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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 February 2021 (18.02.2021)

WIPO | PCT

(10) International Publication Number
WO 2021/028227 A1

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

(21) International Application Number:
PCT/EP2020/071445

(22) International Filing Date:
29 July 2020 (29.07.2020)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
19191192.4 12 August 2019 (12.08.2019) EP

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

(72) Inventor: **LORD, Andrew**; Ground Floor, Faraday Building, 1 Knightrider Street, London EC4V 5BT (GB).

(74) Agent: **BRITISH TELECOMMUNICATIONS PUBLIC LIMITED COMPANY, INTELLECTUAL PROPERTY DEPARTMENT**; Ground Floor, Faraday Building 1 Knightrider Street, London EC4V 5BT (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, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

WO 2021/028227 A1

(54) Title: IMPROVEMENTS TO QKD METHODS

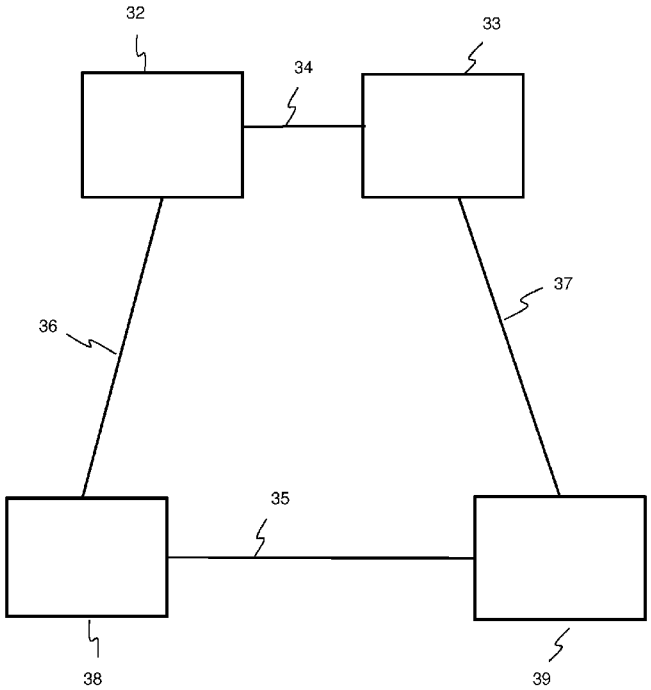

Fig. 3

(57) Abstract: There is herein disclosed a method of performing Quantum Key Distribution for generating a shared secret key, the method comprising, at a first node, preparing or measuring a plurality of non-orthogonal quantum states, each of the plurality of non-orthogonal quantum states being prepared or measured using a respective one of a first set of basis states, and, at a second node, preparing or measuring the plurality of non-orthogonal quantum states each, of the plurality of non-orthogonal quantum states being prepared or measured using a respective one of a second set of basis states, and, at a third node, obtaining an indication of the first set of basis states from the first node and performing a key agreement stage with a fourth node to agree the shared secret key, the key agreement stage involving the first and second sets of basis states.

[Continued on next page]

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

Published:

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

Improvements to QKD methods

QKD (Quantum Key Distribution) is a known method of highly-secure communication which enables two parties to produce a shared secret key. In one example of a QKD network, there is a transmitting unit (referred to as Alice) which prepares a single photon pulse in a randomly-chosen basis state, and encodes the pulse with a randomly-chosen bit value of 0 or 1. The basis state could be, for example, a polarisation state (e.g. rectilinear or diagonal). The pulse is then transmitted to a receiving unit (referred to as Bob) which measures the value encoded onto it in its own randomly-chosen basis state. The process is repeated for each of a string of pulses. Alice and Bob then exchange information relating to the basis states that each used. They use that information to discard from their records, the bit values of pulses for which the basis state Alice used was different to the basis state Bob used. This leaves Alice and Bob with the same list of bit values (i.e. a list of 1's and 0's) which constitutes a shared secret quantum key.

This secret quantum key is considered to be very secure because any attempt to intercept the transmission of the pulses by an eavesdropper causes the bit values encoded onto them to be irretrievably lost. This loss of data can be detected by Alice and Bob during checking procedures.

A problem with QKD systems is that the distance optical pulses can travel in an optical fibre is limited, the largest possible distance being about 200km. Therefore if two communicating parties are located further apart than this distance, QKD will not work. Furthermore, due to their large expense, QKD systems are found in only a limited number of places in the world. These factors mean that QKD systems are not a realistic option for many companies that would otherwise choose to use them.

Attempts to address this problem have included using a secure "trusted node". The trusted node is placed in the optical path between the two parties (e.g. two companies) that wish to communicate securely (one company being located at a transmitter (Alice) and the other at a receiver (Bob)). The trusted node contains a receiver (i.e. a Bob) and a transmitter (i.e. an Alice). The first company establishes a quantum key with the Bob in the trusted node. The second company establishes a separate quantum key in the manner described above, with the Alice in the trusted node. The two companies can therefore communicate securely with each other over twice the distance that was

previously possible. This process is described in greater detail below, with reference to Fig. 2. A disadvantage of this technique is that the distance between Alice and Bob is not significantly increased. Furthermore, this technique necessitates the establishing of two separate quantum keys.

It would be desirable to provide an improved QKD system which overcomes and/or mitigates some or all of the above-mentioned and/or other disadvantages associated with the prior art.

According to a first aspect of the invention there is provided a method of performing Quantum Key Distribution (QKD) for generating a shared secret key, the method comprising

at a first node, preparing or measuring a plurality of non-orthogonal quantum states, each of the plurality of non-orthogonal quantum states being prepared or measured using a respective one of a first set of basis states,

at a second node, preparing or measuring the plurality of non-orthogonal quantum states each, of the plurality of non-orthogonal quantum states being prepared or measured using a respective one of a second set of basis states,

at a third node, obtaining an indication of the first set of basis states from the first node and performing a key agreement stage with a fourth node to agree the shared secret key, the key agreement stage involving the first and second sets of basis states.

In some embodiments the fourth node is the second node. In preferred embodiments the fourth node is different to the second node.

The invention is intended for use with any protocol, such as prepare-and-measure protocols or entanglement protocols. In methods performed in accordance with entanglement protocols, the method may comprise, at the first node, measuring the plurality of non-orthogonal quantum states, and may further comprise, at the second node, measuring the plurality of non-orthogonal quantum states. In methods performed in accordance with prepare-and-measure protocols, the method may comprise, at the first node, preparing the plurality of non-orthogonal quantum states, and may further comprise, at the second node, measuring the plurality of non-orthogonal quantum states.

The step of preparing a plurality of non-orthogonal quantum states may comprise encoding a respective bit value onto each of the plurality of non-orthogonal quantum states. The step of measuring a plurality of non-orthogonal quantum states may comprise measuring a bit value for each of the plurality of non-orthogonal quantum states.

The invention is applicable to both discrete-variable QKD (DV-QKD) and continuous-variable QKD (CV-QKD). In embodiments using DV-QKD, the first and second sets of basis states may be polarisation states such as rectilinear and diagonal. Furthermore, the bit values encoded onto the plurality of non-orthogonal quantum states may be discrete values such as ones and zeroes. In embodiments using CV-QKD, the first and second sets of basis states may be quadratures such as position and momentum. Furthermore, the bit values encoded onto the plurality of non-orthogonal quantum states may be non-discrete values such as Gaussian values.

The step of, at the third node, obtaining the first set of basis states from the first node may comprise obtaining the first set of basis states from the third node directly and may comprise transmitting the first set of basis states from the first node to the third node. This may take place via an optical link.

The first node and/or the second node may be quantum nodes. The method may further comprise transmitting the plurality of non-orthogonal quantum states from the first node to the second node. The step of transmitting the plurality of non-orthogonal quantum states from the first node to the second node may take place of over a quantum channel which may be and optical fibre or may be free space.

The step of encoding a bit value onto each of the plurality of non-orthogonal quantum states may comprise generating a plurality of random bit values which may be generated using a random number generator. The first set of basis states may be randomly-chosen using a random number generator. The second set of basis states to the plurality of non-orthogonal quantum states may be randomly-chosen using a different random number generator.

The method may further comprise, for each of the plurality of non-orthogonal quantum states, making a record of the bit value encoded onto the quantum state and/or making

a record of the which of the first set of basis states the quantum state is prepared in and/or making a record of the time of transmission of the quantum state from the first node.

The method may further comprise, for each of the plurality of non-orthogonal quantum states, making a record of the measured bit value of the quantum state and/or making a record of the which of the second set of basis states is used to measure the quantum state and/or making a record of the time of receipt of the quantum state at the second node.

The method may further comprise performing an authentication check between the third node and the fourth node. The authentication check may comprise the fourth node sending the third node information establishing the identity of the fourth node. The authentication check may comprise the third node sending the fourth node information establishing the identity of the third node.

The method further comprises determining the bit values encoded onto those ones of the plurality of non-orthogonal quantum states which were prepared and measured in the same basis state. This may comprise transmitting, from the fourth node to the third node, an indication of the basis states that were used to measure the plurality of non-orthogonal quantum states. Alternatively this may comprise transmitting, from the third node to the fourth node, an indication of the basis states that were used to prepare the plurality of non-orthogonal quantum states. In either case, the method may further comprise comparing the indication of the basis states that were used to measure the plurality of non-orthogonal quantum states with the basis states that were used to prepare the plurality of non-orthogonal quantum states. The method may further comprise transmitting an indication of the common basis states from the third node to the fourth node or vice versa. The bit values corresponding to the common basis states may constitute the shared quantum key. The transmissions between the third and fourth nodes may be encrypted.

The third and fourth node may perform encrypted communication using the shared quantum key. This may comprise encrypting data at the third node using the secret key. The encrypted data may be sent to the fourth node. The data may be decrypted at the fourth node. The third node may be a customer premises.

The method may further comprise transmitting, from the first node to the third node, an indication of the bit values encoded onto the plurality of non-orthogonal quantum states and/or an indication of which of the first set of basis states were used to prepare the plurality of non-orthogonal quantum states and/or an indication of the time of transmission of the plurality of non-orthogonal quantum states from the first node. These transmissions between the first node and the third node may be encrypted. The encryption may be symmetric key encryption and may be AES512. The information contained in these transmissions may be transmitted without being stored in the first node.

These transmissions between the first and third nodes may take place via optical fibre. The third node may be located remotely from the first node. The third node may be located more than 10km from the first node. The third node may be located more than 100km from the first node. The third node may be located more than 1000km from the first node.

The method may further comprise transmitting, from the second node to the fourth node, an indication of the measured bit values of the plurality of non-orthogonal quantum states and/or an indication of the which of the second set of basis states were used to measure the plurality of non-orthogonal quantum states and/or an indication of the time each of the plurality of non-orthogonal quantum states were received at the second node from the first node. These transmissions between the second and fourth nodes may take place via an optical fibre and may be encrypted. The encryption may be symmetric key encryption and may be AES512. The information contained in these transmissions may be transmitted without being stored in the second node. The second node may be located remotely from the fourth node. The second node may be located more than 10km from the fourth node. The second node may be located more than 100km from the fourth node. The second node may be located more than 1000km from the fourth node.

In some embodiments the first node may be located aboard a satellite. The second node may be located in a ground station. Transmissions between the first and second nodes may take place via the atmosphere. In these embodiments, the fourth node may be located in a customer's premises. Transmissions between the second and fourth nodes

may take place via by optical fibre. These transmissions between the second and fourth nodes may be encrypted. The encryption may be symmetric key encryption and may be AES512. The second node may be located remotely from the fourth node. The second node may be located more than 10km from the fourth node. The second node may be located more than 100km from the fourth node. The second node may be located more than 1000km from the fourth node. The third node may be located in a different customer premises, which may be remote from the first. The transmissions from the first node to the third node may pass through a second ground station. The transmissions between the first node and the second ground station may be QKD encrypted.

In some embodiments there is a fifth node and a sixth node. In these embodiment the fifth and sixth nodes perform a key agreement stage as defined in relation to the third and fourth nodes. The fifth and six nodes thus comprise a second key agreement pair, the first key agreement pair being the third and fourth node. Further embodiments may comprise a plurality of such key agreement pairs.

The method may further comprise performing a check for whether the plurality of non-orthogonal quantum states have been intercepted by an eavesdropper. This may comprise comparing the bit values encoded onto a portion of the plurality of non-orthogonal quantum states with the measured bit values for that portion of the plurality of non-orthogonal quantum states. The check may further comprise sending, from the third node to the fourth node, an indication of the bit values that have been encoded onto the plurality of non-orthogonal quantum states. Alternatively, the check may comprise sending, from the fourth node to the third node, an indication of the bit values that were measured in relation to the plurality of non-orthogonal quantum states. The method may further comprise discontinuing the method of performing QKD if more than a threshold number of the encoded bit values for the portion of the plurality of non-orthogonal quantum states are found to be different to the measured bit values for the portion of the plurality of non-orthogonal quantum states. In alternative embodiments, the check for whether the plurality of pulses has been intercepted by an eavesdropper is instead performed between the first node and the second node.

According to a second aspect of the invention there is provided an arrangement for performing QKD in order to generate a shared secret key, the arrangement comprising:
a first node and a second node

the first node being adapted to prepare or measure a plurality of non-orthogonal quantum states using a respective one of a first set of basis states,
the second node being adapted to prepare or measure a plurality of non-orthogonal quantum states using a respective one of a second set of basis states,,
the arrangement further comprising a third node and a fourth node,
the third node being adapted to obtain an indication of the first set of basis states from the first node, and to perform a key agreement stage with the fourth node to agree the shared secret key, the key agreement stage involving the first and second sets of basis states.

The invention will now be described in detail, for illustration purposes only, and with reference to the appended drawings, in which:

Fig. 1 is a schematic view of a known QKD arrangement;

Fig. 2 is a schematic view of a further known QKD arrangement;

Fig. 3 is a schematic view of a first embodiment in accordance with the invention;

Fig. 4 is a schematic view of a second embodiment in accordance with the invention.

Figure 1 shows a known QKD arrangement 1 operating on the BB84 protocol. It comprises a transmitter 2 (referred to as Alice) and a receiver 3 (referred to as Bob). Alice 2 is connected to Bob 3 by a quantum communication channel 4 and also by a classical (i.e. non-quantum) communication channel 5. The quantum channel 4 is an optical fibre and the classical channel 5 is also an optical fibre.

The process of QKD involves two stages: the quantum transmission stage and the key agreement stage. The quantum transmission stage involves, at Alice 2, encoding a randomly-chosen bit value (1 or 0) onto an optical pulse, then preparing the pulse in one of two basis states (again, randomly chosen), and then transmitting the pulse to Bob 3 via the quantum channel 4. Alice uses a random number (RNG) generator (not shown) to obtain the random 1 or 0 value and uses a different RNG to obtain the random basis state. In the example of QKD described here, preparing the pulse in a basis state means preparing the pulse in a particular polarisation state. In the first basis state the direction

of polarisation is rectilinear. In the second basis state the direction of polarisation is diagonal, i.e. at 45° to the rectilinear direction.

Bob receives the pulse transmitted by Alice. Bob measures the pulse by randomly choosing one of the two basis states, and measuring the received pulse in that basis state and measuring the bit value. If the basis state Bob has chosen happens to be the same as the basis state Alice used, the bit value Bob measures will be the same as the bit value Alice used. If Bob's basis state is not the same as Alice's, the bit value Bob measures will be a random value. This process is repeated on each of a string of pulses. For each pulse, Alice records the time of transmission, the bit value that Alice encodes onto the pulse and the basis state Alice uses. Bob records the time of receipt of the pulse, the basis state that Bob uses and the bit value that Bob measures.

Next comes the key agreement stage. Bob sends Alice a list containing, for each pulse in the string received by Bob: (i) the time Bob received the pulse and (ii) the basis state that Bob measured the pulse in. Alice then replies to Bob, indicating which of the pulses Bob measured using the same basis state that Alice used. Each of Alice and Bob then discard their bit values which correspond to pulses for which Alice and Bob used different basis states. This leaves Alice and Bob with the same list of bit values (i.e. 1's and 0's). This list is a quantum key which Alice and Bob can use to encrypt messages for sending between them via a classical channel.

As noted above, a problem is that the pulses do not propagate over large distances in optical fibre. This means that it is not possible to establish a quantum key between remote nodes. A prior art system for addressing this is shown at Fig 2. Fig 2 shows an Alice 12, which I will refer to as first Alice 12, a Bob 23 which I will refer to as second Bob 23 and a trusted node 20. Trusted node 20 contains a Bob (first Bob 13) which is connected to first Alice 12 by both quantum and classical channels. Trusted node 20 also contains an Alice (second Alice 22) which is connected to second Bob 23 by both quantum and classical channels. First Alice 12 and second Bob 23 are connected by a classical channel 21. In use, first Alice 12 establishes a quantum key with first Bob 13 in the manner described above. First Alice and first Bob are then able to send data between each other securely over the classical channel linking them by encrypting that data using their shared quantum key. Furthermore, second Alice 22 establishes a quantum key with second Bob 13 in the manner described above. Second Alice and second Bob are

also then able to send data between each other securely over the classical channel linking them by encrypting that data using their shared quantum key. First Bob 13 and second Alice 22 then each give their respective quantum key to trusted node 20, which combines the two quantum keys into a third key by performing a simple XOR operation. First Bob 13 and second Alice 22 then encrypt the third key using their respective quantum keys and send them to first Alice 12 and second Bob 23 respectively. First Alice 12 and second Bob 23 can then communicate data securely over the classical channel linking them by encrypting the data using the third key.

The present invention addresses the problem in a different way – see Fig. 3. In the present invention, there is a conventional QKD transmitter which I will refer to as Original Alice 32. Original Alice 32 corresponds to the first node defined above. Furthermore there is a conventional QKD receiver which I will refer to as Original Bob 33. Original Bob 33 corresponds to the second node defined above. Original Alice 32 and Original Bob 33 are linked by a quantum channel 34. The distance between Original Alice 32 and Original Bob 33 is approximately 1km.

Original Alice 32 and Original Bob 33 perform the quantum transmission stage of a conventional QKD process. In other words, for each of a string of pulses, Original Alice 32 encodes a random value in a random basis state and transmits the pulse to Original Bob 33. Alice records the value, basis state and transmission time. Original Bob 33 the measures the incoming pulse in its own randomly chosen basis state. Original Bob 33 records the basis state it used, the measured value and the receipt time.

Original Alice has established a secure link to a remote node 38 via a classical channel 36. I will refer to the remote node 38 as Virtual Alice 38. This link is secured using public key cryptography. Once the quantum transmission stage has finished, Original Alice 32 encrypts its data (i.e. the encoded value, basis state used and transmission time for each pulse) using the symmetric encryption algorithm AES512. Original Alice 32 then sends this encrypted data to Virtual Alice 38 via a classical channel 36. Virtual Alice 38 corresponds to the third node defined above. Virtual Alice 38 receives and decrypts the data. The classical channel 36 is an optical fibre. The distance between Original Alice 32 and Virtual Alice 38 is approximately 50km.

Furthermore, Original Bob 33 encrypts its own data (i.e. the measured bit value, basis state used and receipt time for each pulse) using the symmetric encryption algorithm AES512 and sends it to a remote node 39 via a classical channel 37. I will refer to the remote node 39 as Virtual Bob 39. Virtual Bob 39 corresponds to the fourth node defined above. Virtual Bob 39 receives and decrypts the data. The classical channel 37 is an optical fibre. The distance between Original Bob 33 and Virtual Bob 39 is approximately 50km. The distance between Virtual Alice 38 and Virtual Bob 39 is approximately 50km.

Please note that the distances mentioned in the preceding two paragraphs are for illustration only and could be much larger, e.g. thousands of kilometres.

Virtual Alice 38 then performs the key agreement stage with Virtual Bob 39. This key agreement stage follows the conventional QKD key agreement process described above. In particular, Virtual Bob 39 sends Virtual Alice 38 a list containing, for each pulse in the string: (i) the basis state that Original Bob 33 used; and (ii) the time that Original Bob 33 received the pulse. Virtual Alice 38 then replies to Virtual Bob 39, indicating which of the pulses Original Bob 33 measured using the same basis state that Original Alice 32 used. These transmissions between Virtual Alice 38 and Virtual Bob 39 are encrypted using a secret key shared by Virtual Alice 38 and Virtual Bob 39. Each of Virtual Alice 38 and Virtual Bob 39 then discard their bit values which correspond to pulses for which Original Alice 32 and Original Bob 33 used different basis states. This leaves Virtual Alice 38 and Virtual Bob 39 with the same list of bit values. This list is a quantum key which Virtual Alice 38 and Virtual Bob 39 can use to encrypt data for sending between them via the classical channel 35.

If the link 39 between Original Alice 32 and Virtual Alice 38 were hacked, this alone would not give the hacker the quantum key that Virtual Alice 38 and Virtual Bob 39 have established. The hacker would obtain, for each pulse, the value Original Alice 32 encoded, the basis state Original Alice 32 applied and the time of transmission by Original Alice 32. However, to obtain the quantum key, the hacker would also need the basis states original Bob 33 used when receiving the pulses. To obtain that data, the hacker would additionally have to hack the link 37 between original Bob 33 and Virtual Bob 39. Obtaining the quantum key would therefore involve cracking two totally separate AES encryptions.

A further embodiment of the invention is depicted in Fig 4. Fig. 4 shows a satellite 42 which is capable of sending a signal to a base station 43. The base station 43 is connected by a classical channel 47 (which is an optical fibre) to the premises 49 of a customer who will be a party to the secure communication. The satellite 42 acts as the Alice in QKD and the base station 43 acts as Bob. The satellite 42 performs the quantum transmission stage of QKD with the base station 43. In other words, for each of a string of pulses, satellite 42 prepares a random bit value in a random basis state and transmits the pulse to base station 43. Satellite 42 records the bit value, basis state and transmission time. Base station 43 measures each incoming pulse in a randomly chosen basis state. Base station 43 records the basis state it used, the measured bit value and the receipt time.

Once the quantum transmission stage has finished, base station 43 encrypts the encoded bit value it measured, the basis state it used and receipt time for each pulse, using the symmetric encryption algorithm AES512. Base station 43 then sends this encrypted data to the customer 49 via a classical channel 47. The customer 49 then decrypts the data.

The satellite 42 encrypts the encoded bit value it measured, the basis state it used and receipt time for each pulse, using the symmetric encryption algorithm AES512. The satellite 42 then continues moving on its path around the globe and establishes a new quantum key with a second base station 50 by conventional QKD. The satellite 42 then encrypts the encrypted data with the quantum key and transmits it to the second base station 50. The second base station 50 decrypts the data, re-encrypts it with a key it shares with a second customer 52 and sends the re-encrypted data to the second customer 52 via link 51. The first customer 49 (Virtual Bob) and the second customer 52 (Virtual Alice) are therefore each on possession of the necessary data for performing the key agreement stage with each other. This is what they then do. In particular, customer 49 sends its record of encoded bit values and receipt times to customer 52 over a public key encrypted classical link (not shown). Customer 52 then sends customer 49 an indication of which pulses share common basis states. Both customers then discard the bit values corresponding to pulses for which different basis states were used, leaving the two customers with the same list of bit values (i.e. a shared secret quantum key). The two customer can then use this key to perform QKD encrypted communication with each other over the classical channel.

Claims

1. A method of performing Quantum Key Distribution for generating a shared secret key, the method comprising

at a first node, preparing or measuring a plurality of non-orthogonal quantum states, each of the plurality of non-orthogonal quantum states being prepared or measured using a respective one of a first set of basis states,

at a second node, preparing or measuring the plurality of non-orthogonal quantum states each of the plurality of non-orthogonal quantum states being prepared or measured using a respective one of a second set of basis states,

at a third node, obtaining an indication of the first set of basis states from the first node and performing a key agreement stage with a fourth node to agree the shared secret key, the key agreement stage involving the first and second sets of basis states.

2. A method according to claim 1, wherein the fourth node is different to the second node.

3. A method according to claim 1 or claim 2, the method further comprising, at the third node, obtaining the first set of basis states from the first node via an optical link.

4. A method according to any preceding claim, the method further comprising transmitting, from the first node to the third node, an indication of the bit values encoded onto the plurality of non-orthogonal quantum states.

5. A method according to any preceding claim, the method further comprising transmitting, from the first node to the third node, an indication of the time of transmission of the plurality of non-orthogonal quantum states from the first node.

6. A method according to claim 4 or claim 5, wherein the transmissions between the first and third nodes are encrypted.

7. A method according to claim 6, wherein the encryption is symmetric key encryption.

8. A method according to any preceding claim, the method further comprising performing an authentication check between the third node and the fourth node.

9. A method according to any preceding claim, wherein the third and fourth node perform encrypted communication with each other using the shared quantum key.

10. A method according to any preceding claim, the method further comprising transmitting, from the second node to the fourth node, an indication of the which of the second set of basis states were used to measure the plurality of non-orthogonal quantum states.

11. A method according to claim 11, wherein the transmitting step takes place over an optical fibre.

12. A method according to claim 10 or claim 11, the method further comprising the step of encrypting the indication of which of the second set of basis states were used to measure the plurality of non-orthogonal quantum states.

13. A method according to any preceding claim, the method further comprising transmitting, from the second node to the fourth node, an indication of the measured bit values of the plurality of non-orthogonal quantum states.

14. A method according to claim 1, wherein the fourth node is the same as the second node.

15. An arrangement for performing QKD in order to generate a shared secret key, the arrangement comprising:
a first node and a second node,
the first node being adapted to prepare or measure a plurality of non-orthogonal quantum states using a respective one of a first set of basis states,
the second node being adapted to prepare or measure a plurality of non-orthogonal quantum states using a respective one of a second set of basis states,
the arrangement further comprising a third node and a fourth node,
the third node being adapted to obtain an indication of the first set of basis states from the first node, and to perform a key agreement stage with the fourth node to agree the shared secret key, the key agreement stage involving the first and second sets of basis states.

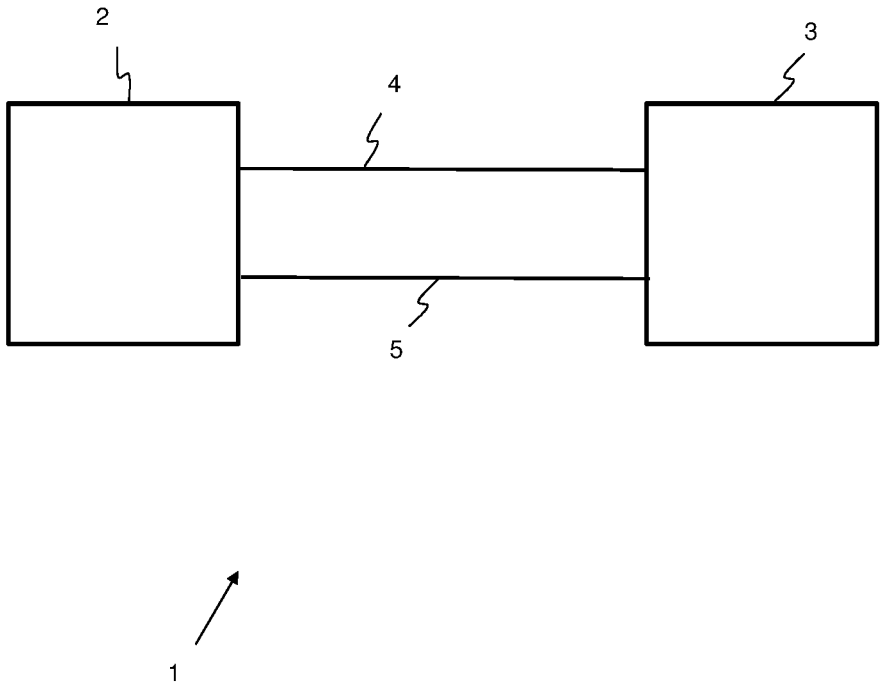

Fig. 1

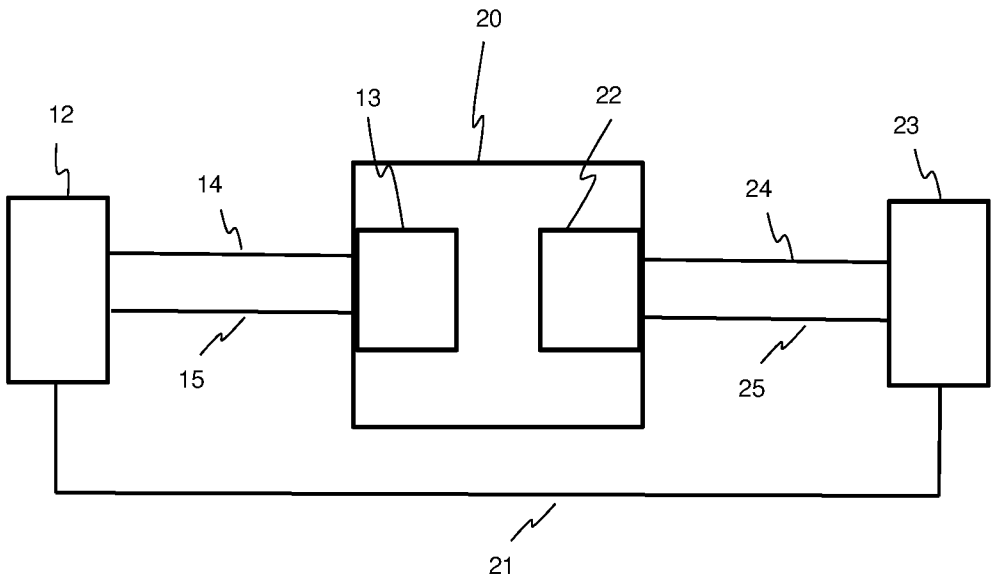

Fig. 2

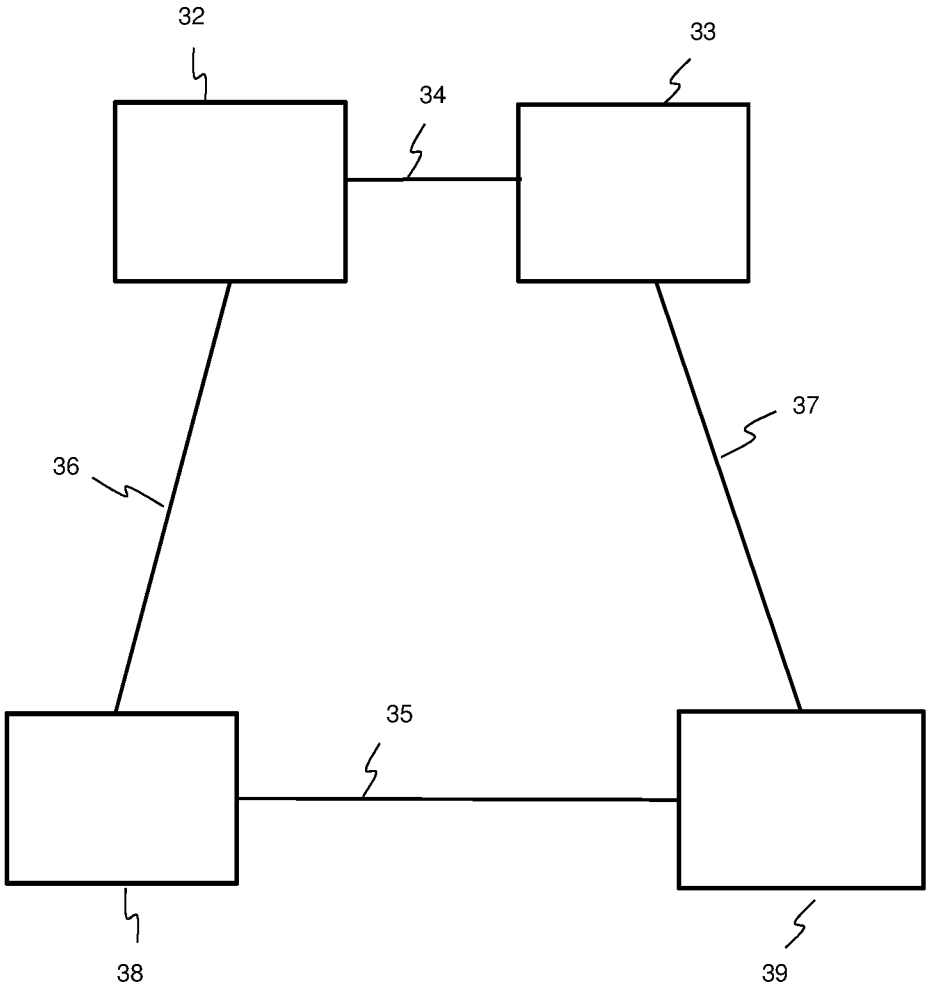

Fig. 3

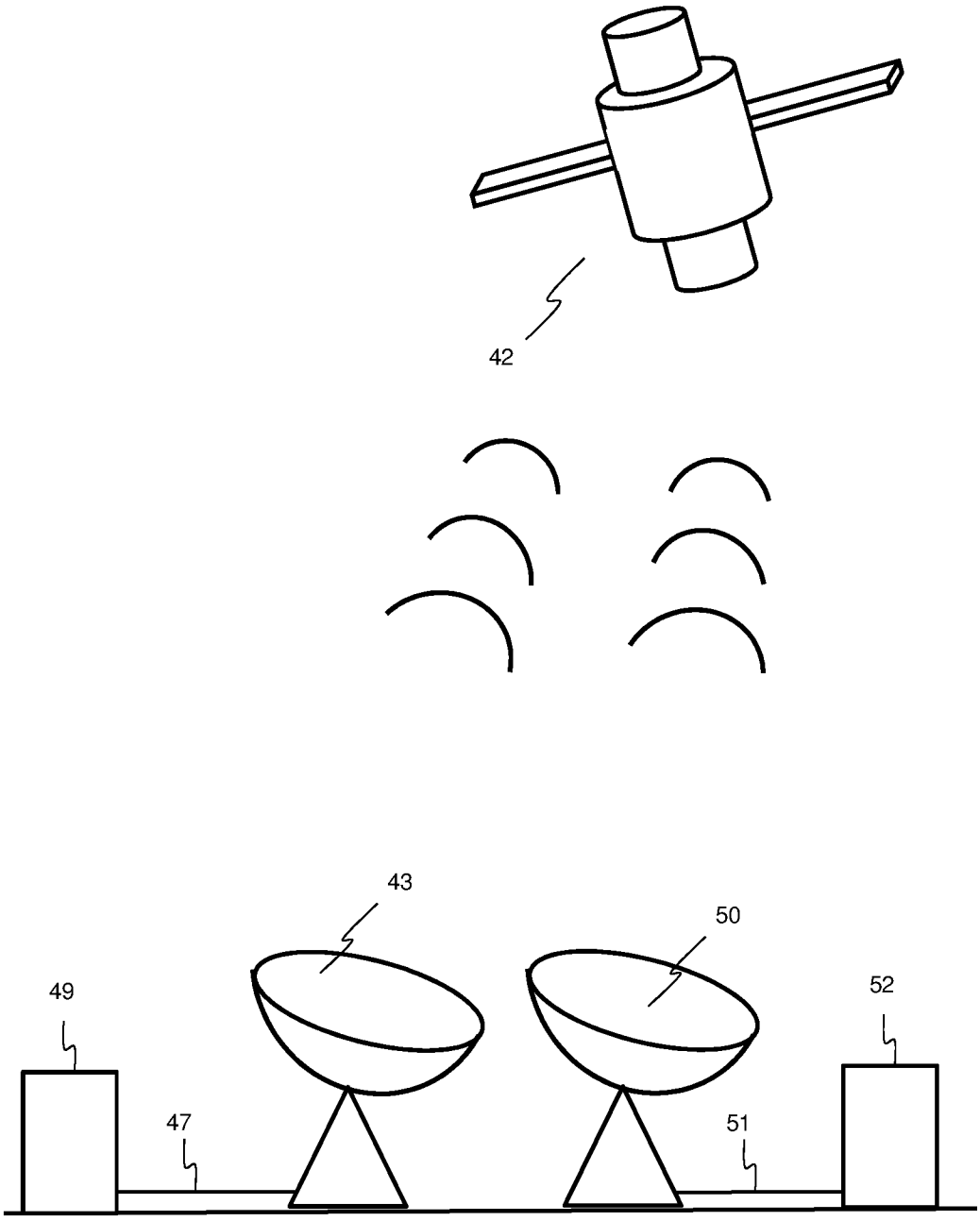

Fig. 4

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2020/071445

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

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

B. FIELDS SEARCHED

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

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	ZHI-ROU LIU ET AL: "Mediated Semi-Quantum Key Distribution Without Invoking Quantum Measurement", ANNALEN DER PHYSIK., vol. 530, no. 1700206, 29 January 2018 (2018-01-29), pages 1-9, XP055639202, DE ISSN: 0003-3804, DOI: 10.1002/andp.201700206 abstract Chapter 3: "Proposed Scheme"; pages 4-5	1-15
A	US 2007/076883 A1 (KUANG RANDY [CA]) 5 April 2007 (2007-04-05) abstract paragraph [0010]	1-15

-/--

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

[X] See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 August 2020	26/08/2020

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	Di Felice, M

1

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

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WILLIAM STACEY ET AL: "The Security of Quantum Key Distribution using a Simplified Trusted Relay", ARXIV.ORG, CORNELL UNIVERSITY LIBRARY, 201 OLIN LIBRARY CORNELL UNIVERSITY ITHACA, NY 14853, 19 August 2014 (2014-08-19), XP081391156, DOI: 10.1103/PHYSREVA.91.012338 abstract Chapter II. "STR Protocol"; pages 1-3 -----	1-15

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2020/071445

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2007076883 A1	05-04-2007	US 2007076878 A1	05-04-2007
		US 2007076883 A1	05-04-2007
		WO 2007036013 A1	05-04-2007