NUS
National University
of Singapore

CQT
Centre for
Quantum
Technologies

# TOWARDS RANDOM NUMBER GENERATION VIA STELLAR LIGHT

**HO Kim Hung**

**A0122417R**

**Supervisor: Professor Christian KURTSIEFER**

***A Thesis submitted to the Department of Physics (NUS) in partial fulfilment of requirements for the degree of Bachelor of Science with Honours***

# Contents

# Acknowledgement

Foremost, I would like to express my sincere gratitude to my supervisor Prof. Christian Kurtsiefer for giving me the opportunity to learn from him during this project, and for his patience, motivation, enthusiasm, and immense knowledge. His guidance helped me in all time of research. I could not have imagined having a better supervisor and mentor for my honors project.

Besides my supervisor, I would like to thank the colleagues in CQT: Dr Tan Peng Kian, Chng Mei Yuen Brenda, Shi Yicheng, Nguyen Chi Huan for their encouragement, insightful comments, and help professionally and personally.

# Abstract

Photons emitted by celestial objects can be used to generate trusted random numbers. In this experiment, a 14 inch aperture telescope was pointed at the moon, and single-photon avalanche detectors to detect the arrival times. As the generation of photons are at random times as seen with a 2 ns time bin timestamp, the arrival times are also random. The signals from the timestamp was enough to produce random bits at a rate of 551,808 bits/s that pass the standard NIST statistical test.

# 1 Introduction

Random numbers are used in many aspect of society, such as simulating and modelling in Monte Carlo simulation [1], filling in unimportant details in designs like position of the blades of grass in an architect design, or in entertainment like gambling. Apart from these, random numbers are mostly used in generating security keys for cryptography. There are a few criteria for a number to be random. When generating a single random number, each number is drawn in a set of possible value with equal probability, i.e., a uniform distribution. On the other hand, when generating a sequence of numbers, each number is drawn independent of other draws. However as a quote from Donald Knuth [2], what we use in society is not random number, but random number sequences.

> In a sense, there is no such thing as a random number. For example, is 2 a random number? Rather, we speak of a sequence of independent random numbers with a specified distribution.

## 1.1 Cryptography

One of the most widely usage of random numbers today is cryptography. For example, the one-time pad (OTP) [3]. This OTP procedure was developed by Gilbert Vernam and Joseph Mauborgne which is described by figure 1. This key is the most essential security feature in encryption, if this key is predictable or breached, all cryptography breaks down. Therefore, the best kind of key to ensure a safe feature will be a key generated by random numbers.

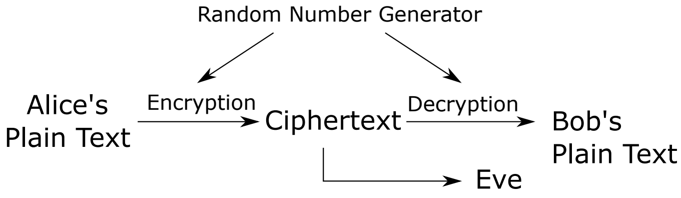


Figure 1: A message from Alice is encrypted with a key generated by a random number generator. The ciphertext is produced by operating a bitwise XOR between the key and the message, then sent to Bob via the internet. Bob then perform another bitwise XOR on the ciphertext and the key to obtain the plain text. If Eve was able to get hold of the ciphertext, she will not be able to extract information about the original message other than the length of the message.

One of the advantages of the OTP is that it is unbreakable for hackers as long as the key is random, and the eavesdropper will take $2^n$ seconds to try all possibility of $n$ bit long keys assuming each permutation takes 1 second to test. The length of n is typically on the order of thousands, therefore the time taken to test all of the permutation exceeds the age of the universe. On the other hand, OTP will require a large amount of random bits in order to supply the demand for one message, not to mention conversations. Therefore, there is a demand for random number generators today.

## 1.2 Random Number Generation

There are mainly two types of random number generators (RNG). The first type of generators are pseudo-RNG. These are basically a mathematical algorithm that takes in a input seed and outputs a number. For example, the linear congruential generator where it requires four input seeds, a multiplier $a$ , increment $c$, modulus $m$, and a initial value $X_0$. The algorithm in which it follows is

$$X_{n+1} = (a \cdot X_n + c)\, mod\, m \tag{1}$$

where it will generate random numbers ranging from 0 to $m - 1$. This number sequence is not a random sequence, but it only appears to be random. The benefits of pseudo-RNG over random number generators is that they give a higher generation rate of random bits. Also, a pseudo-RNG does not require any external devices to take measures as it does not involve any physical process. Pseudo-RNG in fact does not produce random number sequences but appears to be random. This is because given the algorithm and the initial seeds, the output will be exactly the same. However, we do not always need true random numbers. For example, in simulations and modelling, the same set of random inputs to differentiate the effects of a variable in a model from the features of the number sequence.

The second type of generators are physical RNG. These inherit their randomness properties from an external input which are assumed to be random. Such external inputs may be processes like radioactive decay [4], or the position of a mouse cursor on the screen, etc. Since it takes input from a process, a external device is needed to do a measurement like a Geiger counter. Therefore, the output number sequences generally is slower compared to the pseudo-RNG but unreproducible. Consequently, this would be the better choice of generators for encryption.

A sub class of physical RNG is the quantum random number generators (QRNG) which takes input from quantum processes which is a probabilistic processes as suggested by quantum theory's postulates. A quantum system that is in a superposition of states will collapse into one possible state after a measurement was made which makes it a good candidate for a random process. Such a process could be the path in which a photon takes as it passes through a polarizing beam splitter (PBS).

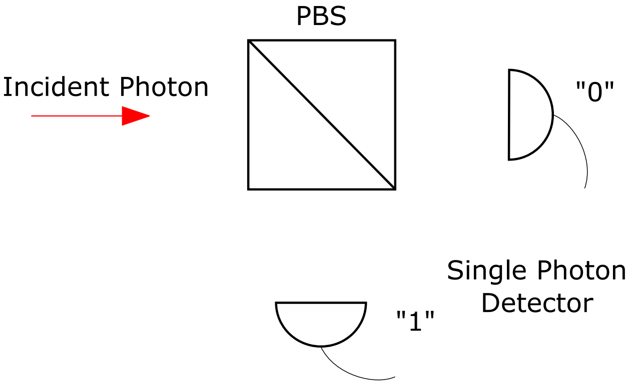


Figure 2: A quantum random generator on single photon events basis. The incident photon with a $\frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$ have 50% chance of being transmitted and reflected due to the probabilistic nature, which will in turn incident on the two detector, where we decide which detector corresponding to a '0' or a '1' bit.

### 1.3 Statistical Test

There are two properties of random number generators that makes them good. The first will be the rate of production which is dependent on the process and the extraction method. Such as taking the difference between the number of detected decay products and the mean number, versus taking the time of each detection and taking the least significant bit. The second property is the quality of random numbers, i.e., whether the outputs form a uniform distribution. We can test them via statistical tests like National Institute of Standards and Technology (NIST) randomness test suit [5], which consist of 13 tests.

### 1.4 Using Stellar Light as a Source of Randomness

There are many random processes that are available to us, such as vacuum fluctuations [6] or radioactive decays [4]. However, we choose to use the arrival time of cosmic photons as the random variable in our physical RNG, or more precisely, the timing interval between two consecutive photon detection from two stellar sources. The timing interval information is preferred compared to the absolute times of photon detection because it removes the biasness from the starting time of the experiment which are controlled by the user. Furthermore, we ensure that both stellar light sources are uncorrelated by each other, i.e., they are space-like separated from each other. Since the information from celestial object A cannot reach B before reaching the detector on Earth. In the case that the two photons are correlated, i.e. information from A reached B before reaching Earth, this will imply that information can travel faster than the speed of light which does not follow Einstein's postulates [7].

Another reason to use cosmic photons instead of a light bulb that is Earth-bound, is that

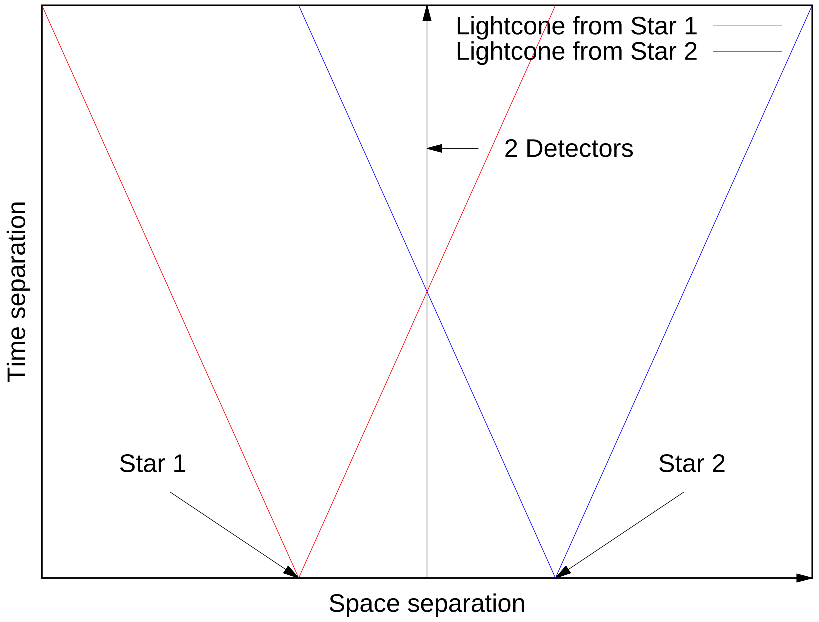


Figure 3: A spacetime diagram of two events depicted in red and blue, the light from event 1 reaches the detector before reaching event 2.

the cosmic photons are unlikely to be tempered with. In order to tamper with it, the hacker would need to do it in the past, or build a light source that follows the detector which requires the light source to be collimated, and moving in sidereal rate. Since we are along the equator, that would need a geostationary satellite. However, if we are not along the equator, the light source would need a source of energy to propel them to move like a geostationary satellite.

# 2 Theory

## 2.1 The Light Source

### 2.1.1 Blackbody Radiation

As we look up in the sky at night, some stars appear blue such as Rigel [8], while others looks red such as Betelgeuse [9]. This is due to the surface temperature of of the stars, with Rigel a surface temperature of roughly 13,000 K and Betelgeuse, a surface temperature of 3,600 K. These emission of light is correlated with the temperature of the hot objects via the Wein's displacement law [10], equation 2.

$$\lambda_{max} T = 0.002897755 \quad m \quad K \tag{2}$$

In 1900, a German physicist Max Planck modified the Wein's displacement law to fit the blackbody spectrum, equation 3 and figure 4, while avoiding ultraviolet catastrophe [11].

$$S_\lambda = \frac{2hc^2}{\lambda^5} \frac{1}{e^{\frac{hc}{\lambda k T}} - 1} \tag{3}$$

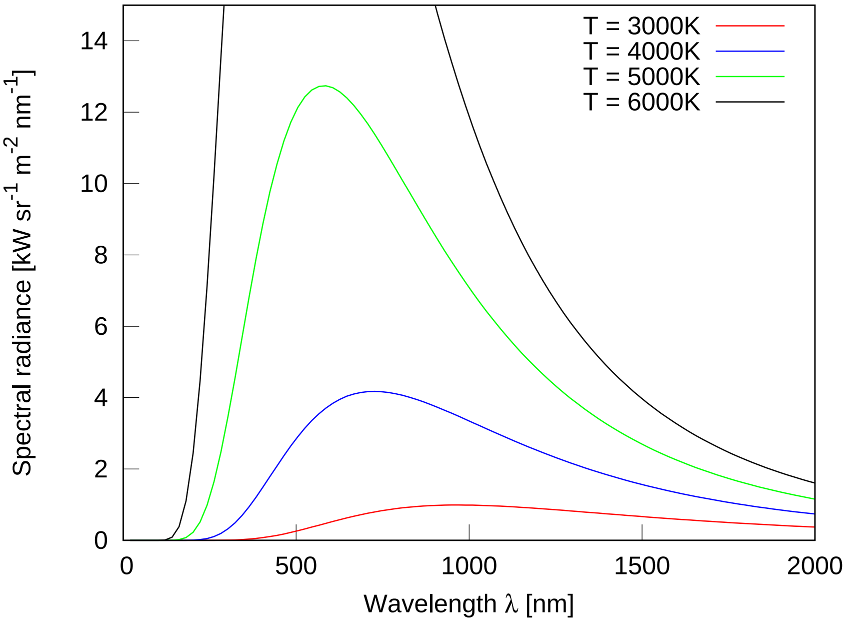


Figure 4: Blackbody spectrum of temperature at 3000K, 4000K, 5000K, 6000K. We can observe that as the temperature increases, the peak of the curve moves towards shorter wavelengths and the full-wave half maximum decreases or the bandwidth increases.

From figure 4, we can see that the bandwidth of a blackbody with a temperature of 5000 K is on the order of 700 nm. Since the coherence time, $\tau_c$, of a thermal source is approximately the inverse of the bandwidth [12], $\Delta f$, the coherence time of a blackbody is on the order of femtoseconds.

$$\tau_c \approx \frac{1}{\Delta f} \tag{4}$$

### 2.1.2 2nd Order Coherence

To have some idea on the timing interval between consecutive photons of different light sources, we introduce the idea of 2nd order coherence, $g^{(2)}(\tau)$. In quantum optics, correlation functions describes the statistical and coherence properties of an electromagnetic field, $E$. The degree of coherence is the normalized correlation of electric field. The normalised $g^{(2)}(\tau)$ is the probability of detecting a photoevent at the other detector after a period of time $\tau$ after the first detector detects a photoevent [12].

$$g^{(2)}(\vec{r}_1, t_1; \vec{r}_2, t_2) = \frac{\langle E^*(\vec{r}_1, t_1) E^*(\vec{r}_2, t_2) E(\vec{r}_1, t_1) E(\vec{r}_2, t_2)\rangle}{\langle \mid E(\vec{r}_1, t_1) \mid^2 \rangle \langle \mid E(\vec{r}_2, t_2) \mid^2 \rangle} \tag{5}$$

$$g^{(2)}(\tau) = \frac{\langle I(t) I(t+\tau)\rangle}{\langle I(t)\rangle^2} \tag{6}$$

where $I$ is the intensity of light.

In order to characterize stationary monomode sources, it is easier to consider $g^{(2)}(0)$, this is because as $\tau$ increases to infinity, normalised $g^{(2)}(\tau)$ will always be 1, which does not give much information about the light source. In figure 5, we show the different $g^{(2)}(0)$ values of a single photon light source, coherent source, and a thermal source.

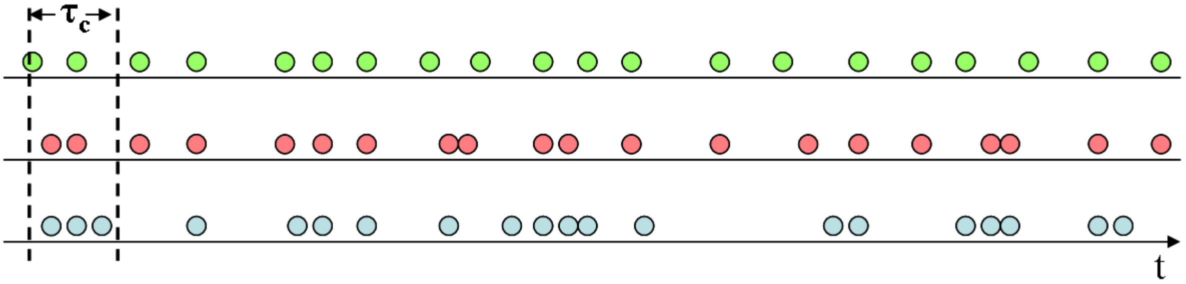


Figure 5: A diagram showing the properties of light with various $g^{(2)}$ values. The green row shows an anti-bunched light source which follows a sub-Poisson distribution, i.e. $g^{(2)} < 1$, example of such a light source is a single photon emitter. The red row shows a coherent light source which follows a Poisson distribution, i.e. $g^{(2)} = 1$, such a light source is a laser. While the blue row shows a bunched light source which follows a super-Poisson distribution, i.e. $g^{(2)} = 2$, such a light source is a thermal source.

### 2.1.3 Spectrum of Thermal Source

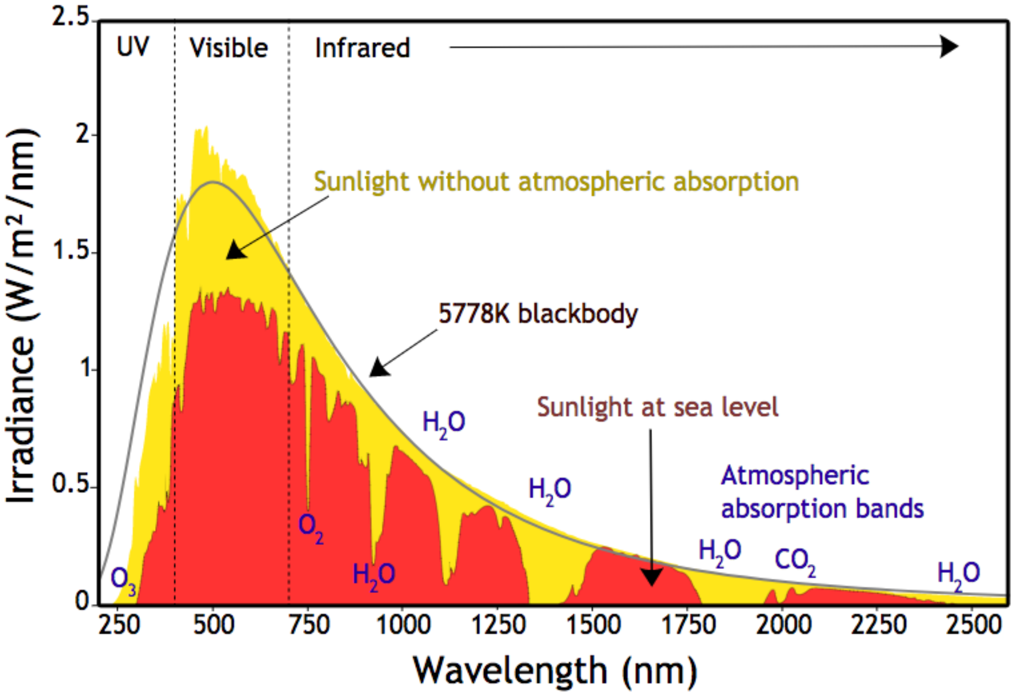


Figure 6: Spectrum of Sun taken from http://physicsbuzz.physicscentral.com/2017/10/physics-in-autumn-sunrise.html.

From the previous section, it suggests that the photons from a thermal source should exhibit super-Poisson distribution. However, when we observe the photons of a thermal source in figure 6, the central peak, $\lambda$, is on the order of 550 nm and full-wave half maximum, $\Delta\lambda$ of the curve is on the order of 300 nm, i.e. not monomode. Since the coherence time is inverse of the bandwidth [12], the coherence time is on the order of femtoseconds. Therefore, as long as the time-bin of the time stamp is much much larger than femtoseconds, the detected photons will follow a Poisson distribution instead of super-Poisson, i.e. $g^{(2)} = 1$. Hence, the arrival times of photons can be used as a random variable. It is good to take note that the spectrum cannot fit to a blackbody curve due to several reasons. First, it is due to the absorption from the Earth's atmosphere and interstellar dusts which reddens the spectrum [13]. Second, the may spectrometer used is not efficient at all wavelengths. Nevertheless, the FWHM of the spectrum can be used to estimate the coherence time of thermal sources.

$$\begin{aligned} f &= \frac{c}{\lambda} \\ df &= \frac{cd\lambda}{\lambda^2} \\ \tau_c &\approx \frac{1}{\Delta f} = \frac{\lambda^2}{c\Delta\lambda} \\ &\approx 3.36fs \ll 2ns \end{aligned} \tag{7}$$

## 2.2 Quantifying Randomness

### 2.2.1 Shannon Entropy

In order to find out how much information to extract from the timing interval, we study about Shannon entropy of a Poisson source in equation 9 to quantify the amount of "randomness". Shannon's information theory is the measure of information, and Shannon entropy, given by equation 8 is the amount of information encoded in a ensemble measured in bits [14], where $p_k$ gives the probability of event $k$ happening. It can also be interpreted as the minimum number of bits to express the contents. For example, the amount of entropy in a fair coin is 1 bit as the $p_k = \frac{1}{2}$.

$$\begin{aligned} H &= -\sum p_k \log_2 p_k \\ &= -\frac{1}{2}\log_2\frac{1}{2} - \frac{1}{2}\log_2\frac{1}{2} = 1 \end{aligned} \tag{8}$$

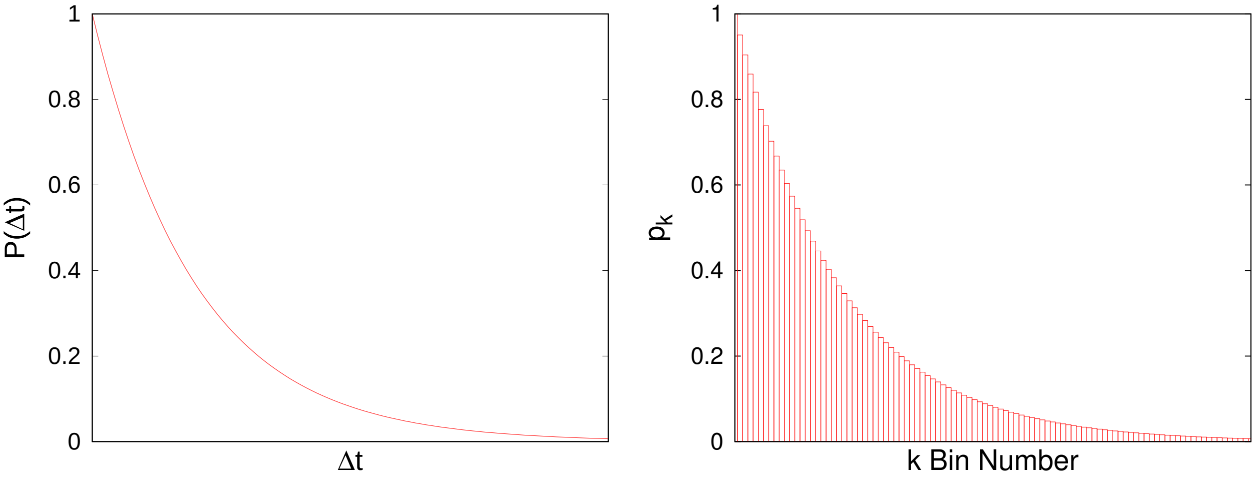
Let us consider a source which emits photons that follows a Poisson distribution, probability of $k$ events in a time interval is $e^{-\lambda}\frac{\lambda^k}{k!}$, and we detect the photons with a detector where $k$ is the time-bin number, $T$ is the time-bin size, $r$ is the average count rate. $\Delta t$ is the timing interval between two consecutive photon detection.

We show that the probability distribution of various timing interval, $P(\Delta t)$, is given by equation 9 [15].

$$P(\Delta t) = r \cdot e^{-\Delta t \cdot r} \tag{9}$$

However, the timestamp gives a discrete timing interval in terms of bin number, therefore a discretization is performed. $p_k$ is the probability of two consecutive photon with timing interval registered as k time bin apart.

$$\begin{aligned} p_k &= \int_{k\cdot T}^{(k+1)\cdot T} r \cdot e^{-\Delta t \cdot r} d\Delta t \\ &= \int_{k\cdot T\cdot r}^{(k+1)\cdot T\cdot r} e^{-\beta} d\beta, \qquad \beta = r\cdot\Delta t \\ &= -e^{-\beta}\Big|_{k\cdot T\cdot r}^{(k+1)\cdot T\cdot r} \\ &= e^{-k\cdot T\cdot r}\cdot(1-e^{-T\cdot r}) \\ &\approx e^{-k\cdot T\cdot r}\cdot(1-(1-T\cdot r) \\ &= T\cdot r\cdot e^{-k\cdot T\cdot r} \end{aligned} \tag{10}$$



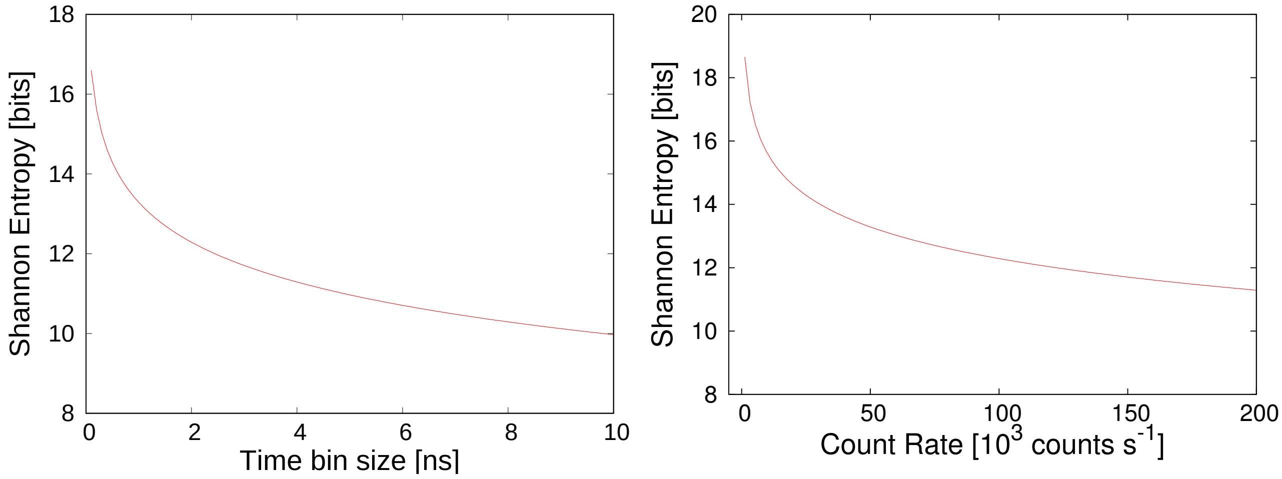
(a) Before discretization.

(b) After discretization.

Figure 7: We plot equation 9 in (a). This shows the probability distribution of various timing interval as a continuous function. However, the timestamp outputs the timing interval in discrete time bins, therefore discretization is performed and plotted in (b).

Afterwhich, the theoretical Shannon entropy of a Poisson source is shown in equation 11.

$$
\begin{aligned}
H &= -\sum_{k=1}^{N} p_k \log_2 p_k \\
&= -\sum_{k=1}^{N} T \cdot r \cdot e^{-k \cdot T \cdot r} \cdot \log_2(T \cdot r \cdot e^{-k \cdot \Delta t \cdot r}), \qquad \alpha = r \cdot T \\
&= -\sum_{k=1}^{N} \alpha \cdot e^{-\alpha \cdot k}[\log_2(\alpha) + \log_2(e^{-\alpha \cdot k})] \\
&= -\frac{\alpha}{\ln 2}\left\{\sum_{k=1}^{N}(e^{-\alpha \cdot k} \cdot \ln \alpha - \alpha \cdot k \cdot e^{-\alpha \cdot k})\right\} \\
&= -\frac{\alpha}{\ln 2}\sum_{k=1}^{N} e^{-\alpha \cdot k} + \sum_{k=1}^{N} \frac{\alpha^2}{\ln 2}\frac{\partial}{\partial \alpha} e^{-\alpha \cdot k} \\
&= -\frac{\alpha \cdot \ln \alpha}{\ln 2}\frac{1}{1 - e^{-\alpha}} - \frac{\alpha^3 \cdot e^{-\alpha}}{\ln 2[1 - e^{-\alpha}]^2}
\end{aligned}
\tag{11}
$$



(a) H as a function of time bin size.

(b) H as a function of count rate.

Figure 8: We plot the Shannon entropy as in equation 11 with constant count rate of 100 000 counts per second as shown in (a). As the bin size increases, the amount of entropy decreases. We plot the Shannon entropy as in equation 11 with constant time bin at 2 ns as shown in (b). We can see that count rate increases, the amount of entropy decreases. This is consistent as the rate or time bin size increases, the number of bins between consecutive photons decreases, hence the amount of bits needed to represent it decreases.

# 3 Experimental Set-up

## 3.1 Measuring Spectrum

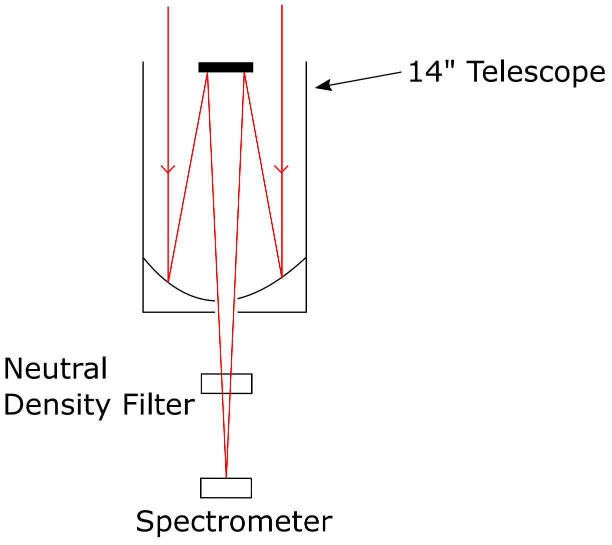


Figure 9: Diagram of experimental setup to measure the spectrum of celestial objects. One 14 inch aperture telescope with a spectrometer. The beam passes through a neutral density filter in order to attenuate the amount of light entering the spectrometer to prevent saturation.

First, we verify the spectrum of the Sun as mentioned in section 2.1.3 by using a Ocean Optics USB2000+ spectrometer [16]. The spectrum of the Jupiter and the Moon was measured with the help of the telescope and the Sun is measured without the telescope because the intensity of sunlight is very high.

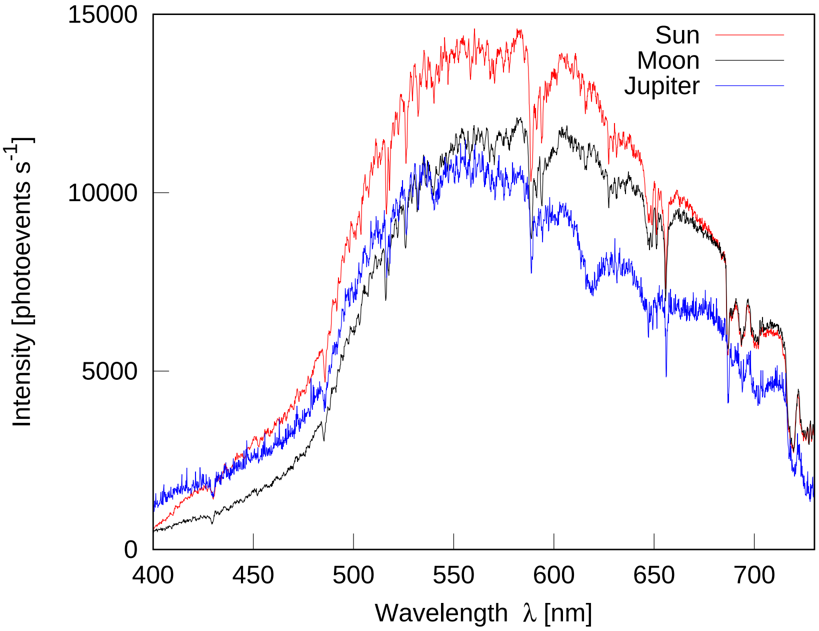


Figure 10: Spectrum of the Sun, Moon, Jupiter.

From figure 10, we observed that all three of the celestial objects have similar spectra as they have similar absorption lines at 580 nm, 660 nm and 680 nm. Since the light from Jupiter and the Moon are reflected light from the Sun, it is not surprising that the spectra are similiar. We can also see that the bandwidth of the Sun is on the order of 200 nm which corresponds to a coherence time in the order of femtoseconds.

$$\begin{aligned} \tau_c \approx \frac{1}{\Delta f} = \frac{\lambda^2}{c\Delta\lambda} \\ \approx 5.04 fs \ll 2ns \end{aligned} \tag{12}$$

## 3.2 Collecting Cosmic Photons

To collect cosmic photons, we have a set-up as shown in figure 11. The 14 inch telescope has a diffraction limit, $\theta$ of 0.326 arcsec [17] that follows the Dawe's limit in equation 13.

$$\theta = \frac{4.56}{D} \tag{13}$$

where $D$ = aperture size in inches = 14.

The diffraction limit of the telescope corresponds to one pixel on the CMOS sensor, which is basically a camera, acting as an eyepiece. The image shown by the CMOS sensor will tell whether the telescope is in focus when looking at a diffraction-limited source, i.e. a star, since it

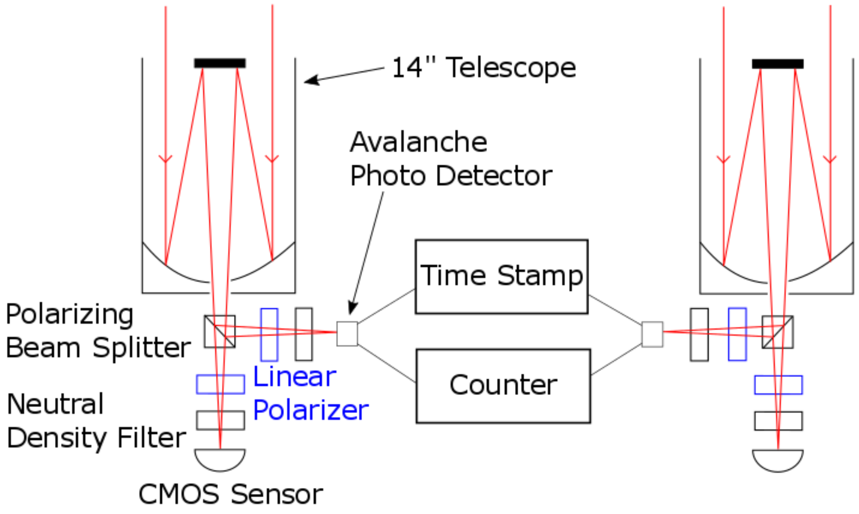


Figure 11: Diagram of experimental setup to collect photons from celestial object. Two 14 inch aperture telescope with a avalanche photon detector connected to a time-stamp, and a counter. The beam path passes through a polarizing beam splitter, linear polarizer and a neutral density filter.

will appear as a single pixel. The distances between PBS and CMOS sensor, PBS and detector are approximately the same, so that once the image on the sensor is in focus, the image on the detector is also in focus. The telescope is also collimated with the help of a Duncan mask which covers the aperture of the telescope at 60° interval, allowing better determining which screws on the secondary mirror to adjust to collimate the telescope. This ensures that uncollimated light does not enter the avalanche photon detector (APD), i.e. surrounding light from street lamps, etc, and most of the detected light comes from the celestial object. The telescope is mounted on a equatorial mount for easier tracking via the right ascension and declination axis.

The collected light passes through a polarizing beam splitter (PBS) to split the beam to the APD for detection and the CMOS sensor to aim the telescope. A PBS was used instead of a BS was to save some space on the contraption attached onto the telescope. The contraption contains the optical elements and detectors. The center of mass of the contraption needs to be close to the telescope in order to reduce torque and vibration during the tracking of the celestial object. A linear polarizer is placed on a rotation mount to provide an angle between the light's initial polarization and the axis of the polarizer as suggested by Malus's law, equation 14 [18]. This allows the count rate on the APD to be controlled in a continuous function, acting like a fine adjustment knob.

$$I = I_0 \cos^2 \theta \tag{14}$$

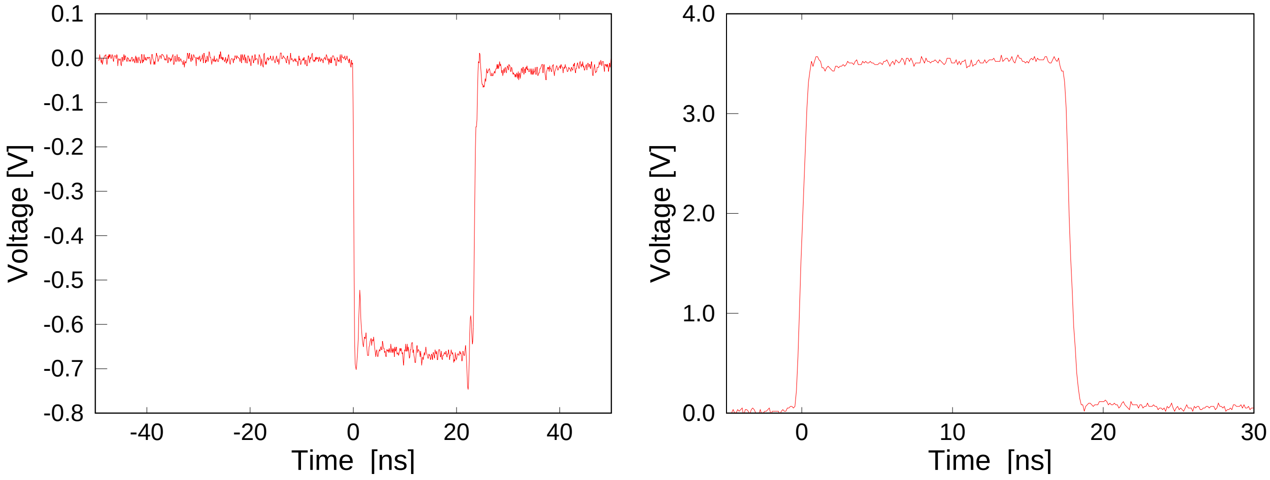
where $I_0$ = initial intensity, and $\theta$ = the angle between initial polarization and the optical axis of the polarizer.

After the polarizer, a neutral density (ND) filter is placed to further control the count rate on the APD. The ND filter follows equation 15 and allows the count rate on the APD to be controlled in a discrete function due to the optical densities of the ND filters available. Ultimately, the count rate of the APD is monitored by sending the signals from the APD to a counter during the experiment. The count rate on the APD cannot be too high as they may saturate or every time-bin will register a photon which does not produce random bits. On the other hand it cannot be too low as it will give a very low rate of generation. This gives us a upper bound of approximately 6 million counts per second as the APD saturates.

$$T = 10^{-OD} \tag{15}$$

where $T$ = transmittion, and $OD$ = optical density.

The APD used is a single photon detector from Micro Photon Devices [19] with a dead time of 77 ns. It has two output channels, Nuclear Instrumentation Module (NIM) and Transistor-Transistor Logic (TTL) with a timing resolution of 250 ps and 50 ps respectively. The TTL output is sent to the counter as it does not need to have high timing resolution, while the NIM output is sent to a time-stamp since it is the random variable being measured. The time-stamp used has a time-bin, $T$, of 2 ns which is much much larger than coherence time in equation 7. Therefore, the thermal source will show a Poisson distribution instead of super Poisson distribution [12].



(a) NIM signal.

(b) TTL signal.

Figure 12: Pulse signals produced by NIM output channel of the APD seen in an oscilloscope which is a pseudo-square pulse with -700 mV in depth and 20 ns wide, where each photoevent detection produce one pulse shown in (a). Pulse signal generated by TTL output, right, of the APD measured with an oscilloscope which is a pseudo-square pulse with 3.5V high and about 20ns wide shown in (b).

We count the number of photoevents every 100 $\mu s$ from moonlight at a rate of 122,624 counts per second, which gives us a average count of 12 counts per 100 $\mu s$. Since the average count per 100 $\mu s$ is larger than 1, the Poisson distribution can be approximated to a Gaussian curve. The mean value of the Gaussian curve is 11.95 counts and the FWHM is 7.36. We note that the distribution cannot be fitted to a Gaussian curve as it is slightly skewed due to the inconsistent count rate.

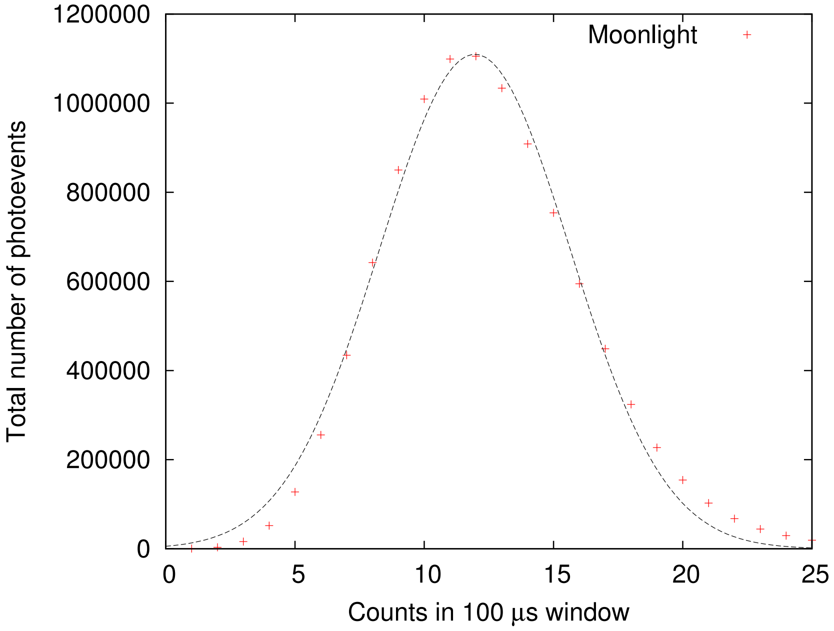


Figure 13: A distribution of number of photoevent from moonlight every 100 $\mu s$ (red). It is not fitted perfectly to a Poisson distribution but could be due to the inconsistent count rate. But it is a good approximation of a Poisson source.

# 4 Random Number Extraction

## 4.1 Least Significant Bit

With the nanosecond timestamp, the infomation of the arrival time is encoded into a 32 bit string of 0 and 1. The least significant bit (LSB), i.e. the first bit from the right, correspond to a 2 ns time-bin. One way of extracting random bits will be taking this least significant bit. The reason the LSB is taken instead of other bits is that the LSB changes more frequently. If the bit does not change frequently, there will be long strings of 1 or 0. For example, the second hand changes compared to the hour hand. In our extraction process, we harvest the 4 LSB, i.e. the 4 right most bit, of the absolute times of each photo event to increase the extraction rate.

## 4.2 Hash Matrix

Another way to extract random bits from the arrival times is to perform hashing by using a random matrix, M [20]. This is because the last few bits may not be very reliable, and there is a possibility that Eve knows about some information on the bits. A hash function maps arbitrary strings of data to a fixed length output in a deterministic, public, and “random” manner. Each element in the matrix is to be populated by random bits. These random bits will come from the even-odd parity of the timing intervals. The size of the hash matrix will be a H by 32 matrix, where H is the Shannon entropy. Next, we perform a binary matrix multiplication with a bit vector, $x$ which is populated by the absolute time of photoevents [21]. A binary matrix multiplication similar to a normal matrix multiplication except that the plus operator becomes an XOR operation and the multiplication operator becomes an AND operator.

$$H(x) = \qquad M \qquad \times \quad x \tag{16}$$

$$\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & \cdots & \\ 1 & \ddots & & \\ \vdots & & & \\ & & & \end{pmatrix} \times \begin{pmatrix} 1 \\ 1 \\ \vdots \\ \vdots \\ 0 \end{pmatrix} \tag{17}$$

If we were to take a pair of keys, $x$ and $y$ where $x \neq y$. Both keys will differ in someplace, as an example we take $x$ and $y$ differ only in the $i$th position, i.e. $x_i = 0$ and $y_i = 1$. Imagine we first choose all of M but the $i$th column. Over the remaining choices of $i$th column, $H(x)$ is fixed. However, each of the different $2^{32}$ settings of the $i$th column gives a different $H(y)$ value.

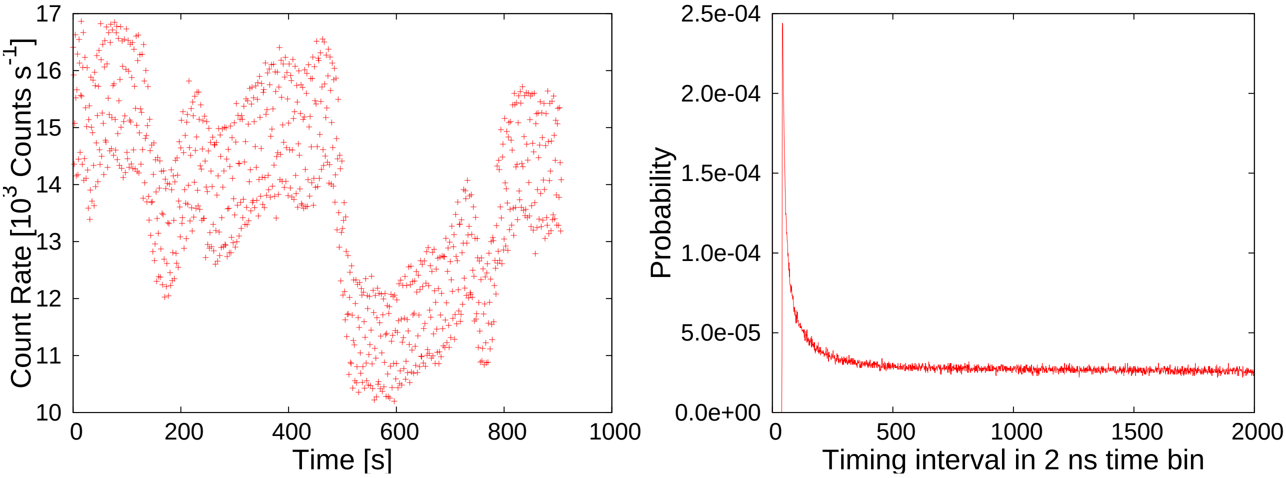
Therefore, there is exactly a $\frac{1}{2^{32}}$ chance of $H(x) = H(y)$. This process helps to even out the probability distribution of the random variable [22].

This will allow us to extract H number of bits per detected photons. Since the information encoded in the arrival time is H bits, therefore extracting more than H bits should carry no randomness, and should fail the NIST test. In practise, the number of rows in the matrix is not taken to be equal as Shannon entropy but sightly less than the entropy.

# 5 Results and Discussion

As a proof-of-concept, only one APD was used and sunlight was incident on it. The APD is exposed to sunlight for 15 minutes at an average rate of 6848 counts per sec. The timing interval between two successive detection was measured and plotted onto a histogram. With equation 8, where $\alpha = r \cdot T = (6848) \cdot (2 \times 10^{-9})$, the entropy was calculated to be 16.45 bits while the theoretical entropy with an average rate of 6848 counts per second is 16.15 bits given by equation 11 with a discrepancy of 1.85 %.

$$H = -\frac{\alpha \cdot \ln \alpha}{\ln 2} \frac{1}{1 - e^{-\alpha}} - \frac{\alpha^3 \cdot e^{-\alpha}}{\ln 2[1 - e^{-\alpha}]^2}$$



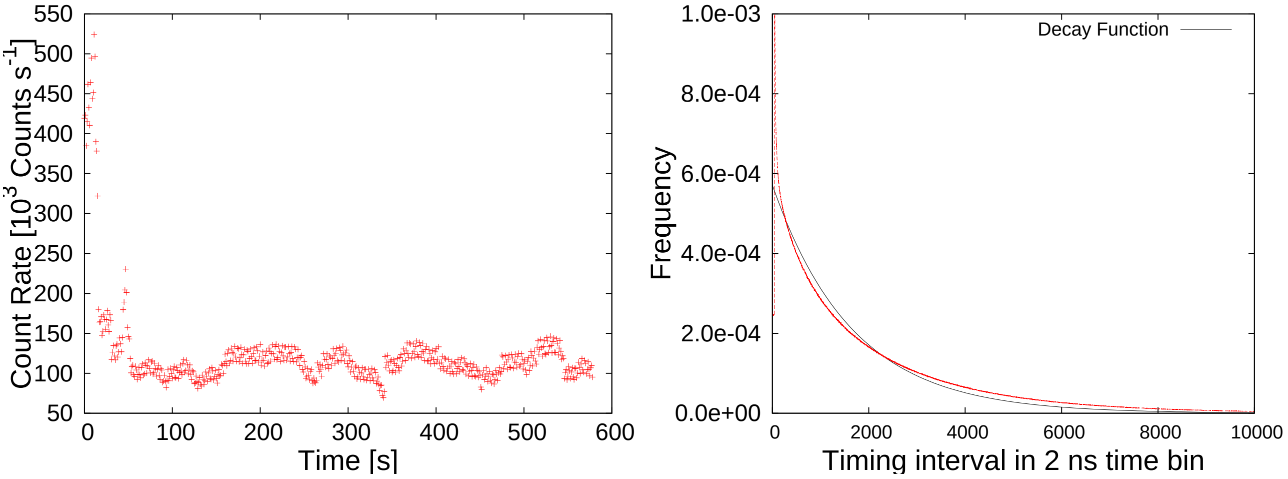
(a) Count rate of sunlight.

(b) Measured distribution of $p_k$.

Figure 14: A plot of the countrate during the experiment, shown in (a), with 1 detector detecting photon from the sun, where time 0 refers to the start of experiment. It shows a fluctuating countrate between 8500 to 5000 with an average count rate of 6848 counts per second over a duration of 907 seconds. A histogram of the timing intervals of detected photoevents, shown in (b), from the sun at an average rate of 6848 counts per second. The tail decreases slowly to 0 after time-bin 200000. We observed an offset of approximately 40 time-bins which corresponds to 80 ns. This is due to the deadtime of the APD [19] and the pulse width of the signal output from the detectors as shown in figure 12a which correspond to about 97 ns and hence 49 time-bins.

With the absolute arrival times of the photons, the 4 LSB of each measurement was extracted and the NIST test was performed on them. The result of the 4 LSB was able to pass the NIST test. We compare the number of ones and zeroes from the 4 LSB and we get a ratio of 0.50002 : 0.49998 zeroes to ones.

Next the LSB of the timing intervals was extracted and run it through the NIST test. The result was also able to pass the NIST test. This give us a generation rate of 30,816 bits/s.We compare the number of ones and zeroes from the 4 LSB and we get a ratio of 0.5002 : 0.4998



(a) Count rate of moonlight.

(b) Histogram of probability of k time bin interval.

Figure 15: A plot of the countrate during the experiment with 2 detectors detecting photons from the moon, shown in (a), where time 0 refers to the start of experiment. It shows a fluctuating countrate between 50,000 to 150,000 with an average count rate of 2 detectors at 122,624 counts per second over a duration of 579 seconds. A histogram of the timing intervals of detected photoevents from the Moon at a total average rate of 122,624 counts per second of two APD , shown in (b). With an tail that appears to look like an exponential decay function as shown in equation 10, $T \cdot r \cdot e^{-k \cdot T \cdot r}$. However it could not be fitted to a decay function due to the non-constant rate of photoevents.

zeroes to ones. With these two methods, the generation rate is limited by the rate of incident photons.

Next, we build a 11 by 32 hash matrix by filling up with the LSB of the timing intervals. Although the Shannon entropy is 16 bits, we do not build a 16 by 32 matrix as the last few bits may not be very trustworthy random numbers. Upon hashing, the output is able to pass the NIST test with 400000 stream length and 20 bit stream. We compare the number of ones and zeroes from the 4 LSB and we get a ratio of 0.500002 : 0.499998 zeroes to ones. With this method of extraction, it increases the generation rate to 68,480 bits/s. We attempt to build a 20 by 32 hash matrix, i.e. larger than the Shannon entropy, and it was able to fail the NIST test as expected.

In another test, the two telescopes with two APDs attached was pointed at the Moon and collected photons for 9.56 mins at a total average rate of 122,624 counts per second. Similarly, we substitute $\alpha = r \cdot T = (122624) \cdot (2 \times 10^{-9})$ into equation 8, the Shannon entropy was calculated to be 12.41 bits and the theoretical entropy is 11.99 bits, with a discrepancy of 3.50%.

$$H = -\frac{\alpha \cdot \ln \alpha}{\ln 2} \frac{1}{1 - e^{-\alpha}} - \frac{\alpha^3 \cdot e^{-\alpha}}{\ln 2 [1 - e^{-\alpha}]^2}$$

The tail of the histogram could not be fitted to a decay function due to the rate of photons not being constant as shown in figure 15a. However, it does appear to look like a decay function.

We perform the same operations as before, extracting the 4 LSB and the LSB of the absolute time and timing intervals respectively, and both outputs are able to pass the NIST test, giving a generation rate of 551,808 bits/s. We compare the number of ones and zeroes from the 4 LSB of the absolute time and we get a ratio of 0.50002 : 0.49998 zeroes to ones and the ratio of ones and zeroes from the LSB of timing interval is 0.5006 : 0.4994.

However, when the 10 by 32 hash matrix was built with the even-odd parity of the timing interval and acting it on the timing interval, it was unable to pass the NIST test. This may be due to some interference during the beginning of the experiment as shown in figure 15a where the count rate was very high as compared to the others.

# 6 Conclusion and Outlook

We are able to measure the spectra of Jupiter, the Moon and the Sun to see that the bandwidth of a thermal source is wide, on the order of 200 nm, therefore a short coherence time, on the order of femtoseconds. In addition, we collect photons from the Sun with one APD, and the Moon with two APDs to extract randomness from the timing information. Randomness are extracted by taking the 4 LSB of the absolute time of photons, the LSB of the timing interval between consecutive photons and hashing.

There are some more work to solve some bugs in the data from the Moon. The results from the hashing of the photons from the Moon are unexpected as the timing intervals should be random and the hash matrix are therefore populated with random bits. But the output of the hashing could not pass the NIST test.

Apart from this, we can further increase the reliability of the random numbers by reducing the probability of the photons incident on the two APD being correlated. We can do this by pointing the telescopes at two different stars, and not just any stars, but two space-like separated stars. This is because of Albert Einstein's postulates of special relativity which states that nothing can travel faster than the speed of light [7], even information. Information from star A will reach Earth before reaching star B, hence star A cannot be correlated with star B.

We extract randomness from the two stars by performing a bitwise XOR operation between the timing information from star A and star B. Since the result of XOR gives the correlation between the two string, and the two stars are ensured to be uncorrelated, the output output will give "randomness".

Consequently, we are able to use the setup in different ways. One, we can use the setup as a cosmic RNG [23]. The output of the RNG can also be used in cryptography, etc. Another way to use the setup could be to perform a Bell's test [24].

# References

[1] Christian P Robert. *Monte carlo methods.* Wiley Online Library, 2004.

[2] Donald Ervin Knuth. *The art of computer programming*, volume 3. Pearson Education, 1997.

[3] Wade Trappe. *Introduction to cryptography with coding theory.* Pearson Education India, 2006.

[4] Kenneth S Krane and David Halliday. *Introductory nuclear physics*, volume 465. Wiley New York, 1988.

[5] Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, and Elaine Barker. A statistical test suite for random and pseudorandom number generators for cryptographic applications. Technical report, Booz-Allen and Hamilton Inc Mclean Va, 2001.

[6] Yicheng Shi, Brenda Chng, and Christian Kurtsiefer. Random numbers from vacuum fluctuations. *Applied Physics Letters*, 109(4):041101, 2016.

[7] A Einstein. The foundation of the generalised theory of relativity. *On a Heuristic Point of View about the Creation and Conversion of Light 1 On the Electrodynamics of Moving Bodies 10 The Development of Our Views on the Composition and Essence of Radiation 11 The Field Equations of Gravitation 19 The Foundation of the Generalised Theory of Relativity*, 22:22, 1916.

[8] G Israelian, E Chentsov, and F Musaev. The inhomogeneous circumstellar envelope of rigel ($\beta$ orionis a). *Monthly Notices of the Royal Astronomical Society*, 290(3):521–532, 1997.

[9] Bernd Freytag, Matthias Steffen, and Bertil Dorch. Spots on the surface of betelgeuse–results from new 3 d stellar convection models. *Astronomische Nachrichten*, 323(3-4):213–219, 2002.

[10] Bradley W Carroll and Dale A Ostlie. *An introduction to modern astrophysics.* Cambridge University Press, 2017.

[11] Max Planck. Ueber das gesetz der energieverteilung im normalspectrum. *Annalen der physik*, 309(3):553–563, 1901.

[12] Mark Fox. *Quantum optics: an introduction*, volume 15. OUP Oxford, 2006.

[13] AE Whitford. The law of interstellar reddening. *The Astronomical Journal*, 63:201–207, 1958.

[14] Claude Elwood Shannon. A mathematical theory of communication. *ACM SIGMOBILE Mobile Computing and Communications Review*, 5(1):3–55, 2001.

[15] John CB Cooper. The poisson and exponential distributions. *Mathematical Spectrum*, 37(3):123–125, 2005.

[16] Inc Ocean Optics. Ocean optics usb2000+ datasheet, 2001.

[17] Meade. Meade lx850 datasheet, 2013.

[18] Edward Collett. *Field guide to polarization*, volume 15. 2005.

[19] Micro Photon Devices. Pdm series datasheet, 2013.

[20] Ivan Marcikic, Antia Lamas-Linares, and Christian Kurtsiefer. Free-space quantum key distribution with entangled photons. *Applied Physics Letters*, 89(10):101122, 2006.

[21] David JC MacKay. *Information theory, inference and learning algorithms.* Cambridge university press, 2003.

[22] Douglas R. Stinson. Universal hashing and authentication codes. *Designs, Codes and Cryptography*, 4(3):369–380, 1994.

[23] Cheng Wu, Bing Bai, Yang Liu, Xiaoming Zhang, Meng Yang, Yuan Cao, Jianfeng Wang, Shaohua Zhang, Hongyan Zhou, Xiheng Shi, et al. Random number generation with cosmic photons. *Physical review letters*, 118(14):140402, 2017.

[24] Johannes Handsteiner, Andrew S Friedman, Dominik Rauch, Jason Gallicchio, Bo Liu, Hannes Hosp, Johannes Kofler, David Bricher, Matthias Fink, Calvin Leung, et al. Cosmic bell test: measurement settings from milky way stars. *Physical review letters*, 118(6):060401, 2017.