

Claims

1. A method of scheduling and managing key data in a satellite quantum key distribution system comprising a constellation of one or more satellites and a plurality of user ground stations, the method comprising:
 - 5 using a satellite of the constellation of satellites to deliver key data to a user ground station using a quantum communication link;
at the user ground station, storing the delivered key data and reporting the amount of delivered key data;
 - 10 using the satellite to deliver key data to at least one other user ground station requiring common encryption keys with the user ground station using a respective quantum communication link;
at each other user ground station, storing the delivered key data and reporting the amount of delivered key data;
 - 15 based upon the reports, determining an amount of the delivered key data which is commonly stored at all of the user ground station and the at least one other user ground station; and
instructing the user ground station and the at least one other user ground station to release the commonly stored delivered key data.
- 20 2. The method as claimed in claim 1, wherein the determining an amount of the delivered key data which is commonly stored at all of the user ground station and the at least one other user ground station is carried out at a key management system.
3. The method as claimed in claim 1 or claim 2, wherein, when the satellite of the constellation of satellites delivers key data to the user ground station the satellite stores a
25 copy of the key data on the satellite.
4. The method as claimed in claim 3, wherein the satellite uses the copy of the key data stored on the satellite to deliver key data to at least one other user ground station.
5. The method as claimed in claim 3 or claim 4, wherein, when the satellite has delivered key data which is commonly stored at all of the user ground station and the at least
30 one other user ground station, the satellite deletes the commonly stored key data from the copy of the key data on the satellite.
6. The method as claimed in any preceding claim, wherein the key data delivered to a user ground station comprises blocks of data, each block being assigned a unique identifier, and the reporting the amount of delivered key data comprises reporting the unique identifier of

each received block together with metadata associated with the unique identifier which identifies the total size of the block.

7. The method as claimed in claim 6, wherein the metadata associated with the unique identifier also identifies the status of the block.

- 5 8. The method as claimed in claim 6 or claim 7, wherein each block is assigned the unique identifier by the user ground station; or
wherein each block is assigned the unique identifier by the satellite.

9. The method as claimed in any one of claims 6 to 8, wherein reporting the amount of delivered key data at each other user ground station comprises reporting the unique identifier of each at least partially received block together with metadata associated with the unique identifier which identifies the total size of the block and the current amount of the block stored at that other user ground station.
- 10

10. The method as claimed in any of claims 6 to 9, wherein the metadata associated with the unique identifier identifies the user ground station and the at least one other user ground station.
- 15

11. The method as claimed in any of claims 6 to 10, wherein the metadata associated with the unique identifier comprises a data integrity check.

12. The method as claimed in any preceding claim, wherein the at least one other ground station comprises plural other ground stations.

- 20 13. The method as claimed in any preceding claim, wherein each of the user ground station and the at least one other user ground station respond to the instruction to release the commonly stored delivered key data by formatting the commonly stored data into formatted keys and releasing the formatted keys.

14. The method as claimed in any preceding claim, wherein the key data is delivered to the user ground station and one other user ground station by a methodology comprising:
forming quantum optical communication links from the satellite to the user ground stations and the other user ground station to send respective photons of entangled pairs to each of the user ground station and the other user ground station;
- 25

- detecting the quantum information of the respective photons at each of the user ground station and the other user ground station; and
- 30
- conducting an encryption key agreement process between user ground station and the other user ground station using the detected quantum information to determine key data.

15. The method as claimed in any preceding claim, wherein the key data is delivered to the user ground station and to the at least one other user ground station by a methodology comprising:
- generating a first string of random numbers on the satellite;
 - 5 using the first string of random numbers to form a first quantum optical communication link from the satellite to the user ground station;
 - conducting an encryption key agreement process between the satellite and the user ground station using the first string of random numbers to determine the key data;
 - storing the key data on the satellite;
 - 10 and subsequently:
 - generating a second string of random numbers on the satellite;
 - using the second string of random numbers to form a second quantum optical communication link from the satellite to one of the at least one other user ground stations;
 - conducting an encryption key agreement process between the satellite and the one of
 - 15 the at least one other user ground stations using the second string of random numbers to determine second key data;
 - sending one-time-pad "OTP" data of an OTP operation of the key data and the second key data from the satellite to the one of the at least one other user ground stations;
 - using the second key data and the OTP data to derive the key data at the one of the
 - 20 at least one other user ground stations.
16. The method as claimed in claim 15, wherein the methodology further comprises subsequently:
- generating a further string of random numbers on the satellite;
 - using the further string of random numbers to form a further quantum optical
 - 25 communication link from the satellite to a further one of the at least one other user ground stations;
 - conducting an encryption key agreement process between the satellite and the further one of the at least one other user ground stations using the further string of random numbers to determine further key data;
 - 30 sending OTP data of an OTP operation of the key data and the further key data from the satellite to the further one of the at least one other user ground stations;
 - using the further key data and the OTP data to derive the key data at the further one of the at least one other user ground stations.
- 35 17. The method as claimed in claim 15 or claim 16, wherein the OTP operation is an XOR operation and the OTP data is XOR data.

18. The method as claimed in any preceding claim, wherein satellites of the constellation are able to use multiple methodologies to deliver key data.
19. The method as claimed in any preceding claim, wherein the constellation of satellites
5 comprises one satellite or multiple satellites.
20. The method as claimed in any preceding claim, wherein the method is a computer implemented method.
- 10 21. The method as claimed in any preceding claim, and further comprising, after using the satellite to deliver key data to at least one other user ground station requiring common encryption keys with the user ground station using a respective quantum communication link, harvesting a portion of the delivered key data for utilization in internal security functions associated with the delivery.
- 15 22. The method as claimed in claim 21, wherein the harvesting a portion of the delivered key data comprises the satellite and the at least one other user ground station retaining a portion of the key data, such retained key data not being available for release by the user ground station and the at least one other user ground station.
- 20 23. The method as claimed in claim 22, wherein the retained key data is used to provide authentication and encryption for current and future quantum key delivery.
- 25 24. A method of scheduling managing key data in a satellite quantum key distribution system comprising a constellation of one or more satellites and a plurality of user ground stations, the method comprising:
- delivering key data stored at a user ground station from the user ground station to a satellite of the constellation of satellites using a quantum communication link;
- 30 at the user ground station, reporting the amount of delivered key data;
- at the satellite, storing the delivered key data;
- the satellite using the copy of the key data stored on the satellite to deliver the key data to at least one other user ground station requiring common encryption keys with the user ground station using a respective quantum communication link;
- 35 at each other user ground station, storing the delivered key data and reporting the amount of delivered key data;

based upon the reports, determining an amount of the delivered key data which is commonly stored at all of the user ground station and the at least one other user ground station; and

5 instructing the user ground station and the at least one other user ground station to release the commonly stored delivered key data.

25. The method as claimed in claim 24, wherein the determining an amount of the delivered key data which is commonly stored at all of the user ground station and the at least one other user ground station is carried out at a key management system.

10

26. The method as claimed in claim 24 or claim 25, wherein, when the satellite has delivered key data which is commonly stored at all of the user ground station and the at least one other user ground station, the satellite deletes the commonly stored key data from the copy of the key data on the satellite.

15

27. The method as claimed in any one of claims 24 to 26, wherein the key data delivered to the satellite comprises blocks of data, each block being assigned a unique identifier, and the reporting the amount of delivered key data comprises reporting the unique identifier of each received block together with metadata associated with the unique identifier which identifies the total size of the block.

20

28. The method as claimed in claim 27, wherein the metadata associated with the unique identifier also identifies the status of the block

25 29. The method as claimed in claim 27 or claim 28, wherein each block is assigned the unique identifier by the user ground station; or
 wherein each block is assigned the unique identifier by the satellite.

30 30. The method as claimed in any one of claims 27 to 29, wherein reporting the amount of delivered key data at each other user ground station comprises reporting the unique identifier of each at least partially received block together with metadata associated with the unique identifier which identifies the total size of the block and the current amount of the block stored at that other user ground station.

35 31. The method as claimed in any of claims 27 to 30, wherein the metadata associated with the unique identifier identifies the user ground station and the at least one other user ground station.

32. The method as claimed in any of claims 27 to 31, wherein the metadata associated with the unique identifier comprises a data integrity check.
- 5 33. The method as claimed in any one of claims 24 to 32, wherein the at least one other ground station comprises plural other ground stations.
- 10 34. The method as claimed in any one of claims 24 to 33, wherein each of the user ground station and the at least one other user ground station respond to the instruction to release the commonly stored delivered key data by formatting the commonly stored data into formatted keys and releasing the formatted keys.
- 15 35. The method as claimed in any one of claims 24 to 34, wherein the key data is delivered to the satellite and to the at least one other user ground station by a methodology comprising:
generating a first string of random numbers on the satellite;
using the first string of random numbers to form a first quantum optical communication link from the satellite to the user ground station;
conducting an encryption key agreement process between the satellite and the user ground station using the first string of random numbers to determine first key data;
20 the first user ground station sending one-time-pad "OTP" data of an OTP operation of the first key data and the key data to the satellite;
using the first key data and the OTP data to derive the key data at the satellite;
storing the key data on the satellite;
and subsequently:
25 generating a second string of random numbers on the satellite;
using the second string of random numbers to form a second quantum optical communication link from the satellite to one of the at least one other user ground stations;
conducting an encryption key agreement process between the satellite and the one of the at least one other user ground stations using the second string of random numbers to
30 determine second key data;
sending OTP data of the key data and the second key data from the satellite to the one of the at least one other user ground stations; and
using the second key data and the OTP data to derive the key data at the one of the at least one other user ground stations.
- 35 36. The method as claimed in claim 35, wherein the methodology further comprises subsequently:
generating a further string of random numbers on the satellite;

using the further string of random numbers to form a further quantum optical communication link from the satellite to a further one of the at least one other user ground stations;

- 5 conducting an encryption key agreement process between the satellite and the further one of the at least one other user ground stations using the further string of random numbers to determine further key data;

 sending OTP data of an OTP operation of the key data and the further key data from the satellite to the further one of the at least one other user ground stations; and

- 10 using the further key data and the OTP data to derive the key data at the further one of the at least one other user ground stations.

37. The method as claimed in claim 35 or claim 36, wherein the OTP operation is an XOR operation and the OTP data is XOR data.

38. The method as claimed in any one of claims 24 to 37, wherein satellites of the constellation are able to use multiple methodologies to carry out the encryption key delivery communication sessions.

39. The method as claimed in any one of claims 24 to 38, wherein the constellation of satellites comprises one satellite or multiple satellites.

40. The method as claimed in any one of claims 24 to 39, wherein the method is a computer implemented method.

- 20 41. The method as claimed in any one of claims 24 to 40, and further comprising, after the satellite using the copy of the key data stored on the satellite to deliver the key data to at least one other user ground station requiring common encryption keys with the user ground station using a respective quantum communication link, harvesting a portion of the delivered key data for utilization in internal security functions associated with the delivery.

- 25 42. The method as claimed in claim 41, wherein the harvesting a portion of the delivered key data comprises the satellite and the at least one other user ground station retaining a portion of the key data, such retained key data not being available for release by the user ground station and the at least one other user ground station.

- 30 43. The method as claimed in claim 42, wherein the retained key data is used to provide authentication and encryption for current and future quantum key delivery

44. A satellite quantum key distribution system comprising a constellation of one or more satellites and a plurality of user ground stations, the system comprising:

a satellite of the constellation of satellites arranged to deliver key data to a user ground station using a quantum communication link;

a user ground station arranged to store the delivered key data and report the amount of delivered key data;

5 wherein the satellite is further arranged to deliver key data to at least one other user ground station requiring common encryption keys with the user ground station using a respective quantum communication link; and

each at least one other user ground station is arranged to store the delivered key data and report the amount of delivered key data; and

10 the system further comprising means arranged to, based upon the reports, determine an amount of the delivered key data which is commonly stored at all of the user ground station and the at least one other user ground station; and

instruct the user ground station and the at least one other user ground station to release the commonly stored delivered key data.

15

45. The system of claim 44, wherein the means arranged to determine an amount of the delivered key data which is commonly stored at all of the user ground station and the at least one other user ground station is a key management system.

20 46. The system of claim 44 or claim 45, wherein the satellite is further arranged to store a copy of the key data on the satellite when the satellite delivers key data to the user ground station.

25 47. The system of claim 46, wherein the satellite is further arranged to use the copy of the key data stored on the satellite to deliver key data to at least one other user ground station.

30 48. The system of claim 46 or claim 47, wherein the satellite is arranged to delete the commonly stored key data from the copy of the key data on the satellite when the satellite has delivered key data which is commonly stored at all of the user ground station and the at least one other user ground station.

35 49. The system of any of claims 44 to 48, wherein the satellite is arranged to deliver key data to a user ground station, the key data comprising blocks of data, each block being assigned a unique identifier; and

each at least one other user ground station is arranged to report the amount of delivered key data by reporting the unique identifier of each received block together

with metadata associated with the unique identifier which identifies the total size of the block.

50. The system as claimed in claim 49, wherein the metadata associated with the unique
5 identifier also identifies the status of the block.

51. The system as claimed in claim 49 or claim 50, wherein the user ground station is
arranged to assign each block the unique identifier; or
10 wherein the satellite is arranged to assign each block the unique identifier.

52. The system as claimed in any of claims 49 to 51, wherein each other user ground
station is arranged to report the amount of delivered key data by reporting the unique
identifier of each at least partially received block together with metadata associated with the
unique identifier which identifies the total size of the block and the current amount of the block
15 stored at that other user ground station.

53. The system as claimed in any of claims 49 to 52, wherein the metadata associated
with the unique identifier identifies the user ground station and the at least one other user
ground station.

54. The system as claimed in any of claims 49 to 53, wherein the metadata associated
20 with the unique identifier comprises a data integrity check.

55. The system as claimed in any one of claims 44 to 54, wherein the at least one other
ground station comprises plural other ground stations.

56. The system as claimed in any of claims 44 to 55, wherein each of the user ground
station and the at least one other user ground station are arranged to respond to the
25 instruction to release the commonly stored delivered key data by formatting the commonly
stored data into formatted keys and releasing the formatted keys.

57. The system as claimed in any of claims 44 to 56, wherein the satellite is arranged to
deliver the key data to the user ground station and one other user ground station by a
methodology comprising:
30 forming quantum optical communication links from the satellite to the user ground
stations and the other user ground station to send respective photons of entangled pairs
to each of the user ground station and the other user ground station;
detecting the quantum information of the respective photons at each of the user
ground station and the other user ground station; and

conducting an encryption key agreement process between user ground station and the other user ground station using the detected quantum information to determine key data.

- 5 58. The system as claimed in any of claims 44 to 57, wherein the satellite is arranged to deliver key data to the user ground station and to the at least one other user ground station by a methodology comprising:
- 10 generating a first string of random numbers on the satellite;
 using the first string of random numbers to form a first quantum optical communication link from the satellite to the user ground station;
 conducting an encryption key agreement process between the satellite and the user ground station using the first string of random numbers to determine the key data;
 storing the key data on the satellite;
15 and subsequently:
 generating a second string of random numbers on the satellite;
 using the second string of random numbers to form a second quantum optical communication link from the satellite to one of the at least one other user ground stations;
20 conducting an encryption key agreement process between the satellite and the one of the at least one other user ground stations using the second string of random numbers to determine second key data;
 sending one-time-pad "OTP" data of an OTP operation of the key data and the second key data from the satellite to the one of the at least one other user ground stations; and
25 using the second key data and the OTP data to derive the key data at the one of the at least one other user ground stations.

59. The system as claimed in claim 58, wherein the methodology further comprises subsequently:
- 30 generating a further string of random numbers on the satellite;
 using the further string of random numbers to form a further quantum optical communication link from the satellite to a further one of the at least one other user ground stations;
 conducting an encryption key agreement process between the satellite and the further one of the at least one other user ground stations using the further string of random numbers to determine further key data;
35 sending OTP data of an OTP operation of the key data and the further key data from the satellite to the further one of the at least one other user ground stations; and

using the further key data and the OTP data to derive the key data at the further one of the at least one other user ground stations.

60. The system as claimed in claim 58 or claim 59, wherein the OTP operation is an XOR operation and the OTP data is XOR data.

5 61. The system as claimed in any of claims 44 to 60, wherein satellites of the constellation are arranged to use multiple methodologies to deliver key data.

62. The system as claimed in any of claims 44 to 61, wherein the constellation of satellites comprises one satellite or multiple satellites.

63. The system as claimed in any one of claims 44 to 62, and further comprising the
10 system harvesting a portion of the delivered key data for utilization in internal security functions associated with the delivery.

64. The system as claimed in claim 63, wherein the harvesting a portion of the delivered key data comprises the satellite and the at least one other user ground station retaining a portion of the key data, such retained key data not being available for release by the at least
15 one other user ground station.

65. The system as claimed in claim 64, wherein the system is arranged to use the retained key data to provide authentication and encryption for current and future quantum key delivery.

66. A satellite quantum key distribution system comprising a constellation of one or more
20 satellites and a plurality of user ground stations, the system comprising:

a satellite of the constellation of satellites arranged to deliver key data stored at a user ground station using a quantum communication link;

a user ground station arranged to report the amount of delivered key data;

25 wherein the satellite is further arranged to store the delivered key data and to use the copy of the key data stored on the satellite to deliver the key data to at least one other user ground station requiring common encryption keys with the user ground station using a respective quantum communication link;

each at least one other user ground station arranged to store the delivered key data and report the amount of delivered key data;

30 the system further comprising means arranged to, based upon the reports, determine an amount of the delivered key data which is commonly stored at all of the user ground station and the at least one other user ground station; and

instruct the user ground station and the at least one other user ground station to release the commonly stored delivered key data.

- 5 67. The system of claim 66, wherein the means arranged to determine an amount of the delivered key data which is commonly stored at all of the user ground station and the at least one other user ground station is a key management system.
- 10 68. The system of claim 66 or claim 67, wherein the satellite is arranged to delete the commonly stored key data from the copy of the key data on the satellite when the satellite has delivered key data which is commonly stored at all of the user ground station and the at least one other user ground station.
- 15 69. The system of any of claims 66 to 68, wherein the satellite is arranged to deliver key data to a user ground station, the key data comprising blocks of data, each block being assigned a unique identifier; and
each at least one other user ground station is arranged to report the amount of delivered key data by reporting the unique identifier of each received block together with metadata associated with the unique identifier which identifies the total size of the block.
- 20 70. The system as claimed in claim 69, wherein the metadata associated with the unique identifier also identifies the status of the block.
71. The system as claimed in claim 69 or claim 70, wherein the user ground station is arranged to assign each block the unique identifier; or
wherein the satellite is arranged to assign each block the unique identifier
- 25 72. The system as claimed in any of claims 66 to 71, wherein each other user ground station is arranged to report the amount of delivered key data by reporting the unique identifier of each at least partially received block together with metadata associated with the unique identifier which identifies the total size of the block and the current amount of the block stored at that other user ground station.
- 30 73. The system as claimed in any of claims 69 to 72, wherein the metadata associated with the unique identifier identifies the user ground station and the at least one other user ground station.
74. The system as claimed in any of claims 69 to 73, wherein the metadata associated with the unique identifier comprises a data integrity check.

75. The system as claimed in any one of claims 66 to 74, wherein the at least one other ground station comprises plural other ground stations.

76. The system as claimed in any of claims 66 to 75, wherein each of the user ground station and the at least one other user ground station are arranged to respond to the
5 instruction to release the commonly stored delivered key data by formatting the commonly stored data into formatted keys and releasing the formatted keys.

77. The system as claimed in any of claims 66 to 76, wherein the satellite is arranged to deliver the key data to the user ground station and one other user ground station by a methodology comprising:

10 generating a first string of random numbers on the satellite;
 using the first string of random numbers to form a first quantum optical communication link from the satellite to the user ground station;
 conducting an encryption key agreement process between the satellite and the user ground station using the first string of random numbers to determine first key data;
15 the first user ground station sending one-time-pad "OTP" data of an OTP operation of the first key data and the key data to the satellite;
 using the first key data and the OTP data to derive the key data at the satellite;
 storing the key data on the satellite;
 and subsequently:
20 generating a second string of random numbers on the satellite;
 using the second string of random numbers to form a second quantum optical communication link from the satellite to one of the at least one other user ground stations;
 conducting an encryption key agreement process between the satellite and the one of the at least one other user ground stations using the second string of random numbers to
25 determine second key data;
 sending OTP data of the key data and the second key data from the satellite to the one of the at least one other user ground stations; and
 using the second key data and the OTP data to derive the key data at the one of the at least one other user ground stations.

30 78. The system as claimed in claim 77, wherein the methodology further comprises subsequently:
 generating a further string of random numbers on the satellite;
 using the further string of random numbers to form a further quantum optical communication link from the satellite to a further one of the at least one other user ground
35 stations;

- conducting an encryption key agreement process between the satellite and the further one of the at least one other user ground stations using the further string of random numbers to determine further key data;
- 5 sending OTP data of an OTP operation of the key data and the further key data from the satellite to the further one of the at least one other user ground stations; and
- using the further key data and the OTP data to derive the key data at the further one of the at least one other user ground stations.
79. The system as claimed in claim 77 or claim 78, wherein the OTP operation is an XOR
10 operation and the OTP data is XOR data.
80. The system as claimed in any of claims 66 to 79, wherein satellites of the constellation are arranged to use multiple methodologies to deliver key data.
81. The system as claimed in any of claims 66 to 80, wherein the constellation of satellites comprises one satellite or multiple satellites.
- 15 82. The system as claimed in any one of claims 66 to 81, and further comprising the system harvesting a portion of the delivered key data for utilization in internal security functions associated with the delivery.
83. The system as claimed in claim 82, wherein the harvesting a portion of the delivered key data comprises the satellite and the at least one other user ground station retaining a
20 portion of the key data, such retained key data not being available for release by the at least one other user ground station.
84. The system as claimed in claim 83, wherein the system is arranged to use the retained key data to provide authentication and encryption for current and future quantum key delivery.
- 25 85. An apparatus comprising a processor unit, a memory unit and a communication interface, the processor unit connected to the memory unit and the communication unit, wherein the apparatus is configured to implement the computer-implemented method according to any of claims 1 to 43.
86. A computer-readable medium comprising code or computer instructions stored
30 thereon, which when executed by a processor unit, causes the processor unit to perform the computer-implemented method according to any one of claims 1 to 43.