Claims

1. A computer-implemented method for performing a digital signature according to a public key signature scheme, the method comprising

computing a presignature;

providing a master secret key pair, the master secret key pair comprising a first master secret key and a second master secret key;

providing a master public key pair, the master public key pair comprising a first master public key and a second master public key';

deriving a secret subkey from the master secret key pair;

deriving a public subkey from the master public key pair; and

performing the digital signature by means of the secret subkey and the computed presignature.

2. A computer-implemented method according to claim 1, wherein the digital signature is a threshold signature.

3. A computer-implemented method according to claim 1 or claim 2, wherein

deriving the secret subkey from the master secret key pair comprises performing a first algebraic operation on the master secret key pair; and

deriving the public subkey from the master public key pair comprises performing a second algebraic operation on the master public key pair.

4. A computer-implemented method according to claim 3, wherein the first algebraic operation and the second algebraic operation are the same.

5. A computer-implemented method according to claim 3 or 4, wherein the first algebraic operation and the second algebraic operation are linear operations.

6. A computer-implemented method according to any of the preceding claims, wherein

deriving the secret subkey from the master secret key pair comprises performing a mixed key derivation such that the secret subkey depends on both the first master secret key and the second master secret key and the public subkey depends on both the first master public key and the second master public key.

7. A computer-implemented method according to any of the preceding claims, wherein the digital signature is a digital signature according to a signature algorithm based on discrete logarithms.

8. A computer-implemented method according to any of the preceding claims, wherein the digital signature is a digital signature according to a signature algorithm based on elliptic curves.

9. A computer-implemented method according to claim 8, wherein the elliptic curve digital signature algorithm operates on an elliptic curve E defined over in particular $\mathbb{Z}_p$ and generated by a point G of order q, in particular prime order q,

wherein

$(D, D') \coloneqq (dG, d'G)$; and wherein

D is the first master public key;

D' is the second master public key;

d is the first master secret key;

d' is the second master secret key.

10. A computer-implemented method according to claim 8 or 9, wherein the digital signature is a digital signature according to the Elliptic Curve Digital Signature Algorithm (ECDSA).

11. A computer-implemented method according to any of the preceding claims, further comprising

providing a discriminant e, in particular a discriminant $e \in \mathbb{Z}_q$;

deriving the secret subkey from the master secret key pair by computing

$d'' := d + ed'$;

and

deriving the public subkey D'' from the master public key pair by computing

$D'' := D + eD'$, wherein

D is the first master public key;

D' is the second master public key;

d is the first master secret key;

d' is the second master secret key;

d'' is the secret subkey; and

D'' is the public subkey.

12. A computer-implemented method according to claim 11, further comprising

deriving the discriminant e by a hash function.

13. A computer-implemented method according to claim 12, further comprising

deriving the discriminant e by applying the hash function on a set of hash input data, the hash input

data comprising an arbitrary identifier, the master public key pair and/or further input data.

14. A computer-implemented method according to claim 13, wherein the arbitrary identifier uniquely identifies ownership and/or context of the public subkey or the secret subkey.

15. A computer-implemented method according to any of the preceding claims, further comprising

receiving a signing request to perform the digital signature on a message;

re-randomizing the presignature; and

performing the digital signature on the message with the re-randomized presignature.

16. A computer-implemented method according claim 15, wherein

computing the presignature comprises computing a random nonce; and

re-randomizing the presignature comprises re-randomizing the nonce.

17. A computer-implemented method according to claim 15 or 16, wherein re-randomizing the presignature comprises performing an algebraic operation on the presignature.

18. A computer-implemented method according to any of the preceding claims 15-17, wherein re-randomizing the presignature comprises performing a linear operation on the presignature.

19. A computer-implemented method according to any of the preceding claims 15-18, wherein re-randomizing the presignature comprises computing

a non-predictable public re-randomization value; and

utilizing the public re-randomization value for the re-randomizing of the presignature.

20. A computer-implemented method according to claim 19, wherein the non-predictable public re-randomization value is generated after receiving the signing request.

21. A computer-implemented method according to claim 19 or 20, further comprising performing a pseudo-random generation of the public re-randomization value.

22. A computer-implemented method according to any of the preceding claims 19 or 20, further comprising deriving the public re-randomization value by applying a hash function to at least the message or a hash of the message.

23. A computer-implemented method according to claim 22, further comprising deriving the public re-randomization value by applying the hash function to the public key of the digital signature and/or to other inputs.

24. A computer-implemented method according to any of the preceding claims 19-23, further comprising deriving the public re-randomization value from a random beacon.

25. A computer-implemented method according to claim 9, wherein

computing the presignature comprises

generating a random element r' by:

$r' \leftarrow \mathbb{Z}_q^*$;

and computing

$R' \leftarrow r'G \in E.$

26. A computer-implemented method according to claims 19 and 25, wherein re-randomizing the presignature comprises computing

$r := r' + \delta;$

$R := R' + \delta G;$

wherein $\delta \in \mathbb{Z}_q$ is the non-predictable public re-randomization value.

27. A computing system for performing a digital signature according to a public key signature scheme, the computing system being configured to perform a computer-implemented method comprising

computing a presignature;

providing a master secret key pair, the master secret key pair comprising a first master secret key and a second master secret key;

providing a master public key pair, the master public key pair comprising a first master public key and a second master public key';

deriving a secret subkey from the master secret key pair;

deriving a public subkey from the master public key pair; and

performing the digital signature by means of the secret subkey and the computed presignature.

28. A computer program product for performing a digital signature according to a public key signature scheme, the computer program product comprising a computer readable storage medium having program instructions embodied therewith, the program instructions

executable by the computing system to cause the computing system to perform a method comprising

computing a presignature;

providing a master secret key pair, the master secret key pair comprising a first master secret key and a second master secret key;

providing a master public key pair, the master public key pair comprising a first master public key and a second master public key';

deriving a secret subkey from the master secret key pair;

deriving a public subkey from the master public key pair; and

performing the digital signature by means of the secret subkey and the computed presignature.