# Unpredictable Random Number Generator

Yutaka Shikano

Quantum Computing Center, Keio University,
Yokohama 223-8522, Japan,
and
Institute for Quantum Studies, Chapman University,
Orange, CA 92866, USA.
Email: yutaka.shikano@keio.jp

March 9, 2020

## 1 Unpredictability and Random Numbers

Prediction is supposed to be a fruitful product of good science. For example, in the case of a falling apple, Newtonian mechanics can in principle, predict the real-time path of this apple, whose mass is known under the initial condition. Since this is assumed to be applied to the rigid body approximation (as in the case of the apple), the precision of the real-time path is limited. Most physical models that describe complex and dynamical natural phenomena are based on several approximations of the target phenomena. In the Japanese essay written by Sin-Itiro Tomonaga [1], who won the Nobel Prize in physics with Julian Seymour Schwinger and Richard Phillips Feynman in 1965, tried to answer the question *what is physics?*" as follows:

> Physics seeks for the existing laws of any natural phenomena around us[1] in pursuit of relying on the observational facts.

The established laws in physics may not be effective in predicting the real-time path. David Deutsch, who initiated the concept of a quantum computer in the year 1985 [2], claimed the concept as an aid to "*better understanding*" of

[1]It is noted that this deals with non-biological phenomena as an annotation in the original quote.

nature because of the modifications made to several existing laws of nature in the history of science [3]. By understanding these phenomena using classical mechanics, we can predict the real-time path under all known conditions. It is known that this simulation may lack a computational resource under the current or near-future technological level.

In the digital computational world, as a byproduct of scientific achievement, computation is often used for prediction. This computational prediction is not only useful in daily life, such as for weather forecast and stock price predictions, but also for basic science. As an example of a basic science application, in the case of laser interferometer gravitational-wave detectors such as LIGO, VIRGO, and KAGRA, the real-time feedback/feedforward system is essentially used for stable operation, and it requires huge computational resources. Historically, the first electronic general-purpose digital computer, ENIAC, was designed and primarily used to calculate artillery firing tables for the United States Army's Ballistic Research Laboratory. However, its first program was a study on the feasibility of a hydrogen bomb [4]. John von Neumann and Stanisław Marcin Ulam demonstrated that the speed of ENIAC would enable quick calculations by using the Monte Carlo method such that the calculation of the distance that neutrons were likely travel through various materials could be performed much more quickly [5, 6]. Because the Monte Carlo method requires quickly generated random numbers, John von Neumann initiated a pseudo random number generator (PRNG) by using the middle-square method [7]. The basic structure of a PRNG consists of a nonlinear function and an external initial value, which is called a *seed*. Because scientific tasks require reproducibility of the obtained results, scientific computations using the randomized method require the exact and complete results each time. This can be carried out by the same seed. In our daily lives, PRNGs are widely used for simulation, gaming, and security. This technology vitally supports our digital world. In digital gaming, such as Pokémon, several game players have already hacked the random number generator (RNG) in the game to tune it to their desired situation. This is often called an *RNG manipulation*. If such individuals hack the PRNGs in our security system, the security system will be easily broken. In this situation, almost all cryptographic techniques such as RSA, post-quantum, and quantum key distribution, are ineffective [8]. This is because the mathematical proofs of most cryptographic techniques assume the existence of uniform random number digits. The probabilistic seed cannot be generated since the computational machine implemented the universal Turing machine such that the von Neumann architecture is deterministic. The output sequence generated from any PRNG is essentially predictable. Meanwhile, a physical RNG was initiated by Maurice George Kendall and Michael James Babington

Smith in 1938 [9]. The world's first commercially available general-purpose digital computer, Ferranti Mark 1, generated random number bits by using electrical noise, in the year 1951 [10]. The classical mechanics based physical RNG, such as tossing a coin, has the same problems as those in the PRNG. Therefore, in principle, PRNG is predictable. When a randomized source of a physical PNG such as electrical noise, temperature, and timestamp is based on external measurable parameters, it also has the same problem.

A "true" uniform RNG has a mathematically simple form, which is similar to a binary random variable $\{X_i\}_{i=1}^N$, which has the following probability distribution

$$\Pr[X_i = 0] = \Pr[X_i = 1] = \frac{1}{2} \tag{1}$$

for all $i = 1, 2, \cdots, N$. Moreover, the binary random variables $\{X_i\}_{i=1}^N$ are independent and identically distributed (*i.i.d.*). When a certain RNG completely satisfies the above mathematical form, it becomes unpredictable; hence, we cannot perfectly predict a future binary sequence. According to Kentaro Tamura, who is my collaborator on this project,

> "Physics is not fair but the random number is fair."

He made this statement when we decided to start this random-number project. The above-mentioned RNG does not satisfy the "true" uniform RNG. While there are several statistical tests on the RNGs, such as NIST Test Suites, TEST U01, and Diharder, the RNGs passing all statistical tests cannot be guaranteed as the "true" uniform RNG. As one of the "true" uniform RNG candidates, a generation process itself has a probabilistic structure. Technically, a measurement process that obeys the rules of quantum mechanics is conceivable. This is called the Born rule, which is considered as one of the mathematical axioms of quantum mechanics. Then, a quantum-mechanics based RNG, the so-called *quantum random number generator (QRNG)*, is considered while we have to take into account the established laws of physics. It is to be noted that a macroscopic theory such as statistical physics adopts a probabilistic treatment. When the underlying microscopic theory is described in classical physics, this probabilistic treatment of the macroscopic state is not required because infinite computational resources are available to be used. This is attributed to a coarse graining process from the microscopic deterministic dynamics to macroscopic theory.

# 2 Seedless Random Number Generator

A simple procedure of QRNG is

1. setting the initial quantum state, denoted as $|0\rangle$, of the two-level quantum system $\mathcal{H}_2 := \text{span}\{|0\rangle, |1\rangle\}$.

2. generating the quantum-mechanical superposition from the initial state;

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left( |0\rangle + |1\rangle \right). \tag{2}$$

3. measuring the generated quantum state $|\psi\rangle$ on the basis of $|0\rangle$ and $|1\rangle$. Then, the output quantum state changes, depending on the measurement outcome. The measurement output itself becomes the random number bit.

4. resetting the initial quantum state or preparing a new quantum state.

Step 1 has the same requirement as that of building a universal quantum computer according to the DiVicenzo criteria [11]. Steps 1 and 2 have the same external procedure to control the quantum state. In Step 2, the quantum gate of the quantum computer is implemented, and the Hadamard gate is applied. In Step 3, a one-bit random number is generated in accordance with the Born rule. In the resetting case of Step 4, this process requires the same energy consumption when different quantum states are reset to the same initial state. Because QRNG has the same external operation, this RNG is seedless. Almost all QRNGs are experimentally implemented in quantum optics [12, 13]. However, the reset process is not considered. The violation of Bell inequality is related to the private randomness expansion, which means that a small private random seed can be expanded into a longer private random string [14]. This private randomness expansion was experimentally demonstrated [15]. By utilizing the loop-hole free Bell test, the private randomness expansion was experimentally performed [16, 17]. However, for any randomness expansion protocols, a one-bit random seed is required.

A quantum computer essentially becomes a QRNG as illustrated in Fig. 1. In a small-integrated quantum bit (qubit) machine, the quantum circuit corresponding to QRNG was run through the cloud service [18, 19, 20]. The generated output sequences were far from the ideal uniform RNG. However, a non-ideal output indicates the status of a quantum computer. As a simple hardware benchmarking, our QRNGs detected a temporal correlation [20]. Because the generated output comes from a quantum measurement for each qubit, which is subject to the Born rule, non-ideal output sequences still have a chance to be unpredictable. This verification on the unpredictability of the

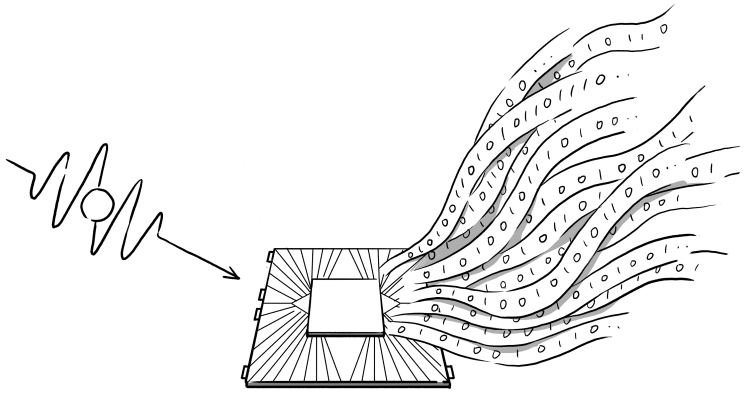

Figure 1: Schematic figure on quantum random numbers generated from a quantum computer.

generated sequences from a quantum computer strengthened the evidence on why nature is subjected to quantum mechanics.

# 3 Concluding Remarks

The history of random number generators can be traced back to the origin of digital computers, i.e., right from the time of ENIAC. Thus, there has always been a vicious circle of prediction and generation of random numbers. However, a PRNG is predictable. For the development of ultimate secure systems, an unpredictable RNG is required. A quantum random number generator (QRNG) is one such candidate. Verifying the unpredictable randomness of a QRNG is equivalent to answering the question on why quantum mechanics needs a probabilistic structure. Therefore, we have been pursuing QRNGs that are aimed for fundamental research as well as for practical applications. The quantum computers that were invented as a new computational paradigm in the year 1985 [2] can be called as QRNGs. However, the universal Turing machine cannot generate an unpredictable random bit. This clearly shows the advantage of a quantum computer as indicated in Ref. [21]. Moreover, we deduced that a QRNG does not need an integrated qubits machine. Therefore, we conclude with the following quote:

> A quantum random number generator is an ultimate application of a one-qubit quantum computer.

# References


[1] S. Tomonaga, *What is physics?* (Iwanami, Tokyo, 1979) [in Japanese].

[2] D. Deutsch, Proceedings of the Royal Society of London A **400**, 97 – 117 (1985).

[3] D. Deutsch, *The Beginning of Infinity* (Penguin, London, 2012).

[4] H. H. Goldstine, *The Computer from Pascal to von Neumann* (Princeton University Press, Princeton, 1980).

[5] R. Eckhard, Los Alamos Science Special Issue **15**, 131 – 141 (1987).

[6] M. Mazhdrakov, D. Benov, and N. Valkanov, *The Monte Carlo Method. Engineering Applications.* (ACMO Academic Press, Sofia, Bulgaria, 2018).

[7] J. von Neumann, Journal of Research of the National Bureau of Standards **3**, 36 – 38 (1951).

[8] O. Goldreich, *Modern Cryptography, Probabilistic Proofs and Pseudorandomness* (Springer-Verlag, Berlin, 1998).

[9] M. G. Kendall and B. B. Smith, Journal of the Royal Statistical Society **101**, 147 – 166 (1938).

[10] F. C. Williams and T. Kilbum, in AIEE-IRE'51, 57 – 61 (1951).

[11] D. P. DiVincenzo, Fortschritte der Physik **48**, 771 – 783 (2000).

[12] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, npj Quantum Information **2**, 16021 (2016).

[13] M. Herrero-Collantes and J. C. Garcia-Escartin, Reviews of Modern Physics **89**, 015004 (2017).

[14] R. Colbeck, *Quantum And Relativistic Protocols For Secure Multi-Party Computation*, Ph. D thesis, University of Cambridge (2006).

[15] S. Pironio, A. Acin, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, Nature **464**, 1021 – 1024 (2010).

[16] L. K. Shalm, Y. Zhang, J. C. Bienfang, C. Schlager, M. J. Stevens, M. D. Mazurek, C. Abellan, W. Amaya, M. W. Mitchell, M. A. Alhejji, H. Fu, J. Ornstein, R. P. Mirin, S. W. Nam, and E. Knill, arXiv:1912.11158.

[17] W.-Z. Liu, M.-H. Li, S. Ragy, S.-R. Zhao, B. Bai, Y. Liu, P. J. Brown, J. Zhang, R. Colbeck, J. Fan, Q. Zhang, and J.-W. Pan, arXiv:1912.11159.

[18] K. Tamura and Y. Shikano, in *Proceedings of Workshop on Quantum Computing and Quantum Information*, edited by M. Hirvensalo and A. Yakaryilmaz, TUCS Lecture Notes **30**, 13–25 (2019).

[19] K. Tamura and Y. Shikano, arXiv:1906.04410, accepted in *International Symposium on Mathematics, Quantum Theory, and Cryptography: Proceedings of MQC 2019*, edited by T. Takagi, M. Wakayama, K. Tanaka, N. Kunihiro, K. Kimoto, and Y. Ikematsu (Springer Nature, 2020).

[20] Y. Shikano, K. Tamura, and R. Raymond, *Detecting Temporal Correlation via Quantum Random Number Generation*, accepted in Electronic Proceedings in Theoretical Computer Science.

[21] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. S. L. Brandao, D. A. Buell, B. Burkett, Y. Chen, Z. Chen, B. Chiaro, R. Collins, W. Courtney, A. Dunsworth, E. Farhi, B. Foxen, A. Fowler, C. Gidney, M. Giustina, R. Graff, K. Guerin, S. Habegger, M. P. Harrigan, M. J. Hartmann, A. Ho, M. Hoffmann, T. Huang, T. S. Humble, S. V. Isakov, E. Jeffrey, Z. Jiang, D. Kafri, K. Kechedzhi, J. Kelly, P. V. Klimov, S. Knysh, A. Korotkov, F. Kostritsa, D. Landhuis, M. Lindmark, E. Lucero, D. Lyakh, S. Mandr'a, J. R. McClean, M. McEwen, A. Megrant, X. Mi, K. Michielsen, M. Mohseni, J. Mutus, O. Naaman, M. Neeley, C. Neill, M. Y. Niu, E. Ostby, A. Petukhov, J. C. Platt, C. Quintana, E. G. Rieffel, P. Roushan, N. C. Rubin, D. Sank, K. J. Satzinger, V. Smelyanskiy, K. J. Sung, M. D. Trevithick, A. Vainsencher, B. Villalonga, T. White, Z. J. Yao, P. Yeh, A. Zalcman, H. Neven, and J. M. Martinis, Nature **574**, 505 – 510 (2019).