

CLAIMS

1. A user computing device comprising:
 - at least one processor;
 - at least one memory communicatively coupled to the at least one processor;
 - at least one network interface communicatively coupled to the at least one processor and configured to communicate with at least one remotely located computing device; and
 - wherein the at least one network interface is configured to receive a plurality of public encryption keys from the at least one remotely located computing device;
 - wherein the at least one processor is configured to:
 - split at least one secret into a plurality of shares, wherein at least a subset of the plurality of shares is sufficient to reconstruct the at least one secret; and
 - encrypt each of the plurality of shares based on a different public encryption key of the plurality of public encryption keys to create a plurality of encrypted shares;
 - wherein the at least one network interface is configured to communicate the plurality of encrypted shares to the at least one remotely located computing device.
2. The user computing device of claim 1, wherein the at least one processor is further configured to encrypt and sign each of the plurality of encrypted shares using an Elliptic Curve Diffie Hellman (ECDH) operation.
3. The user computing device of claim 1, wherein the at least one processor is configured to encrypt using an Elliptic Curve Diffie Hellman (ECDH) operation, comprising:
 - determining a plurality of ECDH keys, each determined based on a private signature key and a respective public encryption key of the plurality of public encryption keys;
 - determining a plurality of Advanced Encryption Standard (AES) keys, each determined as a hash of a respective ECDH key, a public signature key, and the respective public encryption key of the plurality of public encryption keys; and
 - encrypting each of the plurality of shares, combined with a respective AES key, into a respective encrypted share.
4. The user computing device of claim 1, wherein the plurality of public encryption keys are each part of a different encryption key pair with a different private key, each different private key stored on a different computing device.

5. The user computing device of claim 1,
wherein the at least one network interface is configured to receive at least a first subset of a first plurality of encrypted shares from the at least one remotely located computing device;
wherein the at least one processor is configured to:
decrypt each of the first subset of the first plurality of encrypted shares to create a first plurality of un-encrypted shares; and
reconstruct the at least one secret using the first plurality of un-encrypted shares.
6. The user computing device of claim 5,
wherein the at least one network interface is configured to communicate at least one recovery public encryption key to the at least one remotely located computing device;
wherein the at least one processor is configured to decrypt each of the first subset of the first plurality of encrypted shares based on at least one recovery private decryption key corresponding to the at least one recovery public encryption key.
7. The user computing device of claim 6, wherein the at least one processor is further configured to generate a plurality of hashes from the plurality of shares prior to encryption;
wherein the at least one network interface is further configured to communicate the plurality of hashes to the at least one remotely located computing device.
8. A user computing device comprising:
at least one processor;
at least one memory communicatively coupled to the at least one processor;
at least one network interface communicatively coupled to the at least one processor and configured to communicate with at least one remotely located computing device of a plurality of remotely located computing devices;
wherein the at least one network interface is configured to communicate at least one recovery public encryption key to the at least one remotely located computing device of the plurality of remotely located computing devices, wherein at least one recovery private decryption key corresponds to the at least one recovery public encryption key; and

wherein the at least one network interface is configured to receive at least a subset of a first plurality of recovery encrypted shares from the at least one remotely located computing device of the plurality of remotely located computing devices;

wherein the at least one processor is configured to:

decrypt each of the subset of the first plurality of recovery encrypted shares to create a first plurality of un-encrypted shares based on the at least one recovery private decryption key corresponding to the at least one recovery public encryption key; and

reconstruct at least one secret using the first plurality of un-encrypted shares.

9. The user computing device of claim 8, wherein the at least one processor is configured to reconstruct the at least one secret using the first plurality of un-encrypted shares through at least one of polynomial interpolation or Shamir secret sharing.

10. The user computing device of claim 8, wherein the first plurality of un-encrypted shares are Shamir shares;

wherein the at least one processor is configured to reconstruct the at least one secret using a second plurality of shares using Shamir secret sharing.

11. The user computing device of claim 8, wherein the at least one processor is configured to decrypt using an Elliptic Curve Diffie Hellman (ECDH) operation, comprising:

determining at least one recovery ECDH key, each determined based on a respective recovery public signature key of at least one recovery public signature key and a respective recovery public encryption key of the at least one recovery private decryption key;

for each recovery ECDH key, determining an Advanced Encryption Standard (AES) key as a hash of a respective recovery ECDH key of the at least one recovery ECDH key, the respective recovery public signature key of the at least one recovery public signature key, and the respective recovery public encryption key of the at least one recovery public encryption key; and

decrypt each of the subset of the first plurality of recovery encrypted shares, combined with a corresponding recovery AES key, into a respective un-encrypted share.

12. A system comprising:
a first user computing device;

at least one remotely located computing device configured to communicate with the first user computing device; and

wherein the at least one remotely located computing device is configured to communicate a plurality of public encryption keys to the first user computing device;

wherein the first user computing device is configured to:

split at least one secret into a plurality of shares, wherein at least a subset of the plurality of shares is sufficient to reconstruct the at least one secret;

encrypt each of the plurality of shares based on a different public encryption key of the plurality of public encryption keys to create a plurality of encrypted shares; and

communicate the plurality of encrypted shares to the at least one remotely located computing device;

wherein the at least one remotely located computing device is configured to store the plurality of encrypted shares.

13. The system of claim 12, wherein the first user computing device is further configured to sign each of the plurality of encrypted shares using a private signature key.

14. The system of claim 12, wherein the plurality of public encryption keys are each part of a different encryption key pair with a different private key, each different private key stored on a different computing device.

15. The system of claim 12, wherein the first user computing device is configured to encrypt using an Elliptic Curve Diffie Hellman (ECDH) operation, comprising:

determining a plurality of ECDH keys, each determined based on a private signature key and a respective public encryption key of the plurality of public encryption keys;

determining a plurality of Advanced Encryption Standard (AES) keys, each determined as a hash of a respective ECDH key, a public signature key, and the respective public encryption key of the plurality of public encryption keys; and

encrypting each of the plurality of shares, along with a respective AES key, into a respective encrypted share of the plurality of encrypted shares.

16. The system of claim 15, further comprising:
a second user computing device;

wherein the second user computing device is configured to communicate at least one recovery public encryption key to the at least one remotely located computing device;

wherein the at least one remotely located computing device is configured to communicate at least one recovery encrypted share to the second user computing device; and

wherein the second user computing device is configured to decrypt each of the at least one recovery encrypted share to create a first plurality of un-encrypted shares based on at least one recovery private decryption key corresponding to the at least one recovery public encryption key;

wherein the second user computing device is configured to reconstruct the at least one secret using the first plurality of un-encrypted shares.

17. The system of claim 16, wherein the at least one recovery private decryption key is a single recovery private decryption key; and

wherein the at least one recovery public encryption key is a single recovery public encryption key.

18. The system of claim 17, wherein each of a plurality of trusted computing devices is configured to decrypt using the Elliptic Curve Diffie Hellman (ECDH) operation, comprising:

determining at least one recovery ECDH key, each determined based on a respective recovery public signature key and a respective one of the at least one recovery private decryption key;

for each respective recovery ECDH key of the at least one recovery ECDH key, determining an Advanced Encryption Standard (AES) key as a hash of a respective recovery ECDH key of the at least one recovery ECDH key, the respective recovery public signature key, and a respective recovery public encryption key; and

decrypt each of the at least one recovery encrypted share, combined with a corresponding recovery AES key, into a respective un-encrypted share of the first plurality of un-encrypted shares.

19. A system comprising:

a user computing device;

at least one remotely located computing device configured to communicate with the user computing device;

wherein the user computing device is configured to communicate at least one recovery public encryption key to one or more remotely located computing devices of the at least one remotely located computing device, wherein at least one recovery private decryption key corresponds to the at least one recovery public encryption key; and

wherein the at least one remotely located computing device is configured to communicate at least a subset of a first plurality of recovery encrypted shares to the user computing device;

wherein the user computing device is configured to:

decrypt each of the subset of the first plurality of recovery encrypted shares to create a first plurality of un-encrypted shares based on the at least one recovery private decryption key corresponding to the at least one recovery public encryption key; and

reconstruct at least one secret using the first plurality of un-encrypted shares.

20. The system of claim 19, wherein the user computing device is further configured to reconstruct the at least one secret using the first plurality of un-encrypted shares through at least one of polynomial interpolation or Shamir secret sharing.

21. The system of claim 19, wherein the first plurality of un-encrypted shares are Shamir shares;

wherein the user computing device is further configured to reconstruct the at least one secret using a second plurality of shares using Shamir secret sharing.

22. The system of claim 19, wherein the user computing device is configured to decrypt using an Elliptic Curve Diffie Hellman (ECDH) operation, comprising:

determining at least one recovery ECDH key, each determined based on a respective recovery public signature key of at least one recovery public signature key and a respective recovery public encryption key of the at least one recovery private decryption key;

for each recovery ECDH key of the at least one recovery ECDH key, determining an Advanced Encryption Standard (AES) key as a hash of a respective recovery ECDH key of the at least one recovery ECDH key, the respective recovery public signature key of the at least one recovery public signature key, and the respective recovery public encryption key of the at least one recovery public encryption key; and

decrypt each of the subset of the first plurality of recovery encrypted shares, combined with a corresponding recovery AES key, into a respective un-encrypted share.

23. A computerized method comprising:

communicating a plurality of public encryption keys from at least one remotely located computing device to a first user computing device;

splitting at least one secret into a plurality of shares at the first user computing device, wherein at least a subset of the plurality of shares is sufficient to reconstruct the at least one secret;

encrypting each of the plurality of shares based on a different public encryption key of the plurality of public encryption keys at the first user computing device to create a plurality of encrypted shares;

communicating the plurality of encrypted shares from the first user computing device to the at least one remotely located computing device; and

storing the plurality of encrypted shares at the at least one remotely located computing device.

24. The computerized method of claim 23, further comprising:

transferring, via at least one mobile storage device, each of the plurality of encrypted shares from the at least one remotely located computing device to a respective trusted computing device of a plurality of trusted computing devices;

decrypting, at each trusted computing device, a respective encrypted share into a respective un-encrypted share of a plurality of un-encrypted shares; and

verifying, at each trusted computing device, that the respective un-encrypted share of the plurality of un-encrypted shares matches one of the plurality of shares before it was encrypted.

25. The computerized method of claim 24, wherein decrypting comprises using an Elliptic Curve Diffie Hellman (ECDH) operation, comprising:

determining at least one recovery ECDH key, each determined based on a respective recovery public signature key and at least one recovery private decryption key;

for each respective recovery ECDH key of the at least one recovery ECDH key, determining an Advanced Encryption Standard (AES) key as a hash of a respective recovery ECDH key, the respective recovery public signature key, and a respective recovery public

encryption key; and decrypt each encrypted share, combined with a corresponding recovery AES key, into the respective un-encrypted share.

26. The computerized method of claim 24, further comprising:

- generating, at the first user computing device, hashes of the plurality of shares;
- communicating the hashes of the plurality of shares to the at least one remotely located computing device;
- transferring each of the hashes from the at least one remotely located computing device to the respective trusted computing device of the plurality of trusted computing devices; and
- generating a plurality of recovery hashes from the plurality of un-encrypted shares; wherein verifying comprises comparing the hashes with the plurality of recovery hashes to determine whether data in the plurality of un-encrypted shares is accurate.

27. The computerized method of claim 26, further comprising:

- re-encrypting the plurality of un-encrypted shares into recovery encrypted shares;
- transferring the plurality of un-encrypted shares to the at least one remotely located computing device;
- communicating the recovery encrypted shares to a second user computing device from the at least one remotely located computing device;
- decrypting each of the recovery encrypted shares at the second user computing device to create a plurality of decrypted shares; and
- reconstructing the at least one secret at the second user computing device using the plurality of decrypted shares.

28. The computerized method of claim 26, wherein re-encrypting comprises using an Elliptic Curve Diffie Hellman (ECDH) operation, comprising:

- determining a plurality of recovery ECDH keys, each determined based on a respective recovery private signature key and a respective recovery public encryption key;
- determining a plurality of Advanced Encryption Standard (AES) keys, each determined as a hash of a respective recovery ECDH key of the plurality of recovery ECDH keys, a respective recovery public signature key, and the respective recovery public encryption key; and

encrypting each of the plurality of un-encrypted shares, along with a respective AES key, into a respective recovery encrypted share of recovery encrypted shares.

29. A computerized method comprising:

communicating at least one recovery public encryption key to at least one remotely located computing device from a user computing device, wherein at least one recovery private decryption key corresponds to the at least one recovery public encryption key;

communicating at least a subset of a first plurality of recovery encrypted shares to the user computing device from the at least one remotely located computing device;

decrypting each of the subset of the first plurality of recovery encrypted shares at the user computing device to create a first plurality of un-encrypted shares based on the at least one recovery private decryption key corresponding to the at least one recovery public encryption key; and

reconstructing at least one secret at the user computing device using the first plurality of un-encrypted shares.

30. The computerized method of claim 29, further comprising:

encrypting a first plurality of shares at one or more trusted computing devices based on the at least one recovery public encryption key into the at least the subset of the first plurality of recovery encrypted shares prior to communicating the at least the subset of the first plurality of recovery encrypted shares to the user computing device from the at least one remotely located computing device.

31. The computerized method of claim 30, wherein encrypting comprises using an Elliptic Curve Diffie Hellman (ECDH) operation, comprising:

determining a plurality of recovery ECDH keys, each determined based on a respective recovery private signature key and a respective recovery public encryption key;

determining a plurality of Advanced Encryption Standard (AES) keys, each determined as a hash of a respective recovery ECDH key of the plurality of recovery ECDH keys, a respective recovery public signature key of at least one recovery public signature key, and the respective recovery public encryption key; and

encrypting each of the first plurality of un-encrypted shares, along with a respective AES key, into a respective one of the first plurality of recovery encrypted shares.

32. The computerized method of claim 29, wherein decrypting comprises using an Elliptic Curve Diffie Hellman (ECDH) operation, comprising:
- determining at least one recovery ECDH key, each determined based on a respective recovery public signature key of at least one recovery public signature key and one of the at least one recovery private decryption key;
 - for each recovery ECDH key of the at least one recovery ECDH key, determining an Advanced Encryption Standard (AES) key as a hash of a respective recovery ECDH key of the at least one recovery ECDH key, the respective recovery public signature key of the at least one recovery public signature key, and one of the at least one recovery public encryption key; and
 - decrypt each of the subset of the first plurality of recovery encrypted shares, combined with a corresponding recovery AES key, into a respective un-encrypted share.
33. The user computing device of claim 1 or the system of claim 12, wherein each different public encryption key of the plurality of public encryption keys is derived using a Hierarchical Deterministic (HD) methodology from a different master seed key.
34. The user computing device of claim 1 or the system of claim 12, wherein the plurality of shares are Shamir secret shares.
35. The user computing device of claim 1 or the system of claim 12, wherein the at least one secret is split into the plurality of shares through at least one of polynomial interpolation or Shamir secret sharing.
36. The user computing device of claims 1 or 8 or the system of claims 12 or 19, wherein the at least one secret is used to encrypt first data, decrypt second data, and sign transactions.
37. The user computing device of claim 4 or the system of claim 14, wherein each different computing device is located at a different physical location from other different computing devices.
38. The user computing device of claims 6 or 8 or the system of claims 16 or 19, wherein each different recovery public encryption key of the at least one recovery public encryption

key is part of a different recovery encryption key pair with a different recovery private decryption key of the at least one recovery private decryption key.

39. The user computing device of claims 6 or 8 or the system of claims 16 or 19, wherein the at least one recovery private decryption key is a single recovery private decryption key; wherein the at least one recovery public encryption key is a single recovery public encryption key.

40. The user computing device of claim 8 or the system of claim 19, wherein the first plurality of un-encrypted shares are Shamir secret shares.