New quantum research promises stronger digital data protection

Researchers said the new method offers enhanced protection on digital platforms by using truly random numbers to generate keys for encrypting passwords.

R Krishnakumar DHNS

The team experimented with the generation of unpredictable random numbers, an unexplored domain, that help devices against tampering.

Bengaluru: In an important step forward in protection of sensitive digital data, a team of Indian scientists has devised a user-friendly way to generate truly unpredictable random numbers that are crucial for stronger encryption in quantum communications.

Researchers from Raman Research Institute (RRI), Indian Institute of Science (IISc), Indian Institute of Science Education and Research (IISER) Thiruvananthapuram, and the Bose Institute, Kolkata, said the new method offers enhanced protection on digital platforms by using truly random numbers to generate keys for encrypting passwords.

Extending work done at RRI's Quantum Information and Computing lab, the team experimented with the generation of unpredictable random numbers, an unexplored domain, that help devices

against tampering. These numbers are crucial in applications including cryptographic key generation, secure password creation, and digital signatures. Pingal Pratyush Nath, a PhD student at IISc, is the first author of the paper, published in Physical Review Letters.

The security of quantum communications depends on inherent randomness, like the randomness in the measurement bases chosen by the sender and the receiver. This randomness prevents malicious agents from deciphering secure information through prior knowledge of such a choice of bases.

The experimental setup was found to display resilience against attacks. “The certified random numbers are important because any predictability of these numbers can compromise the entire security system, making it vulnerable to attacks. These numbers ensure the robustness of encryption, authentication and data integrity processes and maintain trust and security in digital interactions,” Professor Urbasi Sinha, faculty at RRI and corresponding author of the paper, said.

Debashis Saha, faculty, IISER Thiruvananthapuram and co-author, highlighted the advantages in generating certified random numbers using this method, including strongly protected passwords and multi-factor authentication that add a layer of security.

RRI said engineering interventions and innovations can help devices that adopt this method find powerful applications in cybersecurity and data encryption, and in diverse randomness-based simulations and randomised control trial statistical studies.

“These include economic surveys, drug designing/testing, as well as for any futuristic technology that would rely on provable unpredictability as a critical resource,” Dipankar Home, professor at Bose Institute and co-author, said.

Read more at: https://www.deccanherald.com/india/new-quantum-research-promises-stronger-digital-data-protection-3101901