Claims

1. A quantum key generation method, comprising:

receiving, by a quantum reception device, a quantum transmission from a quantum transmission device, the quantum transmission including encoded quantum bits for obtaining a quantum key; and

decoding and detecting the quantum bits from the quantum transmission to obtain a detected bit-sequence,

wherein the encoding or the decoding of the quantum bits uses a key generation bit-sequence received from an encryptor device, the encryptor device being configured to perform post-processing to obtain a quantum key and detect tampering.

2. The quantum key generation method according to claim 1, further comprising:

obtaining a derived value from the detected bit-sequence; and

verifying that the derived value is consistent with an expected value of the derived value corresponding to a test value of a same statistical characteristic that is dependent on a statistical property of a key generation bit-sequence used for encoding or decoding of quantum bits to detect tampering.

3. The quantum key generation method according to claim 2, wherein verifying that the derived value is consistent with an expected value of the derived value comprises:

obtaining a first detection probability of the quantum bits with basis selection made based on test bits of the key generation bit-sequence;

obtaining a second detection probability of the quantum bits with basis selection made based on non-test bits of the key generation bit-sequence; and

verifying the consistency of the first detection probability and the second detection probability to detect tampering.

4. The quantum key generation method according to claim 2, wherein the derived value comprises an indicator of the statistical characteristic and wherein verifying that the derived value is consistent with the expected value of the derived value comprises verifying that the indicator of the statistical characteristic is consistent with an expected value of the indicator of the statistical characteristic.

5. The quantum key generation method according to claim 4, further comprising:

generating the key generation bit-sequence; and

obtaining the test value of the statistical characteristic, wherein obtaining the test value of the statistical characteristic comprises calculating the test value from the generated key generation bit-sequence.

6. The quantum key generation method according to claim 5, wherein calculating the test value from the generated key generation bit-sequence comprises:

splitting the key generation bit-sequence into a plurality of test blocks; and

calculating a block statistical property of each of the plurality of test blocks, the statistical characteristic being dependent on the block statistical property of each of the plurality of test blocks.

7. The quantum key generation method according to claim 6, wherein the block statistical property is a statistical bias.

8. The quantum key generation method according to claim 5, wherein the steps of generating the key generation bit-sequence, and obtaining the test value of the statistical characteristic comprise:

identifying the test value of the statistical characteristic; and

generating the key generation bit-sequence based on the identified test value of the statistical characteristic.

9. The quantum key generation method according to claim 8, further comprising:

generating an initial bit-sequence comprising an initial statistical property; and

inserting one or more test blocks, each comprising one or more test bits, into the initial bit-sequence to generate the key generation bit-sequence associated with the statistical characteristic being dependent on a block statistical property of each of the one or more test blocks, the initial statistical property and the block statistical property being different; the key generation bit-sequence being used for encoding or decoding quantum bits to obtain the quantum key.

10. The quantum key generation method according to claim 9, wherein the block statistical property is a statistical bias, and the statistical bias p of each of the plurality of test blocks is chosen such as to satisfy $1/\sqrt{(2M)}<p<1/\sqrt{L}$, where L is the

size of each of the plurality of test blocks and 2M is the total number of bits, and wherein the biases of all of the plurality of test blocks approximately cancel out.

11. A quantum key generation system, comprising:

a quantum reception device configured to receive a quantum transmission including encoded quantum bits for obtaining a quantum key and to detect the quantum bits from the quantum transmission to obtain a detected bit-sequence;

a quantum transmission device configured to send the quantum transmission to the quantum reception device;

a first encryptor device configured to generate a first key generation bit-sequence;

a second encryptor device configured to receive the detected bit-sequence from the quantum reception device;

a first communication link; and

a second communication link,

wherein the first key generation bit-sequence is transmitted from the first encryptor device to the quantum transmission device via the first communication link for encoding the quantum bits,

wherein the detected bit-sequence is transmitted from the quantum reception device to the second encryptor via the second communication link,

wherein the first encryptor device and the second encryptor device perform post-processing to obtain a quantum key and detect tampering.

12. The quantum key generation system according to claim 11, wherein the second encryptor device is configured to generate a second key generation bit-sequence, and wherein the second key generation bit-sequence is transmitted from the second encryptor device to the quantum reception device for measurement basis selection.

13. The quantum key generation system according to claim 12, wherein a derived value is obtained from the detected bit-sequence, and wherein the obtained derived value is verified to be consistent with an expected value of the derived value corresponding to a test value of a same statistical characteristic that is dependent on a statistical property of the first key generation bit-sequence or the second key generation bit-sequence to detect tampering.

14. The quantum key generation system according to claim 13, wherein the first key generation bit-sequence or the second key generation bit-sequence includes at least one test block, a statistical property of the first key generation bit-sequence or the second key generation bit-sequence being associated with a block statistical property of the at least one test block.

15. The quantum key generation system according to claim 14, further comprising:

an initial bit-sequence generator configured to generate an initial bit-sequence comprising an initial statistical property; and

a number processor configured to insert at least one test block each containing one or more test bits, into the initial bit-sequence to generate the first key generation bit-sequence or the second key generation bit-sequence, the initial statistical property and the block statistical property being different; the first key generation bit-sequence or the second key generation bit-sequence being used for encoding or decoding the quantum bits to obtain the quantum key.

16. The quantum key generation system according to claim 14, further comprising:

a bit-sequence generator configured to generate the first key generation bit-sequence or the second key generation bit-sequence for encoding or decoding the quantum bits to obtain the quantum key; and

a number processor configured to split the first key generation bit-sequence or the second key generation bit-sequence into the at least one test block, and calculate the block statistical property of the at least one test block to determine a statistical characteristic being dependent on the block statistical property of the at least one test block.

17. A quantum key generation method, comprising:

generating a key generation bit-sequence by inserting one or more test blocks into an initial bit-sequence or by using a bit-sequence generator;

transmitting the key generation bit-sequence to a quantum transmission device over a first communication link or to a quantum reception device over a second communication link;

using the key generation bit-sequence for encoding at the quantum transmission device, or decoding at the quantum reception device;

transmitting the encoded quantum bits from the quantum transmission device to the quantum reception device;

decoding and detecting the quantum bits from the quantum transmission to obtain a detected bit-sequence;

receiving the detected bit-sequence from the quantum reception device over the second communication link;

obtaining a first detection probability of the quantum bits with basis selection made based on test bits of the key generation bit-sequence;

obtaining a second detection probability of the quantum bits with basis selection made based on non-test bits of the key generation bit-sequence;

verifying the consistency of the first detection probability and the second detection probability to detect tampering; and

performing post-processing to obtain a quantum key.

18. The quantum key generation method according to claim 17, wherein the biases of all the one or more test blocks approximately cancel out, and wherein a true bias and a block length of each of the one or more test blocks are chosen to enable the true bias to be hidden.

19. The quantum key generation method according to claim 18, further comprising:

aggregating all detected bits in the detected bit-sequence with positions corresponding to positively biased test blocks into a first check block and all detected bits in the detected bit-sequence with positions corresponding to negatively biased test blocks into a second check block;

obtaining a derived value in the form of a sample bias for both the first check block and the second check block; and

verifying that the overall sample bias value of corresponding test blocks of the key generation bit-sequence is retained for both the first and second check blocks to detect tampering.

20. The quantum key generation method according to claim 17, wherein the key generation bit sequence is generated using the bit-sequence generator, the test blocks are obtained from the key generation bit-sequence.