

CLAIMS

1. A method for splitting a transaction key in a key management system, wherein the key management system comprises a management device for managing user devices of users in a user group and a hardware security module connected to the management device, and the method comprises: at the hardware security module,

acquiring, by the hardware security module from the management device, a number of the users of the user group and a first predetermined value, wherein the first predetermined value indicates a minimum number of users for recovering the transaction key, and wherein the user group is configured to manage the transaction key;

randomly generating, by the hardware security module, the transaction key associated with processing authority of this transaction based on messages about other users except for a splitting user determined for splitting the transaction key in the user group, wherein the messages about other users at least indicate public keys of the other users;

splitting, by the hardware security module, the transaction key into a plurality of sub-keys of the same number as the number of the users, wherein each sub-key in the plurality of sub-keys corresponds to one user in the user group; and

encrypting, by the hardware security module, the plurality of sub-keys respectively with public keys of the users corresponding to the plurality of sub-keys;

wherein the hardware security module is not accessible by any user device of any user in the user group.

2. The method according to claim 1, further comprising: at the management device, designating or randomly determining the splitting user in the user group.

3. The method according to claim 1, wherein the messages about other users also indicate at least one of the following:

signature information for verifying public keys of the other users;

identifiers of the other users;

signature information of a hash value of combined data of the other users; and

a validity period of the messages about other users.

4. The method according to claim 3, wherein randomly generating the transaction key associated with processing authority of this transaction comprises:

determining, based on the signature information of the public keys of the other users, whether the public keys of the other users pass verification; and

randomly generating, in response to the public keys of the other users passing verification, a plurality of random numbers that are of the same number as the first predetermined value and configured to construct a splitting polynomial, wherein the plurality of random numbers configured to construct a splitting polynomial comprise the transaction key.

5. The method according to claim 4, wherein the messages about other users also indicate a certificate of the management device, and determining, based on the signature information of the public keys of the other users, whether the public keys of the other users pass verification further comprises:

determining whether the certificate of the management device passes verification, and

determining, based on the signature information of the public keys of the other users, whether the public keys of the other users pass verification in response to determining that the certificate of the management device passes verification.

6. The method according to claim 4, wherein splitting the transaction key into a plurality of sub-keys of the same number as the number of the users comprises:

determining the plurality of sub-keys based on the number of the users of the user group and the plurality of random numbers configured to construct a splitting polynomial, wherein each sub-key comprises a first sub-key component and a second sub-key component.

7. The method according to claim 1, wherein encrypting the plurality of sub-keys respectively with public keys of the users corresponding to the plurality of sub-keys comprises:

encrypting the sub-keys based on the public keys of the users corresponding to the sub-keys and a validity periods of the messages about other users.

8. The method according to claim 1, further comprises: at the management device, signing a random number with a private key of the management device to generate signature data, and sending the generated signature data to a group-forming user determined for forming the user group; and

receiving, from the group-forming user, business information about the user group, public keys of the user devices, and the signature data signed with a private key of a user device of the group-forming user, wherein the business information at least comprises the number of the users of the user group and the first predetermined value.

9. A method for recovering a transaction key in a key management system, wherein the key management system comprises a management device for managing user devices of users in a user group and a hardware security module connected to the management device, and the method comprises: at the hardware security module,

acquiring, by the hardware security module from the management device, a recovery message for recovering the transaction key, wherein the recovery message comprises a number of verified users who agreed on this transaction in the user group and an identifier of a user that is determined to be a recovery user for recovering the transaction key in the user group, wherein the user group is configured to manage the transaction key;

recovering, by the hardware security module, the transaction key based on sub-keys of the verified users in response to determining that the number of the verified users is greater than or equal to a first predetermined value, wherein the sub-keys of the verified users were generated, by the hardware security module, by splitting the transaction key in advance; and

signing a transaction request regarding this transaction based on the recovered transaction key;

wherein the hardware security module is not accessible by any user device of any user in the group.

10. The method according to claim 9, further comprising: at the management device, designating or randomly determining the recovery user in the user group.

11. The method according to claim 9, wherein the sub-keys of the verified users are encrypted with a public key of the recovery user.

12. The method according to claim 11, wherein the sub-keys of the verified users and an association random number associated with the transaction are encrypted together with the public key of the recovery user.

13. The method according to claim 9, wherein the recovery message also indicates at least one of the following:

an association random number associated with this transaction;

the sub-keys of the verified users and the association random number that are encrypted with a public key of the recovery user;

signature information of the verified users;

a certificate of the management device; and

signature information of a hash value of the recovery message.

14. The method according to claim 9, further comprising: at the management device, sending, in response to receiving a request for the transaction, transaction information for determining whether to agree on this transaction to the users of the user group, wherein the transaction information at least indicates transaction content of this transaction and an identifier of the recovery user;

acquiring a sub-key of each verified user who agrees on this transaction in the user group, wherein the sub-keys of the verified users are encrypted with a public key of the recovery user; and

sending, in response to determining that conditions of the transaction is met, the recovery message to the hardware security module.

15. The method according to claim 1 or 9, wherein the user devices of the users each further comprise a biometric module configured to determine, based on pre-stored biological characteristics

of an authorized user, whether an operator operating the user device is the authorized user of the user device.

16. A computer program product, tangibly stored on a non-transitory computer-readable storage medium and comprising machine-executable instructions, wherein the machine-executable instructions are configured to, when executed, cause a machine to execute steps of the method according to any one of claims 1-14.

17. A computer-readable storage medium storing machine-executable instructions, wherein the machine-executable instructions are configured to, when executed, cause a machine to execute steps of the method according to any one of claims 1-14.

18. A key management system, comprising a processor, a memory, and computer programs stored in the memory, wherein the computer programs are configured to, when executed by the processor, cause the key management system to execute steps of the method according to any one of claims 1-14.