Quantum Random Number Generation using Quandela Photonic Quantum Computer

Muriel A. de Souza

msouza@inmetro.gov.br

Instituto Nacional de Metrologia, Qualidade e Tecnologia

Flávia P. Agostini

Instituto Nacional de Metrologia, Qualidade e Tecnologia

Luiz Vicente G. Tarelho

Instituto Nacional de Metrologia, Qualidade e Tecnologia

Research Article

Keywords: Random Number, Photonic Quantum Computer, Quandela, Ascella.

Posted Date: April 2nd, 2024

DOI: https://doi.org/10.21203/rs.3.rs-4177514/v1

Additional Declarations: No competing interests reported.

Version of Record: A version of this preprint was published at Quantum Information Processing on November 23rd, 2024. See the published version at https://doi.org/10.1007/s11128-024-04593-6.

Quantum Random Number Generation using Quandela Photonic Quantum Computer

Muriel A. de Souza[1*], Flavia P. Agostini[1] and Luiz Vicente G. Tarelho[1]

[1*]Instituto Nacional de Metrologia, Qualidade e Tecnologia, INMETRO, Av. Nossa Senhora das Graças, 50, Duque de Caxias, 25250-020, Rio de Janeiro, Brazil.

*Corresponding author(s). E-mail(s): msouza@inmetro.gov.br;
Contributing authors: fpagostini@inmetro.gov.br;
lvtarelho@inmetro.gov.br;

Abstract

Quantum mechanics, characterized by its intrinsically probabilistic nature, offers a promising avenue for random number generation, which is essential for applications such as cryptography and computational simulations. With the recent advancements in quantum computing and simulation, numerous studies have emerged utilizing these methods for the generation of random numbers. This research delves into the exploration of random number generation utilizing the Ascella photonic quantum computer developed by Quandela, renowned for its implementation of single-photon-based qubits. Leveraging both the Ascella photonic simulator (SIM Ascella) and the quantum processing unit (QPU Ascella) within the Perceval framework, this investigation examines the capability to generate random sequences through the superposition of quantum states, generated using photons and beam splitters. The analysis includes a performance comparison between simulations and experimental tests with the quantum computer, subjecting the outcomes to the NIST SP 800-22 randomness tests. While initial simulations suggested a high degree of randomness, practical implementation revealed certain disparities attributed to factors such as decoherence, imperfections in beam splitters and single-photon sources, as well as quantum noise. This study contributes to the understanding of random number generation on quantum platforms, identifying challenges and limitations while providing strategies for future enhancements in this quantum technology.

Keywords: Random Number, Photonic Quantum Computer, Quandela, Ascella.

1 Introduction

Quantum technologies emerge as a revolutionary frontier in science and technology, heralding an era of unprecedented advances and challenging our conventional understanding of computing and information security[1]. At the heart of these advancements lies quantum computing, which, by leveraging the principles of quantum mechanics, promises to solve complex problems far beyond the capacity of classical supercomputers. This transformative potential is particularly significant in the generation of random numbers, a critical aspect in various areas such as cryptography, information security, and computational simulations. The pursuit of truly random numbers leads to quantum physics, due to its inherently probabilistic nature. Through this, various quantum random number generators have been developed, exploring different sources of entropy and detection systems to produce pure randomness [2–9].

The significance of generating intrinsically random numbers is magnified by the advent of quantum computers. The security of cryptographic systems, for instance, fundamentally relies on the randomness of the generated keys. With quantum computers capable of running powerful algorithms like Shor's algorithm[10], the need for robust randomness becomes even more critical to reinforce cryptographic security. Furthermore, quantum computers are designed to simulate complex quantum systems where randomness is an intrinsic feature, highlighting the need for reliable sources of randomness.

However, many of the numbers currently used under the premise of being random are not genuinely so, as they originate from deterministic algorithms or phenomena. These numbers are termed pseudo-random, for although they may satisfy tests for randomness, they are based on seeds that are not intrinsically random to generate longer sequences[11]. To address this issue, one turns to quantum physics and quantum principles, such as superposition, which are inherently unpredictable and cannot be replicated. Quantum superposition has profound implications for both quantum computing and the generation of random numbers. Quantum processes, such as quantum tunneling or photon splitting, generate random outcomes that, due to the superposition of quantum states, are intrinsically unpredictable, and these outcomes can thus be harnessed to obtain truly random numbers[12].

One method of generating truly random numbers that has gained prominence in recent years is through the use of quantum computers, as they are based on fundamental quantum principles. Experiments conducted in 2019 demonstrated the use of IBM's 20-qubit quantum computer, the 20Q Tokyo[13], where qubits were prepared in a quantum superposition state between the $|0\rangle$ and $|0\rangle$ states, through the application of a Hadamard (H) gate, and then measured. This represents the simplest example of measuring qubits in superposition to generate random numbers; however, the results obtained showed that the samples were biased and correlated, necessitating post-processing to pass statistical tests[14]. Subsequent papers have been published using multiple H gates[15] and other combinations of quantum logic gates[16–18].

Currently, various types of quantum computers are being developed around the world, and in this paper, an optical quantum computer, the Quandela[19, 20], is utilized, which was developed by a French company established in 2017 and uses single-photon-based qubits. The aim of this work is to prepare qubits in a quantum

superposition of states (through the use of beam splitters) and perform measurements, in order to generate random sequences. This optical quantum computer is equipped with an open source framework for programming photonic quantum computers called Perceval[21], which is accessible via the Quandela Cloud platform[22].

The first section of this study provides a brief overview of quantum computers, discussing their various types. Following this, an explanation of Quandela's optical quantum computer is given, highlighting its specific features. In section 3, the tests conducted using the Perceval framework are detailed, emphasizing the procedure and methodology employed. Subsequently, in section 4, the results obtained are presented, including an analysis of the randomness tests to which they were subjected.

2 Quantum Computers

Quantum computing emerges as a revolutionary frontier in computer science, promising to transform the way calculations are performed and complex problems are approached. This multidisciplinary field merges the fundamental principles of quantum mechanics with information theory, presenting a revolutionary perspective compared to classical computing[23].

In quantum computing, unlike in classical computing, the fundamental unit is the qubit, which stands for "quantum bit." Similar to the bit, the qubit can assume two states, 0 and 1; however, unlike the bit, the qubit possesses the additional capability to exist in superposition states of both[24]. Unlike the classical bit, which relies on electrical signals, the qubit is generated from quantum systems, such as atoms, nuclear spins, or polarized photons. The states 0 and 1 are encoded through a "computational basis" $|0\rangle$, $|1\rangle$, where the notation "$|\ \rangle$" represents states in Quantum Mechanics. A qubit can exist in two states: pure, akin to the classical bit, and in superposition, represented as a linear combination of the fundamental states, $\alpha|0\rangle + \beta|1\rangle$, where α and β are complex coefficients and $|\alpha|^2$ and $|\beta|^2$ are the probabilities of measuring the states $|0\rangle$ and $|1\rangle$, respectively[25].

The race for quantum technology is advancing rapidly in both academia and industry. Various companies and research groups are focused on the ambitious goal of building quantum computers that can significantly enhance computational power[26]. Currently, different types of quantum computers are being developed, each with its peculiarities regarding development and manufacturing. Among them are: trapped ion computers, which use ions trapped by electromagnetic fields and whose qubits are represented by the energy states of the ions[23]; nuclear magnetic resonance quantum computers, which use the spin states of molecular nuclei as qubits[23]; superconducting quantum computers, where the superconducting qubits are made from electrical circuits, including capacitors and Josephson junctions[27]; photonic quantum computers, which utilize photons as qubits, among others.

Concurrently with hardware, specific software is being developed to leverage the unique properties of qubits, enabling the execution of quantum computations. Simulators are essential tools for the development of quantum algorithms, and cloud availability has democratized access to some quantum computers.

2.1 Quandela

Photonic quantum computers utilize photons as qubits, and operations are performed using linear optics, such as beam splitters, rotation plates, phase shifters, and interferometers. Quandela stands out for its ability to operate at room temperatures and is currently engaged in the development and commercialization of sources for optical qubits based on single photons. However, achieving this purity in the emission of single photons is a highly challenging task, necessitating the implementation of active methods to suppress the probability of multiple photon emission[28].

The characterization of the single-photon source is conducted through the study of the source's purity and the indistinguishability of the photons. The purity is tested via its second-order correlation function g(2), where P(n) is the probability of having n photons per event, which can be approximated to:

$$g(2) \approx \frac{2P(2)}{[P(1)]^2} \tag{1}$$

For an ideal single-photon source, the number of coincidences is zero, and therefore, g(2) = 0. In practice, the aim is to minimize the value of this second-order correlation function. The value obtained for the source developed by Quandela is 0.019[28]. The indistinguishability of the produced photons can be measured using a Hong-Ou-Mandel interferometer[29] and studying its visibility (V_{HOM}), which has a value of 1 when the number of coincidences is equal to 0 (the ideal case, where the photons are completely indistinguishable). For the single-photon source developed by Quandela, this visibility equals 0.918[28].

The production of single photons is achieved through the use of heralded photons, generated by the process of Spontaneous Parametric Down-Conversion (SPDC). This nonlinear optical phenomenon occurs when an incident photon in a nonlinear crystal is converted into two photons of lower energy. Due to the quantum entanglement of these converted photons, the detection of one allows the inference of the existence of the second, without the need for direct measurement[28].

2.1.1 Encoding of qubits

In this photonic quantum computer, qubits are created through "path encoding," where two spatial modes per photon are used. Essentially, the presence of the photon in one of the two modes can represent the basic quantum states $|0\rangle$ and $|1\rangle$. This technique of using two modes to represent a binary state is the basis for defining a qubit. Thus, using "i" photons and "2i" modes, one can define an input quantum state with "i" qubits [30]. By using the input state passing through the linear optical circuit of "m" modes, and using the "n-i" remaining single photons, and "m-2i" remaining modes as ancillary modes and photons (to perform appropriate post-selections), any unitary transformation of "i" qubits on the input state can be implemented, thereby enabling universal quantum computing[30], as suggested by the famous Knill-Laflamme-Milburn protocol for universal quantum computing with qubits [31].

2.1.2 Perceval Framework

Perceval is an open-source software integrated in a Python library used by Quandela to model and test quantum optical systems[21]. It allows for the construction of photonic quantum circuits using beam splitters, wave plates etc., or sub-circuits with fixed numbers of spatial modes ("photon paths"). A distinct feature of Ascella QPU Simulator is its ability to incorporate different types of noise into the models it simulates. This is crucial for an accurate representation of quantum systems in the real world, where factors such as photon loss, decoherence, and thermal fluctuations can significantly impact performance[30]. Perceval operates based on detailed simulation of quantum optical components, such as single-photon sources, beam splitters, interferometers, and detectors. It utilizes advanced algorithms to model the behavior of these components under various configurations and operational conditions[30].

3 Methodology

The generation of random numbers using quantum computers available in the cloud is a rapidly evolving field, with a growing number of publications over the last 5 years [13–18, 32–35]. These publications are based on quantum superposition, which is a property of quantum mechanics that distinguishes it from classical physics. In this property, a quantum system can exist simultaneously in multiple states, and the inherent randomness arises from the uncertainty of the system until measurement is performed.

One method of generating random numbers using single photons involves a beam splitter (BS). When a photon encounters a BS, it has an equal probability of being transmitted or reflected. Consequently, the photon is placed in a state of quantum superposition, and by measuring which path the photon takes after passing through the beam splitter, a random outcome is obtained (Figure 1). If the photon is detected on the transmission path, the result can be interpreted as 1; if detected on the reflection path, it can be interpreted as 0, thereby generating a bit of random information[36, 37]. Repeating this process multiple times can generate sequences of random bits.

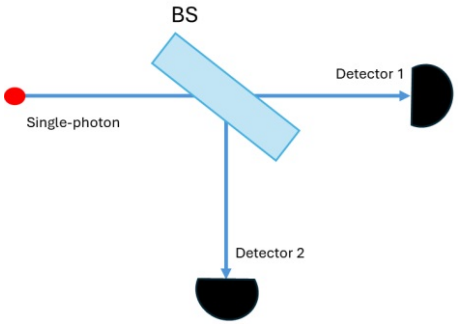


Fig. 1 Generation of random numbers using single photons and a beam splitter (BS)

This article presents the generation of random numbers using the Ascella[38] photonic quantum computer, available on the Quandela Cloud platform[22], which is a single-photon quantum computer. The tests are conducted using the photonic quantum simulator (SIM:Ascella) and the computer itself (QPU:Ascella, where QPU stands for "Quantum Processing Unit").

3.1 Optical Circuit

In the Perceval environment, a circuit was configured as illustrated in Figure 2, which details the "paths" of photon entry and exit, in addition to the beam splitter, operating with 1 photon, and consequently 2 modes, representing 1 qubit. The Fock state [1,0] was created, representing the qubit state $|0\rangle$, where 1 photon enters through path 0. These experiments were initially carried out on the quantum simulator (SIM:Ascella) to test the program and subsequently on the quantum computer hardware (QPU:Ascella). Series of measurements were conducted with 1 Mb (megabit) each, allowing for the testing of the optical quantum computer, as well as evaluating the accuracy and fidelity of the simulator in replicating experimental conditions.

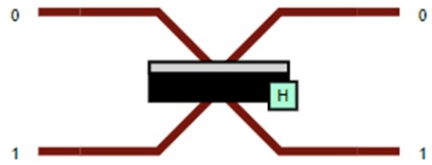


Fig. 2 Circuit constructed for the generation of random numbers using a beam splitter, 1 photon, and two modes (1 qubit)

Upon conducting the measurements, a minimal incidence, close to 0.005%, of [1,1] events was observed, corresponding to photons emerging simultaneously at both outputs. These results are due to imperfections in the source, and this occurrence is recorded even with the use of the simulator, calibrated to emulate the noises present in the actual quantum computer. As a result, the Fock states [1,0] and [0,1], corresponding to the qubits —0⟩ and —1⟩, respectively, were obtained. The frequency of each state was evaluated, and the results of this investigation are illustrated in Figure 3.

4 Results and discussion

Series of measurements were conducted with 1 Mbits each. An analysis of the frequency of occurrence of the quantum states —0⟩ and —1⟩, corresponding to the Fock states [1,0] and [0,1], respectively, was carried out to evaluate the behavior of both the simulator and the quantum computer. Ideally, an equitable distribution of the states is expected, with a frequency of 50% for each. The output Fock states [1,1] did not impact the result, and, as can be seen in Figure 3, the performance of the quantum hardware has not yet reached the ideal frequency.

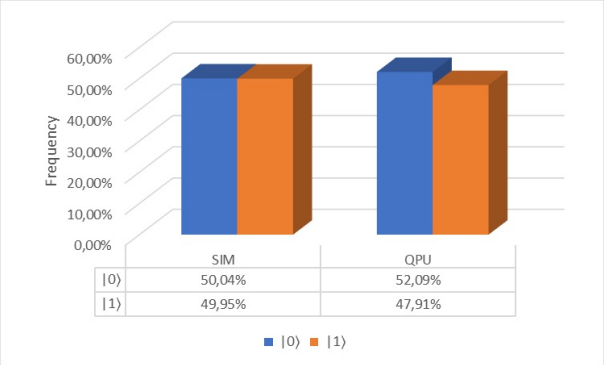


Fig. 3 Histogram of the frequency of occurrence of each quantum state for the Ascella quantum computer and simulator – Quandela

4.1 Randomness tests

The primary objective of randomness testing is to conduct a statistical assessment of a generator's ability to produce bits that are unbiased and uncorrelated. For this purpose, analyses are conducted on the output of the generator, where unwanted patterns, trends, or repetitions may indicate flaws in randomness. To this end, there are various established test suites, among them, the NIST SP 800-22 test suite[39], developed by the National Institute of Standards and Technology in the United States. This suite consists of a series of statistical procedures designed to examine different aspects of randomness. Each test focuses on a specific characteristic of the generator's output, such as the distribution of values, the frequency of patterns, the presence of repetitive sequences, among others, aiming to detect deviations from ideally random behavior. The tests contained in this suite demonstrate the quality of the randomness generated, allowing for the identification and correction of potential vulnerabilities.

In the research, 15 distinct tests were applied:

1 - *Frequency:* to determine if the number of ones and zeros is approximately the same (as shown in Figure 3);

2 - *Frequency Test within a Block:* to determine if the proportion of ones within a block of M bits is approximately M/2;

3- *Runs Test:* to test the total number of uninterrupted sequences of identical bits;

4 - *Test for the Longest Run of Ones in a Block:* to test if the Longest Run is consistent with what is expected in a random sequence;

5 - *Binary Matrix Rank:* to check for linear dependence among fixed-length substrings of the original sequence;

6 - *Discrete Fourier Transform (FFT):* to detect periodic features;

7 - *Non-overlapping Template Matching:* divides the sequence into blocks and searches for template matches in each block without allowing overlaps;

8 - *Overlapping Template Matching:* to search for all possible template matches, including overlaps;

9 - *Maurer's "Universal Statistical":* the aim of the test is to detect whether or not the sequence can be compressed without loss of information;

10 - *Linear Complexity:* to determine if the sequence is complex enough to be considered random;

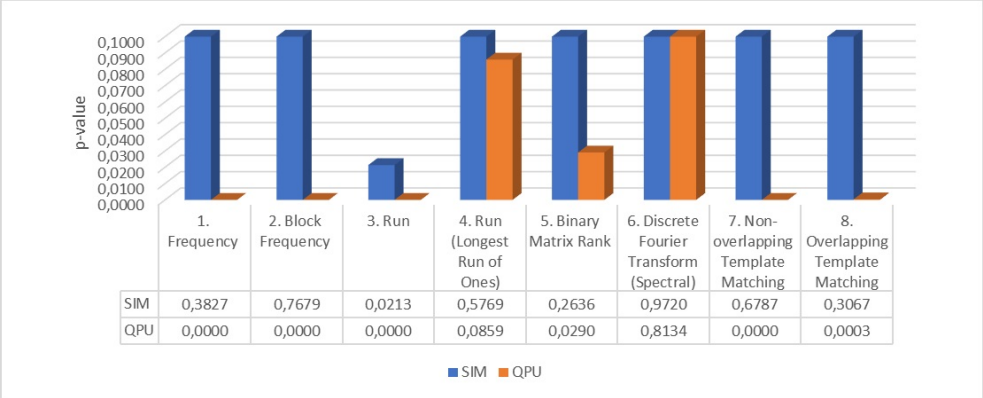
11 - *Serial:* This test focuses on the frequency of all possible overlapping m-bit patterns;

12 - *Approximate Entropy:* the frequency of all possible overlapping m-bit patterns;

13 - *Cumulative Sums (forward and reverse):* adjusts digits to -1 and 1 and determines the cumulative sums, which should be close to zero;

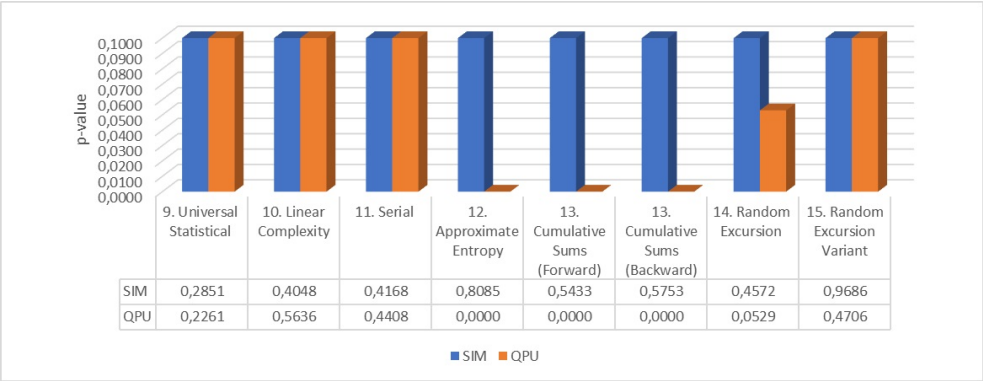
14 - *Random Excursions:* to detect deviations in the distribution of the number of visits of the random walk to a certain "state";

15 - *Random Excursions Variant:* to analyze the total number of visits to each state across the sequence;



	1. Frequency	2. Block Frequency	3. Run	4. Run (Longest Run of Ones)	5. Binary Matrix Rank	6. Discrete Fourier Transform (Spectral)	7. Non-overlapping Template Matching	8. Overlapping Template Matching
SIM	0,3827	0,7679	0,0213	0,5769	0,2636	0,9720	0,6787	0,3067
QPU	0,0000	0,0000	0,0000	0,0859	0,0290	0,8134	0,0000	0,0003

Fig. 4 Results for the p-value, utilizing NIST statistical tests from 1 to 8



	9. Universal Statistical	10. Linear Complexity	11. Serial	12. Approximate Entropy	13. Cumulative Sums (Forward)	13. Cumulative Sums (Backward)	14. Random Excursion	15. Random Excursion Variant
SIM	0,2851	0,4048	0,4168	0,8085	0,5433	0,5753	0,4572	0,9686
QPU	0,2261	0,5636	0,4408	0,0000	0,0000	0,0000	0,0529	0,4706

Fig. 5 Results for the p-value, utilizing NIST statistical tests from 9 to 15

In this study, a significance level α of 0.01 was adopted, implying that results with a p-value lower than α are interpreted as non-random. Figures 4 and 5 illustrate the p-values obtained in all 15 tests applied to both the simulator (SIM:Ascella) and the quantum computer hardware (QPU:Ascella). For optimized visualization of the results, the maximum value for the y-axis in the graphs was set to 0.1. It is important to note that no data post-selection was performed. For the Random Excursion and Random Excursion Variant tests (14 and 15), which yield multiple p-values as outcomes, the Fisher's Combined Probability Test[40] was employed to aggregate these values into a singular p-value result. This method facilitates a consolidated statistical interpretation from multiple test outcomes.

It was observed that the simulator passed all tests, demonstrating adequate generation of random sequences. However, the performance of the QPU revealed limitations, not meeting the randomness criteria in 8 out of the 15 tests applied. This finding suggests the need for post-processing of the data generated by the QPU so that the results can be considered adequately random and, consequently, applicable to practical needs.

Simulations play a crucial role in the development and testing of physical hardware. They enable users to test optical quantum circuits in a simulated environment, modeling the behavior of photons in superposition, albeit on a classical computer, which generates sequences known as pseudo-random. The QPU:Ascella hardware performs real experiments, thus being limited to the quantum technologies available at the moment. Discrepancies encountered may arise from various factors, such as decoherence, one of the primary challenges in quantum computing, resulting from the loss of the system's quantum properties; imperfections in the beam splitter (BS) or the single-photon source; quantum noise, including thermal and electromagnetic fluctuations; and measurement errors, stemming from various sources due to imperfections in measurement devices.

The photonic quantum computer developed by Quandela has made significant strides in quantum computing and has specialized in the development of single-photon sources, bringing numerous technological advancements, especially in the field of photonic quantum computers. This study not only highlights Quandela's significant contributions to advancing quantum computing but also underscores the importance of continuous improvement to overcome existing challenges in the field. Quandela's efforts in overcoming these challenges and its dedication to enhancing quantum technology are indispensable for the evolution of this promising field.

5 Conclusion

This study explored the ability of the photonic quantum computer Ascella, developed by Quandela, to generate random numbers, a crucial element in fields such as cryptography and computational simulations. Using both a photonic simulator (SIM:Ascella) and the quantum hardware (QPU:Ascella), the randomness of the sequences generated in controlled and practical environments was compared. While the simulated environment met randomness standards in all 15 NIST SP 800-22 tests, the performance of the quantum hardware revealed discrepancies. Specifically, the QPU Ascella did not

pass 8 of the NIST tests: Frequency Test, Block Frequency Test, Runs Test, Non-Overlapping and Overlapping Template Machine, Approximate Entropy Test, and Cumulative Sums Test. These failures indicate an uneven distribution of zeros and ones, high predictability, and deviations in cumulative sums, among others, questioning the purity and unpredictability of the sequences generated by the QPU in question. The discrepancies between the simulator and real hardware results highlight the challenges faced in the physical implementation of quantum systems for random number generation. Factors such as decoherence, imperfections in beam splitters and single-photon sources, quantum noise, and measurement errors significantly contribute to the limitations observed in the performance of quantum hardware. This work emphasizes the significant impact of Quandela's contributions to the field of quantum computing and the importance of future research to overcome technical challenges, improving the accuracy of components, calibration and error correction, all crucial for the continuous evolution of quantum technology.

Acknowledgements. We are very much thankfull and acknowledge the use of Quandela Cloud Plataform for this work. The views expressed are those of the authors and do not reflect the official policy or position of Quandela team.

References

[1] Tzalenchuk, A., Spethmann, N., Prior, T., Hendricks, J.H., Pan, Y., Bubanja, V., Temporão, G.P., Yu, D.-H., Ilić, D., Goldstein, B.L.: The expanding role of national metrology institutes in the quantum era. Nature Physics **18**(7), 724–727 (2022) https://doi.org/10.1038/s41567-022-01659-z

[2] Leone, N., Azzini, S., Mazzucchi, S., Moretti, V., Pavesi, L.: Certified quantum random-number generator based on single-photon entanglement. Physical Review Applied **17**(3), 034011 (2022) https://doi.org/10.1103/PhysRevApplied.17.034011

[3] Ma, X., Yuan, X., Cao, Z., Qi, B., Zhang, Z.: Quantum random number generation. npj Quantum Information **2**(1), 1–9 (2016) https://doi.org/10.1038/npjqi.2016.21

[4] Applegate, M., Thomas, O., Dynes, J., Yuan, Z., Ritchie, D., Shields, A.: Efficient and robust quantum random number generation by photon number detection. Applied Physics Letters **107**(7) (2015) https://doi.org/10.1063/1.4928732

[5] Bronner, P., Strunz, A., Silberhorn, C., Meyn, J.-P.: Demonstrating quantum random with single photons. European journal of physics **30**(5), 1189 (2009) https://doi.org/10.1088/0143-0807/30/5/026

[6] Wayne, M.A., Jeffrey, E.R., Akselrod, G.M., Kwiat, P.G.: Photon arrival time quantum random number generation. Journal of Modern Optics **56**(4), 516–522 (2009) https://doi.org/10.1080/09500340802553244

[7] Ma, H.-Q., Xie, Y., Wu, L.-A.: Random number generation based on the time of arrival of single photons. Applied optics **44**(36), 7760–7763 (2005) https://doi.org/10.1364/AO.44.007760

[8] Hai-Qiang, M., Su-Mei, W., Da, Z., Jun-Tao, C., Ling-Ling, J., Yan-Xue, H., Ling-An, W.: A random number generator based on quantum entangled photon pairs. Chinese Physics Letters **21**(10), 1961 (2004) https://doi.org/10.1088/0256-307X/21/10/027

[9] Jennewein, T., Achleitner, U., Weihs, G., Weinfurter, H., Zeilinger, A.: A fast and compact quantum random number generator. Review of Scientific Instruments **71**(4), 1675–1680 (2000) https://doi.org/10.1063/1.1150518

[10] Bhatia, V., Ramkumar, K.: An efficient quantum computing technique for cracking rsa using shor's algorithm. In: 2020 IEEE 5th International Conference on Computing Communication and Automation (ICCCA), pp. 89–94 (2020). https://doi.org/10.1109/ICCCA49541.2020.9250806 . IEEE

[11] Mannalatha, V., Mishra, S., Pathak, A.: A comprehensive review of quantum random number generators: Concepts, classification and the origin of randomness. Quantum Information Processing **22**(12), 439 (2023) https://doi.org/10.1007/s11128-023-04175-y

[12] Biswas, R., Roy Talukdar, D., Roy, U.: Verifying the reliability of quantum random number generator: A comprehensive testing approach. SN Computer Science **5**(1), 140 (2024) https://doi.org/10.1007/s42979-023-02323-w

[13] Tamura, K., Shikano, Y.: Quantum random number generation with the superconducting quantum computer ibm 20q tokyo. Cryptology ePrint Archive (2020)

[14] Tamura, K., Shikano, Y.: Quantum random numbers generated by a cloud superconducting quantum computer. In: International Symposium on Mathematics, Quantum Theory, and Cryptography: Proceedings of MQC 2019, pp. 17–37 (2021). https://doi.org/10.1007/978-981-15-5191-8_6 . Springer Singapore

[15] Kumar, V., Rayappan, J.B.B., Amirtharajan, R., Praveenkumar, P.: Quantum true random number generation on ibm's cloud platform. Journal of King Saud University-Computer and Information Sciences **34**(8), 6453–6465 (2022) https://doi.org/10.1016/j.jksuci.2022.01.015

[16] Salehi, R., Razaghi, M., Fotouhi, B.: Hybrid hadamard and controlled-hadamard based quantum random number generators in ibm qx. Physica Scripta **97**(6), 065101 (2022) https://doi.org/10.1088/1402-4896/ac698b

[17] Kumar, V., Pravinkumar, P.: Quantum random number generator on ibm qx. Journal of Cryptographic Engineering, 1–7 (2023) https://doi.org/10.1007/s13389-023-00341-1

[18] Kumar, V., Pravinkumar, P.: Simulation of qtrng on ibm's q experience using rotation and phase quantum gates. International Journal of Theoretical Physics **62**(8), 179 (2023) https://doi.org/10.1007/s10773-023-05422-9

[19] Senellart, P.: Semiconductor single-photon sources: progresses and applications. Photoniques (107), 40–43 (2021) https://doi.org/10.1051/photon/202110740

[20] Maring, N., Fyrillas, A., Pont, M., Ivanov, E., Stepanov, P., Margaria, N., Hease, W., Pishchagin, A., Au, T.H., Boissier, S., *et al.*: A general-purpose single-photon-based quantum computing platform. arXiv preprint arXiv:2306.00874 (2023) https://doi.org/10.48550/ARXIV.2306.00874

[21] Heurtel, N., Fyrillas, A., De Gliniasty, G., Le Bihan, R., Malherbe, S., Pailhas, M., Bertasi, E., Bourdoncle, B., Emeriau, P.-E., Mezher, R., *et al.*: Perceval: A software platform for discrete variable photonic quantum computing. Quantum **7**, 931 (2023) https://doi.org/10.22331/q-2023-02-21-931

[22] Quandela Cloud. Available in: https://cloud.quandela.com/. Access at: March 20, 2024

[23] Ladd, T.D., Jelezko, F., Laflamme, R., Nakamura, Y., Monroe, C., O'Brien, J.L.: Quantum computers. nature **464**(7285), 45–53 (2010) https://doi.org/10.1038/nature08812

[24] Nandhini, S., Singh, H., Akash, U.: An extensive review on quantum computers. Advances in Engineering Software **174**, 103337 (2022) https://doi.org/10.1016/j.advengsoft.2022.103337

[25] Nielsen, M.A., Chuang, I.L.: Quantum computation and quantum information: 10th anniversary edition (2010) https://doi.org/10.1017/CBO9780511976667

[26] Yang, Z., Zolanvari, M., Jain, R.: A survey of important issues in quantum computing and communications. IEEE Communications Surveys & Tutorials (2023) https://doi.org/10.1109/COMST.2023.3254481

[27] Wang, Y.: Analysis on the mechanism of superconducting quantum computer. In: Journal of Physics: Conference Series, vol. 1634, p. 012040 (2020). https://doi.org/10.1088/1742-6596/1634/1/012040 . IOP Publishing

[28] Boissier, S.: Single-Photon Sources (Part 1). Available in: https://medium.com/quandela/single-photon-sources-part-1-517d9c1a22bc. Access at: March 08, 2024

[29] Hong, C.-K., Ou, Z.-Y., Mandel, L.: Measurement of subpicosecond time intervals between two photons by interference. Physical review letters **59**(18), 2044 (1987) https://doi.org/10.1103/PhysRevLett.59.2044

[30] Quandela/Perceval. Available in: https://github.com/Quandela/Perceval/blob/

main/CONTRIBUTING.md.%20Perceval. Access at: March 13, 2024

[31] Knill, E., Laflamme, R., Milburn, G.J.: A scheme for efficient quantum computation with linear optics. nature **409**(6816), 46–52 (2001) https://doi.org/10.1038/35051009

[32] Yadav, A., Mishra, S., Pathak, A.: Partial loopholes free device independent quantum random number generator using ibm's quantum computers. arXiv preprint arXiv:2309.05299 (2023) https://doi.org/http://arxiv.org/abs/2309.05299

[33] Jacak, M.M., Jóźwiak, P., Niemczuk, J., Jacak, J.E.: Quantum generators of random numbers. Scientific Reports **11**(1), 16108 (2021) https://doi.org/10.1038/s41598-021-95388-7

[34] Orts, F., Filatovas, E., Garzón, E.M., Ortega, G.: A quantum circuit to generate random numbers within a specific interval. EPJ Quantum Technology **10**(1), 17 (2023) https://doi.org/10.1140/epjqt/s40507-023-00174-1

[35] Sinha, A., Henderson, E.R., Henderson, J.M., Larson, E.C., Thornton, M.A.: A programmable true random number generator using commercial quantum computers. In: Quantum Information Science, Sensing, and Computation XV, vol. 12517, pp. 35–49 (2023). https://doi.org/10.1117/12.2663497 . SPIE

[36] Kollmitzer, C., Petscharnig, S., Suda, M., Mehic, M.: Quantum random number generation, 11–34 (2020) https://doi.org/10.1007/978-3-319-72596-3_2

[37] Huang, L., Zhou, H., Feng, K., Xie, C.: Quantum random number cloud platform. npj Quantum Information **7**(1), 1–7 (2021) https://doi.org/10.1038/s41534-021-00442-x

[38] Team, Q.: Exploring Ascella, the Single-Photon Quantum Computing Prototype. Available in: https://medium.com/quandela/exploring-ascella-the-single-photon-quantum-computing-prototype-af92f9133428. Access at: January 16, 2024

[39] Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Barker, E., Leigh, S., Levenson, M., Vangel, M., Banks, D., Heckert, A., et al.: A statistical test suite for random and pseudorandom number generators for cryptographic applications **22** (2001) https://doi.org/10.6028/NIST.SP.800-22r1a

[40] Zhang, H., Wu, Z.: The generalized fisher's combination and accurate p-value calculation under dependence. Biometrics **79**(2), 1159–1172 (2023) https://doi.org/10.1111/biom.13634