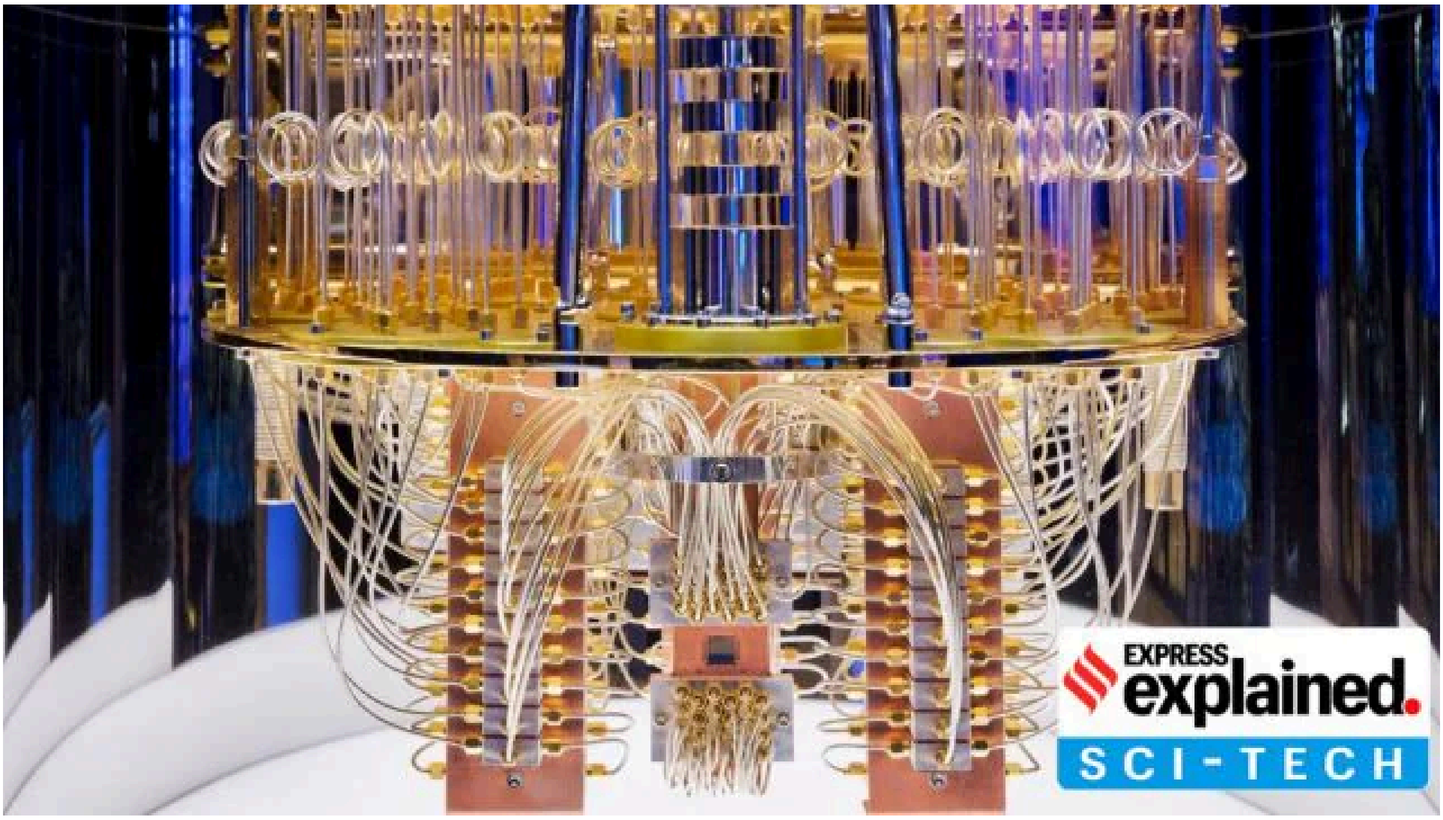
The Indian EXPRESS
JOURNALISM OF COURAGE

Quantum breakthrough in digital security: How Indian researchers achieved this, significance

For the first time, a technique to generate true random numbers is ready to be deployed in real-life situations. It potentially paves the way for the development of hack-proof digital security.

Written by Amitabh Sinha Follow
New Delhi | Updated: October 10, 2025 09:08 PM IST
6 min read



The interior of IBM's quantum computer (The European Space Agency/IBM Research)

In a significant breakthrough that can have profound implications for digital and online security, an Indian research group has developed new quantum techniques to generate and certify truly random numbers.

Researchers from Bengaluru-based Raman Research Institute, led by quantum physicist Urbasi Sinha, used a readily available general-purpose quantum computer to experimentally demonstrate and certify the generation of true random numbers.

This means that, for the first time, a technique to generate true random numbers is ready to be deployed in real-life situations. It potentially paves the way for the development of hack-proof digital security.

Random numbers in the quantum computing era

Randomly-generated numbers are critical to digital security. In fact, very large randomly-generated numbers are the foundation on which modern encryption systems and security architectures are built. The defining feature of such numbers is that they are created in completely random processes, not by following any pattern or algorithm. As a result, they cannot be guessed or predicted. Anything built on top of them — passwords, encryption keys, or authentication systems – become highly secure against hacking.

Our current systems, however, do not use truly random numbers. Instead, they use what are known as pseudorandom numbers, generated through computer algorithms. These algorithms are sophisticated enough to ensure that the very large numbers they produce appear random and are extremely difficult to predict without knowledge of how the algorithm works, as well as its initial input.

These pseudorandom numbers are good enough for securing our existing networks and information systems. Even the fastest computers, applying brute-force algorithms, would take centuries or longer to decode the passwords or encryption keys based on these numbers.

All this may change with the advent of quantum computers, which utilise the highly unique and unusual properties of the quantum world to store and process data. These computers handle data in a manner that allows them to efficiently perform complex tasks that go beyond the capabilities of traditional computers. This renders realistic vulnerabilities in the current architectures of digital security.

Strengthening the current security architecture is, therefore, one of the major areas of scientific research, which is where techniques to generate truly random numbers become so important.

Randomness in nature

True randomness is observed in some natural or physical processes that are inherently random, not from any algorithm. Radioactivity and weather events are a few examples of random processes in nature. The quantum behaviour of microscopic particles is also inherently random.

Scientists have been using some of these processes, particularly quantum properties, to generate truly random numbers. In the microscopic world, particles do not have definite properties until they are measured. A photon or electron, for example, can exist in multiple states at the same time, and only when it is measured does it choose one definite state over the other. This happens entirely randomly, with no definite way to predict this behaviour.

If a stream of photons is sent through a device and measured for a particular property, some of the photons might exhibit one behaviour, and can be assigned the number 0, while others can be assigned 1. The resulting sequence of 0s and 1s can be truly random. This is how a Quantum Random Number Generator typically works.

Physics Nobel 2025 | **How winners revealed quantum physics in action**

But even this is not foolproof. The device can be faulty or biased, compromising the entire set-up, or worse, making it vulnerable to hacking. In such a scenario, the integrity of the generated numbers cannot be ascertained. This is the problem of certification. It cannot be certified whether the number is the result of the underlying natural randomness of the process, or from a fault or manipulation of the device.

“In the context of security, we tend to give almost supernatural powers to the malicious actors. We assume that the malicious actor has the capacity to do whatever is theoretically possible to hack the system, howsoever difficult or improbable it might be. The end goal of a secure system, therefore, is not to make it incredibly difficult to hack into, but impossible, something that is not even theoretically possible to do as per our current knowledge,” Urbasi Sinha said.

How the breakthrough was achieved

Sinha has been working on device-independent quantum random number generation, using another quantum property called entanglement.

In the **quantum world**, two particles, such as photons or electrons, that have interacted previously may be mysteriously linked to each other, with the behaviour of one instantaneously influencing that of the other, regardless of the physical distance between them. Each particle can be measured independently and in a randomly chosen manner, and the results compared.

The inherent quantum behaviour and randomness of this linkage is established if the outcomes violate a property called Bell's Inequality.

Several scientific groups have run such experiments and generated random numbers, but have to contend with the challenge of separating the two particles by at least a couple hundred metres to eliminate any possibility of external interference. A set-up exceeding two hundred metres in size is not a practical proposition in real-life situations.

Sinha used a slightly modified approach. Instead of using spatial separation in two particles, she used time separation in a single particle to look for violations of another property, the Leggett-Garg inequality. In 2024, Sinha's laboratory at RRI became the first one to generate truly random numbers by showing the violations of Leggett-Garg inequality in a loophole-free experimental set-up.

She has now taken this a step further. "Till now, we generated random numbers through experiments that were carried out in carefully controlled environments, in our laboratory. This time, we have run our experiments on a commercially available quantum computer, which is not customised. This is important because it shows that our technique is robust enough to be applied in real-life situations in which there is a lot of noise and other disturbances," Sinha said.

Sinha's result is a major breakthrough with huge commercial and strategic implications. It is the kind of fundamental research that the National Quantum Mission was set up to support. In fact, it is the first major globally-relevant research output from the National Quantum Mission so far.

Presently, Sinha's technique is still a laboratory-scale product, and needs to be developed further into a full-fledged commercial solution that can be marketed and deployed in security systems, which will require more research grants and support from both the government as well as private organisations.

FROM THE HOMEPAGE

Sealing key passes to redeployment: Army gears for first Valley winter afte...

He was killed like an animal: Father of 22-year-old engineer beaten to...