Quantum random number generator a definitive guide

Allan Wandia

Abstract

A quantum random number generator (QRNG) is a device that generates random numbers using quantum phenomena. Quantum phenomena are inherently random, so QRNGs can produce truly random numbers that are impossible to predict. This makes them ideal for use in applications where security is critical, such as cryptography and gambling, and also in computational methods such as Monte Carlo simulations and programming, over the large field of cryptography for generating crypto code-masking messages, as well as in commercial applications like lottery games and slot machines. Recently, the range of applications requiring random numbers has been extended with the development of quantum cryptography and quantum information processing (1). There are a number of different types of QRNGs, but they all work by exploiting some aspect of quantum mechanics. For example, one type of QRNG uses the random decay of radioactive atoms to generate random numbers. Another type uses the interference of light waves to create random patterns. QRNGs are still in their early stages of development, but they have the potential to revolutionize the way we generate random numbers.

But how does a quantum random number generator actually work?

Methods used to simulate randomness in quantum systems

These papers describe different methods for generating random numbers using quantum mechanics. (1) describes a quantum random number generator based on splitting a beam of photons on a beam splitter and detecting the resulting photons. (2) reports on a random number generator that uses the intrinsic randomness of photonic emission in semiconductors and subsequent detection by the photoelectric effect. (3) proposes a quantum random number generator that uses an entangled photon pair in a Bell singlet state and is certified explicitly by value indefiniteness. All of these methods rely on the intrinsic randomness of quantum mechanical processes to generate random numbers.

Photon beam splitting

The principle of operation of the random generator is shown in *Figure 1*. For the case of the 50 : 50 beam splitter (BS) (Figure 1(a)), each individual photon coming from the light source and traveling through the beam splitter has, for itself, equal probability of being found in either output of the beam splitter. If a polarizing beam splitter (PBS) is used (Figure 1(b)), then each individual photon polarized at 45◦ has equal probability of being found in the H (horizontal) polarization or V (vertical) polarization output of the polarizer. Anyhow, quantum theory predicts for both cases that the individual “decisions” are truly random and independent of each other. In our devices, this feature is implemented by detecting the photons in the two output beams with

single photon detectors and combining the detection pulse with a toggle switch (S), which has two states, 0 and 1. If detector D1 fires, then the switch is flipped to state 0 and left in this state until a detection event in detector D2 occurs, leaving the switch in state 1 until an event in detector D1 happens, and S is set to state 0. (Figure 1(c)). In the case that several detections occur in a row in the same detector, then only the first detection will toggle the switch S into the corresponding state, and the following detections leave the switch unaltered. Consequently, the toggling of the switch between its two states constitutes a binary random signal,, with the randomness lying in the times of the transitions between the two states. In order to avoid any effects of the photon statistic of the source or optical interference on the behavior of the generator, the light source should be set to produce $\ll$ 1 photon per coherence time. (1)

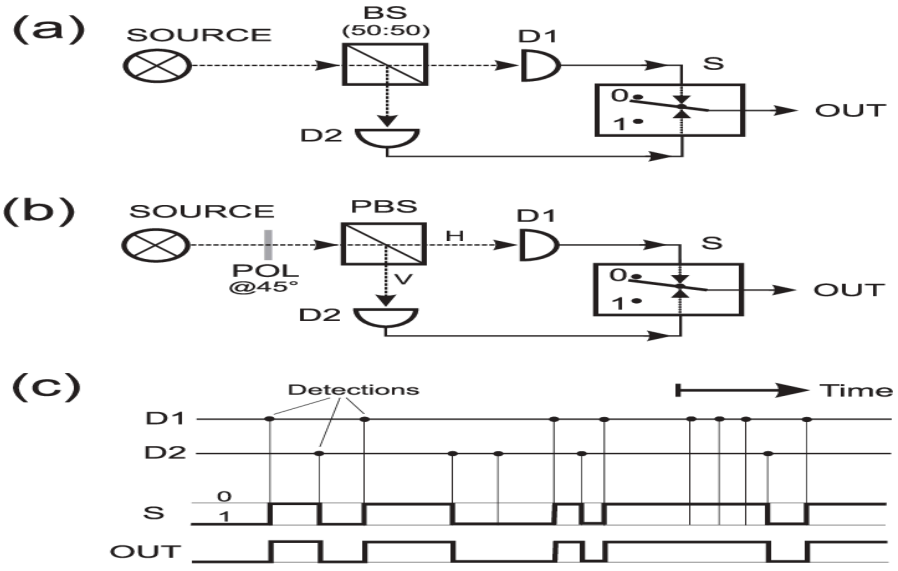
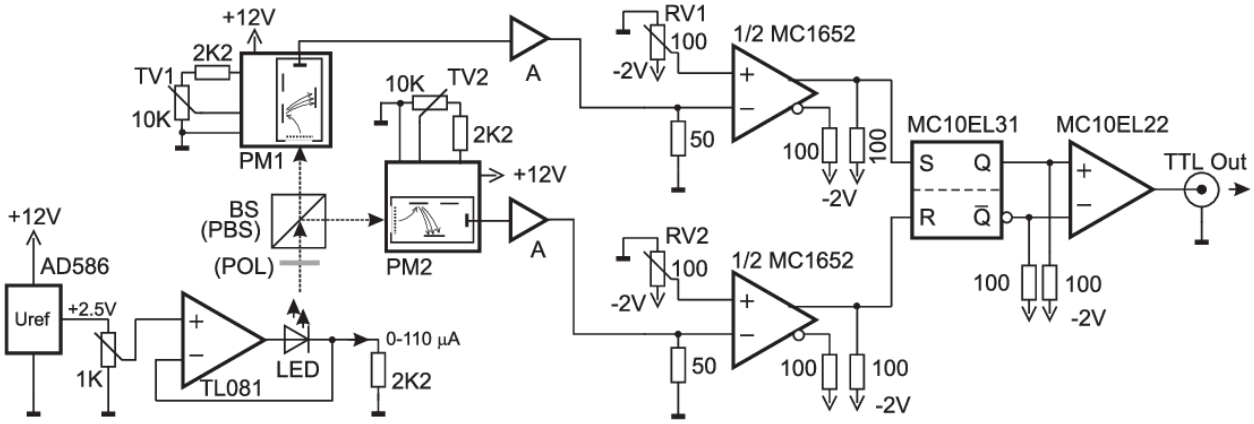


Figure 2 shows the circuit diagram of the physical quantum random generator. The light source is a red light-emitting diode (LED) driven by an adjustable current source (AD586 and TL081) with a maximum current of 110 μA. Due to the very short coherence length of this kind of source (< 1 ps), it can be ascertained that most of the time there are no photons present within the coherence time of the source, thus eliminating the effects of source photon statistics or optical interference. The light emerging from the LED is guided through a piece of pipe to the beam splitter, which can be either a 50:50 beam splitter or a polarizing beam splitter. In the latter case, the photons are polarized beforehand with polarization foil (POL) at 45◦ with respect to the axis of the dual channel polarization analyzer (PBS). The photons in the two output beams are detected with fast photo multipliers 16 (PM1, PM2). The PMs are enclosed modules that contain all necessary electronics as well as a generator for the tube voltage, and thus only require a +12 V supply. The tube voltages can be adjusted with potentiometers (TV1, TV2) for optimal detection of pulse rates and pulse amplitudes. The output signals are amplified in two Becker Hickl amplifier modules (A) and transmitted to the signal electronics, which are realized in emitter-coupled logic (ECL). The detector pulses are converted into ECL signals by two comparators (MC1652) in reference to adjustable threshold voltages set by potentiometers (RV1, RV2). The actual synthesis of the random signal is done within a RS-flip-flop (MC10EL31), as PM1 triggers the S-input and PM2 triggers the R-input of the flip-flop. The output of this flip-flop toggles between the high and low states depending on whether the last detection occurred in PM1 or PM2. Finally, the random signal is converted from ECL to TTL logic levels (MC10EL22) for further usage. In order to generate random numbers on a personal computer, the signal from the random generator is sampled periodically and accumulated in a 32-bit wide

shift register (Figure 3). Every 32 clock cycle, the contents of the shift register are transferred in parallel to a personal computer via a fast digital I/O board. In this way, a continuous stream of random numbers is transferred to a personal computer. (1)



Up to now, no general definition of randomness exists, and discussions still go on. Two reasonable and widely accepted conditions for the randomness of any binary sequence is its being “chaotic” a"typical”. The first of these concepts was introduced by Kolmogorov and deals with the algorithmic complexity of the sequence, while the second originates from Martin-Lov and says that no particular random sequence must have any features that make it distinguishable from all random sequences . With pseudorandom generators, it is always possible to predict all of their properties with more or less mathematical effort, due to knowing their algorithm. Thus one may easily reject their randomness 5 from a rigorous point of view. In contrast, the most desired feature of a true random generator, its “truth”, bears the principal impossibility of ever describing such a generator completely and proving its randomness beyond any doubt. This could only be done by recording its random sequence for an infinite time. One is obviously limited experimentally to finite samples taken out of the infinite random sequence. There are lots of empirical tests, mostly developed in connection with certain Monte Carlo simulation problems,

for testing the randomness of such finite samples. The more tests one sample passes, the higher we estimate its randomness. We estimate a test for randomness the better, the smaller or more hidden the regularities may be that it can detect . As the range of tests for the randomness of a sequence is almost unlimited we must find tests which can serve as an appropriate measure of randomness according to the specific requirements of our application. Since the experiment that our random generators are designed for demands random signals at a high rate, we focus on the time the random generators take to establish a random state of its signal starting from a point in time where the output state and the internal state of the generator may be known. We will briefly describe the relatively intuitive tests that will be applied to data samples taken from the random generator, which we consider to be sufficient in qualifying the device for its use in the experiment.. Autocorrelation Time of the Signal: For a binary sequence as produced by our random generator the autocorrelation function exhibits an exponential decay of the form: $A() = A0e - 2R||$, where R is the average toggle rate of the signal, A0 is the normalization constant and τ is the delay time. Per definition the autocorrelation time is given by $ac = 12R$. 6 The autocorrelation function is a measure for the average correlation between the signal at a time t and later time $t + \tau$. 2. Internal Delay within the Device: The internal delay time within the device between the emission of a photon and its effect on the output signal. This internal delay time is the minimal time the generator needs to establish a truly random state of its output. . Equidistribution of the Signal: This is the most obvious and simple test of randomness of our device, as for a random generator the occurrence of each event must be equally probable. Yet, by itself the equidistribution is not a criterion for the randomness of a sequence. . Distribution of Time Intervals between Events: The transitions of the signal generated by our system are

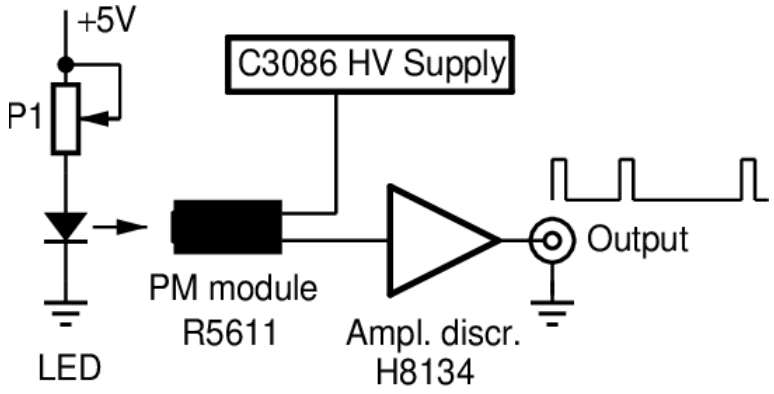
independent of any preceding events and signals within the device. For such a Poissonian process the time intervals between successive events are distributed exponentially in the following way: $p(T) = p0e - T/T0$, where p(T) is the probability of a time interval T between two events, $T0 = 1/R$ is the mean time interval and is the reciprocal value of the average toggle rate *R* defined earlier and $p0$ is the normalization constant. The evaluation of $p(T)$ A data sample taken from our generator shows directly for which time intervals the independence between events is ascertained and for which time intervals the signal is dominated by bandwidth limits or other deficiencies within the system. Further Illustrative Tests of Randomness: These statistical tests will be applied to samples of random numbers produced by the random generator in order to illustrate the functionality of the device. For the application our random generators are designed for, these statistical measures are not as important as the tests described above, and the tests proposed here represent just a tiny selection of possible tests. Yet, these tests allow a cautious comparison of random numbers produced with our device with random numbers taken from other sources. The code for the evaluation of these tests was developed in 11 . (a) Equidistribution and Entropy of n–Bit Blocks: Provided that the sample data set is sufficiently long, all possible n–bit blocks (where n is the length of the block) should appear with equal probability within the data set. A direct, but insufficient, way of determining the equidistribution of a data set is to evaluate the mean value of all n–bit blocks, which should be $(2n - 1)/2$. This will give the same result for any symmetric distribution. The distribution of n–bit blocks of a data set corresponds to the entropy, a value which is often used in the context of random number analysis. The entropy is defined as: $Hn = -Xnpilog2pi$ and is expressed in

units of bits. pi is the empirically determined probability for finding the i–th block. For a set of random numbers a block of the length n should produce n bits of entropy. In the case of bytes, which are blocks of 8 bits, the entropy of these blocks should be 8 bits. Blocks of n Zeros or Ones: Another test for the randomness of a set of bits is the counting of blocks of consecutive zeros or ones. Each bit is equally likely a zero as a one, therefore the probability of finding blocks of n concatenated zeros or ones should be proportional to a 2^{-n} function. (c) Monte-Carlo estimation of π: A pretty way of demonstrating the quality of a set of random numbers produced by a random generator is a simple Monte Carlo estimation of π. The idea is to map the numbers onto points on a square with a quarter circle fitted into the square and count the points which lay within the quarter circle. The ratio of the number of points lying in the circle and the total 8 number of points is an estimation of π.

Practical realization of the random pulse generator

The random pulse generator is made of a photon source followed by a single photon detector. As a source of photons we have used a standard low-efficiency red light emitting diode (LED). LE diodes are direct bandgap devices which produce incoherent light by spontaneous emission which is essentially a random process. If operated at sufficiently low power, LED emits photons which are virtually independent of each other, that is the photon emission is then a Poissonian process . The important parameter here is the coherence time τcohr, a time scale at which photons are becoming to be correlated. The coherence time can be estimated by help of the Heisenberg uncertainty relation, assuming Gaussian emission spectrum pulse shaping circuits, whose dead time can be set at a desired length, are well known in the art, see for example .In our

experiments we have used Hamamatsu photomultiplier with bialkali photocathode R5611, high voltage source C3830, and the photon counting unit C3866 (amplifier + discriminator + pulse shaper). Dead time of this photon counting system is about 25 ns, very stable and independent of brightness of the LED. The low quantum efficiency of only about 0.05 percent of the bialkali photocathode at the wavelength of the LED presents no problem in our application. We have intentionally used low efficiency red LEDs because its widest wavelength spectrum in comparison to other LEDs indicates the highest randomness of emitted photons. (2)



entangled photon pair in a Bell singlet state

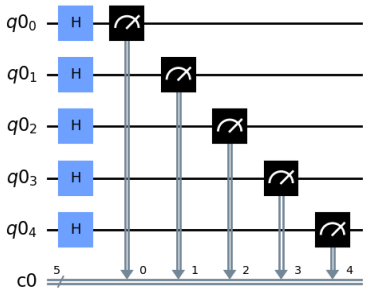
In what follows, a proposal for a QRNG depicted in Fig. 1, previously put forward in Ref. , will be discussed in detail. It utilizes the singlet state of two two-state particles (e.g., photons of linear polarization) proportional to |H1V2i − |V1H2i, which is form invariant in all measurement directions. A single photon light source (presumably an LED) is attenuated so more than one photon is rarely in the beam path at the same time. These photons impinge on a source of singlet states of photons (presumably by spontaneous parametric down-conversion in a nonlinear medium). The two resulting entangled photons are then analyzed with respect to their linear polarization state at some directions which are $\pi/4$ radians “apart,” symbolized by “$\oplus$” and “$\otimes$,”

respectively. Due to the required four-dimensional Hilbert space, this QRNG is “protected” by Bell- as well as Kochen-Specker- and Greenberger-Horne-Zeilinger-type value indefiniteness . The protocol utilizes all three principal types of quantum indeterminism: (i) the indeterminacy of individual outcomes of single events as proposed by Born and Dirac; (ii) quantum complementarity (due to the use of conjugate variables), as put forward by Heisenberg, Pauli and Bohr; and (iii) value indefiniteness due to Bell, Kochen & Specker, and Greenberger, Horne & Zeilinger. This, essentially, is the same experimental configuration as the one used for a measurement of the correlation function at the angle of $\pi/4$ radians (45°). Whereas the correlation function averages over “a large number” of single contributions, a random sequence can be obtained by concatenating these single pairs of outcomes via addition modulo 2. Formally, suppose that for the ith experimental run, the two outcomes are $O \oplus i \in \{0,1\}$ corresponding to $D \oplus 0$ or $D \oplus 1$, and $O \otimes i \in \{0,1\}$ corresponding to $D \otimes 0$ or $D \otimes 1$. These two outcomes $O \oplus i$ and $O \otimes i$, which themselves form two sequences of random bits, are subsequently combined by the XOR operation, which amounts to their parity, or to the addition modulo 2 according to Table II (in what follows, depending on the formal context, XOR refers to either a binary function of two binary observables, or to the logical operation). Stated differently, one outcome is used as a one time pad to “encrypt” the other outcome, and vice versa. As a result, one obtains a sequence $x = x1x2 \ldots xn$ with $xi = O \oplus i + O \otimes i \bmod 2$. For the XORd sequence to still be certifiably incomputable (via value indefiniteness), one must prove this certification is preserved under XORing—indeed strong incomputability itself is not necessarily preserved. By necessity any QRNG certified by value indefiniteness must operate nontrivially in a Hilbert space of dimension $n \geq 3$. To transform the n-ary (incomputable) sequence into a binary

one, a function f : {0,1,...,n−1} → {0,1,λ} must be used (λ is the empty string); 7 O ⊕ i O ⊗ i O ⊕ i XOR O ⊗ i 0 0 0 0 1 1 1 0 1 1 1 0 . The logical exclusive or operation. to claim certification, the strong incomputability of the bits must still be guaranteed after the application of f . This is a fundamental issue which has to be checked for existing QRNGs such as that in Ref. ; without it one cannot claim to produce truly indeterministic bits. In general incomputability itself is not preserved by f ; however by consideration of the value indefiniteness of the source the certification can be seen to hold under XOR as well as when discarding bits . (3)

My Solution to the QRNG using qiskit

At their core, quantum random number generators set up a superposition on one or more qubits using the Hadamard gate. This gate moves qubits from the 0 state to an equal superposition of the 0 and 1 state, meaning that you're equally likely to measure a qubit value of 0 or 1 at the end of the quantum circuit. If you treat a string of qubits as a binary value (1111 = 15, for example), then applying a Hadamard gate to every qubit and then making a measurement will generate a random bitstring, and therefore a random number. (Allan, n.d.)



Challenges and limitations

One limitation is that they can be affected by noise. This can be caused by environmental factors, such as temperature fluctuations or electromagnetic radiation. Another limitation is that they can be expensive to build and maintain.One limitation of these systems is that they can be affected by noise. This can be caused by environmental factors, such as temperature fluctuations or electromagnetic radiation. For example, if the temperature of the system changes too much, it can cause the system to malfunction. Additionally, if there is too much electromagnetic radiation in the area, it can also cause the system to malfunction. Another limitation of these systems is that they can be expensive to build and maintain. This is because they require a lot of specialized equipment and expertise to build and maintain. Additionally, the components of these systems can be expensive, which can add to the overall cost of the system.also the limitations of pure randomness in this part were gonna get more philosophical there is Ramsey theory is a branch of mathematics that concerns the appearance of order in a substructure given a structure of a known size. It is named after the British mathematician and philosopher Frank P. Ramsey. The theory suggests that pure randomness is impossible, especially for large structures. Mathematician Theodore Motzkin suggested that "while disorder is more probable in general, complete disorder is impossible"According to Ramsey theory, pure randomness is impossible, especially for large structures. Mathematician Theodore Motzkin suggested that "while disorder is more probable in general, complete disorder is impossible". Assuming a deterministic universe, an effect must occur with a cause, making true randomness impossible. However, in quantum theory, randomness is possible. Physicists suggest that what we normally call “random” is not truly

random, but only appears so. The randomness is a reflection of our ignorance about the thing being observed, rather than something inherent to it.

Conclusion

In conclusion, randomness is a complex and fascinating topic. While it is often thought of as something that is simply unpredictable, there is much more to it than that. Randomness is essential for many aspects of our lives, from the security of our online transactions to the creation of new art and music. While there are still many challenges to overcome, our efforts to create pure randomness for research purposes are making great progress. I am excited to see what the future holds for this field of research.

Bibliography

1. Jennewein T, Achleitner U, Weihs G, Weinfurter H, Zeilinger A. A fast and compact quantum random number generator. Rev Sci Instrum. 2000 Apr 1;71(4):1675–80.
2. Stipcević M, Rogina BM. Quantum random number generator based on photonic emission in semiconductors. Rev Sci Instrum. 2007 Apr;78(4):045104.
3. Abbott AA, Claude CS, Svozil K. A quantum random number generator certified by value indefiniteness. Math Struct Comp Sci. 2014 June;24(3).
4. Allan. (n.d.). Quantum random number generator using qiskit https://github.com/DarkStarStrix/Quantum_Random_Number_Generator