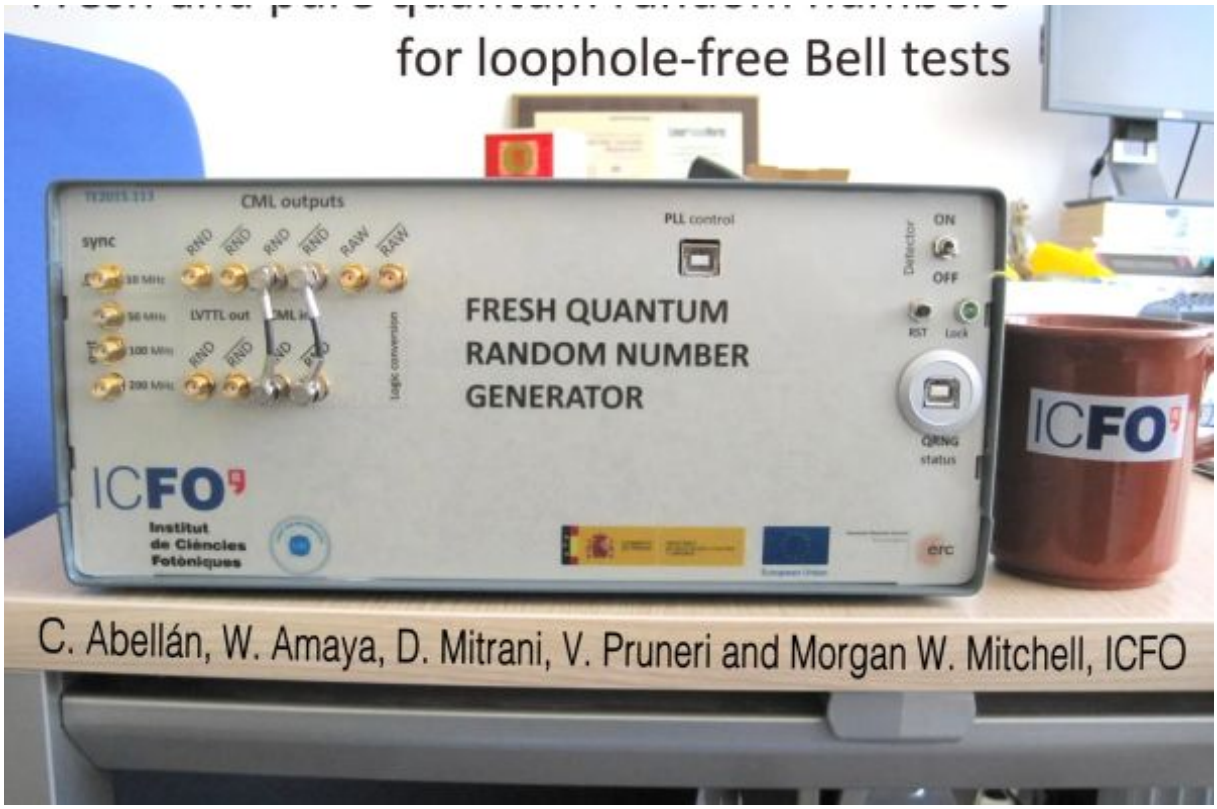


NIST and Partners Use Quantum Mechanics to Make a Factory for Random Numbers

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.?

i¿½True randomness is something that nothing in the universe can predict in advance,i¿½ said Krister Shalm, a physicist at the 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, i¿½God does not play dice wi h the universe.i¿½ Scientists have since proved that Einstein was wrong. Unlike dic or computer algorithms, quantum mechanics is inherently random. Carrying out a qua tum experiment called a Bell test, Shalm and his team have transformed this source of rue quantum randomness into a traceable and certifiable random-number service. Their res lts were just published in Nature.

i¿½If God does play dice with the universe, then you can turn that into the best rand m number generator that the universe allows,i¿½ Shalm said. i¿½We really wanted to ta e that experiment out of the lab and turn it into a useful public serv ce.i¿½ 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 i¿½refinesi ?½ into random numbers published by the beac

The role of ICFO and Quside

ICFO researchers (including co-founders of Quside) 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 i¿½entangledi¿½ photons whose properties are correl ted 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 phy ics allows, enabling researchers to verify the randomness. Einstein called this qua tum nonlocality i¿½spooky action at a distan e.i¿½ Choosing what properties of entangled particles to measure must be made very quic ly, and with a high degree of confidence in the randomness. That is the contribution from CFO and Quside. 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 s
urce of its numbers, and the most transparent source of random numbers to date. That's bec
use 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 trus
ing 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
oing to trust the other to generate the random numbers, but they can trust a randomness
bea**It is 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**,i¿½ comments ICREA and ICFO Prof. Morg
n Mitchell, who was involved in the study. Dr. Carlos Abellan, CEO of QuSide, adds: i¿½**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.**i¿

A new publicly available service

i¿½CURBy is one of the first publicly available services that operates with a provable quant
m advantage. That's a big milestone for us,i¿½ Shalm explained. i¿½The quality and ori
in of these random bits can be directly certified in a way that conventional random
umber generators are unable
o.i¿½ NIST performed one of the first complete experimental Bell tests in 2015, whic
firmly established that 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. Onc
the photons reach the labs, their polarizations are measured. The outcomes of the
e measurements are truly random. This process is repeated 250,000 times per seco
d. 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
he universe's best coin fl
p. NIST and its collaborators added the ability to trace and verify every step in the randomn
ss generation process. They developed the Twine protocol, which marks each set of data for
he beacon with a hash. Hashes are used in blockchain technology to mark sets of data wit
 a digital fingerprint, allowing each block of data to be identified and scrutiniz
d. The Twine protocol allows any user to verify the data behind each random number, explai
ed Jasper Palfree, a research assistant on the project at the University of Colorado Boulder.
he protocol can expand to let other random number beacons join the hash graph, creatin
 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 toge
her into a traceable data structure. It also provides security, allowing Twine protocol particip
nts to immediately spot manipulation of the data. i¿½The Twine protocol lets us weave to
ether all these other beacons into a tapestry of trust,i¿½ Palfre
 added. The whole process is open source and available to the public, allowing anyone to
ot only check their work, but even build on the beacon to create their own rando
 number ge
erator. CURBy can be used anywhere an independent, public source of random numbers
ould be useful, such as selecting jury candidates, making a random selection for an
udit, 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