

Indian scientists develop simpler method for quantum-based digital security

TNN | Oct 4, 2025, 03.31 PM IST



BENGALURU: Researchers in India have developed a new way to generate truly random numbers using quantum computers, a breakthrough that could make digital security systems harder to crack.

The work was done by scientists at the Raman Research Institute (RRI) in Bengaluru, working with colleagues from the Indian Institute of Science (IISc) and the University of Calgary. Their findings were published this year.

Random numbers are vital for digital security. They protect bank accounts, encrypt messages, and secure online transactions. But regular computers cannot make truly random numbers. They follow set rules, which means their “random” numbers can theoretically be predicted. Quantum mechanics, however, is inherently random. The researchers found a way to harness this randomness using quantum computers.

Previous methods for generating certified random numbers required complex laboratory setups with multiple particles separated over long distances. The Indian team simplified this. They used just one qubit—the basic unit of a quantum computer—and measured it at different times rather than separating particles in space.

This approach worked on IBM’s quantum computer, which is available through the cloud. Anyone with internet access could potentially use it.

The research builds on work the team started in 2022. That year, they proved quantum mechanics was correct by testing how single particles of light behaved over time. They closed all possible loopholes in their experiment, making their results conclusive.

In 2024, they built a quantum random number generator that produced nearly 1 million certified random bits. Now, in 2025, they have shown the same process works on commercial quantum computers, not just in specialised laboratories.

“The trilogy advances one idea across three frontiers—rigorous foundational validation, practical certification of randomness, and deployment—culminating in certified randomness

running on quantum computers in the cloud,” Prof Urbasi Sinha, who heads the Quantum Information and Computing (QuIC) lab at RRI, said.

The simplicity of the new method is its main advantage. Current quantum computers are small and prone to errors, but they can still generate certified random numbers using this technique.

This matters for cryptography, where security depends on digital keys being completely unguessable. The new method makes such systems more practical to implement. It also helps test how well individual qubits in quantum computers are working, providing a way to check the quality of quantum hardware.

RRI is funded by India's department of science and technology. The work shows quantum computers can do more than solve specialised mathematical problems. They can now provide practical tools for secure communications.