P.L.RAJ IAS & IPS ACADEMY
Building Bureaucrats Since 2006

4. Amplifying Random Numbers – Science & Technology

Researchers at ETH Zürich have experimentally demonstrated device-independent randomness amplification, converting weakly random data into certifiably perfect randomness using quantum entanglement.

1. This breakthrough addresses fundamental limitations of classical computing in generating truly random numbers essential for cryptographic security.
2. The advance has significant implications for cybersecurity, blockchain technology, and digital infrastructure protection.

1.Understanding Randomness in Digital Security

Importance of Random Numbers

1. Modern digital security relies on cryptographic keys, which are generated using random numbers ensuring unpredictability.
2. If random numbers contain patterns or biases, attackers may predict keys and compromise encryption exposing sensitive data.
3. True randomness is fundamental to cryptographic strength preventing systematic attacks.

Challenge of Achieving True Randomness

1. True randomness is difficult to achieve because practical random number generators often contain small biases due to noise, heat, or hardware imperfections.
2. Even tiny biases in random sequences can be exploited by sophisticated attacks over time.
3. This represents fundamental limitation of classical computation motivating search for quantum methods.

2.Randomness Amplification Technology

Definition and Process

1. Randomness amplification is the process of starting with imperfect or biased random source and using quantum correlations generated through entanglement to produce output that is certifiably unbiased and unpredictable.
2. The quantum entanglement enables detection and elimination of patterns present in classical randomness.

Mechanism

1. ETH Zürich researchers used quantum entanglement between particles to analyze weak randomness from classical sources.
2. Quantum correlations allowed verification of randomness quality and amplification of weak randomness into strong randomness.
3. The output can be certified as genuinely random meeting cryptographic security standards.

Potential Applications

1. Lotteries and gaming systems requiring certified fairness benefit from amplified randomness.
2. Blockchain systems rely on unpredictable randomness for consensus mechanisms and security.
3. Auditing and compliance requiring verifiable randomness for selection processes.
4. Secure digital infrastructure protecting critical systems from predictable vulnerabilities.

Limitations

1. Setup is currently large, complex, and laboratory-based limiting practical deployment.
2. Output rates are much lower than commercial random-number generators requiring optimization for practical use.
3. Significant research and development needed for miniaturization and scalability.

3.Cybercrime Context and Impact

Understanding Cybercrime

1. Cybercrime refers to criminal activities involving use of computers, networks, and digital technologies.
2. Encompasses wide range of illicit activities in virtual space including data theft, system compromise, and unauthorized access.
3. Cybercriminals employ various techniques and tools exploiting vulnerabilities in networks and systems.

Crime Statistics

1. As per NCRB Crime in India 2024 Report, overall crime rate in India declined by 6% in 2024 compared with 2023.
2. However, there was increase of over 17% in cybercrime cases showing rising digital threats.

National Security Implications

1. Cybercrime poses threat to national security when state-sponsored actors or criminal organizations target critical infrastructure.
2. Government institutions and military systems are high-priority targets for sophisticated cyber-attacks.

Data Breach Consequences

1. Data breaches lead to exposure of personal information, trade secrets, intellectual property, and confidential data.
2. Breach impacts include financial losses, regulatory penalties, and reputational damage.

Service Disruption Risks

1. Cyber-attacks disrupt essential services including power grids, communication networks, and transportation systems.
2. Infrastructure attacks create cascading failures affecting millions of people.

Reputational Damage

1. Organizations falling victim to cyber-attacks often suffer reputational damage affecting customer trust and market position.

4.Government of India's Cybersecurity Initiatives

Indian Computer Emergency Response Team (CERT-In)

1. CERT-In is national nodal agency for responding to cybersecurity incidents providing proactive and reactive support.
2. Provides critical role in ensuring security and resilience of country's cyber infrastructure.

National Critical Information Infrastructure Protection Centre (NCIIPC)

1. Responsible for protecting critical information infrastructure from cyber threats identifying and designating critical sectors.
2. Advises organizations in critical sectors on enhancing cybersecurity measures.

Cyber Crime Prevention Against Women & Children (CCPWC) Scheme

1. Ministry of Home Affairs provides financial assistance to States and UTs supporting cyber forensic-cum-training laboratories.

2. Supports training and hiring of junior cyber consultants addressing skill gaps.

Indian Cyber Crime Coordination Centre (I4C)

1. Provides framework and ecosystem for Law Enforcement Agencies dealing with cybercrimes comprehensively.
2. Joint Cyber Coordination Teams constituted for seven regions enabling coordinated response.

National Cyber Crime Reporting Portal

1. Launched enabling public to report all types of cybercrimes facilitating rapid response.
2. Toll-free number 1930 operationalized for cyber complaint assistance.
3. Citizen Financial Cyber Fraud Reporting and Management System enables immediate financial fraud reporting.

Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre)

1. Creates awareness about botnet and malware infections providing detection and cleaning tools.
2. Provides cybersecurity tips and best practices for citizens and organizations.

5.Way Forward

1. **Scale Randomness Amplification** - Develop practical implementations of quantum randomness amplification for commercial deployment.
2. **Strengthen Cybersecurity Infrastructure** - Enhance CERT-In and NCIIPC capabilities for rapid threat detection and response.
3. **Promote Cyber Awareness** - Conduct nationwide campaigns on cybersecurity best practices and threat awareness.
4.
5. **Support Research** - Fund quantum computing and cryptography research developing next-generation security technologies.
6. **International Cooperation** - Collaborate with international cybersecurity bodies on threat intelligence and response mechanisms.

Source - **https -//www.thehindu.com/sci-tech/science/technique-to-amplify-random-numbers-is-digital-security-breakthrough/article71076263.ece# -~ -text=By%20tapping%20into%20the%20power,for%20any%20attacker%20to%20predict&text=Most%20digital%20security%20relies%20today%20on%20random%20numbers%20to%20generate%20cryptographic%20keys.**