



NIST and Partners Use Quantum Mechanics to Make a Factory for Random Numbers

[NIST](#) and its partners at the [University of Colorado Boulder](#), in collaboration with ICFO and QuSide, built the first random number generator that uses quantum entanglement to produce verifiable random numbers.

Broadcast as a free public service, the Colorado University Randomness Beacon (CURBy) can be used anywhere an independent, public source of random numbers would be useful, such as selecting jury candidates or assigning resources through a public lottery.

June 12, 2025

Randomness is incredibly useful. People often draw straws, throw dice or flip coins to make fair choices. Random numbers can enable auditors to make completely unbiased selections. Randomness is also key in security; if a password or code is an unguessable string of

numbers, it's harder to crack. Many of our cryptographic systems today use random number generators to produce secure keys.

But how do you know that a random number is truly random? Classical computer algorithms can only create pseudo-random numbers, and someone with enough knowledge of the algorithm or the system could manipulate it or predict the next number. An expert in sleight of hand could rig a coin flip to guarantee a heads or tails result. Even the most careful coin flips can have bias; with enough study, their outcomes could be predicted.?

True randomness is something that nothing in the universe can predict in advance, said Krister Shalm, a physicist at [National Institute of Standards and Technology \(NIST\)](#). Even if a random number generator used seemingly random processes in nature, it would be hard to verify that those numbers are truly random, Shalm added.

Einstein believed that nature isn't random, famously saying, "God does not play dice with the universe." Scientists have since proved that Einstein was wrong. Unlike dice or computer algorithms, quantum mechanics is inherently random. Carrying out a quantum experiment called a Bell test, Shalm and his team have transformed this source of true quantum randomness into a traceable and certifiable random-number service. Their results were just published [Nature](#).

If God does play dice with the universe, then you can turn that into the best random number generator that the universe allows," Shalm said. "We really wanted to take that experiment out of the lab and turn it into a useful public service." To make that happen, NIST researchers and their colleagues at the University of Colorado Boulder created the [Colorado University Randomness Beacon \(CURBy\)](#). CURBy produces random numbers automatically and broadcasts them daily through a website for anyone to use.

At the heart of this service is the NIST-run Bell test, which provides truly random results. This randomness acts as a kind of raw material that the rest of the researchers' setup refines into random numbers published by the beacon.

The role of ICFO and Qside

ICFO researchers (including co-founders of Qside) and ICFO EW engineering staff, invented and built the fast quantum random number generators used by NIST for the Bell Tests.

The Bell test measures pairs of entangled photons whose properties are correlated even when separated by vast distances. When researchers measure an individual particle, the outcome is random, but the properties of the pair are more correlated than classical physics allows, enabling researchers to verify the randomness. Einstein called this quantum nonlocality "spooky action at a distance."

Choosing what properties of entangled particles to measure must be made very quickly, and with a high degree of confidence in the randomness. That is the contribution from ICFO and Qside. Thanks to that, the result of the measurements in the Bell test were also ran-

om, but at a highe

level. This is the first random number generator service to use quantum nonlocality as a source of its numbers, and the most transparent source of random numbers to date. That's because the results are certifiable and traceable to a greater extent than ever before. In fact, the big advance of the project is a way for users to trust the resulting numbers without trusting the partners involved in their generation. Imagine two political parties agree to verify the results of an election by double-checking a random sample of the ballots. Neither party is going to trust the other to generate the random numbers, but they can trust a randomness beacon as a privilege to contribute to this first-of-its-kind generation of public randomness using Nobel-prize-winning quantum physics. It is a clear example of how quantum technologies can contribute to security in the internet age," comments ICREA and ICFO Prof. Morgan Mitchell, who was involved in the study. Dr. Carlos Abellan, CEO of QuSide, adds: "It's truly an honor to contribute to this experiment with our quantum random number generation technology; at QuSide, we continue to push the industrialization path for this new randomness generation devices with advanced verification capabilities."

It is a clear example of how quantum technologies can contribute to security in the internet age, comments ICREA and ICFO Prof. Morgan Mitchell, who was involved in the study. Dr. Carlos Abellan, CEO of QuSide, adds: **"It's truly an honor to contribute to this experiment with our quantum random number generation technology; at QuSide, we continue to push the industrialization path for this new randomness generation devices with advanced verification capabilities."**

A new publicly available service

"CURBy is one of the first publicly available services that operates with a provable quantum advantage. That's a big milestone for us," Shalm explained. "The quality and origin of these random bits can be directly certified in a way that conventional random number generators are unable to."

NIST performed one of the first complete experimental Bell tests in 2015, which firmly established [quantum mechanics is truly random](#). In 2018, NIST pioneered methods to use these Bell tests to build [the world's first sources of true randomness](#).

However, turning these quantum correlations into random numbers is hard work. NIST's first breakthrough demonstrations of the Bell test required months of setup to run for a few hours, and it took a great deal of time to collect enough data to generate 512 bits of true randomness. Shalm and the team spent the past few years building the experiment to be robust and to run automatically so it can provide random numbers on demand. In its first 40 days of operation, the protocol produced random numbers 7,434 times out of 7,454 attempts, a 99.7% success rate.

How do the researchers generate and certify randomness?

The process starts by generating a pair of entangled photons inside a special nonlinear crystal. The photons travel via optical fiber to separate labs at opposite ends of the hall. Once the photons reach the labs, their polarizations are measured. The outcomes of the measurements are truly random. This process is repeated 250,000 times per second. NIST passes millions of these quantum coin flips to a computer program at the University of Colorado Boulder. Special processing steps then turn them into a set of random bits that

no one, not even Einstein, could have predicted. In some sense, this system acts as the universe's best coin flip.

NIST and its collaborators added the ability to trace and verify every step in the randomness generation process. They developed the Twine protocol, which marks each set of data for the beacon with a hash. Hashes are used in blockchain technology to mark sets of data with a digital fingerprint, allowing each block of data to be identified and scrutinized. The Twine protocol allows any user to verify the data behind each random number, explained Jasper Palfrey, a research assistant on the project at the University of Colorado Boulder. The protocol can expand to let other random number beacons join the hash graph, creating a network of randomness that everyone contributes to but no individual control.

Intertwining these hash chains acts as a timestamp, linking the data for the beacon together into a traceable data structure. It also provides security, allowing Twine protocol participants to immediately spot manipulation of the data. The Twine protocol lets us weave together all these other beacons into a tapestry of trust, Palfrey added. The whole process is open source and available to the public, allowing anyone to not only check their work, but even build on the beacon to create their own random number generator. CURBy can be used anywhere an independent, public source of random numbers would be useful, such as selecting jury candidates, making a random selection for an audit, or assigning resources through a public

Reference:

Gautam A. Kavuri et al. Traceable random numbers from a non-local quantum advantage. Nature. Published online June 11, 2025. DOI: [10.1038/s41586-025-09054-3](https://doi.org/10.1038/s41586-025-09054-3)