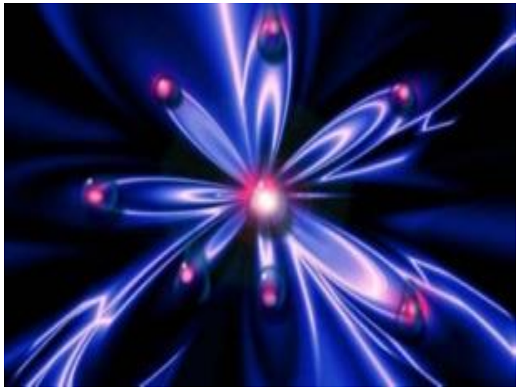
From Bell's theorem to the device-independent quantum information scenario

Antonio Acín
ICREA Professor at ICFO-Institut de Ciencies Fotoniques, Barcelona
AXA Chair in Quantum Information Science

30th IFT Xmas Workshop, Madrid, Spain, 11 December 2024

Quantum information science

What happens when we encode information on quantum particles?

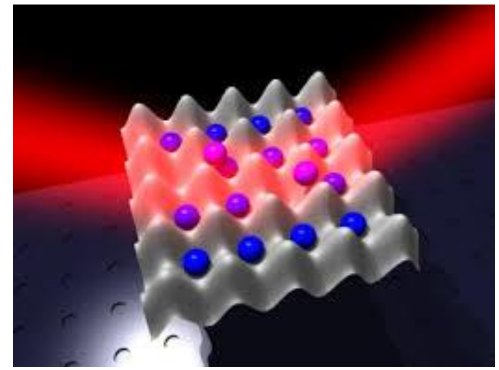


Novel information applications become possible thanks to quantum effects, e.g. more powerful computers and secure cryptography.

Change of paradigm: **physics matters!**

Quantum information technologies

Quantum Computer



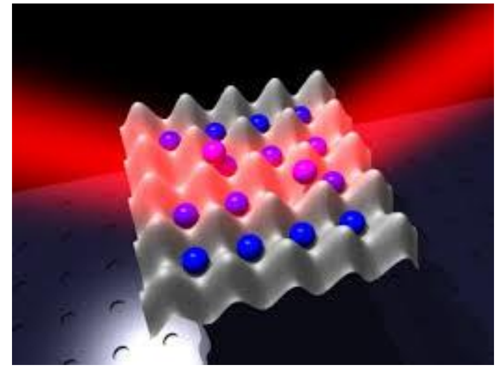
Quantum Simulator

Quantum Cryptography

QRNG

Quantum certification

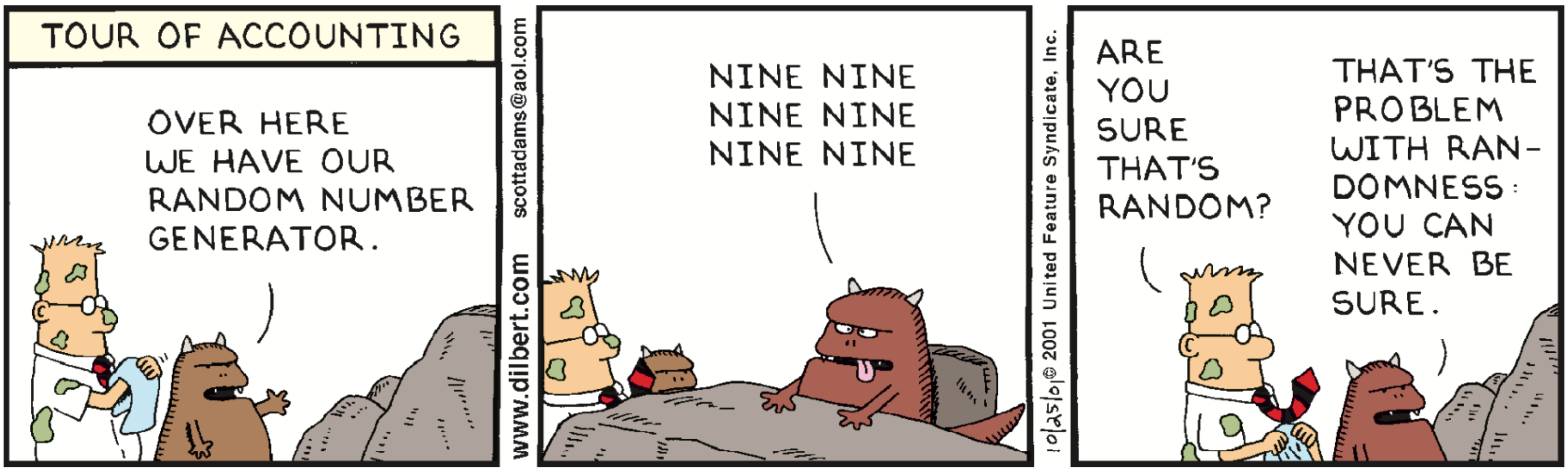
Is this a quantum computer?

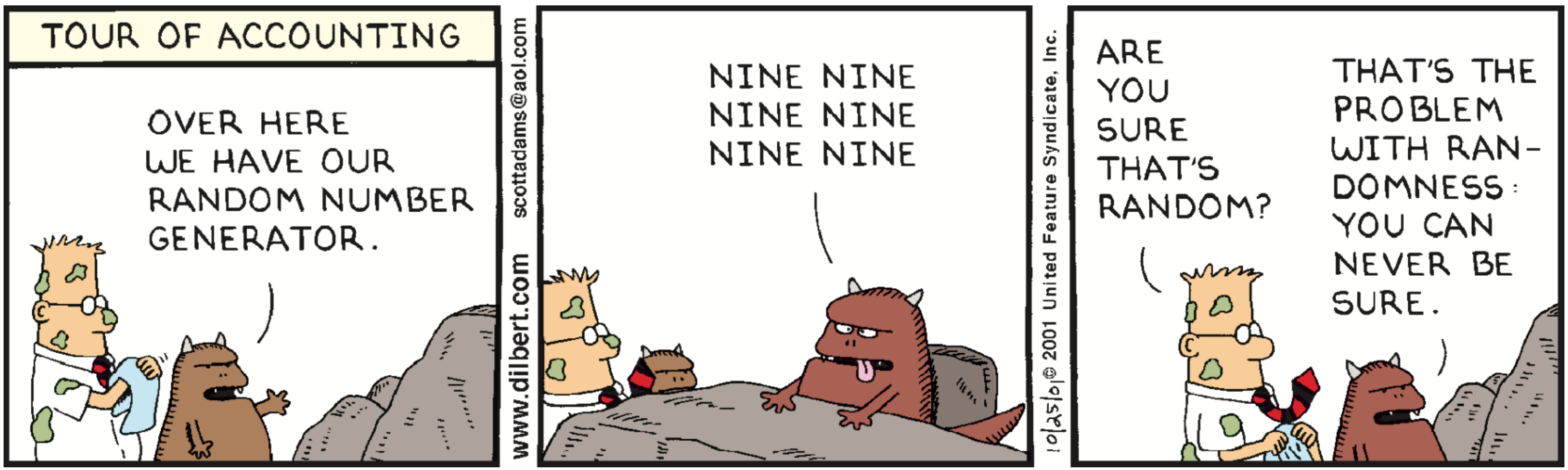


Does this properly simulate
a quantum system?

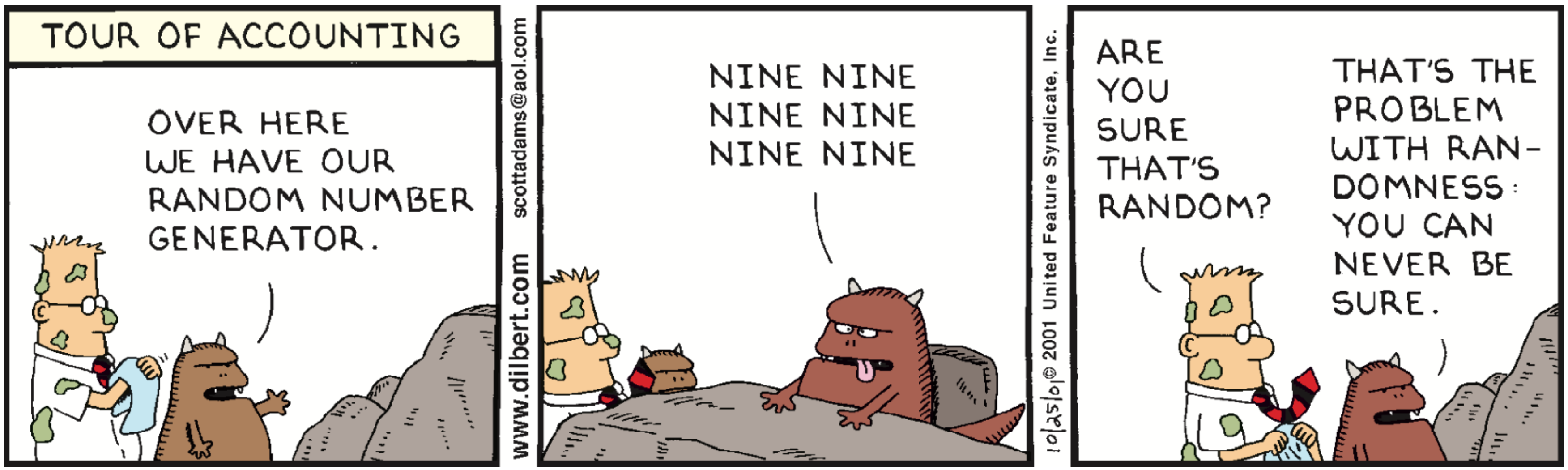
Is this cryptographically secure?

Is this quantum random?


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



Can one certify the presence of (quantum) randomness?



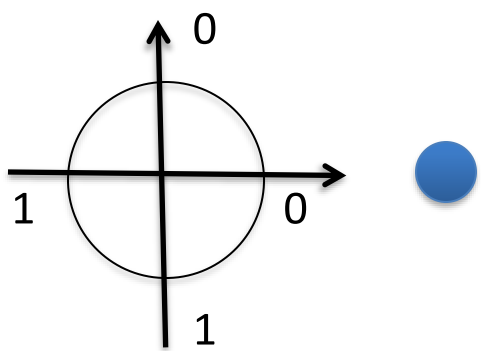
How can one certify a quantum device from its outputs?

Quantum key distribution

Standard schemes: Bennett-Brassard 84 (BB84) protocol

Alice

Bob

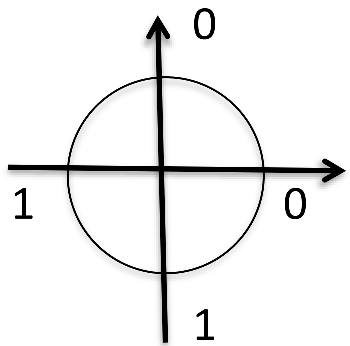


- Alice encodes a random bit into a two-dimensional quantum particle. The basis for encoding is also chosen randomly between x and z. The particle is sent to Bob.

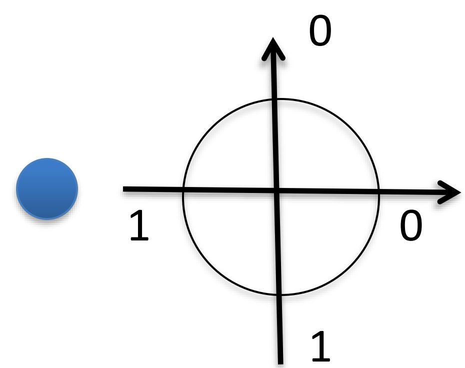
Quantum key distribution

Standard schemes: Bennett-Brassard 84 (BB84) protocol

Alice



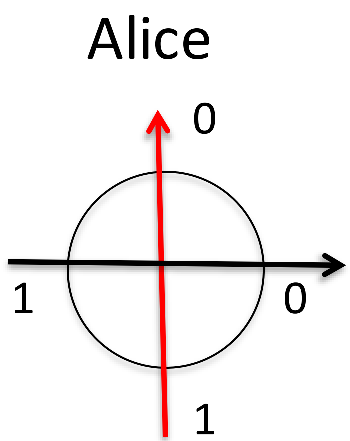
Bob

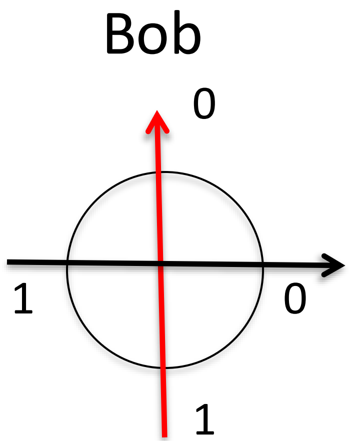


- Alice encodes a random bit into a two-dimensional quantum particle. The basis for encoding is also chosen randomly between x and z. The particle is sent to Bob.
- Bob also chooses randomly in which basis to measure the quantum particle.

Quantum key distribution

Standard schemes: Bennett-Brassard 84 (BB84) protocol





- Alice encodes a random bit into a two-dimensional quantum particle. The basis for encoding is also chosen randomly between x and z. The particle is sent to Bob.
- Bob also chooses randomly in which basis to measure the quantum particle.
- When the bases coincide the results are identical. These cases are kept.

Quantum key distribution

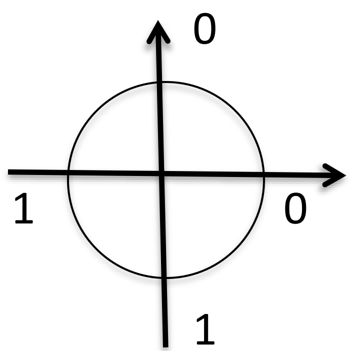
Standard schemes: Bennett-Brassard 84 (BB84) protocol

- Alice encodes a random bit into a two-dimensional quantum particle. The basis for encoding is also chosen randomly between x and z. The particle is sent to Bob.
- Bob also chooses randomly in which basis to measure the quantum particle.
- When the bases coincide the results are identical. These cases are kept.
- When the bases are different, the results are random. These cases are removed.

Quantum key distribution

Standard schemes: Bennett-Brassard 84 (BB84) protocol

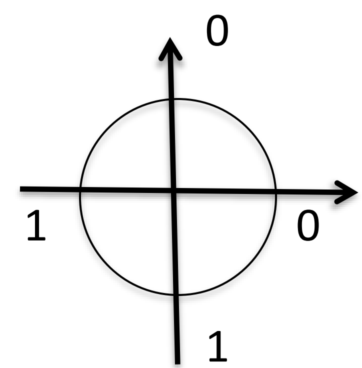
Alice



0
1
1
0
0
0
.
.
.

0
1
1
0
0
0
.
.
.

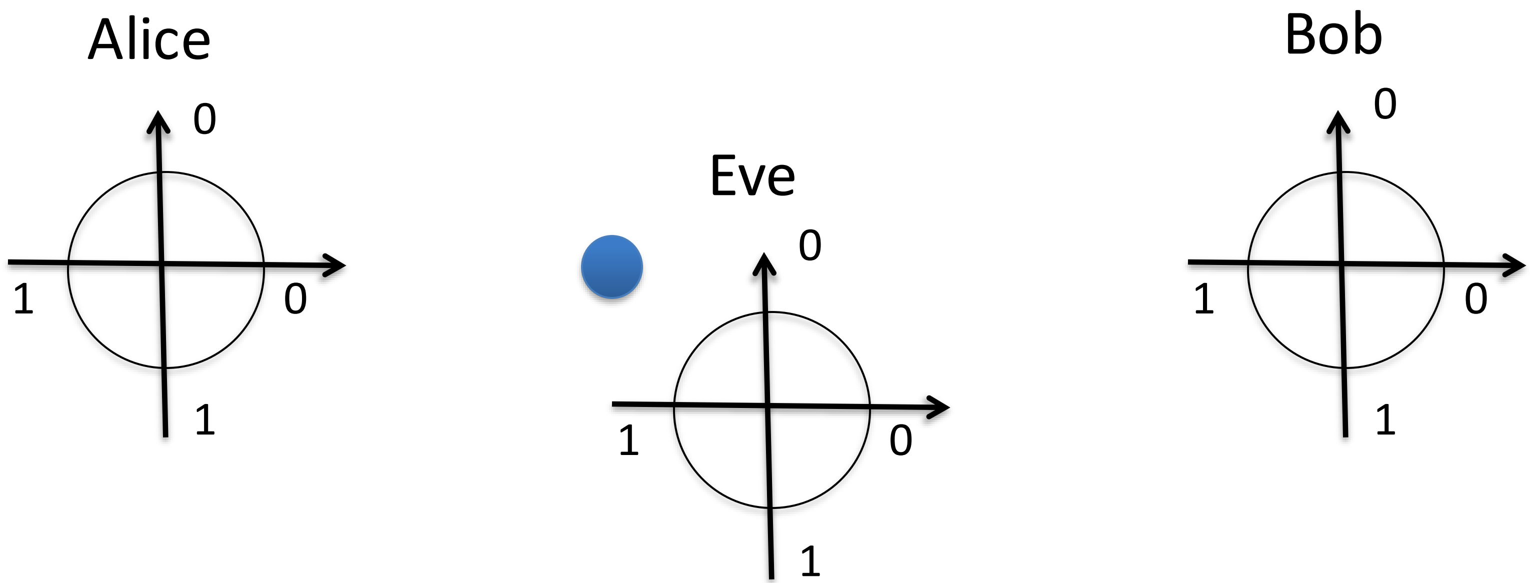
Bob



- Alice encodes a random bit into a two-dimensional quantum particle. The basis for encoding is also chosen randomly between x and z. The particle is sent to Bob.
- Bob also chooses randomly in which basis to measure the quantum particle.
- When the bases coincide the results are identical. These cases are kept.
- When the bases are different, the results are random. These cases are removed.
- At the end, of the process, Alice and Bob share a list of perfectly correlated and random bits ➔ **a secret key**!

Quantum key distribution

Standard schemes: Bennett-Brassard 84 (BB84) protocol



Eve intercepts the quantum particles while they travel through the channel.
However, she does not know in which basis to measure!
Heisenberg uncertainty principle: impossible to perform two non-commuting measurements.

Quantum key distribution

- Quantum key distribution protocols are based on **physical security**.
- Assumption: quantum theory offers a correct physical description of the devices.
- No assumption is required on the eavesdropper's power, provided it does not contradict any quantum law.
- Using this (these) assumption(s), the security of the schemes can be proven, that is, one can construct a **security proof**.

Quantum hacking

NATURE PHOTONICS | LETTER

Hacking commercial quantum cryptography systems by tailored bright illumination

Lars Lydersen, Carlos Wiechers, Christoffer Wittmann, Dominique Elser, Johannes Skaar & Vadim Makarov

Published online 29 August 2010 | Nature | doi:10.1038/news.2010.436

News

Hackers blind quantum cryptographers

Lasers crack commercial encryption systems, leaving no trace.

Zeeya Merali

Quantum hacking

NATURE PHOTONICS | LETTER

Hacking commercial quantum cryptography systems by tailored bright illumination

Lars Lydersen, Carlos Wiechers, Christoffer Wittmann, Dominique Elser, Johannes Skaar & Vadim Makarov

Published online 29 August 2010 | Nature | doi:10.1038/news.2010.436

News

Hackers blind quantum cryptographers

Lasers crack commercial encryption systems, leaving no trace.

Zeeya Merali

How come?!

Quantum hacking

Quantum hacking attacks break the implementation, not the principle.

Quantum hacking

Quantum hacking attacks break the implementation, not the principle.

Theory

- Prepare states in a Hilbert space of dimension two.
- Measure observables in the same space, e.g. spin-1/2 measurements.

Quantum hacking

Quantum hacking attacks break the implementation, not the principle.

Theory

- Prepare states in a Hilbert space of dimension two.
- Measure observables in the same space, e.g. spin-1/2 measurements.

Implementation

- Prepare states using an attenuated laser source.
- Measure polarization of light using single-photon detectors.

Quantum hacking

Quantum hacking attacks break the implementation, not the principle.

Theoretical security proof

- Prepare states in a Hilbert space of dimension two.
- Measure observables in the same space, e.g. spin-1/2 measurements.

Implementation

- Prepare states using an attenuated laser source.
- Measure polarization of light using single-photon detectors.

Quantum hacking

Quantum hacking attacks break the implementation, not the principle.

Theoretical security proof

- Prepare states in a Hilbert space of dimension two.
- Measure observables in the same space, e.g. spin-1/2 measurements.

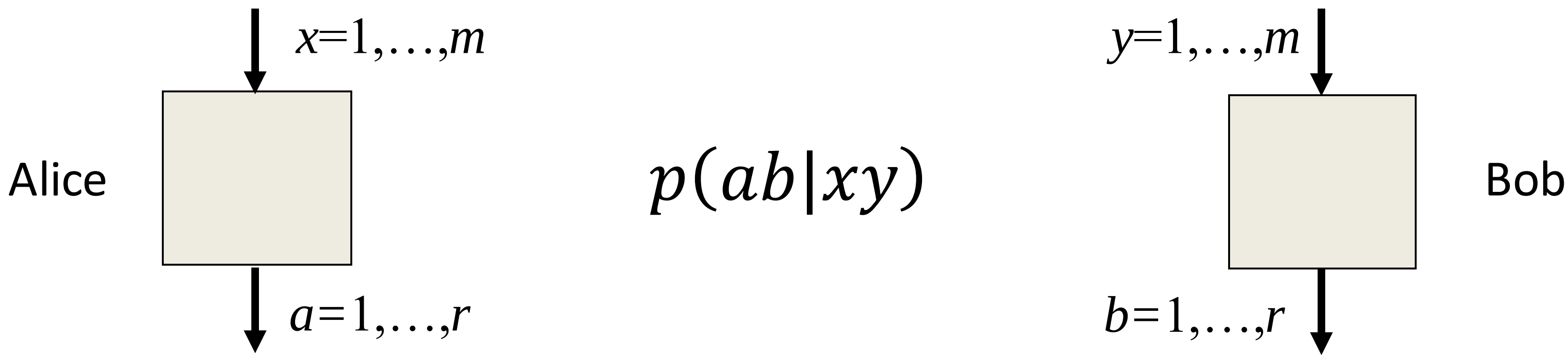
Implementation

- Prepare states using an attenuated laser source.
- Measure polarization of light using single-photon detectors.

Moral: the unavoidable mismatch between theoretical requirements and implementation is an important weakness in quantum information protocols, especially in adversarial scenarios. Physical details become a weakness!

A solution to the hacking problem

Device-Independent Quantum Key Distribution

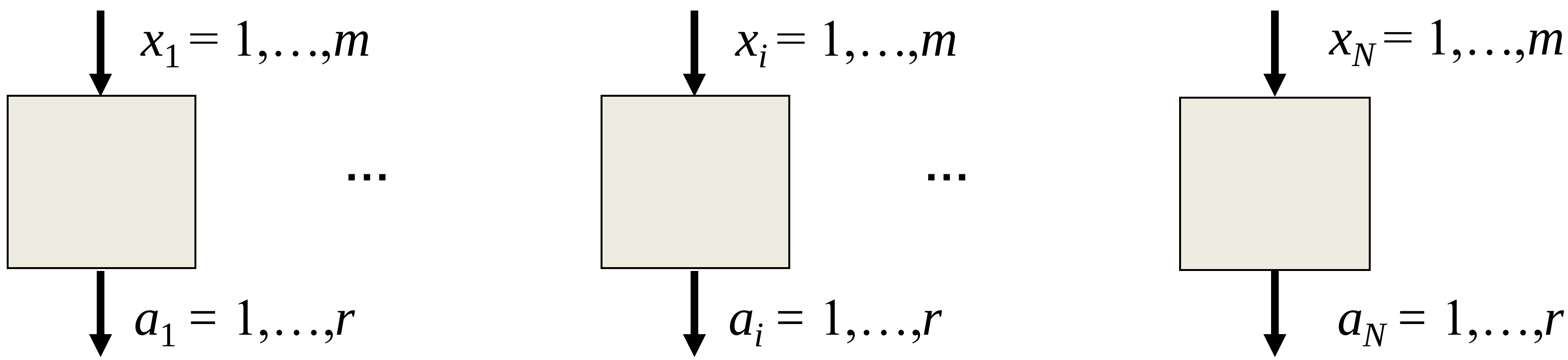


Protocols that establish a secure key only from the observed statistics and without making any assumption about the internal working of the devices used to obtain it.

A. Acín *et al.*, Phys. Rev. Lett. 98, 230501 (2007)

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**.

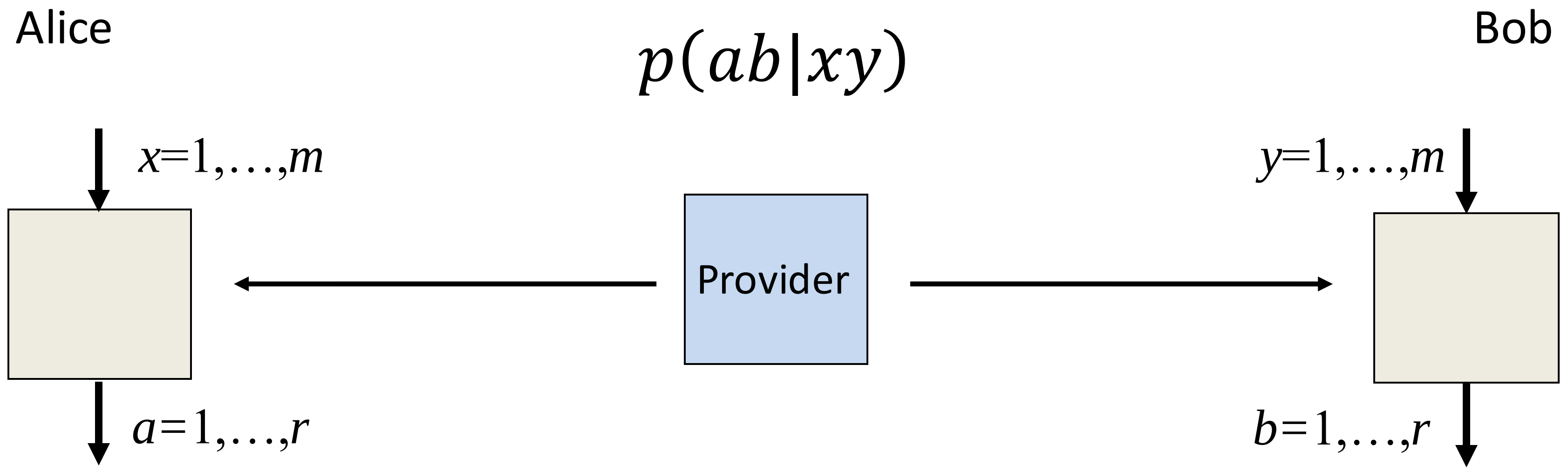


Observed statistics

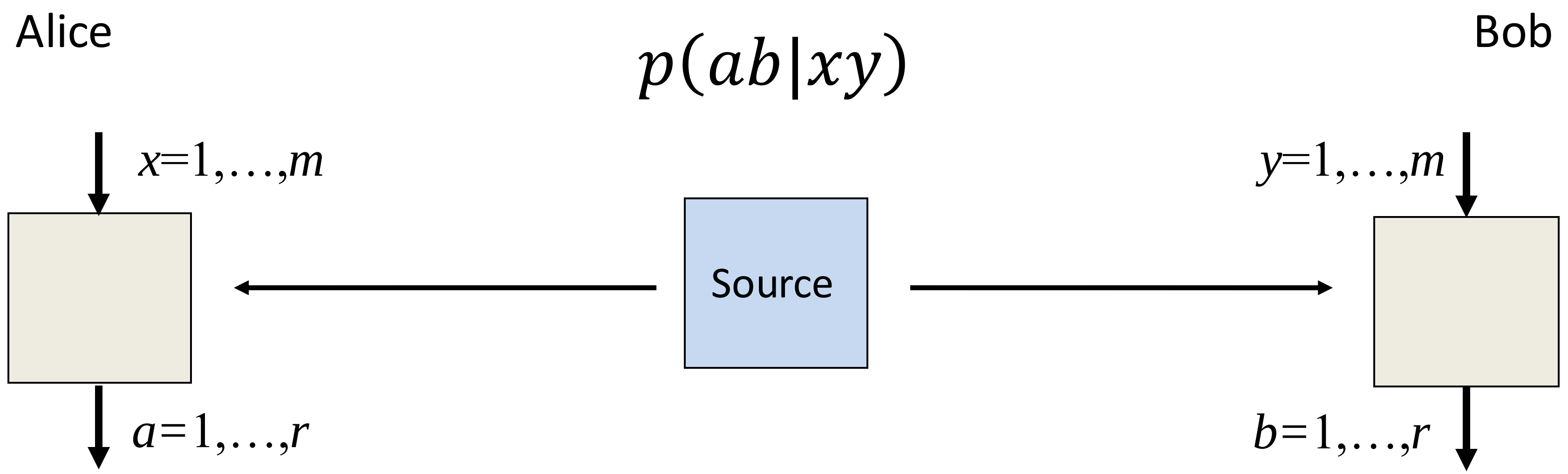
$$p(a_1 \ldots a_N | x_1 \ldots x_N)$$

Why is this possible?

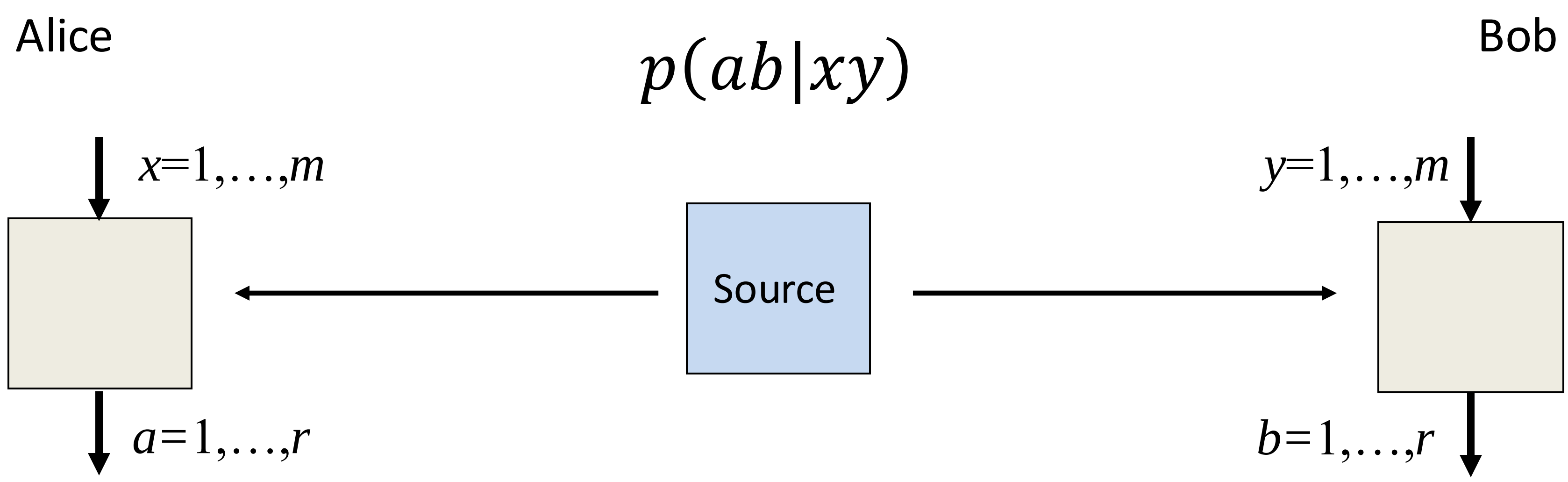
From certification to Bell's theorem



From certification to Bell's theorem

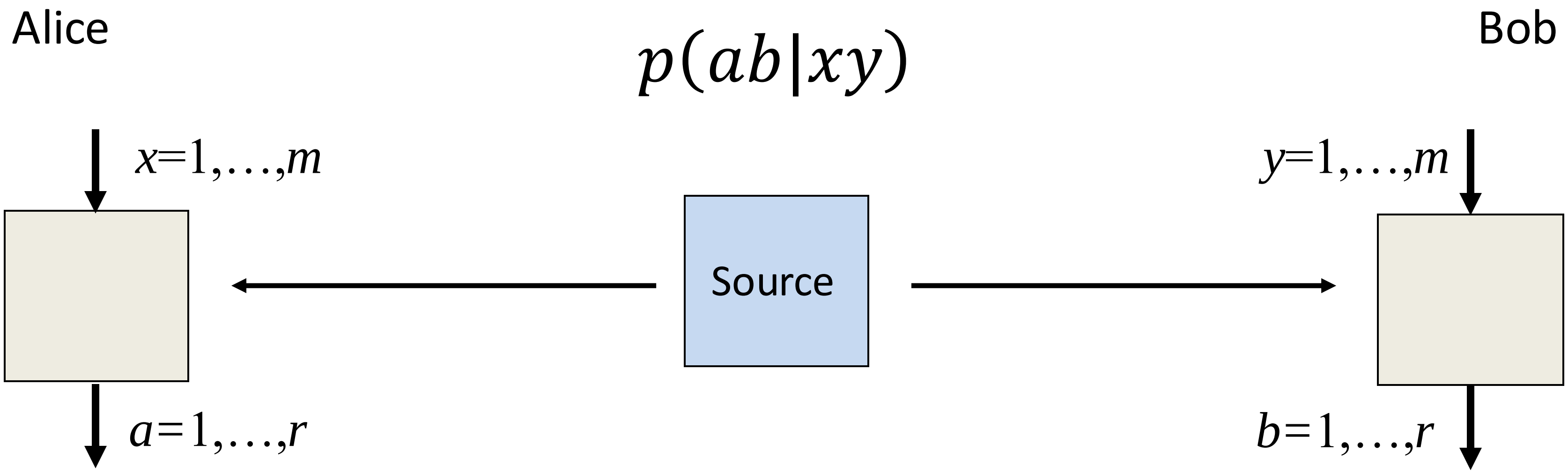


From certification to Bell's theorem



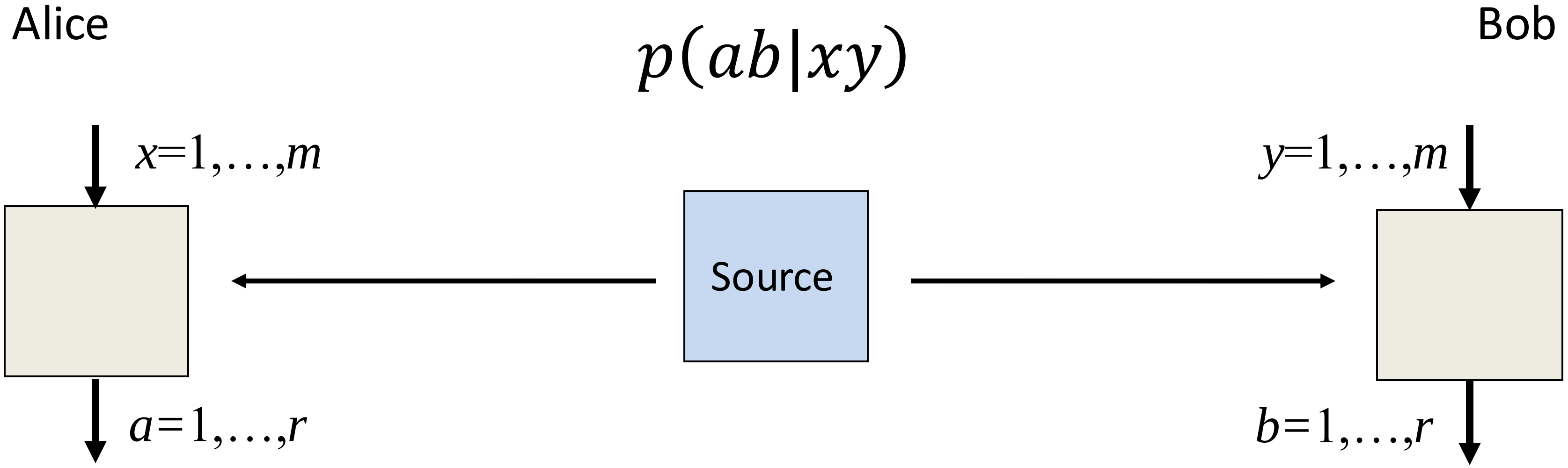
This is nothing but a Bell test, in which local measurements are performed on two separated systems, prepared by the source.

One of the main lessons of Bell's 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's theorem

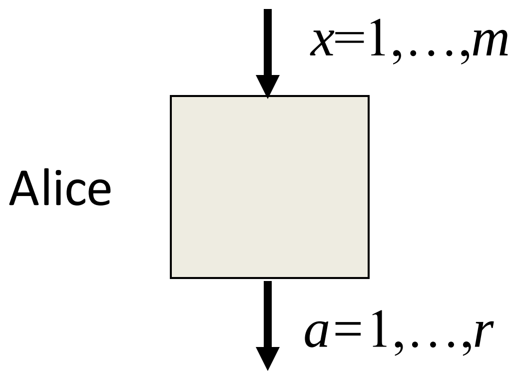


The statistics of an experiment, a.k.a. correlations, depends on the physical properties of the measured systems.

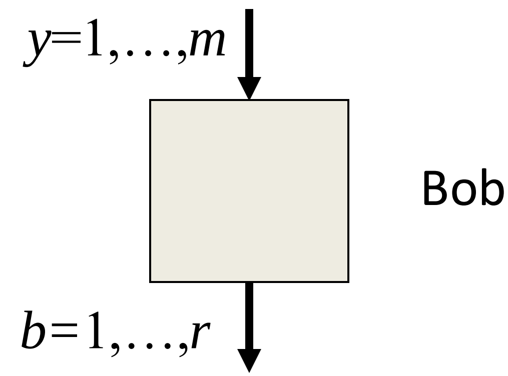
Physical principles impose limits on correlations.

Physical correlations

The object we deal with is a conditional probability distribution of the outputs given the inputs, which encapsulates the correlations among devices.

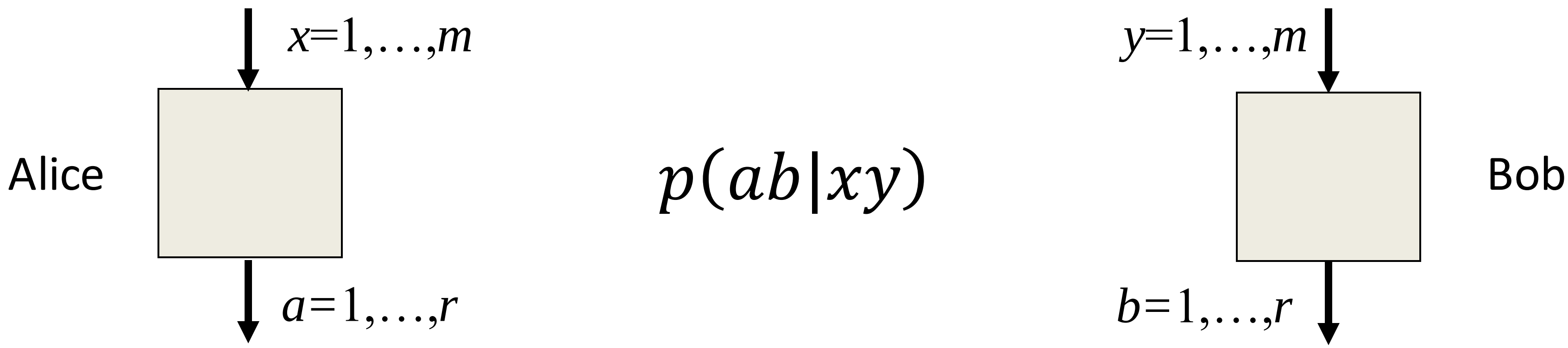


$$p(ab|xy)$$



Physical correlations

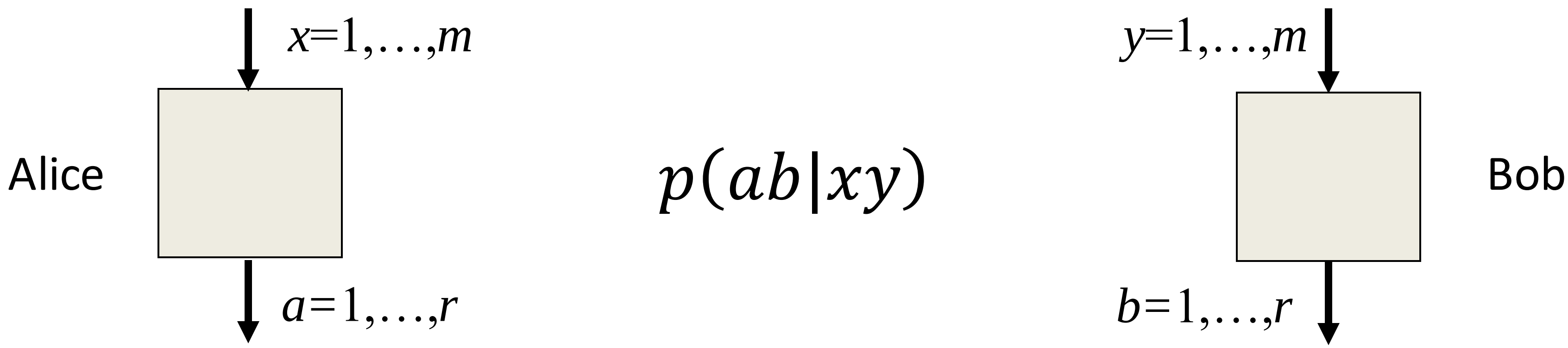
The object we deal with is a conditional probability distribution of the outputs given the inputs, which encapsulates the correlations among devices.



$$p(ab|xy) = \begin{pmatrix} p(1,1|1,1) & p(2,1|1,1) & \cdots & p(r,r|1,1) \\ & & & \\ & & & \end{pmatrix}$$

Physical correlations

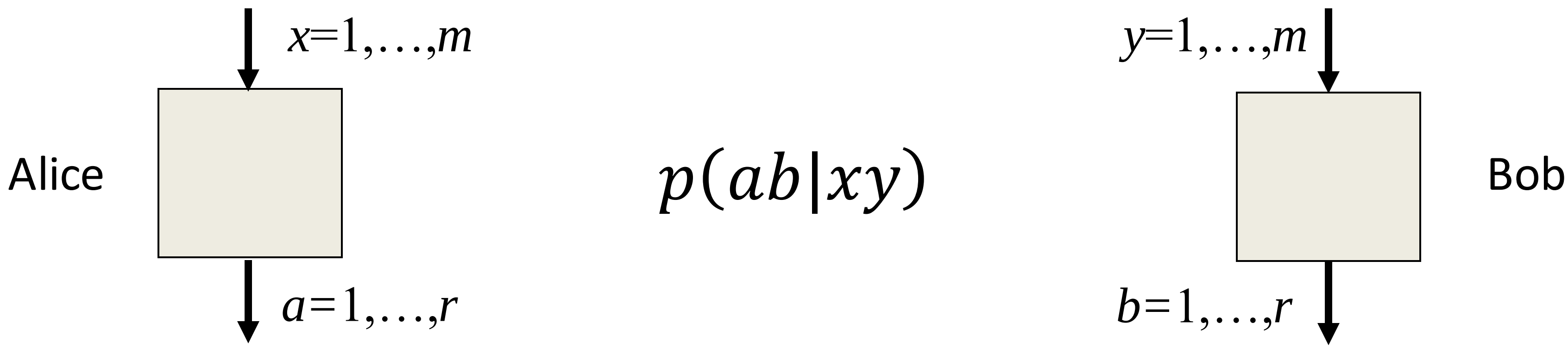
The object we deal with is a conditional probability distribution of the outputs given the inputs, which encapsulates the correlations among devices.



$$p(ab|xy) = \begin{pmatrix} \underbrace{p(1,1|1,1) \quad p(2,1|1,1) \quad \cdots \quad p(r,r|1,1)}_{\displaystyle\sum_{ab} p(ab|1,1) = 1} \end{pmatrix}$$

Physical correlations

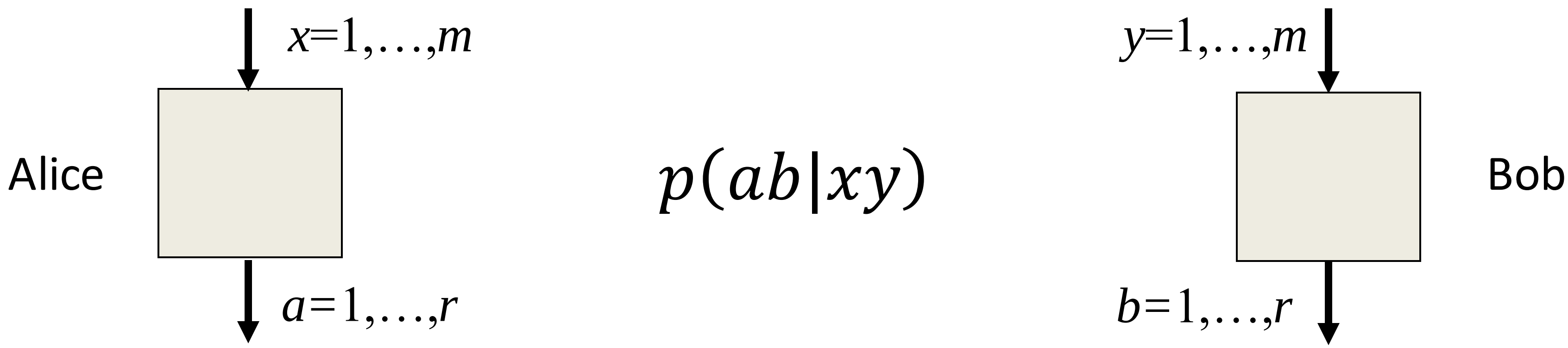
The object we deal with is a conditional probability distribution of the outputs given the inputs, which encapsulates the correlations among devices.



$$p(ab|xy) = \begin{pmatrix} p(1{,}1|1{,}1) & p(2,1|1{,}1) & \cdots & p(r,r|1{,}1) \\ \underbrace{p(1{,}1|2{,}1) \quad p(2{,}1|2{,}1) \quad \cdots \quad p(r,r|2{,}1)}_{\sum_{ab} p(ab|2{,}1)\, =\, 1} & & & \end{pmatrix}$$

Physical correlations

The object we deal with is a conditional probability distribution of the outputs given the inputs, which encapsulates the correlations among devices.

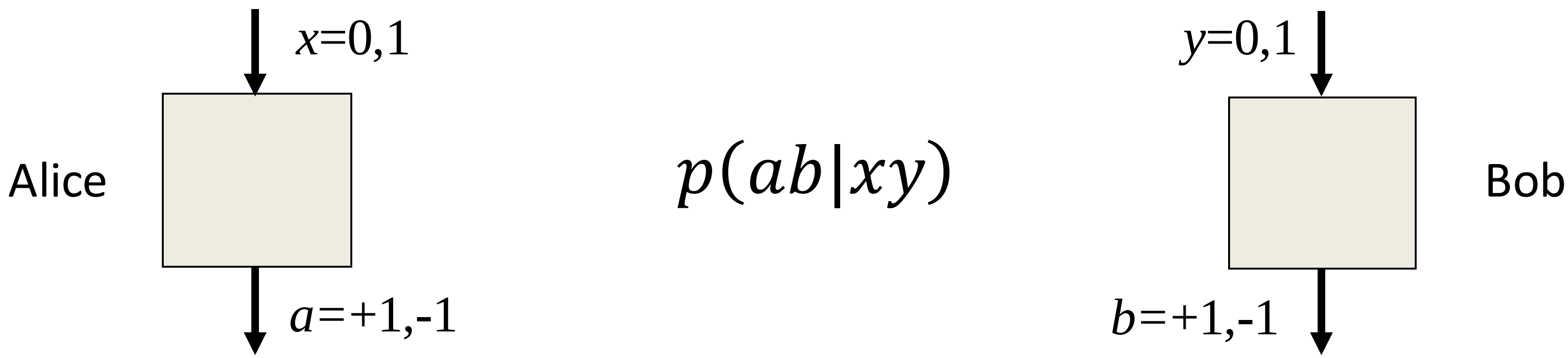


$$p(ab|xy) = \begin{pmatrix} p(1,1|1,1) & p(2,1|1,1) & \cdots & p(r,r|1,1) \\ p(1,1|2,1) & p(2,1|2,1) & \cdots & p(r,r|2,1) \\ \vdots & \vdots & \ddots & \vdots \\ p(1,1|m,m) & p(2,1|m,m) & \cdots & p(r,r|m,m) \end{pmatrix}$$

$$p(ab|xy) \geq 0, \sum_{ab} p(ab|1,1) = 1$$

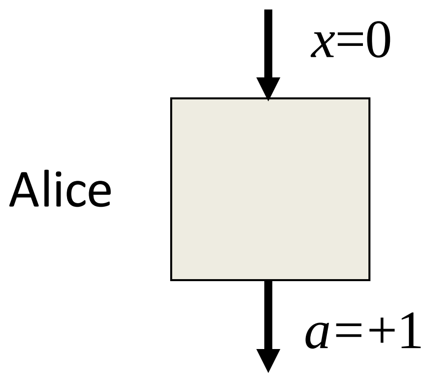
Example

Example

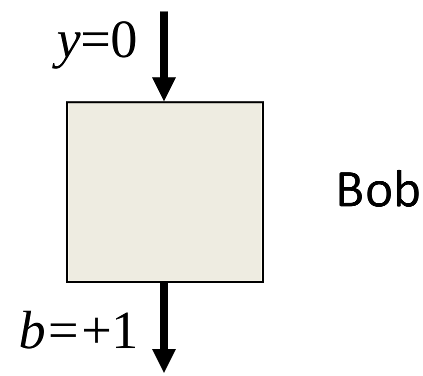


$$p(ab|xy) = \begin{pmatrix} p(+1,+1|0,0) & p(+1,-1|0,0) & p(-1,+1|0,0) & p(-1,-1|0,0) \\ p(+1,+1|0,1) & p(+1,-1|0,1) & p(-1,+1|0,1) & p(-1,-1|0,1) \\ p(+1,+1|1,0) & p(+1,-1|1,0) & p(-1,+1|1,0) & p(-1,-1|1,0) \\ p(+1,+1|1,1) & p(+1,-1|1,1) & p(-1,+1|1,1) & p(-1,-1|1,1) \end{pmatrix}$$

Example

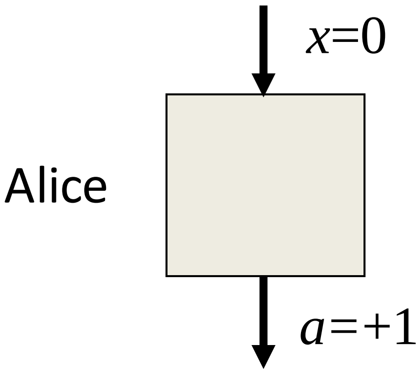


$$p(+1,+1|0,0) = \frac{1}{2}$$

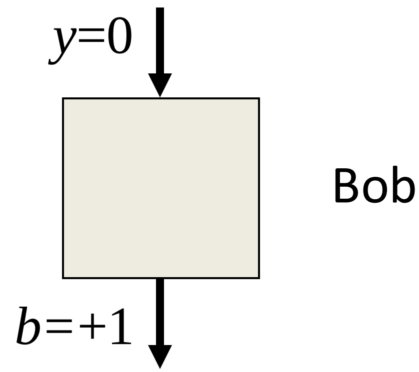


$$p(ab|xy) = \begin{pmatrix} p(+1,+1|0,0) & p(+1,-1|0,0) & p(-1,+1|0,0) & p(-1,-1|0,0) \\ p(+1,+1|0,1) & p(+1,-1|0,1) & p(-1,+1|0,1) & p(-1,-1|0,1) \\ p(+1,+1|1,0) & p(+1,-1|1,0) & p(-1,+1|1,0) & p(-1,-1|1,0) \\ p(+1,+1|1,1) & p(+1,-1|1,1) & p(-1,+1|1,1) & p(-1,-1|1,1) \end{pmatrix}$$

Example

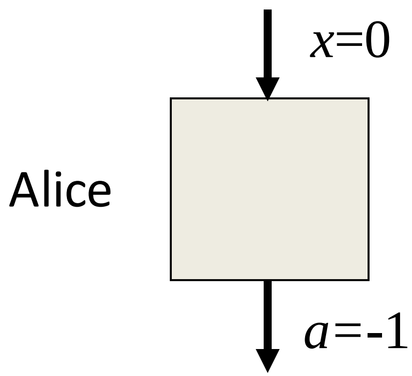


$$p(+1,+1|0,0) = \frac{1}{2}$$

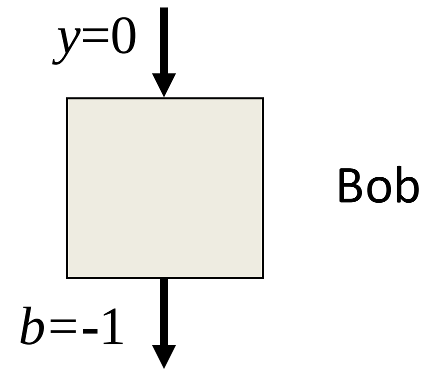


$$p(ab|xy) = \begin{pmatrix} 1/2 & p(+1,-1|0,0) & p(-1,+1|0,0) & p(-1,-1|0,0) \\ p(+1,+1|0,1) & p(+1,-1|0,1) & p(-1,+1|0,1) & p(-1,-1|0,1) \\ p(+1,+1|1,0) & p(+1,-1|1,0) & p(-1,+1|1,0) & p(-1,-1|1,0) \\ p(+1,+1|1,1) & p(+1,-1|1,1) & p(-1,+1|1,1) & p(-1,-1|1,1) \end{pmatrix}$$

Example

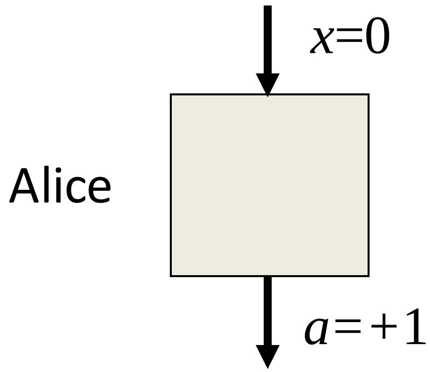


$$p(-1,-1|0{,}0)=\frac{1}{2}$$

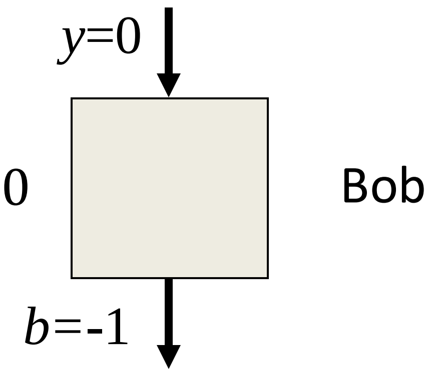


$$p(ab|xy)=\begin{pmatrix} 1/2 & p(+1,-1|0{,}0) & p(-1,+1|0{,}0) & 1/2 \\ p(+1,+1|0{,}1) & p(+1,-1|0{,}1) & p(-1,+1|0{,}1) & p(-1,-1|0{,}1) \\ p(+1,+1|1{,}0) & p(+1,-1|1{,}0) & p(-1,+1|1{,}0) & p(-1,-1|1{,}0) \\ p(+1,+1|1{,}1) & p(+1,-1|1{,}1) & p(-1,+1|1{,}1) & p(-1,-1|1{,}1) \end{pmatrix}$$

Example



$$p(+1,-1|0,0) = p(-1,+1|0,0) = 0$$



$$p(ab|xy) = \begin{pmatrix} 1/2 & 0 & 0 & 1/2 \\ p(+1,+1|0,1) & p(+1,-1|0,1) & p(-1,+1|0,1) & p(-1,-1|0,1) \\ p(+1,+1|1,0) & p(+1,-1|1,0) & p(-1,+1|1,0) & p(-1,-1|1,0) \\ p(+1,+1|1,1) & p(+1,-1|1,1) & p(-1,+1|1,1) & p(-1,-1|1,1) \end{pmatrix}$$

Example

$$p(ab|xy) = \begin{pmatrix} 1/2 & 0 & 0 & 1/2 \\ 1/2 & 0 & 0 & 1/2 \\ p(+1,+1|1,0) & p(+1,-1|1,0) & p(-1,+1|1,0) & p(-1,-1|1,0) \\ p(+1,+1|1,1) & p(+1,-1|1,1) & p(-1,+1|1,1) & p(-1,-1|1,1) \end{pmatrix}$$

Example

$$p(ab|xy) = \begin{pmatrix} 1/2 & 0 & 0 & 1/2 \\ 1/2 & 0 & 0 & 1/2 \\ 1/2 & 0 & 0 & 1/2 \\ p(+1,+1|1,1) & p(+1,-1|1,1) & p(-1,+1|1,1) & p(-1,-1|1,1) \end{pmatrix}$$

Example

$$p(ab|xy) = \begin{pmatrix} 1/2 & 0 & 0 & 1/2 \\ 1/2 & 0 & 0 & 1/2 \\ 1/2 & 0 & 0 & 1/2 \\ 0 & 1/2 & 1/2 & 0 \end{pmatrix}$$

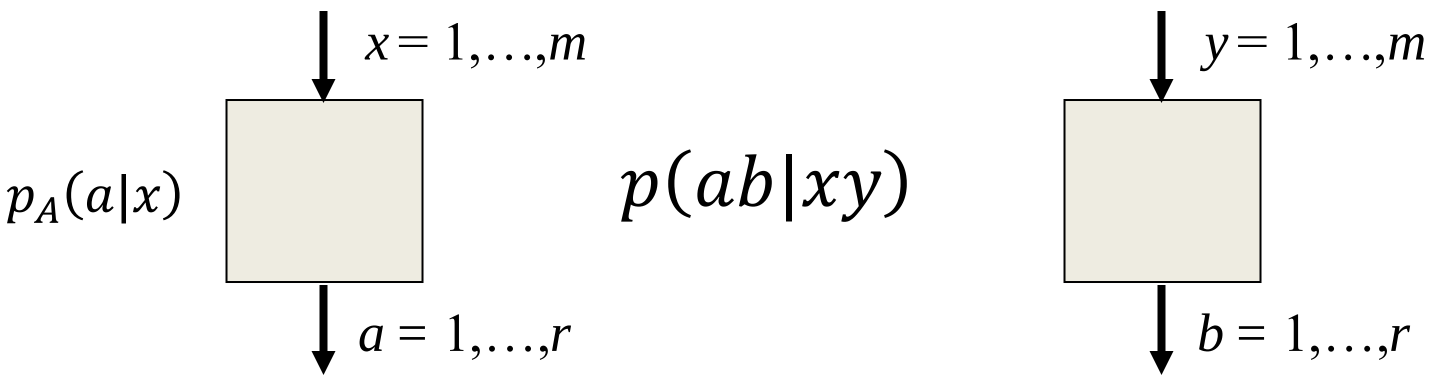
Physical correlations

Physical principles impose limits on correlations.

Physical correlations

Physical principles impose limits on correlations.

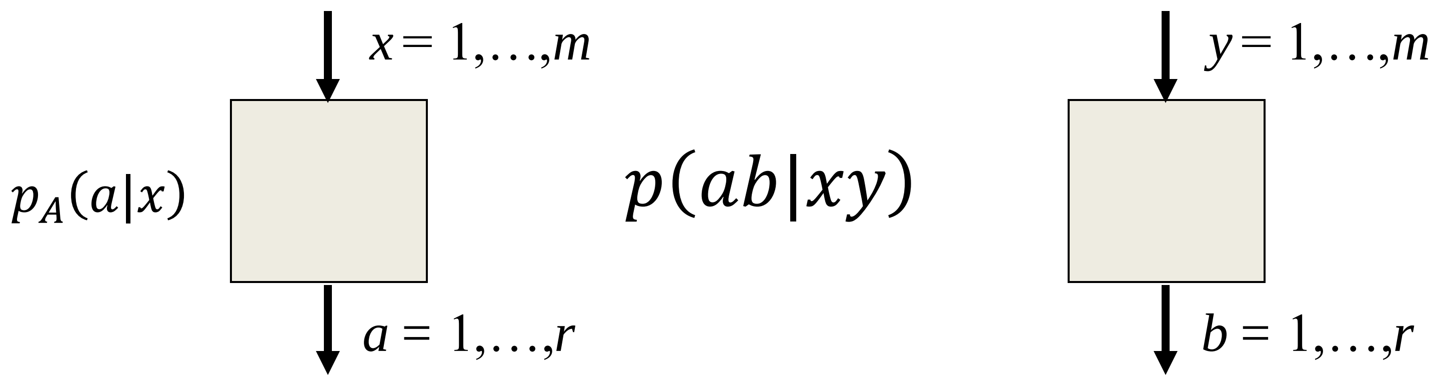
No-signalling correlations: correlations compatible with the no-signalling principle, i.e. the impossibility of instantaneous communication.



Physical correlations

Physical principles impose limits on correlations.

No-signalling correlations: correlations compatible with the no-signalling principle, i.e. the impossibility of instantaneous communication.

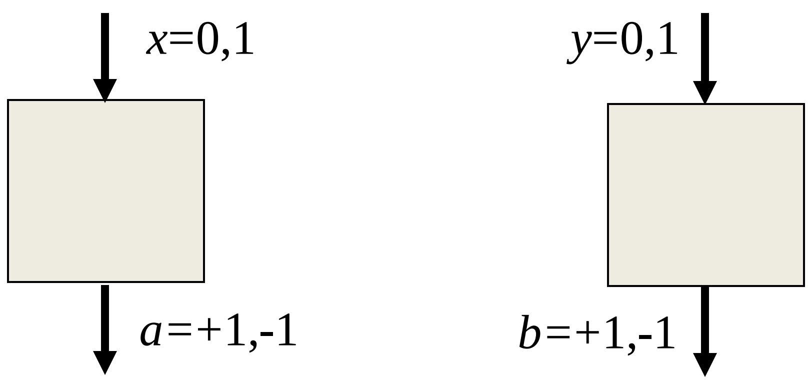


$$\sum_{a_{k+1}\ldots a_N} p(a_1 \ldots a_N | x_1 \ldots x_N) = p(a_1 \ldots a_k | x_1 \ldots x_k)$$

Physical correlations

No-signalling correlations: correlations compatible with the no-signalling principle, i.e. the impossibility of instantaneous communication.

$$\sum_{a_{k+1}\dots a_N} p(a_1 \dots a_N | x_1 \dots x_N) = p(a_1 \dots a_k | x_1 \dots x_k)$$

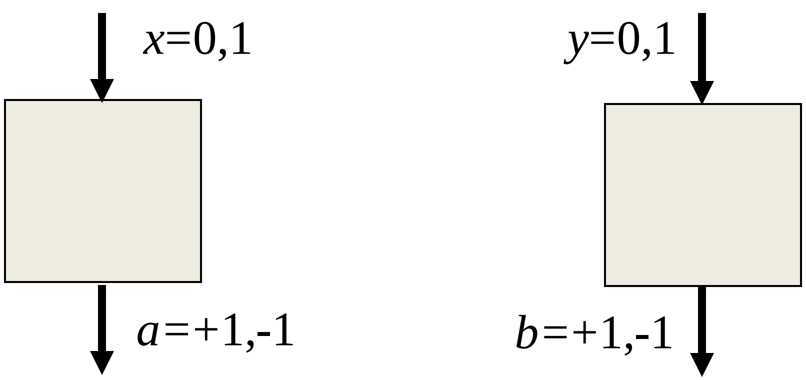


$$\begin{array}{c} \\ 00 \\ 01 \\ 10 \\ 11 \end{array}
\begin{array}{c} \begin{array}{cccc} ++ & +- & -+ & -- \end{array} \\ \begin{pmatrix} 1/2 & 0 & 0 & 1/2 \\ 1/2 & 0 & 0 & 1/2 \\ 1/2 & 0 & 0 & 1/2 \\ 0 & 1/2 & 1/2 & 0 \end{pmatrix} \end{array}$$

Physical correlations

No-signalling correlations: correlations compatible with the no-signalling principle, i.e. the impossibility of instantaneous communication.

$$\sum_{a_{k+1}\dots a_N} p(a_1 \dots a_N | x_1 \dots x_N) = p(a_1 \dots a_k | x_1 \dots x_k)$$



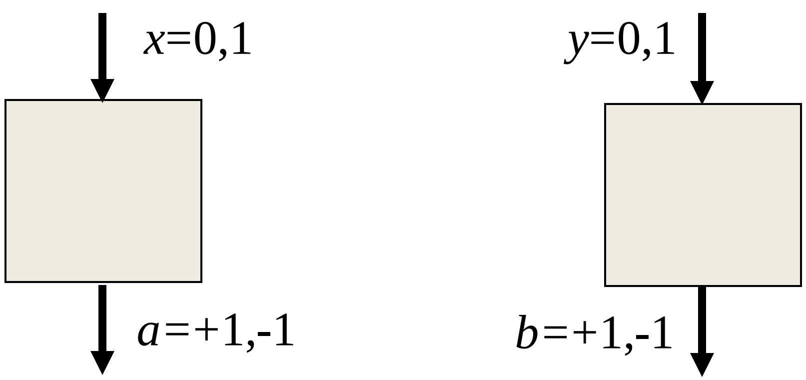
$$\begin{array}{c c} & \begin{array}{cccc} ++ & +- & -+ & -- \end{array} \\ \begin{array}{c} 00 \\ 01 \\ 10 \\ 11 \end{array} & \begin{pmatrix} 1/2 & 0 & 0 & 1/2 \\ 1/2 & 0 & 0 & 1/2 \\ 1/2 & 0 & 0 & 1/2 \\ 0 & 1/2 & 1/2 & 0 \end{pmatrix} \end{array}$$

$$p_A(+1|0) = p(+1,+1|00) + p(+1,-1|00) = \frac{1}{2}$$

Physical correlations

No-signalling correlations: correlations compatible with the no-signalling principle, i.e. the impossibility of instantaneous communication.

$$\sum_{a_{k+1}\dots a_N} p(a_1 \dots a_N | x_1 \dots x_N) = p(a_1 \dots a_k | x_1 \dots x_k)$$



$$\begin{array}{c} \\ 00 \\ 01 \\ 10 \\ 11 \end{array} \begin{array}{c} \begin{array}{cccc} ++ & +- & -+ & -- \end{array} \\ \begin{pmatrix} 1/2 & 0 & 0 & 1/2 \\ 1/2 & 0 & 0 & 1/2 \\ 1/2 & 0 & 0 & 1/2 \\ 0 & 1/2 & 1/2 & 0 \end{pmatrix} \end{array}$$

$$p_A(+1|0) = p(+1,+1|00) + p(+1,-1|00) = \frac{1}{2} = p(+1,+1|01) + p(+1,-1|01)$$

Physical correlations

Classical correlations: deterministic processes at each place determine the output given the input and what comes from the source.

$$p(ab|xy) = \sum_{\lambda} p(\lambda) D_A(a|x,\lambda) D_B(b|y,\lambda)$$

These are the standard "EPR" correlations. Independently of fundamental issues, these are the correlations achievable by classical means. Bell inequalities define the limits on these correlations.

Physical correlations

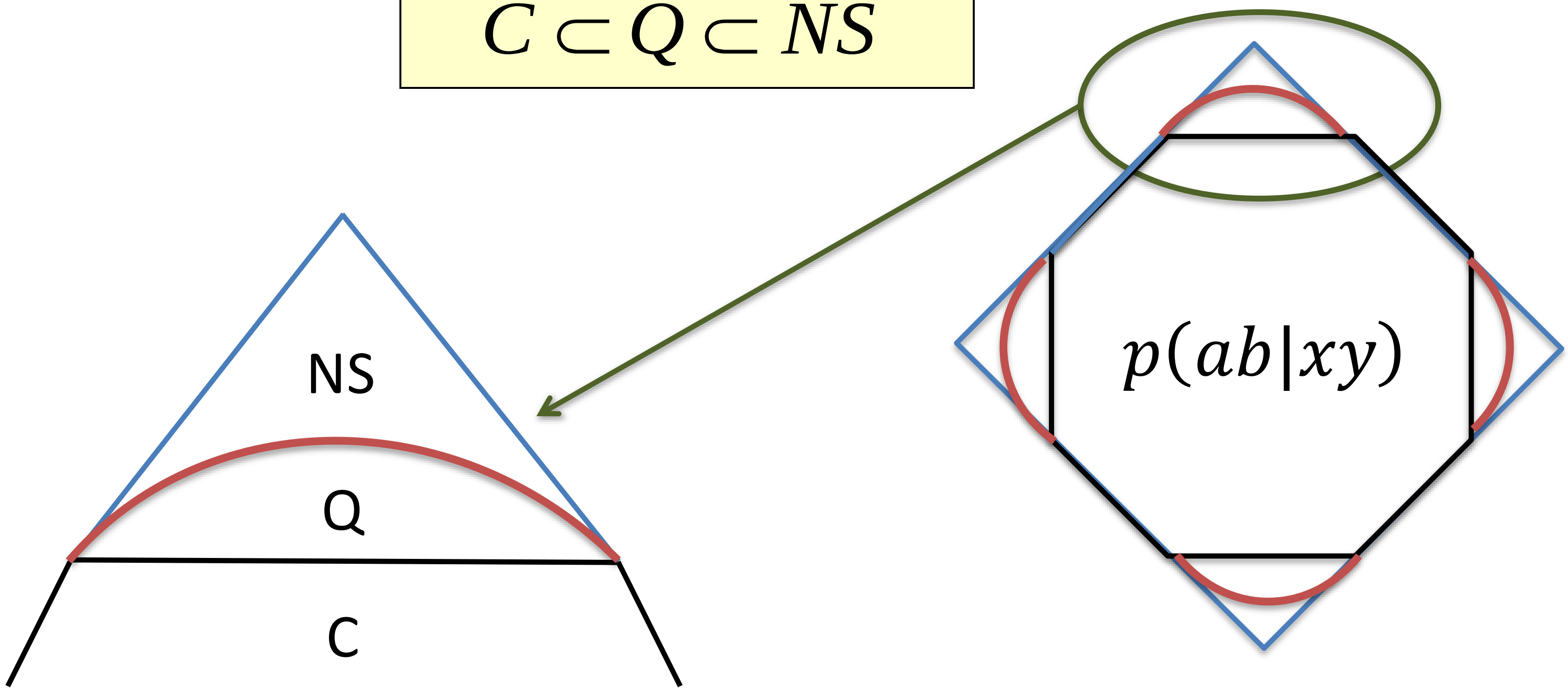
Quantum correlations: local measurements on a shared quantum state.

$$p(ab|xy) = \langle\psi|\Pi_{a|x} \otimes \Pi_{b|y}|\psi\rangle$$

Everything is expressed in terms of operators (the quantum state and the measurement projectors) acting on a Hilbert space. However, it can be any Hilbert space, of arbitrary dimension.

Physical correlations

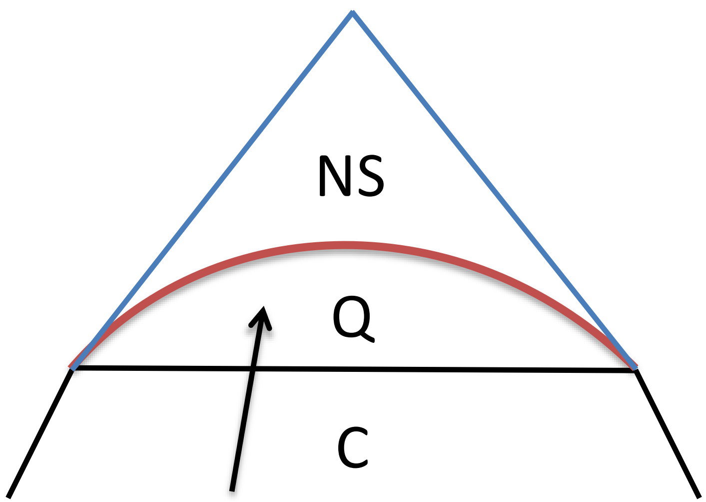
$$C \subset Q \subset NS$$



Physical correlations

Bell

$$\boxed{C \subset Q \subset NS}$$



There exist correlations that cannot be explained by classical models. These (quantum) correlations are known as **non-local** and they are detected by the violation of a Bell inequality.

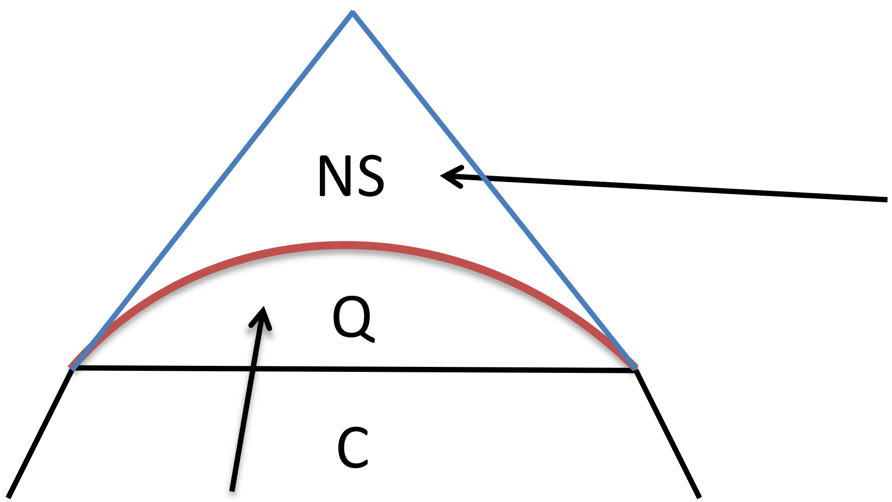
Physical correlations

Bell

$$\boxed{C \subset Q \subset NS}$$

Tsirelson

Popescu-Rohrlich

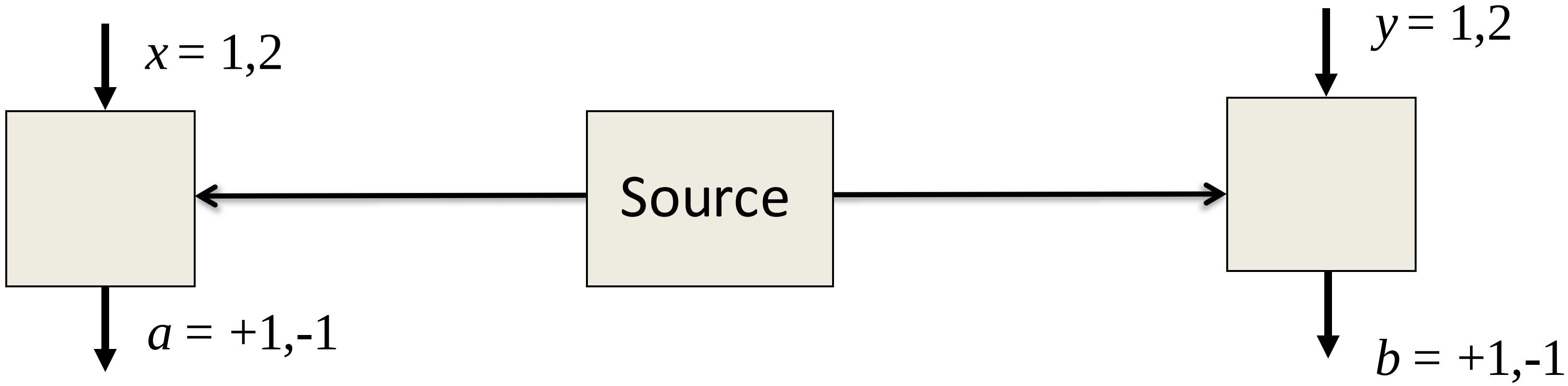


There exist correlations that are compatible with the no-signalling principle but cannot be obtained by performing local measurements on a quantum state.

There exist correlations that cannot be explained by classical models. These (quantum) correlations are known as **non-local** and they are detected by the violation of a Bell inequality.

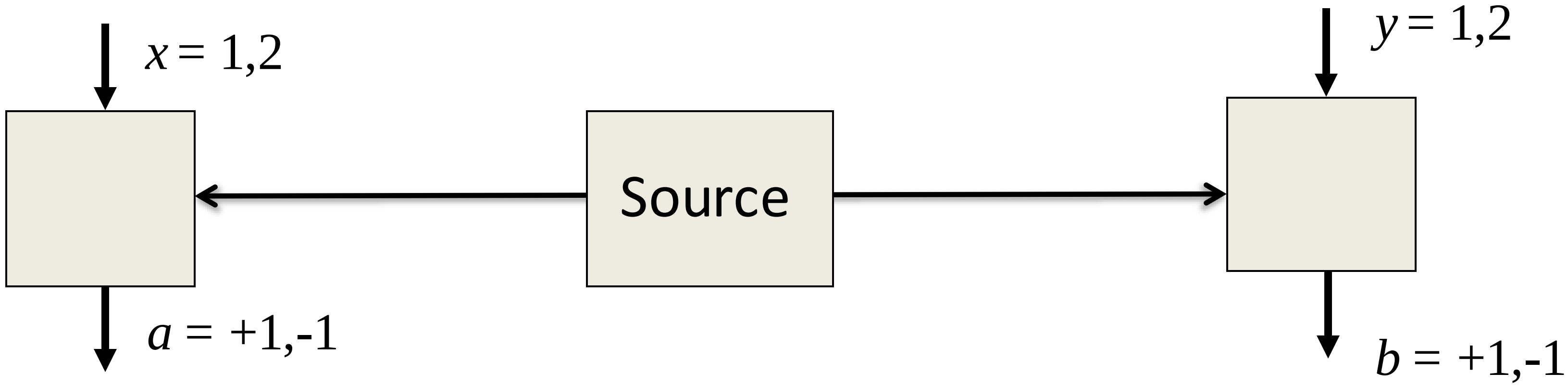
A crash course on Bell inequalities

Example: CHSH Bell inequality



$$CHSH = A_1B_1 + A_1B_2 + A_2B_1 - A_2B_2$$

Example: CHSH Bell inequality



$$CHSH = A_1B_1 + A_1B_2 + A_2B_1 - A_2B_2$$

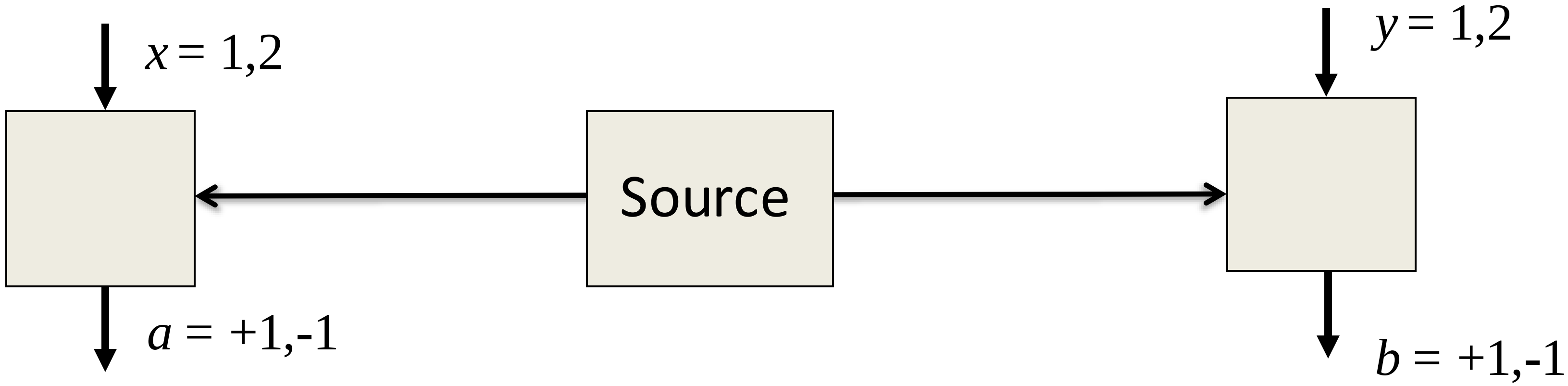
In classical physics, observables have well-defined values, now +1 or -1.

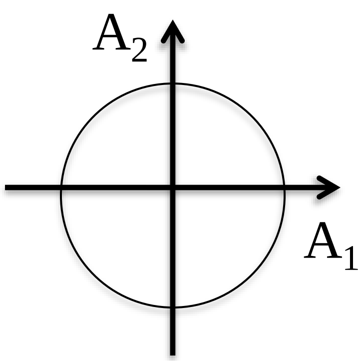
Under this assumption: $CHSH \leq 2$

Example: $A_1 = A_2 = B_1 = B_2 = +1 \rightarrow CHSH = +2.$

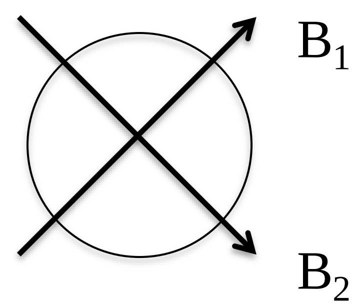
So, the expectation value of this quantity also satisfies $\langle CHSH \rangle \leq 2$

Quantum Bell inequality violation



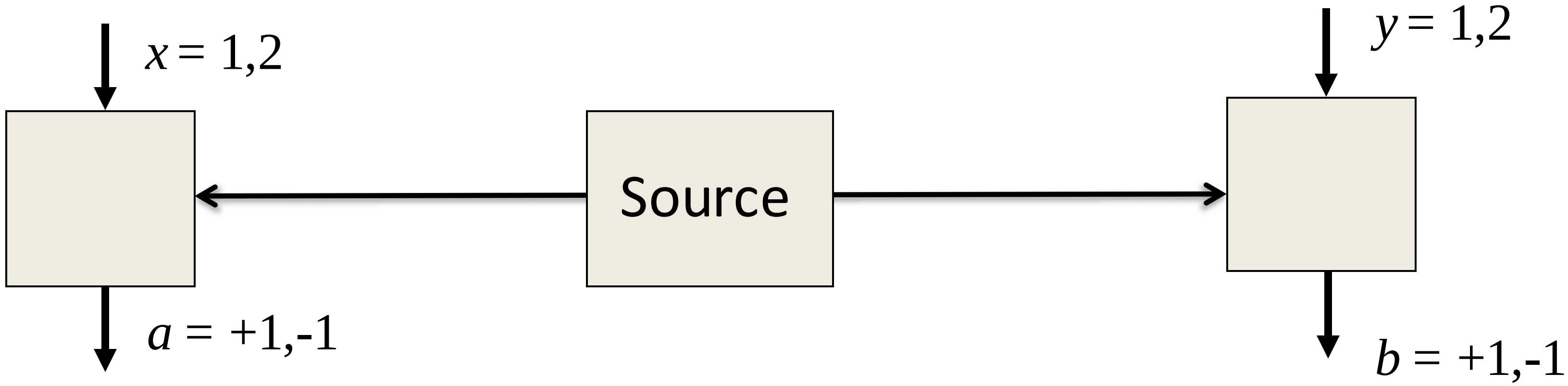


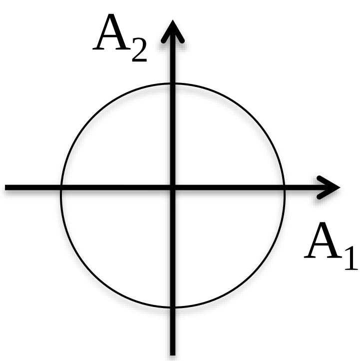
$$|\Phi^{+}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$



Classical values are now replaced by operators.

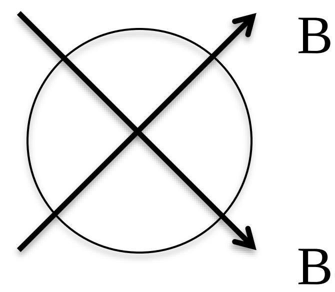
Quantum Bell inequality violation





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

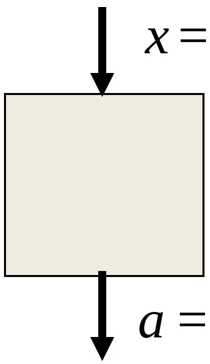
Classical values are now replaced by operators.



$$\langle CHSH \rangle = \langle A_1 \otimes B_1 \rangle_{\Phi^+} + \langle A_1 \otimes B_2 \rangle_{\Phi^+} + \langle A_2 \otimes B_1 \rangle_{\Phi^+} - \langle A_2 \otimes B_2 \rangle_{\Phi^+} = \mathbf{2\sqrt{2} > 2\ !!}$$

Example: CHSH scenario

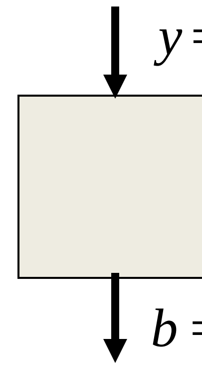
$x = 1,2$



$a = +1,-1$

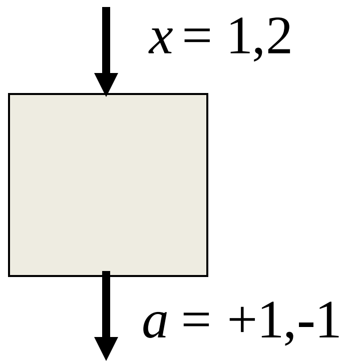
$$CHSH = A_1B_1 + A_1B_2 + A_2B_1 - A_2B_2$$

$y = 1,2$

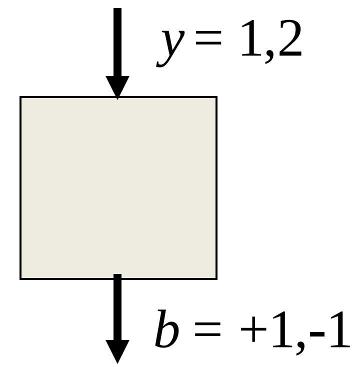


$b = +1,-1$

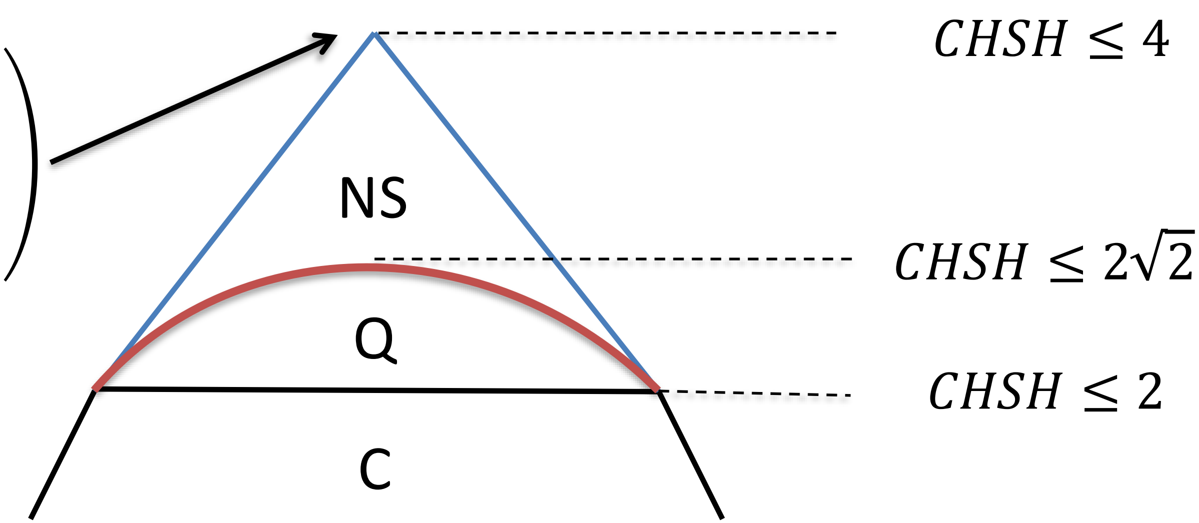
Example: CHSH scenario



$$CHSH = A_1B_1 + A_1B_2 + A_2B_1 - A_2B_2$$



$$\begin{pmatrix} 1/2 & 0 & 0 & 1/2 \\ 1/2 & 0 & 0 & 1/2 \\ 1/2 & 0 & 0 & 1/2 \\ 0 & 1/2 & 1/2 & 0 \end{pmatrix}$$



Characterization of Quantum Correlations

Navascués, Pironio, Acin, PRL 2007, NJP 2009

Characterizing quantum correlations

Given $p(a,b|x,y)$, does it have a quantum realization?

$$p\left(a,b|x,y\right) = \langle \Psi | M_a^x \otimes M_b^y | \Psi \rangle$$

$$\sum_a M_a^x = 1$$

$$M_a^x M_{a'}^x = \delta_{a'a} M_a^x$$

Example:

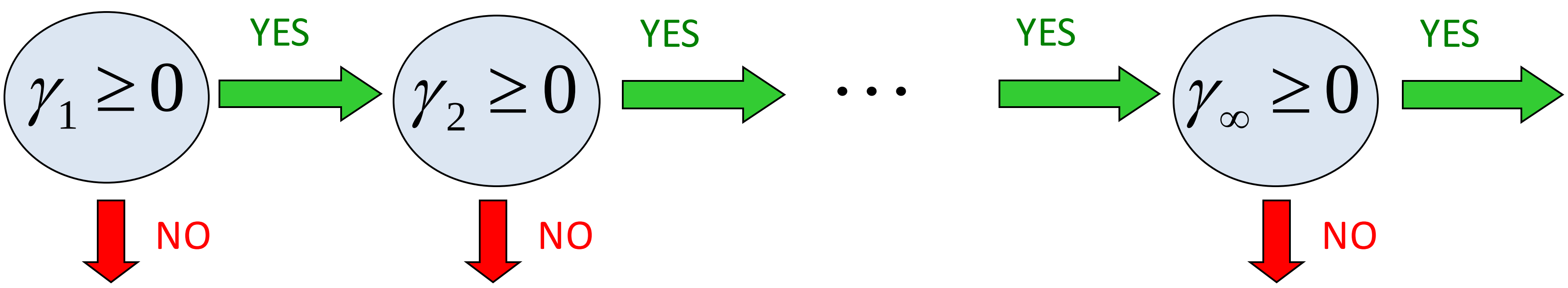
$$p\left(a,b|0,0\right) = p\left(a,b|0,1\right) = p\left(a,b|1,0\right) = \frac{1}{8}\left(2+\sqrt{3},2-\sqrt{3},2-\sqrt{3},2+\sqrt{3}\right)$$

$$p\left(a,b|1,1\right) = \left(0.245,0.255,0.255,0.245\right)$$

Previous work by Tsirelson

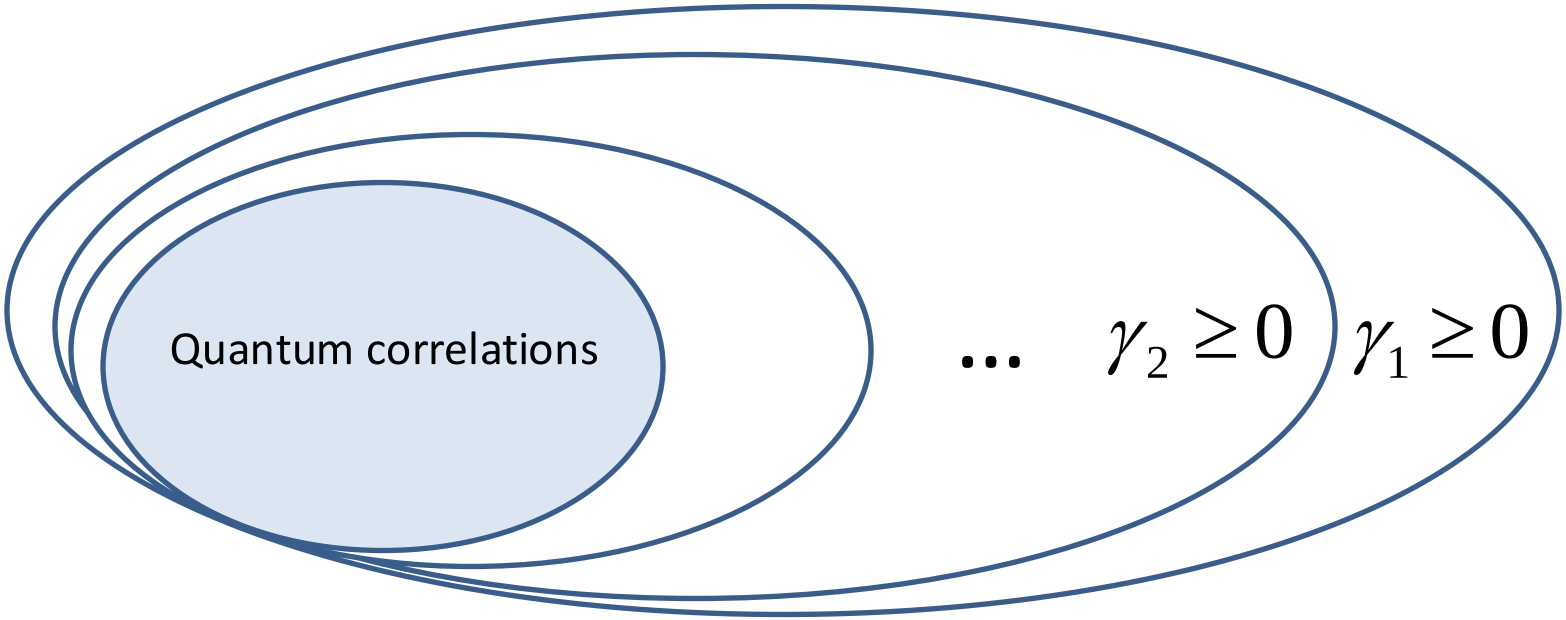
NPA hierarchy

Given a probability distribution $p(a,b|x,y)$, we have defined a hierarchy consisting of a series of tests based on semi-definite programming techniques allowing the detection of supra-quantum correlations.



The hierarchy is asymptotically convergent.

NPA hierarchy



Every step in the hierarchy defines a convex set that is included in the previous step. Convergence is provably attained asymptotically.

In many situations convergence is attained after a few steps. But there is evidence that there may be situations that require an infinite number of steps.

Characterizing quantum correlations

Example:

$$p(a,b|0,0) = p(a,b|0,1) = p(a,b|1,0) = \frac{1}{8}\left(2+\sqrt{3},2-\sqrt{3},2-\sqrt{3},2+\sqrt{3}\right)$$

$$p(a,b|1,1) = (0.245,0.255,0.255,0.245)$$

Solution: it is not quantum, that is, there exists no quantum state of two particles and local measurements acting on them that produce these correlations.

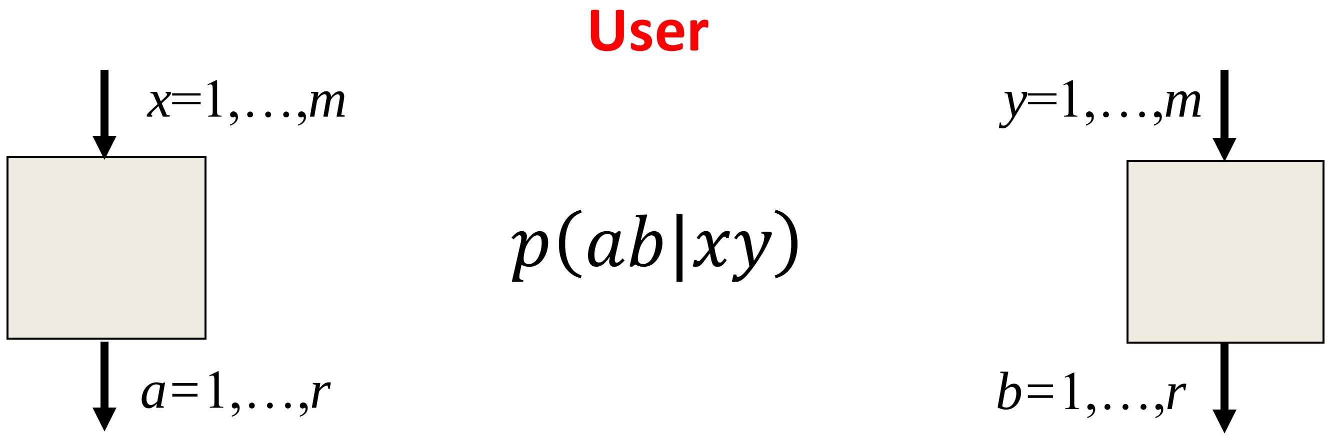
The experimental observation of these correlations would imply the failure of quantum physics, as Bell violations did for classical physics.

Protocols for Device-Independent Randomness Generation

R. Colbeck, PhD Thesis, arXiv:0911.3814
S. Pironio *et al.*, Nature 464, 1021 (2010)
R. Colbeck and A. Kent, J. Phys. A: Math. Th. 44, 095305 (2011)

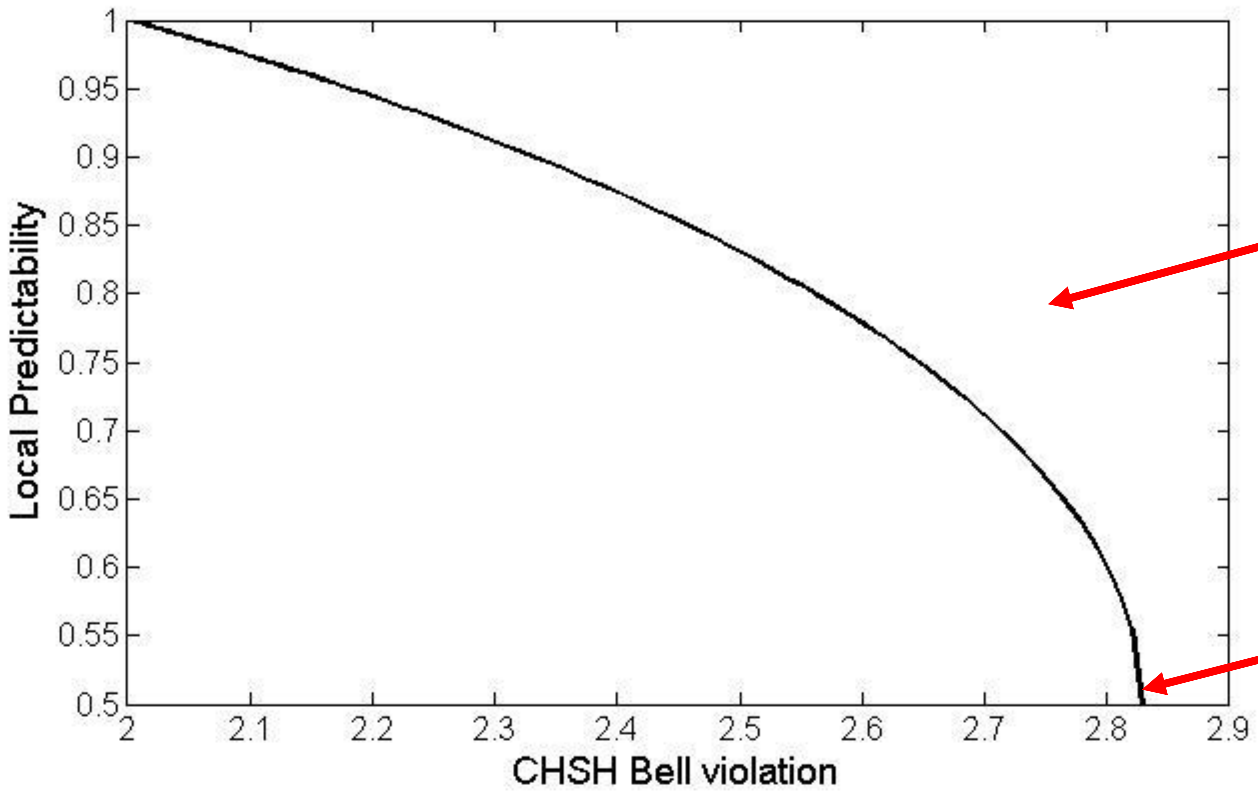
Bell-certified quantum randomness

The outcomes of a Bell experiment cannot be predicted in advance.



It is possible to bound the randomness of the outputs from the Bell inequality violation, which is a function only of the observed statistics.

Bell-certified quantum randomness



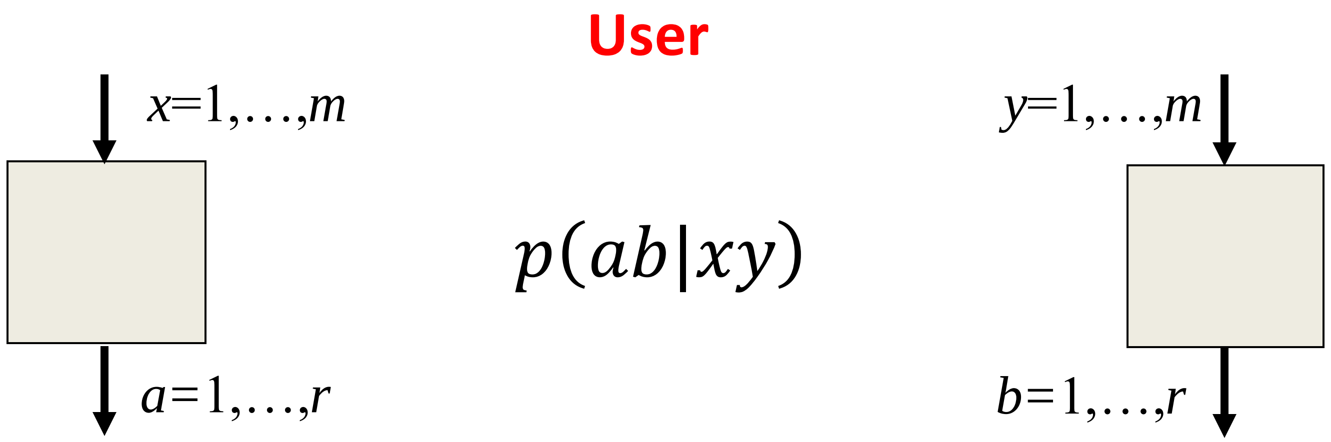
All the region above the curve is impossible within Quantum Mechanics.

One pure random bit.

S. Pironio *et al.*, Nature 464, 1021 (2010)

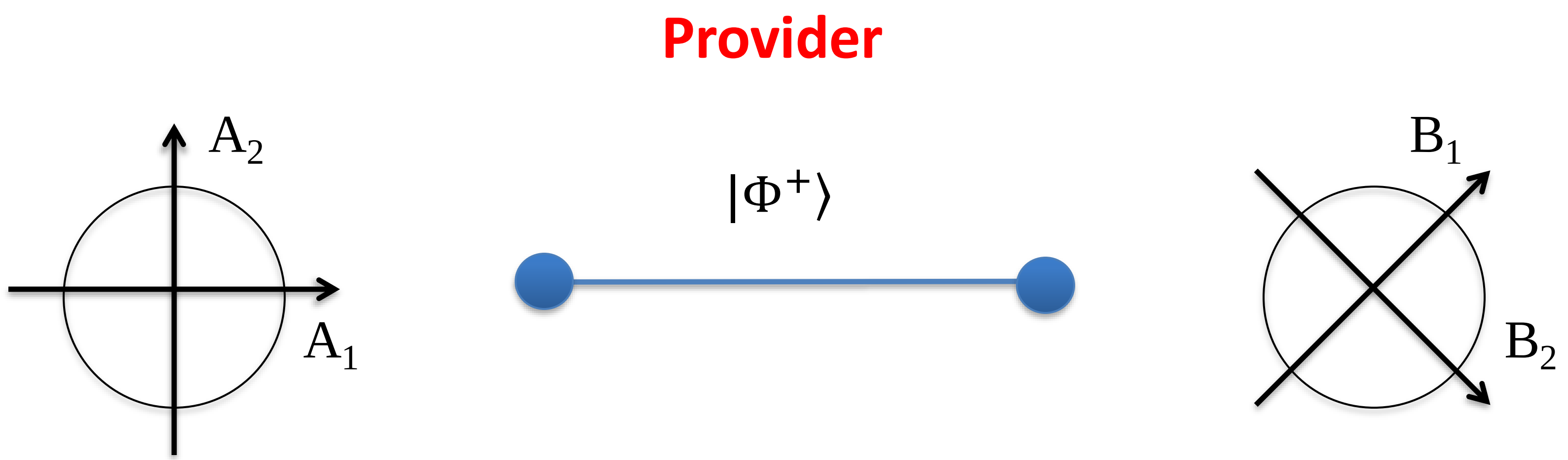
Bell-certified quantum randomness

The outcomes of a Bell experiment cannot be predicted in advance.



It is possible to bound the randomness of the outputs from the Bell inequality violation, which is a function only of the observed statistics.

Bell-certified quantum randomness

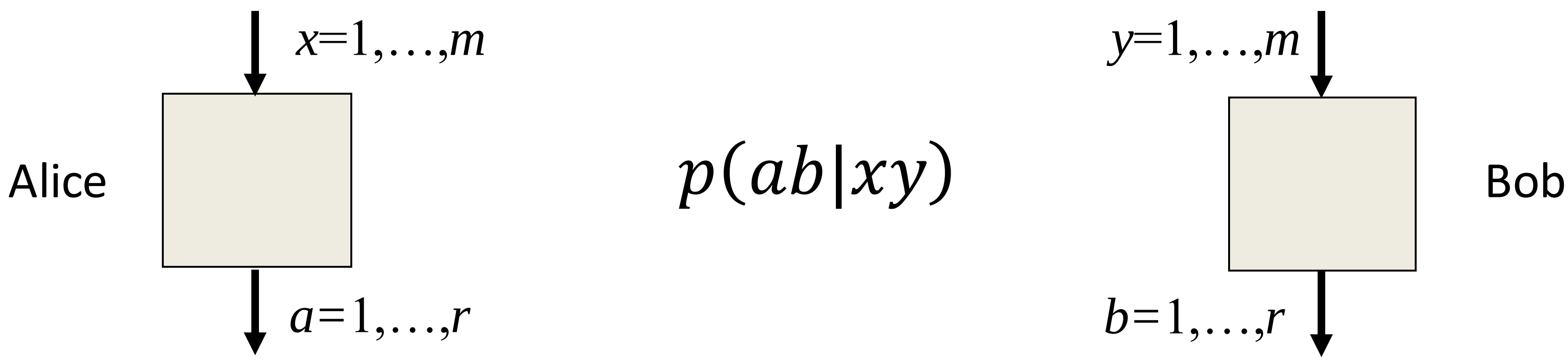


The provider is not device-independent: devices and their details are crucial for the implementation! But they are irrelevant for the user’s certification.

Protocols for Device-Independent Quantum Key Distribution

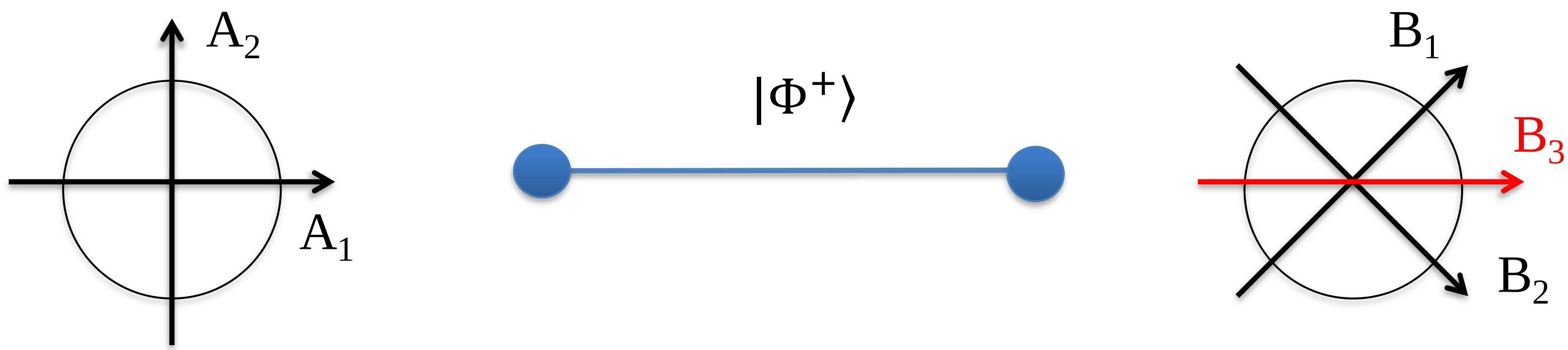
A. Acín *et al.*, Phys. Rev. Lett. 98, 230501 (2007)

DI Quantum Key Distribution



- One of the inputs (or more) are used on each side to generate the secret key.
- The generated statistics, which should violate a Bell inequality, is used to bound the eavesdropper's knowledge.

DI Quantum Key Distribution



- Bases A_1 and B_3 are used to construct the key.
- Bases 1 and 2 on each side are used to estimate the CHSH violation and, from it, Eve's knowledge.

$$K \geq I(A:B) - \chi(A:E)$$

Device-Independent Scenario

Quantum Information Theory

Protocols

Quantum Foundations

Generalized theories
Quantum correlations

Many-body physics

Non-locality of many-body states
Methods for many-body certification

Quantum Optics

Implementation of
protocols

Device-Independent Scenario

Quantum Information Theory

Protocols

Quantum Foundations

Generalized theories
Quantum correlations

Many-body physics

Non-locality of many-body states
Methods for many-body certification

Quantum Optics

Implementation of protocols

Quantum foundations

↓

Quantum information theory

Quantum foundations

Quantum information theory

Quantum theory based on real numbers can be experimentally falsified

M.-O. Renou *et al.*, Nature 600, 625 (2021)

Complex numbers in quantum theory

Quantum mechanics is the first theory formulated in terms of complex numbers.

1. To any physical system it is associated a complex Hilbert space H.
2. A physical state of the system is specified by a vector in this space $|\psi\rangle \in H$.
3. A measurement Π of R outcomes is specified by a set of r orthogonal projectors, $\{\Pi_r\}_{r=1,\dots,R}$, acting on H that sum up to the identity, $\sum_r \Pi_r = 1$.
4. Born rule: The probability of observing result r when performing measurement Π on a system in state $|\psi\rangle$ is $P(r) = \langle\psi| \Pi_r |\psi\rangle$.
5. System composition: the Hilbert space associated to a system made of two subsystems, A and B, is the tensor product of the two subsystem Hilbert spaces, $H_{AB} = H_A \otimes H_B$.

Complex numbers in quantum theory

Letter from Schrödinger to Lorentz (1926):

'What is unpleasant here, and indeed directly to be objected to, is the use of complex numbers. $\boldsymbol{\psi}$ is surely fundamentally a real function'

Complex numbers in quantum theory

What happens if we replace complex numbers by real numbers in quantum theory?

Complex numbers in quantum theory

What happens if we replace complex numbers by real numbers in quantum theory?

1. To any physical system it is associated a complex Hilbert space H.

2. A physical state of the system is specified by a vector in this space $|\psi\rangle \in H$.

3. A measurement Π of R outcomes is specified by a set of r orthogonal projectors, $\{\Pi_r\}_{r=1,\ldots,R}$, acting on H that sum up to the identity, $\sum_r \Pi_r = 1$.

4. Born rule: The probability of observing result r when performing measurement Π on a system in state $|\psi\rangle$ is $P(r) = \langle\psi|\, \Pi_r|\psi\rangle$.

5. System composition: the Hilbert space associated to a system made of two subsystems, A and B, is the tensor product of the two subsystem Hilbert spaces, $H_{AB} = H_A \otimes H_B$.

Complex numbers in quantum theory

What happens if we replace complex numbers by real numbers in quantum theory?

1. To any physical system it is associated a **real** Hilbert space H.

2. A physical state of the system is specified by a vector in this space $|\psi\rangle \in H$.

3. A measurement Π of R outcomes is specified by a set of r orthogonal projectors, $\{\Pi_r\}_{r=1,\ldots,R}$, acting on H that sum up to the identity, $\sum_r \Pi_r = 1$.

4. Born rule: The probability of observing result r when performing measurement Π on a system in state $|\psi\rangle$ is $P(r) = \langle\psi|\,\Pi_r|\psi\rangle$.

5. System composition: the Hilbert space associated to a system made of two subsystems, A and B, is the tensor product of the two subsystem Hilbert spaces, $H_{AB} = H_A \otimes H_B$.

Complex numbers in quantum theory

What happens if we replace complex numbers by real numbers in quantum theory?

1. To any physical system it is associated a **real** Hilbert space H.

2. A physical state of the system is specified by a vector in this space $|\psi\rangle \in H$.

3. A measurement Π of R outcomes is specified by a set of r orthogonal projectors, $\{\Pi_r\}_{r=1,\ldots,R}$, acting on H that sum up to the identity, $\sum_r \Pi_r = 1$.

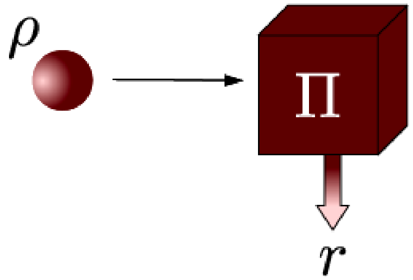
4. Born rule: The probability of observing result r when performing measurement Π on a system in state $|\psi\rangle$ is $P(r) = \langle\psi| \Pi_r |\psi\rangle$.

5. System composition: the Hilbert space associated to a system made of two subsystems, A and B, is the tensor product of the two subsystem Hilbert spaces, $H_{AB} = H_A \otimes H_B$.

C. M. Caves, C. A. Fuchs, and P. Rungta, Foundations of Physics Letters 14, 199 (2001)

Single systems

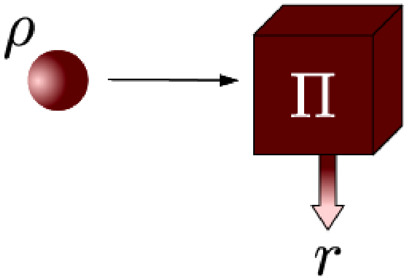
Complex



$$P(r) = \mathrm{tr}(\rho \Pi_r)$$

Single systems

Complex

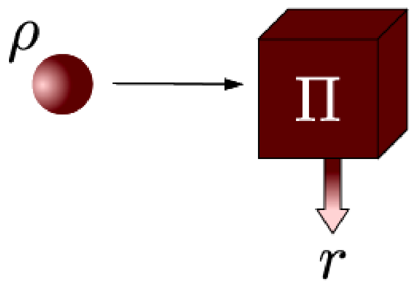


$$P(r) = \mathrm{tr}(\rho \Pi_r)$$

Complex operators

Single systems

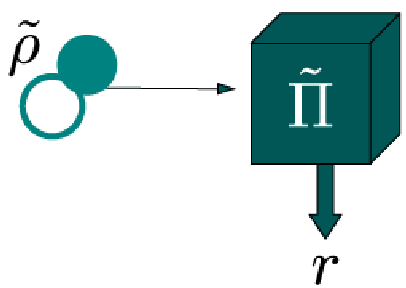
Complex



$$P(r) = \mathrm{tr}(\rho \Pi_r)$$

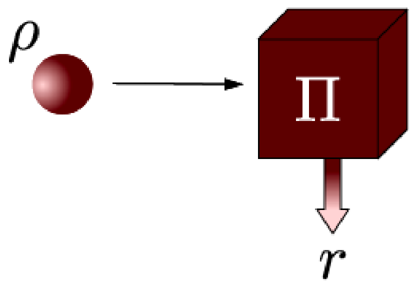
Complex operators

Real



Single systems

Complex

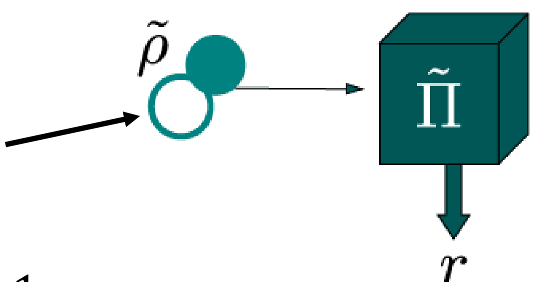


$$P(r) = \mathrm{tr}(\rho \Pi_r)$$

Complex operators

Real

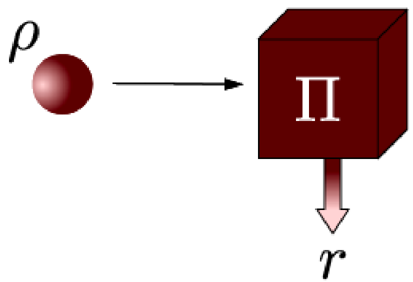
Extra qubit



$$|\pm i\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm i|1\rangle)$$

Single systems

Complex



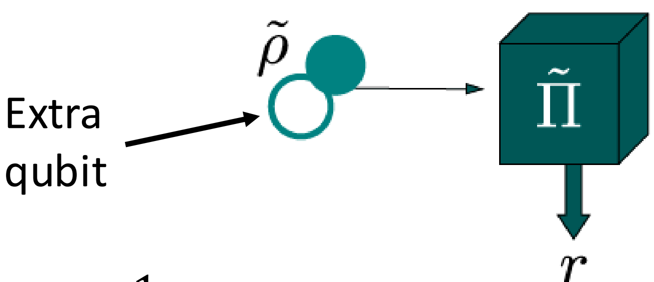
$$P(r) = \mathrm{tr}(\rho\Pi_r)$$

Complex operators

Real

$$\tilde{\rho} = \frac{1}{2}(\rho \otimes |{+i}\rangle\langle{+i}| + \rho^* \otimes |{-i}\rangle\langle{-i}|)$$

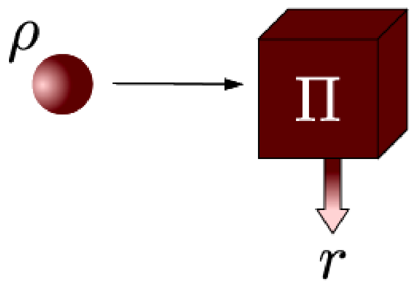
$$\tilde{\Pi}_r = \Pi_r \otimes |{+i}\rangle\langle{+i}| + \Pi_r^* \otimes |{-i}\rangle\langle{-i}|$$



$$|{\pm i}\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm i|1\rangle)$$

Single systems

Complex



$$P(r) = \mathrm{tr}(\rho \Pi_r)$$

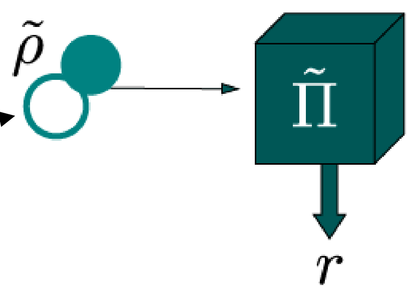
Complex operators

Real

$$\tilde{\rho} = \frac{1}{2}(\rho \otimes |{+i}\rangle\langle{+i}| + \rho^* \otimes |{-i}\rangle\langle{-i}|)$$

$$\tilde{\Pi}_r = \Pi_r \otimes |{+i}\rangle\langle{+i}| + \Pi_r^* \otimes |{-i}\rangle\langle{-i}|$$

Extra qubit



Since $P(r) = P^*(r) = \mathrm{tr}(\rho^* \Pi_r^*)$:

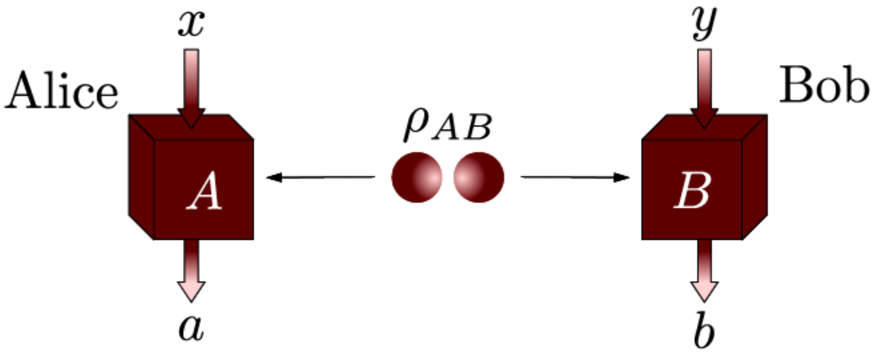
$$|{\pm i}\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm i|1\rangle)$$

$$P(r) = \mathrm{tr}(\rho \Pi_r) = \mathrm{tr}\big(\tilde{\rho}\tilde{\Pi}_r\big)$$

Real operators

Composite systems

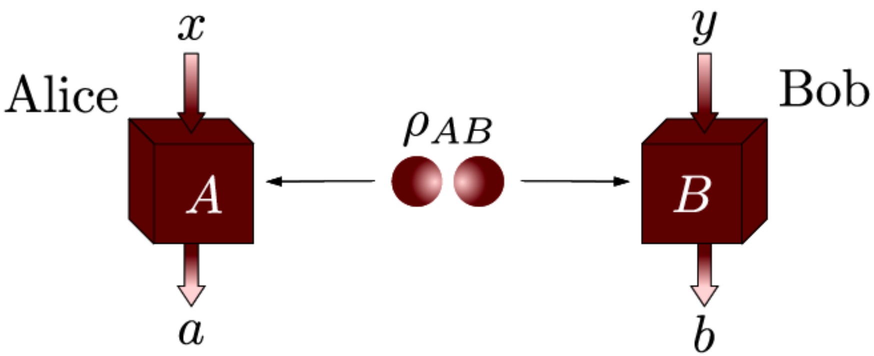
Complex



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

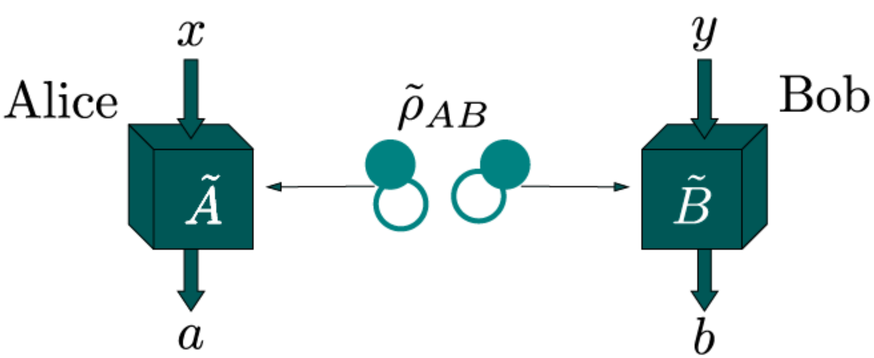
Composite systems

Complex



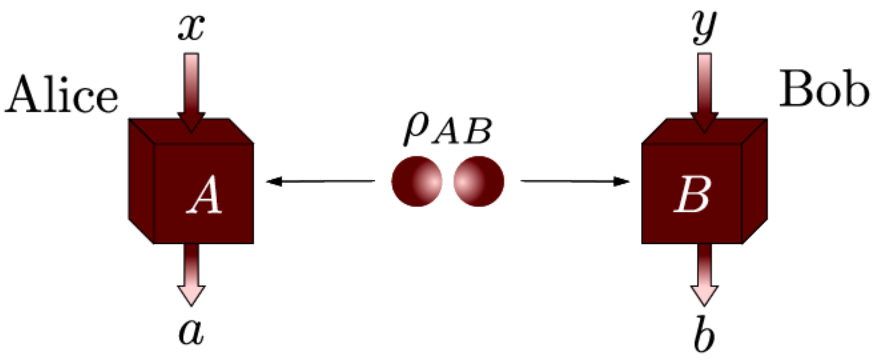
$$P(ab|xy) = \mathrm{tr}\left(\rho_{AB}\Pi_{a|x} \otimes \Pi_{b|y}\right)$$

Real



Composite systems

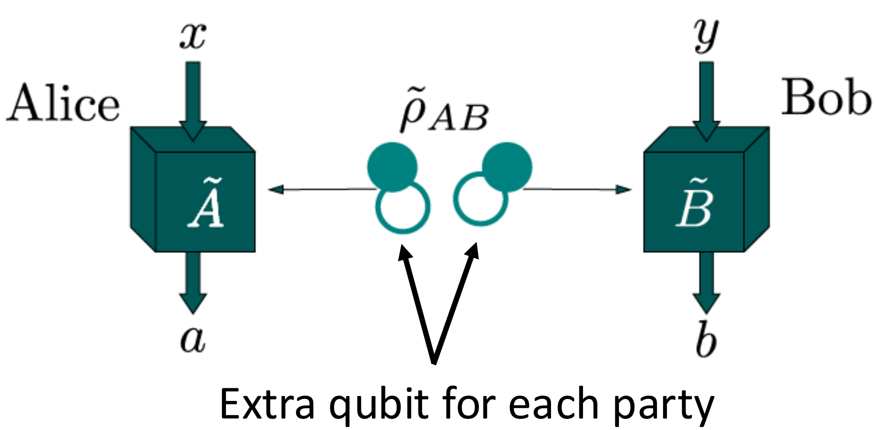
Complex



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

Real

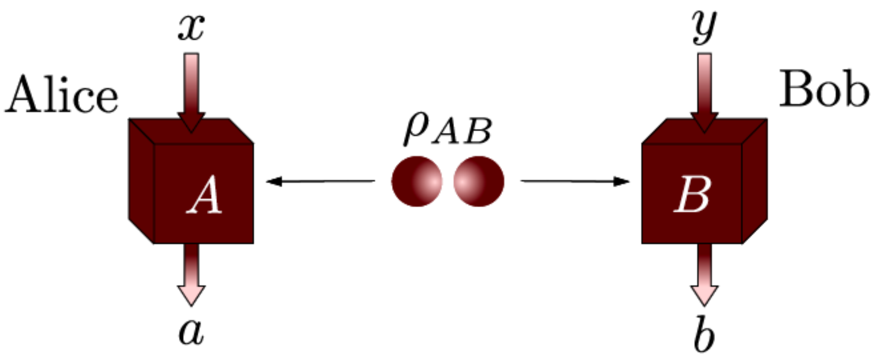
$$\tilde{\rho}_{AB} = \frac{1}{2}\left(\rho_{AB} \otimes |{+i}\rangle\langle{+i}|^{\otimes 2} + \rho_{AB}^{*} \otimes |{-i}\rangle\langle{-i}|^{\otimes 2}\right)$$



$$\tilde{\Pi}_{a|x} = \Pi_{a|x} \otimes |{+i}\rangle\langle{+i}| + \Pi_{a|x}^{*} \otimes |{-i}\rangle\langle{-i}|$$

Composite systems

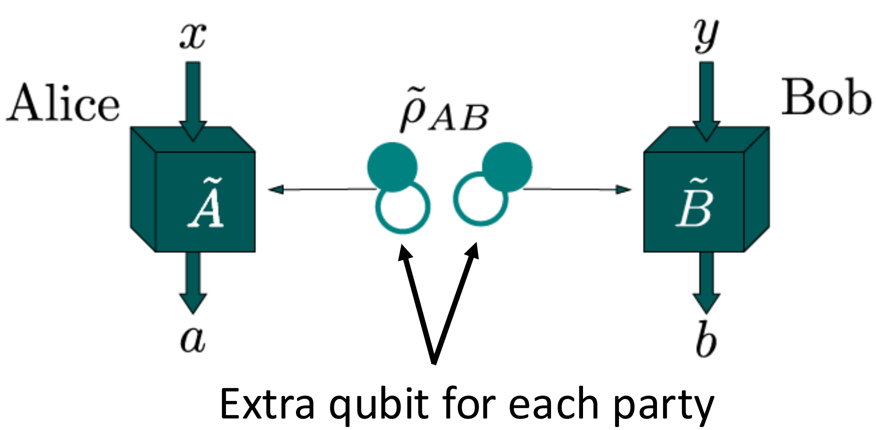
Complex



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

Real

$$\tilde{\rho}_{AB} = \frac{1}{2}\left(\rho_{AB} \otimes |+i\rangle\langle +i|^{\otimes 2} + \rho_{AB}^{*} \otimes |-i\rangle\langle -i|^{\otimes 2}\right)$$

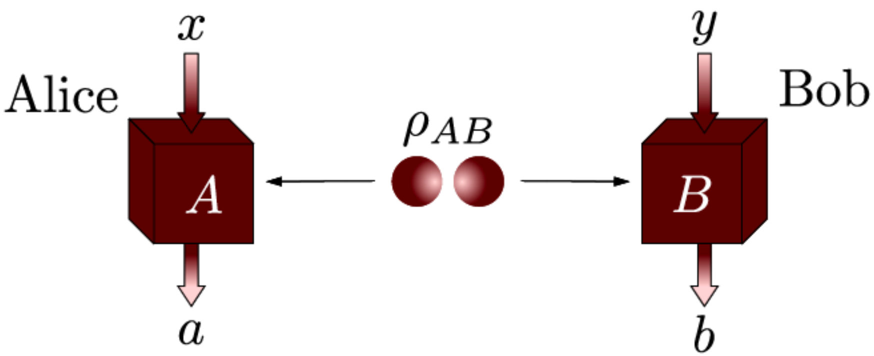


$$\tilde{\Pi}_{a|x} = \Pi_{a|x} \otimes |+i\rangle\langle +i| + \Pi_{a|x}^{*} \otimes |-i\rangle\langle -i|$$

$$P(ab|xy) = \mathrm{tr}\left(\tilde{\rho}_{AB}\tilde{\Pi}_{a|x} \otimes \tilde{\Pi}_{b|y}\right)$$

Composite systems

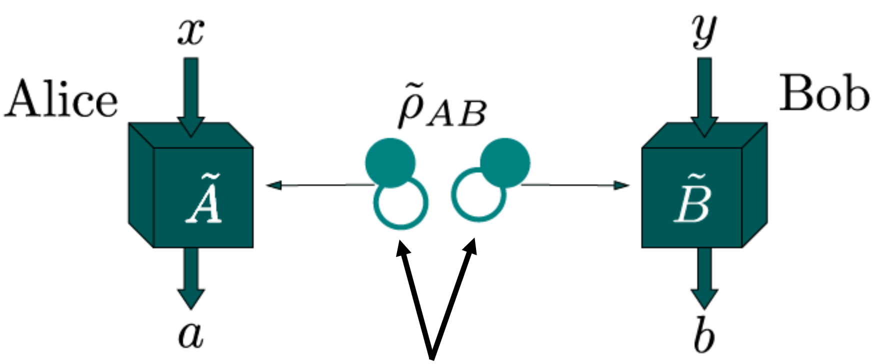
Complex



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

Real

$$\tilde{\rho}_{AB} = \frac{1}{2}\left(\rho_{AB} \otimes |+i\rangle\langle +i|^{\otimes 2} + \rho_{AB}^{*} \otimes |-i\rangle\langle -i|^{\otimes 2}\right)$$



$$\tilde{\Pi}_{a|x} = \Pi_{a|x} \otimes |+i\rangle\langle +i| + \Pi_{a|x}^{*} \otimes |-i\rangle\langle -i|$$

$$P(ab|xy) = \mathrm{tr}\left(\tilde{\rho}_{AB} \tilde{\Pi}_{a|x} \otimes \tilde{\Pi}_{b|y}\right)$$

Extra qubit for each party

Correlations are used to synchronize the use of the state or its complex conjugate.

M. McKague, M. Mosca, N. Gisin, PRL 2009

Quantum network

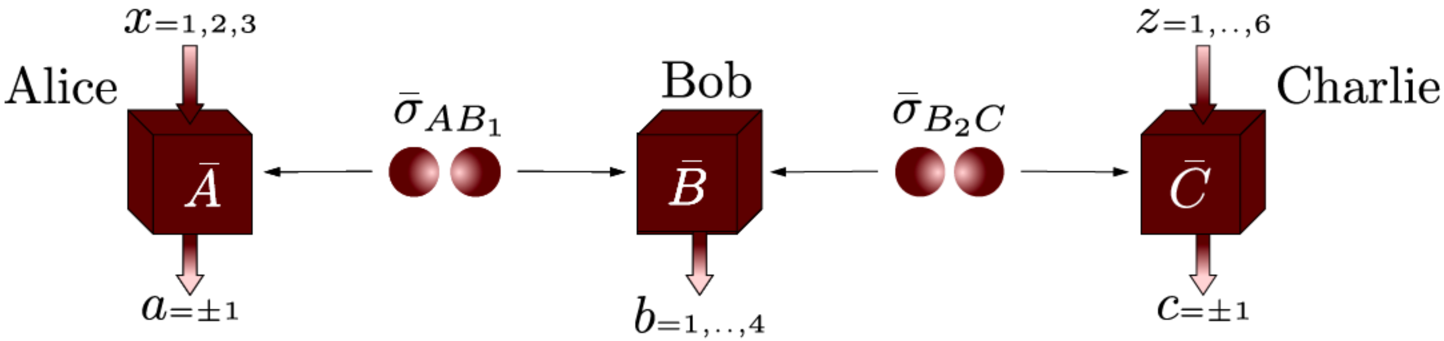
Key idea: use independent preparations and measurements, that can be entangled.

Quantum network

Key idea: use independent preparations and measurements, that can be entangled.

Complex

$$P(abc|xz) = \mathrm{tr}\left(\bar{\sigma}_{AB_1} \otimes \bar{\sigma}_{B_2C} \Pi_{a|x} \otimes \Pi_b \otimes \Pi_{c|z}\right)$$



Real and complex quantum theory lead to different correlations in an entanglement swapping experiment. Real quantum theory can be falsified.

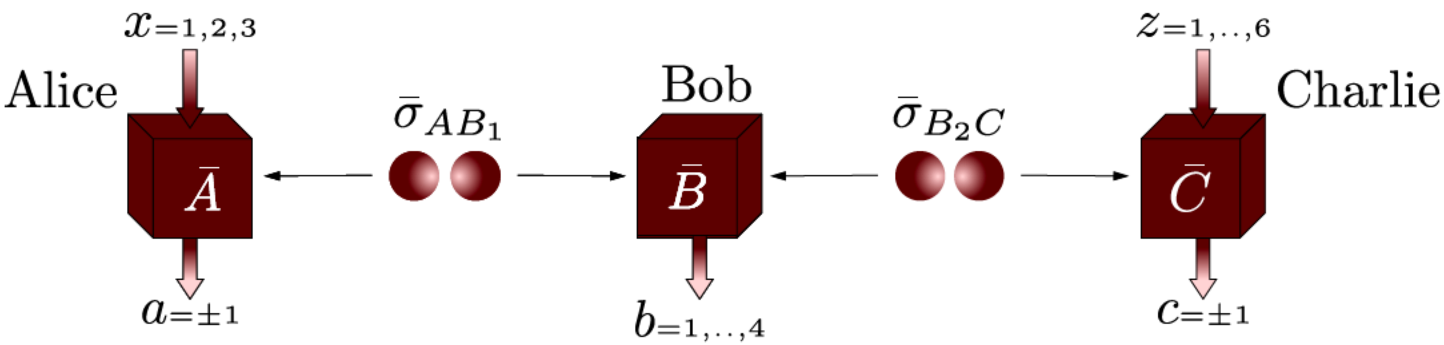
M.-O. Renou *et al.*, Nature 600, 625 (2021)

Quantum network

Key idea: use independent preparations and measurements, that can be entangled.

Complex

$$P(abc|xz)=\mathrm{tr}\left(\bar{\sigma}_{AB_1} \otimes \bar{\sigma}_{B_2C}\Pi_{a|x} \otimes \Pi_b \otimes \Pi_{c|z}\right)$$



Real and complex quantum theory lead to different correlations in an entanglement swapping experiment. Real quantum theory can be falsified.

M.-O. Renou *et al.*, Nature 600, 625 (2021)

Z.-D. Li *et al.*, PRL 128, 040402 (2022); M.-C. Chen *et al.*, PRL 128, 040403 (2022)

Device-Independent Scenario

Quantum Information Theory

Protocols

Quantum Foundations

Generalized theories
Quantum correlations

Many-body physics

Non-locality of many-body states
Methods for many-body certification

Quantum Optics

Implementation of
protocols

Setups for device-independent quantum key distribution

Setups for device-independent quantum key distribution

How to observe a proper Bell violation at large distances?

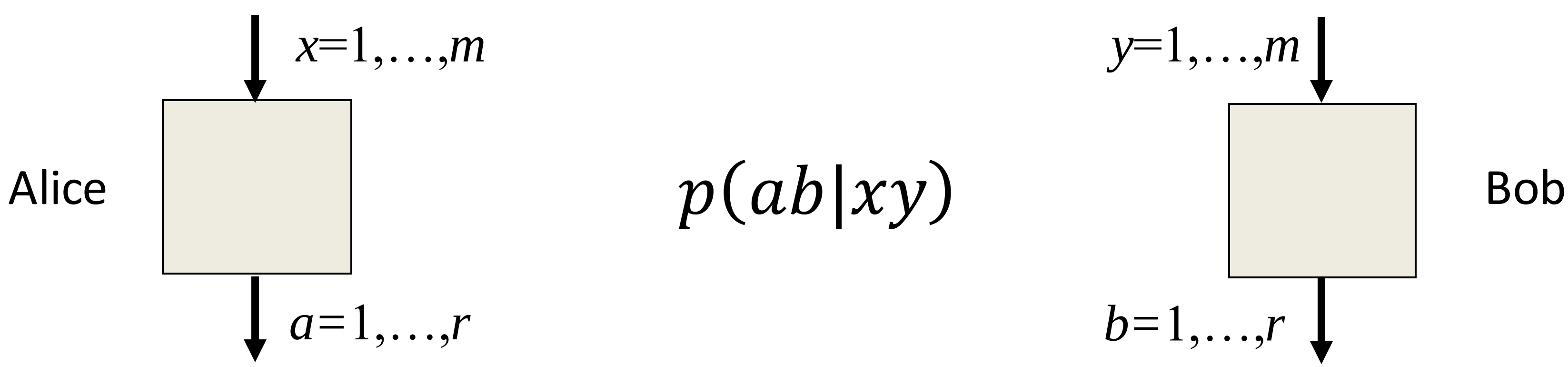
Implementations of DIQKD

- The implementation of DIQKD is extremely challenging. It requires a proper Bell test at two distant locations.

Implementations of DIQKD

- The implementation of DIQKD is extremely challenging. It requires a proper Bell test at two distant locations.

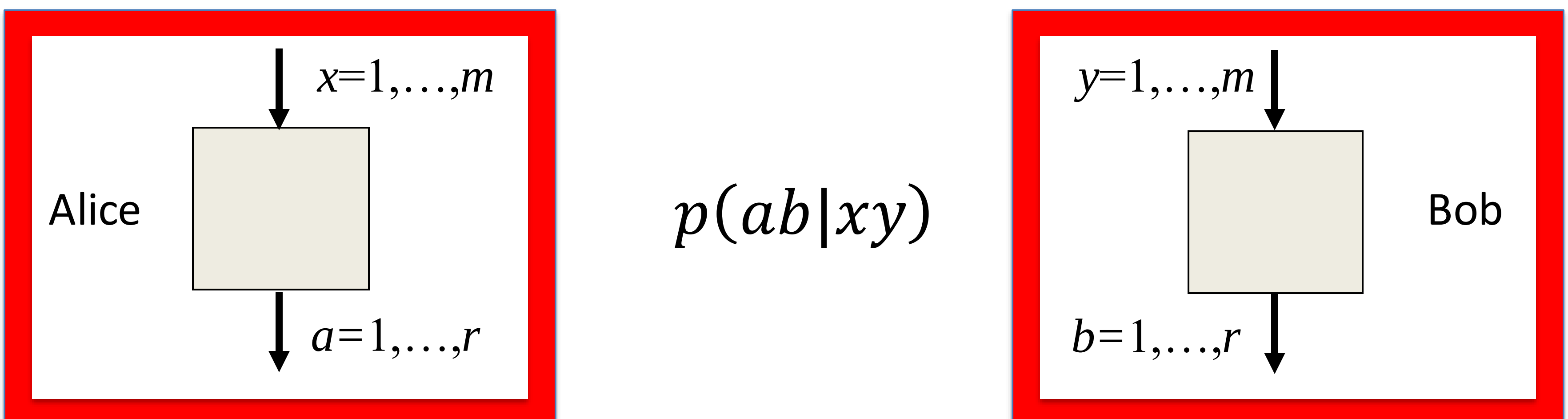
- The locality loophole is somehow artificial in this context, as it requires two devices communicating their inputs. Then, why not the outputs to the eavesdropper?



Implementations of DIQKD

- The implementation of DIQKD is extremely challenging. It requires a proper Bell test at two distant locations.

- The locality loophole is somehow artificial in this context, as it requires two devices communicating their inputs. Then, why not the outputs to the eavesdropper?



- **Some shielding is always implicitly assumed in any crypto scenario.**

Implementations of DIQKD

- The implementation of DIQKD thus requires a detection-loophole-free Bell test at two distant locations.

- Fake Bell violations have been demonstrated exploiting channel losses in Gerhardt et al., Phys. Rev. Lett. 107, 170404 (2011)?

Implementations of DIQKD

- The implementation of DIQKD thus requires a detection-loophole-free Bell test at two distant locations.
- Fake Bell violations have been demonstrated exploiting channel losses in Gerhardt et al., Phys. Rev. Lett. 107, 170404 (2011)?
- Losses affect the violation, and therefore the bound on Eve's knowledge, but also the correlations between the users.

$$K \geq I(A:B) - \chi(A:E)$$

- Detection efficiencies needed for security are higher than for Bell violation, of the order of 90-95%.

Losses in DIQKD

- Local losses may be seen just as a technological issue: better coupling, components and detectors. Yet, **local losses are challenging**.

Losses in DIQKD

- Local losses may be seen just as a technological issue: better coupling, components and detectors. Yet, **local losses are challenging**.

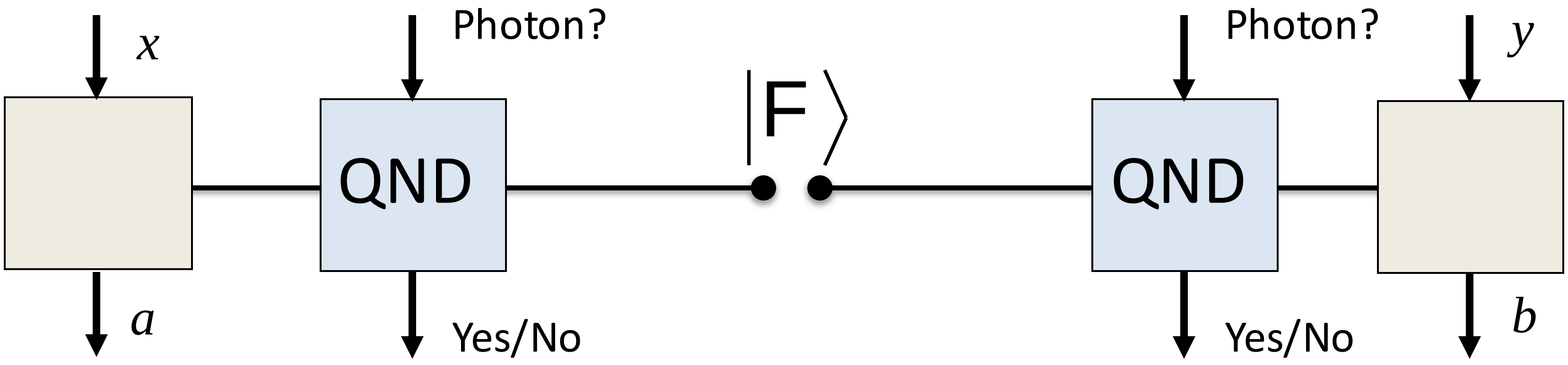
- What about channel losses? They are unavoidable!

Losses in DIQKD

- Local losses may be seen just as a technological issue: better coupling, components and detectors. Yet, **local losses are challenging**.

- What about channel losses? They are unavoidable!

- A solution: **QND measurements.** It is checked if the photon has arrived before performing the Bell test.

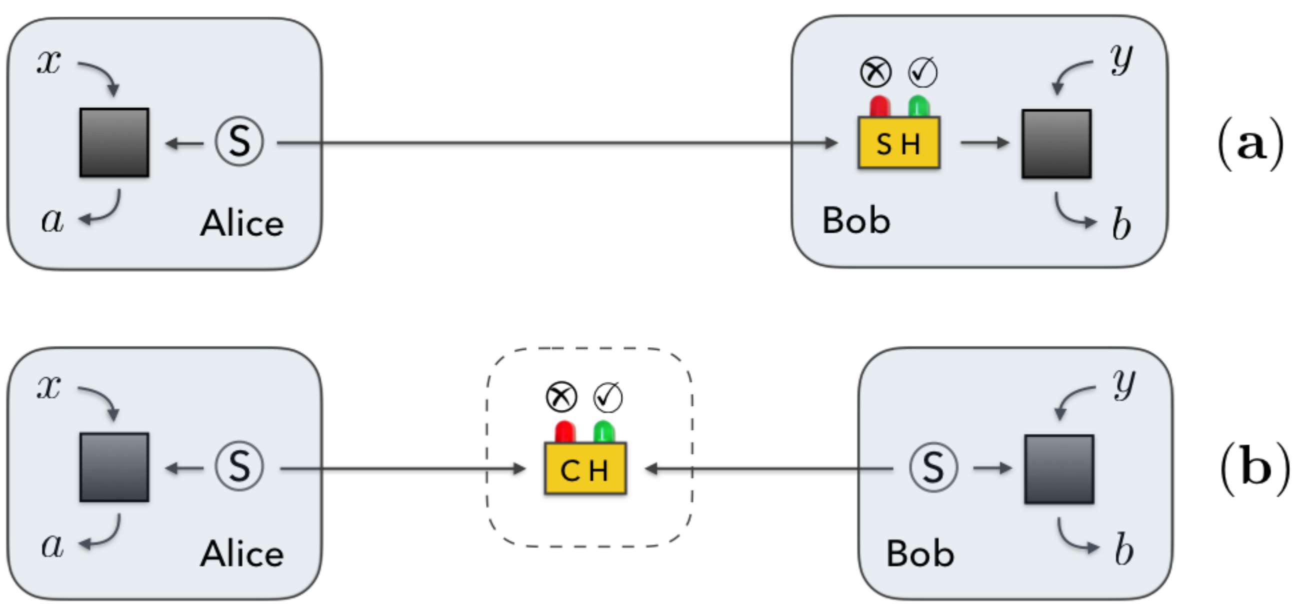


Channel losses become irrelevant for the protocol security (not for the rate).

Heralding schemes

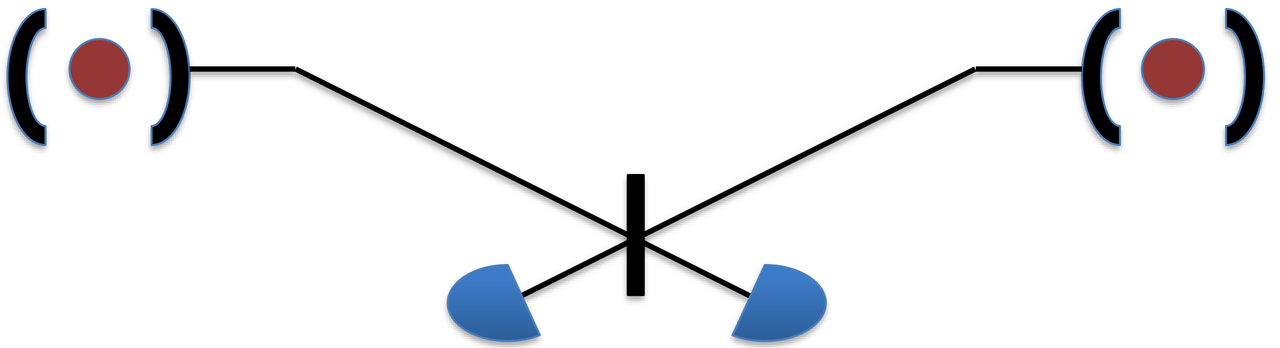
- QND are challenging. They can be replaced by heralding process, at one side (Side Heralding) or at a central station (Central Heralding) witnessing the correct state preparation.

- Correlations are kept only after successful heralding.



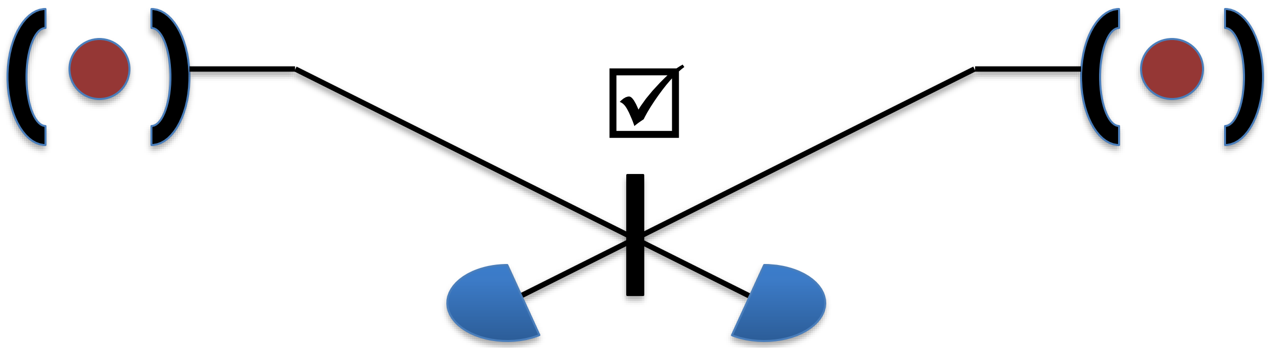
Remote entanglement preparation

Schemes for remote entanglement preparation between distant particles are also valid in this scenario (Hanson, Monroe and Weinfurter's groups).



Remote entanglement preparation

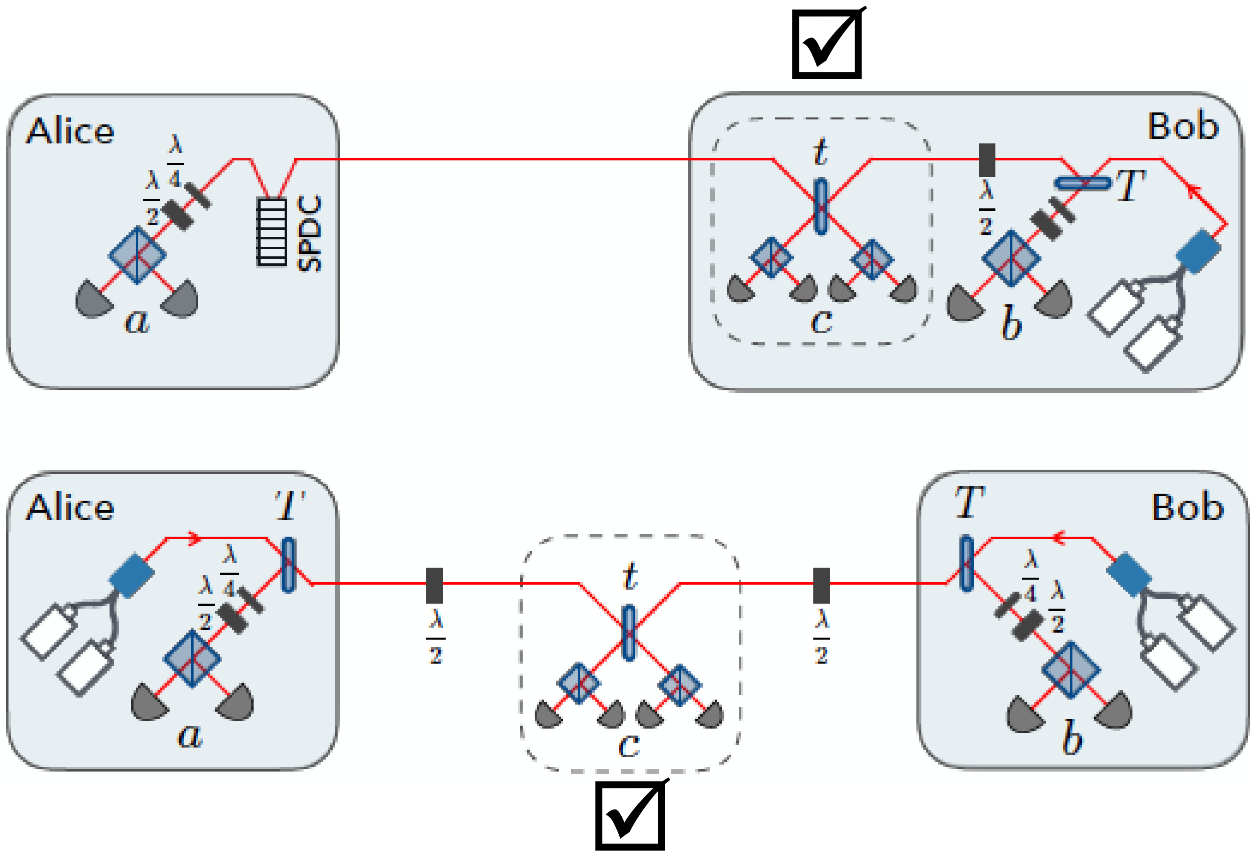
Schemes for remote entanglement preparation between distant particles are also valid in this scenario (Hanson, Monroe and Weinfurter's groups).



Conditioned on the double-click in the intermediate station, entanglement is created among the trapped particles.

Channel losses irrelevant and the almost perfect detection at the stations.

Single-photon schemes



Both schemes produce an entangled state between Alice and Bob at first order.
Kolodynski *et al.*, Quantum 4, 260 (2020)

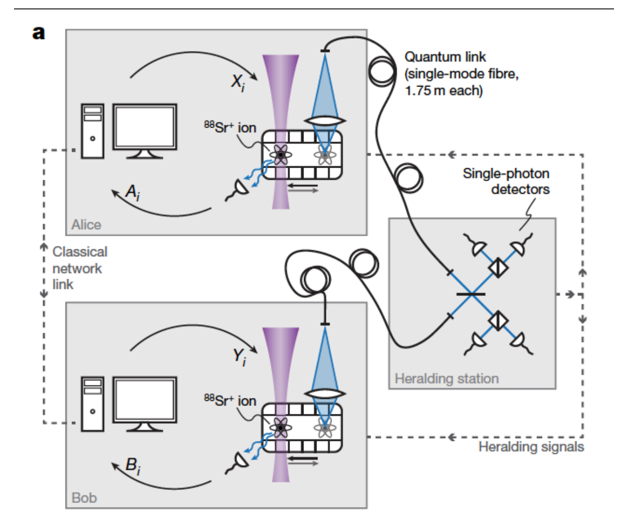
First proof-of-principle demonstrations

Article

Experimental quantum key distribution certified by Bell's theorem

https://doi.org/10.1038/s41586-022-04941-5
Received: 29 September 2021
Accepted: 7 June 2022

D. P. Nadlinger[1✉], P. Drmota[1], B. C. Nichol[1], G. Araneda[1], D. Main[1], R. Srinivas[1], D. M. Lucas[1], C. J. Ballance[1✉], K. Ivanov[2], E. Y.-Z. Tan[3], P. Sekatski[4], R. L. Urbanke[2], R. Renner[3], N. Sangouard[5✉] & J.-D. Bancal[5✉]



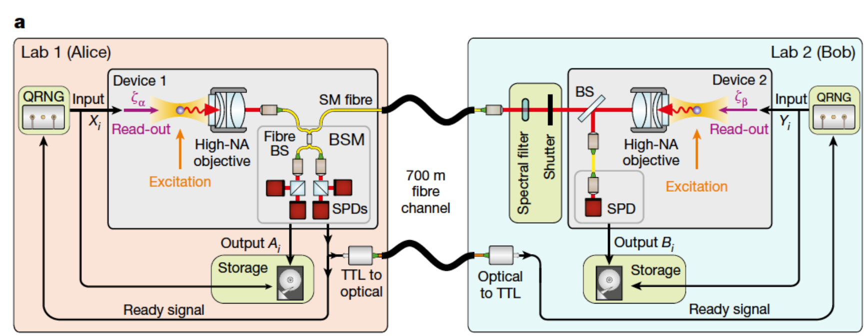
Trapped ions. Distance: 2m.
Key rate: >90kbits / 8 hours.

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

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✉]



Trapped atoms. Distance: 400m.
No key rate, but possible if more rounds were available.

Conclusions

- Device-independent protocols offer self-certified performance.

- The observation of non-locality is a necessary condition for device-independent quantum information processing.

Conclusions

- Device-independent protocols offer self-certified performance.

- The observation of non-locality is a necessary condition for device-independent quantum information processing.

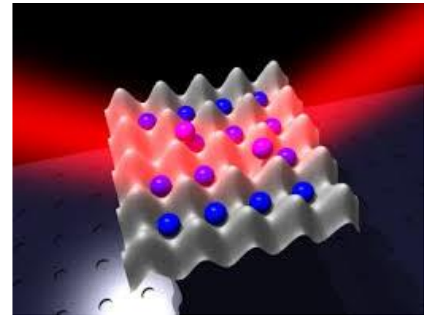
- Protocols exist for randomness generation, secure key distribution and self-testing. What are the limitations and possibilities of the scenario?

Conclusions

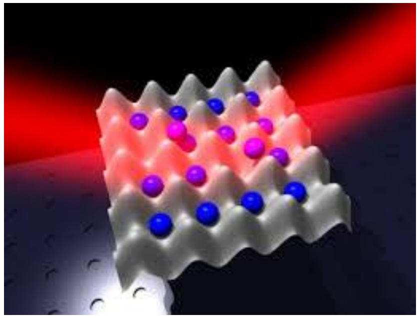
- Device-independent protocols offer self-certified performance.
- The observation of non-locality is a necessary condition for device-independent quantum information processing.
- Protocols exist for randomness generation, secure key distribution and self-testing. What are the limitations and possibilities of the scenario?
- The implementation requires a detection-loophole-free violation. Experimentally challenging, especially when considering distant parties as in a cryptographic scenario. Single photons are promising in this direction.

Conclusions

- Device-independent protocols offer self-certified performance.
- The observation of non-locality is a necessary condition for device-independent quantum information processing.
- Protocols exist for randomness generation, secure key distribution and self-testing. What are the limitations and possibilities of the scenario?
- The implementation requires a detection-loophole-free violation. Experimentally challenging, especially when considering distant parties as in a cryptographic scenario. Single photons are promising in this direction.
- The framework also provides new light on other fields: quantum foundations, quantum optics and many-body physics.



Quantum Certification: is a complex quantum device random? Secret? A quantum computer? Entangled?



Quantum Certification: is a complex quantum device random? Secret? A quantum computer? Entangled?

What can we say about complex quantum systems when using limited (because scalable) classical information?

Device-Independent Scenario

Quantum Information Theory

Protocols

Quantum Foundations

Generalized theories
Quantum correlations

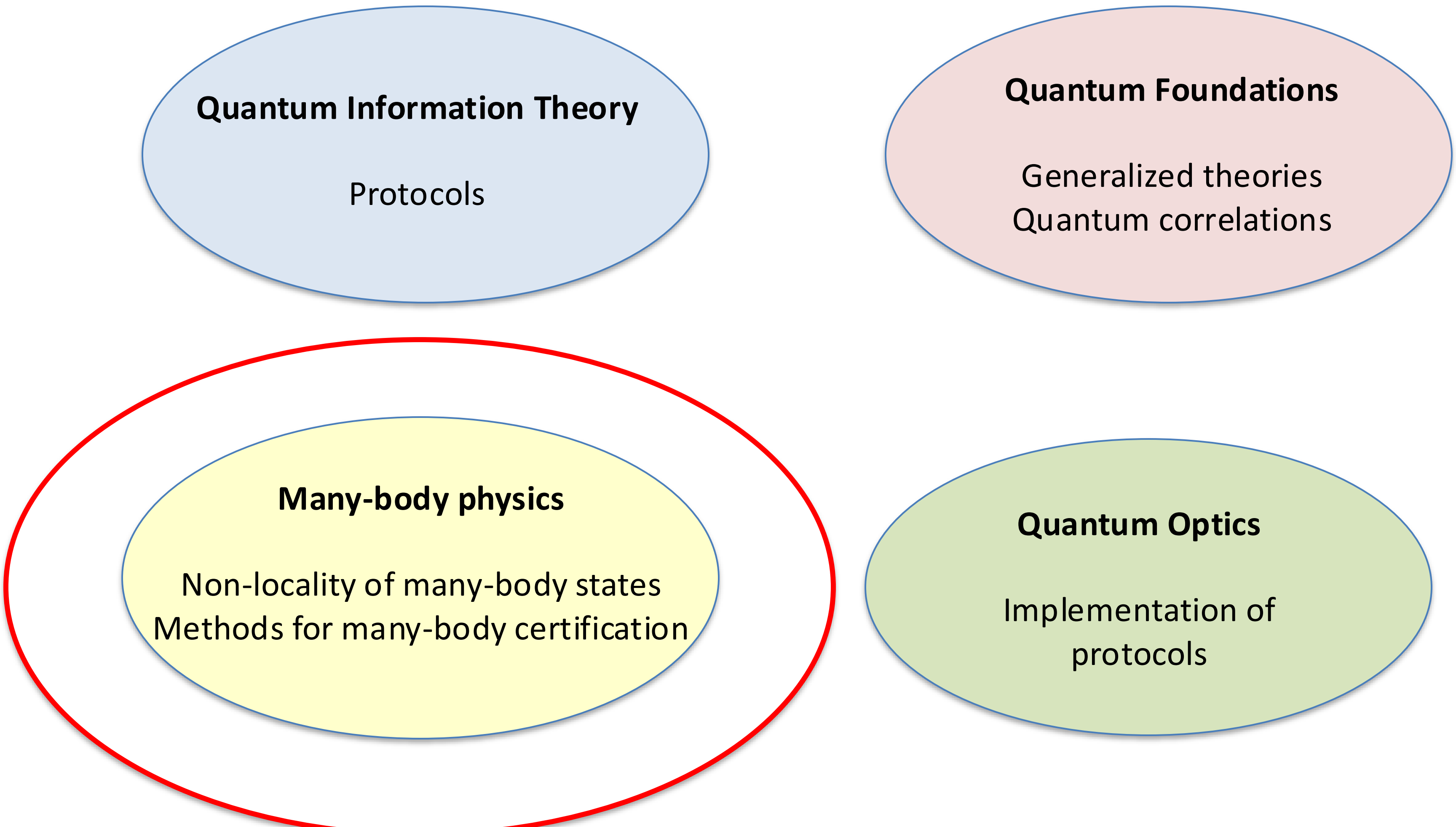
Many-body physics

Non-locality of many-body states
Methods for many-body certification

Quantum Optics

Implementation of protocols

Device-Independent Scenario

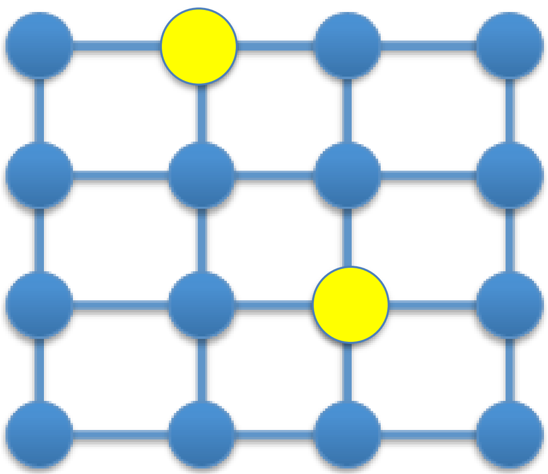


Detecting non-locality in many-body quantum states

J. Tura, R. Augusiak, A. B. Sainz, T. Vértesi, M. Lewenstein, A. Acín

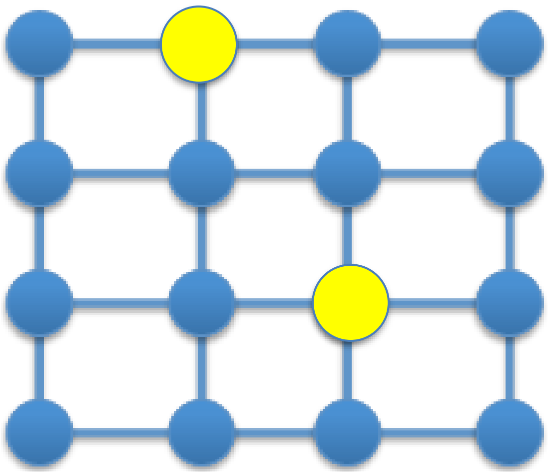
Science 344, no. 6189, 1256-1258 (2014)

Non-locality of many-body systems



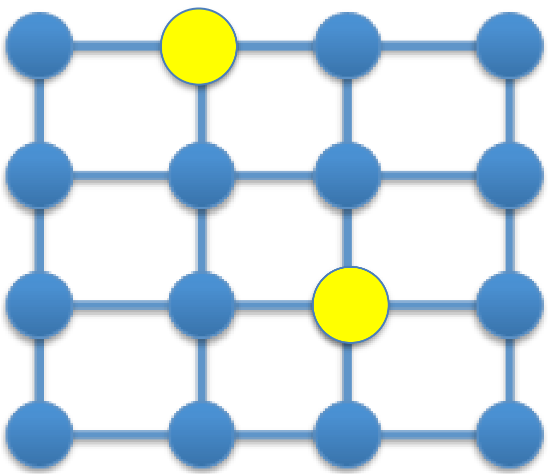
Do natural many-body quantum states display non-local correlations when subjected to natural 2-body observables?

Non-locality of many-body systems



Do the weakest form of correlations, represented by 2-body correlation functions, suffice to detect the non-locality of systems of an arbitrary number of particles?

Non-locality of many-body systems



Do the weakest form of correlations, represented by 2-body correlation functions, suffice to detect the non-locality of systems of an arbitrary number of particles?

We provided an affirmative answer to the previous question by constructing Bell inequalities made only of 2-body correlation functions and proving their quantum violation for any number of particles.

Non-locality of many-body states

- We derived general techniques for the study of non-locality of many-body quantum systems.
- We showed how 2-body correlation function suffice for the non-locality detection of systems of arbitrary size.
- We provided violations for Dicke states, which are ground states of interacting systems (LMG Hamiltonian).
- Some of the derived inequalities can be measured by means of first and second moment of global spin observables.

Experimental observation

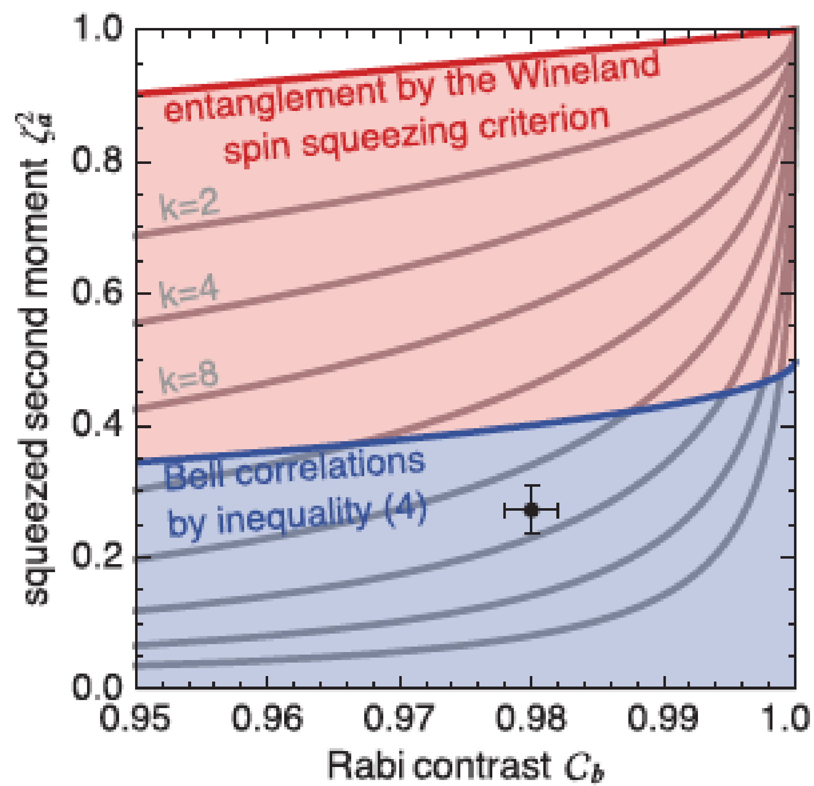
Our inequalities have already been violated in a BEC consisting of 480 particles.

QUANTUM OPTICS

Bell correlations in a Bose-Einstein condensate

Roman Schmied,[1*] Jean-Daniel Bancal,[2,4*] Baptiste Allard,[1*] Matteo Fadel,[1] Valerio Scarani,[2,3] Philipp Treutlein,[1†] Nicolas Sangouard[4†]

The violation was inferred by means of the first and second moments of global-spin observables.



Device-Independent Scenario

Quantum Information Theory

Protocols

Quantum Foundations

Generalized theories
Quantum correlations

Many-body physics

Non-locality of many-body states
Methods for many-body certification

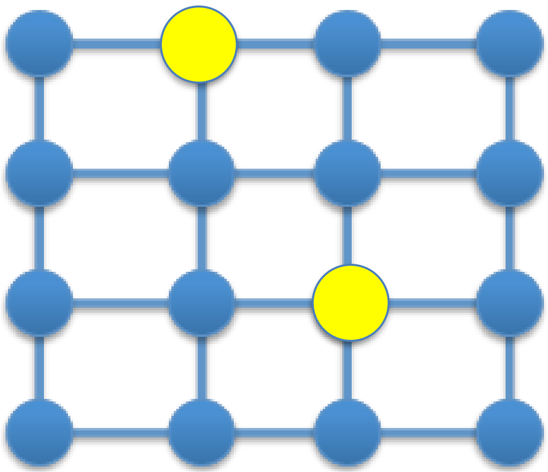
Quantum Optics

Implementation of
protocols

Detecting non-locality in many-body quantum states

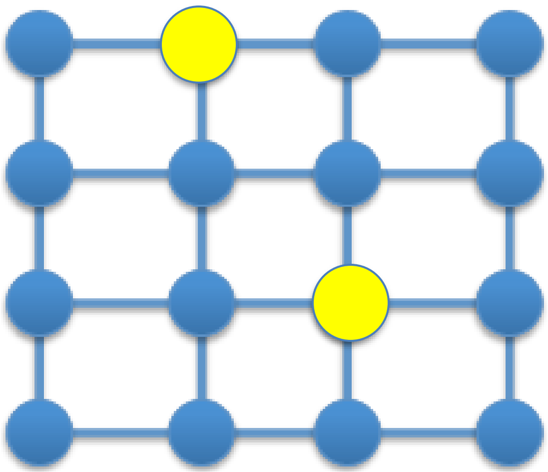
J. Tura, R. Augusiak, A. B. Sainz, T. Vértesi, M. Lewenstein, A. Acín
Science 344, no. 6189, 1256-1258 (2014)

Non-locality of many-body systems



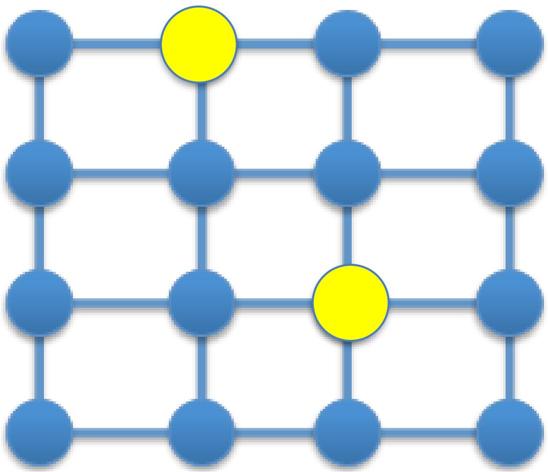
Do natural many-body quantum states display non-local correlations when subjected to natural 2-body observables?

Non-locality of many-body systems



Do the weakest form of correlations, represented by 2-body correlation functions, suffice to detect the non-locality of systems of an arbitrary number of particles?

Non-locality of many-body systems



Do the weakest form of correlations, represented by 2-body correlation functions, suffice to detect the non-locality of systems of an arbitrary number of particles?

We provided an affirmative answer to the previous question by constructing Bell inequalities made only of 2-body correlation functions and proving their quantum violation for any number of particles.

Non-locality of many-body systems

Key idea: restrict the study to symmetric Bell inequalities.

$$B = \alpha S_1 + \beta S_2 + \gamma S_{11} + \delta S_{12} + \varepsilon S_{22} \le \beta_C$$

$$S_k = \sum_{i=1}^{N} A_k^{(i)} \qquad S_{kl} = \sum_{i \neq j=1}^{N} A_k^{(i)} A_l^{(j)}$$

Non-locality of many-body systems

Key idea: restrict the study to symmetric Bell inequalities.

$$B = \alpha S_1 + \beta S_2 + \gamma S_{11} + \delta S_{12} + \epsilon S_{22} \le b_C$$

$$S_k = \sum_{i=1}^{N} A_k^{(i)} \qquad S_{kl} = \sum_{i \ne j=1}^{N} A_k^{(i)} A_l^{(j)}$$

In the quantum case, variables are replaced by operators. As an example, take:

$$A_1^{(i)} = \sigma_x \quad A_2^{(i)} = \sigma_z$$

Total spin in the *x* direction.

$$S_1 = \sum_{i=1}^{N} \sigma_x^{(i)} \qquad S_{21} = \sum_{i \ne j=1}^{N} \sigma_z^{(i)} \sigma_x^{(j)}$$

It can be estimated through second moments of total spin in *x* and *z* directions.

Non-locality of many-body states

- We derived general techniques for the study of non-locality of many-body quantum systems.

- We showed how 2-body correlation function suffice for the non-locality detection of systems of arbitrary size.

- We provided violations for Dicke states, which are ground states of interacting systems (LMG Hamiltonian).

- Some of the derived inequalities can be measured by means of first and second moment of global spin observables.

Experimental observation

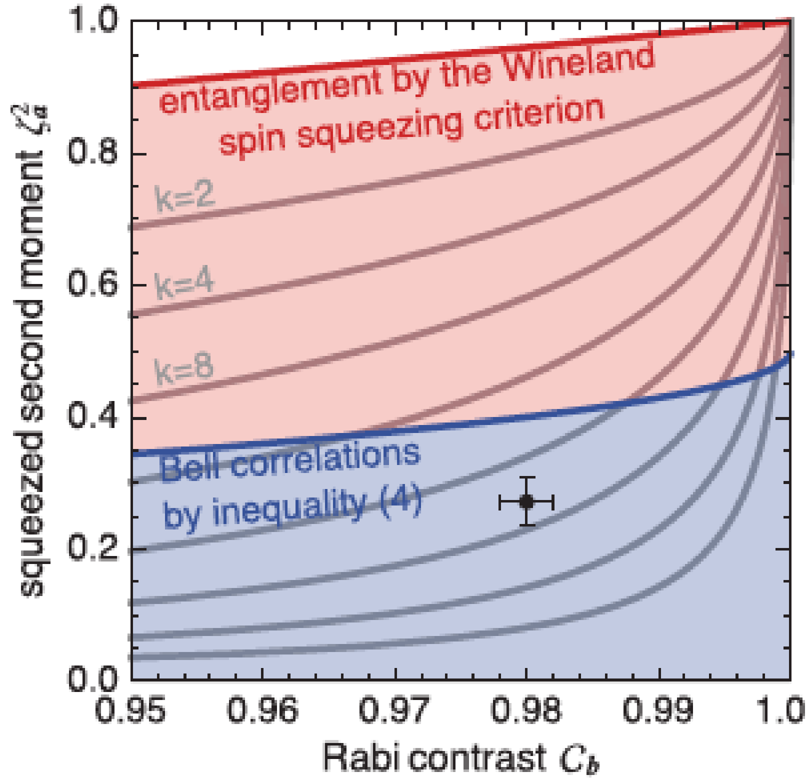
Our inequalities have already been violated in a BEC consisting of 480 particles.

QUANTUM OPTICS

Bell correlations in a Bose-Einstein condensate

Roman Schmied,[1]* Jean-Daniel Bancal,[2,4]* Baptiste Allard,[1]* Matteo Fadel,[1]
Valerio Scarani,[2,3] Philipp Treutlein,[1]† Nicolas Sangouard[4]†

The violation was inferred by means of the first and second moments of global-spin observables.



Energy as a detector of nonlocality of many-body spin systems

J. Tura, G. De las Cuevas, R. Augusiak, M. Lewenstein, A. Acín, J. I. Cirac

Phys. Rev. X 7, 021005 (2017)

Energy as non-locality detector

Standard many-body Hamiltonian operator, e.g.:

$$H = \sum_{i=1}^{N} \left(\left(1+\gamma\right) \sigma_X^{(i)} \otimes \sigma_X^{(i+1)} + \left(1-\gamma\right) \sigma_Y^{(i)} \otimes \sigma_Y^{(i+1)} \right)$$

Energy as non-locality detector

Standard many-body Hamiltonian operator, e.g.:

$$H = \sum_{i=1}^{N} \left((1+\gamma)\,\sigma_X^{(i)} \otimes \sigma_X^{(i+1)} + (1-\gamma)\,\sigma_Y^{(i)} \otimes \sigma_Y^{(i+1)} \right)$$

We want to associate a Bell inequality to this operator.
Key idea: replace quantum observables by classical values.

$$H = \sum_{i=1}^{N} \left((1+\gamma)\,A_1^{(i)} \otimes A_1^{(i+1)} + (1-\gamma)\,A_2^{(i)} \otimes A_2^{(i+1)} \right)$$

Energy as non-locality detector

Standard many-body Hamiltonian operator, e.g.:

$$H = \sum_{i=1}^{N} \left((1+\gamma)\, \sigma_X^{(i)} \otimes \sigma_X^{(i+1)} + (1-\gamma)\, \sigma_Y^{(i)} \otimes \sigma_Y^{(i+1)} \right)$$

We want to associate a Bell inequality to this operator.
Key idea: replace quantum observables by classical values.

$$H = \sum_{i=1}^{N} \left((1+\gamma)\, A_1^{(i)} \otimes A_1^{(i+1)} + (1-\gamma)\, A_2^{(i)} \otimes A_2^{(i+1)} \right)$$

If the ground-state energy of the quantum system E_{Q} is smaller than the ground-state energy of the classical system E_{C}, non-locality follows from the observation of an energy smaller than the classical minimum energy.

Classical and quantum energies

- In general, computing the ground-state energy of an interacting system is a hard computational problem.

- However, in classical 1D systems with local interactions, the ground-state energy can be computed by means of dynamic programming with an effort linear in size.

- For the quantum value, we use 1D Hamiltonians that can be diagonalized using Jordan-Wigner transformations. This is again efficient.

- The combination of these two methods allow the construction of Bell inequalities from Hamiltonian operators for big system sizes.

Illustration of the method

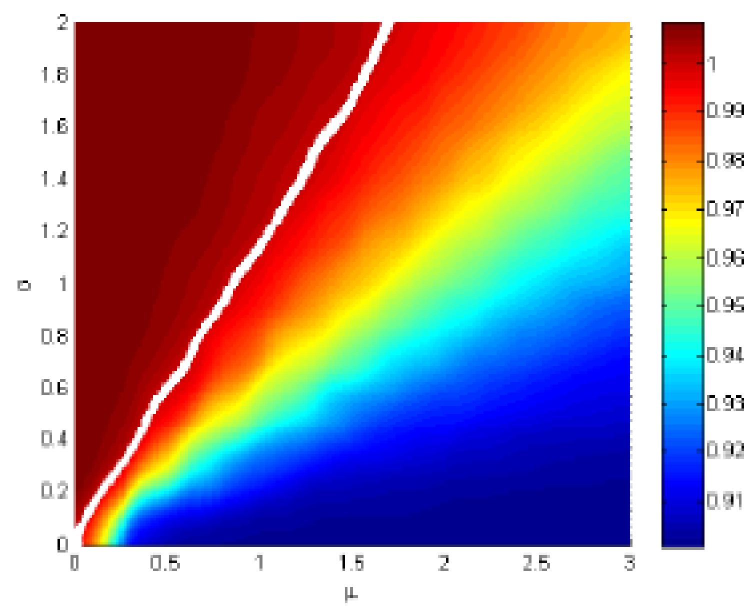
Spin glass:

$$H = \sum_{i=1}^{N} G_{\mu,\sigma}^{(i)} \left(\sigma_{\pi/4}^{(i)} \otimes \sigma_{\pi/4}^{(i+1)} + \sigma_{Y}^{(i)} \otimes \sigma_{Y}^{(i+1)} \right)$$

where the couplings are generated with a Gaussian probability distribution of mean μ and variance σ.

Ratio between the classical and quantum ground-state energy, for a 100-spin systems with PBC and averaged over 1000 realizations.

A violation is observed for large values of σ/μ.



Efficient device-independent entanglement detection of multipartite systems

F. Baccari, D. Cavalcanti, P. Wittek and A. Acín

Phys. Rev. X 7, 021042 (2017)

Idea of the method

Correlations $\mathrm{P}(r_1 r_2 \ldots r_N | m_1 m_2 \ldots m_N)$ among N particles don't violate any Bell inequality.

There exists a Hilbert space in which correlations $\mathrm{P}(r_1 r_2 \ldots r_N | m_1 m_2 \ldots m_N)$ can be written as commuting measurements acting on a quantum state.

$$P\left(r_1 r_2 \ldots r_N \middle| m_1 m_2 \ldots m_N\right) = \mathrm{tr}\left(\rho\, M_{r_1}^{m_1} \otimes M_{r_2}^{m_2} \otimes \ldots \otimes M_{r_N}^{m_N}\right)$$

$$\left[M_{r_i}^{m_i}, M_{r'_i}^{m'_i}\right] = 0$$

Idea of the method

In the past, we designed a method to check if some correlations can be written as:

$$P\left(r_1 r_2 \ldots r_N \middle| m_1 m_2 \ldots m_N\right) = \mathrm{tr}\left(\rho\, M_{r_1}^{m_1} \otimes M_{r_2}^{m_2} \otimes \ldots \otimes M_{r_N}^{m_N}\right)$$

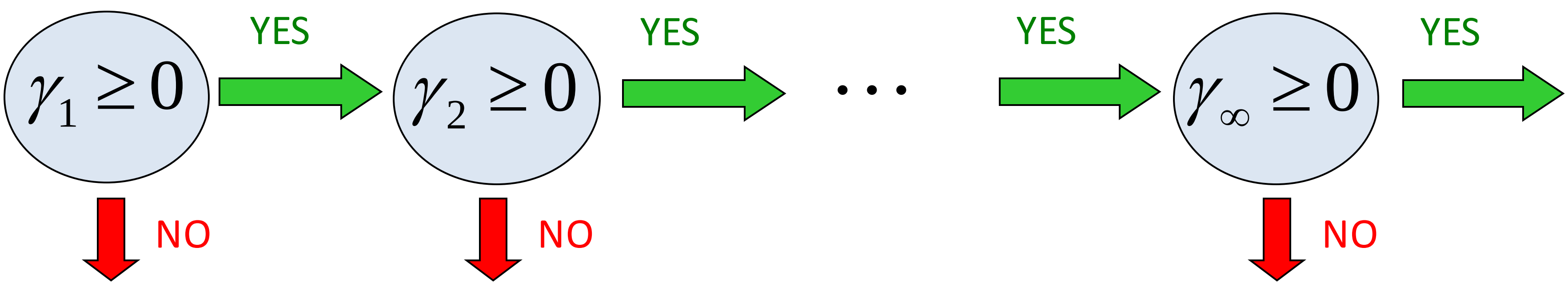
Idea of the method

In the past, we designed a method to check if some correlations can be written as:

$$P\left(r_1 r_2 \ldots r_N \middle| m_1 m_2 \ldots m_N\right) = \mathrm{tr}\left(r\, M_{r_1}^{m_1} \text{ Ä } M_{r_2}^{m_2} \text{ Ä} \ldots \text{Ä } M_{r_N}^{m_N}\right)$$

The method consists of a hierarchy of semi-definite programming (SDP) tests that become computationally more demanding. It is asymptotically convergent.

Navascués, Pironio, Acin, PRL 2007, NJP 2009



Idea of the method

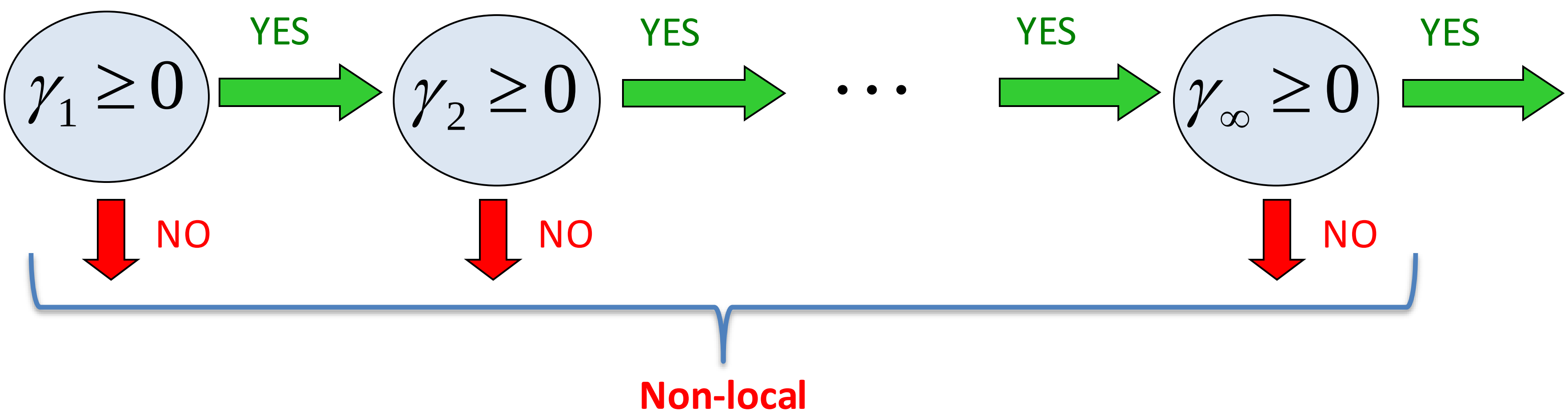
Now, it is rather easy to modify the method so that it incorporates the commutation relations among measurements on each system:

$$P\left(r_1 r_2 \ldots r_N \middle| m_1 m_2 \ldots m_N\right) = \mathrm{tr}\left(\rho M_{r_1}^{m_1} \otimes M_{r_2}^{m_2} \otimes \ldots \otimes M_{r_N}^{m_N}\right) \quad \left[M_{r_i}^{m_i}, M_{r'_i}^{m'_i}\right] = 0$$

Idea of the method

Now, it is rather easy to modify the method so that it incorporates the commutation relations among measurements on each system:

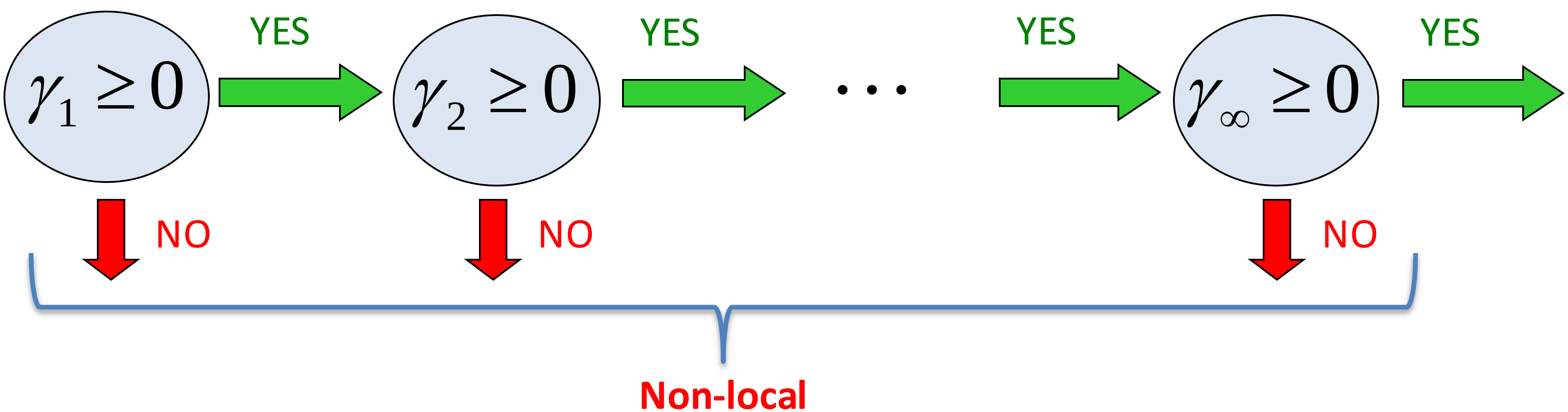
$$P\left(r_1 r_2 \ldots r_N \middle| m_1 m_2 \ldots m_N\right) = \mathrm{tr}\left(\rho\, M_{r_1}^{m_1} \otimes M_{r_2}^{m_2} \otimes \ldots \otimes M_{r_N}^{m_N}\right) \qquad \left[M_{r_i}^{m_i}, M_{r'_i}^{m'_i}\right] = 0$$



Idea of the method

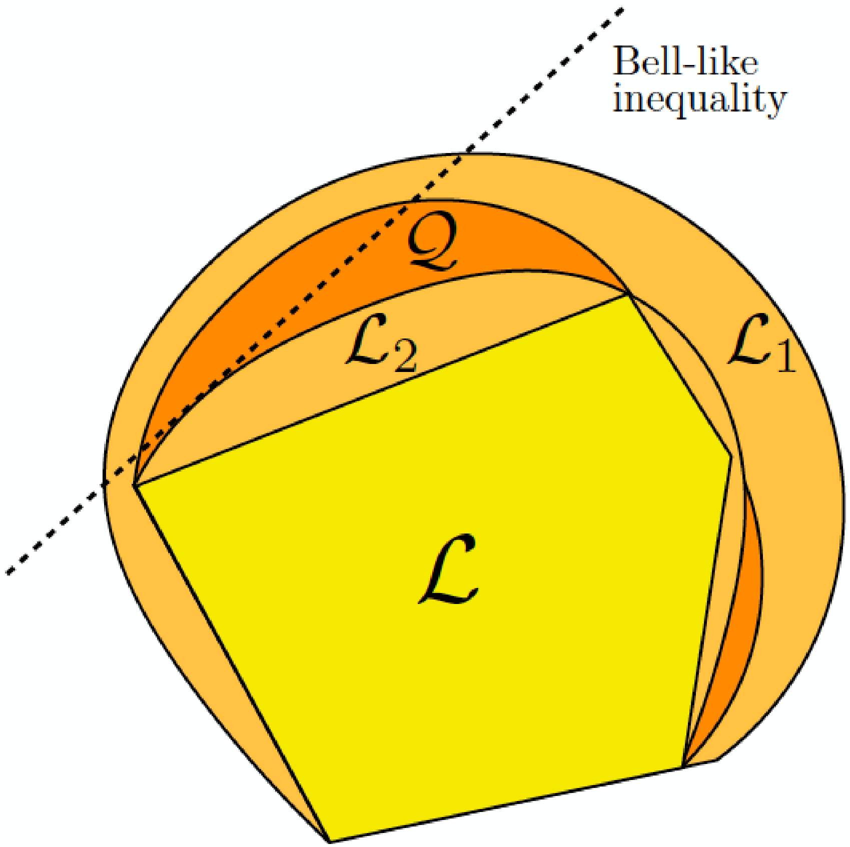
Now, it is rather easy to modify the method so that it incorporates the commutation relations among measurements on each system:

$$P\left(r_1 r_2 \ldots r_N \middle| m_1 m_2 \ldots m_N\right) = \mathrm{tr}\left(\rho M_{r_1}^{m_1} \otimes M_{r_2}^{m_2} \otimes \ldots \otimes M_{r_N}^{m_N}\right) \quad \left[M_{r_i}^{m_i}, M_{r'_i}^{m'_i}\right] = 0$$



It is also possible to modify the method so that it takes into account only partial and not the full statistics, e.g. only few-body correlation functions.

Idea of the method



- Any step in the hierarchy defines a tighter outer approximation to the set of local correlations.
- Deciding whether some observed correlations belong to a given set can be efficiently decided by SDP.
- When correlations are outside the set, it is possible to extract a Bell inequality certifying this.

Idea of the method

1. If a quantum state is separable then local measurements performed on it produce local correlations (i.e. correlations admitting a local model).

2. Any local correlations can be realized by performing commuting local measurements on a quantum state.

3. Correlations produced by commuting local measurements define a positive moment matrix with constraints associated to the commutation of all the measurements.

4. Our method consists in checking if the observed correlations are consistent with such positive moment matrix. In the negative case the correlations are certified to be nonlocal, and the state entangled in a device-independent way.

Application of the method

Detection of W state: $$|W\rangle = \frac{1}{\sqrt{N}}\left(|10\ldots0\rangle + |01\ldots0\rangle + \ldots + |00\ldots1\rangle\right)$$

Application of the method

Detection of W state: $$|W\rangle = \frac{1}{\sqrt{N}}\left(|10\ldots0\rangle + |01\ldots0\rangle + \ldots + |00\ldots1\rangle\right)$$

Local measurements: σ_X, σ_Z

Order of the correlation functions: 4 $$\left\langle \sigma_X^{(i)} \otimes \sigma_X^{(j)} \otimes \sigma_Z^{(k)} \otimes \sigma_X^{(l)} \right\rangle$$

Scalability of number of measurements: N^4

Robustness to white noise: $$(1-p)|W\rangle\langle W| + p\frac{1}{2^N}$$

Application of the method

Detection of W state: $$|W\rangle = \frac{1}{\sqrt{N}}\left(|10\ldots0\rangle + |01\ldots0\rangle + \ldots + |00\ldots1\rangle\right)$$

Local measurements: σ_X, σ_Z

Order of the correlation functions: 4

Scalability of number of measurements: N^4

Robustness to white noise: $$(1-p)|W\rangle\langle W| + p\frac{1}{2^N}$$

N	p_{max}	N	p_{max}	N	p_{max}
5	0.29	14	0.14	23	0.08
6	0.29	15	0.13	24	0.075
7	0.27	16	0.12	25	0.075
8	0.25	17	0.11	26	0.07
9	0.22	18	0.105	27	0.07
10	0.20	19	0.10	28	0.065
11	0.18	20	0.095	29	0.065
12	0.16	21	0.09		
13	0.15	22	0.085		

Results: the method detects the non-locality until 29 particles (possibly even more) with a resistance that decreases with the number of particles (6.5% for 29 particles).

Application of the method

Detection of GHZ state: $$|GHZ\rangle = \frac{1}{\sqrt{2}}\left(|00\ldots0\rangle + |11\ldots1\rangle\right)$$

Application of the method

Detection of GHZ state: $\left|GHZ\right\rangle = \frac{1}{\sqrt{2}}\left(\left|00\ldots0\right\rangle + \left|11\ldots1\right\rangle\right)$

Local measurements: σ_X, σ_D

Order of the correlation functions: 4 $\left\langle \sigma_X^{(i)} \otimes \sigma_X^{(j)} \otimes \sigma_X^{(k)} \otimes \sigma_D^{(l)} \right\rangle$

plus 2 full-body correlation functions. $\left\langle \sigma_X^{(1)} \otimes \sigma_X^{(2)} \otimes \ldots \otimes \sigma_X^{(N)} \right\rangle$

$$\left\langle \sigma_D^{(1)} \otimes \sigma_X^{(2)} \otimes \ldots \otimes \sigma_X^{(N)} \right\rangle$$

Scalability of number of measurements: N^4

Application of the method

Detection of GHZ state: $$\left|GHZ\right\rangle = \frac{1}{\sqrt{2}}\left(\left|00\ldots0\right\rangle + \left|11\ldots1\right\rangle\right)$$

Local measurements: S_X, S_D

Order of the correlation functions: 4

plus 2 full-body correlation functions.

Scalability of number of measurements: N^4

N	p_{max}	N	p_{max}	N	p_{max}
5	0.105	14	0.135	23	0.14
6	0.11	15	0.135	24	0.145
7	0.115	16	0.135	25	0.145
8	0.115	17	0.135	26	0.145
9	0.12	18	0.14	27	0.145
10	0.125	19	0.14	28	0.145
11	0.125	20	0.14	29	?
12	0.13	21	0.14		
13	0.13	22	0.14		

Results: the method detects the non-locality until 29 particles (possibly even more) with a resistance that seems to be constant and equal to 14.5%.

Conclusions

Device-independent quantum information processing

- Protocols
- Implementations

Information principles

Complexity aspects of quantum correlations

Quantum Foundations

- Generalized probabilistic theories
- Quantum vs supra-quantum correlations

Conclusions

Device-independent quantum information processing

- Protocols
- Implementations

Information principles

Complexity aspects of quantum correlations

Quantum Foundations

- Generalized probabilistic theories
- Quantum vs supra-quantum correlations

Many-body physics

- Non-locality of many-body states
- New methods for many-body simulation?

Beyond quantum theory?

- Decoherence functional approach to q physics
- Almost quantum theory?