CONVENTION - COMPANY - PCT
(By Employment Contract & Applicant is Applicant in Basic Appln)

A24692/AU

P/00/008b
Section 29 (1)
Regulation 3.1(2)

678049

AUSTRALIA

PATENTS ACT 1990

NOTICE OF ENTITLEMENT

We, BRITISH TELECOMMUNICATIONS public limited company, of 81 Newgate Street, London, EC1A 7AJ, England, being the applicant and nominated person in respect of Application No. 75440/94, state the following:-

1. The person nominated for the grant of the patent has entitlement from the actual inventor as follows:

If a patent were granted to the actual inventor in respect of the invention the nominated person would be entitled to have the patent assigned to it.

2. The person nominated for the grant of the patent is the applicant of the basic applications listed in the declaration under Article 8 of the PCT.

3. The basic applications listed in the declaration under Article 8 of the PCT are the first applications made in a Convention country in respect of the invention.

For and on behalf of
BRITISH TELECOMMUNICATIONS public limited company

..... (Signature)

29 FEB 1996
..... (Date)

Name: ROBERTS, SIMON CHRISTORPHER

Title: PATENT ATTORNEY

File: 18561

SHELSTON WATERS
60 MARGARET STREET, SYDNEY, AUSTRALIA

AU9475440

(12) PATENT ABRIDGMENT (11) Document No. AU-B-75440/94
(19) AUSTRALIAN PATENT OFFICE (10) Acceptance No 678049

(54) Title
SYSTEM AND METHOD FOR QUANTUM CRYPTOGRAPHY

International Patent Classification(s)
(51)[6] H04L 009/08

(21) Application No. : 75440/94 (22) Application Date : 08.09.94

(87) PCT Publication Number : WO95/07584

(30) Priority Data

(31) Number	(32) Date	(33) Country
93307120	09.09.93	EP EUROPEAN PATENT OFFICE (EP)
93307121	09.09.93	EP EUROPEAN PATENT OFFICE (EP)
9302075	06.10.93	WO WORLD INTELLECTUAL PROPERTY ORGANIZ ATION (WIPO)
93310228	17.12.93	EP EUROPEAN PATENT OFFICE (EP)
9302637	23.12.93	WO WORLD INTELLECTUAL PROPERTY ORGANIZ ATION (WIPO)

(43) Publication Date : 27.03.95

(44) Publication Date of Accepted Application : 15.05.97

(71) Applicant(s)
BRITISH TELECOMMUNICATIONS PUBLIC LIMITED COMPANY

(72) Inventor(s)
KEITH JAMES BLOW

(74) Attorney or Agent
SHELSTON WATERS , Level 21, 60 Margaret Street, SYDNEY NSW 2000

(57) Claim

1. A method of communication using quantum cryptography characterised in that the encryption alphabet used in coding signals for transmission on a quantum channel comprises pairs of operators applied successively to respective ones of a pair of single-photon signals transmitted onto the quantum channel with a predetermined delay between them, and in that in a step of detecting the single-photon signals, the signals of each pair are split according to their encoded state and directed to different detectors via paths giving a differential delay substantially complementary to the said pre-determined delay and coincidence detection is employed at the detectors to eliminate spurious counts.

OPI DATE 27/03/95 APPLN. ID 75440/94
AOJP DATE 18/05/95 PCT NUMBER PCT/GB94/01954
AU9475440

(51) International Patent Classification 6 :
H04L 9/08

A1

(11) International Publication Number: WO 95/07584

(43) International Publication Date: 16 March 1995 (16.03.95)

(21) International Application Number: PCT/GB94/01954

(22) International Filing Date: 8 September 1994 (08.09.94)

(30) Priority Data:
93307120.1 9 September 1993 (09.09.93) EP
(34) Countries for which the regional or international application was filed: AT et al.
93307121.9 9 September 1993 (09.09.93) EP
(34) Countries for which the regional or international application was filed: AT et al.
PCT/GB93/02075 6 October 1993 (06.10.93) WO
(34) Countries for which the regional or international application was filed: GB et al.
93310228.7 17 December 1993 (17.12.93) EP
(34) Countries for which the regional or international application was filed: AT et al.
PCT/GB93/02637 23 December 1993 (23.12.93) WO
(34) Countries for which the regional or international application was filed: GB et al.

(71) Applicant *(for all designated States except US)*: BRITISH TELECOMMUNICATIONS PUBLIC LIMITED COMPANY [GB/GB]; 81 Newgate Street, London EC1A 7AJ (GB).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: BLOW, Keith, James [GB/GB]; 14 Cobbold Road, Woodbridge, Suffolk IP12 1HA (GB).

(74) Agent: GILL JENNINGS & EVERY; Broadgate House, 7 Eldon Street, London EC2M 7LH (GB).

(81) Designated States: AU, CA, JP, KR, NZ, US, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

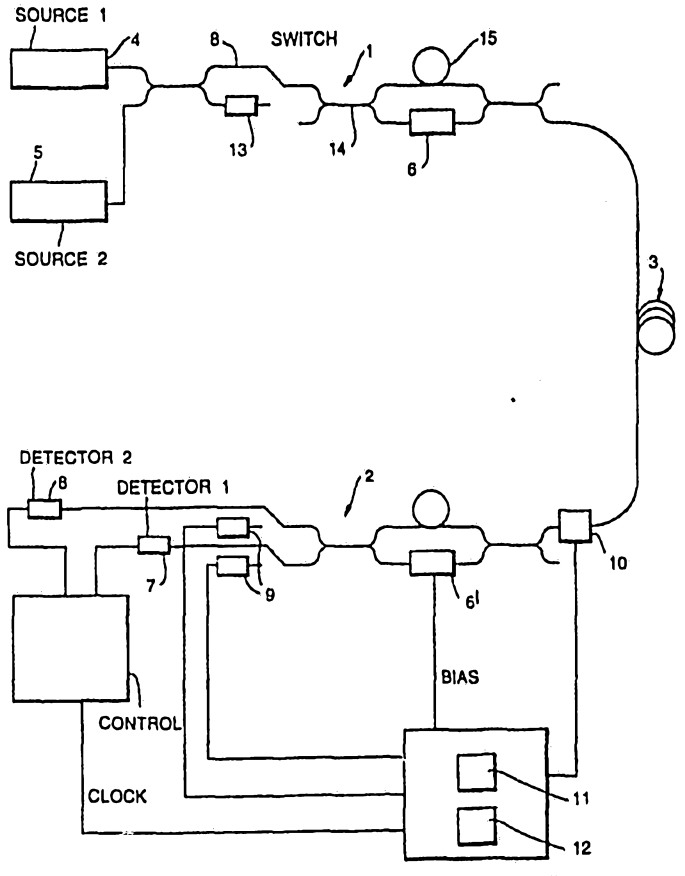
Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

678049

(54) Title: SYSTEM AND METHOD FOR QUANTUM CRYPTOGRAPHY

(57) Abstract

In a method of communication using quantum cryptography an encryption alphabet is used for coding signals for transmission on a quantum channel. The encryption alphabet comprises pairs of operators applied successively to single-photon signals transmitted onto the quantum channel with a pre-determined delay between them. When the signals are detected, the different signals of each pair are split according to their encoded state and directed to different detectors via paths giving a differential delay. The delay is substantially complementary to the original pre-determined delay. Coincidence detection is employed at the detectors to eliminate spurious detection counts.



System and Method for Quantum Cryptography

BACKGROUND TO THE INVENTION

The present invention relates to a system for the communication of encrypted data and in particular to a system employing the technique known as quantum cryptography.

In quantum cryptography data is encoded at the transmitter and decoded at the receiver using some specified algorithm which is assumed to be freely available to all users of the system, whether authorised or otherwise. The security of the system depends upon the key to the algorithm being available only to the authorised users. To this end, the key is distributed over a secure quantum channel, that is a channel carried by single-photon signals and exhibiting non-classical behaviour, as further discussed below. In the present specification, the term "single-photon" encompasses any signal having the required quantum properties. It may be generated from a highly attenuated source having in general no more than one and on average very much less than one photon per output signal, or may comprise single-photons generated by parametric down conversion. Both these techniques are described and claimed in our copending International application PCT/GB 93/02637 (WO 94/15422), the disclosures of which are incorporated herein by reference.

After the exchange of single-photon signals, the transmitter and the receiver then communicate over a separate channel, known as the public channel, to compare the transmitted and the received data. The presence of any eavesdropper intercepting the transmitted key results in a change in the statistics of the received data, which can be detected. Accordingly, in the absence of any such change in the statistics of the data, the key is known to be secure. The secret key thus established is used in the encryption and decryption of subsequent communications between the transmitter and receiver. The subsequent transmissions will generally, but not necessarily, be

carried on the same transmission channel as was used for establishing the key. For added security, the existing key may periodically be replaced by a newly generated key.

In general, a method of communication using quantum cryptography includes the steps of:

(a) randomly selecting one of a plurality of coding alphabets corresponding to different non-commuting quantum mechanical operators and encoding a signal for transmission on the quantum channel using the selected operator;

(b) randomly selecting one of the different quantum mechanical operators and using that in detecting the signal transmitted in step (a);

(c) repeating steps (a) and (b) for each of a multiplicity of subsequent signals;

(d) communicating between the transmitter and the receiver independently of the encryption alphabets to determine for which of the transmitted signals common operators were selected by the transmitter and receiver;

(e) comparing the signals transmitted and received in steps (a) and (b) to detect any discrepancy resulting from the presence of an eavesdropper; and,

(f) in the event that in step (e) no eavesdropper is detected, using at least some of the data transmitted in steps (a) and (b) as a key for encryption/decryption of subsequent data transmissions between the transmitter and receiver. This scheme is described in detail in C.H. Bennett, G. Brassard, S. Briedbart and S. Veesner in "Advances in Cryptology: proceedings with Crypto 82 (Pleenham, New York 1983); C.H. Bennett and G. Brassard, IBM Technical Disclosure Bulletin 28 3153 (1985).

In the term "encryption alphabet" as used herein, "encryption" refers to the coding of the single-photon pulses during the key distribution phase rather than to the subsequent encryption of text for transmission once a key has been established.

As described in our co-pending International filed this day entitled "QUANTUM CRYPTOGRAPHY ON A MULTIPLE

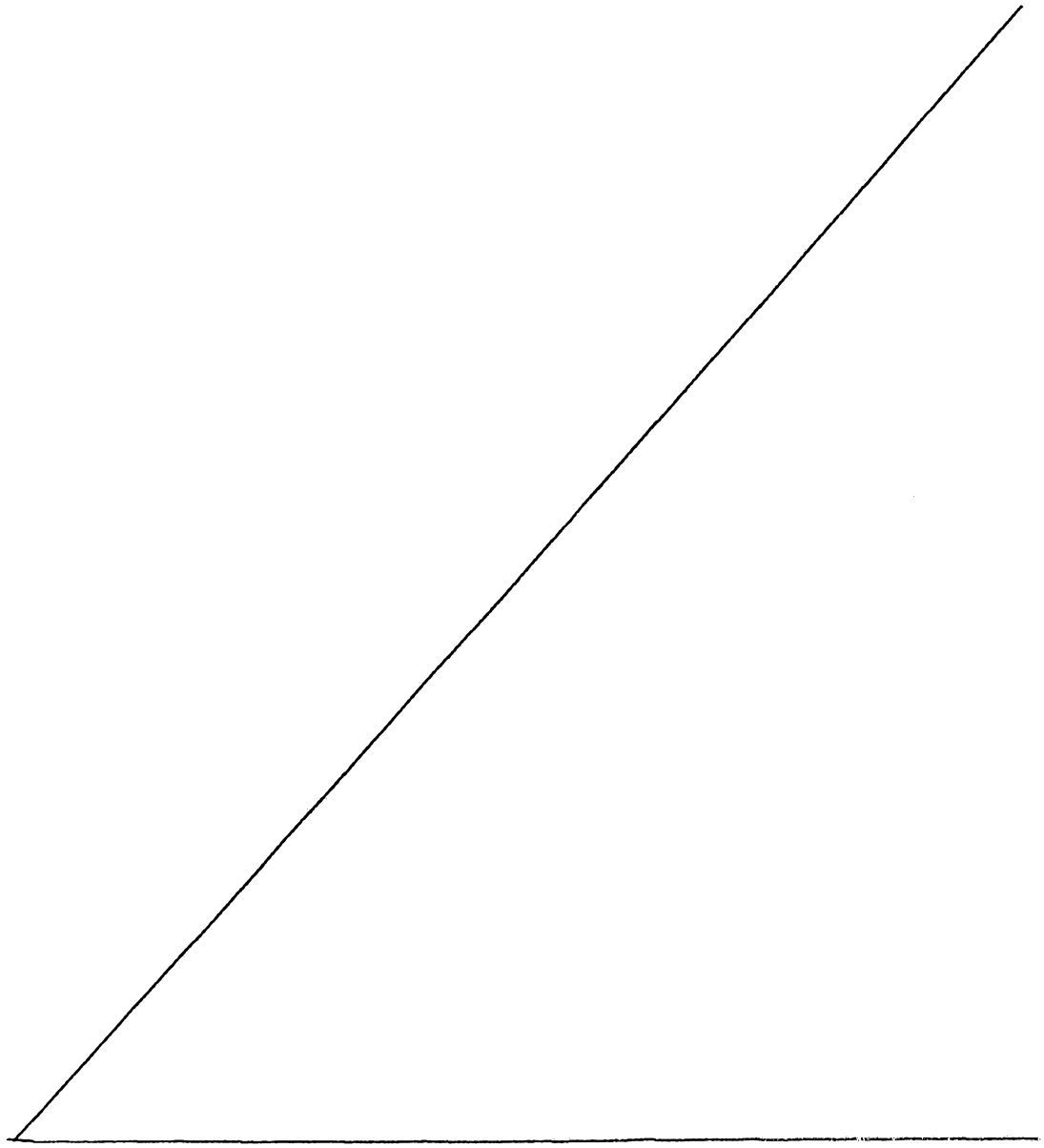
ACCESS NETWORK", WO95/07582, incorporated herein by reference, this basic quantum cryptographic technique may be extended for use in multiple-access networks. It may also be used in a configuration in which signals from the receiver are looped back to the transmitter and step of detecting using selected quantum mechanical operators is carried out there at the transmitter. This arrangement is described and claimed in our further co-pending International application also filed this day and entitled "QUANTUM CRYPTOGRAPHY", WO95/07585, also incorporated herein by reference.

SUMMARY OF THE INVENTION

According to a first aspect of the present invention, a method of communication using quantum cryptography is characterised in that the encryption alphabet used in coding signals for transmission on a quantum channel comprises pairs of operators applied successively to respective ones of a pair of single-photon signals transmitted onto the quantum channel with a predetermined delay between them, and in that in a step of detecting the single-photon signals, the signals of each pair are split according to their encoded state and directed to different detectors via paths giving a differential delay substantially complementary to the said predetermined delay and coincidence detection is employed at the detectors to eliminate spurious counts.

The present invention provides a method of quantum cryptography which is far less sensitive to system noise, and in particular to the effects of dark counts in the detectors for the single-photon signals. This is achieved

by encoding pairs (or larger groups) of single-photon signals and outputting them onto the transmission medium providing the quantum channel with a predetermined delay between them. Subsequently, the two single-photon signals are directed to different detectors depending on, for example, their encoded phase states. The path lengths to the different detectors differ by an amount providing a



delay substantially complementary to the original predetermined delay between the first and second of the single-photon signals making up the pair. That is to say, the leading single-photon signal is directed to a detector via the longer path, while the lagging single-photon signal is directed to the other detector by a shorter path, so that appropriately encoded signals arrive substantially simultaneously at the respective detectors, which is to say any time difference is smaller than the coincidence window of the detector.

Dark counts are particularly a problem with APD's operating in the 1300nm transmission window, and so the present invention is particularly advantageous when applied to such devices, or to other detectors where dark counts are a significant problem.

The operators applied to the single-photon signals may be phase operators or polarisation operators. Preferably each single-photon signal is split and passes through two paths, one only of the two paths including a phase or polarisation modulator, the signals from the two paths being recombined at the detector. A delay may be provided in one of the signal paths to separate the two paths in the time-domain.

The preferred implementations of the present invention use a Mach-Zehnder configuration to modulate the single-photon signals. This involves each single-photon signal passing through a beam splitter and then going through two branches, one only of which includes a modulator which applies a phase or polarisation shift relative to the other unmodulated path. A time delay may be introduced in one of the paths to keep the two branches separated in the time-domain while they are transmitted along a single transmission channel. This splitting of an individual single-photon signal and the use a time delay between the different branches of a Mach-Zehnder interferometer is known in the prior art and is described for example in our above-cited co-pending International application no.

PCT/GB 93/02637 (WO 94/15422) . This use of a time delay between different components of an individual single-photon signal and the application of a relative phase or polarisation shift in one of the branches is to be distinguished from the use of a time delay between different single-photon signals and the application of different operators to the different signals which is the subject of the present invention.

According to a second aspect of the present invention, there is provided a communications system including means for generating pairs of single-photon signals, means for applying pairs of operators successively to the single-photon signals and outputting them onto a quantum channel with a pre-determined delay between them, a pair of detectors connected to the quantum channel via paths giving a differential delay complementary to the said pre-determined delay, means for splitting incoming single-photon signals according to their encoded states and directing them to the different detectors, and means for detecting the coincident arrival of signals at the detectors.

BRIEF DESCRIPTION OF THE DRAWINGS

Embodiments of the present invention will now be described in detail by way of example only with reference to the accompanying Figures in which;

Figure 1 is a schematic of a prior art quantum cryptography system;

Figure 2 is a schematic of a system embodying the present invention;

Figure 3 is a detailed circuit diagram of a system embodying the present invention;

Figures 4a and 4b are single-photon sources using parametric down conversion;

Figures 5a and 5b are transmitter and detector stages respectively of a second embodiment;

Figure 6 is a schematic of the second embodiment; and

Figure 7 is a coincidence detection system.

DESCRIPTION OF EXAMPLES

Figure 1a shows schematically a prior art quantum cryptography system. This uses at the transmitter a single source which may be, for example, a highly attenuated laser producing in general no more than one photon per output pulse. The single-photon signals from this source then pass through a 50:50 beam splitter. A modulator, which in the present example is a phase modulator, is included in one branch of the signal path. This may apply, for example, a π phase shift relative to the other branch. Signals from the two branches are then output onto the transmission channel with a delay between them. At the detectors a complementary structure is used with a further beam splitter and a complementary delay in the other of the two branches so that the two components are recombined. A modulator is again provided in one of the branches at the detector and is used to determine the basis used for detection. The output of the system is encoded as a 1 or a 0 depending upon which of the two detectors receives the output pulse.

Figure 2 shows a circuit embodying the present invention. Again at the detector a pair of detectors are used, but in addition a coincidence gate (CG) is connected to the output of the detectors. At the transmitter two single-photon sources are used: a first source coupled to the first beam splitter by a short transmission path, and a second source coupled to the other side of the beam splitter by a longer transmission path. As before, a modulator, in the present example a phase modulator, is coupled in one of the branches beyond the beam splitter. A complementary structure is used at the detectors, with the path difference between the two detectors arranged to be the same as the path difference between the sources.

A new protocol is adopted for use with this system. First consider the propagation of an individual single-photon pulse through the system. Two phase changes are applied in the two half Mach-Zehnder interferometers at the

transmitter and receiver respectively. If the total phase change is 0 or π then the pulse will appear at one or other of the two detectors with unit probability. In other words, the phase change applied to a pulse can steer it to one or other of the detectors. As indicated above, in systems embodying the present invention, two single-photon pulses are used, one from each source. The relationship between the different path lengths at the sources and the detectors is such that we can obtain coincidence by arranging for a photon from source 1 to arrive at detector 2 and vice versa. Table 1 below lists the phase changes which can be used to guarantee coincidence. This table shows only the $(0, \pi)$ basis, but we can add $\pi/2$ to each phase to obtain the $(\pi/2, 3\pi/2)$ basis. In the table "phase 1" and "phase 2" refers to the phases applied at the transmitter and receiver respectively.

Table 2 shows the pairs of phases applied to the two pulses as they pass through the system. Within the $(0, \pi)$ basis the transmitter may, for example use $(0, \pi)$ to code for a 1, that is a phase change of 0 applied to the first pulse and a phase change of π applied to the second pulse; and a phase change of π followed by a phase change of 0 to encode for a "0". Then, for those received pulses for which the receiver measures in the same basis, if the receiver applies a phase change of π to the first incoming pulse and a phase change of 0 to the second incoming pulse then if a coincident output is obtained from the detectors it is known that the transmitter must have encoded with the sequence $(0, \pi)$ i.e. has encoded a logical "1". Where a coincident output is obtained and the receiver has applied phase changes of $(0, \pi)$ then the transmitter is assumed to have encoded the phase changes $(\pi, 0)$ i.e. a logical "0".

The delay between the first and second single-photon pulses of each pair needs to be greater than the coincidence window of the coincidence detector employed at the receiver. In the present example, that detector has a coincidence window of 8ns and so this sets a lower bound

for the separation of the pulses. In practice, a separation between the pulses in the range 10-20ns is used. The phase modulators are therefore required to be relatively high bandwidth devices capable of switching states on a comparably short time scale. In the embodiment described below, the phase modulator is a lithium niobate crystal. Alternatives are the use of a fibre modulator with the phase-modulation effected by XPM induced by a control beam switched into the fibre, or ferro-electric liquid crystal modulators may be used. A further alternative is the use of fast non-linear semiconductor devices.

After the quantum transmission has taken place, a public communication is performed as in conventional systems. Only those events where coincidence is obtained are considered, and the subset of events where the same basis was used at the source and the detector are used to establish a secure key. Any errors detected by a statistical test of this data subset would reveal the presence of an eavesdropper on the network. In the absence of any such errors, the transmitter and receiver can confidently use the remainder of the data as a shared secret key for subsequent encoded transmissions between themselves. Practical quantum channels, however, will suffer from unavoidable background error rates due to detector dark counts, and environmentally-induced fluctuations in the polarisation (or phase) state in the fibre etc. In this case the public discussion phase contains an additional stage of error correction and so-called "privacy amplification", as further discussed in our above-cited co-pending international application filed today (ref: 80/4541/03). This both ensures that the transmitter and receiver end up with identical keys and that any key information leaked to an eavesdropper is an arbitrarily small fraction of one bit. This procedure is outlined in C.H. Bennett, F. Bessette, G. Brassard, L.

Salvail and J. Smolin: "Experimental Quantum Cryptography", J. Cryptology, 5, 3 (1992).

Figure 3 shows in detail a fibre-base optical communications system embodying the present invention. The system comprises a transmitter 1, a receiver 2, and an optical transmission fibre 3 linking the transmitter to the receiver. The transmitter includes two optical sources 4, 5 each provided by a pulsed semiconductor laser. In the present example each laser is an Hitachi series HL1361 DFB laser diode operating at 5mw optical power at 1290-1330nm. The two lasers are driven in synchronism. The output pulses are connected to the transmission system via paths of different lengths so as to provide a predetermined delay between the pulses. When the system is used for quantum transmissions, an attenuator 13 is switched into the path of the pulses output from the lasers so as to reduce the intensity to a level where each pulse has an average no more than one photon. The attenuated pulses are then split at a fibre coupler 14 so as to pass through two branches one of which includes a fibre delay 15 and the other of which includes a phase modulator 6. As described above, the phase modulator is used to apply pairs of phase operators to the pairs of single-photon pulses from the sources using a randomly selected encoding basis. The resulting signals are coupled onto the transmission fibre 3 and from there to the receiver. At the receiver the pulses are again split between two paths one including a fibre delay and the other including a phase modulator. Signals from the two branches are then recombined and output to two single-photon detectors 7, 8. As with the laser sources, the detectors are connected to this system by paths of different lengths providing a delay complementary to that introduced at the source.

The detection circuits are shown in further detail in Figure 4. Each detector is an avalanche photo diode biased beyond breakdown and operating in the Geiger mode with passive quenching, as discussed in P.D. Townsend, J.G.

Rarity and P.R. Tapster, Electronics Letters, 29, 634 (1993). Silicon APDs such as the SPCM-100-PQ (GE Canada Electro Optics) can be used in 400-1060nm wavelength range, while germanium or InGaAs devices such as MDL5102P or MDL5500P (NEC) can be used in the 1000-1550nm range. A distinctive feature of the present inventions is that it makes operation at wavelengths around 1300nm practical. At this wavelength, detectors of the type described above suffer relatively high dark count rates. However the present invention greatly reduces the loss of data from the dark count. Consider a detector with a dark count rate η which is being used to count photons in a time interval τ. The number of dark counts in this interval is $\eta\tau$ and this number is less than unity. When two such detectors are used, the number of coincident counts is $(\eta\tau)^2$ which in general is significantly smaller than the number of counts at a single detector.

As an alternative to APD's, other single-photon detectors may be used, such as e.g., photomultiplier tubes (PMTs).

Figure 5 shows the coincidence detection system in further detail. Electrical pulses from the two APDs are amplified and then passed through a discriminator. The discriminator rejects low level amplifier noise by generating an electrical pulse of definite height and width only when the amplified signals exceed a specified threshold level. The LeCroy 612A and 622 amplifier and discriminator modules would be suitable for this purpose. Processed pulses from the two detectors are used as inputs to the two input channels of a coincidence gate such as the LeCroy 622. When operating in the AND mode this module generates an output pulse only if pulses arrive at the two inputs within 8ns of each other. The temporal width of the coincidence window means that the two pulse pairs in the fibre must be separated by greater than 8ns in order to avoid spurious coincidence detections.

As an alternative to the use of attenuated semiconductor lasers, the two single-photon sources may be provided using parametric down conversion. A suitable source of this type is shown in Figure 4a, using a non-linear crystal NLC formed from KDP. It is advantageous to use two such circuits driven in synchronism to provide the two sources. Then if the outputs of the two source photodetectors are ANDed together as shown in Figure 4b, it can be determined when the required simultaneous output have been produced. The transmitter can then be arranged to store data, i.e. the record of the modulation basis and logical value encoded, only for those time slots in which a simultaneous output has occurred. This avoids the storing of redundant data.

As an alternative, a single down-conversion crystal may be used to provide both sources. In that case the photodetector and gate is eliminated from the circuit, and the two output branches from the crystal provide the two sources. With this arrangement, it is not known when simultaneous outputs have occurred, and so it is necessary to store data for every time slot.

The presently described example is arranged to carry out a calibration function as described in the present applicants co-pending British application no. 9226995.4. To this end, the transmitter is provided with an alternative output path from the semiconductor lasers which bypasses the attenuator. This produces a bright multi-photon signal which is transmitted across the network and is used both for calibration of the network initially, and also for the public discussion phase of the quantum cryptographic protocol. To receive the multi-photon pulses from the sources, a complementary standard detector 9 is provided in the receiver.

In use, any communication between the transmitter and the receiver is initialised by using the multi-photon signals to measure the output polarisation from the transmission fibre 3. A polarisation compensator 10 in the

receiver 2 is then adjusted via a feedback loop in order to linearise the output polarisation and match it to the preferred polarisation axis of the receiver. For the case of phase encoding, the transmitter and receiver then use the multi-photon signals to calibrate the relative phase shift in their interferometer. This involves setting the AC drive voltages to the respective phase modulators 20 and using the feed back circuit to maximise the output from the interferometer output port by either changing the DC bias to the receiver's modulator, or via an additional phase-shifting component. This then completes the calibration of the system. The optical switches in the transmitter and receiver are then set to establish a quantum channel by connecting the low intensity source and the single-photon detectors respectively to the transmission fibre.

The calibration steps may be repeated intermittently as and when necessary.

The bright multi-photon source may also be used to communicate a system clock to the receiver for synchronisation of the transmitter and receiver time-slots. During this process, the output from the public channel detector is passed through an electronic filter 11 to provide an oscillating signal at the pulse repetition frequency. This is then used to lock a local oscillator 12 in the receiver to the optical source frequency. This local oscillator then provides the timing information required by the receiver during the quantum transmission stage of the protocol. Each time the transmission system is re-calibrated via the public channel the local oscillator may be re-timed so as to avoid the accumulation of any timing errors.

The quantum key distribution channel is arranged to operate independently of other transmission channels which pass betweem the transmitter and receiver carrying either the encrypted data or standard (non-encrypted) signals. This is important since the quantum channel operates in a non-continuous burst transmission mode, whereas in general

the data channels will be required to provide uninterrupted continuous transmission. The required separation of the quantum channel may be provided through use of a reserved wavelength, different from that used by the data channels. In this case the quantum channel could be isolated by means of wavelength-sensitive passive optical components such as WDM couplers (e.g. Scifam Fibre Optics P2SWM13/15B) and filters (e.g. JDS TB1300A). The quantum channel may lie within the 1300 nm telecommunication window along with several other channels reserved for conventional signal traffic. Alternatively the 850 nm window is reserved for the quantum channel. This has the advantage that single-photon detectors for this wavelength (Silicon APDs) are relatively insensitive to 1300 nm light and therefore isolation from the data channels is easier to achieve. This approach would require WDM couplers such as the JDS WD813 to combine and separate the quantum and conventional channels. Alternatively the 1500nm band might be used for conventional signal traffic while the 1300nm band is reserved for the quantum channel. Since, the sensitivity of germanium APDs is high at 1300nm and falls rapidly for wavelengths longer than about 1400nm, these detectors would be an attractive choice for this particular wavelength division scheme. The wavelength separation technique would also allow active components such as optical amplifiers (e.g. erbium or praseodymium rare-earth-doped fibre amplifiers) to be used at the data channel wavelengths, whilst operating the quantum channel at a wavelength outside the spontaneous emission spectrum of the amplifier. If this were not the case, the spontaneously generated photons from the amplifier would easily saturate the detectors on the quantum channel.

Alternatively, it is possible to operate the quantum and data channels at the same wavelength, and achieve isolation by means of polarisation- or time-division multiplexing. The former case uses phase-encoding for the quantum channel, as described, e.g., in our co-pending

International application PCT/GB 93/02637. The data channel operates on the orthogonal polarisation mode of the fibre, with isolation obtained by means of polarisation splitting couplers such as the JDS PB 100. In the time-division scheme, certain time slots are reserved for multi-photon data pulses which are detected by standard receivers linked to the network via standard fibre couplers. Saturation of the single-photon detectors during these time slots could be prevented either by means of switchable attenuators (intensity modulators) or by turning off the reverse bias to the devices. Any of these isolation techniques may also be employed to send the system timing information concurrently with the quantum key data. This approach may be useful if, for example, the timing jitter on the receiver local oscillators is too large to maintain system synchronisation over the timescale required for the quantum transmission. A further alternative technique provides the timing data concurrently with the quantum transmission using the same wavelength as the quantum channel. The receiver now contains, in addition, a standard detector such as a sensitive PIN-FET that is connected to the transmission fibre by a weak fibre tap that splits off e.g. ~10% of the incoming pulse intensity. The intensity of every n-th pulse is made sufficiently large, say 10^5 photons, that the standard detector registers a pulse which can be used for timing purposes. If n is sufficiently large, e.g. 1000, the APDs will not suffer from heating effects or saturation, and a x1000 frequency multiplier can be used in the receiver to generate a local oscillator at the clock frequency.

Although the embodiment of Figure 3 uses a simple point-to-point configuration, it will be appreciated that the present invention can be used with a wide range of different system topologies. These include multiple-access networks having, for example, star, tree or ring configurations and may include a looped-back path from the receiver to the transmitter as described in our above-cited

co-pending European applications. As described in those applications, the transmitter may output un-modulated signals which are modulated at the receiver and returned to the transmitter.

Figure 6 shows a further embodiment using a multiple access network connecting a plurality of receivers R1,R2... to a transmitter in the form of a "controller" including both a transmit stage TS and a detector stage DS. Figures 5a and 5b show in detail the transmitter and detector stages respectively. In the transmitter output stage of this embodiment, a first pulsed semiconductor laser 51, operating at a first wavelength λ_q, where, e.g., λ_q=1300nm provides the optical source for the quantum channel. The laser and a modulator driver 55 for a phase modulator 54 are controlled by a microprocessor 56. The phase modulator 54 is located in one branch of the transmitter. A polarisation controller PC (e.g. BT&D/HP MCP1000) is located in the other branch of the transmitter. A second semiconductor laser 52 provides a bright multi-photon source at a wavelength λ_s where, e.g., λ_s=1560nm. This signal is used for timing and calibration as described above. The signal at λ_s is coupled to the output of the transmitter via a WDM coupler 57 which may be, e.g. a JDS WD1315 series device.

As an alternative to the use of separate sources for the quantum channel and the timing signal, a single semiconductor laser may be used feeding its output via a fused fibre coupler FC to two different branches, one including an attenuator, and the other branch being unattenuated, as in the previous embodiments discussed above. An optical switch may then be used to select either the bright or attenuated output. Depending upon the frequency requirement, either a slow electro-mechanical device such as the JDS Fitel SW12 or a fast electro-optic device such as the United Technologies Photonics YBBM could be used.

In the receiver of this embodiment, a respective control microprocessor 57 controls the receiver phase modulator 58 via a modulator driver 59. The receiver control processor also controls a detector bias supply 60 for the a pair of single-photon detectors 601, 602. In both the transmitter and the receiver, where the signal path branches, fused-fibre 50/50 couplers are used. Suitable couplers are available commercially from SIFAM as model P22S13AA50. The timing signal at λ_s is detected by a PIN-FET receiver 64.

Appropriate phase modulators 54, 58 for the data encoding and decoding are lithium niobate or semiconductor phase modulators operating at, e.g., 1-10MHZ. An appropriate lithium niobate device is available commercially as IOC PM1300. An appropriate driver for the phase modulators is a Tektronix AWG2020, and this can also be used as a clock generator for the system. For the single-photon detectors, APDs as discussed above with reference to Figure 3 may be used. Significant improvements could be obtained by combining the phase modulators and fibre devices shown in Figures 5a and 5b into single integrated structures. Variations on the current design or that discussed in P.D. Townsend, J.G. rarity and P.R. Tapster, Elect. Lett. 29, 634 (1993) could be integrated onto a lithium niobate chip with the fibre paths replaced by waveguides and the modulator region defined by electrodes as in a standard device. Alternative fabrication methods include e.g. photo-refractively-defined planar silica waveguide structures or semiconductor waveguide structures. In general, integration should lead to improved stability and compactness for the transmitter and receiver structures. In particular, this embodiment uses an NEC 5103 Ge APD cooled to 77K using, e.g., Hughes 7060H cryo-cooler or a liquid nitrogen dewar or cryostat. In the transmitter in this embodiment, just a single source is used for the quantum channel, with the delay between the

pair of pulses being provided by a delay loop D in one of a pair of branches connected to the source.

The key distribution protocol requires each pair of received photons to be associated with a given clock period and also identified as a 0 or 1 depending the results of the coninicidence detection and the state of the modulator, as described above. These functions are performed by a time interval analyser 62 (e.g. Hewlett-Packard 53110A). The start signals for this device are provided by the APD output after processing by amplifiers, discriminators and a coincidence gate as already detailed.

The timing signal referred to above may take the form of either a single trigger pulse, which is then used to initiate a burst of key data on the quantum channel, or as a continuous stream of pulses at the system clock frequency which are used to re-time the receiver clock between key transmissions. Before key transmission commences, the receiver varies the phase modulator DC bias level in order to zero the phase shift in the interferometer (i.e. photon transmission probability is maximised at one output port and minimised at the other). Figures 5a and 5b also show the relative spatial, temporal and polarisation changes experienced by the two components of a quantum channel pulse as they propagate through the transmitter and receiver. If all fibres in the system are polarisation-preserving then no active polarisation control or static polarisation controllers are required in the system. However if standard fibre is used for the transmission link then active polarisation control will be required at the input to the receiver. This can be performed using a standard detector, feedback circuit and automated polarisation control as described in our co-pending International application PCT/GB93/02637 (WO94/15422).

The present invention may be implemented on a network in which one or more receivers modulate a received single photon signal and return it to the transmitter where single photon detection takes place. Such networks are described

in PCT/GB 93/02637. A possible attack upon such an implementation requires Eve (the eavesdropper) to intercept the quantum channel on both sides of a given user Bob. Then by transmitting and detecting a multi-photon signal Eve can determine unambiguously the state of Bob's modulator. Again in practice it is likely to be very difficult for Eve to establish connections to two or more points in the network . Nonetheless, where it desired to protect against an attack of the type described this may be done by providing at least one of the receivers on the network with a photon detector connected to the network by a relatively weak tap. This photon detector need not be of the sensitivity of the single photon detectors employed conventionally in receivers, nor need every user have such a detector. The presence of such a detector in the network facilitates the detection of any multi-photon probe used by Eve.

In embodiments using a multiple access loop, at the end of the public discussion phase the transmitter has established a distinct sequence of r secret bits with each ith terminal R_i on the network. These secret bits can be used both for authentication and the generation of a respective shared key K_i, as described for the standard point-to-point application in C.H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin: J. Crypt., 5, 3 (1992) and Bennett/Brassard IBM Tech. Discl. (already referenced above). If required, the controller/transmitter can then use the individual K_i as keys in one-time pad encryptions of a master network key or keys. The latter can then be securely distributed to all receivers/terminals, or subsets of terminals, on the network. Consequently, two types of encrypted communication are enabled. In one-to-one communications the controller and R_i use K_i to encrypt the multi-photon data signals that are broadcast in either direction on the network. Hence, although these signals are broadcast on the network and are therefore accessible to all receivers, only R_i and the controller can decode

these particular data transmissions. In this scenario secure inter-terminal communications can still take place between e.g. R_i and R_j, however the controller must act as an interpreter using its knowledge of K_i and K_j to decode and encode the incoming and outgoing signals. Any-to-any communications can also take place among subsets of terminals sharing a master key, and in this case, if a transmission path goes via the controller, the controller only needs to perform routing or re-transmission of the incoming encoded data. A fresh key may be transmitted periodically, to maintain security.

TABLE 1

From	Phase 1	Phase 2	To
Source 1	0	π	Detector 2
Source 1	π	0	Detector 2
Source 2	0	π	Detector 1
Source 2	π	0	Detector 1

TABLE 2

Phase 1	Phase 2
$(0,\pi)$	$(\pi,0)$
$(\pi,0)$	$(0,\pi)$
$(\pi/2,3\pi/2)$	$(\pi/2,3\pi/2)$
$(3\pi/2,\pi/2)$	$(3\pi/2,\pi/2)$

CLAIMS

1. A method of communication using quantum cryptography characterised in that the encryption alphabet used in coding signals for transmission on a quantum channel comprises pairs of operators applied successively to respective ones of a pair of single-photon signals transmitted onto the quantum channel with a predetermined delay between them, and in that in a step of detecting the single-photon signals, the signals of each pair are split according to their encoded state and directed to different detectors via paths giving a differential delay substantially complementary to the said pre-determined delay and coincidence detection is employed at the detectors to eliminate spurious counts.

2. A method according to claim 1, in which in the step of coding each single-photon signal, the single-photon signal is split between two paths, one only of the two paths including a phase or polarisation modulator, the signals from the two paths being recombined before the step of detecting.

3. A method according to claim 2, in which a delay is provided in one of the two paths to separate the two paths in the time-domain.

4. A method according to any one of the preceding claims, in which the step of decoding the single-photon signals includes randomly selecting a detection basis, and within that detection basis applying a first operator to a first incoming photon of the pair, and a second, different, operator to a second incoming photon of the pair, or

alternatively applying the second operator to the first photon and the first operator to the second photon; when a coincident output is obtained, the signal being detected as logical 1 or logical 0 according to which of the alternative sequences of operators was selected.

5. A method according to any of the preceding claims, in which the single-photon signals are at a wavelength in the region of 1300nm.

6. A communications system including means for generating pairs of single-photon signals, means for applying pairs of operators successively to the single-photon signals and outputting them onto a quantum channel with a pre-determined delay between them, a pair of detectors connected to the quantum channel via paths giving a differential delay complementary to the said pre-determined delay, means for splitting incoming single-photon signals according to their encoded states and directing them to the different detectors, and means for detecting the coincident arrival of signals at the detectors.

7. A system according to claim 6, in which the means for generating pairs of single-photon signals, comprise a pair of optical sources connected to the quantum channel by different paths giving the pre-determined differential delay.

8. A system according to claim 7, including means for detecting when coincident outputs are produced by the two-sources.

9. A system according to claim 8, in which the optical sources comprise a pair of parametric down conversion sources, each of the sources including a detector in one of its output branches, the output of the two detectors in the respective sources being ANDed to generate a signal indicating coincident output from the two sources.

10. A system according to any one of claims 6-9, in which the detectors are avalanche photo-diodes.

11. A system according to any one of claims 6 to 10, in which the means for detecting coincident arrival comprises a coincidence gate connected to the different detectors.

12. A system according to any one of claims 6 to 11, in which the quantum channel is carried on a multiple access network.

13. A communication system substantially as hereinbefore described with reference to Figure 3 or Figures 5a, 5b and 6 of the accompanying drawings.

DATED this 25th day of February, 1997

BRITISH TELECOMMUNICATIONS public limited company

Attorney: PETER R. HEATHCOTE
Fellow Institute of Patent Attorneys of Australia
of SHELSTON WATERS

Fig.1.

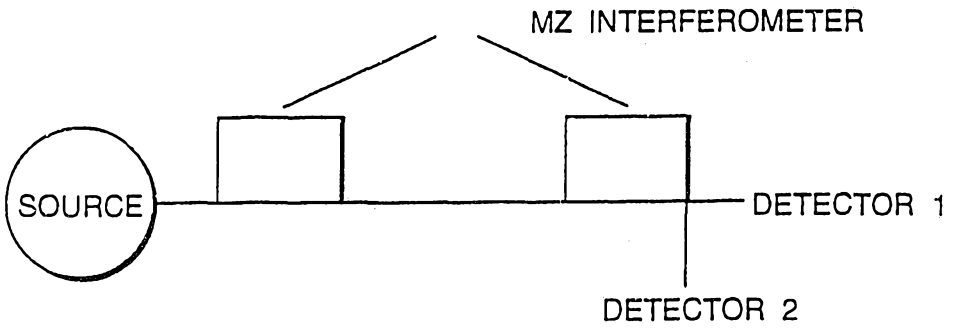
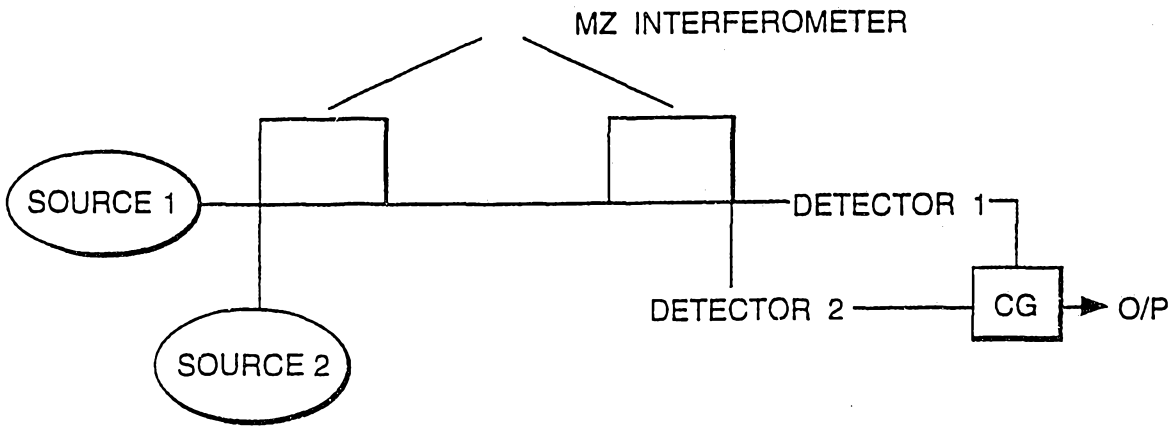

MZ INTERFEROMETER
SOURCE
DETECTOR 1
DETECTOR 2

Fig.2.


MZ INTERFEROMETER
SOURCE 1
DETECTOR 1
DETECTOR 2
CG
O/P
SOURCE 2

75440/94

Fig.3.

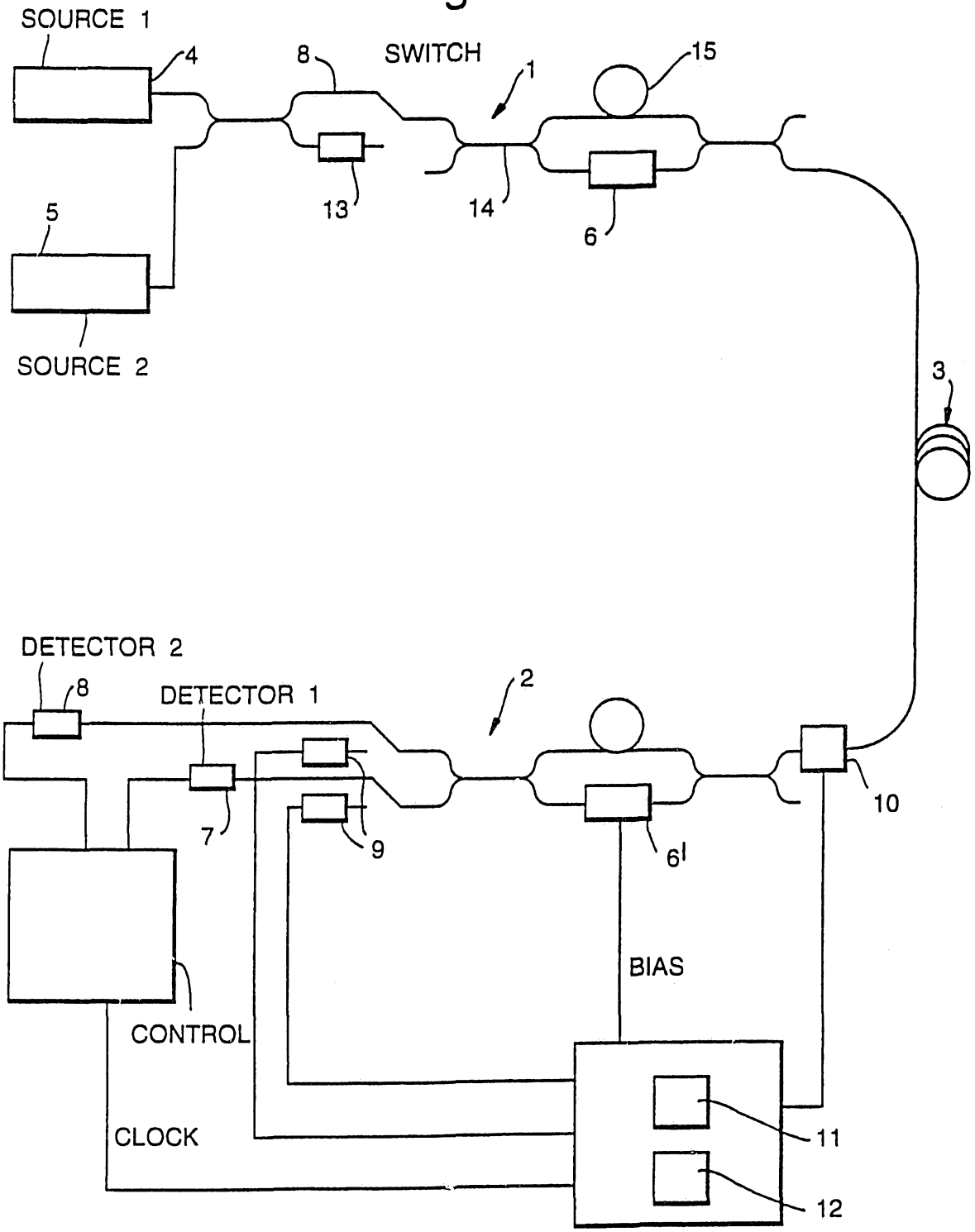


Fig.4a.

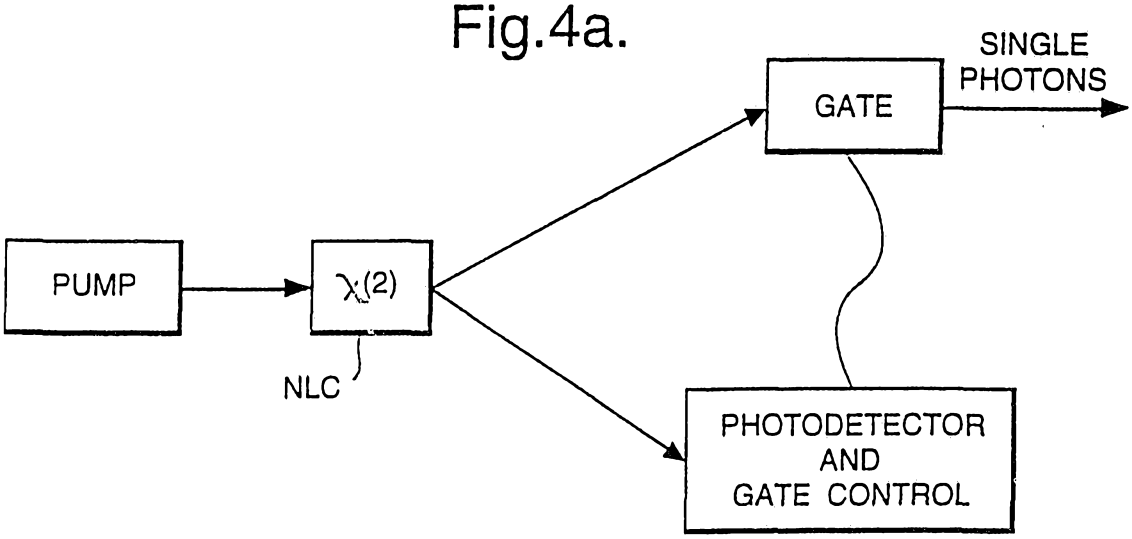
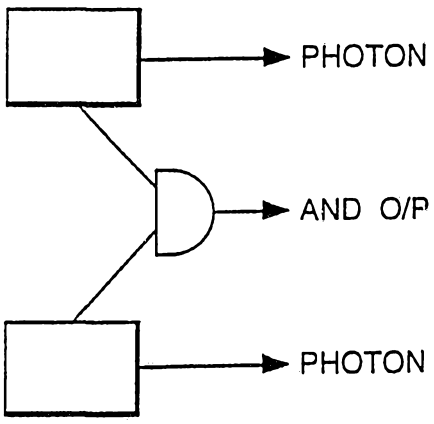

SINGLE
PHOTONS
GATE
PUMP
χ(2)
NLC
PHOTODETECTOR
AND
GATE CONTROL

Fig.4b.


PHOTON
AND O/P
PHOTON

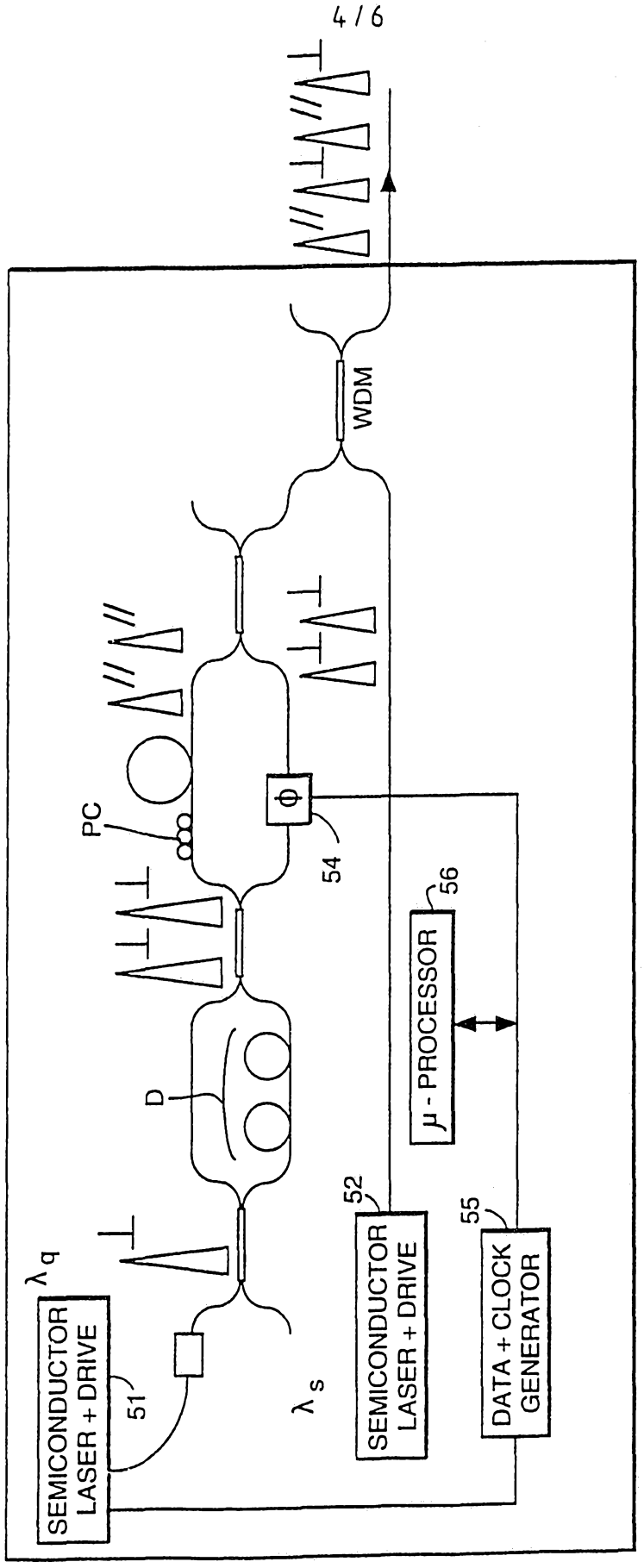

TRANSMITTER
SEMICONDUCTOR LASER + DRIVE
51
λ_q
λ_s
D
PC
54
ϕ
WDM
SEMICONDUCTOR LASER + DRIVE
52
μ - PROCESSOR
56
DATA + CLOCK GENERATOR
55

Fig.5a.

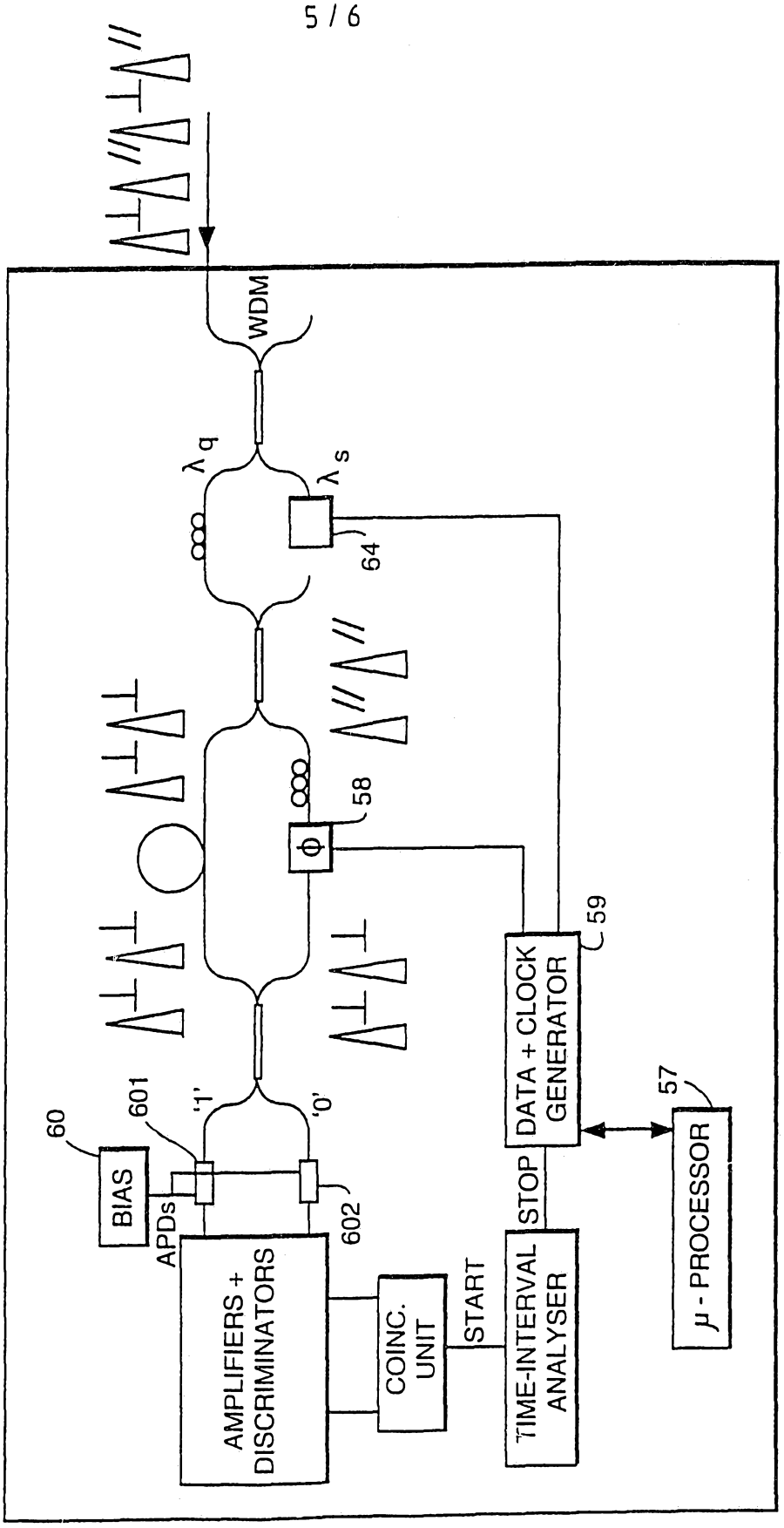

DETECTOR
WDM
λq
λs
64
58
60
601
'1'
'0'
BIAS
APDs
602
AMPLIFIERS + DISCRIMINATORS
COINC. UNIT
START
STOP
TIME-INTERVAL ANALYSER
DATA + CLOCK GENERATOR
59
57
μ - PROCESSOR

Fig.5b.

Fig.6.

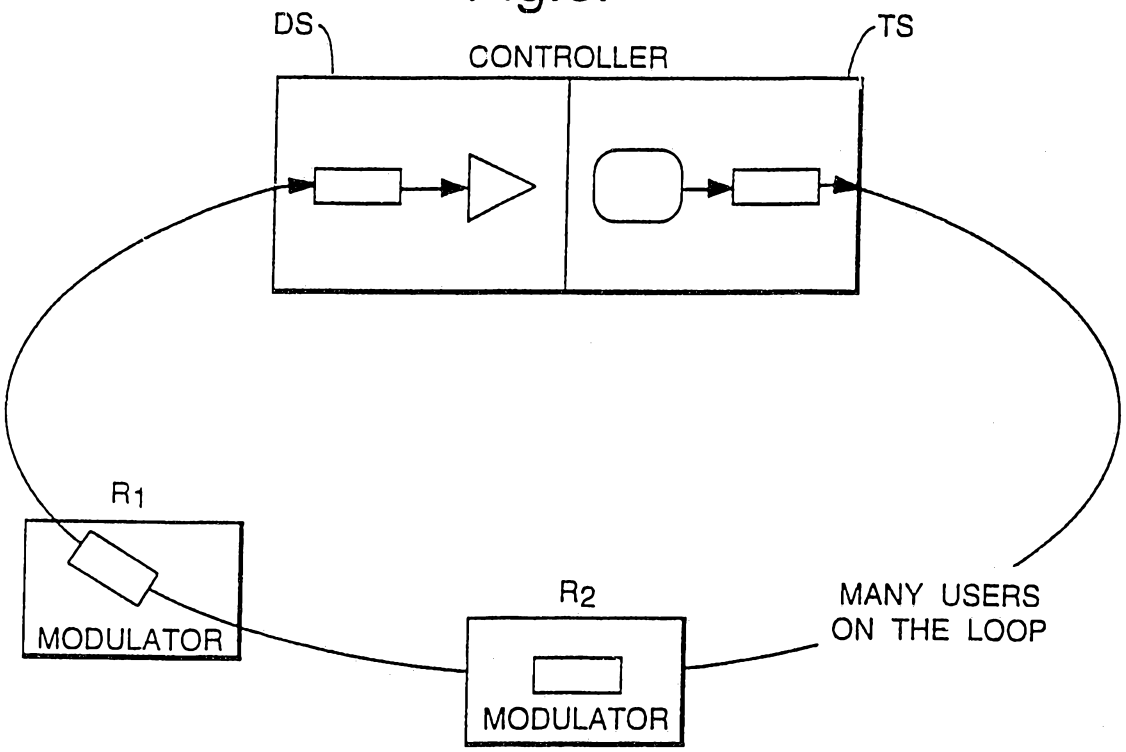
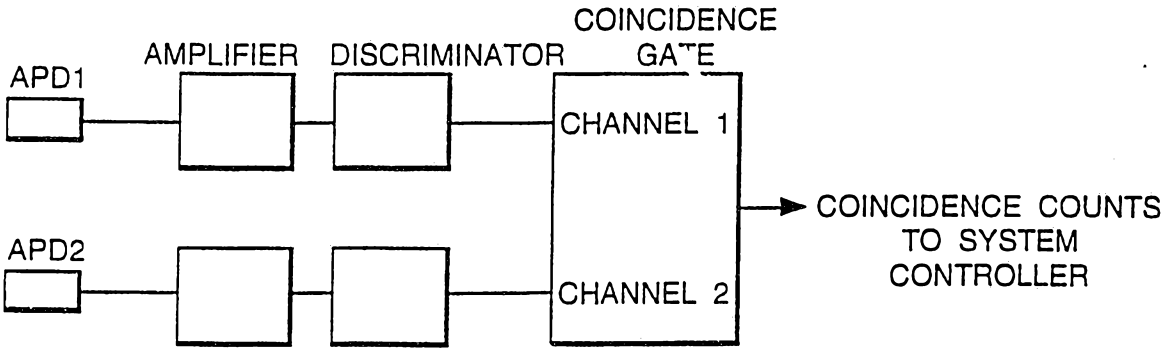

DS
CONTROLLER
TS
R1
MODULATOR
R2
MODULATOR
MANY USERS
ON THE LOOP

Fig.7.


COINCIDENCE
AMPLIFIER
DISCRIMINATOR
GATE
APD1
CHANNEL 1
COINCIDENCE COUNTS
TO SYSTEM
CONTROLLER
APD2
CHANNEL 2

INTERNATIONAL SEARCH REPORT

Inte· onal Application No
PCT/GB 94/01954

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 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)
IPC 6 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)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	ELECTRONICS LETTERS, vol.29, no.7, 1 April 1993, STEVENAGE GB pages 634 - 635, XP361197 P.D.TOWNSEND ET. AL. 'SINGLE PHOTON INTERFERENCE IN 10km LONG OPTICAL FIBRE INTERFEROMETER' cited in the application see page 634, left column, line 26 - page 635, left column, line 20 see figure 1 --- -/--	1-3,5,6, 10

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

[X] Patent family members are listed in 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

1

Date of the actual completion of the international search	Date of mailing of the international search report
28 November 1994	05. 01. 95

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, Tx. 31 651 epo nl, Fax (+ 31-70) 340-3016	Lydon, M

INTERNATIONAL SEARCH REPORT

International Application No
PCT/GB 94/01954

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	ELECTRONICS LETTERS, vol.29, no.14, 8 July 1993, STEVENAGE GB pages 1291 - 1293, XP322277 P.D.TOWNSEND ET. AL. 'ENHANCED SINGLE PHOTON FRINGE VISIBILITY IN A 10km-LONG PROTOTYPE QUANTUM CRYPTOGRAPHY CHANNEL' see page 1291, right column, line 20 - page 1292, left column, line 8 see page 1292, left column, line 23 - line 30 see figure 1	1-3,5,6
A	EUROPHYSICS LETTERS, vol.23, no.6, 20 August 1993, SWITZERLAND pages 383 - 388 A.MULLER ET AL. 'EXPERIMENTAL DEMONSTARATION OF QUANTUM CRYPTOGRAPHY USING POLARIZED PHOTONS IN OPTICAL FIBRE OVER MORE THAN 1 km' see page 385, line 2 - line 16 see page 385, line 19 - page 386, line 20 see figures 1,2	1,6,10
A	US,A,5 243 649 (FRANSON) 7 September 1993 see column 2, line 4 - line 26 see column 6, line 36 - column 7, line 47 see figures 1,6	1,6

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter ..nal Application No
PCT/GB 94/01954

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US-A-5243649	07-09-93	NONE	