CLAIMS

1. A method of using a quantum random number generator, QRNG, for security applications, the method comprising the steps of:

generating one or more quantum keys using the QRNG, including one or more quantum encryption keys;

storing, using a secure network, corresponding sets of the quantum keys in a server located at a controlled access location and in a quantum key token, QKT, for a user, respectively; and

using the corresponding sets of quantum keys for secure transmission between the server and a user device comprising the QKT when outside the secure network or for access control to the controlled access location;

wherein generating the quantum encryption keys comprises limiting a length of the quantum encryption keys to be not greater than the quantum entropy of the keys generated by the QRNG via a randomness extractor.

2. The method of claim 1, wherein generating the quantum keys comprises generating one or more quantum access control keys, wherein the quantum encryption keys are configured for use in the secure transmission and the quantum access control keys are configured for use in the access control.

3. The method of claims 1 or 2, comprising deleting the quantum keys from the server and the QKT after each use in the secure transmission or the access control.

4. The method of any one of claims 1 to 3, wherein generating the quantum keys comprises using a randomness extractor coupled to the QRNG.

5. The method of claim 4. wherein the randomness extractor is executed by a field programmable gate array, FPGA.

6. The method of any one of claims 1 to 5, wherein using the quantum key in the secure transmission comprise encrypting/decrypting a message and its digest using the quantum key.

7. The method of any one of claims 1 to 6, wherein using the quantum key in the secure transmission comprises using the server as a relay for secure transmissions between users.

8. A system for security applications, the system comprising:

a quantum random number generator, QRNG, for generating one or more quantum keys, including one or more quantum encryption keys;

a secure network comprising a server and a user device comprising a quantum key token, QKT, wherein corresponding sets of the quantum keys are stored in the server located at a controlled access location and in the QKT, respectively;

wherein the server and the user device are configured for using the corresponding sets of quantum keys for secure transmission between the server and the user device when located outside the secure network or for access control to the controlled access location; and

wherein the QRNG is configured for limiting a length of the quantum encryption keys to be not greater than the quantum entropy of the keys generated by the QRNG via a randomness extractor.

9. The system of claim 8, wherein the QRNG is configured for generating one or more quantum access control keys, wherein the quantum encryption keys are configured for use in the secure transmission and the quantum access control keys are configured for use in the access control.

10. The system of claims 8 or 9, wherein the server and the user device are configured for deleting the quantum keys from the server and the QKT after each use in the secure transmission or the access control.

11. The system of any one of claims 8 to 10, wherein the QRNG is configured for using a randomness extractor coupled to the QRNG.

12. The system of claim 11, wherein the randomness extractor is executed by a field programmable gate array, FPGA.

13. The system of any one of claims 8 to 12, wherein the user device and the server are configured for encrypting/decrypting a message and its digest using the quantum key.

14. The system of any one of claims 8 to 13, wherein the server is configured to function as a relay for secure transmissions between users.

15. A user device for a system for security applications, the user device comprising a quantum key token, QKT, configured for storing a set of quantum keys, including one or more quantum encryption keys, generated by a quantum random number generator, QRNG, via the secure network;

wherein the user device is configured for using the set of quantum keys for secure transmission with a server located at a controlled access location when the user device is located outside the secure network or for access control to the controlled access location; and

wherein a length of the quantum encryption keys is limited to be not greater than the quantum entropy of the keys generated by the QRNG via a randomness extractor.

16. The user device of claim 15, wherein the quantum key comprise one or more quantum access control keys, wherein the quantum encryption keys are configured for use in the secure transmission and the quantum access control keys are configured for use int the access control.

17. The user device of claims 15 or 16, wherein the user device is configured for deleting the quantum keys from the server and the QKT after each use in the secure transmission or the access control.

18. The system of any one of claims 15 to 17, wherein the user device is configured for encrypting/decrypting a message and its digest using the quantum key.

19. The system of any one of claims 15 to 18, wherein the system for security applications comprises the system of any one of claims 8 to 14.