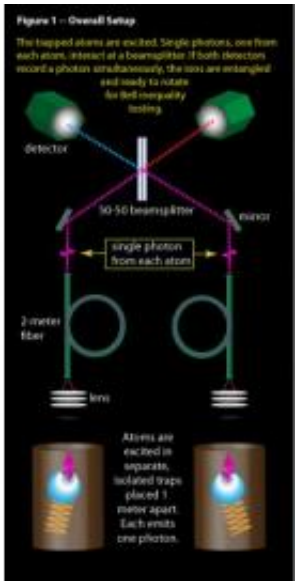
Random, but not by chance: A quantum random-number generator for encryption, security

14 April 2010



This is the experimental setup. Credit: JQI

Researchers have devised a new kind of random number generator, for encrypted communications and other uses, that is cryptographically secure, inherently private and - most importantly - certified random by laws of physics.

That is important because randomness is surprisingly rare. Although the welter of events that transpire in the course of daily life can certainly seem haphazard and arbitrary, none of them is genuinely random in the sense that they could not be predicted given sufficient knowledge. Indeed, true randomness is almost impossible to come by.

That situation is a source of urgent and persistent concern to cryptographers who need to encrypt valuable data and messages by using a long string of random numbers to form a "key" to encode and decode the information. For practical purposes, encoders typically employ various mathematical algorithms called "pseudo-random number generators" to approximate the ideal. But they can never be completely certain that the system used to produce those number strings is invulnerable to adversaries or that a seemingly random sequence is not, in fact, predictable in some manner.

Now, however, a team of experimentalists from the Joint Quantum Institute (JQI) , in partnership with European quantum information scientists, has demonstrated a method of producing a certifiably random string of numbers based on fundamental principles of quantum mechanics. They report their results in the 15 April 2010 issue of *Nature*.

"Classical physics simply does not permit genuine randomness in the strict sense," says JQI Fellow Chris Monroe, who led the experimental team. "That is, the outcome of any classical physical process can ultimately be determined with enough information about initial conditions. Only quantum processes can be truly random - and even then, we must trust that the device is indeed quantum and has no remnant of classical physics in it."

In quantum mechanics, the science of matter and energy on the smallest scales, specific properties of objects (such as the position of an electron or the polarization of a photon) can be inherently uncertain. Although the probability of any particular property can be calculated in advance, those properties take on particular values only when measured; and the values are intrinsically random. So in theory, one could obtain a series of random numbers by performing a series of quantum measurements that were entirely independent of one another.

"Such a sequence would, of course, be intrinsically random," says Dzmitry Matsukevich of JQI, a coauthor of the report in *Nature*. "However, most

people would probably prefer to buy an existing quantum device rather than build a quantum random number generator themselves. Unfortunately in this case it is very difficult to ensure that the device produces a string of random numbers that is not known to anyone else. For example, instead of a real quantum random number generator, someone might sell you a "black box" device that has a memory filled with random numbers loaded in advance. This device would probably pass all existing tests of randomness. But someone would still have a copy of all the numbers."

There is, however, a procedure that guarantees the presence of truly random quantum measurements, generated only at - and completely unique to - a particular place and time, which might be termed "private randomness." It was invented by physicist John Bell in 1964 to test a central hypothesis of quantum mechanics: namely, that two objects such as photons or matter particles can enter an exotic condition called "entanglement" in which their states become so utterly interdependent that if a measurement is performed to determine a property of one (which will, of course, be a random value), the corresponding property of the other is instantly determined as well, even if the two objects are separated by distances so large that no information could possibly pass between them after the measurement is made on the first object.

Many scientists, notably including Albert Einstein, found that notion completely unacceptable, arguing instead that so-called "entangled" objects must actually possess some hidden variables which give the objects specific properties in advance of a measurement. Otherwise, a purely local measurement of Object 1 would have an instantaneous effect on Object 2, even if Object 2 was light-years away at the time of the measurement - a phenomenon Einstein dismissed as "spooky action at a distance." For 30 years, there was no convincing way of determining experimentally whether Einstein was right or wrong.

Then Bell came up with a revolutionary method that involved counting the correlations between measurements made on the two objects as the measuring devices were switched among numerous different orientations. Bell showed mathematically that if the objects were not entangled, their correlations would have to be smaller than a certain value, expressed as an "inequality." If they were entangled, however, the correlation rate could be higher, "violating" the inequality. Various kinds of Bell tests performed in recent decades on entangled systems have shown such inequality violation, and thus confirmed the nonlocality of quantum mechanics. But the JQI experiment was the first to violate a Bell inequality between systems separated over a distance without missing any of the events.

"Violation of a Bell inequality is possible only if the system obeys the laws of quantum mechanics," Matsukevich says. "Therefore if we verify a Bell inequality violation between isolated systems while not missing events, we can ensure that our device produces private randomness. We don't need the atoms to be too far apart, only far enough so that they could be shielded from each other, as would be done anyway in a real cryptographic setting."

To do so, the JQI group placed a single atom in each of two completely isolated enclosures spaced a meter apart. They then proceeded to entangle the two atoms using a now-familiar method based on single photons travelling between the atoms. (For a description of this process, which last year made headlines as the first successful "teleportation" of information between remote atoms, see http://www.physorg.com/news151856605.html and http://www.sciencemag.org/cgi/content/abstract/323/5913/486.)

Every time their apparatus signaled that entanglement had been achieved, the researchers rotated each atom on its axes according to a random schedule and then took a measurement of each atom's emitted light. The value from each of two atoms was then used to generate a binary number.

The researchers performed more than 3000 consecutive entanglement events in the course of about a month, confirming Bell inequality violation and in the process generating a string of 42 random private binary digits at a 99% confidence level. As a result, they write in *Nature*, "we can, for the first

time, certify that new randomness is produced in an experiment without a detailed model of the device." That is, the process relies only on achieving entanglement and performing operations on the entangled objects, not on the specific details of how entanglement was achieved.

At present, "the random bit generation rate is extremely slow," said Monroe, "but we expect speedups by orders of magnitude in coming years as we more efficiently entangle the atoms, perhaps by using atom-like quantum systems embedded in a solid-state chip." Then by violating the Bell inequality over much larger distances, Monroe added that "such a system could be deployed for a more secure type of data encryption."

Provided by University of Maryland