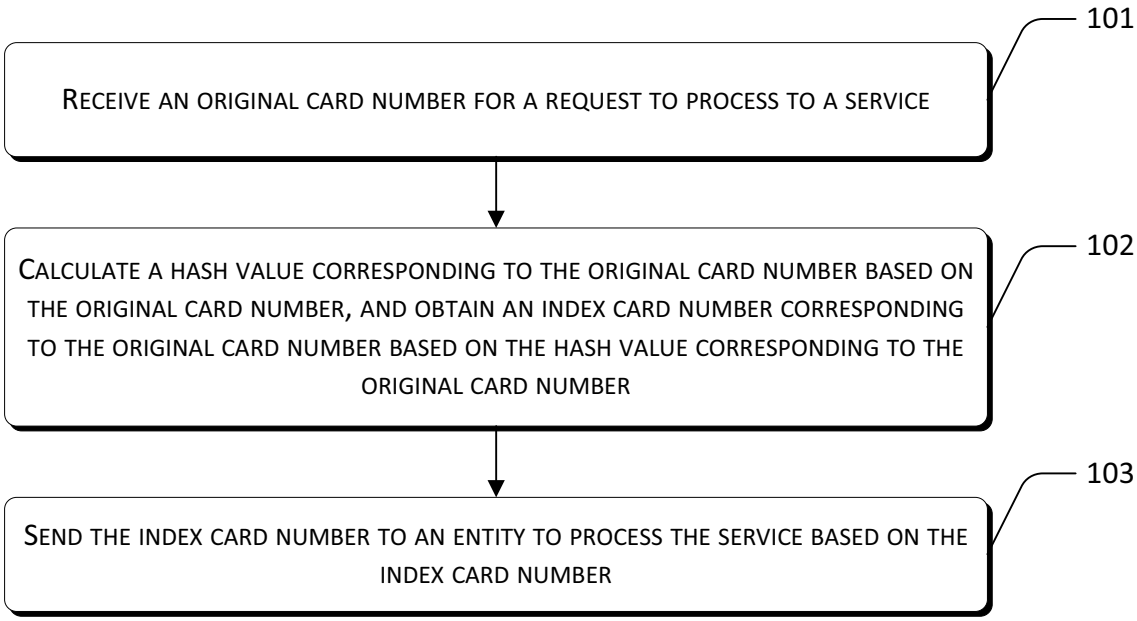

101
RECEIVE AN ORIGINAL CARD NUMBER FOR A REQUEST TO PROCESS TO A SERVICE
102
CALCULATE A HASH VALUE CORRESPONDING TO THE ORIGINAL CARD NUMBER BASED ON THE ORIGINAL CARD NUMBER, AND OBTAIN AN INDEX CARD NUMBER CORRESPONDING TO THE ORIGINAL CARD NUMBER BASED ON THE HASH VALUE CORRESPONDING TO THE ORIGINAL CARD NUMBER
103
SEND THE INDEX CARD NUMBER TO AN ENTITY TO PROCESS THE SERVICE BASED ON THE INDEX CARD NUMBER

FIG. 1

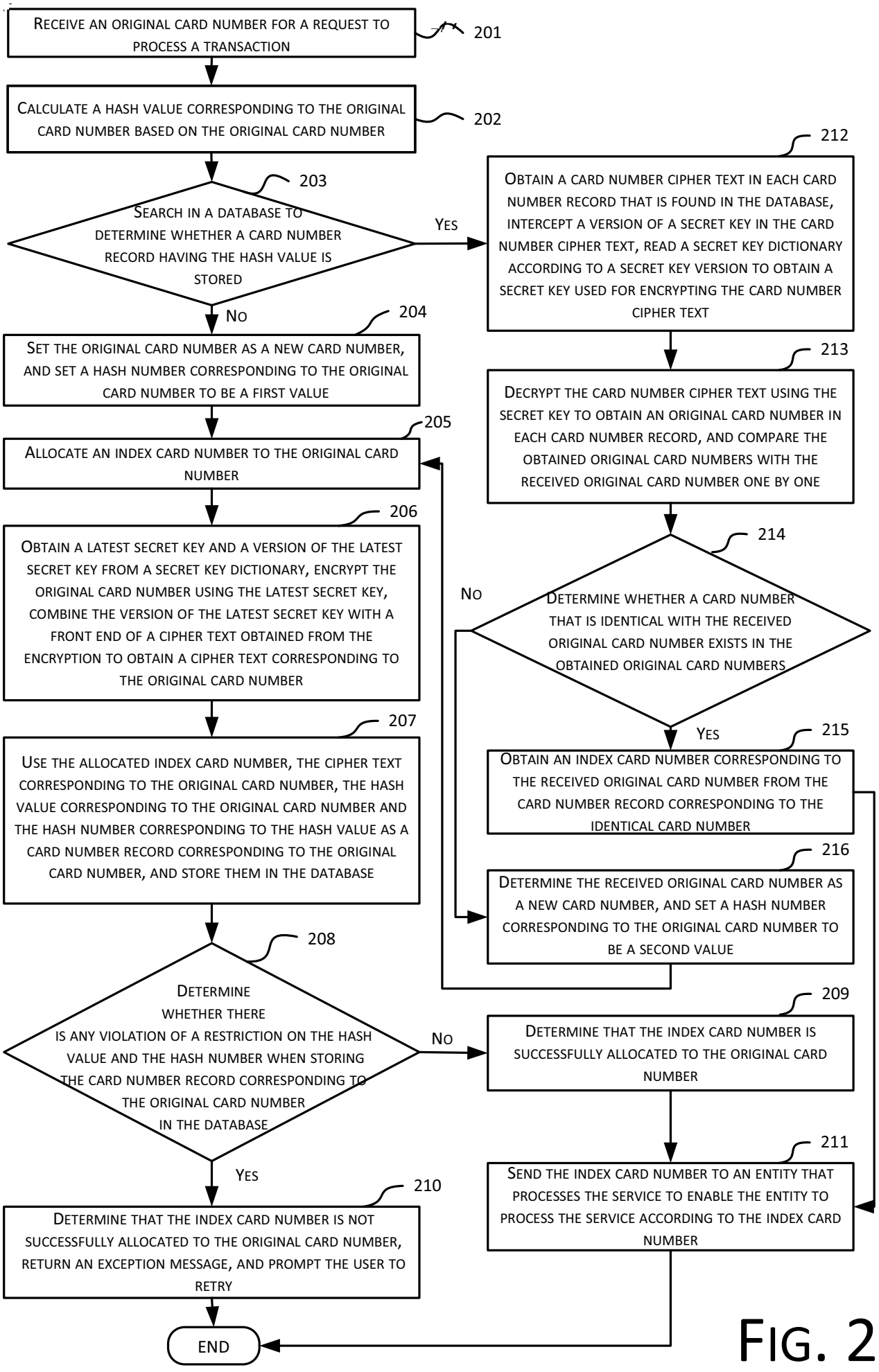

Receive an original card number for a request to process a transaction
201
Calculate a hash value corresponding to the original card number based on the original card number
202
203
Search in a database to determine whether a card number record having the hash value is stored
Yes
No
204
Set the original card number as a new card number, and set a hash number corresponding to the original card number to be a first value
205
Allocate an index card number to the original card number
206
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, 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
207
Use 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 store them in the database
208
Determine whether there is any violation of a restriction on the hash value and the hash number when storing the card number record corresponding to the original card number in the database
No
Yes
209
Determine that the index card number is successfully allocated to the original card number
210
Determine that the index card number is not successfully allocated to the original card number, return an exception message, and prompt the user to retry
211
Send the index card number to an entity that processes the service to enable the entity to process the service according to the index card number
212
Obtain a card number cipher text in each card number record that is found in the database, intercept a version of a secret key in the card number cipher text, read a secret key dictionary according to a secret key version to obtain a secret key used for encrypting the card number cipher text
213
Decrypt the card number cipher text using the secret key to obtain an original card number in each card number record, and compare the obtained original card numbers with the received original card number one by one
214
Determine whether a card number that is identical with the received original card number exists in the obtained original card numbers
No
Yes
215
Obtain an index card number corresponding to the received original card number from the card number record corresponding to the identical card number
216
Determine the received original card number as a new card number, and set a hash number corresponding to the original card number to be a second value
END

FIG. 2

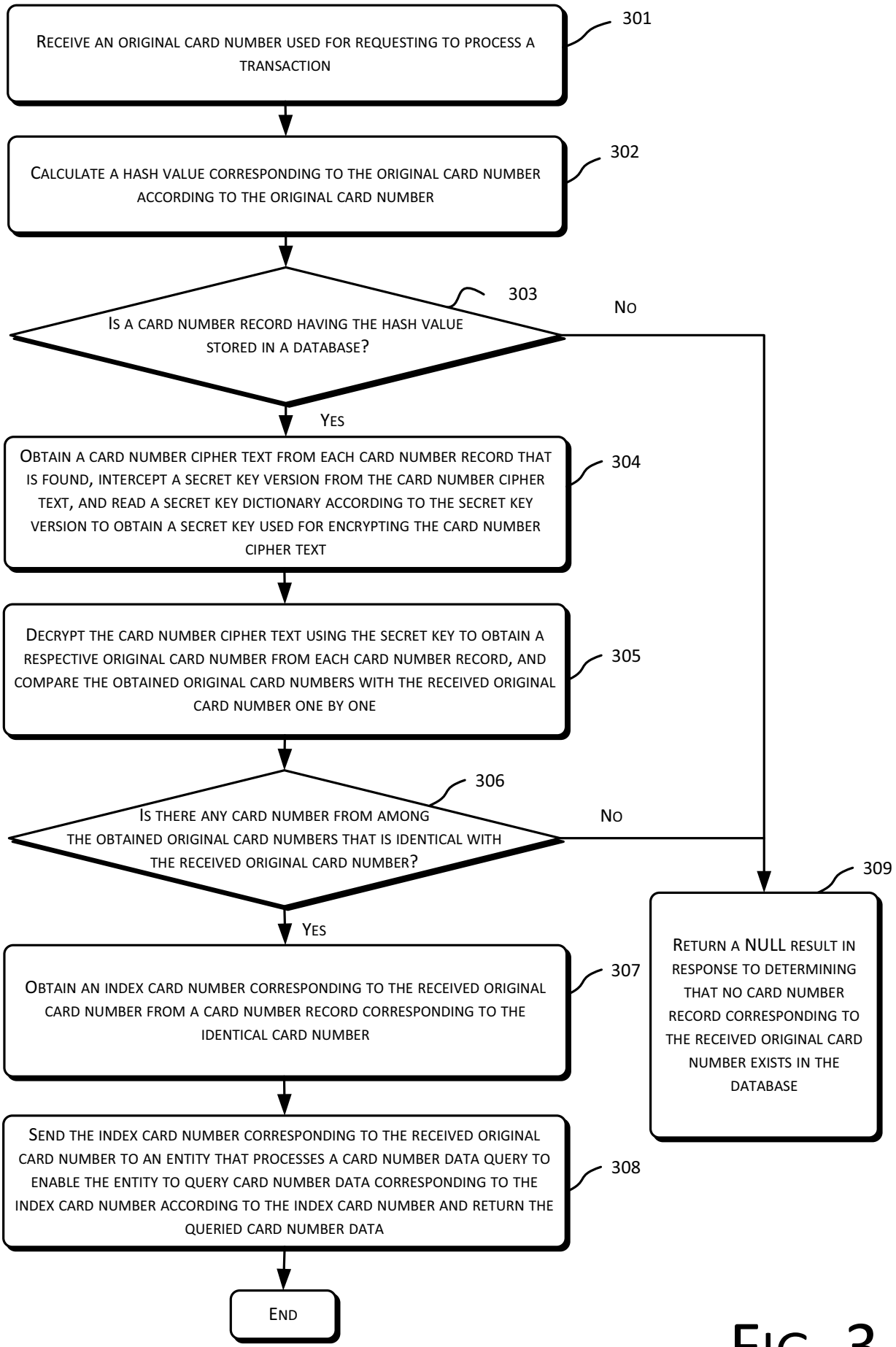

RECEIVE AN ORIGINAL CARD NUMBER USED FOR REQUESTING TO PROCESS A TRANSACTION
301
CALCULATE A HASH VALUE CORRESPONDING TO THE ORIGINAL CARD NUMBER ACCORDING TO THE ORIGINAL CARD NUMBER
302
IS A CARD NUMBER RECORD HAVING THE HASH VALUE STORED IN A DATABASE?
303
NO
YES
OBTAIN A CARD NUMBER CIPHER TEXT FROM EACH CARD NUMBER RECORD THAT IS FOUND, INTERCEPT A SECRET KEY VERSION FROM THE CARD NUMBER CIPHER TEXT, AND READ A SECRET KEY DICTIONARY ACCORDING TO THE SECRET KEY VERSION TO OBTAIN A SECRET KEY USED FOR ENCRYPTING THE CARD NUMBER CIPHER TEXT
304
DECRYPT THE CARD NUMBER CIPHER TEXT USING THE SECRET KEY TO OBTAIN A RESPECTIVE ORIGINAL CARD NUMBER FROM EACH CARD NUMBER RECORD, AND COMPARE THE OBTAINED ORIGINAL CARD NUMBERS WITH THE RECEIVED ORIGINAL CARD NUMBER ONE BY ONE
305
IS THERE ANY CARD NUMBER FROM AMONG THE OBTAINED ORIGINAL CARD NUMBERS THAT IS IDENTICAL WITH THE RECEIVED ORIGINAL CARD NUMBER?
306
NO
YES
OBTAIN AN INDEX CARD NUMBER CORRESPONDING TO THE RECEIVED ORIGINAL CARD NUMBER FROM A CARD NUMBER RECORD CORRESPONDING TO THE IDENTICAL CARD NUMBER
307
SEND THE INDEX CARD NUMBER CORRESPONDING TO THE RECEIVED ORIGINAL CARD NUMBER TO AN ENTITY THAT PROCESSES A CARD NUMBER DATA QUERY TO ENABLE THE ENTITY TO QUERY CARD NUMBER DATA CORRESPONDING TO THE INDEX CARD NUMBER ACCORDING TO THE INDEX CARD NUMBER AND RETURN THE QUERIED CARD NUMBER DATA
308
END
RETURN A NULL RESULT IN RESPONSE TO DETERMINING THAT NO CARD NUMBER RECORD CORRESPONDING TO THE RECEIVED ORIGINAL CARD NUMBER EXISTS IN THE DATABASE
309

FIG. 3

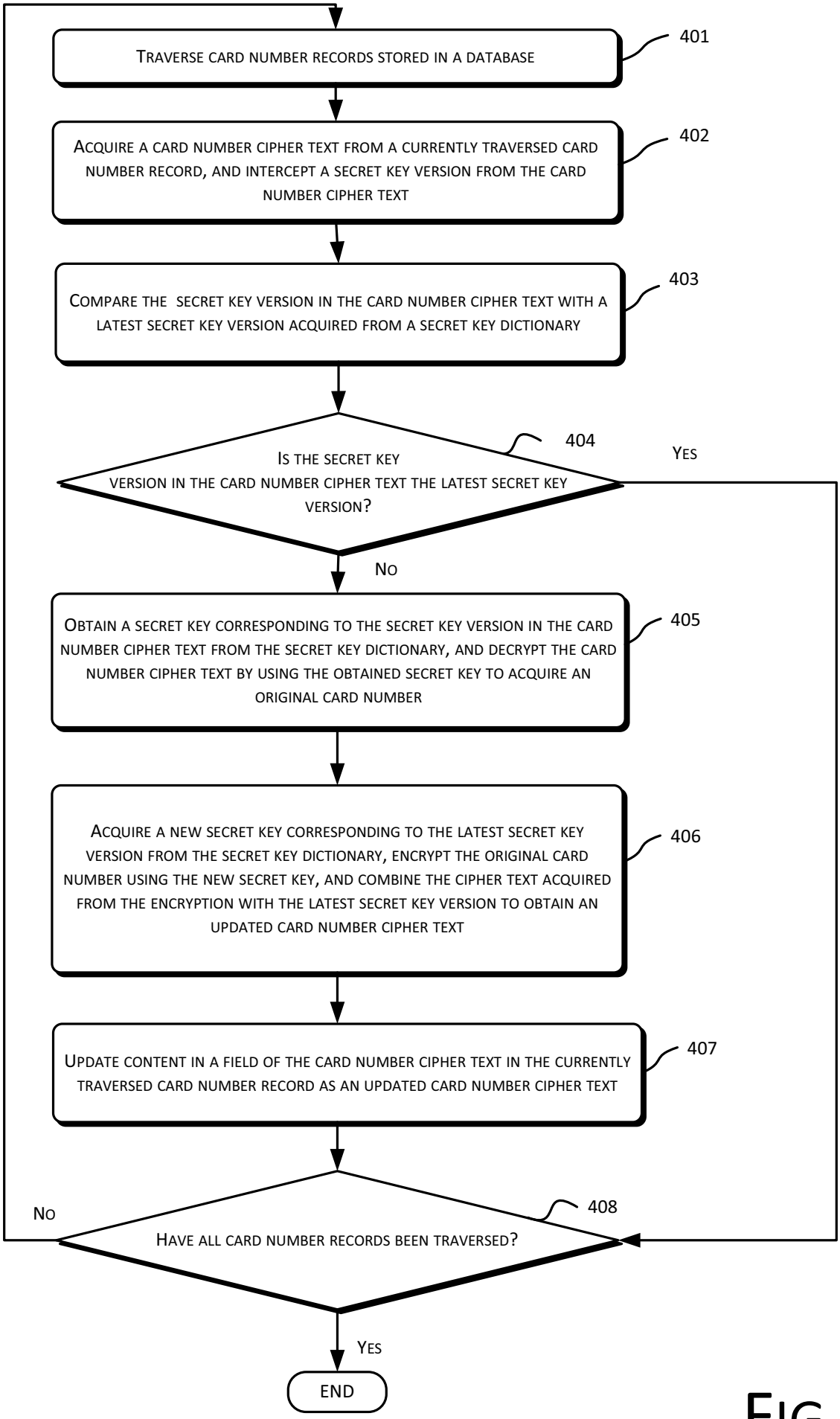

TRAVERSE CARD NUMBER RECORDS STORED IN A DATABASE
401
ACQUIRE A CARD NUMBER CIPHER TEXT FROM A CURRENTLY TRAVERSED CARD NUMBER RECORD, AND INTERCEPT A SECRET KEY VERSION FROM THE CARD NUMBER CIPHER TEXT
402
COMPARE THE SECRET KEY VERSION IN THE CARD NUMBER CIPHER TEXT WITH A LATEST SECRET KEY VERSION ACQUIRED FROM A SECRET KEY DICTIONARY
403
IS THE SECRET KEY VERSION IN THE CARD NUMBER CIPHER TEXT THE LATEST SECRET KEY VERSION?
404
YES
NO
OBTAIN A SECRET KEY CORRESPONDING TO THE SECRET KEY VERSION IN THE CARD NUMBER CIPHER TEXT FROM THE SECRET KEY DICTIONARY, AND DECRYPT THE CARD NUMBER CIPHER TEXT BY USING THE OBTAINED SECRET KEY TO ACQUIRE AN ORIGINAL CARD NUMBER
405
ACQUIRE A NEW SECRET KEY CORRESPONDING TO THE LATEST SECRET KEY VERSION FROM THE SECRET KEY DICTIONARY, ENCRYPT THE ORIGINAL CARD NUMBER USING THE NEW SECRET KEY, AND COMBINE THE CIPHER TEXT ACQUIRED FROM THE ENCRYPTION WITH THE LATEST SECRET KEY VERSION TO OBTAIN AN UPDATED CARD NUMBER CIPHER TEXT
406
UPDATE CONTENT IN A FIELD OF THE CARD NUMBER CIPHER TEXT IN THE CURRENTLY TRAVERSED CARD NUMBER RECORD AS AN UPDATED CARD NUMBER CIPHER TEXT
407
NO
HAVE ALL CARD NUMBER RECORDS BEEN TRAVERSED?
408
YES
END

FIG. 4


500
Receiving module 51
Calculation module 52
Acquisition module 53
Sending module 54

FIG. 5

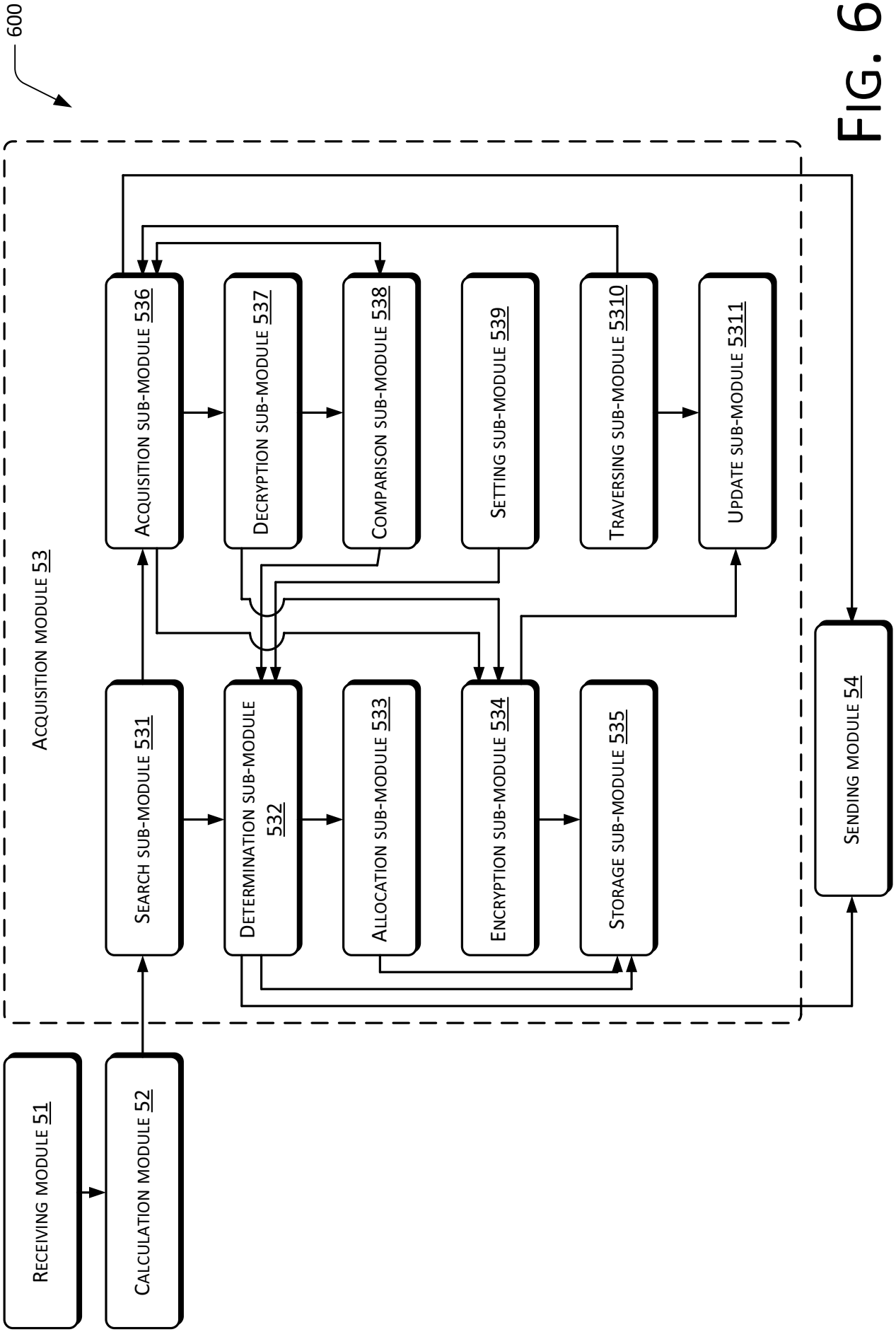

600
Receiving module 51
Calculation module 52
Acquisition module 53
Search sub-module 531
Determination sub-module 532
Allocation sub-module 533
Encryption sub-module 534
Storage sub-module 535
Acquisition sub-module 536
Decryption sub-module 537
Comparison sub-module 538
Setting sub-module 539
Traversing sub-module 5310
Update sub-module 5311
Sending module 54

FIG. 6

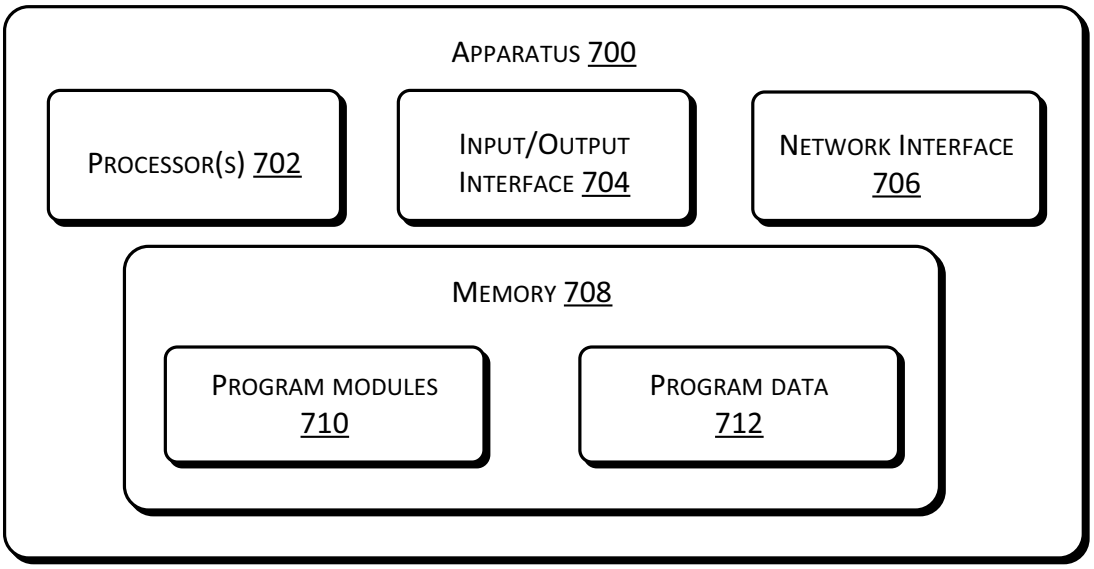

APPARATUS 700
PROCESSOR(S) 702
INPUT/OUTPUT INTERFACE 704
NETWORK INTERFACE 706
MEMORY 708
PROGRAM MODULES 710
PROGRAM DATA 712

FIG. 7