Assessing Predictability in Quantum-Generated Random Sequences through Statistical Analysis

Sepehr Akbari

Aptil 15, 2025

1 Hypothesis

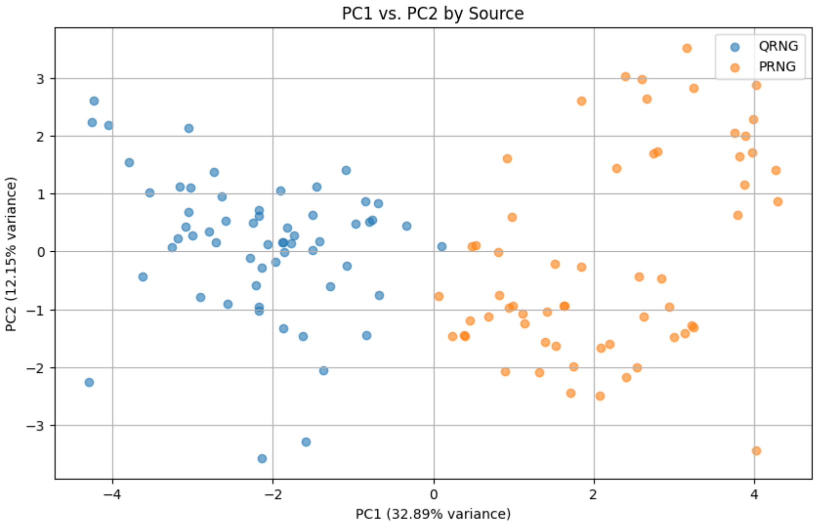
This study is motivated by the fundamental distinction between classical pseudorandom number generators (PRNGs) and quantum random number generators (QRNGs). While PRNGs produce sequences that appear random but are ultimately generated by deterministic algorithms, QRNGs rely on the inherently probabilistic nature of quantum measurements, making them theoretically unpredictable.

We hypothesize that sequences generated by QRNGs exhibit stronger statistical randomness properties than those generated by classical PRNGs. Specifically, we propose that QRNG outputs will demonstrate greater uniformity, reduced structural dependencies, and less evidence of periodic behavior compared to widely-used PRNGs such as Mersenne Twister (MT19937), Linear Congruential Generator (LCG), and XORShift.

Furthermore, we anticipate that through statistical testing across multiple dimensions of randomness—namely uniformity, structural patterns, and periodicity—QRNGs will consistently outperform classical generators. This performance gap will be quantifiable via a composite randomness score derived from principal component analysis (PCA) of various test outputs, offering a statistically robust framework for evaluating unpredictability in random number sequences.

2 Results

To assess the quality of randomness in quantum and classical generators, we applied a suite of statistical tests categorized across three dimensions: uniformity, structural patterns, and periodicity. The results were aggregated into a feature vector for each generator output, followed by principal component analysis (PCA) to reduce dimensionality and identify key discriminative features.



As shown in the Figure, the PCA projection of the test results reveals a clear separation between quantum-generated sequences (QRNG) and classical pseudo-random generators (PRNGs) along the first principal component (PC1), which accounts for 32.89% of the total variance. Quantum samples cluster tightly on the left, while classical sources — including MT19937, LCG, and XORShift — are distributed more widely on the right. This separation confirms that the statistical characteristics of QRNG outputs are distinct and consistently different from those of classical PRNGs.

2.1 Uniformity

Across tests such as Chi-squared, Kolmogorov–Smirnov (KS), and Frequency tests, PRNGs generally yielded higher p-values (e.g., KS 0.00025 vs. QRNG's 0.00038), indicating slightly better adherence to theoretical distributions. However, the Empirical Mean from the Equidistribution test was nearly ideal for QRNG (0.5009 vs. PRNG's 0.4997), suggesting a balanced bit output.

2.2 Structural Patterns

QRNG outperformed PRNGs in terms of serial autocorrelation, with a lower correlation coefficient (–0.0053 for QRNG vs. –0.00076 for PRNGs on average), implying reduced sequential dependencies. QRNG's Permutation Test and Gap Test also showed more irregularity in structure, although all sources exhibited very small p-values, suggesting detectable patterns in all cases when tested at high sensitivity.

2.3 Periodicity

In the Entropy Test, QRNG sequences had slightly lower entropy (3.441 vs. 3.447 for some PRNGs), though all values were close to the theoretical maximum of $\log_2(10) \approx 3.32$–3.47 range. QRNG also demonstrated shorter dominant periods (8.6 vs. 16.9 for PRNG) and higher dominant frequencies in the Fourier Transform test, reinforcing the lack of long-range periodic patterns.

2.4 Overview

The PCA-based separation reflects these underlying statistical differences. The QRNG sequences exhibited greater randomness across multiple dimensions, especially in terms of structure and periodicity. While classical PRNGs were optimized for uniformity, subtle deterministic patterns remain detectable through higher-order statistical measures.

3 Outcome

Randomness is a cornerstone of modern computational science, underpinning fields ranging from cryptography and statistical sampling to physical simulations and artificial intelligence. In domains that aim to faithfully replicate or model the unpredictability of nature — such as Monte Carlo simulations, molecular dynamics, and climate modeling — the presence of subtle patterns or periodicities in pseudo-random number generators (PRNGs) can lead to biased or inaccurate outcomes. As such, there is growing interest in the use of quantum random number generators (QRNGs), which exploit quantum indeterminacy to produce theoretically uncorrelated outputs.

Our analysis demonstrates that quantum-generated sequences differ meaningfully from those of PRNGs across multiple statistical dimensions, particularly in measures of structure and periodicity. While PRNGs often achieve excellent uniformity, their algorithmic nature leaves detectable traces that QRNGs avoid. This distinction makes QRNGs increasingly attractive for high-stakes applications where even minor deviations from ideal randomness can accumulate and skew results.

To support further research and practical adoption, we are developing an open-source Python package that simplifies the process of evaluating randomness. This tool will incorporate our full testing suite and composite scoring methodology, allowing researchers, engineers, and educators to rigorously assess randomness in their own data — whether from simulations, hardware sources, or generative algorithms.

In bridging statistical rigor with quantum capabilities, our work contributes to a growing foundation for trustworthy randomness in computation, reinforcing the role of quantum technologies in next-generation scientific and cryptographic systems.