PHYS212 Final Report: Quantum Random Number Generator

Ege Aydın
Department of Physics, Bilkent University
(Dated: May 9, 2021)

Random number generation is a vital process in many computer science applications, arguably most importantly in cryptography. It is vital for random numbers to be truly random and cannot be guessed in any way. One way of generating such numbers is to make use of the randomness that occurs from quantum tunneling phenomenon. If a device can capture when the tunneling event occurs, the data can be used to get a random variable with an exponential distribution. Finally, using inverse transform sampling method the raw data can be transformed into desired random distribution and used in any application.

I. INTRODUCTION

In order to make sure that the encryption is secure, first the random numbers that are used to generate keys must be truly random. If an attacker can somehow guess the result of the random key generation, the encryption becomes invalid. Currently computers use pseudo random number generator(PRNG) that uses user actions as an entropy source to seed a random number generator[1]. However, this is not truly random since with the RNG seed the whole system is a deterministic process. Rather than PRNGs, true RNGs use non-deterministic entropy sources[2]. In quantum physics, the Schrödinger's equation and the concept of probability waves show that the particles do not act in a deterministic manner so they can be used as randomness sources.

There are many ways to extract random entropy from many quantum sources. One way involves optics and how photons are delivered in energy packets but not in a continuous stream. If a photon source is connected to a 50-50 beam splitter, and two output of the beam splitter is observed with a sensor, it will be seen that the photon chooses one of the two possible path in a random manner[3]. For such a device however, a faint laser that consistently send very little amount of photons and two single photon detectors are necessary. In order to get correct readings, very precise instruments are necessary which makes the price of the device soar[4].

Another way is to use shot noise that occur with semiconductors. For example an avalanche diode can be used as an entropy source. However, Some deterministic factors such as temperature, electromagnetic interference, etc. also creates noise and they are very hard to distinguish from the actual true random noise caused by the quantum effect[5].

In this project, a Geiger-Müller tube is used to get random numbers. The idea is that a uranium atom emits alpha rays due to quantum tunnelling where the alpha particle can escape the nucleus with some probability even though it doesn't have enough potential. Then if we can observe every time an emission occurs, we can treat the time intervals between emissions as a continuous random variable(RV). If we can determine the probability distribution of the random variable, the inverse transform sampling method can be used to generate random numbers with a desired distribution[6].

II. THEORY

The quantum tunneling can be expressed with the following equations: Schrodinger's equation is:

$$i\hbar\frac{\partial\Psi}{\partial t} = -\frac{\hbar}{2m}\frac{\partial^2\Psi}{\partial x^2} + V\Psi$$

$$\frac{\partial^2 u}{\partial x^2} = \frac{2m}{\hbar}(V-E)u$$

Assuming a structure with a barrier, we can solve this equation.

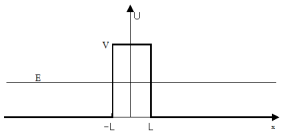

Figure 1. Potential barrier

Here, there are 3 partitions. In the left and right part, $V - E = -E$ and negative. In the middle part, $V - E$ term is positive.

For for the left part, the solution represents a standing wave:

$$\frac{\partial^2 u}{\partial x^2} = -k^2 u$$

$$k = \sqrt{\frac{2m}{\hbar}E} \tag{1}$$

$$u(x) = A_1 e^{jkx} + A_2 e^{-jkx}$$

The solution of the right part is similar but it represents a travelling wave in $+x$ direction:

$$u(x) = Ce^{jkx}$$

For the middle part we got a exponentially decaying probability:

$$\frac{\partial^2 u}{\partial x^2} = K^2 u$$

$$K = \sqrt{\frac{2m}{\hbar}(V-E)} \tag{2}$$

$$u(x) = B_1 e^{Kx} + B_2 e^{-Kx}$$

Using boundary conditions these equations can be used to get the following:

$$A_2 = A_1 e^{-2jkx}\frac{Q-1}{Q+1} \tag{3}$$

$$Q = \frac{\cosh(2KL) - (jk/K)\sinh(2KL)}{\cosh(2KL) - (K/jk)\sinh(2KL)} \tag{4}$$

In these equations, A_1 is proportional to inputted particles, A_2 can be thought as the reflected part and C is the particles that pass the barrier. From conservation of particles, we can say that:

$$|A_1|^2 - |A_2|^2 = |C|^2$$

The absolute value of eq. 3 cancels out the complex exponential:

$$|A_2| = |A_1|\left|\frac{Q-1}{Q+1}\right|$$

The fraction of the particles that get through the barrier is simply $\frac{|C|^2}{|A_1|^2}$.

$$f = \frac{|C|^2}{|A_1|^2} = 1 - \frac{|A_2|^2}{|A_1|^2} = 1 - \left|\frac{Q-1}{Q+1}\right|^2$$

$$f = 1 - \frac{1}{\cosh^2(2KL) + \frac{1}{4}(k/K - K/k)^2\sinh^2(2KL)}$$

For large KL, $\sinh(2KL) \approx \cosh(2KL) \approx e^{2KL}$ can be approximated. Then the equation above can be simplified as the following:

$$f \approx \frac{e^{-4KL}}{1 + \frac{1}{4}(k/K - K/k)^2}$$

This number shows us the fraction of particles that get through the potential barrier with respect to input. For the nuclear decay, the input can be assumed to occur continuously and independently at a constant average rate. Since every emission has a rate of tunnelling we found above, the time between each emission is an exponential distribution with λ that is determined by f and number of particles[7].

III. METHODOLOGY

The experiment's main device is the Geiger-Müller tube. The data can be collected if the Geiger-Müller tube can be properly operated. The datasheet of the aforementioned tube implies a 400V source is necessary for operation. In order to generate this voltage, a ZVS circuit is used. The ZVS circuit uses a high voltage transformer and resonates the primary of the transformer with a capacitor, which results in high voltages in the secondary. After the circuit is designed, it's printed on a PCB and placed inside a plastic box for safety. The 400V

Figure 2. ZVS high voltage generator circuit in its plastic box

DC output is connected to the Geiger-Müller tube over some resistors. When an emission is detected, the tube conducts which causes 400V voltage spikes over the tube. These spikes are then reduced to 5V spikes with voltage dividers and it's 400V DC component is filtered using a capacitor. The output is than measured and recorded using an oscilloscope at 20kHz sampling rate for 8 minutes.

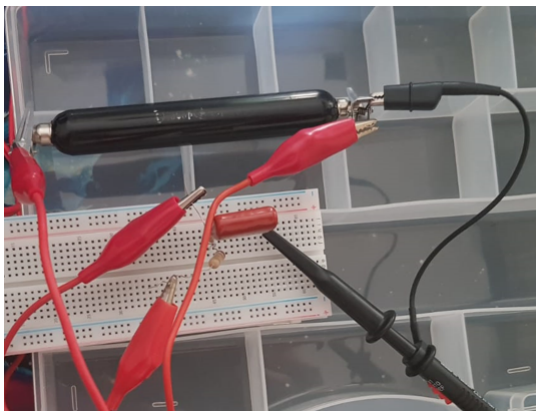

Figure 3. Geiger-Müller tube and aforementioned voltage divider-capacitor circuit

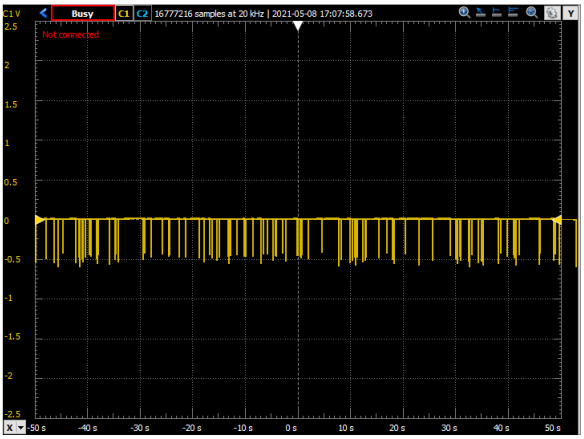

Figure 4. Part of the data acquisition

After the data is exported, a simple Matlab code is used to detect the spikes and get the time interval between each two consecutive detection.

```
spikes = diff(S<-0.1)>0.5;
detection_times = t(spikes);
random_intervals = diff(detection_times);
```

First line turns spikes into pulses by categorizing whether the signal is below -0.1 or not. Then it calculates differences between adjacent elements which makes rising edges 1 and falling edges -1 and the rest zero. Then we take the rising edges only by checking if it is greater than 0.5. After finding the spikes, their times are saved to a variable called "detection_times". Then the difference between each consequent detection is calculated in the third line.

$$f(x;\lambda) = \begin{cases} \lambda e^{-\lambda x} & \text{for } x \geq 0 \\ 0 & \text{for } x < 0 \end{cases}$$

We shown in theory part that the output has to be distributed according to exponential distribution function given above. It is not possible to directly fit the probability distribution to the data however, we can easily calculate the cumulative probability distribution of the data then fit the CDF of the exponential distribution on the data.

$$F(x;\lambda) = \begin{cases} 1 - e^{-\lambda x} & \text{for } x \geq 0 \\ 0 & \text{for } x < 0 \end{cases}$$

The cumulative probability function of this data is generated as seen in the figure below. Then exponential distribution CDF that is given above is fitted to the data. As can be seen in the figure below, it fitted the data perfectly. The result had a $\lambda = 1.1412$.

Now that we know the λ, we can graph its probability distribution.

Since we now know the probability distribution of the random variable, for any given time interval t between emissions, it is possible to calculate the $P(X \leq t)$ and

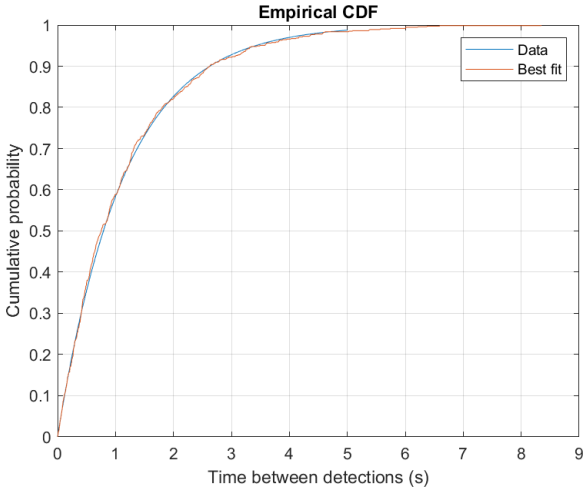

Figure 5. Cumulative distribution function from data and fitted exponential distribution.

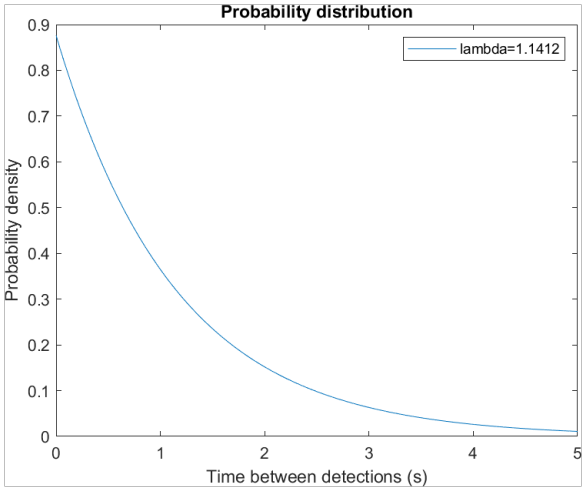

Figure 6. Probability distribution function from fitted exponential distribution.

plug it into the inverse normal distribution. This effectively converts our exponential random variable X to a normal distribution with zero mean and unit variance.

```
rnd=norminv(expcdf(random_intervals, lambda));
```

Finally, the Chi square test is applied to the generated random numbers to test their randomness.

```
[h,p,stats] = chi2gof(rnd)
```

This gave $h = 0, p = 0.9877$, which means it passes the chi square test and is indeed random[8].

Some of the random numbers are: -2.24414226, 0.44187537, 0.03095986, 2.08994029, -0.10723249... And as seen, they are continuous random numbers. We can confirm that the distribution of the random numbers are indeed a uniform Gaussian distribution.

The 8 minutes of runtime gave 716 random numbers. This is very low compared to the throughput of a PRNG. However there are many methods to make this process

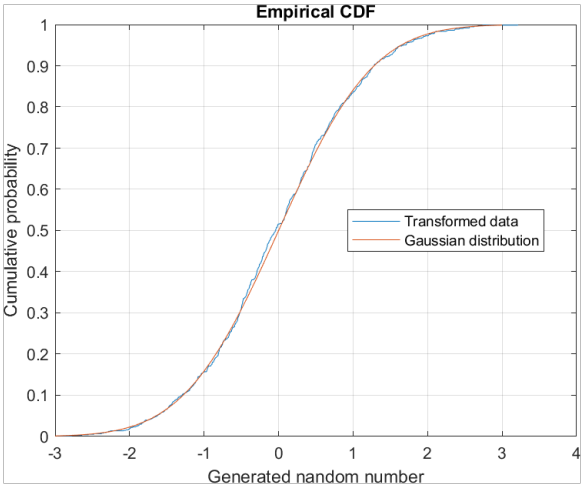

Figure 7. Cumulative distribution of the random numbers compared with zero mean unit variance normal distribution.

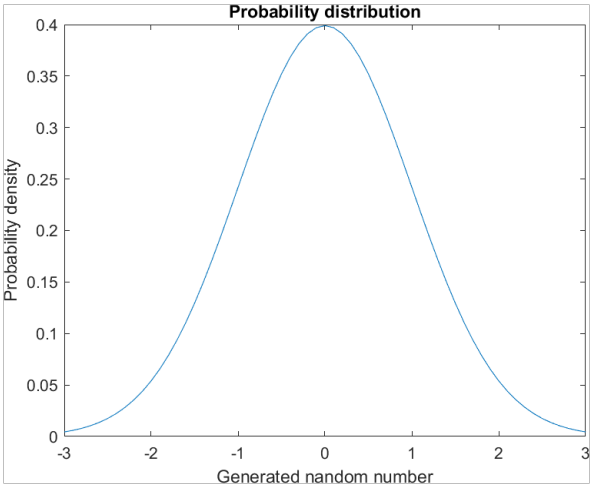

Figure 8. Probability distribution of the random numbers

faster and get more random numbers easily[9]. This suggests that one day this kind of device may be integrated into the computers and used to generate the random numbers.

IV. APPLICATION

A total of 1400 normally distributed random numbers are generated using the method described above. An application of these numbers will be explained in this section. This application consists of creating randomly generated faces from these true random numbers. The face generation process is as the following. First principle component analysis(PCA) will be applied over a dataset consisting of many different faces. This process gives us the main components that composes a face, which are called "eigenfaces". All the faces in the dataset can be constructed from these eigenfaces with their corresponding coefficient vectors[10]

When the distribution of the elements of those coefficient vectors across different faces are calculated, it is seen that they vary with a uniform normal distribution just like our random values. This suggests that we can take a subset from our random values and use them to reconstruct the image using the eigenfaces.

Figure 9. Randomly generated faces from the true random numbers

V. CONCLUSION

In this project, the goal was to generate truly random numbers that cannot be predicted in any condition. In order to create a device that is capable of outputting true randomness, first a source that can output true randomness had to be chosen. The classical physics present no such attribute since although there are many process that seem random, classical physics processes are deterministic. This is not the case with the quantum physics as probability waves and Schrödinger's equation suggest. This equation enables a phenomenon that is called quantum tunneling that enables particles with not enough energy to pass energy barriers. It is possible to make use of this in order to construct a true random number generator. In this project, we used a Geiger-Müller tube to measure when those tunneling occurs and make use of the random time intervals between two events to create a normally distributed random number by making use of inverse transform sampling. After generating the random numbers, those random numbers are used to randomly create faces using a concept called eigenfaces. As a result, the desired device was indeed created and truly random numbers were created using the process that is explained in this report.

[1] M. Bellare, S. Goldwasser, and D. Micciancio, "pseudo-random" number generation within cryptographic algorithms: The dds case, in *Annual International Cryptology Conference* (Springer, 1997) pp. 277–291.

[2] V. Bagini and M. Bucci, A design of reliable true random number generator for cryptographic applications, in *International Workshop on Cryptographic Hardware and Embedded Systems* (Springer, 1999) pp. 204–218.

[3] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, Optical quantum random number generator, Journal of Modern Optics **47**, 595 (2000).

[4] S. Tisa, F. Villa, A. Giudice, G. Simmerle, and F. Zappa, High-speed quantum random number generation using cmos photon counting detectors, IEEE Journal of Selected Topics in Quantum Electronics **21**, 23 (2014).

[5] P. V. Vezeteu, I. I. Popescu, and D. I. Nastac, The generation of random numbers using the quantum tunnel effect in transistors, in *2019 IEEE 25th International Symposium for Design and Technology in Electronic Packaging (SIITME)* (2019) pp. 379–382.

[6] M. Herrero-Collantes and J. C. Garcia-Escartin, Quantum random number generators, Reviews of Modern Physics **89**, 015004 (2017).

[7] C. Samanta, P. R. Chowdhury, and D. Basu, Predictions of alpha decay half lives of heavy and superheavy elements, Nuclear Physics A **789**, 142 (2007).

[8] M. L. McHugh, The chi-square test of independence, Biochemia medica **23**, 143 (2013).

[9] D. Stucki, S. Burri, E. Charbon, C. Chunnilall, A. Meneghetti, and F. Regazzoni, Towards a high-speed quantum random number generator, in *Emerging Technologies in Security and Defence; and Quantum Security II; and Unmanned Sensor Systems X*, Vol. 8899 (International Society for Optics and Photonics, 2013) p. 88990R.

[10] P. J. Hancock, Evolving faces from principal components, Behavior Research Methods, Instruments, & Computers **32**, 327 (2000).