

CLAIMS

1. A computer-implemented method of generating a share of a digital signature of a message, wherein a threshold number of different signature shares from respective participants of a group of participants are required to generate the digital signature, wherein each participant has a respective private key share, the method being performed by a first one of the participants and comprising:
 - generating a first message-independent component and a first message-dependent component, wherein the message-independent component is generated based on a first private key share, wherein the message-dependent component is generated based on the message, wherein each participant has a respective ephemeral private key share, and wherein the first message-independent component and/or the first message-dependent component is based on a first ephemeral private key share;
 - 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.
2. The method of claim 1, wherein the message-independent component is generated prior to obtaining the message.
3. The method of claim 1 or claim 2, wherein the first signature share comprises the message-independent component.
4. The method of any of claims 1 to claim 3, wherein the first private key share is generated using a joint secret sharing scheme for generating a share of a first private key.
5. The method of claim 4, wherein generating the first private key 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 first private key share based on the first data item and each of the respective data items.

6. The method of claim 5, 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 respective participants.

7. The method of claim 5, 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.

8. The method of claim 7, wherein each participant has a respective shared value based on an ephemeral public key corresponding to the ephemeral private key, and wherein the first message-independent component is based on the shared value.

9. The method of any preceding claim, wherein the first ephemeral private key share is generated using the joint secret sharing scheme for generating a share of the ephemeral private key.

10. The method of claim any preceding claim, wherein the first message-independent component is generated based on an inverse corresponding to the first ephemeral private key share.

11. The method of claim 10, wherein generating the inverse of the first ephemeral private key share comprises:

generating an intermediate value based on the ephemeral private key and a first blinding key; and

generating the inverse of the first ephemeral private key share based on an inverse of the intermediate value and a first blinding key share of the first blinding key.

12. The method of claim 11, wherein the first blinding key share is generated using the joint secret sharing scheme for generating a share of the first blinding key.
13. The method of claim 11 or claim 12, wherein the intermediate value is generated by
generating a first multiplicative key share based on the first ephemeral private key share and the blinding key share;
obtaining a respective multiplicative key share from at least the threshold number of participants; and
generating the intermediate value based on the first multiplicative key share and each of the respective multiplicative key shares.
14. The method of claim 13, comprising transmitting the first multiplicative key share to at least each of the threshold number of participants.
15. The method of any preceding claim, wherein the message-independent component is generated based on a second blinding key share of a second blinding key.
16. The method of claim 15, wherein the second blinding key share is generated using the joint secret sharing scheme for generating a share of the second blinding key.
17. The method of claim 10 or any claim dependent thereon, wherein the first message-independent component is generated based on a first pre-signature share, wherein the first pre-signature share is generated based on:
a first intermediary share, the first intermediary share being generated based on the first private key share and the inverse corresponding to the first ephemeral private key share; and
a respective intermediary share obtained from at least the threshold number of participants.

18. The method of claim 10 when dependent on any of claims 1 to 16, wherein the first message-independent component is generated based on a first pre-signature share, wherein the first pre-signature share is generated based on:
- a first intermediary share, the first intermediary share being generated based on the first private key share and the first blinding key share;
 - a respective intermediary share obtained from at least the threshold number of participants.
19. The method of claim 18, wherein the first pre-signature share is generated based on the inverse corresponding to the first ephemeral private key share.
20. The method of any of claims 17 to 19, wherein the first intermediary share is generated based on the second blinding key share.
21. The method of any of claims 17 to 20, wherein the first pre-signature share is generated based on the shared value.
22. The method of claim 21, wherein the first intermediary share is generated based on the shared value.
23. The method of either claim 17 or claim 18, or any claim dependent thereon, comprising transmitting the first intermediary share to at least the threshold number of participants.
24. The method of any preceding claim, comprising generating a plurality of different instances of the message-independent component.
25. The method of any preceding claim, comprising generating a plurality of different instances of the first ephemeral private key shares.
26. The method of claim 24 or claim 25, comprising generating a plurality of different instances of the first blinding key share and/or the second blinding key share.

27. The method of either claim 17 or claim 18, or any claim dependent thereon, comprising generating a plurality of different instances of the first pre-signature shares.
28. The method of any preceding claim, comprising obtaining the message from the coordinator.
29. The method of any of claims 1 to 28, comprising generating the message.
30. The method of any preceding claim, wherein the message is a hash of a second message.
31. The method of any preceding claim, wherein said causing of the first signature share to be made available to the coordinator comprises at least one of:
transmitting the first signature share to the coordinator;
broadcasting the first signature share to one or more of the threshold number of participants.
32. The method of any preceding claim, wherein said causing of the first message-independent component to be made available to the coordinator comprises at least one of:
transmitting the first message-independent component to the coordinator;
broadcasting the first message-independent component to one or more of the threshold number of participants.
33. A computer-implemented method of generating a digital signature of a message, wherein a threshold number of different signature shares from respective participants of a group of participants are required to generate the digital signature, wherein each participant has a respective private key share, wherein each participant has a respective ephemeral private key share, the method being performed by a coordinator and comprising:
obtaining at least a threshold number of respective message-independent components, wherein each respective message-independent component is generated based on a respective private key share;

obtaining at least the threshold number of respective signature shares, wherein each respective signature share is based on at least a respective message-dependent component, and wherein each respective message-dependent component is generated based on the message; and

generating the signature of the message based on each of the obtained signature shares and each of the obtained message-independent components, wherein each message-independent component and/or message-dependent component is based on a respective ephemeral private key share.

34. The method of claim 33, wherein each respective signature share is based on the respective message-independent component.

35. The method of claim 33, comprising:
generating a common message-independent component based on each of the obtained message-independent components; and
generating the signature based on the common message-independent component.

36. The method of claim 35, wherein each participant has a shared value based on an ephemeral public key corresponding to the ephemeral private key, and wherein each respective message-independent component is based on the shared value.

37. The method of any of claims 33 to claim 36, comprising transmitting the message to one, some or all of the participants in the threshold number of participants.

38. The method of any of claims 33 to claim 37, comprising transmitting a request for a respective signature share to at least the threshold number of participants.

39. The method of any of claims 33 to claim 38, comprising generating one of the obtained signature shares.

40. The method of any of claims 33 to 39, comprising outputting the signature.

41. The method of claim 40, wherein outputting the signature comprises:
transmitting the signature to one or more parties; and/or
recording the signature on a digital medium; and/or
making the signature available to the public.
42. The method of any preceding claim, wherein the message comprises at least part of a blockchain transaction.
43. The method of any preceding claim, wherein the threshold number of participants is less than the total number of participants in the group of participants.
44. 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 43.
45. A computer program embodied on computer-readable storage and configured so as, when run on computer equipment of claim 46, to perform the method of any of claims 1 to 43.