Randomness and quantum non-locality

Antonio Acín
ICREA Professor at ICFO-Institut de Ciencies Fotoniques, Barcelona

QCRYPT 2012, Singapore, September 2012

Collaborators

Serge Massar

Stefano Pironio

Leandro Aolita

Gonzalo De la Torre

Chirag Dhara

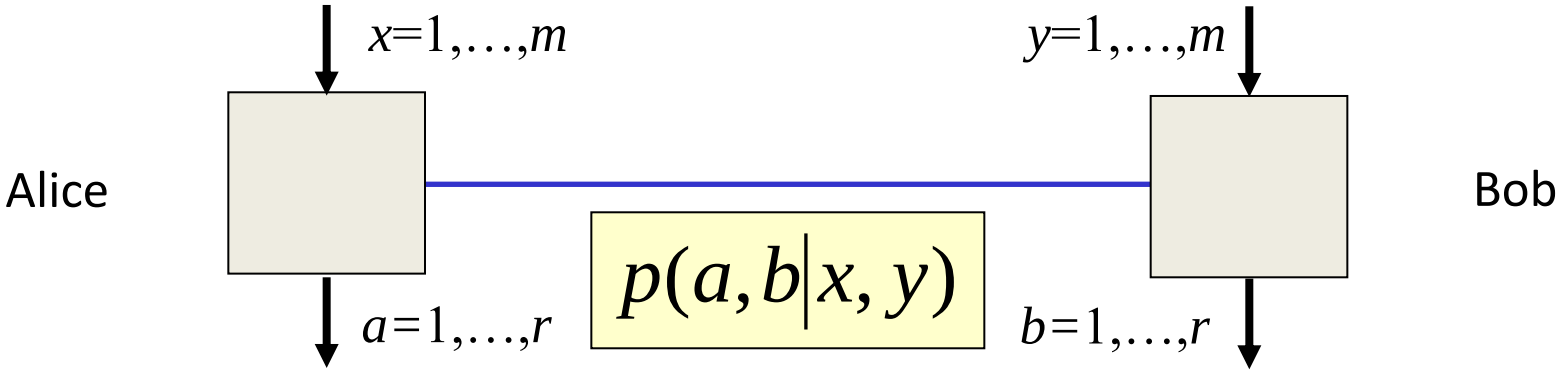
Rodrigo Gallego

Lluis Masanes

Giuseppe Prettico

Device-Independent Quantum Information Processing

Goal: to construct information protocols whose performance is independent of the internal working of the devices.

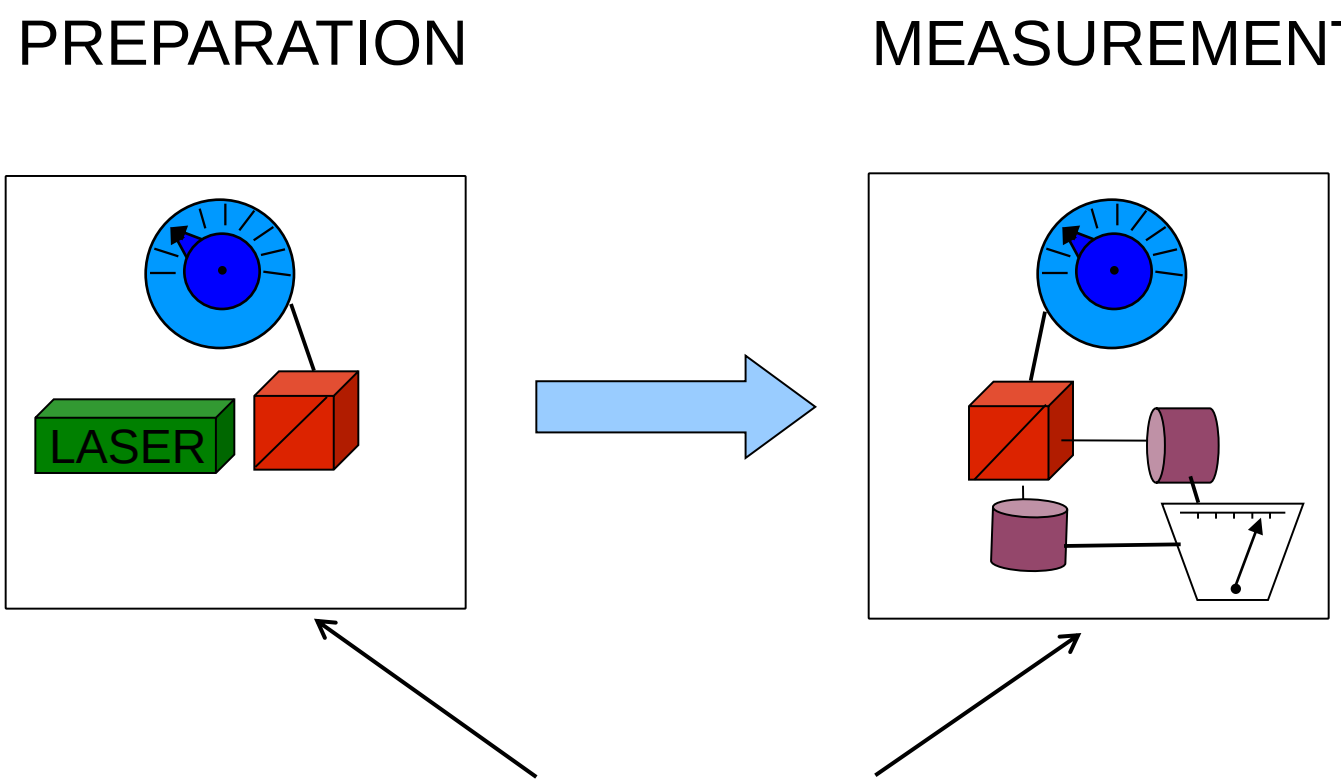


No assumption on the devices, which are seen as black-boxes producing a classical output given a classical input. It is however assumed that:

(i) the devices do not communicate during the input-output process

(ii) this process should be compatible with the laws of Nature / Quantum Physics.

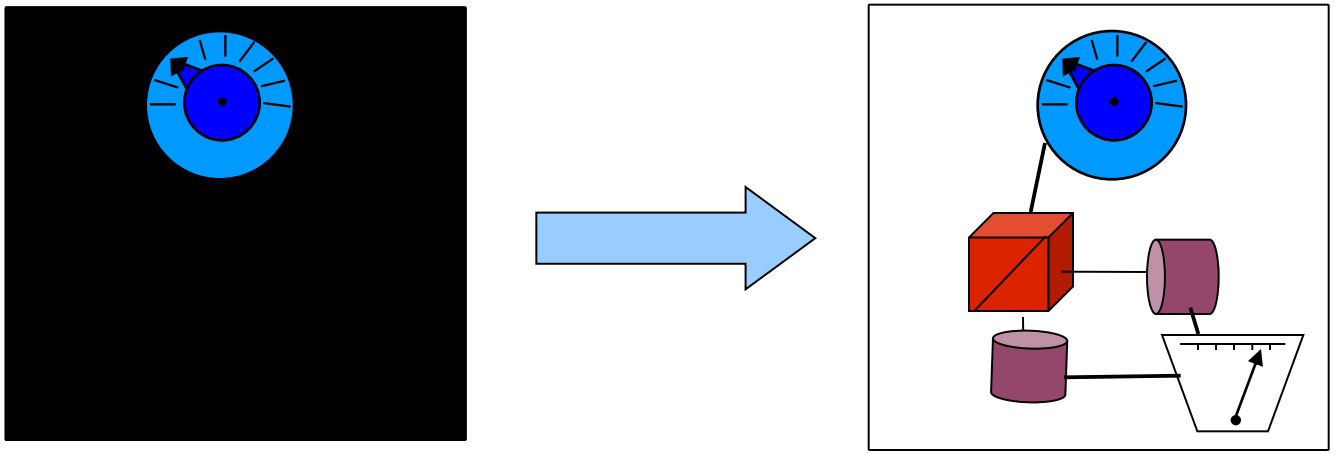
From standard to DI protocols



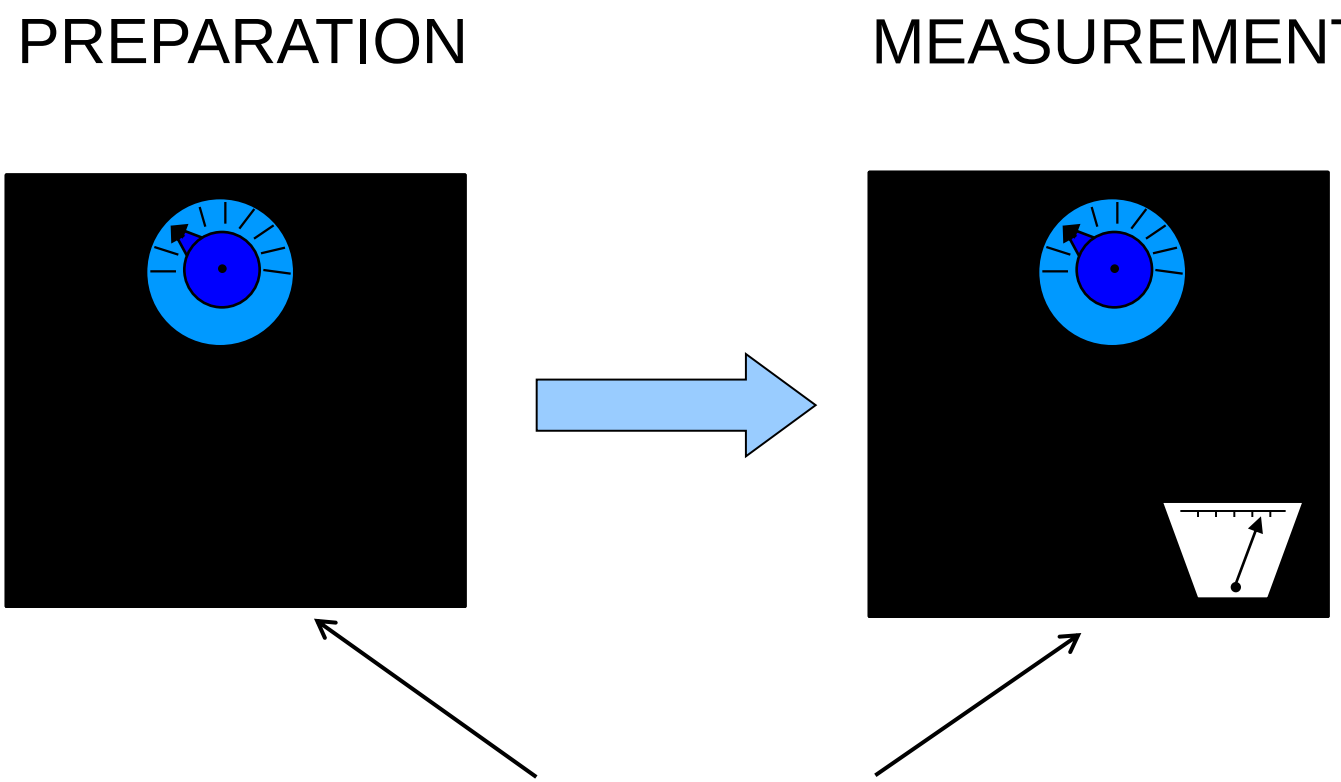
From standard to DI protocols

PREPARATION

MEASUREMENT



From standard to DI protocols



Physical Correlations

Physical principles translate into limits on correlations.

1) **Classical correlations**: correlations established by classical means.

$$p(a,b|x,y) = \sum_{\lambda} p(\lambda) p(a|x,\lambda) q(b|y,\lambda)$$

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

Physical Correlations

2) **Quantum correlations**: correlations established by quantum means.

$$p(a,b|x,y) = tr\left(\rho_{AB} M_a^x \otimes M_b^y\right)$$

$$\sum_a M_a^x = 1$$

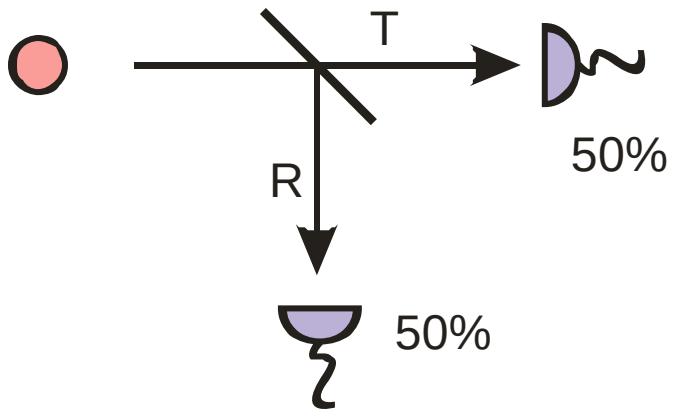
$$M_{a'}^x M_a^x = \delta_{aa'} M_a^x$$

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

$$\sum_b p(a,b|x,y) = p(a|x)$$

Randomness in quantum physics

Folklore: Quantum physics is random.
WHY?!



These two situations are in principle equivalent.

Randomness in classical physics

In the classical world, there is no such thing as true randomness. Any random process is simply a consequence of:

1) Imperfections in the preparation of the system and/or

2) Partial knowledge

Example:

If an observer has perfect knowledge of the initial position and speed of the ball and the size and shape of the roulette, the result can be predicted with certainty.

Randomness in classical physics

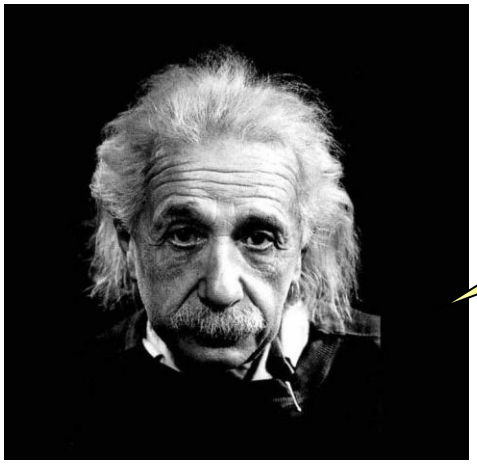
Randomness is, thus, a simple consequence of our limitations, for instance in our observation and computational capabilities, information storage and the preparation of the systems.

However, the theory does not incorporate any form of randomness. Given a perfect knowledge of the initial conditions in a system, it is in principle possible to predict its future (and past) behaviour.

LAPLACE

We may regard the present state of the universe as the effect of its past and the cause of its future. An intellect which at a certain moment would know all forces that set nature in motion, and all positions of all items of which nature is composed, if this intellect were also vast enough to submit these data to analysis, it would embrace in a single formula the movements of the greatest bodies of the universe and those of the tiniest atom; for such an intellect nothing would be uncertain and the future just like the past would be present before its eyes.

The EPR program



God does not play dice!

• After all, quantum randomness should have the same explanation as its classical counterpart: a consequence of noise or lack of knowledge.

• The fact that Quantum Physics is able to predict only the probabilities of events reflects the incompleteness of the theory.

• There should be another theory, not necessarily in contradiction with quantum physics, containing new variables not appearing in the quantum formalism. The knowledge of these, at the moment hidden, variables will make quantum randomness disappear.

Bell inequalities

In 1964, John Bell proved that theories à la EPR are incompatible with the correlations observed between entangled quantum particles. These correlations violate some conditions, in the form of inequalities, which are satisfied by all EPR models.

From the point of randomness, the experimental violation of any Bell inequality implies that a new form of randomness, intrinsic and not due to noise or lack of knowledge, is available in the quantum world.

Quantum physics is random because it is non-local.

Non-locality and randomness

Do non-local quantum correlations necessarily imply the existence of fully unpredictable processes in nature?

The answer to this question can be affirmative only if:

- No-signalling is assumed. Otherwise, Bohm's theory is a deterministic, yet signalling, theory that reproduces all quantum predictions.

- Some initial form of randomness is also assumed. If the choice of measurements in a Bell test is known in advance, it is possible to reproduce any Bell violation with a deterministic model.

Non-locality and randomness

Putting all these things together, the strongest possible result one can hope for relating randomness and quantum non-locality is:

Assuming the validity of the no-signalling principle and given an initial source of imperfect randomness, which can be arbitrarily small but non-zero, do non-local quantum correlations imply the existence of completely random processes in nature?

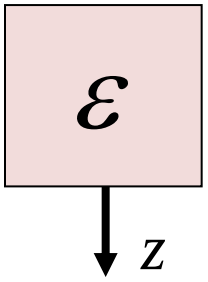
Yes! R. Gallego *et al.*, to be submitted.

We are left with a binary choice concerning randomness:
either our world is super-deterministic, in the sense that all actions, including the choice of measurements by different observers, have been pre-programmed, or there are provable completely unpredictable processes in nature.

Randomness amplification

Information task that aims at producing arbitrarily pure random bits from a source of imperfect random bits.

Santha-Vazirani (SV) source:



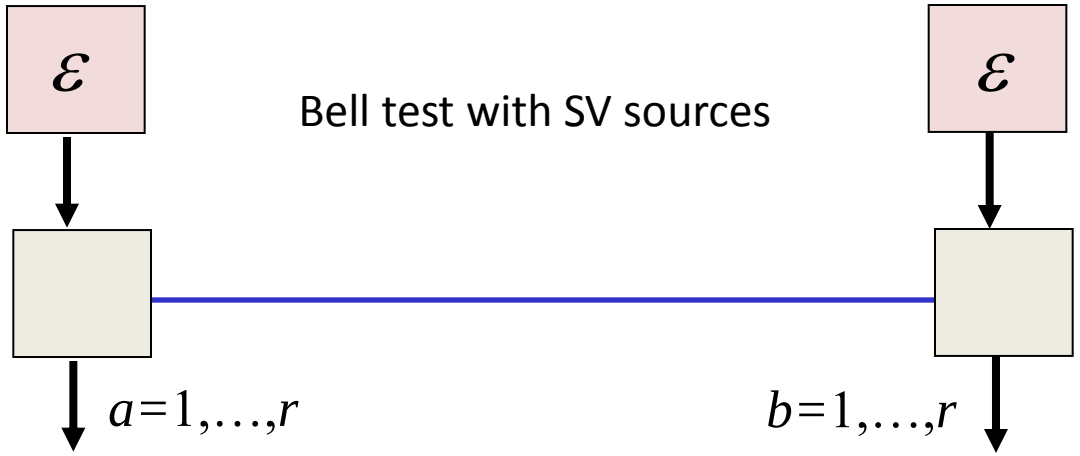
$$\frac{1}{2} - \varepsilon \leq \Pr\left(z = 0 \middle| \text{rest}\right) \leq \frac{1}{2} + \varepsilon$$

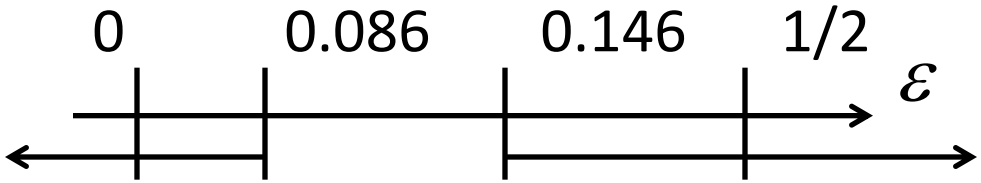
Randomness amplification: obtain a new SV source with $\varepsilon' \to 0$ by using the initial source with $\varepsilon > 0$. Efficiency issues are irrelevant.

Santha&Vazirani: randomness amplification is impossible classically.
Our work: full randomness amplification is possible using quantum non-locality.

Randomness amplification

Randomness amplification using quantum non-locality has first been considered by Colbeck and Renner (Nature Phys. 2012).





Full amplification

No amplification using the chained inequalities in the same limit.

Randomness amplification

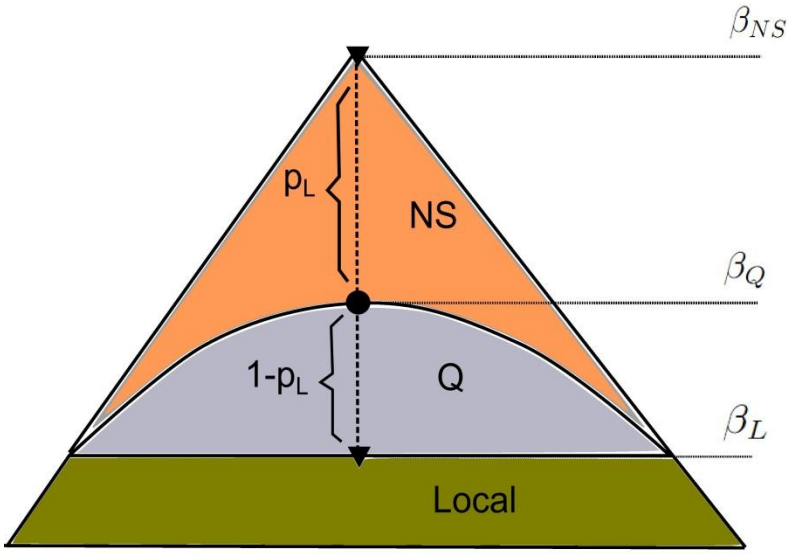
- It is convenient to adopt a cryptographic perspective and assume that the devices used for the Bell test have been prepared by an adversary using any non-signalling resource, that can even be supra-quantum.

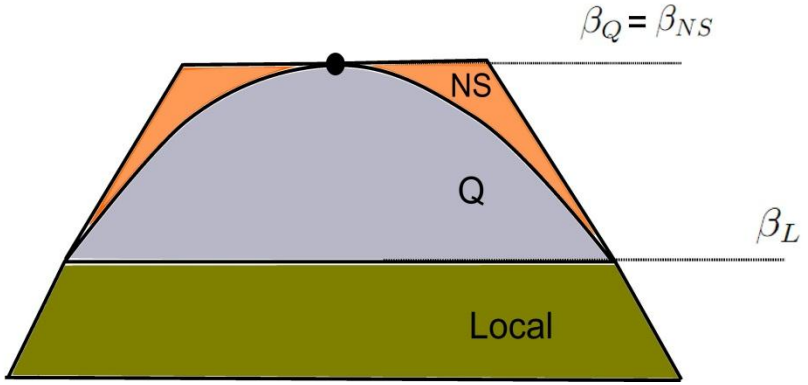
- In the preparation the adversary has also access to all pre-existing variables.

- Full randomness amplification is equivalent to proving that the adversary predictability on the final bits can be made arbitrarily small.

GHZ correlations

There exist quantum correlations that attain the maximal non-signalling violation of a Bell inequality. These correlations are known as GHZ.

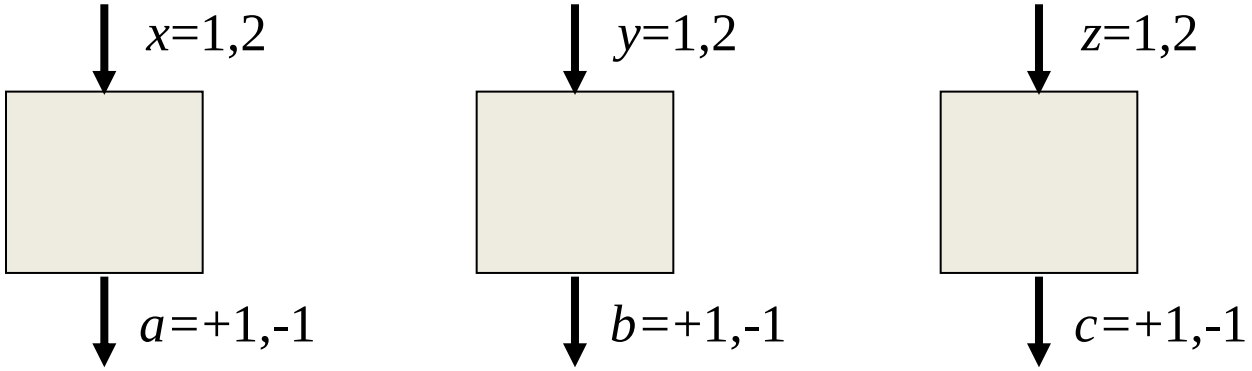




GHZ correlations, that is correlations with no local part, are necessary for full randomness amplification.

GHZ correlations

GHZ correlations however are not sufficient. Example: 3-party Mermin Bell inequality.

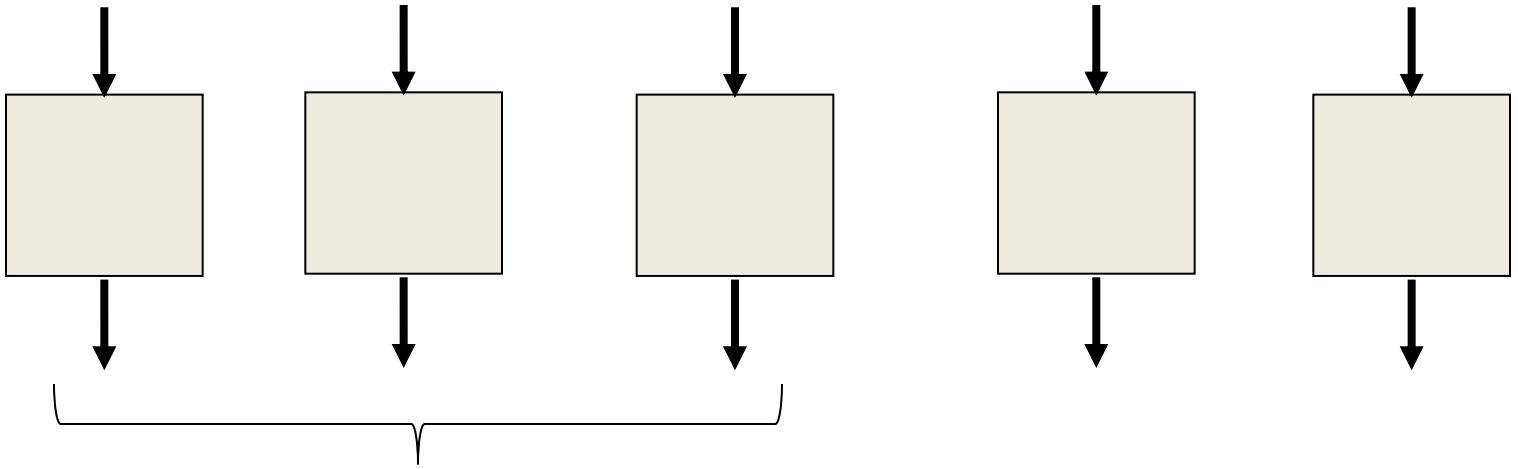


$$A_1B_1C_2 + A_1B_2C_1 + A_2B_1C_1 - A_2B_2C_2 \leq 2$$

An eavesdropper can fix any function of the outputs using non-signalling correlations that attain 4 in the previous Bell expression.

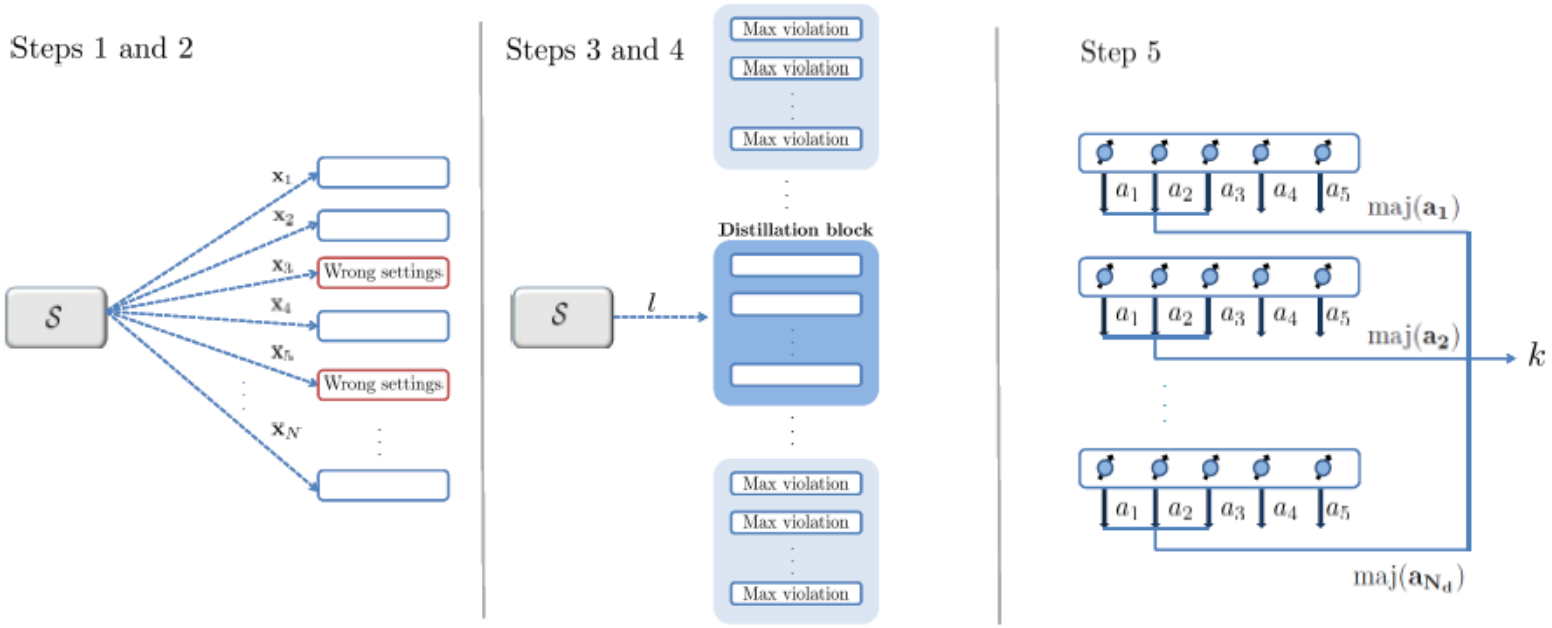
GHZ correlations

This result fails for larger number of parties. Example: 5-party Mermin Bell inequality.



An eavesdropper can predict the majority function of three of the outputs with probability not larger than 3/4. This implies that it is possible to get $\varepsilon' = 1/4$ from any SV source using the 5-party Mermin inequality.

Final protocol



The final protocol builds on this 5-party Bell test. By taking many instances of this Bell test we manage to:

(i) Show how ε' can be made arbitrarily small. We apply techniques introduced by Masanes for privacy amplification (PRL'11).

(ii) Include an estimation part that verifies the devices. We apply techniques introduced by Barrett, Hardy and Kent (PRL'05).

Quantum randomness

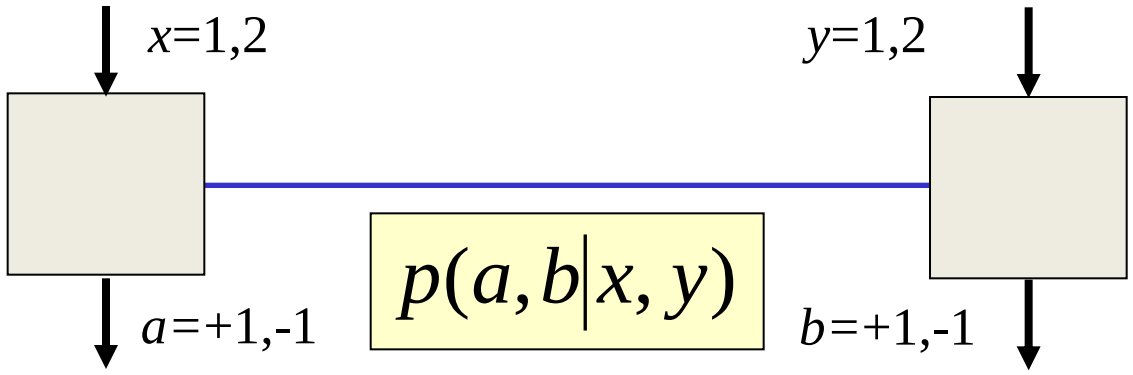
From the point of randomness, the experimental violation of any Bell inequality implies that a new form of randomness, intrinsic and not due to noise or lack of knowledge, is available in the quantum world.

How can we exploit this new form of randomness?

Beyond fundamental issues, randomness is an extremely valuable resource in our society with plenty of applications.

Randomness vs quantum non-locality

We want to explore the relation between non-locality, measured by the violation β of a Bell inequality, and local randomness, quantified by the parameter $r = \max_{a,x} p(a|x)$. Clearly, if $\beta = 0 \rightarrow r = 1$.

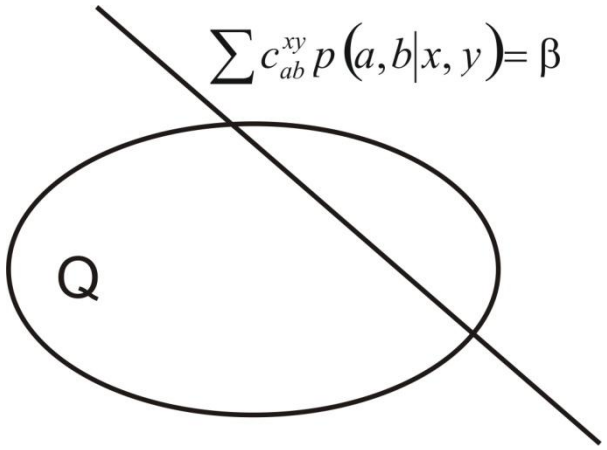


Randomness vs quantum non-locality

$$P_x = \max_a \; p(a|x)$$

$$p(a,b|x,y) \in Q$$

$$\sum c_{ab}^{xy} p(a,b|x,y) = \beta$$



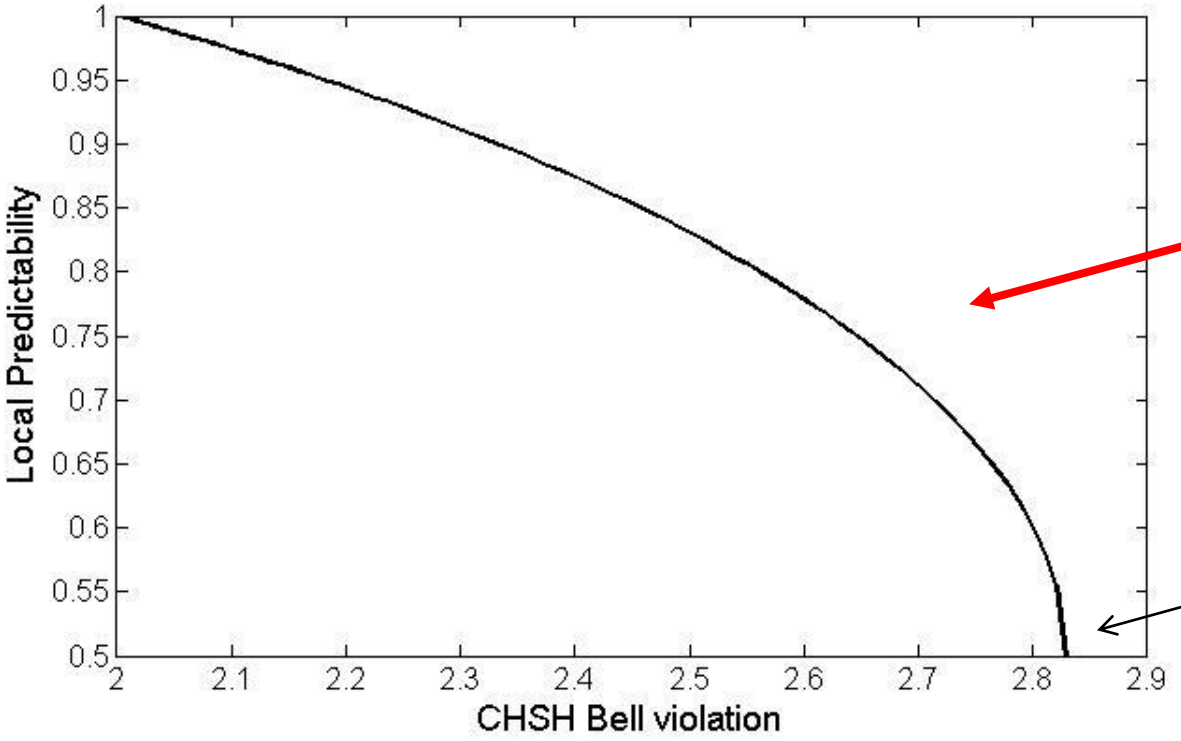
These bounds can be applied for Device-Independent

*) Randomness Generation (expansion), S. Pironio *et al.*, Nature 2010.

*) Quantum Key Distribution, Masanes, Pironio, Acin, Nature Comms 2011.

Randomness vs quantum non-locality

We can solve the previous optimization problem using the hierarchy of SDP conditions to bound quantum correlations of Navascues, Pironio, Acin, PRL 2007.



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

One pure random bit.

At the point of maximal violation the two outcomes define 1.23 bits of randomness.

Maximal randomness in Bell tests

$$\mathrm{CHSH} = \langle A_1 B_1 \rangle + \langle A_1 B_2 \rangle + \langle A_2 B_1 \rangle - \langle A_2 B_2 \rangle$$

At the point of maximal quantum violation, all local outcomes are random: $\langle A_1 \rangle = \langle A_2 \rangle = \langle B_1 \rangle = \langle B_2 \rangle = 0$.

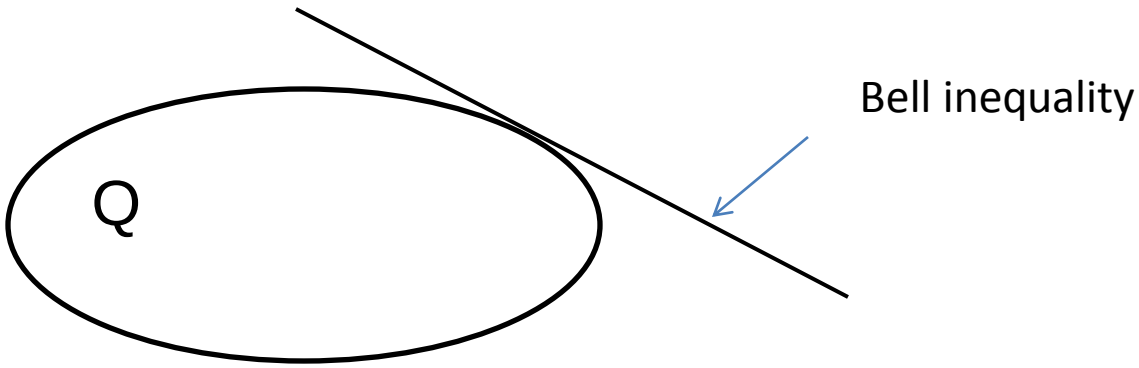
$$I_\beta = \langle A_1 B_1 \rangle + \langle A_1 B_2 \rangle + \langle A_2 B_1 \rangle - \langle A_2 B_2 \rangle + \beta \langle A_1 \rangle$$

At the point of maximal quantum violation, only the output of the second measurement by Alice is random: $\langle A_2 \rangle = 0$, Acin, Massar, Pironio, PRL 2012.

Why? When do Bell tests certify maximal randomness?

Simple argument

Assumption: the correlations attaining the maximal quantum violation are unique.



Simple argument

Consider some quantum correlations attaining the maximum violation of the CHSH inequality P_1. These correlations are equivalently defined by the value of all the correlators:

$$(\langle A_1\rangle, \langle A_2\rangle, \langle B_1\rangle, \langle B_2\rangle, \langle A_1B_1\rangle, \langle A_1B_2\rangle, \langle A_2B_1\rangle, \langle B_1B_2\rangle)$$

Consider the map: $A_i \to -A_i$ and $B_i \to -B_i$. Under this map, the previous correlations are mapped into P_2, defined by:

$$(-\langle A_1\rangle, -\langle A_2\rangle, -\langle B_1\rangle, -\langle B_2\rangle, \langle A_1B_1\rangle, \langle A_1B_2\rangle, \langle A_2B_1\rangle, \langle B_1B_2\rangle)$$

Note however that the two-party correlators remain unchanged, and so the CHSH value. But we assume that the correlations maximally violating the inequality are unique. Thus:

$$\langle A_1\rangle = \langle A_2\rangle = \langle B_1\rangle = \langle B_2\rangle = 0$$

Simple argument

Thus, uniqueness + symmetries → maximal randomness.

$$I_\beta = \langle A_1 B_1 \rangle + \langle A_1 B_2 \rangle + \langle A_2 B_1 \rangle - \langle A_2 B_2 \rangle + \beta \langle A_2 \rangle$$

Transform $A_2 \to -A_2$:

$$I_\beta = \langle A_1 B_1 \rangle + \langle A_1 B_2 \rangle - \langle A_2 B_1 \rangle + \langle A_2 B_2 \rangle + \beta \langle A_1 \rangle$$

Exchange $B_1 \leftrightarrow B_2$:

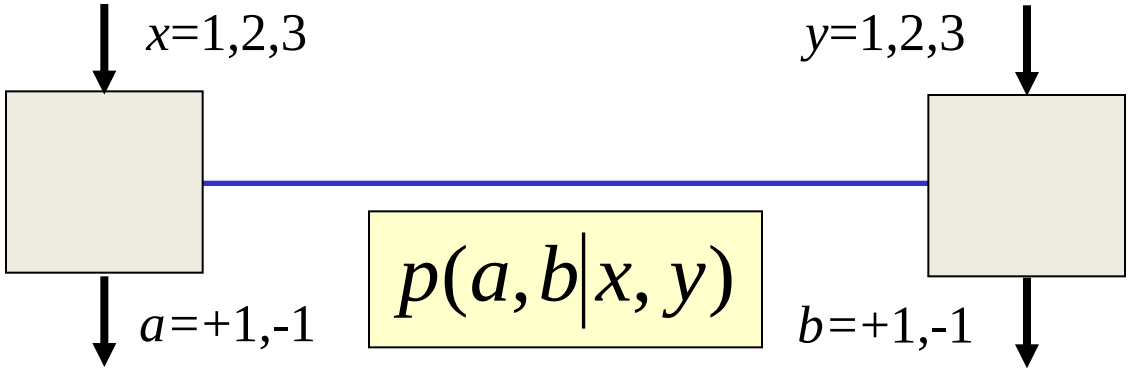
$$I_\beta = \langle A_1 B_2 \rangle + \langle A_1 B_1 \rangle - \langle A_2 B_2 \rangle + \langle A_2 B_1 \rangle + \beta \langle A_1 \rangle$$

The value of the inequality remains unchanged: $\langle A_2 \rangle$=0.

Certified maximal randomness

Question: is there any N-party Bell test in which the binary outcomes of some measurements define N bits?

Yes. Joint work with De la Torre, Dhara, Prettico, in preparation.



$$p(a_1 = b_1) + p(b_1 = a_2) + p(a_2 = b_2) + p(b_2 = a_3) + p(a_3 = b_3) + p(b_3 \neq a_1) \leq 5$$

At the point of maximal quantum violation, a_1 and b_2 define two pure random bits. This result has been certified by the SDP hierarchy.

Certified maximal randomness

- We have examples of N parties, with odd N, generating N random bits.
- We have proven that if general non-signalling correlations become available, it is impossible to certified N bits of randomness.
- The maximum amount of randomness that can be certified in a Bell test against non-signalling eavesdroppers is bounded by $1/(2^N - 1)$.
- If the theory is maximally non-local, maximal randomness cannot be certified. The bounded non-locality of quantum physics allows one to certify maximal randomness.
- Quantum physics is random because non-local. Now, it is not maximally non-local because it is maximally random.

Randomness amplification

- Randomness amplification: produce bits of arbitrarily high randomness from bits of imperfect randomness.
- Full randomness amplification is possible using quantum non-locality.
- Assuming non-signalling, either our world is super-deterministic, in the sense that all actions, including the choice of measurements by different observers, have been pre-programmed, or there are provable completely unpredictable processes in nature.
- Simpler schemes? Bipartite scenario?
- How does noise affect these results?
- Randomness amplification against quantum eavesdroppers?

Randomness and correlations

- There exist quantum correlations that allow one to certify that the measurement results by N parties define N random bits.
- Maximal randomness certification is impossible for general non-signalling correlations.
- What's the maximal amount of randomness that can be certified in a general non-signalling theory?
- Are there other non-signalling theories, apart from quantum physics, that permit maximal randomness certification?

ICFOnest program

ICFOnest post-doctoral program: it aims at providing high-level training and support for outstanding international researchers in the early stages of their careers.

Deadline: September 30 2012, **last call!**

http://nestpostdocs.icfo.es/