Quantum Optics and Laser
Grangier-Roger-Aspect experiment

Andrea Turci

October 2024

1 Introduction

The Grangier-Roger-Aspect (GRA) experiment serves as a landmark in understanding light's quantum properties, investigating its behavior as a particle. Conceived in the 1980s, the experiment aimed to test quantum mechanics by examining single-photon interference and nonlocality. Specifically, it used a beam splitter to observe how individual photons act when they encounter a choice between two pathways: transmission or reflection. Classical physics would suggest that light, as a wave, might split across both paths, resulting in detections in both channels at the same time. Yet, GRA's results showed that photons behave as indivisible quantum units, reaching only one detector per instance.
This observed "anticorrelation" was key in proving that light's behavior cannot be completely described by classical wave theories: instead, individual photons have probabilistic, discrete detection events, confirming their existence as single, undivided quanta. This experiment validated the notion that light possesses an inherent quantized nature, functioning as separate particles during measurement and supporting the dual wave-particle nature of light.
In this study, we first produce photon pairs through a nonlinear optical process called Spontaneous Parametric Down Conversion (SPDC), which allows one photon to serve as a "herald" for the other, which we then analyze. Subsequently, we examine photon arrival times post-beam splitter, analyzing both the transmitted and reflected channels. By examining the distribution of these arrival times, we investigate the fundamentally random and discrete nature of photon detection events.
Additionally, photon arrival times enable the creation of a Quantum Random Number Generator (QRNG) due to the probabilistic aspect of photon detection. Recording the precise arrival times of photons in the transmitted channel, we generate a random number sequence. Due to the intrinsic randomness of photon emission in a coherent state, this quantum-derived process offers an unbiased foundation suitable for applications in secure communication, cryptographic systems, and high-fidelity simulations.

2 Theoretical Framework

In quantum optics experiments, single-photon phenomena are crucial for understanding the intrinsic randomness of quantum mechanics. The Grangier-Roger-Aspect (GRA) experiment applies these principles to study the behavior of individual photons and test the foundational aspects of quantum mechanics.

2.1 Malus' Law

Malus' Law describes the change in intensity of a linearly polarized light beam as it passes through a polarizing filter, which is used to modulate light intensity in quantum optics experi-

ments and to align light in a specific direction. When a beam of light with an initial intensity I_0 and a polarization angle θ passes through a polarizer oriented at an angle α relative to the light's polarization direction, the transmitted intensity I is given by:

$$I = I_0 \cos^2(\theta - \alpha) \tag{1}$$

where I_0 is the initial intensity of the incoming light, θ is the angle of the initial polarization direction of the light, and α is the angle of the transmission axis of the polarizer. When the angle $\theta - \alpha$ is $0°$, the transmitted intensity is at its maximum and equals I_0; when the angle is $90°$, the transmitted intensity becomes zero, as the light is entirely blocked by the polarizer.

2.2 Spontaneous Parametric Down Conversion (SPDC)

Spontaneous Parametric Down Conversion (SPDC) is a quantum optical process where a single photon from a high-energy beam (the pump photon) splits spontaneously into two lower-energy photons, known as the signal and idler photons, see Figure 1.

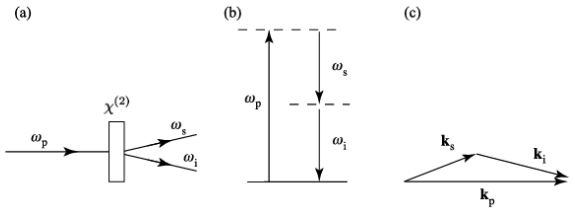

Figure 1: *(a) Schematic illustration of the process of spontaneous parametric down-conversion (SPDC). (b) Energy-level description and (c) wavevector description of the process.*

This phenomenon results from the nonlinear interaction between the pump photon and a nonlinear crystal, which is typically engineered to enable such conversions. In a medium with second-order susceptibility $\chi^{(2)}$, the electric polarization $\vec{P}$ of the medium can be described as:

$$\vec{P} = \epsilon_0 \chi^{(2)} \vec{E}^2 \tag{2}$$

where $\vec{E}$ represents the electric field of the incident photon, and ϵ_0 is the permittivity of free space.
During SPDC, both energy conservation and momentum conservation (phase matching) must be satisfied:

$$\hbar\omega_p = \hbar\omega_s + \hbar\omega_i \tag{3}$$

$$\vec{k}_p = \vec{k}_s + \vec{k}_i \tag{4}$$

where ω_p, ω_s, and ω_i are the angular frequencies of the pump, signal, and idler photons, respectively, and $\vec{k}_p$, $\vec{k}_s$, and $\vec{k}_i$ represent their wave vectors. These relationships ensure the energy and momentum of the resulting photons match those of the pump photon. When ω_s and ω_i are equal, degenerate SPDC occurs: in this case, the pump photon splits into two photons with identical frequencies and energy, each having half the frequency of the pump photon:

$$\omega_p = 2\omega_s = 2\omega_i \tag{5}$$

This condition is met under specific phase-matching scenarios, typically achieved by adjusting the nonlinear crystal's properties (temperature, orientation, and type) and the pump wavelength.

The photon pairs generated through SPDC are typically entangled in terms of polarization, momentum, or frequency. Usually, the crystal is engineered to produce pairs of entangled photons with orthogonal polarizations (type II SPDC, used in this experiment), valuable in quantum information and quantum communication. This arrangement is feasible because each photon follows a cone of emission at an angle determined by energy and momentum conservation laws. In type II SPDC, the signal and idler photons are emitted on overlapping but distinct cones, creating "zones of coincidence" where we can collect polarization-entangled photons, see Figure 2.

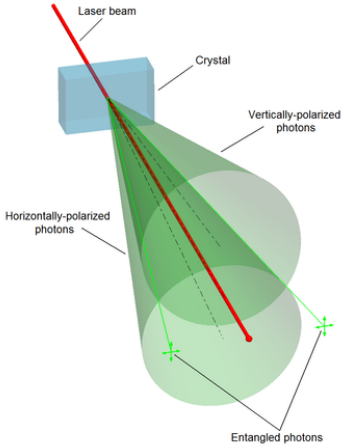

Figure 2: *Type II SPDC: a non-linear crystal produces couples of entangled photons with opposite polarization.*

In this experiment, we utilize the fact that SPDC consistently produces pairs of correlated photons; one of the two acts as a "herald" for the other, which we then analyze.

2.3 Beam Splitter

In classical optics, a beam splitter is usually modeled as an optical device that divides an incoming light beam into two distinct paths. Assuming an ideal, lossless 50:50 beam splitter, the amplitude of the incident electric field E_{in} is equally split between the transmitted and reflected paths. For a 50:50 beam splitter, the relationship between the input and output fields can be described by:

$$E_t = \frac{1}{\sqrt{2}} E_{\text{in}}, \quad E_r = \frac{i}{\sqrt{2}} E_{\text{in}} \tag{6}$$

where i represents a phase shift of $\pi/2$ introduced upon reflection. This phase shift is a defining characteristic of the beam splitter, resulting in destructive interference when the two beams interfere at the output ports of the device. The intensities of the transmitted and reflected beams, given by $I \propto |E|^2$, are each half of the input intensity I_{in}.

In experiments involving single photons and photodetectors, we can describe the classical behavior of the beam splitter by examining the count rates of each detector. In a "triggered experiment" such as this one using SPDC, the detection probabilities can be defined as:

$$p_t = \frac{N_t}{N}, \quad p_r = \frac{N_r}{N}, \quad p_c = \frac{N_c}{N} \tag{7}$$

where p_t is the probability of the photon being transmitted, p_r is the probability of the photon being reflected, and p_c is the probability of a coincidence detection. It can be shown that, according to classical theory:

$$p_c \geq p_r p_t \tag{8}$$

or equivalently,

$$\alpha \geq 1, \quad \text{where } \alpha = \frac{p_c}{p_r p_t} = \frac{N_c N}{N_r N_t} \tag{9}$$

These inequalities imply that the classical coincidence probability p_c is always greater than or equal to the accidental coincidence probability, which equals $p_r p_t$. Therefore, violating Equation 9 provides an anticorrelation criterion, which serves as a marker of nonclassical behavior.

Nonclassical behavior arises because the classical model does not account for the indivisibility of photons, treating light (even at very low intensities) as continuous waves. Due to photon indivisibility, a quantum effect, each photon is either fully reflected or fully transmitted; single photons do not split. From this reasoning, we expect a very low value for p_c, leading to a violation of Equation 9.

2.4 Quantum Description of a Beam Splitter

In quantum optics, a beam splitter is defined by how it transforms input photon states. We consider an incident photon in a mode described by annihilation operators $\hat{a}$ and $\hat{b}$ for the two input ports of the beam splitter. The output modes are then represented by operators $\hat{c}$ and $\hat{d}$ for the transmitted and reflected paths, respectively.
For a 50:50 beam splitter, the transformation is given by:

$$\hat{c} = \frac{1}{\sqrt{2}}(\hat{a} + i\hat{b}), \quad \hat{d} = \frac{1}{\sqrt{2}}(i\hat{a} + \hat{b}) \tag{10}$$

where the factor i again represents the $\pi/2$ phase shift upon reflection.
When a single photon state $|1\rangle_a|0\rangle_b$ (where one photon is in mode a and none in b) passes through the beam splitter, the output state becomes:

$$|1\rangle_a|0\rangle_b \to \frac{1}{\sqrt{2}}(|1\rangle_c|0\rangle_d + i|0\rangle_c|1\rangle_d) \tag{11}$$

indicating that the photon is now in a superposition of the transmitted and reflected modes. Similarly, if one photon exists in each of the input modes a and b, the output state is transformed into:

$$|1\rangle_a|1\rangle_b \to \frac{1}{2}(|2\rangle_c|0\rangle_d - |0\rangle_c|2\rangle_d) \tag{12}$$

showing two-photon interference, where both photons emerge in the same mode. This quantum treatment of the beam splitter uncovers phenomena such as photon bunching, unexplainable by classical optics and unique to quantum interference.

2.5 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.

2.6 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:

$$H_0 = -p_0 \log_2 p_0 - p_1 \log_2 p_1 \tag{13}$$

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:

$$\chi^2 = \sum \frac{(O_i - E_i)^2}{E_i} \tag{14}$$

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:

$$r = \frac{\sum (x_i - \mu)(x_{i+1} - \mu)}{\sum (x_i - \mu)^2} \tag{15}$$

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

2.7 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 apparatus was designed with precision to facilitate accurate single-photon detection and ensure effective light management. As depicted in Figure 3, the setup includes a gas laser, various optical components (such as mirrors, polarizers, and lenses), a nonlinear crystal, and a photon counting system.

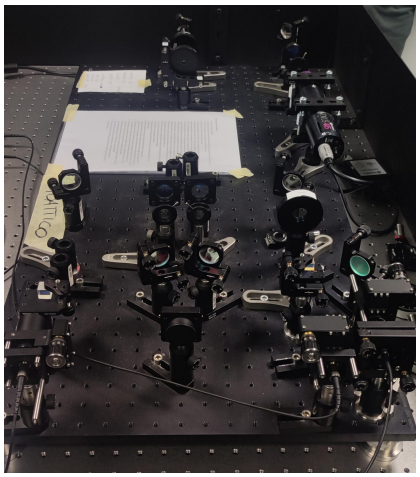

Figure 3: *Representation of the experimental setup, where it is possible to see the different components explained in the text.*

Each component plays a crucial role, detailed as follows:

1. **Gas Tube Laser**: A gas laser serves as the light source, emitting a purplish beam with a wavelength of 405 nm. This monochromatic and phase-stable light is ideal for experiments demanding controlled, coherent light.

2. **Mirrors and Polarizers**: Mirrors and polarizers direct and adjust the intensity of the laser beam, adhering to Malus' Law as per Equation 1. A collimator at the end of this system transforms the diverging beam into a parallel one before it encounters the nonlinear crystal.

3. **Nonlinear Crystal**: The nonlinear beta barium borate (BBO) crystal is used here to produce pairs of entangled photons through Spontaneous Parametric Down Conversion (SPDC), as elaborated in the Theoretical Framework Section. This step is critical for generating photon pairs with correlated behavior.

4. **Pinholes**: Pinholes provide spatial filtering, allowing only photons within selected paths to pass through. This minimizes background noise, isolates specific sections of the photon beams, and enhances the visibility of quantum interference patterns.

5. **Secondary Mirrors and Polarizers**: An additional system of mirrors and polarizers directs the herald photon and the paired photon along separate paths, enhancing detection by minimizing interference.

6. **Beam Splitter**: A polarized beam splitter divides photons based on their polarization (horizontal or vertical). This component ensures that photons are separated into transmitted or reflected paths according to their polarization, as described in the Theoretical Framework Section.

7. **Collimators**: Light beams are directed through collimators that gather the beams and couple them into optical fibers. This alignment ensures efficient transmission while preserving beam intensity.

8. **Optical Fiber**: Optical fibers carry the collimated beams to the photon detection system, reducing loss and keeping the signal isolated from external interference.

9. **Single Photon Counting Modules (SPCM)**: These modules use Single-Photon Avalanche Diodes (SPADs) to detect individual photons, producing a current pulse or "click" with each detection. To prevent noise interference, all unnecessary light sources are switched off, and the detectors are shielded with a black cloth.

10. **Time Tagger**: The time tagger records each photon detection event with nanosecond precision. Each of the three channels of the time tagger corresponds to the herald, transmitted, and reflected photons (Channels 1, 2, and 3, respectively).

11. **Computer**: A computer collects and processes the time-tagged data, forming datasets for photon behavior analysis and the quantum random number sequence generation.

To ensure stable operation, all components are mounted on a vibration-isolated optical table. This minimizes external disturbances like air currents or vibrations, which could otherwise impact the detection accuracy and compromise experimental results. The precise positioning and shielding of each element are essential to preserve data fidelity throughout the photon detection process.

4 Results

4.1 Malus' Law

To begin with, we will validate Malus' Law by examining the number of photons transmitted as we adjust the angle of the polarizer, aiming to confirm the validity of Equation 1. As shown in Figure 4, we present the collected data along with the corresponding fitting curve described by the function:

$$f(\theta) = a\cos^2(b\theta + c) \tag{16}$$

From the visual representation, it is evident that the fitting is quite accurate, achieving a percentage RMSE (Root Mean Square Error) of 0.4%. This fitting allows us to determine optimal parameter values; the most significant parameters regarding our experimental configuration are b and c, which pertain to the angular aspects of the fit. We can, however, overlook the amplitude parameter as it aligns with our expectations. The fitting results yield $b = 0.998 \pm 0.002$ and $c = (-25.890 \pm 0.003)^\circ$. The value of b aligns perfectly with the theoretical prediction from

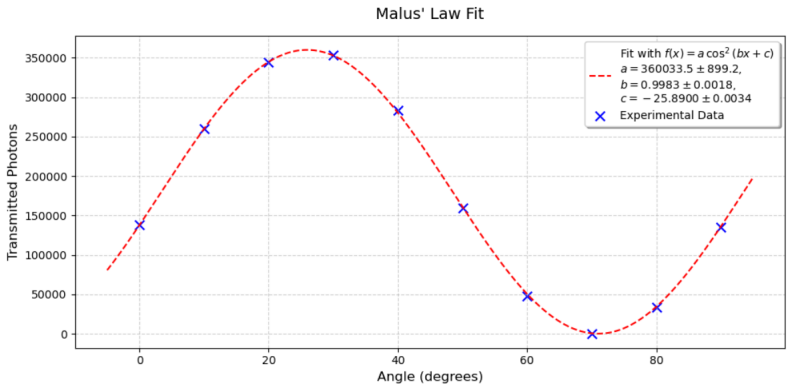

Figure 4: *Polarizers modulate intensity following Malus' law*

Equation 1 (where $b = 1$). Conversely, the parameter c indicates the angle of the polarizer's transmission axis, suggesting maximum transmission occurs at $\alpha_1 = -25.89°$ and minimum transmission at $\alpha_2 = \alpha_1 + 45°$.

4.2 GRA Experiment

Initially, we should briefly review the entire dataset. Figure 5 illustrates the photon counts over time (count per 5 seconds) throughout the detection period.

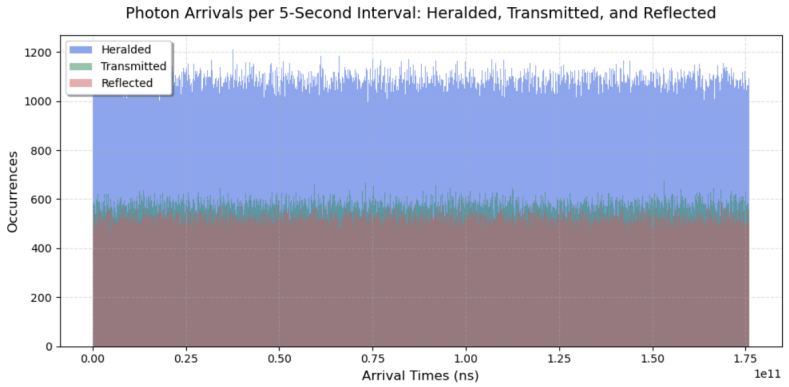

Figure 5: *Herald, transmitted, reflected photons arrival times (representing counts/5sec).*

This histogram immediately reveals that herald photons are approximately twice as numerous compared to the transmitted and reflected photons, which is consistent with expectations (since each pair of photons includes one herald and either one transmitted or reflected). Additionally, it is observed that the number of reflected photons is slightly less than that of transmitted photons, likely attributable to the beam splitter's imperfect 50:50 ratio; however, this imperfection does not hinder our experimental goals.

For our analysis, it is crucial to consider the herald photons, as they serve as our control to verify whether a pair of photons has been produced. Consequently, we analyze the timestamps from the time tagger to identify simultaneous events. The definition of simultaneous events significantly impacts our results, necessitating careful selection of an appropriate time window for considering events as simultaneous. A window that is too expansive risks losing insight into values near zero (which are particularly relevant), while a too-narrow window may exclude essential events, leading to insufficient statistical significance. For this analysis, I selected a window of $\Delta T = 50\,\mu s \approx 4\,ns$, which appears reasonable for defining simultaneous events, considering the different path lengths for herald versus transmitted/reflected photons. By examining the delay distributions between the transmitted/reflected photons and the nearest herald photon (within

this window), we generate the histograms depicted in Figure 6.

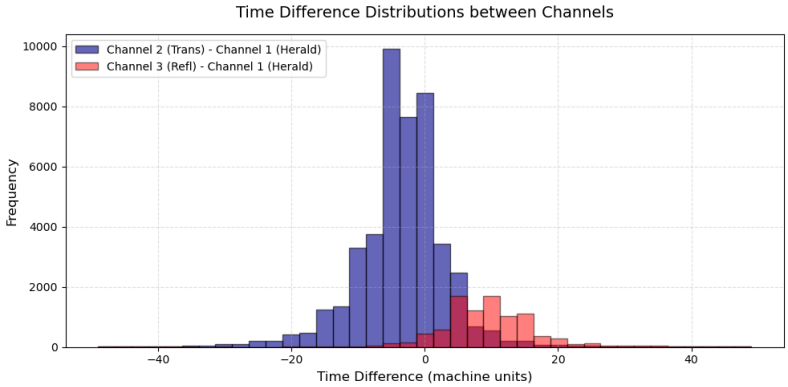

Figure 6: *Delay distributions between Channels 1 and 2 and between Channels 1 and 3.*

The histogram representing the delay between Channel 1 and Channel 2 (Herald and Transmitted) shows a peak around zero (or slightly negative values), whereas the histogram for the delay between Channel 1 and Channel 3 (Herald and Reflected) peaks at positive values. This difference again arises from the varied distances that different photons travel in the previously described experimental setup. Furthermore, there is a notable disparity in the amplitude and width of the two distributions, likely due to the beam splitter's deviation from a perfect 50:50 ratio, which leads to a higher occurrence of transmitted photons (approximately 10% more frequent) during the entire detection period.

To enhance our analysis, we first normalize these distributions and subsequently fit them with a normal distribution. This approach is justified as these delay distributions typically exhibit Gaussian characteristics due to several contributing factors.

First, the uncertainty in emission times plays a role; while SPDC photons are theoretically generated simultaneously, minor fluctuations in the crystal and environmental variables (such as temperature) can introduce small timing variations in photon emissions, resulting in slight random shifts in the arrival times of herald and transmitted photons. Second, detector timing jitter is another factor; photodetectors experience inherent timing uncertainty, known as jitter, characterized by random fluctuations in the precise moment a photon is detected. This jitter introduces Gaussian noise into the time difference measurements, contributing to a normal distribution of delays. Lastly, the Central Limit Theorem is applicable here, as the total delay is influenced by multiple independent, small random factors, indicating that the summation of numerous independent random variables will yield a normal distribution, even if the individual variations are not strictly Gaussian.

The outcomes of this procedure are illustrated in Figure 7, where both distributions resemble a normal distribution, yielding satisfactory RMSE values (0.0350 for Transmitted-Herald and 0.0323 for Reflected-Herald).

The numerical values of the mean and standard deviation (indicative of the bell width) are presented in Table 1 and Table 2, calculated numerically and derived from the optimal fitting parameters, respectively.

Notably, there is a discrepancy between these values, warranting a discussion to highlight potential sources of difference. Regarding the transmitted delay distribution, both the numer-

Statistic	**Mean (μ)**	**Std (μ)**
Channels 2 - 1	-3.48 $\pm$ 0.09	9.01 $\pm$ 0.07
Channels 3 - 1	9.30 $\pm$ 0.03	6.99 $\pm$ 0.02

Table 1: Numerical Statistics

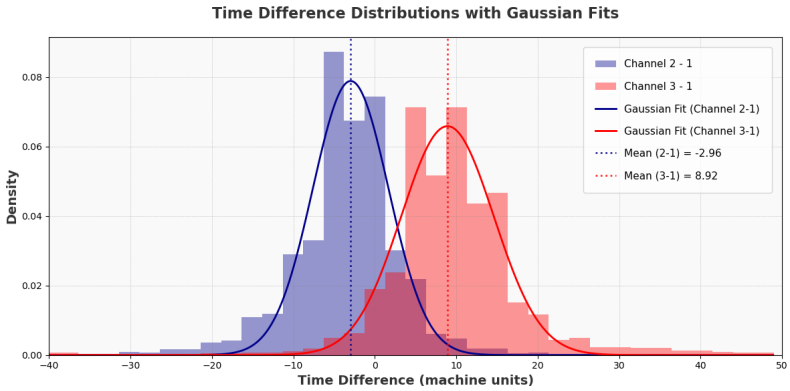

Figure 7: *Delay distributions with normal fits.*

ical results and fitting yield similar mean values. However, the standard deviation obtained numerically is approximately double that derived from the fit, likely due to the histogram's tails being broader than anticipated, thus increasing the deviation from the mean. In the case of the reflected delay distribution, the agreement is somewhat better, although there are still discrepancies in both mean and standard deviation. Here, the issue likely arises from low statistics, which prevent the distribution from perfectly resembling a normal distribution.

In both instances, a greater occurrence count would enhance the significance of these distributions and yield improved alignment with the fitting results. Additionally, adjusting the time window for defining simultaneous events could affect the tail populations, resulting in a more accurate standard deviation.

The final aspect of the analysis involves calculating the value of α, as defined in Equation 9. Table 3 summarizes the counts of double and triple coincidences recorded during the experiment.

The counts of double coincidences between transmitted and reflected photons, as well as the triple coincidences, are quite low compared to the overall counts (specifically, 0.012 ‰ and 0.080 ‰, respectively), which aligns with expectations (ideally, these values should approach zero). These occurrences likely stem from electrical noise or external photons and are not of significant concern. Applying Equation 9, we arrive at $\alpha = 0.00125 \pm 0.00009$, with the relative error calculated using the quadrature sum of the errors related to the detection probabilities. This result aligns perfectly with our expectations, confirming that we are operating within a quantum framework and that photons are indeed indivisible, as evidenced by the negligible probability of coincidence between transmitted and reflected photons.

5 Quantum Random Number Generator

The quantum random number generator utilizes photon arrival times to generate random bit sequences, as outlined in the Theoretical Framework Section. After constructing a bit list and grouping it into bytes, we obtained a sequence of decimal values The distribution of bytes is depicted in Figure 8 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.

Channel Pair	**Mean (μ)**	**Std (μ)**
Channels 2 - 1	-2.96 $\pm$ 0.24	4.66 $\pm$ 0.24
Channels 3 - 1	8.92 $\pm$ 0.32	5.68 $\pm$ 0.32

Table 2: Fit Statistics

Type of Coincidence	Count
Triple Coincidences	26
Double Coincidences (H-T)	45180
Double Coincidences (H-R)	9498
Double Coincidences (T-R)	175

Table 3: Coincidence Counts

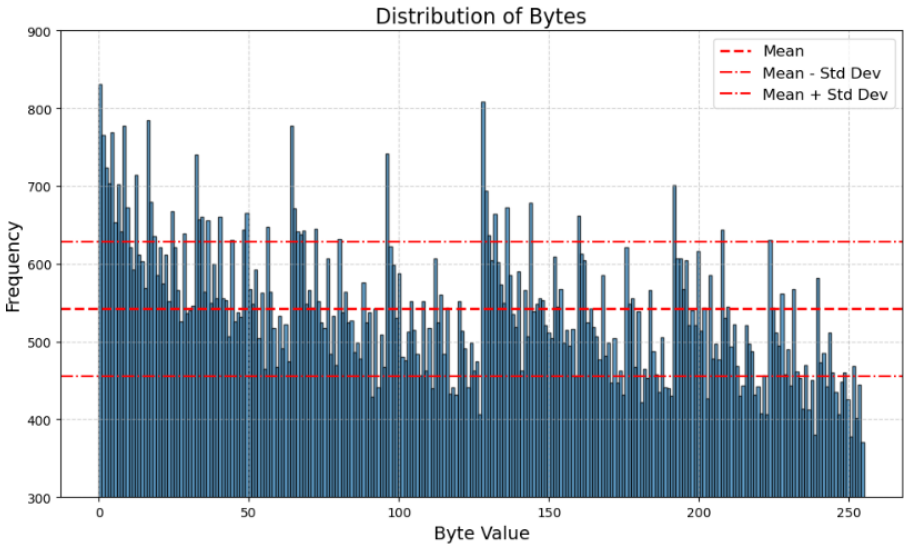

Figure 8: *Distribution of bytes created from the photon-counts events. An almost uniform distribution is obtained.*

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 9.

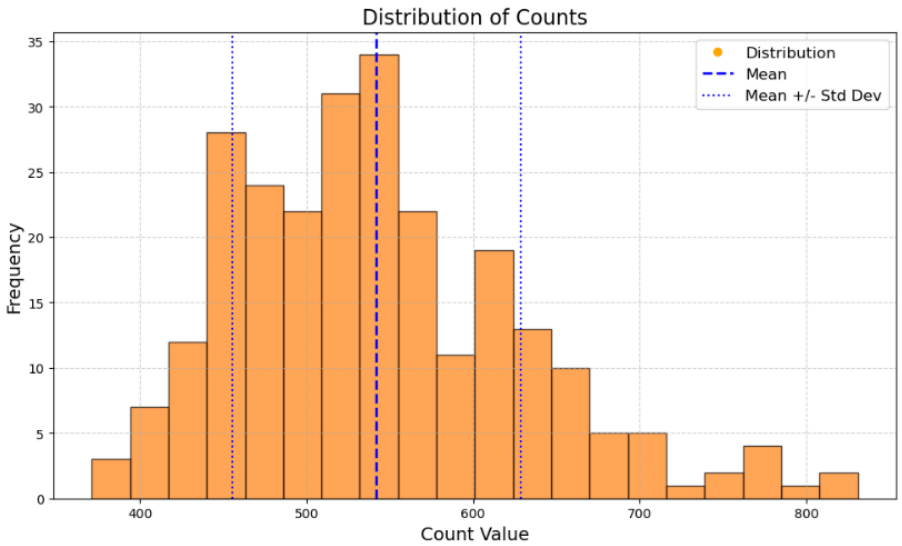

Figure 9: *Distribution of the counts of the bytes created from the photon count events*

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 10, 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.

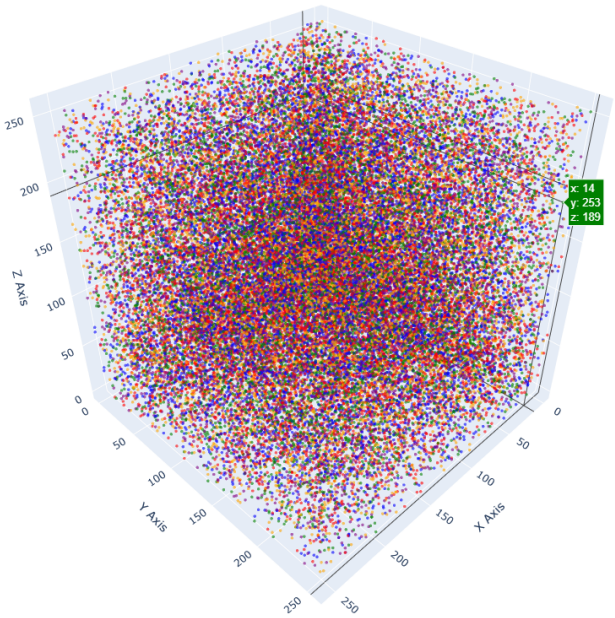

Figure 10: *A 3D representation of the distribution of the bytes, useful to highlight the absence of structures or patterns and the presence of a random data distribution.*

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 = 0.998025 bits per bit.
Optimum compression would reduce the size of this 1109816 bit file by 0
percent.
Chi square distribution for 1109816 samples is 3037.41, and randomly would
exceed this value less than 0.01 percent of the times.
Arithmetic mean value of data bits is 0.4738 (0.5 = random).
Monte Carlo value for Pi is 3.287920073 (error 4.66 percent).
Serial correlation coefficient is 0.013837 (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, even though the error is not negligible still in the quantum version; 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 Conclusions

In this report, we examined the functionality of a heralded single-photon source based on Spontaneous Parametric Down-Conversion (SPDC) within the framework of the GRA experiment. The results confirm Malus' law, illustrating a strong alignment of the transmission model for polarized photons with an RMSE of 0.4%. The fit parameters b and c, essential for our setup, showed excellent agreement with theoretical predictions.
We also studied the delay distributions between heralded and transmitted/reflected photons. Numerical and fit-based analyses of the delay distributions were consistent, though minor differences were observed, likely due to imperfections in the detection setup, particularly the beam splitter's performance, and some low detection counts. The standard deviations from both numerical and fit approaches confirm that timing resolution falls within the expected noise range. We noted that increased data points would enhance the fit's agreement with numerical statistics. Additionally, we tested a quantum random number generator (QRNG) using the photon detection data. Analysis of the generated sequence showed high entropy, minimal serial correlation,

and alignment with expected randomness criteria, contrasting with results from a pseudo-random sequence. This supports the view that QRNGs based on quantum events produce true randomness, which is beneficial for secure cryptographic applications.
Our findings validate that the SPDC source, combined with the heralded detection setup, functions as a reliable single-photon source, demonstrating the non-classical properties essential for advanced quantum experiments. This is further corroborated by the low α value, well below the classical threshold.

7 Code

All the data and the code for the data analysis can be found in this public Github repository: https://github.com/sdracia/Q-OpticsLaser

References

[1] P. Grangier, G. Roger and A. Aspect, *Experimental Evidence for a Photon Anticorrelation Effect on a Beam Splitter: A New Light on Single-Photon Interferences*, Europhysics letters (1986).

[2] E. Hecht, *Optics*, 5th ed., Addison-Wesley (2017).

[3] R. W. Boyd, *Nonlinear Optics*, Academic Press (2020).

[4] J. Walker, *HotBits: Genuine Random Numbers from Radioactive Decay*, https://www.fourmilab.ch/random/.