

CLAIMS

1. A method of encrypting data in a network system, the method comprising:

- generating within a trusted network of the network system an associated private key based on an attribute associated with an user;
- generating within the trusted network a homomorphically encrypted associated private key based on the associated private key via homomorphic encryption;
- generating within the trusted network a homomorphic key pair comprising a public key and a corresponding private key paired with the public key;
- transmitting the homomorphically encrypted associated private key from the trusted network to a non-trusted network of the network system;
- generating within the trusted network encrypted data based on said data;
- generating within the trusted network a control key;
- generating within the trusted network an attribute based encrypted control key based on the control key, via attribute based encryption based on the attribute associated with the user;
- generating within the trusted network a homomorphically and attribute based encrypted control key based on the attribute based encrypted control key, via homomorphic encryption; and
- transmitting the encrypted data, and the homomorphically and attribute based encrypted control key, from the trusted network to the non-trusted network;

wherein the encrypted data is configured to be decrypted based on the control key; and

wherein based on a request from the user, the control key is generated within the non-trusted network based on the homomorphically encrypted associated private key, the homomorphically encrypted and attribute based encrypted control key, and the corresponding private key of the homomorphic key pair.

2. The method according to claim 1, further comprising:

- generating within the trusted network a data key; and
- generating within the trusted network an encrypted data key, the encrypted data key configured to be decrypted by the control key;

wherein the encrypted data is configured to be decrypted by the data key so that the encrypted data is configured to be indirectly decrypted based on the control key.

3. The method according to claim 2, further comprising:

transmitting the encrypted data key from the trusted network to the non-trusted network.

4. The method according to claim 1,

wherein the homomorphic encryption is a fully homomorphic encryption.

5. The method according to claim 1,

wherein the non-trusted network, upon request from a data owner, is configured to delete the homomorphically and attribute based encrypted control key.

6. The method according to claim 2,

wherein the trusted network, upon request from a data owner, is configured to obtain the homomorphically and attribute based encrypted control key, and encrypted data key, from the non-trusted network.

7. The method according to claim 6,

wherein the trusted network is further configured to decrypt the control key based on the homomorphically and attribute based encrypted control key; and further configured to decrypt the data key based on the encrypted data key, via the control key.

8. The method according to claim 7,

wherein the trusted network is further configured to generate a new control key different from the control key; and further configured to generate a new encrypted data key, the new encrypted data key configured to be decrypted by the new control key

9. The method according to claim 8,

wherein the trusted network is further configured to generate a new attribute based encrypted control key based on the new control key, via attribute based encryption based on the attribute associated with the user;

wherein the trusted network is further configured to generate a new homomorphically and attribute based encrypted control key, based on the new attribute based encrypted control key, via homomorphic encryption.

10. The method according to claim 9,

wherein the trusted network is further configured to transmit the new homomorphically and attribute based encrypted control key, and the new encrypted data key, to the non-trusted network.

11. A method of decrypting encrypted data in a network system, the method comprising:

generating a control key within a non-trusted network based on a homomorphically encrypted associated private key, a homomorphically encrypted and attribute based encrypted control key, and a corresponding private key of a homomorphic key pair; and

decrypting encrypted data based on the control key;

wherein the homomorphically encrypted associated private key is generated within a trusted network of the network system based on an associated private key via homomorphic encryption, the associated private key generated based on an attribute associated with an user;

wherein the homomorphic key pair comprising a public key and the corresponding private key is generated by the trusted network;

wherein the homomorphically encrypted associated private key is transmitted from the trusted network to the non-trusted network of the network system;

wherein the encrypted data is generated within the trusted network based on data;

wherein the homomorphically encrypted and attribute based encrypted control key is generated based on an attribute based encrypted control key via homomorphic encryption, the attribute based encrypted control key is generated based on a control key generated within the trusted network, via the attribute associated with the user;

wherein the encrypted data, and the homomorphically and attribute based encrypted control key, are transmitted from the trusted network to the non-trusted network.

12. A network system comprising:

a trusted network; and

a non-trusted network connected to the trusted network;

wherein the trusted network is configured to generate an associated private key based on an attribute associated with an user;

wherein the trusted network is configured to generate a homomorphically encrypted associated private key based on the associated private key via homomorphic encryption;

wherein the trusted network is further configured to generate a homomorphic key pair comprising a public key and a corresponding private key paired with the public key;

wherein the trusted network is configured to transmit the homomorphically encrypted associated private key to the non-trusted network;

wherein the trusted network is configured to generate encrypted data based on data;

wherein the trusted network is configured to generate a control key;

wherein the trusted network is configured to generate within the trusted network an attribute based encrypted control key, based on the control key via attribute based encryption, based on the attribute associated with the user;

wherein the trusted network is configured to generate a homomorphically and attribute based encrypted control key, based on the attribute based encrypted control key, via homomorphic encryption;

wherein the trusted network is configured to transmit the encrypted data, and the homomorphically and attribute based encrypted control key, to the non-trusted network;

wherein the encrypted data is configured to be decrypted based on the control key; and

wherein based on a request from the user, the non-trusted network is configured to generate the control key based on the homomorphically encrypted associated private key, the homomorphically encrypted and attribute based encrypted control key, and the corresponding private key of the homomorphic key pair.

13. The network system according to claim 12,
wherein the trusted network system is configured to generate a data key;
wherein the trusted network system is configured to generate an encrypted data key, the encrypted data key configured to be decrypted by the control key;
wherein the encrypted data is configured to be decrypted by the data key so that the encrypted data is configured to be indirectly decrypted based on the control key; and
wherein the network system is configured to transmit the encrypted data key from the trusted network to the non-trusted network.

14. The network system according to claim 12,
wherein the trusted network comprises:
a cryptography agnostic key management (CAKM) administration tool module;
a ciphertext policy attribute-based encryption (CP-ABE) library module;
a homomorphic encryption (HE) module; and
a data owner tool module.

15. The network system according to claim 14,
wherein the ciphertext policy attribute-based encryption library module is configured to, on a request from the cryptography agnostic key management administration tool module, generate the associated private key based on the attribute associated with the user; and
wherein the ciphertext policy attribute-based encryption library module is configured to, on a request from the data owner tool module, generate the attribute based encrypted control key based on the control key, via attribute based encryption based on the attribute associated with the user.

16. The network system according to claim 14,
wherein the homomorphic encryption module of the trusted network is configured to, on a request from the cryptography agnostic key management administration tool module, configured to generate the homomorphic key pair;

wherein the homomorphic encryption module of the trusted network is configured to, on a further request from the cryptography agnostic key management administration tool module, configured to generate the homomorphically encrypted associated private key, based on the first private key, via homomorphic encryption; and

wherein the homomorphic encryption module of the trusted network is configured to, on a request from the data owner tool module, generate the homomorphically and attribute based encrypted control key, based on the attribute based encrypted control key, via homomorphic encryption.

17. The network system according to claim 12,

wherein the non-trusted network comprises:

a cryptography agnostic key management (CAKM) broker module;

a compute node module;

a data store module;

a homomorphic encryption module; and

an encrypted key store module.

18. The network system according to claim 17,

wherein the homomorphically encrypted associated private key is transmitted to the cryptography agnostic key management broker module, and the homomorphic key pair is transmitted to the compute node module.

19. The network system according to claim 17,

wherein the encrypted data is transmitted to the data store module, and the homomorphically and attribute based encrypted control key is transmitted to the cryptography agnostic key management broker module.

20. The network system according to claim 17,

wherein based on the request from the user, the homomorphic encryption module of the non-trusted network is configured to generate a homomorphically encrypted control key based on the

homomorphically encrypted associated private key, and the homomorphically encrypted and attribute based encrypted control key; and

wherein the compute node is further configured to generate the control key based on the homomorphically encrypted control key generated by the homomorphic encryption module of the non-trusted network and the corresponding private key of the homomorphic key pair.