New quantum method generates really random numbers

April 11 2018

NIST researchers have developed a method for generating numbers guaranteed to be random by quantum mechanics. Credit: Irvine/NIST

Researchers at the National Institute of Standards and Technology (NIST) have developed a method for generating numbers guaranteed to

be random by quantum mechanics. Described in the April 12 issue of *Nature*, the experimental technique surpasses all previous methods for ensuring the unpredictability of its random numbers and may enhance security and trust in cryptographic systems.

The new NIST method generates digital bits (1s and 0s) with photons, or particles of light, using data generated in an improved version of a landmark 2015 NIST physics experiment. That experiment showed conclusively that what Einstein derided as "spooky action at a distance" is real. In the new work, researchers process the spooky output to certify and quantify the randomness available in the data and generate a string of much more random bits.

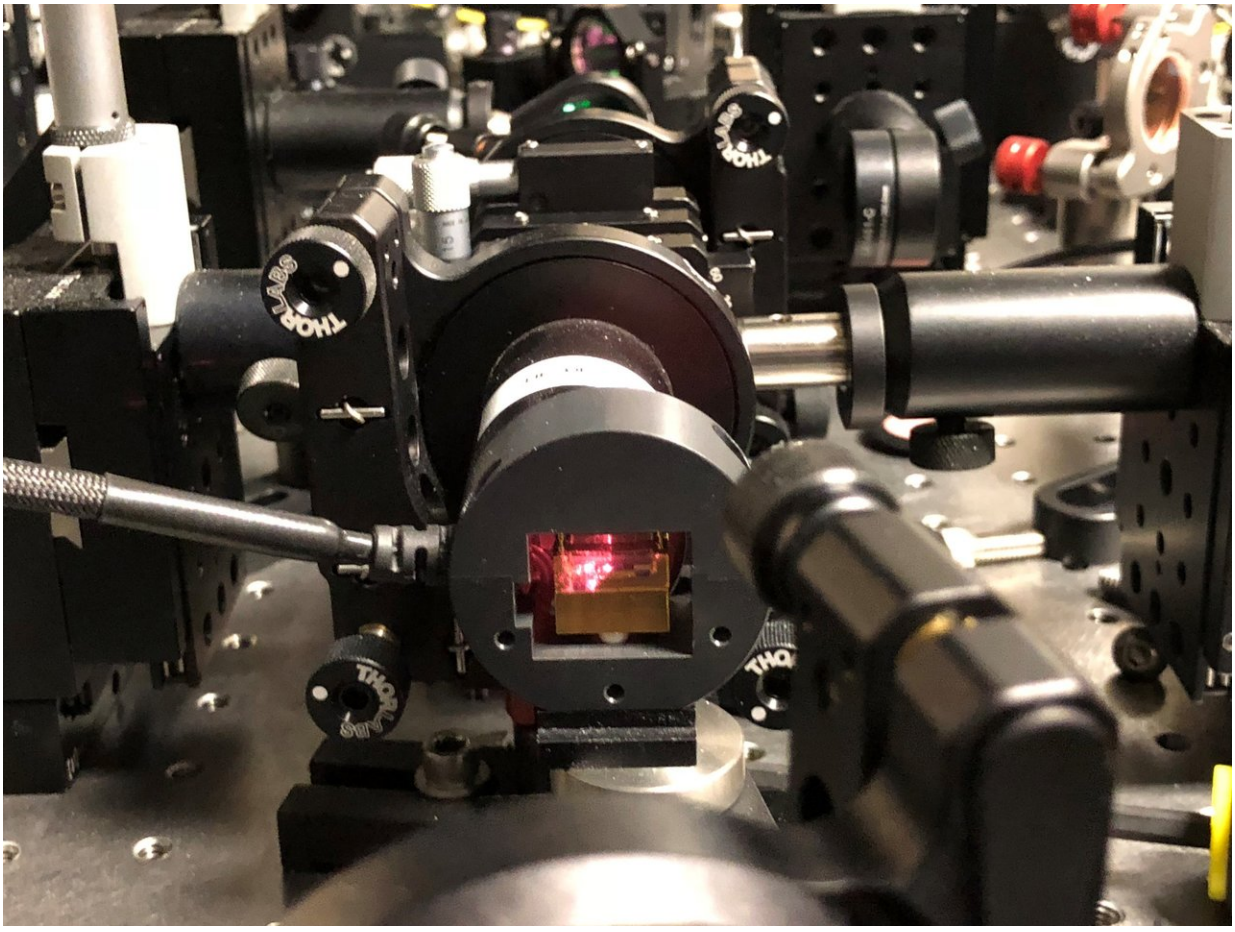
Random numbers are used hundreds of billions of times a day to encrypt data in electronic networks. But these numbers are not certifiably random in an absolute sense. That's because they are generated by software formulas or physical devices whose supposedly random output could be undermined by factors such as predictable sources of noise. Running statistical tests can help,but no statistical test on the output alone can absolutely guarantee that the output was unpredictable, especially if an adversary has tampered with the device.

"It's hard to guarantee that a given classical source is really unpredictable," NIST mathematician Peter Bierhorst said. "Our quantum source and protocol is like a fail-safe. We're sure that no one can predict our numbers."

"Something like a coin flip may seem random, but its outcome could be predicted if one could see the exact path of the coin as it tumbles. Quantum randomness, on the other hand, is real randomness. We're very sure we're seeing quantum randomness because only a quantum system could produce these statistical correlations between our measurement choices and outcomes."

The new quantum-based method is part of an ongoing effort to enhance NIST's public randomness beacon, which broadcasts random bits for applications such as secure multiparty computation. The NIST beacon currently relies on commercial sources.

Quantum mechanics provides a superior source of randomness because measurements of some quantum particles (those in a "superposition" of both 0 and 1 at the same time) have fundamentally unpredictable results. Researchers can easily measure a quantum system. But it's hard to prove that measurements are being made of a quantum system and not a classical system in disguise.



Credit: Shalm/NIST

In NIST's experiment, that proof comes from observing the spooky quantum correlations between pairs of distant photons while closing the "loopholes" that might otherwise allow non-random bits to appear to be random. For example, the two measurement stations are positioned too far apart to allow hidden communications between them; by the laws of physics any such exchanges would be limited to the speed of light.

Random numbers are generated in two steps. First, the spooky action experiment generates a long string of bits through a "Bell test," in which researchers measure correlations between the properties of the pairs of photons. The timing of the measurements ensures that the correlations cannot be explained by classical processes such as pre-existing conditions or exchanges of information at, or slower than,the speed of light. Statistical tests of the correlations demonstrate that quantum mechanics is at work,and these data allow the researchers to quantify the amount of randomness present in the long string of bits.

That randomness may be spread very thin throughout the long string of bits. For example, nearly every bit might be 0 with only a few being 1. To obtain a short, uniform string with concentrated randomness such that each bit has a 50/50 chance of being 0 or 1, a second step called "extraction" is performed. NIST researchers developed software to process the Bell test data into a shorter string of bits that are nearly uniform; that is, with 0s and 1s equally likely. The full process requires the input of two independent strings of random bits to select measurement settings for the Bell tests and to "seed" the software to help extract the randomness from the original data. NIST researchers used a conventional random number generator to generate these input strings.

From 55,110,210 trials of the Bell test, each of which produces two bits, researchers extracted 1,024bits certified to be uniform to within one trillionth of 1 percent.

"A perfect coin toss would be uniform, and we made 1,024 bits almost perfectly uniform, each extremely close to equally likely to be 0 or 1," Bierhorst said.

Other researchers have previously used Bell tests to generate random numbers, but the NIST method is the first to use a loophole-free Bell test and to process the resulting data through extraction. Extractors and seeds are already used in classical random number generators; in fact, random seeds are essential in computer security and can be used as encryption keys.

In the new NIST method, the final numbers are certified to be random even if the measurement settings and seed are publicly known; the only requirement is that the Bell test experiment be physically isolated from customers and hackers. "The idea is you get something better out (private randomness) than what you put in (public randomness)," Bierhorst said.

More information: Experimentally generated randomness certified by the impossibility of superluminal signals, *Nature* (2018). nature.com/articles/doi:10.1038/s41586-018-0019-0

Provided by National Institute of Standards and Technology