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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
26 November 2009 (26.11.2009)

PCT

(10) International Publication Number
WO 2009/141585 A1

(51) International Patent Classification:
H04L 9/08 (2006.01)

(21) International Application Number:
PCT/GB2009/001222

(22) International Filing Date:
15 May 2009 (15.05.2009)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

0809044.1	19 May 2008 (19.05.2008)	GB
61/071,806	19 May 2008 (19.05.2008)	US

(71) Applicant *(for all designated States except US)*: **QINETIQ LIMITED** [GB/GB]; Registered Office, 85 Buckingham Gate, London SW1E 6PD (GB).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **WISEMAN, Simon, Robert** [GB/GB]; QinetiQ Limited, Malvern Technology Centre, St Andrews Road, Malvern, Worcestershire WR14 3PS (GB). **LOWANS, Brian, Sinclair** [GB/GB]; QinetiQ Limited, Malvern Technology Centre, St Andrews Road, Malvern, Worcestershire WR14 3PS (GB). **AYLING, Stephen, Gerard** [GB/GB]; QinetiQ Limited, Malvern Technology Centre, St Andrews Road, Malvern, Worcestershire WR14 3PS (GB). **FINLAYSON, Ewan, David** [GB/GB]; QinetiQ Limited, Malvern Technology Centre, St Andrews Road, Malvern, Worcestershire WR14 3PS (GB).

(74) Agent: **TOCHER, Alastair**; QinetiQ Limited, Intellectual Property, Malvern Technology Centre, St Andrews Road, Malvern, Worcestershire WR143PS (GB).

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

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

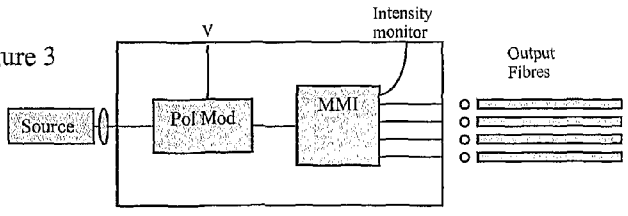
— *of inventorship (Rule 4.17(iv))*

Published:

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

(54) Title: MULTIPLEXED QUANTUM KEY DISTRIBUTION

Figure 3



(57) Abstract: The present invention relates to an improved quantum signal transmitter, which has a plurality of quantum output channels having at least one optical source and at least one optical splitter acting on the output of said at least one source. Such a transmitter can easily be used with existing passive optical network (PON) systems and can be a compact piece of equipment.

WO 2009/141585 A1

Multiplexed Quantum Key Distribution

This invention relates to an improved quantum transmitter for use in quantum key distribution.

Quantum key distribution (QKD) is a well known technique which offers the possibility of secure distribution/generation of cryptographic keys for use in encryption. QKD relies on fundamental quantum properties and allows two parties, commonly referred to as Alice and Bob, to exchange a value and know that an eavesdropper, usually referred to as Eve, has not learnt much about the value. QKD allows key material to be securely derived by Alice and Bob as needed, which offers significant advantages over other methods of key distribution.

Bennett and Brassard described a QKD protocol in C.H.Bennett and G.Brassard, "Quantum cryptography: 'Public key distribution and coin tossing'," IEE Conf. Computers Systems Signal Processing, Bangalore, India 1984 which has become known as the BB84 protocol. This protocol uses the transmission of a suitably encoded series of single photons (a quantum exchange) followed by an open discussion via any conventional communication medium (a key agreement stage) to allow Alice and Bob to derive a shared string of random numbers. As single photons are used in the quantum exchange the only way Eve can gain any information about this exchange is to intercept the single photons sent by Alice and measure the information herself. To avoid detection she should also transmit a photon to Bob which attempts to replicate the original photon she intercepted. Due to the random choice of encoding and the quantum nature of the photons Eve can not guarantee to pass a correctly encoded photon to Bob and this will generate a statistical error which will be spotted by Alice and Bob during their conventional communication.

QKD therefore offers a secure means of distributing new key material which protects against eavesdropping.

It is also known to apply QKD to securing communications over networks. British Telecom patent US5,768,378 teaches that QKD may also be used to distribute keys between a single sender (Alice) and multiple receivers (Bobs) via a passive optical network (PON). Light sent downstream from the Alice end encounters one or more passive optical network switches which distribute the light between their outputs. In

terms of sending single photons for QKD each photon traverses one of the downstream paths at random and ends up at one particular Bob. A passive optical network can be used as part of a switched star network where each PON is connected to a central switch for receiving upstream messages from an endpoint and broadcasting it back to the PON on which the destination endpoint is located.

Typically in an optical network there are actually a plurality of passive optical network splitters arranged in a distribution rack. Convention PON transmitter/receiver cards are quad pack supporting four separate fibre PONs.

It is an object of the present invention to provide an improved quantum signal transmitter and in particular one which can easily be used with existing PON systems.

Thus according to the present invention there is provided a quantum signal transmitter having a plurality of quantum output channels having at least one optical source and at least one optical splitter acting on the output of said at least one optical source.

The quantum signal transmitter of the present invention therefore has one or more optical sources as is conventional in a quantum transmitter device. Preferably a single optical source is used and the output subsequently modulated to provide the quantum signal but the skilled person will be aware of some arrangements of quantum transmitter which use a separate source to produce each separate state required by the quantum signal. In any arrangement a single set of optical sources is used in the present invention but provide a quantum signal on each of the plurality of quantum output channels, i.e. a single source (or set of sources) produce a plurality of quantum signals, each on a separate output channel. Each output channel can be arranged to connect with a separate optical link and thus a single optical source in the quantum transmitter (Alice) of the present invention can be used to communicate with a plurality of quantum receivers (Bobs). When used in an optical network environment this means that a single optical source can be shared between multiple PONs. This significantly reduces not only the cost of the equipment but also the size of the equipment which is an important consideration for network applications and for interfacing with existing equipment.

As used in the present specification the term quantum signal is any signal which may be used as the basis of a quantum key agreement protocol as would be understood by one skilled in the art. For instance the quantum signal may comprise a series of suitably

modulated single photons. The skilled person will be well aware of various modulation schemes which may be used, for instance phase modulation or polarisation modulation. The modulation of the quantum properties, e.g. phase or polarisation shall be referred to as quantum modulation.

Conveniently the at least one optical splitter comprises a multi-mode interference waveguide. Multi-mode interference (MMI) waveguide devices are known devices which can be used to split optical signals. Suitable MMI waveguides are described, for instance, in US5,410,625 and/or US5,428,698, the contents of both of which are incorporated herein by reference. MMI devices are reliable and may involve no moving parts so can be robust. MMI devices may also be very small and, as waveguide devices, may be integrated into an optical circuit. The multi-mode interference waveguide may therefore be integrated with the other optical devices of quantum signal transmitter, for instance the optical source, any intensity modulators and any polarisation modulators. The optical components of the quantum signal transmitter may therefore be formed on a single chip possibly together with the control electronics. Thus the present invention can enable a single line card in a distribution rack to provide the quantum transmitter for a plurality of PONs and thus can be used with standard industry equipment.

The optical splitter, for instance an MMI waveguide, may be passive and provide an amplitude split between the various outputs. In terms of single photon signals this means a photon will be transmitted randomly to one of the outputs.

The use of passive splitters does avoid the need for active control with associated control circuitry and power requirements. However passive splitting has the effect of increasing optical losses and this may not be acceptable for all situations. For instance where the quantum signal consists of a series of single photons the and source is an attenuated laser the security requirement may be an average of 0.1 photons per pulse. Were the optical splitter to have four outputs then each fibre must have an average intensity of 0.025 photons per pulse.

In this embodiment the output of the source, which may be a single photon source or may be an attenuated bright source such as a laser, may be modulated by a quantum modulator to apply the necessary quantum modulation prior to being split by the passive splitter. The signal may also be intensity modulated if necessary to provide the necessary attenuation to achieve the desired number of photons per pulse. As will be

described later in more detail the intensity modulation may be direct or indirect and the transmitter may comprise an intensity modulator.

In another embodiment however the optical source is a bright source, i.e. not single photon, such as a laser or light emitting diode, and the transmitter comprises a quantum modulator arranged on each output channel. In other words the output of the source comprises a plurality of photons and thus these photons will be split between the various outputs of the optical splitter depending on the arrangement of the splitter. Where a passive symmetrically splitter is used the output of the source will be divided equally between the output channels. Each channel therefore receives some photons which are modulated by the quantum modulators. Each channel is in effect a separate quantum channel at this stage and hence the modulation applied to each channel should be entirely separate from the modulation applied to another channel to preserve security. This will therefore require either a dedicated random number generator for each quantum modulator or a shared random number generator to be able to operate fast enough to supply each quantum modulator with its own distinct set of random numbers to perform the necessary quantum modulation. Each output channel also comprises an intensity modulator acting on each output channel to achieve the desired photon attenuation, i.e. to achieve the desired number of photons per pulse, for instance an average of 0.1.

In another embodiment the optical splitter is controllable to control the distribution of the optical signal between the output channels. In other words the optical splitter directs light from the source to a selected one (or more but generally it will be one) of the output channels. Where the source is a single photon source, either a truly single photon source or an attenuated laser or light emitting diode, the photons produced by the source may be directed to different outputs at different times. Whilst the light may be directed equally between the output channels the splitter may direct different numbers of photons to different output channels. The splitter may direct photons to each channel to account for different amounts of loss on different channels.

It will be clear that the transmitter of the present invention transmits a quantum signal, such a series of single photons, down each of the output channels to ultimately be detected by a quantum receiver. If the channels have different amounts of optical loss, for instance if one channel is longer, than another, then the number of photons received

at the end of the longer channel will be lower than the number received at the end of the shorter channel. If photons were distributed equally between the channels and each channel required a certain number of photons to be detected before a key agreement step could take place it will be apparent that the longer channel will take longer to reach the requisite number of detected photons than the shorter channel. If however the optical splitter of transmitter device were arranged to direct photons to the longer channel twice as often as it was arranged to direct photons to the shorter channel then the rate of receipt of photons at the ends of both channels would be about equal.

Similarly the optical splitter may be arranged to direct photons to each channel to account for different numbers of receivers on each channel. Were an output channel connected to an common optical channel connecting a plurality of a quantum receivers to the transmitter via at least one optical splitter then the photons transmitted down the channel will be divided between the respective receivers. Each receiver will therefore only receive some of the transmitted photons and thus rate of receipt of photons at the receiver will be reduced compared to a channel having an unbroken optical path to a single receiver (ignoring other losses for now). The splitter may therefore direct photons to each output channel dependent on how many quantum receivers are connected to that channel.

Additionally or alternatively the quantum transmitter may be adapted to receive feedback from appropriate receivers and control the optical splitter to direct photons to each channel in response to the feedback, for instance to ensure a desired rates of photon receipt at each receiver. The splitter could maintain the same rate of receipt at each receiver or may be arranged to ensure that certain priority receivers receive more photons or do not drop below a certain photon detection rate.

The active optical splitter may comprise at least one MMI waveguide router device. MMI waveguide router devices are known, for instance as described in US5,428,698, and comprise a first 1 to n way MMI waveguide coupled to a second n to n MMI waveguide by n single mode waveguides. Phase modulators are arranged on the n single mode waveguides and by appropriate phase control an input optical signal can be steered to a desired output of the second MMI waveguide.

In one embodiment the optical path from the source to a first output channel may be different to the optical path from the source to second output channel so as to introduce

a time delay into first output channel relative to the second output channel. Each output channel may have a different delay.

In all the embodiments described above where the source is not a true single photon source, but instead is a bright source such as a laser or light emitting diode, there will be a need to attenuate the signal to provide the desired number of photons. Usually to ensure single photon signals are transmitted the average number of photons per pulse is set to around 0.1. However, to improve security of attenuated sources it is also known to send decoy pulses having a greater number of photons at random intervals but a certain average rate. This allows Bob to check that he is receiving the correct amount of pulses from Alice and an eavesdropper is not controlling the receipt of pulses by Bob.

There is therefore a need to apply intensity modulation to the optical signal at some point in the optical path to provide the desired number of photons per pulse in the output channels.

The intensity modulation may be direct or indirect. Direct intensity modulation relates to control of the source to produce pulses having the desired number of photons at the output. Indirect modulation refers to the intensity modulation being applied by other components with the quantum transmitter, for instance a dedicated intensity modulator.

In either case the quantum signal transmitter may comprise one at least one intensity monitor arranged to monitor the intensity of the optical signal. The intensity modulator could be connected to an output of the optical splitter. The intensity output from the splitter can be used to determine what the output intensity will be at each output channel taking into account known losses from the optical components acting on the signal after the passive splitter and hence it can be used to determine the intensity modulation that needs to be applied.

Measuring the intensity at the output of the optical splitter represents a convenient way of obtaining a part of the signal which can be used for intensity monitoring. The intensity monitoring would clearly take into account the optical split performed by the optical splitter. Using an MMI splitter the intensity output may be asymmetric about the outputs, in other words the intensity of the input signal may be distributed unevenly between the outputs. This avoids the need to use more of the input signal than in necessary for intensity monitoring.

The present invention relates particularly to a quantum signal transmitter for use in a PON. The transmitter may be arranged on a line card for use in a distribution rack. Conveniently at least one output channel of the quantum transmitter is connected to the backplane of the distribution rack. This allows the quantum transmitter in each line card to communicate with a quantum receiver located on the distribution rack. The quantum receiver in the distribution rack may be linked to a key management centre responsible for generating and controlling cryptographic keys ultimately used by the endpoint users for message traffic. Conveniently the key management centre uses QKD to establish secure communications with the quantum receiver in the distribution rack. In this way a series of quantum links is established from the key management centre to the distribution rack, for the distribution rack to each individual line card and from each line card to the endpoints on the appropriate PONs.

The invention will now be described by way of example only with respect to the following figures, of which:

Figure 1 shows a schematic of a standard QKD transmitter (Alice) and receiver (Bob) arranged over a single optical link,

Figure 2 illustrates a first embodiment of the present invention which time division multiplexes the quantum signal between the multiple outputs,

Figure 3 illustrates a second embodiment having a passive MMI splitter,

Figure 4 illustrates a third embodiment in which each output has a different delay, and

Figure 5 shows an embodiment which produces parallel distinct quantum signals from a single source.

Referring to figure 1 the basic structure of a standard QKD system is shown. The quantum transmitter 102, typically referred to as Alice, is optically linked to the quantum receiver 104, typically referred to a Bob. The optical link may be through free space or any suitable waveguide but for illustration will be described herein as being a fibre optic link. A typical Alice unit compromises a random number generator 106, quantum transmitter 108, controlling logic 110 and classical transceiver 112. The quantum transmitter 108 produces a series of single photons, each photon being randomly encoded using a value produced by the random number generator. The skilled person will readily appreciate that there are a number of different known encoding protocols and a number of suitable transmitters which could be used for QKD and hence these aspects will not be described further. For the purposes of this description a BB84 type protocol will be assumed wherein one of two encoding bases is chosen at random for each photon and the photon is randomly encoded with a data value of 1 or 0 in the chosen encoding base. The data regarding the applied encoding base and data value for each photon is passed to the Alice control logic 110.

The series of encoded single photons are transmitted through the fibre optic to the Bob unit 104. A typical Bob unit comprises a quantum receiver 116 which randomly chooses an encoding base with which to measure the photon and then determines a data value

for the photon in the chosen base. The output of the quantum receiver 116, which indicates the applied encoding base and measured value for each detected photon is passed to Bob control logic 118.

Alice control logic 110 and Bob control logic 118 then communicate with each other via classical transceivers 112 and 120 respectively to establish a common shared key as is well known. Note as used herein the term logic means any suitable device arrangement for performing the key agreement protocols. The control logic may be a suitable designed ASIC or a suitably programmed FPGA. The control logic could also be a suitably programmed microprocessor.

In establishing a common shared key, Alice control logic 110 and Bob control logic 118 mutually authenticate each other in order to exclude the possibility of a man-in-the-middle attack. Such authentication is a well known procedure and may, for example, involve the two parties applying digital signatures to the messages they exchange. The digital signatures are generated and validated by means of a cryptographic key referred to as the identity key for the link. This may be based on symmetric cryptographic techniques in which case the identity key is a secret value known only to both parties.

Having used QKD to establish a new common shared key value, and mutually authenticated each other, Alice control logic 110 and Bob control logic 118 use that value in part to update the secret identity key and in part as an encryption key for protecting subsequent communication between them. The encryption key is passed to a suitable crypto-unit (not shown) for encrypting plaintext message traffic and decrypting encrypted message traffic sent on the classical communication channel.

The present invention relates to a quantum transmitter, often referred to as an Alice, which has multiple separate outputs. In other words a transmitter which can transmit a different quantum signal on each of a plurality of quantum links, for instance via different fibre optic cable. The quantum transmitter of the present invention can be implemented as a single integrated optical circuit with the necessary control logic and thus comprises a very compact piece of equipment. Size can be important in network environments, as is the need to interface with existing equipment. The present invention can be implemented on a line card for use in a distribution rack as would be understood by one skilled in the art.

Figures 2 to 5 illustrate various embodiments of the invention. In all these embodiments the Alice control logic, random number generator and classical transceiver is omitted for clarity. The embodiments are described in relation to QKD scheme, such as BB84, using polarisation modulation for encoding the quantum signal but the skilled person will appreciate that other modulation schemes exist and could be used in the present invention.

Figure 2 shows an embodiment of the invention having temporal control of the outputs. In this scheme the output of source is split proportionally through the outputs of a Multi-Mode Interference (MMI) waveguide device. The MMI device is a signal routing device such as described in US5,428,698 and has a single input to a first MMI region having four outputs. The outputs of the first MMI region are inputs to a second MMI region having four inputs and four outputs. Between the first and second MMI regions are four single mode waveguide each having a phase modulator. Each output of the first MMI region is phase modulated independently in such a way that the inputs to the second MMI region are out of phase and interference results in an asymmetric split at its output such a the photon only travels through one of the outputs of the MMI device (the MMI works as an addressable optical switch between its outputs). Operation of such a device is described in US5,428,698, in particular with reference to Figure 7 thereof and column 11, line 62 to column 12, line 54. The contents of US5,428,698 and in particular the section referred to above are incorporated herein by reference. The MMI device may be implemented as a hollow waveguide device in a suitable semiconductor substrate or may be implemented as a solid waveguide in a material such a Gallium Arsenide. The MMI device is thus small and can be integrated into a photonic circuit with the source.

A polarisation modulator is arranged on each of the outputs of the MMI device to apply an appropriate polarisation modulation to encode the quantum signal. The polarisation modulator is preferably a device such as described in published international patent application WO 2008/032048. This polarisation modulator can apply the necessary polarisation modulation required at high speed to produce the quantum signal. The polarisation modulator may also be fabricated from GaAs and can be integrated with the output waveguide of the MMI device resulting in a very compact. low cost and robust design. Since each output is time multiplexed, only a single random number generator signal is required to determine the polarisation modulation applied and the signal is multiplexed in phase with the previous MMI device. The output from each polarisation modulator is fed to a separate output optical fibre.

In this way, time multiplexing allows the quantum transmitter to determine which pulses are emitted through each fibre in a time shared method and this may not be symmetric to ensure desired detection rates at the different receivers connected via the fibre.

A passive tap from the second MMI region is used to monitor the intensity throughput in real-time and provides feedback for either direct intensity modulation of the laser or, indirect intensity modulation by a dedicated intensity modulator such an additional Mach-Zehnder MMI design (not shown). Indirect modulation may be preferable to direct modulation as it can be achieved at high speeds and with high bandwidth – better than may be achieved with direct modulation and allowing use of components such as light emitting diodes as the source which otherwise would not be possible. Further, using indirect intensity modulation means that a laser source can be operated as CW source which is generally better for lifetime of the source than direct modulation. Note that the tap for the intensity monitor is shown as taken from the second MMI region. However it could alternatively be obtained from the first MMI region or even from both regions.

Figure 3 shows an embodiment having passive optical output. Here the output of the source is directed to a polarisation modulator of the type described above. The polarisation modulator operates in response to a random number generator (not shown) to produce a quantum signal which is then passed to a passive MMI 1 to 4 way splitter of the type described in US5,410,625. In this embodiment, there is no direct control of the temporal variation in the output intensity, it instead relies on a passive amplitude split between the outputs. This has the effect of increasing the optical losses and may unsuitable for some applications. For example, each time the number of output fibres increases by a factor of two the total losses increase by at least 3dB. However, in some cases the loss budget may allow this to be implemented. If security requires an average of 0.1 photons per pulse then each output fibre in this example must have an intensity of 0.025 photons per pulse. Again a tap from the passive MMI device may be taken for the purposes of monitoring the intensity and used to control intensity modulators (not shown).

Figure 4 shows an embodiment of the invention having time delays in the different channels. This technique generates a time delay between each of the separate optical outputs through application of a path delay in each layer of a splitter arrangement. This

fixed time delay is then subsequently used during the key establishment process to determine which optical connection is currently being made.

The arrangement in figure 4 consists of a first MMI implemented Mach-Zehnder (MZ) interferometer. This device comprises a first MMI region connected to a second MMI region via two single mode waveguide regions, one of which has a phase modulator arranged to provide a phase delay. This device acts similarly to the routing device described above and which sends each pulse to one of two arms. The MZ MMI devices also allow control over the intensity of the pulse sent to each of the arms and thus can be used to provide all or part of the intensity modulation required.

The lower arm has a fixed optical path delay. Each arm then splits through separate MMI MZ interferometers such that each output either receives no path delay or a fixed path delay. In this way the four main output channels receive four different path delays and they will transmit pulses of photons at different times. An array of polarisation modulators can then apply the required polarisation state to suit the destination through each of the fibres.

Figure 5 shows an embodiment which produces parallel quantum signals. In this embodiment the light source is a high intensity pulsed device producing short temporal pulses (<1ns) at a rate of several 100 MHz (the raw key generation bit rate). The light signal is input to a single monolithically integrated optical chip which includes a 1:4 MMI splitter, four independent polarisation modulators (of the type described above) and four independent intensity modulators with integrated intensity monitors. The four outputs of the MMI are individually polarisation and intensity modulated and coupled into their own output fibre. The intensity modulators reduce the photon emission rate to 0.1 photons per pulse on each fibre channel. The electronics for driving the two sets of modulators can be monolithically integrated and share a common connector feed to the integrated modulator chip package in order to aid miniaturisation and reduce costs. Although QKD photons can appear simultaneously on any of the output fibres this does not affect the QKD security since each fibre channel has its own separate QKD key information.

Claims

1. A quantum signal transmitter having a plurality of quantum output channels having at least one optical source and at least one optical splitter acting on the output of said at least one source.

2. A quantum signal transmitter as claimed in claim 1 wherein there is a single optical source.

3. A quantum signal transmitter according to claim 1 or claim 2 wherein the at least one optical splitter comprises a multi-mode interference waveguide.

4. A quantum signal transmitter according to any preceding claim wherein the optical splitter is passive.

5. A quantum signal transmitter according to any preceding claim wherein the optical source is a bright source and the transmitter further comprises a quantum modulator on each output channel.

6. A quantum signal transmitter according to claim 5 further comprises an intensity modulator arranged on each output channel.

7. A quantum signal transmitter according to any preceding claim arranged to produce parallel quantum signals on each of the output channels.

8. A quantum signal transmitter according to any of claims 1 to 3 wherein the optical splitter is controllable to control the distribution of the output of the optical source between the output channels.

9. A quantum signal transmitter according to claim 8 wherein the optical splitter distributes the output of the optical source equally between the output channels.

10. A quantum signal transmitter according to claim 8 wherein the optical splitter directs different numbers of photons to different output channels.

11. A quantum signal transmitter according to claim 10 wherein the optical splitter directs photons to each channel to account for different amounts of loss on different channels.

12. A quantum signal transmitter according to claim 10 or claim 11 wherein the optical splitter directs photons to each channel to account for different numbers of receivers on each channel.

13. A quantum signal transmitter according to claim 10 wherein the optical splitter directs photons to each channel in response to feedback from appropriate receivers of the output quantum signals.

14. A quantum signal transmitter according to any of claims 8 to 13 wherein the optical splitter comprises at least one MMI waveguide router device.

15. A quantum signal transmitter according to any preceding claim wherein the optical path length from the source to a first output channel is different to the optical path length from the source to second output channel so as to introduce a time delay into first output channel relative to the second output channel.

16. A quantum signal transmitter according to claim 15 wherein each output channel may have a different delay.

17. A quantum signal transmitter according to any preceding claim wherein the optical splitter and at least one optical source comprise an integrated photonic circuit.

18. A quantum signal transmitter according to claim 17 further comprising at least one integrated quantum modulator.

Figure 1

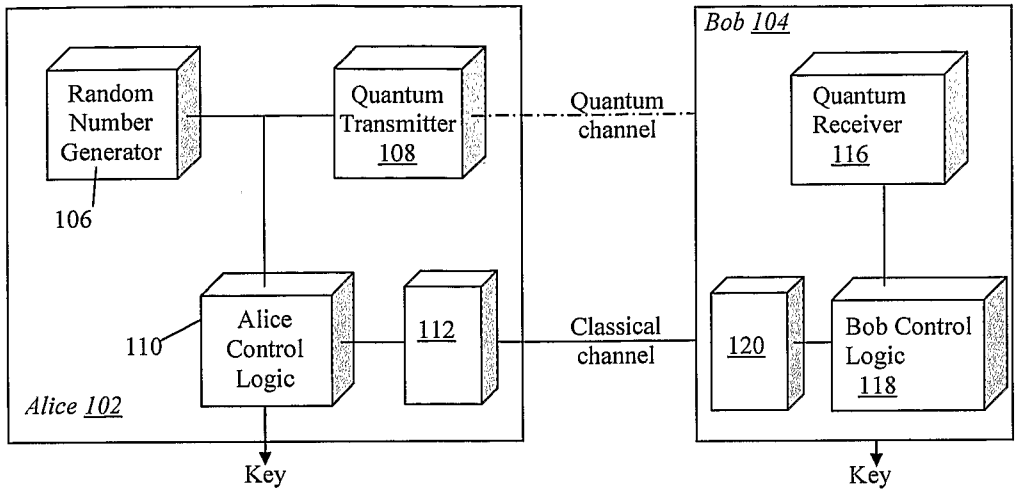


Figure 2

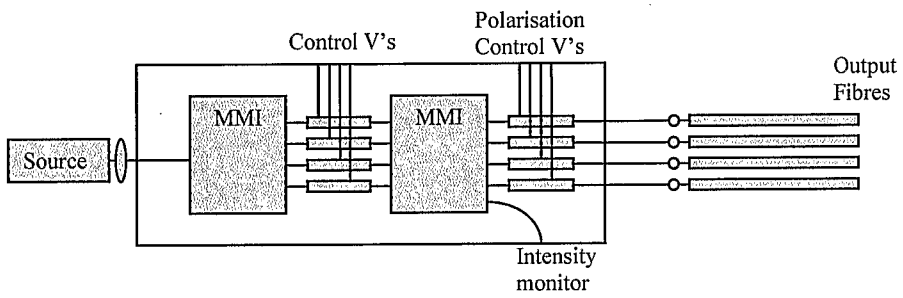


Figure 3

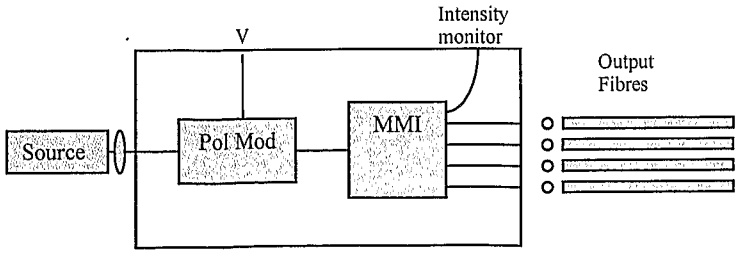


Figure 4

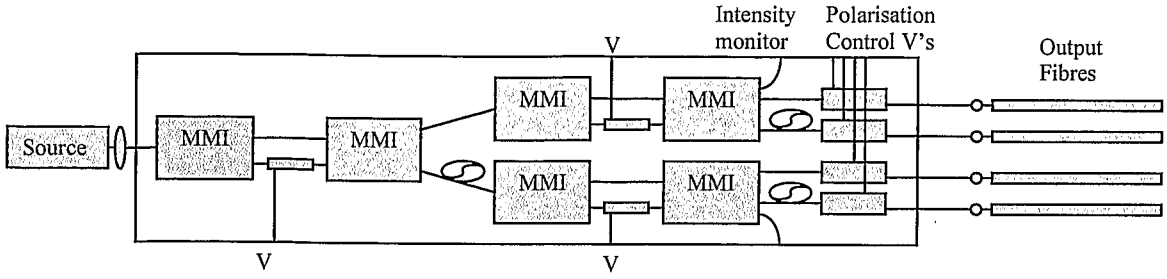
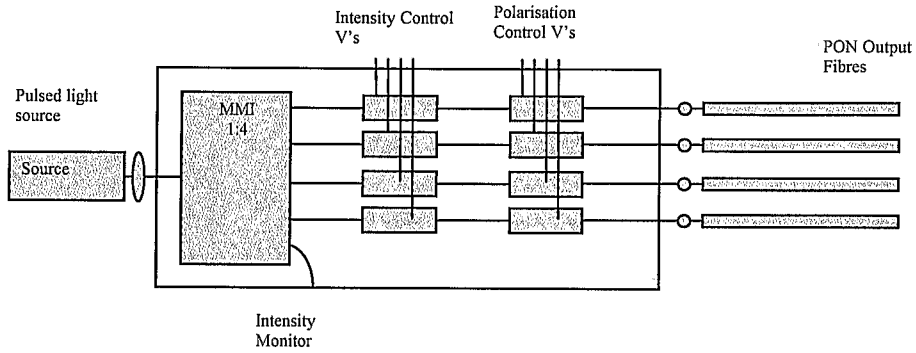


Figure 5



INTERNATIONAL SEARCH REPORT

International application No
PCT/GB2009/001222

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/08

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)
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 practical, search terms used)
EPO-Internal, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	VERONICA FERNANDEZ ET AL: "Passive Optical Network Approach to Gigahertz-Clocked Multiuser Quantum Key Distribution" IEEE JOURNAL OF QUANTUM ELECTRONICS, IEEE SERVICE CENTER, PISCATAWAY, NJ, USA, vol. 11, no. 2, 1 February 2007 (2007-02-01), pages 130-138, XP011156042 ISSN: 0018-9197 page 130 - page 132; figure 4 ----- -/--	1-18

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

[ ] See patent family annex.

* Special categories of cited documents :

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

"E" earlier document 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
26 June 2009	06/07/2009

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

INTERNATIONAL SEARCH REPORT

International application No
PCT/GB2009/001222

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	FERNANDEZ V ET AL: "Gigahertz Clocked Quantum Key Distribution in Passive Optical Networks" LEOS SUMMER TOPICAL MEETINGS, 2006 DIGEST OF THE QUEBEC CITY, QC, CANADA 17-19 JULY 2006, PISCATAWAY, NJ, USA,IEEE, 17 July 2006 (2006-07-17), pages 36-37, XP010940123 ISBN: 978-1-4244-0090-4 page 36; figure 1	1-18

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