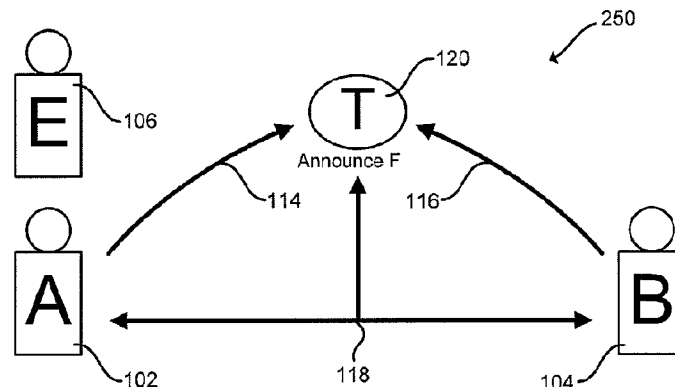




(86) **Date de dépôt PCT/PCT Filing Date:** 2012/09/12
(87) **Date publication PCT/PCT Publication Date:** 2013/03/21
(45) **Date de délivrance/Issue Date:** 2020/04/14
(85) **Entrée phase nationale/National Entry:** 2015/02/24
(86) **N° demande PCT/PCT Application No.:** CA 2012/050633
(87) **N° publication PCT/PCT Publication No.:** 2013/037062
(30) **Priorité/Priority:** 2011/09/12 (US61/573,137)

(51) **Cl.Int./Int.Cl. H04L 9/08** (2006.01),
H04L 1/00 (2006.01)
(72) **Inventeurs/Inventors:**
LUTKENHAUS, NORBERT, CA;
MA, XIONGFENG, GB
(73) **Propriétaires/Owners:**
LUTKENHAUS, NORBERT, CA;
MA, XIONGFENG, GB
(74) **Agent:** GOWLING WLG (CANADA) LLP

(54) **Titre : SYSTEME ET PROCEDE DE CRYPTOGRAPHIE QUANTIQUE**
(54) **Title: SYSTEM AND METHOD FOR QUANTUM KEY DISTRIBUTION**



(57) **Abrégé/Abstract:**

Abstract: A method and system for quantum key distribution (QKD) between a first location and a second location through an intermediate location. The system and method include executing a quantum phase between each of the first and second locations and the intermediate location to determine a first location raw data string at the first location, a first-intermediate raw data string at the intermediate location, a second location raw data string at the second location, and a second-intermediate raw data string at the intermediate location, respectively; calculating, at the intermediate location, announcement data based on a function of the first and second-intermediate raw data strings; announcing, at the intermediary location, the announcement data over a classical channel; and deriving, at each of the first and second locations, a secret key based on the available data and on communications between the first and second locations via a classical channel.

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

(19) World Intellectual Property
Organization
International Bureau



(10) International Publication Number
WO 2013/037062 A1

(43) International Publication Date
21 March 2013 (21.03.2013)

(51) International Patent Classification:

H04L 9/08 (2006.01) *H04L 1/00* (2006.01)
G06N 99/00 (2010.01)

(21) International Application Number:

PCT/CA2012/050633

(22) International Filing Date:

12 September 2012 (12.09.2012)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

61/573,137 12 September 2011 (12.09.2011) US

(72) Inventors; and

(71) **Applicants** : LÜTKENHAUS, Norbert [DE/CA]; 196
Pineland Court, Waterloo, Ontario N2T 2T1 (CA). MA,
Xiongfeng [CN/GB]; Flat 125, Summertown House, 369
Banbury Road, Oxford Oxfordshire OX2 7RD (GB).

(74) **Agents**: HENDERSON, Neil et al.; Borden Ladner Ger-
vais LLP, World Exchange Plaza, 100 Queen Street, Suite
1100, Ottawa, Ontario K1P 1J9 (CA).

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

(84) **Designated States** (*unless otherwise indicated, for every
kind of regional protection available*): ARIPO (BW, GH,
GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, 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,
ML, MR, NE, SN, TD, TG).

Published:

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

(54) **Title**: SYSTEM AND METHOD FOR QUANTUM KEY DISTRIBUTION

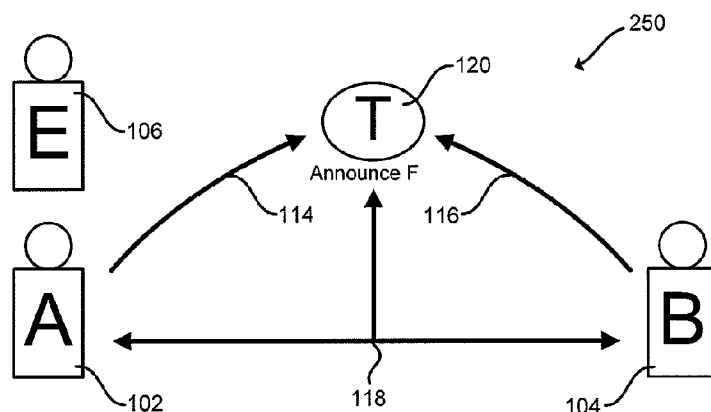


Fig. 3

(57) **Abstract**: Abstract: A method and system for quantum key distribution (QKD) between a first location and a second location through an intermediate location. The system and method include executing a quantum phase between each of the first and second locations and the intermediate location to determine a first location raw data string at the first location, a first-intermediate raw data string at the intermediate location, a second location raw data string at the second location, and a second-intermediate raw data string at the intermediate location, respectively; calculating, at the intermediate location, announcement data based on a function of the first and second-intermediate raw data strings; announcing, at the intermediary location, the announcement data over a classical channel; and deriving, at each of the first and second locations, a secret key based on the available data and on communications between the first and second locations via a classical channel.

SYSTEM AND METHOD FOR QUANTUM KEY DISTRIBUTION

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit of priority of U.S. Provisional Patent
5 Application No. 61/573,137 filed September 12, 2011.

FIELD

[0002] The present disclosure relates generally to quantum key distribution. More
particularly, the present disclosure relates to establishing a secret quantum key through
10 an intermediate node.

BACKGROUND

[0003] In cryptography, a secure communication channel can generally be
provided if two legitimate users have access to a common, secret key. One of the
15 difficulties in secure communications is to make sure that each legitimate user obtains the
secret key without interference or eavesdropping by a non-legitimate party. As such,
many secret key distribution systems have been developed over the years. Most recently,
cryptographers have begun using quantum techniques to securely distribute/create secret
keys (called "quantum key distribution" (QKD)). For example, QKD protocols include the
20 6-state protocol or the BB84 protocol.

[0004] QKD protocols generally comprise two phases: a quantum phase and a
classical phase. In the quantum phase, quantum states (for example, qubits) are
distributed via a quantum channel. The nature of the quantum channel is such that it is
possible to detect if the signal has been tampered with and this allows for stronger
25 security in the secret keys. Upon receipt of the quantum signal, the legitimate users
measure the quantum states to obtain classical information about the quantum states. In
the classical phase, classical information is exchanged using a specified communication
protocol over the classical channel to determine the secret key.

[0005] One of the difficulties of quantum key distribution protocols is that quantum
30 channels cannot be established in certain circumstances. For example, quantum states
are typically communicated using photons, for example, via optical fiber or through free
space (line of sight). In either case, transmitting is limited by signal loss over distance
and, particularly in the free space case, may also be limited by environmental factors. In

optical fibers, the transmittance of the quantum signal is generally limited by loss which grows exponentially as the distance increases based on, for example, the loss coefficients of the optical fiber. It is anticipated that maximum distances will be a few hundred kilometers.

5 **[0006]** In order to overcome this problem, conventional systems make use of intermediate nodes between the two legitimate users. These intermediate nodes may be part of a trusted repeater network or a proposed quantum repeater network.

10 **[0007]** In a trusted repeater network, one or more trusted intermediate nodes are provided between the legitimate end users and point-to-point communications are used among the legitimate users and the trusted nodes. In the point-to-point communications, the QKD protocol is used to establish a secret key between the first legitimate user and the trusted node and then, in the case of only one node, between the trusted node and the second legitimate user. If there are multiple nodes, a secret key would be established between each intermediate node as well.

15 **[0008]** In a proposed quantum repeater network, the legitimate users each create a maximal entangled state and each keeps one entangled state subsystem and sends the other entangled state subsystem to an intermediate node over a quantum channel. The intermediate node saves these quantum states into quantum memory and performs a joint Bell measurement on the arriving signals and announces a Bell measurement result via the classical channel. This produces a quantum correlation that is shared between the legitimate users (that is, an entangled state). The entangled state is then used to complete the QKD protocol and establish a secret key, without further involvement from the intermediate node.

20 **[0009]** While trusted repeater network systems can be effective, it is often necessary to have a large number of complex intermediate nodes between legitimate users or among legitimate users in a network. This can lead to additional costs and complexity. Further, quantum repeater networks have yet to be practically implemented. As such there is a need for improved systems and methods of quantum key distribution.

30 **SUMMARY**

[0010] It is an object of the present disclosure to overcome or mitigate at least one disadvantage of previous systems and methods.

[0011] In a first aspect, the present disclosure provides a method for quantum key distribution (QKD) between a first location (A) and a second location (B) through an

intermediate location (T). The method for QKD includes executing a quantum phase between the first location (A) and the intermediate location (T) to determine a first location raw data string (R_A) at the first location and a first-intermediate raw data string (R_{AT}) at the intermediate location (T); executing a quantum phase between the second location (B) and the intermediate location (T) to determine a second location raw data string (R_B) at the second location (B) and a second-intermediate raw data string (R_{TB}) at the intermediate location (T); calculating, at the intermediate location (T), announcement data based on a function (F) of the first-intermediate raw data string (R_{AT}) and the second-intermediate raw data string (R_{TB}); announcing, at the intermediary location (T), the announcement data over a classical channel; and deriving, at each of the first and second locations (A, B), a secret key (K_{AB}) based on the first location raw data string (R_A), the second location raw data string (R_B), and the announcement data and on communications between the first and second locations (A, B) via the classical channel.

[0012] This method is intended to provide a reduced complexity at the intermediate location/node in that the physical requirements and processing capacity required can be reduced compared to conventional systems as discussed in further detail herein.

[0013] In a further aspect, the intermediate location may be a plurality of intermediate locations. In this case, the plurality of intermediate locations may include either a quantum detector and a quantum emitter such that each intermediate location may include only one type of quantum hardware while passing signals accordingly.

[0014] In one particular case, deriving a secret key (K_{AB}) may include performing error correction between the first location (A) and the second location (B) over a classical channel. In another case, deriving a secret key (K_{AB}) may include performing privacy amplification between the first location (A) and the second location (B) over a classical channel.

[0015] In a further aspect, the present disclosure provides a method for QKD at an intermediate location (T). The method for QKD includes executing a quantum phase with a first location (A) over a quantum channel to obtain a first raw data string (R_{AT}); executing a quantum phase with a second location (B) over a quantum channel to obtain a second raw data string (R_{TB}), calculating announcement data based on a function (F) of the first raw data string (R_{AT}) and the second raw data string (R_{TB}); and announcing the announcement data over a classical channel.

[0016] In another particular case, executing the quantum phase with a first location (A) may include receiving a first quantum signal from the first location (A) over a quantum channel and measuring the first quantum signal to obtain the first raw data string (R_{AT}). Similarly, executing the quantum phase with a second location (B) may include
5 receiving a second quantum signal from the second location (B) over a quantum channel and measuring the second quantum signal to obtain the second raw data string (R_{TB}).

[0017] In a further particular case, the function (F) may be a parity function and the announcement data may include parity data and measurement bases.

[0018] In a further particular case, the announcing of the announcement data may
10 include announcing error correction information.

[0019] In other particular cases, the execution of the quantum phase may include determining an error estimate.

[0020] According to another aspect herein, there is provided a system for quantum key distribution (QKD) at an intermediate location (T), the system including: a
15 quantum phase system configured to execute a quantum phase with a first location (A) over a quantum channel to obtain a first raw data string (R_{AT}) and execute a quantum phase with a second location (B) over a quantum channel to obtain a second raw data string (R_{TB}); a processor for calculating announcement data based on a function (F) of the first raw data string (R_{AT}) and the second raw data string (R_{TB}); and a classical system
20 configured to announce the announcement data over a classical channel.

[0021] In a particular case, the function (F) may be a parity function and the announcement data comprises parity data and measurement bases.

[0022] Other aspects and features of the present disclosure will become apparent to those ordinarily skilled in the art upon review of the following description of specific
25 embodiments in conjunction with the accompanying figures.

BRIEF DESCRIPTION OF THE DRAWINGS

[0023] Embodiments of the present disclosure will now be described, by way of example only, with reference to the attached Figures.

30 [0024] Fig. 1 is an example system for quantum key distribution;

[0025] Fig. 2 is an example system for quantum key distribution with an intermediate node;

[0026] Fig. 3 is an example system for quantum key distribution with an intermediate node according to an embodiment herein;

- [0027] Fig. 4 is a schematic diagram of an intermediate node in accordance with an embodiment herein;
- [0028] Fig. 5 is a flow chart of a method for quantum key distribution in accordance with an embodiment herein;
- 5 [0029] Fig. 6 is a flow chart of a method for quantum key distribution in accordance with another embodiment;
- [0030] Fig. 7 a graph of a key rate as a function of an error rate, in accordance with an embodiment; and
- [0031] Fig. 8 a graph of a key rate as a function of a total number of exchanged
10 signals, in accordance with an embodiment.

DETAILED DESCRIPTION

[0032] Generally, the present disclosure provides improved methods and systems for quantum key distribution that simplify the distribution protocol and result in lower cost
15 intermediate nodes (sometimes referred to as “repeaters”).

[0033] In order to better understand the nature of the systems and methods herein, it is useful to consider a conventional system and method for Quantum Key Distribution (QKD) in further detail. Figure 1 illustrates a conventional system 100 for providing a secret key using a QKD protocol. The QKD protocol aims to establish a key
20 between two legitimate and remote users, first user A (Alice) 102 and second user B (Bob) 104, in the presence of an eavesdropper (Eve) 106; that is, a non-legitimate user that may intentionally interfere with or intercept information related to the secret key. The secret key is intended to be secret, secure, and random.

[0034] QKD protocols generally comprise two phases: a quantum phase and a
25 classical phase.

[0035] In the quantum phase, quantum states (for example, qubits) are distributed via a quantum signal between Alice 102 and Bob 104 over a quantum channel 110. The quantum channel 110 may be for example, a fibre optic or line-of-sight channel over which photons can be transmitted. In some cases, the eavesdropper (Eve) 106 may
30 actually be the controller or provider of the quantum channel 110.

[0036] In the quantum phase, the quantum signals may be intercepted or interfered with by Eve 106. However, Alice 102 and/or Bob 104 may discover that Eve 106 has obtained information about the quantum signal based on a fundamental aspect of quantum mechanics stating that the process of measuring a quantum system disturbs

the system. As such, in order for Eve 106 to obtain information about a quantum signal, Eve 106 will affect the quantum signal such that the signal will be disturbed and Eve 106 can be discovered. In an ideal system, Alice 102 and Bob 104 could discover the presence of Eve 106 from the classical measurement data. However, the quantum
5 channel 110 typically includes noise or imperfections in the transmission line. There may also be noise or imperfections in the users' detectors. As such, it may not be possible to distinguish between these imperfections and the disturbances caused by the presence of Eve 106. In order to guarantee security all of these errors may be assumed to be caused by eavesdropping.

10 **[0037]** Upon receipt of the quantum signal, Alice 102 and Bob 104 measure the quantum states to obtain classical information (classical measurement data) about the quantum states.

[0038] In the classical phase, measurement information related to the measurement of the classical information are exchanged between Alice 102 and Bob 104
15 over an authenticated classical channel 108 to determine the secret key from the classical information. The classical channel 108 may be one or more of various communication networks, for example, radio, telephone or any of various computer networks, including the Internet. The classical channel 108 may be public, so that it can be accessed by Eve 106. However, the classical channel 108 is assumed to be
20 authenticated such that it cannot be interfered with by Eve 106.

[0039] After the exchange of measurement information related to the quantum signal, Alice 102 and Bob 104 then perform Parameter Estimation (PE), Error Correction (EC), and Privacy Amplification (PA) to convert the classical measurement data into a secure key.

25 **[0040]** Parameter Estimation is used to extract an initial key from the classical measurement data. The parameter estimation can, for example, be based on a set of density matrices compatible with the observed joint probability distribution of measurement outcomes, which are initially determined using a proof technique for the QKD protocol.

30 **[0041]** Error Correction is carried out between Alice 102 and Bob 104's initial keys in order to reduce errors introduced during the communication. Alice 102 and Bob 104 exchange information over the classic channel 108 so that Bob 104 can correct or remove errors in his version of the initial/raw key, ending up with Alice's initial/raw key. As the classic channel 108 is generally public (in particular, accessible to Eve 106),

minimal information about the initial key is sent. The error correction may be conducted using low density parity check codes (LDPC) involving one-way error correction, or a cascade protocol, which uses recursive rounds of sending data to produce a generally identical key with a high probability.

- 5 **[0042]** Privacy Amplification is a method for reducing and effectively eliminating the risk that any information has been obtained by Eve 106. Privacy Amplification uses Alice 102 and Bob's 104 error corrected key to produce a new shorter key, such that Eve 106 may only have negligible information about the new key. In one example, Alice 102 chooses at random an element of a two-universal hashing function from a predefined set,
10 and communicates this choice to Bob 104. Alice 102 and Bob 104 independently apply this hash function to their corrected raw key and obtain the final secret key.

- [0043]** As noted above, establishing a secret key over a distance can be limited by signal loss over distance and other factors. As such an intermediate/repeater node can be provided between Alice 102 and Bob 104. Also as noted above, the intermediate
15 node may be a trusted repeater node or a quantum repeater node.

- [0044]** Figure 2 illustrates an exemplary system 200 for providing a common secret key using a QKD protocol. The system 200 comprises two legitimate and remote users as in Figure 1, user A (Alice) 102 and user B (Bob) 104, in the presence of an eavesdropper (Eve) 106. In the system 200 there is an intermediary node (Tom) 112.
20 The system 200 comprises a quantum channel 114 between Alice 102 and Tom 112 and a quantum channel 116 between Bob 104 and Tom 112. The system 200 comprises a classic channel 118 among Alice 102, Bob 104, and Tom 112.

- [0045]** In a conventional trusted repeater network (TRN) system, the intermediary node 112 is a trusted repeater node. Tom 112 performs a QKD protocol with Alice 102
25 via quantum channel 114 to establish a secret key K_{AT} . Tom 112 performs a QKD protocol with Bob 104 via quantum channel 116 to establish a secret key K_{TB} . In the traditional TRN system, the quantum channels 114, 116 are direct but, other characteristics, such as being authenticated, do not need to be specified.

- [0046]** Tom 112 now has the two independent secret keys K_{AT} and K_{TB} . Tom 112
30 then performs the parameter estimation and computes a parity function P_K (for example, the bitwise parity of both keys) from K_{AT} and K_{TB} , where $P_K = K_{AT} \text{ XOR } K_{TB}$. Tom 112 announces P_K publicly via a classical channel 118, such that Alice 102 and Bob 104 can determine a common key. In particular, Bob 104 may calculate the common secret key using: $K_{TB} \text{ XOR } P_K = K_{TB} \text{ XOR } K_{AT} \text{ XOR } K_{TB} = K_{TA}$.

[0047] The public announcement by Tom 112 of P_K does not contain any information about the resulting common key, thus the key is secure. However, this conventional TRN system is limited as Tom 112 must be involved twice in all steps of the classical phase of the QKD protocol which requires significant computation and communication resources. Further, Tom 112 must be a trusted intermediate node as, at the end of the QKD protocol, Tom 112 has full access to the final secret key.

[0048] In a conventional quantum repeater network (QRN) system, the intermediary node 112 is a quantum repeater node. Alice 102 and Bob 104 each determine a maximal entangled state. Alice 102 keeps one entangled state subsystem and sends the other entangled state subsystem Q_{AS} to Tom 112 via a quantum channel 114. Bob 104 keeps one entangled state subsystem and sends the other entangled state subsystem Q_{SB} to Tom 112 via a quantum channel 116. Tom 112 performs a joint Bell measurement on the arriving signals Q_{AS} , Q_{SB} and announces a Bell measurement result (P_{Bell}) via the public channel 118. This announcement allows for determination of a quantum correlation that is shared between Alice's qubits and Bob's qubits. The quantum correlation establishes an entangled state between Alice 102 and Bob 104. Alice 102 and Bob 104 use the entangled state to complete the QKD protocol and establish a secret key, without further involvement from Tom 112.

[0049] In the proposed QRN system, Tom 112 has no information about the final secret key and does not need to be trusted. Alice 102 and Bob 104 can verify from their data that Tom 112 followed the protocol. Tom 112 is not involved in the parameter estimation and does not need to have the computational resources to extract a key from the data. However, the QRN system does require that Tom 112 have a quantum memory and perform a joint measurement on the quantum signals received from Alice 102 and Bob 104. As such, it can be difficult to equip Tom 112 to handle the storage and measurements needed.

[0050] Accordingly, it was determined that there is a need to provide a protocol intended to maintain security but decrease the computational or physical (e.g. quantum memories) requirements of the intermediate node 112. Such a reduction is intended to reduce cost and complexity of intermediate nodes. Such an improvement is expected to have particular impact when a satellite is used as an intermediate node because satellites tend to have limited communication and computational capacity as well as strict equipment/physical standards due to power constraints and the harsh environment of space.

[0051] Figure 3 illustrates an embodiment of an improved system 250 for QKD. The system 250 is similar to that illustrated in Figure 2 and similar reference numbers will be used for similar elements. In the improved system, the intermediate node Tom 120 is modified in order to process an improved QKD protocol. In particular, the system 250 is less complex as described further below.

[0052] Figure 4 illustrates an intermediate node 300 for performing a QKD protocol in accordance with an embodiment herein. The intermediate node 300, may be, for example, Tom 120 of Figure 3. The node 300 includes a classical system 302 comprising a classical receiver and a classical sender for receiving and sending a classical signal over a classical channel 118.

[0053] The node 300 also includes a quantum sub-system 304, which may be either a quantum detector for receiving a quantum signal or a quantum emitter for sending a quantum signal. The quantum sub-system 304 interfaces with the quantum channels 114, 116 of Figure 3. It will be understood that a node 300 may be configured as either a quantum receiver or emitter depending on its location in the network. In a multiple node example, the intermediate nodes may alternate between emitter and receiver in order to provide less complex intermediate nodes.

[0054] The node 300 also comprises a processor 306 for processing sending data, measurement data, and classical data related to the signals. The device 300 may also comprise a memory 308 for storing classical data and related information.

[0055] Figure 5 illustrates a method 400 for performing quantum key distribution in accordance with an embodiment herein and making use of the system 250 of Figure 3. Initially, Alice 102 (at 402) and Bob 104 (at 404) each perform the quantum phase with Tom 120 via the quantum channels 114, 116. The quantum phase does not need to be conducted simultaneously or involve the same quantum protocol. For example, two independent quantum protocols (at 406 and 408, respectively) can be used. In this case, Eve 106 is assumed to have access to the quantum channels 114, 116.

[0056] Tom 120 receives and measures the quantum signals and obtains classical information about the quantum signals, including classical measurement data strings and information related to the classical measurement data strings, for example, the basis choices used by Tom 120 in making the measurements. Tom 120 then prepares a function (F) of the classical information to determine announcement data. At 410, Tom 120 then announces the announcement data on classical channel 118. Alice 102 (at 412) and Bob 104 (at 414) use the announcement data together with their own

data to determine correlations and establish a secret key between themselves using error correction and privacy amplification.

[0057] The proposed protocol is intended to have the advantage that Tom 120 does not need to have the computational resources to extract a secret key from the measurement data as would be required in a conventional TRN system. Instead Tom 120 performs a simple state transfer and measurement and reports on the results. As such, there is a reduced need for computational resources and, further, no quantum memory is required and joint measurements are also not required as would be the case in conventional QRN networks.

[0058] Figure 6 illustrates another embodiment of a method 500 for quantum key distribution (QKD) showing a particular implementation of the method of Figure 5. The method 500 for QKD may be performed by Alice 102, Bob 104, and Tom 312 of Figure 3, for example.

[0059] At 502, Alice 102 sends a quantum signal to Tom 120. At 504, Tom 120 receives the quantum signal from Alice. As noted above, it will be understood that the quantum phase (i.e. sending of a quantum signal) is symmetric in the sense that either of Alice or Tom may be the sender and the other the receiver. At 508, Alice announces the bases of the measurements performed in the protocol via the classical channel. At 510, optionally Alice performs an error estimation. At 512, Alice determines a raw data string R_A .

[0060] At 514, Tom measures the quantum phase of the signal. At 516, Tom announces the bases of the measurements performed in the protocol. At 518, optionally Tom performs an error estimation. During error estimation between Alice and Tom, in its simplest form, one party announces a random subset of its data such that the other party can look up its corresponding subset of data and thus have an estimation of the errors. The choice of who announces the random subset of data and who compares the data is independent of the role in preparation and measurement of the quantum states. At 520, Tom determines a raw data string R_{AT} .

[0061] At 522, Bob sends a quantum signal to Tom. At 524, Tom receives the quantum signal from Bob. At 528, Bob announces the bases performed in the protocol. At 530, optionally Bob performs an error estimation. At 532, Bob determines a raw data string R_B .

[0062] At 534, Tom measures the quantum signal from/to Bob. At 536, Tom announces all bases of the measurements performed in the protocol. At 538, optionally

Tom performs an error estimation, similar to that discussed above between Alice and Tom. At 540, Tom determines a raw data string R_{TB} .

[0063] It will be understood that in each of the above, the elements disclosed are performed in a co-ordinated fashion among Alice, Bob and Tom.

- 5 **[0064]** At 542, Tom determines an announcement function F that acts on the raw data strings R_{AT} and R_{TB} to provide an announcement result/data. For example, Function F is selected to create a partition of a subset of the raw data strings R_{AT} and R_{TB} by creating sets of data with the same function value.

- 10 **[0065]** In a particular case, the function F may include the measurement basis and also a parity function of the measurement results and the announcement result is the parity bits P_R calculated from the measurement results as $P_R = R_{AT} \text{ XOR } R_{TB}$. It will be understood that the function F does not necessarily include the measurement bases.

[0066] At 544, Tom announces the announcement result via the classical channel.

- 15 **[0067]** In the case where the announcement by Tom 312 is the parity bits P_R , at 546, Bob may calculate a modified string $\sim R_B$, from $\sim R_B = R_B \text{ XOR } P_R$.

- [0068]** At 548 and 550 Alice and Bob derive a secret key K_{AB} from Alice's raw data string R_A , Bob's raw data string R_B , and the announcement result via the public/classical channel. Where the announcement result is the parity bits P_R , Alice (at 20 548) and Bob (at 550) derive a secret key K_{AB} from Alice's raw data strings R_A and Bob's modified string $\sim R_B$ via a public discussion channel using parameter estimation techniques and also using sifting of data based on the various announcements of measurement bases. In one simple protocol, Alice and Bob will discard all events where their respective basis choice disagrees with the basis choice at the intermediate node (Tom). Alice and Bob also perform error correction and privacy amplification in accordance with conventional point-to-point QKD protocols. During the classical communication, Alice and Bob decide whether to abort the QKD protocol, for example, based on too many errors, too small a key, or the like. If they do not abort, Alice and Bob accept the output of the protocol as a secret key.

- 30 **[0069]** During this classical communication 548, 550 a substantial amount of classical communication is exchanged to perform the error correction and the privacy amplification. Privacy amplification and error correction also require a substantial amount of computation to execute. Accordingly, there are certain advantages to having Alice and Bob perform error correction and privacy amplification without the involvement of Tom.

- [0070]** The error estimation at 508, 516, 528, and 536 is intended to provide Alice and Bob with a description of all multi-partite quantum states shared between Alice, Bob, and Tom, from which the extractable secret key rate for Alice and Bob can be calculated for given announcements by Tom. The error estimation calculation process includes
- 5 Tom's public announcements on a random subset of signals, for example by external random choices of signals or by random selections by Tom. The error estimation process is intended to determine how much secret key can be extracted by Alice and Bob at 548, 550, for example, to provide an estimate of the amount of privacy amplification that Alice 102 and Bob 104 perform.
- 10 **[0071]** In keeping with standard QKD protocols, the systems and methods herein assume the authentication of classical channels to guarantee security of the resulting secret keys.
- [0072]** It will be understood that the method 500 may also be adapted to be performed on larger trusted repeater networks where multiple trusted nodes may be
- 15 configured in a similar manner and make announcements in a similar way as the intermediate node Tom 120.
- [0073]** In executing the method 500, Tom does not need to have the full computational resources that would ordinarily be necessary to perform full parameter estimation and error correction and privacy amplification in the case of conventional
- 20 trusted repeater networks. Further, the amount of traffic on the public channels involving Tom is reduced. Still further, Tom does not directly have a clear copy of the final key K_{AB} . Although Tom still needs to be trusted to some extent since Tom can compute the final key from its own knowledge and the information being exchanged between Alice and Bob, the level of trust needed is somewhat diminished. In some cases, Alice and Bob
- 25 may use further encryption (for example, computationally secure encryption) of their public discussion to increase the difficulty for Tom of obtaining a full copy of the key. This may be particularly advantageous in larger multi-node networks.
- [0074]** Other intermediate protocols that involve the use of less than full key development may be understood by one of skill in the art after understanding the
- 30 concepts disclosed herein. For example, in another embodiment, the method 400 or 500 may further include Tom also announcing partial or full error correction information to Alice and Bob. This option may be used depending on the available processing power and bandwidth of the system.

[0075] In any cryptographic protocol, it is important to consider the security proof for the protocol to determine that the key can be safely distributed. The following description is intended to represent an exemplary security proof framework but it will be understood that various security proofs may be available within the framework.

- 5 **[0076]** In the security proof framework, each of data X, Y are sent by Alice 102 and Bob 104 and Tom 120 measures/detects the measured outcomes X', Y'. Tom then combines the outcomes using an announcement function F:

$$F: X' \times Y' \rightarrow \Gamma \quad \gamma \in \Gamma$$

$$\Upsilon^\gamma = \{(x', y') | F(x', y') = \gamma\}$$

to obtain a classical announcement result γ .

- 10 **[0077]** Tom's announcement strategy is used to produce a classical correlation between Alice's and Bob's data. For any announcement, Alice and Bob are classically correlated within the subset and Eve has some partial information. Using this announcement strategy, the correlations of the legitimate users, Alice and Bob, are intended to suffice to do error correction and privacy amplification independently of Tom.

- 15 **[0078]** Tom 120 then announces the announcement result/data γ publicly. Based on the announcement result, Alice 102 and Bob 104 repartition their data and extract a key rate condition based on the classical announced result:

$$\rho_{ABE} = \sum_{\gamma} P(\gamma) \rho_{ABE}^{\gamma} \otimes |\gamma\rangle\langle\gamma|_{ABE}^{\otimes 3} \quad \rho_{ABE}^{\gamma} = \sum_{x', y' \in \Upsilon^\gamma} p_{x', y'} (M_{x'}^{\gamma} \otimes M_{y'}^{\gamma}) \Psi \otimes \Psi \otimes \Psi$$

20

The final key is extracted from:

$$R = \sum_{\gamma} P(\gamma) R^{\gamma}$$

$$R^{\gamma} = I(A: B | \gamma) - \chi(A: E | \gamma)$$

- It will be understood that, upon reviewing the present document, various announcement functions (F) may be available. Further, the key rate can be optimized over all possible announcement functions F.
- 25

[0079] In one particular example of key rates for single links involving infinite key limit, asymmetric basis choice, and key from z-basis, when using 6-state protocol, key

rates may be determined from: $R_{x, 6state}^D[e_x, e_z] = I[e_z] - \chi[e_x, e_z]$, $I[e_z] = 1 - h[e_z]$ is

the amount the mutual information between Alice 102 and Tom 112 (for only one channel) in which $h[x]$ is the binary entropy. The Holevo quantity in this case is

$$\chi[e_x, e_z] = e_z + (1 - e_z)h\left[\frac{1 - (e_x + e_z/2)}{1 - e_z}\right]$$

[0080] When using BB84 protocol, key rates may be determined

5 from $R_{x, BB84}^D[e_x, e_z] = 1 - h[e_z] - h[e_x]$.

[0081] As one particular example, it is possible to consider the case of a parity bit announcement. Considering the infinite key limit case, the parity bits P_R , may be

determined from $F(x', y') = x' \oplus y'$.

[0082] In the 6-state protocol, if Tom 112 (called "S" in this example – Satellite) is

10 assumed to contribute to parameter estimation, the total state $\rho_{AS_AS_BB}$ and consequently

the pure state $|\Psi\rangle_{AS_AS_BB}$ can be constructed from each party's observables. The resulting key rate follows closely that of a direct link but with particular effective rates in

the different parts: $R_{x, 6\text{-state}}^P[e_x, e_z] = I[E_z] - \chi[E_x, \overline{E_z}]$.

[0083] In the mutual information part of the equation, the error rate is replaced by:

15 $e_z \rightarrow E_z = e_z^a(1 - e_z^b) + e_z^b(1 - e_z^a)$. The Holevo quantity changes are:

$$\begin{cases} e_x \rightarrow E_x = e_x^a(1 - e_x^b) + e_x^b(1 - e_x^a) \\ e_z \rightarrow \overline{E_z} = e_z^a + e_z^b - e_z^b e_z^a \end{cases}$$

[0084] In the BB84 protocol, similar to computation of a secret key for the direct link, an optimization over some constraints is made due to incompleteness of positive-operator valued measure (POVM) elements. The final expression is:

20 $R_{x, BB84}^P[e_x, e_z] = 1 - h[E_z] - h[E_x]$.

[0085] Based on initial security proof calculations, embodiments of the QKD protocol described herein are secure against collective attack, which can be extended to the more general case of coherent attacks, by established techniques, for example by using a post selection technique. Also, established techniques will allow for detailed

25 analysis of the effects of finite amounts of signal exchanges.

[0086] Figure 7 illustrates anticipated key rates as a function of single link error rate Q for both 6-state and BB84 protocols. Curves 802, 804 indicate 6-state protocol in

parity announcement format (i.e. according to embodiments of the systems and methods herein with double link communication) and direct, single link format, respectively. Curves 808, 810 refer to the BB84 protocol in parity announcement format (i.e. according to embodiments of the systems and methods herein) and direct link format, respectively.

- 5 Lastly, curve 806, which closely follows curve 802, refers to a particular case in which embodiments of the systems and methods herein make use of an announcement by the intermediate node involving both parity and phase values in 6-state protocol. In the case of BB84 protocol, a similar calculation can be done.

[0087] In a standard security proof of QKD, the key rate is derived under some
10 assumptions that might not hold in practical QKD. For example, the assumption that legitimate users (Alice, Bob, Tom) can send infinite amount of signal can not hold in practice. In a practical situation, there is a limit on the number of signals transmitted.

[0088] Figure 8 illustrates a key rate 902 as a function of total number of
exchanged signals N 904. The solid curves 906, 910, 916 refer to the BB84 protocol and
15 the dashed curves 908, 912, 914 indicate 6-state protocol. The values of the error rate are $Q = 0.5\%$ (curves 906, 908), 2% (curves 910, 912), and 5% (curves 914, 916).

[0089] It will be understood by one of skill in the art, after understanding the
concepts herein, that the systems and methods outlined herein can be extended to other
signal sources, such as weak laser pulses and the like, and can also be operated via
20 lossy quantum channels. The protocol described can be used or adapted according to the signal source and channel characteristics. For example, in one simple case, a source such as a weak laser pulse could be used with the same unaltered protocol described above. In another case, the protocol described above may be combined with the established method of decoy states to estimate which fraction of events originate from the
25 ideal qubit implementation, and what the parameter estimation on those signals would yield. From that a new key rate can be calculated and extracted via error correction and privacy amplification.

[0090] In the preceding description, for purposes of explanation, numerous details
are set forth in order to provide a thorough understanding of the embodiments. However,
30 it will be apparent to one skilled in the art that these specific details may not be required. In other instances, well-known structures are shown in block diagram form in order not to obscure the understanding. For example, specific details are not provided as to whether the embodiments described herein are implemented as a software routine, hardware circuit, firmware, or a combination thereof.

[0091] Embodiments of the disclosure can be represented as a computer program product stored in a machine-readable medium (also referred to as a computer-readable medium, a processor-readable medium, or a computer usable medium having a computer-readable program code embodied therein). The machine-readable medium can be any suitable tangible, non-transitory medium, including magnetic, optical, or electrical storage medium including a diskette, compact disk read only memory (CD-ROM), memory device (volatile or non-volatile), or similar storage mechanism. The machine-readable medium can contain various sets of instructions, code sequences, configuration information, or other data, which, when executed, cause a processor to perform steps in a method according to an embodiment of the disclosure. Those of ordinary skill in the art will appreciate that other instructions and operations necessary to implement the described implementations can also be stored on the machine-readable medium. The instructions stored on the machine-readable medium can be executed by a processor or other suitable processing device, and can interface with circuitry to perform the described tasks.

[0092] The above-described embodiments are intended to be examples only. Alterations, modifications and variations can be effected to the particular embodiments by those of skill in the art without departing from the scope, which is defined solely by the claims appended hereto.

20

WHAT IS CLAIMED IS:

1. A method for quantum key distribution (QKD) between a first location (A) and a
second location (B) through an intermediate location (T), the method comprising:
5 executing a quantum phase between the first location (A) and the intermediate
 location (T) to determine a first location raw data string (R_A) at the first location
 and a first-intermediate raw data string (R_{AT}) at the intermediate location (T);
 executing a quantum phase between the second location (B) and the intermediate
 location (T) to determine a second location raw data string (R_B) at the second
10 location (B) and a second-intermediate raw data string (R_{TB}) at the intermediate
 location (T);
 calculating, at the intermediate location (T), announcement data based on a
 function (F) of the first-intermediate raw data string (R_{AT}) and the second-
 intermediate raw data string (R_{TB});
15 announcing, at the intermediary location (T), the announcement data over a
 classical channel; and
 deriving, at each of the first and second locations (A, B), a secret key (K_{AB}) based
 on the first location raw data string (R_A), the second location raw data string (R_B),
 and the announcement data and on communications between the first and second
20 locations (A, B) via the classical channel.
2. The method of claim 1, wherein the function (F) is a parity function and the
announcement data comprises parity data and measurement bases.
- 25 3. The method of claim 2, wherein the announcing announcement data further
comprises announcing error correction information.
4. The method of claim 1, further comprising determining an error estimate during
the execution of the quantum phase.
- 30 5. The method of claim 1, wherein the intermediate location is a plurality of
intermediate locations.

6. The method of claim 5, wherein the plurality of intermediate locations each comprise one of a quantum detector and a quantum emitter.
7. The method of claim 1, wherein the deriving a secret key (K_{AB}) further comprises
5 performing error correction between the first location (A) and the second location (B) over a classical channel.
8. The method of claim 1, wherein the deriving a secret key (K_{AB}) further comprises performing privacy amplification between the first location (A) and the second location (B)
10 over a classical channel.
9. A method for quantum key distribution (QKD) at an intermediate location (T), the method comprising:
executing a quantum phase with a first location (A) over a quantum channel to
15 obtain a first raw data string (R_{AT});
executing a quantum phase with a second location (B) over a quantum channel to obtain a second raw data string (R_{TB});
calculating announcement data based on a function (F) of the first raw data string (R_{AT}) and the second raw data string (R_{TB}); and
20 announcing the announcement data over a classical channel.
10. The method of claim 9, wherein the executing the quantum phase with a first location (A) comprises:
receiving a first quantum signal from the first location (A) over a quantum channel;
25 and
measuring the first quantum signal to obtain the first raw data string (R_{AT}).
11. The method of claim 9, wherein the executing the quantum phase with a second location (B) comprises:
30 receiving a second quantum signal from the second location (B) over a quantum channel; and
measuring the second quantum signal to obtain the second raw data string (R_{TB});

12. The method of claim 9, wherein the function (F) is a parity function and the announcement data comprises parity data and measurement bases.
13. The method of claim 12, wherein the announcing announcement data further
5 comprises announcing error correction information.
14. The method of claim 9, further comprising determining an error estimate during the execution of the quantum phase.
- 10 15. A system for quantum key distribution (QKD) at an intermediate location (T), the system comprising:
a quantum system configured to execute a quantum phase with a first location (A) over a quantum channel to obtain a first raw data string (R_{AT}) and execute a quantum phase with a second location (B) over a quantum channel to obtain a
15 second raw data string (R_{TB});
a processor for calculating announcement data based on a function (F) of the first raw data string (R_{AT}) and the second raw data string (R_{TB}); and
a classical system configured to announce the announcement data over a classical channel.
20
16. The system of claim 15, wherein the function (F) is a parity function and the announcement data comprises parity data and measurement bases.

1/6

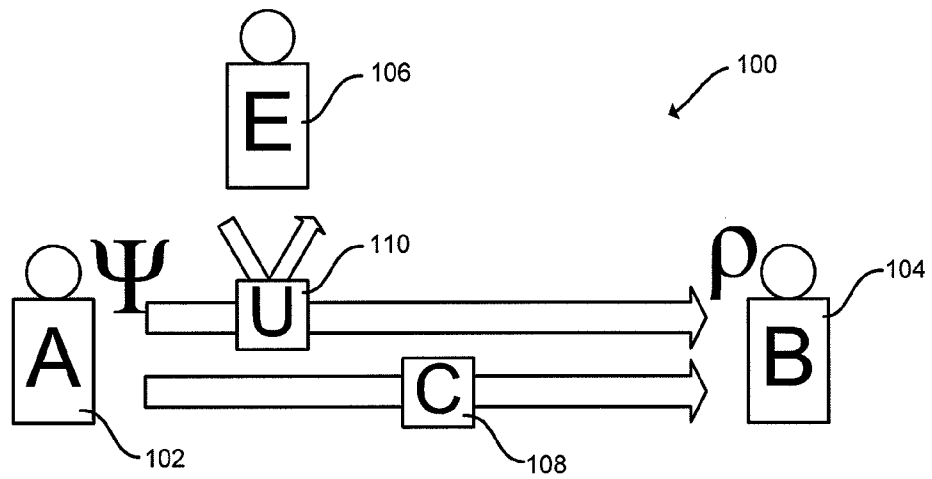


Fig. 1

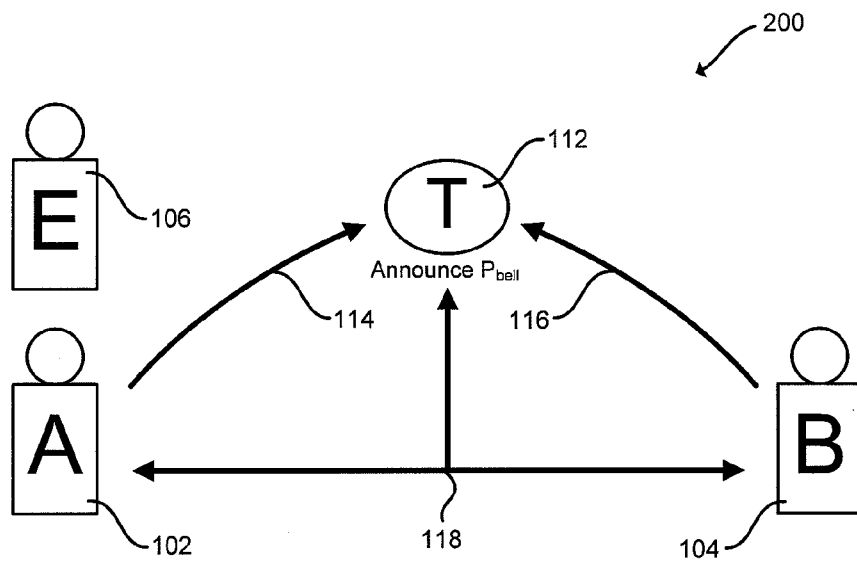


Fig. 2

2/6

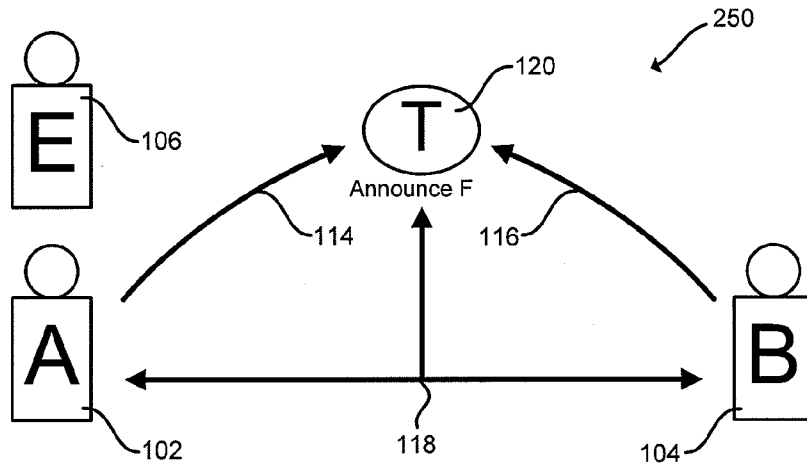


Fig. 3

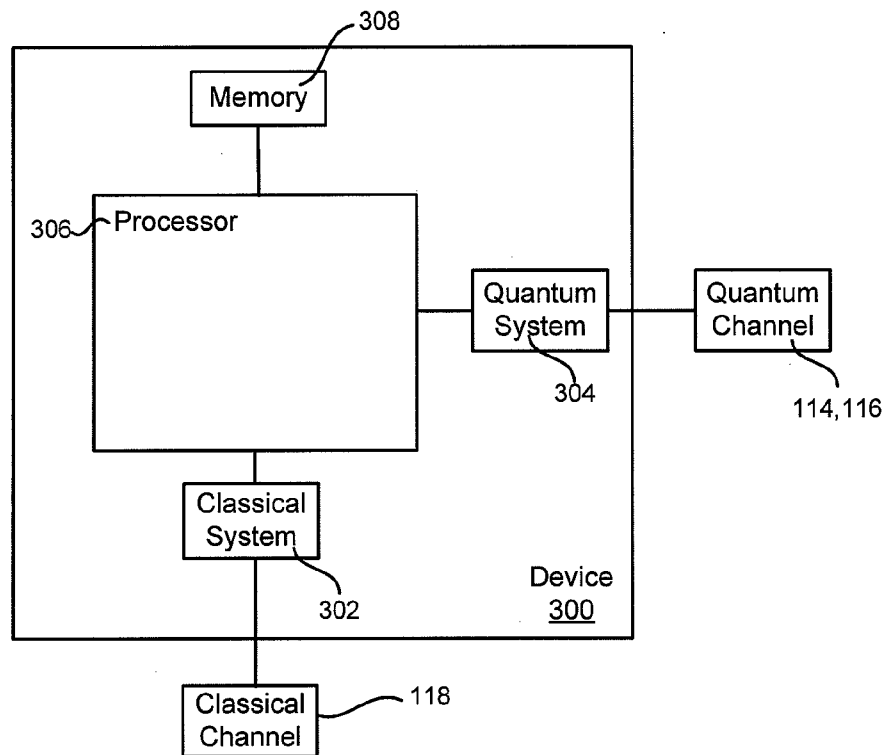


Fig. 4

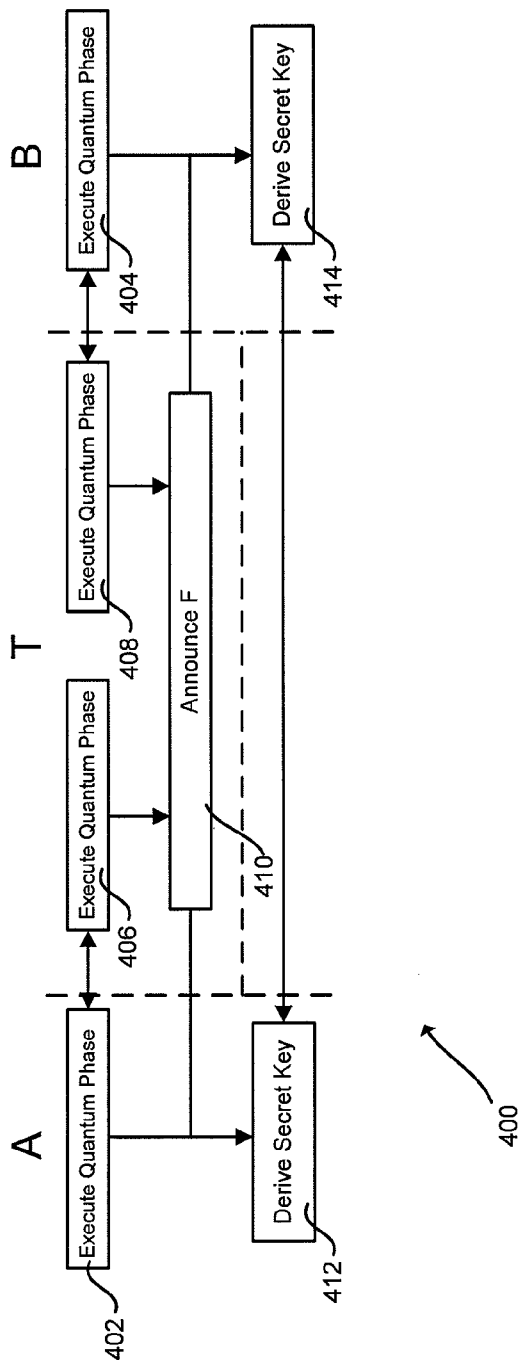


Fig. 5

4/6

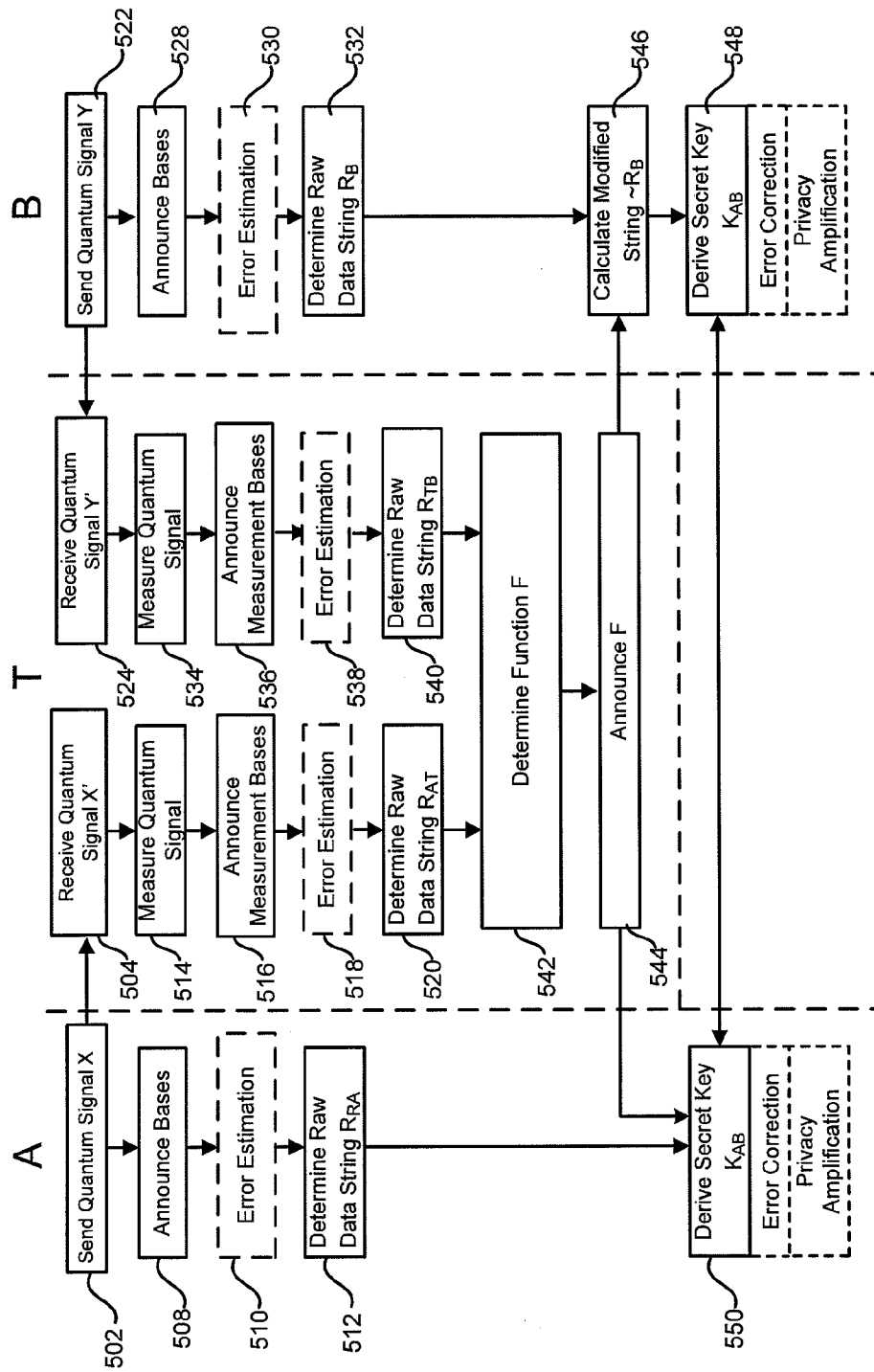


Fig. 6

5/6

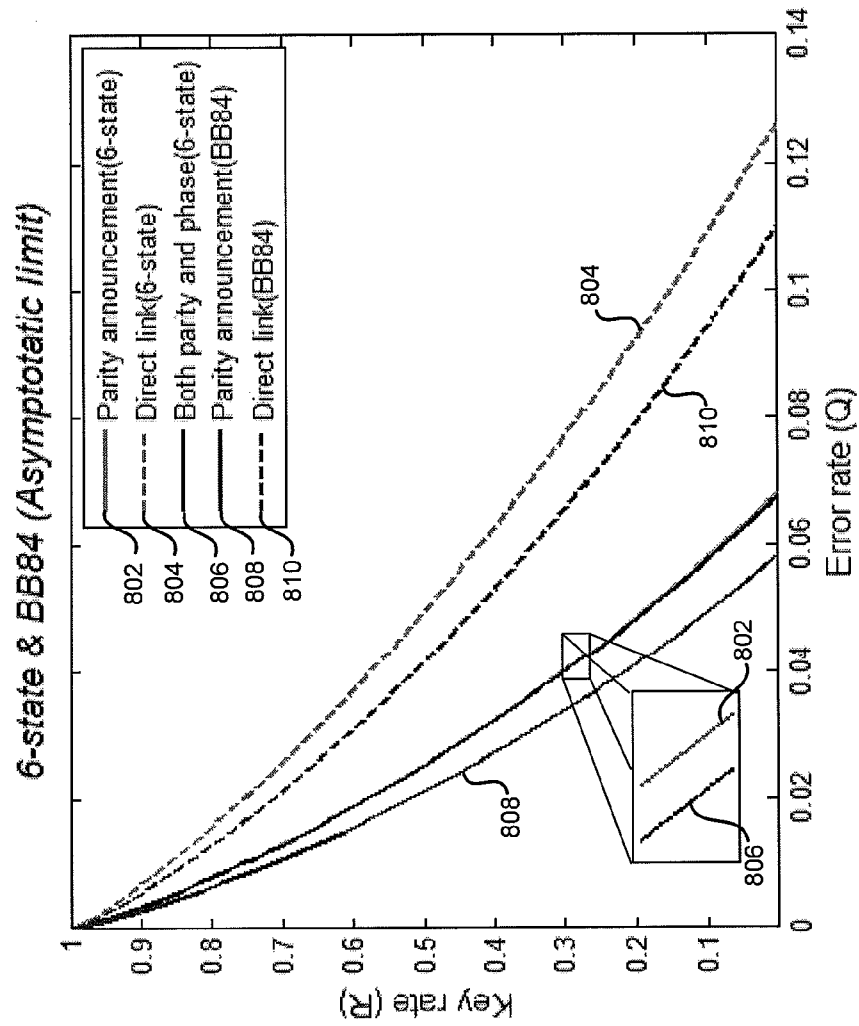


Fig. 7

6/6

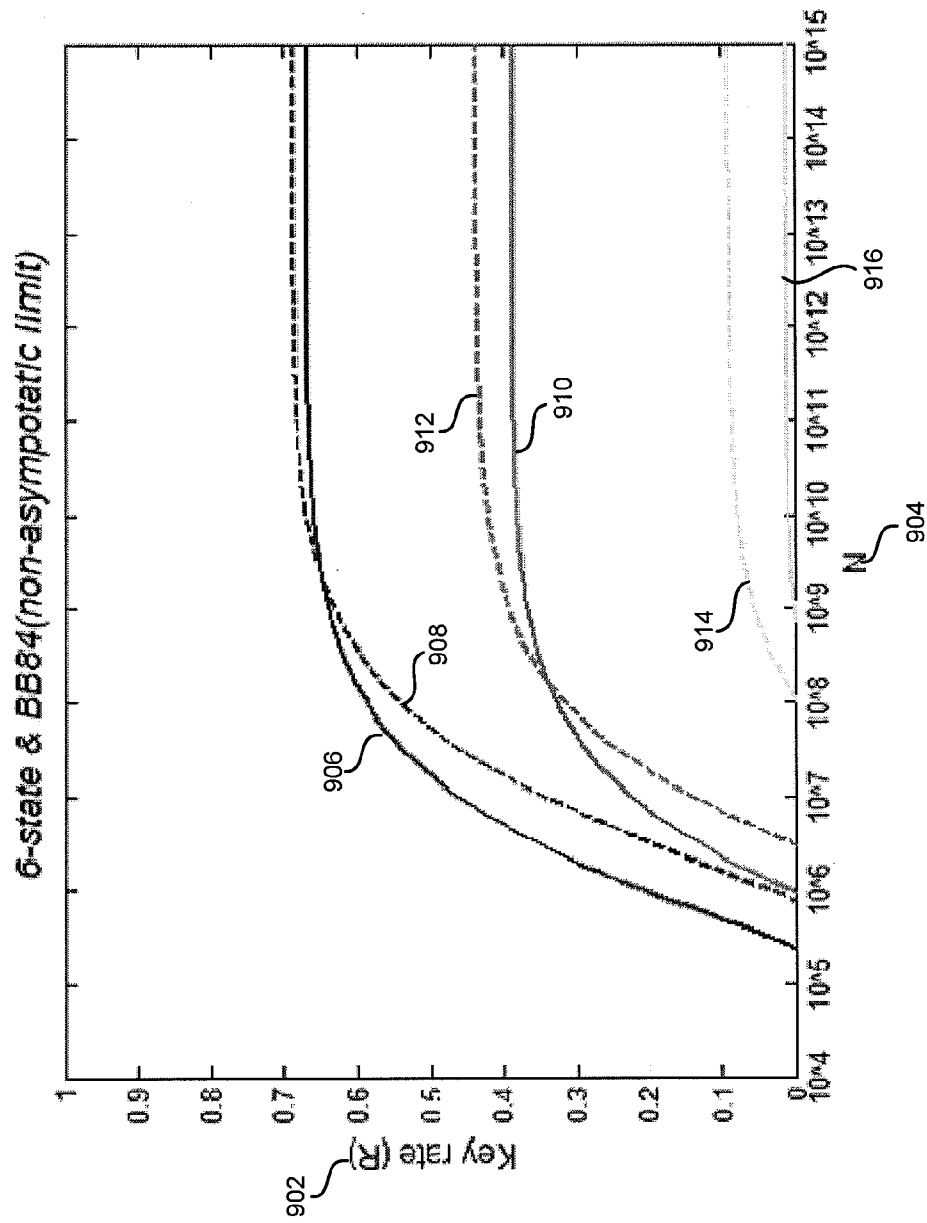


Fig. 8

