

B'luru scientists show quantum path to 'unhackable' OTP

ASRA MAVAD
BENGALURU, DHNS

Quantum researchers led by a senior scientist at the Raman Research Institute (RRI) in Bengaluru have created a "simplified" way for "unhackable" digital security, which could protect banking passwords and encrypted data from cyber attacks.

The new research at RRI, in collaboration with scientists at the IISc and the University of Calgary in Canada, has proven that it is possible to generate secure, certified random numbers using the inherent randomness in quantum physics.

The results were published



NUMBERS GAME

- **Random numbers**
Sequence of numbers which are unpredictable
- **Pseudo-random numbers**
Created by in-principled predictable algorithms using an initial value, hence hackable
- **Certified random numbers**
Created by harnessing physical phenomena which are unpredictable, hence harder to hack

in a journal recently.

'Random numbers' here refer to a sequence of numbers that is unpredictable. Globally, they are utilised to ensure secure communication in various strategic fields, such as the generation of one-time password

(OTP) for banking services and encrypting private chats.

However, pseudo-random numbers created by classical computers become predictable beyond a point, making them hackable.

► **Cyber security, Page 5**

B'luru scientist & team pave way for 'unhackable'...

Cyber security, from Page 1

"For data security, you cannot rely on these. Which is where quantum random number generators come in. Here, quantum mechanics is used in its inherent unpredictability to generate these random numbers. However, these are all device-dependent random numbers, and this comes with its limitations as it suffers from the same fallacies the device

suffers from. Plus, a device can be tampered with by a third party. Our research focuses on a device-independent random number generator to enable certified quantum randomness," explained Urbasi Sinha, head of the Quantum Information and Computing (QuIC) lab at the RRI.

While such certified quantum randomness has been achieved before, the scientists here used a new approach to

simplify the process. This was achieved by using the mathematical concept of the Leggett-Garg inequality, instead of Bell's inequality.

The researchers showed that certified quantum randomness could be realised on a general-purpose quantum computer available through the cloud and does not need elaborate optical tables or specialised labs.

"This is a game-changer as

it shows that even today's noisy and small-scale quantum processors can deliver a resource as fundamental as certified randomness. Quantum and quantum-enabled security is going to be our next frontier. This research will broaden the scope of what quantum computers are capable of," Sinha added. The team's research has been published in the journal *Frontiers in Quantum Science and Technology*.