# Implementation of Random nature of Qubits for Random Number Generation via Simulation

Sahil Imtiyaz[1], Jamal A Nasir[2], Junaid Ul Haq[3], Qin Zhao[4], Wail Mardini[5]
[1,2] Department of Computer Science International Islamic University, Islamabad 44000
3Center of Theoretical Physics, Jamia Millia Islamia., New Delhi
4Department of Physics, National University of Singapore 2 Science Drive 3, Singapore 117551
5Jordan University of Science and Technology, Jordan
Corresponding E-mail: saahilimtiyaz@gmail.com,

*__Corresponding Author:__ *saahilimtiyaz@gmail.com, Tel.: +91-91495-89995*

## ABSTRACT

Random Number Generation implemented through Quantum-Classical integration. The system includes a plural source of light with coherent states such that each state has an indeterminate number of photons. This varying Photon number produces varying current when input to an avalanche photodiode and the characteristics of this hardware element (Avalanche Photodiode) is changed by varying the temperature, pressure and electric field of the electronic system. The varying characteristics introduce Classical noise of Quantum origin that forms the basic idea for Random Number Generation. The varying electric field on the other hand increases the reverse voltage and hence acts as a gain for the photon incident on its hardware Every state has different photon number and corresponding photodiode characteristic that is being fetch to analog to digital converter that eventually generates an absolute random number. The gain value of photon is multiplexed with the actual message and acts as a modulation technique. We utilize dye laser simulation and rhodium molecule as a site for this implementation via test particle. As the parameters are shifted and varied, there is an increase in the quantum nature of particle and then starts becoming classical due to decoherence and noise factor and then eventually randomize. This property can be best utilized for random number generation owing to this randomization.

Keywords: Topology, Qubit, Dye Laser, Simulation

## INTRODUCTION

Communication security in complex computer networks is one of the central and fundamental issue of most information and communication technology and consequently have had increased the interest and scope of cryptographic encryption techiniques.The security of a given encryption technique relies on the crucial assumption that user have access to secret keys. The secret key is the fundamental aspect for the security of some sensitive information over a communication channel. A common way to generate secret key is to use a random number generator. There are three main fundamental properties required for an absolute random number generation.
The first main fundamental requirement for a random number generation is equiprobability that is it should have an ability to produce random sequences at uniform distribution having equal

probabilities. The mathematical notion for analyzing the quality in this aspect can be defined as difference in the apparent probabilistic distribution to the actual uniform distribution. The second fundamental requirement for random number generation is the ability to produce actual randomness, meaning ability to generate unpredictable numbers, since any correlation among the generated numbers is detrimental. If there is any sort of valid rule or equation between the generations of two consecutive random numbers then it would be easy for the third party to easily predict the next random number. The final aspect of the random number generation is the security and this parameter is actually a derived aspect of equiprobability and unpredictability. These three parameters are fundamental and significant of random number generation as if there would be any divergence from the discussed paradigm then eventually the third party could predict the secret key easily[45]

The phases and transitions in the progress of random number generation is from using simple classical methods and then introduction of quantum paradigm proved to be an effective approach for fast generation of numbers with random equation between the consecutive outputs and hence adding speed and security to it. Classical approach being based on the expected phenomena with macroscopic nature so its often predictable on the other hand quantum approach deals with the microscopic phenomena that is efficient from security and speed perspectives. Many methods and approaches have been implemented on the above discussed paradigms and the results are extremely significant. When the speed of the random number generator is increased there is often a trade off with the security of the concerned machine as when speed is increased then it becomes hard for the random generator to output unpredictable equiprobable random numbers with at least no equation governing them. As a result of this fact the classical method inherits the secure platform for the random generation and the quantum platform manages the speed of generation of random numbers. Although both of the approaches have been physically implemented on the circuit and logical level and in some cases both approaches may have lest introduced but the present proposal design is being implemented by using Quantum-Classical integration for random number generation so that we could model a controlled random number machine that would be secure and fast in a logical fashion.

The above Idea for generation of random number that can act as secret key in cryptography is being implemented via principle of classical and quantum mechanics A Plural coherent source emitting photon but every individual coherent state being variable in terms of photon number is being fetched to a photo diode that changes it to current as per photoelectric effect. There is a constant fluctuation in intensity of light as there is constant phase difference in each state as a result there is variable indeterminate emission of photon number in each coherent state. Each coherent state with some photon number is fetch to a photodiode and it is converted to current before it is output to ADC the characteristics of photodiode is changed in each state by changing the temperature or pressure of the diode due to some transistor action connected to it. The output is analog in nature and is digitalized with a ADC. Each there are mainly two main approaches for the generation of random numbers depending upon the type of mode and their method. The two approaches being Pseudo-Random Number Generation (PRNG) and the other is Hardware based Random Number Generation (HRNG). The PRNG is a deterministic algorithm for generating a sequence of uniformly distributed numbers that approximates to the actual random number as the generated numbers are not purely random in nature as it is basically determined by the set of initial parameters and eventually repeats idle after some time and is due to the finiteness of the computer. Initialization of the algorithm is done by an internal state of computer such as current

time, mouse click, or even keyboard stroke. The algorithm will produce same sequence after a meanwhile when initialized with the same input. The merit of this approach is speed but security is being compromised.

The other safer way for the generation of Random Number Generation is based on Hardware from a physical process including thermal noise, avalanche noise and even time drift. The main demerit of this technique is the the rate of generation of random numbers. HRNG can be divided into three main categories depending on the physical phenomena used as a source of randomness. The first category used classical macroscopic approach and they are often predictable as macroscopic system obeys deterministic laws of classical physics. The other category is based on deterministic phenomena of microscopic world, the constituents being electrons or protons. This approach is also predictable although microscopic world is unpredictable but it is not purely quantum as there are classical instincts contained in it, exploiting deterministic means to distort electronic noise.

The third category for the generation of Random number is based on Quantum Phenomena and this physics is actually the integrated view of randomness and moreover the two properties of equiprobability and unpredictability are naturally inherited in it. Recently this Ideas was harnessed for Random Number generation using a pulse consisting on average of a single photon travelling through a semi transparent mirror. The mutually exclusive events reflection and transmission are detected and associated with one of the binary outcomes but it lacks speed or rate of generation although the generated values were unpredictable and equiprobable. The other quantum number generator involves utilization of quantum noise from an optical homodyne detection apparatus. The system utilizes quantum noise generated by splitting laser light. But it had some practical issues and further improvement was devised by employing a laser source of coherent and plural nature which had indeterminate photon number, fetch to photo diode to produce analog current which is digitalized, and generating random number. Recently the research of generation of random number has reached 80mbps and after resolving it with other constraints it's found to be 68mbps but although the speed or rate of generation of quantum number using quantum spontaneous emission of laser is fast but prone to predictable and hence security may be compromised. The present research proposal makes a tradeoff between security and speed or rate of generation of quantum number using Classical-Quantum Integrated system digital signal can be decoded in some decimal value and that value is our Random number.[45]

The proposed research maintains the unpredictable nature of the machine by escalating the concepts of Classical Approach and speed is maintained correspondingly by the Quantum Approach. Our goal is to minimize the factor that can apprehend and anticipate the equation between the random number generations. As there is immense unpredictability in the coherent states then adding a variable characteristic transistor will add and embed inherently to the scope of unpredictability and on side grounds the speed of generation remains effective and fast. The main Physical element that is being introduced as a major part of the proposal is utilization of avalanche photodiode for detection of photons from the coherent source. There are mainly two main approaches for the generation of random numbers depending upon the type of mode and their method. The two approaches being Pseudo-Random Number Generation (PRNG) and the other is Hardware based Random Number Generation (HRNG). The PRNG is a deterministic algorithm for generating a sequence of uniformly distributed numbers that approximates to the actual random number as the generated numbers are not purely random in nature as it is basically determined by the set of initial parameters and eventually repeats idle after some time and is due

to the finiteness of the computer. Initialization of the algorithm is done by an internal state of computer such as current time, mouse click, or even keyboard stroke. The algorithm will produce same sequence after a meanwhile when initialized with the same input. The merit of this approach is speed but security is being compromised.

We utilize dye laser simulation and rhodium molecule as a site for this implementation via test particle. As the parameters are shifted and varied, there is an increase in the quantum nature of particle and then starts becoming classical due to decoherence and noise factor and then eventually randomize. This property can be best utilized for random number generation owing to this randomization. It includes quantum adiabatic evolution and implementation in machine learning [18-28]

**Related Work**

There are mainly two main approaches for the generation of random numbers depending upon the type of mode and their method. The two approaches being Pseudo-Random Number Generation (PRNG) and the other is Hardware based Random Number Generation (HRNG). The PRNG is a deterministic algorithm for generating a sequence of uniformly distributed numbers that approximates to the actual random number as the generated numbers are not purely random in nature as it is basically determined by the set of initial parameters and eventually repeats idle after some time and is due to the finiteness of the computer. Initialization of the algorithm is done by an internal state of computer such as current time, mouse click, or even keyboard stroke. The algorithm will produce same sequence after a meanwhile when initialized with the same input. The merit of this approach is speed but security is being compromised.
The other safer way for the generation of Random Number Generation is based on Hardware from a physical process including thermal noise, avalanche noise and even time drift. The main demerit of this technique is the rate of generation of random numbers. HRNG can be divided into three main categories depending on the physical phenomena used as a source of randomness. The first category used classical macroscopic approach and they are often predictable as macroscopic system obeys deterministic laws of classical physics. The other category is based on deterministic phenomena of microscopic world, the constituents being electrons or protons. This approach is also predictable although microscopic world is unpredictable but it is not purely quantum as there are classical instincts contained in it, exploiting deterministic means to distort electronic noise

The third category for the generation of Random number is based on Quantum Phenomena [34] and this physics is actually the integrated view of randomness and moreover the two properties of equiprobability and unpredictability are naturally inherited in it. Recently this Idea was harnessed for Random Number generation using a pulse consisting on average of a single photon travelling through a semi transparent mirror. [3]The mutually exclusive events reflection and transmission are detected and associated with one of the binary outcomes but it lacks speed or rate of generation although the generated values were unpredictable and equiprobable. The other quantum number generator involves utilization of quantum [29-32] noise from an optical homodyne detection apparatus. The system utilizes quantum noise generated by splitting laser light. But it had some practical issues and further improvement was devised by employing a laser

source of coherent and plural nature which had indeterminate photon number, fetch to photo diode to produce analog current which is digitalized, and generating random number. Recently the research of generation of random number has reached 80mbps and after resolving it with other constraints its found to be 68mbps but although the speed or rate of generation of quantum number using quantum spontaneous emission of laser [33]is fast but prone to predictable and hence security may be compromised. The present research proposal makes a tradeoff between security and speed or rate of generation of quantum number using Classical-Quantum Integrated system.

*A. Implementation*

The main underlying concept that may be physically implemented on hardware comprises of some main components. The apparatus consists of a laser source that is coherent in nature with multiple states having constant phase difference between the consecutive light source and this phase difference for physical interpretation can be changed into intensity so consequently the coherent source has intensity differences. Each state has an indeterminate number of photons and as a direct consequence there is difference in intensity of each state. The output is fetch to a photo detector and in this proposal this is the main area of concern as there is classical integration in the methodology of generation of Random number and that is being deployed in the photo detector. The laser utilized is a dye laser that uses rhodium molecule for mapping the scenario. The data point shows randomized behavior from quantum towards Classical and then eventually randomized. The photo detector that is being implemented in the system can special type of photodiode named as Avalanche photodiode. [3] The Avalanche photodiode is maintained at varying characteristics by varying the electric field and consequently noise of classical and quantum nature is produced and has a random nature which will be added to the intensity of the photon from coherent source with specific gain. Then afterwards the output is given a analog to digital converter then consequently generates Random number. The randomness of this system depends in the randomized nature of the test particle in the rhodium di-oxygen vent mapping laser width with voltage and laser intensity with energy.

*B. Methodology*

First of all the practical schema [1, 2] will comprise of a laser that will be coherent in nature and as a result there will be phase difference constant in nature and also will have corresponding intensity shifts. The laser source is maintained at constant pressure and temperature as if these parameters would vary then it would inherit a known equation in photon number that is emitted by the laser as the pressure and temperature constraints are classical in nature. When the laser emits its photons, it is found that all the photons will have constant phase difference and hence each coherent state will produce indeterminate number of photons in each state

that will be totally having no interference of classical paradigm. The laser is operated at threshold before stimulated emission. So in each state there will be indeterminate number of photons and hence it will act as quantum interference in our proposed model as the emission is clearly a Quantum driven process.
After the laser emits indeterminate number of photons in each stage, the output is fetch to a photo detector and in the proposal an Avalanche photodiode is implemented. The specific photo detector is chosen as it has a random way of producing noise and also the gain factor can be varied due to the electric field. The Avalanche diode changes light signal into electric signal with gain factor component adding to it. The output current of the Avalanche diode fluctuates in the absence of light as well as in its presence. The noise in this current arises from three sources: randomness in the number and in the positions at which dark carrier pairs are generated, randomness in the photon arrival number, and randomness in the carrier multiplication process. All the randomness in noise are classical in nature and hence there is an integrated system of Quantum-Classical approach.

The dark carriers are random and they are produces when even no light is incident on it, there is also randomness due to number of photon incident on it and as it has been already proposed that the source produces indeterminate number of photons in every stage so the second type of noise in the Avalanche is also purely random in nature. The last component of noise is due to multiplication gain process which is to add gain factor to the signal. Nowadays we can add a gain of greater than 1500 under the reverse voltage. Since we know that the reverse bias voltage is limited as above its specific value its minority carriers avalanche off and break the depletion region and it becomes a sort of forward bias. So the limited reverse bias is a practical impediment in our proposal but we deploy a controlled bias voltage by never making the device to exceed the reverse voltage threshold. The configuration that I discuss is simple but practically it may be deployed with more circuit schema. The problem is sought out by adding a transistor with it. It can be utilized for optimization for efficiency [13-17]

**Simulation and Results:**
We performed a FORTRAN simulation [33]of the above method using dye laser and rhodium as atom for analysis.The equation describing the change in the population inversion density ‘n’ and photon density ϕ can be written as:

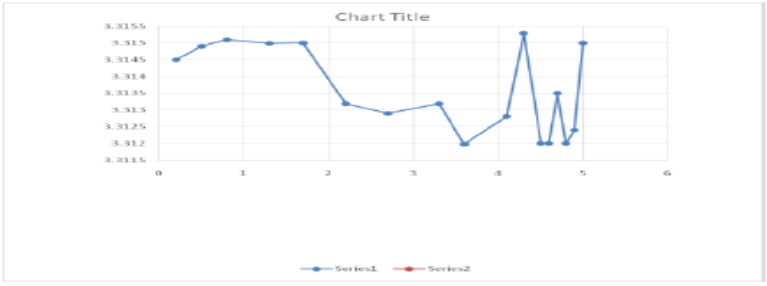
$$\frac{dn}{dt} = -rc\sigma_{se}\emptyset \qquad (2)$$

$$\frac{d\emptyset}{dt} = \left(c\,\sigma_{se}\left(\frac{l}{l'}\right)n\emptyset\right) - \frac{\varepsilon}{t_r}\emptyset \qquad (3)$$

The two dynamic equations are coupled and must be solved in iterative manner that allows successive values of population inversion density and photon density to be used to calculate the next value of each [35-41]
**Algorithm**

The simulation algorithm show below has been executed in FORTRAN program [11, 12]

| Time of Evolution | Pulse Width (Dynamics of Qubit) | Peak Power |
|---|---|---|
| 0.2 | 3.3145 | 0.12714 |
| 0.5 | 3.3149 | 0.31771 |
| 0.8 | 3.3151 | 0.50832 |
| 1.3 | 3.31499 | 0.82611 |
| 1.7 | 3.315 | 1.08041 |
| 2.2 | 3.31319 | 1.39838 |
| 2.7 | 3.3129 | 1.71645 |
| 3.3 | 3.31319 | 2.09831 |
| 3,6 | 3.31198 | 2.288929 |
| 4.1 | 3.31281 | 2.607686 |
| 4.3 | 3.31529 | 2.73506 |
| 4.5 | 3.312 | 2.86247 |
| 4.6 | 3.312 | 2.926213 |
| 4.7 | 3.3135 | 2.98988 |
| 4.8 | 3.312 | 3.053636 |
| 4,9 | 3.3124 | 3.11733 |
| 5.0 | 3.315 | 3.18106 |



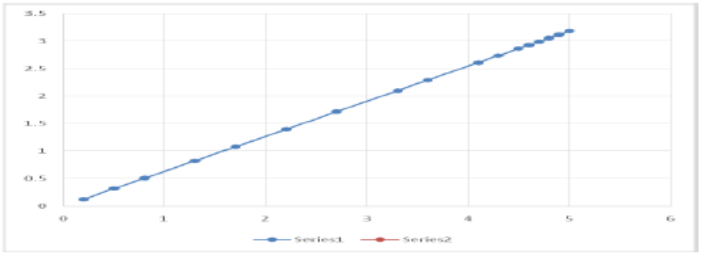




Figure 1: The randomized behaviour of Information in Quantum Environment mapped via Laser Simulations with uniform increasing of input.[6-10]

The simulated results show that there is a point up to which the quantumness of the system can retain its properties by varying the input parameters. It is due to the spacial confinement of the memory that is mapped in terms of pulse width and hence affects the nature of qubits. It increases first and then deceases and eventually gets randomized. It has effect on efficiency of the algorithms.

## III. CONCLUSION

The simulation shows the randomizing behaviour of quantum nature of information. It first shows quantum efficiency and probabilistically can tunnel for optimization then starts decreasing and eventually randomize. It gives new understanding of information in terms of topology that is inert to eternal noise and errors unlike qubits [4, 5]

## ACKNOWLEDGMENT

We are thankful to Centre for Theoretical Physics Jamia Millia Islamia, New Delhi for conducting simulations and graph plotting and for important discussions and perspectives from Dr. Mir Faizal, University of British Columbia, Canada.

[1] Nisim Ofek, et al, *Demonstrating Quantum Error Correction that extends the lifetime of Quantum Information*, [arXi: **1602.04768v1**]

[2] *Millisecond Coherence Time in a Tunable Molecular Electronic Spin Qubit*, Joseph M. Zadrozny et al ACS Cent Sciv.1**(9**); **2015** Dec 23 PMC4827467

[3] Luca Chirolli, Guido Burkand , *Solid State Qubit*, [arXiv: **0809.4716**]

[4] *A short introduction to topological quantum computation* Ville T. Lahtinen1 and Jiannis K. Pachos Sci post phy **, 3 021,2017**

[5] A. Kitaev and J Preskill, *Topological entanglement entropy*, Phys.Rev.Lett**, 96,110404** (**2006)**

[6] I Bloch et al, Quantum Simulation with ultra cold Quantum Gases, Nat.Phys **8**, **267 (2012)**

[7] Niklas M Gerges, Larz Firtz and Drik Schuricht, *Topoloical order in the Kitaev/Majorana Chain in the presence of disorder and interaction*, [arXiv: **1511.02817**]

[8] J.K Pahos et al, *Revealing Anyonic features in toric code quantum simulation*, New . Phys, **11, 083010** (**2009**)

[9] *A short introduction to topological quantum computation* Ville T. Lahtinen1 and Jiannis K. Pachos Sci post phy **, 3 021,2017**

[10] J.S Xu, K Sun, Y.J Han,C.E-Li, J.K Pachos and G.C Guo, *Simuating the Exchange of Majorana Zero Modes with a Photonic System*, Nat. Commun**, 7, 13194(2016)**

[11] Barry Coyle, D., Guerra, D. V. & Kay, R. B., 1995. *An interactive numerical model of diode-pumped, Q-switched/cavity-dumped lasers.*. Journal of Physics D: Applied Physics**, 28(3),** p. **452.**

[12] Kay, R. B. & Waldman, G. S., **1965**. *Complete Solutions to the Rate Equations Describing Q-Spoiled and PTM Laser Operation*.. Journal of Applied Physics**, 36(4),** pp. **1319-1323**.

[13] Djurdje, Jacek, C. & Klinowski, **1995**. *Taboo search: an approach to the multiple minima problem. Science*, **267(5198**), pp. **664-666**.

[14] Edward, F., Goldstone, J. & Gutmann, S., **2002**. *Quantum adiabatic evolution algorithms versus simulated annealing*.. arXiv: arXiv preprint quant-ph/0201031.

[15] Farhi, E., J, G., S, G. & D., N., **2008**. *How to make the quantum adiabatic algorithm fail*.. International Journal of Quantum Information., **06(03),** pp. **503-516**.

[16] Farhi, E. et al., **2001**. *A quantum adiabatic evolution algorithm applied to random instances of an NP-complete problem*.. Science, **292(5516**), pp. **472-475.**

[17] Farhi, E., J, G., S, G. & M., S., **2000**. *Quantum computation by adiabatic evolution.*. arXiv: arXiv preprint quant-ph/0001106

[18] Jamil, M. & Yang, X.-S., **2013**. *A literature survey of benchmark functions for global optimisation problems*.. International Journal of Mathematical Modelling and Numerical Optimisation**, 4(2**), pp. **150-194**.

[19] oender, C., AR, K., GT, T. & L., S., 1982. *A stochastic method for global optimization. Mathematical programming*., **22(1),** pp. **125-140.**

[20] Djurdje, Jacek, C. & Klinowski, 1995. *Taboo search: an approach to the multiple minima problem. Science*, **267(5198**), pp**. 664-666**.

[21] Edward, F., Goldstone, J. & Gutmann, S., **2002**. *Quantum adiabatic evolution algorithms versus simulated annealing*..[ arXiv: preprint quant-ph/0201031.

[22] Farhi, E., J, G., S, G. & D., N., **2008**. *How to make the quantum adiabatic algorithm fail*.. International Journal of Quantum Information., 06(03), pp. **503-516**.

[23] Farhi, E. et al., **2001**. *A quantum adiabatic evolution algorithm applied to random instances of an NP-complete problem*.. Science, **292(5516**), pp. **472-475**.

[24] Reichardt Ben, W., **2004**. *The quantum adiabatic optimization algorithm and local minima*.. ACM, s.n.

[25] Aaronson, S., 2015. *Quantum machine learning: read the fine print.* Nature Physics, **11(4),** pp. **291-293**.

[26] Biamonte, J. et al., **2016**. *Quantum machine learning*. arXiv: arXiv preprint.

[27] Biamonte, J. et al., **2016**. *Quantum machine learning*. arXiv: arXiv preprint.

[28] Cai, X. et al., **2015**. *Entanglement-based machine learning on a quantum computer*.. Physical review letters**., 114(11),** p**. 110504**.

[29] Cohen, T. H., Leiserson, C., RL, R. & C, S., 1990. *Introduction to algorithms*. Cambridge MA: The **MIT** Press.

[30] Kak, S., **2007**. *Quantum Mechanics and Artificial Intelligence. London*, DOI.

[31] Liu, S., Ying, L.and Shakkottai, S., *Influence maximization in social networks: An Ising-model-based approach*, In Proc.48th Annual Allerton Conference on Communication, Control, and Computing **(2010)**

[32] Jianging, Han, F. & Liu, H., 2004. *Challenges of big data analysis. National Science Review*, **1(2),** pp. **293-314**.

[33] Kay, R. B. & Waldman, G. S., **1965**. *Complete Solutions to the Rate Equations Describing Q-Spoiled and PTM Laser Operation.. Journal of Applied Physics*, **36(4),** pp. **1319-1323**.

[34] Quantum Random Number Generators, arXiv:1604.03304v2

[35] *On the Hermatian optical phase operator Journal of Modern Optics*
Vol **36** page **1, 7-19**

[36] *The physics of Quantum* Mechanics by James Biney

[37] Evolution and Prospects for single photo diode and quenching circuits
by Scova vol **51** issue **9-10** pages **1164-1288**

[38] *Avalanche Multiplication Noise characteristics* David IEEE vol 45
Issue 10

[39] Semiconductor devices by Malvino

[40] Network Distributed Quantum Random Number Generation US patent
US 2012/0221615 A1, Aug 30 2012

[41] Debabrata Goswami, Adiabatic Quantum Computing with Phase Modulated Laser Pulses , arXiv:quant-ph/0507268