CLAIMS

1. A computer-implemented method of identifying a denial-of-service attack during a threshold signature scheme, wherein each participant of a group of participants has a respective share of a first shared secret and a respective share of a second shared secret, wherein the method is performed by a first participant of the group and comprises:

calculating a first target share based on at least a first share of the first shared secret and a first share of the second shared secret, wherein the first target share is used to calculate a first signature share of a threshold signature;

calculating a target value based on the first target share and a first predetermined amount of other target shares, wherein each other target share is calculated by a respective participant;

calculating a target public key corresponding to the target value;

calculating a first verification share based on the first share of the first shared secret and a public key corresponding to the second shared secret;

calculating a verification public key based on at least the first verification share and a second predetermined amount of other verification shares, wherein each other verification share is calculated by a respective participant; and

determining whether at least one other participant is attempting a denial-of-service attack based on whether the verification public key matches the target public key.

2. The method of claim 1, comprising sharing the first target share and the first verification share with the other participants in the group.

3. The method of claim 2, wherein said sharing comprises broadcasting the first target share and/or the first verification share to the other participants in the group.

4. The method of any preceding claim, comprising:

obtaining the first predetermined amount of other target shares from the respective participants; and

obtaining the second predetermined amount of other verification shares from the respective participants.

5. The method of any preceding claim, wherein the first share of the first shared secret is calculated by performing a first instance of a joint verification random secret sharing scheme (JVRSS) with the group of participants.

6. The method of any preceding claim, wherein the first share of the second shared secret is calculated by performing a second instance of JVRSS with the group of participants.

7. The method of claim 6, wherein the public key corresponding to the second shared secret is calculated based on the obfuscated coefficients shared by each participant when performing the second instance of JVRSS.

8. The method of any preceding claim, wherein each participant is associated with a respective index of a sequence, wherein the first predetermined amount of other target shares are calculated by those other participants with respective indices following the index of the first participant, and wherein the second predetermined amount of other verification shares are calculated by those other participants with respective indices following the index of the first participant.

9. The method of any preceding claim, wherein the group has a size $N \geq 2t + 1$ wherein the threshold of the first shared secret and of the threshold signature is $t + 1$, and wherein t is the degree of the first shared secret.

10. The method of claim 9, wherein the first predetermined amount is $2t$ and wherein the second predetermined amount is t.

11. The method of claim 9 or claim 10, wherein the group has a size $N > 2t + 1$, wherein said calculating of the verification public key comprises calculating a plurality of verification public keys, each verification public key being calculated based on the first verification share and a different second predetermined amount of other verification shares, and wherein the method comprises:

comparing each of the plurality of verification public keys; and

identifying at least one participant attempting a denial-of-service attack as the participant whose respective verification share results in a verification public key that does not match at least one other verification public key.

12. The method of any preceding claim, wherein the first shared secret is a first blinding key, wherein the second shared secret is an ephemeral key, and wherein the first target share is a multiplicative share.

13. The method of any of claims 1 to 11, wherein each participant of the group of participants has a respective share of a third shared secret, wherein the first target share is calculated based on a first share of the first shared secret, and wherein the verification public key is calculated based on a public key corresponding to the third shared secret.

14. The method of claim 13, wherein the first shared secret is an inverse ephemeral key, the second shared secret is a private key, the third shared secret is a second blinding key, and the first target share is a first intermediary share.

15. The method of claim 13 or claim 14, wherein the first share of the third shared secret is calculated by performing a third instance of JVRSS with the group of participants.

16. The method of claim 6, wherein the public key corresponding to the third shared secret is calculated based on the obfuscated coefficients shared by each participant when performing the third instance of JVRSS.

17. The method of any preceding claim, comprising only using the first target share and/or the target value to calculate the first signature share on condition that the verification public key matches the target public key.

18. 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 17.

19. 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 17.

20. A computer-implemented method of identifying a denial-of-service attack during a threshold signature scheme, wherein each participant of a group of participants has a respective share of a shared private key, a respective share of an ephemeral private key, a respective share of a first blinding key, and a respective share of a second blinding key, wherein the method is performed by a first participant of the group and comprises:

calculating a first public key corresponding to a first inverse ephemeral private key share, wherein first public key is calculated based on i) an inverse of a product of the ephemeral private key and the first blinding key, and ii) a public key corresponding to a first share of the first blinding key;

calculating a second public key corresponding to a pre-signature share, wherein the second public key is calculated based on i) a public key corresponding to an intermediary value and ii) a public key corresponding to a first share of the second blinding key, wherein the intermediary value is based on i) an inverse of the ephemeral private key, ii) the private key and iii) the second blinding key; and

sending the first public key and the second public key to a coordinating party, wherein the coordinating party has access to a first signature share calculated by the first participant, and wherein the first signature share is calculated based on i) a first share of the ephemeral private key, ii) a message, iii) a public key corresponding to the shared private key, and iv) a first share of the second blinding key.

~~21. The method of claim 20, wherein some or all of the respective shares are calculated using respective instances of a joint verifiable random secret sharing (JVRSS) scheme.~~

~~22. The method of claim 20 or claim 21, comprising calculating the inverse of the product of the ephemeral private key and the first blinding key.~~

~~23. The method of any preceding claim, comprising calculating the intermediary value based on a first intermediary share and a respective intermediary share from each other participant.~~

~~24. The method of claim 23, comprising calculating the public key corresponding to the intermediary value.~~

~~25. The method of any preceding claim, comprising calculating the public key corresponding to the first share of the first blinding key.~~

~~26. The method of any preceding claim, comprising calculating the public key corresponding to the first share of the second blinding key.~~

~~27. The method of any preceding claim, comprising:~~

~~calculating the first signature share; and~~

~~sending the first signature share to the coordinating party.~~

~~28. The method of any preceding claim, comprising obtaining the message from the coordinating party.~~

~~29. The method of any of claims 20 to 28, comprising generating the message.~~

~~30. The method of any preceding claim, comprising calculating the public key corresponding to the shared ephemeral private key, and wherein the first signature share is based on a first coordinate of the public key corresponding to the shared ephemeral private key.~~

~~31. A computer-implemented method of identifying a denial-of-service attack, wherein each participant of a group of participants has a respective share of a private key, a respective share of an ephemeral private key, a respective share of a first blinding key, and a respective share of a second blinding key, and wherein the method is performed by a~~

coordinating party configured to generate a signature based on a threshold number of signature shares, and comprises:

receiving a first public key from a first participant;

receiving a second public key from the first participant;

receiving a first signature share from the first participant;

calculating a public key corresponding to a first candidate signature share based on i) the first public key, ii) a message, iii) a public key corresponding to the shared ephemeral private key, and iv) the second public key; and

determining whether the first participant is attempting a denial-of-service attack based on whether a public key corresponding to the first signature share matches the public key corresponding to the first candidate signature share.

32. A computer-implemented method of identifying a denial-of-service attack, wherein each participant of a group of participants has a respective share of a private key, a respective share of an ephemeral private key, a respective share of a first blinding key, and a respective share of a second blinding key, and wherein the method is performed by a coordinating party configured to generate a signature based on a threshold number of signature shares, and comprises:

calculating a first public key corresponding to a first inverse ephemeral private key share of a first participant;

calculating a second public key corresponding to a pre-signature share of the first participant;

receiving a first signature share from the first participant;

calculating a public key corresponding to a candidate first signature share based on i) the first public key, ii) a message, iii) a public key corresponding to the shared ephemeral private key, and iv) the second public key; and

determining whether the first participant is attempting a denial-of-service attack based on whether a public key corresponding to the first signature share matches the public key corresponding to the candidate first signature share.

33. The method of claim 31 or claim 32, comprising, on condition that the public key corresponding to the first signature matches the public key corresponding to the candidate

first signature share, using the first signature share to calculate a signature based on the first signature and one or more additional signature shares calculated by respective participants of the group.

34. The method of claim 33, comprising:

using the first signature share to calculate a signature based on the first signature share and one or more additional signature shares calculated by respective participant of the group, wherein the first signature share is received prior to said receiving or calculating of the first public key and the second public key;

determining whether the signature is an invalid signature; and

performing said determining of whether the first participant is attempting a denial-of-service attack in response to determining that the signature is an invalid signature.

35. The method of claim 34, wherein said determining of whether the signature is an invalid signature comprises verifying the signature against the public key corresponding to the shared private key.

36. 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 20 to 35.

37. 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 20 to 35.