Entropy Analysis and Statistical Testing of a QRNG through Q-Auth.

1. Introduction

Random number generators (RNGs) are essential in cryptography, simulations, and statistical modeling. While classical RNGs, such as pseudo-random number generators (PRNGs) and hardware RNGs, have inherent limitations due to their design, quantum random number generators (QRNGs) leverage quantum phenomena to produce inherently unpredictable outputs. This paper evaluates a QRNG, analyzing its entropy estimates ("h_initial") through NIST SP 800-90B and subjecting its outputs to the comprehensive NIST Statistical Test Suite. The QRNG's performance is compared to classical sources, including the 32-bit Linear Feedback Shift Register (LFSR) and Intel's RDSEED, highlighting its superiority in both entropy and randomness validation.

2. Methodology

2.1 QRNG Implementation

The QRNG under evaluation employs quantum processes to generate binary sequences. The outputs were tested over 10 trials, each producing sufficient data for statistical evaluation.

2.2 Entropy Testing

The NIST SP 800-90B entropy test suite was used to calculate the "h_initial" metric, quantifying the entropy per bit of the random output. This metric serves as a benchmark for randomness quality. The results were compared with classical RNG sources, specifically the 32-bit LFSR and RDSEED.

2.3 NIST Statistical Test Suite

To ensure comprehensive randomness validation, the QRNG's output was subjected to the NIST Statistical Test Suite. This suite evaluates the following:

1. Frequency (Monobit) Test
2. Frequency Test within a Block
3. Runs Test
4. Test for the Longest Run of Ones in a Block
5. Binary Matrix Rank Test
6. Discrete Fourier Transform (Spectral) Test
7. Non-overlapping Template Matching Test
8. Overlapping Template Matching Test
9. Maurer's "Universal Statistical" Test
10. Linear Complexity Test
11. Serial Test
12. Approximate Entropy Test
13. Cumulative Sums (Cusum) Test
14. Random Excursions Test
15. Random Excursions Variant Test

The QRNG passed all 15 tests across all trials, affirming its compliance with stringent randomness requirements.

2.4 Classical RNG Comparisons

- **32-bit LFSR:** A pseudo-RNG known for periodic outputs and deterministic patterns.
- **RDSEED:** A hardware RNG utilizing thermal noise but susceptible to potential biases and side-channel vulnerabilities.

3. Analysis

3.1 QRNG Entropy Results

Statistics:

- **Average Entropy:** 6.9404
- **Standard Deviation:** 0.0893

3.2 Classical RNG Results (Reference Data):

32-bit LFSR:

- **Average Entropy:** 6.870 (per byte, equivalent to 0.859 per bit)
- **Observations:** High standard deviation (0.058 per bit) indicating variability and lower randomness quality.

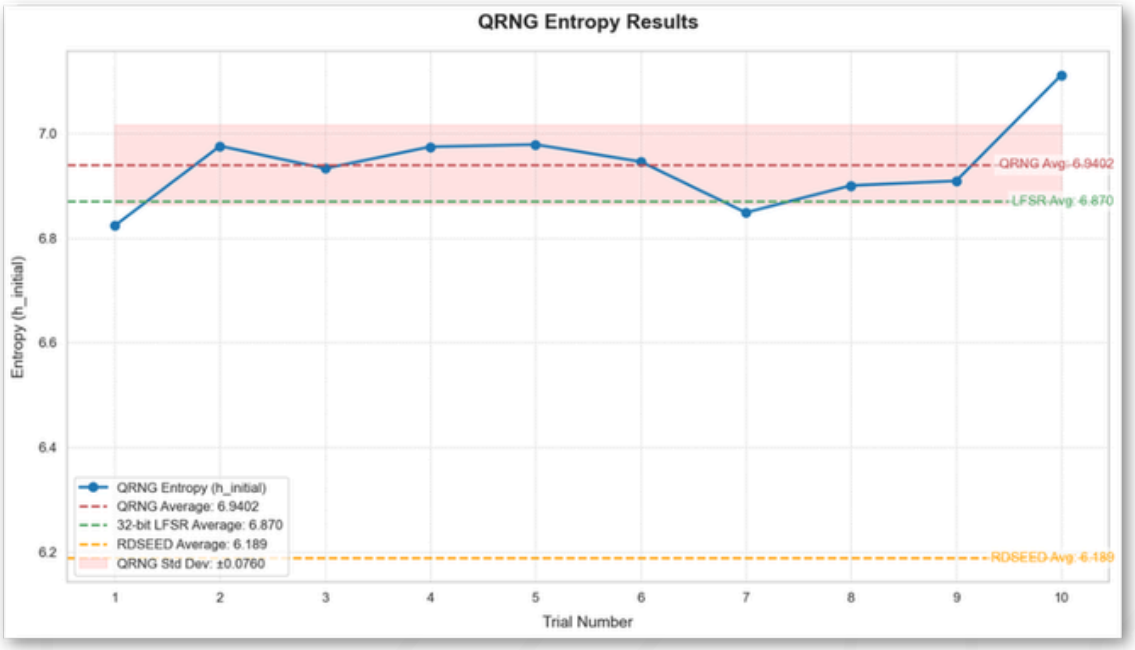
RDSEED:

- **Average Entropy:** 6.189 (per byte, equivalent to 0.852 per bit)
- **Observations:** Lower average entropy compared to both the 32-bit LFSR and the QRNG, highlighting potential statistical biases.

3.3 Comparative Insights

The QRNG consistently achieved entropy estimates higher than both RDSEED and the 32-bit LFSR. With an average entropy of 6.9404, it surpasses the classical sources while maintaining a lower variability (standard deviation of 0.0893), demonstrating superior statistical consistency. Furthermore, the QRNG passed all 15 tests in the NIST Statistical Test Suite for every trial, ensuring exceptional compliance with randomness standards.

4. Results & Validation



- **Entropy Validation:** The QRNG consistently achieved high entropy estimates, surpassing classical RNG sources in average entropy and statistical consistency.

- **Randomness Validation:** The QRNG passed all 15 tests in the NIST Statistical Test Suite across all trials, confirming its reliability for cryptographic and scientific applications.

5. Conclusion

This analysis establishes the QRNG as a next-generation randomness source, excelling in both entropy and comprehensive statistical validation. Its superior entropy estimates and successful completion of all 15 NIST Statistical Test Suite tests underscore its capability as a reliable RNG for critical applications. By eliminating deterministic patterns and leveraging quantum phenomena, the QRNG provides a robust solution to meet the stringent requirements of modern cryptography and simulations.