Quantum Random Number Generators

Jacob Kaufman
(Dated: March 2021)

This report covers the theory behind quantum random number generators, the different types of generators, and the benefits of each type. It also reviews the theory behind non-locality and describes some of the applications of quantum random number generators.

I. INTRODUCTION

Random number generators have many uses such as simulations, statistical sampling, and cryptography, and a genuine random number generator can only be built using the probabilistic nature of quantum mechanics[1]. Because many quantum properties are only probabilities before measurement, those properties can be used to create randomized data that is non-reproducible and unpredictable.

Quantum random number generators (QRNG) are a relatively new field because they defy the classical theories of physics centered around locality. In the past century, physicists have assembled evidence that quantum phenomena can create events non-locally, and QRNGs rely on this principle to generate truly random numbers. Born’s rule tells us that the measurement of a quantum state can be intrinsically random. This means that natural quantum systems create quantum pieces of information, or qubits, when there exists physical superpositions. These qubits can be measured and eventually converted to classical bits, so the main challenge for engineers of QRNGs is to prevent classical properties from interfering with the random quantum processes. Because of the high demand around the abundant applications of random number generators, physicists are consistently improving the quality, speed, or availability of QRNGs.

II. BACKGROUND KNOWLEDGE

A. Bell’s Inequality

The Einstein-Podolsky-Rosen paradox is an argument against quantum mechanics as a complete theory. The thought experiment was that if two entangled particles were very far apart, and one of the particles collapsed, or was measured, the other would collapse instantaneously. In the 1930s Einstein, Podolsky, and Rosen argued that because one particle’s influence cannot travel faster than the speed of light, each particle must contain determined values, or hidden variables, from before they were separated[2].

John Stewart Bell showed that in order for locality to be preserved, the Bell inequality must be true. If there is experimental evidence that supports quantum theory, the inequality will not hold and the answer to the EPR paradox will be nonlocality. Experiments tried “Bell tests” to show that the inequality is not true for quantum systems, but often had to make additional assumptions about detection efficiency or unrelated measurements among others to get the desired result. These assumptions are known as loopholes, and while physicists may not be able to close every loophole, in 2015 an experiment supported nonlocality with 96 percent confidence[3].

B. Stern-Gerlach Experiment

One very simple QRNG is a version the Stern-Gerlach experiment. The experiment sends particles, originally silver atoms, through a magnetic field. The classically expected result is a continuous distribution of paths. Because of each atom’s quantized spin, it is either deflected up or down, giving two discrete points of accumulation[4].

![FIG. 1. The Stern-Gerlach experiment with cesium atoms.](image)

We can use this experiment to generate random numbers by assigning a measurement to each accumulation point. Then we can fire the molecules individually and designate each measurement value to a 0 or 1. Each value is theoretically independent of any physical input.

III. SELF-TESTING QRNG

The true randomness of QRNGs can be tested using Bell tests. We can create a really simple optical random number generator and test it with a Bell inequality to make sure it is more random than classical RNGs. Using the polarization properties of light, we can use a polarized 50/50 beam splitter which is truly random[5]. We can designate classical information values to the measurement devices for the individual photons which reflect off of the beam splitter and the photons which transmit through the beam splitter shown in Figure 2.

The Clauser–Horne–Shimony–Holt (CHSH) inequality is a Bell inequality corresponding to optical tests, and is defined as a series of expectation values
FIG. 2. A simple diagram of a Quantum Random Number Generator built with a polarized beam splitter. Each measurement device is a single photon detector (SPD).

\[ S = \sum_{v,h,v',h'} (-1)^{v' + h' + vh} p(v, h|v', h') \leq S_c = 2 \]

where \( S_c \) is the classical bound. This equation can be decomposed into individual expectation values corresponding to the possible measurements when there are two inputs:

\[ S = |E(v, h) + E(v, h') + E(v', h) - E(v', h')| \leq 2 \]

For a 100 percent efficient quantum beam splitter QRNG, this would result in \( S = 2\sqrt{2} \) which violates the CHSH inequality. We know that because the classical Bell inequality is violated that it must produce truly random numbers[1].

However, it is impossible to experimentally measure coincidences from the beam splitter with 100 percent efficiency, and we need to change the CHSH inequality to include an efficiency factor. The new inequality which covers the detection efficiency loophole is

\[ |E(v, h|c) + E(v, h'|c) + E(v', h|c) - E(v', h'|c)| \leq \frac{4}{\eta} - 2 \]

where \( \eta \) is the efficiency and \( c \) represents the coincidence.

It is clear in this optical case that as soon as the efficiency is lower than around 83 percent, or \( 2/(\sqrt{2} + 1) \), the inequality is not violated. It is very difficult to violate a Bell inequality without loopholes, but it has been done in 2015. Physicists separated entangled electrons by 1.3 km and measured their spins[6].

Other self-testing (or device-independent) QRNGs use different measures of randomness. For example, sophisticated exponential randomness expansion protocols based on the CHSH inequality quadratically expand an input seed of the form \( O(\sqrt{n} \log_2 \sqrt{n}) \). No matter which randomness measure is used, it is important that the loopholes in the experiment are always identified and quantified.

IV. PRACTICAL QRNGS

A. Single Photon Detectors

While self-testing QRNGs are very accurate, they can also be extremely inefficient. More practical QRNGs are not as purely random, but they can generate random numbers at a much faster rate and a relatively low cost. In order to do this practical QRNGs often are designed so that its output randomness does not depend on physical implementations. Practical QRNGs always are influenced by some sort of classical noise, but much of this noise can be subtracted away from the quantum randomness. The isolation of truly random information can be optimized, and there are many ways in which the engineers of more practical QRNGs can try to improve the rates of their generators.

An interesting way to increase the rates of QRNGs is to measure in high dimensional quantum space. If a QRNG measures the time between photons arriving at the single photon detector, it is called a temporal QRNG. These generators can measure the outputs of continuous-wave lasers and record the times of separate detections as shown in Figure 3. This means that the limitation of the rate of generation is the time between measurements of the detector. Temporal QRNGs can generate around \( \log_2(T/\delta t) \) bits of random numbers where \( \delta t \) is the time resolution of the measurement device.

Similarly, spatial QRNGs send photons through \( 1 \times N \)-dimensional beam splitters. An array of detectors can make these measurements, and Figure 4 shows the two-dimensional version of spatial QRNGs. This type of detector can be more expensive than temporal QRNGs because of the number of detectors and less effective because of interference between multiple detectors. Other QRNGs which use single photon detectors measure multiple photon number states like Fock states. This can create random numbers in Poisson or Gaussian distributions which are useful for applications where a random, but realistic sample is needed.

B. Macroscopic Photodetectors

While single photon detectors work great for simple QRNGs, the most efficient generators use macroscopic
FIG. 4. Temporal and Spatial QRNGs allow for higher rates of number generation by working in more than one dimension.

photodetectors. One crucial addition to QNRGs is the quantum vacuum state. The vacuum state in quantum mechanics is not empty space. Instead it describes lowest possible energy state, and often is described as having the same properties as the ground state of a harmonic oscillator. The amplitude and phase of a vacuum state are non-commuting operators, and their commutator relationship is

$$[P, A] = \frac{i}{2}$$

with phase operator $P$ and amplitude $A$. This means they have a superposition in phase space that is $1/4$ units wide, and together form Gaussian distributed random numbers in that phase space. Another use of the quantum vacuum space is based on vacuum noise measurements. The experiment in Figure 5 uses a vacuum mode once to offset the unknown light source before generating randomness by inputting an additional vacuum mode with the unknown light. This original certification process allows for a model of the unknown light to remove any physical predictability[7].

FIG. 5. Temporal and Spatial QRNGs allow for higher rates of number generation by working in more than one dimension.

In a study posted last year, a group of researchers used the noise from spontaneous emission to create non-reproducible random numbers. This quantum process allowed them to create and QRNG from the interference of many lasers in a cavity. By using broad-area semiconductor lasers, they were able to remove spatio-temporal correlations and have a much more random generator. Additionally, the cavity has many photodetectors which allow a total bit rate greater than 100 Tb/s. This bit rate is claimed to be two orders of magnitude larger than the next fastest random bit generator. Figure 6 shows the laser cavity and photodetectors, and Figure 7 shows how the shape of the cavity eliminates the spatio-temporal correlation[8].

FIG. 6. The “ultrafast” random bit generator apparatus creates random bits at over 100 Terabytes per second using multiple parallel photodetectors.

FIG. 7. The specific shape of the laser cavity in the chip-scale QRNG reduces the correlation in the space and time superposition.

V. APPLICATIONS OF QRNGS

Random number generators are extremely important for making sure the lottery is completely random, but there are some more meaningful uses in science and infrastructure as well. One important use of QRNGs is
statistical sampling. Physicists and other scientists often use a random set of numbers to create a large sample and lower their statistical uncertainty. One of the most useful processes is the Monte Carlo simulation which can help explain uncertainties, calculate risks in simulations, or optimize processes. The Monte Carlo simulation is based on a large quantity of random numbers, and in order to be most effective, the numbers have to be as random as possible. With the introduction of low-cost, high-rate QRNGs, scientists can more precisely use the Monte Carlo simulation without the numbers will looking predictable or reproducible at high quantities.

The fastest growing use of random numbers is cryptography. While cryptographers continue to improve their codes to better protect information, the information will always be able to be decoded with enough computing power. Quantum random numbers, however, theoretically cannot be solved. This means that computers trying to discover encrypted data will have to try every combination without knowing which is correct. This comes from the same theory as the thought experiments with Alice and Bob. Both of them measure a state, but if Eve intercepts the state, it collapses. Because the detectors in each of the QRNGs are measuring states as they collapse them, the resulting values are completely random. Cryptographers are mainly challenged by efficiently producing these random numbers[1].

Despite the strides made to speed up generation rates, it still requires a lot of energy to create reliably random numbers. However, as industries around cryptocurrencies and NFTs grow, the demand for random numbers will require quantum random number generators.