

**What is Claimed is:**

1. 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:
    - receiving a first request to encrypt data, wherein the first request indicates the data to be encrypted;
    - encrypting the data based on a first key;
    - determining a first key label for the first key;
    - transmitting the encrypted data and the first key label to a remote device;
    - receiving a second request to decrypt the encrypted data, wherein the second request indicates the encrypted data and the first key label for the first key used to encrypt the data;
    - obtaining a second key from a first key pool;
    - generating a first synchronization request for a key-managing device, which causes the key-managing device to obtain from a second key pool of the key-managing device a third key which is the same as the second key;
    - encrypting, based on the second key, the first key label;
    - transmitting a third request for the first key, wherein the third request includes the encrypted first key label;
    - receiving the first key, wherein the received first key is encrypted based on the third key;

decrypting, based on the second key, the encrypted received first key to obtain a decrypted first key; and  
decrypting the encrypted data based on the decrypted first key.

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

obtaining a first new key from a first key pool;

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

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 first key label.

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.

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 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 first quantum engine of the computer system, one or more key sequences based on a quantum communication with a second quantum engine of the key-managing device;

- 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 second key label for a respective key sequence in the first key pool; and

- generating, by the key-managing device, a third key label for a respective key sequence in the second key pool,

- wherein the second key label and the third key label are generated based on a same algorithm.

7. The computer system of claim 1, wherein the first key is received from the key-managing device.

8. The computer system of claim 2, wherein the method further comprises:

- receiving, based on the dynamic key refreshment protocol, the first synchronization request which indicates the first new key obtained from

the first key pool;

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

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

storing the second new key and the second new key label, thereby facilitating secure encryption and decryption of data on a remote device.

9. The computer system of claim 8,

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.

10. The computer system of claim 8, wherein the first synchronization request includes a first hash value of the first new key, wherein the method further comprises:

computing a second hash value of the second new key; and

verifying the second new key by confirming that the second hash value is the same as the first hash value.

11. The computer system of claim 8, wherein the second new key and the second new key label are stored in a database associated with the computer system, wherein the method further comprises:

receiving a third request for the second new key, wherein the request includes the second key label;

retrieving the second new key from the database based on the second new key label included in the request for the second new key; and

returning the retrieved second new key.

12. The computer system of claim 11, wherein the third request is received from a security device, wherein the retrieved second new key is returned to the security device, wherein the method further comprises:

prior to receiving the third 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 new key label included in the third 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 key;

decrypting the encrypted second new key label based on the fourth key;

and

prior to returning the retrieved second new key, encrypting the retrieved second new key based on the fourth key.

13. 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 first key;

determining a first key label for the first key;

transmitting the encrypted data and the first key label to a remote device;

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

obtaining a second key from a first key pool;

generating a first synchronization request for a key-managing device,

which causes the key-managing device to obtain from a second key pool of the key-managing device a third key which is the same as the second key;

encrypting, based on the second key, the first key label;

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

receiving the first key, wherein the received first key is encrypted based on the third key;

decrypting, based on the second key, the encrypted received first key to obtain a decrypted first key; and

decrypting the encrypted data based on the decrypted first key.

14. The method of claim 13, further comprising updating the first key based on the dynamic key refreshment protocol, which comprises:

obtaining a first new key from a first key pool;

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

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 first key label.

15. The method of claim 14, 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.

16. The method of claim 14, 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.

17. The method of claim 14, further comprising:

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.

18. The method of claim 13, further comprising:

generating, by a first quantum engine of the computer system, one or more key sequences based on a quantum communication with a second quantum engine of the key-managing device;

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 second key label for a respective key sequence in the first key pool; and

generating, by the key-managing device, a third key label for a respective key sequence in the second key pool,

wherein the second key label and the third key label are generated based on a same algorithm.

19. The method of claim 13, wherein the first key is received from the key-managing device.