

CLAIMS

1. A computer-implemented method of generating shares of a shared secret, wherein each of a group of participants has a respective first secret share of the shared secret, wherein the method is performed by a first participant of the group and comprises:
 - generating a respective blinding share of a shared blinding secret,
 - obtaining at least a threshold number of respective intermediary shares from each of the first group of participants, wherein each respective intermediary share is generated based on a respective blinding share and a respective first secret share;
 - generating an intermediary value based on each of the obtained intermediary shares; and
 - generating a respective second secret share of the shared secret, wherein the respective second secret share is generated based on the intermediary value and the respective blinding share.
2. The method of claim 1, wherein a first one of the respective intermediary shares is generated by the first participant.
3. The method of claim 1 or claim 2, wherein a threshold of the shared secret is equal to the threshold of the shared blinding secret.
4. The method of claim 1 or claim 2, wherein a threshold of the shared secret is different compared to the threshold of the shared blinding secret.
5. The method of claim 4, wherein the threshold of the shared secret is greater than the threshold of the shared blinding secret.
6. The method of claim 4, wherein the threshold of the shared secret is less than the threshold of the shared blinding secret.
7. The method of any preceding claim, wherein the respective blinding share of the shared blinding secret is generated using a joint verifiable secret sharing scheme.

8. The method of claim 7, wherein generating the respective blinding share using the joint secret sharing scheme comprises:
- generating a first data item, the first data item being a first polynomial;
 - obtaining a respective data item from at least the threshold number of participants, each respective data item being a respective polynomial generated by a respective participant; and
 - generating the respective blinding share based on the first data item and each of the respective data items.
9. The method of claim 7 or claim 8, wherein obtaining the respective data items comprises obtaining the respective data items over a respective communication channel between the first participant and each of the threshold number of participants.
10. The method of any of claims 7 to 9, comprising transmitting a respective instance of the first polynomial to at least each of the threshold number of participants, wherein the respective instance of the first polynomial is based on a respective participant.
11. The method of any of claims 1 to 7, wherein the respective blinding share of the shared blinding secret is generated using a Shamir's secret sharing scheme.
12. The method of any preceding claim, wherein the respective first secret share of the shared secret is generated using a joint verifiable secret sharing scheme.
13. The method of any of claims 1 to 11, wherein the respective first secret share of the shared secret is generated using a Shamir's secret sharing scheme.
14. The method of any preceding claim, wherein the shared secret is a private key and the respective second secret share is a respective private key share of the private key.

15. The method of claim 14, wherein the shared blinding secret is a blinding private key, wherein the intermediary value is an intermediary private key, and wherein the method comprises:

- generating a first public key corresponding to the private key;
- generating a second public key corresponding to the blinding private key;
- generating a third public key corresponding to the intermediary private key;
- generating a first value based on the first and second public keys; and
- verifying that the second secret share of the shared secret has been generated correctly based on whether the first value matches the third public key.

16. The method of claim 15, comprising:

- in response to determining that the second secret share has not been generated correctly, performing the following steps for one, some or all of the other respective participants:

- obtaining a respective first public key corresponding to the respective first secret share of that participant;

- obtaining a respective second public key corresponding to the respective blinding share of that participant;

- obtaining a respective third public key corresponding to the respective intermediary share of that participant;

- generating a respective first value based on the respective first and second public keys of that participant; and

- verifying that the respective second secret share of the shared secret has been generated correctly by that participant based on whether the respective first value matches the respective third public key.

17. The method of any of claims 14 to 16, comprising:

- obtaining a message; and
- generating a digital signature share based on the message and the respective share of the private key.

18. The method of any of claims 14 to 16, comprising:

obtaining a message;

generating a first message-independent component and a first message-dependent component, wherein the message-independent component is generated based on the respective private key share and wherein the message-dependent component is generated based on the message;

causing the first message-independent component to be made available to a coordinator; and

causing a first signature share to be made available to the coordinator for generating the signature based on at least the threshold number of signature shares, wherein the first signature share comprises at least the message-dependent component.

19. Computer equipment comprising:
- memory comprising one or more memory units; and
- processing apparatus comprising one or more processing units, wherein the memory stores code arranged to run on the processing apparatus, the code being configured so as when on the processing apparatus to perform the method of any of claims 1 to 18.
20. A computer program embodied on computer-readable storage and configured so as, when run on computer equipment, to perform the method of any of claims 1 to 18.