Claims

What is claimed is:

1. A method implemented by one or more computing devices, the method comprising:

receiving an original card number for a request of processing a transaction;

calculating a hash value corresponding to the original card number based on the original card number; and

searching a database to determine whether a card number record having the hash value exists in the database and performing one of the following steps;

determining that a card number record having the hash value does not exist in the database, setting the original card number as a new card number, allocating an index card number to the original card number, and sending the index card number to an entity to process the transaction based on the index card number; and

determining that one or more card number records having the hash value exists in the database, obtaining an index card number corresponding to the received original card number from the card number record corresponding to an identical card number, and sending the index card number to an entity to process the transaction based on the index card number.

2. The method of claim 1, wherein no card number record having the hash value exists in the database, the method further comprising:

setting a hash number corresponding to the original card number to be a first value;

obtaining a latest secret key and a version of the latest secret key from a secret key dictionary;

encrypting the original card number using the latest secret key, and combining the version of the latest secret key with a front end of a cipher text obtained from the encryption to obtain a cipher text corresponding to the original card number; and

using the allocated index card number, the cipher text corresponding to the original card number, the hash value corresponding to the original card number and the hash number corresponding to the hash value as a card number record corresponding to the original card number, and storing the card number record in the database, wherein the index card number is determined to be successfully allocated to the original card number if no

violation of a restriction on the hash value and the hash number exists when storing the card number record corresponding to the original card number in the database.

3. The method of claim 1, wherein one or more card number records having the hash value exists in the database, and the method further comprises:

acquiring a respective card number cipher text in each card number record of the one or more card number records;

intercepting a secret key version from the respective card number cipher text;

reading a secret key dictionary based at least in part on the secret key version to obtain a secret key used for encrypting the respective card number cipher text; and

using the secret key to decrypt the respective card number cipher text to obtain a respective original card number from each card number record; and

comparing the respective original card number of each card number record with the received original card number.

4. The method of claim 3, further comprising:

determining that an original card number of a particular card number record of the one or more card number records is identical with the received original card number; and

obtaining an index card number corresponding to the received original card number from the particular card number record.

5. The method of claim 3, further comprising:

determining that no card number record having an original card number is identical with the received original card number;

setting the received original card number as a new card number;

setting a hash number corresponding to the original card number to be a second value;

allocating an index card number to the original card number;

obtaining a latest secret key and a version of the latest secret key from a secret key dictionary;

encrypting the original card number using the latest secret key;

combining the version of the latest secret key with a front end of a cipher text

obtained from the encryption to obtain a cipher text corresponding to the original card number;

using the allocated index card number, the cipher text corresponding to the original card number, the hash value corresponding to the original card number and the hash number corresponding to the hash value as a card number record corresponding to the original card number; and

storing the card number record in the database, wherein the index card number is determined to be successfully allocated to the original card number if no violation of a restriction on the hash value and the hash number exists when storing the card number record corresponding to the original card number in the database.

6. The method of claim 1, further comprising:

traversing card number records stored in the database;

obtaining a card number cipher text from a currently traversed card number record and intercepting a secret key version from the card number cipher text;

comparing the secret key version of the card number cipher text with a latest secret key version obtained from a secret key dictionary;

obtaining a secret key corresponding to the secret key version of the card number cipher text from the secret key dictionary and using the obtained secret key to decrypt the card number cipher text to obtain the original card number if the secret key version of the card number cipher text is not the latest secret key version;

obtaining a new secret key corresponding to the latest secret key version from the secret key dictionary, encrypting the original card number using the new secret key, and combining a cipher text obtained from the encryption with the latest secret key version to obtain an updated card number cipher text; and

updating a content in a field of the card number cipher text in the currently traversed card number record as an updated card number cipher text.

7. An apparatus comprising:

one or more processors;

memory;

a receiving module stored in the memory and executable by the one or more

processors to receive an original card number used for requesting to process a transaction;

a calculation module stored in the memory and executable by the one or more processors to calculate a hash value corresponding to the original card number based on the original card number received by the receiving module;

an acquisition module stored in the memory and executable by the one or more processors to obtain an index card number corresponding to the original card number based on the hash value corresponding to the original card number calculated by the calculation module, the acquisition module comprising:

a search sub-module to search a database for a stored card number record having the hash value;

a determination sub-module to set the original card number as a new card number when no card number record having the hash value is found in the database;

an allocation sub-module for allocating the index card number to the original card number after the determination sub-module sets the original card number as the new card number;

acquisition and decryption sub-modules to obtain card number records found by the search sub-module; and

a comparison sub-module to compare the respective original card number of each card number record obtained by the acquisition and decryption sub-modules with the received original card number, the acquisition sub-module further obtaining an index card number corresponding to the received original card number from a card number record having a corresponding card number that is identical to the received original card number; and

a sending module stored in the memory and executable by the one or more processors to send the index card number obtained by the acquisition module to an entity that processes the transaction to enable the entity to process the transaction based on the index card number.

8. The apparatus of claim 7, wherein

the allocation sub-module sets a hash number corresponding to the original card number to be a first value, after the determination sub-module sets the original card number as the new card number; and

the acquisition module comprises:

an encryption sub-module to obtain a latest secret key and a version of the latest secret key from a secret key dictionary, encrypt the original card number using the latest secret key, and combine the version of the latest secret key with a front end of a cipher text obtained from the encryption to obtain a cipher text corresponding to the original card number; and

a storage sub-module to use the index card number allocated by the allocation sub-module, the cipher text corresponding to the original card number obtained by the encryption sub-module, the hash value corresponding to the original card number and the hash number corresponding to the hash value as a card number record corresponding to the original card number, and to store the card number record in the database.

9. The apparatus of claim 8, wherein the determination sub-module further determines that the index card number is successfully allocated to the original card number when no violation of a restriction on the hash value and the hash number exists when the storage sub-module stores the card number record corresponding to the original card number in the database.

10. The apparatus of claim 9, wherein the acquisition sub-module obtains a respective card number cipher text in each card number record that is found by the search sub-module, intercepts a secret key version from the respective card number cipher text, reads a secret key dictionary based on the secret key version to obtain a secret key used for encrypting the respective card number cipher text; and

the decryption sub-module decrypts the respective card number cipher text using the secret key that is obtained by the acquisition sub-module to obtain a respective original card number from each card number record.

11. The apparatus of claim 10, wherein the acquisition module further comprises a setting sub-module, and wherein the determination sub-module sets the received original card number as a new card number when the comparison sub-module determines that no card number record having a card number that is identical to the received original card

number exists in the database, and the setting sub-module sets a hash number corresponding to the original card number to be a second value.

12. The apparatus of claim 7, wherein the acquisition module comprises:

a traversing sub-module to traverse card number records stored in a database;

the acquisition sub-module to obtain a respective card number cipher text from a currently traversed card number record and intercept a secret key version from the respective card number cipher text; and

the comparison sub-module to compare the secret key version obtained by the acquisition sub-module with a latest secret key version obtained from a secret key dictionary.

13. The apparatus of claim 12, wherein the acquisition sub-module further obtains a secret key corresponding to the secret key version in the card number cipher text from the secret key dictionary and obtains a new secret key corresponding to the latest secret key version from the secret key dictionary after the decryption sub-module obtains the original card number when the comparison sub-module determines that the secret key version obtained by the acquisition sub-module is not the latest secret key version.

14. The apparatus of claim 13, wherein:

the decryption sub-module decrypts the card number cipher text using the new secret key obtained by the acquisition sub-module to obtain the original card number; and the acquisition module further comprises;

an encryption sub-module to encrypt the original card number obtained by the decryption sub-module using the new secret key obtained by the acquisition sub-module, and to combine a cipher text obtained from the encryption with the latest secret key version to obtain an updated card number cipher text; and

an update sub-module to update content in a field of the card number cipher text in the currently traversed card number record as the updated card number cipher text obtained by the encryption sub-module.

15. One or more computer readable media storing executable instructions that, when executed by one or more processors, cause the one or more processors to perform acts comprising:

receiving an original card number for a request of processing a transaction;

calculating a hash value corresponding to the original card number based on the original card number; and

searching a database to determine whether a card number record having the hash value exists in the database and performing one of the following acts:

determining that a card number record having the hash value does not exist in the database, setting the original card number as a new card number, allocating an index card number to the original card number, and sending the index card number to an entity to process the transaction based on the index card number; and

determining that one or more card number records having the hash value exists in the database, obtaining an index card number corresponding to the received original card number from the card number record corresponding to the identical card number, and sending the index card number to an entity to process the transaction based on the index card number.

16. The one or more computer readable media of claim 15, wherein no card number record having the hash value exists in the database, and the acts further comprise:

setting a hash number corresponding to the original card number to be a first value,

obtaining a latest secret key and a version of the latest secret key from a secret key dictionary;

encrypting the original card number using the latest secret key, and combining the version of the latest secret key with a front end of a cipher text obtained from the encryption to obtain a cipher text corresponding to the original card number; and

using the allocated index card number, the cipher text corresponding to the original card number, the hash value corresponding to the original card number and the hash number corresponding to the hash value as a card number record corresponding to the original card number, and storing the card number record in the database, wherein the index card number is determined to be successfully allocated to the original card number if no

violation of a restriction on the hash value and the hash number exists when storing the card number record corresponding to the original card number in the database.

17. The one or more computer readable media of claim 15, wherein one or more card number records having the hash value exists in the database, and the acts further comprise:

acquiring a respective card number cipher text in each card number record of the one or more card number records;

intercepting a secret key version from the respective card number cipher text;

reading a secret key dictionary based at least in part on the secret key version to obtain a secret key used for encrypting the respective card number cipher text; and

using the secret key to decrypt the respective card number cipher text to obtain a respective original card number from each card number record; and

comparing the respective original card number of each card number record with the received original card number.