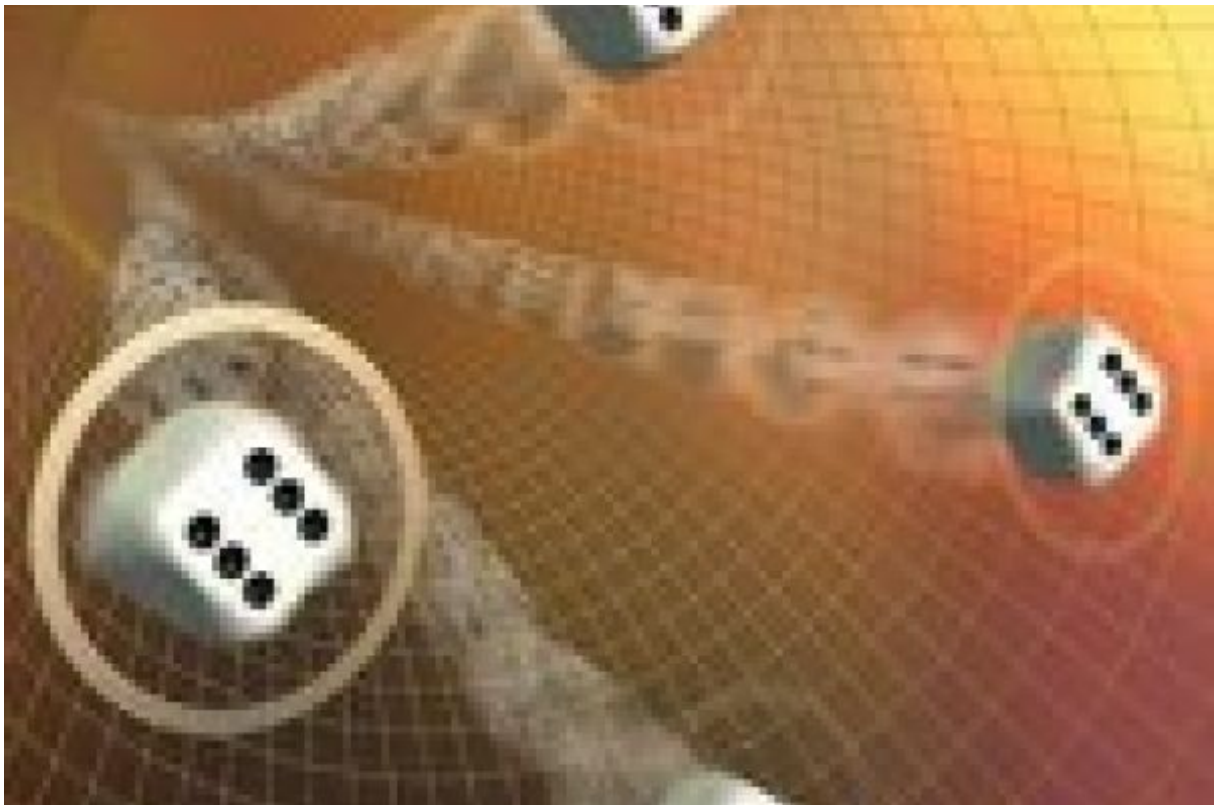

True Randomness in Nature

Nature publishes the first certification of intrinsic quantum randomness by a team including ICFO Prof. Antonio Acin.

April 15, 2010

Getting *Random Numbers Certified by Bell?s Theorem* means that you are able to obtain with no trace of a doubt a truly random sequence of numbers using the most intrinsic quantum feature: non-local correlations of entangled quantum particles, which violates Bell?s inequalities.

In nature we can only find intrinsic randomness in quantum processes. In the classical world, any process is deterministic and what we normally take as randomness is simply consequence of lack of knowledge or control. Still, *ascertaining* the random behaviour of a physical process, even if quantum, represents a remarkably difficult problem. Until now, no device was designed that could certify true randomness in a process.

Now an international team of researchers including ICFO Prof. Antonio Acin describes in Nature how to detect and quantify the intrinsic quantum randomness of a device using the non-local correlations present in entangled quantum states. The team is completed by Dr. Stefano Pironio, and Dr. Serge Massar, from the Universite Libre de Bruxelles, Belgium; Antoine Boyer de la Giroday, from the Cavendish Laboratory, UK; and Dr. Dmitri Matsukevich, Dr. Peter Maunz, Dr. Steve Olmschenk, Dave Hayes, Dr. Le Luo, Andrew Manning, and Prof. Chris Monroe from the University of Maryland, USA.

These results can be exploited to design a novel type of random number generator with no classical analogue. This device produces random numbers which are: certified by Bell?s Theorem; private; and device-independent, in the sense that their random features do not depend on the internal functioning of the devices used in their generation. None of these fundamental properties were met by any of the existing proposals for randomness generation, either classical or quantum.

The authors illustrate their theoretical approach in a Bell test experiment involving two atoms in two distant traps. Using their formalism, they certify for the first time that randomness is produced in an experiment, without requiring detailed knowledge of the inner-workings of the devices involved in it.