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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 January 2021 (14.01.2021)

WIPO | PCT

(10) International Publication Number
WO 2021/006814 A1

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

(21) International Application Number:
PCT/SG2020/050382

(22) International Filing Date:
03 July 2020 (03.07.2020)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10201906290U 05 July 2019 (05.07.2019) SG

(71) Applicant: **NATIONAL UNIVERSITY OF SINGAPORE** [SG/SG]; 21 Lower Kent Ridge Road, Singapore 119077 (SG).

(72) Inventors: **LIM, Ci Wen**; c/o National University of Singapore, Faculty of Engineering, Department of Electrical and Computer Engineering, 21 Lower Kent Ridge Road, Singapore 119077 (SG). **WANG, Chao**; c/o National University of Singapore, Faculty of Engineering, Department of Electrical and Computer Engineering, 21 Lower Kent Ridge Road, Singapore 119077 (SG). **WANG, Yukun**; c/o National University of Singapore, Faculty of Engineering, Department of Electrical and Computer Engineering, 21 Lower Kent Ridge Road, Singapore 119077 (SG).

(74) Agent: **DAVIES COLLISON CAVE ASIA PTE. LTD.**; 10 Collyer Quay #07-01, Ocean Financial Centre, Singapore 049315 (SG).

(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, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO,

(54) Title: QUANTUM RANDOM NUMBER GENERATION SYSTEM AND METHOD

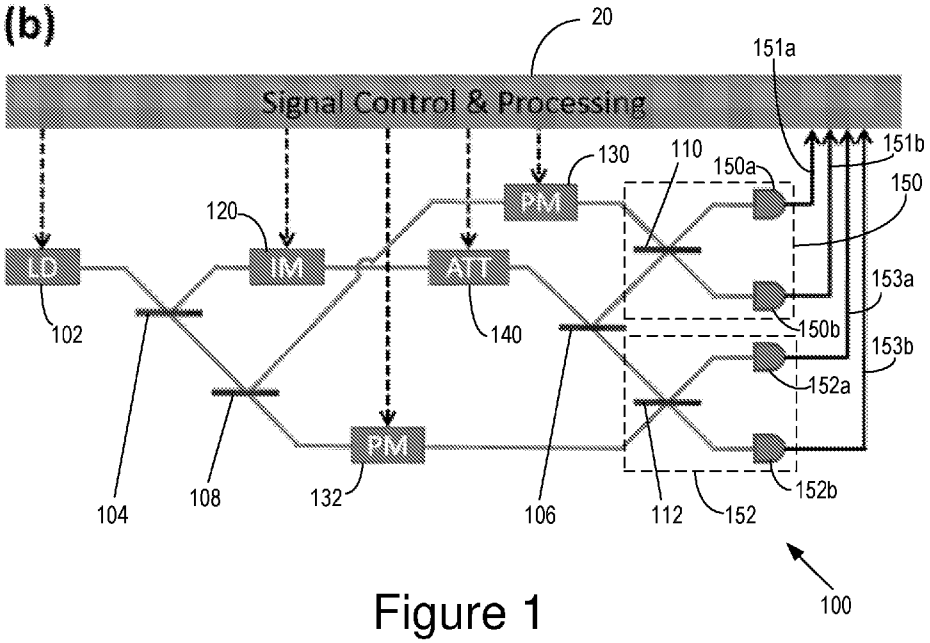

Figure 1

(57) Abstract: A quantum random number generation (QRNG) system includes a single-photon or equivalent single-photon light source; a beam splitter arranged to direct output from the light source to a first homodyne detector having a first local oscillator and a second homodyne detector having a second local oscillator; and a signal control and processing unit. The signal control and processing unit is configured to: vary the phases of the first and second local oscillators; receive, from the first and second homodyne detectors, a plurality of measurements of the output, said plurality of measurements being dependent on the intensity of the light source and the phases of the first and second local oscillators; determine, from the plurality of measurements, whether the CHSH inequality is satisfied; and output one or more random numbers based on whether the CHSH inequality is satisfied.

WO 2021/006814 A1

[Continued on next page]

DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) **Designated States** *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, 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, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *of inventorship (Rule 4.17(iv))*

Published:

— *with international search report (Art. 21(3))*

— *in black and white; the international application as filed contained color or greyscale and is available for download from PATENTSCOPE*

QUANTUM RANDOM NUMBER GENERATION SYSTEM AND METHOD

Technical Field

The present invention relates, in general terms, to a quantum random number generation (QRNG) system and method.

Background

The generation of random numbers is an important activity in many applications, such as cryptography (encryption, authentication, digital signatures), finance (trading algorithms, e-currency), gambling, numerical simulations of physical processes, optimization problems that use Monte Carlo techniques, and fundamental research. The randomness and unpredictability of random numbers is key to information security, especially in cryptographic applications.

Random number generators (RNGs) can be classified into two broad categories: pseudo random number generators (PRNGs), which generate random numbers according to a deterministic algorithm that uses a seed value, and true random number generators (TRNGs), in which random numbers are generated in accordance with unpredictable physical effects, such as turbulences in a flow, or jitter in electrical circuits or circuit components.

A problem with most TRNGs that are based on physical phenomena is that they generate random numbers according to classical physics. Thus, although there is a degree of unpredictability that can be introduced by system noise or chaotic phenomena, the source of random numbers is ultimately deterministic.

As a result, more recently there have been attempts to devise quantum random number generators (QRNGs), based on quantum physical processes. Because quantum phenomena are inherently random, QRNGs provide a way to achieve true random number generation. However, the performance of QRNGs depends on which quantum property is exploited, the proper functioning of system components, and the ability to distinguish between randomness from genuine

quantum process or predictable classical signal.

For example, in one known QRNG product developed by ID Quantique, single photons are injected on a semi-transparent mirror. Depending on which path the photon is detected (reflected or transmitted), the system announces bit 0 or bit 1 as the random output.

The operating principle of the ID Quantique system assumes that single photon generation is fully characterized, that the mirror is an ideal semi-transparent mirror, and that photon detection is perfect. However, if there are some device flaws (as is practically inevitable), or the core components deteriorate over time, the system may not actually implement an ideal quantum process. In other words, it will be difficult to determine if randomness is due to noise or quantum effects.

One solution to this problem is to fully characterize the properties of each component, and to modify the random number generation scheme accordingly. However, this causes another difficulty, namely that it still needs to be verified that the fully characterized system actually produces quantum random numbers in practice. There is presently no clear guidance as to how, or how often, accurate characterization of core quantum components should be performed.

It would be desirable to overcome or alleviate at least one of the above-described problems, or at least to provide a useful alternative.

Summary

Disclosed herein is a quantum random number generation (QRNG) system, including:

a single-photon or equivalent single-photon light source;

a beam splitter arranged to direct output from the light source to a first homodyne detector having a first local oscillator and a second homodyne detector having a second local oscillator; and

a signal control and processing unit configured to:

vary the phases of the first and second local oscillators;

receive, from the first and second homodyne detectors, a plurality of measurements of the output, said plurality of measurements being dependent on the intensity of the light source and the phases of the first and second local oscillators;

determine, from the plurality of measurements, whether the CHSH inequality is satisfied; and

output one or more random numbers based on whether the CHSH inequality is satisfied.

Also disclosed is a quantum random number generation (QRNG) method, including:

directing, by a beam splitter, output from a single-photon or equivalent single-photon light source to a first homodyne detector coupled to a first local oscillator and a second homodyne detector coupled to a second local oscillator;

varying the phases of the first and second local oscillators;

receiving at a signal control and processing unit, from the first and second homodyne detectors, a plurality of measurements of the output, said plurality of measurements being dependent on the intensity of the light source and the phases of the first and second local oscillators;

determining, from the plurality of measurements, whether the CHSH inequality is satisfied; and

outputting one or more random numbers based on whether the CHSH inequality is satisfied.

Also disclosed is a photonic chip including a system as disclosed herein and/or implementing a method as disclosed herein.

Brief description of the drawings

Embodiments of the present invention will now be described, by way of non-limiting example only, with reference to the accompanying drawings in which:

Figures 1(a) and 1(b) show high-level schematic depictions of a quantum

random number generator (QRNG) according to certain embodiments;

Figure 2 is a block diagram of an example architecture of a signal control and processing module of a QRNG;

Figure 3 is a schematic diagram of another possible realization of a QRNG according to certain embodiments;

Figure 4 is a schematic diagram of an example implementation of a QRNG as a photonic chip;

Figure 5 is a graph of the number of random bits as a function of detector threshold, produced by a QRNG according to certain embodiments;

Figure 6 is a graph of CHSH violation as a function of detector threshold for a QRNG according to certain embodiments; and

Figure 7 is another graph of the number of random bits as a function of detector threshold, produced by a QRNG according to certain embodiments.

Detailed description

Embodiments of the present invention provide a method and system for generating certifiable quantum random numbers based on quantum nonlocal correlations and homodyne detection.

Embodiments of the invention are able to guarantee that the output randomness comes from genuine quantum correlations, without using any costly equipment such as single photon detectors.

Embodiments provide a method and system for self-testing QRNG, the randomness of which depends solely on the violation of a Bell's inequality, indicating the genuine random property of quantum entanglement instead of the proper functioning of devices. Accordingly, there can be certainty that the randomness comes from a quantum process, and not from classical noise caused by component deterioration.

In previous QRNG based on Bell's inequality violation, stringent experimental requirements are required, such as high-quality entanglement generation and single photon detection. In contrast, embodiments of the QRNG method disclosed herein can be performed with only off-the-shelf components, such that the cost is greatly reduced compared to previously known approaches.

In general, the method and system according to the present embodiments inject single photons onto a 50:50 beam splitter in a sequence, and thereafter generate a series of entangled quantum states in terms of two different output paths *a* and *b*:

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle_a|1\rangle_b - |1\rangle_a|0\rangle_b)$$

The correlations of these quantum entangled states, which can be quantified by CHSH inequality violations, are utilized to ensure that the randomness is of quantum and not classical nature.

Referring initially to Figure 1(a), an embodiment of a quantum random number generation (QRNG) system 10 includes a single-photon or equivalent single-photon light source 12 configured to output light at single-photon level. The output of source 12 is directed towards a 50:50 beam splitter 14 to generate a train of single-photon entangled states, each of which is detected by either a first measurement device 16 or a second measurement device 18.

The system 10 may broadly be considered to implement three functions: quantum state generation, quantum state measurement, and signal modulation and acquisition.

Quantum state generation may be implemented by the single photon source 12 (which may, for example, include a laser diode, intensity modulator, and attenuator), and the 50:50 beam splitter 14. In the ideal case, a single photon source may be used to generate entanglement. However, it is possible to provide an equivalent single photon source by other means, for example by

using coherent states and the decoy state technique to retrieve the single photon contribution. To perform this technique, the intensity of the coherent states is varied, and appropriate post-processing is performed, as will be described in further detail below. A laser diode may be used to generate the coherent states, an intensity modulator may be used for intensity variation, and an attenuator may be used for single photon level power attenuation.

The quantum state measurement part is depicted as first measurement device 16 and second measurement device 18 in Figure 1(a), which may include two sets of homodyne detectors and associated local oscillators, the phases of which can be controlled by phase modulators. Each homodyne detector may include one pair of photodetectors and electrical amplifiers. By changing the phase of the two local oscillators, measurement statistics conditioned on different settings can be obtained to estimate the degree of Bell violation as well as the minimum randomness that can be obtained from the system.

The first measurement device 16 may comprise a first balanced homodyne detector that is coupled to a first local oscillator; likewise, the second measurement device 18 may comprise a second balanced homodyne detector that is coupled to a second local oscillator. The use of balanced homodyne detectors is advantageous as it means that cooling is not required, thus making the system according to embodiments suitable for integration into photonic chips that operate at room temperature.

The signal modulation and acquisition part, which is represented by the signal control and processing module 20 in Figure 1(a), is responsible for modulation of control signals for components such as the intensity modulator and attenuator of the quantum state generation part and the phase modulators of the quantum state measurement part, real-time calibration of the system, and data processing to generate the final random numbers.

Signal control and processing unit 20 performs a number of functions, including controlling the phases of the first and second local oscillators of the homodyne detectors 16 and 18, controlling the intensity of the source 12, acquiring signals

from photodetectors of homodyne detectors 16 and 18, and performing various processing operations on the acquired signals to facilitate the generation of random numbers. The processing may include, for example, analyzing a sequence of measurements (conditioned on the phases of the local oscillators and the intensity of the source 12) to determine whether the CHSH inequality is satisfied, and thus whether randomness observed in the sequence is due to quantum or classical sources. Randomness extraction may then be performed responsive to detection of violation of the CHSH inequality.

The present invention is predicated on the realization that entanglement of single photons can be used to create random numbers via homodyning measurements on the vacuum and single-photon subspaces. Crucially, in doing so, it is possible to self-test the quality of the quantum process and determine the amount of private randomness that can be extracted from the measurement data. If any system components are faulty, this will be reflected in a reduced degree of Bell violation, and thus a reduction in randomness extraction.

Advantageously, embodiments of the invention make use of ultra-fast homodyne detection and laser sources, thus providing the ability to generate up to and beyond 1GHz of random numbers. In simulations conducted by the present inventors based on off-the-shelf components, it has been found that the method can readily generate up to 1.4 Gbit per second of quantum certified random numbers.

One possible realization of a QRNG system is shown in schematic form in Figure 1(b), in which solid lines represent optical paths, solid lines with arrows represent output signals, and dotted lines with arrows represent control signals.

The QRNG system 100 implements quantum state generation using a laser diode 102 that irradiates a first beam splitter 104. The first beam splitter is arranged to direct a first beam towards an intensity modulator 120, the output of which is directed towards an attenuator 140 that is arranged to attenuate the power of the first beam to single-photon level. The output of the attenuator 140 is directed towards a second beam splitter 106 to generate an entangled state.

The QRNG system 100 implements quantum state measurement using a first balanced homodyne detector 150 and a second balanced homodyne detector 152. A third beam splitter 108 is arranged to receive a second beam from the first beam splitter 104, and to further split the second beam along first and second optical paths towards respective phase modulators 130 and 132. The first phase modulator 130 feeds into the first balanced homodyne detector 150, to provide a first local oscillator signal for the first balanced homodyne detector 150. Likewise, the second phase modulator 132 feeds into the second balanced homodyne detector 152, to provide a second local oscillator signal for the second balanced homodyne detector 152. First balanced homodyne detector 150 includes a beam splitter 110 arranged to direct input photons from the quantum state generation part and the phase modulator 130 into photodetectors 150a and 150b. Second balanced homodyne detector 152 includes a beam splitter 112 arranged to direct input photons from the quantum state generation part and the phase modulator 132 into photodetectors 152a and 152b.

The QRNG system 100 further includes a signal control and processing (SCP) module 20. SCP module 20 transmits control signals to laser diode 102, intensity modulator 120, attenuator 140, and phase modulators 130, 132 to change the intensity of the coherent states from laser diode 102, and the phases of the local oscillator signals for homodyne detectors 150, 152. SCP module 20 also receives photocurrent measurements from the homodyne detectors 150, 152 which form the basis of random number generation. Photocurrent from the photodetectors 150a, 150b travels along signal lines 151a, 151b to SCP module 20, and photocurrent from 152a, 152b travels along signal lines 153a, 153b.

An example architecture of an SCP module 20 is shown in Figure 2. Part or all of the SCP module 20 may be a self-contained component, such as a system-on-a-chip (SOC), but it will be appreciated that different sub-modules of SCP module 20 may form part of separate physical components.

SCP module 20 may include a signal input component 202 to receive photocurrent signals from homodyne detectors 150 and 152, and may also

receive signals from other parts of the QRNG, for example for diagnostic purposes. SCP module 20 also includes a control signal output module 204 that enables the SCP 20 to transmit control signals to components such as the laser diode 102, intensity modulator 120, and attenuator 140, to switch them on or off or to tune them to achieve a desired output intensity. Control signal output 204 also transmits signals to phase modulators 130 and 132 to control their operation, for example to switch between two predetermined phase values of the local oscillators of the homodyne detectors.

The photocurrent signals received at signal input 202 may be preprocessed using methods known in the art, by a preprocessing module 203, and the preprocessed signals may be transmitted to other components of the SCP 20 for further processing.

SCP 20 also includes a process control module 210 that coordinates the overall operation of the SCP 20, and thus of the QRNG 100.

For example, process control module 210 may be configured to conduct a calibration process, via calibration module 212. Calibration module 212 may be configured to turn on laser diode 102, calibrate the intensity of the coherent states using the intensity modulator 120 and attenuator 140, and calibrate the phase references of the local oscillators with phase modulators 130 and 132, by monitoring the homodyne detector 150, 152 output signals received at signal input 102.

Process control module 210 may also be configured to carry out a random number generation process by modulating the intensity and phase of coherent states produced by laser diode 102, determining a plurality of photocurrent measurements at the different intensities and phases, and then passing the plurality of photocurrent measurements to one or more data processing modules that extract random numbers based on the photocurrent measurements.

For example, in each measurement round, process control module 210 may determine the specific intensity of the coherent state $\mu \in \{\mu_1, \mu_2, \ldots \mu_M\}$ and the

phase choices of the local oscillators θ_j^i, where $i \in \{a, b\}$ represents one of the two balanced homodyne detectors 150 and 152, and $j \in \{0,1\}$ indicates two different phase settings of the local oscillator. The intensity and phase choices are then propagated, via intensity modulation component 206 and phase modulation component 208, to intensity modulator 120, attenuator 140, and phase modulators 130, 132, via the control signal output 204.

Process control module 210 may then receive a plurality of photocurrent measurements performed by the balanced homodyne detectors 150, 152. The raw photocurrent measurements may be provided to post-processing module 214, which determines a measurement outcome $M_{i,j}^{\mu}$ from each balanced homodyne detector 150 or 152.

Each measurement outcome represents a photocurrent difference between the photodetectors of the homodyne detector (e.g., the difference between photocurrents measured by photodetectors 150a and 150b of homodyne detector 150). The measurement outcome is conditioned on intensity of the quantum state μ and the phase settings of local oscillator $j \in \{0,1\}$. That is, each measurement is associated with a particular quantum state intensity and local oscillator phase setting.

Post-processing module 214 may compare the measurement results $M_{i,j}^{\mu}$ with a set of predefined post-selecting thresholds$\{-t, t\}$. As will be understood by those skilled in the art, the thresholds may be selected in order to optimize the random number generation rate. If $M_{i,j}^{\mu} > t$, the final measurement result of the specific balanced homodyne detector $\widetilde{M_{i,j}^{\mu}}$ is assigned to be 1, and if $M_{i,j}^{\mu} < -t$, $\widetilde{M_{i,j}^{\mu}}$ is assigned to be -1.

Next, by conditioning on different settings of θ_j^i and related measurement outcome $\widetilde{M_{i,j}^{\mu}}$, post-processing module 214 can obtain the normalized correlation probability (for each coherent state μ), $P^{\mu}_{j_a,j_b,\widetilde{M_{a,j}^{\mu}},\widetilde{M_{b,j}^{\mu}}}$. Further, by deploying the

decoy state technique, the post-processing module 214 can obtain the single photon contribution of the correlation measurement, $P^1_{j_a,j_b,\widetilde{M^{\mu}_{a,j}},\widetilde{M^{\mu}_{b,j}}}$.

The decoy state technique can be used to obtain the statistics of single photon events in the following way.

In the system according to the presently disclosed embodiments, phase-randomized weak coherent states (WCS) having three or more different intensities are used to reconstruct the single photon statistics with high precision.

By randomizing the phase of the coherent states, the density matrix of the coherent state can be rewritten as the mixture of density matrices of a series of photon number states (Fock states), which follows the Poisson distribution. Then the success probability (i.e., the probability that a coherent state generates measurements that fulfil the CHSH inequality) of the three WCS $\{\mu_1, \mu_2, \mu_3\}$ can be represented as:

$$Q_{\mu_1} = P^0_{\mu_1} Y^0 + P^1_{\mu_1} Y^1 + P^2_{\mu_1} Y^0 + \cdots$$

$$Q_{\mu_2} = P^0_{\mu_2} Y^0 + P^1_{\mu_2} Y^1 + P^2_{\mu_2} Y^2 + \cdots$$

$$Q_{\mu_3} = P^0_{\mu_3} Y^0 + P^1_{\mu_3} Y^1 + P^2_{\mu_3} Y^2 + \cdots$$

In the above, Q_{μ_1} indicates the probability that the system obtains successful events (i.e., events that satisfy the CHSH inequality) when phase-randomized coherent state μ_1 is used, $P^0_{\mu_1}$ indicates the probability of zero photons occurring in the WCS with intensity μ_1, and Y^0 means the probability that the system obtains successful events when the zero-photon Fock state $|0\rangle$ has been used, and likewise for the other quantities above. Because the coherent states are weak coherent states, the probabilities of more than 2 photons are very small,

and can be neglected to a good approximation such that the above sums can be truncated at 2-photon order.

Accordingly, by solving the three linear equations above, it is possible to obtain P^1, which is the single photon contribution.

In some embodiments, more than three coherent states may be used in the decoy state technique. This will result in higher precision in the estimate of P^1. It will be understood that the sums above may then be extended to higher order, such that, for example, if four weak coherent states are used, the 3-photon contribution can be included such that there are four equations in four unknowns.

In some previous implementations of the decoy state technique, one or more vacuum states are used as the decoy states. In at least some of the presently disclosed embodiments, all states are weak coherent states.

The single photon correlation probabilities may be provided to a CHSH violation detector 216. Based on the normalized correlation probability, CHSH violation detector 216 can evaluate the Bell violation observed in the system using an inequality called the CHSH inequality:

$$S = E\left(\theta_0^a, \theta_0^b\right) + E\left(\theta_0^a, \theta_1^b\right) + E\left(\theta_1^a, \theta_0^b\right) - E\left(\theta_1^a, \theta_1^b\right),$$

where $E(\theta_{j_a}^a, \theta_{j_b}^b) = (P_{j_a,j_b,-1,-1}^1 - P_{j_a,j_b,-1,1}^1 - P_{j_a,j_b,1,-1}^1 + P_{j_a,j_b,1,1}^1) / (P_{j_a,j_b,-1,-1}^1 + P_{j_a,j_b,-1,1}^1 + P_{j_a,j_b,1,-1}^1 + P_{j_a,j_b,1,1}^1)$. As is known to those skilled in the art, any strategy based on a local deterministic event will lead to $S \leq 2$, while for entangled quantum systems, the outcome of two measurement settings may result in $S > 2$, meaning that not all the observed outputs can be predetermined and that at least some of the results arise from intrinsic quantum correlations. Accordingly, if CHSH violation detector 216 determines that $S > 2$, the current round of measurements may be used to generate quantum random numbers by randomness extraction or privacy amplification.

In cases where $S > 2$, the CHSH violation detector 216 passes the $\widetilde{M_{i,j}^{\mu}}$ to a randomness extractor 218. The amount of randomness (R) of the system 100 (the average number of extractable random numbers in each experimental trial) can be linked to CHSH statistics through the Von Neumann entropy:

$$R \geq 1 - h_2\left(\frac{1}{2} + \frac{1}{2}\sqrt{\frac{S^2}{4} - 1}\right)$$

Randomness extractor 218 may take into account realistic system imperfections like statistical fluctuations of measurement results, possible correlations among a series of measurements, and deploy a more rigorous formula to estimate the final amount of random numbers in a given total number of trials.

Thereafter, a randomness extractor can be constructed accordingly, to distill the final random numbers. For example, a hashing function, such as a universal hashing function, may be used for randomness extraction (see R. Renner and R. König, Universally Composable Privacy Amplification Against Quantum Adversaries. In Theory of Cryptography, 407 – 425 (Springer, 2005), the contents of which are hereby incorporated by reference). In one example, a Toeplitz-hashing extractor may be used. In another example, Trevisan's extractor may be used (see X. Ma et al., Phys. Rev. A 87, 062327, the contents of which are hereby incorporated by reference). Many other randomness extraction or privacy amplifications that are suitable for use in quantum random number generated may be used, as will be appreciated by those skilled in the art.

A seed value for the randomness extractor may be obtained by, for example, using random numbers generated from previous rounds of measurement and random number extraction. Since a universal hashing function does not need to be changed during every round, use of some of the previously generated random numbers should not excessively consume the generated random numbers.

Referring now to Figure 3, a further example of a QRNG 300 is shown. QRNG 300 implements quantum state generation using a laser diode 302 that irradiates a polarizing beam splitter 310. A polarization controller 304 may be interposed in the beam path between the laser diode 302 and first beam splitter 310 to control the intensity distribution between the signal and local oscillators of two balanced homodyne detectors 350, 352. The polarizing beam splitter is arranged to direct a first beam towards an intensity modulator 320, the output of which is directed, via a polarization modulator 330, towards an attenuator 340 that is arranged to attenuate the power of the first beam to single-photon level. The polarization modulator 330 may be used to randomize the phase of the signal for implementation of the decoy state mechanism. In some embodiments, the polarization modulator 330 may not be required for this purpose; for example, a gain-switched laser diode 302 may be used to generate a pulse of coherent states, thereby providing intrinsically random phases for the decoy state mechanism to be deployed. The output of the attenuator 340 is directed towards a beam splitter 314 to generate an entangled state.

The QRNG system 300 implements quantum state measurement using a first balanced homodyne detector 350 and a second balanced homodyne detector 352. A third beam splitter 312 is arranged to receive a second beam from the first (polarizing) beam splitter 310, and to further split the second beam along first and second optical paths towards respective phase modulators 332 and 334. The first phase modulator 332 feeds into the first balanced homodyne detector 350, to provide a first local oscillator signal for the first balanced homodyne detector 350. Likewise, the second phase modulator 332 feeds into the second balanced homodyne detector 352, to provide a second local oscillator signal for the second balanced homodyne detector 352. First and second balanced homodyne detectors 350, 352 may be structured in similar fashion to the first and second homodyne detectors 150, 152 of Figure 1(b).

The components of the QRNG system 300 are each coupled to a signal control and processing (SCP) module, such as the SCP module 20, though these connections are not shown in Figure 4.

Advantageously, the QRNG systems 100, 300 are able to generate quantum random numbers at greater speed than previously known systems, using standard optical components instead of costly and highly customized components such as single-photon detectors. The speed of the QRNG system 100, 300 can be boosted further, by deploying high speed balanced homodyne detectors (such as Finisar CPRV1222A light sensors) for quantum entanglement detection, instead of using conventional shot-noise-limited (SNL) BHDs. A high-speed BHD may have a nominal 3dB bandwidth of 25GHz, over 20 times faster than the state-of-the-art SNL BHD. To address the high electrical noise problem, three reasonable assumptions on the electrical noise can be made: 1) electrical noise from two detectors (e.g. 150, 152) should be independent from each other, 2) electrical noise is independent of the measured quantum signal and 3) it possesses a Gaussian distribution. As such, if these assumptions hold, the effect of electrical noise is equivalent to optical loss on the signal. Hence, the resultant output of the laser source together with the equivalent optical loss can be seen as the source of quantum states. Since the electrical noise of the detectors is independently localized, they will not contribute to the nonlocal correlations of the single photon entangled state. Therefore, the influence of the electrical noise can be easily removed, overcoming the strict trade-off between noise and bandwidth in electrical circuit designs that use SNL BHD.

In fact, other practical issues, like the noise of the data acquisition equipment (e.g. ADC), inefficiency of the photodiode, polarization mismatch between signal and local oscillators and the like, can also be addressed with this loss-equivalent scheme, leading towards the quantum maximal violation of the CHSH inequality.

In a lab-scale system, the output of the BHDs (e.g. 150, 152) may be acquired by a high speed oscilloscope (Tektronix DPO72004C) with a bandwidth of 20GHz and a sample rate of 50 GS/s. The acquired data can then be stored for offline digital signal processing (DSP). As a consequence, the down-converted data with a sample rate of 40GS/s possesses a minimum correlation among the trials according to the Wiener-Khinchin theorem. As will be appreciated, and as discussed above, some embodiments may implement a QRNG in integrated

circuit form (such as in a photonic chip), in which case the data acquisition and DSP functions may be integrated in components within the chip itself.

In some embodiments, the final random output bits may be obtained through high speed randomness extraction on FPGA hardware. In order to account for finite data size effects, the Entropy Accumulating Theorem (EAT) may be used to obtain a random number generation rate in the security proof.

A possible realization of a QRNG as a photonic chip will now be described with reference to Figure 4. The photonic chip 400 is analogous to the QRNG system 300 shown in Figure 3.

It will be appreciated that the photonic chip 400 comprises a number of components and features that are typical for such devices, such as a substrate, and at least one light-guiding (photonic circuit) layer, and that the light-guiding structures may comprise optical fibers, optical waveguides and the like. These components and features will not be described in detail herein.

Photonic chip 400 implements quantum state generation using a laser diode 402 that irradiates a beam splitter 410. Unlike the arrangement of Figure 3, with beam splitters 310 and 312, a single 3-output beam splitter can be used to guide light from the laser diode 402 into three different paths 431, 432 and 433. Paths 431 and 433 are used to generate a local oscillator signal for balanced homodyne detectors 450 and 452 respectively, by phase modulation implemented by respective phase modulators 412 (along path 431) and 414 (along path 433).

Light travels along path 432 to a first interferometer 420 that functions as an intensity modulator. Intensity modulator 420 comprises a first beam splitter 422 that splits the beam into first and second beams, the beams then recombining at a second beam splitter 426, with the first beam having traversed phase modulator 424 on the way. The phase modulator 424 is under the control of signal control and processing module 20.

The output of the intensity modulator 420 is directed towards a second interferometer 440 that functions as an attenuator. Attenuator 440 comprises a first beam splitter 442 that guides light into first and second paths which recombine at a second beam splitter 446. Light travelling along the first path traverses a phase modulator 444 which, again, is under the control of signal control and processing module 20, such that the attenuator 440 can be configured to attenuate the power of the beam emerging from the attenuator 440 to single-photon level. The phase modulator 444 may be used to randomize the phase of the signal for implementation of the decoy state mechanism, or the laser diode 402 may be a gain-switched laser diode that is used to generate a pulse of coherent states, thereby providing intrinsically random phases for the decoy state mechanism to be deployed.

The output of the attenuator 440 is an entangled state that is generated by the beam splitter 446 once the signal has been attenuated to single-photon level. The output entangled state is then measured using the first balanced homodyne detector 450 and second balanced homodyne detector 452. First balanced homodyne detector 450 includes a beam splitter 460 arranged to direct input photons from the attenuator 440 and the phase modulator 412 into photodetectors 450a and 450b. Second balanced homodyne detector 452 includes a beam splitter 462 arranged to direct input photons from the attenuator 440 and the phase modulator 414 into photodetectors 452a and 452b.

As mentioned above, the first phase modulator 412 feeds into the first balanced homodyne detector 450, to provide a first local oscillator signal along path 431 for the first balanced homodyne detector 450. Likewise, the second phase modulator 414 feeds into the second balanced homodyne detector 452, to provide a second local oscillator signal along path 433 for the second balanced homodyne detector 452.

Experimental results

To simulate the practical performance of the QRNG system 100, a realistic model was developed, in accordance with the teachings of J. Appel, D. Hoffman, E. Figueroa, and A. I. Lvovsky, Phys. Rev. A 75, 035802 (2007), the entire contents of which are hereby incorporated by reference, to take into account realistic system imperfections like electrical noise of homodyne detectors 150 and 152, statistical fluctuation of measurements, etc.

The total number of trials (with each trial corresponding to one measurement result from each homodyne detector) for the simulation was set to be 10^{10}. The simulation demonstrated that intrinsic random numbers can be obtained from the system 100 as a function of the post-selecting threshold $\{-t, t\}$, which is illustrated in Figure 5.

Figure 5 shows the total amount of random numbers versus the post-selecting threshold t. δ, ϵ_s, and ϵ_e are error parameters for the calculation. Curve a is the ideal result without considering electrical noise or statistical fluctuations. Curve b corresponds to the results when considering statistical fluctuations and security analysis but without noise. Curve c is the amount of random numbers that can be obtained in practical systems, under the consideration of system noise, statistical fluctuations, etc.

From curve c of Figure 5, which considers practical system imperfections, it can be seen that if the working frequency of the system 100 is set to be 1GHz, a rough random number generation rate of around 140 Mbits/sec can be obtained. This is much higher than existing commercial QRNG products from ID Quantique, which gives a generation rate of 4 Mbits/sec for a single device.

A system in accordance with QRNG 300 was constructed and used to perform quantum random number generation. Using optimized parameters from theoretical analysis of the system 300 (i.e., by modelling the system 300 and determining parameters which maximize the amount of extractable randomness), a CHSH violation of 2.38 was achieved, which can lead to a high throughput random number generation of larger than 1 Gbps.

Figures 6 and 7 show experimental results from the QRNG 300. Figure 6 shows CHSH violation versus threshold settings. The dash-dotted line 602 shows the theoretical CHSH violation (as reflected by S, as discussed above) with an ideal single photon source. The solid line 604 shows the theoretical CHSH violation when a three-intensity decoy state method is used. The circles indicate experimental results achieved by system 300.

Figure 7 shows the final random number generation rate versus the threshold. The solid line indicates the theoretical (simulated) random number generation rate when a three-intensity decoy state method is used, while the circles indicate the experimental results.

As can be seen from the foregoing, embodiments of the present invention provide a simple and economical way to generate randomness from an intrinsic entangled quantum system, which is not influenced by the functioning of constitutive components like beam splitters, detectors, and the like. Instead, modulation of phases and intensities is used to generate measurements from which the randomness can be extracted. This is much easier to control than the condition of electrical or optical system components. In addition, embodiments can be implemented using standard components, thus facilitating implementation in photonic chips. Furthermore, according to simulation results, the estimated amount of random numbers of the presently proposed system can be much higher than that of known QRNG products.

Many modifications will be apparent to those skilled in the art without departing from the scope of the present invention.

Throughout this specification, unless the context requires otherwise, the word "comprise", and variations such as "comprises" and "comprising", will be understood to imply the inclusion of a stated integer or step or group of integers or steps but not the exclusion of any other integer or step or group of integers or steps.

The reference in this specification to any prior publication (or information derived from it), or to any matter which is known, is not, and should not be taken as an acknowledgment or admission or any form of suggestion that that prior publication (or information derived from it) or known matter forms part of the common general knowledge in the field of endeavor to which this specification relates.

Claims

1. A quantum random number generation (QRNG) system, including:

a single-photon or equivalent single-photon light source;

a beam splitter arranged to direct output from the light source to a first homodyne detector having a first local oscillator and a second homodyne detector having a second local oscillator; and

a signal control and processing unit configured to:

vary the phases of the first and second local oscillators;

receive, from the first and second homodyne detectors, a plurality of measurements of the output, said plurality of measurements being dependent on the intensity of the light source and the phases of the first and second local oscillators;

determine, from the plurality of measurements, whether the CHSH inequality is satisfied; and

output one or more random numbers based on whether the CHSH inequality is satisfied.

2. A QRNG system according to claim 1, wherein the light source is configured to generate a plurality of coherent states of varying intensity, and wherein the system includes an attenuator for attenuating the output to single-photon level.

3. A QRNG system according to claim 1 or claim 2, wherein the signal control and processing unit is configured to determine a set of single photon correlation probabilities from said plurality of measurements; and determine, based on the set of single photon correlation probabilities, whether the CHSH inequality is satisfied.

4. A QRNG system according to any one of claims 1 to 3, wherein the signal control and processing unit is configured to apply a threshold to respective measurements prior to determining whether the CHSH inequality is satisfied.

5. A QRNG system according to any one of claims 1 to 4, wherein the signal control and processing unit is configured to apply a randomness extractor to the one or more random numbers.

6. A QRNG system according to claim 5, wherein the randomness extractor is a universal hashing function.

7. A quantum random number generation (QRNG) method, including:

directing, by a beam splitter, output from a single-photon or equivalent single-photon light source to a first homodyne detector coupled to a first local oscillator and a second homodyne detector coupled to a second local oscillator;

varying the phases of the first and second local oscillators;

receiving at a signal control and processing unit, from the first and second homodyne detectors, a plurality of measurements of the output, said plurality of measurements being dependent on the intensity of the light source and the phases of the first and second local oscillators;

determining, from the plurality of measurements, whether the CHSH inequality is satisfied; and

outputting one or more random numbers based on whether the CHSH inequality is satisfied.

8. A QRNG method according to claim 7, wherein the light source is configured to generate a plurality of coherent states of varying intensity; and wherein the method includes attenuating the output to single-photon level.

9. A QRNG method according to claim 7 or claim 8, including determining a set of single photon correlation probabilities from said plurality of measurements; and determining, based on the set of single photon correlation probabilities, whether the CHSH inequality is satisfied.

10. A QRNG method according to any one of claims 7 to 9, including applying a threshold to respective measurements prior to determining whether the CHSH inequality is satisfied.

11. A QRNG method according to any one of claims 7 to 10, including applying a randomness extractor to the one or more random numbers.

12. A QRNG method according to claim 11, wherein the randomness extractor is a universal hashing function.

13. A photonic chip including a QRNG system according to any one of claims 1 to 6, and/or configured to implement a QRNG method according to any one of claims 7 to 12.

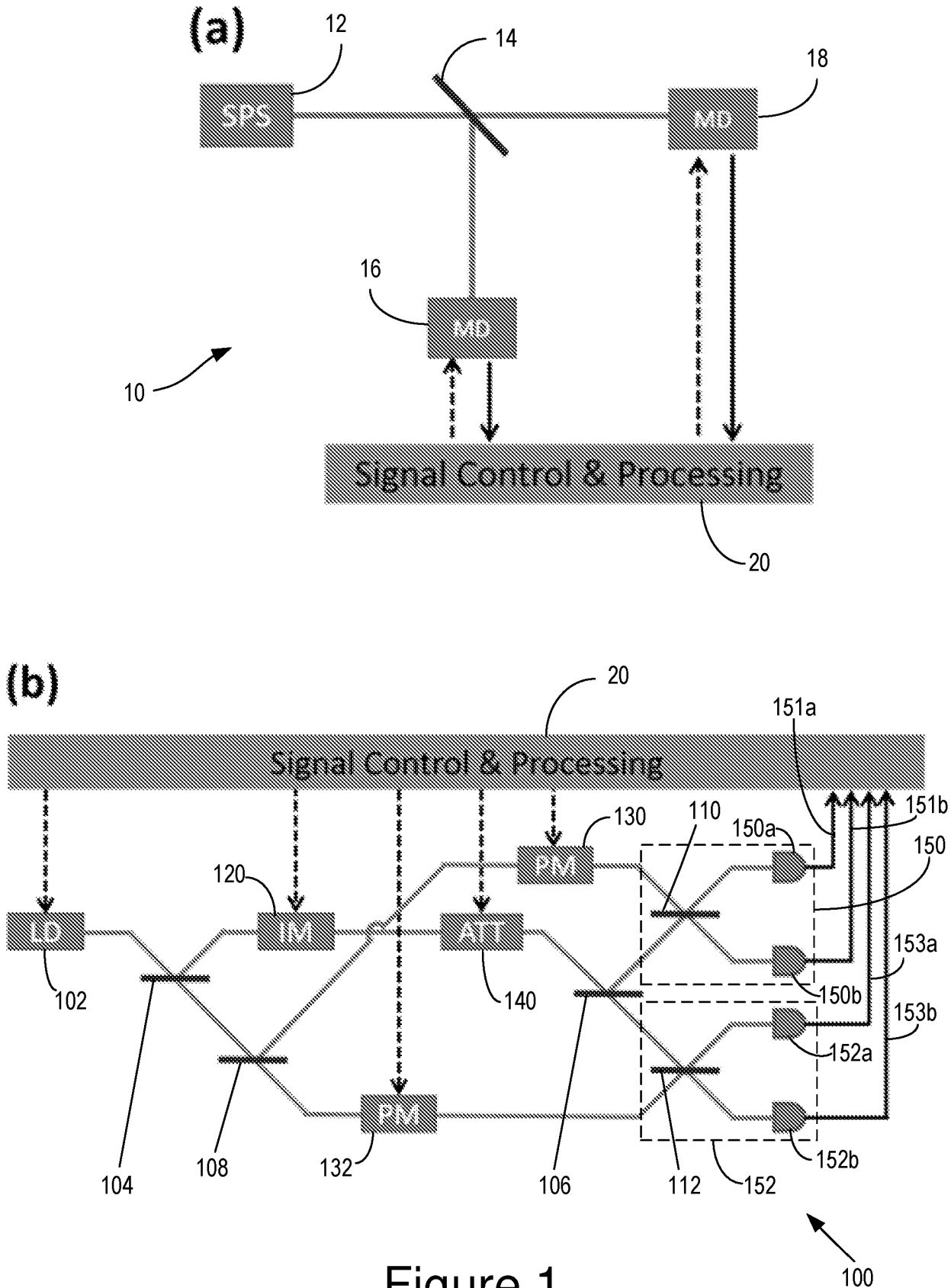
(a)
12
14
18
SPS
MD
16
MD
10
Signal Control & Processing
20
(b)
20
Signal Control & Processing
151a
151b
130
110
150a
150
PM
120
LD
IM
ATT
153a
102
140
150b
153b
152a
PM
104
108
132
106
112
152
152b
100

Figure 1

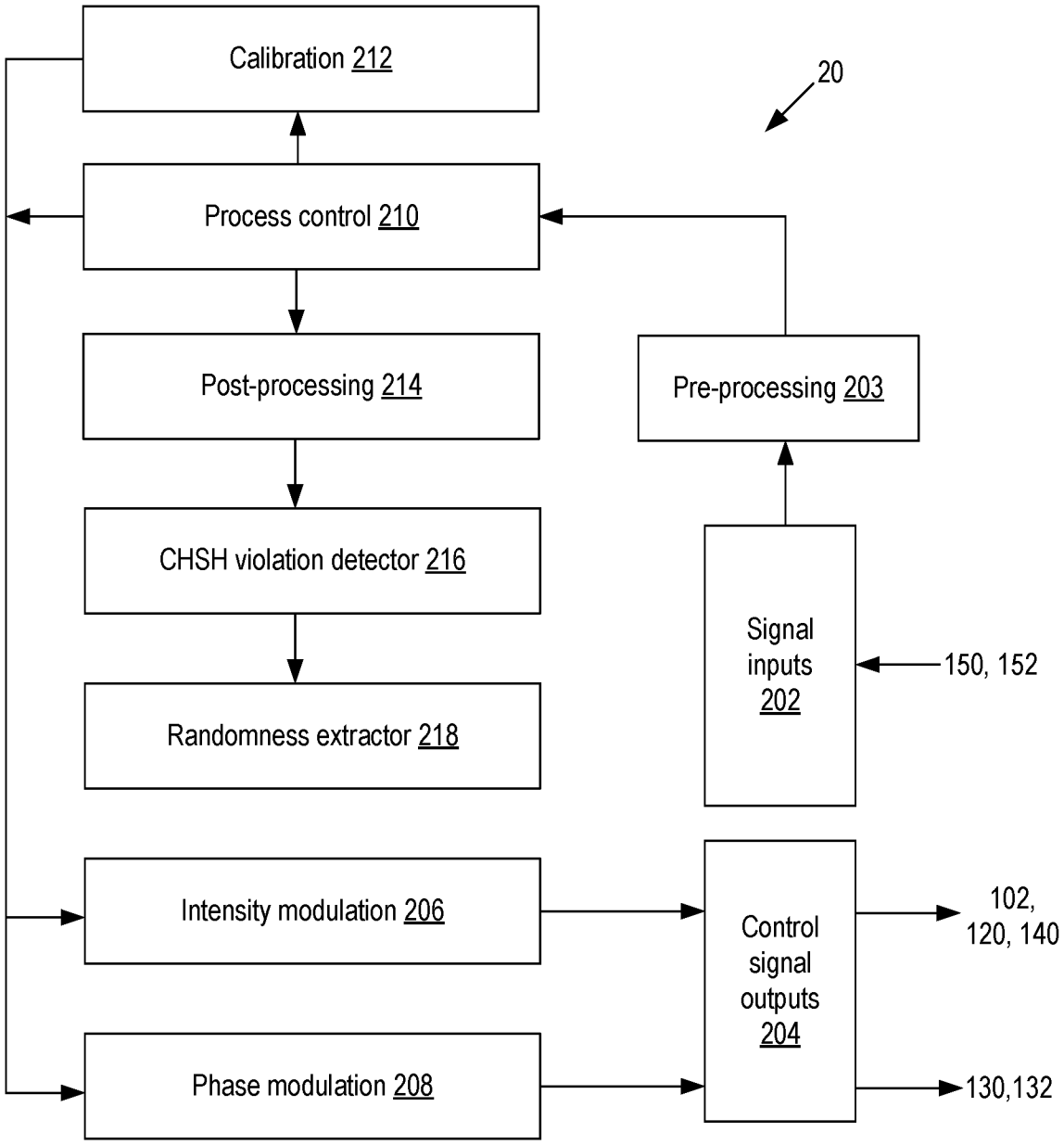
Calibration 212
20
Process control 210
Post-processing 214
Pre-processing 203
CHSH violation detector 216
Signal inputs 202
150, 152
Randomness extractor 218
Intensity modulation 206
Control signal outputs 204
102, 120, 140
Phase modulation 208
130,132

Figure 2

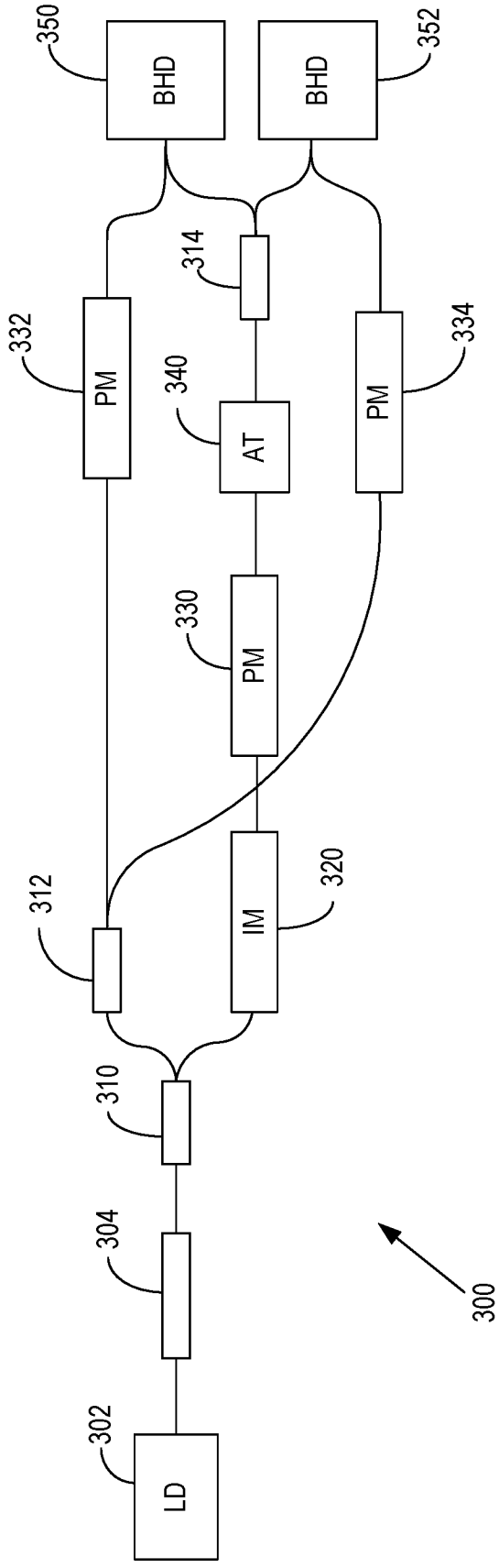
350
BHD
352
BHD
314
332
PM
340
AT
334
PM
330
PM
312
320
IM
310
304
302
LD
300

Figure 3

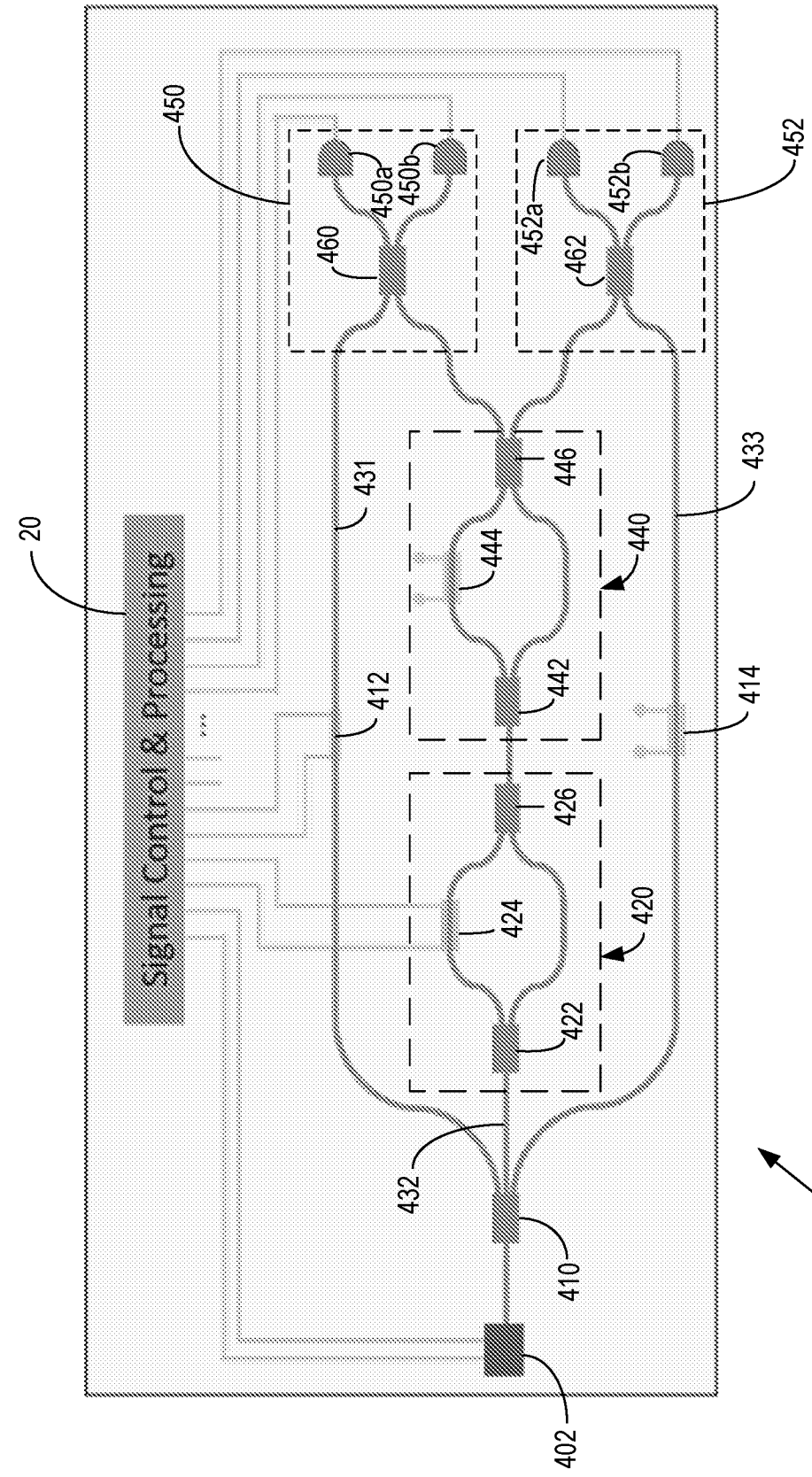
(c)
20
Signal Control & Processing
450
450a
450b
460
452
452a
452b
462
431
433
446
444
440
412
414
442
426
424
420
422
432
410
402
400

Figure 4

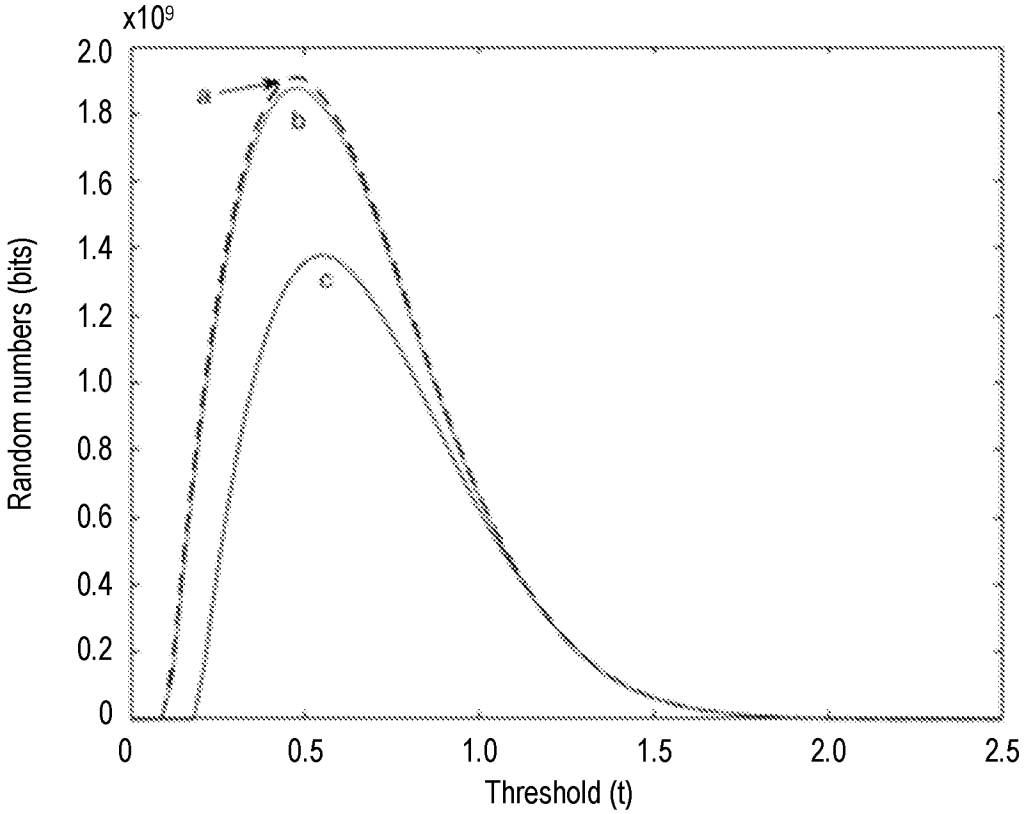
x10^9
2.0
1.8
1.6
1.4
1.2
1.0
0.8
0.6
0.4
0.2
0
Random numbers (bits)
0
0.5
1.0
1.5
2.0
2.5
Threshold (t)

Figure 5

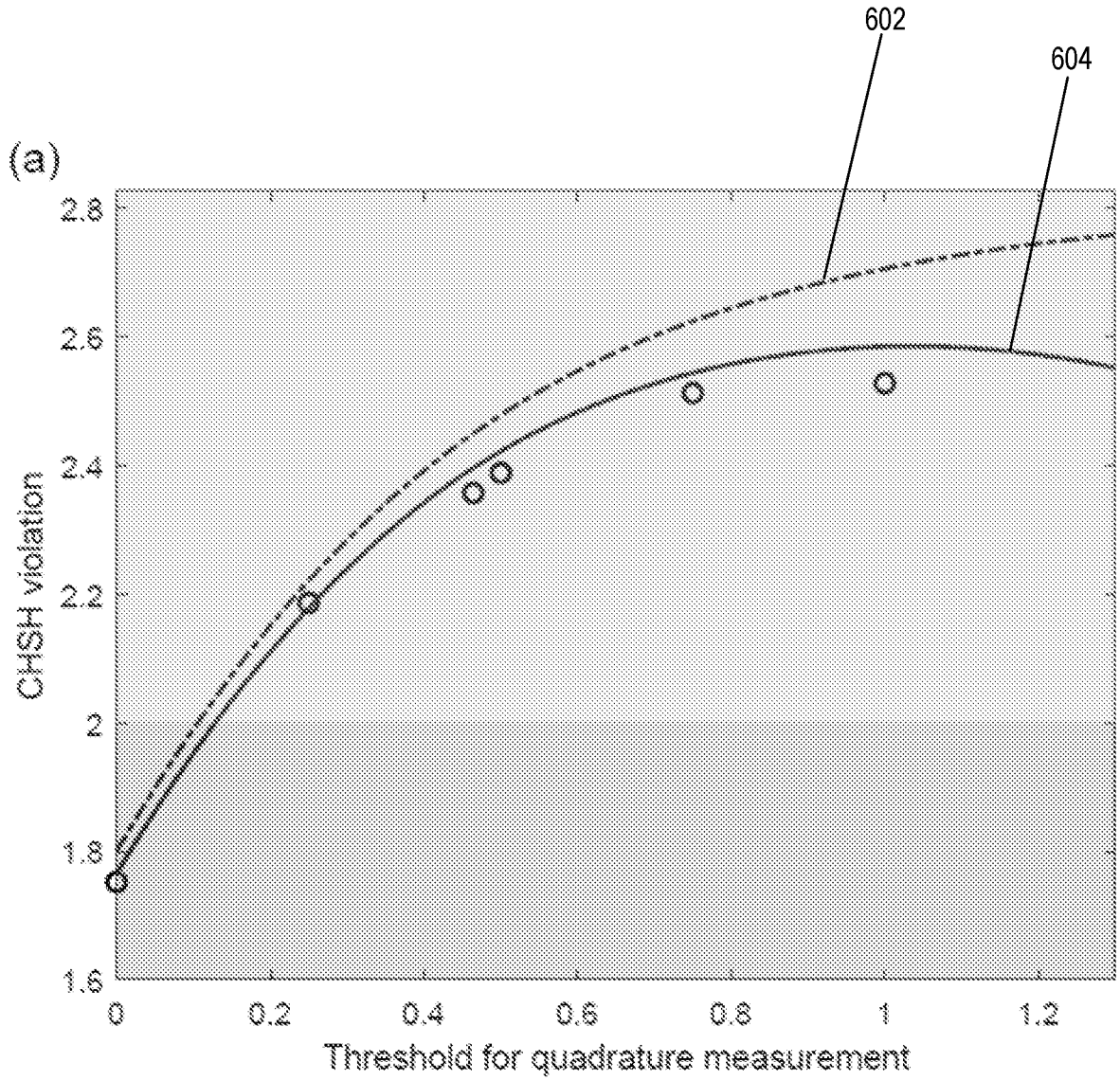
602
604
(a)
2.8
2.6
2.4
2.2
2
1.8
1.6
CHSH violation
0
0.2
0.4
0.6
0.8
1
1.2
Threshold for quadrature measurement

Figure 6

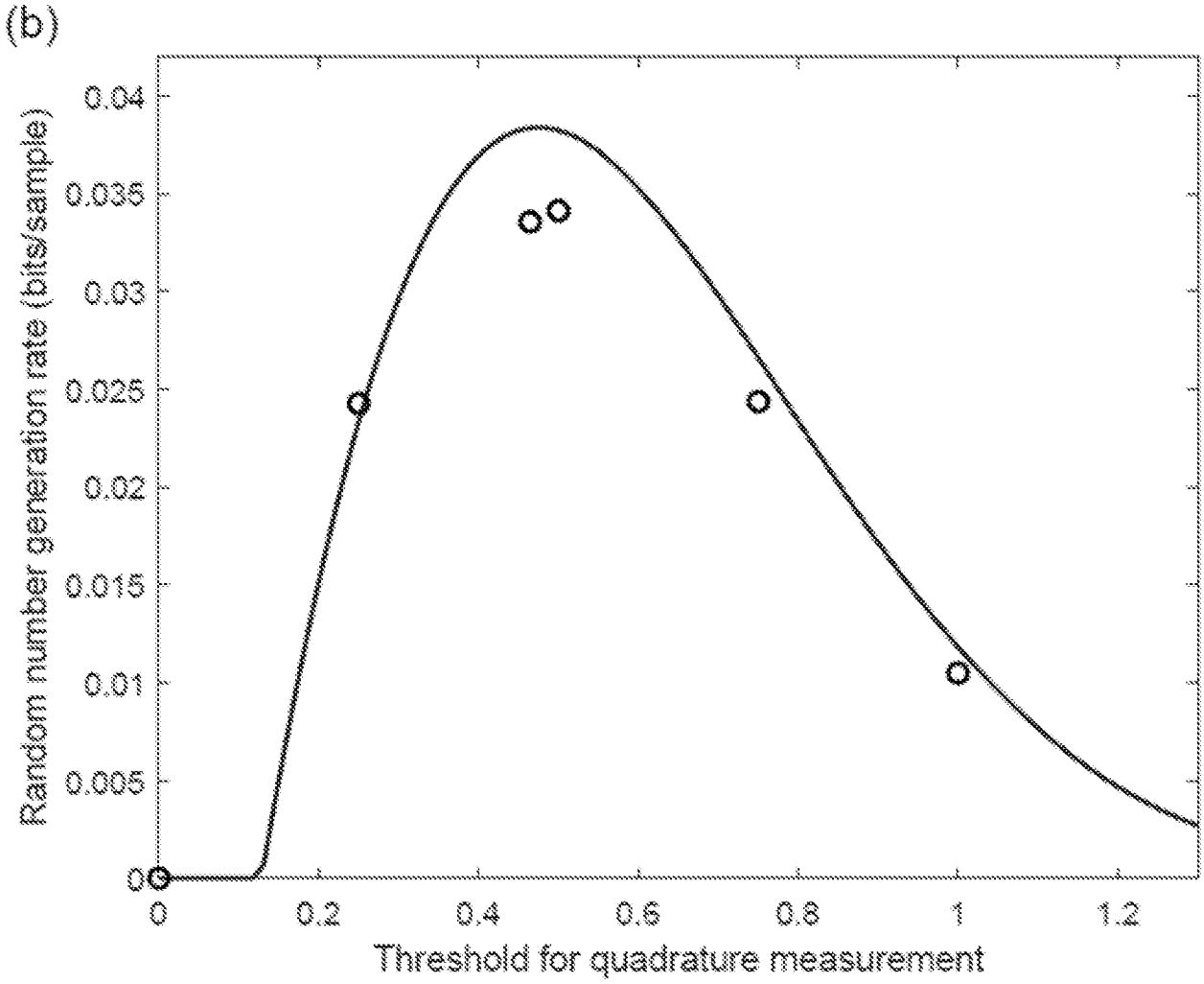
(b)
Random number generation rate (bits/sample)
0.04
0.035
0.03
0.025
0.02
0.015
0.01
0.005
0
0
0.2
0.4
0.6
0.8
1
1.2
Threshold for quadrature measurement

Figure 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SG2020/050382

A. CLASSIFICATION OF SUBJECT MATTER

G06F 7/58 (2006.01)

According to International Patent Classification (IPC)

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F, H04L, H04B, B82Y

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

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

FAMPAT/IEEE Xplore/CNKI: quantum random number generator, QRNG, 量子乱数产生器, beam splitter, 分束器, 分光镜, 分光器, dichroic mirror, 二向色镜, 分色镜, single photon, 单光子, homodyne detector, 零差, 检波器, 探测器, 检测器, oscillator, 振荡器, 震荡器, 发振器, CHSH inequality, CHSH 不等式, Bell's inequality, 贝尔不等式, and other relevant term

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	LIU Y. ET AL., Device-independent quantum random-number generation. *Nature*, 19 September 2018, Vol. 562, pages 548–55 [Retrieved on 2020-08-31] <DOI: HTTPS://DOI.ORG/10.1038/S41586-018-0559-3> Whole document	1-13
A	CN 108984153 A (UNIVERSITY OF SCIENCE AND TECHNOLOGY OF CHINA) 11 December 2018 Whole document of the original non-English language document (a machine translation is enclosed **only** for your reference)	
A	EP 3040853 A1 (UNIVERSITÀ DEGLI STUDI DI PADOVA) 6 July 2016 Whole document, especially Figure 6	

☒ 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

"D" document cited by the applicant in the international application

"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
31/08/2020 *(day/month/year)*	*31/08/2020* *(day/month/year)*

Name and mailing address of the ISA/SG

IPOS INTELLECTUAL PROPERTY OFFICE OF SINGAPORE

Intellectual Property Office of Singapore
1 Paya Lebar Link, #11-03
PLQ 1, Paya Lebar Quarter
Singapore 408533

Email: pct@ipos.gov.sg

Authorized officer

Wang Jiayi (Dr)

IPOS Customer Service Tel. No.: (+65) 6339 8616

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SG2020/050382

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2005-250714 A (NIHON UNIVERSITY) 15 September 2005 Whole document, especially Paragraphs [0015]-[0016] of the machine translation; Figure 1 of the original non-English language document	
A	LEE S.-Y. ET AL., Single-photon quantum nonlocality: Violation of the Clauser-Horne-Shimony-Holt inequality using feasible measurement setups. *PHYSICAL REVIEW A*, 26 January 2017, Vol. 95, pages 012134 [Retrieved on 2020-08-31] <DOI: 10.1103/PHYSREVA.95.012134> Whole document, especially Figure 1 and Table 1	

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/SG2020/050382

Note: This Annex lists known patent family members relating to the patent documents cited in this International Search Report. This Authority is in no way liable for these particulars which are merely given for the purpose of information.

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
CN 108984153 A	11/12/2018	NONE	
EP 3040853 A1	06/07/2016	NONE	
JP 2005-250714 A	15/09/2005	NONE	