

RRI technique yields certified randomness with one qubit

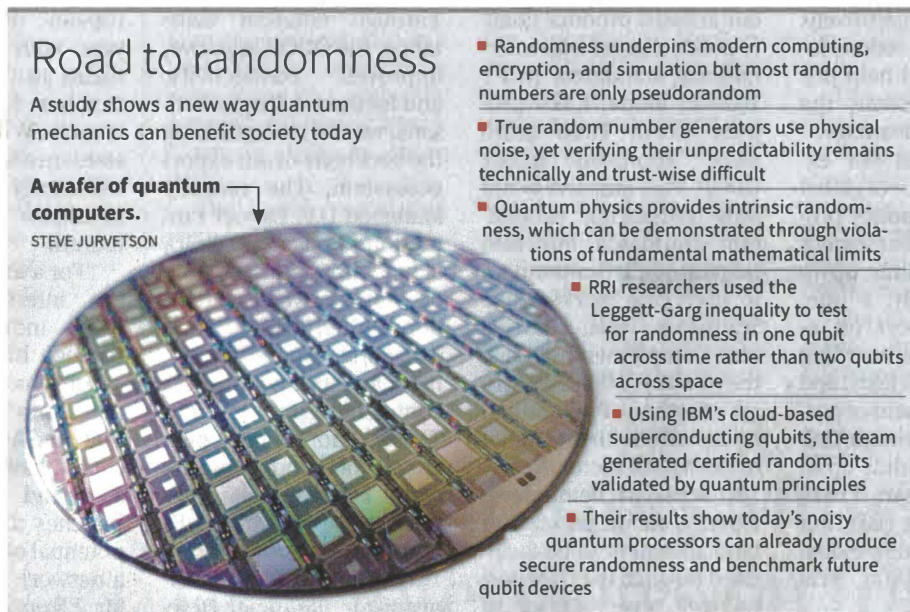
Researchers built simple quantum circuits on IBM's superconducting quantum computers, which are available on cloud; the experiments produced random numbers certified by quantum mechanics, and which classical randomness can't fake

Vasudevan Mukunth

Randomness is essential today. From encrypting sensitive information to simulating biological systems, unpredictable numbers are indispensable. Yet most everyday random numbers aren't truly random. Conventional computers use algorithms called pseudorandom number generators to produce sequences that look random but are ultimately predictable if the starting 'seed' is known. For applications such as cryptography, this predictability is dangerous because attackers could exploit it.

True random number generators try to solve this using physical processes such as electronic noise or radioactive decay, which can't be predetermined. But these devices aren't free of problems either: they degrade over time like any hardware, and also need users to trust manufacturers to not have secretly inserted prerecorded numbers into the system. Certifying they are truly random is also difficult.

Quantum physics is especially powerful here. At its heart is a principle that some outcomes, such as the spin of an electron measured along a chosen axis, are fundamentally random. Physicists have long used quantum experiments to prove this intrinsic randomness, often by showing quantum systems can violate mathematical limits known as Bell inequalities. However, such tests require at least two



entangled qubits to be separated by a large distance, making them impractical for a single quantum computer.

A different inequality, known as the Leggett-Garg inequality (LGI), provides an alternative. Instead of requiring spatial separation, it compares the outcomes of measurements performed at different times on the same system. If LGI is violated while satisfying the 'no signalling in time' condition, which ensures the two readings are completely independent, the results are certified as truly random.

To this end, Raman Research Institute researchers led by Urbasi Sinha asked a question: could modern quantum processors, like those available on the IBM Quantum platform, already be used to generate certified random numbers? If so, this would prove that even the current generation of quantum devices can perform tasks

impossible for classical machines.

The team built simple quantum circuits on IBM's superconducting quantum computers, which are available on the cloud. Each circuit used only one qubit and a sequence of single-qubit gates representing rotations around chosen axes. They made measurements at three times and checked the results for whether the LGI was violated while still satisfying the 'no signalling in time' condition. By carefully varying the parameters and constraints in multiple tests, the team certified the randomness of the generated bits.

The experiments successfully produced random numbers certified by quantum mechanics. On IBM's Brussels backend, the team observed consistent violations of the LGI, although the measured values were slightly below theoretical predictions due to noise.

"The beauty of our implementation is that we have been able to show something as fundamental as certified randomness using a noisy intermediate scale quantum computer," Prof. Sinha, who heads the Quantum Information and Computing (QuIC) lab, said. "We have been able to do this through careful error mitigation techniques and ensuring that 'classical' errors are under control and the randomness is purely from the underlying quantum mechanical principles."

The study has several important implications. It demonstrates foremost that secure random numbers can already be generated on existing quantum computers without elaborate laboratory setups. Demanding only one qubit and shallow circuits, the protocol is feasible for end users who can access quantum computers through cloud platforms.

"There are still a few

challenges to be overcome along the way but the fact that this certification is device-independent makes this a very promising avenue," Prof. Sinha said.

The work also shows how quantum mechanics can benefit society today. Classical randomness can't fake certified randomness, providing a layer of security for applications where unpredictability is paramount, including data encryption, secure communications, and scientific simulations.

The results highlight the importance of error-mitigation tools in making quantum hardware reliable. Techniques such as readout error correction improved the tests' agreement with theory and reinforced trust in the generated randomness, underlying how progress in circuit design can extend the capabilities of noisy devices.

The study also contributes to foundational physics: by confirming violations of the Leggett-Garg inequality on a quantum computer, it offers further validation of quantum theory in a new setting. The same methods could also be used to benchmark qubits individually, providing a tool with which to test future machines.

"We can use our method as a strong benchmark for new qubit registers as they emerge, which will prove how useful these systems are going to be in solving real-world problems," Prof. Sinha said.

The team's results were published in *Frontiers in Quantum Science & Technology* in September.