Claims

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

computing a presignature;

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; 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; wherein the non-predictable public re-randomization value is generated after receiving the signing request.

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

computing the presignature comprises computing a random nonce; and

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

3. A computer-implemented method according to any of the preceding claims, wherein re-randomizing the presignature comprises performing an algebraic operation on the presignature.

4. A computer-implemented method according to any of the preceding claims, wherein re-randomizing the

presignature comprises performing a linear operation on the presignature.

5. A computer-implemented method according to any of the preceding claims, wherein the digital signature is a threshold signature.

6. A computer-implemented method according to any of the preceding claims, further comprising performing a pseudo-random generation of the public re-randomization value.

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

8. A computer-implemented method according to claim 7, 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.

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

10. 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.

11. 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.

12. A computer-implemented method according to any of the preceding claims, wherein the digital signature is a digital signature according to the Elliptic Curve Digital Signature Algorithm (ECDSA).

13. A computer-implemented method according to claim 11 or 12, wherein the digital signature algorithm operates on an elliptic curve E generated by a point G of order q, in particular prime order q, and wherein

computing the presignature comprises

generating a random element r' by:

$r' \leftarrow Z_q^*$;

and

computing

$\mathrm{R}' \leftarrow r'\mathrm{G} \in E$.

14. A computer-implemented method according to claim 13, wherein re-randomizing the presignature comprises computing

$r := r' + \delta$;

$\mathrm{R} := \mathrm{R}' + \delta\mathrm{G}$;

wherein δ is a non-predictable public value.

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

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; and

deriving a public subkey from the master public key pair.

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

17. A computer-implemented method according to claim 15 or 16, wherein the first algebraic operation and the second algebraic operation are the same.

18. A computer-implemented method according to any of the preceding claims 15-17, wherein the first algebraic operation and the second algebraic operation are linear operations.

19. A computer-implemented method according to any of the preceding claims 15-18, 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.

20. A computer-implemented method according to any of the preceding claims 15-19, wherein a digital signature algorithm operates on an elliptic curve E defined over $\mathbb{Z}_p$ and generated by a point G of order q, in particular prime order q,

wherein

$(D, D') := (dG, d'G)$; 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.

21. A computer-implemented method according to any of the preceding claims 15-20, 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.

22. A computer-implemented method according to claim 21, further comprising

deriving the discriminant e by a hash function.

23. A computer-implemented method according to claim 22, 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.

24. A computer-implemented method according to claim 23, wherein the arbitrary identifier uniquely identifies ownership and/or context of the public subkey or the secret subkey.

25. A computer-implemented method according to any of the preceding claims 1-14, further comprising

providing a master key pair comprising a master public key and a master secret key;

deriving subkey pairs comprising a public subkey and a secret subkey from the master key pair by applying an additive shift operation on the master key pair.

26. A computer-implemented method according to claim 25, comprising

providing a discriminant e, in particular a discrimant $e \in Z_q$;

computing the secret subkey by

$d' := d + e$; and

computing the public subkey by

$D' := D + eG$.

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;

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; 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; wherein the non-predictable public re-randomization value is generated after receiving the signing request.

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;

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; 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; wherein the non-predictable public re-randomization value is generated after receiving the signing request.