

CLAIMS

What is claimed is:

1. A data encryption method, comprising:
 - obtaining at least one piece of data to be encrypted;
 - calculating, for each particular piece of data of the at least one piece of data, a data-specific key corresponding to the particular piece of data, the data-specific key being calculated based on a prestored root key and a data identifier of the particular piece of data using a one-way function, wherein:
 - the one-way function is such that the prestored root key is not uniquely derivable from the data-specific key using the one-way function,
 - the particular piece of data corresponds to a particular node of a predetermined tree structure,
 - the data identifier of the particular piece of data represents a path between the particular node and a root node of the predetermined tree structure,
 - the path comprises a plurality of path segments,
 - the data-specific key is calculated based on one or more keys that are different from the prestored root key, each key of the one or more keys being calculated based on a corresponding different path segment of the plurality of path segments, the path segment connecting a corresponding node of the path segment to its parent node; and
 - generating encrypted data corresponding to the particular piece of data by encrypting the particular piece of data using the data-specific key corresponding to the particular piece of data.
2. The method according to claim 1, wherein the at least one piece of data is in a one-to-one correspondence with all leaf nodes of the predetermined tree structure, and wherein calculating the data-specific key corresponding to the particular piece of data comprises:
 - calculating, based on the prestored root key and the path, a key corresponding to a leaf node using the one-way function; and
 - using the key corresponding to the leaf node as the data-specific key.

3. The method according to claim 2, wherein the path corresponds to a sequence of all nodes from the root node to the leaf node, and the prestored root key corresponds to the root node, and wherein calculating, based on the prestored root key and the path, the key corresponding to the leaf node using the one-way function comprises:

using the root node as an input node;

inputting a key corresponding to the input node and path information of a path between a next node and the input node to the one-way function, to calculate a key corresponding to the next node;

determining whether the next node is the leaf node;

in response to determining that the next node is the leaf node, using the calculated key corresponding to the next node as the key corresponding to the leaf node; and

in response to determining that the next node is not the leaf node, using the next node as a new input node to continue to calculate a key corresponding to a next node of the input node in the sequence until the key corresponding to the leaf node is obtained.

4. A key sending method, comprising:

receiving a data decryption request sent by a data decryption device, wherein the data decryption request comprises a data identifier;

calculating a data-specific key based on a prestored root key and the data identifier using a one-way function, wherein:

the one-way function is such that the prestored root key is not uniquely derivable from the data-specific key using the one-way function,

the data identifier corresponds to a particular node of a predetermined tree structure,

the data identifier represents a path between the particular node and a root node of the predetermined tree structure,

the path comprises a plurality of path segments,

the data-specific key is calculated based on one or more keys that are different from the prestored root key, each key of the one or more keys being calculated based on a corresponding different path segment of the plurality of path segments, the path segment connecting a corresponding node of the path segment to

its parent node; and

sending the calculated data-specific key to the data decryption device, wherein the data decryption device decrypts encrypted data corresponding to the data identifier comprised in the data decryption request based on the data-specific key.

5. The method according to claim 4, wherein the encrypted data is in a one-to-one correspondence with all leaf nodes of the predetermined tree structure.

6. The method according to claim 5, wherein the path corresponds to a sequence of all nodes from the root node to a leaf node, and the prestored root key corresponds to the root node, and wherein calculating the data-specific key comprises:

determining the sequence of all nodes based on the path;

using the root node as an input node;

inputting a key corresponding to the input node and path information of a path between a next node and the input node to the one-way function, to calculate a key corresponding to the next node;

determining whether the next node is the last node in the sequence of all nodes;

in response to determining that the next node is the last node in the sequence of all nodes, using the calculated key corresponding to the next node as the data-specific key to be sent to the data decryption device; and

in response to determining that the next node is not the last node in the sequence of all nodes, using the next node as a new input node to continue to calculate a key corresponding to a next node of the input node in the sequence until a key corresponding to the last node in the sequence is obtained.

7. A data decryption method, comprising:

sending a data decryption request to a data encryption device, wherein the data decryption request comprises a data identifier;

receiving a key returned by the data encryption device, wherein the key is calculated by the data encryption device according to the method according to any one of claims 4 to 6; and

decrypting encrypted data corresponding to the data identifier comprised in the data decryption request based on the key.

8. The method according to claim 7, wherein the encrypted data is in a one-to-one correspondence with all leaf nodes of the predetermined tree structure, and wherein decrypting the encrypted data corresponding to the data identifier comprised in the data decryption request based on the key comprises:

in response to determining that the data identifier is path information of a leaf node relative to the root node, decrypting the encrypted data corresponding to the data identifier comprised in the data decryption request by using the key; or

in response to determining the data identifier is path information of an intermediate node relative to the root node, calculating, for each leaf node under the intermediate node, a key corresponding to the leaf node based on path information of the leaf node relative to the intermediate node and the received key using an one-way function, and decrypting the encrypted data corresponding to the leaf node by using the key corresponding to the leaf node.

9. The method according to claim 8, wherein for any leaf node under the intermediate node, path information of the leaf node relative to the intermediate node is a sequence of all nodes from the intermediate node to the leaf node, and wherein calculating, for each leaf node under the intermediate node corresponding to the data identifier, a key corresponding to the leaf node based on path information of the leaf node relative to the intermediate node and the received key using an one-way function comprises:

determining, for each leaf node under the intermediate node corresponding to the data identifier, a sequence based on path information of the leaf node relative to the intermediate node;

using the intermediate node as an input node;

inputting a key corresponding to the input node and path information of a next node of the input node in the sequence relative to the input node to the one-way function, to calculate a key corresponding to the next node;

determining whether the next node is the last node in the sequence;

in response to determining that the next node is the last node in the sequence, using the calculated key corresponding to the next node as a key corresponding to the leaf node; and

in response to determining that the next node is not the last node in the

sequence, using the next node as a new input node to continue to calculate a key corresponding to a next node of the input node in the sequence until a key corresponding to the last node in the sequence is obtained.

10. A data encryption apparatus comprising a plurality of modules for performing the method according to any one of claims 1 to 3, the plurality of modules comprising an acquisition module, a calculation module, and an encryption module.

11. A key sending apparatus comprising a plurality of modules for performing the method according to any one of claims 4 to 6, the plurality of modules comprising a receiving module, a calculation module, and a sending module.

12. A data decryption apparatus comprising a plurality of modules for performing the method according to any one of claims 7 to 9, the plurality of modules comprising a sending module, a receiving module, and a decryption module.

13. A data encryption device, comprising one or more processors and one or more memories, wherein the memory stores a program, and the one or more processors are configured to perform the method according to any one of claims 1 to 3.

14. A key sending device, comprising one or more processors and one or more memories, wherein the memory stores a program, and the one or more processors are configured to perform the method according to any one of claims 4 to 6.

15. A data decryption device, comprising one or more processors and one or more memories, wherein the memory stores a program, and the one or more processors are configured to perform the method according to any one of claims 7 to 9.