# Random number generator by quantum simulator and tests of randomness

**M A Souza[1], F P Agostini[1] and L V G Tarelho[1]**

[1] Division of Metrology for Information and Communication Technology (Dmtic),
Inmetro, Duque de Caxias, 25250-020, Brazil

msouza@inmetro.gov.br

**Abstract**. Quantum simulators have gained significant attention in recent years due to their ability to simulate quantum systems and generate random numbers with the potential for enhanced randomness compared to classical methods. This paper explores the generation of random numbers using quantum simulators and evaluates the randomness of these numbers through various randomness tests. We present an overview of quantum simulators, discuss the principles behind quantum random number generation, and provide an in-depth analysis of randomness tests commonly used to assess the quality of random number sequences. Our findings highlight the strengths and limitations of quantum simulators in generating random numbers and shed light on the effectiveness of different randomness tests in evaluating their randomness.

## 1. Introduction

The concept of random numbers is crucial across various fields, including cryptography, statistical analysis, and Monte Carlo simulations. Traditional random number generators often rely on deterministic algorithms and initial seed values, which may lead to predictable patterns or biases in the generated sequences. Quantum simulators, on the other hand, leverage the inherent randomness and uncertainty of quantum mechanics to produce random numbers that exhibit improved statistical properties.

For measurements in the classical context, it is understood that a certain property of nature has a numerical value. That is, there is a determinism that is inherent in classical physics. With the development of quantum physics, there was a paradigm shift, as magnitudes are intrinsically probabilistic. When a measurement is performed, the result is totally unpredictable, because the properties of objects are uncertain and can only be described probabilistically by a wave function.

With the development of quantum computers with exponentially greater processing capacity than the current ones, and with the innovation process that can be called the Fourth Industrial Revolution, truly random cryptographic keys will be increasingly necessary to guarantee reliability and confidentiality in the exchange and storage of information. The availability of a quantum random number generator is fundamental for the evaluation of cryptographic security modules, since a huge number of cryptographic protocols make use of random numbers and depend on the quality of these random numbers so that adequate levels of security can be guaranteed.

Due to the recent security breach of cryptographic key protocols (Snowden Case in 2013) based on pseudorandom numbers, in 2016 NIST published new recommendations for the use of entropy sources as random number generators and launched in 2018 a service based on the Internet (Web Service) for generating random numbers - Randomnes's Beacon (https://beacon.nist.gov/home). Brazil participates in a joint effort between Chileans and Americans to implement these cyber-physical systems to improve the quality of information security protocols, such as Inmetro's Randomness Beacon (https://beacon.inmetro.gov.br/).

The development of security standards for the random number generation process foresees the construction of an entropy source based on quantum entanglement so that it can be used as a truly random number generator. In this stage of the project, a software that simulates a quantum optics laboratory was used to test optical devices, interferometers, and generate quantum states, to obtain the simplest and most reliable experiment possible.

The software used was *Quantum Flytrap – Virtual Lab* [2]. A HOM interferometer was mounted through it and a detector was placed in each of the two outputs of the beam splitter. Simulations of 100 points, 500 points and 1000 points were made. The results obtained were tested following the article "*A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*" published by NIST in 2001 [3] and passed at least two thirds of the tests. These obtained data cannot be used for random keys that require a high level of security, as this is a computational simulation. However, as the numerical sequences passed in many tests, we have that they are random sequences, but with certain vulnerability in production, that is, they are "pseudorandom" numbers.

## 2. Methodology

### *2.1. Physical concepts*

A quantum random number generator is formed by an entropy source, a physical interaction (interferometer) and a detection system. As a source of entropy, single photon sources are generally used, as this is an application that depends on the quantum nature of light. One way to obtain this type of source is through pairs of correlated photons (figure 1), in which the detection of a photon announces the existence of a twin photon, through Spontaneous Parametric Down Conversion (SPDC), which is a probabilistic process and serves both to produce single photon states, and to explore quantum entanglement [4].

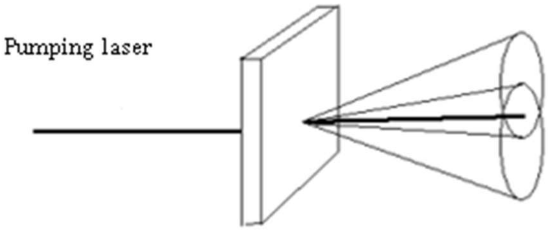


**Figure 1.** Laser pumping a BBO crystal, producing twin photons via SPDC, and emerging from the crystal in separate cones.

SPDC is a non-linear process that converts a photon of higher energy into a pair of photons with lower energy (called signal and idler), respecting the conservation of momentum and energy [5]. It is made using a laser to "pump" a non-linear crystal, which in this project is BBO (Beta-Barium-Borate). Entangled states can be generated in several degrees of freedom, but the most used is polarization entanglement, as it is easier to work with, since there are several optical devices to control this polarization [6]. Quantum entanglement only occurs when the two converted photons are in a quantum superposition of states [7]. With this, it is possible to create the four states shown in equations 1 and 2, known as Bell States, because they strongly violate Bell's inequality [6].

$$|\psi^{\pm}\rangle = \left(|H_1V_2\rangle \pm |H_2V_1\rangle\right)/\sqrt{2} \tag{1}$$

$$|\varphi^{\pm}\rangle = \left(|H_1H_2\rangle \pm |V_2V_1\rangle\right)/\sqrt{2} \tag{2}$$

The interferometer used is the HOM (figure 2), which receives this name because it was developed by three researchers: C. K. Hong, Z. Y. Ou, and L. Mandel, from the University of Rochester [8]. In this interferometer, photons converge to a beam splitter (BS) and interfere with each other in a non-classical way [9].

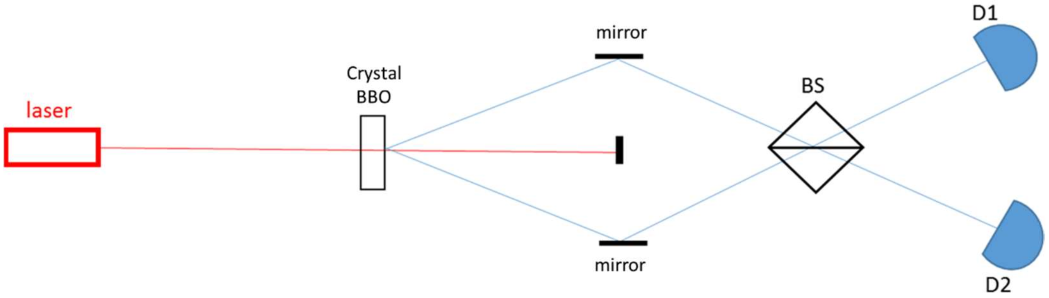


**Figure 2.** HOM interferometer: twin photons interfere in the beam splitter and hit either detector 1 or detector 2.

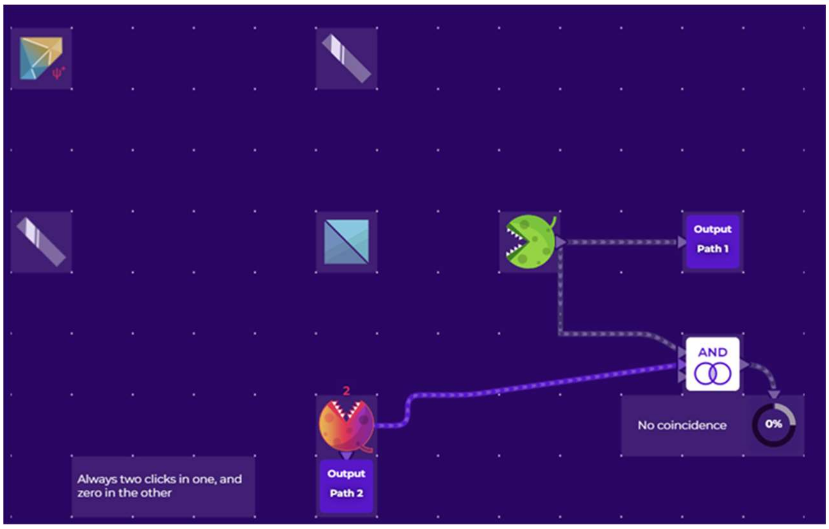
In this interferometer, there is no detection of coincidences. And this is the phenomenon used to generate random numbers, because the probability that both photons leave through port 1 is 50%, as well as the probability that both photons leave through port 2. As there is no coincidence and only one of the detectors is sensitized, the click in one detector can be considered as being bit 0 and in the other as being bit 1.

### *2.2. Proposed experiment*

The simulation of quantum random number generation was performed using the Quantum Flytrap – Virtual Lab software. In this software it is possible to choose the type of photon source, polarizers, mirrors, filters, types of detectors, and operations between them. Mirrors were used to align the interferometer and direct the photons to the beam splitter, which is a Polarized Beam Splitter (PBS). In the detection system, a single photon detector was used in each PBS output. The two detectors are linked together and record each photon that hits them, as well as if there are coincidences, that is, if two detectors receive photons within the same time interval window (figure 3).

For the generation of random numbers, the events in which the two photons hit the same detector were considered. Bit 1 was standardized when the two photons reach detector 1 and bit 0 when the two photons reach detector 2. For this, the interferometer was aligned so that the coincidence counts were zero.

In data acquisition, it is possible to choose the desired flux of photons per second and the number of points to be collected. The results obtained are saved in csv format and exported to a data sheet to be processed.



Always two clicks in one, and zero in the other

**Figure 3.** Using Quantum Flytrap – Virtual Lab to simulate the interferometer. The schematic shows the twin photon source, alignment mirrors, beam splitter, and detectors.

## 3. Results and discussion

Three measurement cycles were performed, each with an average of 30 waves per second. In the first cycle, 100 bits were collected, in the second, 500 bits and in the third, 1,000 bits.

A total of 15 randomness tests were performed according to the NIST publication [3]. There are 15 different tests that correspond to:

- Frequency: to determine if the number of ones and zeros is approximately the same.
- Frequency Test within a Block: determine whether the proportion of ones within a block of M bits is approximately M/2.
- Runs Test: test the total number of uninterrupted sequences of identical bits (called run).
- Test for the Longest Run of Ones in a Block: test if the Longest Run is consistent with what is expected in a random sequence.
- Binary Matrix Rank: check the linear dependence between fixed-length substrings of the original sequence.
- Discrete Fourier Transform (Spectral): detect periodic features.
- Non-overlapping Template Matching and Overlapping Template Matching: detect generators that produce occurrences of a certain pattern.
- Universal Statistical: The purpose of the test is to detect whether the sequence can be compressed without loss of information.
- Linear Complexity: determine whether the sequence is complex enough to be considered random.
- Serial: The focus of this test is the frequency of all possible overlapping m-bit patterns.
- Approximate Entropy: frequency of all possible overlapping m-bit patterns.
- Cumulative Sums: adjust the digits to -1 and 1 and determine the cumulative sums that must be close to zero.
- Random Excursions and Random Excursions Variant: Random Walk within the cumulative sums and test their variances.

These tests were done using a Python program. None of the datasets passed the Universal Statistical test, that is, no sequence can be compressed without losing information. In the Binary Matrix Rank, Overlapping Template Matching and Linear Complexity tests, the sets with 100 and 500 points were not approved. The test for the Longest Run did not pass for the smallest sequence of points due to insufficient data (table 1). Based on these results, it can be inferred that a higher number of bits leads to improved performance in generating random numbers.

**Table 1.** Results for NIST test. When the obtained probability (p) is greater than 0.01, the result is considered true. Tests that do not pass are marked as F (false).

| Statistical test | p-value (100 points) | p-value (500 points) | p-value (1000 points) |
|---|---|---|---|
| Frequency | 0.68915 | 0.79513 | 0.36085 |
| Frequency Test within a Block | 0.68915 | 0.22373 | 0.79680 |
| Runs Test | 0.67692 | 0.04681 | 0.41162 |
| Test for the Longest Run | 0.0 (F) | 0.62208 | 0.65001 |
| Binary Matrix Rank | -1.0 (F) | -1.0 (F) | 0.29189 |
| Discrete Fourier Transform | 0.64635 | 0.79631 | 0.64079 |
| Non-overlapping Template Matching | 0.99999 | 0.53341 | 0.06487 |
| Overlapping Template Matching | 0.0 (F) | 0.0 (F) | 0.88658 |
| Universal Statistical | -1.0 (F) | -1.0 (F) | -1.0 (F) |
| Linear Complexity | -1.0 (F) | -1.0 (F) | 0.80883 |
| Serial | 0.49896 | 0.49896 | 0.25184 |
| Approximate Entropy | 1.0 | 1.0 | 0.97163 |
| Cumulative Sums | 0.54073 | 0.51959 | 0.38911 |
| Random Excursions | 0.95024 | 0.74359 | 0.39425 |
| Random Excursions Variant | 0.31731 | 0.68486 | 0.39646 |

This paper presented an in-depth analysis of random numbers generated by quantum simulators and their evaluation using various randomness tests. Quantum simulators offer promising prospects for generating enhanced random numbers compared to classical methods. However, careful analysis and assessment of these generated sequences through randomness tests are necessary to ensure their suitability for specific applications. Further research and advancements in quantum simulators will likely continue to enhance the generation of random numbers and strengthen their applications in cryptography, secure communication, and statistical analysis.

## References

[1] Pironio, S., Acín, A., Massar, S., Giroday, A. B., Matsukevich, D. N., Maunz, P., Monroe, C. (2010). Random Numbers Certified by Bell's Theorem. Nature.

[2] Quantum Flytrap – Virtual Lab, 2022. Available in: https://lab.quantumflytrap.com/. Access at: July 18th, 2023.

[3] Rukhin, Andrew & Soto, Juan & Nechvatal, James & Smid, Miles & Barker, Elaine. (2001). A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST Special Publication 800-22, Gaithersburg, MD, US,. 800. 163.

[4] Chunnilall, C. J., Degiovanni, I. P., Kück, S., Müller, I., & Sinclair, A. G. (2014). Metrology of single-photon sources and detectors: a review. Optical Engineering, 53.

[5] Rubin, M. H. (1996). Transverse correlation in optical spontaneous parametric down-conversion. Physical Review A, 54(6), 5349-5360.

[6] Kwait, P. G., Mattle, K. W., Zeilinger, A., Sergienko, A., & Shih, Y. (11 de dez. de 1995). New High-Intensity Source of Polarization-Entangled Photon Pairs. Physical Review Letters, 75(24), 4337-4341.

[7] LI, Y. (2020). Methods of Generating Entangled Photon Pairs. Journal Of Physics: Conference Series, 1634(1), 012172.

[8] Hong, C. K., Ou, Z. Y., & Mandel, L. (2 de nov. de 1987). Measurement of subpicosecond time intervals between two photons by interference. Physical Review Letters, 59(18), 2044-2046.

[9] Aguilar, G. H., Souza, M. A., GomeS, R. M., Thompson, J., Celeri, G. M., & Walborn, S. P. (9 de maio de 2019). Experimental investigation of linear-optics-based quantum target detection. Physical Review A, 99(5).