CLAIMS

1. A method of creating symmetric keying material shared between a first node and a second node, the method comprising:
establishing a ~~free space~~ key-generation channel between the first node and the second node;
generating shared symmetric master keying material using physical layer security methods on the ~~free space~~ key-generation channel;
generating random numbers as local keying material on the first node;
encrypting the local keying material using some or all of the shared symmetric master keying material 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 ~~free space optical~~ communication channel ~~in the form of a beam~~, wherein the ~~free space optical~~ communication channel has a higher throughput than the ~~free space~~ key-generation channel; and
decrypting the encrypted local keying material on the second node using the corresponding shared symmetric master keying material to create the symmetric keying material having a larger size than the shared symmetric master keying material.

2. The method according to claim 1, wherein the ~~free space~~ 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 ~~both~~ the ~~free space~~ key-generation channel and/or the ~~free space optical~~ channel.

5. The method according to any one of claims 1 to 4, further comprising:
generating random numbers as additional local keying material on the second node;
encrypting the additional local keying material using some or all of the shared symmetric master keying material 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 thea ~~free space optical~~ communication channel ~~in the form of a beam~~; and

decrypting the encrypted additional local keying material on the first node to create additional symmetric keying material.

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

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

generating second shared symmetric master keying material using physical layer security methods on the second ~~free space~~ key-generation channel;

encrypting local keying material using some or all of the second shared symmetric master keying material 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 ~~free space optical~~ communication channel ~~in the form of a beam~~, wherein the second ~~free space optical~~ communication channel has a higher throughput than the second~~free space~~ key-generation channel; and

decrypting the second encrypted local keying material on the third node using the corresponding second shared symmetric master keying material having a larger size than the second shared symmetric master keying material.

7. The method according to claim 6, wherein the second ~~free space~~ 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 some or all of the shared symmetric master keying material 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 some or all of the shared symmetric master keying material as a seed key, and wherein sending the encrypted local keying material from the first node to the second node over the ~~free space optical~~ communication channel comprises sending the local keying material encrypted according to thean AES algorithm.

~~9. A method in a first node of sharing symmetric keying material with a second node, the method comprising:~~

~~establishing a free space key-generation channel with the second node;~~

generating shared symmetric master keying material using physical security methods on the free space key-generation channel;

generating a random number as local keying material;

encrypting the local keying material using some or all of the shared symmetric master keying material to generate encrypted local keying material; and

sending the encrypted local keying material to the second node over a free space optical communication channel in the form of a beam, wherein the free space optical communication channel has a higher throughput than the free space keygeneration

channel.

10. The method according to claim 9, further comprising:

receiving encrypted additional keying material from the second node over the free space optical communication channel; and

decrypting the encrypted additional keying material using the shared symmetric master keying material to create additional symmetric keying material.

11. The method according to claim 9 or claim 10, further comprising:

establishing a second free space key-generation channel with a third node;

generating second shared symmetric master keying material using physical security methods on the second free space key-generation channel;

encrypting the local keying material using some or all of the second shared symmetric master keying material to generate second encrypted local keying material; and

sending the second encrypted local keying material to the third node over a second free space optical communication channel in the form of a beam, wherein the second free space optical communication channel has a higher throughput than the free space key-generation channel.

21

12. The method according to any one of claims 9 to 11, wherein the free space key-generation channel is a quantum channel.

13. The method according to any one of claims 9 to 12, wherein the first node is a satellite node and the second node is a ground node.

14. The method according to any one of claims 9 to 13, wherein an optical link in the form of a beam is used for both the free space key-generation channel and the free space optical communication channel.

15. The method according to any one of claims 9 to 14, wherein encrypting the local keying material using some or all of the shared symmetric master keying material 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 some or all of the shared symmetric master keying material as a seed key, and wherein sending the encrypted local keying material to the second node over the free space optical communication channel comprises sending the local keying material encrypted according to an AES algorithm.

16. A method in a second node of receiving symmetric keying material from a first node, the method comprising:

establishing a free space key-generation channel with the first node;

generating shared symmetric master keying material using physical layer security on the free space key-generation channel;

receiving encrypted local keying material from the first node over a free space optical communication channel in the form of a beam, wherein the second free space optical communication channel has a higher throughput than the free space keygeneration

channel; and

decrypting the encrypted local keying material key using the shared symmetric master keying material to create symmetric keying material.

17. The method according to claim 16, wherein the key-distribution channel is a quantum communication channel.

18. The method according to any one of claims 16 to 17, wherein the local keying material is encrypted using some or all of the shared symmetric master keying material 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 some or all of the shared symmetric master keying material as a seed key, and the local keying material is sent to the first node encrypted according to an AES algorithm.

19. The method according to any one of claims 16 to 18, wherein the first node is a satellite node and the second node is a ground node.

20. The method according to any one of claims 16 to 19, wherein an optical link in the form of a beam is used for both the free space key-generation channel and the

~~free space optical communication channel.~~

9~~21~~. A first node of a communication system, the first node comprising:

a physical layer security module configured to:

establish a ~~free space~~ key-distribution channel between the first node and a ~~secpmd~~second node of the communication system; and

generate shared symmetric master keying material using a physical layer security method on the ~~free space~~ key-distribution channel;

a random number generator configured to:

generate random numbers as local keying material;

a key management module configured to:

encrypt the local keying material using the using the some or all of the shared symmetric master keying material to generate encrypted local keying material; and

a communication module configured to:

send the encrypted local keying material to the second node over a ~~free space optical~~ communication channel ~~in the form of a beam~~ for generating symmetric keying material for use between the first node and the second node, the symmetric keying material having a larger size than the shared symmetric master keying material, wherein the ~~free space optical~~ communication channel has a higher throughput than the ~~free space~~ key-generation channel.

10~~22~~. The first node according to claim 9~~21~~, wherein the ~~free space~~ key-distribution channel is a quantum communication channel.

11~~23~~. The first node according to claim 9 or 10~~21, or 22~~, wherein the communication module is further configured to receive encrypted additional keying material from the first node over the ~~free space optical~~ communication channel; and the key management module is further configured to decrypt the encrypted additional keying material using the shared symmetric master keying material to create additional symmetric keying material.

~~24. The first node according to any one of claims 21 to 23, wherein the physical layer security module is further configured to establish a second free space keydistribution~~

~~channel with a third node of the communication system; and generate second shared symmetric master keying material using physical layer security methods on the second free space key-distribution channel, the key management module is further configured to encrypt the local keying material using the second~~

~~shared symmetric master keying material to generate second encrypted local keying material; and the communication module is further configured to send the second encrypted local keying material to the third node over a second free space optical communication channel.~~

12~~25~~. The first node according to any one of claims 9 to 11~~21 to 24~~, configured as a satellite.

13~~26~~. The first node according to any one of claims 9 to 12~~21 to 25~~, wherein an optical link in the form of a beam is used for ~~both~~ the ~~free space~~ key-generation channel and/or the ~~free space optical~~ communication channel.

14~~27~~. The first node according to any one of claims 9 to 13~~21 to 26~~, wherein the key management module is configured to operate according to an advanced encryption standard (AES) algorithm wherein an AES key is generated using some or all of the shared symmetric master keying material as a seed key.

15~~28~~. A second node of a communication system, the second node comprising:

a physical layer security module configured to:

establish a ~~free space~~ key-distribution channel between the second node and a first node of the communication system; and

generate shared symmetric master keying material using physical layer security on the ~~free space~~ key-distribution channel;

a communication module configured to:

receive encrypted local keying material from the first node over a ~~free space optical~~ communication channel ~~in the form of a beam~~ for generating symmetric keying material for use between the first node and the second node, the symmetric keying material having a larger size than the symmetric master keying material, wherein the ~~free space optical~~ communication channel has a higher throughput than the ~~free space~~ key-generation channel; and

a key management module configured to:

decrypt the encrypted local keying material using the using the shared symmetric master keying material to create symmetric keying material.

16~~29~~. The second node according to claim 15~~28~~, wherein the ~~free space~~ key-distribution channel is a quantum communication channel.

17~~30~~. The second node according to any one of claims 15 to 16~~28 to 29~~, wherein the second node is a ground node.

18~~31~~. The second node according to any one of claims 15 to 17~~28 to 30~~, wherein an optical link in the form of a beam is used for ~~both~~ the ~~free space~~ key-generation channel and/or the ~~free space optical~~ communication channel.

19~~32~~. The second node according to any one of claims 15 to 18~~28 to 31~~, wherein the key management module is configured to operate according to an advanced encryption standard (AES) algorithm wherein an AES key is generated using some or all of the shared symmetric master keying material as a seed key.

20~~33~~. A communication system comprising a first node according to any one of claims 9 to 14~~21 to 27~~; and a second node according to any one of claims 15 to 19~~28 to 32~~.