Quantum computer generates first 'certified' random number

Unlike regular random numbers that are simply hard to guess, certified random means that the data is completely newly generated and mathematically verified.

A team of researchers from JPMorganChase, Quantinuum, Argonne National Laboratory, Oak Ridge National Laboratory, and the University of Texas has achieved a major milestone in quantum computing. In a new paper published in Nature , they describe how they used a 56-qubit quantum computer to generate random numbers, and then proved that the numbers were truly random using powerful classical supercomputers. This achievement – called *certified* randomness – holds promise for applications in cryptography, security, and fairness.

Unlike regular random numbers that are simply hard to guess, *certified randomness* means that the data is generated from scratch and mathematically verified. Classical computers can't do this on their own, and typically rely on hardware that generates random numbers, which can be tampered with. With the new method, even if someone were to tamper with a quantum computer, they wouldn't be able to fake the randomness and still pass the certification process.

The idea for the protocol was proposed by computer science professor Scott Aaronson at the University of Texas at Austin, who helped develop it with his colleague Shih-Han Hung.
' *When I proposed the protocol in 2018, I never expected to see it implemented today* ,' Aaronson said. ' *Finishing the protocol and proving it works is the first step toward using quantum computers to generate certified random bits for practical cryptographic applications* .'

In the experiment, the team accessed the Quantinuum System Model H2-1 quantum computer via the Internet and applied a method *called Random Circuit* Sampling (RCS) – which is extremely difficult to simulate with classical computers. The process consists of two steps:

1. Send the quantum computer a series of 'challenge circuits' generated from a small amount of random seeds. The quantum computer must choose a random answer from many possibilities.
2. Classical supercomputers would check the results to confirm true randomness.

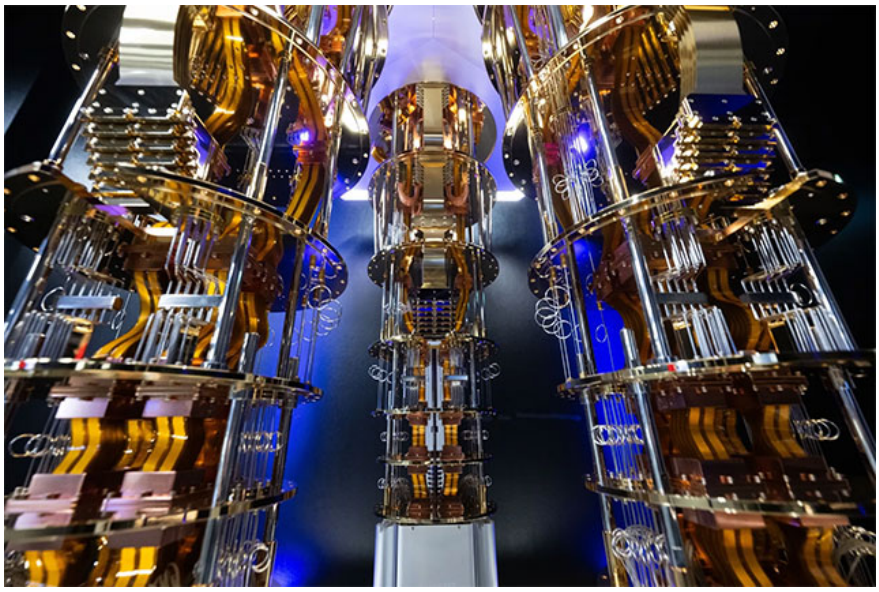
The team used multiple supercomputers with a combined performance of **1.1 ExaFLOPS** to verify **71,313 bits of entropy** – meaning they proved that these bits cannot be generated by a classical computer under practical conditions.

'This is a major milestone, demonstrating that a quantum computer has solved a real-world problem that is far beyond the capabilities of today's supercomputers ,' said Marco Pistoia, Head of Global Applied Technology

Research at JPMorganChase.

The H2 quantum computer was upgraded to 56 qubits in June 2024. Thanks to its high precision and the ability for all qubits to be directly connected to each other, this system performs RCS much more efficiently than the previous generation. Combined with Aaronson's protocol, the breakthrough became a reality.

This result was achieved thanks to the power of the US Department of Energy's leading supercomputing facilities located at Oak Ridge, Argonne and Lawrence Berkeley, said Travis Humble, director of the Quantum Computing User Program at ORNL.



Previously, quantum computers had only demonstrated theoretical superiority over classical computers. But this experiment showed that they can actually solve a real-world problem that classical computers are completely unable to solve.