

What Is Claimed Is:

1. A computer system for facilitating storage encryption and decryption, the system comprising:

a processor; and

5 a memory coupled to the processor and storing instructions, which when executed by the processor cause the processor to perform a method, the method comprising:

receiving a first request to encrypt data, wherein the first request indicates the data to be encrypted;

encrypting the data based on a key;

10 determining a key label for the key; and

transmitting the encrypted data and the key label to a remote device,

thereby facilitating secure encryption and decryption of data on the remote device.

2. The computer system of claim 1, wherein the method further comprises updating
15 the key based on the dynamic key refreshment protocol, which comprises:

obtaining a first new key from a first key pool;

transmitting a first synchronization request to a key-managing device, which causes the key-managing device to obtain from a second key pool of the key-managing device a second new key which is the same as the first new key; and

20 obtaining a first new key label for the first new key, wherein the first new key label is the same as a second new key label obtained for the second new key,

wherein the first new key is the key used to encrypt the data, and wherein the first new key label is the determined key label.

25 3. The computer system of claim 2, wherein the dynamic key refreshment protocol is based on one or more of:

determining that a predetermined time interval has passed; and

receiving the first request.

30 4. The computer system of claim 2, wherein the first new key and the second new key are obtained based on a same method, and wherein the first new key label and the second new key label are obtained based on a same algorithm.

5. The computer system of claim 2, wherein the method further comprises:
computing a first hash value of the first new key;
including the first hash value in the first synchronization request, which allows the key-managing device to verify the second new key by confirming that a second hash value of the
5 second new key is the same as the first hash value.
6. The computer system of claim 1, wherein the method further comprises:
generating, by a quantum engine of the computer system, one or more key sequences
based on a quantum communication with a quantum engine of a key-managing device;
10 storing, by the computer system, the generated key sequences in a first key pool of the
computer system;
storing, by the key-managing device, the generated key sequences in a second key pool of
the key-managing device;
generating, by the computer system, a first key label for a respective key sequence in the
15 first key pool; and
generating, by the key-managing device, a second key label for a respective key sequence
in the second key pool,
wherein the first key label and the second key label are generated based on a same
algorithm.
20
7. A computer system for facilitating data access and data decryption, the system
comprising:
a processor; and
a memory coupled to the processor and storing instructions, which when executed by the
25 processor cause the processor to perform a method, the method comprising:
receiving a first request to decrypt encrypted data, wherein the first request indicates the
encrypted data and a key label for a first key used to encrypt the data;
transmitting a second request for the first key, wherein the second request includes the
key label;
30 receiving the first key; and
decrypting the encrypted data based on the received first key.
8. The computer system of claim 7, wherein the second request is transmitted to a
key-managing device, wherein the first key is received from the key-managing device, wherein
35 the method further comprises:

prior to transmitting the second request to the key-managing device:

obtaining a second key from a first key pool; and

transmitting a synchronization request to the key-managing device, which causes the key-managing device to obtain from a second key pool of the key-managing device a
5 third key which is the same as the second key;

encrypting, based on the second key, the key label included in the second request,

wherein the received first key is encrypted based on the third key; and

decrypting, based on the second key, the encrypted received first key.

10 9. A computer system for facilitating storage encryption and decryption, the system comprising:

a processor; and

a memory coupled to the processor and storing instructions, which when executed by the processor cause the processor to perform a method, the method comprising:

15 receiving, based on a dynamic key refreshment protocol, a first synchronization request which indicates a first key obtained from a first key pool;

obtaining a second key from a second key pool, wherein the second key is the same as the first key;

20 obtaining a second key label for the second key, wherein the second key label is the same as a first key label obtained for the first key; and

storing the second key and the second key label,

thereby facilitating secure encryption and decryption of data on a remote device.

25 10. The computer system of claim 9, wherein the first key and the second key are obtained based on a same method, and wherein the first key label and the second key label are obtained based on a same algorithm.

11. The computer system of claim 9, wherein the first synchronization request includes a first hash value of the first key, wherein the method further comprises:
30 computing a second hash value of the second key; and
verifying the second key by confirming that the second hash value is the same as the first hash value.

12. The computer system of claim 9, wherein the second key and the second key label
35 are stored in a database associated with the computing system, wherein the method further

comprises:

- receiving a request for the second key, wherein the request includes the second key label;
- retrieving the second key from the database based on the second key label included in the request for the second key; and
- 5 returning the retrieved second key.

13. The computer system of claim 12, wherein the request is received from a security device, wherein the retrieved second key is returned to the security device, wherein the method further comprises:

- 10 prior to receiving the request from the security device:
 - receiving, from the security device, a second synchronization request associated with a third key from the first key pool, wherein the second key label included in the request for the second key is encrypted based on the third key; and
 - obtaining, from the second key pool, a fourth key which is the same as the third
 - 15 key;
 - decrypting the encrypted second key label based on the fourth key; and
 - prior to returning the retrieved second key, encrypting the retrieved second key based on the fourth key.

- 20 14. A computer-implemented method for facilitating storage encryption and decryption, the method comprising:
- receiving a first request to encrypt data, wherein the first request indicates the data to be encrypted;
 - encrypting the data based on a key;
 - 25 determining a key label for the key; and
 - transmitting the encrypted data and the key label to a remote device,
 - thereby facilitating secure encryption and decryption of data on the remote device.

15. The method of claim 14, further comprising updating the key based on the
- 30 dynamic key refreshment protocol, which comprises:
- obtaining a first new key from a first key pool;
 - transmitting a first synchronization request to a key-managing device, which causes the key-managing device to obtain from a second key pool of the key-managing device a second new key which is the same as the first new key; and
 - 35 obtaining a first new key label for the first new key, wherein the first new key label is the

same as a second new key label obtained for the second new key,

wherein the first new key is the key used to encrypt the data, and wherein the first new key label is the determined key label.

5 16. The method of claim 15, wherein the dynamic key refreshment protocol is based on one or more of:

 determining that a predetermined time interval has passed; and
 receiving the first request.

10 17. The method of claim 15, wherein the first new key and the second new key are obtained based on a same method, and wherein the first new key label and the second new key label are obtained based on a same algorithm.

 18. The method of claim 15, further comprising:
15 computing a first hash value of the first new key;
 including the first hash value in the first synchronization request, which allows the key-managing device to verify the second new key by confirming that a second hash value of the second new key is the same as the first hash value.

20 19. The method of claim 14, further comprising:
 generating, by a quantum engine of the computer system, one or more key sequences based on a quantum communication with a quantum engine of a key-managing device;
 storing, by the computer system, the generated key sequences in a first key pool of the computer system;
25 storing, by the key-managing device, the generated key sequences in a second key pool of the key-managing device;
 generating, by the computer system, a first key label for a respective key sequence in the first key pool; and
 generating, by the key-managing device, a second key label for a respective key sequence
30 in the second key pool,
 wherein the first key label and the second key label are generated based on a same algorithm.

 20. A computer-implemented method for facilitating data access and data decryption,
35 the method comprising:

receiving a first request to decrypt encrypted data, wherein the first request indicates the encrypted data and a key label for a first key used to encrypt the data;

transmitting a second request for the first key, wherein the second request includes the key label;

- 5 receiving the first key; and
- decrypting the encrypted data based on the received first key.