Claims

1. A computer-implemented method of key exchange between a first endpoint device and a second endpoint device communicatively coupled over communication links via one or more intermediary devices, wherein the first endpoint device is coupled by a first communication link to a first of the one or more intermediary devices, and the second endpoint device and the one or more intermediary devices form a group of devices, wherein each of the one or more intermediary devices is communicatively coupled to at least one other of the one or more intermediary devices via at least one of the communication links and the second endpoint device is coupled to a last of the one or more intermediary devices in the group via a second communication link, the method comprising:

exchanging intermediate key information between the first intermediary device and the first endpoint device based on a first key exchange protocol; and

securely sending data representative of the exchanged intermediate key information from the first intermediary device to the second endpoint device via the intermediary device(s), the secure communications over the communication links of the group of devices based on shared keys exchanged using one or more key exchange protocols over the communication links of the group of devices;

wherein the first and second endpoint devices use a further communication channel therebetween for processing and transforming said intermediate key information into the final shared key.

2. The computer-implemented method as claimed in claim 1, wherein there are N intermediary devices, *N>0*, and the first endpoint device, the *N* intermediary devices and the second endpoint device form a chain, line network or linear array topology with the first endpoint device being communicatively coupled to the second endpoint device via said *N* intermediary devices, wherein the first endpoint device is connected via a first communication link to the first of the *N* intermediary devices in the chain, and the second device is connected via a second communication link to an *N-th* intermediary device in the chain, each of the *N* intermediary devices coupled to an adjacent intermediary device via a further communication link.

3. The computer-implemented method as claimed in any of claims 1 or 2, wherein the first key exchange protocol is configured for detecting eavesdroppers during the exchange of the final shared key.

4. The computer-implemented method as claimed in any of claims 1 to 3, wherein the shared keys for a device are shared keys between said device and any adjacent or neighboring device connected to said device by one of the communication links.

5. The computer-implemented method as claimed in any preceding claim, wherein said each shared key is used for securing the communication of the intermediate key information from one device to next.

6. The computer-implemented method as claimed in claim 5, wherein each intermediary device sends its shared key to the second endpoint device, and only encrypts any incoming communications associated with the intermediate key information with its shared key before forwarding towards the second endpoint device via its nearest neighbour device, wherein the second endpoint device uses the shared keys to decrypt the encrypted intermediate key information.

7. The computer-implemented method as claimed in claim 5, wherein each intermediary device sends its shared key to the second endpoint device, and passes through any incoming communications associated with the intermediate key information via its nearest neighbour device, wherein the second endpoint device uses the shared keys to decrypt the encrypted intermediate key information.

8. The computer-implemented method as claimed in claim 5, wherein each intermediary device cryptographically combines a pair of shared keys exchanged with its nearest neighbour devices, and sends the combined pair of shared keys to the second endpoint device, and the first device cryptographically combining the intermediate key information with a shared key exchanged with an adjacent intermediary device prior to securely communicating the cryptographically combined intermediate key information to the second device, wherein the second endpoint device uses the received cryptographically combined shared keys to decrypt the encrypted or cryptographically combined intermediate key information.

9. The computer-implemented method as claimed in claim 8, wherein cryptographically combining a pair of shared keys comprises performing a one time pad or exclusive OR operation on the pair of shared keys, and cryptographically combining the intermediate key information with a shared key comprises performing a one time pad or exclusive OR operation on the intermediate key information and the shared key.

10. The computer-implemented method as claimed in claim 5, wherein each intermediary device has exchanged a shared key with its nearest neighbour devices using a key exchange protocol, said each intermediary device apart from the first intermediary device having a first and second shared key sends its shared key to the second endpoint device, and only encrypts any incoming communications associated with the intermediate key information with its shared key before forwarding towards the second endpoint device via its nearest neighbour device, wherein the second endpoint device uses the shared keys to decrypt the

encrypted intermediate key information.

11. The computer-implemented method as claimed in any preceding claim, wherein the one or more key exchange protocols used between one or more of the devices in the group of devices for secure communications therebetween are selected from a group of key exchange protocols based on a desired or required trust level in relation to the one or more intermediary devices of the group of devices.

12. The computer-implemented method as claimed in claim 11, wherein when the level of trust is a trust level that is considered an untrusted level, then the one or more key exchange protocols selected include QKD protocols for use in sharing keys with untrusted parties.

13. The computer-implemented method as claimed in any preceding claim, wherein the shared keys for an intermediary device of the one or more intermediary devices of the group of devices are shared keys between said intermediary device and one or more other intermediary devices of the intermediary devices that are adjacent or neighboring the intermediary device in the line network or linear array topology.

14. The computer-implemented method as claimed in any preceding claim, wherein the first communication link includes a first quantum channel and a first classical channel and the first key exchange protocol is a quantum key distribution protocol.

15. The computer-implemented method as claimed in any preceding claim, wherein each of the second communication link and the communication links between the intermediary devices includes a quantum channel and a classical channel and the one or more key exchange protocols is a quantum key distribution protocol different to the first key exchange protocol.

16. The computer-implemented method as claimed in any preceding claim, wherein the first key exchange protocol comprises a key exchange protocol selected 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;

a modified or hybrid-BB84 based version of the BB84 protocol configured in which at least the first device transmits or receives a first set of random symbols over a first quantum channel with the first intermediary device, but withholds the basis set used by the first device for the transmitting or receiving the first set of random symbols over the first quantum channel, wherein the first intermediary device is unable to derive the validly transmitted or

received first set of random symbols by the first device or an exchanged shared key with a second device based on the validly transmitted or received first set of random symbols by the first device;

a modified or hybrid-BB84 based version of the BB84 protocol configured in which at least the first device transmits or receives a first set of random symbols over a first quantum channel with the first intermediary device, but withholds the basis set used by the first device for the transmitting or receiving of the first set of random symbols over the first quantum channel, and at least the second device transmits or receives a second set of random symbols over a second quantum channel with the first intermediary device, but withholds the basis set used by the second device for the transmitting or receiving of the second set of random symbols over the second quantum channel, wherein the intermediary device is unable to derive: the validly transmitted or received first set of random symbols by the first device, the validly transmitted or received second set of random symbols by the second device, and the resulting shared key exchanged between the first and second devices based on the validly transmitted or received first set of random symbols and the validly transmitted or received second set of random symbols;

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.

17. The computer-implemented method as claimed in any preceding claim, wherein exchanging intermediate key information between the first intermediary device and the first endpoint device based on the first key exchange protocol further comprising:

the first key exchange protocol configured for performing at least the steps of:

transmitting or receiving, by the first intermediary device, a first set of random symbols over a first quantum channel with the first endpoint device;

transmitting, from the first intermediary device to the first endpoint device, the basis set used by the first intermediary device for transmitting or receiving the first set of random symbols over the first quantum channel;

generating, by the first intermediary device, first endpoint device intermediate key information comprising data representative of a first intermediate set of symbols based on the validly transmitted or received first set of symbols using the transmitting or receiving basis set used by the first intermediary device when transmitting or receiving the first set of symbols over the first quantum channel;

wherein the first endpoint device withholds the first transmitting or receiving basis set used by the first endpoint device for transmitting or receiving the first set of random symbols over the first quantum channel with the first intermediary device.

18. The computer-implemented method as claimed in claim 17, wherein the first key exchange protocol is a modified or hybrid-BB84 based version of the BB84 protocol.

19. The computer-implemented method as claimed in claim 17 or 18, wherein determining the final shared key, by the first and second endpoint devices, based on the exchanged first endpoint device intermediate key information securely sent via the one or more intermediary devices to the second endpoint device, further comprising:

exchanging, between the first and second endpoint devices over a secure communication channel therebetween, the basis set used by the first endpoint device for transmitting or receiving the first set of random symbols;

determining, by the second endpoint device using the basis set used by the first endpoint device for transmitting or receiving the first set of random symbols and the first endpoint device intermediate key information, a common set of symbols corresponding to at least a portion of the first set of random symbols transmitted or received by the first endpoint device;

exchanging, by the first and second devices over the secure communication channel therebetween, a shared key based on the common set of symbols and the first set of random symbols transmitted or received by the first endpoint device.

20. The computer-implemented method as claimed in any preceding claim, wherein each of the communication links between the group of devices includes a quantum channel and a

classical channel and the one or more key exchange protocols used to exchange the shared keys between the corresponding devices of the group of devices are one or more quantum key distribution protocols.

21. The computer-implemented method as claimed in any of preceding claim, wherein each of the communication links between the one or more intermediary devices includes a quantum channel and a classical channel and the one or more key exchange protocols selected to be used to exchange the shared keys between the corresponding intermediary devices of the one or more intermediary devices are quantum key distribution protocols.

22. The computer-implemented method as claimed in any preceding claim, wherein the one or more key exchange protocols comprises one or more key exchange protocols selected 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;

a modified or hybrid-BB84 based version of the BB84 protocol configured in which at least the first device transmits or receives a first set of random symbols over a first quantum channel with the first intermediary device, but withholds the basis set used by the first device for the transmitting or receiving the first set of random symbols over the first quantum channel, wherein the first intermediary device is unable to derive the validly transmitted or received first set of random symbols by the first device or an exchanged shared key with a second device based on the validly transmitted or received first set of random symbols by the first device;

a modified or hybrid-BB84 based of the BB84 protocol configured in which at least the first device transmits or receives a first set of random symbols over a first quantum channel with the first intermediary device, but withholds the basis set used by the first device for the transmitting or receiving of the first set of random symbols over the first quantum channel, and at least the second device transmits or receives a second set of random symbols over a second quantum channel with the first intermediary device, but withholds the basis set used by the second device for the transmitting or receiving of the second set of random symbols over the second quantum channel, wherein the intermediary device is unable to derive: the validly transmitted or received first set of random symbols by the first device, the validly transmitted or received second set of random symbols by the second device, and the resulting shared key exchanged between the first and second devices based on the validly

transmitted or received first set of random symbols and the validly transmitted or received second set of random symbols;

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.

23. The computer-implemented method as claimed in any preceding claim, wherein the one or more key QKD exchange protocols used between one or more of the devices in the group of devices for secure communications therebetween are selected from a group of key exchange protocols based on a desired or required trust level in relation to the one or more intermediary devices of the group of devices.

24. The computer-implemented method as claimed in claim 23, wherein when the level of trust is a trust level that is considered an untrusted level, then the one or more key exchange protocols selected include QKD protocols for use in sharing keys with untrusted parties.

25. The computer-implemented method as claimed in any preceding claim, wherein the first key exchange protocol and the one or more key exchange protocols are entanglement based QKD protocols, wherein:

exchanging intermediate key information between the first intermediary device and the first endpoint device based on a first key exchange protocol further comprising distributing one or more Einstein–Podolsky–Rosen, EPR, pair(s) between the first intermediary device and the first endpoint device;

distributing one or more EPR pair(s) between each of the one or more intermediary devices;

distributing one or more EPR pair(s) between a last of the one or more intermediary devices and the second device;

securely sending data representative of the exchanged intermediate key information further comprising:

performing, at the first intermediary device, a Bell State Measurement, BSM, on corresponding EPR pairs held by the first intermediary device;

performing, at each other intermediary device, a Bell State Measurement, BSM, on corresponding EPR pairs held by each other intermediary device; and

sending the BSM results from each of the intermediary devices to both the first and second endpoint devices;

wherein the first and second endpoint devices process the BSM results and share EPR pairs for generating the final shared key.

26. The computer-implemented method as claimed in any preceding claim, wherein:

each of the devices in the group of devices is connected to each of its nearest neighbour devices via a quantum channel, wherein each quantum channel is unidirectional depending on the selected one or more key exchange protocols used between said each device and its nearest neighbour devices;

the first and the second endpoint devices have a classically-secured classical channel therebetween;

each of the *N* intermediary devices have a classical channels with each of their nearest neighbour intermediary devices, the method further comprising:

said exchanging first intermediate key information using the first key exchange protocol further comprising:

transmitting or receiving, by the first intermediary device, a first set of random symbols over a first quantum channel with the first endpoint device;

transmitting, from the first intermediary device to the first endpoint device, the basis set used by the first intermediary device for transmitting or receiving the first set of random symbols over the first quantum channel;

generating, by the first intermediary device, first intermediate key information comprising data representative of a first intermediate set of symbols based on the validly transmitted or received first set of symbols using the transmitting or receiving basis set used by the first intermediary device when transmitting or receiving the first set of symbols over the first quantum channel;

wherein the first endpoint device withholds the first transmitting or receiving basis set used by the first endpoint device for transmitting or receiving the first set of random symbols over the first quantum channel with the first intermediary device;

said securely sending data representative of the exchanged first intermediate key information from the first intermediary device to the second endpoint device further comprising:

encrypting the first intermediate key information with a shared key of a neighbouring device of the group of devices;

sending the encrypted first endpoint device intermediate key information to the second endpoint device via said neighbouring device(s) over said communication link therebetween, wherein any remaining intermediary devices securely send the first intermediate key information to said second endpoint device over said communication links therebetween;

wherein said second endpoint device receives the encrypted first intermediate key information and decrypts said encrypted first intermediate key information using a shared key exchanged with one of the intermediary devices to retrieve said first intermediate set of symbols determined by the first intermediary device;

said determining of the final shared key, by the first and second endpoint devices further comprising:

exchanging, between the first and second endpoint devices over a secure communication channel therebetween, the transmitting or receiving basis set used by the first endpoint device for transmitting or receiving the first set of random symbols;

determining, by the second endpoint device using the transmitting or receiving basis set used by the first endpoint device for transmitting or receiving the first set of random symbols and the first intermediate set of symbols, a second set of symbols corresponding to at least a portion of the first set of random symbols transmitted or received by the first endpoint device; and

exchanging, by the first and second devices over the classically-secured communication channel therebetween, a shared key based processing and transforming the first set of random symbols and second set of symbols.

27. The computer-implemented method as claimed in claim 26, wherein the first intermediate key information further comprises data representative from the group of:

said transmitting or receiving basis set used by the first intermediary device when transmitting or receiving said first set of random symbols over the first quantum channel with the first endpoint device; and

said first set of random symbols transmitted or received by the first intermediary device when transmitting or receiving said first set of random symbols with the first endpoint device.

28. The computer-implemented method as claimed in any of claims 26 or 27, wherein said exchanging, by the first endpoint device and second endpoint device over a secure communication channel therebetween, a shared key further comprising performing final key information reconciliation and privacy amplification on the second set of symbols determined

by the second endpoint device and the first set of symbols transmitted or received by the first endpoint device resulting in a final shared symmetric key.

29. The computer-implemented method as claimed in any of claims 26 to 28, wherein the one or more key exchange protocols used for secure communications between the second endpoint device and the first intermediary device is the BB84 key exchange protocol.

30. The computer-implemented method as claimed in any of claims 29, wherein each of the communication links between the group of devices includes a quantum channel and a classical channel and wherein the BB84 key exchange protocol is used to exchange shared keys between the corresponding devices of the group of devices and their neighbour devices of the group of devices.

31. The computer-implemented method as claimed in any previous claim, wherein the first key exchange protocol and the one or more key exchange protocols are classical or post-quantum key exchange protocols.

32. The computer-implemented method as claimed in claim 31, wherein:

exchanging intermediate key information between the first intermediary device and the first endpoint device based on the first key exchange protocol, wherein the intermediate key information is a first shared key between the first intermediary device and the first endpoint device;

for each of the intermediary devices and the second endpoint device exchanging a shared key with each of the nearest neighbouring devices, wherein each of the intermediary devices have a pair of shared keys and the second endpoint device has a shared key exchanged with the intermediary device it is connected to, and the first intermediary device has a second shared key with another intermediary device it is connected to;

securely sending data representative of the exchanged intermediate key information from the first intermediary device to the second endpoint device via the intermediary device(s) based on:

encrypting, by the intermediary device, the intermediate key information with the second shared key of the intermediary device, and sending to the second endpoint device;

for each other intermediary device, cryptographically combining their pairs of shared keys and sending to the second endpoint device;

wherein the second endpoint device uses its shared key and the received cryptographically combined pairs of shared keys from the intermediary devices to decrypt the encrypted intermediate key information, the first and second endpoint devices use the further communication channel to share the knowledge that the first shared key has been received

and decrypted by the second endpoint device, said first shared key comprising the final shared key.

33. The computer-implemented method as claimed in any preceding claim, wherein the first key exchange protocol or the one or more key exchange protocols comprises a classical or post-quantum key exchange protocol from the group of:

classical symmetric key exchange protocols;

Rivest/Shamir/Adelman (RSA) key exchange protocol;

Diffie-Hellman key exchange protocol;

Finite Field Cryptographic key exchange protocols;

Digital Signature Algorithm (DSA) key exchange protocol;

Elliptic Curve (EC) cryptographic key exchange protocol;

ECDSA key exchange protocol and EC-DH (ECDH) key exchange protocol;

Elliptic Curve Diffie Hellman ephemeral-Rivest/Shamir/Adelman (ECDHE-RSA) key exchange protocol;

ECDHE-ECDSA key exchange protocols;

Secure Hash Algorithm (SHA)-2 (384 bit);

SHA-3; key exchange protocols based on, without limitation, for example

Advanced Encryption Standard (AES) (256-bit) based protocols;

Galois Counter Mode based protocols;

Transport Layer Security (TLS), https, SSL, SSH based protocols;

any one or more other classical key exchange protocols;

any one or more future classical key exchange protocols;

any other suitable classical key exchange protocol for exchanging a shared key between endpoint devices or intermediary devices and the like using classical transmissions;

lattice-based cryptographic key exchange protocol(s);

Ring-Learning With Errors (LWE)-based key exchange protocol(s);

Nth degree-truncated polynomial ring units (NTRU)-based key exchange protocol(s);

Stehle–Steinfeld variant of NTRU-based key exchange protocol(s);

Bimodal Lattice Signature Scheme (BLISS)-based key exchange protocol(s);

multivariate-based cryptographic key exchange protocol(s);

Rainbow or Unbalanced Oil and Vinegar (UOV)-based key exchange protocol(s);

Hash-based cryptographic key exchange protocol(s);

Lamport-based cryptographic key exchange protocol(s);

Merkle-based cryptographic key exchange protocol(s);

Code-based cryptographic key exchange protocol(s);

McEliece-based cryptographic key exchange protocol(s);

Niederreiter-based key exchange protocol(s), Courtois, Finiasz and Sendrier

Signature-based key exchange protocol(s);

random linear code encryption scheme (RLCE)-based key exchange protocol(s);

Supersingular elliptic curve isogeny-based cryptographic key exchange protocol(s);

symmetric key quantum resistance-based cryptographic key exchange protocol(s);

any one or more other post-quantum key exchange protocols;

any one or more future post-quantum key exchange protocols; and

any other suitable post-quantum key exchange protocol for exchanging a shared key between endpoint devices or intermediary devices and the like using classical transmissions;

any other suitable classical or post-quantum protocol for exchanging keys between endpoint devices and/or intermediary devices using classical transmissions.

34. The computer-implemented method as claimed in any preceding claim, wherein each classical communication channel is based on one or more types of communication channels from the group of:

optical communication channel;

free-space optical communication channel;

wireless communication channel;

wired communication channel;

radio communication channel;

microwave communication channel;

satellite communication channel;

terrestrial communication channel;

optical fibre communication channel;

optical laser communication channel;

any other type of one or more optical, wireless and/or wired communication channel(s) for transmitting data between devices; and

two or more optical, wireless and/or wired communication channel(s) that form a composite communication channel for transmitting data between devices.

35. The computer-implemented method as claimed in any preceding claim, wherein each quantum communication channel is based on one or more types of quantum communication channels from the group of:

optical quantum communications;

free-space optical quantum communications;

optical fibre quantum communications;

optical laser quantum communications;

quantum entanglement communications;

any other type of quantum communications for transmitting data over a quantum communication channel between devices.

36. The computer-implemented method as claimed in any preceding claim, wherein one or more of the intermediary devices is a satellite apparatus, one or more terrestrial intermediary devices are satellite ground stations of hubs, and the first and second endpoint devices are connected via a terrestrial network to said satellite ground stations or hubs, wherein the first quantum communication channel between the first endpoint device and the first terrestrial intermediary device is a fibre optical quantum communication channel, the second quantum communication channel between the second endpoint device and the last terrestrial intermediary device is a fibre optical quantum communication channel, and the classical communication channel between the first and second endpoint devices is a non-quantum communications channel.

37. The computer-implemented method as claimed in any preceding claim, wherein one or more of the intermediary devices is a satellite and the first endpoint device and second endpoint device are satellites, wherein the first quantum communication channel between the first endpoint device and the first intermediary device is a free-space optical quantum communication channel, the second quantum communication channel between the second endpoint device and the last intermediary device is a free-space optical quantum communication channel, and the classical communication channel between the first and second endpoint devices is a non-quantum communications channel.

38. The computer-implemented method as claimed in any preceding claim, wherein the intermediary devices are satellites forming a satellite mesh network, the first endpoint device and second endpoint device are satellites, wherein the first quantum communication channel between the first endpoint device and the first intermediary device is a free-space optical quantum communication channel, the second quantum communication channel between the second endpoint device and the last intermediary device is a free-space optical quantum communication channel, and the classical communication channel between the first and second endpoint devices is a non-quantum communications channel.

39. The computer-implemented method as claimed in any preceding claim, wherein one or more of the intermediary devices is a terrestrial communication apparatus, the first device and second endpoint device are terrestrial endpoint devices, wherein the first quantum communication channel between the first endpoint device and the first intermediary device is a fibre optic quantum communication channel, the second quantum communication channel is between the second endpoint device and the second intermediary device is a fibre optic quantum communication channel, and the classical communication channel between the first and second endpoint devices is a non-quantum communications channel or classical terrestrial communications channel.

40. The computer-implemented method as claimed in any preceding claim, wherein the classical communications channels are encrypted communication channels.

41. The computer-implemented method as claimed in claim 40, further comprising encrypting transmission data or messages prior to transmitting said data or messages to: the first endpoint device over the first classical communication channel; or the second endpoint device over the second classical communication channel.

42. The computer-implemented method as claimed in any preceding claim, wherein one or more authentication protocols are used by one or more of the intermediary devices and the first or second endpoint devices for authenticating the intermediary device(s), first or second endpoint devices prior to communicating over the classical or quantum communications channels.

43. The computer-implemented method as claimed in claim 42, further comprising authenticating the first and second endpoint device prior to transmitting data to the first and second endpoint device over the classical communication channels, respectively.

44. A computer-implemented method of key exchange between a first endpoint device and a second endpoint device communicatively coupled over communication links via one or more intermediary devices, wherein the first endpoint device is coupled by a first communication link to a first of the one or more intermediary devices, and the second endpoint device and the one or more intermediary devices form a group of devices, wherein each of the one or more intermediary devices is communicatively coupled to at least one other of the one or more intermediary devices via at least one of the communication links and the second endpoint device is coupled to a last of the one or more intermediary devices in the group via a second communication link, the method comprising:

exchanging intermediate key information between the first intermediary device and the first endpoint device based on a first key exchange protocol, wherein the first key exchange protocol is a QKD protocol configured for exchanging the intermediate key information in which the first endpoint device withholds key exchange information from the first intermediary device; and

securely sending data representative of the exchanged intermediate key information from the first intermediary device to the second endpoint device via the intermediary device(s), the secure communications over the communication links of the group of devices based on shared keys exchanged using one or more key exchange protocols over the communication links of the group of devices;

wherein the first and second endpoint devices use a further communication channel therebetween for exchanging said withheld key exchange information and processing and

transforming said intermediate key information with said key exchange information into the final shared key.

45. The computer-implemented method as claimed in claim 44, wherein:

each of the devices in the group of devices is connected to each of its nearest neighbour devices via a quantum channel, wherein each quantum channel is unidirectional depending on the selected one or more key exchange protocols used between said each device and its nearest neighbour devices;

the first and the second endpoint devices have a classically-secured classical channel therebetween;

each of the *N* intermediary devices have a classical channels with each of their nearest neighbour intermediary devices, the method further comprising:

said exchanging first intermediate key information using the first key exchange protocol further comprising:

transmitting or receiving, by the first intermediary device, a first set of random symbols over a first quantum channel with the first endpoint device;

transmitting, from the first intermediary device to the first endpoint device, the basis set used by the first intermediary device for transmitting or receiving the first set of random symbols over the first quantum channel;

generating, by the first intermediary device, first intermediate key information comprising data representative of a first intermediate set of symbols based on the validly transmitted or received first set of symbols using the transmitting or receiving basis set used by the first intermediary device when transmitting or receiving the first set of symbols over the first quantum channel;

wherein the first endpoint device withholds the first transmitting or receiving basis set used by the first endpoint device for transmitting or receiving the first set of random symbols over the first quantum channel with the first intermediary device;

said securely sending data representative of the exchanged first intermediate key information from the first intermediary device to the second endpoint device further comprising:

encrypting the first intermediate key information with a shared key of a neighbouring device of the group of devices;

sending the encrypted first endpoint device intermediate key information to the second endpoint device via said neighbouring device(s) over said communication link therebetween, wherein any remaining intermediary devices securely send the first intermediate key information to said second endpoint device over said communication links therebetween;

wherein said second endpoint device receives the encrypted first intermediate key information and decrypts said encrypted first intermediate key

information using a shared key exchanged with one of the intermediary devices to retrieve said first intermediate set of symbols determined by the first intermediary device;

said determining of the final shared key, by the first and second endpoint devices further comprising:

exchanging, between the first and second endpoint devices over a secure communication channel therebetween, the transmitting or receiving basis set used by the first endpoint device for transmitting or receiving the first set of random symbols;

determining, by the second endpoint device using the transmitting or receiving basis set used by the first endpoint device for transmitting or receiving the first set of random symbols and the first intermediate set of symbols, a second set of symbols corresponding to at least a portion of the first set of random symbols transmitted or received by the first endpoint device; and

exchanging, by the first and second devices over the classically-secured communication channel therebetween, a shared key based processing and transforming the first set of random symbols and second set of symbols.

46. The computer-implemented method as claimed in claim 45, wherein the first intermediate key information further comprises data representative from the group of:

said transmitting or receiving basis set used by the first intermediary device when transmitting or receiving said first set of random symbols over the first quantum channel with the first endpoint device; and

said first set of random symbols transmitted or received by the first intermediary device when transmitting or receiving said first set of random symbols with the first endpoint device.

47. The computer-implemented method as claimed in any of claims 44 to 46, wherein said exchanging, by the first endpoint device and second endpoint device over a secure communication channel therebetween, a shared key further comprising performing final key information reconciliation and privacy amplification on the second set of symbols determined by the second endpoint device and the first set of symbols transmitted or received by the first endpoint device resulting in a final shared symmetric key.

48. The computer-implemented method as claimed in any of claims 44 to 47, wherein the one or more key exchange protocols used for secure communications between the second endpoint device and the first intermediary device is the BB84 key exchange protocol.

49. The computer-implemented method as claimed in any of claims 44 to 48, wherein each of the communication links between the group of devices includes a quantum channel

and a classical channel and wherein the BB84 key exchange protocol is used to exchange shared keys between the corresponding devices of the group of devices and their neighbour devices of the group of devices.

50. A system comprising an intermediary device, a first device and a second device, wherein the intermediary device, first device and second device are configured to implement the corresponding steps of the computer-implemented method according to any of claims 1 to 49.

51. The system as claimed in claim 50, wherein the system is a satellite quantum key distribution system comprising a plurality of satellites, each satellite including the functionality of an intermediary device, each satellite in communication with one or more ground receiving stations, and each ground receiving station including the functionality of the first and/or second endpoint devices.

52. A computer-readable medium comprising computer code or instructions stored thereon, which when executed on one or more processor(s), causes the one or more processor(s) to perform the computer implemented method according to any of claims 1 to 49.