



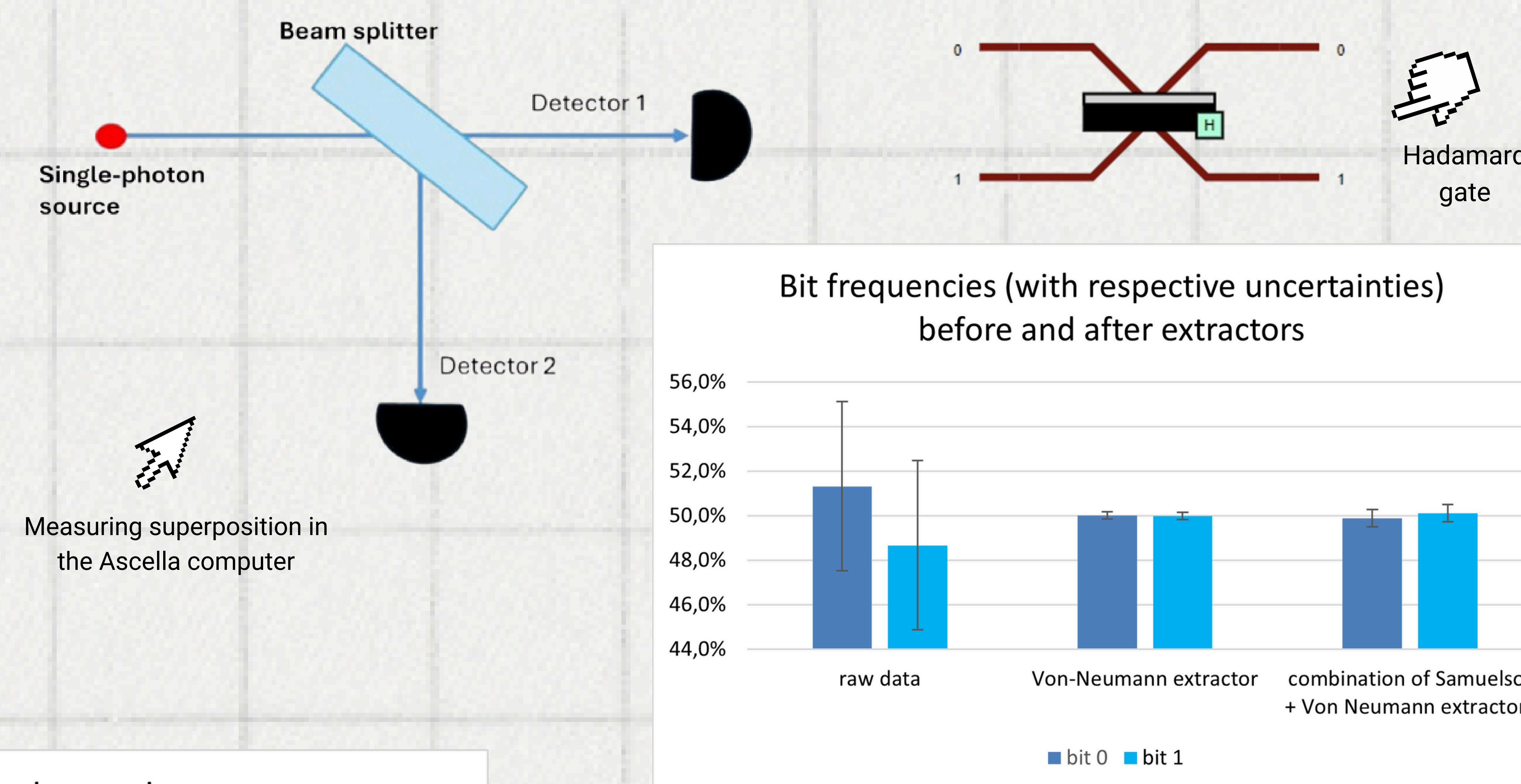
Metrological Analysis of a QRNG Based on the Quandela Photonic Quantum Computer

AUTHORS: MURIEL A. DE SOUZA; FLÁVIA P. AGOSTINI; LUIZ VICENTE G. TARELHO
NATIONAL INSTITUTE OF METROLOGY, QUALITY AND TECHNOLOGY (INMETRO) - BRAZIL
EMAIL: MSOUZA@INMETRO.GOV.BR

ABSTRACT: RANDOM SEQUENCES WERE GENERATED USING A HADAMARD GATE ON A PHOTONIC QUANTUM COMPUTER, FOLLOWED BY METROLOGICAL ANALYSIS. AS THE RAW DATA DID NOT SATISFY NIST RANDOMNESS CRITERIA, RANDOMNESS EXTRACTORS WERE APPLIED TO ENHANCE STATISTICAL QUALITY. THE RESULTS HIGHLIGHT THE POTENTIAL OF PHOTONIC QUANTUM COMPUTING FOR RELIABLE RANDOM NUMBER GENERATION AND THE IMPORTANCE OF METROLOGICAL ASSESSMENTS.

INTRODUCTION

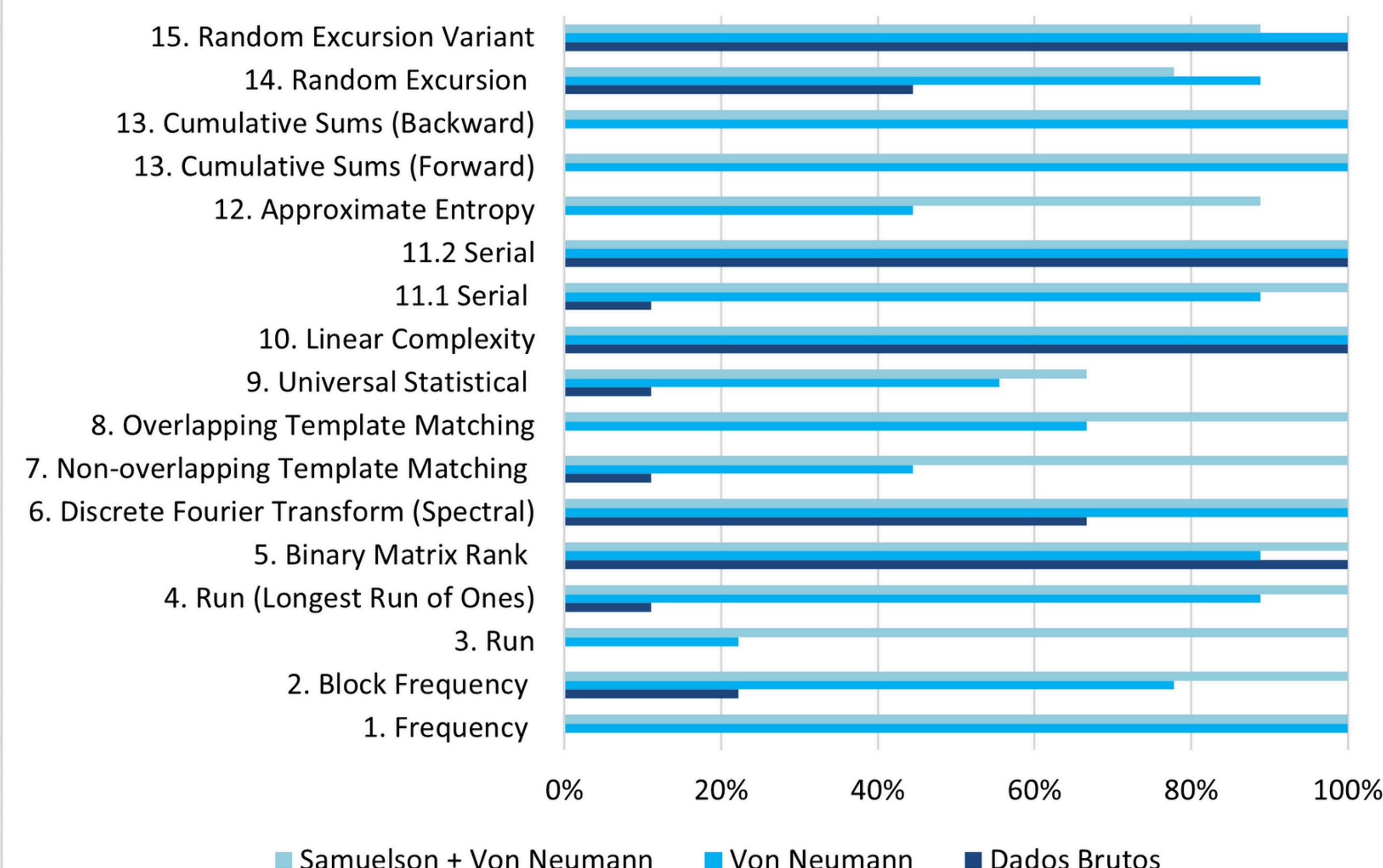
This study investigates quantum random number generation using Quandela's cloud-based quantum computer, Ascella. Photons and beam splitters are employed to create fundamentally random sequences by inducing superposition, acting as a Hadamard gate. In Quandela's system, each qubit consists of two modes and a single photon, which, upon passing through a beam splitter, has an equal probability of exiting as bit 0 or bit 1. Metrological analysis included tests on the optimal photon count, as well as assessments of sequence repeatability and reproducibility before and after applying randomness extractors.



METHODOLOGY

Tests demonstrated that using a single photon per detection event was the optimal approach, as it minimized interference effects. To assess the quality of randomness, statistical tests from NIST SP800-22 and NIST SP800-90B were applied, evaluating biases and independence. Additionally, post-processing techniques were implemented using Von Neumann and Samuelson + Von Neumann extractors to further reduce biases and enhance the overall randomness quality.

Percentage of sequences passing the randomness tests
NIST P800-22



RESULTS

- BIT FREQUENCY DISTRIBUTIONS WERE INITIALLY ANALYZED, AIMING FOR A 50% BALANCE BETWEEN 0S AND 1S. THE SEQUENCES UNDERWENT NIST SP800-22 RANDOMNESS TESTS, WHERE RAW DATA FAILED SEVERAL ASSESSMENTS. POST-PROCESSING USING VON NEUMANN AND SAMUELSON + VON NEUMANN EXTRACTORS SIGNIFICANTLY IMPROVED RANDOMNESS, ALIGNING BIT DISTRIBUTIONS WITH THE IDEAL 50%.
- ENTROPY ANALYSIS WITH NIST SP800-90B REVEALED THAT ALL RAW SEQUENCES FAILED THE IID TEST. AFTER VON NEUMANN EXTRACTION, 22% OF SEQUENCES MET IID CRITERIA, WHILE APPLYING SAMUELSON + VON NEUMANN ENSURED ALL SEQUENCES PASSED, ACHIEVING AN ESTIMATED ENTROPY OF 0.771 ± 0.005 .

REFERENCES

- [1] Quandela, "Quandela Cloud." [Online]. Available: <https://cloud.quandela.com/> [Accessed: Feb. 24, 2025].
- [2] Quandela Team, "Perceval: photonic quantum computing SDK." [Online]. Available: <https://perceval.quandela.net/> [Accessed: Feb. 24, 2025].
- [3] L. E. Bassham et al., "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications," NIST Special Publication (SP) 800-22, National Institute of Standards and Technology, Gaithersburg, MD, 2010. [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-22r1a.pdf> [Accessed: Feb. 24, 2025].
- [4] M. S. Turan et al., "Recommendation for the Entropy Sources Used for Random Bit Generation," NIST Special Publication (SP) 800-90B, National Institute of Standards and Technology, Gaithersburg, MD, 2018. [Online]. Available: <https://csrc.nist.gov/publications/detail/sp/800-90b/final> [Accessed: Feb. 24, 2025].

