Claims

1. A quantum key distributed, QKD, linking apparatus for use with at least two endpoint devices for linking said endpoint devices in a QKD network, the QKD linking apparatus comprising:

a plurality of QKD links, each QKD link having a communication medium comprising a quantum channel and a classical channel, wherein each endpoint is assigned a QKD link connecting said each endpoint to the QKD linking apparatus;

a quantum communication component comprising a plurality of quantum transmitters, each quantum transmitter configured for transmitting quantum transmissions over a quantum channel of one of the QKD links;

a classical transceiver component comprising a plurality of classical transceivers, each classical transceiver configured for transmitting classical data over a classical channel of one of the QKD links and configured for receiving classical data over the classical channel of said one of the QKD links; and

a controller connected to the quantum communication component and the classical transceiver component, the controller configured to:

route or switch data generated for quantum transmission to an endpoint via a quantum transmitter assigned to the endpoint over a quantum channel of the QKD link of the endpoint;

route or switch classical data for classical transmission to an endpoint via a classical transceiver assigned to the endpoint over a classical channel of the QKD link of the endpoint; and

route or switch classical data received by a classical transceiver over the classical channel of the QKD link of an endpoint as required;

the QKD linking apparatus further comprising a random number generator, wherein the controller performs a QKD protocol between a first endpoint device and a second endpoint device, the controller further configured to:

route or switch a first set of random bits or keys output from the random number generator for quantum transmission to the first endpoint device over a quantum channel of the QKD link of the first endpoint device via a quantum transmitter assigned to the first endpoint device, wherein the first endpoint device uses a first quantum receiving basis for receiving the quantum transmission of the first set of random bits or keys;

route or switch an indication of the first set of random bits or keys validly received by the first endpoint device received over the classical channel of the QKD link of the first endpoint device by a classical transceiver assigned to the first endpoint device;

route or switch data representative of the first quantum transmission basis used for transmitting the first set of random bits or keys over a classical channel of the QKD link of the first endpoint device via the classical transceiver assigned to the first endpoint device;

determine a first intermediate set of symbols associated with the QKD linking apparatus based on discarding those first set of random bits or keys that do not correspond to the received indication of the first set of random bits or keys validly received by the first endpoint device;

route or switch a second set of random bits or keys output from the random number generator for quantum transmission to the second endpoint device over a quantum channel of the QKD link of the second endpoint device via a quantum transmitter assigned to the second endpoint device, wherein the second endpoint device uses a second quantum receiving basis for receiving the quantum transmission of the second set of random bits or keys;

route or switch an indication of the second set of random bits or keys validly received by the second endpoint device received from the second endpoint device over the classical channel of the QKD link of the second endpoint via a classical transceiver assigned to the second endpoint device;

route or switch data representative of the second quantum transmission basis used for transmitting the second set of random bits or keys for classical transmission over a classical channel of the QKD link of the second endpoint device via the classical transceiver assigned to the second endpoint device;

determine a second set of intermediate symbols associated with the QKD linking apparatus based on discarding those second set of random bits or keys that do not correspond to the received indication of the second set of random bits or keys validly received by the second endpoint device;

generate an encrypted first intermediate set of symbols using the second intermediate set of symbols;

route or switch the encrypted first intermediate set of symbols over the classical channel of the QKD link of the second endpoint via the classical transceiver assigned to the second endpoint device, wherein the second endpoint device decrypts the first intermediate set of symbols associated with the QKD linking apparatus based on deriving the second intermediate set of symbols associated with the QKD linking apparatus from the received second quantum transmission basis and the second quantum receiving basis;

route or switch data representative of the first quantum transmission basis and the first quantum receiving basis received from the first endpoint device for classical transmission over a classical channel of the QKD link of the second endpoint device via the classical transceiver assigned to the second endpoint device;

route or switch data representative of the second quantum transmission basis and the second quantum receiving basis received from the second endpoint device for classical transmission over a classical channel of the QKD link of the first endpoint device via the classical transceiver assigned to the first endpoint device, wherein the first endpoint device determines a first shared key based on discarding all bits from the received first set of random bits except those bits where the first transmission basis equals the first receiving basis and the second transmission basis equals the second receiving basis, and the second endpoint device determines a second shared key based on discarding all bits from the decrypted first intermediate

set of symbols associated with the QKD linking apparatus except those bits where the first transmission basis equals the first receiving basis and the second transmission basis equals the second receiving basis;

route or switch data representative of error correction and/or privacy amplification in relation to the first and second shared keys over the classical channels of the QKD links of the first and second endpoint devices, wherein the first and second devices determine a final shared key based on the first and second shared keys.

2. A quantum key distributed, QKD, linking apparatus for use with at least two endpoint devices for linking said endpoint devices in a QKD network, the QKD linking apparatus comprising:

a plurality of QKD links, each QKD link having a communication medium comprising a quantum channel and a classical channel, wherein each endpoint is assigned a QKD link connecting said each endpoint to the QKD linking apparatus;

a quantum communication component comprising a plurality of quantum transmitters, each quantum transmitter configured for transmitting quantum transmissions over a quantum channel of one of the QKD links;

a classical transceiver component comprising a plurality of classical transceivers, each classical transceiver configured for transmitting classical data over a classical channel of one of the QKD links and configured for receiving classical data over the classical channel of said one of the QKD links; and

a controller connected to the quantum communication component and the classical transceiver component, the controller configured to:

route or switch data generated for quantum transmission to an endpoint via a quantum transmitter assigned to the endpoint over a quantum channel of the QKD link of the endpoint;

route or switch classical data for classical transmission to an endpoint via a classical transceiver assigned to the endpoint over a classical channel of the QKD link of the endpoint; and route or switch classical data received by a classical transceiver over the classical channel of the QKD link of an endpoint as required;

the QKD linking apparatus further comprising a random number generator, wherein the controller performs a QKD protocol between a first endpoint device and a second endpoint device, the controller further configured to:

route or switch a first set of random bits or keys received by a quantum receiver assigned to the first endpoint device from quantum transmissions from the first endpoint device over a quantum channel of the QKD link of the first endpoint device, wherein the quantum receiver uses a first quantum receiving basis for receiving the quantum transmission of the first set of random bits or keys and the first endpoint device uses a first quantum transmission basis for transmitting the quantum transmission of the first set of random bits or keys;

route or switch an indication of the first set of random bits or keys validly received by the quantum receiver to the first endpoint device over the classical channel of the QKD link of the first endpoint device by a classical transceiver assigned to the first endpoint device;

route or switch data representative of the first quantum receiving basis used for receiving the first set of random bits or keys to the first endpoint device over a classical channel of the QKD link of the first endpoint device via the classical transceiver assigned to the first endpoint device;

determine a first intermediate set of symbols associated with the QKD linking apparatus based on discarding those first set of random bits or keys that were not validly received by the quantum receiver assigned to the first endpoint device;

route or switch a second set of random bits or keys received by a quantum receiver assigned to the second endpoint device from quantum transmissions from the second endpoint device over a quantum channel of the QKD link of the second endpoint device, wherein the quantum receiver uses a second quantum receiving basis for receiving the quantum transmission of the second set of random bits or keys and the second endpoint device uses a second quantum transmission basis for transmitting the quantum transmission of the second set of random bits or keys;

route or switch an indication of the second set of random bits or keys validly received by the quantum receiver to the second endpoint device over the classical channel of the QKD link of the second endpoint device by a classical transceiver assigned to the second endpoint device;

route or switch data representative of the second quantum receiving basis used for receiving the second set of random bits or keys to the second endpoint device over a classical channel of the QKD link of the second endpoint device via the classical transceiver assigned to the second endpoint device;

determine a second intermediate set of symbols associated with the QKD linking apparatus based on discarding those second set of random bits or keys that were not validly received by the quantum receiver assigned to the second endpoint device;

generate an encrypted first intermediate set of symbols using the second intermediate set of symbols;

route or switch the encrypted first intermediate set of symbols over the classical channel of the QKD link of the second endpoint via the classical transceiver assigned to the second endpoint device, wherein the second endpoint device decrypts the encrypted first intermediate set of symbols based on deriving the second intermediate set of symbols associated with the QKD linking apparatus from the received second quantum transmission basis and the second quantum receiving basis;

route or switch data representative of the first quantum transmission basis and the first quantum receiving basis received from the first endpoint device for classical transmission over a

classical channel of the QKD link of the second endpoint device via the classical transceiver assigned to the second endpoint device;

route or switch data representative of the second quantum transmission basis and the second quantum receiving basis received from the second endpoint device for classical transmission over a classical channel of the QKD link of the first endpoint device via the classical transceiver assigned to the first endpoint device, wherein the first endpoint device determines a first shared key based on discarding all bits from the received first set of random bits except those bits where the first transmission basis equals the first receiving basis and the second transmission basis equals the second receiving basis, and the second endpoint device determines a second shared key based on discarding all bits from the decrypted first intermediate set of symbols except those bits where the first transmission basis equals the first receiving basis and the second transmission basis equals the second receiving basis;

route or switch data representative of error correction and/or privacy amplification in relation to the first and second shared keys over the classical channels of the QKD links of the first and second endpoint devices, wherein the first and second devices determine a final shared key based on the first and second shared keys.

3. A quantum key distributed, QKD, linking apparatus for use with at least two endpoint devices for linking said endpoint devices in a QKD network, the QKD linking apparatus comprising:

a plurality of QKD links, each QKD link having a communication medium comprising a quantum channel and a classical channel, wherein each endpoint is assigned a QKD link connecting said each endpoint to the QKD linking apparatus;

a quantum communication component comprising a plurality of quantum transmitters, each quantum transmitter configured for transmitting quantum transmissions over a quantum channel of one of the QKD links;

a classical transceiver component comprising a plurality of classical transceivers, each classical transceiver configured for transmitting classical data over a classical channel of one of the QKD links and configured for receiving classical data over the classical channel of said one of the QKD links; and

a controller connected to the quantum communication component and the classical transceiver component, the controller configured to:

route or switch data generated for quantum transmission to an endpoint via a quantum transmitter assigned to the endpoint over a quantum channel of the QKD link of the endpoint;

route or switch classical data for classical transmission to an endpoint via a classical transceiver assigned to the endpoint over a classical channel of the QKD link of the endpoint; and

route or switch classical data received by a classical transceiver over the classical channel of the QKD link of an endpoint as required;

the QKD linking apparatus further comprising a random number generator, wherein the controller performs a QKD protocol between a first endpoint device and a second endpoint device, the controller further configured to:

route or switch a first set of random bits or keys received by a quantum receiver assigned to the first endpoint device from quantum transmissions from the first endpoint device over a quantum channel of the QKD link of the first endpoint device, wherein the quantum receiver uses a first quantum receiving basis for receiving the quantum transmission of the first set of random bits or keys and the first endpoint device uses a first quantum transmission basis for transmitting the quantum transmission of the first set of random bits or keys;

route or switch an indication of the first set of random bits or keys validly received by the quantum receiver to the first endpoint device over the classical channel of the QKD link of the first endpoint device by a classical transceiver assigned to the first endpoint device;

route or switch data representative of the first quantum receiving basis used for receiving the first set of random bits or keys to the first endpoint device over a classical channel of the QKD link of the first endpoint device via the classical transceiver assigned to the first endpoint device;

determine a first intermediate set of symbols associated with the QKD linking apparatus based on discarding those first set of random bits or keys that were not validly received by the quantum receiver assigned to the first endpoint device;

route or switch a second set of random bits or keys output from a random number generator for quantum transmission to the second endpoint device over a quantum channel of the QKD link of the second endpoint device via a quantum transmitter assigned to the second endpoint device, wherein the second endpoint device uses a second quantum receiving basis for receiving the quantum transmission of the second set of random bits or keys;

route or switch an indication of the second set of random bits or keys validly received by the second endpoint device received from the second endpoint device over the classical channel of the QKD link of the second endpoint via a classical transceiver assigned to the second endpoint device;

route or switch data representative of the second quantum transmission basis used for transmitting the second set of random bits or keys for classical transmission over a classical channel of the QKD link of the second endpoint device via the classical transceiver assigned to the second endpoint device;

determine a second intermediate set of symbols associated with the QKD linking apparatus based on discarding those second set of random bits or keys that do not correspond to the received indication of the second set of random bits or keys validly received by the second endpoint device;

generate an encrypted first intermediate set of symbols using the second intermediate set of symbols;

route or switch the encrypted first intermediate set of symbols over the classical channel of the QKD link of the second endpoint via the classical transceiver assigned to the second endpoint device, wherein the second endpoint device decrypts the encrypted first intermediate set of symbols based on deriving the second intermediate set of symbols associated with the QKD linking apparatus from the received second quantum transmission basis and the second quantum receiving basis;

route or switch data representative of the first quantum transmission basis and the first quantum receiving basis received from the first endpoint device for classical transmission over a classical channel of the QKD link of the second endpoint device via the classical transceiver assigned to the second endpoint device;

route or switch data representative of the second quantum transmission basis and the second quantum receiving basis received from the second endpoint device for classical transmission over a classical channel of the QKD link of the first endpoint device via the classical transceiver assigned to the first endpoint device, wherein the first endpoint device determines a first shared key based on discarding all bits from the received first set of random bits except those bits where the first transmission basis equals the first receiving basis and the second transmission basis equals the second receiving basis, and the second endpoint device determines a second shared key based on discarding all bits from the decrypted first intermediate set of symbols except those bits where the first transmission basis equals the first receiving basis and the second transmission basis equals the second receiving basis;

route or switch data representative of error correction and/or privacy amplification in relation to the first and second shared keys over the classical channels of the QKD links of the first and second endpoint devices, wherein the first and second devices determine a final shared key based on the first and second shared keys.

4. The QKD linking apparatus as claimed in any one of claims 1 to 3, wherein each QKD link has a dedicated quantum transmitter from the quantum communication component and a dedicated classical transceiver from the classical transceiver component for use over the quantum channel and classical channel of the QKD link.

5. The QKD linking apparatus as claimed in any one of claims 1 to 4, wherein the quantum communication component further comprising a plurality of quantum receivers, each quantum receiver configured for receiving quantum transmissions over a quantum channel of one of the QKD links, wherein one or more of the QKD links has a dedicated quantum receiver from the quantum communication component and a dedicated classical transceiver from the classical transceiver component for use over the quantum channel and classical channel of the QKD link, wherein the controller is further configured to

route or switch data received by a quantum receiver from a quantum transmission over the quantum channel of the QKD link of an endpoint device assigned to the quantum receiver.

6. A quantum key distributed, QKD, linking apparatus for use with at least two endpoint devices for linking said endpoint devices in a QKD network, the QKD linking apparatus comprising:

a plurality of QKD links, each QKD link having a communication medium comprising a quantum channel and a classical channel, wherein each endpoint is assigned a QKD link connecting said each endpoint to the QKD linking apparatus;

a quantum communication component comprising a plurality of quantum receivers, each quantum receiver configured for receiving quantum transmissions over a quantum channel of one of the QKD links;

a classical transceiver component comprising a plurality of classical transceivers, each classical transceiver configured for transmitting classical data over a classical channel of one of the QKD links and configured for receiving classical data over the classical channel of said one of the QKD links; and

a controller connected to the quantum communication component and the classical transceiver component, the controller configured to:

route or switch data received in a quantum transmission from an endpoint via a quantum receiver assigned to the endpoint over a quantum channel of the QKD link of the endpoint;

route or switch classical data for classical transmission to an endpoint via a classical transceiver assigned to the endpoint over a classical channel of the QKD link of the endpoint; and

route or switch classical data received by a classical transceiver over the classical channel of the QKD link of an endpoint as required;

the quantum communication component further comprising a plurality of quantum transmitters, each quantum transmitter configured for transmitting quantum transmissions over a quantum channel of one of the QKD links, wherein one or more of the QKD links has a dedicated quantum transmitter from the quantum communication component and a dedicated classical transceiver from the classical transceiver component for use over the quantum channel and classical channel of the QKD link, wherein the controller is further configured to route or switch data generated for quantum transmission to an endpoint device by the quantum transmitter over the quantum channel of the QKD link of the endpoint device assigned to the quantum transmitter;

the QKD linking apparatus further comprising a random number generator, wherein the controller performs a QKD protocol between a first endpoint device and a second endpoint device, the controller further configured to:

route or switch a first set of random bits or keys output from the random number generator for quantum transmission to the first endpoint device over a quantum channel of the QKD link of the first endpoint device via a quantum transmitter assigned to the first endpoint device, wherein the first endpoint device uses a first quantum receiving basis for receiving the quantum transmission of the first set of random bits or keys;

route or switch an indication of the first set of random bits or keys validly received by the first endpoint device received over the classical channel of the QKD link of the first endpoint device by a classical transceiver assigned to the first endpoint device;

route or switch data representative of the first quantum transmission basis used for transmitting the first set of random bits or keys over a classical channel of the QKD link of the first endpoint device via the classical transceiver assigned to the first endpoint device;

determine a first intermediate set of symbols associated with the QKD linking apparatus based on discarding those first set of random bits or keys that do not correspond to the received indication of the first set of random bits or keys validly received by the first endpoint device;

route or switch a second set of random bits or keys output from the random number generator for quantum transmission to the second endpoint device over a quantum channel of the QKD link of the second endpoint device via a quantum transmitter assigned to the second endpoint device, wherein the second endpoint device uses a second quantum receiving basis for receiving the quantum transmission of the second set of random bits or keys;

route or switch an indication of the second set of random bits or keys validly received by the second endpoint device received from the second endpoint device over the classical channel of the QKD link of the second endpoint via a classical transceiver assigned to the second endpoint device;

route or switch data representative of the second quantum transmission basis used for transmitting the second set of random bits or keys for classical transmission over a classical channel of the QKD link of the second endpoint device via the classical transceiver assigned to the second endpoint device;

determine a second set of intermediate symbols associated with the QKD linking apparatus based on discarding those second set of random bits or keys that do not correspond to the received indication of the second set of random bits or keys validly received by the second endpoint device;

generate an encrypted first intermediate set of symbols using the second intermediate set of symbols;

route or switch the encrypted first intermediate set of symbols over the classical channel of the QKD link of the second endpoint via the classical transceiver assigned to the second endpoint device, wherein the second endpoint device decrypts the first intermediate set of symbols associated with the QKD linking apparatus based on deriving the second intermediate set of symbols associated with the QKD linking apparatus from the received second quantum transmission basis and the second quantum receiving basis;

route or switch data representative of the first quantum transmission basis and the first quantum receiving basis received from the first endpoint device for classical transmission over a

classical channel of the QKD link of the second endpoint device via the classical transceiver assigned to the second endpoint device;

route or switch data representative of the second quantum transmission basis and the second quantum receiving basis received from the second endpoint device for classical transmission over a classical channel of the QKD link of the first endpoint device via the classical transceiver assigned to the first endpoint device, wherein the first endpoint device determines a first shared key based on discarding all bits from the received first set of random bits except those bits where the first transmission basis equals the first receiving basis and the second transmission basis equals the second receiving basis, and the second endpoint device determines a second shared key based on discarding all bits from the decrypted first intermediate set of symbols associated with the QKD linking apparatus except those bits where the first transmission basis equals the first receiving basis and the second transmission basis equals the second receiving basis;

route or switch data representative of error correction and/or privacy amplification in relation to the first and second shared keys over the classical channels of the QKD links of the first and second endpoint devices, wherein the first and second devices determine a final shared key based on the first and second shared keys.

7. A quantum key distributed, QKD, linking apparatus for use with at least two endpoint devices for linking said endpoint devices in a QKD network, the QKD linking apparatus comprising:

a plurality of QKD links, each QKD link having a communication medium comprising a quantum channel and a classical channel, wherein each endpoint is assigned a QKD link connecting said each endpoint to the QKD linking apparatus;

a quantum communication component comprising a plurality of quantum receivers, each quantum receiver configured for receiving quantum transmissions over a quantum channel of one of the QKD links;

a classical transceiver component comprising a plurality of classical transceivers, each classical transceiver configured for transmitting classical data over a classical channel of one of the QKD links and configured for receiving classical data over the classical channel of said one of the QKD links; and

a controller connected to the quantum communication component and the classical transceiver component, the controller configured to:

route or switch data received in a quantum transmission from an endpoint via a quantum receiver assigned to the endpoint over a quantum channel of the QKD link of the endpoint;

route or switch classical data for classical transmission to an endpoint via a classical transceiver assigned to the endpoint over a classical channel of the QKD link of the endpoint; and

route or switch classical data received by a classical transceiver over the classical channel of the QKD link of an endpoint as required;

the quantum communication component further comprising a plurality of quantum transmitters, each quantum transmitter configured for transmitting quantum transmissions over a quantum channel of one of the QKD links, wherein one or more of the QKD links has a dedicated quantum transmitter from the quantum communication component and a dedicated classical transceiver from the classical transceiver component for use over the quantum channel and classical channel of the QKD link, wherein the controller is further configured to route or switch data generated for quantum transmission to an endpoint device by the quantum transmitter over the quantum channel of the QKD link of the endpoint device assigned to the quantum transmitter;

the QKD linking apparatus further comprising a random number generator, wherein the controller performs a QKD protocol between a first endpoint device and a second endpoint device, the controller further configured to:

route or switch a first set of random bits or keys received by a quantum receiver assigned to the first endpoint device from quantum transmissions from the first endpoint device over a quantum channel of the QKD link of the first endpoint device, wherein the quantum receiver uses a first quantum receiving basis for receiving the quantum transmission of the first set of random bits or keys and the first endpoint device uses a first quantum transmission basis for transmitting the quantum transmission of the first set of random bits or keys;

route or switch an indication of the first set of random bits or keys validly received by the quantum receiver to the first endpoint device over the classical channel of the QKD link of the first endpoint device by a classical transceiver assigned to the first endpoint device;

route or switch data representative of the first quantum receiving basis used for receiving the first set of random bits or keys to the first endpoint device over a classical channel of the QKD link of the first endpoint device via the classical transceiver assigned to the first endpoint device;

determine a first intermediate set of symbols associated with the QKD linking apparatus based on discarding those first set of random bits or keys that were not validly received by the quantum receiver assigned to the first endpoint device;

route or switch a second set of random bits or keys received by a quantum receiver assigned to the second endpoint device from quantum transmissions from the second endpoint device over a quantum channel of the QKD link of the second endpoint device, wherein the quantum receiver uses a second quantum receiving basis for receiving the quantum transmission of the second set of random bits or keys and the second endpoint device uses a second quantum transmission basis for transmitting the quantum transmission of the second set of random bits or keys;

route or switch an indication of the second set of random bits or keys validly received by the quantum receiver to the second endpoint device over the classical channel of the QKD link of the second endpoint device by a classical transceiver assigned to the second endpoint device;

route or switch data representative of the second quantum receiving basis used for receiving the second set of random bits or keys to the second endpoint device over a classical channel of the QKD link of the second endpoint device via the classical transceiver assigned to the second endpoint device;

determine a second intermediate set of symbols associated with the QKD linking apparatus based on discarding those second set of random bits or keys that were not validly received by the quantum receiver assigned to the second endpoint device;

generate an encrypted first intermediate set of symbols using the second intermediate set of symbols;

route or switch the encrypted first intermediate set of symbols over the classical channel of the QKD link of the second endpoint via the classical transceiver assigned to the second endpoint device, wherein the second endpoint device decrypts the encrypted first intermediate set of symbols based on deriving the second intermediate set of symbols associated with the QKD linking apparatus from the received second quantum transmission basis and the second quantum receiving basis;

route or switch data representative of the first quantum transmission basis and the first quantum receiving basis received from the first endpoint device for classical transmission over a classical channel of the QKD link of the second endpoint device via the classical transceiver assigned to the second endpoint device;

route or switch data representative of the second quantum transmission basis and the second quantum receiving basis received from the second endpoint device for classical transmission over a classical channel of the QKD link of the first endpoint device via the classical transceiver assigned to the first endpoint device, wherein the first endpoint device determines a first shared key based on discarding all bits from the received first set of random bits except those bits where the first transmission basis equals the first receiving basis and the second transmission basis equals the second receiving basis, and the second endpoint device determines a second shared key based on discarding all bits from the decrypted first intermediate set of symbols except those bits where the first transmission basis equals the first receiving basis and the second transmission basis equals the second receiving basis;

route or switch data representative of error correction and/or privacy amplification in relation to the first and second shared keys over the classical channels of the QKD links of the first and second endpoint devices, wherein the first and second devices determine a final shared key based on the first and second shared keys.

8. A quantum key distributed, QKD, linking apparatus for use with at least two endpoint devices for linking said endpoint devices in a QKD network, the QKD linking apparatus comprising:

a plurality of QKD links, each QKD link having a communication medium comprising a quantum channel and a classical channel, wherein each endpoint is assigned a QKD link connecting said each endpoint to the QKD linking apparatus;

a quantum communication component comprising a plurality of quantum receivers, each quantum receiver configured for receiving quantum transmissions over a quantum channel of one of the QKD links;

a classical transceiver component comprising a plurality of classical transceivers, each classical transceiver configured for transmitting classical data over a classical channel of one of the QKD links and configured for receiving classical data over the classical channel of said one of the QKD links; and

a controller connected to the quantum communication component and the classical transceiver component, the controller configured to:

route or switch data received in a quantum transmission from an endpoint via a quantum receiver assigned to the endpoint over a quantum channel of the QKD link of the endpoint;

route or switch classical data for classical transmission to an endpoint via a classical transceiver assigned to the endpoint over a classical channel of the QKD link of the endpoint; and

route or switch classical data received by a classical transceiver over the classical channel of the QKD link of an endpoint as required;

the quantum communication component further comprising a plurality of quantum transmitters, each quantum transmitter configured for transmitting quantum transmissions over a quantum channel of one of the QKD links, wherein one or more of the QKD links has a dedicated quantum transmitter from the quantum communication component and a dedicated classical transceiver from the classical transceiver component for use over the quantum channel and classical channel of the QKD link, wherein the controller is further configured to route or switch data generated for quantum transmission to an endpoint device by the quantum transmitter over the quantum channel of the QKD link of the endpoint device assigned to the quantum transmitter;

the QKD linking apparatus further comprising a random number generator, wherein the controller performs a QKD protocol between a first endpoint device and a second endpoint device, the controller further configured to:

route or switch a first set of random bits or keys received by a quantum receiver assigned to the first endpoint device from quantum transmissions from the first endpoint device over a quantum channel of the QKD link of the first endpoint device, wherein the quantum receiver uses a first quantum receiving basis for receiving the quantum transmission of the first set of random bits or keys and the first endpoint device uses a first quantum transmission basis for transmitting the quantum transmission of the first set of random bits or keys;

route or switch an indication of the first set of random bits or keys validly received by the quantum receiver to the first endpoint device over the classical channel of the QKD link of the first endpoint device by a classical transceiver assigned to the first endpoint device;

route or switch data representative of the first quantum receiving basis used for receiving the first set of random bits or keys to the first endpoint device over a classical channel of the QKD link of the first endpoint device via the classical transceiver assigned to the first endpoint device;

determine a first intermediate set of symbols associated with the QKD linking apparatus based on discarding those first set of random bits or keys that were not validly received by the quantum receiver assigned to the first endpoint device;

route or switch a second set of random bits or keys output from a random number generator for quantum transmission to the second endpoint device over a quantum channel of the QKD link of the second endpoint device via a quantum transmitter assigned to the second endpoint device, wherein the second endpoint device uses a second quantum receiving basis for receiving the quantum transmission of the second set of random bits or keys;

route or switch an indication of the second set of random bits or keys validly received by the second endpoint device received from the second endpoint device over the classical channel of the QKD link of the second endpoint via a classical transceiver assigned to the second endpoint device;

route or switch data representative of the second quantum transmission basis used for transmitting the second set of random bits or keys for classical transmission over a classical channel of the QKD link of the second endpoint device via the classical transceiver assigned to the second endpoint device;

determine a second intermediate set of symbols associated with the QKD linking apparatus based on discarding those second set of random bits or keys that do not correspond to the received indication of the second set of random bits or keys validly received by the second endpoint device;

generate an encrypted first intermediate set of symbols using the second intermediate set of symbols;

route or switch the encrypted first intermediate set of symbols over the classical channel of the QKD link of the second endpoint via the classical transceiver assigned to the second endpoint device, wherein the second endpoint device decrypts the encrypted first intermediate set of symbols based on deriving the second intermediate set of symbols associated with the QKD linking apparatus from the received second quantum transmission basis and the second quantum receiving basis;

route or switch data representative of the first quantum transmission basis and the first quantum receiving basis received from the first endpoint device for classical transmission over a classical channel of the QKD link of the second endpoint device via the classical transceiver assigned to the second endpoint device;

route or switch data representative of the second quantum transmission basis and the second quantum receiving basis received from the second endpoint device for classical transmission over a classical channel of the QKD link of the first endpoint device via the classical transceiver assigned to the first endpoint device, wherein the first endpoint device determines a first shared key based on discarding all bits from the received first set of random bits except those bits where the first transmission basis equals the first receiving basis and the second transmission basis equals the second receiving basis, and the second endpoint device determines a second shared key based on discarding all bits from the

decrypted first intermediate set of symbols except those bits where the first transmission basis equals the first receiving basis and the second transmission basis equals the second receiving basis;

route or switch data representative of error correction and/or privacy amplification in relation to the first and second shared keys over the classical channels of the QKD links of the first and second endpoint devices, wherein the first and second devices determine a final shared key based on the first and second shared keys.

9. The QKD linking apparatus as claimed in any one of claims 6 to 8, wherein each QKD link has a dedicated quantum receiver from the quantum communication component and a dedicated classical transceiver from the classical transceiver component for use over the quantum channel and classical channel of the QKD link.

10. The QKD linking apparatus as claimed in any preceding claim, the QKD linking apparatus further comprising a controller component configured for controlling the quantum communication component for implementing one or more QKD protocols between the QKD linking apparatus and two or more of the endpoint devices, wherein:

the controller component is configured to:

assign, depending on the one or more QKD protocols, an available quantum transmitter or quantum receiver to an endpoint device for use over the QKD link of the endpoint device; and

when implementing one of the QKD protocols between two or more endpoint devices, at least one of the endpoint devices with an assigned quantum transmitter, direct the quantum communication component to route or switch quantum transmissions for the at least one endpoint device to the quantum transmitter assigned to said at least one endpoint device for transmitting said quantum transmissions over the quantum channel of the QKD link of the endpoint device;

when implementing one of the QKD protocols between two or more endpoint devices, at least one of the endpoint devices with an assigned quantum receiver, direct the quantum communication component to route or switch quantum transmissions received by the quantum receiver from the at least one endpoint device over the quantum channel of the QKD link of the endpoint device.

11. The QKD linking apparatus as claimed in any preceding claim, the QKD linking apparatus further comprising a controller component configured for controlling the classical transmission and routing component for implementing one or more QKD protocols between the QKD linking apparatus and two or more of the endpoint devices, wherein:

the controller component is configured to:

assign an available classical transceiver to an endpoint device for use over the QKD link of the endpoint device;

when implementing one of the QKD protocols between two or more endpoint devices each with an assigned classical transceiver, direct the classical transmission and routing component to route or switch classical data for an endpoint device of the two or more endpoint devices to the classical transceiver assigned to said endpoint device to the classical channel of the QKD link of the endpoint device.

12. The QKD linking apparatus as claimed in any preceding claim, wherein, when one of the QKD protocols being performed between the QKD linking apparatus and at least two of the endpoint devices is complete, the controller is further configured to direct the classical transmission and routing component to route or switch secure communications between the classical transceivers assigned to each of the endpoint devices over the corresponding classical channels of the QKD links of said endpoint devices, said communications being secured based on the keys exchanged using the QKD protocol between the two or more endpoint devices.

13. The QKD linking apparatus as claimed in any preceding claim, wherein the quantum transmitters are optical quantum transmitters and the classical transceivers are optical classical transceivers.

14. The QKD linking apparatus as claimed in any preceding claim, wherein the communication medium of one or more QKD links comprises at least one from the group of:

any type of communication medium or media capable of being configured to form a quantum channel for transmission of quantum information and/or capable of being configured to form one or more classical communication channels for transmission of non-quantum or classical communications;

capable of propagating an electromagnetic signal with wavelengths in the visible and/or non-visible electromagnetic spectrum;

capable of propagating an electromagnetic signal with wavelengths in the visible light spectrum;

capable of propagating an electromagnetic signal with wavelengths in the near-infra-red light spectrum;

capable of propagating an electromagnetic signal with wavelengths in the infra-red spectrum;

capable of propagating an electromagnetic signal with wavelengths in the microwave spectrum;

capable of propagating an electromagnetic signal with wavelengths in the Terahertz wavelength spectrum;

any other suitable electromagnetic wavelength for use in at least quantum communications and/or non-quantum communications;

an optical communication medium capable of propagating electromagnetic signals with wavelengths in at least one from the group of: the visible light spectrum, the near-infrared light spectrum, the infra-red and the like;

optical free-space;

an optical cable;

multi-mode optical fibre;

single-mode optical fibre;

one or more optical fibres;

an optical fibre capable of propagating light in the wavelengths of at least one of the visible light spectrum and/or near-infra red light spectrum and the like.

15. The QKD linking apparatus as claimed in any preceding claim, wherein the communication medium of each of the QKD links comprises at least one optical fibre.

16. The QKD linking apparatus as claimed in claim 15, wherein the communication medium of at least one of the QKD links has a single optical fibre that is shared by the quantum and classical channels of said at least one QKD link.

17. The QKD linking apparatus as claimed in claim 16, wherein the quantum transmitter assigned to the endpoint of the QKD link and the classical transceiver assigned to the endpoint of the QKD link are coupled to the quantum channel and classical channel of the single optical fibre of the QKD link via a QKD link coupling arrangement.

18. The QKD linking apparatus as claimed in claim 17, wherein the QKD link coupling arrangement comprises one or more from the group of: one or more optical splitter/combiner device(s) or one or more optical multiplexor/demultiplexor device(s).

19. The QKD linking apparatus as claimed in any of claims 1 to 15, wherein the communication medium, shared by the quantum and classical channels, of at least one of the QKD links comprises a first optical fibre for the quantum channel and a second optical fibre for the classical channel.

20. The QKD linking apparatus as claimed in any of claims 1 to 15, wherein the communication medium, shared by the quantum and classical channels, of at least one of the QKD links comprises a first optical fibre for the quantum channel, a second and third optical fibres for the classical channel.

21. The QKD linking apparatus as claimed in any of claims 1 to 20, further comprising a plurality of homes or offices, each home or office associated with an endpoint device and corresponding QKD link, said QKD link connected between said endpoint device and said quantum communication component and said classical transmission routing component.

22. The QKD linking apparatus as claimed in any of claims 1 to 21, further comprising a road-side cabinet housing the QKD linking apparatus with a backhaul QKD link of the QKD links connected to an exchange.

23. The QKD linking apparatus as claimed in any of claims 1 to 22, wherein the QKD linking apparatus comprises a first QKD linking component comprising the quantum communication component and controller, and a second QKD linking component comprising the classical transceiver routing component, wherein the first QKD linking component is located in a secure facility and the second QKD linking component is located in a public facility.

24. The QKD linking apparatus as claimed in claim 23, wherein the secure facility is an exchange and the public facility is a roadside cabinet.

25. The QKD linking apparatus as claimed in any of claims 1 to 22, wherein the QKD linking apparatus comprises a first QKD linking component comprising the quantum communication component and controller, and a second QKD linking component comprising the classical transceiver routing component, wherein the first QKD linking component is housed in a secure tamper-proof enclosure and the first and second QKD linking components are located in a public facility or roadside cabinet.

26. The QKD linking apparatus as claimed in any of claims 1 to 22, further comprising a radio access network comprising a centralised unit and a plurality of radio masts/radio units configured to service a plurality of mobile units, said centralised unit and each radio mast/radio unit associated with an endpoint device and corresponding QKD link, said QKD link connected between said endpoint device and said quantum communication component and said classical transmission routing component, wherein the QKD linking apparatus is located in a distributed unit of the radio access network.

27. The QKD linking apparatus as claimed in claim 26, wherein the radio access network is based on at least one or more radio access network standards of 3G, 4G, 5G, 6G and/or beyond type standards and/or equivalent radio network/telecommunication standards.

28. The QKD linking apparatus as claimed in claim 26 or 27, wherein the radio access network is a 5G radio access network.

29. The QKD linking apparatus as claimed in any of claims 26 to 28, wherein the radio access network is configured to using the QKD linking apparatus and appropriate QKD protocols for exchanging QKD keys, group keys and the like between the nodes, entities, network nodes/entities, components of

the centralised unit, distributed unit and/or radio masts/radio units for forming part of a QKD network and/or thus enable quantum-safe or secure communications therebetween.

30. The QKD linking apparatus as claimed in any of claims 1 to 22, further comprising a satellite and a plurality of endpoint devices and corresponding QKD links, said each QKD link connected between said each endpoint device and said quantum communication component and said classical transmission routing component, wherein the QKD linking apparatus is located in the satellite.

31. The QKD linking apparatus as claimed in claim 30, wherein each of said QKD links comprises a optical free-space channel for the quantum channel and a satellite communication channel for the classical channel.

32. The QKD linking apparatus as claimed in claim 30 or 31, wherein each of the plurality of endpoint devices comprises an optical telescope and/or optical transceiver.

33. The QKD linking apparatus as claimed in any of claims 30 to 32, wherein the satellite is configured to using the QKD linking apparatus and appropriate QKD protocols for exchanging QKD keys, group keys and the like between the endpoint devices and/or other endpoint devices along the orbital path of the satellite for forming at least part of a QKD network and/or thus enable quantum-safe or secure communications therebetween.

34. The QKD linking apparatus as claimed in any of claims 1 to 22, further comprising an ground station endpoint device with the QKD linking apparatus located therein, the ground station endpoint device comprising one or more optical transmitters and/or optical receiver telescopes, the ground station endpoint device configured to service a plurality of satellites and/or other endpoint devices over corresponding QKD links assigned thereto, said each QKD link connected between said each satellite or endpoint device and said quantum communication component and said classical transmission routing component of the QKD linking apparatus of the ground station endpoint device.

35. The QKD linking apparatus as claimed in claim 34, wherein each of the plurality of satellites comprises an optical telescope and/or optical transceiver and a satellite transceiver for use over their corresponding QKD link.

36. The QKD linking apparatus as claimed in claim 34 or 35, wherein the other endpoint devices connect with the QKD linking apparatus over optical fibre connection and the like.

37. The QKD linking apparatus as claimed in any of claims 34 to 36, wherein the ground station endpoint device is configured to using the QKD linking apparatus and appropriate QKD protocols for exchanging QKD keys, group keys and the like between the satellites and/or other endpoint devices for forming part of a QKD network and/or thus enable quantum-safe or secure communications therebetween.

38. The QKD linking apparatus as claimed in any of claims 1 to 37, wherein the QKD linking apparatus is an untrusted node and the QKD protocols performed by said QKD linking apparatus and said two or more endpoint devices are configured to ensure the QKD linking apparatus cannot derive the resulting QKD keys or keys exchanged output from the QKD protocols and used for securing communications between the two or more endpoint devices.

39. The QKD linking apparatus as claimed in any of claims 1 to 38, wherein the QKD protocol(s) may include one or more from the group of:

a QKD protocol from the Bennett and Brassard 1984, BB84, family of QKD protocols;

the BB84 QKD protocol;modified versions of the BB84 protocol configured to ensure the QKD linking apparatus is unable to derive the resulting exchanged QKD keys between the endpoint devices;

the Bennet 1992, B92, QKD protocol;

the Six-State Protocol, SSP, QKD protocol;

the Scarani Acin Ribordy Gisin 2004, SARG04, QKD protocol;

the Doherty Parrilo Spedalieri 2002, DPS02, QKD protocol;

the differential phase shift, DPS, QKD protocol;

the Eckert 1991, E91, QKD protocol;

the coherent one-way, COW, QKD protocol;

the Khan Murphy Beige 2009, KMB09, QKD protocol;

the Esteban Serna 2009, S09, QKD protocol;

the Serna 2013, S13, QKD protocol;

the A Abushgra K Elleithy 2015, AK15, QKD protocol;

any one or more other entanglement based QKD protocols;

any one or more future QKD protocols; and

any other suitable QKD protocol for exchanging QKD keys between endpoint devices using quantum transmissions and classical transmissions.

40. The QKD linking apparatus as claimed in any of claims 1 to 39, wherein the quantum transmissions to each endpoint device of two or more endpoint devices performing a QKD protocol for exchanging a QKD key therebetween may be performed simultaneously each quantum transmission using a different quantum transmitter assigned to said each endpoint device.

41. The QKD linking apparatus as claimed in any of claims 1 to 39, wherein the quantum transmissions to each endpoint device of two or more endpoint devices performing a QKD protocol for exchanging a QKD key therebetween may be performed sequentially using a different quantum transmitter assigned to said each endpoint device, wherein the controller directs the quantum communication component to route or switch the next quantum transmission for an endpoint device to the corresponding quantum transmitter assigned to said endpoint device for transmission over the quantum channel of the QKD link of said endpoint device when the previous or current quantum transmission for another endpoint device has completed.

42. The QKD linking apparatus as claimed in any of claims 1 to 41, wherein the quantum communication component includes a plurality of quantum receivers coupled to the quantum channel of corresponding QKD links of endpoint devices, wherein quantum transmissions received from each endpoint device of two or more endpoint devices performing a QKD protocol for exchanging a QKD key therebetween may be performed simultaneously, each reception of a quantum transmission using a different quantum receiver assigned to said each endpoint device.

43. The QKD linking apparatus as claimed in any of claims 1 to 42, wherein the quantum communication component includes a plurality of quantum receivers coupled to the quantum channel of corresponding QKD links of endpoint devices, and wherein the quantum transmissions from each endpoint device of two or more endpoint devices performing a QKD protocol for exchanging a QKD key therebetween may be performed sequentially using a different quantum receiver assigned to said each endpoint device, wherein the controller directs the quantum communication component to route or switch the next expected quantum transmission from an endpoint device to the corresponding quantum receiver assigned to said endpoint device for reception of the quantum transmission over the quantum channel of the QKD link from said endpoint device when the previous or current quantum transmission from another endpoint device has completed.

44. The QKD linking apparatus as claimed in any of claims 1 to 43, further comprising a random number generator for generating random quantum bits or keys for quantum transmission.

45. The QKD linking apparatus as claimed in claim 44, wherein the QKD linking apparatus further deletes a generated random set of quantum bits or key once it has been transmitted to an endpoint device using quantum transmissions.

46. The QKD linking apparatus as claimed in any of claims 1 to 45, wherein each quantum transmitter of the quantum communication component further comprises a faint pulse source, FPS, unit

with optical switches for generating the photons in an integrated package with a plurality of matched laser diodes for coupling to the optical fibre of a QKD link.

47. A computer-implemented method for controlling a quantum key distributed, QKD, linking apparatus for use in linking at least two endpoint devices in a QKD network, the QKD linking apparatus comprising:

a plurality of QKD links, each QKD link having a communication medium comprising a quantum channel and a classical channel, wherein each endpoint is assigned a QKD link connecting said each endpoint to the QKD linking apparatus;

a quantum communication component comprising a plurality of quantum receivers, each quantum receiver configured for receiving quantum transmissions over a quantum channel of one of the QKD links;

a classical transceiver component comprising a plurality of classical transceivers, each classical transceiver configured for transmitting classical data over a classical channel of one of the QKD links and configured for receiving classical data over the classical channel of said one of the QKD links; and

wherein the method further comprising:

routing or switching data generated for quantum transmission from an endpoint via a quantum receiver assigned to the endpoint over a quantum channel of the QKD link of the endpoint;

routing or switching classical data for classical transmission to an endpoint via a classical transceiver assigned to the endpoint over a classical channel of the QKD link of the endpoint; and

routing or switching classical data received by a classical transceiver over the classical channel of the QKD link of an endpoint as required;

the quantum communication component further comprising a plurality of quantum transmitters, each quantum transmitter configured for transmitting quantum transmissions over a quantum channel of one of the QKD links, wherein one or more of the QKD links has a dedicated quantum transmitter from the quantum communication component and a dedicated classical transceiver from the classical transceiver component for use over the quantum channel and classical channel of the QKD link, wherein the controller is further configured to route or switch data generated for quantum transmission to an endpoint device by the quantum transmitter over the quantum channel of the QKD link of the endpoint device assigned to the quantum transmitter;

the computer-implemented method further comprising performing a QKD protocol between a first endpoint device and a second endpoint device, by:

routing or switching a first set of random bits or keys output from a random number generator for quantum transmission to the first endpoint device over a quantum channel of the QKD link of the first endpoint device via a quantum transmitter assigned to the first endpoint device, wherein the first endpoint device uses a first quantum receiving basis for receiving the quantum transmission of the first set of random bits or keys;

routing or switching an indication of the first set of random bits or keys validly received by the first endpoint device received over the classical channel of the QKD link of the first endpoint device by a classical transceiver assigned to the first endpoint device;

routing or switching data representative of the first quantum transmission basis used for transmitting the first set of random bits or keys over a classical channel of the QKD link of the first endpoint device via the classical transceiver assigned to the first endpoint device;

determining a first intermediate set of symbols associated with the QKD linking apparatus based on discarding those first set of random bits or keys that do not correspond to the received indication of the first set of random bits or keys validly received by the first endpoint device;

routing or switching a second set of random bits or keys output from the random number generator for quantum transmission to the second endpoint device over a quantum channel of the QKD link of the second endpoint device via a quantum transmitter assigned to the second endpoint device, wherein the second endpoint device uses a second quantum receiving basis for receiving the quantum transmission of the second set of random bits or keys;

routing or switching an indication of the second set of random bits or keys validly received by the second endpoint device received from the second endpoint device over the classical channel of the QKD link of the second endpoint via a classical transceiver assigned to the second endpoint device;

routing or switching data representative of the second quantum transmission basis used for transmitting the second set of random bits or keys for classical transmission over a classical channel of the QKD link of the second endpoint device via the classical transceiver assigned to the second endpoint device;

determining a second intermediate set of symbols associated with the QKD linking apparatus based on discarding those second set of random bits or keys that do not correspond to the received indication of the second set of random bits or keys validly received by the second endpoint device;

generating an encrypted first intermediate set of symbols using the second intermediate set of symbols;

routing or switching the encrypted first intermediate set of symbols over the classical channel of the QKD link of the second endpoint via the classical transceiver assigned to the second endpoint device, wherein the second endpoint device decrypts the encrypted first intermediate set of symbols based on deriving the second intermediate set of symbols associated with the QKD linking apparatus from the received second quantum transmission basis and the second quantum receiving basis;

routing or switching data representative of the first quantum transmission basis and the first quantum receiving basis received from the first endpoint device for classical transmission

over a classical channel of the QKD link of the second endpoint device via the classical transceiver assigned to the second endpoint device;

routing or switching data representative of the second quantum transmission basis and the second quantum receiving basis received from the second endpoint device for classical transmission over a classical channel of the QKD link of the first endpoint device via the classical transceiver assigned to the first endpoint device, wherein the first endpoint device determines a first shared key based on discarding all bits from the received first set of random bits except those bits where the first transmission basis equals the first receiving basis and the second transmission basis equals the second receiving basis, and the second endpoint device determines a second shared key based on discarding all bits from the decrypted first intermediate set of symbols except those bits where the first transmission basis equals the first receiving basis and the second transmission basis equals the second receiving basis;

routing or switching data representative of error correction and/or privacy amplification in relation to the first and second shared keys over the classical channels of the QKD links of the first and second endpoint devices, wherein the first and second devices determine a final shared key based on the first and second shared keys.

48. A computer-implemented method for controlling a quantum key distributed, QKD, linking apparatus for use in linking at least two endpoint devices in a QKD network, the QKD linking apparatus comprising:

a plurality of QKD links, each QKD link having a communication medium comprising a quantum channel and a classical channel, wherein each endpoint is assigned a QKD link connecting said each endpoint to the QKD linking apparatus;

a quantum communication component comprising a plurality of quantum receivers, each quantum receiver configured for receiving quantum transmissions over a quantum channel of one of the QKD links;

a classical transceiver component comprising a plurality of classical transceivers, each classical transceiver configured for transmitting classical data over a classical channel of one of the QKD links and configured for receiving classical data over the classical channel of said one of the QKD links; and

wherein the method further comprising:

routing or switching data generated for quantum transmission from an endpoint via a quantum receiver assigned to the endpoint over a quantum channel of the QKD link of the endpoint;

routing or switching classical data for classical transmission to an endpoint via a classical transceiver assigned to the endpoint over a classical channel of the QKD link of the endpoint; and

routing or switching classical data received by a classical transceiver over the classical channel of the QKD link of an endpoint as required;

the quantum communication component further comprising a plurality of quantum transmitters, each quantum transmitter configured for transmitting quantum transmissions over a quantum channel of one of the QKD links, wherein one or more of the QKD links has a dedicated quantum transmitter from the quantum communication component and a dedicated classical transceiver from the classical transceiver component for use over the quantum channel and classical channel of the QKD link, wherein the controller is further configured to route or switch data generated for quantum transmission to an endpoint device by the quantum transmitter over the quantum channel of the QKD link of the endpoint device assigned to the quantum transmitter;

the computer-implemented method further comprising performing a QKD protocol between a first endpoint device and a second endpoint device, by:

routing or switching a first set of random bits or keys received by a quantum receiver assigned to the first endpoint device from quantum transmissions from the first endpoint device over a quantum channel of the QKD link of the first endpoint device, wherein the quantum receiver uses a first quantum receiving basis for receiving the quantum transmission of the first set of random bits or keys and the first endpoint device uses a first quantum transmission basis for transmitting the quantum transmission of the first set of random bits or keys;

routing or switching an indication of the first set of random bits or keys validly received by the quantum receiver to the first endpoint device over the classical channel of the QKD link of the first endpoint device by a classical transceiver assigned to the first endpoint device;

routing or switching data representative of the first quantum receiving basis used for receiving the first set of random bits or keys to the first endpoint device over a classical channel of the QKD link of the first endpoint device via the classical transceiver assigned to the first endpoint device;

determining a first intermediate set of symbols associated with the QKD linking apparatus based on discarding those first set of random bits or keys that were not validly received by the quantum receiver assigned to the first endpoint device;

routing or switching a second set of random bits or keys received by a quantum receiver assigned to the second endpoint device from quantum transmissions from the second endpoint device over a quantum channel of the QKD link of the second endpoint device, wherein the quantum receiver uses a second quantum receiving basis for receiving the quantum transmission of the second set of random bits or keys and the second endpoint device uses a second quantum transmission basis for transmitting the quantum transmission of the second set of random bits or keys;

routing or switching an indication of the second set of random bits or keys validly received by the quantum receiver to the second endpoint device over the classical channel of the QKD link of the second endpoint device by a classical transceiver assigned to the second endpoint device;

routing or switching data representative of the second quantum receiving basis used for receiving the second set of random bits or keys to the second endpoint device over a classical channel of the QKD link of the second endpoint device via the classical transceiver assigned to the second endpoint device;

determining a second intermediate set of symbols associated with the QKD linking apparatus based on discarding those second set of random bits or keys that were not validly received by the quantum receiver assigned to the second endpoint device;

generating an encrypted first intermediate set of symbols using the second intermediate set of symbols;

routing or switching the encrypted first intermediate set of symbols over the classical channel of the QKD link of the second endpoint via the classical transceiver assigned to the second endpoint device, wherein the second endpoint device decrypts the encrypted first intermediate set of symbols based on deriving the second intermediate set of symbols associated with the QKD linking apparatus from the received second quantum transmission basis and the second quantum receiving basis;

routing or switching data representative of the first quantum transmission basis and the first quantum receiving basis received from the first endpoint device for classical transmission over a classical channel of the QKD link of the second endpoint device via the classical transceiver assigned to the second endpoint device;

routing or switching data representative of the second quantum transmission basis and the second quantum receiving basis received from the second endpoint device for classical transmission over a classical channel of the QKD link of the first endpoint device via the classical transceiver assigned to the first endpoint device, wherein the first endpoint device determines a first shared key based on discarding all bits from the received first set of random bits except those bits where the first transmission basis equals the first receiving basis and the second transmission basis equals the second receiving basis, and the second endpoint device determines a second shared key based on discarding all bits from the decrypted first intermediate set of symbols except those bits where the first transmission basis equals the first receiving basis and the second transmission basis equals the second receiving basis;

routing or switching representative of error correction and/or privacy amplification in relation to the first and second shared keys over the classical channels of the QKD links of the first and second endpoint devices, wherein the first and second devices determine a final shared key based on the first and second shared keys.

49. A computer-implemented method for controlling a quantum key distributed, QKD, linking apparatus for use in linking at least two endpoint devices in a QKD network, the QKD linking apparatus comprising:

a plurality of QKD links, each QKD link having a communication medium comprising a quantum channel and a classical channel, wherein each endpoint is assigned a QKD link connecting said each endpoint to the QKD linking apparatus;

a quantum communication component comprising a plurality of quantum receivers, each quantum receiver configured for receiving quantum transmissions over a quantum channel of one of the QKD links;

a classical transceiver component comprising a plurality of classical transceivers, each classical transceiver configured for transmitting classical data over a classical channel of one of the QKD links and configured for receiving classical data over the classical channel of said one of the QKD links; and

wherein the method further comprising:

routing or switching data generated for quantum transmission from an endpoint via a quantum receiver assigned to the endpoint over a quantum channel of the QKD link of the endpoint;

routing or switching classical data for classical transmission to an endpoint via a classical transceiver assigned to the endpoint over a classical channel of the QKD link of the endpoint; and

routing or switching classical data received by a classical transceiver over the classical channel of the QKD link of an endpoint as required;

the quantum communication component further comprising a plurality of quantum transmitters, each quantum transmitter configured for transmitting quantum transmissions over a quantum channel of one of the QKD links, wherein one or more of the QKD links has a dedicated quantum transmitter from the quantum communication component and a dedicated classical transceiver from the classical transceiver component for use over the quantum channel and classical channel of the QKD link, wherein the controller is further configured to route or switch data generated for quantum transmission to an endpoint device by the quantum transmitter over the quantum channel of the QKD link of the endpoint device assigned to the quantum transmitter;

the computer-implemented method further comprising performing a QKD protocol between a first endpoint device and a second endpoint device, by:

routing or switching a first set of random bits or keys received by a quantum receiver assigned to the first endpoint device from quantum transmissions from the first endpoint device over a quantum channel of the QKD link of the first endpoint device, wherein the quantum receiver uses a first quantum receiving basis for receiving the quantum transmission of the first set of random bits or keys and the first endpoint device uses a first quantum transmission basis for transmitting the quantum transmission of the first set of random bits or keys;

routing or switching an indication of the first set of random bits or keys validly received by the quantum receiver to the first endpoint device over the classical channel of the QKD link of the first endpoint device by a classical transceiver assigned to the first endpoint device;

routing or switching data representative of the first quantum receiving basis used for receiving the first set of random bits or keys to the first endpoint device over a classical channel of the QKD link of the first endpoint device via the classical transceiver assigned to the first endpoint device;

determining a first intermediate set of symbols associated with the QKD linking apparatus based on discarding those first set of random bits or keys that were not validly received by the quantum receiver assigned to the first endpoint device;

routing or switching a second set of random bits or keys output from a random number generator for quantum transmission to the second endpoint device over a quantum channel of the QKD link of the second endpoint device via a quantum transmitter assigned to the second endpoint device, wherein the second endpoint device uses a second quantum receiving basis for receiving the quantum transmission of the second set of random bits or keys;

routing or switching an indication of the second set of random bits or keys validly received by the second endpoint device received from the second endpoint device over the classical channel of the QKD link of the second endpoint via a classical transceiver assigned to the second endpoint device;

routing or switching data representative of the second quantum transmission basis used for transmitting the second set of random bits or keys for classical transmission over a classical channel of the QKD link of the second endpoint device via the classical transceiver assigned to the second endpoint device;

determining a second intermediate set of symbols associated with the QKD linking apparatus based on discarding those second set of random bits or keys that do not correspond to the received indication of the second set of random bits or keys validly received by the second endpoint device;

generating an encrypted first intermediate set of symbols using the second intermediate set of symbols;

routing or switching the encrypted first intermediate set of symbols over the classical channel of the QKD link of the second endpoint via the classical transceiver assigned to the second endpoint device, wherein the second endpoint device decrypts the encrypted first intermediate set of symbols based on deriving the second intermediate set of symbols associated with the QKD linking apparatus from the received second quantum transmission basis and the second quantum receiving basis;

routing or switching data representative of the first quantum transmission basis and the first quantum receiving basis received from the first endpoint device for classical transmission over a classical channel of the QKD link of the second endpoint device via the classical transceiver assigned to the second endpoint device;

routing or switching data representative of the second quantum transmission basis and the second quantum receiving basis received from the second endpoint device for classical transmission over a classical channel of the QKD link of the first endpoint device via the classical transceiver assigned to the first endpoint device, wherein the first endpoint device determines a first shared key based on discarding all bits from the received first set of random bits except those bits where the first transmission

basis equals the first receiving basis and the second transmission basis equals the second receiving basis, and the second endpoint device determines a second shared key based on discarding all bits from the decrypted first intermediate set of symbols except those bits where the first transmission basis equals the first receiving basis and the second transmission basis equals the second receiving basis;

routing or switching data representative of error correction and/or privacy amplification in relation to the first and second shared keys over the classical channels of the QKD links of the first and second endpoint devices, wherein the first and second devices determine a final shared key based on the first and second shared keys.

50. A computer-implemented method for controlling a quantum key distributed, QKD, linking apparatus for use in linking at least two endpoint devices in a QKD network, the QKD linking apparatus comprising:

a plurality of QKD links, each QKD link having a communication medium comprising a quantum channel and a classical channel, wherein each endpoint is assigned a QKD link connecting said each endpoint to the QKD linking apparatus;

a quantum communication component comprising a plurality of quantum receivers, each quantum receiver configured for receiving quantum transmissions over a quantum channel of one of the QKD links;

a classical transceiver component comprising a plurality of classical transceivers, each classical transceiver configured for transmitting classical data over a classical channel of one of the QKD links and configured for receiving classical data over the classical channel of said one of the QKD links; and

wherein the method further comprising:

routing or switching data generated for quantum transmission from an endpoint via a quantum receiver assigned to the endpoint over a quantum channel of the QKD link of the endpoint;

routing or switching classical data for classical transmission to an endpoint via a classical transceiver assigned to the endpoint over a classical channel of the QKD link of the endpoint; and

routing or switching classical data received by a classical transceiver over the classical channel of the QKD link of an endpoint as required;

the quantum communication component further comprising a plurality of quantum transmitters, each quantum transmitter configured for transmitting quantum transmissions over a quantum channel of one of the QKD links, wherein one or more of the QKD links has a dedicated quantum transmitter from the quantum communication component and a dedicated classical transceiver from the classical transceiver component for use over the quantum channel and classical channel of the QKD link, wherein the controller is further configured to route or switch data generated for quantum transmission to an endpoint device by the quantum transmitter over the quantum channel of the QKD link of the endpoint device assigned to the quantum transmitter;

the computer-implemented method performing a QKD protocol between a first endpoint device and a second endpoint device via a QKD linking apparatus by:

sending, from the QKD linking apparatus to the first endpoint device, a first set of random bits or keys output from a random number generator for quantum transmission to the first endpoint device over a quantum channel of the QKD link of the first endpoint device, wherein the first endpoint device uses a first quantum receiving basis for receiving the quantum transmission of the first set of random bits or keys;

receiving, from the first endpoint device, an indication of the first set of random bits or keys validly received by the first endpoint device over a classical channel of the QKD link of the first endpoint device;

sending, from the QKD linking apparatus to the first endpoint device, data representative of the first quantum transmission basis used for transmitting the first set of random bits or keys over a classical channel of the QKD link of the first endpoint device;

determining a first intermediate set of symbols associated with the QKD linking apparatus based on discarding those first set of random bits or keys that do not correspond to the received indication of the first set of random bits or keys validly received by the first endpoint device;

sending, from the QKD linking apparatus to the second endpoint device, a second set of random bits or keys output from the random number generator for quantum transmission to the second endpoint device over a quantum channel of the QKD link of the second endpoint device, wherein the second endpoint device uses a second quantum receiving basis for receiving the quantum transmission of the second set of random bits or keys;

receiving, from the second endpoint device, an indication of the second set of random bits or keys validly received by the second endpoint device over the classical channel of the QKD link of the second endpoint;

sending, to the second endpoint device, data representative of the second quantum transmission basis used for transmitting the second set of random bits or keys over a classical channel of the QKD link of the second endpoint device via the classical transceiver assigned to the second endpoint device;

determining a second intermediate set of symbols associated with the QKD linking apparatus based on discarding those second set of random bits or keys that do not correspond to the received indication of the second set of random bits or keys validly received by the second endpoint device;

generating an encrypted first intermediate set of symbols using the second intermediate set of symbols;

sending, to the second endpoint device, the encrypted first intermediate set of symbols over the classical channel of the QKD link of the second endpoint, wherein the second endpoint device decrypts the encrypted first intermediate set of symbols based on deriving the second

intermediate set of symbols associated with the QKD linking apparatus from the received second quantum transmission basis and the second quantum receiving basis;

receiving, from the first endpoint device, data representative of the first quantum transmission basis and the first quantum receiving basis over the classical channel of the QKD link of the first endpoint device;

sending, to the second endpoint device, data representative of the first quantum transmission basis and the first quantum receiving basis over the classical channel of the QKD link of the second endpoint device;

receiving, from the second endpoint device, data representative of the second quantum transmission basis and the second quantum receiving basis over the classical channel of the QKD link of the second endpoint device;

sending, to the first endpoint device, data representative of the second quantum transmission basis and the second quantum receiving basis over the classical channel of the QKD link of the first endpoint device, wherein the first endpoint device determines a first shared key based on discarding all bits from the received first set of random bits except those bits where the first transmission basis equals the first receiving basis and the second transmission basis equals the second receiving basis, and the second endpoint device determines a second shared key based on discarding all bits from the decrypted first intermediate set of symbols except those bits where the first transmission basis equals the first receiving basis and the second transmission basis equals the second receiving basis;

sending, between the first and second endpoint devices, data representative of error correction and/or privacy amplification in relation to the first and second shared keys over the classical channels of the QKD links of the first and second endpoint devices, wherein the first and second devices determine a final shared key based on the error correction and/or privacy amplification in relation to the first and second shared keys.

51. A computer-implemented method for controlling a quantum key distributed, QKD, linking apparatus for use in linking at least two endpoint devices in a QKD network, the QKD linking apparatus comprising:

a plurality of QKD links, each QKD link having a communication medium comprising a quantum channel and a classical channel, wherein each endpoint is assigned a QKD link connecting said each endpoint to the QKD linking apparatus;

a quantum communication component comprising a plurality of quantum receivers, each quantum receiver configured for receiving quantum transmissions over a quantum channel of one of the QKD links;

a classical transceiver component comprising a plurality of classical transceivers, each classical transceiver configured for transmitting classical data over a classical channel of one of the QKD links and configured for receiving classical data over the classical channel of said one of the QKD links; and

wherein the method further comprising:

routing or switching data generated for quantum transmission from an endpoint via a quantum receiver assigned to the endpoint over a quantum channel of the QKD link of the endpoint;

routing or switching classical data for classical transmission to an endpoint via a classical transceiver assigned to the endpoint over a classical channel of the QKD link of the endpoint; and

routing or switching classical data received by a classical transceiver over the classical channel of the QKD link of an endpoint as required;

the quantum communication component further comprising a plurality of quantum transmitters, each quantum transmitter configured for transmitting quantum transmissions over a quantum channel of one of the QKD links, wherein one or more of the QKD links has a dedicated quantum transmitter from the quantum communication component and a dedicated classical transceiver from the classical transceiver component for use over the quantum channel and classical channel of the QKD link, wherein the controller is further configured to route or switch data generated for quantum transmission to an endpoint device by the quantum transmitter over the quantum channel of the QKD link of the endpoint device assigned to the quantum transmitter;

the computer-implemented method performing a QKD protocol between a first endpoint device and a second endpoint device via a QKD linking apparatus, by:

receiving, from the first endpoint device, a first set of random bits or keys from quantum transmissions of the first endpoint device over a quantum channel of the QKD link of the first endpoint device, wherein a first quantum receiving basis is used for receiving the quantum transmission of the first set of random bits or keys and the first endpoint device uses a first quantum transmission basis for transmitting the quantum transmission of the first set of random bits or keys;

sending, to the first endpoint device, an indication of the first set of random bits or keys validly received over the classical channel of the QKD link of the first endpoint device;

sending, to the first endpoint device, data representative of the first quantum receiving basis used for receiving the first set of random bits or keys over a classical channel of the QKD link of the first endpoint device;

determining a first intermediate set of symbols associated with the QKD linking apparatus based on discarding those first set of random bits or keys that were not validly received by the quantum receiver assigned to the first endpoint device;

receiving, from the second endpoint device, a second set of random bits or keys from quantum transmission of the second endpoint device over a quantum channel of the QKD link of the second endpoint device, wherein a second quantum receiving basis is used for receiving the quantum transmission of the second set of random bits or keys and the second endpoint device

uses a second quantum transmission basis for transmitting the quantum transmission of the second set of random bits or keys;

sending, to the second endpoint device, an indication of the second set of random bits or keys validly received over the classical channel of the QKD link of the second endpoint device;

sending, to the second endpoint device, data representative of the second quantum receiving basis used for receiving the second set of random bits or keys over a classical channel of the QKD link of the second endpoint device;

determining a second intermediate set of symbols associated with the QKD linking apparatus based on discarding those second set of random bits or keys that were not validly received by the quantum receiver assigned to the second endpoint device;

generating an encrypted first intermediate set of symbols using the second intermediate set of symbols;

sending, to the second endpoint device, the encrypted first intermediate set of symbols over the classical channel of the QKD link of the second endpoint, wherein the second endpoint device decrypts the encrypted first intermediate set of symbols based on deriving the second intermediate set of symbols associated with the QKD linking apparatus from the received second quantum transmission basis and the second quantum receiving basis;

receiving, from the first endpoint device, data representative of the first quantum transmission basis and the first quantum receiving basis over the classical channel of the QKD link of the first endpoint device;

sending, to the second endpoint device, data representative of the first quantum transmission basis and the first quantum receiving basis over the classical channel of the QKD link of the second endpoint device;

receiving, from the second endpoint device, data representative of the second quantum transmission basis and the second quantum receiving basis over the classical channel of the QKD link of the second endpoint device;

sending, to the first endpoint device, data representative of the second quantum transmission basis and the second quantum receiving basis over the classical channel of the QKD link of the first endpoint device, wherein the first endpoint device determines a first shared key based on discarding all bits from the received first set of random bits except those bits where the first transmission basis equals the first receiving basis and the second transmission basis equals the second receiving basis, and the second endpoint device determines a second shared key based on discarding all bits from the decrypted first intermediate set of symbols except those bits where the first transmission basis equals the first receiving basis and the second transmission basis equals the second receiving basis;

sending, between the first and second endpoint devices, data representative of error correction and/or privacy amplification in relation to the first and second shared keys over the

classical channels of the QKD links of the first and second endpoint devices, wherein the first and second devices determine a final shared key based on the error correction and/or privacy amplification in relation to the first and second shared keys.

52. A computer-implemented method for controlling a quantum key distributed, QKD, linking apparatus for use in linking at least two endpoint devices in a QKD network, the QKD linking apparatus comprising:

a plurality of QKD links, each QKD link having a communication medium comprising a quantum channel and a classical channel, wherein each endpoint is assigned a QKD link connecting said each endpoint to the QKD linking apparatus;

a quantum communication component comprising a plurality of quantum receivers, each quantum receiver configured for receiving quantum transmissions over a quantum channel of one of the QKD links;

a classical transceiver component comprising a plurality of classical transceivers, each classical transceiver configured for transmitting classical data over a classical channel of one of the QKD links and configured for receiving classical data over the classical channel of said one of the QKD links; and

wherein the method further comprising:

routing or switching data generated for quantum transmission from an endpoint via a quantum receiver assigned to the endpoint over a quantum channel of the QKD link of the endpoint;

routing or switching classical data for classical transmission to an endpoint via a classical transceiver assigned to the endpoint over a classical channel of the QKD link of the endpoint; and

routing or switching classical data received by a classical transceiver over the classical channel of the QKD link of an endpoint as required;

the quantum communication component further comprising a plurality of quantum transmitters, each quantum transmitter configured for transmitting quantum transmissions over a quantum channel of one of the QKD links, wherein one or more of the QKD links has a dedicated quantum transmitter from the quantum communication component and a dedicated classical transceiver from the classical transceiver component for use over the quantum channel and classical channel of the QKD link, wherein the controller is further configured to route or switch data generated for quantum transmission to an endpoint device by the quantum transmitter over the quantum channel of the QKD link of the endpoint device assigned to the quantum transmitter;

the computer-implemented method performing a QKD protocol between a first endpoint device and a second endpoint device via a QKD linking apparatus by:

receiving, from the first endpoint device, a first set of random bits or keys from quantum transmissions of the first endpoint device over a quantum channel of the QKD link of the first endpoint device, wherein a first quantum receiving basis is used for receiving the quantum transmission of the first set of random bits or keys and the first endpoint device uses a first

quantum transmission basis for transmitting the quantum transmission of the first set of random bits or keys;

sending, to the first endpoint device, an indication of the first set of random bits or keys validly received over the classical channel of the QKD link of the first endpoint device;

sending, to the first endpoint device, data representative of the first quantum receiving basis used for receiving the first set of random bits or keys over a classical channel of the QKD link of the first endpoint device;

determining a first intermediate set of symbols associated with the QKD linking apparatus based on discarding those first set of random bits or keys that were not validly received by the quantum receiver assigned to the first endpoint device;

sending, from the QKD linking apparatus to the second endpoint device, a second set of random bits or keys output from the random number generator for quantum transmission to the second endpoint device over a quantum channel of the QKD link of the second endpoint device, wherein the second endpoint device uses a second quantum receiving basis for receiving the quantum transmission of the second set of random bits or keys;

receiving, from the second endpoint device, an indication of the second set of random bits or keys validly received by the second endpoint device over the classical channel of the QKD link of the second endpoint device;

sending, to the second endpoint device, data representative of the second quantum transmission basis used for transmitting the second set of random bits or keys over a classical channel of the QKD link of the second endpoint device via the classical transceiver assigned to the second endpoint device;

determining a second intermediate set of symbols associated with the QKD linking apparatus based on discarding those second set of random bits or keys that do not correspond to the received indication of the second set of random bits or keys validly received by the second endpoint device;

generating an encrypted first partial key using the second partial key;

sending, to the second endpoint device, the encrypted first partial key over the classical channel of the QKD link of the second endpoint, wherein the second endpoint device decrypts the encrypted first intermediate set of symbols based on deriving the second intermediate set of symbols associated with the QKD linking apparatus from the received second quantum transmission basis and the second quantum receiving basis;

receiving, from the first endpoint device, data representative of the first quantum transmission basis and the first quantum receiving basis over the classical channel of the QKD link of the first endpoint device;

sending, to the second endpoint device, data representative of the first quantum transmission basis and the first quantum receiving basis over the classical channel of the QKD link of the second endpoint device;

receiving, from the second endpoint device, data representative of the second quantum transmission basis and the second quantum receiving basis over the classical channel of the QKD link of the second endpoint device;

sending, to the first endpoint device, data representative of the second quantum transmission basis and the second quantum receiving basis over the classical channel of the QKD link of the first endpoint device, wherein the first endpoint device determines a first shared key based on discarding all bits from the received first set of random bits except those bits where the first transmission basis equals the first receiving basis and the second transmission basis equals the second receiving basis, and the second endpoint device determines a second shared key based on discarding all bits from the decrypted first intermediate set of symbols except those bits where the first transmission basis equals the first receiving basis and the second transmission basis equals the second receiving basis;

sending, between the first and second endpoint devices, data representative of error correction and/or privacy amplification in relation to the first and second shared keys over the classical channels of the QKD links of the first and second endpoint devices, wherein the first and second devices determine a final shared key based on the error correction and/or privacy amplification in relation to the first and second shared keys.

53. The computer-implemented method as claimed in any one of claims 47 to 52, further comprising:

assigning an available quantum transmitter to an endpoint device for use over the QKD link of the endpoint device; and

when implementing one of the QKD protocols between two or more endpoint devices each with an assigned quantum transmitters, directing the quantum communication component to route or switch quantum transmissions for an endpoint device of the two or more endpoint devices to the quantum transmitter assigned to said endpoint device for transmitting said quantum transmissions over the quantum channel of the QKD link of the endpoint device.

54. The computer-implemented method as claimed in any of claims 47 to 53, further comprising

assigning an available classical transceiver to an endpoint device for use over the QKD link of the endpoint device;

when implementing one of the QKD protocols between two or more endpoint devices each with an assigned classical transceiver, directing the classical transmission and routing component to route or switch classical data for an endpoint device of the two or more endpoint devices to the classical

transceiver assigned to said endpoint device to the classical channel of the QKD link of the endpoint device.

55. The computer-implemented method as claimed in any of claims 47 to 54, when one of the QKD protocols are being performed between the QKD linking apparatus and at least two of the endpoint devices is complete, the method further comprising, for the two or more endpoint devices, directing the classical transmission and routing component to route or switch secure communications between the classical transceivers assigned to each of the endpoint devices over the corresponding classical channels of the QKD links of said endpoint devices, said communications being secured based on the keys exchanged using the QKD protocol between the two or more endpoint devices.

56. The computer-implemented method as claimed in any of claims 47 to 54, further comprising one or more method steps performed by the QKD linking apparatus according to any of claims 1 to 46.

57. A system comprising:

an QKD linking apparatus according to any of claims 1 to 46; and

a plurality of endpoint devices, each endpoint device coupled to the QKD linking apparatus via a QKD link;

wherein the QKD linking apparatus is configured to link two or more of the endpoint devices into a QKD network.

58. A computer-readable medium comprising computer code or instructions stored thereon, which when executed on a processor, causes the processor to perform the computer implemented method according to any of claims 47 to 56.