True Quantum Randomness

Antonio Acín
ICREA Professor at ICFO-Institut de Ciencies Fotoniques, Barcelona
Serge Massar and Stefano Pironio
Université Libre de Bruxelles, Brussels

Is Science Compatible with our Desire of Freedom?
Social Trends Institute, Barcelona, October 2010

¿Does randomness exist in our macroscopic world?

Randomness in the macroscopic world

In the macroscopic 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 the macroscopic world

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.

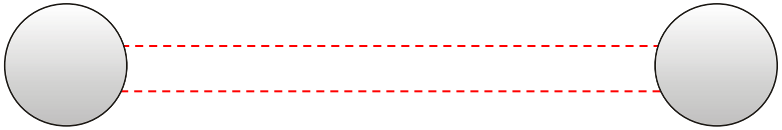
LAPLACE

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.

¿What happens when we move to the microscopic world?

Randomness in the quantum world

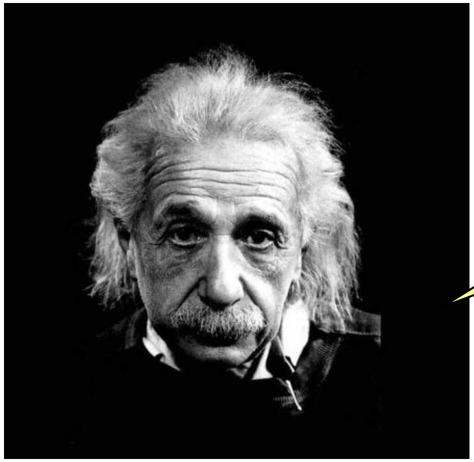
Entanglement: quantum correlated particles when measured give raise to correlations that are classically impossible.



1. The results of local measurements on each particle appear to be random.
2. However, the results on each particle coincide, independently of the distance between the two particles.

In 1935, Einstein, Podolsky and Rosen (EPR) published an article in Physical Review where they suggested the existence of a classical theory, alternative to Quantum Physics and to be discovered, in which these correlations could be explained in a more satisfactory way, without randomness and action at a distance.

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 an alternative theory, not necessarily in contradiction with the quantum predictions, containing new variables not appearing in the quantum formalism. The knowledge of these, at the moment hidden, variables will make quantum randomness disappear. Let’s look for this theory!

Bell inequalities

Hmm, actually EPR theories are in contradiction with Quantum Physics...

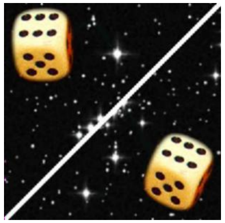
In 1964, John Bell proved that theories à la EPR are incompatible with the correlations observed between entangled quantum particles. These correlations violate some conditions, in the form of inequalities, which are satisfied by all EPR models.

If one observes the violation of a Bell inequality → the EPR program is impossible.

Experimental Bell inequality violation

In 1982, Alain Aspect, in Orsay, performed a conclusive experiment proving the violation of a Bell inequality. The EPR program of a classical-like theory alternative to Quantum Physics has to be abandon.

Since then, plenty of experiments have been done confirming the validity of Quantum Physics and falsifying the EPR models. These correlations, with no classical analogue, are now at our disposal.



Quantum Randomness

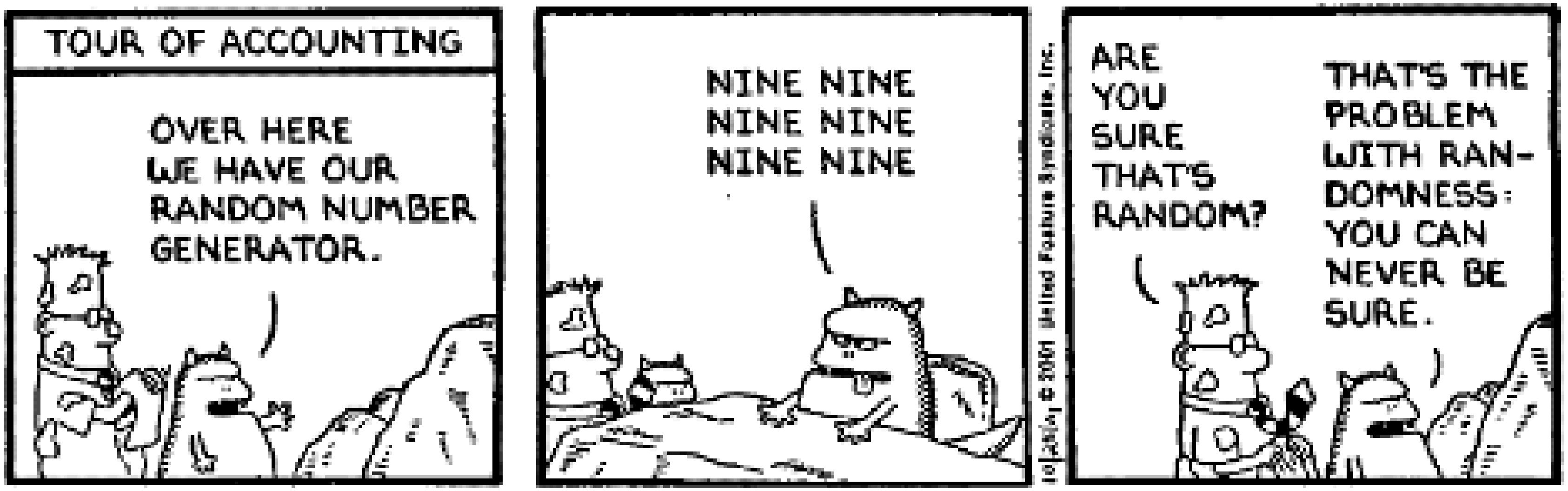
From the point of randomness, the experimental violation of any Bell inequality implies that a new form of randomness, intrinsic and not due to noise or lack of knowledge, is available in the quantum world.

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.

Random Numbers Certified by Bell’s Theorem

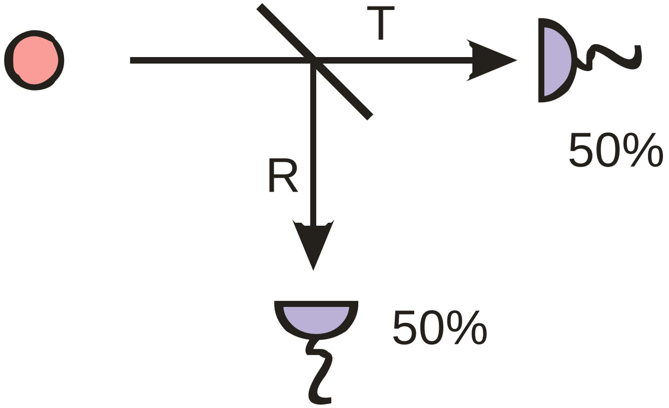
S. Pironio, A. Acin, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning and C. Monroe, Nature 464, 1021 (2010)


TOUR OF ACCOUNTING
OVER HERE WE HAVE OUR RANDOM NUMBER GENERATOR.
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 RANDOMNESS: YOU CAN NEVER BE SURE.

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

Known solutions

- Classical Random Number Generators (CRNG). All of them are of deterministic Nature.
- Quantum Random Number Generators (QRNG). There exist different solutions, but the main idea is encapsulated by the following example:



Single photons are prepared and sent into a mirror with transmittivity equal to ½. The random numbers are provided by the clicks in the detectors.

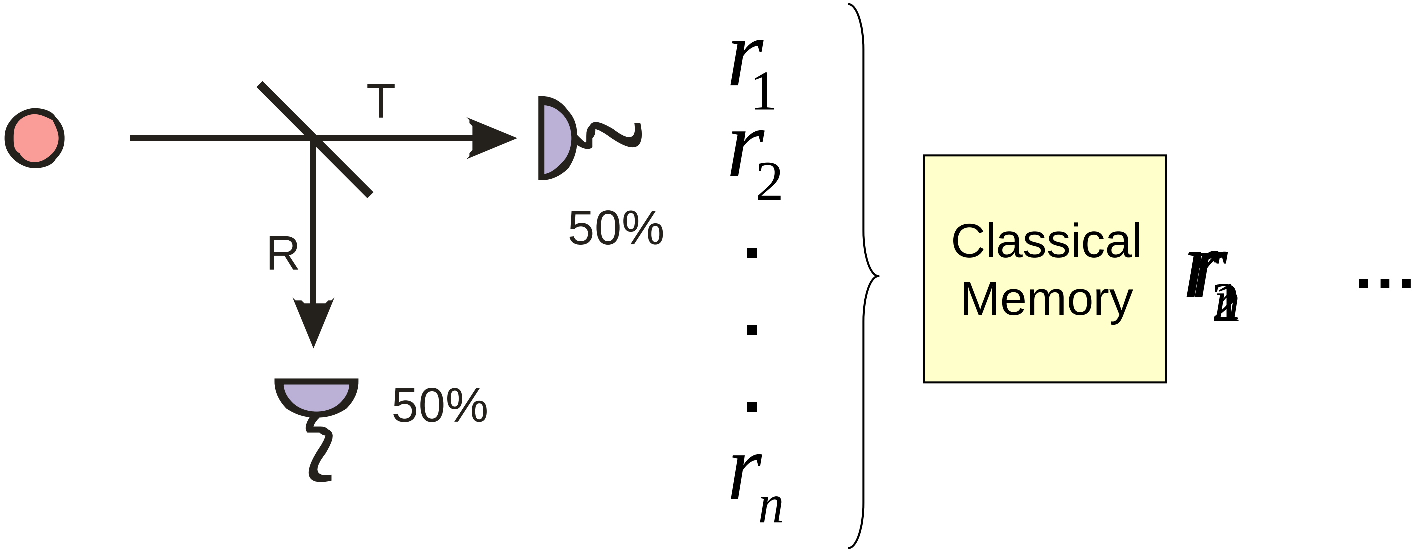
- In any case, all these solutions have three problems, which are important both from a fundamental and practical point of view.

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?
- Do these tests certify any form of quantum randomness? Classical systems pass them!

Problem 2: privacy

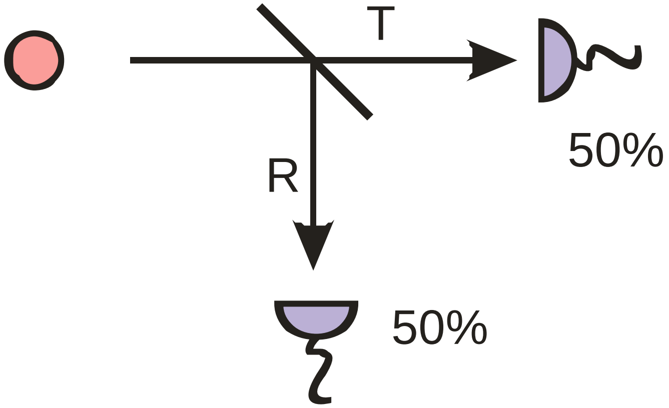
- Many applications require private randomness.



- How can one be sure that the observed random numbers are also random to any other observer, possibly adversarial?

Problem 3: device dependence

- All the solutions crucially rely on the details of the devices used in the generation.



Single photons are prepared and sent into a mirror with transmittivity equal to ½. The random numbers are provided by the clicks in the detectors.

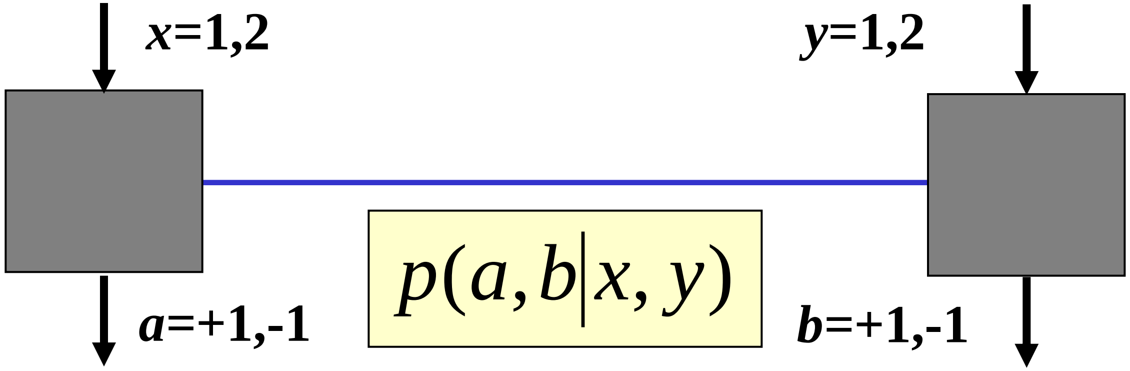
- How can imperfections in the devices affect the quality of the generated numbers? Can these imperfections be exploited by an adversary?

Random Numbers from Bell’s Theorem

- Randomness can be derived from non-local quantum correlations.
- The obtained randomness is certifiable, private and device-independent.
- It represents a novel application of Quantum Information Theory, solving a task whose classical realization is, at least, unclear.
- These techniques allow quantifying the intrinsic quantum randomness generated in Bell tests.

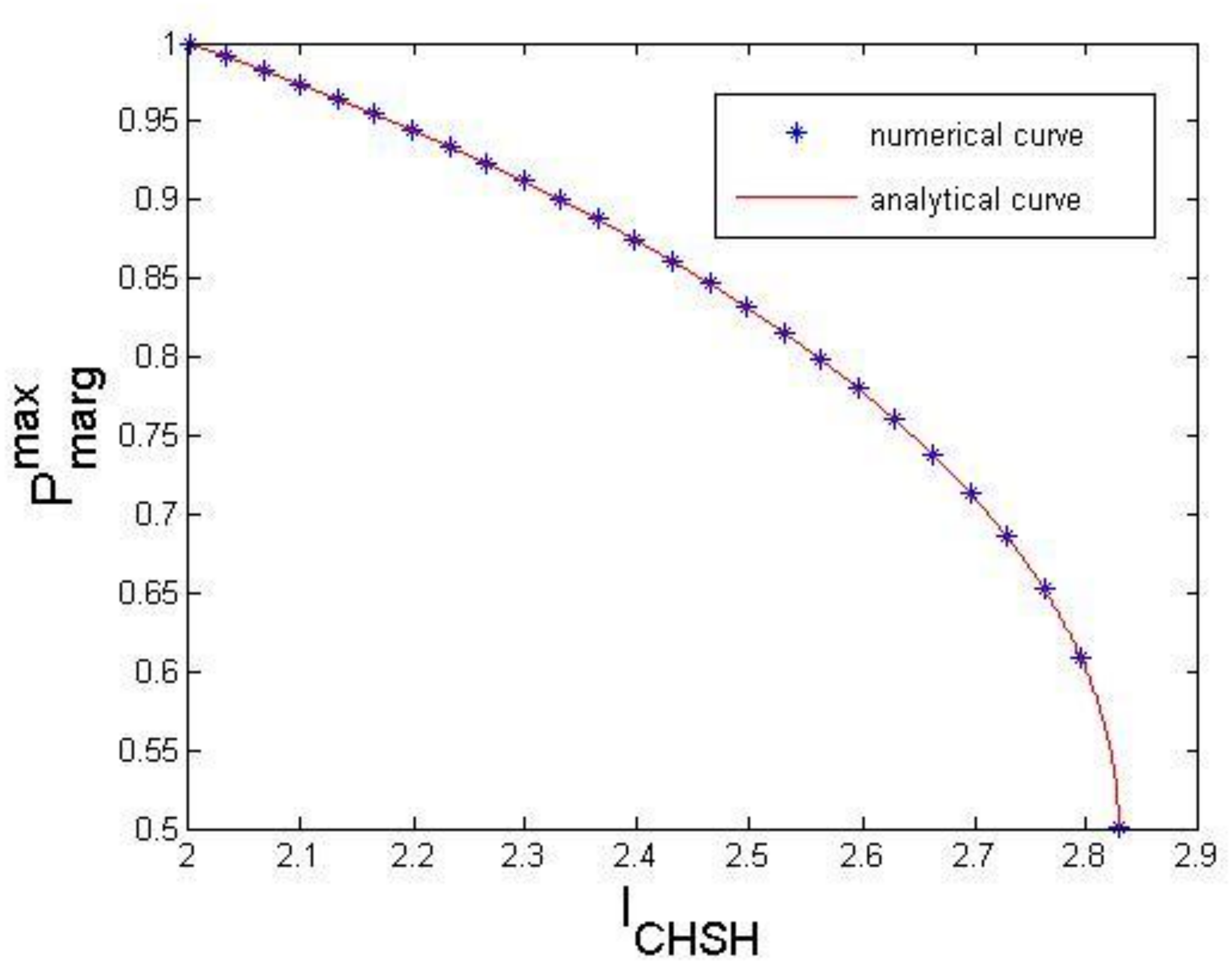
Random Numbers from Bell’s Theorem

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

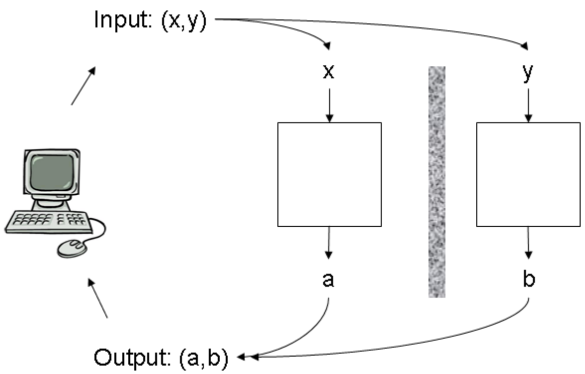


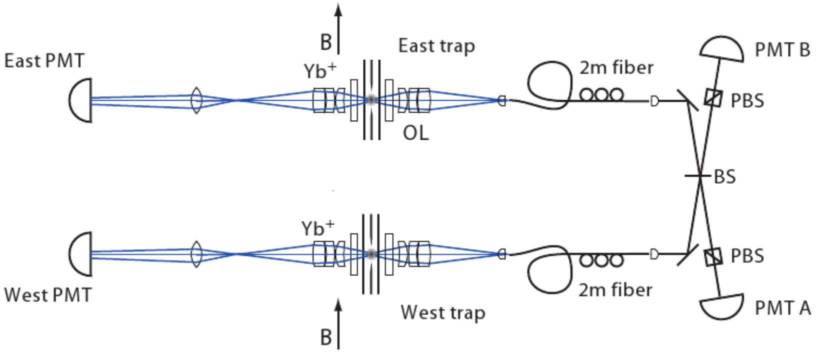
ICFO Institut de Ciències Fotòniques

Results



Experimental realization





- The two-box scenario is performed by two atomic particles located in two distant traps.
- Using our theoretical techniques, we can certify that 42 new random bits are generated in the experiment.
- It is the first time that randomness generation is certified without making any detailed assumption about the internal working of the devices.

Concluding Remarks

Non-locality, randomness and no-signalling

No-signalling principle: information does not propagate instantaneously.

Non-locality + Determinism → Signalling

The experimental observation of Bell inequalities imply that our world is either random or allows signalling (or both). It is a matter of choice!

Non-locality depend on the fact that measurements are unknown in advance. In the ultimate limit, this is due to the free will of the observers.

Free Will + Determinism → Signalling

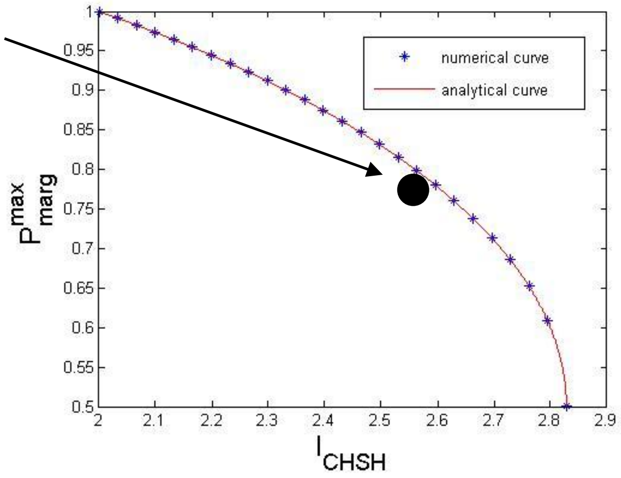
Take-home question

(C or Q)RNG

DIQRNE

Specifications: it passes all statistical randomness tests.

Specifications:



It won’t pass all the existing randomness tests!

Which device is more random?