Self Correcting Quantum Random Number Generators using Tapered Amplifiers

R. C. Pooser, P. G. Evans, T. S. Humble, W. P. Grice, B. P. Williams
Computational Sciences Directorate, Oak Ridge National Laboratory, Oak Ridge, TN 37831, USA
pooserrc@ornl.gov

Abstract: We present a new implementation of a quantum random number generator that consists of tapered amplifier optical semiconductor devices and an array of random number registration techniques, including quantum feedback/forward control for removing bias.

OCIS codes: (000.0000) General; (000.0000) General [8- pt. type. For codes, see www.opticsinfobase.org/submit/ocis.]

1. Introduction

Random numbers are critical to a diverse array of applications from encryption to electronic gambling machines. Bias (the propensity for some members of a distribution to occur more frequently than others), leads to predictability, which compromises the usefulness or security of a system based on random numbers [1]. Further, all pseudorandom number generators (PRNG) are by definition deterministic. This means that with enough characterization either via the number distribution or by directly examining the algorithm, the PRNG can become predictable. One way to characterize the security of a PRNG is by measuring its period (or its autocorrelation which is related to the period).

On the other hand, QRNGs are intrinsically nonperiodic and nondeterministic. If the measurement outcomes occur with equal probability (zero bias), then, the quantum system maximizes entropy across its distribution, or more formally, the bits of entropy per bit approaches unity. Even in QRNGs, however, sources of bias exist as the quantum states are converted to classical numbers. We have developed a quantum mechanical method for detecting and removing bias in quantum systems in order to restore the quantum superposition to its original unpredictable set of all possible outcomes. The method uses weak measurements (WM) to study the quantum statistics of the state and look for bias in the distribution, which is then used to feedback control on the state source or forward control on the measurement basis.

Our implementation uses a new QRNG based on tapered amplifiers (TA) in order to examine the performance of various random number registration methods. In one implementation the waiting time distribution can be sampled and used as a source of random numbers. In another implementation, the output of the TA can be split on a beamsplitter and either attenuated to single photons per unit time or left as a macroscopic quantity. In one case the source of randomness is derived from the quantum optics of the beamsplitter (which has a binomial distribution), and a photon detected on either output corresponds to a random bit. In the other case, the TA output is used as a local oscillator for homodyne detection of the quantum vacuum fluctuations on the other port of the beamsplitter which are sampled as random numbers [2]. Below we present these implementations with a focus on the self-correcting QRNG (SCQRNG).

2. Waiting Time Distribution

The TA-based QRNG can operate using the arrival time method [3], as the electron hole pairs within the diode have a lifetime that leads to a random emission time. The schematic in Fig. 1(a) shows the arrangement for a QRNG based on the waiting time distribution experimentally obtained in Fig. 1(b). Figure 1(c) shows a histogram of the distribution of bits between 0 and 1 after thresholding the arrival time of each incoming photon.

The source shows 0.90 bits of entropy per bit before hashing or filtering the data, and passes most of the NIST randomness tests (2 significant failures). By choosing appropriate binning or by hashing the data, the entropy per bit approaches 0.99, and the randomness tests show the requisite binomial distribution of failures per trial.

Figure 1: (a) Schematic of TA-based QRNG based on waiting time (b) waiting time distribution and (c) thresholded histogram.
3. Beam Splitter Implementation and Quantum State Stabilization

The combination of weak measurements combined with feed forward and feedback onto the state source and measurement apparatus comprises quantum state stabilization (QSS), whereby the QRNG corrects itself for bias. Figure 2 shows the basic setup for a beamsplitter QRNG based on polarization with a weak polarization measurement apparatus. The WM consists of a pair of polarization sensitive beam displacers. An optional half waveplate can be used in between them to tune the strength of the measurement. A detection event at the single photon detector located just after the WM indicates a full projection of the polarization state, while the absence of a click indicates a transmission of a slightly perturbed polarization state. Thus, the beam displacers and half waveplate combination acts as a tunable Brewster plate [4]. The statistics of the polarization state garnered from the WM detector, correlated with the absolute count rate after the beamsplitter, can be used to determine the degree to which the measurement basis matches the photon polarization basis, and feedforward can then be used to change the measurement basis as a result, removing polarization bias effects before subsequent photons are converted to numbers. Likewise, feedback control on the laser and output waveplate can change its current and temperature in order to tailor the output quantum state both in terms of polarization and photons per unit time.

![Fig. 2: a beam splitter QRNG with weak polarization measurement and feedback / feed forward.](image_url)

The WM shown in Fig. 2 is not the only way to characterize the polarization. Using only a single beam displacer (such as a quartz plate), set at an angle such that the displacement of horizontal from vertical is much smaller than the beam waist, comprises a WM [5]. A potential advantage is that this technique can be used in combination with a continuous variable (CV) QRNG based on beam splitters, in which the laser output acts as a local oscillator in a homodyne detector for detection of vacuum noise.

3. Conclusion and Outlook

Here we have demonstrated a QRNG based on TA optical emission using various number registration methods. We have also outlined methods for self-detecting and removing bias both in discrete photon counting and CV methods. Finally, the TA has the capability to output amplified spontaneous emission (ASE) when operated at a high current. This allows it to be used as a very high bitrate physical random number generator based on ASE [6], which is the subject of a future study.

4. Acknowledgements

This work was performed at Oak Ridge National Laboratory, operated by UT-Battelle for the U.S. Department of energy under contract no. DE-AC05-00OR22725.

5. References