Quantum TRNG for Secure Data Transmission

DR. S. K. Rajalakshmi[1], M. Logeshwari[2], S. Swasthika Janani[3], R. Priyadharshini[4]

[1]Assistant Professor Department of Electronics and communication Engineering, A.V.C College of Engineering, Mayiladuthurai, Tamil Nadu

[2,3,4]IV-ECE, Department of Electronics and communication Engineering A.V.C College of Engineering, Mayiladuthurai, Tamil Nadu

DOI: https://doi.org/10.51584/IJRIAS.2026.11010095

Received: 24 January 2026; Accepted: 29 January 2026; Published: 11 February 2026

ABSTRACT

Secure data transmission depends on unpredictable cryptographic keys. Conventional pseudorandom number generators are deterministic and vulnerable to prediction. This work proposes a Quantum True Random Number Generator (Q-TRNG) that uses quantum superposition and noise to produce truly random numbers. The generated quantum entropy is converted into high-quality random bits and applied to secure encryption, improving confidentiality and resistance to attacks. The proposed system offers a reliable and future- ready solution for quantum-grade secure communication.

Keywords: Q-TRNG, Quantum Randomness, Secure Data Transmission, Cryptography, Entropy

INTRODUCTION

Secure data transmission is a fundamental requirement in modern digital systems, including cloud services, IoT networks, financial platforms, and e-governance applications. The confidentiality and integrity of transmitted information depend strongly on cryptographic mechanisms, where the quality of encryption keys is determined by the randomness used during key generation. Most conventional systems rely on pseudo-random number generators (PRNGs), which are software-driven and deterministic, making them vulnerable in security-critical applications **[1]**.which are software-driven and deterministic. Even though PRNGs are fast and widely used, their outputs may become predictable when weak seeding, repeated patterns, environmental influence, or implementation flaws occur. Such predictability creates security gaps that attackers can exploit through key-guessing, traffic analysis, or repeated-sequence attacks.

Quantum True Random Number Generators (Q-TRNGs) provide a stronger alternative by extracting entropy from quantum physical processes that are inherently unpredictable. Unlike algorithm-based randomness, quantum phenomena such as superposition, phase fluctuations, and vacuum noise generate randomness that cannot be reproduced or reverse-engineered. By using optical components like a stabilized laser source, beam splitter, and interference-based sensing, Q-TRNG systems can generate high-entropy random bits suitable for cryptographic operations.

This project focuses on designing a Q-TRNG architecture that produces statistically uniform random numbers and integrates them into secure communication workflows. By strengthening the randomness foundation of encryption, the proposed approach enhances data confidentiality, improves resistance to cyberattacks, and offers a futureready solution for high-security digital transmission environments.

LITERATUREREVIWE

Random number generation is the backbone of modern cryptographic security because it directly impacts key strength, authentication reliability, and resistance to pattern- based attacks. Several studies highlight that pseudo-random number generators (PRNGs), although efficient, may introduce bias or repeatable structures when affected by algorithmic limitations, weak seeding, or predictable internal states. In contrast, Quantum Random

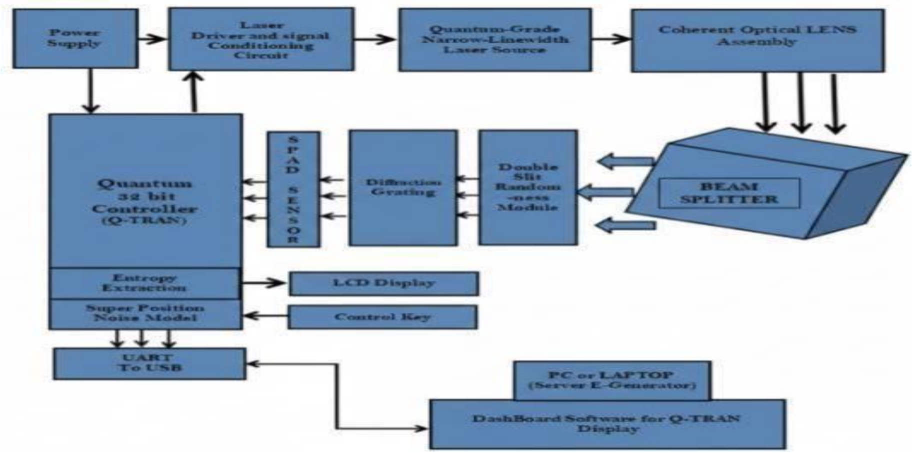
Number Generators (QRNGs) are widely recognized for producing entropy derived from quantum phenomena, enabling improved security for applications such as multifactor authentication, randomized encryption schemes, and one- time-pad style keying methods.

Researchers in quantum-enhanced randomness have explored multiple directions, including quantum gate methods and photon-based systems, each with unique advantages and limitations **[2]**. How ever, such methods often lack guidance for handling qubit error rate variations and may suffer from efficiency concerns when generating random bits using limited qubit resources. Other studies investigate alternative randomness models, such as cellular automata-based systems and neural networkdriven generators, aiming to increase unpredictability. Yet, these approaches frequently provide limited realworld validation, incomplete security analysis, and insufficient scalability discussions.

PROPOSEDMETHODALOGY

The proposed system designs a Quantum True Random Number Generation (Q-TRNG) framework for strengthening secure data transmission and cryptographic protection. Instead of depending on deterministic pseudo- random generators, the model obtains randomness directly from IBM's real-time quantum computing environment, ensuring that generated values are highly unpredictable and resistant to pattern-based attacks.

Initially, the quantum platform prepares qubits in a superposition state using quantum gate operations such as the Hadamard transformation. The system performs repeated measurements on the qubits, where each observation produces an unbiased binary output (0 or 1). These measurement results are collected as a raw quantum bitstream. To ensure reliability, the generated stream is continuously monitored and tested to avoid repeated sequences or external influence.


Power Supply
Laser Driver and signal Conditioning Circuit
Quantum-Grade Narrow-Linewidth Laser Source
Coherent Optical LENS Assembly
Quantum 32 bit Controller (Q-TRAN)
SPAD SENSOR
Diffraction Grating
Double Slit Random -ness Module
BEAM SPLITTER
Entropy Extraction
Super Position Noise Model
LCD Display
Control Key
UART To USB
PC or LAPTOP (Server E-Generator)
DashBoard Software for Q-TRAN Display

The obtained quantum random numbers demonstrate high entropy and unpredictability, making them suitable for cryptographic applications, as validated through standard statistical tests **[3]**. First, a primality evaluation is performed to validate whether generated values can serve as strong prime candidates when required for secure encryption routines. Next, the random outputs are utilized in the padding mechanism, where additional random characters are inserted to match encryption block requirements and prevent plaintext pattern leakage. Finally, the input data file is encrypted using the quantum-derived keys, and the system performs security validation by analyzing integration strength and vulnerability resistance.

The final outcome of this methodology is a scalable and efficient quantum-enabled randomness generation pipeline that improves encryption robustness, increases key unpredictability, and supports secure communication with minimal manual intervention.

RESULTS & DISCUSSION

The Quantum True Random Number Generator (Q- TRNG) was implemented on IBM Cloud's quantum computing platform, utilizing its live environment to generate truly unpredictable random values. The system relied on preparing qubits in superposition states, ensuring that each measurement outcome was fundamentally random and not influenced by classical computational patterns.

Measurements were performed repeatedly, producing binary sequences that were then converted into decimal numbers for analysis and practical use. Across multiple runs and varying numbers of qubits, the sequences displayed non- repetitive patterns and probability distributions that closely approached uniformity, reflecting the inherent randomness of quantum superposition. Minor fluctuations in the distribution were observed due to quantum decoherence and hardware noise, but the overall quality of randomness remained high.

The quantum-generated numbers were applied to cryptographic operations such as key generation and padding. Compared to traditional pseudorandom generators, these outputs exhibited greater unpredictability, minimizing susceptibility to pattern-based attacks and enhancing the security of encrypted data. These results confirm that IBM's quantum platform can reliably produce high-entropy, unbiased random numbers, providing a practical and scalable solution for secure data communication in modern cryptographic systems.

CONCLUSION

The integration of cloud computing, cryptography, and quantum physics paves the way for highly secure data management. Developing quantumresistant algorithms, interdisciplinary collaboration, and strategic approaches will ensure robust cybersecurity and advance nextgeneration cryptographic architectures.

REFERENCES

1. S. T. Author et al., "A Method for Implementing a SHA256 Hardware Accelerator Inside a Quantum True Random Number Generator (QTRNG)," in Proc. 2025 IEEE International Conference on Quantum Cryptography and Secure Systems, IEEE Xplore, 2025.
2. "Quantum and Post-Quantum Cryptography," in Cyber Security and Digital Forensics: Challenges and Future Trends, IEEE Xplore, 2025.
3. Rukhin et al., "A statistical test suite for random and pseudorandom number generators," NIST Special Publication 800-22, 2022.