A Generator for Unique Quantum Random Numbers Based on Bosonic Stimulation

Akshata Shenoy H., *S. Omkar, *R. Srikanth, T. Srinivas

Applied Photonics Lab, ECE Dept, Indian Institute of Science, Bangalore, * Poornaprajna Institute of Scientific Research, Bangalore.

Abstract : Conventional methods for random number generation are based on deterministic computational algorithms and an initial seed, and are technically only pseudo-random. Quantum indeterminacy provides the possibility for generating genuine randomness, guaranteed by the very laws of Physics. Here we propose a method to realize a quantum random number generator based on bosonic stimulation, that requires only weak coherent pulses and conventional avalanche photo-diode detectors.

Introduction: Random numbers are crucial for various tasks, among them generating cryptographic secret keys, authentication, Monte-Carlo simulations, digital signatures, statistical sampling, etc. Random number generators can be classified into two types: pseudo-random number generators (PRNG) and true random number generators (TRNG). A PRNG is an algorithm, computational or physical, for generating a sequence of numbers that approximates the properties of random numbers. A physical or hardware version is typically based on stochastic noise or chaotic dynamics in a suitable physical system. Computational PRNGs are based on computational algorithms that generate sequences of numbers of very long periodicity, making them look like true random numbers for sufficiently short sequences. Careful observation over long periods will in principle reveal some kind of pattern or correlation, suggestive of non-randomness. As far as is known today, the inherent indeterminism or fluctuations in quantum phenomena is the only source of true randomness, an essential ingredient in quantum cryptography. Various proposed underlying physical processes for quantum random number generators (QRNGs) include: quantum measurement of single photons, an entangled system, coherent states or vacuum states; phase noise, spin noise, or radioactive decay or photonic emission. In this work, we propose a novel method of QRNG that is a quite different indeterministic paradigm from the above two. It uses bosonic stimulation to randomly amplify weak coherent pulses to intense pulses that can be easily detected by a conventional APDs.

Practical Realization: A concrete idea for realizing a random bosonic stimulator is to use a lasing medium that supports two radiation modes, for example by vertical and horizontal polarization of the same frequency . A scheme of the proposed experiment is given in figure. Two equal intensity, highly attenuated modes of coherent states are input into a lasing medium. To ensure that the two inputs are synchronized and of equal intensity, a calibrated Mach-Zehnder set-up is used with an attenuated coherent laser pulse fed into one of its input ports. This results in an output consisting of two (un-entangled) coherent pulses with half the intensity. A half wave plate in one of the arms ensures that the polarization in one arm rotated to be 90˚with respect to the other. Each mode in a pulse corresponds to a ball color in the Polya urn problem. Because of bosonic stimulation, the output intensity will randomly favor vertical or horizontal polarization. Let I_H (I_V) denote the intensity of the outcoming light in the horizontal (vertical) polarization mode. The production of intensities can be approximated as a two stage process: 1. Poisson process that produces a distribution of photon numbers from the de-excited atoms. 2. Within each number , there is a Polya process that determines the distribution into the two modes. The Poisson process creates laser light entangled states of atoms in the lasing medium, which can be described as,

$$|\alpha\rangle = e^{-|\alpha^2|/2} \sum_{j=0}^{\infty} \frac{\alpha^j}{\sqrt{j!}} |j\rangle |\xi_p\rangle$$

The joint system of the modes and atoms evolves in a manner given by,

$$|n,m\rangle |\xi_p\rangle \rightarrow \frac{1}{\sqrt{n+m+2}} (\sqrt{n+1}\,|n+1,m\rangle |b\rangle + \sqrt{m+1}\,|n,m+1\rangle |r\rangle) |\xi_{p+1}\rangle$$

$$\rightarrow \frac{1}{\sqrt{(n+m+2)(n+m+3)}} (\sqrt{(n+1)(n+2)}\,|n+2,m\rangle |b,b\rangle + \sqrt{(n+1)(m+1)}\,|n+1,m+1\rangle * (|b,r\rangle + |r,b\rangle) + \sqrt{(m+1)(m+2)}\,|n,m+2\rangle |r,r\rangle) |\xi_{p+2}\rangle$$

Bosonic Stimulation: If there are N particles in a given quantum state then the probability that an incoming boson makes a transition into that state is proportional to N+1. Bosons obey B-E statistics which entails that the transition probability of a boson is enhanced by the presence of identical particles in that state.

Polya-Urn Problem : Let the initial population of two states labelled as "blue" and red" be b(0) and r(0), respectively. As the incoming balls start populating the two states, the subsequent growth in population of the modes exhibits Polya urn behavior.The probabilistic law of evolution of the fractional population at ith instance is given by bosonic stimulation to be,

$$\{ b(i), r(i) \} \longrightarrow \begin{cases} (\, b(i)+1, r(i)\,) \text{ with probability } b(i)+1 \,/\, [\, b(i) + r(i) + 2] \\ (\, b(i), r(i)+1\,) \text{ with probability } r(i)+1 \,/\, [\, b(i) + r(i) + 2] \end{cases}$$

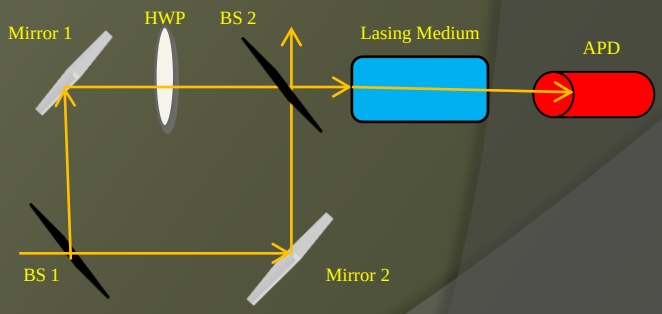
The limiting value t ≡ b(i)/[b(i)+r(i)] for a large I itself varies randomly in the range [0,1] from run to run having a beta distribution,

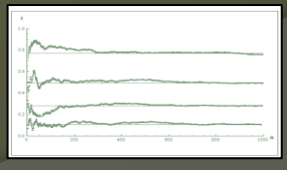
$$f(t;\beta,\rho) = \frac{1}{B[\beta,\rho]} t^{\beta-1}(1-t)^{\rho-1}$$

where B is the beta function that normalizes f, β= b'/c, ρ= r'/c, b'≡ b(0)+S b, r'≡ r(0)+ Sr. For bosonic stimulation shifts Sb = Sr = 1.

Depending on the number of trial runs, the final state can have an arbitrarily large number of bosons. Depending on whether t > 0:5 (blue dominates) or t < 0:5 (red dominates), one generates a random bit 0 or 1. This can serve as the basis of generating random bits at a rate determined by the frequency with which each run can be repeated. Thus, the phenomenon of bosonic stimulation acts as a macroscopic QRNG.

Experimental Set-Up and Results:





Two bit generation per run :

t < t ¼	x = 00
t ¼ ≤ t < t ½	x = 01
t ½ ≤ t < t ¾	x = 10
t ≥ t ¾	x = 11

References: [1] M. Luby, Pseudorandomness and Cryptographic Applications. Princeton Univ Press (1996).
[2] I. Kanter, Y. Aviad, I. Reidler, E. Cohen and M. Rosenbluh, An optical ultrafast random bit generator Nature Photonics 4, 58 (2010).
[3] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden. Quantum Cryptography. Rev. Mod. Phys. 74, 145 (2002); arXiv:quant-ph/0101098.
[4] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger. A fast and compact quantum random number generator. Review of Scientic Instruments 71, 1675 (2000).
[5] J. Dynes, Z. Yuan, A. Sharpe, and A. Shields. A high speed, postprocessing free, quantum random number generator. Applied Physics Letters 93, 031109 (2008).
[6] I. J. Owens, R. J. Hughes and J. E. Nordholt. Phys. Rev. A 78, 022307 (2008).
[7] M. Ren, E. Wu, Y. Liang, Y. Jian, G. Wu and H. Zeng. Phys. Rev. A 83, 023820 (2011)
[8] N. Kumar, arXiv:Cond-mat/ 0204443v2.
[9] N. Kumar and R.Srikanth, 'Bosonic Stimulation as a natural realization of Polya urn problem', Physics Letters A, 2006, 359, 281.

Conclusion: We have proposed a novel QRNG principle, based on bosonic stimulation, in which, while the state preparation procedure presents experimental challenges, the detection and read-out parts are easier to implement. In an actual experiment, it is possible that systematic experimental biases might introduce correlations into the sequence of bits produced, thereby degrading the randomness. Statistical analyses like the Diehard tests and National Institute of Standards and Testing (NIST) suite of tests for randomness have to be carried out to know the quality of randomness and improve upon it.