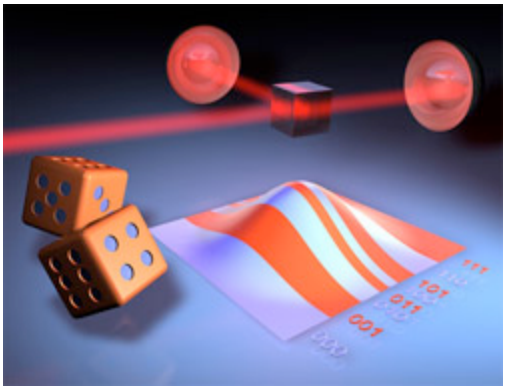
Physicists claim first true random number generation

Sept. 13, 2010
Courtesy of the Max Planck Society,
the University of Maryland
and World Science staff

Seemingly random events seen in daily life, such as the results of dice throws, actually have definite causes that determine them exactly. So they are not really random. This is true for objects that are at least large enough to see with ordinary microscopes; such objects follow the laws of what is known as "classical" physics.

But in the realm of quantum physics—the rules that govern atoms or smaller objects—it's not unusual to find events that, by all measures, are truly random. In other words, they cannot be predicted no matter how much you know about what led to up to them.



Max Planck researchers reported that they used a strong laser (coming from the left), a beam splitter, two detectors and some electronic components in their setup. The detectors were used to measure the randomly varying intensity of the quantum noise. The statistical spread of the measured values follows a bell-shaped or "Gaussian" curve (bottom). Individual values were assigned to sections of the bell-shaped curve that correspond to a number. (Courtesy MPI for the Physics of Light)

This year, for the first time, scientists have built devices that exploit quantum physics to generate what they say are real random numbers. Such numbers can't be obtained even with ordinary computers, which can simulate randomness but not really produce it.

True random numbers can be useful to securely encrypt data and to simulate economic processes and climate changes, among other things.

One set of new findings was reported in the Aug. 29 online issue of the research journal *Nature Photonics*. The researchers exploited the fact that measurements based on quantum physics can only produce a specific result with a certain probability, that is, randomly.

The phenomenon we commonly refer to as chance is merely a result of a lack of knowledge. If we knew the location, speed and other characteristics of all of the particles in the universe with absolute certainty, according to classical physics we could predict everything, including dice throws and lottery results.

By the same token, computer-generated random numbers "simulate randomness, but with the help of suitable tests and a sufficient volume of data, a pattern can usually be identified," said researcher Christoph Marquardt of the Max Planck Institute for the Physics of Light in Erlangen, Germany.

True randomness only exists in quantum physics. 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[ed] this randomness of quantum-mechanical processes to generate random numbers," said Marquardt.

He and a group of colleagues used vacuum fluctuations, a sort of background static that permeates empty space.

Such fluctuations are another characteristic of the quantum world: there is no true emptiness. Even in an "empty" space devoid of visible light, packets of energy equivalent to half of a photon, or light particle, can be formed. These leave tracks detectable in sophisticated measurements. This random "noise," called vacuum fluctuations, arises only when the physicists look for it, that is, when they carry out a measurement.

To measure the noise, Marquardt and colleagues split a strong laser beam into equal parts using a device called a beam splitter. This device had two input ports to collect incoming light, and two output ports to release outgoing light. The researchers covered the second input port to block light from entering. The vacuum fluctuations were still there, however, and they influenced the two output beams.

When the scientists measured the two output beams and subtracted the results from each other, they were not left with nothing. What remained, they said, was the quantum noise, whose precise values depended on chance.

"True random numbers are difficult to generate but they are needed for a lot of applications," said Gerd Leuchs, director of the Max Planck Institute. 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.

There are other quantum processes besides vacuum fluctuations that can produce true randomness, the physicists said. But their setup made it easier to separate these fluctuations from "classical" noise, or everyday types of seemingly random processes. These would pollute the measurements by introducing something that's not really random. "Classical" noise can result from, say, the slight wobbling of a measurement instrument.

Also, "the vacuum fluctuations provide unique random numbers" that can't be copied by a "data spy," said Marquardt. "We do not need either a particularly good laser or particularly expensive detectors for the set-up," added Christian Gabriel of the institute.

Marquardt's group isn't the first to have claimed true random number generation. Earlier this year, researchers with the Joint Quantum Institute, a partnership of the University of Maryland and the U.S. National Institute of Standards and Technology, claimed to have used the phenomenon of quantum entanglement to communicate random numbers. In quantum entanglement, two particles set apart some distance from each other are found to have exactly the same properties, some of which are random, at a given point in time. This phenomenon can in principle be used to securely send the random information between two, arbitrarily distant points.

"The random bit generation rate is extremely slow" by this method, said the institute's Chris Monroe last April, "but we expect speedups by orders of magnitude in coming years as we more efficiently entangle the atoms." The findings appeared in the April 15 issue of the research journal *Nature.*