



(12) **DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION**

(13) **A1**

(86) Date de dépôt PCT/PCT Filing Date: 2019/03/29
(87) Date publication PCT/PCT Publication Date: 2019/06/27
(85) Entrée phase nationale/National Entry: 2019/09/27
(86) N° demande PCT/PCT Application No.: CN 2019/080372
(87) N° publication PCT/PCT Publication No.: 2019/120322

(51) Cl.Int./Int.Cl. *H04L 9/14* (2006.01),
G06F 21/32 (2013.01), *G06F 21/62* (2013.01),
H04L 9/06 (2006.01), *H04L 9/32* (2006.01)
(71) Demandeur/Applicant:
ALIBABA GROUP HOLDING LIMITED, KY
(72) Inventeurs/Inventors:
FENG, ZHIYUAN, CN;
LI, YANPENG, CN;
CHENG, LONG, CN
(74) Agent: KIRBY EADES GALE BAKER

(54) Titre : GESTION DE CLES CRYPTOGRAPHIQUES A PARTIR D'INFORMATIONS D'IDENTITE
(54) Title: MANAGING CRYPTOGRAPHIC KEYS BASED ON IDENTITY INFORMATION

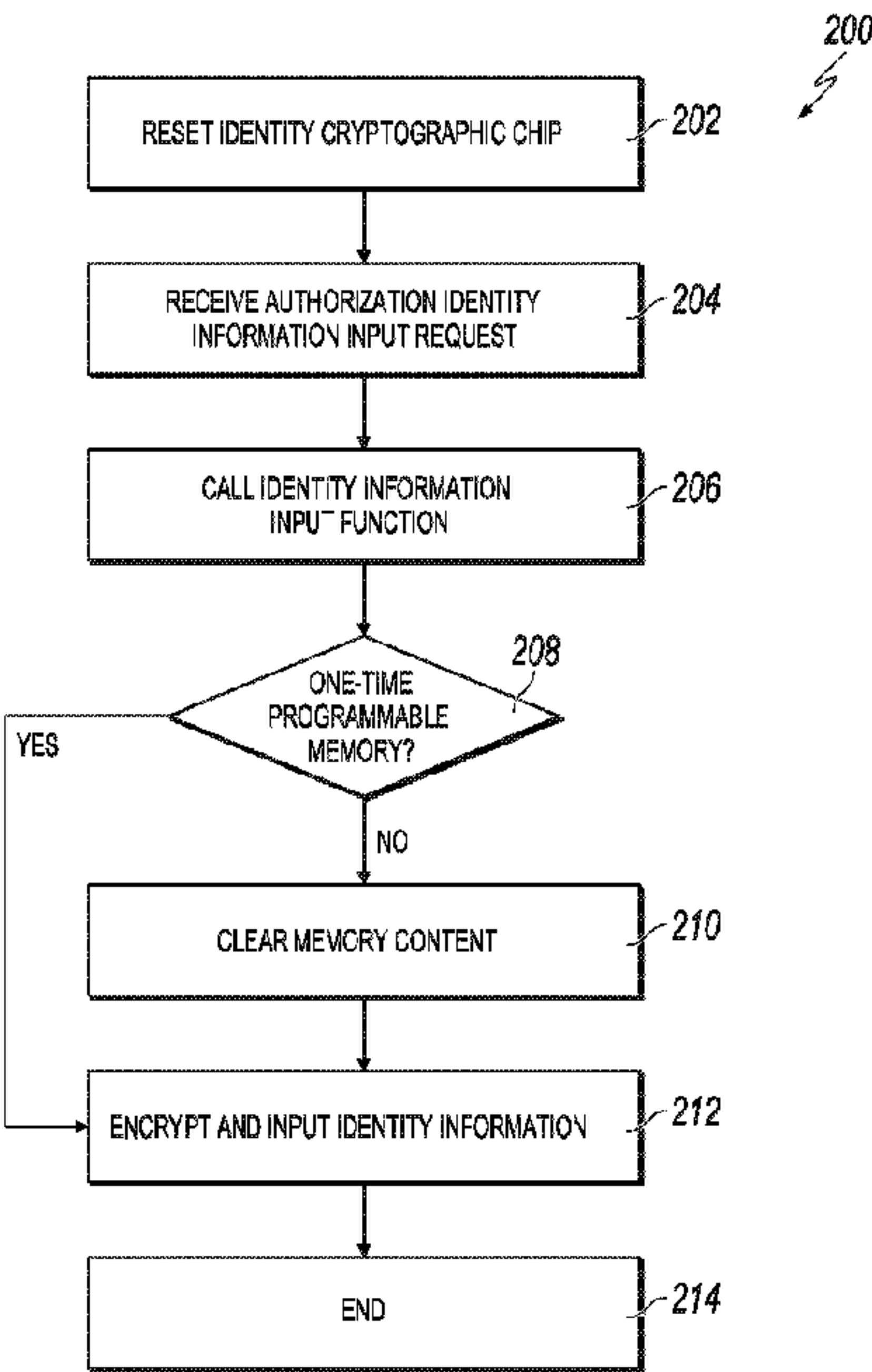


FIG. 2

(57) **Abrégé/Abstract:**

Disclosed herein are methods, systems, and apparatus, including computer programs encoded on computer storage media, for managing cryptographic keys based on user identity information. One of the methods includes receiving biometric information associated with a user and a request to store a user key pair to a memory on an identity cryptographic chip (ICC); comparing the biometric information associated with the user with biometric information pre-stored in the memory as pre-stored biometric information; in response to determining that the biometric information associated with the user matches the pre-stored biometric information, encrypting the user key pair to provide an encrypted user key pair; and storing the encrypted user key pair to the memory.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
27 June 2019 (27.06.2019)



(10) International Publication Number
WO 2019/120322 A2

(51) International Patent Classification:
Not classified

(21) International Application Number:
PCT/CN2019/080372

(22) International Filing Date:
29 March 2019 (29.03.2019)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **ALIBABA GROUP HOLDING LIMITED**
[—/CN]; Fourth Floor, One Capital Place, P.O. BOX 847,
George Town, Grand Cayman (KY).

(72) Inventors: **FENG, Zhiyuan**; Alibaba Group Legal Department 5/F, Building 3, No.969 West Wen Yi Road, Yu Hang District, Hangzhou, Zhejiang 311121 (CN). **LI, Yanpeng**; Alibaba Group Legal Department 5/F, Building 3, No.969 West Wen Yi Road, Yu Hang District, Hangzhou, Zhejiang 311121 (CN). **CHENG, Long**; Alibaba Group Legal Department 5/F, Building 3, No.969 West Wen Yi Road, Yu Hang District, Hangzhou, Zhejiang 311121 (CN).

(74) Agent: **BEIJING BESTIPR INTELLECTUAL PROPERTY LAW CORPORATION**; Room 409, Tower B, Ka

Wah Building, No. 9 Shangdi 3rd Street, Haidian District, Beijing 100085 (CN).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

(54) Title: MANAGING CRYPTOGRAPHIC KEYS BASED ON IDENTITY INFORMATION

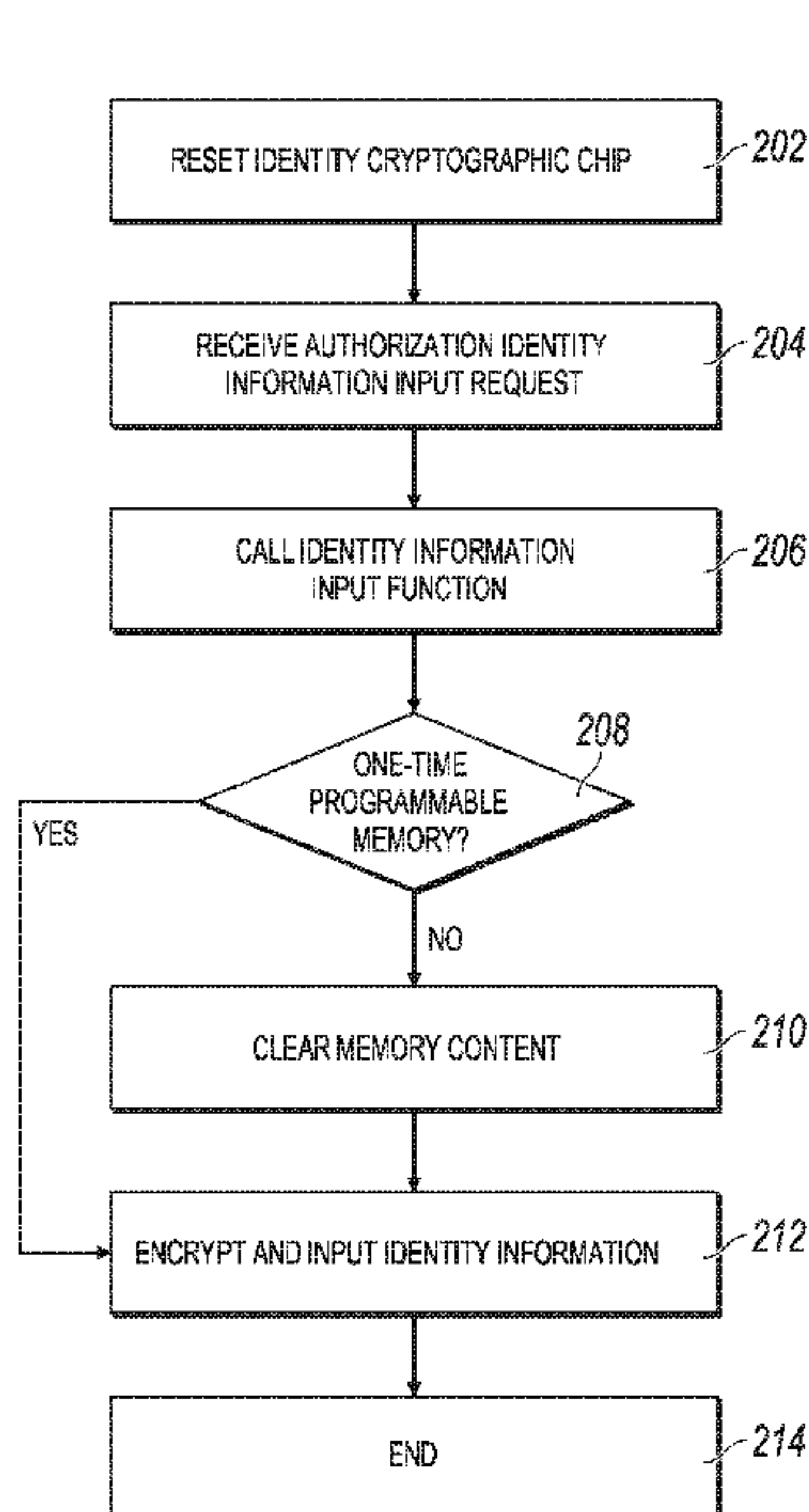


FIG. 2

(57) Abstract: Disclosed herein are methods, systems, and apparatus, including computer programs encoded on computer storage media, for managing cryptographic keys based on user identity information. One of the methods includes receiving biometric information associated with a user and a request to store a user key pair to a memory on an identity cryptographic chip (ICC); comparing the biometric information associated with the user with biometric information pre-stored in the memory as pre-stored biometric information; in response to determining that the biometric information associated with the user matches the pre-stored biometric information, encrypting the user key pair to provide an encrypted user key pair; and storing the encrypted user key pair to the memory.

WO 2019/120322 A2

WO 2019/120322 A2 |

Published:

- *upon request of the applicant, before the expiration of the time limit referred to in Article 21(2)(a)*
- *without international search report and to be republished upon receipt of that report (Rule 48.2(g))*

MANAGING CRYPTOGRAPHIC KEYS BASED ON IDENTITY INFORMATION

TECHNICAL FIELD

[0001] This specification relates to identity authentication technology and data security.

BACKGROUND

[0002] Identity authentication technology is commonly used in computer networks to verify user identity and ensure data security. Identity information, as other information digitally stored or communicated in the computer networks, can be represented by a set of data. Computers can identify and authenticate a user based on a digital identity of the user. For data security, it is important to ensure that a digital identity belongs to an authorized user, or in other words, the digital identity matches the actual identity.

[0003] As technology has evolved, decentralized systems, such as blockchain networks and Internet of things (IoT) networks have emerged. Under decentralized systems, it is possible for individuals to safely self-store their own identity information. For example, a user can hold a digital wallet, which stores a private key that the user can use to add a digital signature to authorize transactions in a blockchain network or on IoT devices. The private key is normally stored as a data string with cryptographic semantics on a computing device and is intended to be only accessible to the user. As other data strings, the private key can potentially be copied and shared. Any users who have the private key can control digital assets associated with the private key. Moreover, the digital assets cannot be retrieved if the private key is lost. Therefore, secure storage and efficient use of cryptographic keys can be important.

[0004] It would be desirable to develop a key management technology that can safely manage cryptographic keys based on the true identity of a user.

SUMMARY

[0005] This specification describes technologies for managing cryptographic keys based on user identity information. These technologies generally involve receiving, by an identity cryptographic chip (ICC), biometric information and a request for storing a user key pair to a memory on the ICC, determining that the biometric information matches biometric

information pre-stored on the chip, and encrypting and storing the user key pair to the memory on the ICC.

[0006] This specification also provides one or more non-transitory computer-readable storage media coupled to one or more processors and having instructions stored thereon which, when executed by the one or more processors, cause the one or more processors to perform operations in accordance with embodiments of the methods provided herein.

[0007] This specification further provides a system for implementing the methods provided herein. The system includes one or more processors, and a computer-readable storage medium coupled to the one or more processors having instructions stored thereon which, when executed by the one or more processors, cause the one or more processors to perform operations in accordance with embodiments of the methods provided herein.

[0008] It is appreciated that methods in accordance with this specification may include any combination of the aspects and features described herein. That is, methods in accordance with this specification are not limited to the combinations of aspects and features specifically described herein, but also include any combination of the aspects and features provided.

[0009] The details of one or more embodiments of this specification are set forth in the accompanying drawings and the description below. Other features and advantages of this specification will be apparent from the description and drawings, and from the claims.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] FIG. 1 is a diagram illustrating an example of an identity cryptographic chip for performing processes that can be used to execute embodiments of this specification.

[0011] FIG. 2 is a flowchart illustrating an example of a process for identity cryptographic chip initialization in accordance with embodiments of this specification.

[0012] FIG. 3 is a flowchart illustrating an example of a process for information input to an identity cryptographic chip in accordance with embodiments of this specification.

[0013] FIG. 4 is a flowchart illustrating an example of a process for performing a cryptographic operation using an identity cryptographic chip in accordance with embodiments of this specification.

[0014] FIG. 5 is a diagram illustrating an example of a key management device in accordance with embodiments of this specification.

[0015] FIG. 6 depicts an example of a method that can be executed in accordance with embodiments of this specification.

[0016] FIG. 7 depicts examples of modules of an apparatus in accordance with embodiments of this specification.

[0017] Like reference numbers and designations in the various drawings indicate like elements.

DETAILED DESCRIPTION

[0018] This specification describes technologies for managing cryptographic keys based on user identity information. These technologies generally involve receiving, by an identity cryptographic chip (ICC), biometric information and a request for storing a user key pair to a memory on the ICC, determining that the biometric information matches biometric information pre-stored on the chip, and encrypting and storing the user key pair to the memory on the ICC.

[0019] FIG. 1 is a diagram illustrating an example of an ICC 100 for performing processes that can be used to execute embodiments of this specification. At a high-level, the ICC 100 can be a computer chip that includes a memory 102 and a logic computing component 104. The ICC 100 can be used for securely performing cryptographic operations. In some embodiments, the ICC 100 can be a chip set that includes one or more chip components. The memory 102 and the logic computing component 104 can be integrated to different chip components. In some embodiments, the memory 102 can be used to provide permanent storage. In some examples, the memory 102 can be a programmable read-only memory (PROM) that allows to be written once and is read-only afterwards. In some examples, the memory 102 can be an electrically erasable programmable read-only memory (EEPROM) or a Flash memory which can be reformatted and reprogrammed. In some embodiments, the logic computing component can be an application specific integrated circuit (ASIC) or a single chip microcomputer (SCM).

[0020] In some computer networks, cryptography is implemented to maintain privacy of data or transactions. For example, in a blockchain network, if two nodes want to keep a transaction private, such that other nodes in the blockchain network cannot discern details of the transaction, the nodes can encrypt the transaction data. Example cryptographic operations include, without limitation, symmetric key encryption and asymmetric key encryption.

Symmetric encryption refers to an encryption process that uses a single key for both encryption (generating ciphertext from plaintext), and decryption (generating plaintext from ciphertext).

[0021] Asymmetric encryption uses key pairs that each include a private key, and a public key, the private key being known only to a respective user, and the public key that can be disseminated openly. A user can use the public key of another user to encrypt data, and the encrypted data can be decrypted using the private key of the another user.

[0022] Asymmetric encryption can be used to provide digital signatures, which enables users in a transaction to confirm other users in the transaction, as well as the validity of the transaction. For example, a user can digitally sign a message, and another user can confirm that the message was sent by the user based on the digital signature. Digital signatures can also be used to ensure that messages are not tampered with in transit. For example, user A is to send a message to user B. User A generates a hash of the message, and then, using its private key, encrypts the hash to provide a digital signature as the encrypted hash. User A appends the digital signature to the message, and sends the message with digital signature to user B. User B decrypts the digital signature using the public key of user A, and extracts the hash. User B hashes the message and compares the hashes. If the hashes are same, user B can confirm that the message was indeed from user A, and was not tampered with.

[0023] The ICC 100 can be used for securely performing cryptographic operations based on verifying user identity information. The memory 102 can be used to store trusted user identity information and cryptographic key information. The memory 102 can also store identity authentication algorithms (e.g., as computer-executable code) and cryptographic operation algorithms (e.g., as computer-executable code). In some embodiments, information and algorithms stored in the memory 102 are encrypted to prevent leakage thereof, even when the ICC 100 is reverse engineered. When a request for performing a cryptographic operation is received from a user, the logic computing component 104 can use identity information collected from the user and the trusted user identity information stored in memory 102 to verify the identity of the user based on the identity authentication algorithm. For example, if the identity information is a fingerprint image of a fingerprint of the user, the identity authentication algorithm can be a local authentication algorithm that compares the fingerprint image collected from the user and a stored fingerprint image. If the

collected fingerprint image matches the stored fingerprint image, the identity of the user is successfully verified. The logic computing component 104 can then use the stored cryptographic key information to perform the requested cryptographic operation. After the cryptographic operation is performed, the operation result can be output by the ICC 100. By using the ICC 100, cryptographic operations can be performed only after an identity of a user is verified or authenticated. As such, the authority of the user to perform the operations can be guaranteed. Moreover, since the cryptographic keys are stored in the ICC 100 as ciphertext, the cryptographic operations are performed inside the ICC 100. Only the operation result is output from the ICC 100. In this manner, security of the cryptographic keys can be ensured.

[0024] At 110, an authorization identity information is input to the ICC 100. The authorization identity information can be input to the ICC 100 during the initialization of the ICC 100. In some embodiments, the authorization identity information can be biometric information of the user, such as fingerprint, voiceprint, heartbeat information, or iris information. In some embodiments, the authorization identity information can be input by the owner of the ICC 100. As will be further discussed in the embodiments of the specification, the user who input the authorization identity information can use it to control cryptographic key input to the ICC 100. Cryptographic keys cannot be input to the ICC 100 unless user identity can be verified based on the authorization identity information.

[0025] The authorization identity information can be used for performing identity verification, so as to provide authorization for storing cryptographic keys or performing cryptographic operations. The identity information can be collected by a computing device communicably coupled with the ICC 100. For example, the computing device can be a smart watch that can detect biometric information of the user.

[0026] At 112, the memory content is cleared and the authorization identity information is written to the memory 102. In some embodiments, the memory 102 is a permanent storage memory. In some embodiments, to prevent from tampering, the identity information can only be written to a storage unit of the memory 102 once. If new identity information needs to be used to replace the existing authorization key, the content of the memory 102 may be erased before the new identity information can be written. In some embodiments, the

authorization identity information can be encrypted before writing to the memory 102 to enhance security.

[0027] At 114, identity information of the user and a request for writing the asymmetric key pair of the user are received. The asymmetric key pair can be used for performing cryptographic operations to the memory 102, as described herein. It is to be understood that other cryptographic keys can also be requested to be written to the ICC 100 based on specific cryptographic operations. The identity information can be biometric information, such as fingerprint, voiceprint, heartbeat information, or iris information. The identity information can be collected by a computing device communicably coupled with the ICC 100. At 116, the authorization identity information is read from the memory 102 to verify the identity of the user at 118. The verification can be performed based on matching the identity information of the user received at 114 with the authorization identity information. If the identity information matches, the verification is successful. As a result, the user is authenticated as the authorized user of the ICC 100 to allow the asymmetric key pair to be input to the ICC 100. Otherwise, the request at 114 is rejected. At 122, the asymmetric key pair is written to the memory 102 of the ICC 100. In some embodiments, the asymmetric key pair can be encrypted before writing to the memory 102 to enhance security. In some embodiments, the asymmetric key pair can be written to a storage unit of the memory 102 separate from the storage unit storing the authorization identity information.

[0028] At 124, identity information of a user and a request for performing a cryptographic operation are received. The identity information can be collected by a computing device communicably coupled with the ICC 100. For example, the computing device can be a smart watch that can collect biometric information of the user, the biometric information being used as identity information to identify the user. After the identity information is collected, it can be sent to the ICC 100. In some embodiments, the data that the cryptographic operation is to be performed on can also be sent to the ICC 100. For example, if the cryptographic operation is encryption, the corresponding data can be a data file to be encrypted. At 126, the authorization identity information written to the memory 102 at 122 is read from the memory 102 to perform identity verification at 128. The identity verification can be performed based on comparing the identity information received at 124 with the authorization identity information. If the identity information matches, the

verification is successful and the corresponding asymmetric key information is read from the memory 102 at 130 to perform the cryptographic operation. At 132, the cryptographic operation is performed using the suitable cryptographic key. If the identity information does not match, the verification is unsuccessful, and the request for performing the cryptographic operation can be declined. In some embodiments, the identity verification at 128 can be performed using an identity verification algorithm based on the particular type of identity information received. In some embodiments, the cryptographic operation can be performed based on a cryptographic operation algorithm. As described above, the cryptographic operation can be encryption, decryption, and/or adding digital signature to the data. After performing the cryptographic operation, the operation result can be output at 134.

[0029] As described above, the ICC 100 can create a trusted environment within a hardware for the user to securely store cryptographic keys and use the keys to perform cryptographic operations. For example, an ICC 100 user can store multiple asymmetric key pairs to the ICC 100. Each asymmetric key pair is written to the memory of the ICC 100 after the identity of the user is verified through identity information (e.g., biometric authentication). The identity authentication can be performed based on comparing the identity information collected from the user with identity information pre-stored during initialization of the ICC 100. If the identity information matches, the corresponding identity information and asymmetric key pair can be allowed store in the ICC 100.

[0030] When a cryptographic operation is requested by a user, the ICC 100 can retrieve biometric information and the corresponding asymmetric key pair from the memory. The biometric information can be used to verify the identity of the user, and the asymmetric key pair can be used to perform the requested cryptographic operation after the identity of the user is verified. The cryptographic operation can be performed for various practical scenarios. For example, the cryptographic operation can be an operation to add a digital signature to a blockchain transaction. In this example, a node A can be a computing device within a blockchain network that initiates a request to digitally sign blockchain transaction data with a node B. The blockchain transaction data can be a hashed value of the transaction data between the node A and the node B. The node A can use the ICC 100 to generate the digital signature to the hashed transaction data. To use the ICC 100, identity information provided from the node A is collected and compared with the identity information stored in

the ICC 100. If the collected identity information matches the stored identity information, the node A can be determined as authorized to access and use the ICC 100. A private key assigned to node A and previously stored in the memory of the ICC 100 can be retrieved to generate digital signature to the hashed transaction data. The node A can then send hashed transaction data with digital signature to the node B. The node B decrypts the digital signature using the public key assigned to the node A and extracts the hash. The node B hashes the message and compares the hashes. If the hashes are same, the node B can confirm that the message was indeed from the node A and was not tampered with.

[0031] FIG. 2 is a flowchart illustrating an example of a process 200 for ICC initialization in accordance with embodiments of this specification. In some embodiments, the ICC is initialized by the user of the ICC. In some embodiments, the user can control the cryptographic keys to be stored and used in the ICC to securely perform cryptographic operations.

[0032] At 202, the ICC is reset. In some embodiments, the ICC is reset in response to receiving a request to input authorization identity information. In some embodiments, resetting the ICC can include erasing or reformatting content stored in the memory of the ICC. In some embodiments, resetting the ICC can also include reconfigure or reset settings of the logic computing component of the ICC to default. By resetting the ICC, it can be guaranteed that one authorization identity information is used to control information input to the ICC. Moreover, cryptographic keys previously stored in the ICC are erased to ensure data security. In some embodiments, the ICC is a new ICC and is used for the first time, the ICC can be initialized to accept input of authorization identity information. If the ICC is new, the ICC can be initialized to accept authorization identity information. In some embodiments, the authorization identity information can be biometric information, such as fingerprint, voice print, iris information, and heartbeat information.

[0033] At 204, a request to input identity information input is received by the ICC. At 206, an identity information input function is called to input the authorization identity information to the memory 202. At 208, whether the memory of the ICC is a one-time programmable (OTP) memory is determined. The OTP memory permits data to be written to the memory only once. When a user inputs new authorization identity information to the ICC, any previously stored identity information and cryptographic keys can be erased to

ensure that the new authorization identity does not control cryptographic keys that had been previously entered. Therefore, if the memory is OTP, the authorization identity information can be encrypted and input to the memory at 212. Otherwise, the content of the memory is cleared at 210 before the authorization identity information is encrypted and input to the memory. After 212, the process 200 ends at 214.

[0034] FIG. 3 is a flowchart illustrating an example of a process 300 for information input to an ICC in accordance with embodiments of this specification. After the ICC is initialized, a user can securely store cryptographic keys to the ICC based on verifying its identity information.

[0035] At 302, a request for storing an asymmetric key pair is received by the ICC. At 304, identity information of the user who made the request is received. In some embodiments, the identity information can be collected by a computing device communicably coupled with the ICC. Example computing devices can include, an IoT device, a smart band, a smart watch, a laptop (or a desktop computer), and a smartphone. In some embodiments, the identity information can be biometric information of the user, such as fingerprint, voiceprint, heartbeat information, and iris information. The computing device can include a fingerprint sensor, microphone, heartbeat sensor, or iris scanner to collect the corresponding biometric information. For example, the computing device can be a smart watch that can collect heartbeat information of the user, which can be used as identity information. After the identity information is collected, it can be sent with the asymmetric key pair of the user to the ICC. In some embodiments, the ICC can communicate with the computing device wirelessly based on a wireless communication protocol, such as Bluetooth, NFC, Wi-Fi, or cellular data. In some embodiments, the ICC can be inserted or integrated to the computing device to perform wired communication with the computing device.

[0036] At 306, the identity information is verified based on authorization identity information pre-stored in the ICC. If the received identity information matches the authorization identity information, the asymmetric key pair is encrypted and stored to the memory of the ICC at 308. Afterwards, the process 300 ends at 310. If the received identity information does not match the authorization identity information, the request for storing the asymmetric key pair is declined, and the process 300 ends at 310. In some embodiments, the process 300 can be repeated so that the authorized user can stored a plurality of

cryptographic keys to the ICC corresponding to different user accounts or applications. After the user's cryptographic keys are input to the ICC, the user can use the ICC to securely perform cryptographic operations.

[0037] FIG. 4 is a flowchart illustrating an example of a process 400 for performing a cryptographic operation using an ICC in accordance with embodiments of this specification. At 402, a request for performing a cryptographic operation is received. Examples of cryptographic operations can include data encryption, decryption, and adding digital signature.

[0038] At 404, identity information of a user is received. As discussed in the description of FIG. 3, the identity information can be collected by a computing device and sent to the ICC. At 406, the identity information can be verified. In some embodiments, the identity information can be compared with the identity information stored in the memory of the ICC. If the identity information matches the stored identity information, the verification is successful, the requested cryptographic operation can then be performed at 408 using the user's cryptographic key stored in the memory of the ICC. For example, if the cryptographic key is an asymmetric key pair, the cryptographic operation can be an encryption operation based on the public key of the asymmetric key pair, a decryption operation or a digital signature generation operation based on the private key of the asymmetric key pair. If the identity information does not match the stored identity information, the process 400 ends at 412. After 408, the process 400 proceeds to 410 where the operation result is returned. The operation result can depend on the cryptographic operation performed at 408. For example, if the cryptographic operation is file encryption, a file encrypted using the public key of the user can be returned. Similarly, if the cryptographic operation is file decryption, a file decrypted using the private key of the user can be returned. If the cryptographic operation is adding digital signature, a file with a digital signature generated by the private key of the user can be returned. After 410, the process ends at 412.

[0039] FIG. 5 is a diagram illustrating an example of a key management device 500 in accordance with embodiments of this specification. In some embodiments, the cryptographic keys used by the ICC to perform cryptographic operations for the users can be managed by a key management device 500. The key management device 500 can perform key management 504 and algorithm management 514. Key management 504 can include store

506, write 508, randomly generate 510, and delete 512 of cryptographic keys. The cryptographic keys can include the user key pair associated with the master user and the cryptographic key pairs associated with authorized users of an ICC to perform cryptographic operations.

[0040] The algorithms managed by the algorithm management 514 can include storing and managing identity verification algorithm 516, digital signature verification algorithm 518, encrypt and decrypt algorithm 520, and token algorithm 522. The identity verification algorithm 516 can be used to perform the identity verification as discussed in the description of step 406 of FIG. 4. The digital signature verification algorithm 518 can be used to perform digital signature verification. The encrypt and decrypt algorithm 520 can be used to perform the requested cryptographic operation as discussed in step 408 of FIG. 4. For example, if the requested cryptographic operation is an encryption operation of a user file, the encrypt and decrypt algorithm 520 can be performed to retrieve the public key of the user from the memory of the ICC and encrypt the user file. The token algorithm 522 can be used to manage a token indicative of a time limit or a quantity limit of performing requested cryptographic operations without needing to verify user identity. In some embodiments, a token can be generated and temporarily stored in the memory of the ICC. The token can provide authorizations for performing cryptographic operations for a number of times or in a predetermined time period without needing to verify user identity. For example, a token can be generated to provide authorizations to a user of the ICC for adding digital signatures to the next five files received or within the next three hours, whichever condition is met first. In some embodiments, the token can be cleared and removed from the ICC when it is expired or runs out.

[0041] In some embodiments, the key management device 500 can serve as backup of the ICC. Even if the ICC is lost or destroyed, the cryptographic keys and algorithms for performing cryptographic operations can be retrieved from the key management device 500.

[0042] In some embodiments, the key management device 500 can also perform input management 524. The key management device 500 can be communicably coupled to the ICC to manage algorithm input 526, identity information input 528, cryptographic key input 530, digital signature generation 532, and identity verification 534.

[0043] FIG. 6 depicts an example of a method 600 that can be executed in accordance with embodiments of this specification. For clarity of presentation, the description that follows generally describes method 600 in the context of the other figures in this description. However, it will be understood that method 600 can be performed, for example, by any system, environment, software, and hardware, or a combination of systems, environments, software, and hardware, as appropriate. In some embodiments, various steps of method 600 can be run in parallel, in combination, in loops, or in any order. In some embodiments, the method 600 can be performed by an ICC described in accordance with embodiments of this specification.

[0044] At 602, biometric information associated with a user and a request to store a user key pair to a memory on an ICC. In some embodiments, the pre-stored biometric information is stored in the memory during initialization of the ICC. The public authorization key and the private authorization key are an asymmetric-key pair assigned to a master user of the ICC. In some embodiments, initialization of the ICC comprises: storing identity authentication code executable to authenticate the user based on the pre-stored biometric information. In some embodiments, initialization of the ICC further comprises: storing first cryptographic operation code executable to add a digital signature based on the user key pair; and storing second cryptographic operation code executable to perform file encryption or file decryption based on the user key pair.

[0045] In some embodiments, the request to store the user key pair is a first request, the biometric information is first biometric information, and wherein the method 600 further comprises: receiving second biometric information and a second request for adding a digital signature to a file; authenticating the second request based on matching the second biometric information to the pre-stored biometric information; and adding the digital signature to the file based on the first cryptographic operation code and a private key of the user key pair. In some embodiments, the identity information is biometric information associated with the user. In some embodiments, the method 600 further comprises: receiving third biometric information and a third request for encrypting or decrypting a file; authenticating the user based on matching the third biometric information to the pre-stored biometric information; and performing encryption or decryption based on the third request, the second cryptographic operation code, and a public key or the private key of the user key pair.

[0046] In some embodiments, the biometric information associated with the user is compared with the pre-stored biometric information is performed based on biometric recognition; and the biometric recognition includes one or more of fingerprint recognition, voiceprint recognition, iris-scanning, facial recognition, and heartbeat recognition.

[0047] At 604, the biometric information associated with the user is compared with biometric information pre-stored in the memory as pre-stored biometric information. In some embodiments, the memory is a programmable read-only memory (PROM), an electrically erasable PROM or a flash memory, and wherein the identity information and the user key pair are stored in separate storage units of the memory.

[0048] At 606, in response to determining that the biometric information associated with the user matches the pre-stored biometric information, the user key pair is encrypted to provide an encrypted user key pair.

[0049] At 608, the encrypted user key pair is stored to the memory.

[0050] FIG. 7 depicts examples of modules of an apparatus 700 in accordance with embodiments of this specification. The apparatus 700 can be an example of an embodiment of an ICC. The apparatus 700 can correspond to the embodiments described above, and the apparatus 700 includes the following:

[0051] A request receiving module 702 to receive biometric information associated with a user and a request to store a user key pair to a memory on an ICC. An identity information comparison module 704 to compare the biometric information associated with the user with biometric information pre-stored in the memory as pre-stored biometric information. An encryption module 706 to encrypt the user key pair to provide an encrypted user key pair, in response to determining that the biometric information associated with the user matches the pre-stored biometric information. A storing module 708 to store the identity information and the user key pair to the memory.

[0052] In an optional embodiment, the pre-stored biometric information is stored in the memory during initialization of the ICC. In an optional embodiment, initialization of the ICC comprises: storing identity authentication code executable to authenticate the user based on the pre-stored biometric information. In an optional embodiment, initialization of the ICC comprises: storing first cryptographic operation code executable to add a digital signature

based on the user key pair; and storing second cryptographic operation code executable to perform file encryption or file decryption based on the user key pair.

[0053] In an optional embodiment, the memory is a programmable read-only memory (PROM), an electrically erasable PROM or a flash memory, and wherein the biometric information and the user key pair are stored in separate storage units of the memory.

[0054] The system, apparatus, module, or unit illustrated in the previous embodiments can be implemented by using a computer chip or an entity, or can be implemented by using a product having a certain function. A typical embodiment device is a computer, and the computer can be a personal computer, a laptop computer, a cellular phone, a camera phone, a smartphone, a personal digital assistant, a media player, a navigation device, an email receiving and sending device, a game console, a tablet computer, a wearable device, or any combination of these devices.

[0055] For an embodiment process of functions and roles of each module in the apparatus, references can be made to an embodiment process of corresponding steps in the previous method. Details are omitted here for simplicity.

[0056] Because an apparatus embodiment basically corresponds to a method embodiment, for related parts, references can be made to related descriptions in the method embodiment. The previously described apparatus embodiment is merely an example. The modules described as separate parts may or may not be physically separate, and parts displayed as modules may or may not be physical modules, may be located in one position, or may be distributed on a number of network modules. Some or all of the modules can be selected based on actual demands to achieve the objectives of the solutions of the specification. A person of ordinary skill in the art can understand and implement the embodiments of the present application without creative efforts.

[0057] The techniques described in this specification produce several technical effects. For example, embodiments of the subject matter permit an user of an ICC to store multiple cryptographic keys for securely perform cryptographic operations. The cryptographic keys can be stored to the ICC based on verifying the user's identity information. The ICC will reject cryptographic key information input if the identity information verification fails.

[0058] To request the ICC for performing cryptographic operations, a user's identity information needs to be collected and verified against the identity information previously

authenticated and stored in the ICC. As such, it can be ensured that the user who requested the cryptographic operation is the user of the cryptographic keys.

[0059] Moreover, the identity information and cryptographic keys can be encrypted before storing to the memory of the ICC. The information is only decrypted in ICC to perform corresponding identity verification and cryptographic operations. The cryptographic operations are performed inside of the ICC and only the operational result is output from the ICC. Therefore, ICC users' identity information and cryptographic keys are secure and cannot be revealed even if the ICC is hacked or reverse engineered. In some embodiments, a key management device can be used to store the identity information and cryptographic keys in ciphertext to provide backup to the ICC and further enhance data security.

[0060] A computing device can be used to collect user identity information and initiate request for cryptographic operations. The ICC can communicate with the computing device wirelessly through various communications protocols, or it can be integrated or inserted to the computing device to be easily used for secured cryptographic operations.

[0061] Embodiments of the subject matter and the actions and operations described in this specification can be implemented in digital electronic circuitry, in tangibly-embodied computer software or firmware, in computer hardware, including the structures disclosed in this specification and their structural equivalents, or in combinations of one or more of them. Embodiments of the subject matter described in this specification can be implemented as one or more computer programs, e.g., one or more modules of computer program instructions, encoded on a computer program carrier, for execution by, or to control the operation of, data processing apparatus. For example, a computer program carrier can include one or more computer-readable storage media that have instructions encoded or stored thereon. The carrier may be a tangible non-transitory computer-readable medium, such as a magnetic, magneto optical, or optical disk, a solid state drive, a random access memory (RAM), a read-only memory (ROM), or other types of media. Alternatively, or in addition, the carrier may be an artificially generated propagated signal, e.g., a machine-generated electrical, optical, or electromagnetic signal that is generated to encode information for transmission to suitable receiver apparatus for execution by a data processing apparatus. The computer storage medium can be or be part of a machine-readable storage device, a machine-readable storage

substrate, a random or serial access memory device, or a combination of one or more of them. A computer storage medium is not a propagated signal.

[0062] A computer program, which may also be referred to or described as a program, software, a software application, an app, a module, a software module, an engine, a script, or code, can be written in any form of programming language, including compiled or interpreted languages, or declarative or procedural languages; and it can be deployed in any form, including as a stand-alone program or as a module, component, engine, subroutine, or other unit suitable for executing in a computing environment, which environment may include one or more computers interconnected by a data communication network in one or more locations.

[0063] A computer program may, but need not, correspond to a file in a file system. A computer program can be stored in a portion of a file that holds other programs or data, e.g., one or more scripts stored in a markup language document, in a single file dedicated to the program in question, or in multiple coordinated files, e.g., files that store one or more modules, sub programs, or portions of code.

[0064] Processors for execution of a computer program include, by way of example, both general- and special-purpose microprocessors, and any one or more processors of any kind of digital computer. Generally, a processor will receive the instructions of the computer program for execution as well as data from a non-transitory computer-readable medium coupled to the processor.

[0065] The term “data processing apparatus” encompasses all kinds of apparatuses, devices, and machines for processing data, including by way of example a programmable processor, a computer, or multiple processors or computers. Data processing apparatus can include special-purpose logic circuitry, e.g., an FPGA (field programmable gate array), an ASIC (application specific integrated circuit), or a GPU (graphics processing unit). The apparatus can also include, in addition to hardware, code that creates an execution environment for computer programs, e.g., code that constitutes processor firmware, a protocol stack, a database management system, an operating system, or a combination of one or more of them.

[0066] The processes and logic flows described in this specification can be performed by one or more computers or processors executing one or more computer programs to perform

operations by operating on input data and generating output. The processes and logic flows can also be performed by special-purpose logic circuitry, e.g., an FPGA, an ASIC, or a GPU, or by a combination of special-purpose logic circuitry and one or more programmed computers.

[0067] Computers suitable for the execution of a computer program can be based on general or special-purpose microprocessors or both, or any other kind of central processing unit. Generally, a central processing unit will receive instructions and data from a read only memory or a random access memory or both. Elements of a computer can include a central processing unit for executing instructions and one or more memory devices for storing instructions and data. The central processing unit and the memory can be supplemented by, or incorporated in, special-purpose logic circuitry.

[0068] Generally, a computer will also include, or be operatively coupled to receive data from or transfer data to one or more storage devices. The storage devices can be, for example, magnetic, magneto optical, or optical disks, solid state drives, or any other type of non-transitory, computer-readable media. However, a computer need not have such devices. Thus, a computer may be coupled to one or more storage devices, such as, one or more memories, that are local and/or remote. For example, a computer can include one or more local memories that are integral components of the computer, or the computer can be coupled to one or more remote memories that are in a cloud network. Moreover, a computer can be embedded in another device, e.g., a mobile telephone, a personal digital assistant (PDA), a mobile audio or video player, a game console, a Global Positioning System (GPS) receiver, or a portable storage device, e.g., a universal serial bus (USB) flash drive, to name just a few.

[0069] Components can be “coupled to” each other by being commutatively such as electrically or optically connected to one another, either directly or via one or more intermediate components. Components can also be “coupled to” each other if one of the components is integrated into the other. For example, a storage component that is integrated into a processor (e.g., an L2 cache component) is “coupled to” the processor.

[0070] To provide for interaction with a user, embodiments of the subject matter described in this specification can be implemented on, or configured to communicate with, a computer having a display device, e.g., a LCD (liquid crystal display) monitor, for displaying information to the user, and an input device by which the user can provide input to the

computer, e.g., a keyboard and a pointing device, e.g., a mouse, a trackball or touchpad. Other kinds of devices can be used to provide for interaction with a user as well; for example, feedback provided to the user can be any form of sensory feedback, e.g., visual feedback, auditory feedback, or tactile feedback; and input from the user can be received in any form, including acoustic, speech, or tactile input. In addition, a computer can interact with a user by sending documents to and receiving documents from a device that is used by the user; for example, by sending web pages to a web browser on a user's device in response to requests received from the web browser, or by interacting with an app running on a user device, e.g., a smartphone or electronic tablet. Also, a computer can interact with a user by sending text messages or other forms of message to a personal device, e.g., a smartphone that is running a messaging application, and receiving responsive messages from the user in return.

[0071] This specification uses the term “configured to” in connection with systems, apparatus, and computer program components. For a system of one or more computers to be configured to perform particular operations or actions means that the system has installed on it software, firmware, hardware, or a combination of them that in operation cause the system to perform the operations or actions. For one or more computer programs to be configured to perform particular operations or actions means that the one or more programs include instructions that, when executed by data processing apparatus, cause the apparatus to perform the operations or actions. For special-purpose logic circuitry to be configured to perform particular operations or actions means that the circuitry has electronic logic that performs the operations or actions.

[0072] While this specification contains many specific embodiment details, these should not be construed as limitations on the scope of what is being claimed, which is defined by the claims themselves, but rather as descriptions of features that may be specific to particular embodiments. Certain features that are described in this specification in the context of separate embodiments can also be realized in combination in a single embodiment. Conversely, various features that are described in the context of a single embodiment can also be realized in multiple embodiments separately or in any suitable subcombination. Moreover, although features may be described above as acting in certain combinations and even initially be claimed as such, one or more features from a claimed combination can in

some cases be excised from the combination, and the claim may be directed to a subcombination or variation of a subcombination.

[0073] Similarly, while operations are depicted in the drawings and recited in the claims in a particular order, this should not be understood as requiring that such operations be performed in the particular order shown or in sequential order, or that all illustrated operations be performed, to achieve desirable results. In certain circumstances, multitasking and parallel processing may be advantageous. Moreover, the separation of various system modules and components in the embodiments described above should not be understood as requiring such separation in all embodiments, and it should be understood that the described program components and systems can generally be integrated together in a single software product or packaged into multiple software products.

[0074] Particular embodiments of the subject matter have been described. Other embodiments are within the scope of the following claims. For example, the actions recited in the claims can be performed in a different order and still achieve desirable results. As one example, the processes depicted in the accompanying figures do not necessarily require the particular order shown, or sequential order, to achieve desirable results. In some cases, multitasking and parallel processing may be advantageous.

What is claimed is:

CLAIMS

1. A computer-implemented method for managing user key pairs, the method comprising:

receiving biometric information associated with a user and a request to store a user key pair to a memory on an identity cryptographic chip (ICC);

comparing the biometric information associated with the user with biometric information pre-stored in the memory as pre-stored biometric information;

in response to determining that the biometric information associated with the user matches the pre-stored biometric information, encrypting the user key pair to provide an encrypted user key pair; and

storing the encrypted user key pair to the memory.

2. The computer-implemented method of claim 1, wherein the pre-stored biometric information is stored in the memory during initialization of the ICC.

3. The computer-implemented method of claim 2, wherein initialization of the ICC comprises:

storing identity authentication code executable to authenticate the user based on the pre-stored biometric information.

4. The computer-implemented method of either claim 2 or claim 3, wherein initialization of the ICC comprises:

storing first cryptographic operation code executable to add a digital signature based on the user key pair; and

storing second cryptographic operation code executable to perform file encryption or file decryption based on the user key pair.

5. The computer-implemented method of claim 4, wherein the request to store the user key pair is a first request, the biometric information is first biometric information, and wherein the computer-implemented method further comprises:

receiving second biometric information and a second request for adding a digital signature to a file;

authenticating the second request based on matching the second biometric information to the pre-stored biometric information; and

adding the digital signature to the file based on the first cryptographic operation code and a private key of the user key pair.

6. The computer-implemented method of claim 5, further comprises:

receiving third biometric information and a third request for encrypting or decrypting a file;

authenticating the user based on matching the third biometric information to the pre-stored biometric information; and

performing encryption or decryption based on the third request, the second cryptographic operation code, and a public key or the private key of the user key pair.

7. The computer-implemented method of any of the preceding claims, wherein:

comparing the biometric information associated with the user with the pre-stored biometric information is performed based on biometric recognition; and

the biometric recognition includes one or more of fingerprint recognition, voiceprint recognition, iris-scanning, facial recognition, and heartbeat recognition.

8. The computer-implemented method of any of the preceding claims, wherein the memory is a programmable read-only memory (PROM), an electrically erasable PROM or a flash memory, and wherein the biometric information and the user key pair are stored in separate storage units of the memory.

9. A system for managing user key pairs, comprising:

one or more processors; and

one or more computer-readable memories coupled to the one or more processors and having instructions stored thereon that are executable by the one or more processors to perform the method of any one of claims 1-8.

10. An apparatus for managing user key pairs, the apparatus comprising a plurality of modules for performing the method of any one of claims 1-8.

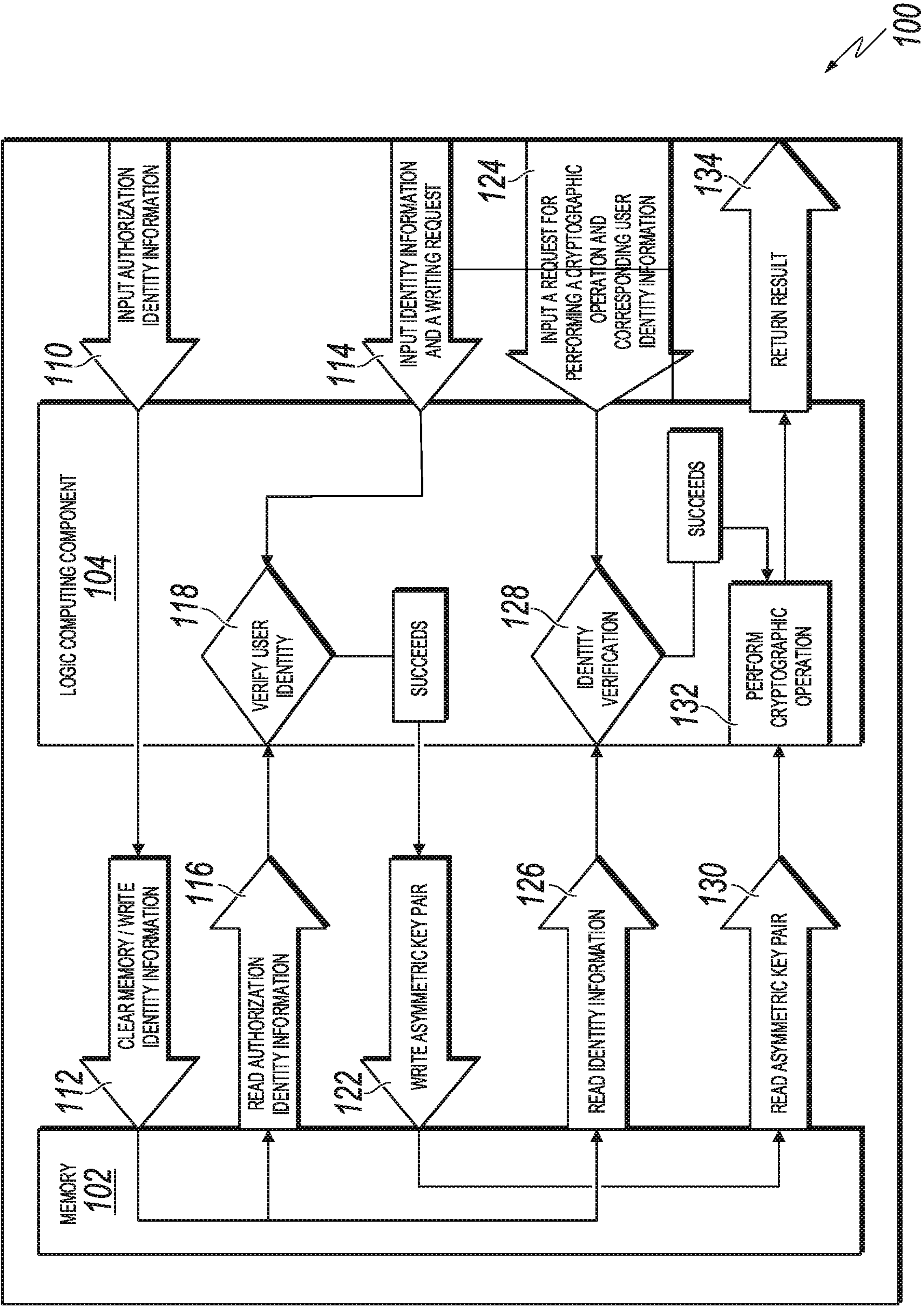
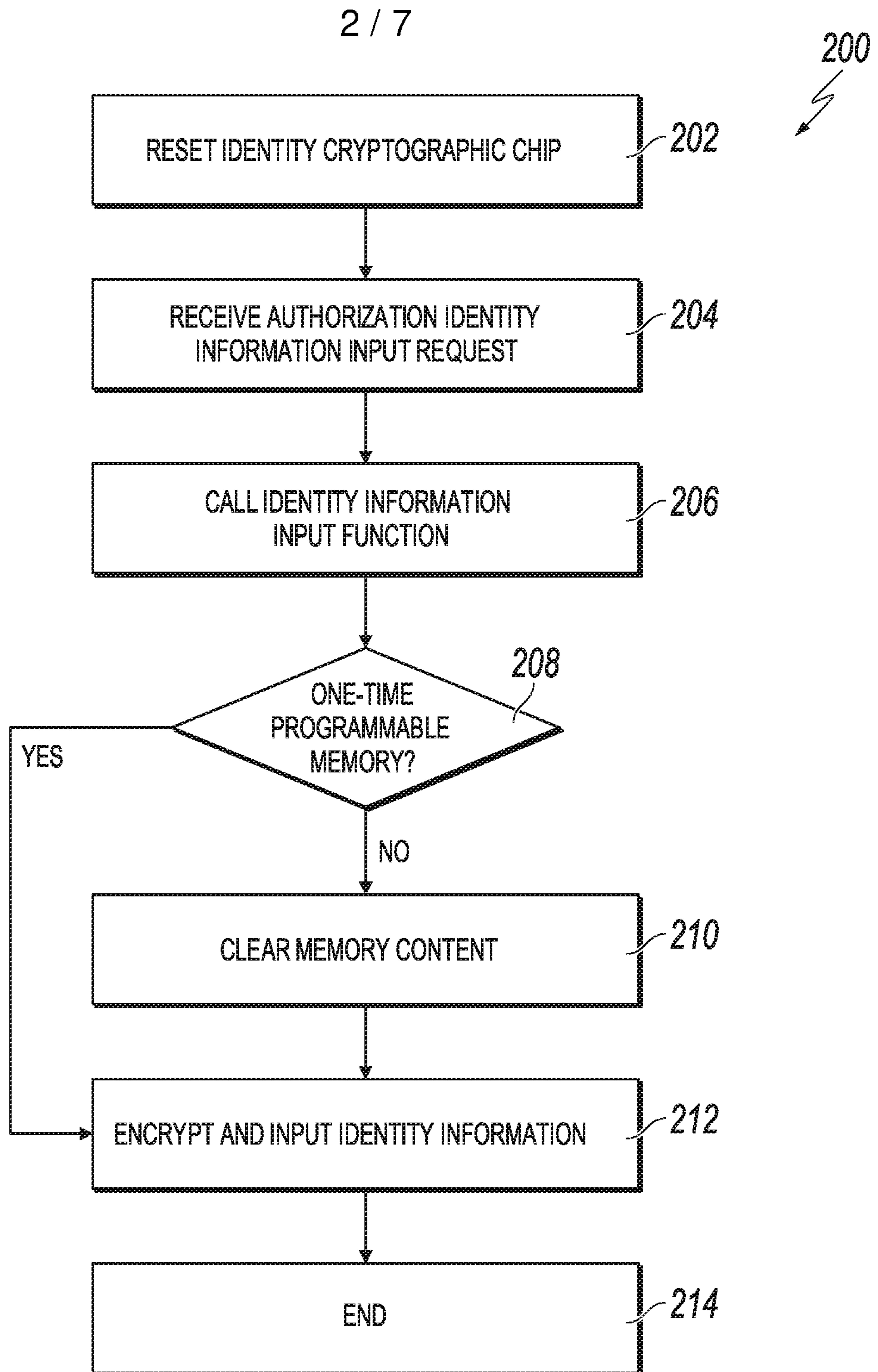
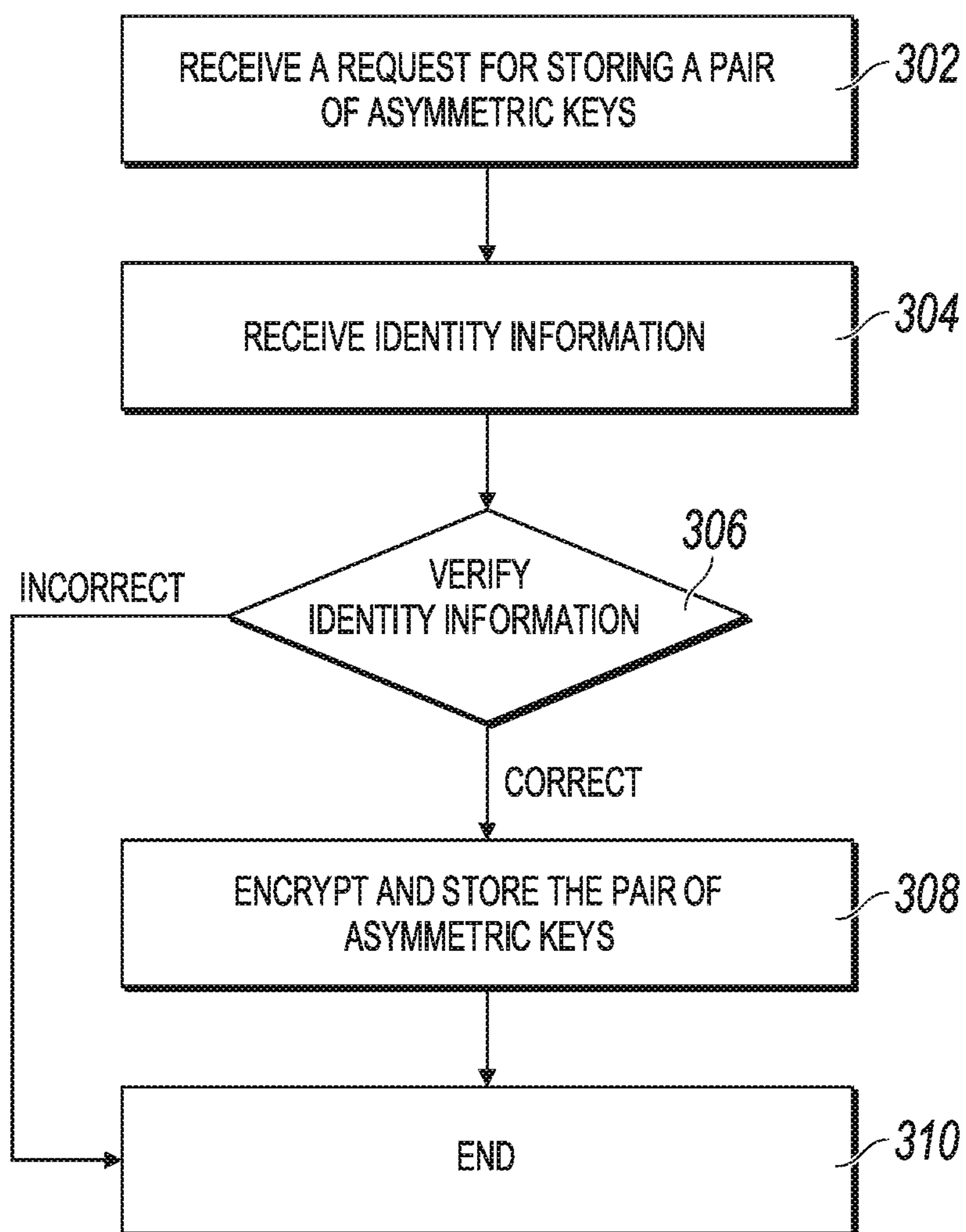


FIG. 1

**FIG. 2**

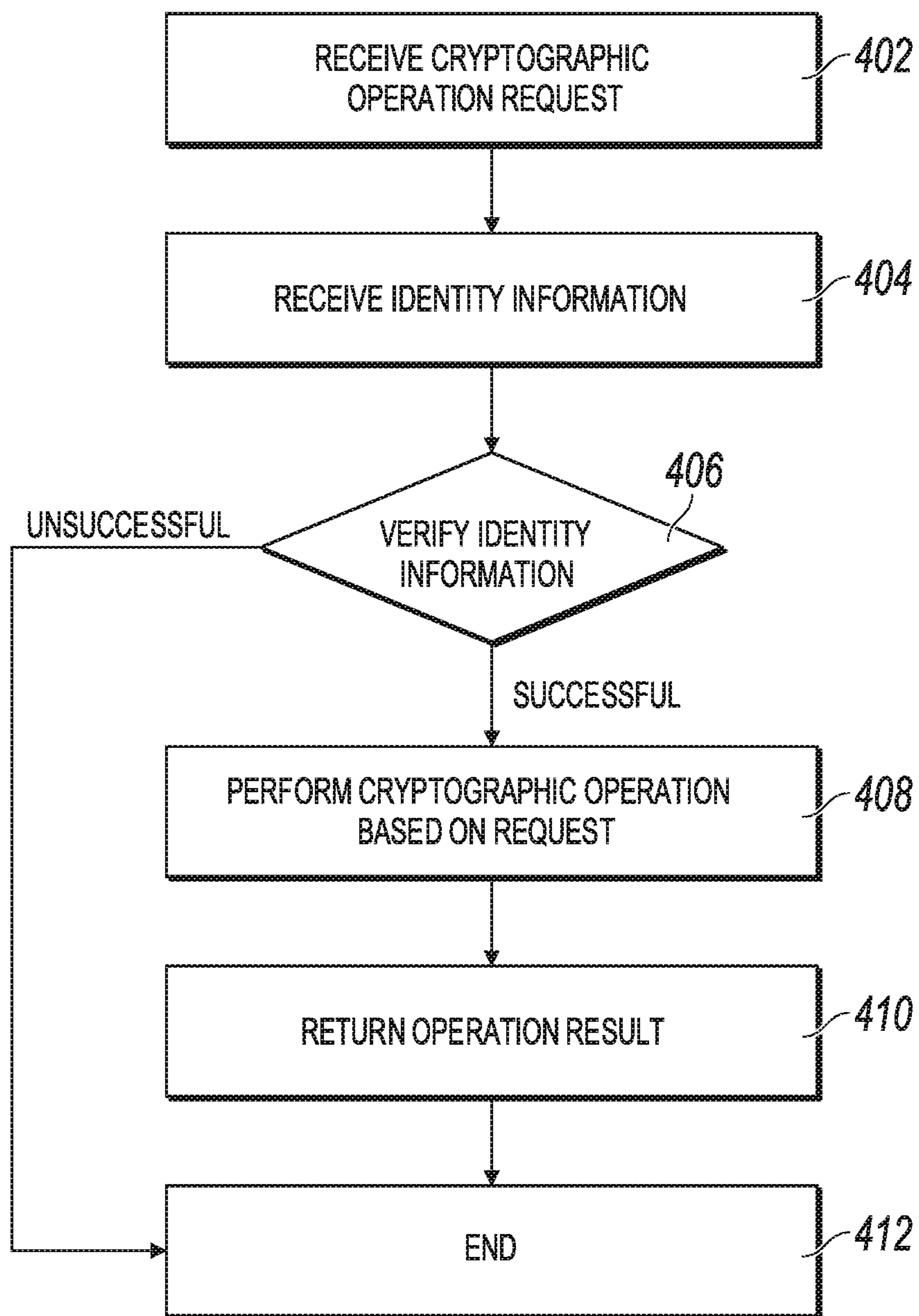
3 / 7

300

**FIG. 3**

4 / 7

400

**FIG. 4**

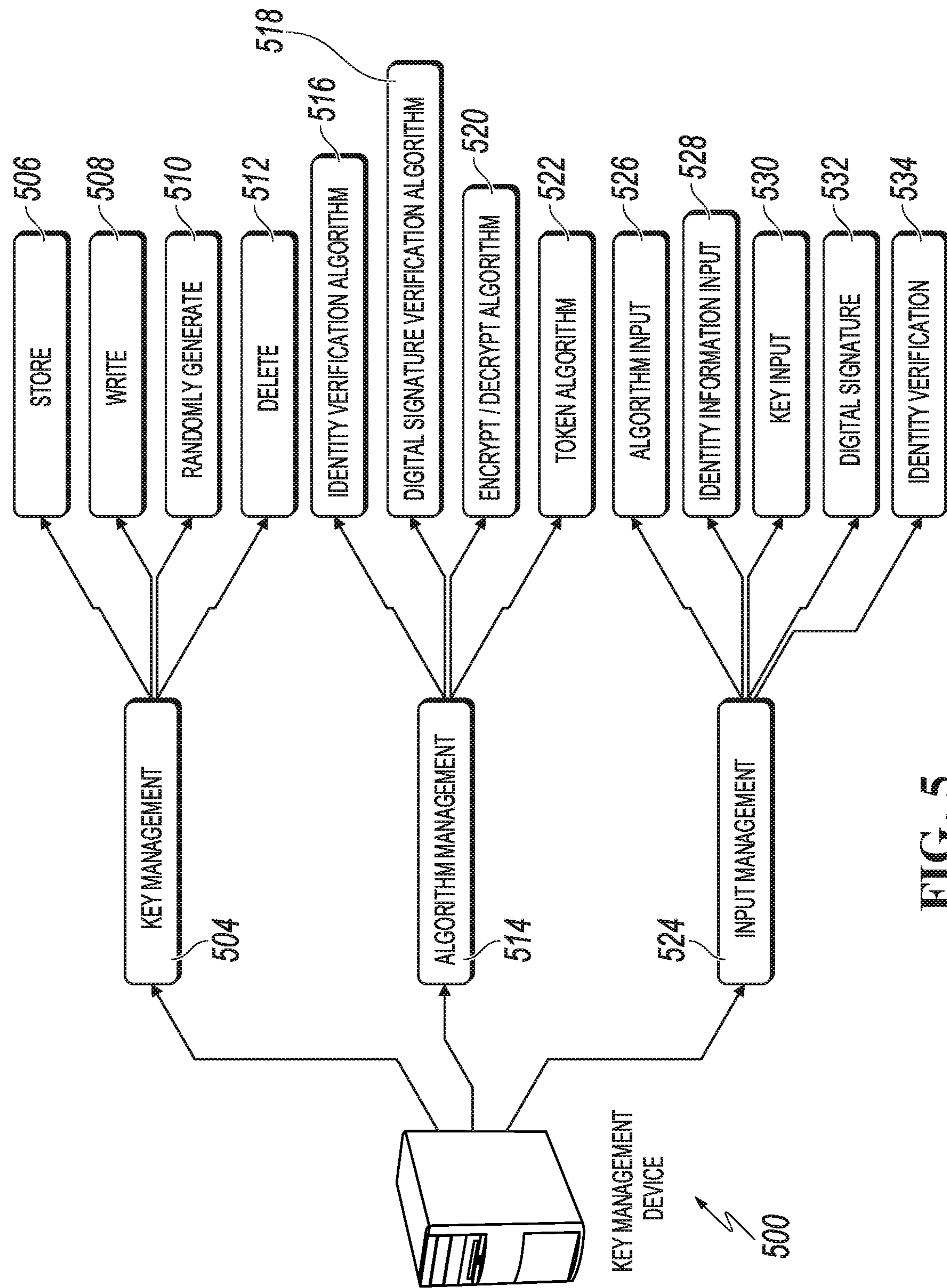
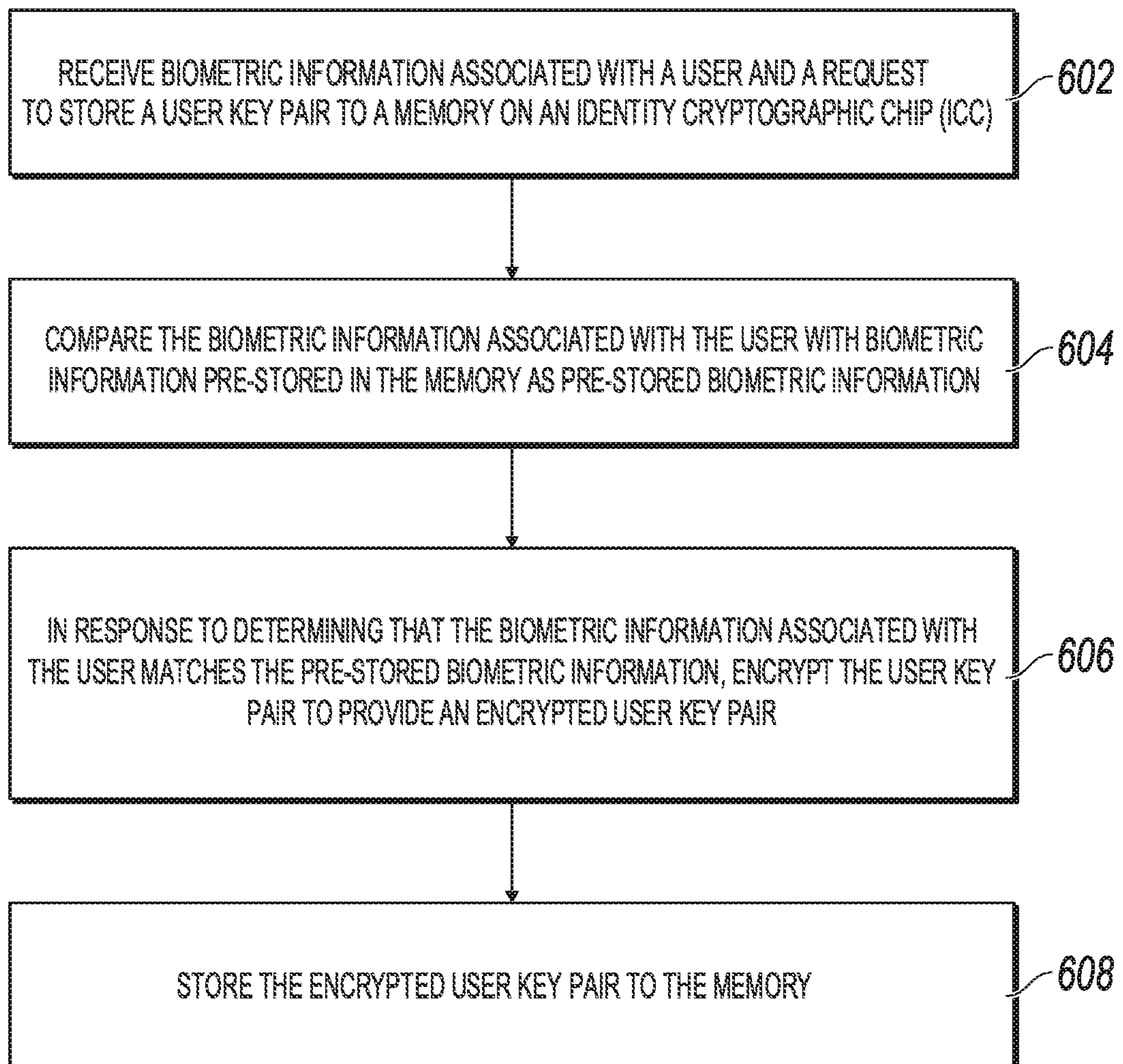


FIG. 5

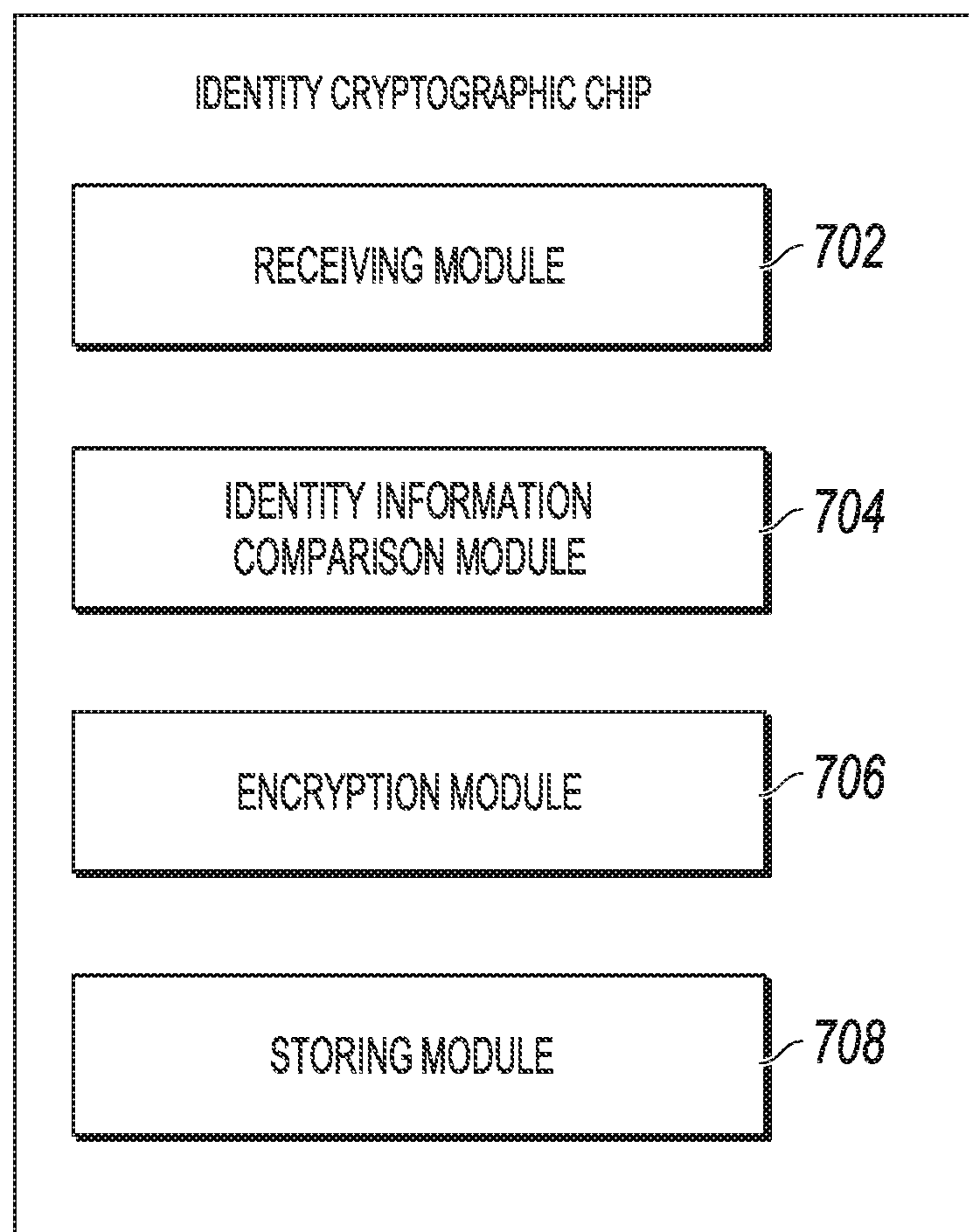
6 / 7

600

**FIG. 6**

7 / 7

700

**FIG. 7**

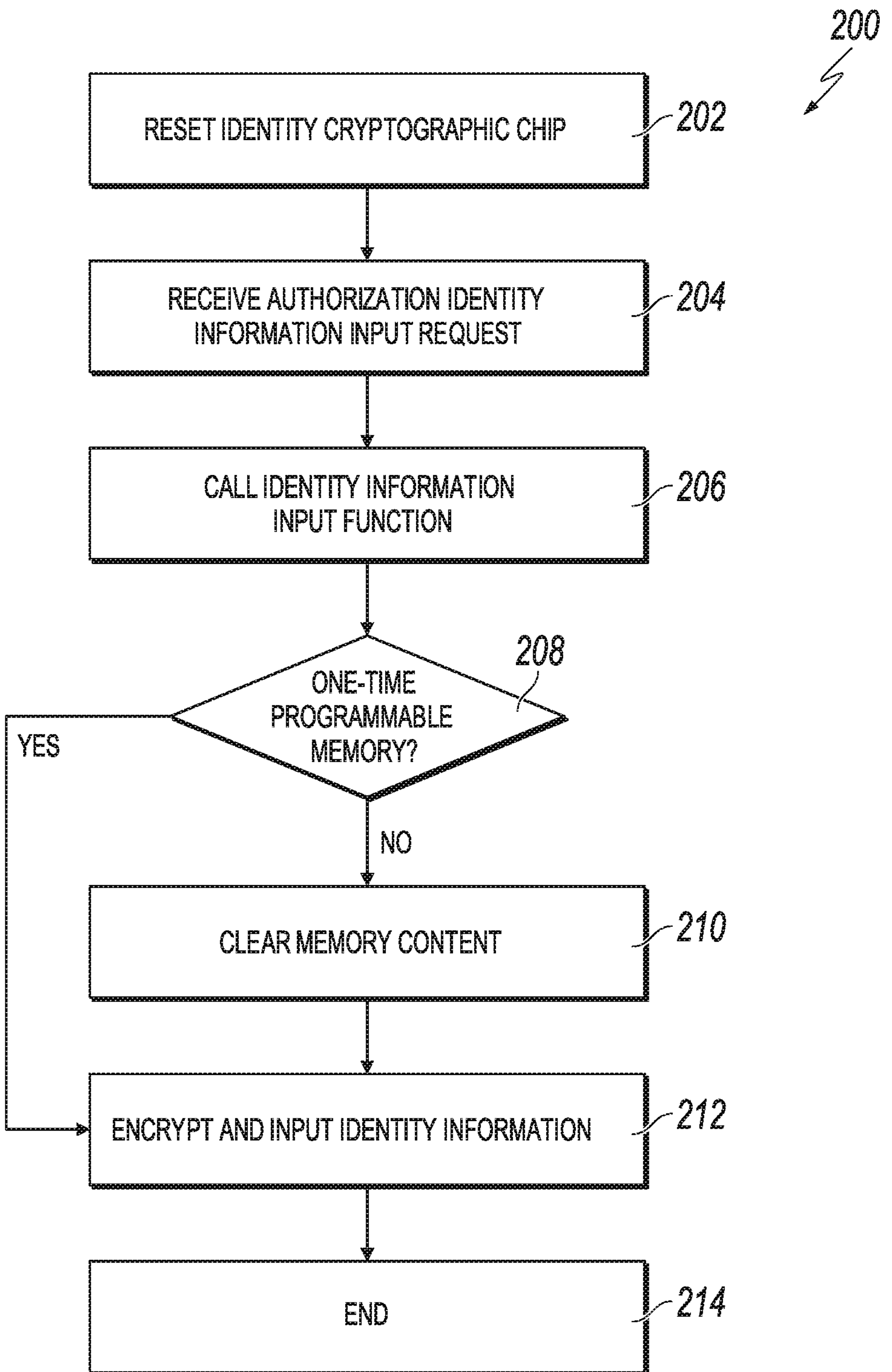


FIG. 2