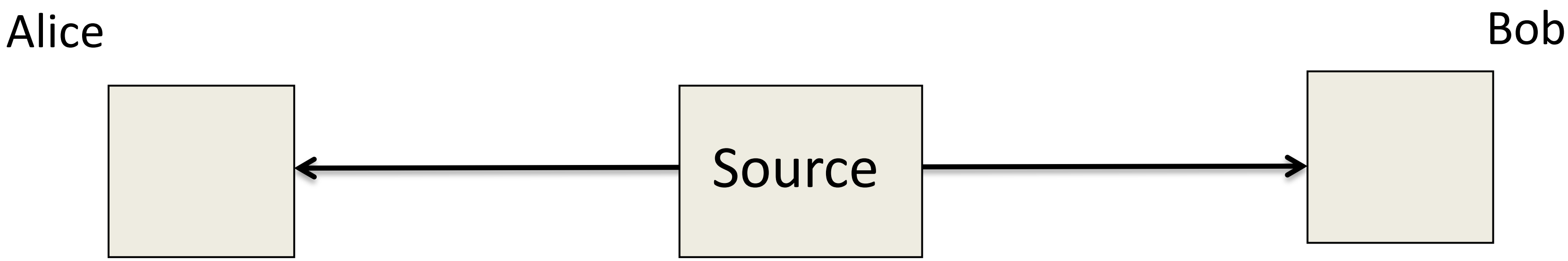
$$P(a,b,c|x,y,z)$$



$$\sum_c P(a,b,c|x,y,z) = P(a,b|x,y,z) = P(a,b|x,y)$$

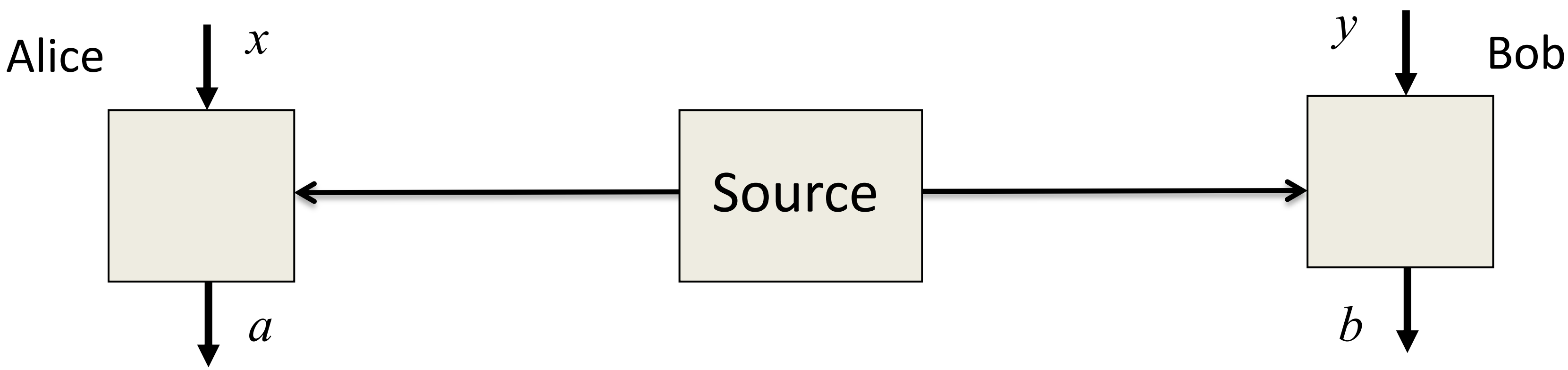
$$\sum_b P(a,b,c|x,y,z) = P(a,c|x,z) = P(a|x)P(c|z)$$

The Bell scenario



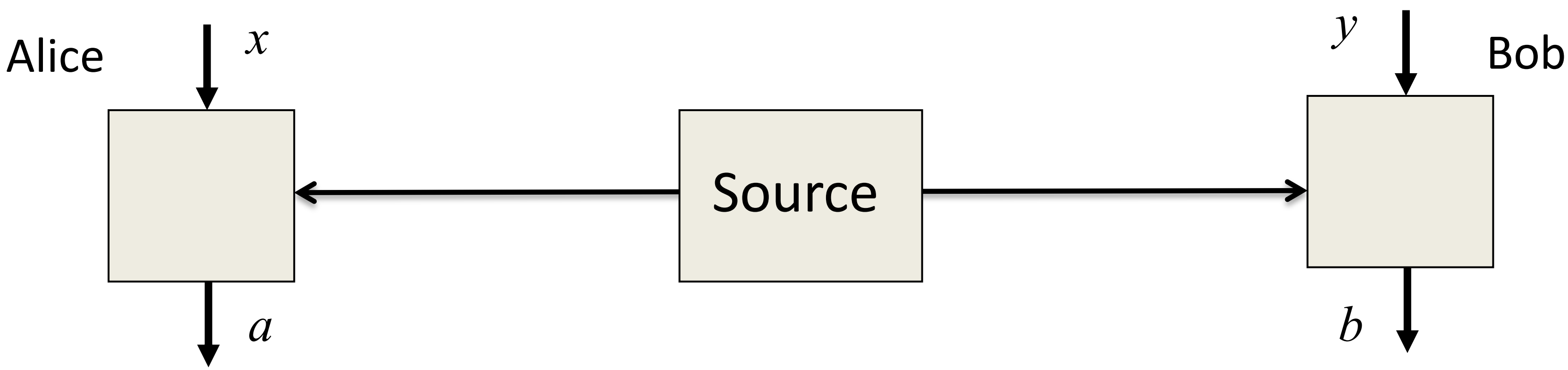
- A source prepares two systems (particles) and distributes them to two distant observers, Alice and Bob.

The Bell scenario



- A source prepares two systems (particles) and distributes them to two distant observers, Alice and Bob.
- The two distant observers apply measurements to each particle. The choices of measurements are labeled by *x* and *y* and the outputs by *a* and *b*.

The Bell scenario

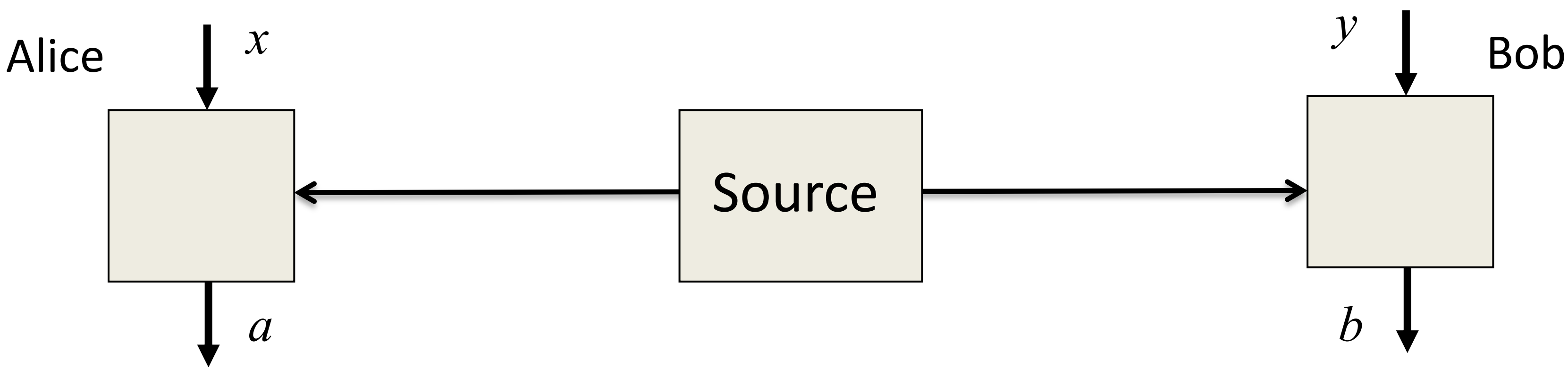


- A source prepares two systems (particles) and distributes them to two distant observers, Alice and Bob.

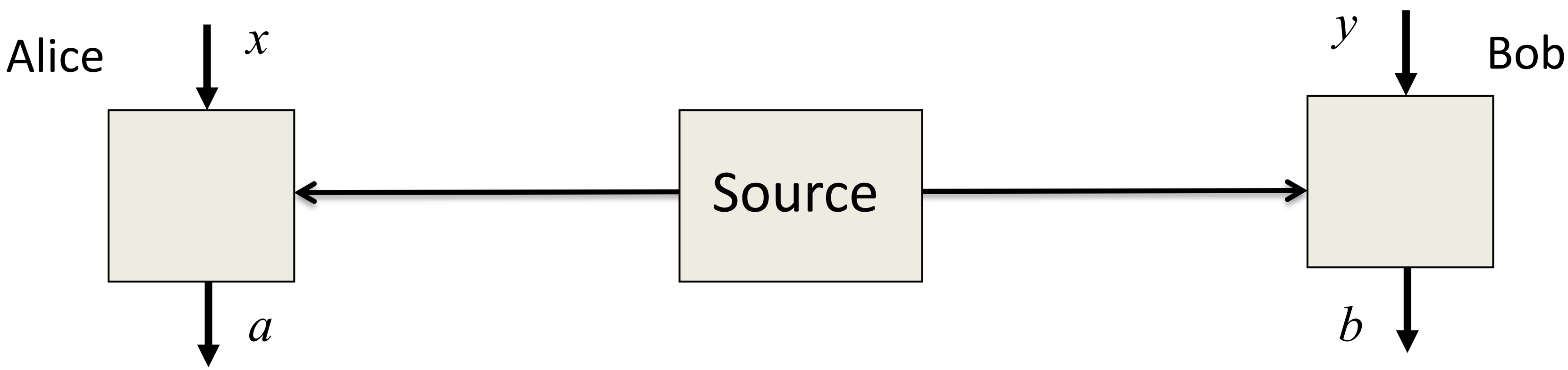
- The two distant observers apply measurements to each particle. The choices of measurements are labeled by *x* and *y* and the outputs by *a* and *b*.

- We have not specified anything in the experiment: whether the particles are quantum, whether they have a given energy,… NOTHING. We just provide labels to the actions in the experiment. The language so far is theory independent.

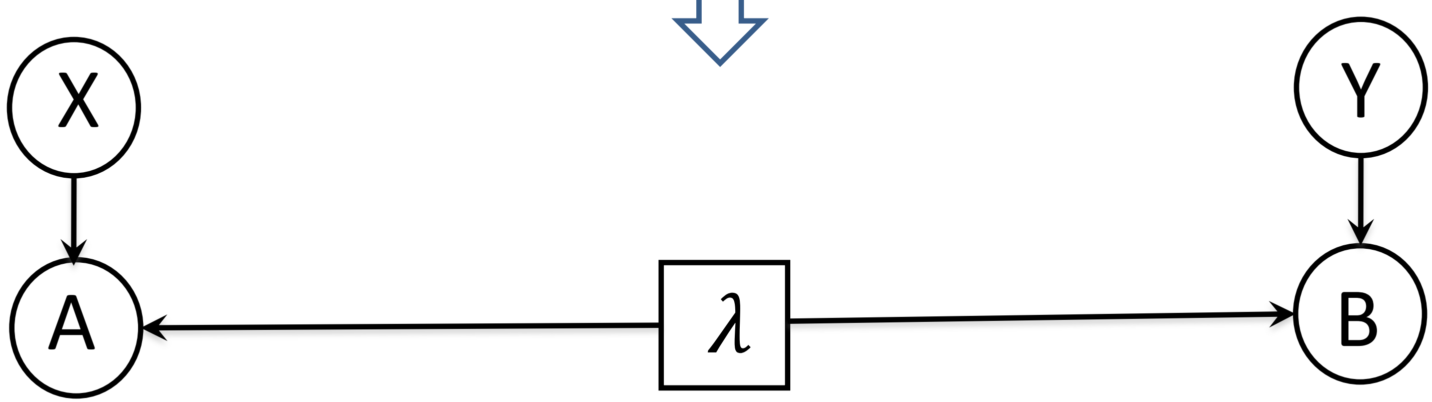
The Bell scenario



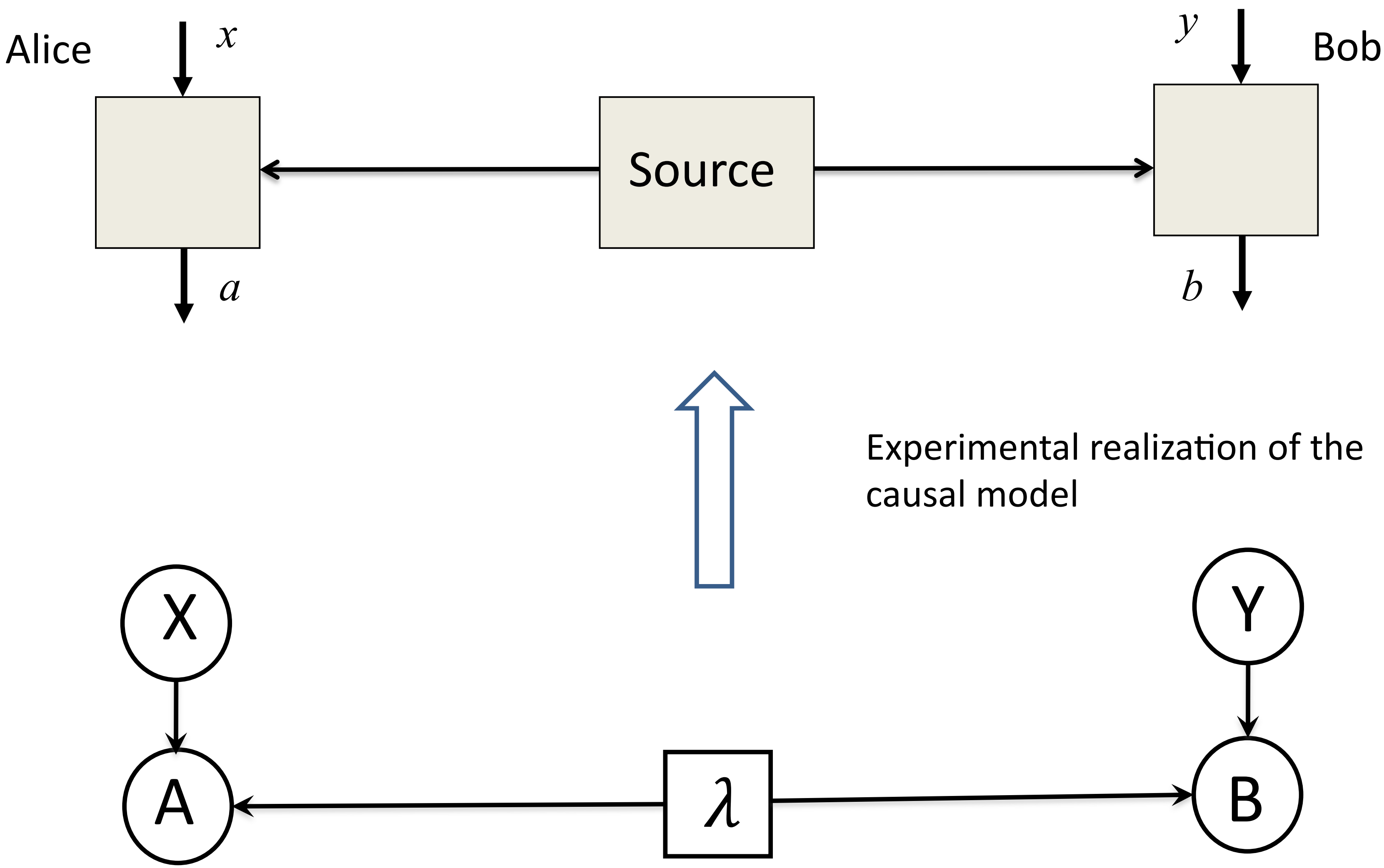
The Bell scenario



Causal model for the experiment



The Bell scenario

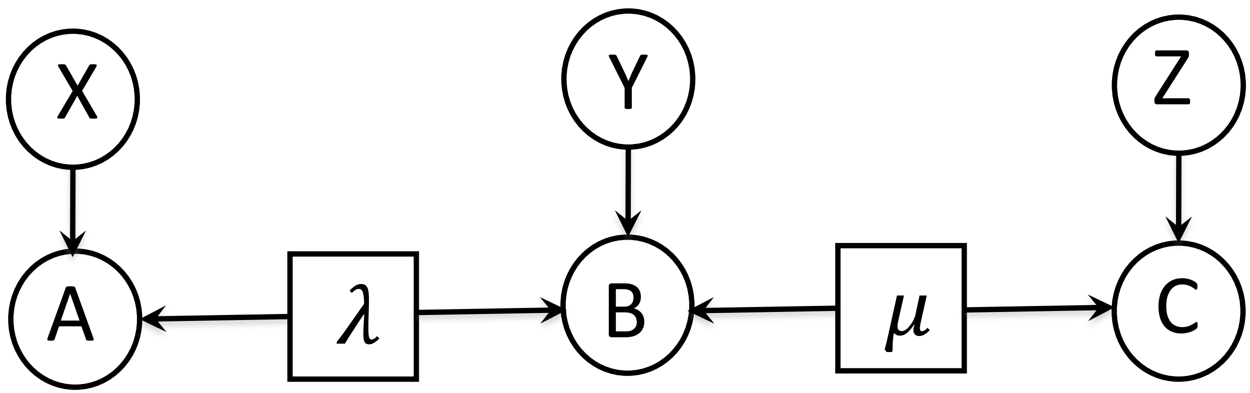


Deterministic causal models

Outputs observed at a given point in space-time are defined by **deterministic** functions of their causes.

Deterministic causal models

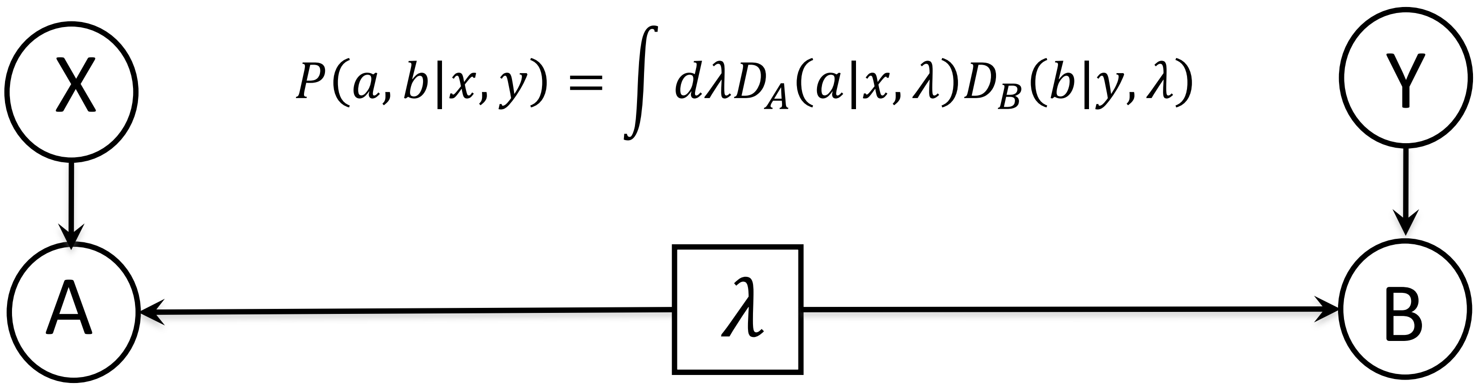
Outputs observed at a given point in space-time are defined by **deterministic** functions of their causes. Example:



$$P(a,b,c|x,y,z) = \iint d\lambda d\mu D_A(a|x,\lambda) D_B(b|y,\lambda,\mu) D_C(c|z,\mu)$$

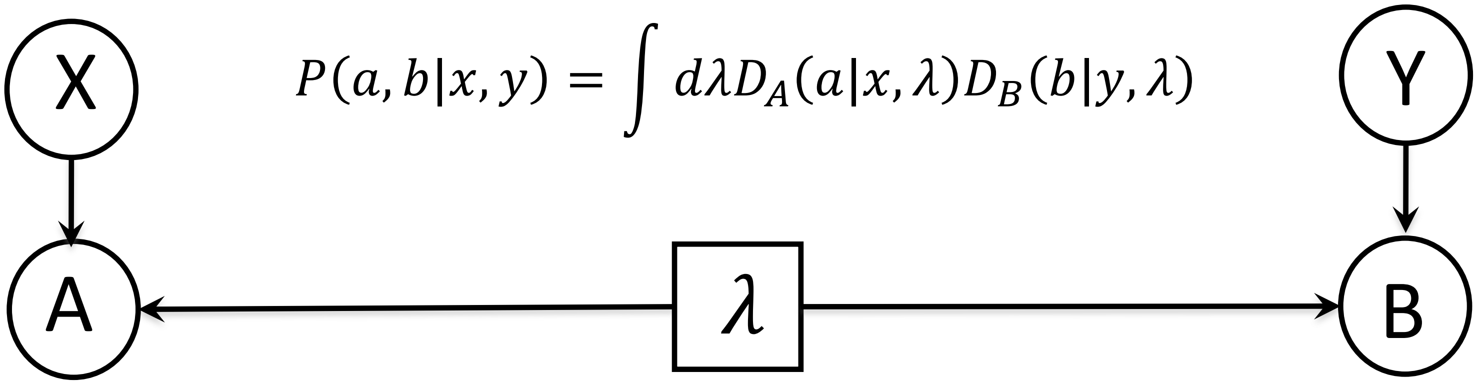
Bell inequalities

$$P(a,b|x,y) = \int d\lambda D_A(a|x,\lambda) D_B(b|y,\lambda)$$



Bell inequalities

$$P(a,b|x,y) = \int d\lambda D_A(a|x,\lambda) D_B(b|y,\lambda)$$

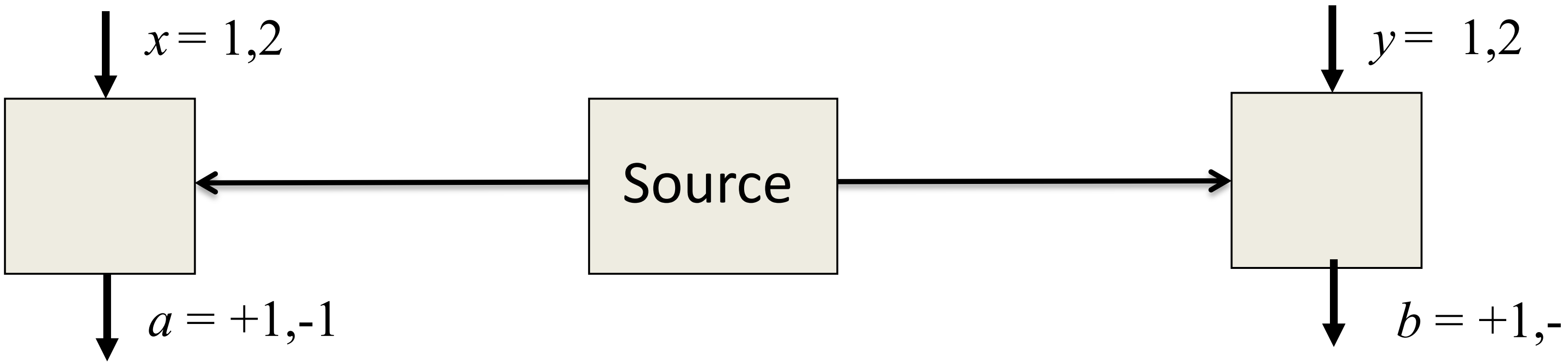


- Bell inequalities are inequalities constructed from linear combination of the observed statistics which are satisfied by classical correlations:

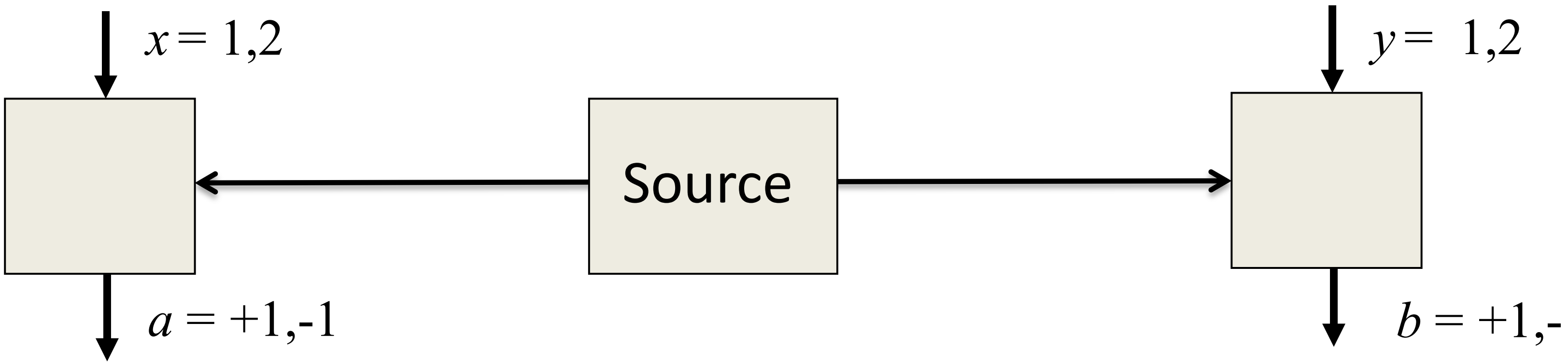
$$\sum_{a,b,x,y} c_{a,b,x,y} P(a,b|x,y) \leq \beta_L$$

- No quantum law is used in the previous discussion. Bell inequalities have nothing to do with quantum physics. But they are satisfied by classical EPR models.

Example: CHSH Bell inequality



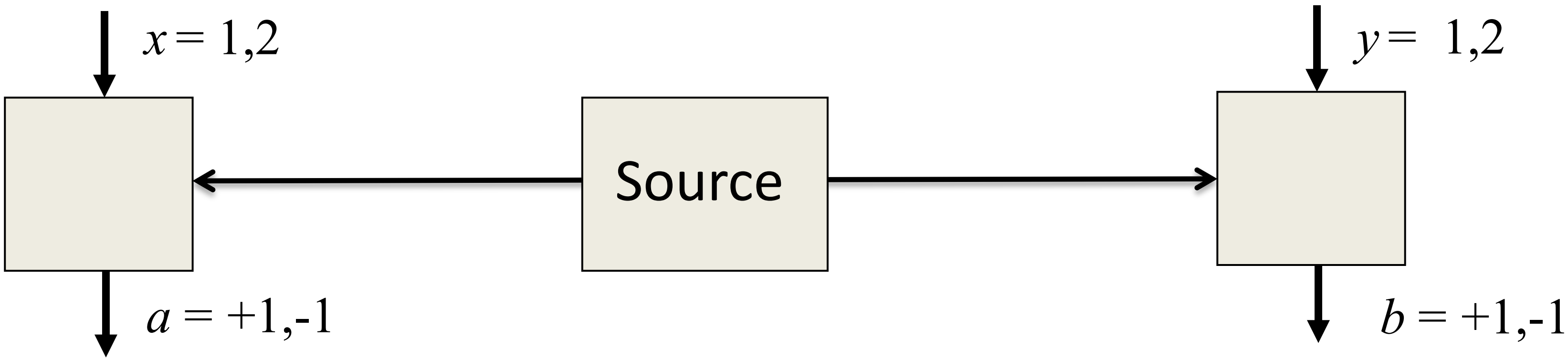
Example: CHSH Bell inequality



John Clauser

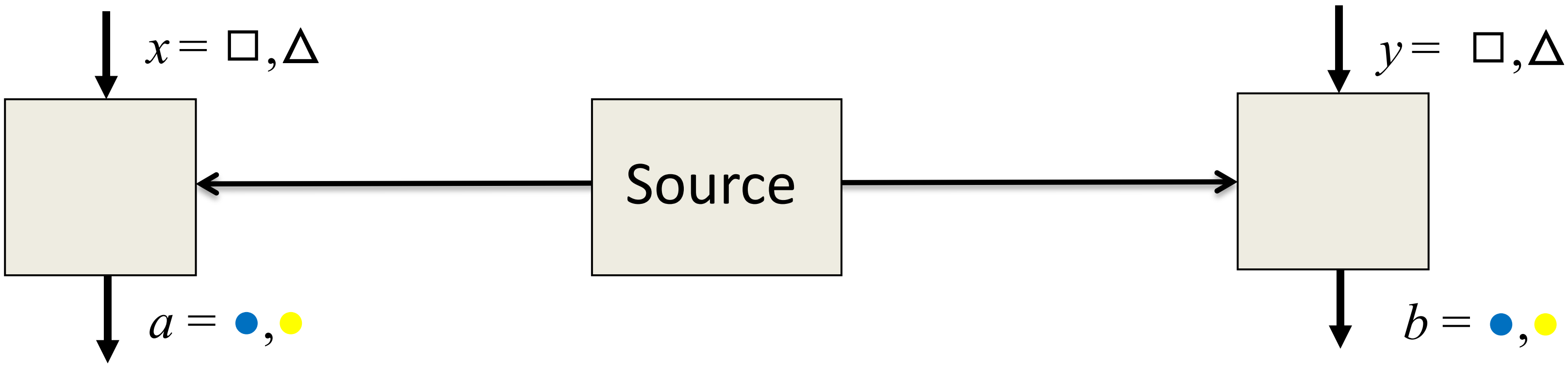
CHSH = **Clauser** Horne Shimony Holt

Example: CHSH Bell inequality



$$CHSH = P(A_1 = B_1) + P(A_1 = B_2) + P(A_2 = B_1) + P(A_2 \neq B_2)$$

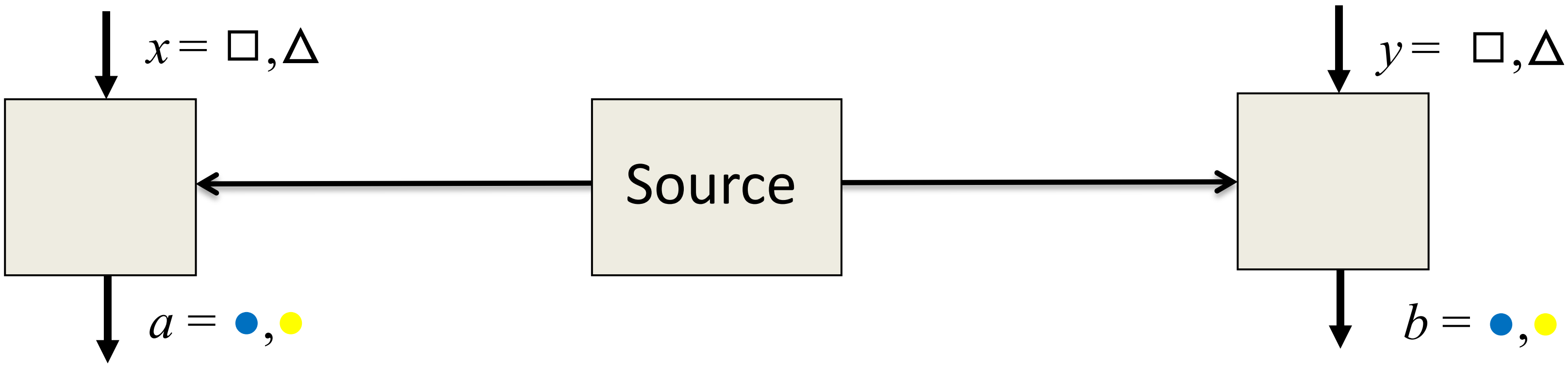
Example: CHSH Bell inequality



$$CHSH = P(A_1 = B_1) + P(A_1 = B_2) + P(A_2 = B_1) + P(A_2 \neq B_2)$$

$\square_A = \square_B$ $\square_A = \Delta_B$ $\Delta_A = \square_B$ $\Delta_A \neq \Delta_B$

Example: CHSH Bell inequality

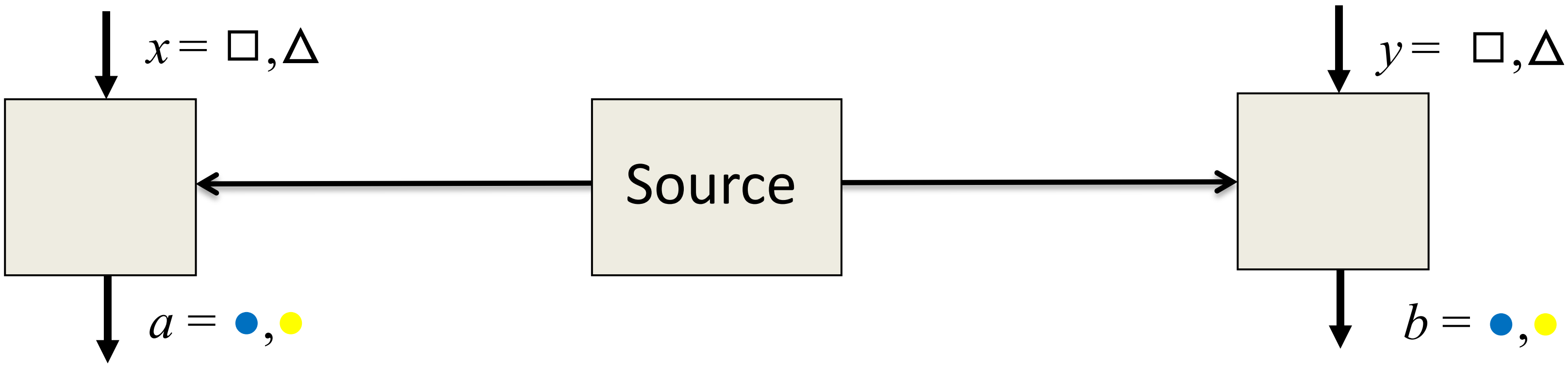


$$CHSH = P(A_1 = B_1) + P(A_1 = B_2) + P(A_2 = B_1) + P(A_2 \neq B_2)$$

$\square_A = \square_B$ $\square_A = \Delta_B$ $\Delta_A = \square_B$ $\Delta_A \neq \Delta_B$

$\square_B = \Delta_B$

Example: CHSH Bell inequality



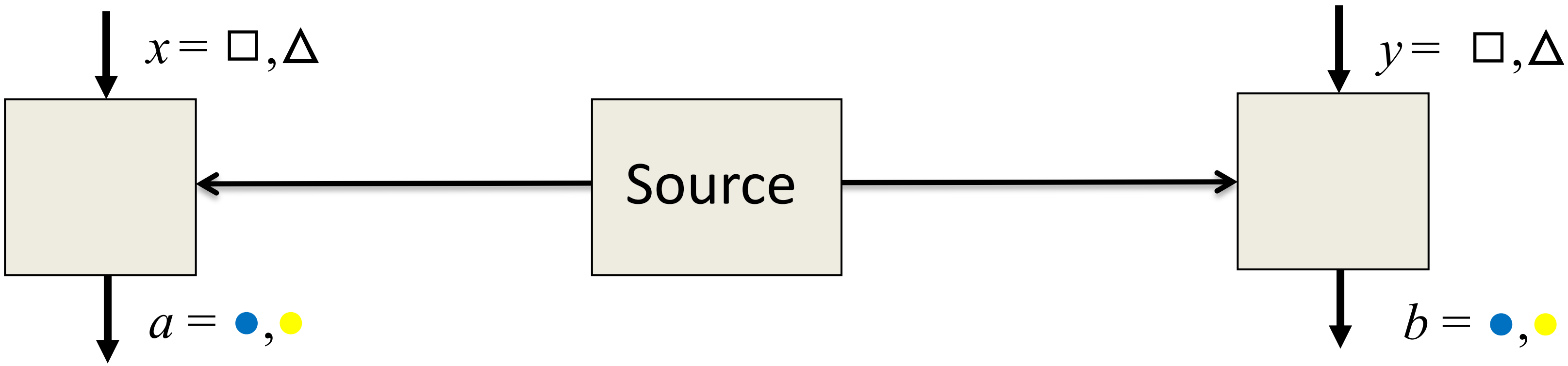
$$CHSH = P(A_1 = B_1) + P(A_1 = B_2) + P(A_2 = B_1) + P(A_2 \neq B_2)$$

$□_A = □_B$ $□_A = Δ_B$ $Δ_A = □_B$ $Δ_A \neq Δ_B$

$□_B = Δ_B$

$Δ_A = Δ_B$

Example: CHSH Bell inequality



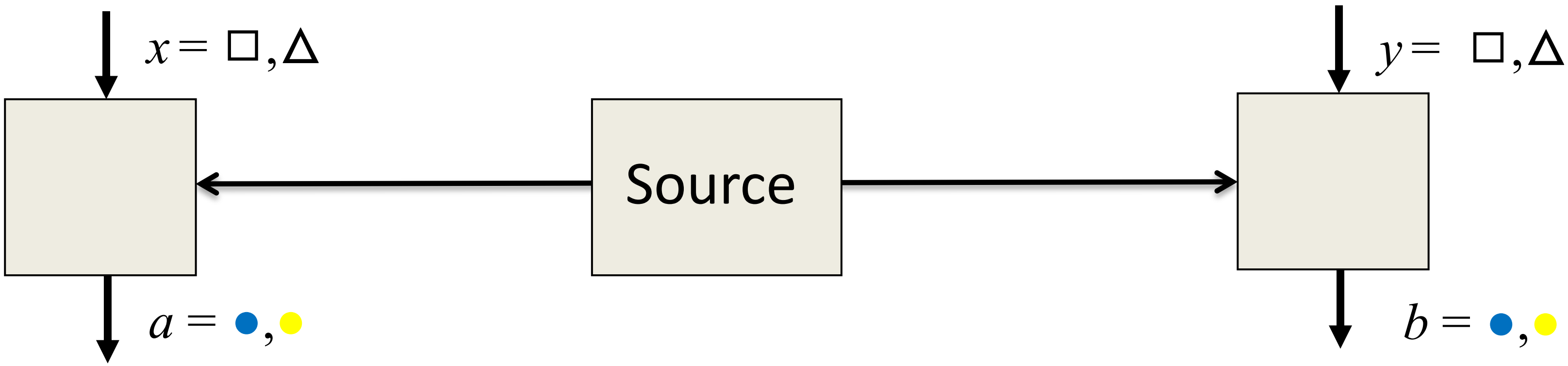
$$CHSH = P(A_1 = B_1) + P(A_1 = B_2) + P(A_2 = B_1) + P(A_2 \neq B_2)$$

$\square_A = \square_B$ $\square_A = \Delta_B$ $\Delta_A = \square_B$ $\Delta_A \neq \Delta_B$

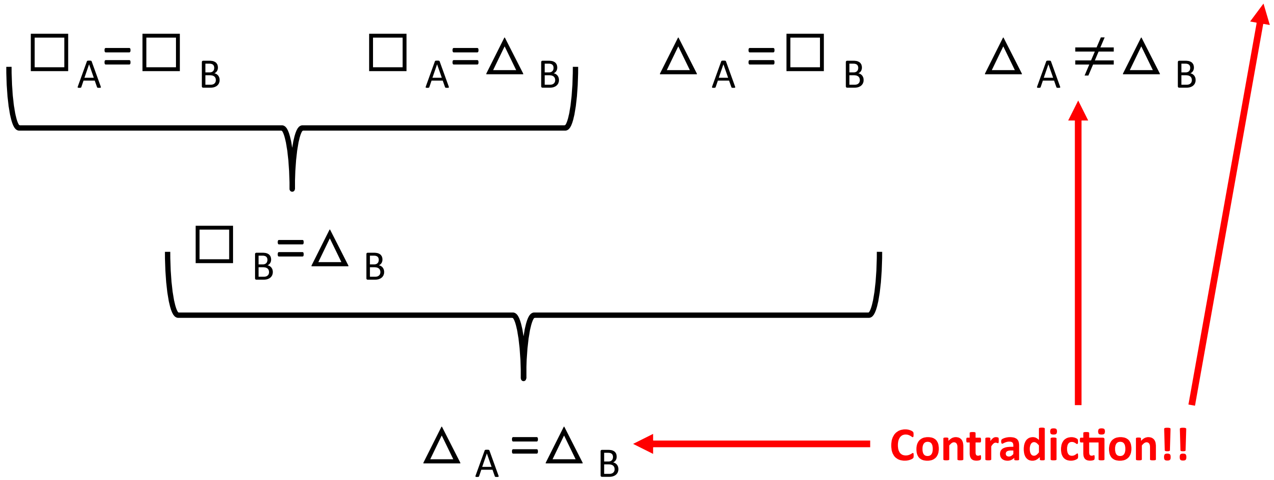
$\square_B = \Delta_B$

$\Delta_A = \Delta_B$ ← **Contradiction!!**

Example: CHSH Bell inequality



$$CHSH = P(A_1 = B_1) + P(A_1 = B_2) + P(A_2 = B_1) + P(A_2 \neq B_2) \leq 3$$

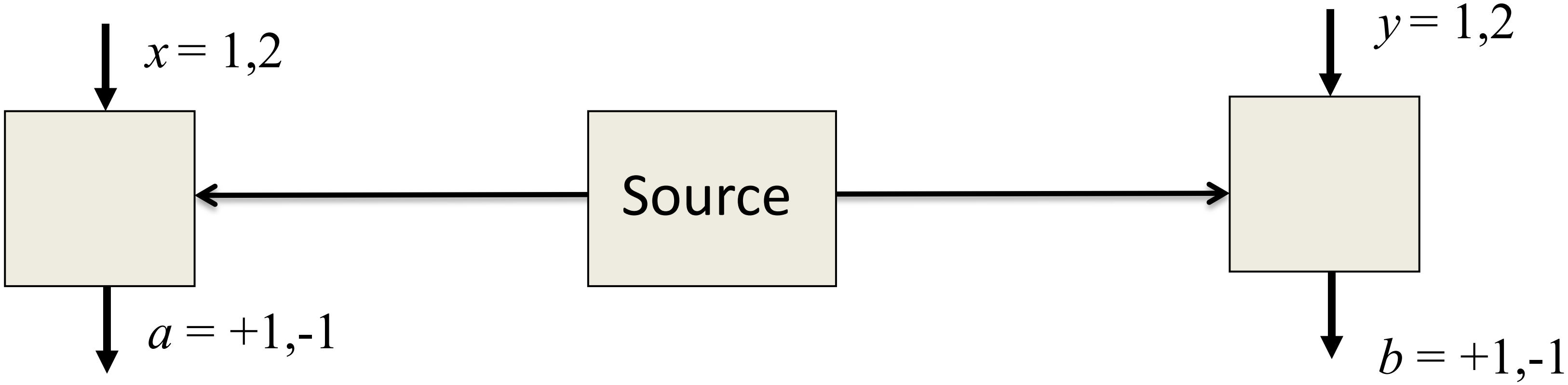


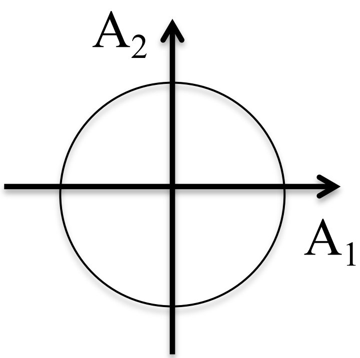
And now, finally, quantum physics come into play because…

And now, finally, quantum physics come into play because…

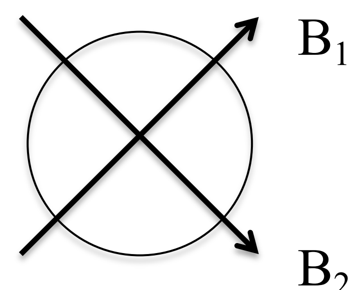
Measurements on correlated quantum particles
may violate a Bell inequality!!

Quantum Bell inequality violation



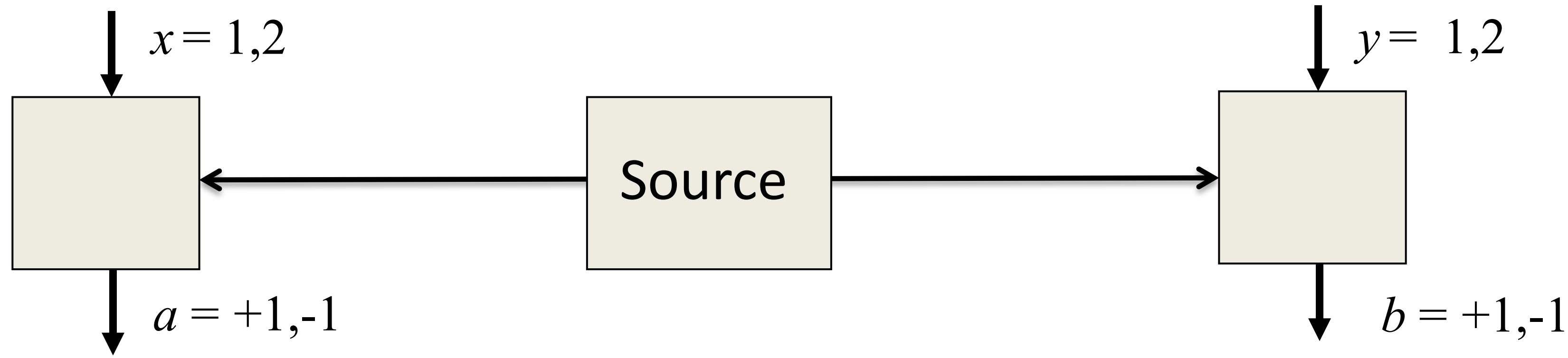


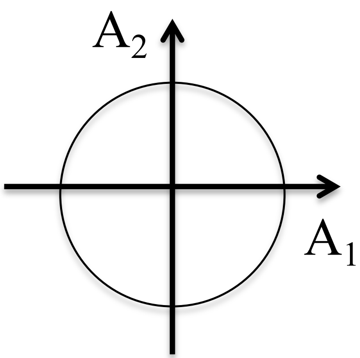
$$|\Phi^{+}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$



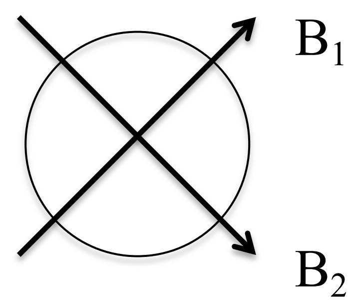
Classical values are now replaced by operators.

Quantum Bell inequality violation





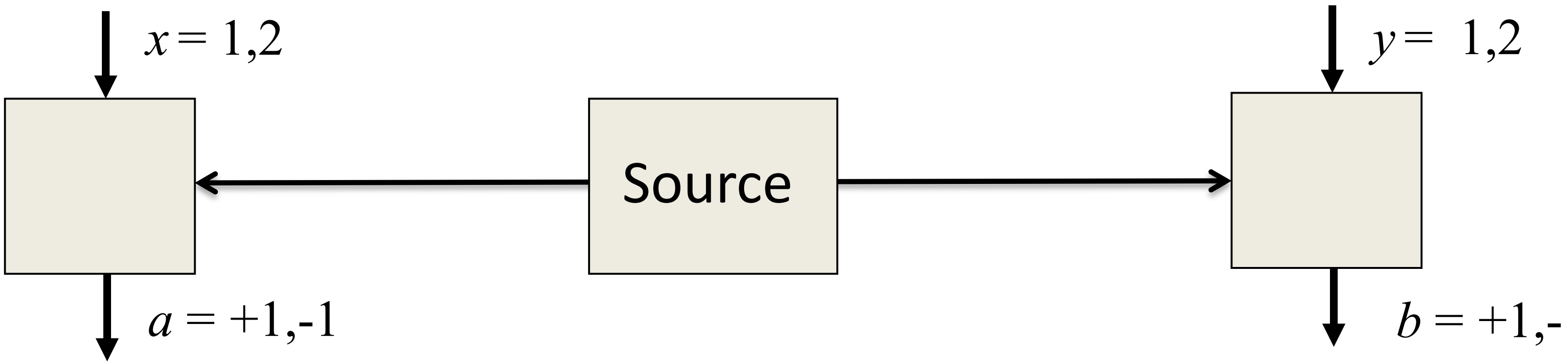
$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$



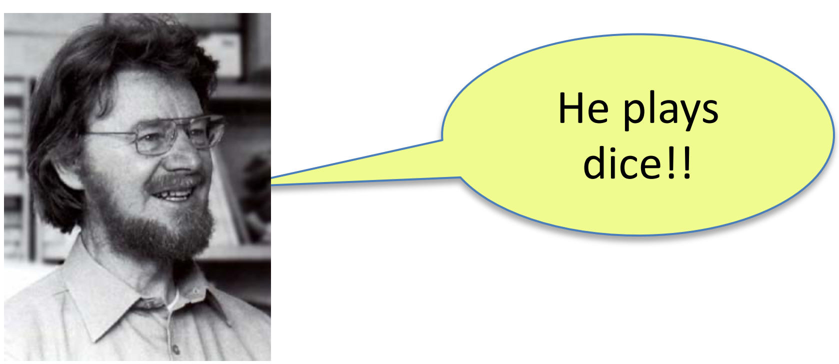
Classical values are now replaced by operators.

$$CHSH = P(A_1 = B_1) + P(A_1 = B_2) + P(A_2 = B_1) + P(A_2 \neq B_2)$$
$$= 2 + \sqrt{2} \approx \mathbf{3.4 > 3!!}$$

Quantum Bell inequality violation



$$CHSH = P(A_1 = B_1) + P(A_1 = B_2) + P(A_2 = B_1) + P(A_2 \neq B_2)$$
$$= 2 + \sqrt{2} \approx \mathbf{3.4 > 3!!}$$

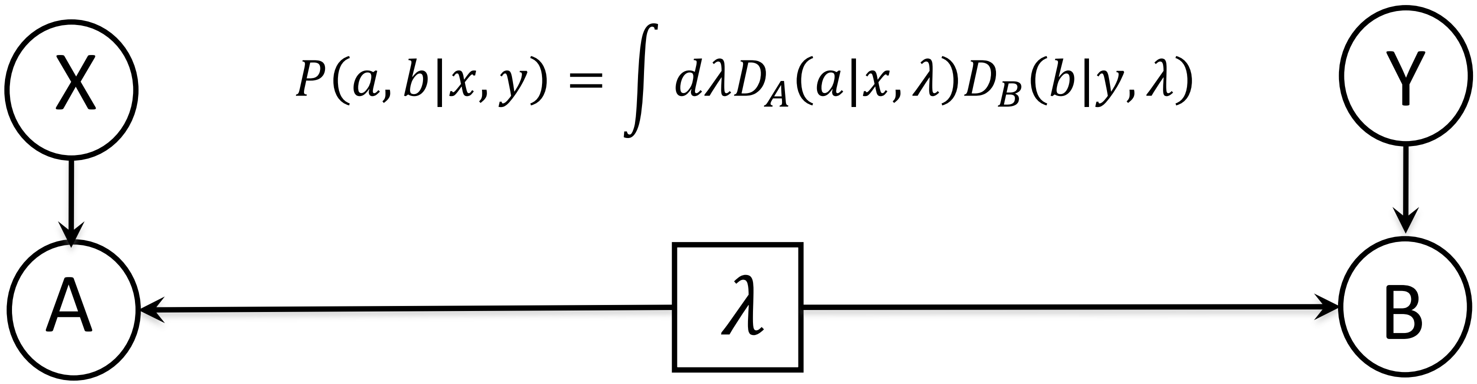


Quantum correlations cannot be explained by deterministic models satisfying the experimental causality constraints.

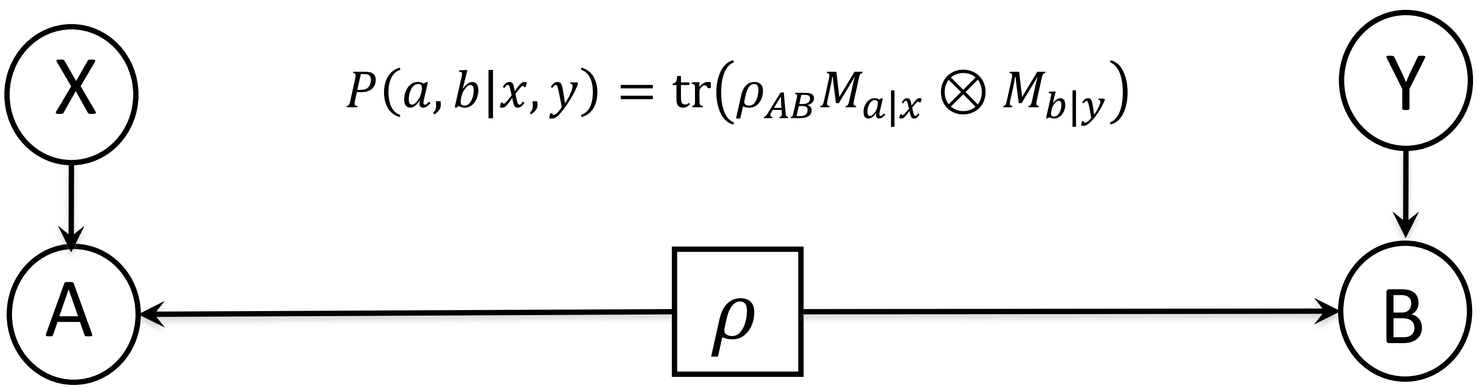
Quantum causality

Bell nonlocal correlations can be explained by a quantum causal model, but not by the causal deterministic counterpart.

$$P(a,b|x,y) = \int d\lambda D_A(a|x,\lambda) D_B(b|y,\lambda)$$

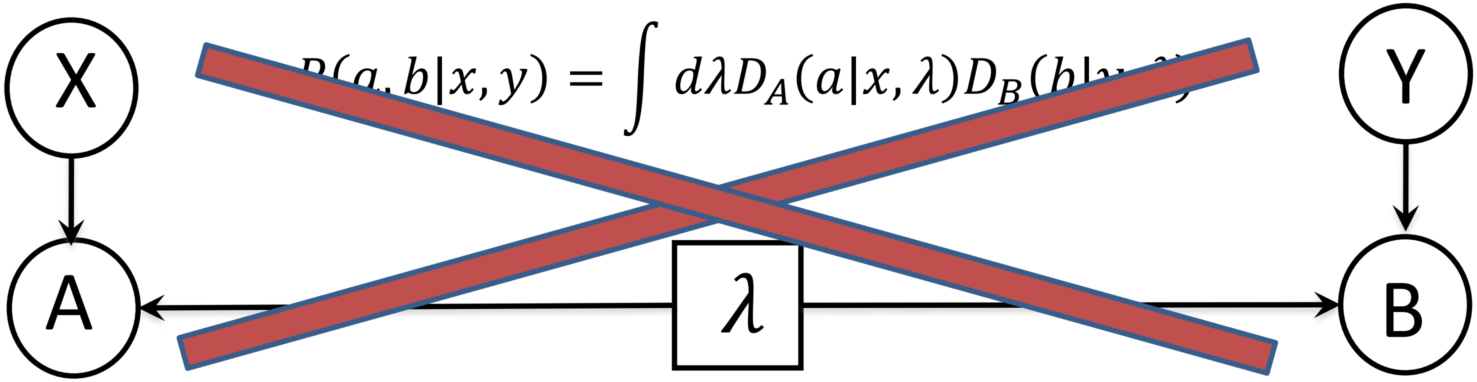


$$P(a,b|x,y) = \mathrm{tr}\big(\rho_{AB} M_{a|x} \otimes M_{b|y}\big)$$

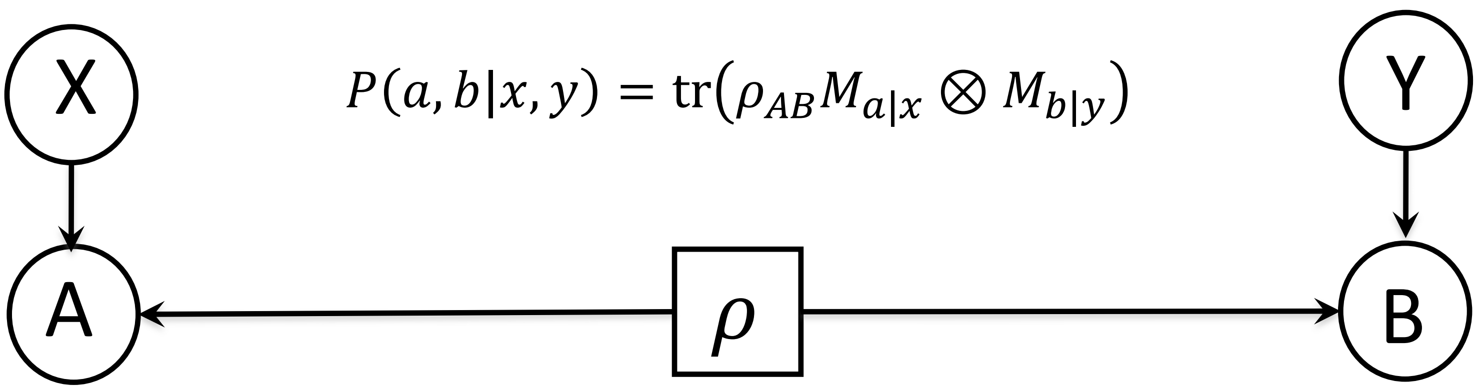


Quantum causality

Bell nonlocal correlations can be explained by a quantum causal model, but not by the causal deterministic counterpart.



$$P(a,b|x,y) = \int d\lambda D_A(a|x,\lambda) D_B(b|y,\lambda)$$

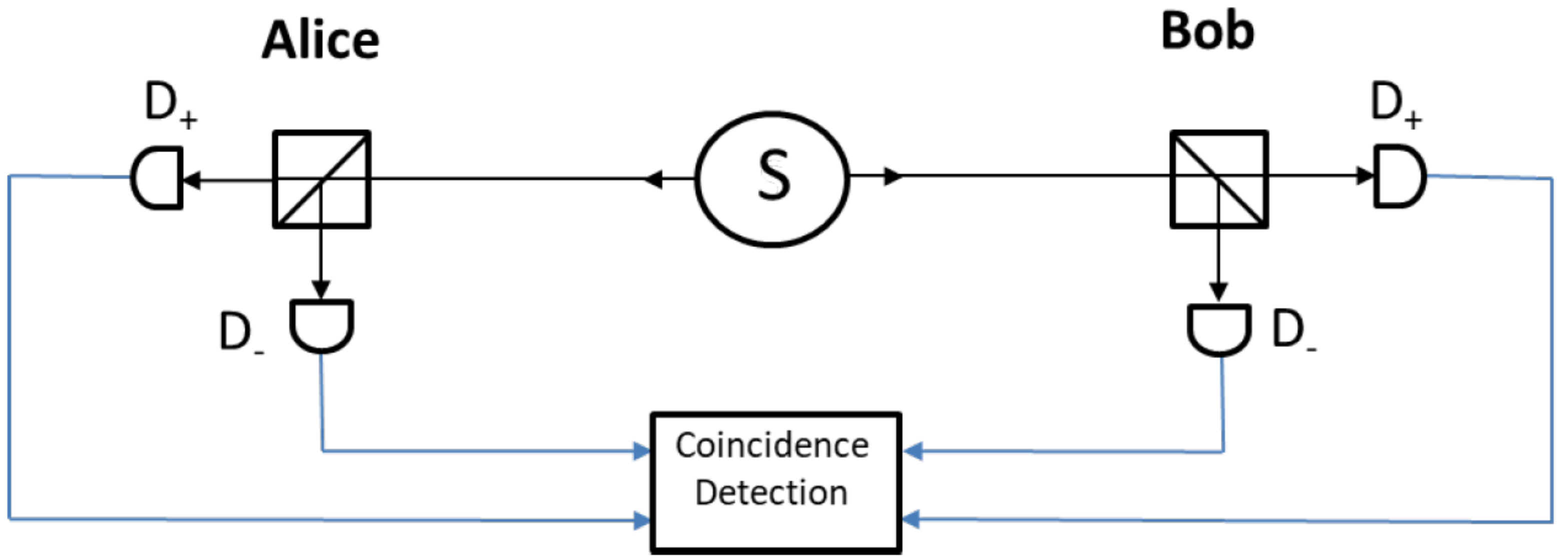


$$P(a,b|x,y) = \mathrm{tr}\left(\rho_{AB} M_{a|x} \otimes M_{b|y}\right)$$

Bell experiments

Entanglement can be observed between any pair of quantum particles.

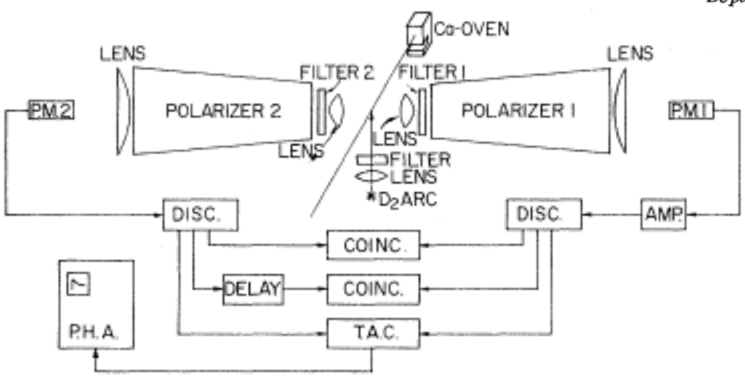
Bell experiments



Entanglement can be observed between any pair of quantum particles.

If the goal is to send these particles to two distant places, better use quanta of light → entangled photons.

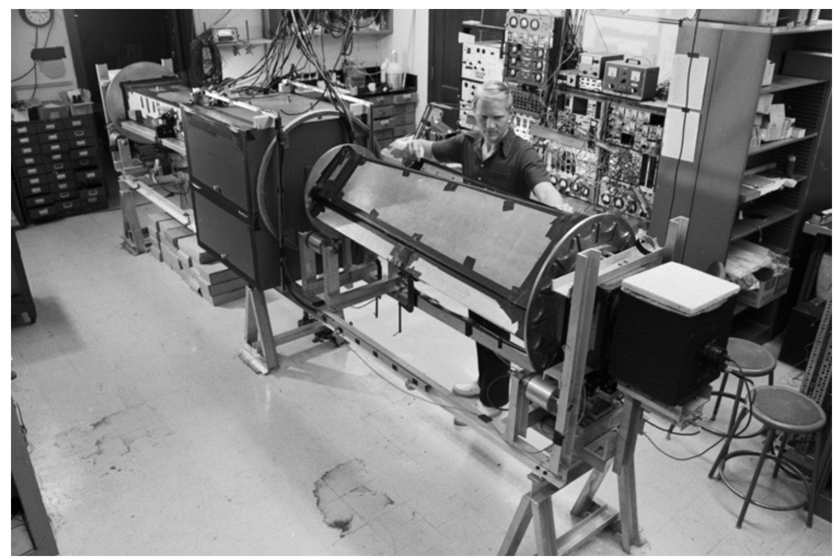
First Bell experiments



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)

John Clauser



First Bell experiments

Alain Aspect

VOLUME 49, NUMBER 2 PHYSICAL REVIEW LETTERS 12 JULY 1982

Experimental Realization of Einstein-Podolsky-Rosen-Bohm *Gedankenexperiment*: A New Violation of Bell's Inequalities

Alain Aspect, Philippe Grangier, and Gérard Roger
Institut d'Optique Théorique et Appliquée, Laboratoire associé au Centre National de la Recherche Scientifique, Université Paris-Sud, F-91406 Orsay, France
(Received 30 December 1981)

Experimental Test of Bell's Inequalities Using Time-Varying Analyzers

Alain Aspect, Jean Dalibard,[a] and Gérard Roger
Institut d'Optique Théorique et Appliquée, F-91406 Orsay Cédex, France
(Received 27 September 1982)

First Bell experiments

Alain Aspect

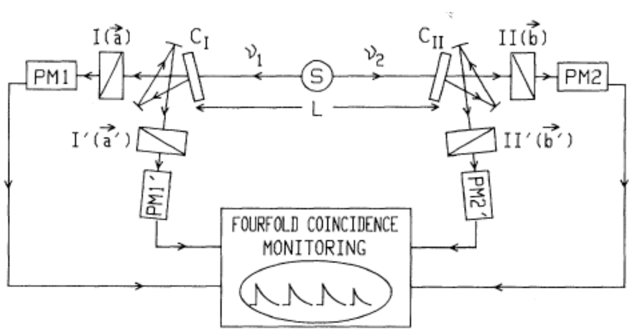
VOLUME 49, NUMBER 2 PHYSICAL REVIEW LETTERS 12 JULY 1982

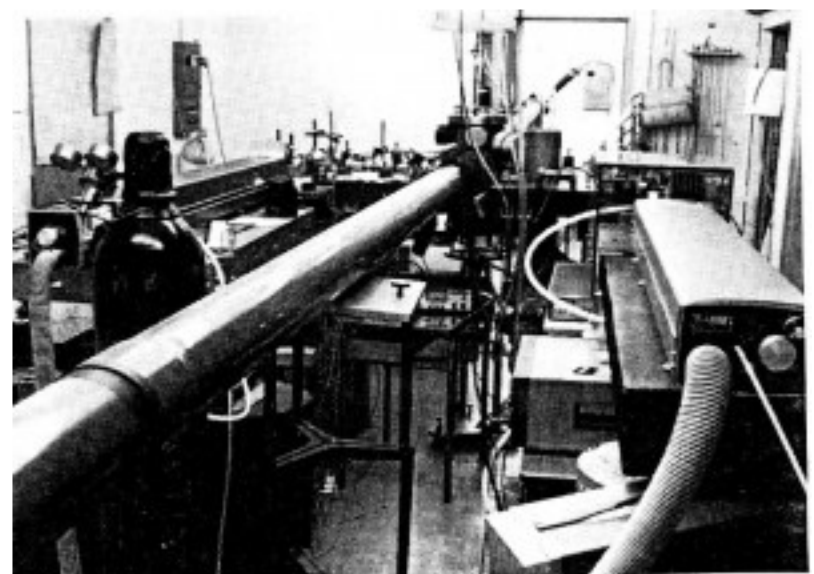
Experimental Realization of Einstein-Podolsky-Rosen-Bohm *Gedankenexperiment*: A New Violation of Bell's Inequalities

Alain Aspect, Philippe Grangier, and Gérard Roger
Institut d'Optique Théorique et Appliquée, Laboratoire associé au Centre National de la Recherche Scientifique, Université Paris-Sud, F-91406 Orsay, France
(Received 30 December 1981)

Experimental Test of Bell's Inequalities Using Time-Varying Analyzers

Alain Aspect, Jean Dalibard,[a] and Gérard Roger
Institut d'Optique Théorique et Appliquée, F-91406 Orsay Cédex, France
(Received 27 September 1982)





Experimental quantum teleportation

Anton Zeilinger

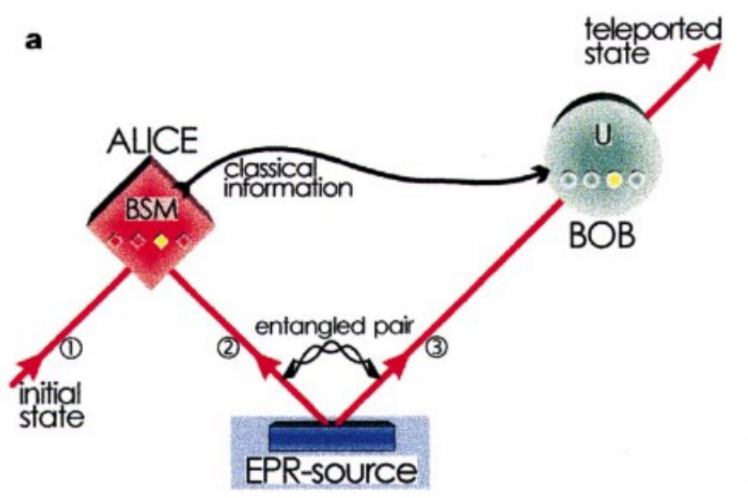
articles

Experimental quantum teleportation

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

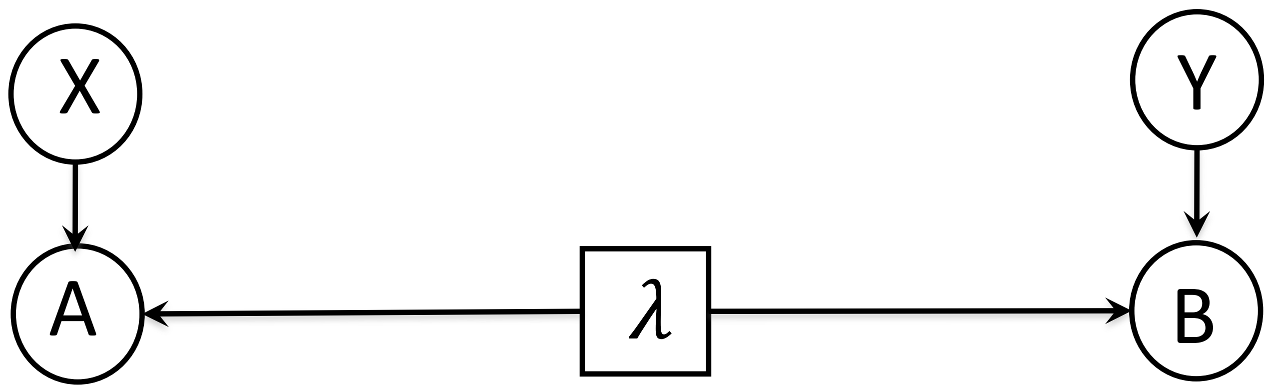
Institut für Experimentalphysik, Universität Innsbruck, Technikerstr. 25, A-6020 Innsbruck, Austria

1997



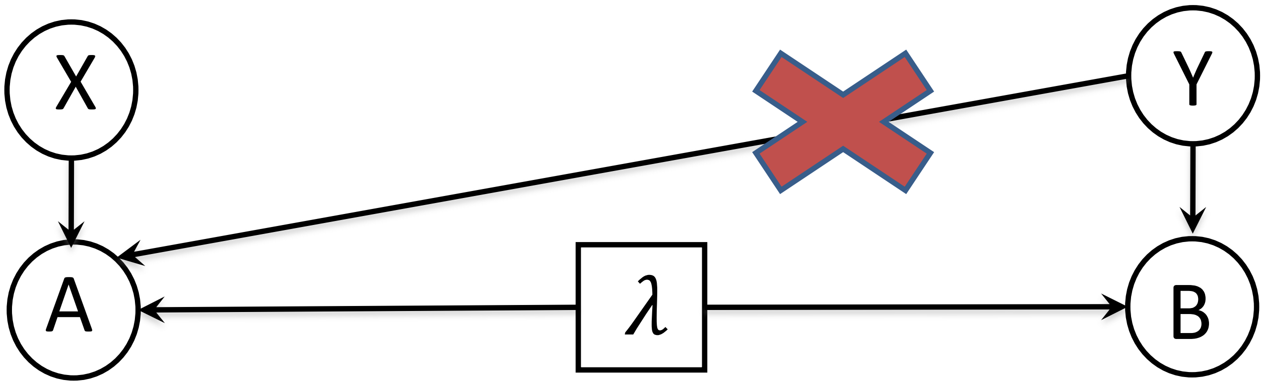
Bell experiments

The setup should enforced the constraints of the causal network.



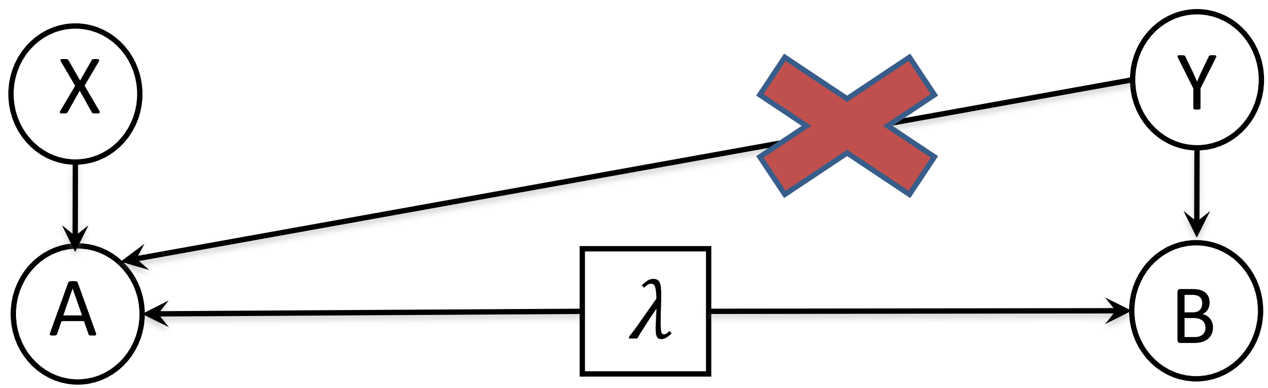
Bell experiments

The setup should enforced the constraints of the causal network.



Bell experiments

The setup should enforced the constraints of the causal network.



Often space-like considerations are used to exclude non-wanted causal connections.
IMO: not necessarily stronger than other type of considerations. Example: choose the settings in a Bell test with Twitter and the Valladolid phone book.
There are many ways of excluding causal constraints, none with 100% confidence.
Recall that this possible extra causal links do not lead to “noticeable” effects.

Let’s stop for a while…

- If you are not surprised by this result, my talk is a failure.

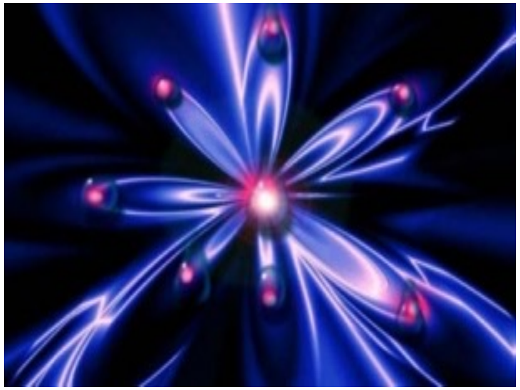
- Bell inequality violation is the phenomenon where quantum physics more radically departs from our classical intuition.

- Bell inequality violations have been observed in many labs: it is confirmed that EPR classical models cannot explain nature.

- Can we use this phenomenon for something?

Quantum Information Theory

What happens when we encode information on quantum particles?

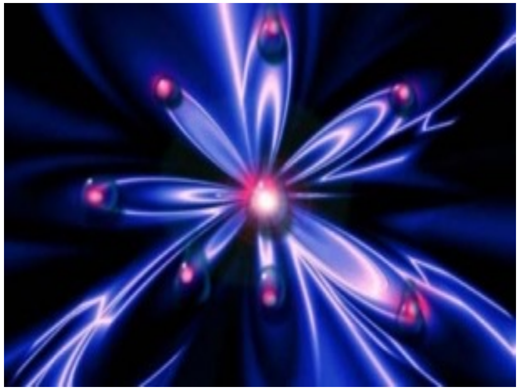


Novel information applications become possible thanks to quantum effects, e.g. more powerful computers and secure cryptography.

Change of paradigm: **physics matters!**

Quantum Information Theory

What happens when we encode information on quantum particles?



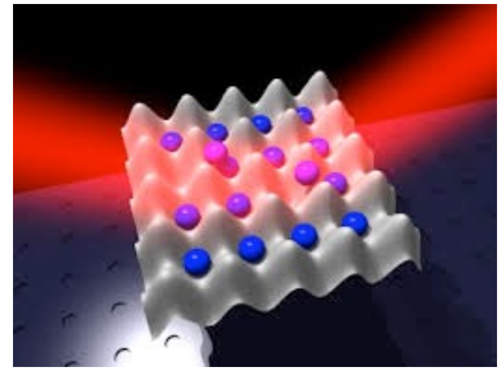
Novel information applications become possible thanks to quantum effects, e.g. more powerful computers and secure cryptography.

Change of paradigm: **physics matters!**

Yet, the role of Bell nonlocality in standard quantum information theory is quite marginal.

Quantum information technologies

Quantum Computer



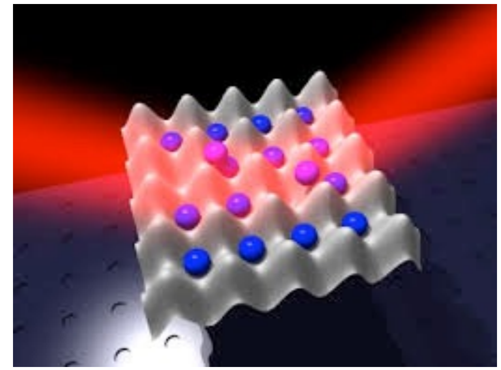
Quantum Simulator

Quantum Cryptography

QRNG

Quantum certification

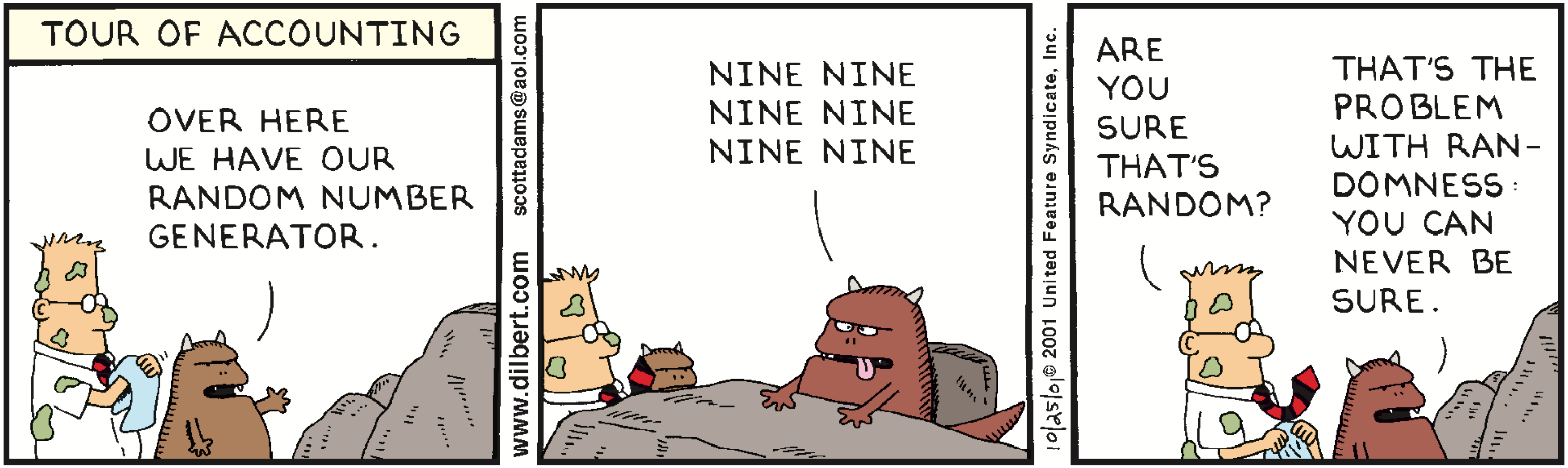
Is this a quantum computer?

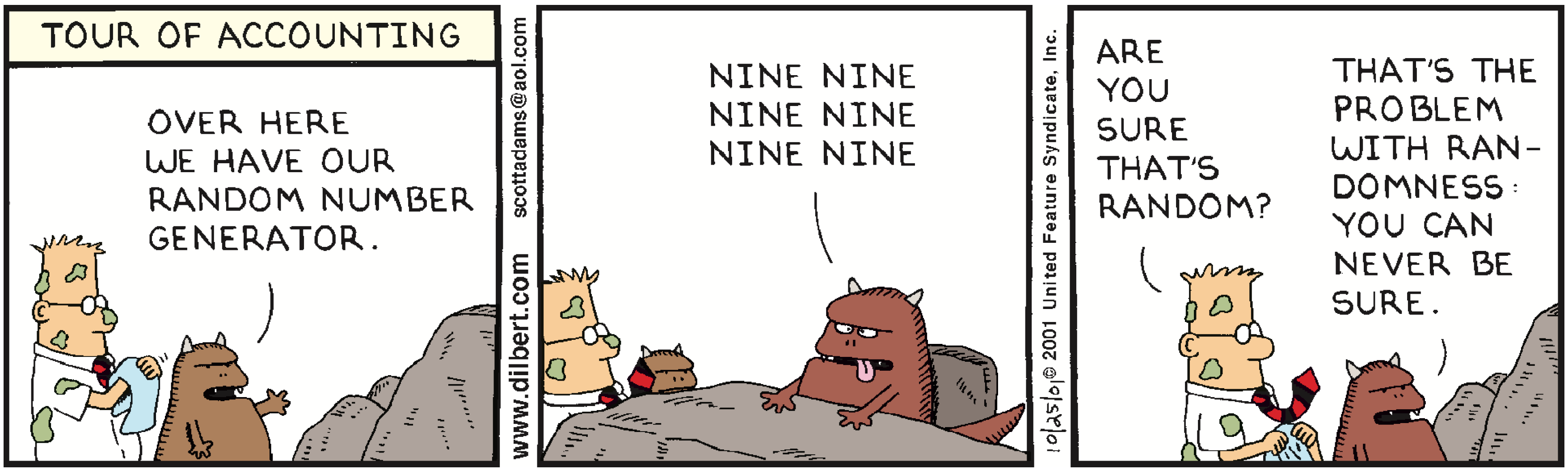


Does this properly simulate
a quantum system?

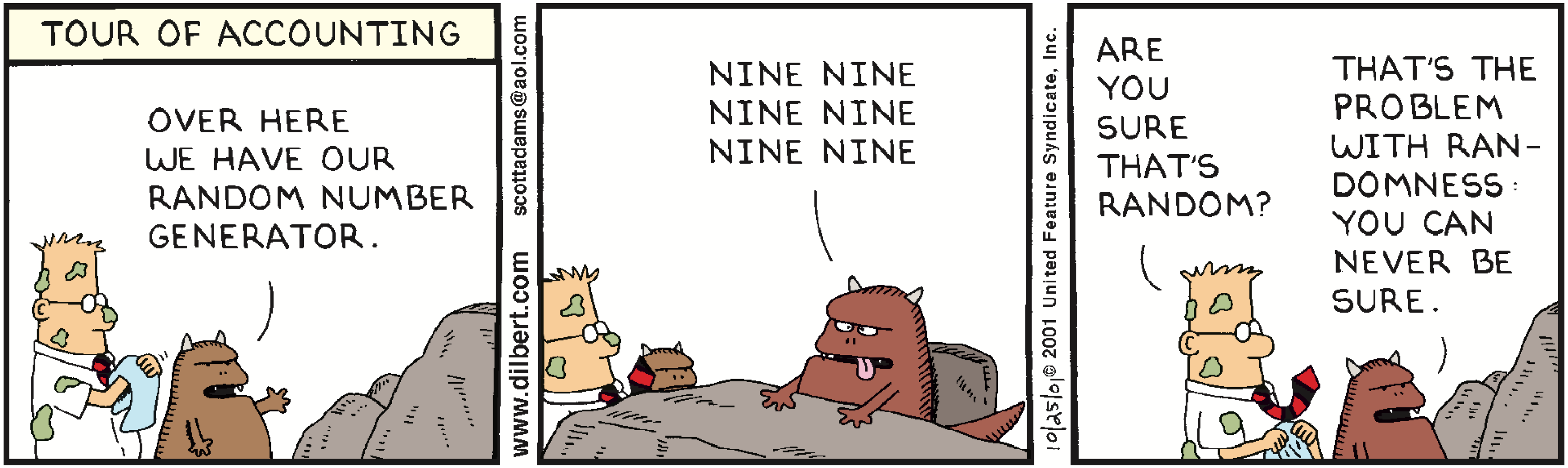
Is this cryptographically secure?

Is this quantum random?


TOUR OF ACCOUNTING
OVER HERE WE HAVE OUR RANDOM NUMBER GENERATOR.
scottadams@aol.com
www.dilbert.com
NINE NINE NINE NINE NINE NINE
10/25/01 © 2001 United Feature Syndicate, Inc.
ARE YOU SURE THAT'S RANDOM?
THAT'S THE PROBLEM WITH RAN-DOMNESS: YOU CAN NEVER BE SURE.

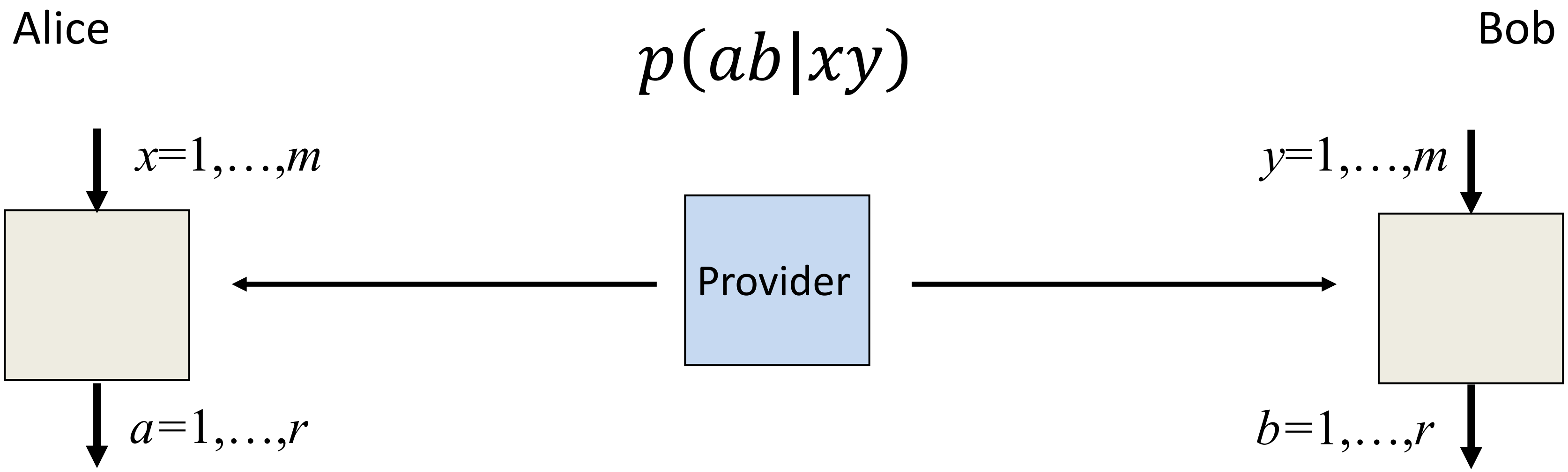


Can one certify the presence of (quantum) randomness?

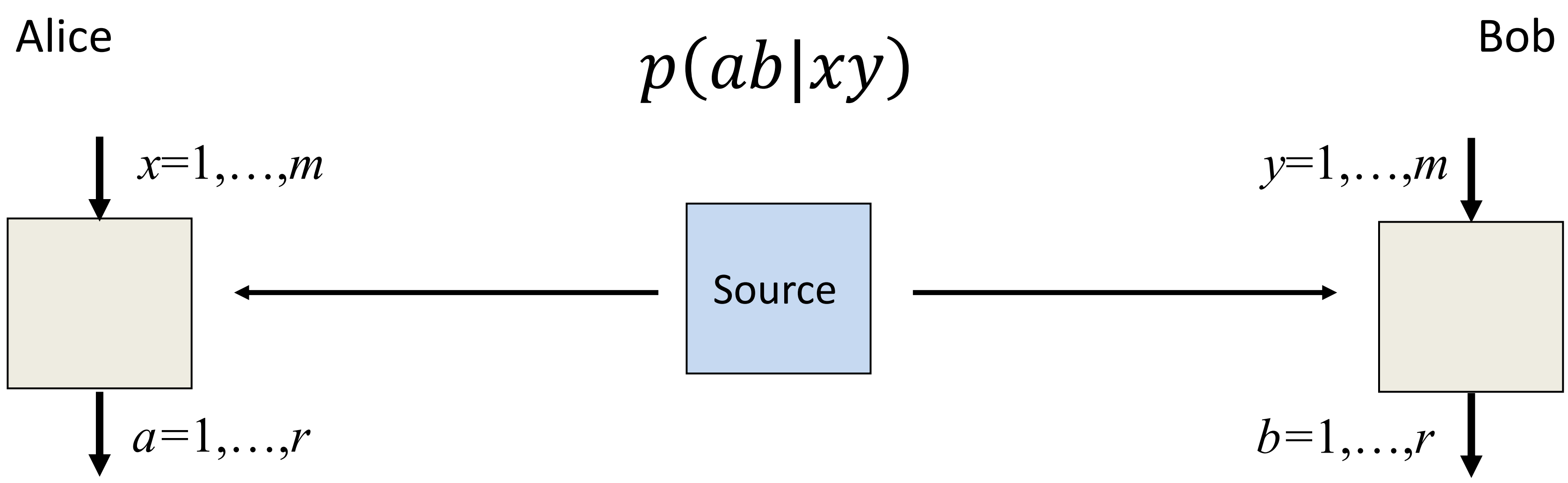


How can one certify a quantum device from its outputs?

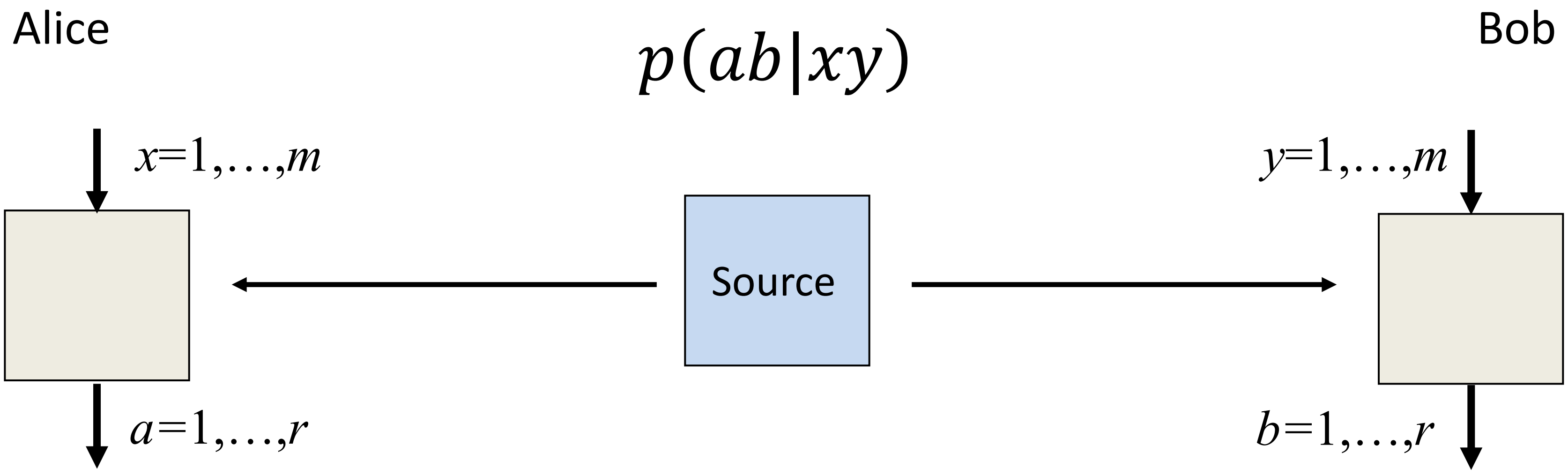
From certification to Bell theorem



From certification to Bell theorem

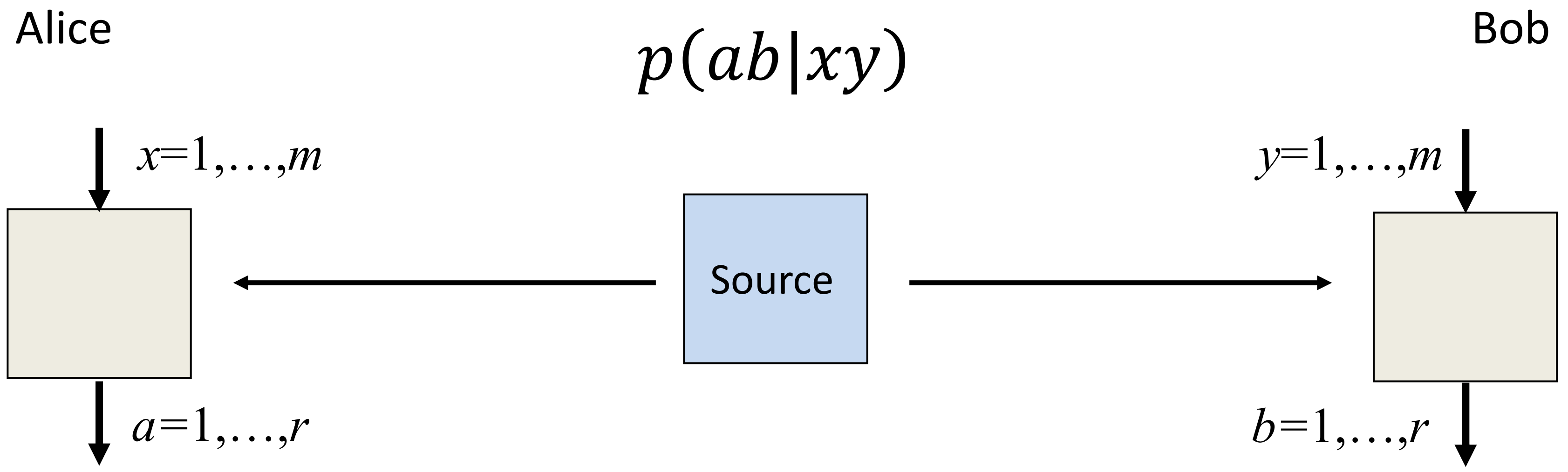


From certification to Bell theorem



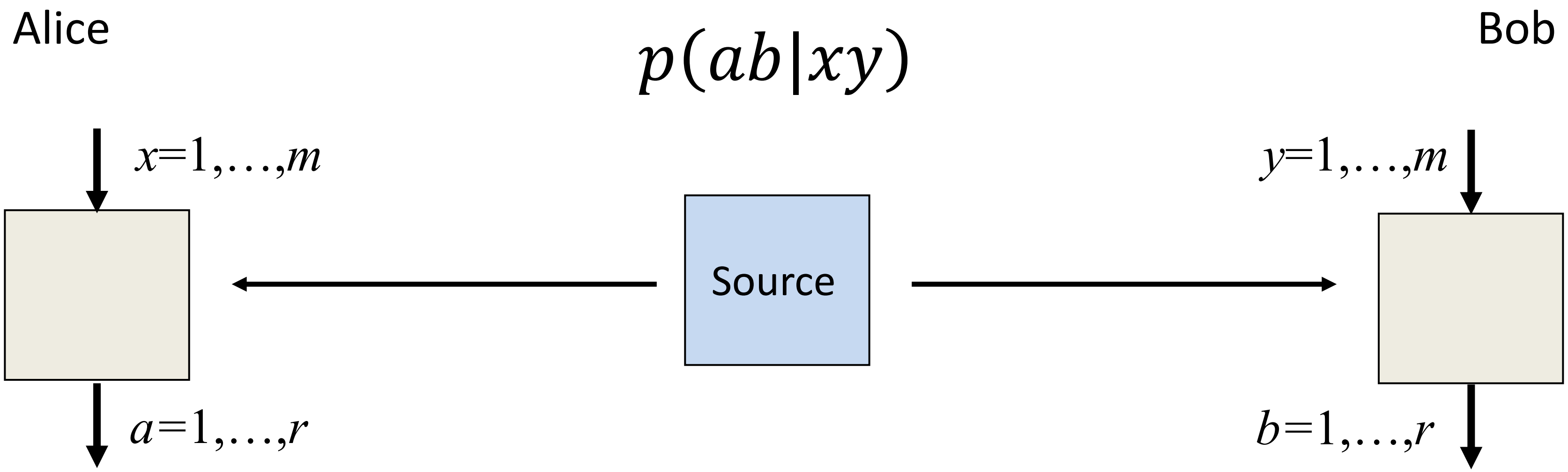
This is nothing but a Bell test, in which local measurements are performed on two separated systems, prepared by the source.

One of the main lessons of Bell theorem



The statistics of an experiment, a.k.a. correlations, depends on the physical properties of the measured systems.

One of the main lessons of Bell theorem



The statistics of an experiment, a.k.a. correlations, depends on the physical properties of the measured systems.

The observation of a Bell violation certified that Alice and Bob have quantum (entangled) devices.

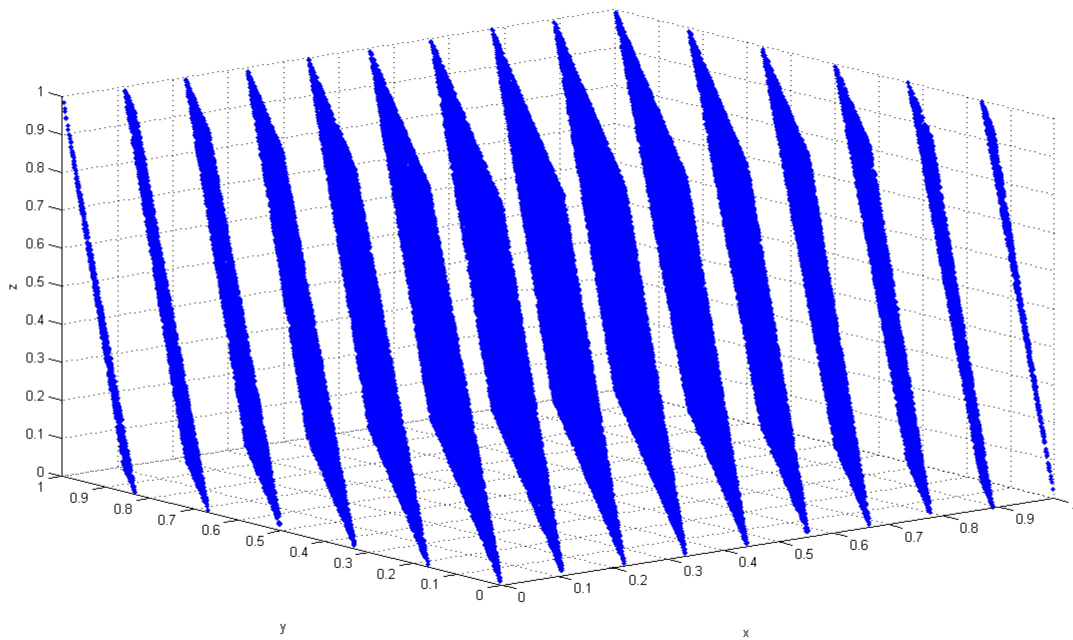
Bell certified QRNG

Problem 1: certification

- Good randomness is usually verified by a series of statistical tests.
- There exist chaotic systems, of deterministic nature, that pass all existing randomness tests.
- Do these tests really certify the presence of randomness? It is well known that no finite set of tests can do it.
- Do these tests certify any form of quantum randomness? Classical systems pass them!

RANDU

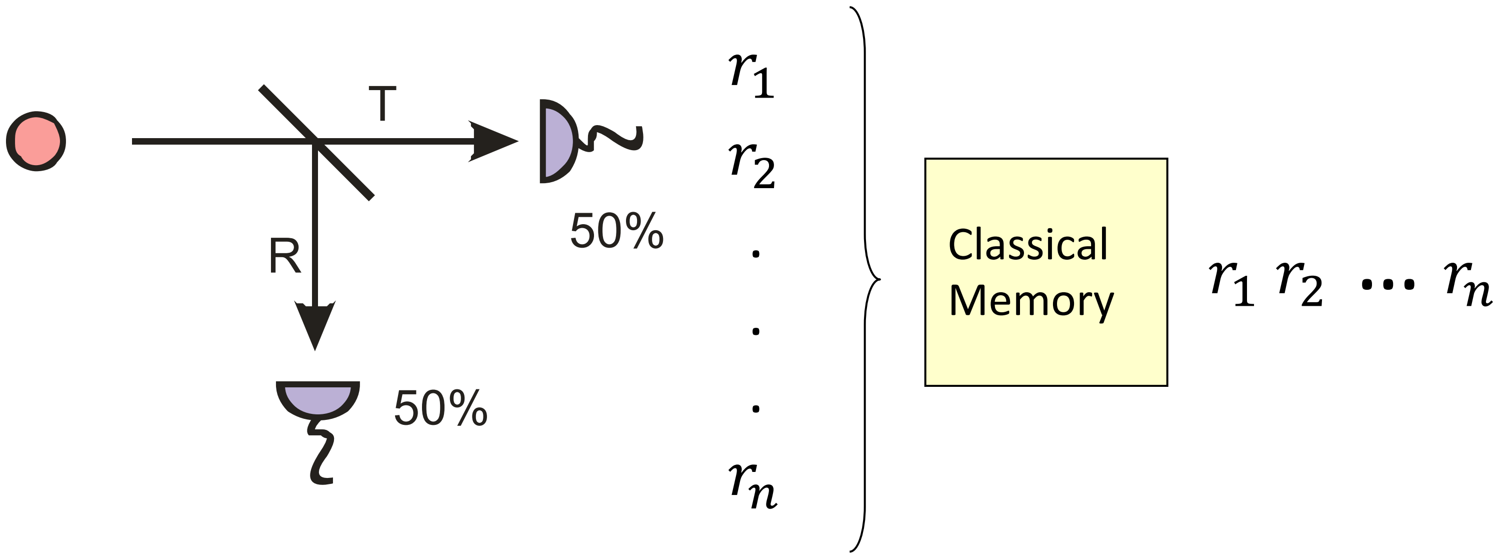
RANDU is an infamous linear congruential pseudorandom number generator of the Park–Miller type, which has been used since the 1960s.



Three-dimensional plot of 100,000 values generated with RANDU. Each point represents 3 subsequent pseudorandom values. It is clearly seen that the points fall in 15 two-dimensional planes.

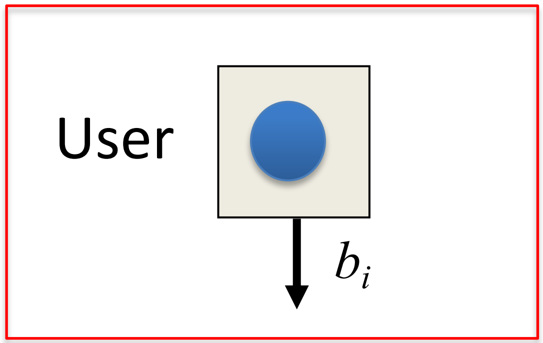
Problem 2: privacy

The memory-stick attack

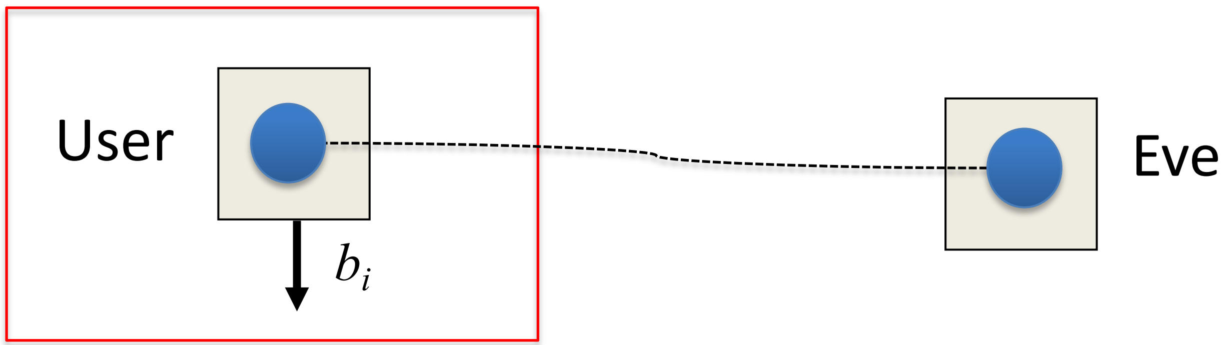


The provider has access to a proper RNG. The provider uses it to generate a long sequence of good random numbers, stores them into a memory stick and sells it as a proper RNG to the user. The numbers generated by the user look random. However, they can be perfectly predicted by the adversary

Definition of randomness

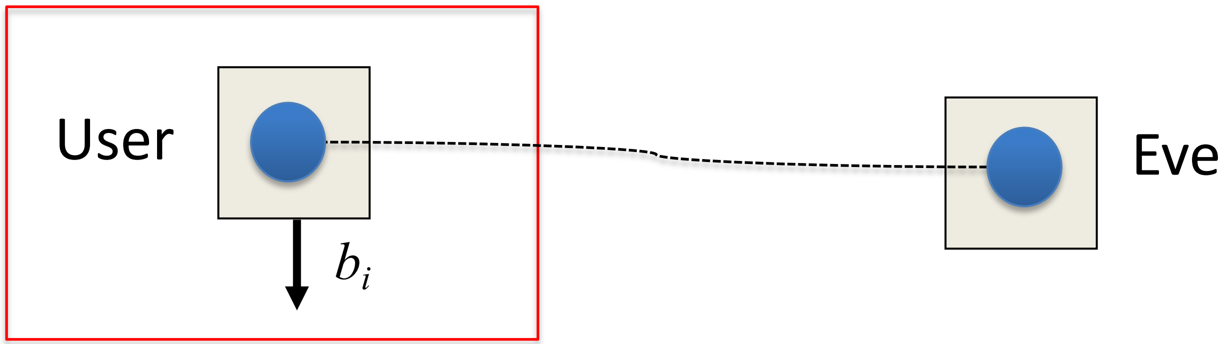


Definition of randomness



N bits are **perfectly random** if they are unpredictable, not only to the user of the device, but to **any observer**.

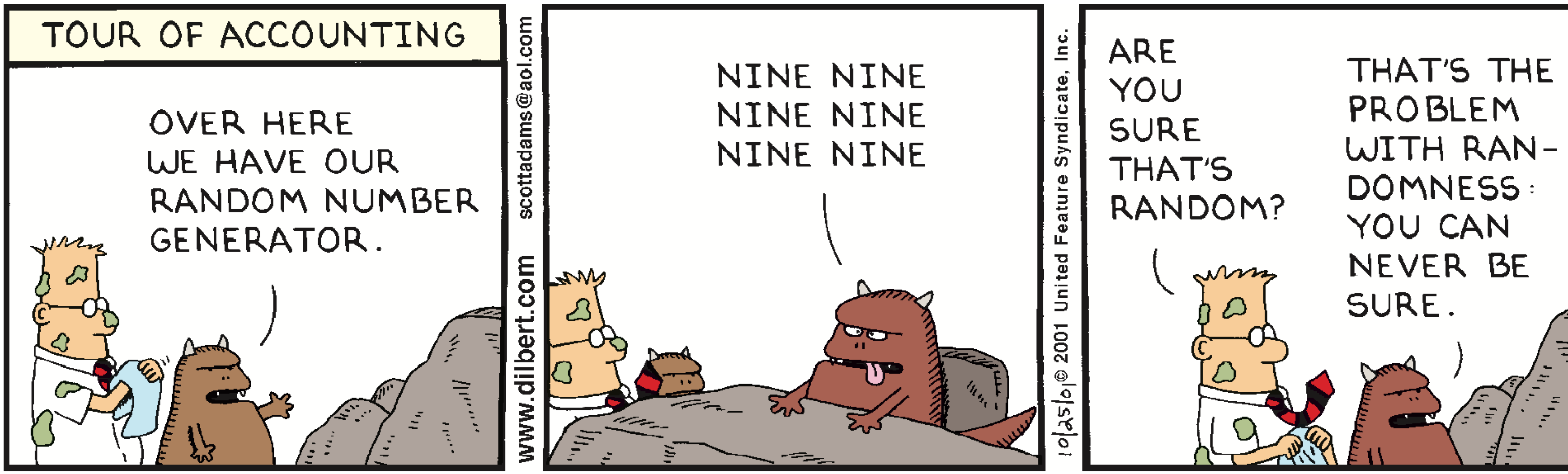
Definition of randomness

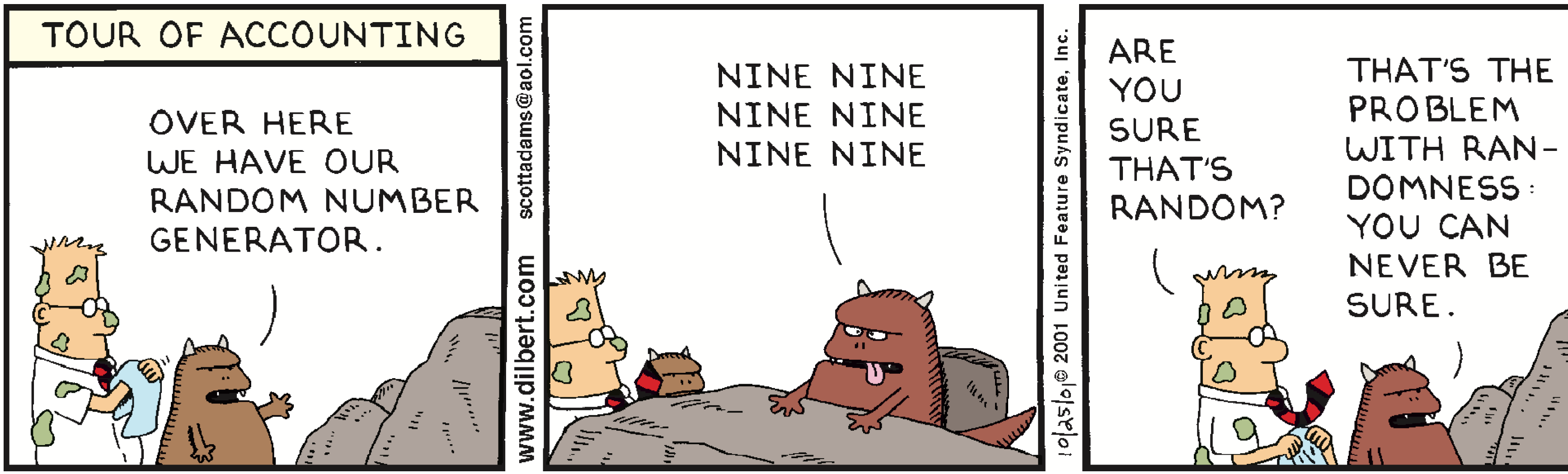


N bits are **perfectly random** if they are unpredictable, not only to the user of the device, but to **any observer**.

This definition is satisfactory both from a fundamental and applied perspective.

- From a fundamental perspective it is difficult to argue that a process is random if there could exist an observer able to predict its outcomes.
- From a practical perspective, by demanding that the results should look random to any observer, the generated randomness is guaranteed to be **private**.


TOUR OF ACCOUNTING
OVER HERE WE HAVE OUR RANDOM NUMBER GENERATOR.
NINE NINE NINE NINE NINE NINE
ARE YOU SURE THAT'S RANDOM?
THAT'S THE PROBLEM WITH RAN-DOMNESS: YOU CAN NEVER BE SURE.
scottadams@aol.com
www.dilbert.com
© 2001 United Feature Syndicate, Inc.



Can the presence of randomness be guaranteed by any physical mechanism?

Quantum Bell violation

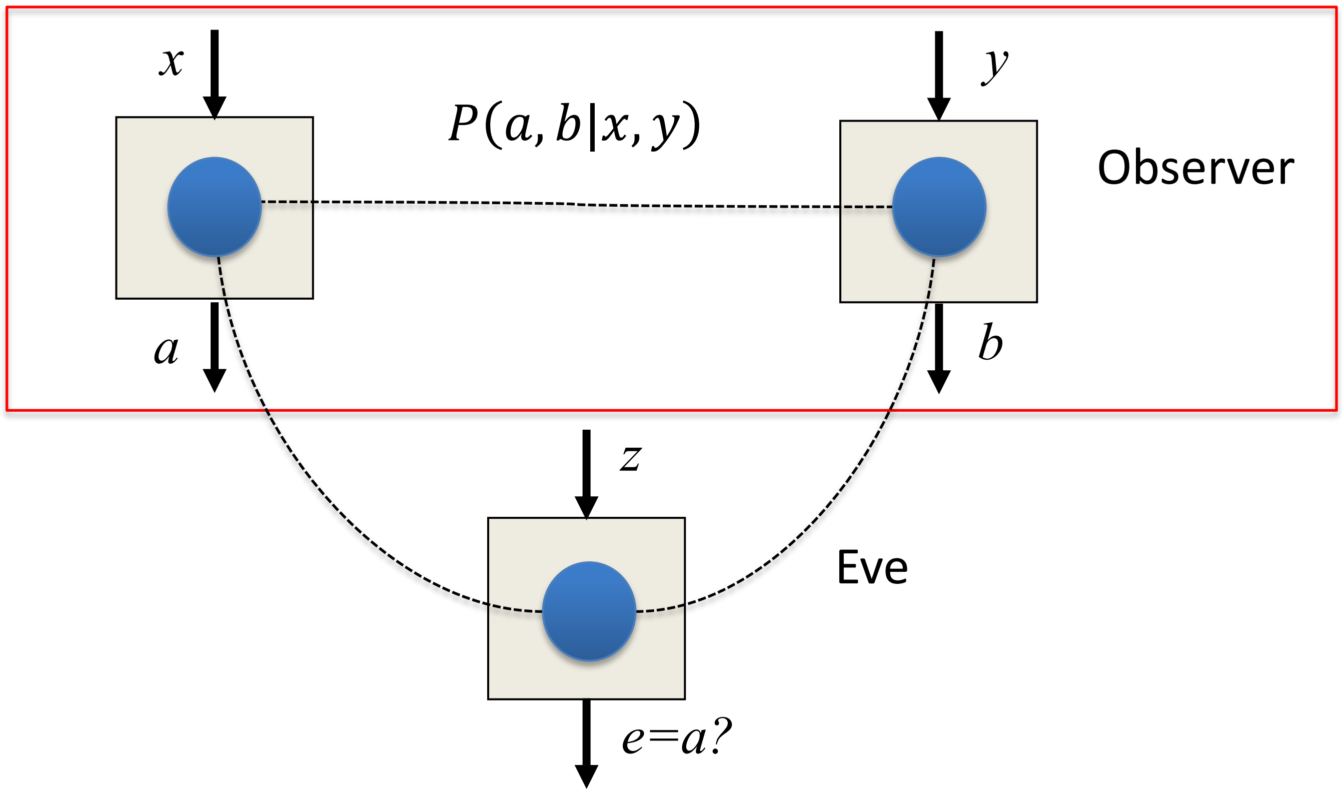
- Bell inequalities are conditions satisfied by classical models in which measurement outputs are pre-determined.

- Correlations observed when measuring entangled states may lead to a violation of Bell inequality and, therefore, do not have a classical counterpart. These correlations are usually called non-local.

- If some observed correlations violate a Bell inequality, the outcomes could not have pre-determined in advance ➔ **They are random.**

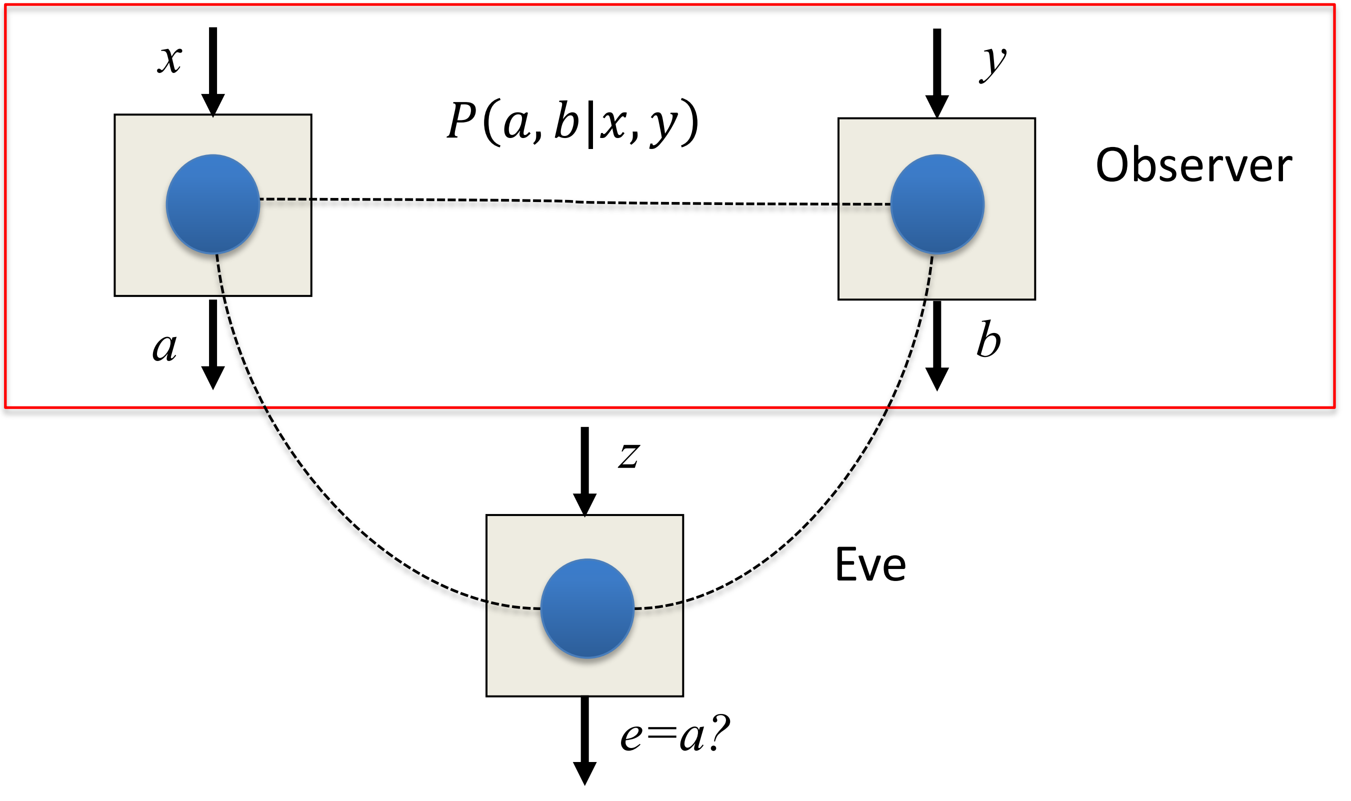
- If some observed correlations violate a Bell inequality, they cannot be reproduced classically ➔ **The devices are quantum.**

Certified randomness



Ask the provider not one but **two** devices. If a Bell inequality violation is observed, the outputs contain some randomness.

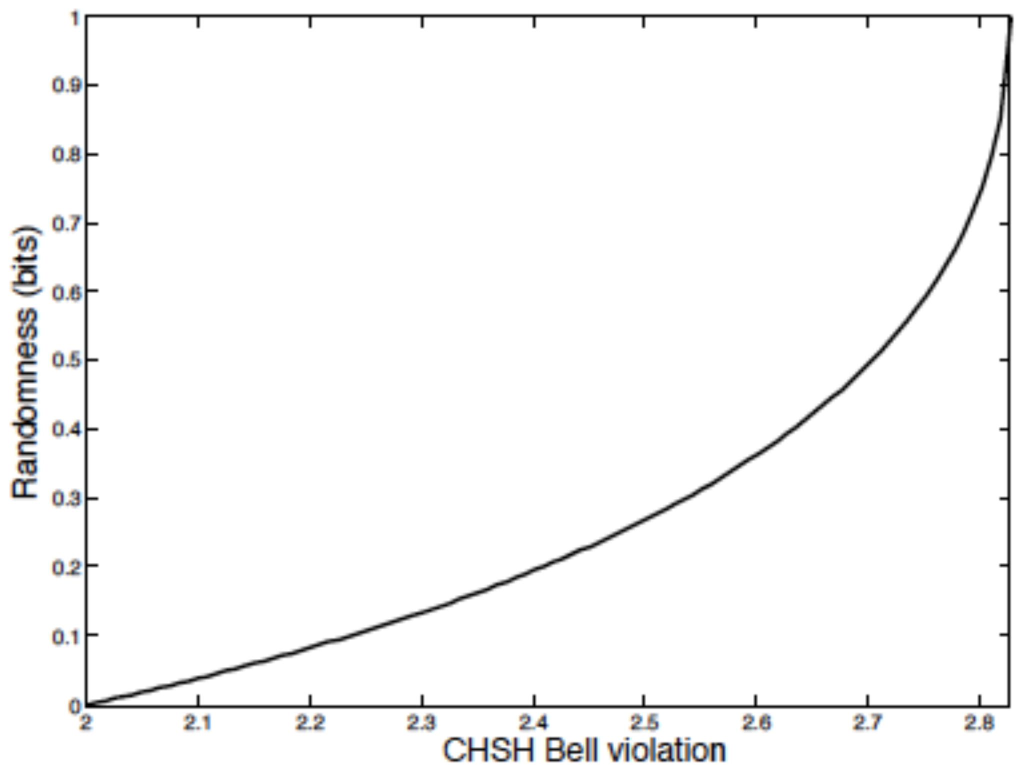
Certified randomness



Ask the provider not one but **two** devices. If a Bell inequality violation is observed, the outputs contain some randomness.
The certification is device-independent, in the sense that it does not rely on any assumption on the internal working of the device.

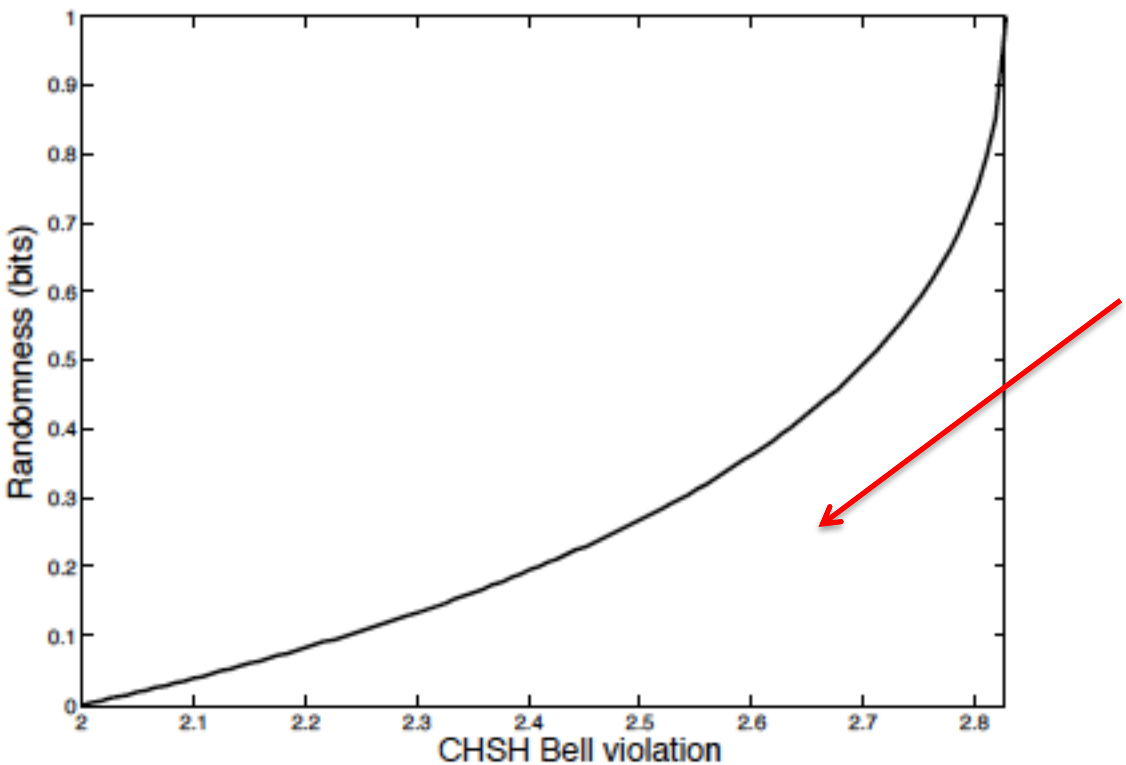
Certified randomness

The randomness in the outputs can be estimated from the amount of Bell violation.
At no violation, there is no randomness. One random bit at maximal violation.



Certified randomness

The randomness in the outputs can be estimated from the amount of Bell violation. At no violation, there is no randomness. One random bit at maximal violation.

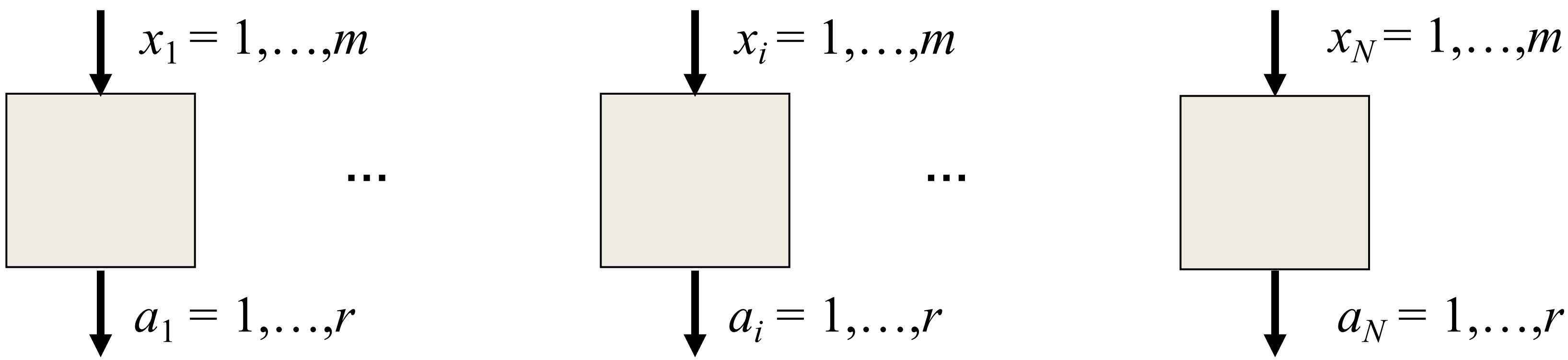


This region is impossible within quantum physics. The certified randomness is not a consequence of ignorance!

A quantum information theory based solely on Bell nonlocality?

DI quantum information processing

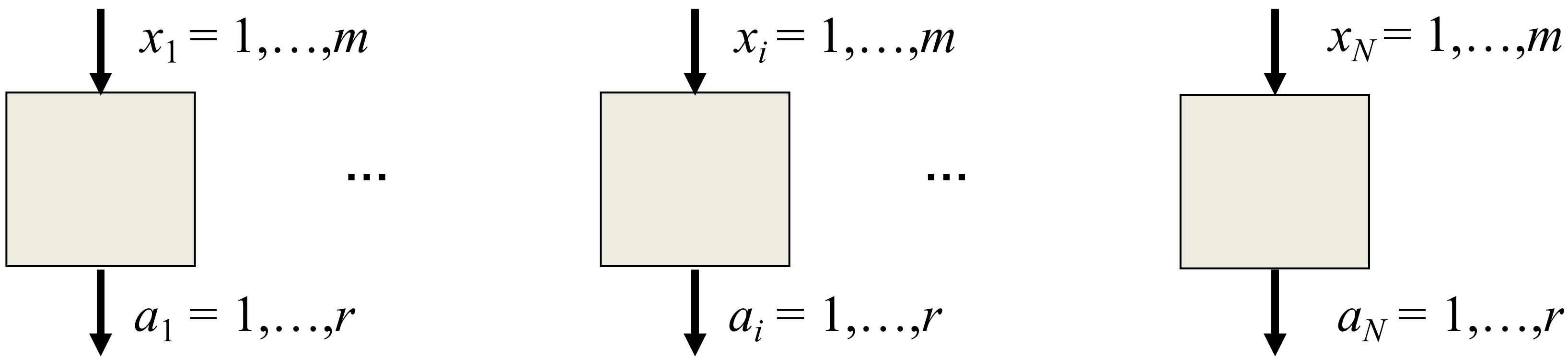
Develop a new form of **quantum information theory** in a scenario where the users' devices are just seen as (quantum) **black boxes** processing classical information. The resulting protocols have **self-certification**.



Observed statistics

$$p(a_1 \ldots a_N | x_1 \ldots x_N)$$

DI quantum information processing



Observed statistics

$$p(a_1 \ldots a_N | x_1 \ldots x_N)$$

Clearly, if some correlations are local ➔ they can be reproduced classically ➔ no improvement can be expected over classical information theory.

Bell nonlocality is a necessary condition for any task in this scenario.

Conclusions

- Bell inequalities are conditions satisfied by classical models in which measurement outputs of non-communicating observers are pre-determined.

Conclusions

- Bell inequalities are conditions satisfied by classical models in which measurement outputs of non-communicating observers are pre-determined.

- Correlations observed when measuring entangled states may lead to a violation of Bell inequality and, therefore, do not have a classical counterpart.

Conclusions

- Bell inequalities are conditions satisfied by classical models in which measurement outputs of non-communicating observers are pre-determined.

- Correlations observed when measuring entangled states may lead to a violation of Bell inequality and, therefore, do not have a classical counterpart.

- If some observed correlations violate a Bell inequality, the outcomes could not have pre-determined in advance ➔ **They are random.**

Conclusions

- Bell inequalities are conditions satisfied by classical models in which measurement outputs of non-communicating observers are pre-determined.

- Correlations observed when measuring entangled states may lead to a violation of Bell inequality and, therefore, do not have a classical counterpart.

- If some observed correlations violate a Bell inequality, the outcomes could not have pre-determined in advance ➔ **They are random.**

- If some observed correlations violate a Bell inequality, they cannot be reproduced classically ➔ **The devices are quantum.**

Conclusions

- Bell inequalities are conditions satisfied by classical models in which measurement outputs of non-communicating observers are pre-determined.

- Correlations observed when measuring entangled states may lead to a violation of Bell inequality and, therefore, do not have a classical counterpart.

- If some observed correlations violate a Bell inequality, the outcomes could not have pre-determined in advance ➔ **They are random.**

- If some observed correlations violate a Bell inequality, they cannot be reproduced classically ➔ **The devices are quantum.**

- A novel type of quantum information theory, known as device-independent quantum information processing, is possible when using quantum Bell nonlocality.

Conclusions

- Bell inequalities are conditions satisfied by classical models in which measurement outputs of non-communicating observers are pre-determined.
- Correlations observed when measuring entangled states may lead to a violation of Bell inequality and, therefore, do not have a classical counterpart.
- If some observed correlations violate a Bell inequality, the outcomes could not have pre-determined in advance ➔ **They are random.**
- If some observed correlations violate a Bell inequality, they cannot be reproduced classically ➔ **The devices are quantum.**
- A novel type of quantum information theory, known as device-independent quantum information processing, is possible when using quantum Bell nonlocality.
- The implementation of device-independent protocols is experimentally challenging, but appears feasible with near-future quantum technologies.