MBNA Publishing House Constanta 2021

Proceedings of the International Scientific Conference SEA-CONF

SEA-CONF PAPER • OPEN ACCESS

An short analysis of modern methods in random number generators

To cite this article: V. CORNACIU, C. RĂCUCIU and L. ZISU, Proceedings of the International Scientific Conference SEA-CONF 2021, pg.224-232.

Available online at www.anmb.ro

ISSN: 2457-144X; ISSN-L: 2457-144X

doi: 10.21279/2457-144X-21-030

An short analysis of modern methods in random number generators

V Cornaciu[1] C Răcuciu[2] and L Zisu
[1]PhD Candidate, Military Technical Academy-Electronic, Information and Communications Systems for Defense and Security, George Coșbuc nr. 39-49, Bucharest, 050141, Romania.

[2]Prof. Eng. PhD, Titu Maiorescu University-Faculty of Computer Science, Văcărești nr. 187, Bucharest, 004051, Romania.

[3]PhD Candidate, Military Technical Academy-Electronic, Information and Communications Systems for Defense and Security, George Coșbuc nr. 39-49, Bucharest, 050141, Romania.

[1]veronica_zanfir@yahoo.com

[2]ciprian.racuciu@gmail.com

[3]liliana.zisu@ gmail.com

Abstract. The generation of random numbers at high speed and high security is at the heart of economic activities and is of great importance. Online trading and data encryption systems, computer telecommunications, online gambling, finance, among many others, are based on fast and secure random number generators. Usually, these generators are based on numerical algorithms that seemingly produce unpredictable number sequences, but the need for fast generation and the highest possible security of such sequences of numbers, made their design require more and more modern methods.In this article we will make a brief analysis of one of the newest method of generating random numbers, namely the quantum method. The main quantum generation technologies are reviewed, from the oldest ones that were based on radioactive degradation or noise to the modern ones that use quantum light.

Keywords. Random number generaton, quantum random generator, photons.

1. Introduction

With the rapid development of communication technology and the widespread use of the Internet and mobile networks, people have paid more and more attention to information security.

Over time, many methods and procedures have been used to make random number generators. Among these we mention: manual methods (use different devices such as: dice, ballot boxes, roulette, etc., but are rarely used in numerical simulation due to low speed), physical methods (based on analogies between some intrinsically random physical processes (radioactive processes, electronic processes generating white noise, etc.), memorization methods and analytical procedures (using recurrence relations). By far, the most studied were pseudo-random number generators (PRNGs).

PRNGs are based on deterministic functions that continuously update the current state of the PRNG, which leads to a succession of random states. Moreover, PRNGs are implemented in the

digital domain using computers or FPGAs; therefore, they can be engaged in high speed applications. However, in the digital world there are only a finite number of states that can be produced. For example, if the PRNG states are represented using k-bits, the PRNG will produce up to 2^k different random states and then repeat the same sequence again. To overcome this problem, PRNG designers need to increase the length of the period as much as possible. Consequently, much research has been conducted to find the appropriate state of the transition matrix that can cope with many state bits, k and maintain the maximum length period of 2^k. [33,34]

On the other hand, in order to obtain cryptographically secure PRNGs, it is convenient to generate truly random numbers that can ideally be obtained from intrinsically random or unpredictable processes. For this reason, researchers have increasingly focused on sources of entropy as unpredictable as possible.

Quantum mechanics offers interesting new protocols at the intersection of computer science, telecommunications, information theory and physics. Results such as protocols for quantum key distribution [2] and efficient algorithms for problems that are considered or known to be difficult for classical computers [6,10] shows that quantum physics can have a profound impact on how security, cryptography and computing can be thought of.

Although quantum technology has gained impressive momentum in recent decades, it is not yet possible to say that it is so developed for a universal quantum computer.

Among the quantum technologies that have registered a significant boom, we mention the distribution of quantum keys. In this sense, many systems have been developed, and some have even made their mark on the market [23,27].

Another technology that has gained momentum lately is that of quantum random number generators. QRNGs are devices that use quantum phenomena to generate random numbers and have applicability from stochastic simulation to cryptography.

Regardless of the field in which they are used and the technologies used for their production, random numbers generators have to accomplish some essential conditions with a higher or lower weight. These must pass the main statistical tests, must be robust from the cryptographic point of view, to have a relatively high generation speed and to generate a large quantity of random numbers. There are numerous studies in which different generators are analised, but only a few that propose a selection method of them. In [7], authors developed a multi-criteria evaluation procedure of pseudo-number generators to weigh them in relation to others and a method of determining the weight of each evaluation criterion.

The purpose of this article is to collect and present the most advanced protocols using quantum physics. The article is structured in three chapters. Chapter 2 presents the beginnings of quantum generators, namely those based on radioactive degradation or noise produced in various electronic devices. Section 3 discusses how the optics influenced QRNGs. Technologies such as branch paths, photon emission sources or Raman scattering are presented and are some of the most eloquent examples of such generators.

2. The beginnings of generators based on quantum phenomena

In the second half of the twentieth century, with the growing development of computer simulations, the need for random number generators appeared. It was therefore natural for researchers to turn to intrinsic sources of randomness. Some of these sources are radioactive degradation and noise sources. Geiger-Muller (GM) tubes being sensitive enough to capture and amplify α, β and γ radiation formed the basis of quantum random number generation technology.

The first QRNGs had a lot in common. Most used digital counters to convert pulses from the source into random numbers. Another method is to synchronize with a digital clock. The conversion into random numbers could be done in the following ways. For example, in the case of the generators in [15, 35] there is used a counter operated by a fast clock. It is read and reset to zero each time a number is received on the detector. However, the distribution of values is not uniform and a certain

correction is needed. This correction is made by taking the least significant figure in the case of Isida and Ikeda (1956) or by checking the parity of the number of pulses in the case of Vincent, 1970.

Another method used is to use a slow clock to determine when to read the counter. In the case of the generator from [28], the pulses in the GM detector increase the value of a counter. When the slow clock produces a new pulse, the counter value is used as a random digit and the count starts again from 0. The output corresponds to the number of particles counted in each clock period.

Radioactive decay has also been used to generate white noise for analog computers [14, 20]. They have been used in aircraft design simulation, in communications and in simulation problems that require broadband signal. The pulses in the GM detector trigger a change in state in the voltage signal. If a particle is detected, the signal goes from high to low voltage, or vice versa, and the signal is directed to a low-pass filter to complete the noise generator.

The initial concepts were later improved and are still in use. We mention here the case of the Walker generator [36], which has been operating since 1996. The operating principle consists in comparing the times between two consecutive pulses with the times between the previously generated pulses and changing the generation criterion for each pair of times in order to compensate for small biases. systemic that could favor slightly unbalanced intervals.

Figure 1 provides a graph of the method description.

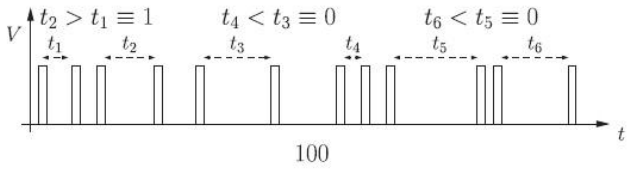

Figure 1: Time difference method

More recently, Geiger counters have been replaced by semiconductor detectors. Semiconductor detectors are convenient because they do not require the same high voltage as Geiger tubes. Also, the use of semiconductor devices in a very wide range on the market, greatly simplifies the design of these types of generators. In the case of the generator from [1] the system reads a fast clock every time a pulse arrives. If the clock is in a high state (in the high voltage level of the clock cycle) on arrival, the generator output a 1. If it is in a low state, it output a 0.

QRNGs based on radioactive degradation offer a good way to obtain high quality random numbers, but they have many disadvantages. One of them is the rather low bit generation rate. Another problem is the need for a radioactive source. Natural sources of radiation are extremely limited and radioactivity must be very high. For this reason, the revised QRNGs use highly radioactive materials. We mention cobalt-60 ([15]), strontium-90 ([28]), cesium-137 ([36]), americium-241 ([1]) or nickel-63 ([8]). However, the use of these types of materials requires improved handling measures and the integration of various computers. Another disadvantage is that of downtime. Dead time is the minimum time required for the GM tube to regain its full detection capability and can range from tens of nanoseconds to a few microseconds. This limits the counting rate to the MHz range. Semiconductor detectors must also complete the carriers after each detection and have downtime in the microsecond interval. Another disadvantage of these types of generators is that they suffer large material losses due to radiation.

Another preferred source of entropy generators of classical physical random numbers is the noise in electronic circuits. The noise source is usually a resistor, but other elements can take its place. For example, the integration of a Zener diode into the reverse fault region is an extremely popular choice. The generation of random bits is done by comparing the voltage fluctuations with a certain threshold.

Generators [13] and [24] use two types of noise sources. These are shot noise known as Schottkz noises and thermal noise or Johnson-Nyquist noises. In practice, both noises tend to occur side by side

and are difficult to isolate. In many cases, the boundary between Schottky and thermal fluctuations is blurred [18].

3. Modern technologies of quantum number generators

Most existing QRNGs are based on quantum optics. The main reason is that randomness is present in many of the parameters of quantum light states. We find sources of randomness in the light emitted by diodes, laser light or in photon sources. Of the multitude of quantum states of light, Fock states and coherent states are the most relevant for generating random numbers.

The main interest is to produce unique uncorrelated photons. There are many technologies for their production and detection[3, 9]. Among these detectors we mention those from[12, 21]. For all these types of detectors, the decision of the existence of the photon is simple. The main problems that these detectors face are their high cost due to the fact that most use applications for photon detection and the fact that it takes time to recover after a detection. All of these limitations affect quantum random number generators.

3.1. Branching path generators

A first subcategory of quantum optical generators is that of generators that use photon measurements to overlap two or more paths.

For example, if we define a state $|1\rangle_1 |0\rangle_2$ that represents a photon in the first of the two possible paths and a state $|0\rangle_1 |1\rangle_2$ with the photon in the second path, we can perform a superposition

$$\frac{|1\rangle_1 |0\rangle_2 + |0\rangle_1 |1\rangle_2}{\sqrt{2}}$$

Conceptually, the easiest way to produce random numbers through this path division is to place two detectors D_0 and D_1, one for each output and generating a bit each time a photon is detected. Clicks in D_0 would produce a 0 bit and clicks in D_1 would produce a 1, as is shown in Figure 2.

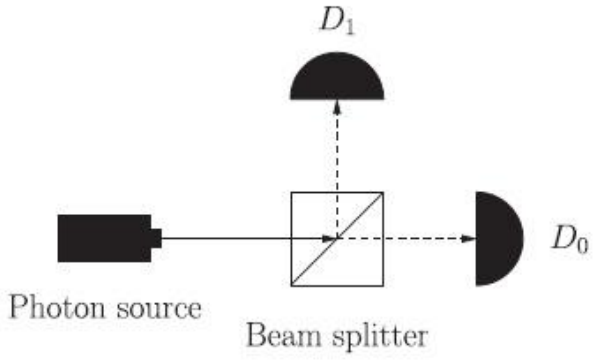

Figure 2. Conceptual representation of quantum measurements with detectors in various positions

In [39], the authors used as a polarization alternative to path conversion a weak laser source with a single-photon attenuated linear polarization and a Fresnel prism separating the positive and negative circular polarization components, to direct them to two avalanche photodiodes. If an electronic device is introduced to control the polarization of the source, the generator can be adjusted to produce the desired probabilities for each bit value as in [40].

Another example is the generators in [29] and [30] implemented in fiber optic systems. They use a laser source that produces a coherent state with an amplitude greater than 1, that maximizes the rate of random bit generation.

The main problem of QRNGs with optical branching pathways is downtime after a click. This can cause mismatches between neighboring bits. Other shortcomings can occur due to afterpulsing which can create correlated bits, pulses with more than one photon can produce simultaneous detections or there can be cycles without photons. All this leads to the limitation of the generation rate to a few Mbps. Counteracting these problems can be done in several ways. The generator in [16] includes a configuration phase in which the tube voltage and threshold detection of photodetectors can be adjusted to compensate for detection efficiency and path coupling differences or by applying an unbiased algorithm that distills a random sequence at the cost of losing a few bits.

The problem of differences in efficiency in photon detection can be avoided by converting path superpositions into time superpositions as in[31].

The generation rate can also be improved if the generator measures several possible paths. This approach requires more complex devices, but optical circuits integrated in silicone chips can be an economical option. The generator case in [11] offers a variant of an integrated generator with eight outputs that can produce three bits per measurement, with the possibility of expansion to 16 outputs.

Another problem is choosing the photon source. In most cases, the photons come from LEDs or low laser light. Recent studies have shown that light sources have a faster photon rate and under these conditions single photon sources provide the fastest bit generation [22].

3.2 Photon count generators

Another category of quantum generators is that represented by those that count the number of photons that arrive in a certain period of time. If T it is the respective period of time then the number of photons arriving in time T respects a Poisson distribution given by

$$P(n) = \frac{(\lambda T)^n}{n!} e^{-\lambda T}$$

In the generator [19] the least significant bit in the photon count is counted, and the thermal and poorly coherent sources are compared.

Another approach is to compare the number of photons resulting at different times. If n_1 and n_2 represents the number of photons resulting at two consecutive time points, by comparison $n_1 > n_2$ a 1 can be generated and a 0 otherwise, as it happens in the case of the generator [25] .

However, there are generators that assign more bits per detection depending on the number of photons resulting. The obtained results are grouped in sets with equal probabilities, this requiring the adjustment of the level of photons produced [17].

Depending on the rate of photons resulting in the time period T , it is possible that the second, third or least significant bits are evenly distributed. On this principle it is baset the generator in [32] wich is integrated into a CMOS chip based on an array of single-photon avalanche diodes (SPADs) and digital counters. The device is made of an array of independent cells, each containing a single photon avalanche diode, a sensing front-end and a digital counting electronics. The QRNG produces up to 200 Mb / s.

Other types of generators use common everyday devices. In [26] a quantum random number generator is created using as a light source the camera integrated in a mobile phone. A randomness extractor is used to eliminate correlations and noise effects.

In [37,38,41] a number of three quantum number generators are produced in which photon counting involves taking bins of length T and divided into smaller bins containing 0 or 1 photon and the use of procedures to transform large non-uniform Poisson bins into a uniform random variable.

3.3 Raman scattering based generators

Another source of randomness is given by the interaction between photons and quantum vibrational states of certain materials. The phenomenon of Raman scattering is used to obtain

random bits. In Raman scattering, two effects are important. One is that of spontaneous Raman scattering (SpRS), where a photon is scattered when it interacts with molecular lattice that absorbs or creates a photon to produce a photon with a higher or lower frequency, and the second effect is stimulated Raman scattering, (SRS), where a photon with a certain frequency corresponds to the energy difference between a photon pump and the matching phonon in a spontaneous Raman scattering event stimulates the production of a new photon of the same frequency.

Raman scattering has a couple of important effects. One of them is spontaneous Raman scattering (SpRS) where a photon is scattered when it interacts with a molecular lattice that absorbs or creates a phonon to produce a new photon of a higher or lower frequency. If the wavelength of the scattered photon is larger and the energy difference is converted into a photon we speak of a Stokes photon. If there is an energy gain and an incoming photon and an existing phonon produce a scattered photon of a smaller wavelength we speak of an anti-Stokes photon.

A first approach to these types of effects is in [4] . Here is created a quantum random number generator based on the phase measurement of Stokes light generated by amplification of zero-point vacuum fluctuations using stimulated Raman scattering. A pump pulse is focussed into a 3 mm CVD diamond plate, generating a Stokes field with random phase. The pump field is filtered out using a bandpass filter, leaving only the Stokes field which is then combined with a reference pulse at a beamsplitter. A small lateral tilt is introduced and an interferogram is then measured using a linear CCD array, as seen in Figure 3.

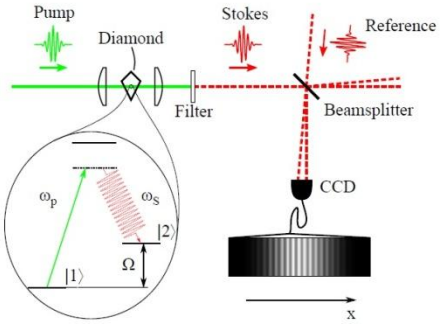

Figure 3: Schematic diagram of Busterd random number generator 2011

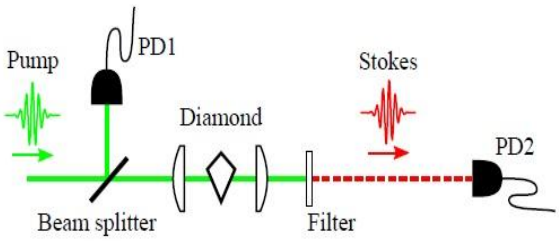

Figure4: Schematic diagram of Busterd random number generator 2013

However, there is a problem with this generator. Power fluctuations in the pump pulses can mask the quantum effect that want to be measure. The subsequent variant of this generator [5] solved this problem. The pump pulse is focussed into a diamond plate, generating a Stokes sideband by SISRS. The Stokes pulse is spectrally-filtered from the pump, and its energy is measured by PD2 photodiode. Part of the pump pulse energy is separated using a beamsplitter in front of the diamond, and is measured by photodiode PD1 (figure 4). In order to extract the entropy, the measured intensity values are corrected with the power values of the monitored reference and the compensated amplitude measurements are binned into intensity ranges that are assigned a bit string. As a last step, the sequence is applied Toeplitz hashing to remove bias and classical noise.

Most generators that use single photon detectors are limited to a few MHz. Current technologies can bring the rate close to the physical Raman limit. One of these technologies uses the division of the spectrum into at least two channels, thus obtaining more than one bit per measurement.

Conclusion

In this article we have tried to present some of the main technologies used in quantum number generators. However, their list is much larger and constantly expanding.

Quantum random number generators are some of the most widely used and mature technologies today. From the use of radioactive degradation or noise in various electronic devices to those with branching paths, photon emission sources or Raman scatering, quantum mechanics offers multiple paths for generating random bits. There has come a time when megabyte generation rates per second are commonplace. Moreover, the era of random number generation at very high speeds and at high capacities is booming. The era of generators using laser-based entropy has begun. In february 2021, a team of international scientists has developed a laser that can generate 254 trillion random digits per second, more than a hundred times faster than computer-based random number generators (RNG). It can generate 250 terabytes of random bits per second. In fact, it was so fast that the team behind it struggled to record its output using a high-speed camera. According to the researchers, their system trumps physical random number generators both in speed and through its ability to create many bitstreams simultaneously.

References

[1] Alkassar A., Nicolay T., Rohe M., *Obtaining true-random binary numbers from a weak radioactive source*, Computational Science and Its Applications—ICCSA 2005, Pt II, Lecture Notes in Computer Science, Vol. 3481 (Springer, Berlin), pp. 634–646, 2005.

[2] Bennett C. H., Brassard G., *Quantum cryptography: Public key distribution and coin tossing*, in Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India (IEEE, New York), pp. 175, 1984.

[3] Buller G. S., Collins R. J., *Single-photon generation and detection*, Meas. Sci. Technol. 21, 2010.

[4] Bustard P. J., Moffatt D., Lausten R., Wu G., Walmsley I. A., Sussman B. J., *Quantum random bit generation using stimulated Raman scattering*, Opt. Express 19, 25173–25180, 2011.

[5] Bustard P. J., et all *Quantum random bit generation using energy fluctuations in stimulated Raman scattering*, Opt. Express 21, 2013.

[6] Childs A. M., W. van Dam, *Quantum algorithms for algebraic problems*, Rev. Mod. Phys. 82, 1–52, 2010.

[7] Cornaciu V., Răcuciu C., *Multi-criteria method for evaluation of the pseudorandom number generators using thermodynamic systems behaviour*, Mircea cel Batran Naval Academy Scientific Bulletin **22(2)** pp. 305-312, 2019.

[8] Duggirala R., Lal A., Radhakrishnan S., *Radioisotope Decay Rate Based Counting Clock*, in MEMS Reference shelf 6 (Springer-Verlag, New York), pp. 127–170, 2010.

[9] Eisaman M. D., Fan J.,Migdall A. L., Polyakov S. V., *Single-photon sources and detectors*, Rev. Sci. Instrum. 82, 2011.

[10] Ekert, A. K., Jozsa R., *Quantum computation and Shor's factoring algorithm*, Rev. Mod. Phys. 68, 733–753, 1996.

[11] Gräfe M., et all, , *On-chip generation of high-order single-photon W-states*, Nat. Photonics 8, 791–795, 2014.

[12] Hadfield R. H., *Single-photon detectors for optical quantum information applications*, Nat. Photonics 3, 696–705, 2009.

[13] Holman W. T., Connelly J. A., Dowlatabadi A. B., *An integrated analog/digital random noise source*, IEEE Trans.Circuits Syst. I 44, 521–528, 1997.

[14] Howe R. M., *Design fundamentals of analog computer components* (Van Nostrand, Princeton, NJ) , 1961.

[15] Isida, M., H. Ikeda, *Random number generator*, Ann. Inst. Stat. Math. 8, 119–126, 1956.

[16] Jennewein T., Achleitner U., Weihs G., Weinfurter H., Zeilinger A., *A Fast and Compact Quantum Random Number Generator*, Rev. Sci. Instrum. 71, 1675–1680, 2000.

[17] Jian Y., Ren M., Wu E., Wu G., Zeng H., *Two-bit quantum random number generator based on photon-numberresolving detection*, Rev. Sci. Instrum. 82, 2011.
[18] Landauer R., *Solid-state shot noise*, Phys. Rev. B 47, 16427–16432, 1993.
[19] Lopes Soares, Mendonça E., F. A., Ramos R. V., *Quantum Random Number Generator Using Only One Single-Photon Detector*, IEEE Photonics Technol. Lett. 26, 851–853, 2014.
[20] Manelis B., *Generating random noise*, Electronics 8, 66–69, 1961.
[21] Marsili F., et all., *Detecting single infrared photons with 93% system efficiency*, Nat. Photonics 7, 210, 2013.
[22] Oberreiter L., Gerhardt I., *Light on a beam splitter: More randomness with single photons*, Laser Photonics Rev. 10, 108–115, 2016.
[23] Peev M., et al., *The SECOQC quantum key distribution network in Vienna*, New J. Phys. 11, 2009.
[24] Petrie C. S., Connelly J. A., *A noise-based IC random number generator for applications in cryptography*, IEEE Trans. Circuits Syst. I 47, 615–621, 2000.
[25] Ren M., et all, *Quantum random-number generator based on a photon-numberresolving detector*, Phys. Rev. A 83, 2011.
[26] Sanguinetti B., Martin A., Zbinden H., Gisin N., Quantum Random Number Generation on a Mobile Phone, Phys. Rev. X 4, 2014.
[27] Sasaki M., et al., *Field test of quantum key distribution in the Tokyo QKD Network*, Opt. Express 19, 2011.
[28] Schmidt, H., 1970b, "Quantum Mechanical Random Number Generator," J. Appl. Phys. 41, 462–468.
[29] Soubusta J., Haderka O., Hendrych M., *Quantum random number generator*, in Proc. SPIE, 12th Czech-Slovak-Polish Optical Conference on Wave and Quantum Aspects of Contemporary Optics, Vol. 4356 (SPIE–International Society for Optical Engineering, Bellingham, WA), pp. 54–60, 2001.
[30] Soubusta J., Haderka O., Hendrych M., Pavlicek P., *Experimental realization of Quantum random number generator*, in Proc. SPIE, 13th Czech-Slovak-Polish Optical Conference on Wave and Quantum Aspects of Contemporary Optics, Vol. 5259 (SPIE–International Society for Optical Engineering, Bellingham, WA), pp. 7–13, 2003.
[31] Stefanov A., Gisin N., Guinnard O., Guinnard L., Zbinden H., *Optical quantum random number generator*, J. Mod. Opt. 47, 595–598, 2000.
[32] Tisa S., Villa F., Giudice A., Simmerle G., Zappa F., *High-Speed Quantum Random Number Generation Using CMOS Photon Counting Detectors*, IEEE J. Sel. Top. Quantum Electron.21, 23–29, 2015.
[33] Thomas DB, Luk W.,*High quality uniform random number generation using LUT optimised state-transition matrices*, Journal VLSI Signal Process; 47(1). 2007,
[34] Thomas DB, Luk W., The *LUT-SR family of uniform random number generators for FPGA architectures*, IEEE Trans Very Large Scale Integr (VLSI) Syst, 21(4): 761-770, 2013.
[35] Vincent C. H., *The generation of truly random binary numbers*, J. Phys. E 3, 594, 1970.
[36] Walker J., *HotBits: Genuine random numbers, generated by radioactive decay*, http://www.fourmilab.ch/hotbits/, 1996.
[37] Wang F.-X., et all, *Robust quantum random number generator based on avalanche photodiodes*, J. Lightwave Technol. 33, 3319–3326, 2015.
[38] Wang J.-M., et all, *A Bias-Free Quantum Random Number Generation Using Photon Arrival Time Selectively*, IEEE Photonics J. 7, No. 2, 1–8, 2015.
[39] Wang P. X., Longo G., Li Y. S., *Scheme for a quantum random number generator*, J. Appl. Phys. 100, 2006
[40] Xu, M., et all, Adjustable unbalanced quantum randomnumber generator, Chin. Optic. Lett. 13, 2015.
[41] Yan Q., Zhao B., Hua Z., Liao Q., Yang H., *High-speed quantum-random number generation*

by continuous measurement of arrival time of photons, Rev. Sci. Instrum. 86, 2015.