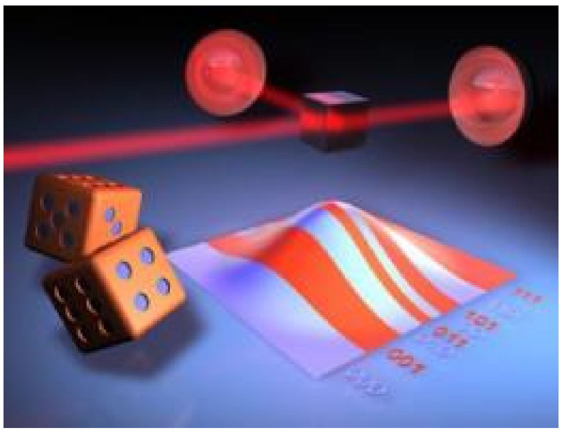
Random numbers game with quantum dice

September 9 2010



A true game of chance: Max Planck researchers produce true random numbers by making the randomly varying intensity of the quantum noise visible. To do this, they use a strong laser (coming from the left), a beam splitter, two identical detectors and several electronic components. The statistical spread of the measured values follows a Gaussian bell-shaped curve (bottom). Individual values are assigned to sections of the bell-shaped curve that correspond to a number. Credit: Max Planck Institute

(PhysOrg.com) -- A simple device measures the quantum noise of vacuum fluctuations and generates true random numbers.

Behind every coincidence lies a plan - in the world of classical physics, at least. In principle, every event, including the fall of dice or the outcome of a game of roulette, can be explained in mathematical terms. Researchers at the Max Planck Institute for the Physics of Light in Erlangen have constructed a device that works on the principle of true randomness. With the help of quantum physics, their machine generates random numbers that cannot be predicted in advance. The researchers exploit the fact that measurements based on quantum physics can only produce a special result with a certain degree of probability, that is, randomly. True random numbers are needed for the secure encryption of data and to enable the reliable simulation of economic processes and changes in the climate. (Nature Photonics online publication, August 29, 2010)

The phenomenon we commonly refer to as chance is merely a question of a lack of knowledge. If we knew the location, speed and other classical characteristics of all of the particles in the universe with absolute certainty, we would be able to predict almost all processes in the world of everyday experience. It would even be possible to predict the outcome of a puzzle or lottery numbers. Even if they are designed for this purpose, the results provided by computer programs are far from random: "They merely simulate randomness but with the help of suitable tests and a sufficient volume of data, a pattern can usually be identified," says Christoph Marquardt. In response to this problem, a group of researchers working with Gerd Leuchs and Christoph Marquardt at the Max Planck Institute for the Physics of Light and the University of Erlangen-Nuremberg and Ulrik Andersen from the Technical University of Denmark have developed a generator for true random numbers.

True randomness only exists in the world of quantum mechanics. A quantum particle will remain in one place or another and move at one speed or another with a certain degree of probability. "We exploit this randomness of quantum-mechanical processes to generate random numbers," says Christoph Marquardt.

The scientists use vacuum fluctuations as quantum dice. Such fluctuations are another characteristic of the quantum world: there is nothing that does not exist there. Even in absolute darkness, the energy of a half photon is available and, although it remains invisible, it leaves tracks that are detectable in sophisticated measurements: these tracks take the form of quantum noise. This completely random noise only arises when the physicists look for it, that is, when they carry out a measurement.

To make the quantum noise visible, the scientists resorted once again to the quantum physics box of tricks: they split a strong laser beam into equal parts using a beam splitter. A beam splitter has two input and output ports. The researchers covered the second input port to block light from entering. The vacuum fluctuations were still there, however, and they influenced the two partial output beams. The physicists then send them to the detectors and measure the intensity of the photon stream. Each photon produces an electron and the resulting electrical current is registered by the detector.

When the scientists subtract the measurement curves produced by the two detectors from each other, they are not left with nothing. What remains is the quantum noise. "During measurement the quantum-mechanical wave function is converted into a measured value," says Christian Gabriel, who carried out the experiment with the random generator with his colleagues at the Max Planck Institute in Erlangen: "The statistics are predefined but the intensity measured remains a matter of pure chance." When plotted in a Gaussian bell-shaped curve, the weakest values arise frequently while the strongest occur rarely. The researchers divided the bell-shaped curve of the intensity spread into sections with areas of equal size and assigned a number to each section.

Needless to say, the researchers did not decipher this quantum mechanics puzzle to pass the time during their coffee breaks. "True random numbers are difficult to generate but they are needed for a lot of applications," says Gerd Leuchs, Director of the Max Planck Institute for the Physics of Light in Erlangen. Security technology, in particular, needs random combinations of numbers to encode bank data for transfer. Random numbers can also be used to simulate complex processes whose outcome depends on probabilities. For example, economists use such Monte Carlo simulations to predict market developments and meteorologists use them to model changes in the weather and climate.

There is a good reason why the Erlangen-based physicists chose to produce the random numbers using highly complex vacuum fluctuations rather than other random quantum processes. When physicists observe the velocity distribution of electrons or the quantum noise of a laser, for example, the random quantum noise is usually superimposed by classical noise, which is not random. "When we want to measure the quantum noise of a laser beam, we also observe classical noise that originates, for example, from a shaking mirror," says Christoffer Wittmann who also worked on the experiment. In principle, the vibration of the mirror can be calculated as a classical physical process and therefore destroys the random game of chance.

"Admittedly, we also get a certain amount of classical noise from the measurement electronics," says Wolfgang Mauerer who studied this aspect of the experiment. "But we know our system very well and can calculate this noise very accurately and remove it." Not only can the quantum fluctuations enable the physicists to eavesdrop on the pure quantum noise, no one else can listen in. "The vacuum fluctuations provide unique random numbers," says Christoph Marquardt. With other quantum processes, this proof is more difficult to provide and the danger arises that a data spy will obtain a copy of the numbers. "This is precisely what we want to avoid in the case of random numbers for data keys," says Marquardt.

Although the quantum dice are based on mysterious phenomena from the quantum world that are entirely counterintuitive to everyday experience, the physicists do not require particularly sophisticated equipment to observe them. The technical components of their random generator can be found among the basic equipment used in many laser laboratories. "We do not need either a particularly good laser or particularly expensive detectors for the set-up," explains Christian Gabriel. This is, no doubt, one of the reasons why companies have already expressed interest in acquiring this technology for commercial use.

More information: Christian Gabriel, Christoffer Wittmann, Denis Sych, Ruifang Dong, Wolfgang Mauerer, Ulrik L. Andersen, Christoph Marquardt und Gerd Leuchs, A generator for unique quantum random numbers based on vacuum states. *Nature Photonics*, online publication August 29, 2010

Provided by Max-Planck-Gesellschaft