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:

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;

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

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

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 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 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 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:

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.

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 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;

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;

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;

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 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 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 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 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;

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;

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;

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 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 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 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;

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 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 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 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.

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.

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.

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 comprises one satellite or multiple satellites.

28. The method as claimed in any preceding claim, wherein the method is a computer implemented method.

29. 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.

30. The apparatus as claimed in claim 29, 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.

31. The apparatus as claimed in claim 29 or claim 30, 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.

32. The apparatus as claimed in any one of claims 29 to 31, 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.

33. The apparatus as claimed in any one of claims 29 to 32, 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.

34. The apparatus as claimed in claim 33, 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.

35. The apparatus as claimed in any one of claims 29 to 34, 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.

36. The apparatus as claimed in any one of claims 29 to 35, 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.

37. The apparatus as claimed in any one of claims 29 to 36, 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.

38. The apparatus as claimed in claim 37, wherein the quantum optical communication links from the satellite to the two user ground stations use the E91 protocol.

39. The apparatus as claimed in any one of claims 29 to 38, 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;

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:

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 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;

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

40. The apparatus as claimed in any one of claims 29 to 39, 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.

41. The apparatus as claimed in claim 40, 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.

42. The apparatus as claimed in claim 39, 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 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;

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.

43. The apparatus as claimed in any one of claims 29 to 42, 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;

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;

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;

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 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.

44. The apparatus as claimed in claim 43, 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 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;

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.

45. The apparatus as claimed in any of claims 40 to 44, wherein the OTP operation is an XOR operation and the OTP data is XOR data.

46. The apparatus as claimed in any of claims 39 to 45, wherein the quantum optical communication links use a Prepare and Measure protocol, and preferably, the BB 84 Decoy State protocol.

47. The apparatus as claimed in any one of claims 29 to 46, wherein satellites of the constellation are able to use multiple methodologies to carry out the encryption key delivery communication sessions.

48. The apparatus as claimed in claim 47, wherein the contact predictor module is 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.

49. The apparatus as claimed in any one of claims 29 to 48, wherein the contact predictor module is 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 only for regions where the satellite will be in eclipse.

50. The apparatus as claimed in any one of claims 29 to 49, 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.

51. The apparatus as claimed in claim 50, wherein each user ground station has a respective threshold value.

52. The apparatus as claimed in claim 51, wherein the threshold value is based on a size of an encryption key store of the user ground station.

53. The apparatus as claimed in any one of claims 29 to 52, 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 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.

54. The apparatus as claimed in any one of claims 29 to 53, wherein the contact predictor module is arranged to identify listed user ground stations to which encryption key delivery can 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.

55. The apparatus as claimed in any one of claims 29 to 54, wherein the constellation of satellites comprises one satellite or multiple satellites.

56. The apparatus as claimed in any one of claims 29 to 55, wherein the method is a computer implemented method.

57. 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 28.

58. 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.

59. 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:

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;

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

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

an expected time duration before each identified user ground station runs out of encryption keys.