1. Quantum Randomness - Science & Technology

Quantum breakthrough in digital security - How Indian researchers achieved this, significance. Indian researchers at RRI, Bengaluru, have generated true quantum random numbers using a commercial quantum computer, verified through Leggett-Garg inequality violations, marking a major leap in quantum cryptography and secure digital infrastructure.

1. Context and Significance - Researchers from the Raman Research Institute (RRI), Bengaluru, have successfully generated and certified truly random numbers using a commercial quantum computer. This marks a major milestone in quantum cryptography and digital security, establishing India's capability to produce certified quantum randomness outside of ideal laboratory setups.

2. Random Numbers - Random numbers are sequences generated by completely unpredictable processes, without following any fixed pattern or logic. These are essential for digital systems — particularly for encryption keys, authentication codes, and cybersecurity protocols. Their unpredictability ensures data integrity and privacy against hacking or code-breaking attempts.

3. Difference Between Pseudorandom and True Random Numbers

Type	Source	Predictability	Common Use	Security Concern
Pseudorandom Numbers	Generated using computer algorithms	Deterministic and repeatable	Used in current digital systems	May be cracked with powerful algorithms or quantum computers
True Random Numbers	Generated from natural/quantum processes	Unpredictable	Used in advanced cryptography	Immune to algorithmic prediction

4. The Quantum Advantage - Quantum mechanics introduces inherent uncertainty — the outcome of measuring a quantum particle (like a photon or electron) cannot be predicted beforehand. Quantum Random Number Generators (QRNGs) exploit this property to generate truly random 0s and 1s. This makes them ideal for next-generation encryption systems in the post-quantum era.

5. Innovation by RRI Researchers - The RRI team used time-separated measurements of single particles to demonstrate violations of the Leggett-Garg inequality. This confirmed that the observed randomness is not due to hidden classical processes but is genuinely quantum in origin. The method is robust to real-world noise and can be implemented on existing commercial quantum computers, not just in research labs.

6. Leggett-Garg Inequality (LGI) – The Core Principle - Proposed in 1985 by Anthony Leggett and Anupam Garg. Tests whether a system's properties are determined independently of observation (as in classical physics) or influenced by the act of measurement (as in quantum physics). If the inequality is violated, it means the system exhibits quantum behaviour, implying true randomness. The RRI team used temporal quantum correlations (measurements at different times) rather than spatial entanglement, making their approach simpler and practical.

7. Certification of Quantum Randomness - Device-independent methods such as LGI-based tests or entanglement verification ensure that no hidden bias or device fault affects randomness. This certification makes the output suitable for high-security applications.

8. Applications and Impact

Digital Security - Provides hack-proof encryption resistant to quantum attacks.
Quantum Computing - Supplies certified random inputs for quantum algorithms.
Cyber Infrastructure - Supports India's secure data architecture and digital governance systems.
National Quantum Mission - Strengthens India's global position in quantum communication and cryptography.

9. Global Context - Quantum random number generation is being pursued by several nations including the USA, China, and Japan for strategic and cybersecurity purposes. India's success demonstrates technological sovereignty and aligns with the Atmanirbhar Bharat vision in frontier

technologies.
Source - https - //indianexpress.com/article/explained/explained-sci-tech/quantum-random-number-india-significance-10297527/