Claims

1. A computer-implemented method for quantum-safe quantum streaming of data items from a first endpoint device to a second endpoint device via a server of a quantum cloud platform, the method, performed at the first endpoint device, comprising:

splitting a data item into a plurality of data shards that allow reconstruction of the data item;

encrypting each of the data shards separately using a first cryptographic key ,wherein the first cryptographic key is shared between the first endpoint device and the second endpoint device;

establishing a series or a first plurality of secure channels with a server of a quantum cloud platform using a second cryptographic key, wherein the second cryptographic key is shared between the first endpoint device and the server; and

transmitting the plurality of encrypted shards towards the second endpoint device via the server over the series or plurality of secure channels.

2. The computer-implemented method according to claim 1, wherein the first cryptographic key is a first quantum-safe key, and/or the second cryptographic key is a second quantum-safe key.

3. The computer-implemented method according to claim 1 or 2, wherein the first and second cryptographic keys are different.

4. The computer-implemented method according to any preceding claim, wherein the quantum cloud platform comprises:

a quantum-safe. QS, network, the QS network comprising:

one or more QS servers, and

a repository for storing and accessing the data items.

5. The computer-implemented method according to claim 4, wherein each of the one or more QS servers comprises: a hardware security module, HSM, for storing an identical set of quantum distributed, QD, keys or quantum-safe key,

wherein the identical set of QD keys are distributed to each of the one or more QS servers in a quantum-safe manner.

6. The computer-implemented method according to claim 5, wherein each of the one or more QS servers is configured to communicate securely with each of the other QS servers and with the repository using one or more available QD keys from the identical set of QD keys.

7. The computer-implemented method according to claim 6, wherein one or more further available QD keys are distributed as quantum-safe keys to each of the first and second endpoint devices.

8. The computer-implemented method according to any preceding claim, wherein the data item may be reconstructed from a partial subset of the plurality of data shards.

9. The computer-implemented method according to any preceding claim, wherein the data item may be reconstructed based on metadata comprising information for reassembling the data item from the plurality of data shards.

10. A computer-implemented method for quantum safe quantum streaming of data items from a first endpoint device to a second endpoint device via a server of a quantum cloud platform, the method, performed at the server, comprising:

receiving a plurality of encrypted data shards of a data item from the first endpoint device via a first series or plurality of secure channels,

wherein each data shard is encrypted using a first cryptographic key known only to the first endpoint device and the second endpoint device,

wherein the data item can be reconstructed from the plurality of data shards, and

wherein the first series or plurality of secure channels is established with the first endpoint device based on a second cryptographic key known only to the first endpoint device and the server;

securely storing the encrypted data shards of the data item in a secure storage of the quantum cloud platform;

in response to the second endpoint logging onto the quantum cloud platform, establishing a second series or plurality of secure channels with the second endpoint using a third cryptographic key, wherein the third cryptographic key is shared between the second endpoint device and the server;

retrieving the encrypted data shards of the data item from secure storage; and

transmitting the encrypted data shards over the second series or plurality of secure channels to the second endpoint device.

11. The computer-implemented method of claim 10, wherein the first cryptographic key is a first quantum-safe key, the second cryptographic key is a second quantum-safe key, and/or the third cryptographic key is a third quantum-sage key.

12. The computer-implemented method according to claim 10 or 11, wherein the first encryption key is different to the second and third encryption keys.

13. The computer-implemented method according to any of claims 10 to 12, wherein the second and third encryption keys are different.

14. The computer-implemented method according to any of claims 10 to 13, wherein the quantum cloud platform comprises:

a quantum-safe. QS, network, the QS network comprising:

one or more QS servers, and

a repository for storing and accessing the data items.

15. The computer-implemented method according to claim 14, wherein each of the one or more QS servers comprises: a hardware security module, HSM, for storing an identical set of quantum distributed, QD, keys or quantum-safe key,

wherein the identical set of QD keys are distributed to each of the one or more QS servers in a quantum-safe manner.

16. The computer-implemented method according to claim 15, wherein each of the one or more QS servers is configured to communicate securely with each of the other QS servers and with the repository using one or more available QD keys from the identical set of QD keys.

17. The computer-implemented method according to claim 16, wherein one or more further available QD keys are distributed as quantum-safe keys to each of the first and second endpoint devices.

18. The computer-implemented method according to any of claims 10 to 17, wherein the data item may be reconstructed from a partial subset of the plurality of data shards.

19. The computer-implemented method according to any of claims 10 to 18, wherein the data item may be reconstructed based on metadata comprising information for reassembling the data item from the plurality of data shards.

20. The computer-implemented method according to claim 19, further comprising storing the metadata in the secure storage of the quantum cloud platform.

21. The computer-implemented method according to any of claims 10 to 20, further comprising storing a plurality of copies of one or more of the encrypted data shards, wherein each copy is associated with a unique infrastructure generated quantum key.

22. A computer-implemented method for quantum safe quantum streaming of data items from a first endpoint device to a second endpoint device via a server of a quantum cloud platform, the method, performed at the second device comprising:

connecting to the quantum cloud platform;

in response to a data transfer of an encrypted data item from the first endpoint device, the encrypted data item being encrypted with a first cryptographic key known only to the first and second endpoints, establishing a series or plurality of secure channels with the server using a third cryptographic key, which is known only to the second endpoint device and the server;

receiving a plurality of encrypted data shards of the encrypted data item from the server over the plurality of secure channels, wherein the data item can be reconstructed from the plurality of data shards; and

decrypting the encrypted data shards using the first cryptographic key to reconstruct the data item transferred from the first endpoint device.

23. The computer-implemented method according to claim 22, wherein the first cryptographic key is a first quantum-safe key, and/or the third cryptographic key is a third quantum-safe key.

24. The computer-implemented method according to claim 22 or 23, wherein the first and third cryptographic keys are different.

25. The computer-implemented method according to any of claims 22 to 24, wherein the quantum cloud platform comprises:

a quantum-safe. QS, network, the QS network comprising:

one or more QS servers, and

a repository for storing and accessing the data items.

26. The computer-implemented method according to claim 25, wherein each of the one or more QS servers comprises: a hardware security module, HSM, for storing an identical set of quantum distributed, QD, keys or quantum-safe key,

wherein the identical set of QD keys are distributed to each of the one or more QS servers in a quantum-safe manner.

27. The computer-implemented method according to claim 26, wherein each of the one or more QS servers is configured to communicate securely with each of the other QS servers and with the repository using one or more available QD keys from the identical set of QD keys.

28. The computer-implemented method according to claim 27, wherein one or more further available QD keys are distributed as quantum-safe keys to each of the first and second endpoint devices.

29. The computer-implemented method according to any of claims 22 to 28, wherein the data item may be reconstructed from a partial subset of the plurality of data shards.

30. The computer-implemented method according to any of claims 22 to 29, wherein the data item may be reconstructed based on metadata comprising information for reassembling the data item from the plurality of data shards.

31. The computer-implemented method according to any of claims 22 to 30, further comprising, prior to establishing the series or plurality of secure channel receiving a notification from the quantum cloud platform that a data transfer from the first endpoint device is waiting; and

in response to receiving the notification, establishing the series or plurality of secure channels.

32. The computer-implemented method according to claim 31, wherein if the second endpoint device does not receive the notification, further comprising, performing one or more other operations or transfers.

33. A computer-implemented method for quantum safe quantum streaming between a first endpoint device and second endpoint device via a server of a quantum cloud platform comprising:

splitting, at the first endpoint device, a data item into a plurality of data shards that allow reconstruction of the data item;

encrypting, at the first endpoint device, each of the data shards separately using a first cryptographic key shared between the first endpoint device and the second endpoint device;

establishing, between the first endpoint device and the server, a first series or plurality of secure channels with the server of the quantum cloud platform using a second

cryptographic key, the second cryptographic key being shared between the first endpoint device and the server; and

transmitting, from the first endpoint device to the server, the plurality of encrypted shards towards the second endpoint device via the server over the plurality of secure channels;

receiving, at the server, the plurality of encrypted data shards of the data item transmitted from the first endpoint device over the first plurality of secure channels, each data shard encrypted using the first cryptographic key known only to the first endpoint device and the second endpoint device;

securely storing, by the server, the encrypted data shards of the data item in a secure storage of the quantum cloud platform;

in response to the second endpoint logging onto the quantum cloud platform, establishing a second series or plurality of secure channels with the second endpoint using a third cryptographic key, the third cryptographic key shared between the second endpoint device and the server;

retrieving the encrypted data shards of the data item from secure storage;

transmitting the encrypted data shards over the second plurality of secure channels to the second endpoint device;

receiving, at the second endpoint, a plurality of encrypted data shards of the encrypted data item from the server over the second series or plurality of secure channels; and

decrypting the encrypted data shards using the first cryptographic key to reconstruct the data item transferred from the first endpoint device.

34. The computer-implemented method according to claim 33, when the first cryptographic key is a first quantum safe key, the second cryptographic key is a second quantum safe key, and/or the third cryptographic key is a third quantum-safe key.

35. The computer-implemented method according to claim 33 or 34, wherein the first encryption key is different to the second and third encryption keys.

36. The computer-implemented method according to any of claims 33 to 35, wherein the second and third encryption keys are different.

37. The computer-implemented method according to any of claims 33 to 36, wherein the quantum cloud platform comprises:

a quantum-safe (QS) network, the QS network comprising:

one or more QS server(s) and

a repository for storing and accessing the data items.

38. The computer-implemented method according to claim 37, wherein each QS server comprises: a hardware security module, HSM, for storing an identical set of quantum distributed, QD, keys or quantum-safe keys,

wherein the identical set of QD keys are distributed to each of said QS servers in a quantum-safe manner.

39. The computer-implemented method according to claim 38, wherein each of the QS servers is configured to communicate securely with each of the other QS servers and with the repository using one or more available QD keys from the identical set of QD keys.

40. The computer-implemented method according to claim 39, wherein one or more further available QD keys from the set of QD keys are distributed as quantum safe keys to each of the first and second endpoint devices.

41. The computer-implemented method according to any of claims 33 to 40, wherein the data item may be reconstructed from a partial subset of the plurality of data shards.

42. The computer-implemented method according to any of claims 33 to 41, wherein the data item may be reconstructed based on metadata comprising information for reassembling the data item from the plurality of data shards.

43. The computer-implemented method according to claim 42, further comprising storing, by the server, the metadata in the secure storage of the quantum cloud platform.

44. The computer-implemented method according to any of claims 33 to 43, further comprising storing, by the server, a plurality of copies of one or more of the encrypted data shards, wherein each copy is associated with a unique infrastructure generated quantum key.

45. The computer-implemented method according to any of claims 33 to 44, further comprising, prior to establishing the series or plurality of secure channel receiving, by the second endpoint device, a notification from the quantum cloud platform that a data transfer from the first endpoint device is waiting; and

in response to receiving the notification, establishing the second series or plurality of secure channels.

46. The computer-implemented method according to claim 45, wherein if the second endpoint device does not receive the notification, further comprising, performing, by the second endpoint device, one or more other operations or transfers.

47. An apparatus comprising a processor unit, a memory unit, and a communication interface, the processor unit connected to the memory unit and the communication interface, wherein the processor unit, memory unit and communication interface are adapted to implement the computer-implemented method as claimed in any one of claims 1 to 32.

48. A system comprising:

a first endpoint device comprising an apparatus according to claim 47, wherein the first endpoint device is operatively configured to implement the method of any one of claims 1 to 9;

a second endpoint device comprising an apparatus according to claim 47, wherein the second endpoint device is operatively configured to implement the method of any one of claims 22 to 32; and

a server comprising an apparatus according to claim 47, wherein the server is operatively configured to implement the method of any one of claims 10 to 21;

wherein the first endpoint device, the second endpoint device and the server are configured to communicate with each other.

49. The system according to claim 48, wherein the first endpoint device, the second endpoint device and the server are operatively configured to communicate with each other to implement the computer-implemented method according to any one of claims 33 to 46.

50. 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 1 to 46.

51. A computer program product comprising instructions which, when the program is executed by a computer, cause the computer to carry out the method according to any of claims 1 to 46.

52. An apparatus configured to carry out the method according to any of claims 1 to 46.