CLAIMS

What is claimed is:

1. A quantum-capable secure user and data authentication system comprising:

a first communication device;

a first key distribution module communicatively coupled to the first communication device for secure communication therewith;

a second communication device; and

a second key distribution module communicatively coupled to the second communication device for secure communication therewith,

wherein the first communication device and the second communication device enable quantum-safe authentication therebetween while a key distribution protocol between the first key distribution module and the second key distribution module is utilized to establish a shared random between the first communication device and the second communication device, and wherein the first communication device and the second communication device have established a pre-agreed secret password and utilize the pre-agreed secret password and the shared random for the quantum-safe authentication therebetween.

2. The system in accordance with Claim 1 wherein the quantum-safe authentication utilizes Learning Parity with Noise (LPN) post-quantum cryptography.

3. The system in accordance with Claim 2 wherein the LPN post-quantum cryptography comprises a Hopper-Blum protocol.

4. The system in accordance with any of the preceding claims wherein either or both of the first key distribution module and the second key distribution module comprise a SPDC photonic communication module for the key distribution protocol therebetween.

5. The system in accordance with any of the preceding claims wherein either or both of the first key distribution module and the second key distribution module comprise a Quantum Key Distribution (QKD) module, and wherein the key distribution protocol between the first key distribution module and the second key distribution module comprises QKD protocol.

6. The system in accordance with any of the preceding claims wherein the first key distribution module is communicatively coupled to the first communication device via a secure Application Programming Interface (API), and wherein the second key distribution module is communicatively coupled to the second communication device via a secure API.

7. The system in accordance with any of the preceding claims wherein the shared random comprises a first challenge matrix.

8. The system in accordance with Claim 7 wherein the first communication device generates a response cryptogram based on the challenge matrix and the pre-agreed secret password and sends the response cryptogram to the second communication device.

9. The system in accordance with Claim 8 wherein the first communication device further generates the response cryptogram based on randomly-generated noise of a pre-defined probability.

10. The system in accordance with Claim 8 or Claim 9 wherein the second communication device authenticates the first communication device in response to the response cryptogram, a second challenge matrix derived from the shared random and the pre-agreed secret password.

11. The system in accordance with Claim 10 wherein the second communication authenticates the first communication device if a weight determined based on the response cryptogram, the second challenge matrix and the pre-agreed secret password is within a predefined acceptable authentication window.

12. The system in accordance with Claim 9 wherein the first communication device further generates the response cryptogram based on a tag vector, and wherein the tag vector is determined in response to a hash value of a message to be sent from the first communication device to the second communication device.

13. The system in accordance with Claim 12 wherein the tag vector is further determined in response to the hash value of the message to be sent from the first communication device to the second communication device and a tag matrix, wherein the quantum-safe authentication further includes the first key distribution module and the second key distribution module sharing the tag matrix therebetween.

14. The system in accordance with Claim 12 or Claim 13 wherein, after the message is sent from the first communication device and received at the second communication, the second communication device authenticates the first communication device and the message in response to the response cryptogram, a second challenge matrix derived from the shared random, the tag vector, and the pre-agreed secret password.

15. The system in accordance with Claim 14 wherein the second communication authenticates the first communication device and the message if a weight determined based on the response cryptogram, the second challenge matrix, the tag vector, and the pre-agreed secret password is within a predefined acceptable authentication window.

16. A method for quantum-capable secure user and data authentication in a system including a first communication device communicatively coupled to a first Quantum Key Distribution (QKD) module and a second communication device communicatively coupled to a second QKD module, wherein the first communication device and the second communication device are communicatively coupled across a first communication path, the method comprising:

the first communication device and the second communication device establishing a pre-agreed secret password therebetween; and

the first communication device and the second communication device enabling quantum-safe authentication therebetween in response to lightweight communication

between the first QKD module and the second QKD module to establish a shared random therebetween.

17. The method in accordance with Claim 16 wherein the quantum-safe authentication utilizes Learning Parity with Noise (LPN) post-quantum cryptography.

18. The method in accordance with Claims 16 or 17 wherein the shared random comprises a first challenge matrix

19. The method in accordance with Claim 18 wherein the first communication device and the second communication device enabling quantum-safe authentication therebetween comprises:

the first communication device generating a response cryptogram based on the challenge matrix and the pre-agreed secret password; and

the first communication device sending the response cryptogram to the second communication device.

20. The method in accordance with Claim 19 wherein the first communication device and the second communication device enabling quantum-safe authentication therebetween further comprises the first communication device generating the response cryptogram based on randomly-generated noise of a pre-defined probability.