India’s Quantum Breakthrough in Cybersecurity: True Random Numbers for Unhackable Encryption

October 13, 2025 • vajiramandravi.com

Digital Security Latest News

- In a major advancement for cybersecurity, researchers at Bengaluru’s Raman Research Institute have successfully developed and certified a quantum-based method for generating true random numbers.
- Using a general-purpose **quantum computer**, the team experimentally demonstrated authentic randomness, a crucial element for creating unhackable encryption systems.
- This marks the first time such a technique is ready for real-world deployment, potentially laying the foundation for next-generation, hack-proof digital security.

Random Numbers in the Quantum Computing Era

- Random numbers are the foundation of modern digital security, forming the basis for encryption keys, passwords, and authentication systems.
- Their strength lies in being completely unpredictable, ensuring data remains secure from hacking attempts.

Pseudorandom Numbers and Their Limits

- Currently, most systems use pseudorandom numbers — numbers generated through computer algorithms that only simulate randomness.
- While these are nearly impossible to predict without knowing the algorithm and input seed, they are not truly random.
- These pseudorandom systems are sufficiently secure for now; even with brute-force attacks, traditional computers would take centuries to break their encryption.
- However, the **emergence of quantum computers**, which exploit quantum properties like superposition and entanglement, **poses new vulnerabilities to current encryption systems**.
- Quantum computers can process data exponentially faster, potentially decoding existing cryptographic protections that rely on pseudorandomness.

The Need for True Randomness

- As quantum computing advances, there’s a growing need to upgrade digital security using truly random numbers generated from quantum processes.
- Such quantum randomness could make future encryption systems virtually unbreakable, protecting sensitive data in the post-quantum era.

Randomness in Nature and Its Role in Quantum Security

- Unlike algorithmic generation, **true randomness** exists in **natural phenomena** such as **radioactive decay**, **weather fluctuations**, and especially **quantum behaviour** of microscopic particles.
- In the **quantum realm**, particles like photons or electrons exist in multiple states simultaneously, and only upon measurement do they randomly collapse into a definite state — a process that cannot be predicted.

How Quantum Random Number Generators Work

- A Quantum Random Number Generator (QRNG) uses this unpredictability.
- For instance, when a stream of photons is measured for a specific property, outcomes are assigned as 0 or 1, creating a truly random binary sequence.
- However, if the device is biased or faulty, the randomness can be compromised — introducing vulnerabilities that can be exploited by hackers.

The Challenge of Certification

- Even with quantum systems, verifying that numbers are **genuinely random** is difficult.
- This **problem of certification** arises because external interference or internal defects can mimic randomness, making **authenticity uncertain**.
- Cybersecurity must assume that malicious actors possess limitless hacking potential.
- Thus, the aim is not merely to make systems hard to hack, but to make hacking theoretically impossible under known physical laws — a goal that quantum-certified randomness seeks to achieve.

From Entanglement to True Randomness

- Quantum physicists at the Raman Research Institute (RRI) have pioneered a **device-independent method** for generating **true random numbers**, leveraging a quantum property known as **entanglement**.
- In entanglement, two particles remain mysteriously linked, with the behaviour of one instantly influencing the other, regardless of distance.
- Randomness is confirmed when their **measurement outcomes violate Bell's Inequality**, a signature of genuine quantum behaviour.
    - The violation of Bell's Inequality means that the quantum world **cannot** be explained by a local, predetermined plan. It confirms two major things:
        - **Genuine Randomness:** The results of quantum measurements are truly, fundamentally random.
        - **Spooky Connection (Non-locality):** Particles can be instantaneously linked across vast distances, a connection that is stronger than any "classical" signal could achieve.

Global Significance and Future Potential

- The current achievement represents the first major globally relevant output from **India's National Quantum Mission**, aligning perfectly with its goals of advancing quantum technologies.
- While still in the laboratory stage, the method could evolve into a commercial-grade system for hack-proof digital security with further support from government and private funding.
- This marks a transformative step in quantum cryptography and cybersecurity, positioning India among global leaders in quantum technology innovation.

Source: IE | ToI
