

Claims

1. A computer-implemented method for redistribution of a (n,t) -secret sharing of a secret from a set of dealers to a set of receivers, the (n,t) -secret sharing comprising n secret shares, wherein a threshold number $t \leq n$ of the secret shares is sufficient to reconstruct the secret, the method comprising:

performing, by each of at least the threshold number t of dealers, the steps of:

creating a (n',t') -secret sharing of its respective secret share, the (n',t') -secret sharing comprising n' secret sub-shares of its respective secret share, wherein a threshold number $t' \leq n'$ of the secret sub-shares is sufficient to reconstruct the secret share;

creating a set of ciphertexts, the set of ciphertexts comprising for each receiver one encrypted sub-share of the n' secret sub-shares of its respective secret share, the encrypted secret sub-share being encrypted with respect to a public encryption key of a public-key encryption scheme of the respective receiver;

generating a non-interactive zero-knowledge proof that the set of ciphertexts jointly contain a redistribution of its secret share;

broadcasting a dealing to the set of receivers, the dealing comprising the set of ciphertexts for the set of receivers and the corresponding non-interactive zero-knowledge proof;

using a public-key encryption scheme with forward secrecy for encrypting the secret sub-shares for the receivers, wherein the encryption scheme is configured to perform a chunked encryption of the sub-

shares, wherein each sub-share is split into a plurality of plaintexts each representing a chunk; and
generating, by the set of dealers, a further non-interactive zero-knowledge proof, the further zero-knowledge proof being configured to prove that the chunked encryption is correct.

2. A computer-implemented method according to claim 1, further comprising

checking, by a predefined set of parties, in particular by the set of receivers, the non-interactive zero-knowledge proofs of the dealings; and

once a sufficient number t of proofs have been successfully checked,

decrypting, by each of the receivers, its encrypted sub-shares across the dealings; and

combining, by each of the receivers, the decrypted sub-shares to a new secret share of the secret.

3. A computer-implemented method according to any of the preceding claims, wherein the zero-knowledge proofs are publicly verifiable zero-knowledge proofs such that any party can verify them.

4. A computer-implemented method according to any of the preceding claims, wherein the secret sharing is a linear secret sharing, in particular a Shamir secret sharing.

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

creating, by each dealer, associated public key material associated to its secret share and its secret sharing of said secret share; and

adding the associated public key material to the dealing.

6. A computer-implemented method according to claim 5, wherein the associated public key material comprises

a public group element related to the secret share of each dealer; and/or

public group elements which are related to the secret sharing created by each dealer.

7. A computer-implemented method according to any of the preceding claims, wherein the secret is a secret key corresponding to a public verification key of a public key signature scheme.

8. A computer-implemented method according to any of the preceding claims 2 to 7, further comprising
 creating, by any party, in particular a receiver, from the associated public key material created by the set of dealers new associated public key material associated to the new secret sharing and the new secret shares of the set of receivers.

9. A computer-implemented method according to claims 5, 6, 7 and/or 8, wherein the creating of the new associated public key material comprises

deriving the new associated public key material from the associated public key material created by the set of dealers, the new associated public key material comprising

public share verification keys which are associated to the new secret shares of the receivers;

a public verification key related to the secret key; and/or

elements from which the public share verification keys of the receivers and/or the public verification key may be derived.

10. A computer-implemented method according to any of the preceding claims, further comprising using a public-key encryption scheme with chosen ciphertext attack security for encrypting the secret sub-shares for the set of receivers.

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

wherein the encryption scheme with forward secrecy is a binary tree encryption scheme.

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

wherein the public-key encryption scheme is a multi-receiver encryption scheme, the multi-receiver encryption scheme being configured to encrypt the sub-shares of a dealer to the public encryption keys of the set of receivers.

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

wherein the multi-receiver encryption scheme uses shared randomness to encrypt the sub-shares of the set of dealers to the public encryption keys of the set of receivers.

14. A computer-implemented method according to any of the claims 2 to 13, further comprising performing the decrypting of the encrypted sub-shares in a separate process, on a virtual hardware security module, or on a hardware security module.

15. A computer-implemented method according to any of the preceding claims, wherein the step of broadcasting the dealings comprises putting the dealings on a bulletin board.

16. A distributed network comprising a plurality of nodes, wherein the network is configured to perform a computer-implemented method for redistribution of a (n,t) -secret sharing of a secret from a set of dealers to a set of receivers, the (n,t) -secret sharing comprising n secret shares, wherein a threshold number $t \leq n$ of the secret shares is sufficient to reconstruct the secret s , the method comprising:

performing, by each of at least the threshold number t of dealers, the steps of:

creating a (n',t') -secret sharing of its respective secret share, the (n',t') -secret sharing comprising n' secret sub-shares of its respective secret share, wherein a threshold number $t' \leq n'$ of the

secret sub-shares is sufficient to reconstruct the secret share;

creating a set of ciphertexts, the set of ciphertexts comprising for each receiver one encrypted sub-share of the n' 'secret sub-shares of its respective secret share, the encrypted secret sub-share being encrypted with respect to a public encryption key of a public-key encryption scheme of the respective receiver;

generating a non-interactive zero-knowledge proof that the set of ciphertexts jointly contain a redistribution of its secret share;

broadcasting a dealing to the set of receivers, the dealing comprising the set of ciphertexts for the set of receivers and the corresponding non-interactive zero-knowledge proof;

using a public-key encryption scheme with forward secrecy for encrypting the secret sub-shares for the receivers, wherein the encryption scheme is configured to perform a chunked encryption of the sub-shares, wherein each sub-share is split into a plurality of plaintexts each representing a chunk; and

generating, by the set of dealers, a further non-interactive zero-knowledge proof, the further zero-knowledge proof being configured to prove that the chunked encryption is correct.

17. A node for a distributed network according to claim 16.

18. A computer program product for redistribution of a (n,t) -secret sharing of a secret from a set of dealers to a set of receivers, the (n,t) -secret sharing comprising n secret shares, wherein a threshold number $t \leq n$ of the secret shares is sufficient to reconstruct the secret, the computer program product comprising a computer readable storage medium having program instructions embodied therewith, the program instructions executable by one

or more nodes of a distributed network to cause the one or more nodes to perform a method comprising

performing, by each of at least the threshold number t of dealers, the steps of:

creating a (n', t') -secret sharing of its respective secret share, the (n', t') -secret sharing comprising n' secret sub-shares of its respective secret share, wherein a threshold number $t' \leq n'$ of the secret sub-shares is sufficient to reconstruct the secret share;

creating a set of ciphertexts, the set of ciphertexts comprising for each receiver one encrypted sub-share of the n' secret sub-shares of its respective secret share, the encrypted secret sub-share being encrypted with respect to a public encryption key of a public-key encryption scheme of the respective receiver;

generating a non-interactive zero-knowledge proof that the set of ciphertexts jointly contain a redistribution of its secret share;

broadcasting a dealing to the set of receivers, the dealing comprising the set of ciphertexts for the set of receivers and the corresponding non-interactive zero-knowledge proof;

using a public-key encryption scheme with forward secrecy for encrypting the secret sub-shares for the receivers, wherein the encryption scheme is configured to perform a chunked encryption of the sub-shares, wherein each sub-share is split into a plurality of plaintexts each representing a chunk; and

generating, by the set of dealers, a further non-interactive zero-knowledge proof, the further zero-knowledge proof being configured to prove that the chunked encryption is correct.