Quantum Optics and Laser
Arecchi's wheel experiment

Andrea Turci

October 2024

1 Introduction

Since the early scientific conversations between Isaac Newton and Christiaan Huygens, two renowned scientists have been debating the nature of light for centuries. Their opposing perspectives on the nature of light are very distinct from one another. While researching the photoelectric phenomenon, Newton developed the particle theory of light, arguing that light was made up of tiny particles, or "corpuscles." This hypothesis foreshadowed Einstein's findings. Huygens, on the other hand, maintained that light acted like a wave and extended out from a source in all directions. At the time, phenomena like reflection and diffraction were not well understood, thus this theory was the most widely accepted. Until the development of quantum mechanics in the early 20th century, this wave-particle duality remained unsolved. Experiments like the photoelectric effect and black-body radiation gave compelling evidence for the presence of a discrete character of light.
In this experiment, we focus on two different quantum states of light: thermal states and coherent states, in an attempt to explore the granularity of light by studying its particle-like behavior. Thermal light, which comes from conventional lightbulbs or natural light sources, reflects a wide range of photon energies and has random phase and amplitude changes. Contrarily, coherent light produced by lasers has a restricted distribution due to its closely linked photons with stable phase relationships. We will investigate the discrete photon distributions of these states through this experiment, which will help us understand how various physical circumstances might lead to their emergence.
Lastly, we'll utilize our photons' arrival timings to construct a Quantum Random Number Generator. This is made feasible by the fact that quantum physics makes some operations, like the emission or detection of individual photons, essentially random. Unlike classical random number generators, which are frequently based on deterministic algorithms, we can derive a truly random sequence of numbers by measuring the exact moment at which each photon arrives. This sequence of numbers is dependent on the unpredictability of quantum events, making it more secure and less biased. There are undoubtedly many uses for the randomness produced by this process, ranging from secure communications and encryption to intricate modeling and simulations.

2 Theoretical Framework

In modern quantum optics, the focus has shifted towards understanding the quantum states of light and how these can be manipulated and measured to harness fundamental quantum properties. This experiment leverages two quantum states of light—coherent states and thermal states—in order to explore the random nature of photon arrivals and use them to generate random numbers. Understanding these states and their statistical properties is essential to interpreting the experiment and constructing a Quantum Random Number Generator (QRNG).

2.1 Quantum States of Light: Coherent and Thermal

Light can be described in different quantum states, with each state characterized by distinct photon statistics. Coherent light, typically produced by lasers, represents a highly ordered quantum state where photons maintain a fixed phase relationship. In contrast, thermal light, emitted by conventional sources like light bulbs or the sun, represents a more chaotic state where photons exhibit random fluctuations in phase and amplitude.
Mathematically, the photon statistics of these states can be distinguished by their respective probability distributions. For coherent light, the photon number distribution follows a Poisson distribution:

$$P(n) = \frac{\langle n \rangle^n e^{-\langle n \rangle}}{n!} \tag{1}$$

where $P(n)$ represents the probability of detecting n photons, and $\langle n \rangle$ is the average photon count. The Poisson distribution indicates that photon detection events are statistically independent and the intervals between photon arrivals follow an exponential distribution. This independence is crucial for generating random numbers, as each photon arrival represents a quantum event that cannot be predicted by prior measurements.
On the other hand, thermal light is characterized by a Bose-Einstein distribution:

$$P(n) = \frac{\langle n \rangle^n}{(\langle n \rangle + 1)^{n+1}} \tag{2}$$

which describes the probability of detecting n photons in a thermal state, where $\langle n \rangle = \frac{1}{e^{\frac{\hbar\omega}{kT}} - 1}$. Unlike coherent light, thermal light exhibits greater fluctuations in photon number, with a wider spread around the average photon count. These fluctuations arise due to the random phase and amplitude variations inherent in thermal light. For both distributions, the associated momenta can be found in Appendix 7

2.2 Photon Detection as a Quantum Process

The detection of individual photons is inherently a quantum mechanical process. When a photon is absorbed by a photodetector, it produces a discrete electronic signal, often referred to as a click. Each click corresponds to the detection of a single photon, and the time of each detection is recorded with high precision. Crucially, the arrival times of photons are random, governed by the quantum mechanical nature of the light source.

In the case of coherent light, the arrival of photons follows a Poissonian process, where the time intervals between successive photon detections are exponentially distributed. The probability density function for the time intervals Δt between photon arrivals is given by:

$$f(\Delta t) = \lambda e^{-\lambda \Delta t} \tag{3}$$

where λ is the average photon detection rate. This exponential distribution ensures that the photon detection process is random and that each detection event is independent of previous events. This independence is a critical feature for constructing a quantum random number generator, as it guarantees the unpredictability of the generated random numbers.

2.3 Quantum Random Number Generation (QRNG)

The unpredictability of photon detection events allows us to generate a sequence of truly random numbers. Classical random number generators, such as those based on deterministic algorithms, produce sequences that are fundamentally predictable if the algorithm and initial conditions are known. In contrast, a Quantum Random Number Generator (QRNG) takes advantage of the

inherent randomness in quantum mechanics to produce sequences that are unpredictable, even in principle.
In this experiment, random numbers are generated by detecting the arrival times of photons and extracting random bits from these times. The process can be outlined as follows:

1. Photon Detection: Each photon detection is recorded with a timestamp, denoted as t_i, which represents the exact moment the photon was detected.

2. Time Interval Calculation: The time intervals $\Delta t_i = t_{i+1} - t_i$ between successive photon detections are computed. These time intervals follow the exponential distribution described above, reflecting the random nature of photon arrivals.

3. Bit Extraction: For each pair of consecutive time intervals Δt_i and Δt_{i+1}, a bit is generated. If $\Delta t_{i+1} > \Delta t_i$, a bit value of 1 is assigned; otherwise, a bit value of 0 is assigned. This method exploits the randomness in the detection times to produce a random sequence of bits.

4. Byte Construction: The generated bits are grouped into blocks of 8 to form bytes. These bytes are then used to create a sequence of random numbers. The statistical properties of the sequence can be analyzed to assess its randomness.

The resulting byte distribution is expected to follow a uniform distribution if the photon detection process is truly random. This uniformity is a key indicator that the QRNG is functioning as expected, producing random data suitable for cryptographic and other applications that require high-quality randomness.

2.4 Statistical Measures of Randomness

Several statistical tests can be applied to the generated sequence to assess its degree of randomness. These tests include:

1. Entropy: Entropy is a measure of the unpredictability or randomness of a data sequence. For a binary sequence, the entropy per bit is given by:

$$H_0 = -p_0 \log_2 p_0 - p_1 \log_2 p_1 \tag{4}$$

   where p_0 and p_1 are the probabilities of observing a 0 or 1, respectively. For a truly random sequence, the entropy should approach 1 bit per bit, indicating maximum unpredictability.

2. Chi-Square Test: This test compares the observed frequency distribution of the bytes to the expected uniform distribution. The chi-square statistic is computed as:

$$\chi^2 = \sum \frac{(O_i - E_i)^2}{E_i} \tag{5}$$

   where O_i is the observed frequency of byte i, and E_i is the expected frequency. A small chi-square value indicates that the observed distribution is close to the expected random distribution.

3. Monte Carlo Pi Approximation: The sequence of random numbers can be used to estimate the value of π using a Monte Carlo method. Successive bytes are interpreted as coordinates in a 2D plane, and the proportion of points that fall within the unit circle provides an estimate of π. For a random sequence, the estimate should converge to the true value of π as more points are sampled.

4. Serial Correlation: Serial correlation measures the degree to which each byte in the sequence is correlated with the previous byte. For a truly random sequence, the serial correlation coefficient should be close to zero, indicating no dependency between adjacent bytes. The serial correlation coefficient is calculated as:

$$r = \frac{\sum(x_i - \mu)(x_{i+1} - \mu)}{\sum(x_i - \mu)^2} \tag{6}$$

where x_i are the byte values, and μ is the mean of the sequence.

2.5 Applications and Implications of QRNG

The ability to generate truly random numbers has profound implications for fields such as cryptography, secure communications, and simulations. In cryptography, for example, the security of encryption algorithms relies on the unpredictability of the random numbers used to generate keys. Classical pseudo-random number generators (PRNGs) can be vulnerable to attacks if the underlying algorithm or seed is known, making QRNGs a superior alternative for secure key generation.
In this experiment, the randomness generated by photon detection is compared to a classical pseudo-random number generator. The quantum randomness, as demonstrated through statistical tests, exhibits far superior characteristics in terms of entropy, uniformity, and lack of correlation. This highlights the potential of QRNGs for real-world applications where high-quality randomness is crucial.

3 Apparatus

The experimental setup for investigating the quantum properties of light and generating quantum random numbers is composed of several key optical and electronic components. These components allow the control and manipulation of light, as well as the precise detection and recording of single photons. Below is a detailed description of each component, its function, and its role in the experiment:

1. Gas Tube Laser: The light source in this experiment is a gas laser, which emits coherent light. This type of laser produces a highly monochromatic and phase-stable beam, ideal for experiments requiring precise control over the light's properties. The coherent nature of the emitted light means that photons exhibit a well-defined phase relationship and follow Poissonian statistics, which is crucial for the coherent light regime in this study. The laser also allows the investigation of quantum randomness in a controlled environment.

2. Polarizer: A polarizing filter is placed in the optical path to control the power of the emitted light. By adjusting the orientation of the polarizer, the intensity of the light can be finely tuned. In this way it ensures that the laser output can be controlled to achieve the desired experimental conditions, particularly when switching between the coherent and thermal light regimes.

3. Arecchi Wheel: The Arecchi wheel is a rotating device with a reflective surface that introduces fluctuations in the phase and amplitude of the light beam. When the wheel is stationary, the light remains in a coherent state, but when the wheel is in motion, it simulates thermal light by disrupting the coherent nature of the laser, introducing random fluctuations that mimic the properties of thermal (chaotic) light.

4. Lens: A convex lens is used to focus the beam, ensuring that the light is concentrated onto a small area for precise alignment with the optical system. The focusing of the beam helps optimizing the intensity and direction of the light before it enters the optical fiber, ensuring efficient coupling into the subsequent components.

5. Iris Diaphragm: The iris diaphragm is an adjustable aperture that can be opened or closed to control the amount of light entering the optical system. By adjusting the diameter of the iris, the intensity of light reaching the photon counter can be fine-tuned.

6. Collimator: The collimator is an optical device that collects the divergent light beam from free space and converts it into a parallel beam before coupling it into an optical fiber. The collimator ensures that the light entering the fiber is properly aligned and maintains the necessary intensity for efficient transmission.

7. Optical Fiber: The optical fiber transmits the collimated light from the experimental setup to the photon counting system with minimal loss. The fiber ensures that the light path remains stable and isolated from external disturbances.

8. Single Photon Counting Module (SPCM): The photon counter is a highly sensitive detector, often based on a silicon avalanche photodiode (APD). When a photon strikes the detector, it generates a peak of current, which is recorded as a photon detection event. This module is designed to detect individual photons with high temporal precision.

9. Time Tagger: The time tagger is an electronic device that logs the exact time at which each photon detection event occurs. The time resolution of the tagger is typically in the nanosecond range, ensuring precise timestamping of each photon event.

10. Computer: The computer is used to process the data collected by the time tagger and produces the datasets that are used for the analysis result. In particular, the computer will produce two columns: the first one that is the Time Tag of arrival in machine unit of 80.955 ps, and a second one which is the channel (in our case always channel 1).

    A picture of the setup is reported in Figure 1.

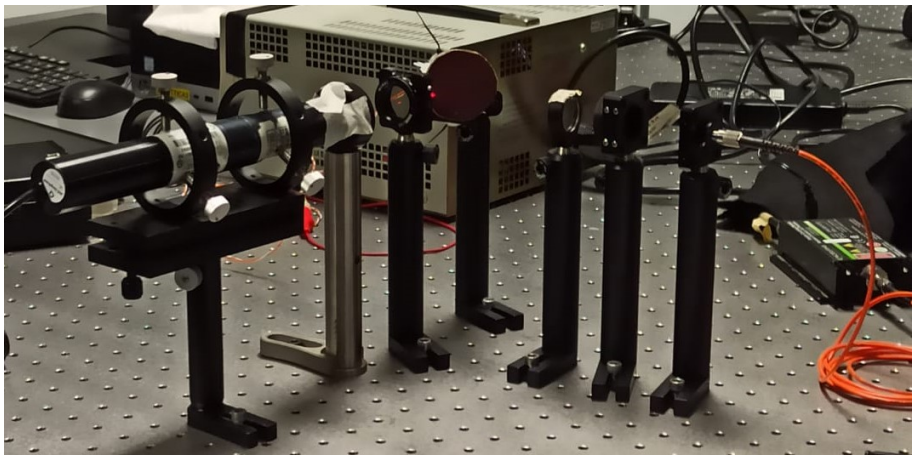

Figure 1: *Picture of the experimental setup*

4 Results

First, we now display the results in the Static-Wheel scenario. For this regime, several datasets have been acquired, and here the analysis of one of them is considered.
The data set is made up of Time Tags in machine units ($80.955ps$) of the photon-count events registered by the apparatus.
Since Poissonian processes are characterized by exponentially distributed time intervals between events (with a constant average rate), in order to verify that the process is indeed Poissonian we perform the difference between consecutive time tags (i.e., time intervals

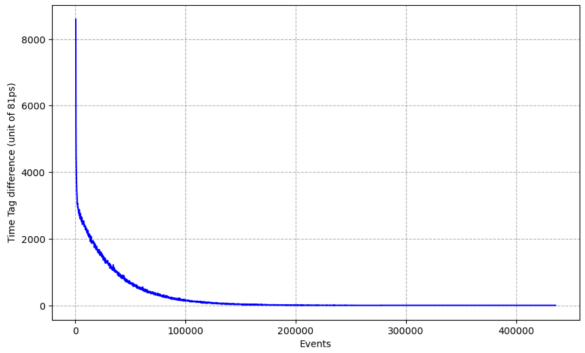

Figure 2: *Time Tag difference for the photon-count events in machine units (*80.955 *ps), in the static wheel regime*

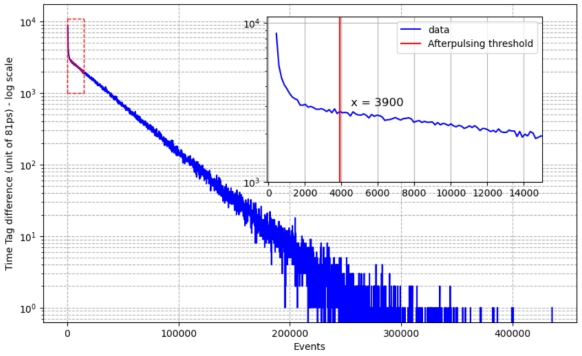

Figure 3: *Time Tag difference for the photon-count events in logarithmic scale, in the static wheel regime. Zoom on the first part to highlight the afterpulsing threshold at 3900.*

between photon detection events).
In Figures 2 and 3 the time difference in machine unit is displayed both with linear and logarithmic scale.

Figure 2 clearly shows the exponential trend, apart from the first spike. This can be clearly viewed and analyzed in Figure 3, where the time tag has been put in logarithmic scale; in this latter case the trend is of course linear, with the exception of the signal before the so-called afterpulsing threshold, which is put at 3900 to be safe, having an afterpulsing probability of 0.5% with 1.3 Mclicks.
Afterpulsing is a phenomenon that occurs in photon detectors, where residual charges trapped in the detector material from previous detection events get released after a certain delay, causing additional false signals. These false signals mimic real photon detection events and can interfere with accurate measurement of photon statistics.
In order to verify how much the data resemble a Poissonian distribution, an exponential fit of the data is applied, where only the time difference after the afterpulsing threshold has been taken into consideration; the result is depicted in Figure 4,

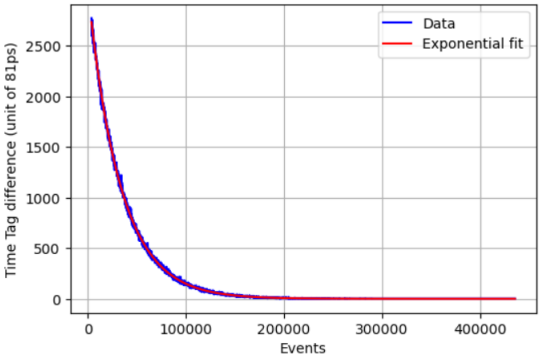

Figure 4: *Time Tag difference for the photon-count event, in the static wheel regime, and the associated exponential fit, which yields* $Ampl = 3079.5 \pm 3.0$ *machine units and* $\tau = 33049 \pm 40$.

where the best parameters are $Ampl = 3079.5 \pm 3.0$ machine units and $\tau = 33049 \pm 40$.
A closer look to the dead time of the photodiode is studied, which refers to the period immediately following a detection event during which the detector is temporarily unable to record any further events. It is expected to be around $10 - 100$ ns. Actually, zooming in the previous graph one obtains Figure 5:

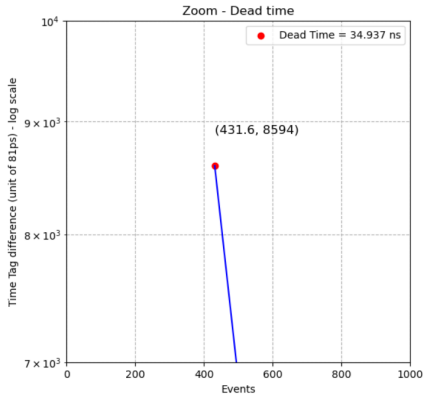

Figure 5: *Time Tag difference of photon-count events, in the static wheel regime, with a zoom to highlight the dead time, which is equal to* 34.9 *ns.*

so, a dead time equal to 34.9 ns.

Consequently, for this dataset time tags are grouped in time bins, i.e. intervals of a duration of $10\mu s$ and the number of events in each time bin is counted. In this way the following histogram is derived in Figure 6, showing the occurrences of each number of counts:

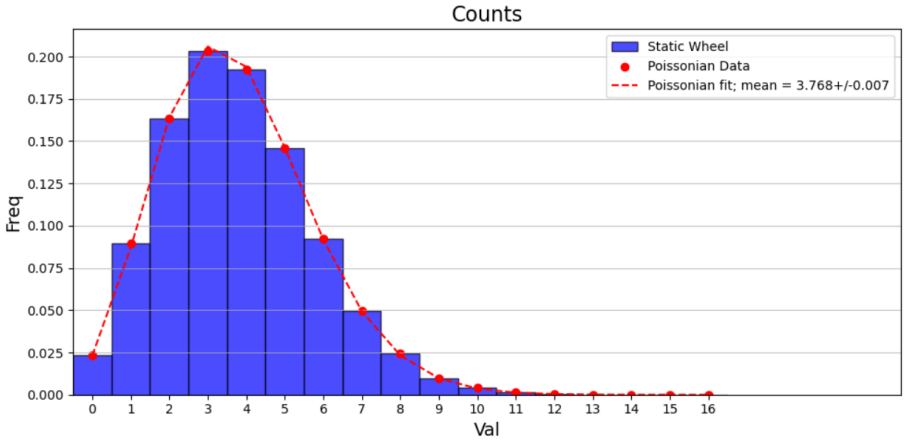

Figure 6: *Histogram showing the occurrences of each number of photon-counts, in the static wheel regime, and the associated Poissonian fit yielding* $\bar{n} = 3.768 \pm 0.007$.

where also the Poissonian fit has been applied on the data, according to Equation 1.
First of all, one can clearly see the Poissonian distribution of the counts that resemble a coherent source of light, as expected, thus showing that the light in the case of the static wheel is indeed the light of the laser. Secondly, the fit yields a mean value for the average photon count of $\bar{n} = 3.768 \pm 0.007$.
Additionally, it is possible perform a comparison between the analytical and numerical statistics, taking into account the formulas in 7.1. The results are reported in Table 1.

Statistic	**Numerical**	**Analytical**
Mean	3.78	3.77
Variance	3.85	3.77
Skewness	3.91	3.77
Kurtosis	46.87	46.31

Table 1: Numerical and Analytical Statistics for Static Wheel.

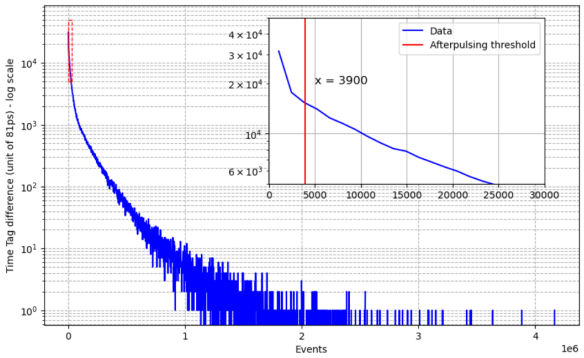

Figure 7: *Time Tag difference for the photon-count events in logarithmic scale, in the spinning wheel regime. Zoom on the first part to highlight the afterpulsing threshold at 3900.*

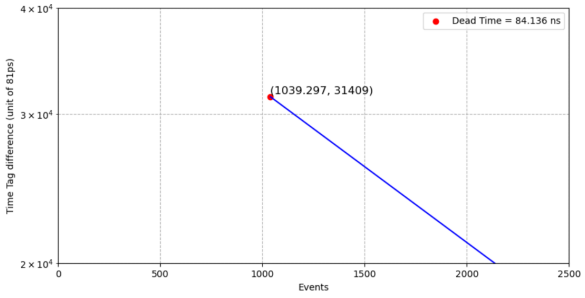

Figure 8: *Time Tag difference of photon-count events, in the spinning wheel regime, with a zoom to highlight the dead time, which is equal to 84.136 ns*

So it is possible to see that the numerical and analytical statistics are compatible with each other.

The same analysis can be performed in the case of the spinning wheel.
Performing the difference between consecutive tags (expressed in machine units) and putting the y axis in logarithmic scale for a better overview, Figures 7 and 8 are obtained:

In Figure 7 the afterpulsing threshold has been highlighted and set to 3900 as before, while in Figure 8 the dead time is depicted and calculated to be 84.136 ns.
Consequently, also for this regime time tags are grouped in time bins, i.e. intervals of a duration of $10\mu s$ and the number of event in each time bin is counted. In this way the following histogram is derived and shown in Figure 9, showing the occurrences of each number of counts:

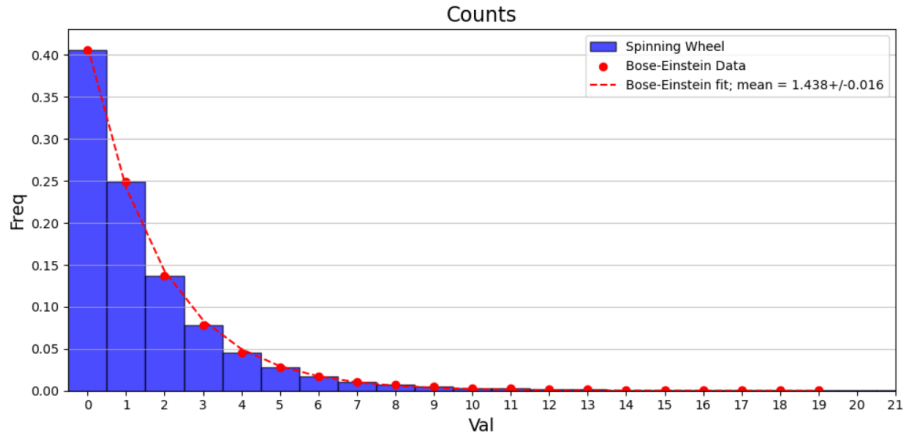

Figure 9: *Histogram showing the occurrences of each number of photon-counts, in the spinning wheel regime, and the associated Bose-Einstein fit yielding* $\bar{n} = 1.438 \pm 0.016$.

where also the fit using the Bose-Einstein distribution has been applied on the data, using Equation 2.
First of all, one can clearly see from the fit that the event count distribution resembles a thermal source of light, meaning that the regime of the spinning wheel produces an "averaging" effect changing the distribution of the light from the Poissonian to the Bose-Einstein one. In particular, the fit yields a mean value for the average photon count of $\bar{n} = 1.438 \pm 0.016$.

Additionally, it is possible perform a comparison between the analytical and numerical statistics, taking into account the formulas in 7.1. The results are reported in Table 2.

Statistic	Numerical	Analytical
Mean	2.27	2.38
Variance	8.01	8.02
Skewness	8.71	18.41
Kurtosis	64.2	131.5

Table 2: Numerical and Analytical Statistics for Spinning Wheel.

So it is possible to see that the numerical and analytical statistics are compatible with each other, except for the Skewness and Kurtosis statistics for which further analysis needs to be implemented.

For seek of clarity the histogram depicting both the regimes and the corresponding distribution is shown in Figure 10.

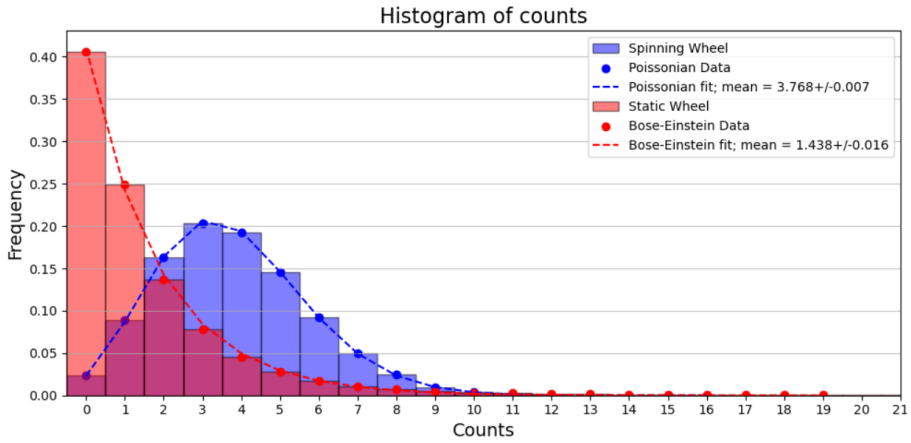

Figure 10: *A comparison between the two distributions of photon-count events, in the static and spinning wheel regime, and the associated fits.*

5 Quantum Random Number Generator

Due to the considerations done in the Theoretical Framework section, the photon detection is fundamentally a quantum process. In the context of the Arecchi experiment, so using a Poissonian laser light, the arrival of individual photons is a random quantum event.
Since the events are independent, we can use them to generate a genuine random set of data. In Figure 11 the individual detection of the first 50 photons is depicted, where one can notice approximately the randomness of the process that needs to be further analyzed.

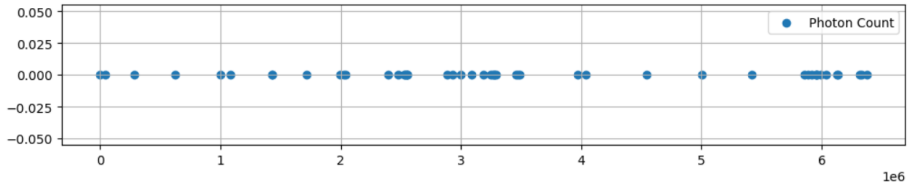

Figure 11: *Distribution of the individual detection of the first 50 photons*

Subsequently, the three acquired dataset in the static wheel regime have been merged together, where the differences of subsequent clicks have been computed and the ones lower than 3900 have been discarded.
At this point, from the dataset a list of random bytes is created in this way: for each pair of data points, the algorithm produces a 1 bit if the current value is greater than the previous one, and 0 otherwise. Combining them in blocks of 8 the string of bits is then converted into bytes. The distribution of bytes is depicted in Figure 12 where it is possible to observe a uniform distribution, almost completely within one standard deviation from the mean value. This clearly indicates that the process is random and suitable for a random extraction.

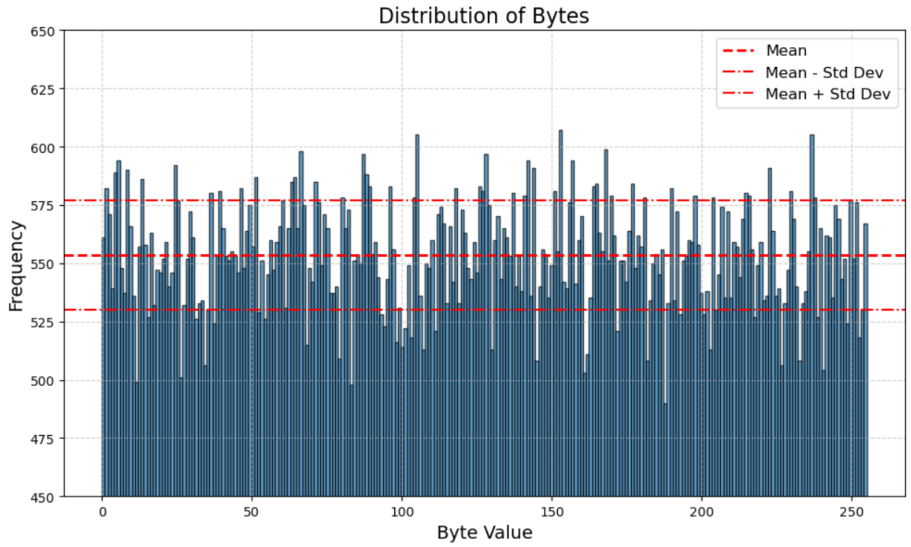

Figure 12: *Distribution of bytes created from the photon-counts events. An almost uniform distribution is obtained.*

Afterwards, a process to verify the presence of periodic artifacts or regular patterns (a "comb-like" structure) in the data after an extraction is performed. For this reason, the comb distribution about average number of byte appearance is depicted in Figure 13.

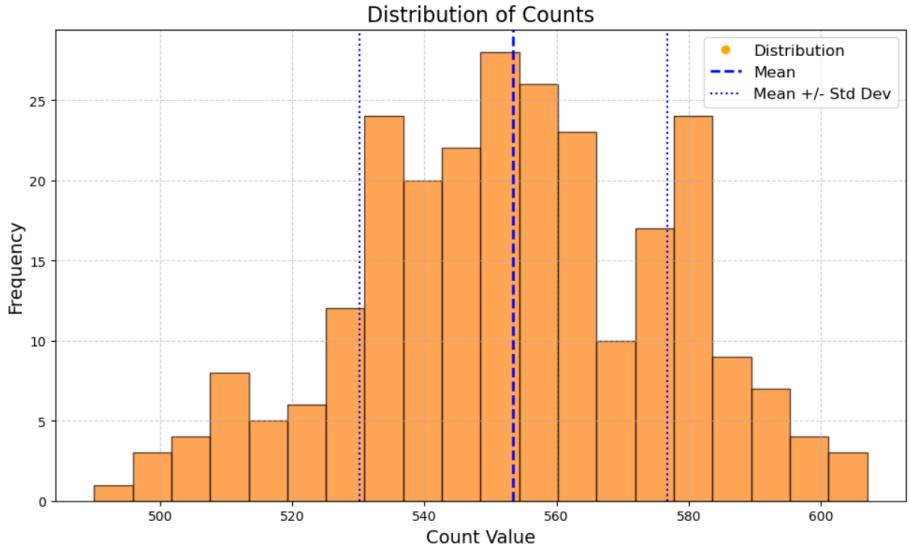

Figure 13: *Distribution of the counts of the bytes created from the photon count events*

The "comb" distribution resembles a Bell (normal) distribution, suggesting that the byte frequencies in the data are centered around a mean value with symmetrical spread or variation on either side.
A Bell-like distribution indicates that most byte appearances are clustered around the average value, with fewer occurrences as one moves away from the mean in either direction. This is typical for natural fluctuations in random processes and suggests that the procedure to build a quantum random number generator is indeed correct.
Moreover, it is possible to provide the distribution of the bytes in three-dimensional space, in order to analyze the presence or lack of clear structure or pattern in the random number data. This is shown in Figure 14, where one can clearly see the absence of such patterns or structures, and since the scatter plot appears uniformly distributed and "foggy," this suggests that the bytes are behaving randomly.

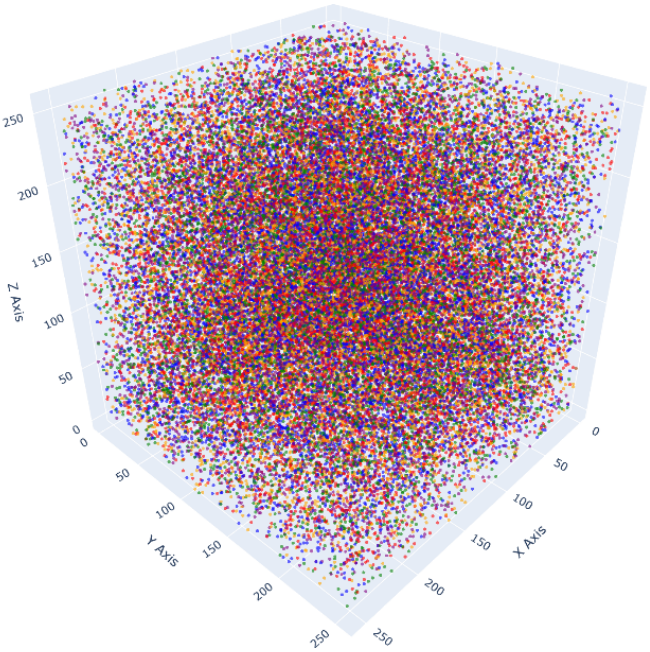

Figure 14: *A 3D representation of the distribution of the bytes, useful to highlight the absence of structures or patterns and the presence of a random data distribution.*

Finally, it is possible to perform other tests in order to quantify the randomness of this Quantum Random Number Generator, compared to the pseudo-random number generator algorithms often used in libraries like `random` from `numpy`.
In particular, the program `ent` is used in order to apply various tests to sequences of bytes. The program is useful for evaluating random number generators for encryption and statistical sampling applications, compression algorithms, and other applications where the information density of a file is of interest.
Among these tests, this program applies:

- The chi-square test: it is a widely method used to assess the randomness of data. It compares the observed byte distribution in a file to the expected distribution for a random sequence. The result is expressed as a percentage, indicating how often a truly random sequence would produce a similar result.
- Arithmetic Mean: Calculates the average byte (or bit) value in a file. For random data, the mean should be around 127.5 for bytes or 0.5 for bits. Deviations from these values indicate consistently high or low values in the data.
- Monte Carlo Value for π: Uses successive 6-byte sequences to estimate the value of

π by simulating points inside a square and circle. The accuracy improves with large data sets, and random data should yield a π value close to the real π.

- Serial Correlation Coefficient: Measures the dependency of each byte on the previous one. A value near zero indicates randomness, while values closer to 1 suggest predictable, non-random data. Non-random files like `C` programs or uncompressed bitmaps tend to have higher correlation coefficients.

Using the bytes produced as previously described and applying this program executing it with `./ent -b data/qrng.bin`, the following output is provided:

```
Entropy = 0.999998 bits per bit.
Optimum compression would reduce the size of this 1133472 bit file
by 0 percent.
Chi square distribution for 1133472 samples is 3.91, and randomly would
exceed this value 4.79 percent of the times.
Arithmetic mean value of data bits is 0.4991 (0.5 = random).
Monte Carlo value for Pi is 3.132548488 (error 0.29 percent).
Serial correlation coefficient is 0.001281 (totally uncorrelated =
0.0).
```

On the other hand, executing the same program with `./ent -b data/prng.bin` on the string of bytes produced using the library `random` from `numpy`, one gets the following results:

```
Entropy = 0.337140 bits per bit.
Optimum compression would reduce the size of this 9067776 bit file
by 66 percent.
Chi square distribution for 9067776 samples is 6943734.05, and randomly
would exceed this value less than 0.01 percent of the times.
Arithmetic mean value of data bits is 0.0625 (0.5 = random).
Monte Carlo value for Pi is 4.000000000 (error 27.32 percent).
Serial correlation coefficient is 0.400637 (totally uncorrelated =
0.0).
```

Finally, comparing the two generation techniques with the results of all the tests, it is possible to conclude that the degree of randomness is significantly higher in the quantum version, using the detection of single photons to produce the string of bytes; this underlines the supremacy with the respect to the classical pseudo-random number generation and highlights the potential applications that this method can have in various fields.

6 Conclusion

The experiment was designed to explore the quantum nature of light and its application in generating random numbers through the detection of single photons. Two distinct regimes were analyzed: the static wheel regime, where light behaves in a coherent (Poissonian) manner, and the spinning wheel regime, where light follows a thermal (Bose-Einstein) distribution. Following this, the detected photons were used to generate random numbers through a Quantum Random Number Generator (QRNG). The performance of this QRNG was then compared with that of a classical pseudo-random number generator (PRNG). The results of the experiment are summarized below.

Results from the Static Wheel Regime In the static wheel regime, the light source is a laser emitting coherent light. This regime is characterized by a Poissonian distribution of photon arrival times, which was confirmed by the following results:

(a) Exponential Fit of Photon Arrival Times: The time differences between consecutive photon detections were analyzed, yielding an exponential fit with parameters:
- Amplitude: 3079.5 ± 3.0 machine units
- Decay constant: $\tau = 33049 \pm 40$ machine units

These results confirm the expected Poissonian nature of the photon detection process.

(b) Photon Detection Dead Time: By analyzing the photon arrival data, the dead time of the photodiode was determined to be 34.9 ns, which falls within the expected range for such detectors.

(c) Photon Count Distribution: A histogram of the photon count in time bins was fitted with a Poisson distribution, yielding an average photon count $\langle n \rangle = 3.768 \pm 0.007$. This confirms that the light source is behaving as a coherent (Poissonian) source, with photon counts distributed according to a Poisson process.

Results from the Spinning Wheel Regime In the spinning wheel regime, the rotating wheel introduces fluctuations in the light path, which causes the photon statistics to shift from a Poissonian distribution to a thermal (Bose-Einstein) distribution:

(a) Exponential Fit of Photon Arrival Times: In this regime, the exponential fit was again applied, but with different parameters due to the altered light behavior:
- Dead time: 84.136 ns, reflecting a slower response compared to the static wheel regime.

(b) Photon Count Distribution: The histogram of photon counts was fitted with a Bose-Einstein distribution, yielding an average photon count of $\langle n \rangle = 1.438 \pm 0.016$. This shift to Bose-Einstein statistics confirms that the spinning wheel transforms the light into a thermal source, where the random phase fluctuations of the light dominate.

These results clearly demonstrate the fundamental difference in photon statistics between coherent and thermal light, providing a foundation for the use of quantum randomness in subsequent experiments.

Results from the Quantum Random Number Generator (QRNG) The photon detection process, being inherently quantum mechanical, was used to generate random numbers by recording the arrival times of individual photons. These times were processed to produce random bits, which were then grouped into bytes. The randomness of the generated sequence was evaluated using several statistical tests.

(a) Entropy: The entropy per bit for the QRNG-generated sequence was measured to be 0.999998 bits per bit, indicating that the sequence is almost perfectly random, with no significant bias in the bit values.

(b) Chi-Square Test: The chi-square statistic for the QRNG sequence was 3.91, corresponding to a probability of 4.79% that a random sequence would exceed this value. This suggests that the QRNG-generated byte distribution is well within the expected range for a truly random sequence.

(c) Arithmetic Mean: The arithmetic mean of the QRNG-generated bits was 0.4991, extremely close to the theoretical mean of 0.5 for a perfectly random sequence. This result further confirms the balance between 0s and 1s in the generated sequence.

(d) Monte Carlo Pi Approximation: Using the QRNG sequence to estimate π via the Monte Carlo method, the result was 3.132548488, with an error of 0.29% compared to the true value of π (3.14159). This small error supports the randomness

of the sequence, as the Monte Carlo method converges to the true value of π only if the sequence is random.

(e) Serial Correlation: The serial correlation coefficient for the QRNG sequence was 0.001281, which is very close to zero. This indicates a lack of dependency between consecutive bytes, confirming the independence of the generated random bits.

Comparison with Pseudo-Random Number Generator (PRNG) For comparison, a pseudo-random number generator (PRNG) was used to generate a sequence of random numbers, and the same statistical tests were applied:

(a) Entropy: The entropy per bit for the PRNG sequence was 0.337140 bits per bit, significantly lower than that of the QRNG. This low entropy indicates a high degree of predictability and structure in the PRNG sequence, making it less suitable for applications requiring true randomness.

(b) Chi-Square Test: The chi-square statistic for the PRNG sequence was $6,943,734.05$, with the probability of a random sequence exceeding this value being less than 0.01%. This extremely high chi-square value suggests that the PRNG-generated byte distribution is highly non-random and biased.

(c) Arithmetic Mean: The mean value of the PRNG-generated bits was 0.0625, a significant deviation from the ideal value of 0.5. This indicates a strong bias towards low values, confirming the lack of randomness in the PRNG sequence.

(d) Monte Carlo Pi Approximation: The Monte Carlo Pi approximation using the PRNG sequence yielded a value of 4.000000000, with an error of 27.32% compared to the true value of π. This large error reflects the poor randomness of the PRNG-generated sequence.

(e) Serial Correlation: The serial correlation coefficient for the PRNG sequence was 0.400637, indicating a strong correlation between consecutive bytes. This suggests that the PRNG sequence is highly predictable and fails to exhibit the independence characteristic of random data.

The results of this experiment clearly demonstrate the superiority of the quantum random number generator (QRNG) over classical pseudo-random number generation (PRNG). The QRNG, leveraging the inherent unpredictability of quantum photon detection events, produced a sequence with near-perfect randomness across all statistical tests. In contrast, the PRNG exhibited significant biases and correlations, failing to meet the randomness criteria required for secure cryptographic applications or high-fidelity simulations.

These results underline the potential of quantum-based random number generators for applications in cryptography, secure communications, and stochastic simulations, where the quality of randomness is paramount.

7 Appendix

7.1 Distributions' Momenta

In statistics, the momenta of a distribution provide critical insights into its shape and characteristics. For discrete random variables, the n-th moment about the origin is defined as the expected value of the n-th power of the variable, expressed mathematically as:

$$\mu'_n = E[X^n] = \sum_{k=0}^{\infty} k^n P(X = k), \tag{7}$$

where $P(X = k)$ is the probability mass function of the random variable X. Most of the times, we are interested in quantities strictly related to the momenta rather the momenta themselves, which are more informative about the distribution. After the mean (first momentum), we usually care about variance, skewness and kurtosis:

- **Variance:** Variance measures the dispersion of a set of values relative to their mean. It is the second central moment and is defined as:

$$\text{Variance} = \sigma^2 = E[(X - \mu)^2] = \mu'_2, \tag{8}$$

  where X is the random variable, μ is the mean, and μ'_2 is the second moment about the origin. A higher variance indicates greater spread in the data.

- **Skewness:** Skewness quantifies the asymmetry of a probability distribution. It is the third standardized moment, defined as:

$$\text{Skewness} = \gamma_1 = \frac{E[(X - \mu)^3]}{\sigma^3} = \frac{\mu'_3}{\sigma^3}, \tag{9}$$

  where μ'_3 is the third moment about the origin. A skewness of zero indicates a symmetric distribution, while positive or negative values indicate right or left skewness, respectively.

- **Kurtosis:** Kurtosis measures the "tailedness" of a distribution, indicating the presence of outliers. It is defined as the fourth standardized moment:

$$\text{Kurtosis} = \gamma_2 = \frac{E[(X - \mu)^4]}{\sigma^4} = \frac{\mu'_4}{\sigma^4}, \tag{10}$$

  where μ'_4 is the fourth moment about the origin. A normal distribution has a kurtosis of 3, which can be adjusted to excess kurtosis (subtracting 3) to assess whether a distribution is more or less peaked than normal.

Table 3 summarizes the value of these quantities fot the Poissonian and the Bose-Einstein distributions.

Statistic	**Poissonian**	**Bose-Einstein**
Mean	μ	μ
Variance	μ	$\mu + \mu^2$
Skewness	μ	$3\mu + 2\mu^2$
Kurtosis	$\mu + 3\mu^2$	$12\mu + 4\mu^2 + 6\mu^3$

Table 3: Analytical form of momenta for Poissonian and Bose-Einstein distributions.

References

[1] M. Fox, *Quantum Optics - An Introduction*, Oxford University Press (2006).

[2] J. Walker, *HotBits: Genuine Random Numbers from Radioactive Decay*, https://www.fourmilab.ch/random/, accessed October 18, 2024.