RQI-Audit: Variance Attribution and Automated Statistical Certification of Random Number Generators Across Programming Language Environments

Rodriguez Munoz, Jose (School: Dr. Pedro Albizu Campus)

Random number generation underpins cryptography, simulation, distributed systems, and machine learning, yet the relative impact of generator architecture versus programming language implementation remains poorly quantified. This study resolves that question through a controlled, large-scale systems evaluation and introduces RQI-Audit, a deployable framework for automated statistical certification of randomness in software environments. Default and cryptographically secure generators were evaluated across Python, C/C++, Java, JavaScript, Go, and Rust using pinned Docker environments, fixed runtime versions, and documented seed policies to ensure reproducibility. For each language-generator pair, 177 independent sequences of 5.64 million 64-bit integers were generated and evaluated using NIST SP 800-22, selected TestU01 components, entropy metrics, collision statistics, and autocorrelation analysis. Results were aggregated into a power-calibrated Randomness Quality Index that preserves detection sensitivity under fixed compute budgets. Factorial analysis showed that generator architecture explains 92% of variance in statistical quality, while programming language contributes 2%, establishing generator selection as the dominant design decision. Modern generators such as MT19937, PCG, and Xoshiro remain stable across languages, while linear congruential generators exhibit systematic degradation. A controlled corruption suite injected structural defects to validate detection sensitivity. ROC analysis achieved near-perfect discrimination between valid and corrupted outputs, with AUC above 0.997. RQI-Audit enables continuous, reproducible auditing of randomness in CI pipelines and reduces the risk of undetected statistical failure in security-critical and data-driven systems.

Awards Won: