

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

(21) International Application Number:

PCT/MY2009/000147

(22) International Filing Date:

16 September 2009 (16.09.2009)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

PI 20083600 16 September 2008 (16.09.2008) MY

(71) Applicant (for all designated States except US): **MIMOS BERHAD** [MY/MY]; Technology Park Malaysia, 57000 Kuala Lumpur (MY).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **SURYADI** [MY/MY]; Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY). **NORZALIMAN bin MOHD. ZAIN, Mohd.** [MY/MY]; Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY). **WAHIDDIN, Mohamed, Ridza** [MY/MY]; Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY).(74) Agent: **MIRANDAH, Patrick**; Patrick Mirandah Co. (Malaysia) SDN BHD, Suite 3B-19-3 Plaza Sentral, Jalan Stesen Sentral 5, 50470 Kuala Lumpur (MY).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))

[Continued on next page]

(54) Title: METHOD AND APPARATUS FOR QUANTUM-MECHANICALLY GENERATING A RANDOM NUMBER

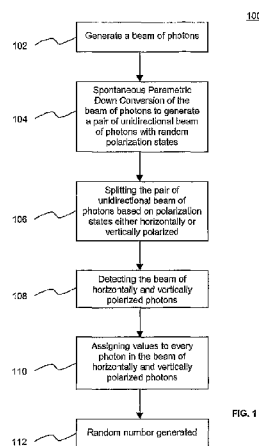


FIG. 1

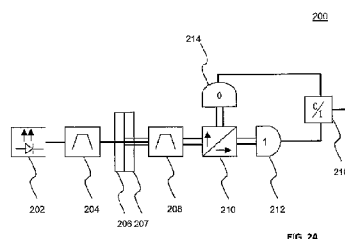


FIG. 2A

(57) Abstract: A method (100) and apparatus (200) for quantum-mechanically generating a random number based on polarization states of spontaneous parametric down-converted photons. The method (100) and apparatus (200) comprises a photon source (202) to generate a beam of photons (102), a first type-I nonlinear crystal (206) and a type-I second nonlinear crystal (207) to down-convert the beam of photons through spontaneous parametric down conversions to generate a pair of unidirectional beam of photons with random polarization states (104), characterized in that the first type-I nonlinear crystal (206) is adjacent to the second type-I nonlinear crystal (207) and optical axis of the first type-I nonlinear crystal (206) is orthogonal to optical axis of the second type-I nonlinear crystal (208), a polarized beam splitter (210) to split the pair of unidirectional beam of photons based on polarization states of the pair of unidirectional beam of photons into a beam of horizontally polarized photons and a beam of vertically polarized photons (106), a first detector (212) and a second detector (214) to detect the presence of the beam of horizontally polarized photons and the beam of vertically polarized photons respectively (108), and an electronic logic (216) to assign a first value to every photon in the beam of horizontally polarized photons and assign a second value to every photon in the beam of vertically polarized photons to generate a random number (110).



Published:

- *without international search report and to be republished
upon receipt of that report (Rule 48.2(g))*

METHOD AND APPARATUS FOR QUANTUM-MECHANICALLY GENERATING A RANDOM NUMBER

FIELD OF INVENTION

5

The present invention relates to a method and apparatus for quantum-mechanically generating a random number.

BACKGROUND ART

10

The science of quantum information had revolutionized growth in the field of communication and computing, contributing major advancements in the area of data encryption and data processing. The application of quantum information science in random number generators has improved the functionality of a random number
15 generator, such as generating cryptographic keys for an ultra-secure data encryption, computer simulation and modeling as well as statistical sampling.

Conventionally, random number generators are based on software, more specifically complex mathematical equations and algorithms to generate random numbers that are
20 characterized as pseudo-random numbers. These pseudo-random numbers are predictable and reproducible, and hence ineffective for generating cryptographic keys in data encryption.

A shift was observed from software based to hardware based random number
25 generators, whereby these hardware based random number generators leveraged on

the randomness of various macroscopic phenomena such as thermal noise and photoelectric effect as well as various quantum phenomena. Thermal noise and the photoelectric effect are unpredictable phenomenas that are able to generate truly random numbers. However, the generator design is complex and the implementation of the same requires immense effort.

The application of quantum information science in random number generators leverages on the various quantum phenomena and that has since been developed to generate truly random numbers and simultaneously ensuring that the generator design is simple and implementation of the same is practical and not complicated. In line with this effort, several quantum random number generators employ the concept of statistics of single photon transmission and reflection on an optical 50/50 beam splitter. However, producing a single photon state and designing an optical 50/50 beam splitter can be difficult and complicated.

SUMMARY OF INVENTION

In one embodiment of the present invention is a method for quantum-mechanically generating a random number based on polarization states of spontaneous parametric down converted photons, the method comprising generating a beam of photons, down
5 converting the beam of photons through spontaneous parametric down conversions to generate a pair of unidirectional beam of photons with random polarization states, splitting the pair of unidirectional beam of photons based on polarization states of the pair of unidirectional beam of photons into a beam of horizontally polarized photons and
10 a beam of vertically polarized photons, detecting the presence of the beam of horizontally polarized photons and detecting the presence of the beam of vertically polarized photons and assigning a first value to every photon in the beam of horizontally polarized photons and assigning a second value to every photon in the beam of vertically polarized photons to generate a random number.

15 In another embodiment of the present invention is an apparatus for quantum-mechanically generating a random number based on polarization states of spontaneous parametric down converted photons, the apparatus comprising a photon source to generate a beam of photons, a first type-I nonlinear crystal and a second type-I
20 nonlinear crystal to down convert the beam of photons through spontaneous parametric down conversions to generate a pair of unidirectional beam of photons with random polarization states, characterized in that the first type-I nonlinear crystal is adjacent to the second type-I nonlinear crystal and an optical axis of the first type-I nonlinear crystal is orthogonal to an optical axis of the second type-I nonlinear crystal, a polarized beam
25 splitter to split the pair of unidirectional beam of photons based on polarization states of

the pair of unidirectional beam of photons into a beam of horizontally polarized photons and a beam of vertically polarized photons, a first detector to detect the presence of the beam of horizontally polarized photons and a second detector to detect the presence of the beam of vertically polarized photons, and an electronic logic to assign a first value to every photon in the beam of horizontally polarized photons and assign a second value to every photon in the beam of vertically polarized photons to generate a random number.

The present invention consists of several novel features and a combination of parts hereinafter fully described and illustrated in the accompanying drawings, it being understood that various changes in the details may be made without departing from the scope of the invention or sacrificing any of the advantages of the present invention.

BRIEF DESCRIPTION OF THE ACCOMPANYING DRAWINGS

For the purpose of facilitating an understanding of the present invention, there is illustrated in the accompanying drawings, from an inspection of which, when considered
5 in connection with the following description, the invention, its construction and operation and many of its advantages would be readily understood and appreciated.

FIG. 1 is a flowchart illustrating the method for quantum-mechanically generating a random number.

10

FIG. 2A is an illustrative view of the apparatus for quantum-mechanically generating a random number.

FIG. 2B is an illustrative view of the suitably configured nonlinear type-I crystal.

15

FIG. 3 is an illustrative view of the apparatus for quantum-mechanically generating a random number indicating the signal paths.

FIG. 4A is an illustrative view of the beam of photons.

20

FIG. 4B is an illustrative view of the spontaneously down converted beam of photons comprising of the residual beam of photons and the pair of unidirectional beam of photons.

5 FIG. 4C is an illustrative view of the pair of unidirectional beam of photons.

FIG. 4D is an illustrative view of the beam of vertically polarized photons.

FIG. 4E is an illustrative view of the beam of horizontally polarized photons.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention relates to a method and apparatus for quantum-mechanically generating a random number. Hereinafter, this specification will describe the present invention according to the preferred embodiments of the present invention. However, it is to be understood that limiting the description to the preferred embodiments of the invention is merely to facilitate discussion of the present invention and it is envisioned that those skilled in the art may devise various modifications and equivalents without departing from the scope of the appended claims.

10

The present invention describes a method and an apparatus for quantum-mechanically generating a random number based on polarization states of spontaneous parametric down converted photons.

15 The method and apparatus for quantum-mechanically generating a random number of the present invention describes a quantum random number generator based on the randomness of polarization state of down converted photons, through spontaneous parametric down conversion. The advantage of this quantum random number generator is that the randomness of quantum state is dependent on the statistical polarization state
20 of the pairs of spontaneous parametric down converted photons generated from the nonlinear optical interaction process fashioned by the nonlinear crystal.

Spontaneous parametric down conversion is one of the most versatile quantum optical processes. This process begins with a single photon being bombarded and absorbed by
25 a specific nonlinear crystal material. The said specific nonlinear crystal material splits the

single photon into a pair of photons known also as the down converted photons or spontaneous parametric down converted photons, each having a lower energy and momentum level compared to the original single photon. However, the combined energy level of the photon pairs is equal to that of the original single photon.

5

Spontaneous parametric down conversion is stimulated by random vacuum fluctuations. As such the photon pairs are randomly generated and the probability of the occurrence of down conversion is extremely small. On average, down conversion occurs in only one out of every 10 billion photons. In addition to its random occurrences, spontaneous parametric down conversion generates down converted photons with random polarization states that is either horizontal or vertical polarization states. The randomness of polarization states, either horizontal or vertical polarization states, is guaranteed by the coherent quantum mechanical superposition of the polarization states, assuming that the current understanding of quantum mechanics is fundamentally true.

15

These polarization states of every photon pair can be measured using classical polarization analyzer and detected using sensitive photon detector, such as avalanche photon detectors. These randomly polarized states are digitized by defining for example, the horizontal polarized photon as bit value "0" and the vertical polarized photon as bit value "1" and a truly random number series can be produced using an electronic logic system. Alternatively, the digitization may result in the horizontal polarized photon assigned as bit value "1" and the vertical polarized photon as bit value "0" to generated a truly random number series.

20

25

The randomness of this quantum random number generator apparatus only depends on the randomness of polarization photon states generated by the nonlinear crystal. Since the randomness of the random number is completely dependent on the randomness of the polarization of the spontaneous random down conversion of the photons, there is no longer a need to provide a single photon state or a perfect 50/50 beam splitter.

Reference is now being made to FIG.1. FIG. 1 is a flowchart illustrating the method for quantum-mechanically generating a random number. The method (100) includes generating a beam of photons (102), spontaneous parametric down conversion of the beam of photons to generate a pair of unidirectional beam of photons with random polarization states (104), splitting the pair of unidirectional beam of photons based on polarization states either horizontally or vertically polarized (106), detecting the beam of horizontally and vertically polarized photons (108) and assigning values to every photon in the beam of horizontally and vertically polarized photons (110) that finally results in a random number being generated (112).

Reference is now being made to FIGs. 2A and 2B. FIG. 2A is an illustrative view of the apparatus for quantum-mechanically generating a random number. The apparatus (200) includes a quantum state preparatory that comprises a photon source (202), a neural density filter (204), a suitably configured nonlinear type-I crystal (206, 207) and a bandpass filter (208) and a quantum state analyzer that comprises a polarized beam splitter (210), a first detector (212), a second detector (214) and an electronic logic (216). FIG. 2B is an illustrative view of the suitably configured nonlinear type-I crystal (206, 207).

Reference is now being made to FIGs. 3, 4A, 4B, 4C, 4D and 4E. FIG. 3 is an illustrative view of the apparatus for quantum-mechanically generating a random number indicating the signal paths. FIGs. 4A, 4B, 4C, 4D and 4E are illustrative views of the various signal paths as indicated in FIG. 3.

5

Reference is now collectively being made to FIGs. 1, 2A, 2B, 3, 4A, 4B, 4C, 4D and 4E. The method (100) and apparatus (200) for quantum-mechanically generating a random number based on polarization states of spontaneous parametric down converted photons begins with a photon source (202) generating a beam of photons (102). A laser pump is the most commonly used photon source and it provides a high intensity laser that generates the beam of photons. There are two main types of laser pumps, the first is a continuous wave laser pump that generates a continuous beam of photons and the second is a pulse laser pump that generates a pulsed beam of photons. Both types of laser pumps are suitable for generating the beam of photons for the purpose of quantum-mechanically generating a random number based on polarization states of spontaneous parametric down converted photons.

The generated beam of photons is passed through a neutral density filter (204) to adjust the density level of the beam of photons. The neural density filter (204) is used to control the intensity of the laser to obtain the optimum density level required for spontaneous parametric down conversion of the beam of photons without compromising the characteristics of the same. The preferred density level to successfully down convert the beam of photons through spontaneous parametric down conversion is typically greater than 10^7 photons per pulse. FIG. 4A is an illustrative view of the beam of photons

generated by the photon source and passed through the neutral density filter at the signal path (302) of FIG. 3.

Once the preferred density level is achieved, the beam of photons is down converted through spontaneous parametric down conversions to generate a pair of unidirectional beam of photons with random polarization states (104). The beam of photons is bombarded onto a suitably configured nonlinear crystal.

The nonlinear crystal is either a crystal of the certain chemical structure, such as beta-barium borate (BBO), or an artificial crystal, such as periodically poled LiNO_3 (PPLN), or a photonic crystal. These crystals have the property of optical nonlinearity, whereby the polarizability of these crystals depends on the square or higher power of an applied electrical field. A single photon, when bombarded and absorbed by such a crystal, will be split or down converted into a pair of spontaneous parametric down converted photons and the probability of the occurrence of down conversion is extremely small.

The nonlinear crystal is suitably configured to provide for type-I phase matching such that both the photons in the pair of spontaneous parametric down converted photons have the same polarization states. The suitably configured nonlinear crystal (206, 207) comprises of a first type-I nonlinear crystal (206) and a second type-I nonlinear crystal (207). The first type-I nonlinear crystal (206) is placed adjacent to the second type-I nonlinear crystal (207) and the optical axis (218) of the first type-I nonlinear crystal (206) is orthogonal to optical axis (220) of the second type-I nonlinear crystal (206).

The first configuration of the optical axes (218, 220) may be such that the first type-I nonlinear crystal (206) has a horizontal optical axis (218) and the second type-I

nonlinear crystal (207) has a vertical optical axis (220). Due to this type-I nonlinear crystal phase matching, the spontaneous parametric down converted photons generated from first type-I nonlinear crystal (206) is vertically polarized, $|VV\rangle$ and the spontaneous parametric down converted photons generated from second type-I nonlinear crystal (207) is horizontally polarized, $|HH\rangle$.

Alternatively, the second configuration of the optical axes may be such that the first type-I nonlinear crystal (206) has a vertical optical axis and the second type-I nonlinear crystal (207) has a horizontal optical axis. Due to this type-I nonlinear crystal phase matching, the spontaneous parametric down converted photons generated from first type-I nonlinear crystal (206) is horizontally polarized, $|HH\rangle$ and the spontaneous parametric down converted photons generated from second type-I nonlinear crystal (207) is vertically polarized, $|VV\rangle$.

In both configurations of optical axes, the polarization states of the spontaneous parametric down converted photons are coherent quantum mechanical superposition of the respective polarization photon states that is given by

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle)$$

The probability of occurrence of the vertical polarization spontaneous parametric down conversion process is equal to that of the occurrence of the horizontal polarization spontaneous parametric down conversion process. It is impossible to distinguish which of these processes will or has occurred, rendering it to be a truly random process

capable of generating a pair of spontaneous parametric down converted photons with random polarization states.

The spontaneous parametric down conversion is performed under collinear and degenerate conditions whereby the pair of spontaneous parametric down converted photons have a propagation direction identical to that of the beam of photons generated by the laser pump and having a wavelength half of that of the beam of photons generated by the laser pump.

10 The suitably configured nonlinear crystal (206, 207) down-converts the beam of photons through spontaneous parametric down conversions to generate a pair of unidirectional beam of photons with random polarization states. The first type-I nonlinear crystal (206) is used for a first spontaneous parametric down conversion under collinear and degenerate conditions to generate the pair of unidirectional beam of photons with
15 polarization states orthogonal to that of the optical axis (218) of the first type-I nonlinear crystal (206) and the second type-I nonlinear crystal (207) is used for a second spontaneous parametric down conversion under collinear and degenerate conditions to generate the pair of unidirectional beam of photons with polarization states orthogonal to that of the optical axis (220) of the second type-I nonlinear crystal (207).

20

The description and drawings, more specifically FIG. 2B refers to the first configuration of the optical axes (218, 220) for convenience of explanation and illustration. By way of the first configuration of the optical axes (218, 220), the first type-I nonlinear crystal (206) is used for the first spontaneous parametric down conversion under collinear and
25 degenerate conditions to randomly generate the pair of unidirectional beam of photons with vertically polarized photons and the second type-I nonlinear crystal (207) is used for

the second spontaneous parametric down conversion under collinear and degenerate conditions to randomly generate the pair of unidirectional beam of photons with vertically polarized photons.

- 5 Due to the fact that the spontaneous parametric down conversions are performed under collinear and degenerate conditions, the pair of unidirectional beam of photons have a propagation direction identical to that of the beam of photons and have a wavelength half of that of the beam of photons.
- 10 FIG. 4B is an illustrative view of the spontaneously down converted beam of photons comprising of the residual beam of photons and the pair of unidirectional beam of photons at the signal path (304) of FIG. 3. The pair of unidirectional beam of photons at the signal path (304) of FIG. 3 consists of multiple photons that have the same polarization states due to the type-I phase matching, however, the probability of the
- 15 photon being either vertically polarized or horizontally polarized is equal, rendering it impossible to distinguish which polarization will or has occurred.

The residual beam of photons is considered as a form of noise. Since the wavelength of the pair of the unidirectional beam of photons is half of the wavelength of the residual

20 beam of photons, the residual beam of photons can be easily blocked by a bandpass filter (208). The bandpass filter (208) is configured to attenuate the residual beam of photons and only the pair of the unidirectional beam of photons is passed to the polarized beam splitter (210) as shown in FIG. 4C.

- 25 FIG. 4C is an illustrative view of the pair of unidirectional beam of photons passed to the polarized beam splitter (210) at the signal path (306) of FIG. 3. There is no longer the

residual beam of photons and polarization states of every photon in the pair of unidirectional beam of photons pair can be analyzed and detected for further digitization to generate a random number. In FIG. 4C, the clear circles represent vertically polarized photons and the black circles represent horizontally polarized photons.

5

The polarized beam splitter (210) is used to split the pair of the unidirectional beam of photons based on the polarization state, horizontally and vertically polarized photons. The most common form of a polarized beam splitter is a cube, configured out of two adjacent triangular glass prisms. The alternative design is the half-silvered mirror, which is a plate of glass with a thin coating of aluminium such that at a 45 degree angle, one polarization state is transmitted and the other is reflected.

10

The polarized beam splitter (210) comprises a first input to accept the pair of unidirectional beam of photons, a first output to release the beam of horizontally polarized photons and a second output to release the beam of vertically polarized photons. The polarized beam splitter (210) splits the pair of unidirectional beam of photons based on polarization states of the pair of unidirectional beam of photons into a beam of horizontally polarized photons and a beam of vertically polarized photons.

15

The vertically polarized photons will be reflected by the polarized beam splitter (210) through the second output. FIG. 4D is an illustrative view of the beam of vertically polarized photons at the signal path (310) of FIG. 3. The horizontally polarized photons will be transmitted by the polarized beam splitter (210) through the first output. FIG. 4E is an illustrative view of the beam of horizontally polarized photons at the signal path (308) of FIG. 3.

20
25

The vertically polarized photons and the horizontally polarized photons will then be passed through detectors that detect the presence of the same. The presence of the beam of horizontally polarized photons is detected by the first detector (212) and the presence of the beam of vertically polarized photons is detected by the second detector (214). This application requires the use of single photon detection and the most common of the same is the avalanche photon detector or avalanche photodiodes. The type of detector system is determined by the type of photon source applied. The first detector (212) and the second detector (214) are either active-quenching or passive-quenching detector systems.

If the beam of photons is a continuous beam of photons, active-quenching detector system is used for detecting the presence of the beam of horizontally polarized photons and detecting the presence of the beam of vertically polarized photons (108), wherein the frequency of the continuous wave laser pump is not synchronized to an open-gate-time of the first detector (212) and the second detector (214).

If the beam of photons is a pulsed beam of photons, passive-quenching detector system is used for detecting the presence of the beam of horizontally polarized photons and detecting the presence of the beam of vertically polarized photons (108), wherein the frequency of the continuous wave laser pump is synchronized to an open-gate-time of the first detector (212) and the second detector (214).

The beam of horizontally polarized photons and the beam of vertically polarized photons detected by the detector system are fed into an electronic logic (216). The electronic logic (216) digitizes the polarized photon states by assigning a first value to every photon

in the beam of horizontally polarized photons and a second value to every photon in the beam of vertically polarized photons to generate a random number.

The electronic logic (216) assigns a bit value '1' to every photon in the beam of horizontally polarized photons and assigns a bit value '0' to every photon in the beam of vertically polarized photons to generate the random number comprising a series of bit values, "1"s and "0"s. Alternatively, the electronic logic (216) may assign a bit value '0' to every photon in the beam of horizontally polarized photons and assign a bit value '1' to every photon in the beam of vertically polarized photons to generate the random number comprising a series of bit values, "1"s and "0"s.

CLAIMS

1. A method (100) for quantum-mechanically generating a random number based on polarization states of spontaneous parametric down converted photons, the method comprising:

generating a beam of photons (102);

down-converting the beam of photons through spontaneous parametric down conversions to generate a pair of unidirectional beam of photons with random polarization states (104);

splitting the pair of unidirectional beam of photons based on polarization states of the pair of unidirectional beam of photons into a beam of horizontally polarized photons and a beam of vertically polarized photons (106);

detecting the presence of the beam of horizontally polarized photons and detecting the presence of the beam of vertically polarized photons (108); and

assigning a first value to every photon in the beam of horizontally polarized photons and assigning a second value to every photon in the beam of vertically polarized photons to generate a random number (110).

2. A method according to claim 1, wherein the beam of photons is a continuous beam of photons.

3. A method according to claim 1, wherein the beam of photons is a pulsed beam of photons.

4. A method according to claim 1, wherein down converting the beam of photons through spontaneous parametric down conversions to generate the pair of unidirectional beam of photons with random polarization states (104) comprises:

adjusting a density level of the beam of photons;

- 5 a first spontaneous parametric down conversion under collinear and degenerate conditions to generate the pair of unidirectional beam of photons with polarization states orthogonal to that of an optical axis of a first type-I nonlinear crystal and a second spontaneous parametric down conversion under collinear and degenerate conditions to generate the pair of unidirectional beam of photons with polarization states orthogonal to that of an optical axis of a second type-I nonlinear crystal; and
10 filtering residual noise from the pair of unidirectional beam of photons.

5. A method according to claim 4, wherein the pair of unidirectional beam of photons is characterized in that the pair of unidirectional beam of photons
15 comprise horizontally polarized photons and vertically polarized photons, having a propagation direction identical to that of the beam of photons and having a wavelength half of that of the beam of photons.

- 20 6. A method according to claim 1 and 2, wherein if the beam of photons is the continuous beam of photons, active-quenching is used for detecting the presence of the beam of horizontally polarized photons and detecting the presence of the beam of vertically polarized photons (108).

- 25 7. A method according to claim 1 and 3, wherein if the beam of photons is the pulsed beam of photons, passive-quenching is used for detecting the presence of

the beam of horizontally polarized photons and detecting the presence of the beam of vertically polarized photons (108).

8. A method according to claim 1, wherein assigning the first value to every photon
5 in the beam of horizontally polarized photons and assigning the second value to every photon in the beam of vertically polarized photons to generate the random number (110) comprises:

assigning a bit value '1' to every photon in the beam of horizontally polarized photons;

10 assigning a bit value '0' to every photon in the beam of vertically polarized photons; and

generating the random number comprising a series of bit values.

9. An apparatus (200) for quantum-mechanically generating a random number
15 based on polarization states of spontaneous parametric down converted photons, the apparatus comprising:

a photon source (202) to generate a beam of photons;

a first type-I nonlinear crystal (206) and a second type-I nonlinear crystal (207) to down convert the beam of photons through spontaneous
20 parametric down conversions to generate a pair of unidirectional beam of photons with random polarization states,

characterized in that the first type-I nonlinear crystal (206) is adjacent to the second type-I nonlinear crystal (207) and an optical axis (218) of the first type-I nonlinear crystal (206) is
25 orthogonal to an optical axis (220) of the second type-I nonlinear crystal (207);

a polarized beam splitter (210) to split the pair of unidirectional beam of photons based on polarization states of the pair of unidirectional beam of photons into a beam of horizontally polarized photons and a beam of vertically polarized photons;

5 a first detector (212) to detect the presence of the beam of horizontally polarized photons and a second detector (214) to detect the presence of the beam of vertically polarized photons; and
an electronic logic (216) to assign a first value to every photon in the beam of horizontally polarized photons and assign a second value to
10 every photon in the beam of vertically polarized photons to generate a random number.

10. An apparatus according to claim 9, wherein the photon source (202) is a continuous wave laser pump that generates a continuous beam of photons.

15

11. An apparatus according to claim 9, wherein the photon source (202) is a pulse laser pump that generates a pulsed beam of photons.

12. An apparatus according to claim 9, wherein the optical axis (218) of the first type-I nonlinear crystal (206) is either horizontally or vertically orientated.

20

13. An apparatus according to claim 9, wherein a neutral density filter (204) is used to adjust a density level of the beam of photons.

25

14. An apparatus according to claim 9, wherein the beam of photons is bombarded onto the first type-I nonlinear crystal (206) and the second type-I nonlinear crystal

(207), first type-I nonlinear crystal (206) is used for a first spontaneous parametric down conversion under collinear and degenerate conditions to generate the pair of unidirectional beam of photons with polarization states orthogonal to that of the optical axis (218) of the first type-I nonlinear crystal (206) and the second type-I nonlinear crystal (207) is used for a second spontaneous parametric down conversion under collinear and degenerate conditions to generate the pair of unidirectional beam of photons with polarization states orthogonal to that of the optical axis (220) of the second type-I nonlinear crystal (207).

15. An apparatus according to claim 14, wherein the pair of unidirectional beam of photons is characterized in that the pair of unidirectional beam of photons comprise horizontally polarized photons and vertically polarized photons, having a propagation direction identical to that of the beam of photons and having a wavelength half of that of the beam of photons.

16. An apparatus according to claim 9, wherein a bandpass filter (208) is used to filter residual noise from the pair of unidirectional beam of photons.

17. An apparatus according to claim 9, wherein the polarized beam splitter (210) comprises:

- a first input to accept the pair of unidirectional beam of photons;
- a first output to release the beam of horizontally polarized photons; and
- a second output to release the beam of vertically polarized photons;

18. An apparatus according to claim 9 and 10, wherein if the photon source (202) is a continuous wave laser pump that generates the continuous beam of photons, active-quenching is used for detecting the presence of the beam of horizontally polarized photons and detecting the presence the beam of vertically polarized photons, wherein frequency of the continuous wave laser pump is not synchronized to an open-gate-time of the first detector (212) and the second detector (214).

19. An apparatus according to claim 9 and 11, wherein if the photon source (202) is a pulse laser pump that generates the pulsed beam of photons, passive-quenching is used for detecting the presence of the beam of horizontally polarized photons and detecting the presence the beam of vertically polarized photons, wherein frequency of the continuous wave laser pump is synchronized to an open-gate-time of the first detector (212) and the second detector (214).

20. An apparatus according to claim 9, wherein the electronic logic (216) to assign the first value to every photon in the beam of horizontally polarized photons and assigning the second value to every photon in the beam of vertically polarized photons to generate a random number comprises:

the electronic logic (216) assigning a bit value '1' to every photon in the beam of horizontally polarized photons;

the electronic logic (216) assigning a bit value '0' to every photon in the beam of vertically polarized photons; and

the electronic logic (216) generating the random number comprising a series of bit values.

1/4

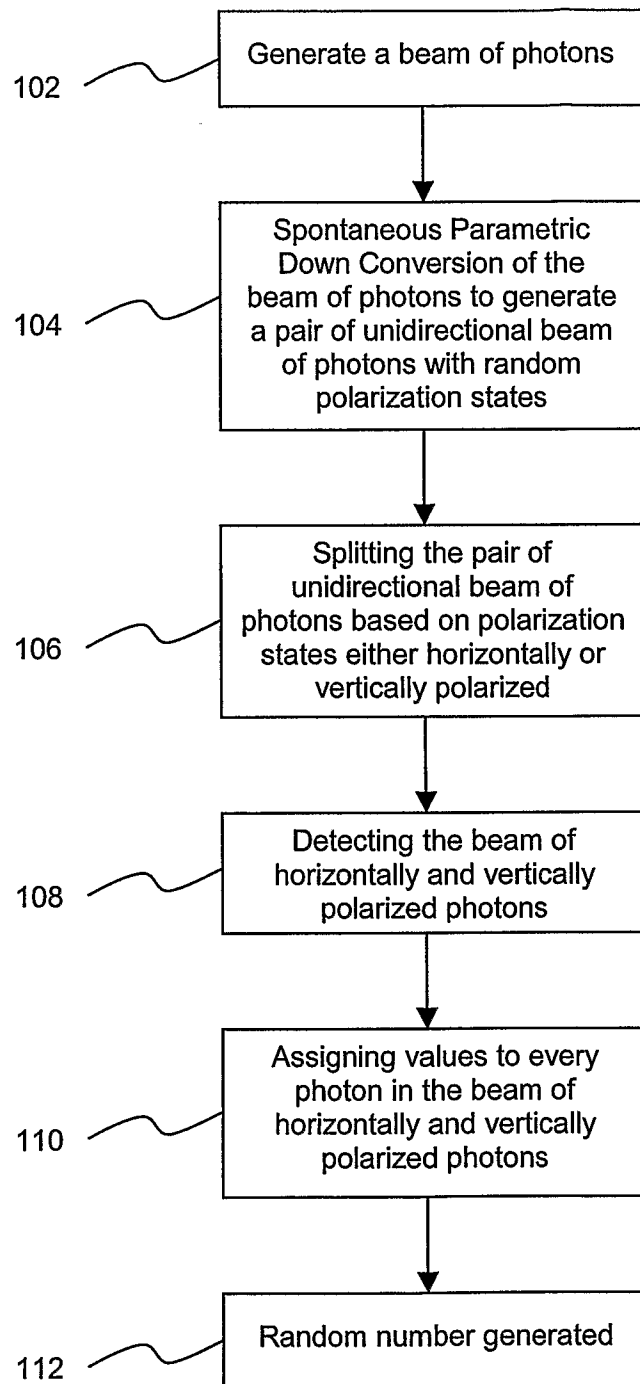
100

FIG. 1

2/4

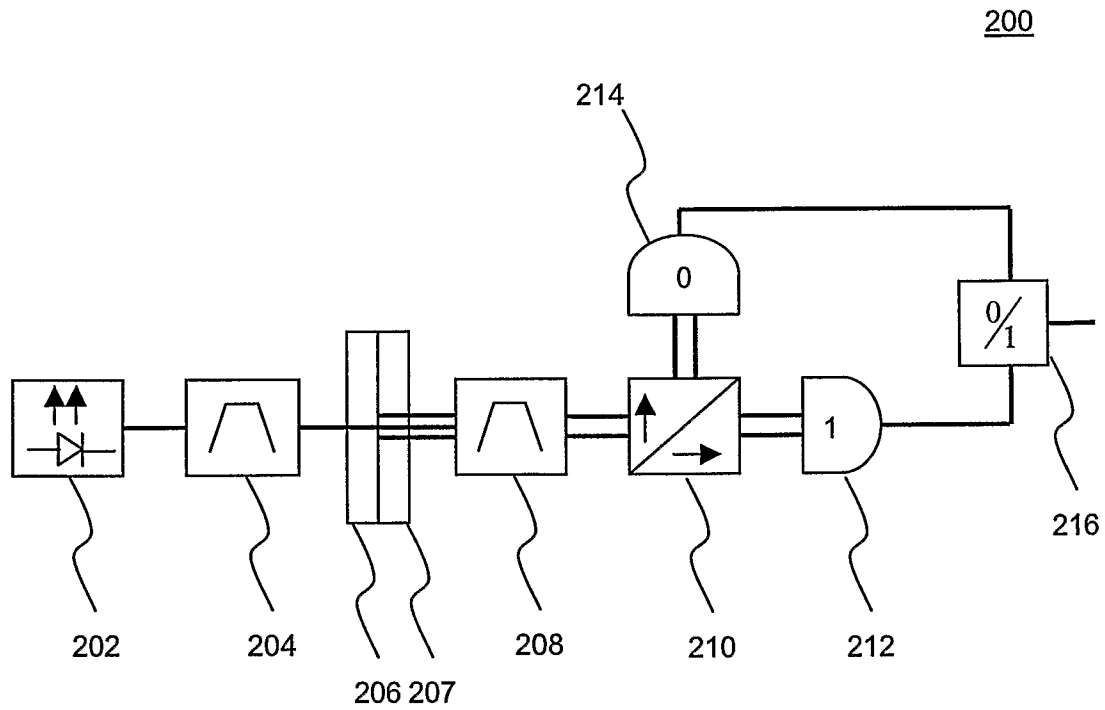


FIG. 2A

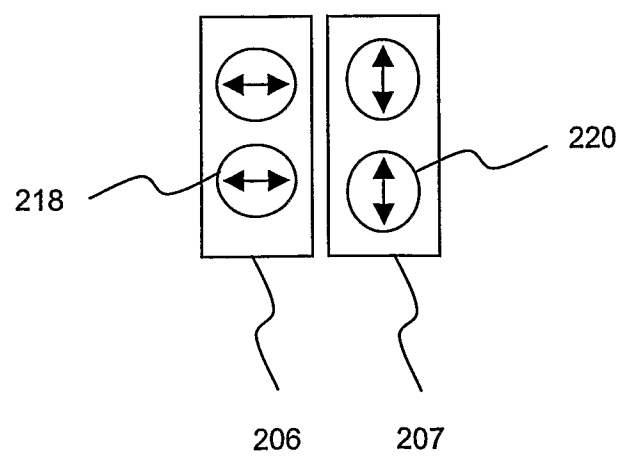


FIG. 2B

3/4

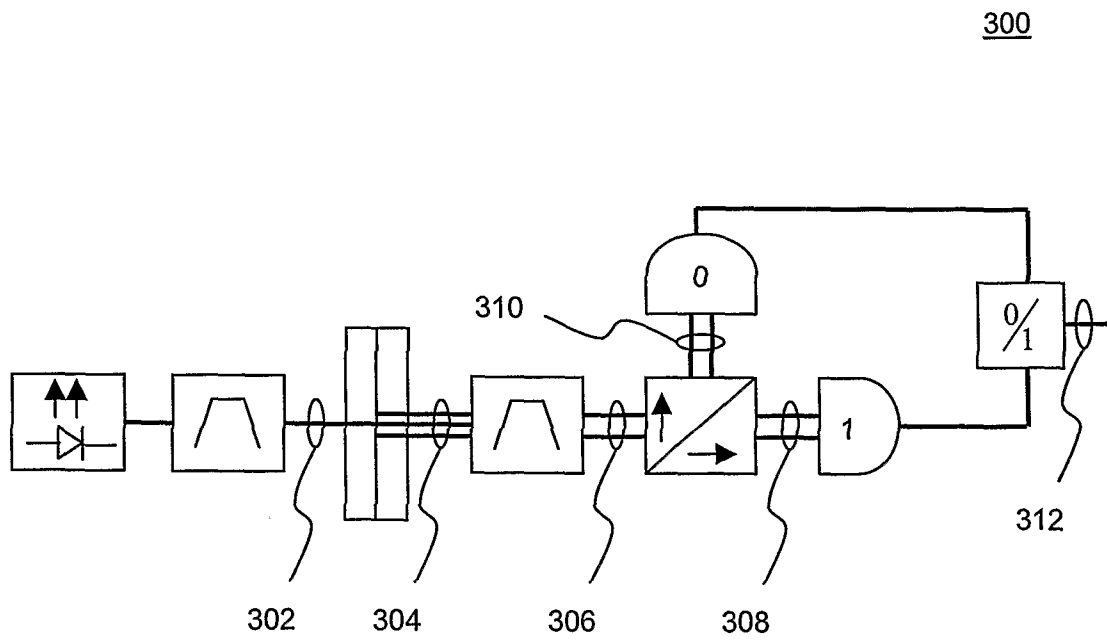


FIG. 3

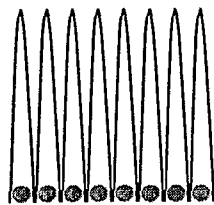


FIG. 4A

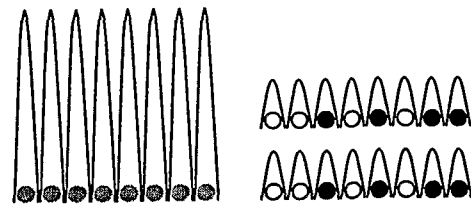


FIG. 4B

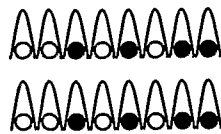


FIG. 4C



FIG. 4D

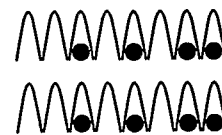


FIG. 4E