CLAIMS

1. A method of creating symmetric keying material shared between a first node and a second node, the method comprising:
establishing a key-generation channel between the first node and the second node;
sharing master keying material comprising at least a first master key between the first node and the second node using physical layer security methods on the key-generation channel;
generating a first amount of random numbers as local keying material on the first node, wherein the local keying material has a larger size than the master keying material;
encrypting the local keying material using the first master key to generate encrypted local keying material on the first node;
sending the encrypted local keying material from the first node to the second node over a communication channel, wherein the communication channel has a higher throughput than the key-generation channel; and
decrypting the encrypted local keying material on the second node using the first master key to recover the local keying material at the second node as the symmetric keying material shared between the first node and the second node and having a larger size than the master keying material shared over the key-generation channel.
2. The method according to claim 1, wherein the key generation channel is a quantum communication channel.
3. The method according to claim 1 or 2, wherein the key generation channel and/or the communication channel are free space channels, and optionally wherein the first node is a satellite node and the second node is a ground node.
4. The method according to any one of claims 1 to 3, wherein the communication channel is an optical channel, and optionally wherein an optical link in the form of a beam is used for the key-generation channel and/or the channel.
5. The method according to any one of claims 1 to 4, further comprising:
generating a second amount of random numbers as additional local keying material on the second node;
encrypting the additional local keying material using the first master key to generate encrypted additional local keying material on the second node;

sending the encrypted additional local keying material from the second node to the first node over the communication channel; and

decrypting the encrypted additional local keying material on the first node to create additional symmetric keying material shared between the first node and the second node.

6. The method according to any one of claims 1 to 5, further comprising:

establishing a second key-generation channel between the first node and a third node;

sharing second master keying material comprising at least a second master key between the first node and the third node using physical layer security methods on the second key-generation channel;

encrypting the local keying material using the second master key to generate a second encrypted local keying material on the first node;

sending the second encrypted local keying material from the first node to the third node over a second communication channel, wherein the second communication channel has a higher throughput than the second key-generation channel; and

decrypting the second encrypted local keying material on the third node using the second master key to recover the local keying material as second symmetric keying material shared between the first node and the third node and having a larger size than the second master keying material shared over the key-generation channel.

7. The method according to claim 6, wherein the second key generation channel is a quantum communication channel.

8. The method according to any one of claims 1 to 7 wherein encrypting the local keying material using the first master key to generate encrypted local keying material comprises encrypting the local keying material according to an advanced encryption standard (AES) algorithm wherein an AES key is generated using the first master key as a seed key, and wherein sending the encrypted local keying material from the first node to the second node over the communication channel comprises sending the local keying material encrypted according to the AES algorithm.

9. A first node of a communication system, the first node comprising:

a physical layer security module configured to:

establish a key-generation channel between the first node and a second node of the communication system; and

share master keying material comprising at least a first master key between the first node and the second node using physical layer security methods on the key-generation channel;

a random number generator configured to:

generate a first amount of random numbers as local keying material, wherein the local keying material has a larger size than the master keying material;

a key management module configured to:

encrypt the local keying material using the first master key to generate encrypted local keying material; and

a communication module configured to:

send the encrypted local keying material to the second node over a communication channel for recovering the local keying material at the second node as symmetric keying material shared between the first node and the second node and having a larger size than the master keying material shared over the key-generation channel, wherein the communication channel has a higher throughput than the key-generation channel.

10. The first node according to claim 9, wherein the key-generation channel is a quantum communication channel.

11. The first node according to claim 9 or 10, wherein the communication module is further configured to receive encrypted additional keying material from the second node over the communication channel; and the key management module is further configured to decrypt the encrypted additional keying material using the first master key to create additional symmetric keying material.

12. The first node according to any one of claims 9 to 11, configured as a satellite.

13. The first node according to any one of claims 9 to 12, wherein an optical link in the form of a beam is used for the key-generation channel and/or the communication channel.

14. The first node according to any one of claims 9 to 13, wherein the key management module is configured to operate according to an advanced encryption standard (AES) algorithm wherein an AES key is generated using the first master key as a seed key.

15. A second node of a communication system, the second node comprising:

a physical layer security module configured to:

establish a key-generation channel between the second node and a first node of the communication system; and

generate shared master keying material comprising at least a master key using physical layer security on the key-generation channel;

a communication module configured to:

receive encrypted local keying material from the first node over a communication channel, wherein the local keying material has a larger size than the master keying material and wherein the communication channel has a higher throughput than the key-generation channel; and

a key management module configured to:

decrypt the encrypted local keying material using the master key to recover the local keying material at the second node as symmetric keying material shared between the first node and the second node and having a larger size than the master keying material shared over the key-generation channel.

16. The second node according to claim 15, wherein the key-generation channel is a quantum communication channel.

17. The second node according to any one of claims 15 to 16, wherein the second node is a ground node.

18. The second node according to any one of claims 15 to 17, wherein an optical link in the form of a beam is used for the key-generation channel and/or the communication channel.

19. The second node according to any one of claims 15 to 18, wherein the key management module is configured to operate according to an advanced encryption standard (AES) algorithm wherein an AES key is generated using the master key as a seed key.

20. A communication system comprising a first node according to any one of claims 9 to 14; and a second node according to any one of claims 15 to 19.