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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
08 August 2019 (08.08.2019)

WIPO | PCT

(10) International Publication Number
WO 2019/149383 A1

(51) International Patent Classification:
*H04B 10/70* (2013.01) *H04L 9/08* (2006.01)

(21) International Application Number:
PCT/EP2018/052829

(22) International Filing Date:
05 February 2018 (05.02.2018)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)** [SE/SE]; 164 83 Stockholm (SE).

(72) Inventors: **CAVALIERE, Fabio**; Ericsson Telecomunicazioni SpA Via Moruzzi 1, 56100 Pisa (IT). **FRESI, Francesco**; Via Moruzzi 1, 56100 Pisa (IT). **MUHAMMAD, Imran**; Via Moruzzi 1, 56100 Pisa (IT). **POTI, Luca**; Via Moruzzi 1, 56100 Pisa (IT).

(74) Agent: **ERICSSON**; Patent Development, Torshamnsgatan 21-23, 164 80 STOCKHOLM (SE).

(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, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, 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, SM, ST, SV, SY, TH, 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, 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).

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

(54) Title: QUANTUM KEY DISTRIBUTION APPARATUS, SYSTEM AND METHOD

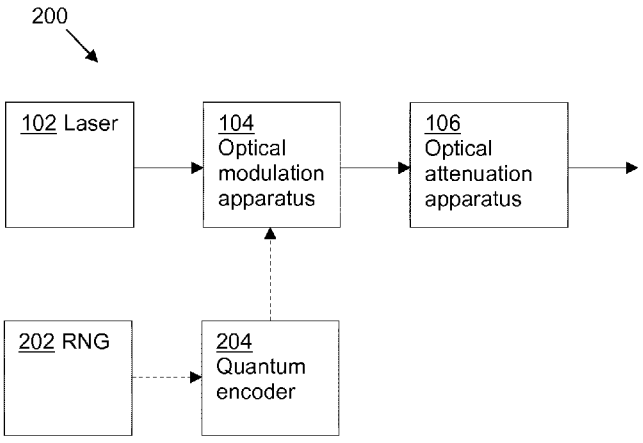


Fig. 2

(57) Abstract: Quantum key distribution apparatus (200) comprising: a gain switched laser (102) configured to generate optical pulses; optical modulation apparatus (104, 402) configured to apply at least one of a respective phase modulation and a respective intensity modulation to the optical pulses to encode respective quantum states on the optical pulses; a random number generator (202); a quantum encoder (204) configured to map a number received from the random number generator into a respective quantum state and to generate an output signal comprising an indication of said least one of a respective phase modulation and a respective intensity modulation; and optical attenuation apparatus (106) configured to attenuate the optical pulses to approximate a single photon source.

WO 2019/149383 A1

# QUANTUM KEY DISTRIBUTION APPARATUS, SYSTEM AND METHOD

## Technical Field

The invention relates to quantum key distribution apparatus, a quantum key distribution system and a method of quantum key distribution.

## Background

Quantum communications systems exploit the possibility of transmitting information encoded in quantum states over an optical fibre link. Quantum states are prepared in such a way that an eavesdropper unavoidably introduces a disturbance in the quantum states transmitted between two interlocutors. Such a disturbance reveals the eavesdropper's activity to the two legitimate partners.

Quantum Key Distribution, QKD, was theoretically proposed in 1984, and the first experimental demonstration came in 1991. The functional blocks of a conventional QKD system are: a Quantum Random Number Generator, QRNG, which generates really randomly distributed voltage values, based on fundamental quantum mechanics principles (thermal or shot noise, photoelectric effect, etc.); an optical modulator, which maps the random number into a physical quantum variable, such as the spin, orbital angular momentum, wavelength, or phase of a photon; an optical fibre link, similar to a classical optical link (note, however, the optical fibre link cannot contain optical amplifiers, due to the non-cloning theorem); an optical filter at the receiver to remove out-of-band noise, which is detrimental for the single photon counting process at the receiver; and an extremely sensitive photodetector, which is ideally able to count single incoming photons. A QKD system is used to implement a quantum cryptography protocol, such as Bennett and Brassard's protocol of quantum cryptography, BB84, as reported for example in S. Agnolini and P. Gallion, "Implementation of BB84 protocol by QPSK modulation using dual-electrode Mach-Zehnder modulator", IEEE ICIT 2004, pages 250-253.

In a conventional QKD system implementation, light source, QRNG and optical modulator are separate blocks. An integrated implementation would allow cost savings but it is not straightforward to achieve, due to the different technologies required. While the optical modulator can be a standard optical phase modulator, single photon sources operating at 1550nm (the wavelength used for optical fibre communication) require technologies which are far from reaching the maturity necessary for commercialization and large-scale production.

At the receiver side, there are two major issues in developing QKD systems that can eventually be commercialized, both often neglected in the specialized scientific literature. Firstly, the optical signal must be filtered by a narrow band filter, having steep edges, in order to cancel the out-of-band noise which would interfere with the received each single photon. On one hand, this requires the use of active filters, to keep the filter's central frequency locked to

that of the incoming signal. On the other hand, in a QKD system, the incoming signal is so weak that control loop operation for frequency locking is troublesome, due to noise. Secondly, due to the weakness of the received signal, consisting of single photons, clock synchronization is extremely problematic.

## Summary

It is an object to provide an improved quantum key distribution apparatus. It is a further object to provide an improved quantum key distribution system. It is a further object to provide an improved method of quantum key distribution.

An aspect of the invention provides quantum key distribution apparatus comprising a gain switched laser, optical modulation apparatus and optical attenuation apparatus. The gain switched laser is configured to generate optical pulses. The optical modulation apparatus is configured to apply at least one of a respective phase modulation and a respective intensity modulation to the optical pulses to encode respective quantum states on the optical pulses. The optical attenuation apparatus is configured to attenuate the optical pulses to approximate a single photon source.

The quantum key distribution, QKD, apparatus advantageously uses a gain switched laser, which has been shown to generate spectrally uncorrelated optical pulses, i.e. optical pulses having independent and randomly distributed phases. An eavesdropper intercepting and measuring one optical pulse therefore cannot infer anything about any other optical pulse transmitted by the QKD apparatus. The optical pulses can therefore be attenuated to approximate a single photon source, removing the need to use a single photon source. The QKD apparatus is a linear scheme, which advantageously does not require additional pump lasers or control loops.

In an embodiment, the quantum key distribution apparatus is configured to implement an encryption protocol. The gain switched laser is configured to generate optical pulses having phases which are randomly distributed between preselected values, dependent on the encryption protocol.

In an embodiment, the optical modulation apparatus is an asymmetric Mach-Zehnder interferometer. Both phase and intensity modulation are advantageously applied in a single device, enabling improved silicon photonic integration.

In an embodiment, the asymmetric Mach-Zehnder interferometer is additionally configured as the optical attenuation apparatus. Both phase modulation and optical attenuation are advantageously applied in a single device, enabling improved silicon photonic integration.

In an embodiment, the optical attenuation apparatus comprises an optical attenuator and the quantum key distribution apparatus further comprises a tuneable optical filter before the optical attenuator. The tuneable optical filter is configured to confine the optical power of the optical pulses around a nominal central frequency. Out-of-band noise may therefore be

removed from the optical pulses, before they are attenuated to approximate a single photon source.

In an embodiment, the quantum key distribution apparatus further comprises a random number generator and a quantum encoder. The quantum encoder is configured to map a number received from the random number generator into a respective quantum state. The quantum encoder is configured to generate an output signal comprising an indication of at least one of a respective phase modulation and a respective intensity modulation to be applied by the optical modulation apparatus to encode the quantum state onto a respective optical pulse.

In an embodiment, the random number generator is configured to generate random bits and the quantum encoder is configured to map a bit received from the random number generator into a respective quantum state.

In an embodiment, the quantum encoder is configured to map a bit sequence received from the random number generator into a respective quantum state.

In an embodiment, the random number generator is a quantum random number generator, QRNG, comprising an optical splitter, an optical interferometer, an optical detector and signal processing apparatus. The optical splitter is configured to power split the optical pulses generated by the laser. The optical interferometer is configured to receive optical pulses from the optical splitter. The optical interferometer comprises a delay element in one arm. The delay element is configured to apply a delay to an optical pulse propagating in said arm such that successive optical pulses are interfered by the optical interferometer, to convert a phase difference between successive optical pulses into an intensity modulation of an output optical signal of the optical interferometer. The optical detector is arranged to detect the output signal. The signal processing apparatus is configured to convert a detected intensity of the output signal into a corresponding amplitude level and to generate an output signal comprising an indication of the amplitude level.

The QRNG of the QKD apparatus advantageously uses the optical pulses generated by the gain switched laser for QKD transmission, and therefore does not require a fully separate QRNG.

In an embodiment, an algorithm is used to derive numbers having a target distribution from the randomly distributed detected intensities.

In an embodiment, the optical attenuation apparatus is selectively operable in one of a first state and a second state. In the first state the optical attenuation apparatus is configured to attenuate the optical pulses to approximate a single photon source. In the second state the optical attenuation apparatus is configured with a minimum attenuation. The QKD apparatus is advantageously operable to swap between two different working conditions: a classical transmission state, where the optical attenuation apparatus is set at a minimum attenuation, and is thereby effectively by-passed, making the optical pulses so strong to enable frequency locking of tuneable optical filters and clock synchronization; and QKD transmission state, where

the attenuation is increased in order to have quasi single-photon emission and quantum key distribution.

In an embodiment, the optical attenuation apparatus is configured to attenuate the optical pulses to such level that a photon number of the optical pulses has an average Poisson distribution of less than 1.

In an embodiment, the optical attenuation apparatus is configured to attenuate the optical pulses to such level that a photon number of the optical pulses has an average Poisson distribution of 0.1.

In an embodiment, the quantum states comprise signal states and at least one decoy state. Decoy states may thus be generated by the same apparatus as signal states.

In an embodiment, the quantum encoder is configured to set a number of decoy states and respective amplitudes of the decoy states according to the encryption protocol. Decoy states may thus be generated by the same apparatus as signal states, by simply setting a required amplitude to be applied by the optical modulation apparatus.

Corresponding embodiments apply also to the quantum key distribution system described below.

An aspect of the invention provides a quantum key distribution system comprising first and second quantum key distribution apparatus. The first and second quantum key distribution apparatus each comprise a gain switched laser, optical modulation apparatus and optical attenuation apparatus. The gain switched laser is configured to generate optical pulses. The optical modulation apparatus is configured to apply at least one of a respective phase modulation and a respective intensity modulation to the optical pulses to encode respective quantum states on the optical pulses. The optical attenuation apparatus is configured to attenuate the optical pulses to approximate a single photon source.

The quantum key distribution, QKD, system advantageously uses gain switched lasers, which have been shown to generate spectrally uncorrelated optical pulses, i.e. optical pulses having independent and randomly distributed phases. An eavesdropper intercepting and measuring an optical pulse transmitted across the QKD system therefore cannot infer anything about any other optical pulse transmitted across the QKD system. The optical pulses can therefore be attenuated to approximate a single photon source, removing the need to use a single photon sources. The QKD system is a linear scheme, which advantageously does not require additional pump lasers or control loops.

In an embodiment, each optical attenuation apparatus is selectively operable in one of a first state and a second state. In the first state the optical attenuation apparatus is configured to attenuate the optical pulses to approximate a single photon source. In the second state the optical attenuation apparatus is configured with a minimum attenuation. The QKD system is advantageously operable to swap between two different working conditions: a classical transmission state, where each optical attenuation apparatus is set at a minimum attenuation, and are thereby effectively by-passed, making the optical pulses so strong to enable frequency

locking of tuneable optical filters and clock synchronization; and QKD transmission state, where the attenuation is increased in order to have quasi single-photon emission and quantum key distribution.

In an embodiment, the first and second quantum key distribution apparatus each further comprise an optical receiver and a tuneable optical filter. Each optical receiver is for receiving an incoming optical signal from the other quantum key distribution apparatus. Each tuneable optical filter is arranged before the respective optical receiver for removing out of band noise from the incoming optical signal. Each quantum key distribution apparatus is operable to tune respective central frequencies of the tuneable optical filters to respective frequencies of the incoming optical signals when the respective optical attenuation apparatus is in the second state. In the second state, where each optical attenuation apparatus is set at a minimum attenuation, and is thereby effectively by-passed, the optical pulses are so strong as to enable frequency locking of tuneable optical filters at the receivers.

In an embodiment, the quantum key distribution apparatus are additionally operable to perform clock synchronisation when the optical attenuators are in the second state. The QKD system is advantageously operable to enable easy clock synchronisation, making the QKD system one which may be practically implemented.

An aspect of the invention provides a method of quantum key distribution comprising steps of: generating optical pulses having independent and randomly distributed phases; applying at least one of a respective phase modulation and a respective intensity modulation to the optical pulses to encode respective quantum states on the optical pulses; and attenuating the optical pulses to approximate a single photon source.

Using optical pulses having independent and randomly distributed phases means that the optical pulses are spectrally uncorrelated, so an eavesdropper intercepting and measuring an optical pulse cannot infer anything about any other optical pulses that she may intercept. The optical pulses can therefore be attenuated to approximate a single photon source, removing the need to use a single photon sources.

In an embodiment, the optical pulses have phases which are randomly distributed between preselected values which are dependent on an encryption protocol.

In an embodiment, the method additionally comprises optically filtering the optical pulses to confine the optical power of the optical pulses around a nominal central frequency before attenuating the optical pulses. Out-of-band noise may therefore be removed from the optical pulses, before they are attenuated to approximate a single photon source.

In an embodiment, the method further comprises steps of: generating random numbers; mapping the random numbers into respective quantum states; and determining at least one of a respective phase modulation and a respective intensity modulation to be applied to encode the quantum states onto respective optical pulses.

In an embodiment, the random numbers are random bits and the random bits are mapped into respective quantum states.

In an embodiment, bit sequences are mapped into respective quantum states.

In an embodiment, the random numbers are generated by: power splitting the optical pulses generated by the laser; interfering successive optical pulses to convert a phase difference between successive optical pulses into an intensity modulation of an output optical signal; detecting the intensity of the output optical signal; converting a detected intensity of the output optical signal into a corresponding amplitude level; and generating an output signal comprising an indication of the amplitude level. Quantum random number generation may be advantageously achieved using the same optical pulses as for QKD transmission, and therefore does not require a fully separate QRNG.

In an embodiment, an algorithm is used to derive numbers having a target distribution from the randomly distributed detected intensities.

In an embodiment, the optical pulses are selectively attenuated at a first attenuation to approximate a single photon source or at a second, minimum, attenuation. The method may advantageously swap between two different working conditions: a classical transmission state, where a minimum attenuation is used, making the optical pulses so strong as to enable frequency locking of tuneable optical filters and clock synchronization; and a QKD transmission state, where the attenuation is increased in order to have quasi single-photon emission and quantum key distribution.

In an embodiment, the optical pulses are attenuated to such level that a photon number of the optical pulses has an average Poisson distribution of less than 1.

In an embodiment, the optical pulses are attenuated to such level that a photon number of the optical pulses has an average Poisson distribution of 0.1.

In an embodiment, the quantum states comprise signal states and at least one decoy state.

In an embodiment, a number of decoy states and respective amplitudes of the decoy states is set according to an encryption protocol to be implemented.

In an embodiment, the method further comprises tuning respective central frequencies of tuneable optical filters to respective frequencies of incoming optical signals when the optical pulses are attenuated at the second, minimum, attenuation, the tuneable optical filters arranged for removing out of band noise from the incoming optical signal.

In an embodiment, the method further comprises performing clock synchronisation when the optical pulses are attenuated at the second, minimum, attenuation.

Embodiments of the invention will now be described, by way of example only, with reference to the accompanying drawings.

## Brief Description of the drawings

Figures 1 to 4 illustrate quantum key distribution apparatus according to embodiments of the invention;

Figures 5 to 7 illustrate quantum key distribution systems according to embodiments of the invention;

Figure 8 illustrates an experimental setup used to verify phase randomness;

Figure 9 shows phase distribution (top) and autocorrelation (bottom) measured using the experimental setup of Figure 8;

Figure 10 shows the Pearson correlation coefficient of the pulses transmitted in the experimental set up of Figure 8; and

Figures 11 to 14 illustrate steps of methods of quantum key distribution according to embodiments of the invention.

## Detailed description

The same reference numbers will used for corresponding features in different embodiments.

An embodiment of the invention, as illustrated in Figure 1, provides quantum key distribution, QKD, apparatus 100 comprising a gain switched laser 102, optical modulation apparatus 104 and optical attenuation apparatus 106.

The gain switched laser is configured to generate optical pulses. The gain switching mechanism produces spectrally uncorrelated optical pulses, i.e. optical pulses having independent and randomly distributed phases, as discussed in more detail with reference to Figures 8 to 10, so that it is not possible, even in principle, for an eavesdropper to infer information about one transmitted pulse by measuring previously transmitted pulses. The gain switched laser may be a directly modulated laser, such as a vertical cavity side emitting laser, VCSEL, or a distributed feedback, DFB, laser and the gain switching mechanism is due to a change of carriers in the laser chip active region caused by modulating the drive current supplied to the laser.

Gain switching is a technique by which a laser can be made to produce pulses of extremely short duration, of the order of picoseconds. In a semiconductor laser, the optical pulses are generated by injecting a large number of carriers (electrons) into the active region of the device, bringing the carrier density within that region from below to above the lasing threshold. When the carrier density exceeds the lasing threshold, the ensuing stimulated emission results in the generation of a large number of photons. However, carriers are depleted as a result of the stimulated emission faster than they are injected, so the carrier density eventually falls back below the lasing threshold which results in the termination of the optical output. If carrier injection has not ceased during this period, then the carrier density in the active region will increase again and the process will repeat itself, generating optical pulses.

The optical modulation apparatus 104 is configured to apply at least one of a respective phase modulation and a respective intensity modulation to the optical pulses, to encode respective quantum states on the optical pulses. A real zero (no optical pulse) and a one (optical

pulse), plus intermediate decoy states, can then be encoded onto the optical pulses by intensity modulation applied by the optical modulation apparatus.

The optical attenuation apparatus 106 is configured to attenuate the optical pulses to approximate a single photon source. An optical source may be considered to be a single photon source if a photon number of the optical pulses has an average Poisson distribution of less than 1. In one embodiment, the optical attenuation apparatus is configured to attenuate the optical pulses to such level that a photon number of the optical pulses has an average Poisson distribution of 0.1.

In an embodiment, the QKD apparatus is configured to implement an encryption protocol. The gain switched laser is configured to generate optical pulses having phases which are randomly distributed between preselected values, dependent on the encryption protocol, such as phase encoded BB84 or decoy states differential phase shift QKD. The preselected phase values may for example be 0 and $\pi$, or 0 and $2\pi$.

Referring to Figure 2, an embodiment of the invention provides QKD apparatus 200 which additionally comprises a random number generator, RNG, 202 and a quantum encoder 204.

The quantum encoder 204 is configured to map a number received from the RNG into a respective quantum state. The quantum encoder is also configured to generate an output signal comprising an indication of at least one of a respective phase modulation and a respective intensity modulation to be applied by the optical modulation apparatus to encode the quantum state onto a respective optical pulse.

In an embodiment, the RNG is configured to generate random bits and the quantum encoder is configured to map a bit received from the random number generator into a respective quantum state. The quantum encoder may be configured to map a bit sequence received from the RNG into a respective quantum state.

Referring to Figures 3 and 4, an embodiment of the invention provides QKD apparatus 400 further comprising a tuneable optical filter 404 and an optical attenuator 406.

The RNG is a quantum random number generator, QRNG, 300 and the optical modulation apparatus is an asymmetric Mach-Zehnder interferometer, AMZI, 402, as illustrated in Figure 4.

The QRNG comprises a first optical splitter 302, an optical interferometer 310, an optical detector 318 and signal processing apparatus 320. The first optical splitter 302 is configured to power split the optical pulses generated by the laser 102, so an optical pulse train output from the laser 102 is split into two equivalent optical pulse trains, one delivered to the AMZI 402 and the other delivered to the optical interferometer 312. The QRNG therefore advantageously uses the optical pulses generated by the laser 102 for QKD, so a fully separate QRNG is not required, saving cost and reducing the size of the QKD apparatus.

The optical interferometer 310 comprises a second optical splitter 312, a delay element 314 and a Mach-Zehnder interferometer, MZI, 316. The optical interferometer 310 is therefore

also an AMZI. The second optical splitter 312 is configured to power split optical pulses received from the first optical splitter 302, so the optical pulse train delivered from the first optical splitter 302 is further split into two equivalent optical pulse trains, one delivered to the delay element 314 and the other delivered to the MZI 316.

The delay element 314 is configured to apply a delay to optical pulses propagating in in one arm of the optical interferometer 310, such that when the two pulse trains are combined at the output of the MZI 316, successive optical pulses are interfered. Random phase differences between successive optical pulses, as generated by the laser 102, are thereby converted into corresponding intensity modulations of an output optical signal of the optical interferometer 310.

The optical detector, which here is a photodiode 318, is arranged to detect the output signal from the MZI 316. The signal processing apparatus, which here is a digital signal processing, DSP, 320 apparatus is configured to convert a detected intensity of the output signal into a corresponding amplitude level and to generate an output signal comprising an indication of the amplitude level. The output signal from the QRNG is delivered to the quantum encoder 204, as described above.

In an embodiment, an algorithm is used to derive numbers having a target distribution from the randomly distributed detected intensities. Common algorithms such as inverse transform sampling or the Box-Muller transformation, for transforming uniformly distributed random variables to a new set of random variables with a Gaussian (or Normal) distribution, may be used.

The AMZI 402 may be configured to apply phase modulation, intensity modulation or both to the optical pulses, under the control of the quantum encoder 204. The AMZI 402 comprises two arms 426, 428, an electrode pair 420 for applying an intensity modulation, IM, and a variable delay line 422 and an unbalance electrode 424 for applying a phase modulation, PM. The voltages and a control signal for the delay line 422 are provided by the quantum encoder 204, to control the amount of phase modulation and/or intensity modulation required to be applied to an optical pulse in order to encode a respective quantum state on the optical pulse.

A quantum state may therefore be encoded in the phase difference between the optical pulses in the two arms of the AMZI 402, in the intensity/amplitude of the optical pulses output from the AMZI or in both phase difference and intensity.

The quantum states are signal states and one or more decoy states, which are applied by means of intensity modulation. In an embodiment, the quantum encoder is configured to set a number of decoy states and respective amplitudes of the decoy states according to the encryption protocol in use, such as phase encoded BB84 and decoy states differential phase shift QKD, as described in "Decoy State Quantum Key Distribution", Physical Review Letters, 94, 230504, 2005. Decoy states are encoded in accordance with pre-determined occurrence probabilities for the respective encryption protocol.

In this embodiment, a separate optical attenuator 406 is provided to attenuate the optical pulses to approximate a single photon source. Alternatively, the AMZI 402 may be configured as both optical modulation and optical attenuation apparatus, so a separate optical attenuation apparatus is not required; the AMZI is configured to apply a phase modulation but no intensity modulation in this alternative arrangement.

The tuneable optical filter 404 is provided before the optical attenuator 406 and is configured to confine the optical power of the optical pulses around a nominal central frequency. Out-of-band noise may therefore be removed from the optical pulses, before they are attenuated. The tuneable optical filter may be a micro-ring, a Bragg grating, or a liquid crystal thin film device, depending on level of silicon integration required for the construction of the QKD apparatus.

Referring to Figure 5, an embodiment of the invention provides a QKD system 500 comprising first and second QKD apparatus 100, 200, 400 as described above.

In an embodiment, the optical attenuation apparatus 106, optical attenuator 406 or AMZI 402 configured for optical attenuation, is selectively operable in either a first, 'QKD transmission', state or a second, 'classical transmission', state. In the QKD transmission state, the optical attenuation apparatus is configured to attenuate the optical pulses to approximate a single photon source, to have quasi single-photon emission and quantum key distribution. In the classical transmission state the optical attenuation apparatus is configured with a minimum attenuation. By setting the optical attenuation apparatus to a minimum attenuation, it is effectively by-passed, making the optical pulses so strong as to enable frequency locking of tuneable optical filters and clock synchronization between pairs of QKD apparatus, such as in the QKD system of Figure 5. Tuning of filters, frequency locking of laser and decoy state levels can be configured when the optical attenuator is set to minimum (second state).

Embodiment of the invention provide QKD systems 600, 700, as illustrated in Figures 6 and 7, in which the first and second QKD apparatus 100, 200, 400 each further comprise an optical receiver 602 and a tuneable optical filter 604.

The optical receiver 602 is for receiving an incoming optical signal from the other QKD apparatus. The tuneable optical filter 604 is arranged before the optical receiver for removing out of band noise from the incoming optical signal.

Each QKD apparatus is operable to tune respective central frequencies of the tuneable optical filters 604 to respective frequencies of the incoming optical signals when the optical attenuation apparatus of each QKD apparatus is in the second state.

In an embodiment, each QKD apparatus 100, 200, 400 is operable to perform clock synchronisation when the optical attenuation apparatus of each QKD apparatus is in the second state.

Compared to other QKD schemes, the QKD apparatus 100, 200, 400 is much cheaper due to the absence of a separate QNRG, the use of cost effective directly modulated lasers, like VCSELs, and the use of a regular optical modulation apparatus, which can be realized in

Silicon photonics. In addition, the QKD system is a linear scheme, which does not require additional pump lasers or control loop. The QKD system 600, 700 also enables easy clock synchronization (an issue seldom addressed by the scientific literature on QKD) and easy locking of tuneable optical filters at the receiver to the signal central frequency.

Figure 8 illustrates an experimental setup 750 used to characterize the phase randomness of the optical pulses generated by a gain switched directly modulated laser. A DFB laser 752 was used, driven by an RF pulse source 754, plus a bias current 756 and temperature control 758. The generated optical pulses were transmitted across an optical fibre to a coherent receiver, CO-Rx, 760, provided with a local oscillator, LO, signal 762. The detected optical pulses were measured using an oscilloscope 770 and post processing performed on a PC 780.

Eight pulse trains, each of 105 optical pulses, were generated by the DFB laser 752 and the phase distribution of the 8 x 105 optical pulses was measured, as shown in Figure 9 (top) together with the autocorrelation function, shown in Figure 9 (bottom). Figure 10 shows Pearson correlation coefficient of the optical pulses, and the phase randomness of the optical pulses is confirmed by the optical pulses having a Pearson correlation coefficient of between +0.015 and -0.015.

Referring to Figure 11, an embodiment of the invention provides a method 800 of QKD comprising steps of: generating 802 optical pulses having independent and randomly distributed phases; applying 804 at least one of a respective phase modulation and a respective intensity modulation to the optical pulses to encode respective quantum states on the optical pulses; and attenuating 806 the optical pulses to approximate a single photon source.

In an embodiment, the optical pulses have phases which are randomly distributed between preselected values which are dependent on an encryption protocol.

Referring to Figure 12, an embodiment of the invention provides a method 900 of QKD further comprising steps of: generating 902 random numbers; mapping 904 the random numbers into respective quantum states; and determining 906 at least one of a respective phase modulation and a respective intensity modulation to be applied to encode the quantum states onto respective optical pulses.

Referring to Figure 13, an embodiment of the invention provides a method 1000 of QKD in which the random numbers are generated by: power splitting 1002 the optical pulses generated by the laser; interfering 1004 successive optical pulses to convert a phase difference between successive optical pulses into an intensity modulation of an output optical signal; detecting 1006 the intensity of the output optical signal; converting 1008 a detected intensity of the output optical signal into a corresponding amplitude level; and generating 1010 an output signal comprising an indication of the amplitude level.

In an embodiment, an algorithm is used to derive numbers having a target distribution from the randomly distributed detected intensities. Common algorithms such as inverse transform sampling or the Box-Muller transformation, for transforming uniformly distributed

random variables to a new set of random variables with a Gaussian (or Normal) distribution, may be used.

Referring to Figure 14, an embodiment of the invention provides a method 1100 of QKD in which the optical pulses are selectively attenuated at either a first attenuation 1102 or at a second attenuation 1104.

At the first attenuation, the optical pulses are attenuated to the optical pulses are attenuated 1102 to such level that a photon number of the optical pulses has an average Poisson distribution of less than 1. In an embodiment, the optical pulses are attenuated 1102 to such level that a photon number of the optical pulses has an average Poisson distribution of 0.1.

The second attenuation is a minimum attenuation, meaning that the optical pulses are strong. The method 1100 additionally comprises tuning 1106 respective central frequencies of tuneable optical filters to respective frequencies of incoming optical signals when the optical pulses are attenuated 1104 at the second, minimum, attenuation. The tuneable optical filters are for removing out of band noise from the incoming optical signal. The method 1100 also comprises performing 1108 clock synchronisation when the optical pulses are attenuated at the second, minimum, attenuation.

The quantum states are signal states and one or more decoy states, which are applied by means of intensity modulation. In an embodiment, a number of decoy states and respective amplitudes of the decoy states are set according to the encryption protocol in use, such as phase encoded BB84 and decoy states differential phase shift QKD, as described in "Decoy State Quantum Key Distribution", Physical Review Letters, 94, 230504, 2005. Decoy states are encoded in accordance with pre-determined occurrence probabilities for the respective encryption protocol.

In an embodiment, the method additionally comprises optically filtering the optical pulses to confine the optical power of the optical pulses around a nominal central frequency before attenuating the optical pulses. Out-of-band noise may therefore be removed from the optical pulses, before they are attenuated to approximate a single photon source.

## CLAIMS

1. Quantum key distribution apparatus comprising:
a gain switched laser configured to generate optical pulses;
optical modulation apparatus configured to apply at least one of a respective phase modulation and a respective intensity modulation to the optical pulses to encode respective quantum states on the optical pulses; and
optical attenuation apparatus configured to attenuate the optical pulses to approximate a single photon source.

2. Quantum key distribution apparatus according to claim 1, further comprising:
a random number generator; and
a quantum encoder configured to map a number received from the random number generator into a respective quantum state and to generate an output signal comprising an indication of at least one of a respective phase modulation and a respective intensity modulation to be applied by the optical modulation apparatus to encode the quantum state onto a respective optical pulse.

3. Quantum key distribution apparatus according to claim 2, wherein the random number generator is a quantum random number generator comprising:
an optical splitter configured to power split the optical pulses generated by the laser;
an optical interferometer configured to receive optical pulses from the optical splitter and comprising a delay element in one arm configured to apply a delay to an optical pulse propagating in said arm such that successive optical pulses are interfered by the optical interferometer, to convert a phase difference between successive optical pulses into an intensity modulation of an output optical signal of the optical interferometer;
an optical detector arranged to detect the output signal; and
signal processing apparatus configured to convert a detected intensity of the output signal into a corresponding amplitude level and to generate an output signal comprising an indication of the amplitude level.

4. Quantum key distribution apparatus according to any preceding claim, wherein the optical attenuation apparatus is selectively operable in one of a first state in which the optical attenuation apparatus is configured to attenuate the optical pulses to approximate a single photon source and a second state in which the optical attenuation apparatus is configured with a minimum attenuation.

5. Quantum key distribution apparatus as claimed in any preceding claim, wherein the optical attenuation apparatus is configured to attenuate the optical pulses to such level that a photon number of the optical pulses has an average Poisson distribution of less than 1.

6. Quantum key distribution apparatus as claimed in any preceding claim, wherein the quantum states comprise signal states and at least one decoy state.

7. A quantum key distribution system comprising first and second quantum key distribution apparatus according to any preceding claim.

8. A quantum key distribution system according to claim 7 when dependent on claim 4, the first and second quantum key distribution apparatus each further comprising:
an optical receiver for receiving an incoming optical signal from the other quantum key distribution apparatus; and
a tuneable optical filter arranged before the optical receiver for removing out of band noise from the incoming optical signal,
and wherein the quantum key distribution apparatus are operable to tune respective central frequencies of the tuneable optical filters to respective frequencies of the incoming optical signals when the optical attenuation apparatus are in the second state.

9. A quantum key distribution system according to claim 8, wherein the quantum key distribution apparatus are additionally operable to perform clock synchronisation when the optical attenuators are in the second state.

10. A method of quantum key distribution comprising steps of:
generating optical pulses having independent and randomly distributed phases;
applying at least one of a respective phase modulation and a respective intensity modulation to the optical pulses to encode respective quantum states on the optical pulses; and
attenuating the optical pulses to approximate a single photon source.

11. A method according to claim 10, further comprising steps of:
generating random numbers;
mapping the random numbers into respective quantum states; and
determining at least one of a respective phase modulation and a respective intensity modulation to be applied to encode the quantum states onto respective optical pulses.

12. A method according to claim 10 or claim 11, wherein the random numbers are generated by:
power splitting the optical pulses generated by the laser;
interfering successive optical pulses to convert a phase difference between successive optical pulses into an intensity modulation of an output optical signal;
detecting the intensity of the output optical signal;
converting a detected intensity of the output optical signal into a corresponding amplitude level; and
generating an output signal comprising an indication of the amplitude level.

13. A method according to any of claims 10 to 12, wherein the optical pulses are selectively attenuated at a first attenuation to approximate a single photon source or at a second, minimum, attenuation.

14. A method according to any of claims 10 to 13, wherein the optical pulses are attenuated to such level that a photon number of the optical pulses has an average Poisson distribution of less than 1.

15. A method according to any of claims 10 to 14, wherein the quantum states comprise signal states and at least one decoy state.

16. A method according to any of claims 13 to 15, further comprising tuning respective central frequencies of tuneable optical filters to respective frequencies of incoming optical signals when the optical pulses are attenuated at the second, minimum, attenuation, the tuneable optical filters arranged for removing out of band noise from the incoming optical signal.

17. A method according to any of claims 13 to 16, further comprising performing clock synchronisation when the optical pulses are attenuated at the second, minimum, attenuation.

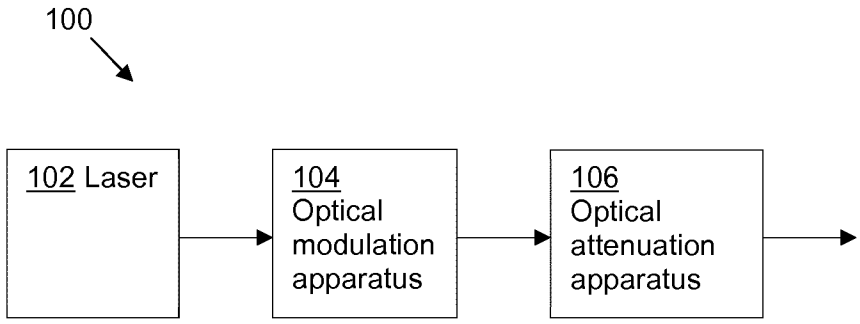
100
102 Laser
104
Optical
modulation
apparatus
106
Optical
attenuation
apparatus

Fig. 1

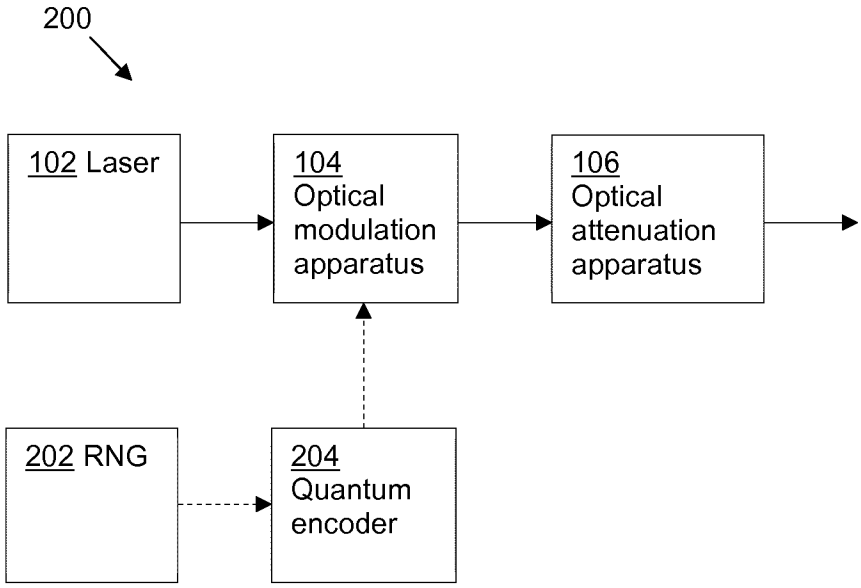
200
102 Laser
104
Optical
modulation
apparatus
106
Optical
attenuation
apparatus
202 RNG
204
Quantum
encoder

Fig. 2

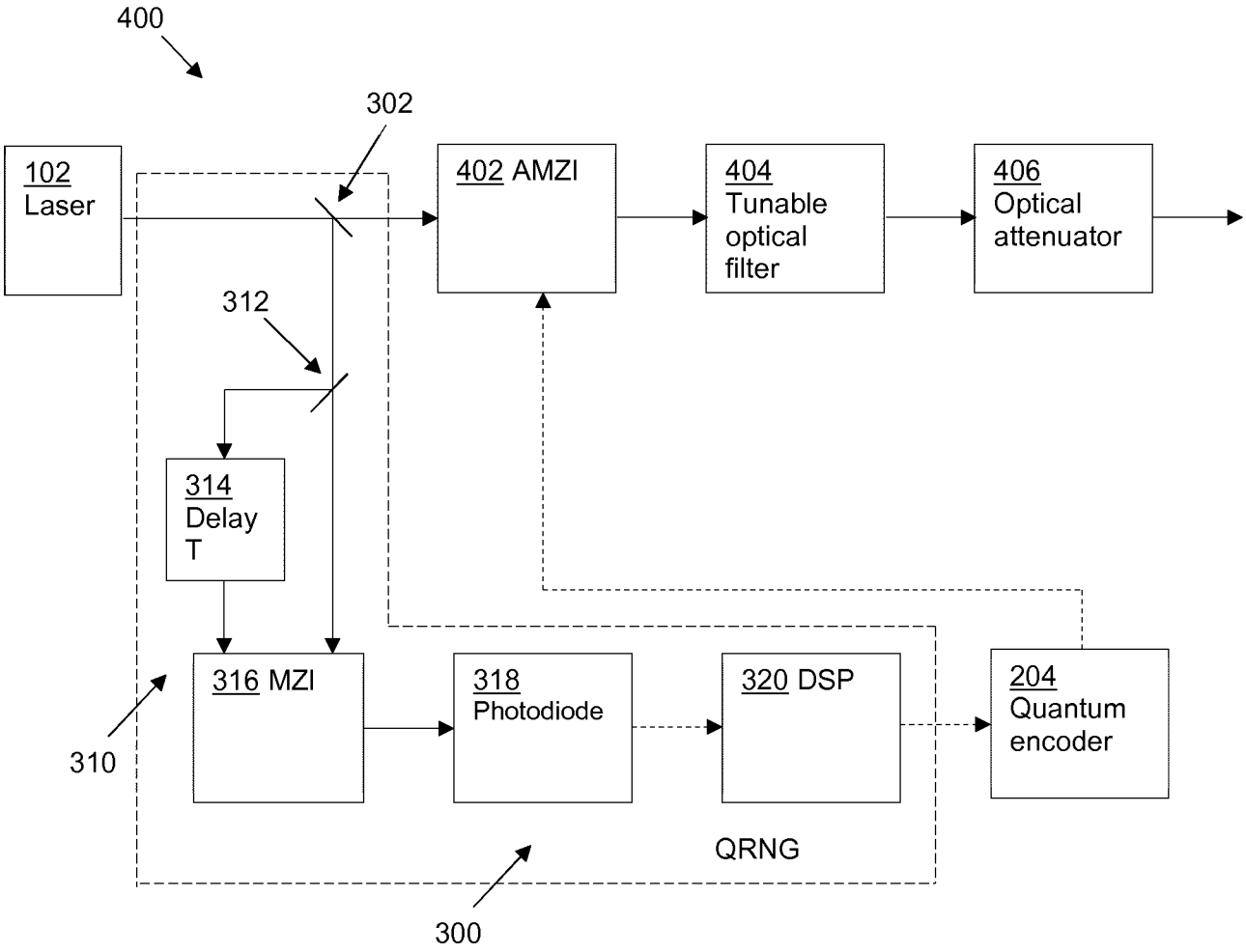
400
302
102
Laser
402 AMZI
404
Tunable
optical
filter
406
Optical
attenuator
312
314
Delay
T
316 MZI
318
Photodiode
320 DSP
204
Quantum
encoder
310
QRNG
300

Fig. 3

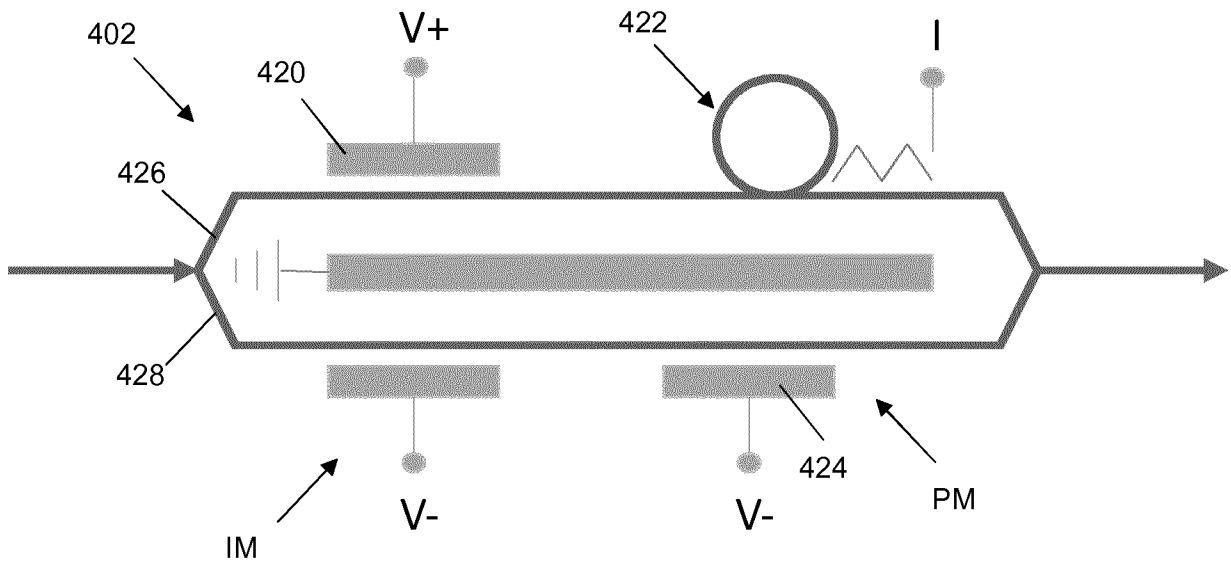
402
V+
422
I
420
426
428
424
PM
IM
V-
V-

Fig. 4

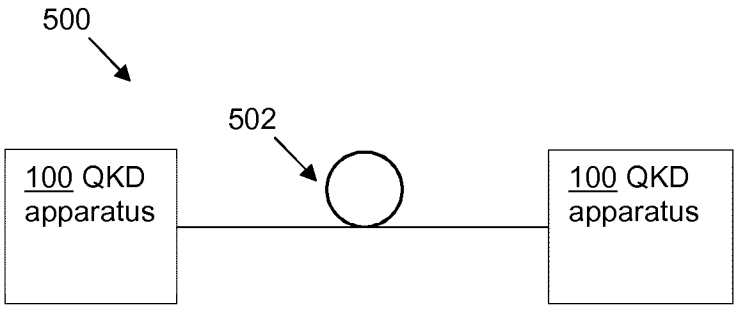
500
502
100 QKD apparatus
100 QKD apparatus

Fig. 5

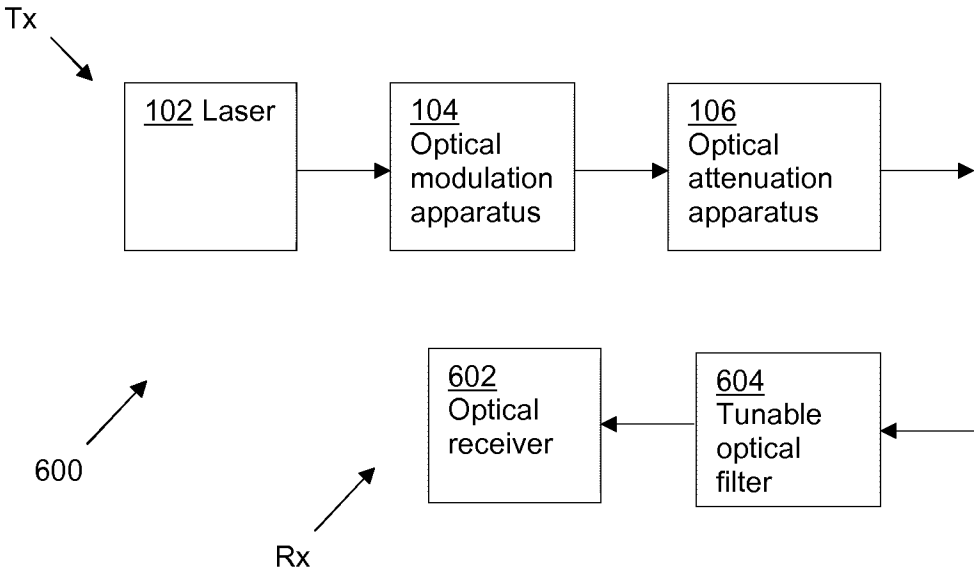
Tx
102 Laser
104 Optical modulation apparatus
106 Optical attenuation apparatus
600
602 Optical receiver
604 Tunable optical filter
Rx

Fig. 6

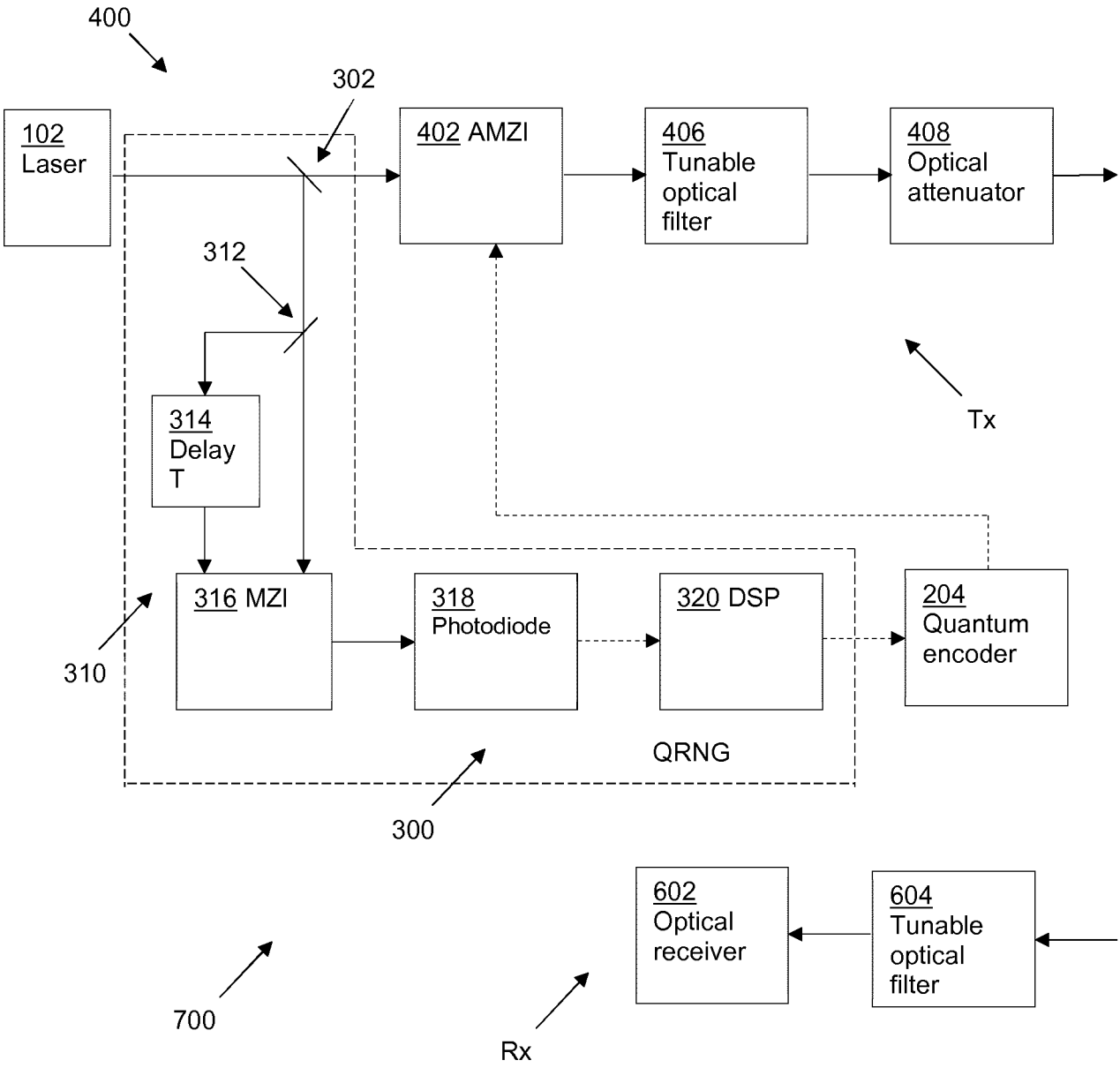
400
302
102
Laser
402 AMZI
406
Tunable
optical
filter
408
Optical
attenuator
312
314
Delay
T
Tx
316 MZI
318
Photodiode
320 DSP
204
Quantum
encoder
310
QRNG
300
602
Optical
receiver
604
Tunable
optical
filter
700
Rx

Fig. 7

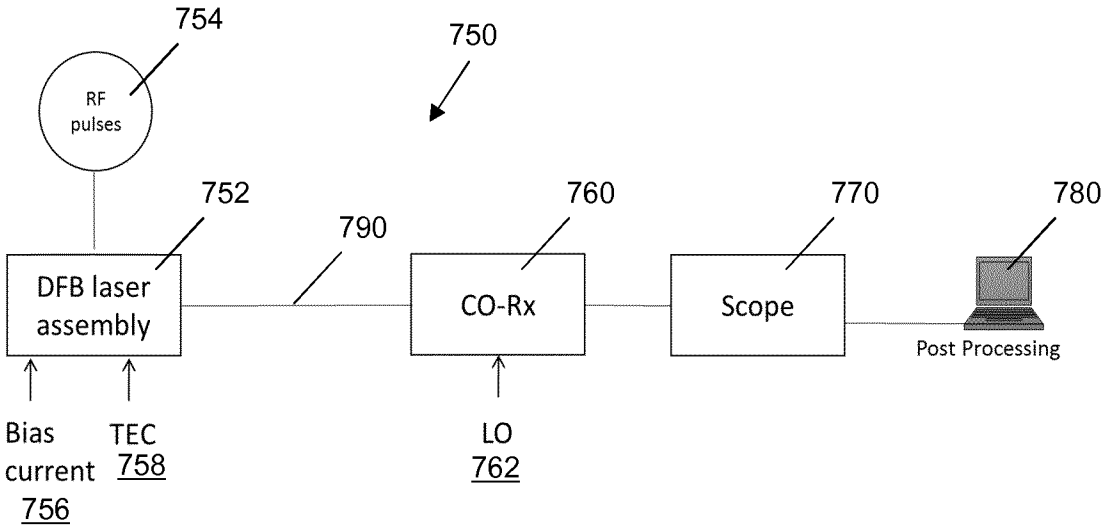
754
RF pulses
750
752
790
760
770
780
DFB laser assembly
CO-Rx
Scope
Post Processing
Bias current 756
TEC 758
LO 762

Fig. 8

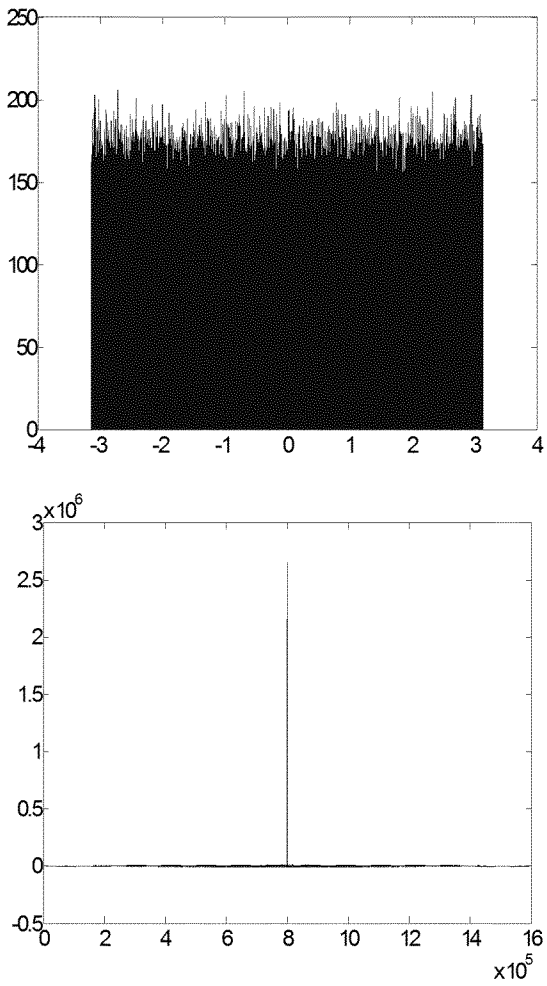
250
200
150
100
50
0
-4 -3 -2 -1 0 1 2 3 4
x10^6
3
2.5
2
1.5
1
0.5
0
-0.5
0 2 4 6 8 10 12 14 16
x10^5

Fig. 9

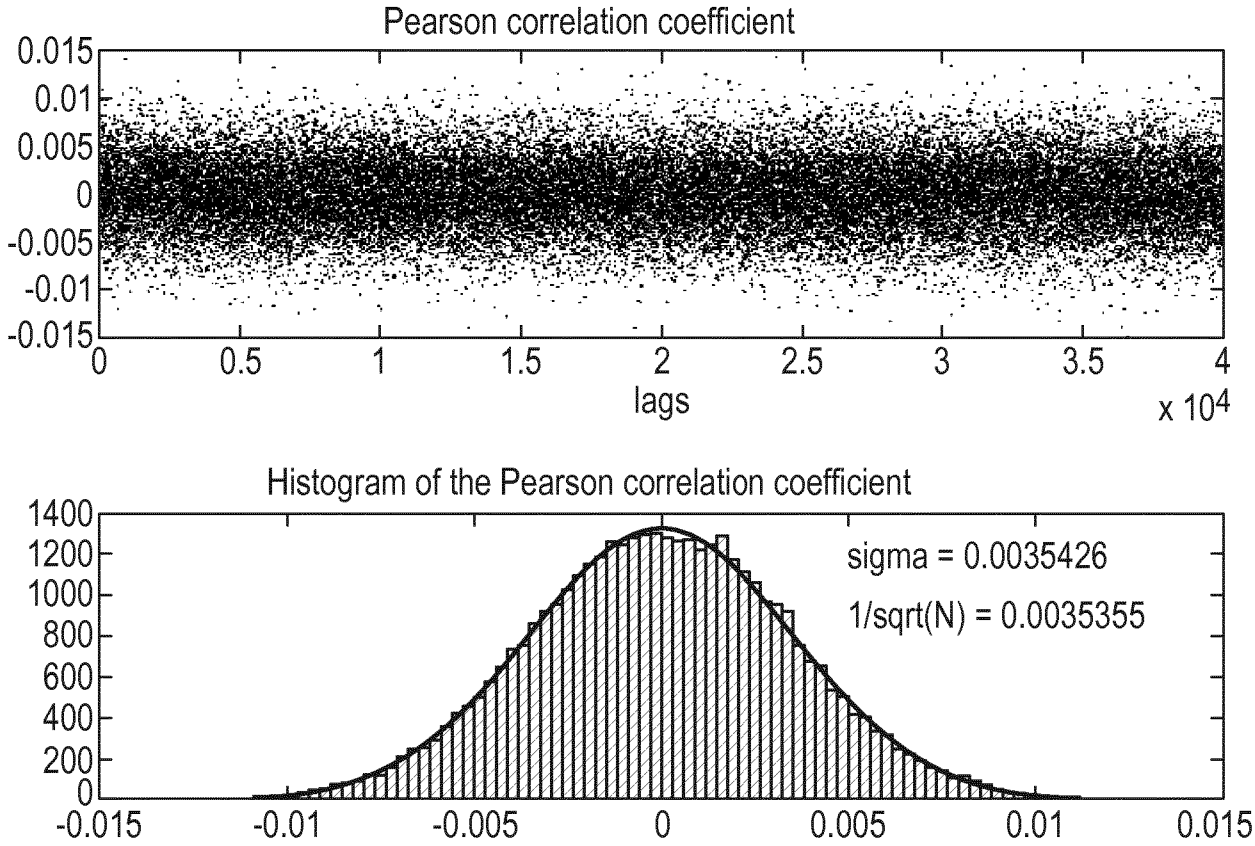
Pearson correlation coefficient
0.015
0.01
0.005
0
-0.005
-0.01
-0.015
0
0.5
1
1.5
2
2.5
3
3.5
4
lags
x 10^4
Histogram of the Pearson correlation coefficient
1400
1200
1000
800
600
400
200
0
sigma = 0.0035426
1/sqrt(N) = 0.0035355
-0.015
-0.01
-0.005
0
0.005
0.01
0.015

Fig. 10

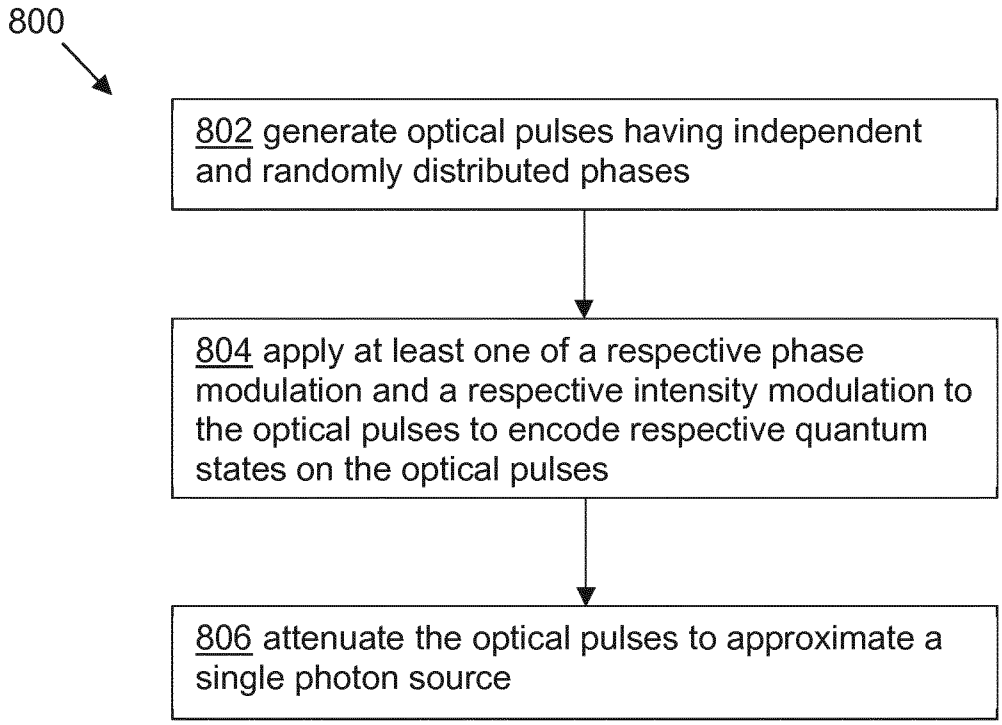
800
802 generate optical pulses having independent and randomly distributed phases
804 apply at least one of a respective phase modulation and a respective intensity modulation to the optical pulses to encode respective quantum states on the optical pulses
806 attenuate the optical pulses to approximate a single photon source

Fig. 11

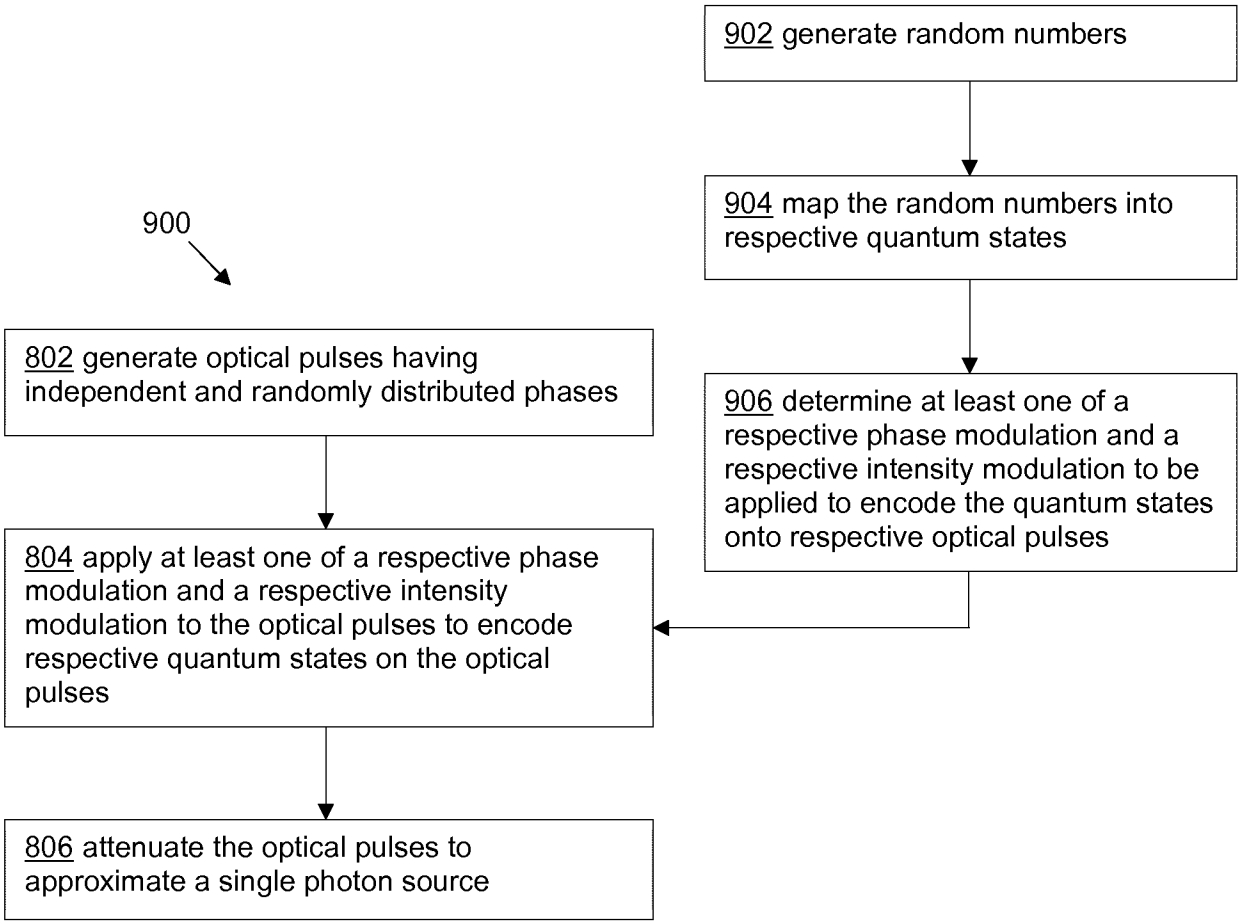
902 generate random numbers
904 map the random numbers into respective quantum states
900
802 generate optical pulses having independent and randomly distributed phases
906 determine at least one of a respective phase modulation and a respective intensity modulation to be applied to encode the quantum states onto respective optical pulses
804 apply at least one of a respective phase modulation and a respective intensity modulation to the optical pulses to encode respective quantum states on the optical pulses
806 attenuate the optical pulses to approximate a single photon source

Fig. 12

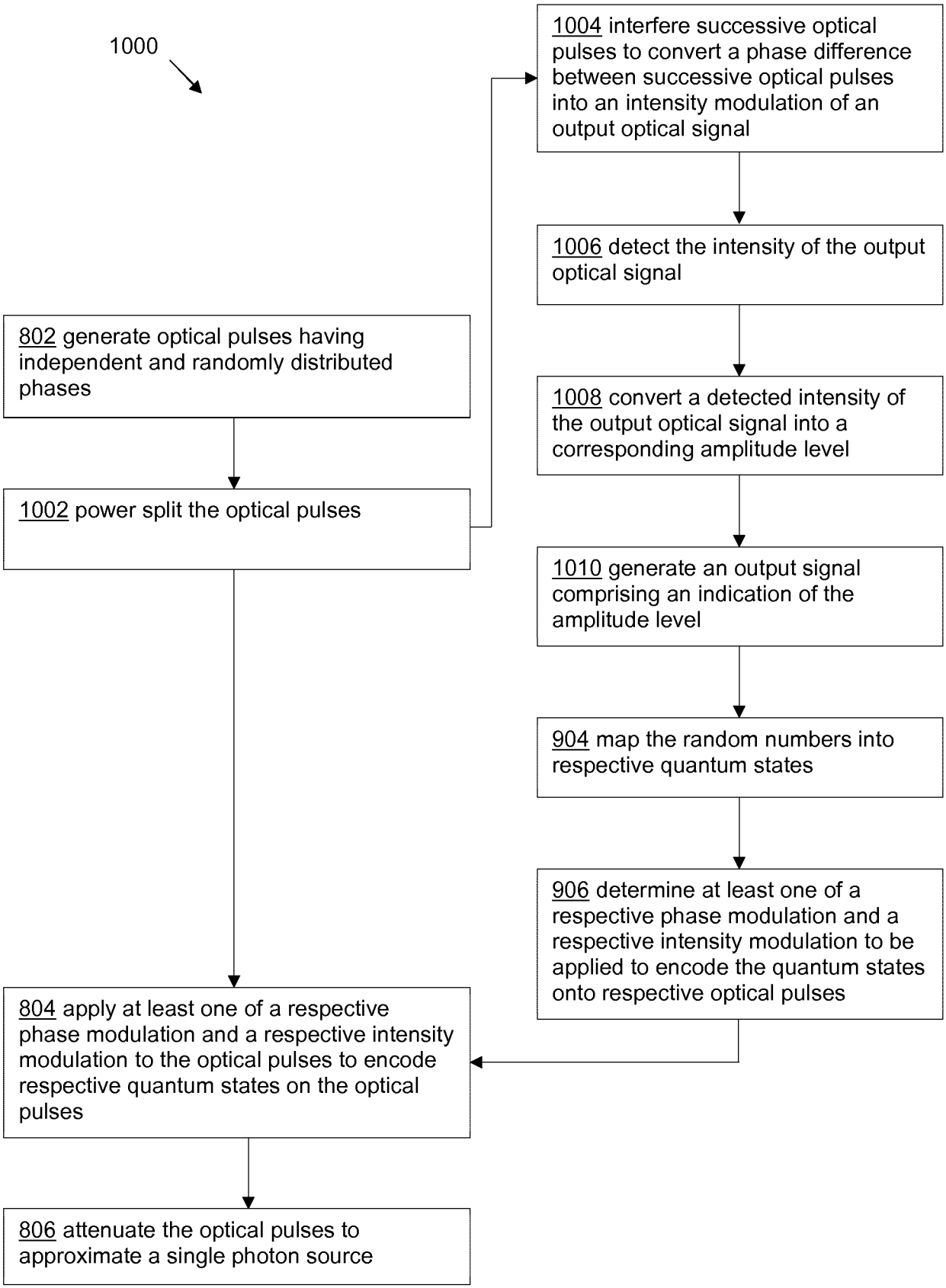
1000
802 generate optical pulses having independent and randomly distributed phases
1002 power split the optical pulses
804 apply at least one of a respective phase modulation and a respective intensity modulation to the optical pulses to encode respective quantum states on the optical pulses
806 attenuate the optical pulses to approximate a single photon source
1004 interfere successive optical pulses to convert a phase difference between successive optical pulses into an intensity modulation of an output optical signal
1006 detect the intensity of the output optical signal
1008 convert a detected intensity of the output optical signal into a corresponding amplitude level
1010 generate an output signal comprising an indication of the amplitude level
904 map the random numbers into respective quantum states
906 determine at least one of a respective phase modulation and a respective intensity modulation to be applied to encode the quantum states onto respective optical pulses

Fig. 13

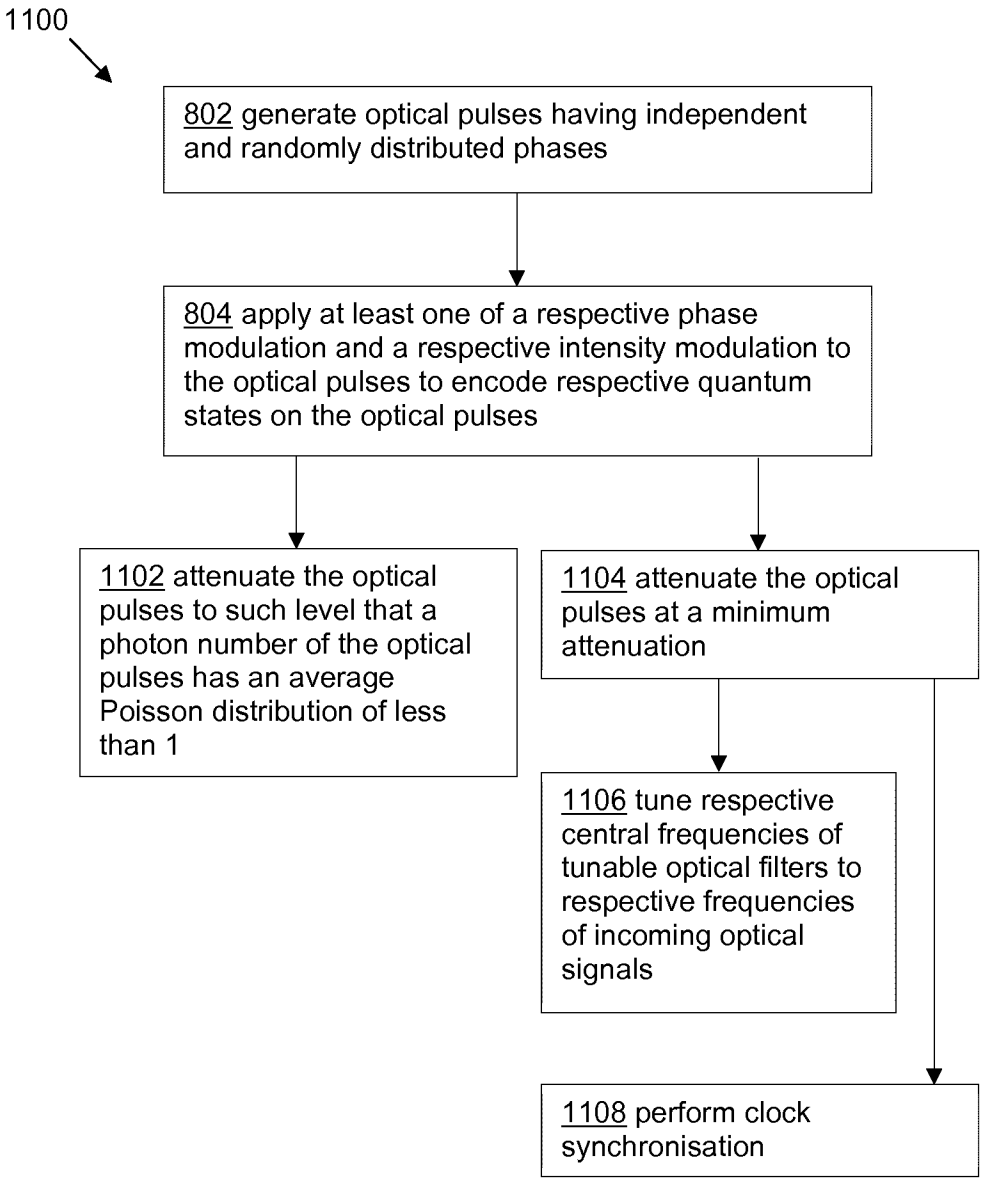
1100
802 generate optical pulses having independent and randomly distributed phases
804 apply at least one of a respective phase modulation and a respective intensity modulation to the optical pulses to encode respective quantum states on the optical pulses
1102 attenuate the optical pulses to such level that a photon number of the optical pulses has an average Poisson distribution of less than 1
1104 attenuate the optical pulses at a minimum attenuation
1106 tune respective central frequencies of tunable optical filters to respective frequencies of incoming optical signals
1108 perform clock synchronisation

Fig. 14

# INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2018/052829

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04B10/70 H04L9/08
ADD.

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04B H04L

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)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | US 2010/027794 A1 (YUAN ZHILIANG [GB] ET AL) 4 February 2010 (2010-02-04) | 1,2, 4-11,13, 14,16,17 |
| Y | paragraph [0002] - paragraph [0004]; figures 2,8,9<br>paragraph [0050] - paragraph [0052]<br>paragraph [0008]<br>paragraph [0064]<br>paragraph [0112] | 3,12 |
| | ----- | |
| Y | GB 2 529 228 A (TOSHIBA RES EUROP LTD [GB]) 17 February 2016 (2016-02-17)<br>page 31, line 10 - page 35, line 5; figures 9,11b | 3,12 |
| | ----- | |
| | -/-- | |

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 23 October 2018 | 02/11/2018 |

| Name and mailing address of the ISA/ | Authorized officer |
|---|---|
| European Patent Office, P.B. 5818 Patentlaan 2<br>NL - 2280 HV Rijswijk<br>Tel. (+31-70) 340-2040,<br>Fax: (+31-70) 340-3016 | Gäde, Sebastian |

2

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

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | US 2002/025041 A1 (TOMITA AKIHISA [JP]) 28 February 2002 (2002-02-28) | 1,2, 4-11, 13-17 |
| A | paragraph [0017] - paragraph [0018]; figure 1 paragraph [0029] - paragraph [0034] | 3,12 |
| X | GB 2 550 263 A (TOSHIBA RES EUROPE LTD [GB]) 15 November 2017 (2017-11-15) | 1,2, 4-11, 13-17 |
| A | page 4, line 35 - page 10, line 22; figures 1,2,3,5,6,7,8 | 3,12 |
| A | WANG FANG-XIANG ET AL: "Robust Quantum Random Number Generator Based on Avalanche Photodiodes", JOURNAL OF LIGHTWAVE TECHNOLOGY, IEEE SERVICE CENTER, NEW YORK, NY, US, vol. 33, no. 15, 12 May 2015 (2015-05-12), pages 3319-3326, XP011585912, ISSN: 0733-8724, DOI: 10.1109/JLT.2015.2432803 [retrieved on 2015-06-26] abstract Section III; figure 3 | 3,12 |
| A | CN 106 354 476 A (ZHEJIANG SHENZHOU LIANGZI NETWORK SCIENCE & TECH CO LTD) 25 January 2017 (2017-01-25) claim 1; figures 1,2,4 | 3,12 |

2

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2018/052829

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| US 2010027794 A1 | 04-02-2010 | GB 2430123 A | 14-03-2007 |
| | | US 2010027794 A1 | 04-02-2010 |
| GB 2529228 A | 17-02-2016 | NONE | |
| US 2002025041 A1 | 28-02-2002 | JP 3829602 B2 | 04-10-2006 |
| | | JP 2002064480 A | 28-02-2002 |
| | | US 2002025041 A1 | 28-02-2002 |
| GB 2550263 A | 15-11-2017 | NONE | |
| CN 106354476 A | 25-01-2017 | NONE | |