(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 December 2006 (21.12.2006)

PCT

(10) International Publication Number
WO 2006/133650 A1

(51) International Patent Classification:
G06F 7/58 (2006.01)

(21) International Application Number:
PCT/CN2006/001361

(22) International Filing Date: 16 June 2006 (16.06.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/691,510 16 June 2005 (16.06.2005) US

(71) Applicant *(for all designated States except US)*: **THE CHINESE UNIVERSITY OF HONG KONG** [CN/CN]; Shatin, N. T., Hong Kong (CN).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **LUO, Yuhui** [CN/CN]; 213# Zhongshan Beilu, Hengyang Hunan 421001 (CN). **CHAN, Kam Tai** [CN/CN]; Flat A, 2/f, Block 22 Greenwood Terrace, 26 Sui Wo Road, Shatin, N.t., Hong Kong (CN).

(74) Agent: **INSIGHT INTELLECTUAL PROPERTY LIMITED**; 19a, 19b, Tower A, Indo Building, No. 48a Zhichun Road, Haidian District, Beijing 100098 (CN).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

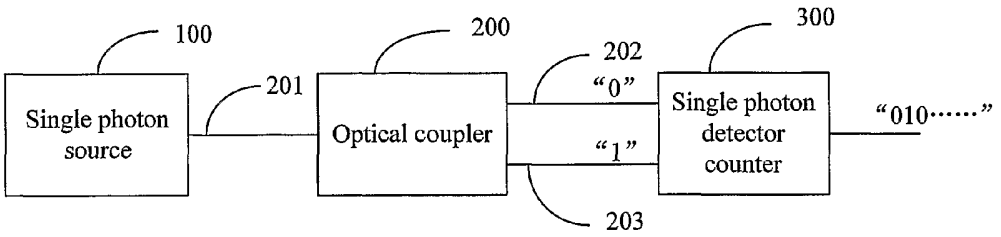
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaration under Rule 4.17:
— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) **Title:** QUANTUM RANDOM NUMBER GENERATORS



(57) **Abstract:** Disclosed is an all-fiber optical quantum random number generator, an optical coupler having an input port and two output ports; a single photon source connected to the input port, emitting a single photon which is transmitted from the input port to the output ports; a single photon detector connected to each of the two output ports, detecting the photon coming out from either of the output ports; and means for generating random numbers according to the detection result of the single photon detector. The generator of the invention can generate truly random numbers.

WO 2006/133650 A1

QUANTUM RANDOM NUMBER GENERATORS

[0001] This application claims the benefit of U.S. provisional patent application No. 60/691,510 filed June 16, 2005 which is explicitly incorporated by reference in its entirety.

FIELD OF THE INVENTION

[0002] The invention relates to a random number generator. More specifically, the invention relates to a random number generator based on quantum optics.

TECHNICAL BACKGROUND OF THE INVENTION

[0003] A random number is a number generated by a process, whose outcome is unpredictable, and which cannot be reproduced. Random numbers are very useful in computer science and engineering, communications, information security, reliability test of communications systems, and other applications. In engineering, random numbers are always used to test the reliability of a system. The quality of test random numbers determines the reliability of the system. Also, in the field of information security, the quality of random numbers is a key factor for the whole security.

[0004] There exist two main types of random number generators, one of which is a software-based generator. From a general point of view, the software generator produces so-called pseudo-random numbers because the sequence produced by an algorithm is always periodic. Although the pseudo-random numbers have been used in some applications, they are not qualified to be used in most applications where randomness requirements are strict.

[0005] Another type is a physical (both classical and quantum physics) random number generator. Macroscopic processes described by classical physics can be used to generate random numbers. Ostensibly random numbers can be generated using "noise" created by minor fluctuations in electronic circuits. It is disputed whether such electronic noise devices generate true random numbers. Determinism is hidden behind complexity. Unfortunately, they are often innately slower than pseudo-random number generators, rendering them unsuitable for any application where a substantial quantity of random numbers is required. Another drawback of the noise-based random number generators is that

it is difficult to ensure that the system does not interact with environmental parameters like the ambient temperature or an electromagnetic field. Electronic noise devices can become unstable over time.

[0006] Recently, a method for generating random numbers based on quantum physics has gained importance. Contrary to classical physics, quantum physics is fundamentally random. It is the only theory within the fabric of modern physics that integrates randomness. This fact was very disturbing to physicists like Einstein who invented the quantum theory of light. Truly random numbers can be generated by monitoring the radioactive decay of radioactive elements. Although such a method based on quantum physics can produce random numbers of excellent quality, such generators are not suitable for commercial applications.

[0007] A spin-off company from the University of Geneva, id Quantique, has marketed a quantum mechanical random number generator based on quantum physics. The randomness is guaranteed by the random behavior of single 'light particles', called photons, hitting a semi-transparent mirror. A photon generated by a source beamed to a semi-transparent mirror is reflected or transmitted with 50 percent probability, and these measurements can be translated into a string of quantum random bits. However, it is a little difficult to align the semi-transparent mirror to a detector. Another drawback is the difficulty to integrate with other devices or components and thus it is difficult to reduce the component size and cost.

SUMMARY OF THE INVENTION

[0008] An object of the present invention is to provide an all-fiber optical random number generator for generating true random numbers by using the random behavior of single photons.

[0009] The random number generator of the invention comprises an optical coupler having an input port and two output ports; a single photon source connected to the input port, emitting a single photon which is transmitted from the input port to the output ports; a single photon detector connected to the output ports, detecting the single photons coming out from either of the output ports; and a device generating random

numbers according to the detection result of the single photon detector.

[0010] The present invention further provides a method for generating random numbers, which comprises generating a string of single photons; coupling the single photons into an optical coupler having two output ports; detecting the single photons coming out from either of the output ports; and generating random numbers according to the detection result.

[0011] The random number generator of the present invention is implemented by all-fiber devices, such as fibers, a variable optical attenuator, a laser and a single photon detector all with fiber connectors, and an optical fiber coupler, which is really simple, inexpensive, reliable and effective. Moreover, it is convenient to connect all the above optical devices by using fiber connectors only and without any need of using lenses or mirrors and complicated procedures for optical alignment.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] FIG. 1 shows the principle of the quantum random number generator according to the invention; and

[0013] FIG. 2 schematically shows an embodiment of the random number generator of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0014] It is known for those skilled in the art that the quantum system is of random property. This property is intrinsic, which can be employed to design a true random number generator.

[0015] As shown in Fig. 1, the random number generator according to an embodiment of the present invention includes a single photon source 100, an optical coupler 200 having an input port 201 and two output ports 202 and 203, and a single photon detector counter 300.

[0016] The single photon source 100 is employed to generate a string of single photons. The single photons are launched into the input port 201 of the optical coupler 200, one by one. The optical coupler 200 is a conventional optical fiber coupler

which has a split ratio of 50:50. The single photon from the single photon source 100 is transmitted from the input port 201 of the coupler 200 to either one of the output ports of the coupler 200. The single photon detector counter 300 is connected to the output ports to detect the photon coming out from either of the output ports. As shown in Fig. 1, a single photon coming out from the output port 202 can be assigned to represent "0" and a single photon coming out from the output port 203 can be assigned to represent "1". The opposite assignment is also valid. In this way, it is possible to obtain true random numbers by using the random behavior of single photons.

[0017] As stated above, each of the two output ports 202 and 203 has an identical probability for the single photon to leave. The optical coupler of the invention allows that the single photon entering the optical coupler has the same probability (50:50) to leave from the port 202 or port 203.

[0018] For port 202, the state can be expressed by

$$|\Psi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad (1)$$

where $|0\rangle$ represents there is no photon coming out from port 202, and $|1\rangle$ represents one photon coming out from port 202.

[0019] The detection result at port 202 is discrete, so the mechanism can generate a discrete random number string if a single photon string is launched into the input port continuously. The result measured at port 203 is complementary to that at port 202. For the generator as discussed above, the total state at ports 202 and 203 can be described by Equation (2)

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle + |1\rangle|0\rangle) \qquad (2).$$

[0020] Equation (2) represents an entangled state.

[0021] From the above-mentioned principle, the quantum system of random property can be easily realized by a single coupler with one input port and two identical

output ports with fiber pigtails and connectors. The random number generator of the present invention is further described with reference to FIG. 2.

[0022] FIG. 2 shows another embodiment of the random number generator of the present invention.

[0023] As shown in Fig. 2, the random number generator of the invention comprises a single photon source which can be implemented by a laser 10 and a variable optical attenuator (VOA) 20; a 50:50 optical fiber coupler 30 including an input port 31 and two output ports 32 and 33; a first Single Photon Detector (SPD) 40 connected to optical coupler 30 via port 32; a second Single Photon Detector (SPD) 60 connected to optical coupler 30 via port 33; and means 50 for generating random numbers from the detection result of the Single Photon Detectors 40 and 60.

[0024] Alternatively, for the single photon source, those that emit exactly one photon per pulse may be available at visible and near-IR wavelengths in the future. Spontaneous parametric down conversion can also be used to create a source of single photons.

[0025] In some embodiments of the invention, the coupler 30 can be implemented by a waveguide or an optical fiber coupler.

[0026] In other embodiments of the invention, the SPD 40 or SPD 60 can be implemented by a semiconductor detector, a charge-coupled device sensor or a photomultiplier tube detector.

[0027] In the invention, the laser 10 emits a beam of light, which is attenuated into a single photon in a measured interval at the VOA 20. The single photon is launched into the input port 31 of the 50:50 coupler 30. After that, the single photon has the same probability to leave the coupler from either the port 32 or port 33. Therefore, the probability of detecting a single photon by the SPD 40 or 60, at either port 32 or port 33, respectively, is 50%, and so is the probability of detecting no photon. Therefore, the outcomes detected at port 32 are intrinsically and hence truly random. For the measurement outcomes at port 33, the bits are complementary to those at port 32, as discussed in above, and are therefore also truly random.

[0028] According to the present invention, the random number generator is

implemented by generating single photons and then propagating them inside a fiber, a fiber coupler and other components that have fiber connectors, which is simple, inexpensive, reliable and effective. Moreover, because of the use of the fiber devices, it is convenient to connect to the single photon detectors just by using fiber connectors, without the need of using lenses or mirrors and complicated procedures for optical alignment.

[0029] In a specific embodiment of the invention, the single photon detectors 40 and 60 are cooled at -51°C and work at a gated mode. The wavelength of the laser employed is around 1550nm. The detection efficiency of the SPDs is more than 10%. A continuous wave conventional laser light beam is attenuated into single photon strings in order to obtain statistical single photons. The count in the measured interval (preferably, is 0.2ns) is less than 0.1 so as to guarantee that statistical single photons can be obtained.

[0030] An NIST test issued by National Institute of Standards Technology is conducted to check the random property of the data obtained by the generator of the present invention. The NIST statistical test suite for random number generators offers a battery of 16 statistical tests. These tests assess the presence of a pattern which, if detected, would indicate that the sequence is non-random. The properties of a random sequence can be described in terms of probability. In each test, a probability, called the P-value, is extracted. This value summarizes the strength of the evidence against the perfect randomness hypothesis. A P-value of zero indicates that the sequence appears to be completely non-random. A P-value larger than 0.01 means that the sequence is considered as random with a confidence of 99%. Here only one method is used to check the experimental data.

[0031] In the test method as mentioned above, the length of the sequence is selected as n = 3724 (which is larger than 100). For example, the sequence is below:

0 1 0 1 0 1 0 0 1 0 0 1 0 1 0 0 1 0 1 0

1 0 0 1 0 1 0 1 0 0 0 1 0 0 0 1 0 0 1 0

1 0 1 0 1 0 1 0 1 0 1 1 0 1 0 0 0 1 0 1

1 0 1 1 0 0 1 1 0 1 1 0 1 0 1 1 0 1 0 1

0 1 1 0 1 0 0 1 0 0 1 0 0 1 1 0 0 1 0 0

0 0 1 0 1 0 1 0 1 0 1 0 1 1 0 0 1 1 1 0

1 0 1 0 0 0 0 1 0 1 1 0 0 0 0 1 0 1 1 0

1 0 0 1 0 0 1 0 1 0 0 0 0 1 0 1 0 1 0 1

0 1 1 0 1 0 0 0 1 0 1 0 0 0 1 0 0 0 0 1

0 1 0 1 0 0 1 1 0 1 1 0 1 0 1 0 1 0 1 0

1 0 1 1 0 1 0 1 1 0 1 1 0 0 1 0 0 1 0 1

0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1

0 1 0 1 0 0 1 0 0 1 1 0 1 1 0 1 1 0 1 0

1 1 0 1 1 0 1 0 0 1 0 1 0 1 1 0 1 0 0 1

0 1 0 1 1 0 1 1 0 1 0 0 1 0 1 0 1 0 1 1

0 1 0 0 1 0 1 0 1 0 1 0 0 0 1 1 0 1 0 0

1 0 1 0 1 0 0 0 1 1 0 1 0 1 0 1 0 1 0 0

1 1 0 0 1 0 1 0 1 1 0 1 0 1 0 1 0 1 0 1

0 0 0 0 1 1 0 1 0 1 0 1 0 1 0 1 0 1 0 0

1 0 1 0 1 0 1 0 1 0 1 0 1 1 0 0 1 0 1 0

0 1 1 0 0 0 0 1 0 1 1 0 1 0 1 0 1 1 0 1

1 0 1 0 1 1 0 1 0 1 0 1 0 0 1 0 1 0 1 1

0 1 0 1 0 1 0 1 0 1 1 0 1 1 0 1 1 0 0 1

1 0 0 1 0 0 0 1 1 1 0 1 0 1 1 0 1 0 1 0

1 0 1 0 0 1 1 0 0 0 0 0 1 0 1 0 0 1 1 0

1 0 0 1 1 0 1 1 0 1 1 1 0 1 0 1 0 1 0 1

0 0 0 1 0 1 0 1 0 1 0 1 0 1 1 1 0 1 0 1

0 0 1 0 1 0 0 1 0 1 0 0 1 1 0 1 0 0 0 1

0 1 1 0 1 0 1 0 1 0 1 0 0 1 0 0 0 1 1 0

1 0 1 0 0 1 1 1 0 1 0 1 0 1 1 0 1 0 1 0

1 0 0 1 1 0 1 0 1 0 1 0 1 1 0 1 0 1 0 1

1 0 0 1 0 1 0 1 0 1 0 1 0 1 0 0 1 1 0 1

0 1 1 0 0 1 0 0 1 0 1 0 1 0 1 1 0 1 0 1

1 1 0 0 0 1 1 0 0 1 1 0 1 0 1 0 1 0 1 0

1 0 1 1 0 0 1 1 0 1 0 1 0 1 0 1 1 1 0 1

0 1 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 0 1

0 1 0 1 0 1 0 1 1 0 1 1 0 1 0 1 0 0 1 0

1 0 1 1 0 0 1 0 0 1 0 0 0 1 0 1 0 1 1 1

0 1 0 0 1 0 1 0 1 0 1 0 1 0 1 1 0 1 1 0

1 0 1 0 0 0 1 0 1 1 1 0 0 1 0 0 0 1 1 1

0 1 1 0 1 1 1 0 0 0 1 0 0 1 0 1 1 0 1 0

1 1 0 0 1 0 1 0 1 0 0 1 1 1 0 1 0 1 0 0

1 0 1 1 1 0 1 0 1 1 0 1 0 0 1 0 1 0 1 1

0 1 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 1

0 0 1 1 0 1 0 0 1 1 0 1 1 0 1 1 1 0 1 1

0 1 1 0 1 0 0 0 1 0 0 1 0 1 0 1 0 1 1 0

0 1 0 1 0 1 1 1 0 1 0 1 0 0 1 1 1 0 1 0

0 1 0 1 0 1 1 1 1 0 0 1 0 1 0 1 1 1 0 1

0 1 0 1 0 0 1 0 1 0 1 1 1 0 0 1 0 1 0 1

0 1 0 1 1 0 1 0 1 0 1 0 1 0 1 1 0 1 0 1

0 1 0 1 1 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1

1 0 1 0 1 1 0 1 0 1 0 0 1 1 0 1 0 1 0 1

0 1 1 1 0 0 1 0 0 0 0 1 0 1 1 0 1 1 0 1

0 1 0 1 1 0 1 0 1 0 0 1 0 1 1 0 0 0 0 1

1 0 0 0 0 1 0 1 0 1 0 0 1 0 1 0 0 1 0 1

0 0 1 0 1 0 1 1 0 1 0 1 0 1 0 1 1 1 0 1

1 0 0 1 0 1 0 1 1 0 1 1 0 1 0 1 1 0 1 0

1 1 0 1 0 1 0 0 1 1 0 0 1 1 0 1 1 0 1 0

1 0 1 0 1 0 1 0 1 0 1 0 1 1 0 1 0 0 0 1

0 1 0 1 0 1 1 0 0 1 0 0 0 1 0 1 0 0 1 0

1 1 0 1 0 1 1 0 1 1 0 1 1 0 0 1 0 1 1 0

0 1 1 1 0 1 0 1 0 1 0 0 1 0 1 0 0 1 0 1

0 0 1 0 0 1 0 1 0 0 1 0 1 0 0 1 1 1 0 1

0 1 0 0 1 0 1 1 0 1 0 1 1 1 0 0 1 1 1 0

1 1 0 1 0 1 0 1 0 1 1 0 1 1 1 0 1 0 0 1

0 1 1 0 1 0 1 0 0 1 0 1 0 1 0 0 1 0 1 1

1 0 0 0 0 1 0 1 0 1 1 0 1 0 1 0 1 0 1 0

1 0 0 1 0 1 0 0 0 1 0 1 1 0 1 0 1 0 1 1

0 1 1 0 1 1 0 1 0 1 0 1 0 0 1 0 1 0 1 0

1 0 1 0 0 1 0 1 1 1 0 1 1 0 1 1 0 1 1 0

1 0 0 0 1 0 1 0 1 0 1 1 0 1 0 1 0 1 0 1

0 0 1 0 1 0 1 1 0 1 0 1 0 0 1 0 1 0 1 0

1 1 0 0 1 0 0 1 0 1 0 0 1 1 0 0 1 1 1 0

0 1 0 1 1 0 1 0 0 1 1 1 0 1 0 1 0 1 1 0

1 1 0 1 0 1 0 0 0 1 1 0 1 0 1 0 0 1 0 1

0 1 0 1 0 1 0 0 1 0 1 0 1 0 1 0 1 0 1 1

0 1 1 0 1 0 1 0 0 1 1 0 1 0 1 0 1 0 1 0

1 0 0 1 0 1 1 0 1 1 1 0 0 1 0 1 0 1 0 0

1 1 0 1 0 1 0 1 1 0 1 1 0 1 0 1 0 1 0 1

0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 0 0 1

0 1 0 1 0 1 1 1 1 0 1 1 0 0 1 0 1 0 1 1

0 0 1 0 1 0 1 0 1 1 0 1 1 0 0 1 0 0 1 0

1 0 0 0 1 0 1 0 1 0 1 0 1 0 1 0 1 1 0 0

1 0 0 0 1 0 1 0 1 0 0 1 0 1 1 0 1 1 0 1

1 1 0 0 1 0 1 1 0 1 1 0 0 1 1 0 1 1 1 0

0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 1 0

1 0 0 1 0 0 1 1 0 0 0 1 1 0 1 0 0 1 0 1

1 0 0 1 1 0 1 0 0 1 1 0 1 0 1 0 0 1 1 0

0 1 0 1 0 1 1 0 1 1 0 1 1 0 1 0 1 0 1 0

1 0 0 1 0 1 0 1 1 0 1 0 1 0 1 0 0 0 1 1

1 0 1 1 0 1 0 1 1 0 1 0 1 1 0 1 1 1 0 1

0 1 0 0 1 0 0 1 1 0 1 1 0 0 0 1 0 0 0 1

0 1 0 0 1 1 0 1 1 0 1 0 0 1 0 1 0 1 1 0

1 0 1 0 0 1 0 1 1 0 1 0 1 0 1 0 1 0 0 1

0 0 1 1 0 1 1 0 1 0 1 0 1 1 0 1 1 0 1 1

0 1 1 0 1 0 1 0 0 1 1 0 1 0 1 0 1 0 0 1

0 0 1 0 0 1 0 0 1 0 1 0 1 0 1 0 1 1 0 0

1 0 1 1 0 1 0 1 0 0 1 0 1 0 1 0 1 0 1 0

1 1 0 0 0 1 0 1 0 1 0 1 1 0 1 0 0 1 0 1

0 1 1 0 1 0 1 1 0 1 0 1 0 1 0 0 1 0 1 1

0 0 1 0 0 0 1 1 0 1 0 0 0 1 0 1 0 0 1 0

0 1 0 1 0 0 1 0 1 0 1 1 0 1 0 1 0 1 0 1

0 1 0 1 0 1 0 1 1 0 0 0 1 0 1 0 1 0 1 0

1 0 1 0 1 0 1 1 0 1 1 0 1 0 1 1 0 1 0 0

1 1 0 0 1 0 1 0 1 1 0 1 1 0 1 1 0 1 0 1

0 0 1 0 1 0 1 0 1 0 0 1 1 0 1 0 0 1 0 1

0 1 0 1 0 1 0 1 1 0 0 1 0 1 0 1 0 1 0 1

1 1 0 1 0 1 0 1 1 1 1 0 1 0 1 0 1 0 1 0

1 0 1 1 1 1 1 0 1 0 1 1 0 1 1 0 1 0 1 1

1 0 1 1 1 0 1 0 0 1 1 0 1 0 0 1 0 1 0 0

1 0 1 0 1 1 0 1 0 1 1 0 1 1 1 0 1 0 1 0

0 1 0 0 0 1 0 1 0 1 0 1 0 1 1 0 1 1 0 1

0 1 1 0 1 0 1 0 1 1 1 0 1 0 1 1 1 0 1 0

1 0 1 1 1 0 0 1 0 1 0 1 1 0 1 1 0 1 0 1

0 1 1 0 0 0 1 0 0 1 0 1 0 1 0 1 1 1 0 0

1 0 1 1 1 0 1 1 0 1 0 1 0 1 1 0 1 1 0 1

0 1 1 0 1 0 1 0 1 0 1 0 1 0 0 1 0 1 1 1

0 1 1 1 1 0 0 1 0 0 1 1 0 1 1 0 0 0 1 1

0 1 0 1 0 1 0 1 1 0 1 1 0 1 0 0 1 0 0 1

0 1 0 1 0 1 0 1 1 0 1 1 0 1 1 0 0 1 0 1

1 0 1 0 1 0 0 1 1 0 0 1 0 0 1 1 0 1 0 1

0 1 0 0 1 0 0 1 0 1 0 0 1 1 1 0 0 1 0 1

1 0 1 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1

1 0 1 0 0 1 0 1 1 0 0 1 1 1 0 1 1 1 1 0

1 0 1 1 0 0 1 0 1 0 1 1 0 1 0 1 0 1 1 0

1 0 1 0 1 1 1 0 0 1 1 0 1 0 1 0 1 0 1 1

0 1 0 0 1 1 1 1 0 1 1 0 1 1 1 1 0 1 1 0

1 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 0

1 1 0 0 1 0 1 1 0 1 0 1 0 1 0 1 0 1 0 1

0 1 0 1 0 1 0 0 1 1 0 0 1 0 1 0 1 0 1 1

0 0 0 1 0 0 1 1 1 0 1 0 1 1 1 1 1 1 1 0

0 0 1 0 1 0 0 0 0 1 0 1 1 0 1 1 0 1 1 1

1 0 1 1 1 0 1 1 0 0 0 1 0 0 1 0 0 1 1 0

1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 1

1 0 1 1 0 1 0 1 0 0 1 1 0 1 0 1 1 1 1 0

1 0 1 0 1 0 0 0 1 0 0 1 1 1 0 1 0 1 1 0

0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 1 0 0 1

0 1 0 0 1 0 0 1 0 0 0 0 1 0 0 0 1 0 1 0

0 0 0 1 1 1 1 0 0 1 0 1 0 1 0 1 0 0 1 0

1 0 1 0 0 1 1 1 0 1 0 1 0 1 1 1 0 0 1 0

1 0 1 0 1 1 0 0 1 1 0 1 0 1 0 1 0 1 0 1

0 0 1 0 1 1 0 0 0 0 1 0 1 0 1 0 1 1 0 1

0 1 0 0 1 0 1 0 1 0 1 0 1 1 0 1 0 0 1 0

1 0 1 1 0 1 0 1 0 0 1 1 1 1 0 1 0 1 0 0

1 0 1 1 1 0 1 0 1 0 1 0 1 1 0 0 1 0 1 1

0 1 0 1 1 1 1 0 0 1 1 0 1 0 1 0 1 0 0 1

0 1 0 1 0 0 0 1 1 0 1 1 1 0 0 1 1 0 1 0

1 0 1 0 0 1 0 0 1 0 1 1 0 0 0 1 1 0 1 0

1 0 1 1 0 0 0 1 0 0 0 0 1 0 0 0 1 0 1 1

0 0 1 1 1 0 1 0 1 0 1 0 1 0 1 0 0 1 0 1

0 1 0 0 1 0 1 0 1 1 0 1 1 0 0 1 1 0 0 0

1 1 1 0 1 1 0 1 1 0 1 1 1 0 1 0 0 1 0 0

0 0 0 0 0 1 0 1 1 0 1 0 1 0 0 1 0 0 1 0

1 0 1 0 0 0 1 1 0 1 1 0 1 1 0 0 1 0 1 0

1 0 0 1 0 0 0 1 0 1 0 1 1 0 1 0 1 0 1 0

1 1 0 0 1 0 0 1 0 1 0 1 0 0 1 0 1 0 1 0

1 1 0 1 0 1 0 0 1 0 1 0 1 1 0 0 1 0 0 1

0 1 0 1 0 1 1 0 1 0 1 0 0 1 0 0 0 0 1 0

0 1 0 1 0 1 0 1 0 1 0 0 0 0 1 1 1 0 1 1

0 1 0 1 1 1 1 0 1 0 1 0 1 0 1 0 1 0 1 0

1 0 0 1 0 1 0 0 0 1 0 1 0 0 1 0 1 0 1 0

1 0 0 0 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1

0 1 1 1 0 1 0 0 1 0 1 1 1 1 0 1 0 1 1 0

0 0 1 0 0 1 0 1 0 1 0 1 1 0 1 1 1 0 0 1

1 0 1 0 1 0 1 0 0 1 0 0 0 0 1 0 0 1 0 1

0 0 1 0 0 1 1 1 0 0 1 0 1 1 0 1 1 0 1 0

1 0 1 0 0 1 0 0 0 0 1 0 1 0 1 0 0 1 0 1

0 0 0 1 0 0 1 1 0 0 1 0 1 0 0 0 1 1 0 1

0 1 1 0 0 0 1 0 0 1 0 1 0 1 1 0 0 1 0 1

1 0 1 0 1 0 0 1 0 0 1 0 1 0 0 0 1 0 0 1

0 0 1 0 1 1 0 1 0 1 0 0 1 0 0 1 0 1 0 0

0 1 0 0 1 0 0 1 0 1 1 0 1 0 1 1 0 0 1 0

1 0 1 0 1 0 0 0 1 1 0 1 1 1 0 1 0 0 1 0

1 0 1 0 0 0 1 0 1 0 1 0 0 1 0 1 0 0 1 1

0 0 1 0 0 1 0 0 1 0 1 1 0 1 0 1 0 0 0 1

0 0 1 0 1 0 1 0 1 0 0 1 0 1 0 1 0 1 1 0

0 0 1 0 1 1 0 1 0 0 0 1 0 1 1 0 0 0 1 0

1 1 1 0 1 0 1 1 1 0 1 0 1 1 0 1 0 1 0 0

1 0 1 1 0 1 1 0 1 1 1 0 0 1 1 0 0 0 1 0

1 1 0 1 0 1 0 1 0 1 0 1 1 0 0 1 1 1 0 1

1 0 0 1 0 1 0 1 1 0 1 0 0 1 0 1 0 1 0 1

0 1 1 1 0 0 1 0 1 1 1 0 1 0 0 0 1 0 1 1

0 1 0 0 1 0 1 0 1 1 0 0 0 0 1 0 1 1 1 0

1 1 1 0 1 0 1 1 0 1 0 1 1 1 1 0 0 1 1 0
1 0 1 0 1 0 1 0 0 1 0 1 0 0 1 0 0 1 0 1
0 1 0 0 1 0 1 0 1 1 0 1 0 1 0 0 1 1 1 0
1 0 1 0

[0032] The Sn = 32, and Sobs = 32/61.024 = 0.524. The corresponding P-value is

$$P-value = erfc\left(\frac{s_{obs}}{\sqrt{2}}\right) = erfc\left(\frac{0.524}{\sqrt{2}}\right) = erfc(0.37) = 0.6008 \qquad (3)$$

[0033] From the standard above mentioned, when P-value is larger than 0.01, i.e. P-value ≥ 0.01, the sequence is random. Therefore, it is obvious to obtain the conclusion that our generator creates random number sequences.

[0034] On the other hand, we measure the randomness of the noise sequence generated from the dark current in the detector, for example, the sequence is:

0 0 1 1 0 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0
1 0 1 0 0 0 0 1 0 0 0 0 1 1 1 0 1 0 0 0
0 1 1 0 0 0 1 1 0 0 1 1 0 0 1 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 1 1 0 0 1 1 0 1 0
0 1 1 1 0 1 0 0 0 0 0 0 0 1 0 1 0 0 1 0 1
0 0 0 0 1 0 1 0 0 0 0 0 0 1 0 0 0 0 0 1 1
0 0 0 0 0 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 1 0 0 0 0 0 0 1 0 0 0 1 1 1 1 0 0 0 0 0
0 1 1 1 1 0 0 0 0 0 0 0 1 0 0 0 0 0 0 1 1
0 1 0 1 0 1 0 0 0 1 0 0 0 1 0 0 0 0 1 0
1 0 0 0 0 0 0 1 0 1 0 0 1 0 0 0 1 0 0 0 0
0 0 1 1 0 0 1 0 0 1 0 0 0 0 0 0 1 1 0 0 0
0 1 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0

0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

1 0 0 1 1 0 0 1 0 0 0 1 0 0 0 0 0 0 1 1

0 0 0 1 0 0 0 1 0 0 0 0 0 0 1 0 0 0 0 0

0 0 0 1 1 0 1 1 0 0 0 0 0 0 0 1 1 0 0 0

0 1 0 1 1 0 0 0 0 0 0 0 0 0 1 0 1 0 0 0

0 0 1 1 0 0 1 0 0 0 0 0 0 0 0 0 1 1 1 0

0 0 0 0 0 0 0 1 1 1 0 0 0 1 0 0 0 0 0 0

0 1 0 0 1 0 0 0 0 1 0 0 0 0 1 0 0 1 0 0

1 1 1 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 1 0

1 1 1 0 1 1 0 0 0 1 0 1 0 0 1 0 0 1 0 0

0 0 0 0 0 0 0 0 0 0 1 0 0 0 1 1 0 0 0 0

0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 1

1 0 0 0 0 0 0 0 1 0 0 1 1 0 0 0 0 1 1 0

0 1 0 0 0 0 1 1 0 0 0 0 0 0 0 1 0 1 0 1

1 1 1 0 1 0 0 0 1 0 0 0 0 1 0 0 1 0 0 0

0 0 1 0 0 1 0 0 0 1 0 0 0 0 0 0 0 0 1 0

1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0

0 1 0 0 0 0 0 0 1 0 1 0 1 0 0 1 0 0 0 0

0 1 0 0 1 0 1 1 0 1 0 1 1 1 0 0 0 1 0 1

0 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 1 1 0 0

0 1 0 1 0 0 0 1 1 0 0 1 0 0 1 0 0 0 0 0

0 0 0 1 0 0 1 1 1 0 0 1 1 0 0 0 0 1 0 0

1 1 0 0 1 0 0 0 1 1 0 0 0 0 0 1 0 0 1 0

0 0 1 0 0 0 1 0 0 1 1 0 0 0 1 1 1 0 0 1

0 0 0 0 1 0 0 1 1 0 1 0 0 1 0 1 0 0 0 0

0 0 0 1 1 0 0 0 0 1 0 0 0 1 0 0 0 0 0 0

1 0 0 0 0 0 0 0 0 0 0 0 1 0 1 0 0 1 0 1 0

1 0 1 0 0 0 0 1 0 0 1 1 0 0 0 0 1 0 0 1

0 0 1 1 0 0 0 0 0 0 0 1 0 0 1 1 1 0 1 1

0 0 0 0 0 1 0 1 0 0 1 1 0 0 1 0 0 1 0 0

1 0 0 0 0 0 1 0 1 0 0 1 0 1 1 1 0 0 0 1

0 0 0 0 0 1 0 1 0 0 0 0 0 1 1 0 0 0 1 0

0 1 0 0 1 0 0 0 0 1 0 1 0 0 0 0 1 0 0 1

1 0 0 0 1 0 0 1 0 0 0 0 1 0 0 0 0 1 0 0

0 0 1 0 0 0 1 0 1 1 1 0 0 0 0 1 1 0 0 1

0 0 0 0 0 0 0 0 0 0 1 0 0 1 0 0 0 0 0 1

0 1 1 0 1 1 0 0 0 0 0 0 0 0 0 1 1 1 0 0

0 1 1 1 0 0 0 1 0 0 0 0 0 1 0 0 0 1 0 0

0 0 0 0 0 0 0 0 1 0 0 0 0 1 0 0 0 0 1 0

0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 1 0 0 0 0

0 0 0 1 1 0 1 0 0 0 1 0 0 0 0 0 0 1 1 1

0 1 1 0 0 0 0 0 1 0 1 0 0 1 1 0 1 0 0 1

1 0 0 1 1 1 0 0 0 0 0 0 0 0 1 0 0 0 0 0

0 0 0 0 0 0 0 1 0 0 0 0 1 0 0 1 0 0 0 1

0 0 1 0 0 0 0 0 0 0 1 0 1 0 0 0 1 0 0 0

1 1 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 1 0

0 0 0 0 1 1 0 0 0 0 0 0 0 0 1 0 0 0 1 1

0 0 0 0 0 0 0 1 1 0 0 1 1 1 0 1 0 0 0 0

0 1 0 0 1 0 0 0 0 0 1 0 1 1 0 0 0 1 0 0

1 0 0 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 1 1 1 0 0

0 1 0 0 0 0 1 0 1 0 0 0 0 1 0 0 0 1 0 1

0 1 0 0 0 0 0 0 1 0 0 0 0 1 0 0 1 0 0 1

1 1 0 0 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0

1 0 0 1 0 0 1 1 0 0 1 0 0 0 0 1 0 0 0 0

1 0 0 0 1 0 1 0 0 0 0 0 0 0 0 0 0 1 0 1

0 0 0 1 1 0 0 1 0 0 1 0 0 0 0 1 0 1 0 0

0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

0 0 0 1 0 0 0 0 0 0 0 1 1 0 0 0 0 1 1 1

0 0 0 0 0 0 0 0 0 0 1 1 0 0 0 0 0 1 0 0

0 0 0 1 0 0 0 1 1 0 0 1 0 0 0 0 0 1 1 0

0 0 0 0 0 0 0 0 0 0 0 0 1 0 1 0 0 0 0 1

0 0 0 1 0 0 1 0 0 0 1 1 0 0 0 0 0 1 0 0

0 0 0 1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0

0 0 0 1 0 0 1 1 0 1 1 1 0 1 0 1 0 0 0 0

0 1 1 0 1 1 1 1 0 0 0 1 0 0 1 1 0 0 1 0

0 0 0 0 0 1 0 0 0 0 0 0 1 0 0 1 1 0 1 1 1

0 0 1 0 0 0 0 1 0 1 0 0 0 1 0 0 0 0 0 0

0 0 0 1 1 0 0 0 0 1 1 0 0 0 0 0 0 1 1 0

0 0 0 1 0 1 0 1 0 0 0 0 0 0 0 1 0 0 0 1

0 0 0 1 0 0 0 0 0 1 0 0 1 1 1 0 1 0 0 0

1 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 1 0 0

0 0 1 0 0 1 0 1 0 1 1 1 1 1 0 0 1 0 0 0

0 0 1 1 0 0 0 1 0 0 0 0 1 1 0 0 0 0 1 0

0 0 0 0 0 1 1 1 0 1 1 0 0 1 0 0 1 0 0 1

0 1 1 1 1 0 0 0 1 1 0 0 0 0 0 1 1 0 1 1

0 0 0 1 0 0 1 1 0 0 0 0 0 0 0 0 1 0 0 1

0 1 0 0 0 0 1 1 1 1 0 0 1 0 0 0 0 0 1 0

1 0 1 0 1 1 0 0 0 0 0 1 0 1 1 0 0 1 0 0

1 0 0 0 0 1 0 1 1 0 0 0 0 1 0 0 0 0 0 0

1 0 0 0 0 0 1 0 0 0 0 0 0 1 1 0 0 0 0 0

0 0 0 1 0 0 0 0 0 0 0 1 0 0 0 1 0 1 0 1

1 0 1 0 0 0 0 0 1 1 0 1 0 0 0 0 1 1 0 1

0 0 1 0 0 0 0 0 0 1 0 1 0 0 1 0 0 0 1 1

0 0 1 1 0 0 0 0 0 1 0 0 1 1 0 0 0 0 0 0

0 1 0 0 0 1 0 0 0 0 1 1 0 0 0 0 0 1 0 1

0 0 0 1 0 0 1 0 1 0 1 1 0 0 1 1 0 0 1 1

1 0 0 1 0 1 0 0 1 0 0 1 1 0 1 0 0 1 0 1

0 1 0 0 1 0 0 1 1 0 0 1 0 1 1 0 0 1 1 0

0 0 0 0 1 0 0 1 0 0 0 1 0 1 0 1 0 0 0 0

1 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 1 1 0

0 0 0 1 0 1 0 0 1 0 1 1 1 0 1 0 0 0 0 0

0 1 0 0 1 1 0 1 0 0 0 0 1 0 0 0 0 1 1 0

0 0 0 0 0 1 0 0 0 1 0 0 0 1 0 0 1 1 0 1

0 1 0 0 1 1 0 0 1 1 1 0 0 0 0 1 1 1 0 1

0 1 1 0 0 0 0 0 0 0 0 0 1 1 1 0 0 0 0 0

1 0 0 0 1 0 1 0 0 0 0 1 1 0 0 0 0 0 0 1

1 0 0 1 0 1 0 1 0 0 0 1 0 0 1 0 1 0 0 0

0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

0 0 1 0 0 1 0 1 1 1 0 0 0 0 1 0 0 1 0 0

0 0 1 1 0 1 1 0 0 1 0 0 1 0 0 1 0 0 0 0

0 1 0 0 1 0 0 0 0 0 1 0 0 0 0 0 0 0 0 1

1 0 1 0 0 0 0 0 0 0 0 0 0 1 1 1 0 0 1 1

0 0 0 0 0 0 1 0 1 0 0 0 1 1 0 1 0 1 1 0

0 0 0 1 0 0 0 1 0 0 0 1 1 0 0 1 0 1 0 1

1 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 1 1 0 0

0 0 0 0 0 0 1 0 0 1 0 0 0 0 0 0 0 0 0 0

0 0 0 1 0 0 0 1 1 1 0 1 0 1 0 0 0 0 1 0

0 0 0 0 1 0 1 0 1 0 1 0 0 0 0 0 0 0 0 0

0 0 0 0 0 0 1 1 0 1 0 0 0 1 0 0 1 0 1 0

1 0 0 0 1 0 1 0 1 0 1 1 1 0 0 0 0 1 0 0

0 1 1 1 0 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0

0 0 0 1 0 0 0 0 1 1 0 0 1 0 0 1 1 0 1 1

0 0 0 0 1 0 0 0 1 0 0 0 0 1 0 0 3 0 0 0

0 0 1 0 0 0 1 1 0 0 0 1 0 0 1 0 0 0 0 1

1 0 1 1 1 1 1 1 1 0 0 0 0 1 0 0 0 1 0 1.

0 0 1 0 0 0 0 0 0 1 1 1 1 1 1 0 0 0 1 0

0 0 0 0 0 1 0 0 0 0 0 0 0 0 1 0 1 1 0 0 0

1 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 1 0 0 1 0

0 1 0 0 0 0 0 0 0 0 0 1 0 0 1 0 1 1 1 0 1

0 0 1 0 1 1 1 0 0 0 0 1 0 0 1 0 0 0 1 0

0 1 1 0 0 0 0 0 1 0 0 0 0 0 0 1 0 0 1 0

0 0 0 0 1 0 0 0 0 1 0 1 0 0 0 0 0 0 0 0

0 0 1 0 0 0 1 0 0 1 0 1 0 0 1 1 0 0 0 1

0 0 0 1 0 0 0 0 0 0 1 0 1 0 0 1 0 0 1 0

1 0 0 0 1 0 0 0 0 1 1 0 0 1 0 0 0 0 0 0

1 0 1 0 0 1 0 0 0 1 1 0 0 0 0 1 0 0 0 0

0 0 1 0 0 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0

1 0 1 0 0 0 0 0 0 0 1 1 0 0 0 0 0 1 0 0

0 0 0 0 1 0 1 1 0 1 0 1 1 0 0 0 0 0 1 0

1 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0

1 0 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0

0 0 0 1 1 0 1 0 0 1 1 0 0 0 0 1 0 0 0 1

1 0 0 0 1 0 0 0 0 0 0 0 0 1 0 1 0 0 0 0 0

1 0 0 1 0 0 0 0 0 0 0 1 0 0 0 1 0 0 0 1 0

1 0 0 0 0 0 1 1 0 1 1 0 1 1 0 1 0 0 1 0

0 0 0 0 0 0 0 0 0 1 0 1 0 0 1 0 0 0 0 0

0 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 1 0 1

1 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

1 0 0 0 0 0 0 1 1 0 0 0 1 0 0 0 1 0 1 1

1 0 0 1 0 1 0 0 0 0 0 1 0 0 0 0 0 0 0 1

1 1 0 0 0 0 0 0 0 1 1 0 0 0 0 0 0 0 0 0

0 0 0 0 0 0 0 1 1 0 0 0 1 0 1 0 0 0 0 0

0 0 0 0 0 1 0 0 0 0 0 1 0 1 0 0 0 0 0 0

1 1 1 0 0 0 0 0 1 0 0 0 0 0 0 1 1 1 1 0

0 1 0 0 0 0 1 0 1 0 1 0 0 1 1 0 1 0 0 0

0 0 0 0 0 0 0 1 0 0 1 0 0 1 0 0 0 1 0 0

0 1 0 0 0 0 1 0 0 0 0 0 0 0 0 1 0 1 1 0

1 0 0 0 0 0 1 1 0 1 1 0 0 0 0 0 0 0 0 0

1 0 1 1 0 1 0 0 1 1 0 0 1 1 1 0 1 0 1 0

0 0 0 0 1 0 1 0 1 1 0 1 1 0 1 0 1 0 0 0

1 0 0 0 0 1 0 1 0 1 0 0 0 1 1 0 0 0 1 0

1 0 0 0 0 0 0 0 1 1 0 1 0 0 1 1 0 0 1 0

0 1 0 1 1 0 0 0 0 1 1 0 0 0 0 0 0 0 0 0

0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0

0 0 0 1 1 0 0 0 0 1 0 0 0 1 0 1 1 0 1 1

0 0 0 0 1 0 0 1 0 1 0 0 0 0 1 1 1 0 1 0

1 0 0 1 0 0 0 0 0 0 1 1 0 0 0 0 0 1 0 0

1 0 0 1 1 0 0 0 0 1 0 1 1 1 0 0 0 0 1 0

0 0 0 0 1 0 1 1 0 0 0 0 0 0 0 0 0 0 0 1

1 0 0 0 0 1 0 0 0 1 1 1 0 0 0 0 0 1 0 0

1 0 0 0 0 1 0 0 1 0 0 1 1 1 1 0 0 0 0 0

1 0 0 0 0 0 0 0 1 0 0 0 0 0 1 1 0 0 0 0

0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 1 0 1 0 0

0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 0 0 0

1 0 1 0 0 0 1 0 0 0 1 0 0 0 0 1 0 0 0 0

0 0 1 0 0 0 0 0 1 0 0 0 0 1 0 0 1 0 1 1

0 0 1 1 0 0 0 1 0 0 0 0 0 0 0 1 1 0 0 0

0 1 0 1 0 1 0 1 1 0 1 0 0 0 0 0 0 0 0 0

1 0 0 0 1 1 0 0 1 1 1 1 1 0 0 0 0 0 0 0

0 1 0 0 1 1 0 1 0 1 0 1 1 0 1 0 0 0 0 0

0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

1 0 0 0 0 1 1 1 0 1 1 0 0 0 0 1 0 0 0 0

1 0 0 0 0 0 0 0 0 1 1 0 0 1 0 1 0 1 1 1

0 1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

0 0 0 1 0 1 1 1 1 0 0 0 0 1 0 0 0 1 0 0

1 0 0 1 0 1 1 0 1 0 1 0 1 1 0 1 0 0 0 1

where the corresponding P-value is 4.08×10^{-154}. From the standard, it is nonrandom.

[0035] According to the standard mentioned above, when P-value is larger than 0.01, i.e. P-value $\geq$ 0.01, the sequence is random. Therefore, it is obvious to obtain

the conclusion that the generator according to the invention creates random number sequences.

[0036] Although the present invention is described with the above embodiments and illustrations, it should be understood for those skilled in the art that various modifications, alternative variants, and equivalents to the invention may be used without departing from the spirit of the invention. Accordingly, the above description should not be taken as limiting the scope of the invention, which is defined by the appended claims.

CLAIMS

1. A random number generator comprising:

an optical coupler having an input port and two output ports;

a single photon source connected to the input port, generating a string of single photons, each single photon is transmitted from the input port to either of the two output ports;

two single photon detectors connected to the two output ports, respectively, detecting the single photon coming out from either of the output ports; and

means for generating random numbers according to the detection result of the single photon detectors.

2. The random number generator of claim 1, wherein the single photon source comprises:

a laser for emitting a beam of light; and

a variable optical attenuator, attenuating the light emitted from the laser into the string of single photons.

3. The random number generator of claim 2, wherein the laser is an arbitrary laser.

4. The random number generator of claim 1, wherein the optical coupler is a waveguide or an optical fiber coupler.

5. The random number generator of claim 1, wherein the optical coupler has a split ratio of 50:50.

6. The random number generator of claim 1, wherein the single photon detector is a semiconductor detector, a charged coupled device sensor or photomultiplier tube detector.

7. The random number generator of claim 1, wherein the laser, the variable optical attenuator, the optical coupler and the single photon detectors are connected by optical fibers using fiber connectors.

8. A random number generator comprising:

an optical coupler having an input port and two output ports;

a single photon source connected to the input port, generating a string of single photons, each single photon is transmitted from the input port to either of the two output ports; and

a photon detector counter connected to the two output ports, detecting the single photon coming out from either of the output ports and generating random numbers according to the detection result of the single photon detectors.

9. A method for generating random numbers, comprising:

generating a string of single photons;

launching each single photon into an optical coupler having two output ports;

detecting the single photon coming out from either of the output ports; and

generating random numbers according to the detection result.

10. The method of claim 9, wherein said generating a string of single photons further comprises:

generating a beam of light; and

attenuating the light into the string of single photons.

11. The method of claim 9, wherein the single photon coming out from one of the output ports represents "1" and the single photon coming out from the other one of the output ports represents "0".

12. The method of claim 9, wherein the optical coupler has a split ratio of

50:50.

13. The method of claim 9, wherein the optical coupler is a waveguide or an optical fiber coupler.

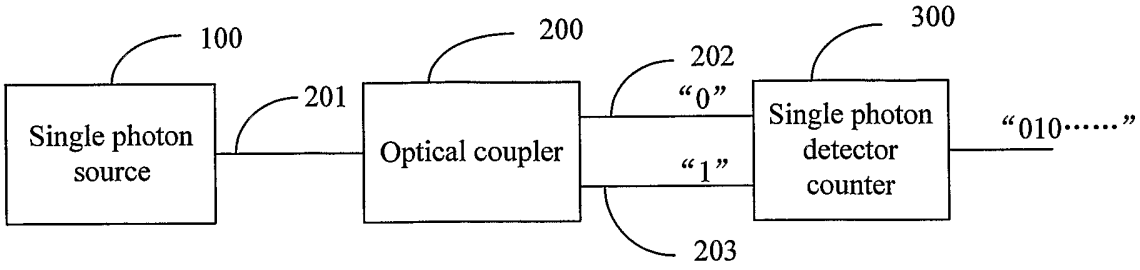

100
200
202
300
201
"0"
Single photon source
Optical coupler
Single photon detector counter
"010……"
"1"
203

FIG. 1

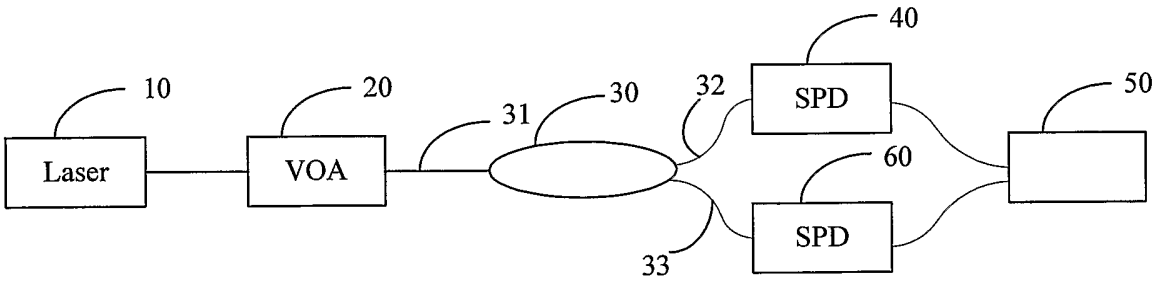

40
10
20
31
30
32
SPD
50
Laser
VOA
60
SPD
33

FIG. 2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2006/001361

A. CLASSIFICATION OF SUBJECT MATTER

G06F 7/58 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F 7/58 (2006.01) i, G06F 12/00 (2006.01) i, G06F 1/02(2006.01)i

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

CNPAT

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, WPI, EPODOC, PAJ: random, number, generator, photon, detector, source, detect, single, laser, optical, counter, launching;

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP,A,2003036168 (MITSUBISHI ELECTRIC CORP) 07.Feb 2003 (07.02.2003) see the paragraphs 0005-0013	1-13
X	CN,A,1396518 (ZHU, Wenjun) 12.Feb 2003 (12.02.2003) see claims 1, 5 and the specification, p.3, lines 20-25; p.6, lines 6-16	1-13

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&"document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
06.Sep 2006 (06.09.2006)	19 • OCT 2006 (19 • 10 • 2006)
Name and mailing address of the ISA/CN The State Intellectual Property Office, the P.R.China 6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China 100088 Facsimile No. 86-10-62019451	Authorized officer ZOU, Bin Telephone No. 86-010 62084953

Form PCT/ISA /210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2006/001361

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
JP,A,2003036168	07.02.2003	none	
CN,A,1396518	12.02.2003	none	