

Claims

1. A method of scheduling encryption key delivery communication sessions 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 producing a list of user ground stations requiring encryption keys;
 for each satellite of the constellation of satellites, determining a region of the earths surface within which the satellite can carry out encryption key delivery communication sessions to user ground stations using a quantum optical communications link during a scheduling period;
- 10 obtaining a cloud cover map;
 comparing the locations of the listed user ground stations, the determined regions of the earths surface for the constellation of satellites, and the cloud cover map, to identify listed user ground stations to which encryption key delivery can be carried out by the constellation of satellites during the scheduling period; and
- 15 determining which of the identified user ground stations each satellite of the constellation of satellites will carry out encryption key delivery communication sessions with at different times in the scheduling period based upon one or more of:
 an amount of unused encryption keys at each identified user ground station;
 and
- 20 an expected time duration before each identified user ground station runs out of encryption keys.
2. The method as claimed in claim 1, wherein the determining which of the identified user ground stations each satellite of the constellation of satellites will carry out encryption
- 25 key delivery communication sessions with at different times in the scheduling period is further based on an amount of encryption keys which were intended to be delivered to each identified user ground station in a previous scheduling period and were not delivered.
3. The method as claimed in claim 1 or claim 2, wherein, when the encryption key delivery sessions require encryption keys to be stored in a satellite, the determining which of
- 30 the identified user ground stations each satellite of the constellation of satellites will carry out encryption key delivery communication sessions with at different times in the scheduling period is further based on an amount of encryption keys stored on each satellite of the constellation of satellites.
4. The method as claimed in any preceding claim, wherein the determining which of the
- 35 identified user ground stations each satellite of the constellation of satellites will carry out encryption key delivery communication sessions with at different times in the scheduling

period is further based on the rate of encryption key delivery which can be supported by optical communication components of the user ground station.

5. The method as claimed in any preceding claim, wherein the determining which of the identified user ground stations each satellite of the constellation of satellites will carry out encryption key delivery communication sessions with at different times in the scheduling period is further based on a photon budget or communication link time budget required to deliver encryption keys from the satellite to the user ground station.

6. The method as claimed in claim 5, wherein the photon budget or communication link time budget required to deliver encryption keys from the satellite to the user ground station is based on one or more of: geometrical factors of the relative positions of the user ground station and the satellite; atmospheric conditions; meteorological conditions; light pollution.

7. The method as claimed in any preceding claim, wherein the determining which of the identified user ground stations each satellite of the constellation of satellites will carry out encryption key delivery communication sessions with at different times in the scheduling period is further based on expected metrological and atmospheric conditions for the user ground station.

8. The method as claimed in any preceding claim, wherein the determining which of the identified user ground stations each satellite of the constellation of satellites will carry out encryption key delivery communication sessions with at different times in the scheduling period is further based on a possible length of an encryption key delivery communication session being limited by geometrical factors of the relative positions of the user ground station and the satellite.

9. The method as claimed in any preceding claim, wherein the encryption key delivery communication sessions are carried out by a methodology comprising:

25 forming quantum optical communication links from a satellite of the constellation to two user ground stations to send respective photons of entangled pairs to each of the user ground stations;

detecting the quantum information of the respective photons at the two user ground stations; and

30 conducting an encryption key agreement process between the two user ground stations using the detected quantum information to determine encryption keys.

10. The method as claimed in claim 9, wherein the quantum optical communication links from the satellite to the two user ground stations use the E91 protocol.

11. The method as claimed in any preceding claim, wherein the encryption key delivery communication sessions are carried out by a methodology comprising:
- generating a first string of random numbers on a satellite of the constellation;
 - using the first string of random numbers to form a first quantum optical
 - 5 communication link from the satellite to a first user ground station;
 - conducting an encryption key agreement process between the satellite and the first user ground station using the first string of random numbers to determine a first encryption key;
 - storing the first encryption key 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 a second user ground station associated with the first user ground station;
 - 15 conducting an encryption key agreement process between the satellite and the second user ground station using the second string of random numbers to determine a second encryption key;
 - sending one-time-pad "OTP" data of an OTP operation of the first encryption key and the second encryption key from the satellite to the second user ground station;
 - 20 using the second encryption key and the OTP data to derive the first encryption key at the second ground station.
12. The method as claimed in any preceding claim, wherein determining which of the identified user ground stations each satellite of the constellation of satellites will carry out encryption key delivery communication sessions with at different times in the scheduling
- 25 period is further based on a number of encryption keys delivered to one or more user ground stations associated with each user ground station.
13. The method as claimed in claim 12, wherein determining which of the identified user ground stations each satellite of the constellation of satellites will carry out encryption key delivery communication sessions with at different times in the scheduling period is carried
- 30 out to ensure that common encryption keys are delivered to associated user ground stations as quickly as possible.
14. The method as claimed in claim 11, 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 user ground station associated with the first user ground station and the second user ground station;
- conducting an encryption key agreement process between the satellite and the
- 5 further user ground station using the further string of random numbers to determine a further encryption key;
- sending OTP data of the first encryption key and the further encryption key from the satellite to the further user ground station;
- using the further encryption key and the OTP data to derive the first encryption key at
- 10 the further ground station.
15. The method as claimed in any preceding claim, wherein the encryption key delivery communication sessions are carried out by a methodology comprising:
- generating a string of random numbers on a satellite of the constellation;
- 15 using the first string of random numbers to form a first quantum optical communication link from the satellite to a first user ground station;
- conducting an encryption key agreement process between the satellite and the first user ground station using the first string of random numbers to determine a first encryption key;
- 20 the first user ground station sending one-time-pad "OTP" data of an OTP operation of the first encryption key and a user encryption key to the satellite;
- using the first encryption key and the OTP data to derive the user encryption key at the satellite;
- storing the user encryption key on the satellite;
- 25 and subsequently:
- forming a second quantum optical communication link from the satellite to a second user ground station associated with the first user ground station;
- generating a second string of random numbers on the satellite;
- using the second string of random numbers to form a second quantum optical
- 30 communication link from the satellite to a second user ground station;
- conducting an encryption key agreement process between the satellite and the second user ground station using the second string of random numbers to determine a second encryption key;
- sending OTP data of the user encryption key and the second encryption key from the
- 35 satellite to the second user ground station;
- using the second encryption key and the OTP data to derive the user encryption key at the second ground station.

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
- 5 communication link from the satellite to a further user ground station associated with the first user ground station and the second user ground station;
- conducting an encryption key agreement process between the satellite and the further user ground station using the further string of random numbers to determine a further encryption key;
- 10 sending OTP data of the user encryption key and the further encryption key from the satellite to the further user ground station;
- using the further encryption key and the OTP data to derive the user encryption key at the further ground station.
17. The method as claimed in any of claims 11 to 16, wherein the OTP operation is an
- 15 XOR operation and the OTP data is XOR data.
18. The method as claimed in any of claims 11 to 17, wherein the quantum optical communication links use a Prepare and Measure protocol, and preferably, the BB 84 Decoy State protocol.
19. The method as claimed in any preceding claim, wherein satellites of the constellation
- 20 are able to use multiple methodologies to carry out the encryption key delivery communication sessions.
20. The method as claimed in claim 19, wherein the determining a region of the earths surface within which the satellite can carry out encryption key delivery communication sessions to user ground stations is carried out separately for each methodology which the
- 25 satellite is able to use.
21. The method as claimed in any preceding claim, wherein the determining a region of the earths surface within which the satellite can carry out encryption key delivery communication sessions to user ground stations is carried out only for regions where the satellite will be in eclipse.
- 30 22. The method as claimed in any preceding claim, wherein the producing a list of user ground stations requiring encryption keys comprises placing a user ground station on the list if the amount of encryption keys stored at the user ground station is below a threshold value.

23. The method as claimed in claim 22, wherein each user ground station has a respective threshold value.
24. The method as claimed in claim 23, wherein the threshold value is based on a size of an encryption key store of the user ground station.
- 5 25. The method as claimed in any preceding claim, wherein the producing a list of user ground stations requiring encryption keys comprises placing a user ground station on the list if an associated user ground station requiring common encryption keys with the user ground station in order to support encryption based services between the user ground station and the associated user ground station is placed on the list.
- 10 26. The method as claimed in any preceding claim, wherein the identifying listed user ground stations to which encryption key delivery can be carried out by the constellation of satellites during the scheduling period further comprises comparing ephemeris data of the satellites of the constellation of one or more satellites.
27. The method as claimed in any preceding claim, wherein the constellation of satellites
15 comprises one satellite or multiple satellites.
28. The method as claimed in any preceding claim, wherein the method is a computer implemented method.
29. A method of scheduling encryption key delivery communication sessions 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:
20 obtaining, for one satellite of the constellation of one or more satellites, information regarding an orbital path of the satellite and information regarding identities and locations of the plurality of user ground stations, and using the obtained information to determine the identities and locations of visible user ground stations of the plurality of
25 user ground stations which will be able to be carry out a communication session with the satellite during a duration of the schedule;
determining a time when each visible user ground station will be able to carry out the communication session with the satellite, obtaining meteorological information relating to a location of each of the visible user ground stations, and determining, based on the
30 obtained meteorological information, which of the visible user ground stations are user ground stations which will be sufficiently cloud free to carry out a communication session with the satellite at the respective determined time;
for each of the sufficiently cloud free user ground stations, obtaining information regarding the volume of encryption keys at the user ground station, and calculating a

priority for encryption key delivery to the user ground station based, at least in part, on the volume of encryption keys at the user ground station;

using the calculated priorities for encryption key delivery to the user ground stations and the determined times when each user ground station will be able to carry out a communication session with the satellite, generating a list of timings and priorities of target user ground stations for distribution of encryption keys from the satellite during the duration of the schedule; and

using the generated list to produce a key distribution schedule which identifies the timing of the communication sessions to be carried out between the satellite and the different user ground stations.

30. The method as claimed in claim 29, wherein the visible user ground stations are determined to be able to be carry out a communication session with the satellite during a duration of the schedule only when the satellite will be in eclipse.

31. The method as claimed in claim 29 or claim 30, and further comprising obtaining a duration of the schedule, and using the obtained information regarding an orbital path of the satellite, the obtained information regarding identities and locations of the plurality of user ground stations, and the obtained duration, to determine the identities and locations of visible user ground stations of the plurality of user ground stations which will be able to be carry out a communication session with the satellite during a duration of the schedule.

32. The method as claimed in any one of claims 29 to 31, and further comprising:

obtaining status information regarding the status of each of the visible user ground stations;

determining from the status information which of the visible user ground stations have a suitable status to carry out an encryption key delivery communication session with the satellite; and

using only the visible user ground stations determined to have a suitable status when determining which of the visible user ground stations are target user ground stations.

33. The method as claimed in any one of claims 29 to 32, wherein the time when each each visible user ground station will be able to carry out the communication session with the satellite is a time period.

34. The method as claimed in claim 33, wherein the time period when each each visible user ground station will be able to carry out the communication session with the satellite is determined by calculating a start time when the satellite reaches a first predetermined

- elevation when ascending from the point of view of the user ground station and a stop time when the satellite reaches a second predetermined elevation when descending from the point of view of the user ground station, and taking the time between the start time and the stop time as the time period when the visible user ground station will be able to carry out the communication session with the satellite.
- 5
35. The method as claimed in claim 34, wherein the first predetermined elevation and the second predetermined elevation are the same elevation.
36. The method as claimed in claim 35, wherein the elevation is 20°.
37. The method as claimed in any one of claims 29 to 36, wherein the meteorological information comprises cloud cover information, or wherein the meteorological information is used to predict cloud cover information, and the cloud cover information is used to determine which of the visible user ground stations are target user ground stations.
- 10
38. The method as claimed in any one of claims 29 to 37, wherein the meteorological information relates to an area centered on a location of each of the visible user ground stations.
- 15
39. The method as claimed in any one of claims 33 to 36, wherein the time period is broken down into a series of shorter time periods and the determining which of the visible user ground stations are target user ground stations which will be sufficiently cloud free to carry out a communication session with the satellite is carried out for each of the shorter time periods.
- 20
40. The method as claimed in any one of claims 29 to 39, and further comprising, for each of the sufficiently cloud free user ground stations, obtaining information regarding a required volume of encryption keys at the user ground station, and calculating a priority for encryption key delivery to the user ground station based, at least in part, on the volume of encryption keys at the user ground station and the required volume of encryption keys at the user ground station.
- 25
41. The method as claimed in any one of claims 29 to 40, and further comprising calculating an anticipated volume of encryption keys which can be transmitted between the satellite and each of the sufficiently cloud free user ground stations during a communication session, and using the calculated priorities for encryption key delivery to the user ground stations, the determined times when each user ground station will be able to carry out a communication session with the satellite, and the anticipated volume of encryption keys which can be transmitted between the satellite and each of the user ground station during
- 30

a communication session to generate the list of timings and priorities of user ground stations for distribution of encryption keys from the satellite during the duration of the schedule.

- 5 42. The method as claimed in any one of claims 29 to 41, wherein the encryption keys comprise secure encryption keys which are not matched, paired or grouped with encryption keys at other user ground stations and allocated encryption keys which are matched, paired or grouped with encryption keys at other user ground stations.
- 10 43. The method as claimed in claim 42, wherein the generating a list of timings and priorities of target user ground stations for distribution of encryption keys from the satellite during the duration of the schedule comprises:
- generating a first list of timings and priorities of target user ground stations for distribution of the secure encryption keys from the satellite during the duration of the schedule; and
- 15 generating a second list of timings and priorities of target user ground stations for distribution of encryption keys from the satellite for matching, pairing or grouping with secure encryption keys at those target user ground stations during the duration of the schedule; and
- both the first generated list and the second generated list are used to produce the key distribution schedule.
- 20 44. The method as claimed in claim 43, and further comprising determining, for each of the sufficiently cloud free user ground stations, a volume of encryption keys stored on the satellite available to be communicated to the user ground station for matching, pairing or grouping with secure encryption keys at the user ground station, and using the calculated priorities for encryption key delivery to the user ground stations, the determined times
- 25 when each user ground station will be able to carry out a communication session with the satellite, and the volume of encryption keys stored on the satellite available to be communicated to the user ground station for matching, pairing or grouping, to generate the list of timings and priorities of user ground stations for distribution of encryption keys from the satellite during the duration of the schedule.
- 30 45. The method as claimed in any one of claims 29 to 44, wherein the information regarding an orbital path of the satellite is an ephemeris of the satellite.
46. The method as claimed in any one of claims 29 to 45, wherein the encryption key delivery communication sessions are carried out by a methodology comprising:

- forming quantum optical communication links from a satellite of the constellation to two user ground stations to send respective photons of entangled pairs to each of the user ground stations;
- 5 detecting the quantum information of the respective photons at the two user ground stations; and
- conducting an encryption key agreement process between the two user ground stations using the detected quantum information to determine encryption keys.
47. The method as claimed in claim 46, wherein the quantum optical communication links
- 10 from the satellite to the two user ground stations use the E91 protocol.
48. The method as claimed in any one of claims 29 to 47, wherein the encryption key delivery communication sessions are carried out by a methodology comprising:
- generating a first string of random numbers on a satellite of the constellation;
- 15 using the first string of random numbers to form a first quantum optical communication link from the satellite to a first user ground station;
- conducting an encryption key agreement process between the satellite and the first user ground station using the first string of random numbers to determine a first encryption key;
- 20 storing the first encryption key on the satellite;
- and subsequently:
- generating a second string of random numbers on the satellite;
- 25 using the second string of random numbers to form a second quantum optical communication link from the satellite to a second user ground station associated with the first user ground station;
- conducting an encryption key agreement process between the satellite and the second user ground station using the second string of random numbers to determine a second encryption key;
- 30 sending one-time-pad "OTP" data of an OTP operation of the first encryption key and the second encryption key from the satellite to the second user ground station;
- using the second encryption key and the OTP data to derive the first encryption key at the second ground station.
49. The method as claimed in claim 48, wherein the methodology further comprises subsequently:
- 35 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 user ground station associated with the first user ground station and the second user ground station;

- conducting an encryption key agreement process between the satellite and the further user ground station using the further string of random numbers to determine a further encryption key;
- 5 sending OTP data of the first encryption key and the further encryption key from the satellite to the further user ground station;
- using the further encryption key and the OTP data to derive the first encryption key at the further ground station.
- 10 50. The method as claimed in any one of claims 29 to 49, wherein the encryption key delivery communication sessions are carried out by a methodology comprising:
- generating a string of random numbers on a satellite of the constellation;
- using the first string of random numbers to form a first quantum optical communication link from the satellite to a first user ground station;
- 15 conducting an encryption key agreement process between the satellite and the first user ground station using the first string of random numbers to determine a first encryption key;
- the first user ground station sending one-time-pad "OTP" data of an OTP operation of the first encryption key and a user encryption key to the satellite;
- 20 using the first encryption key and the OTP data to derive the user encryption key at the satellite;
- storing the user encryption key on the satellite;
- and subsequently:
- forming a second quantum optical communication link from the satellite to a second user ground station associated with the first user ground station;
- 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 a second user ground station;
- conducting an encryption key agreement process between the satellite and the second user ground station using the second string of random numbers to determine a
- 30 second encryption key;
- sending OTP data of the user encryption key and the second encryption key from the satellite to the second user ground station;
- using the second encryption key and the OTP data to derive the user encryption key at the second ground station.
- 35 51. The method as claimed in claim 50, 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 user ground station associated with the first user ground station and the second user ground station;

conducting an encryption key agreement process between the satellite and the
5 further user ground station using the further string of random numbers to determine a further encryption key;

sending OTP data of the user encryption key and the further encryption key from the satellite to the further user ground station;

10 using the further encryption key and the OTP data to derive the user encryption key at the further ground station.

52. The method as claimed in any of claims 48 to 51, wherein the OTP operation is an XOR operation and the OTP data is XOR data.

53. The method as claimed in any of claims 48 to 52, wherein the quantum optical communication links use a Prepare and Measure protocol, and preferably, the BB 84
15 Decoy State protocol.

54. The method as claimed in any one of claims 29 to 53, wherein satellites of the constellation are able to use multiple methodologies to carry out the encryption key delivery communication sessions.

55. The method as claimed in any one of claims 29 to 54, wherein the satellite quantum key distribution system further comprises at least one ground control station, and the method
20 further comprises:

determining, for each satellite of the constellation of one or more satellites, a communication time when the satellite will be able to communicate with the at least one ground control station;

25 determining a time at which generating a schedule for the satellite should start so that the generating a schedule can be completed before the communication time for the satellite; and

commencing the obtaining for each satellite of the constellation of one or more satellites before the determined time.

30 56. The method as claimed in any one of claims 29 to 55, wherein the constellation of satellites comprises one satellite or multiple satellites.

57. The method as claimed in any one of claims 29 to 56, wherein the method is a computer implemented method.

35

58. An apparatus arranged to schedule encryption key delivery communication sessions in a satellite quantum key distribution system comprising a constellation of one or more satellites and a plurality of user ground stations, the apparatus comprising:
- a priority list generation module arranged to produce a list of user ground stations requiring encryption keys;
 - a contact predictor module arranged to, for each satellite of the constellation of satellites:
 - determine a region of the earths surface within which the satellite can carry out encryption key delivery communication sessions to user ground stations using a quantum optical communications link during a scheduling period;
 - obtain a cloud cover map;
 - compare the locations of the listed user ground stations, the determined regions of the earths surface for the constellation of satellites, and the cloud cover map, to identify listed user ground stations to which encryption key delivery can be carried out by the constellation of satellites during the scheduling period; and
 - determine which of the identified user ground stations each satellite of the constellation of satellites will carry out encryption key delivery communication sessions with at different times in the scheduling period based upon one or more of:
 - an amount of unused encryption keys at each identified user ground station; and
 - an expected time duration before each identified user ground station runs out of encryption keys.
59. The apparatus as claimed in claim 58, wherein the contact predictor module is further arranged to determine which of the identified user ground stations each satellite of the constellation of satellites will carry out encryption key delivery communication sessions with at different times in the scheduling period based on an amount of encryption keys which were intended to be delivered to each identified user ground station in a previous scheduling period and were not delivered.
60. The apparatus as claimed in claim 58 or claim 59, wherein, when the encryption key delivery sessions require encryption keys to be stored in a satellite, the contact predictor module is further arranged to determine which of the identified user ground stations each satellite of the constellation of satellites will carry out encryption key delivery communication sessions with at different times in the scheduling period based on an amount of encryption keys stored on each satellite of the constellation of satellites.

61. The apparatus as claimed in any one of claims 58 to 60, wherein the contact predictor module is further arranged to determine which of the identified user ground stations each satellite of the constellation of satellites will carry out encryption key delivery communication sessions with at different times in the scheduling period based on the rate of encryption key delivery which can be supported by optical communication components of the user ground station.

62. The apparatus as claimed in any one of claims 58 to 61, wherein the contact predictor module is further arranged to determine which of the identified user ground stations each satellite of the constellation of satellites will carry out encryption key delivery communication sessions with at different times in the scheduling period based on a photon budget or communication link time budget required to deliver encryption keys from the satellite to the user ground station.

63. The apparatus as claimed in claim 62, wherein the photon budget or communication link time budget required to deliver encryption keys from the satellite to the user ground station is based on one or more of: geometrical factors of the relative positions of the user ground station and the satellite; atmospheric conditions; meteorological conditions; light pollution.

64. The apparatus as claimed in any one of claims 58 to 63, wherein the contact predictor module is further arranged to determine which of the identified user ground stations each satellite of the constellation of satellites will carry out encryption key delivery communication sessions with at different times in the scheduling period based on expected metrological and atmospheric conditions for the user ground station.

65. The apparatus as claimed in any one of claims 58 to 64, wherein the contact predictor module is further arranged to determine which of the identified user ground stations each satellite of the constellation of satellites will carry out encryption key delivery communication sessions with at different times in the scheduling period based on a possible length of an encryption key delivery communication session being limited by geometrical factors of the relative positions of the user ground station and the satellite.

66. The apparatus as claimed in any one of claims 58 to 65, wherein the encryption key delivery communication sessions are carried out by a methodology comprising:

forming quantum optical communication links from a satellite of the constellation to two user ground stations to send respective photons of entangled pairs to each of the user ground stations;

detecting the quantum information of the respective photons at the two user ground stations; and

conducting an encryption key agreement process between the two user ground stations using the detected quantum information to determine encryption keys.

- 5 67. The apparatus as claimed in claim 66, wherein the quantum optical communication links from the satellite to the two user ground stations use the E91 protocol.
68. The apparatus as claimed in any one of claims 58 to 67, wherein the encryption key delivery communication sessions are carried out by a methodology comprising:
- generating a first string of random numbers on a satellite of the constellation;
- using the first string of random numbers to form a first quantum optical
- 10 communication link from the satellite to a first user ground station;
- conducting an encryption key agreement process between the satellite and the first user ground station using the first string of random numbers to determine a first encryption key;
- storing the first encryption key 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 a second user ground station associated with the first user ground station;
- 20 conducting an encryption key agreement process between the satellite and the second user ground station using the second string of random numbers to determine a second encryption key;
- sending one-time-pad "OTP" data of an OTO operation of the first encryption key and the second encryption key from the satellite to the second user ground station;
- 25 using the second encryption key and the OTP data to derive the first encryption key at the second ground station.
69. The apparatus as claimed in any one of claims 58 to 68, wherein determining which of the identified user ground stations each satellite of the constellation of satellites will carry out encryption key delivery communication sessions with at different times in the scheduling period is further based on a number of encryption keys delivered to one or more user ground stations associated with each user ground station.
- 30 70. The apparatus as claimed in claim 69, wherein determining which of the identified user ground stations each satellite of the constellation of satellites will carry out encryption key delivery communication sessions with at different times in the scheduling period is carried out to ensure that common encryption keys are delivered to associated user ground stations as quickly as possible.
- 35

71. The apparatus as claimed in claim 68, wherein the methodology further comprises subsequently:
- generating a further encryption key on the satellite;
 - forming a further quantum optical communication link from the satellite to a further
 - 5 user ground station associated with the first user ground station and the second user ground station;
 - using the further encryption key to encode data into light of the further quantum optical communication link to send the further encryption key to the further user ground station;
 - 10 sending OTP data of the first encryption key and the further encryption key from the satellite to the further user ground station;
 - using the further encryption key and the OTP data to derive the first encryption key at the further ground station.
72. The apparatus as claimed in any one of claims 58 to 71, wherein the encryption key delivery communication sessions are carried out by a methodology comprising:
- generating a string of random numbers on a satellite of the constellation;
 - using the first string of random numbers to form a first quantum optical
 - communication link from the satellite to a first user ground station;
 - 20 conducting an encryption key agreement process between the satellite and the first user ground station using the first string of random numbers to determine a first encryption key;
 - the first user ground station sending one-time-pad "OTP" data of an OTP operation of the first encryption key and a user encryption key to the satellite;
 - 25 using the first encryption key and the OTP data to derive the user encryption key at the satellite;
 - storing the user encryption key on the satellite;
 - and subsequently:
 - forming a second quantum optical communication link from the satellite to a second
 - 30 user ground station associated with the first user ground station;
 - 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 a second user ground station;
 - conducting an encryption key agreement process between the satellite and the
 - 35 second user ground station using the second string of random numbers to determine a second encryption key;
 - sending OTP data of the user encryption key and the second encryption key from the satellite to the second user ground station;

using the second encryption key and the OTP data to derive the user encryption key at the second ground station.

73. The apparatus as claimed in claim 72, wherein the methodology further comprises subsequently:

- 5 generating a further encryption key on the satellite;
 forming a further quantum optical communication link from the satellite to a further user ground station associated with the first user ground station and the second user ground station;
 using the further encryption key to encode data into light of the further quantum
10 optical communication link to send the further encryption key to the further user ground station;
 sending OTP data of the user encryption key and the further encryption key from the satellite to the further user ground station;
 using the further encryption key and the OTP data to derive the user encryption key
15 at the further ground station.

74. The apparatus as claimed in any of claims 69 to 73, wherein the OTP operation is an XOR operation and the OTP data is XOR data.

75. The apparatus as claimed in any of claims 68 to 74, wherein the quantum optical communication links use a Prepare and Measure protocol, and preferably, the BB 84 Decoy
20 State protocol.

76. The apparatus as claimed in any one of claims 58 to 75, wherein satellites of the constellation are able to use multiple methodologies to carry out the encryption key delivery communication sessions.

77. The apparatus as claimed in claim 76, wherein the contact predictor module is
25 arranged to determine a region of the earths surface within which the satellite can carry out encryption key delivery communication sessions to user ground stations separately for each methodology which the satellite is able to use.

78. The apparatus as claimed in any one of claims 58 to 77, wherein the contact predictor module is arranged to determine a region of the earths surface within which the satellite can
30 carry out encryption key delivery communication sessions to user ground stations only for regions where the satellite will be in eclipse.

79. The apparatus as claimed in any one of claims 58 to 78, wherein the priority list generation module is arranged to produce a list of user ground stations requiring encryption

keys by placing a user ground station on the list if the amount of encryption keys stored at the user ground station is below a threshold value.

80. The apparatus as claimed in claim 79, wherein each user ground station has a respective threshold value.

5 81. The apparatus as claimed in claim 80, wherein the threshold value is based on a size of an encryption key store of the user ground station.

82. The apparatus as claimed in any one of claims 58 to 81, wherein the priority list generation module is arranged to produce a list of user ground stations requiring encryption keys by placing a user ground station on the list if an associated user ground station requiring
10 common encryption keys with the user ground station in order to support encryption based services between the user ground station and the associated user ground station is placed on the list.

83. The apparatus as claimed in any one of claims 58 to 82, wherein the contact predictor module is arranged to identify listed user ground stations to which encryption key delivery can
15 be carried out by the constellation of satellites during the scheduling period by comparing ephemeris data of the satellites of the constellation of one or more satellites.

84. The apparatus as claimed in any one of claims 58 to 83, wherein the constellation of satellites comprises one satellite or multiple satellites.

85. The apparatus as claimed in any one of claims 58 to 84, wherein the method is a
20 computer implemented method.

86. An apparatus arranged to schedule encryption key delivery communication sessions in a satellite quantum key distribution system comprising a constellation of one or more satellites and a plurality of user ground stations, the apparatus comprising:

25 means arranged to obtain, for one satellite of the constellation of one or more satellites, information regarding an orbital path of the satellite and information regarding identities and locations of the plurality of user ground stations, and to use the obtained information to determine the identities and locations of visible user ground stations of the plurality of user ground stations which will be able to be carry out a communication session with the satellite during a duration of the schedule;

30 means arranged to determine a time when each visible user ground station will be able to carry out the communication session with the satellite, obtain meteorological information relating to a location of each of the visible user ground stations, and determine, based on the obtained meteorological information, which of the visible user

ground stations are user ground stations which will be sufficiently cloud free to carry out a communication session with the satellite at the respective determined time;

means arranged to, for each of the sufficiently cloud free user ground stations, obtain information regarding the volume of encryption keys at the user ground station, and calculate a priority for encryption key delivery to the user ground station based, at least in part, on the volume of encryption keys at the user ground station;

means arranged to use the calculated priorities for encryption key delivery to the user ground stations and the determined times when each user ground station will be able to carry out a communication session with the satellite, to generate a list of timings and priorities of target user ground stations for distribution of encryption keys from the satellite during the duration of the schedule; and

means arranged to use the generated list to produce a key distribution schedule which identifies the timing of the communication sessions to be carried out between the satellite and the different user ground stations.

87. The apparatus as claimed in claim 86, wherein the visible user ground stations are determined to be able to be carry out a communication session with the satellite during a duration of the schedule only when the satellite will be in eclipse.

88. The apparatus as claimed in claim 86 or claim 87, and further comprising means arranged to obtain a duration of the schedule, and use the obtained information regarding an orbital path of the satellite, the obtained information regarding identities and locations of the plurality of user ground stations, and the obtained duration, to determine the identities and locations of visible user ground stations of the plurality of user ground stations which will be able to be carry out a communication session with the satellite during a duration of the schedule.

89. The apparatus as claimed in any one of claims 86 to 88, and further comprising means arranged to:

obtain status information regarding the status of each of the visible user ground stations;

determine from the status information which of the visible user ground stations have a suitable status to carry out an encryption key delivery communication session with the satellite; and

use only the visible user ground stations determined to have a suitable status when determining which of the visible user ground stations are target user ground stations

90. The apparatus as claimed in any one of claims 86 to 89, wherein the time when each each visible user ground station will be able to carry out the communication session with the satellite is a time period.

5 91. The apparatus as claimed in claim 90, wherein the time period when each each visible user ground station will be able to carry out the communication session with the satellite is determined by calculating a start time when the satellite reaches a first predetermined elevation when ascending from the point of view of the user ground station and a stop time when the satellite reaches a second predetermined elevation when
10 descending from the point of view of the user ground station, and taking the time between the start time and the stop time as the the time period when the visible user ground station will be able to carry out the communication session with the satellite.

92. The apparatus as claimed in claim 91, wherein the first predetermined elevation and the second predetermined elevation are the same elevation.

93. The apparatus as claimed in claim 92, wherein the elevation is 20°.

15 94. The apparatus as claimed in any one of claims 86 to 93, wherein the meteorological information comprises cloud cover information, or wherein the meteorological information is used to predict cloud cover information, and the cloud cover information is used to determine which of the visible user ground stations are target user ground stations.

20 95. The apparatus as claimed in any one of claims 85 to 94, wherein the meteorological information relates to an area centered on a location of each of the visible user ground stations.

96. The apparatus as claimed in any one of claims 91 to 95, wherein the time period is broken down into a series of shorter time periods and the determining which of the visible user ground stations are target user ground stations which will be sufficiently cloud free to
25 carry out a communication session with the satellite is carried out for each of the shorter time periods.

97. The apparatus as claimed in any one of claims 86 to 96, and further comprising means adapted to, for each of the sufficiently cloud free user ground stations, obtain information regarding a required volume of encryption keys at the user ground station, and
30 calculate a priority for encryption key delivery to the user ground station based, at least in part, on the volume of encryption keys at the user ground station and the required volume of encryption keys at the user ground station.

98. The apparatus as claimed in any one of claims 86 to 97, and further comprising means arranged to calculate an anticipated volume of encryption keys which can be transmitted between the satellite and each of the sufficiently cloud free user ground stations during a communication session, and using the calculated priorities for encryption key
5 delivery to the user ground stations, the determined times when each user ground station will be able to carry out a communication session with the satellite, and the anticipated volume of encryption keys which can be transmitted between the satellite and each of the user ground station during a communication session to generate the list of timings and priorities of user
10 ground stations for distribution of encryption keys from the satellite during the duration of the schedule.

99. The apparatus as claimed in any one of claims 86 to 98, wherein the encryption keys comprise secure encryption keys which are not matched, paired or grouped with encryption keys at other user ground stations and allocated encryption keys which are matched, paired or grouped with encryption keys at other user ground stations.

15 100. The apparatus as claimed in claim 99, wherein the generating a list of timings and priorities of target user ground stations for distribution of encryption keys from the satellite during the duration of the schedule comprises:

generating a first list of timings and priorities of target user ground stations for distribution of the secure encryption keys from the satellite during the duration of the
20 schedule; and

generating a second list of timings and priorities of target user ground stations for distribution of encryption keys from the satellite for matching, pairing or grouping with secure encryption keys at those target user ground stations during the duration of the
schedule; and

25 both the first generated list and the second generated list are used to produce the key distribution schedule.

101. The apparatus as claimed in claim 101, and further comprising means arranged to determine, for each of the sufficiently cloud free user ground stations, a volume of encryption
30 keys stored on the satellite available to be communicated to the user ground station for matching, pairing or grouping with secure encryption keys at the user ground station, and to use the calculated priorities for encryption key delivery to the user ground stations, the determined times when each user ground station will be able to carry out a communication session with the satellite, and the volume of encryption keys stored on the satellite available
35 to be communicated to the user ground station for matching, pairing or grouping, to generate the list of timings and priorities of user ground stations for distribution of encryption keys from the satellite during the duration of the schedule.

102. The apparatus as claimed in any one of claims 86 to 101, wherein the information regarding an orbital path of the satellite is an ephemeris of the satellite.

103. The apparatus as claimed in any one of claims 86 to 102, wherein the encryption key delivery communication sessions are carried out by a methodology comprising:

- 5 forming quantum optical communication links from a satellite of the constellation to two user ground stations to send respective photons of entangled pairs to each of the user ground stations;
 detecting the quantum information of the respective photons at the two user ground stations; and
10 conducting an encryption key agreement process between the two user ground stations using the detected quantum information to determine encryption keys.

104. The apparatus as claimed in claim 103, wherein the quantum optical communication links from the satellite to the two user ground stations use the E91 protocol.

- 15 105. The apparatus as claimed in any one of claims 86 to 104, wherein the encryption key delivery communication sessions are carried out by a methodology comprising:
 generating a first string of random numbers on a satellite of the constellation;
 using the first string of random numbers to form a first quantum optical communication link from the satellite to a first user ground station;
20 conducting an encryption key agreement process between the satellite and the first user ground station using the first string of random numbers to determine a first encryption key;
 storing the first encryption key 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 a second user ground station associated with the first user ground station;
 conducting an encryption key agreement process between the satellite and the
30 second user ground station using the second string of random numbers to determine a second encryption key;
 sending one-time-pad "OTP" data of an OTP operation of the first encryption key and the second encryption key from the satellite to the second user ground station;
 using the second encryption key and the OTP data to derive the first encryption key
35 at the second ground station.

106. The apparatus as claimed in claim 105, 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
 - 5 communication link from the satellite to a further user ground station associated with the first user ground station and the second user ground station;
 - conducting an encryption key agreement process between the satellite and the further user ground station using the further string of random numbers to determine a further encryption key;
 - 10 sending OTP data of the first encryption key and the further encryption key from the satellite to the further user ground station;
 - using the further encryption key and the OTP data to derive the first encryption key at the further ground station.
107. The apparatus as claimed in any one of claims 86 to 106, wherein the encryption key
- 15 delivery communication sessions are carried out by a methodology comprising:
 - generating a string of random numbers on a satellite of the constellation;
 - using the first string of random numbers to form a first quantum optical communication link from the satellite to a first user ground station;
 - conducting an encryption key agreement process between the satellite and the first
 - 20 user ground station using the first string of random numbers to determine a first encryption key;
 - the first user ground station sending one-time-pad "OTP" data of an OTP operation of the first encryption key and a user encryption key to the satellite;
 - using the first encryption key and the OTP data to derive the user encryption key at
 - 25 the satellite;
 - storing the user encryption key on the satellite;
 - and subsequently:
 - forming a second quantum optical communication link from the satellite to a second user ground station associated with the first user ground station;
 - 30 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 a second user ground station;
 - conducting an encryption key agreement process between the satellite and the second user ground station using the second string of random numbers to determine a
 - 35 second encryption key;
 - sending OTP data of the user encryption key and the second encryption key from the satellite to the second user ground station;

using the second encryption key and the OTP data to derive the user encryption key at the second ground station.

108. The apparatus as claimed in claim 107, wherein the methodology further comprises subsequently:

- 5 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 user ground station associated with the first user ground station and the second user ground station;
 conducting an encryption key agreement process between the satellite and the
10 further user ground station using the further string of random numbers to determine a further encryption key;
 sending OTP data of the user encryption key and the further encryption key from the satellite to the further user ground station;
 using the further encryption key and the OTP data to derive the user encryption key
15 at the further ground station.

109. The apparatus as claimed in any of claims 105 to 108, wherein the OTP operation is an XOR operation and the OTP data is XOR data.

110. The apparatus as claimed in any of claims 105 to 109, wherein the quantum optical communication links use a Prepare and Measure protocol, and preferably, the BB 84 Decoy
20 State protocol.

111. The apparatus as claimed in any one of claims 86 to 110, wherein satellites of the constellation are able to use multiple methodologies to carry out the encryption key delivery communication sessions.

112. The apparatus as claimed in any one of claims 86 to 111, wherein the satellite
25 quantum key distribution system further comprises at least one ground control station, and the apparatus further comprises:
 means arranged to determine, for each satellite of the constellation of one or more satellites, a communication time when the satellite will be able to communicate with the at least one ground control station;
30 means arranged to determine a time at which generating a schedule for the satellite should start so that the generating a schedule can be completed before the communication time for the satellite; and
 wherein the means arranged to obtain, for each satellite of the constellation of one or more satellites, is arranged to commence the obtaining before the determined time

113. The apparatus as claimed in any one of claims 86 to 112, wherein the constellation of satellites comprises one satellite or multiple satellites.

114. 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,
5 wherein the apparatus is configured to implement the computer-implemented method according to any of claims 1 to 28.

115. 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,
10 wherein the apparatus is configured to implement the computer-implemented method according to any of claims 29 to 57.

116. A computer-readable medium comprising code or computer instructions stored 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 28.

117. A computer-readable medium comprising code or computer instructions stored
15 thereon, which when executed by a processor unit, causes the processor unit to perform the computer-implemented method according to any one of claims 29 to 57.

118. A method of scheduling encryption key delivery communication sessions 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:

20 for each satellite of the constellation of satellites, identifying user ground stations requiring encryption keys with which the satellite can carry out encryption key delivery communication sessions using a quantum optical communications link during a scheduling period;

25 obtaining cloud cover information;
comparing the locations of the identified user ground stations, and the cloud cover information, to identify user ground stations to which encryption key delivery can be carried out by the satellite during the scheduling period; and

30 determining which of the identified user ground stations to which encryption key delivery can be carried out the satellite will carry out encryption key delivery communication sessions with at different times in the scheduling period based upon one or more of:

an amount of unused encryption keys at each identified user ground station;
and
35 an expected time duration before each identified user ground station runs out of encryption keys.