

Claims

1. A computer-implemented method of quantum key distribution between a first device and a second device, the method, performed by an intermediary device, comprising:
  - transmitting a first secret symbol string over a first quantum channel to the first
  - 5 device, each symbol of the first secret symbol string modulated by a basis state randomly selected from a set of bases;
  - transmitting a first basis set over a first communication channel to the first device, the first basis set comprising data representative of the randomly selected bases used to modulate each symbol of the first secret symbol string;
  - 10 transmitting a second secret symbol string over a second quantum channel to the second device, each symbol of the second secret symbol string modulated by a basis state randomly selected from the set of bases;
  - transmitting a second basis set over a second communication channel to the second device, the second basis set comprising data representative of the randomly selected bases
  - 15 used to modulate each symbol of the second secret symbol string;
  - generating a third symbol string based on combining the first and second secret symbol strings;
  - transmitting to the second device, via the second communication channel, data representative of the third symbol string;
  - 20 wherein the first device and second device perform a quantum key exchange based on:
    - the first device using the received first basis set to determine a first received set of secret symbols comprising symbols of the first secret symbol string transmitted over the first quantum channel that were successfully received by the first device;
    - 25 the second device uses the received second basis set to determine a second received set of secret symbols comprising symbols of the second secret symbol string transmitted over the second quantum channel that were successfully received by the second device;
    - the second device generates a fourth set of symbols based on combining the second received set of secret symbols with the received third symbol string, wherein one or more symbols of the fourth set of symbols correspond to one or more symbols of the first symbol string;
    - 30 the first device and second device performing symbol sifting operations over a third communication channel between the based on the first received set of secret symbols at the first device and the fourth set of symbols at the second device for
    - 35 generating a common set of sifted symbols for forming a cryptographic key at the first and second devices.

2. The computer-implemented method according to claim 1, further comprising:  
receiving from the first device, over the first communication channel, data  
representative of the symbol positions of the symbols in the first secret symbol string  
transmitted over the first quantum communication channel that were successfully received by  
5 the first device;  
generating a first set of symbols based on those symbols of the first secret symbol  
string that correspond to the received data representative of the symbol positions of symbols  
from the first secret symbol string successfully received by the first device;  
receiving from the second device, over the second communication channel, data  
10 representative of the symbol positions of the symbols in the second secret symbol string  
transmitted over the second quantum communication channel that were successfully received  
by the second device;  
generating a second set of symbols based on those symbols of the second secret  
symbol string that correspond to the received data representative of the symbol positions of  
15 symbols from the second secret symbol string successfully received by the second device;  
and  
said generating the third symbol string further comprising generating the third symbol  
string based on combining the first set of symbols and second set of symbols.
3. The computer-implemented method according to claims 1 or 2, the method further  
20 comprising, prior to transmitting the randomly selected bases to the first device, performing  
said receiving from the first device, over the first communication channel, data representative  
of the symbol positions of the symbols in the first secret symbol string transmitted over the  
first quantum communication channel that were successfully received by the first device.
4. The computer-implemented method according to any of claims 1 to 3, the method  
25 further comprising, prior to transmitting the randomly selected bases to the second device,  
performing said receiving from the second device, over the second communication channel,  
data representative of the symbol positions of the symbols in the second secret symbol string  
transmitted over the second quantum communication channel that were successfully received  
by the second device.
- 30 5. The computer-implemented method according to claims 1 to 4, the method further  
comprising the first device and second device performing a quantum key exchange based on:  
the first device forms the first received set of secret symbols based on the  
received first basis set and the symbols that were successfully received from the first  
secret symbol string transmitted over the first quantum communication channel,  
35 wherein each symbol of the first received set of secret symbols is a symbol of the first  
secret symbol string that was successfully received by the first device in which the

basis used for receiving said symbol matches the corresponding basis in the received first basis set used to transmit said symbol;

5           the second device forms the second received set of secret symbols based on the received second basis set and the symbols that were successfully received from the second secret symbol string transmitted over the second quantum communication channel, wherein each symbol of the second received set of secret symbols is a symbol of the second secret symbol string that was successfully received by the second device in which the basis used for receiving said symbol matches the corresponding basis in the received second basis set used to transmit said symbol;

10           the second device generates the fourth set of symbols based combining the second received set of secret symbols with the received third symbol string, wherein one or more symbols of the fourth set of symbols correspond to one or more symbols of the first set of symbols;

15           the first device and second device performing symbol sifting operations over the third communication channel therebetween based on the first received set of secret symbols at the first device and the fourth set of symbols at the second device for generating a common set of sifted symbols for forming a cryptographic key at the first and second devices.

20           6.       The computer-implemented method according to any one of claims 2 to 5, wherein said generating the third symbol string further comprising:

in response to determining the length of the first set of symbols is less than the length of the second set of symbols:

truncating the second set of symbols to the length of the first set of symbols;

and

25           generating the third symbol string based on combining the first set of symbols with the truncated second set of symbols;

in response to determining the length of the second set of symbols is less than the length of the first set of symbols:

truncating the first set of symbols to the length of the second set of symbols;

30           and

generating the third symbol string based on combining the truncated first set of symbols with the second set of symbols.

35           7.       The computer-implemented method according to any one of claims 2 to 6, wherein said generating the third symbol string further comprising:

in response to determining the length of the first set of symbols is less than the length of the second set of symbols:

- adjusting the second set of symbols by removing an agreed set of symbols from the second set of symbols until the adjusted length of the adjusted second set of symbols is the same as the first set of symbols; and
- 5 generating the third symbol string based on combining the first set of symbols with the adjusted second set of symbols;
- in response to determining the length of the second set of symbols is less than the length of the first set of symbols:
- adjusting the first set of symbols by removing an agreed set of symbols from the first set of symbols until the adjusted length of the adjusted first set of symbols is
- 10 the same as the second set of symbols; and
- generating the third symbol string based on combining the adjusted first set of symbols with the second set of symbols.
8. The computer-implemented method according to any one of claims 2 to 7, wherein generating the third symbol string further comprises one or more from the group of:
- 15 generating the third symbol string based on performing an XOR operation using data representative of a first set of bits and a second set of bits, the first set of bits based on converting each of the symbols in the first set of symbols to a string of bits and the second set of bits based on converting each of the symbols in the second set of symbols to a string of bits;
- 20 generating the third bit string based on performing one time pad encryption operation(s) using data representative of, at least in part, the first set of symbols and the second set of symbols; and
- generating the third symbol string based on performing any other type of operation for obfuscating one or more symbols of the first set of symbols using the second set of symbols.

9. The computer-implemented method according to any one of claims 2 to 8, wherein the second device generating the fourth symbol string further comprises one or more from the group of:
- 5 generating the fourth symbol string based on performing an XOR operation using the second received set of secret symbols and the received third symbol string;
- generating the fourth symbol string based on performing one time pad decryption operation(s) using the received second set of secret symbols and the third secret symbol string; and
- 10 generating the fourth symbol string based on performing any other type of operation for extracting one or more symbols of the first secret symbol string using the second received set of secret symbols and the third symbol string.
10. The computer-implemented method according to any preceding claim, wherein generating the third symbol string further comprises one or more from the group of:
- 15 generating the third symbol string based on performing an XOR operation using data representative of, at least in part, the first secret symbol string and the second secret symbol string;
- generating the third symbol string based on performing one time pad encryption operation(s) using data representative of, at least in part, the first secret symbol string and the second secret symbol string; and
- 20 generating the third symbol string based on performing any other type of operation for obfuscating one or more symbols of the first secret symbol string using the second secret symbol string.
11. The computer-implemented method according to any preceding claim, wherein the second device generating the fourth symbol string further comprises one or more from the group of:
- 25 generating the fourth symbol string based on performing an XOR operation using data representative of, at least in part, the second secret symbol string and the third symbol string;
- generating the fourth symbol string based on performing one time pad decryption operation(s) using data representative, of at least in part, the second secret symbol string and the third secret symbol string; and
- 30 generating the fourth symbol string based on performing any other type of operation for extracting one or more symbols of the first secret symbol string using data representative of, at least in part, the second secret symbol string and the third symbol string.

12. The computer-implemented method according to any preceding claim, wherein the first device and second device performing symbol sifting operations over the third communication channel therebetween based on:

5 the first device forms a first matching basis set based on the first received set of secret symbols, wherein the first matching basis set includes all the basis states the first device used to receive the symbols of the first received set of secret symbols that match the corresponding basis states of the received first basis set used to transmit said symbol of the first set of symbols; and

10 the first device sends over the third communication channel data representative of the first matching basis set to the second device;

the second device forms a second matching basis set based on the second received set of secret symbols, wherein the second matching basis set includes all the basis states the second device used to receive the symbols of the second received set of secret symbols that match the corresponding basis states of the received second basis set used to transmit said symbol of the second set of symbols;

15 the second device sends over the third communication channel data representative of the second matching basis set to the first device;

20 the first device generates a first common set of sifted symbols based on discarding each symbol in the first received set of secret symbols in which the corresponding basis in the first matching basis set is different to the corresponding basis in the received second matching basis set;

25 the second device generates a second common set of sifted symbols based on discarding each symbol in the fourth set of symbols in which the corresponding basis in the received first matching basis set is different to the corresponding basis in the second matching basis set; and

the first and second devices forming a cryptographic key based on the first and second common set of sifted symbols, respectively.

13. The computer-implemented method according to claim 12, wherein the first and second device perform error detection and/or correction on the first and second common sets of sifted bits.

14. A computer-implemented method of quantum key distribution between a first device and a second device, the method, performed by the first device, comprising:

35 receiving, from an intermediary device, over a quantum channel a first secret symbol string, wherein the intermediary device modulated each symbol of the first secret symbol string using a basis state of a basis selected at random from a set of bases for transmission over the quantum channel;

demodulating the received first secret symbol string, where each received first secret symbol is demodulated using a basis state of a basis selected at random from the set of bases;

5 receiving, from the intermediary device, data representative of a first basis set over a first communication channel, the first basis set comprising data representative of the randomly selected bases used by the intermediary device to modulate each symbol of the first secret symbol string;

determining a first received set of secret symbols from the received first secret symbol string that are successfully received using the received first basis set;

10 performing sifting operation(s) with the second device using the first received set of secret symbols of the first device and another set of secret symbols determined by the second device for generating a common sifted set of symbols for forming a cryptographic key with the second device, wherein the other set of secret symbols are associated with the first received set of secret symbols; and

15 the second device determines the other set of secret symbols based on, at least in part, a second secret symbol string received by the second device over a second quantum channel from the intermediary device and, at least in part, a third secret symbol string received by the second device over a second communication channel from the intermediary device, wherein the third secret symbol string is based on a combination of, at least in part,  
20 the second secret symbol string and the first secret symbol string, and the second device generates the other set of secret symbols based on a combination of the received third secret symbol string and, at least in part, the second secret symbol string.

15. The computer-implemented method according to claim 14, further comprising transmitting, to the intermediary device, over the first communication channel, data  
25 representative of the symbol positions of the symbols in the first secret symbol string that were successfully received by the first device over the quantum communication channel.

16. The computer-implemented method according to claim 15, the method further comprising, prior to receiving the first basis set, performing said transmitting from the first device to the intermediary device over the first communication channel data representative of  
30 the symbol positions of the symbols in the first secret symbol string successfully received by the first device over the quantum communication channel.

17. The computer-implemented method according to claims 15 to 16, the method further comprising the first device and second device performing a quantum key exchange based on:  
35 forming the first received set of secret symbols based on the received first basis set and the symbols that were successfully received from the first secret symbol string transmitted by the intermediary device over the quantum communication channel, wherein

each symbol of the first received set of secret symbols is a symbol of the first secret symbol string that was successfully received by the first device in which the basis used for receiving said symbol matches the corresponding basis in the received first basis set used to transmit said symbol;

- 5            wherein the second device forms a second received set of secret symbols based on a received second basis set and the symbols that were successfully received from the second secret symbol string transmitted by the intermediary device over the second quantum channel, wherein each symbol of the second received set of secret symbols is a symbol of the second secret symbol string that was successfully received by the second device in which the  
10        basis used for receiving said symbol matches the corresponding basis in the received second basis set used to transmit said symbol; and

- the second device generates the other set of symbols based on combining the second received set of secret symbols with the received third symbol string, wherein one or more symbols of the other set of symbols correspond to one or more symbols of the first set  
15        of symbols; and

             performing symbol sifting operations with the second device over the third communication channel based on the first received set of secret symbols at the first device and the other set of symbols at the second device for generating a common set of sifted symbols for forming a cryptographic key at the first and second devices.

- 20        18.        The computer-implemented method according to claims 14 to 17, wherein the combination of the second secret symbol string and the first secret symbol string comprises generating the third symbol string using an XOR operation on data representative of the second secret symbol string and the first secret symbol string.

- 25        19.        The computer-implemented method according to any one of claims 14 to 18, wherein generating the third symbol string further comprises one or more from the group of:

             generating the third symbol string based on performing an XOR operation using data representative of, at least in part, the first secret symbol string and the second secret symbol string;

- 30               generating the third symbol string based on performing one time pad encryption operation(s) using data representative of, at least in part, the first secret symbol string and the second secret symbol string; and

             generating the third symbol string based on performing any other type of operation for obfuscating one or more symbols of the first secret symbol string using the second secret symbol string.

20. The computer-implemented method according to any one of claims 14 to 19, wherein the second device generating the other symbol string further comprises one or more from the group of:

- 5 generating the other symbol string based on performing an XOR operation using data representative of, at least in part, the received second secret symbol string and the received third symbol string;
- generating the other symbol string based on performing one time pad decryption operation(s) using data representative, of at least in part, the received second secret symbol string and the received third secret symbol string; and
- 10 generating the other symbol string based on performing any other type of operation for extracting one or more symbols of the first secret symbol string using data representative of, at least in part, the received second secret symbol string and the received third symbol string.

21. The computer-implemented method according to any of claims 14 to 20, wherein performing the symbol sifting operations with the second device over the third communication channel further comprising:

- forming a first matching basis set based on the first received set of secret symbols, wherein the first matching basis set includes all the basis states the first device used to receive the symbols of the first received set of secret symbols that match the corresponding basis states of the received first basis set used by the intermediary device to transmit said symbol of the first secret symbol string; and

transmitting to the second device over the third communication channel data representative of the first matching basis set, wherein:

- receiving from the second device over the third communication channel data representative of a second matching basis set, wherein the second device forms the second matching basis set based on the second received set of secret symbols, wherein the second matching basis set includes all the basis states the second device used to receive the symbols of the second received set of secret symbols that match the corresponding basis states of the received second basis set used by the intermediary device to transmit said symbol of the second secret symbol string;

- generating a first common set of sifted symbols based on discarding each symbol in the first received set of secret symbols in which the corresponding basis in the first matching basis set is different to the corresponding basis in the received second matching basis set, wherein the second device generates a second common set of sifted symbols based on discarding each symbol in the other set of secret symbols in which the corresponding basis in the received first matching basis set is different to the corresponding basis in the second matching basis set; and

forming a cryptographic key based on the first common set of sifted symbols, wherein the second device forms the cryptographic key based on the second common set of sifted symbols.

22. The computer-implemented method according to claim 21, further comprising
- 5 performing error detection and/or correction with the second device on the first and second common sets of sifted symbols.
23. A computer-implemented method of quantum key distribution between a first device and a second device, the method, performed by the second device, comprising:
- 10 receiving, from an intermediary device, over a quantum channel a second secret symbol string, wherein the intermediary device modulated each symbol of the second secret symbol string using a basis state of a basis selected at random from a set of bases;
- demodulating the received second secret symbol string, where each received second secret symbol is demodulated using a basis state of a basis selected at random from the set of bases;
- 15 receiving data representative of the randomly selected bases used to modulate each symbol of the second secret symbol string by the intermediary device;
- determining a second set of secret symbols from the received second secret symbol string that are validly received based on comparing the randomly selected bases used to demodulate the second secret symbol string and the received randomly selected bases used
- 20 to modulate the second secret symbol string;
- receiving, from the intermediary device, data representative of a third symbol string, the third symbol string generated by the intermediary device based on a combination of, at least in part, the second secret symbol string and a first secret symbol string, the first secret symbol string sent from the intermediary device to the first device over another quantum
- 25 channel;
- determining a fourth set of secret symbols based on combining, at least in part, the received third symbol string with the received second set of secret symbols; and
- performing sifting with the first device using the fourth set of secret symbols and another set of secret symbols determined by the first device for generating a common sifted
- 30 set of symbols for forming a cryptographic key, wherein the other set of secret symbols are associated with the first secret symbol string that is determined to be validly received by the first device.

24. The computer-implemented method according to claim 23, further comprising transmitting, to the intermediary device, over the second communication channel, data representative of the symbol positions of the symbols in the second secret symbol string that were successfully received over the quantum channel.
- 5 25. The computer-implemented method according to claims 23 or 24, the method further comprising, prior to receiving the second basis set, performing said transmitting from the second device to the intermediary device over the second communication channel data representative of the symbol positions of the symbols in the second secret symbol string successfully received by the second device over the quantum communication channel.
- 10 26. The computer-implemented method according to claims 15 to 16, the method further comprising the first device and second device performing a quantum key exchange based on:  
forming a second received set of secret symbols based on the received second basis set and the symbols that were successfully received from the second secret symbol string transmitted by the intermediary device over the second quantum channel, wherein each  
15 symbol of the second received set of secret symbols is a symbol of the second secret symbol string that was successfully received by the second device in which the basis used for receiving said symbol matches the corresponding basis in the received second basis set used to transmit said symbol; and  
the second device generates the fourth set of symbols based on combining the  
20 second received set of secret symbols with the received third symbol string, wherein one or more symbols of the fourth set of symbols correspond to one or more symbols of the first set of symbols; and  
wherein the first device forms the first received set of secret symbols based on a received first basis set and the symbols that were successfully received from the first secret  
25 symbol string transmitted by the intermediary device over the other quantum communication channel to the first device, wherein each symbol of the first received set of secret symbols is a symbol of the first secret symbol string that was successfully received by the first device in which the basis used for receiving said symbol matches the corresponding basis in the received first basis set used to transmit said symbol;
- 30 performing symbol sifting operations with the first device over the third communication channel based on the first received set of secret symbols at the first device and the fourth set of symbols at the second device for generating a common set of sifted symbols for forming a cryptographic key at the first and second devices.
27. The computer-implemented method according to claims 23 to 26, wherein the  
35 combination of the second secret symbol string and the first secret symbol string comprises

generating the third symbol string using an XOR operation on data representative of the second secret symbol string and the first secret symbol string.

28. The computer-implemented method according to any one of claims 23 to 27, wherein generating the third symbol string by the intermediary device further comprises one or more
- 5 from the group of:
- generating the third symbol string based on performing an XOR operation using data representative of, at least in part, the first secret symbol string and the second secret symbol string;
  - generating the third symbol string based on performing one time pad encryption

10 operation(s) using data representative of, at least in part, the first secret symbol string and the second secret symbol string; and

  - generating the third symbol string based on performing any other type of operation for obfuscating one or more symbols of the first secret symbol string using the second secret symbol string.
- 15 29. The computer-implemented method according to any one of claims 23 to 28, wherein generating the fourth symbol string further comprises one or more from the group of:
- generating the fourth symbol string based on performing an XOR operation using data representative of, at least in part, the received second secret symbol string and the received third symbol string;
  - generating the fourth symbol string based on performing one time pad decryption

20 operation(s) using data representative, of at least in part, the received second secret symbol string and the received third secret symbol string; and

  - generating the fourth symbol string based on performing any other type of operation for extracting one or more symbols of the first secret symbol string using data representative

25 of, at least in part, the received second secret symbol string and the received third symbol string.
30. The computer-implemented method according to any of claims 23 to 29, wherein performing the symbol sifting operations with the first device over the third communication channel further comprising:
- the first device forming a first matching basis set based on a first received set of secret symbols, wherein the first matching basis set includes all the basis states the first device used to receive the symbols of the first received set of secret symbols that match the corresponding basis states of the received first basis set used by the intermediary device to transmit said symbol of the first secret symbol string; and

35 receiving at the second device over the third communication channel data representative of the first matching basis set;

- transmitting to the first device over the third communication channel data representative of a second matching basis set, wherein the second device forms the second matching basis set based on the second received set of secret symbols, wherein the second matching basis set includes all the basis states the second device used to receive the
- 5 symbols of the second received set of secret symbols that match the corresponding basis states of the received second basis set used by the intermediary device to transmit said symbol of the second secret symbol string;
- generating a second common set of sifted symbols based on discarding each symbol in the fourth set of secret symbols in which the corresponding basis in the received first
- 10 matching basis set is different to the corresponding basis in the second matching basis set, wherein the first device generates a first common set of sifted symbols based on discarding each symbol in the first received set of secret symbols in which the corresponding basis in the first matching basis set is different to the corresponding basis in the received second matching basis set; and
- 15 forming a cryptographic key based on the first common set of sifted symbols, wherein the second device forms the cryptographic key based on the second common set of sifted symbols.
31. The computer-implemented method according to claim 30, further comprising performing error detection and/or correction with the second device on the first and second
- 20 common sets of sifted symbols.
32. A computer-implemented method of quantum key distribution between a first device and a second device, the method comprising:
- transmitting, by an intermediary device, a first secret symbol string over a first quantum channel to the first device, each symbol of the first secret symbol string modulated
- 25 by a basis state randomly selected from a set of bases;
- transmitting, by the intermediary device, a first basis set over a first communication channel to the first device, the first basis set comprising data representative of the randomly selected bases used to modulate each symbol of the first secret symbol string;
- transmitting, by the intermediary device, a second secret symbol string over a second
- 30 quantum channel to the second device, each symbol of the second secret symbol string modulated by a basis state randomly selected from the set of bases;
- transmitting, by the intermediary device, a second basis set over a second communication channel to the second device, the second basis set comprising data representative of the randomly selected bases used to modulate each symbol of the second
- 35 secret symbol string;
- generating, by the intermediary device, a third symbol string based on combining the first and second secret symbol strings;

transmitting, by the intermediary device, to the second device, via the second communication channel, data representative of the third symbol string;

5 determining, by the first device, a first received set of secret symbols using the received first basis set, the first received set of secret symbols comprising symbols of the first secret symbol string transmitted over the first quantum channel that were successfully received by the first device;

10 determining, by the second device, a second received set of secret symbols using the received second basis set, the second received set of secret symbols comprising symbols of the second secret symbol string transmitted over the second quantum channel that were successfully received by the second device;

generating, by the second device, a fourth set of symbols based on combining the second received set of secret symbols with the received third symbol string, wherein one or more symbols of the fourth set of symbols correspond to one or more symbols of the first symbol string;

15 performing, by the first device and second device, symbol sifting operations over a third communication channel the based on the first received set of secret symbols at the first device and the fourth set of symbols at the second device for generating a common set of sifted symbols for forming a cryptographic key at the first and second devices.

33. The computer-implemented method according to claim 32, further comprising:

20 transmitting, by the first device, over the first communication channel to the intermediary device data representative of the symbol positions of the symbols in the first secret symbol string transmitted by the intermediary device over the first quantum communication channel that were successfully received by the first device;

25 generating, at the intermediary device, a first set of symbols based on those symbols of the first secret symbol string that correspond to the data representative of the symbol positions of symbols from the first secret symbol string successfully received by the first device;

30 transmitting, by the second device, over the second communication channel to the intermediary device data representative of the symbol positions of the symbols in the second secret symbol string transmitted by the intermediary device over the second quantum communication channel that were successfully received by the second device;

35 generating, at the intermediary device, a second set of symbols based on those symbols of the second secret symbol string that correspond to the received data representative of the symbol positions of symbols from the second secret symbol string successfully received by the second device; and

said generating, by the intermediary device, the third symbol string further comprising generating, by the intermediary device, the third symbol string based on combining the first set of symbols and second set of symbols.

34. The computer-implemented method according to claims 32 or 33, the method further comprising:

- 5 prior to transmitting the randomly selected bases to the first device, performing said receiving from the first device, over the first communication channel, data representative of the symbol positions of the symbols in the first secret symbol string transmitted over the first quantum communication channel that were successfully received by the first device; and
- 10 prior to transmitting the randomly selected bases to the second device, performing said receiving from the second device, over the second communication channel, data representative of the symbol positions of the symbols in the second secret symbol string transmitted over the second quantum communication channel that were successfully received by the second device.

35. The computer-implemented method according to claims 33 to 34, the method further comprising the first device and second device performing a quantum key exchange by:

5 determining, by the first device, a first received set of secret symbols based on the received first basis set and the symbols that were successfully received from the first secret symbol string transmitted over the first quantum communication channel, wherein each symbol of the first received set of secret symbols is a symbol of the first secret symbol string that was successfully received by the first device in which the basis used for receiving said symbol matches the corresponding basis in the received first basis set used to transmit said symbol;

10 determining, by the second device, a second received set of secret symbols based on the received second basis set and the symbols that were successfully received from the second secret symbol string transmitted over the second quantum communication channel, wherein each symbol of the second received set of secret symbols is a symbol of the second secret symbol string that was successfully received by the second device in which the basis used for receiving said symbol matches the corresponding basis in the received second basis set used to transmit said symbol;

15 generating, by the second device, the fourth set of symbols based combining the second received set of secret symbols with the received third symbol string, wherein one or more symbols of the fourth set of symbols correspond to one or more symbols of the first set of symbols;

20 performing sifting operations between the first device and second device over the third communication channel based on the first received set of secret symbols at the first device and the fourth set of symbols at the second device for generating a common set of sifted symbols for forming a cryptographic key at the first and second devices.

25

36. The computer-implemented method according to any one of claims 32 to 35, wherein said generating the third symbol string further comprising:

30 in response to determining the length of the first set of symbols is less than the length of the second set of symbols:

truncating the second set of symbols to the length of the first set of symbols;

and

generating the third symbol string based on combining the first set of symbols with the truncated second set of symbols;

35 in response to determining the length of the second set of symbols is less than the length of the first set of symbols:

truncating the first set of symbols to the length of the second set of symbols;

and

generating the third symbol string based on combining the truncated first set of symbols with the second set of symbols.

37. The computer-implemented method according to any one of claims 32 to 36, wherein said generating the third symbol string further comprising:

5 in response to determining the length of the first set of symbols is less than the length of the second set of symbols:

adjusting the second set of symbols by removing an agreed set of symbols from the second set of symbols until the adjusted length of the adjusted second set of symbols is the same as the first set of symbols; and

10 generating the third symbol string based on combining the first set of symbols with the adjusted second set of symbols;  
in response to determining the length of the second set of symbols is less than the length of the first set of symbols:

15 adjusting the first set of symbols by removing an agreed set of symbols from the first set of symbols until the adjusted length of the adjusted first set of symbols is the same as the second set of symbols; and

generating the third symbol string based on combining the adjusted first set of symbols with the second set of symbols.

38. The computer-implemented method according to any one of claims 32 to 37, wherein generating the third symbol string further comprises one or more from the group of:

20 generating the third symbol string based on performing an XOR operation using data representative of a first set of symbols and a second set of symbols, the first set of symbols based on converting each of the symbols in the first set of symbols to a string of symbols and the second set of symbols based on converting each of the symbols in the second set of  
25 symbols to a string of symbols;

generating the third symbol string based on performing one time pad encryption operation(s) using data representative of, at least in part, the first set of symbols and the second set of symbols; and

30 generating the third symbol string based on performing any other type of operation for obfuscating one or more symbols of the first set of symbols using the second set of symbols.

39. The computer-implemented method according to any one of claims 32 to 38, wherein the second device generating the fourth symbol string further comprises one or more from the group of:

35 generating the fourth symbol string based on performing an XOR operation using the second received set of secret symbols and the received third symbol string;

generating the fourth symbol string based on performing one time pad decryption operation(s) using the received second set of secret symbols and the third secret symbol string; and

- 5 generating the fourth symbol string based on performing any other type of operation for extracting one or more symbols of the first secret symbol string using the second received set of secret symbols and the third symbol string.

40. The computer-implemented method according to any one of claims 32 to 39, wherein generating the third symbol string further comprises one or more from the group of:

- 10 generating the third symbol string based on performing an XOR operation using data representative of, at least in part, the first secret symbol string and the second secret symbol string;

generating the third symbol string based on performing one time pad encryption operation(s) using data representative of, at least in part, the first secret symbol string and the second secret symbol string; and

- 15 generating the third symbol string based on performing any other type of operation for obfuscating one or more symbols of the first secret symbol string using the second secret symbol string.

41. The computer-implemented method according to any one of claims 32 to 40, wherein the second device generating the fourth symbol string further comprises one or more from the group of:

- 20 generating the fourth symbol string based on performing an XOR operation using data representative of, at least in part, the second secret symbol string and the third symbol string;

- 25 generating the fourth symbol string based on performing one time pad decryption operation(s) using data representative, of at least in part, the second secret symbol string and the third secret symbol string; and

generating the fourth symbol string based on performing any other type of operation for extracting one or more symbols of the first secret symbol string using data representative of, at least in part, the second secret symbol string and the third symbol string.

- 30 42. The computer-implemented method according to any one of claims 32 to 41, wherein the first device and second device performing symbol sifting operations over the third communication channel therebetween based on:

- 35 the first device forms a first matching basis set based on the first received set of secret symbols, wherein the first matching basis set includes all the basis states the first device used to receive the symbols of the first received set of secret symbols that match the

corresponding basis states of the received first basis set used to transmit said symbol of the first set of symbols; and

the first device sends over the third communication channel data representative of the first matching basis set to the second device;

5 the second device forms a second matching basis set based on the second received set of secret symbols, wherein the second matching basis set includes all the basis states the second device used to receive the symbols of the second received set of secret symbols that match the corresponding basis states of the received second basis set used to transmit said symbol of the second set of symbols;

10 the second device sends over the third communication channel data representative of the second matching basis set to the first device;

the first device generates a first common set of sifted symbols based on discarding each symbol in the first received set of secret symbols in which the corresponding basis in the first matching basis set is different to the corresponding basis in the received second

15 matching basis set;

the second device generates a second common set of sifted symbols based on discarding each symbol in the fourth set of secret symbols in which the corresponding basis in the received first matching basis set is different to the corresponding basis in the second matching basis set; and

20 the first and second devices forming a cryptographic key based on the first and second common set of sifted symbols, respectively.

43. The computer-implemented method according to any one of claims 32 to 42, wherein the first device and second device performing symbol sifting operations over the third communication channel therebetween based on:

25 generating, by the first device, a first basis flag set based on the first received set of secret symbols and the received first basis set, wherein the first basis flag set includes an indication of each valid and invalid symbol of the first received set of secret symbols based on comparing the received first basis set with the basis set used by the first device to demodulate the symbols associated with the first received set of secret symbols; and

30 sending, from the first device over the third communication channel, data representative of the first basis flag set to the second device;

generating, by the second device, a second basis flag set based on the second received set of secret symbols and the received second basis set, wherein the second basis flag set includes an indication of each valid and invalid symbol of the second received set of secret symbols based on comparing the received second basis set with the basis set used by the second device to demodulate the symbols associated with the second received set of secret symbols;

35

- sending, from the second device over the third communication channel, data representative of the second basis flag set to the first device;
- generating, by the first device, a first common set of sifted symbols based on discarding each symbol in the first received set of secret symbols in which the corresponding indication in the first basis flag set is different to the corresponding indication in the received second basis flag set;
- generating, by the second device, a second common set of sifted symbols based on discarding each symbol in the fourth set of secret symbols in which the corresponding indication in the second basis flag set is different to the corresponding indication in the received first basis flag set;
- performing error detection and correction between the first and second common sets of sifted symbols to generate a common set of sifted symbols; and
- generating a cryptographic key at the first and second devices based on the common set of sifted symbols.
44. The computer-implemented method according to any preceding claim, wherein each symbol represents  $2^n$  binary bits, for  $n > 1$ .
45. The computer-implemented method as claimed in any preceding claim, wherein each symbol represents a binary bit for  $n = 1$ .
46. The computer-implemented method according to any preceding claim, further comprising generating a first secret symbol string by randomly selecting a symbols using a random number generator.
47. The computer-implemented method according to any preceding claim, further comprising generating a second secret symbol string by randomly selecting symbols using a random number generator.
48. The computer-implemented method according to claims 46 or 47, wherein the random number generator is based on one or more from the group of:
- a cryptographic random number generator;
  - a quantum qubit random number generator; or
  - any suitable random number generator.
49. The computer-implemented method according to any preceding claim, wherein the set of bases comprises at least two bases, each basis comprising at least two basis states, wherein the at least two basis states of each basis are orthogonal and the at least two basis states of said each basis are non-orthogonal to the at least two basis states of another basis of the set of bases.

50. The computer-implemented method according to claim 49, wherein the set of bases comprises two bases and each basis of the set of bases comprises two basis states.

51. The computer-implemented method according to claims 49 or 50, wherein the set of bases for modulating symbols for transmission over the first or second quantum channel

5 comprises at least two bases from the group of:

a rectilinear basis;

a diagonal basis;

a spherical basis;

a circular basis; and

10 any other type of basis comprising two basis states.

52. The computer-implemented method according to claim 51, wherein the first and second quantum channels are optical quantum channels and the set of bases comprises at least two bases from the group of:

a rectilinear photon polarisation basis;

15 a diagonal photon polarisation basis;

a spherical photon polarisation basis;

a circular photon polarisation basis; and

any other type of photon basis comprising two basis states.

53. The computer-implemented method according to any preceding claim, wherein the  
20 first communication channel is based on a classical communication channel formed between the intermediary device and the first device.

54. The computer-implemented method according to any preceding claim, wherein the second communication channel is based on a classical communication channel formed between the intermediary device and the second device.

25 55. The computer-implemented method as claimed in any of claims 53 or 54, wherein the classical communication channel is based on one or more types of communication channels from the group of:

optical communication channel;

free-space optical communication channel;

30 wireless communication channel;

wired communication channel;

radio communication channel;

microwave communication channel;

satellite communication channel;

35 terrestrial communication channel;

optical fibre communication channel;  
optical laser communication channel;  
any other type of one or more optical, wireless and/or wired communication  
channel(s) for transmitting data between devices; and  
5 two or more optical, wireless and/or wired communication channel(s) that form a  
composite communication channel for transmitting data between devices.

56. The computer-implemented method as claimed in any preceding claim, wherein a  
quantum communication channel is based on one or more types of quantum communication  
channels from the group of:  
10 optical quantum communications;  
free-space optical quantum communications;  
optical fibre quantum communications;  
optical laser quantum communications;  
any other type of quantum communications for transmitting data over a quantum  
15 communication channel between devices.

57. The computer-implemented method as claimed in any preceding claim, wherein the  
intermediary device is a satellite apparatus, the first device and second device are satellite  
ground stations or devices, wherein the first quantum communication channel is a free-space  
20 optical quantum communication channel, the second quantum communication channel is a  
free-space optical quantum communication channel, and the first and second communication  
channels are non-quantum satellite communications channels.

58. The computer-implemented method as claimed in any of claims 1 to 56, wherein the  
intermediary device is a ground station or device, the first device and second device are  
25 satellites, wherein the first quantum communication channel is a free-space optical quantum  
communication channel, the second quantum communication channel is a free-space optical  
quantum communication channel, and the first and second communication channels are non-  
quantum satellite communications channels.

59. The computer-implemented method as claimed in any of claims 1 to 56, wherein the  
intermediary device is a terrestrial communication apparatus, the first device and second  
30 device are terrestrial devices, wherein the first quantum communication channel is a fibre  
optic quantum communication channel, the second quantum communication channel is a fibre  
optic quantum communication channel, and the first and second communication channels are  
classical terrestrial communications channels.

60. The computer-implemented method as claimed in any of claims 1 to 56, wherein the intermediary device is a terrestrial communication apparatus, the first device and second device are terrestrial devices, wherein the first quantum communication channel is a free-space optic quantum communication channel, the second quantum communication channel is a free-space optic quantum communication channel, and the first and second communication channels are classical terrestrial communications channels.
61. The computer-implemented method as claimed in any of claims 1 to 56, wherein the intermediary device is a terrestrial communication apparatus, the first device and second device are terrestrial devices, wherein the first quantum communication channel is a free-space optic quantum communication channel, the second quantum communication channel is a fibre optic quantum communication channel, and the first and second communication channels are classical terrestrial communications channels.
62. The computer-implemented method as claimed in any preceding claim, wherein the first and second communications channels are encrypted communication channels.
63. The computer-implemented method as claimed in claim 62, further comprising encrypting transmission data or messages prior to transmitting said data or messages to: the first device over the first classical communication channel; or the second device over the second classical communication channel.
64. The computer-implemented method as claimed in any preceding claim, wherein one or more authentication protocols are used by the intermediary device and the first or second device for authenticating the intermediary, first or second devices prior to communicating over the first or second communications channels.
65. The computer-implemented method as claimed in claim 64, further comprising authenticating the first and second device prior to transmitting data to the first and second device over the first and second communication channels, respectively.
66. The computer-implemented method as claimed in any preceding claim, further comprising selecting a decoy state protocol from a set of decoy state protocols for use in transmitting data over the first or second quantum channels.
67. An intermediary apparatus comprising a processor unit, a memory unit, and a communication interface, the processor unit connected to the memory unit and the communication interface, wherein the processor unit, memory unit and communication interface are adapted to implement the computer-implemented method as claimed in any of claims 1 to 13 or 44 to 66 when dependent on claims 1 to 13.

68. An apparatus comprising a processor unit, a memory unit, and a communication interface, the processor unit connected to the memory unit and the communication interface, wherein the processor unit, memory unit and communication interface are adapted to implement the computer-implemented method as claimed in any of claims 14 to 22 or 44 to 66 when dependent on claims 14 to 22.
69. An apparatus comprising a processor unit, a memory unit, and a communication interface, the processor unit connected to the memory unit and the communication interface, wherein the processor unit, memory unit and communication interface are adapted to implement the computer-implemented method as claimed in any of claims 23 to 31 or 44 to 66 when dependent on claims 23 to 31.
70. A system comprising:  
an intermediary device comprising an apparatus according to claim 67;  
an first device comprising an apparatus according to claim 68; and  
a second device comprising an apparatus according to claim 69;  
wherein the intermediary device, first device and second device are configured to communicate with each other for establishing a shared a cryptographic key between the first and second devices.
71. A system comprising an intermediary device, a first device and a second device, wherein the intermediary device, first device and second device are configured to implement the corresponding steps of the computer-implemented method according to any of claims 32 to 43 or 44 to 66 when dependent on claims 32 to 43.
72. The system as claimed in claims 70 or 71, wherein the system is a satellite quantum key distribution system comprising a plurality of satellites, each satellite including the functionality of an intermediary device, each satellite in communication with one or more ground receiving stations, and each ground receiving station including the functionality of the first and/or second devices.
73. A computer-readable medium comprising computer code or instructions stored thereon, which when executed on a processor, causes the processor to perform the computer implemented method according to any of claims 1 to 13 or 44 to 66 when dependent on claims 1 to 13.
74. A computer-readable medium comprising computer code or instructions stored thereon, which when executed on a processor, causes the processor to perform the computer implemented method according to any of claims 14 to 22 or 44 to 66 when dependent on claims 14 to 22.

75. A computer-readable medium comprising computer code or instructions stored thereon, which when executed on a processor, causes the processor to perform the computer implemented method according to any of claims 23 to 31 or 44 to 66 when dependent on claims 23 to 31.

- 5 76. A computer-readable medium comprising computer code or instructions stored thereon, which when executed on one or more processor(s), causes the one or more processor(s) to perform the computer implemented method according to any of claims 32 to 43 or 44 to 66 when dependent on claims 32 to 43.