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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
25 January 2007 (25.01.2007)

PCT

(10) International Publication Number
WO 2007/011990 A2

(51) International Patent Classification:
H04L 9/30 (2006.01)

(21) International Application Number:
PCT/US2006/027978

(22) International Filing Date: 17 July 2006 (17.07.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/182,520 15 July 2005 (15.07.2005) US

(71) Applicant *(for all designated States except US)*: **TYFONE INC.** [US/US]; 5520 SW Macadam Ave., Suite 250, Portland, OR 97219 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **NARENDRA, Siva G.** [IN/US]; 7180 SW, 84th Ave, Portland, OR 97223 (US). **TADEPALLI, Prabhakar** [US/IN]; 290 Phase II, Adarsh Palm Meadows, Airport Whitefield Road, Bangalore, Karnataka 560 066 (IN). **SPITZER, Thomas N.** [US/US]; 2642 SW, Bucharest Ct., Portland, OR 97225 (US).

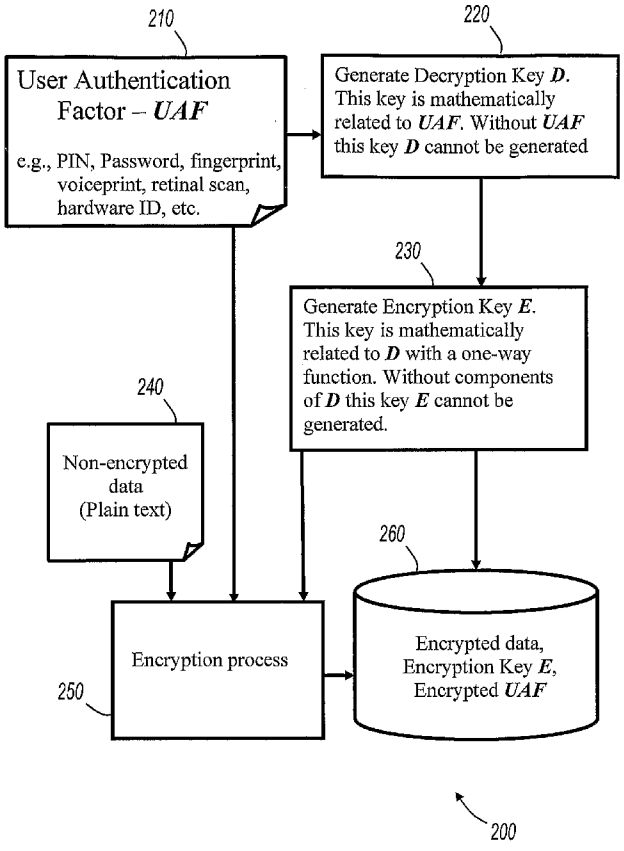
(74) Agent: **LEMOINE PATENT SERVICES**; Intellevate LLC-Patent & Trademark Services, 900 Second Ave South, Suite 1700, Minneapolis, MN 55402 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SY, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT,

[Continued on next page]

(54) Title: ASYMMETRIC CRYPTOGRAPHY WITH USER AUTHENTICATION



(57) Abstract: A device uses a user authentication factor to generate a decryption key for use in asymmetric cryptography. An encryption key is generated from the decryption key using a one-way function.

WO 2007/011990 A2

RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

ASYMMETRIC CRYPTOGRAPHY WITH USER AUTHENTICATION

Field

The present invention relates generally to secure data storage, and more specifically to the use of asymmetric cryptography for secure data storage.

Background

Cryptography may be used to limit access to data. For example, sensitive data in computers or networks may be encrypted to block access by unauthorized users. Cryptography may be utilized to securely store information or to securely share information.

Different types of cryptography are in use today. Examples include symmetric cryptography and asymmetric cryptography. In symmetric cryptography, encryption and decryption are performed with the same "key." Symmetric cryptography is sometimes also referred to as secret key cryptography, because the key cannot be disclosed for the data to remain secure. Triple-DES cryptography is an example of symmetric cryptography.

Asymmetric cryptography uses two keys: an encryption key, and a decryption key, where the encryption key is derived from the decryption key using a one-way function. In asymmetric cryptography, the encryption key (also referred to as the public key) can be disclosed since it can only encrypt and not decrypt data. The decryption key (also referred to as the private key) cannot be disclosed for the data to remain secure. Examples of asymmetric cryptography include Rivest-Shamir-Adleman (RSA) and elliptic curve cryptography.

Brief Description of the Drawings

Figure 1 shows a mobile electronic device in accordance with various embodiments of the present invention;

Figures 2 and 3 show flow diagrams in accordance with various embodiments of the present invention; and

Figure 4 shows a computer system in accordance with various embodiments of the present invention.

Description of Embodiments

In the following detailed description, reference is made to the accompanying drawings that show, by way of illustration, various embodiments of an invention. These embodiments are described in sufficient detail to enable those skilled in the art to practice the invention. It is to be understood that the various embodiments of the invention, although different, are not necessarily mutually exclusive. For example, a particular feature, structure, or characteristic described in connection with one embodiment may be implemented within other embodiments without departing from the spirit and scope of the invention. In addition, it is to be understood that the location or arrangement of individual elements within each disclosed embodiment may be modified without departing from the spirit and scope of the invention. The following detailed description is, therefore, not to be taken in a limiting sense, and the scope of the present invention is defined only by the appended claims, appropriately interpreted, along with the full range of equivalents to which the claims are entitled. In the drawings, like numerals refer to the same or similar functionality throughout the several views.

Figure 1 shows a mobile electronic device. Mobile electronic device 100 may be any type of electronic device considered to be mobile. For example, mobile electronic device 100 may be a personal digital assistant (PDA), a smartphone, a mobile phone, a handheld computer, or any other device capable of operating as described herein. Figure 1 also shows secondary electronic device 120. Secondary electronic device 120 is shown as a key fob separate from mobile electronic device 100 in Figure 1, but this is not a limitation of the present invention. For example, secondary electronic device 120 may be a card that attaches to, and detaches from, mobile electronic device 100. Accordingly, secondary electronic device 120 may be separate from, or separable from, mobile electronic device 100.

Mobile electronic device 100 is shown including controls 106, fingerprint scanner 108, voice input 104, and retinal scanner 102. Fingerprint scanner 108, voice input 104, and retinal scanner 102 are examples of biometric information collection devices capable of collecting biometric information to authenticate a user of mobile device 100. Controls 106 represent an input device capable of accepting other types of user authentication information, such as a password or personal identification number (PIN).

Biometric information, passwords, and PINs are examples of user authentication factors (UAF) useful to authenticate a user to mobile electronic device 100. For example, access to mobile device 100 or features of mobile electronic device 100 may be limited to users that satisfy certain requirements with respect to matching UAFs.

Other types of information may also be used as user authentication factors. For example, UAFs may include unique identifiers (IDs) related to hardware devices such as mobile electronic device 100 or secondary electronic device 120. In some embodiments of the present invention, user authentication is performed using a combination of UAFs. For example, a unique ID may be combined with biometric information to authenticate a user to mobile electronic device 100. Unique IDs may be received by mobile electronic device 100 in many ways. For example, a unique ID may be provided by secondary electronic device 120 using a wireless interface, or by physical contact between mobile electronic device 100 and secondary electronic device 120. Also for example, a unique ID may be provided by an internal subsystem within mobile electronic device 100, such as a hard disk drive, a memory subsystem, or a processor.

Mobile electronic device 100 may provide secure data storage or secure data transfer using asymmetric cryptography that utilizes UAFs. For example, a decryption key may be generated from a mathematical representation of one or more UAFs, and an encryption key may then be derived from the decryption key using a one-way function. Asymmetric cryptography embodiments are described in further detail below with reference to later figures.

Mobile electronic device 100 may include a mechanism to allow mobile electronic device 100 to communicate with a wired or wireless network. For example, mobile electronic device 100 may include circuitry to communicate with a cellular phone network. Note that in these embodiments, mobile electronic device 100 may or may not be a phone. For example, mobile electronic device 100 may be a cellular telephone having asymmetric cryptography capabilities. Also for example, mobile electronic device 100 may be a non-telephonic device that has cellular network connectivity. Examples include personal digital assistants, and handheld devices dedicated to secure data storage or secure data exchange. Further, mobile electronic device 100 may be a non-telephonic device having wired or wireless connectivity to a network other than a cellular network, and in some embodiments, mobile electronic device 100 may be a device without network connectivity. Examples include, but are not limited to: Blackberry devices available from Research in Motion (RIM), music players such as MP3 players, cameras, and the like.

In some embodiments, mobile electronic device 100 is an example of a "wearable" device that is capable of securely storing or exchanging data. For example, in some embodiments, mobile electronic device 100 may have the form factor of a wristwatch. Some embodiments of the present invention may have other wearable form factors. For example, a wearable mobile electronic device may be worn in such a manner that it contacts human skin, or it may be worn on clothing. Any wearable intelligent electronic device may be employed without departing from the scope of the present invention.

Figure 2 shows a flow diagram in accordance with various embodiments of the present invention. Diagram 200 represents data flow and actions that may be performed when encrypting data in accordance with various embodiments of the present invention. The various actions represented in Figure 2 may be performed by a mobile electronic device such as mobile electronic device 100 (Figure 1), although this is not a limitation of the present invention. For example, the various actions in

Figure 2 may be performed by a non-mobile computing device such as a desktop computer, workstation, or mainframe computer.

Block 210 represents the collection of one or more user authentication factors (UAFs). As shown in block 210, a UAF may be biometric information, a password or PIN, a hardware ID, or any combination. For example, a user may provide a fingerprint and also present a secondary electronic device that transmits a unique hardware ID. The fingerprint and the hardware ID may together be considered a UAF. The collection of UAF may be performed with biometric sensors such as those shown on mobile electronic device 100 (Figure 1). Further, the collection of UAF may be performed over a wired or wireless interface.

At 220, a decryption key ***D*** is generated from the UAF. Any functional relationship may be used to relate ***D*** to the UAF. For example, if the generation of ***D*** uses one or more prime numbers, prime number generation or selection may be a function of the UAF. Further, in some embodiments, ***D*** may be set equal to a numerical representation of the UAF. Without the UAF, the decryption key ***D*** cannot be generated.

At 230, an encryption key ***E*** is generated from the decryption key ***D*** using a one-way function. Without components of ***D***, ***E*** cannot be generated. Any type of one-way function may be utilized without departing from the scope of the present invention. For example, a one-way function built on the Rivest-Shamir-Adleman (RSA) public key encryption algorithm may be utilized.

The encryption process at 250 encrypts data 240 and the UAF using encryption key ***E***. The encrypted data, encrypted UAF, and encryption key ***E*** are stored 260. The decryption key ***D*** is not stored.

Figure 3 shows a flow diagram in accordance with various embodiments of the present invention. Diagram 300 represents data flow and actions that may be performed when decrypting data in accordance with various embodiments of the present invention. The various actions represented in Figure 3 may be performed by a mobile electronic device such as mobile electronic device 100 (Figure 1), although this is not a limitation of the present invention. For example, the various actions in

Figure 3 may be performed by a non-mobile computing device such as a desktop computer, workstation, or mainframe computer.

Block 310 represents the collection of one or more user authentication factors (UAFs). The UAF in block 310 is collected for the decryption of data and is referred to as UAF' to distinguish it from the UAF collected when the data is encrypted (Figure 2). As shown in block 310, a UAF' may be biometric information, a password or PIN, a hardware ID, or any combination. For example, a user may provide a fingerprint and also present a secondary electronic device that transmits a unique hardware ID. The fingerprint and the hardware ID may together be considered a UAF'. The collection of UAF' may be performed with biometric sensors such as those shown on mobile electronic device 100 (Figure 1). Further, the collection of UAF' may be performed over a wired or wireless interface.

The encrypted data, encryption key ***E***, and encrypted UAF are shown stored at 260 as a product of the various actions shown in Figure 2. At 320, the collected UAF' is encrypted using ***E***, and the result is compared with the encrypted UAF stored at 260. If there is no match, then data access is denied at 340. If there is a match (signifying that UAF and UAF' are equal), then the decryption key ***D*** is generated from UAF' at 360. The decryption key ***D*** is used to decrypt the data at 350, and the result is the non-encrypted data 240.

Using asymmetric encryption embodiments represented by Figure 2, once the encryption process is completed, the data stored does not include the decryption key ***D***. Using asymmetric decryption embodiments represented by Figure 3, the stored data cannot be decrypted unless and until the UAF' is authenticated to be correct. The UAF verification process only utilizes the encryption key ***E***, and therefore does not require the decryption key ***D***.

As described above, the user authentication factor (UAF) can include one or more of biometric factors identifying an individual, passwords or PINs identifying a privileged person or class of persons, or hardware device specific IDs that identify the presence or proximity of a particular piece of equipment. In some embodiments, the UAF used to generate the decryption key ***D*** is formed by combining biometric

information with one or more hardware IDs. In these embodiments, a valid user may only access encrypted data when a particular piece of hardware is present. For example, a hardware ID from secondary device 120 (Figure 1) may be combined with a user's fingerprint to form a UAF used to generate ***D***. Also for example, a hardware ID from within mobile electronic device 100 (Figure 1) may be combined with a biometric factor collected by one or more of the various biometric collection components shown in Figure 1.

Figure 4 shows a computer system in accordance with various embodiments of the present invention. Computer system 400 may be a mobile electronic device such as mobile electronic device 100 (Figure 1), or may be a non-mobile device such as a desktop computer, workstation, server, or mainframe. Computer system 400 includes processor 460, user authentication factor (UAF) collection component 410, asymmetric cryptography engine 430, and storage component 450.

UAF collection component 410 includes one or more components capable of collecting user authentication factors. For example, UAF collection component 410 may include wireless interface 412 to communicate with other electronic devices to receive user authentication factors. Any type of UAF information may be received over wireless interface 412. For example, wireless interface 412 may communicate with a secondary wireless device such as a mobile phone or key fob having a unique ID that is used as a UAF. Also for example, wireless interface 412 may communicate with other computer systems that provide one or more UAFs.

Biometric collection component 414 may include one or more interfaces to collect biometric information of a user. For example, biometric collection component 414 may include a fingerprint scanner, a retinal scanner, a voice recorder, or the like. Unique ID 416 may be collected by UAF collection component 410 in many different ways. For example, one or more subsystems within computer system 400 may provide a unique hardware ID for use as a UAF. Further, unique ID 416 may be provided by a hardware device that is separate from, or separable from, computer system 400.

UAF collection component 410 may be implemented in hardware, software, or any combination. For example, wireless interface 412 may include a network interface card (NIC) that includes a processing device and firmware. Further, biometric collection component 414 may include hardware to provide a physical interface to a person, and may also include a device driver to be executed by processor 460. User authentication factors collected by UAF collection component 410 may be utilized to generate decryption keys in an asymmetric cryptography engine. For example, UAF collection component may provide the UAF referenced in Figure 2 and the UAF' referenced in Figure 3.

Asymmetric cryptography engine 430 includes decryption key generation component 432, encryption key generation component 434, decryption process component 436, and encryption process component 438. The various components of asymmetric cryptography engine 430 may be implemented in hardware, software or any combination. For example, the various components may be implemented in software that is executed by processor 460. In these embodiments, the various components of asymmetric cryptography engine 430 may be embodied as instructions on a machine readable medium such as a memory device, hard disk drive, or other storage medium.

In some embodiments, decryption key generation component 432 generates a decryption key ***D*** from a user authentication factor. For example, decryption key generation component 432 may perform actions shown at 220 in Figure 2 or at 360 in Figure 3. In some embodiments, encryption key generation component 434 generates an encryption key ***E*** from a decryption key ***D*** using a one-way function. For example, encryption key generation component 434 may perform actions shown at 230 in Figure 2.

In some embodiments, decryption process component 436 utilizes a decryption key ***D*** to decrypt encrypted data. For example, decryption process component 436 may perform actions shown at 350 in Figure 3. Also in some embodiments, encryption process component 438 utilizes an encryption key ***E*** to

encrypt data. For example, encryption process component 438 may perform actions shown at 250 in Figure 2.

Storage component 450 may be any type of storage component capable of storing encrypted data, encrypted UAFs, and encryption keys. For example, storage component 450 may be a memory such as a static random access memory (SRAM), dynamic random access memory (DRAM), or FLASH memory. Also for example, storage component 450 may be a hard disk, floppy disk, CDROM storage, or any other type of storage. Storage component 450 may also include a machine readable medium that includes instructions that when accessed result in processor 460 performing actions. For example, storage component 450 may have instructions to implement the various components of asymmetric cryptography engine 430.

Processor 460 represents a processor capable of communicating with the other blocks shown in computer system 400. For example, processor 460 may be a microprocessor, a digital signal processor (DSP), a microcontroller, or the like. Further, processor 460 may be formed from state machines or other sequential logic. In operation, processor 460 may read instructions and/or data from storage component 450, asymmetric cryptography engine 430, or UAF collection component 410. For example, processor 460 may execute program instructions that implement asymmetric cryptography engine 430.

Although the present invention has been described in conjunction with certain embodiments, it is to be understood that modifications and variations may be resorted to without departing from the spirit and scope of the invention as those skilled in the art readily understand. Such modifications and variations are considered to be within the scope of the invention and the appended claims.

What is claimed is:

1. A method for encrypting data comprising:
receiving at least one user authentication factor;
generating a decryption key from the at least one user authentication factor;
generating an encryption key from a one-way function of the decryption key; and
encrypting data using the encryption key.

2. The method of claim 1 wherein the at least one user authentication factor includes a unique ID for a hardware device.

3. The method of claim 2 wherein the hardware device comprises a hardware device physically separate from an apparatus performing the method.

4. The method of claim 2 wherein the hardware device comprises a hardware device physically separable from an apparatus performing the method.

5. The method of claim 1 wherein the at least one user authentication factor includes a biometric factor.

6. The method of claim 1 wherein the at least one user authentication factor includes a unique ID for a hardware device and a biometric factor.

7. The method of claim 1 wherein generating a decryption key comprises setting the decryption key equal to the at least one user authentication factor.

8. The method of claim 1 further comprising encrypting the at least one user authentication factor using the encryption key to produce an encrypted at least one user authentication factor.

9. The method of claim 8 further comprising:
storing the encrypted data;
storing the encryption key; and
storing the encrypted at least one user authentication factor.

10. A method for decrypting data comprising:
receiving at least one user authentication factor;
generating a decryption key from the at least one user authentication factor; and
decrypting stored data using the decryption key.

11. The method of claim 10 further comprising encrypting the at least one user authentication factor using a stored encryption key to produce a result, and comparing the result with a stored encrypted user authentication factor.

12. The method of claim 10 wherein the at least one user authentication factor includes a unique ID for a hardware device.

13. The method of claim 12 wherein the hardware device comprises a hardware device physically separate from an apparatus performing the method.

14. The method of claim 12 wherein the hardware device comprises a hardware device physically separable from an apparatus performing the method.

15. The method of claim 10 wherein the at least one user authentication factor includes a biometric factor.

16. The method of claim 10 wherein the at least one user authentication factor includes a unique ID for a hardware device and a biometric factor.

17. An apparatus with a machine accessible medium having instructions stored thereon that when accessed result in a machine performing:

receiving at least one user authentication factor;

generating a decryption key from the at least one user authentication factor;

generating an encryption key from a one-way function of the decryption key; and

encrypting data using the encryption key.

18. The apparatus of claim 17 wherein the at least one user authentication factor includes a unique ID for a hardware device.

19. The apparatus of claim 18 wherein the hardware device comprises a hardware device physically separate from the machine performing the method.

20. The apparatus of claim 18 wherein the hardware device comprises a hardware device physically separable from the machine performing the method.

21. The apparatus of claim 17 wherein the at least one user authentication factor includes a biometric factor.

22. The apparatus of claim 17 wherein the at least one user authentication factor includes a unique ID for a hardware device and a biometric factor.

23. An apparatus with a machine accessible medium having instructions stored thereon that when accessed result in a machine performing:

receiving at least one user authentication factor;

generating a decryption key from the at least one user authentication factor; and

decrypting stored data using the decryption key.

24. The apparatus of claim 23 wherein the instructions, when accessed, further result in the machine performing:

encrypting the at least one user authentication factor using a stored encryption key to produce a result, and comparing the result with a stored encrypted user authentication factor.

25. The apparatus of claim 23 wherein the at least one user authentication factor includes a unique ID for a hardware device.

26. The apparatus of claim 25 wherein the hardware device comprises a hardware device physically separate from the machine performing the method.

27. The apparatus of claim 25 wherein the hardware device comprises a hardware device physically separable from the machine performing the method.

28. The apparatus of claim 23 wherein the at least one user authentication factor includes a biometric factor.

29. The apparatus of claim 23 wherein the at least one user authentication factor includes a unique ID for a hardware device and a biometric factor.

30. A computer system for storing and accessing encrypted data, comprising:

a user authentication factor collection component to receive at least one user authentication factor;

a decryption key generation component to generate a decryption key from the at least one user authentication factor;

an encryption key generation component to generate an encryption key from the decryption key using a one-way function;

an encryption process component to encrypt data using the encryption key; and

a decryption process component to decrypt encrypted data using the decryption key.

31. The computer system of claim 30 further comprising a storage component to store the encryption key and not the decryption key.

32. The computer system of claim 30 wherein the user authentication factor collection component is configured to receive a unique ID for a hardware device as a user authentication factor.

33. The computer system of claim 32 wherein the hardware device comprises a hardware device physically separable from the computer system.

34. The computer system of claim 30 wherein the user authentication factor collection component is configured to receive a biometric factor as a user authentication factor.

35. The computer system of claim 30 wherein the user authentication factor collection component is configured to receive a unique ID for a hardware device and a biometric factor as user authentication factors.

36. An apparatus comprising:

means for collecting at least one user authentication factor;

means for generating a decryption key from the at least one user authentication factor;

means for generating an encryption key from the decryption key using a one-way function;

means for encrypting data using the encryption key; and

means for decrypting data using the decryption key.

37. A handheld device to store encrypted data, comprising:

a biometric collection device to collect a biometric user authentication factor; and

an asymmetric cryptography engine to generate an asymmetric decryption key from the biometric user authentication factor, and to generate an asymmetric encryption key from the asymmetric decryption key.

38. The handheld device of claim 37 wherein the biometric collection device comprises a fingerprint collection device.

39. The handheld device of claim 37 wherein the biometric collection device comprises a retinal scanner.

40. The handheld device of claim 37 further comprising a wireless interface to receive a unique ID from a wireless device.

41. The handheld device of claim 40 wherein the asymmetric cryptography engine is configured to generate the asymmetric cryptography key from the unique ID and the biometric user authentication factor.

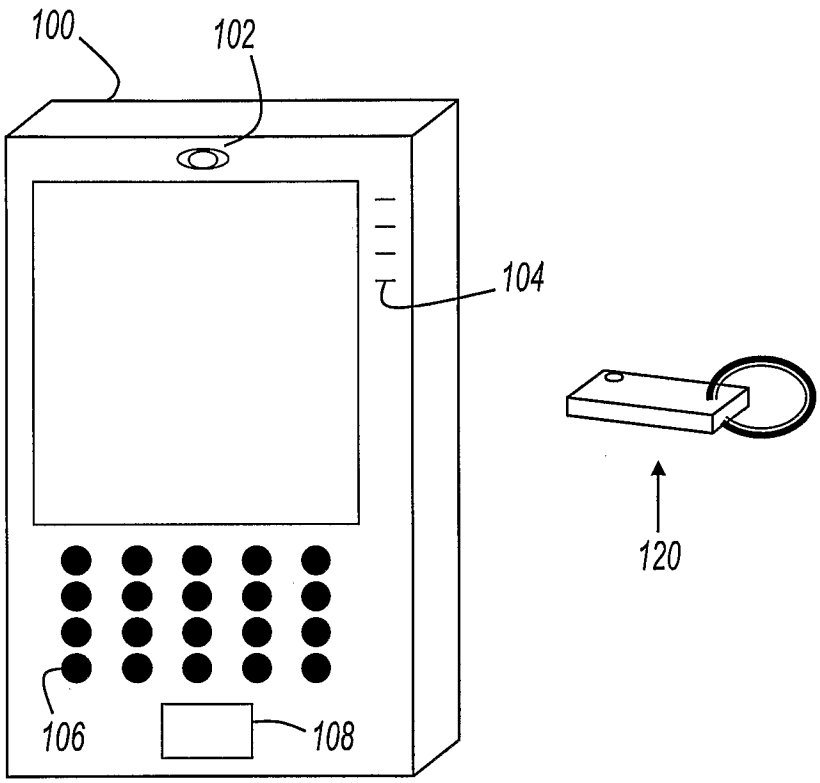


FIG. 1

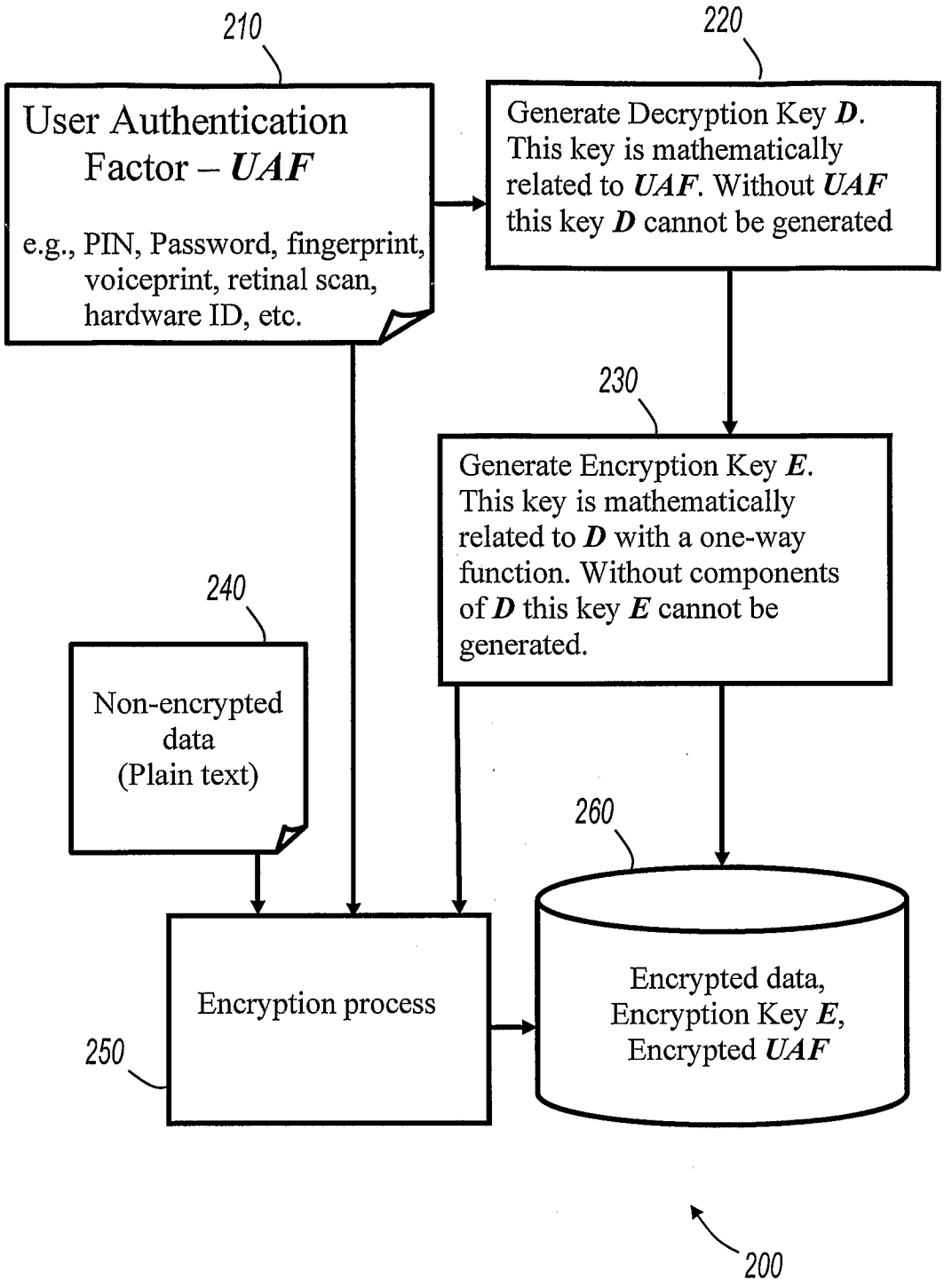

210
User Authentication Factor – UAF
e.g., PIN, Password, fingerprint, voiceprint, retinal scan, hardware ID, etc.
220
Generate Decryption Key D. This key is mathematically related to UAF. Without UAF this key D cannot be generated
230
Generate Encryption Key E. This key is mathematically related to D with a one-way function. Without components of D this key E cannot be generated.
240
Non-encrypted data (Plain text)
260
Encrypted data, Encryption Key E, Encrypted UAF
Encryption process
250
200

FIG. 2

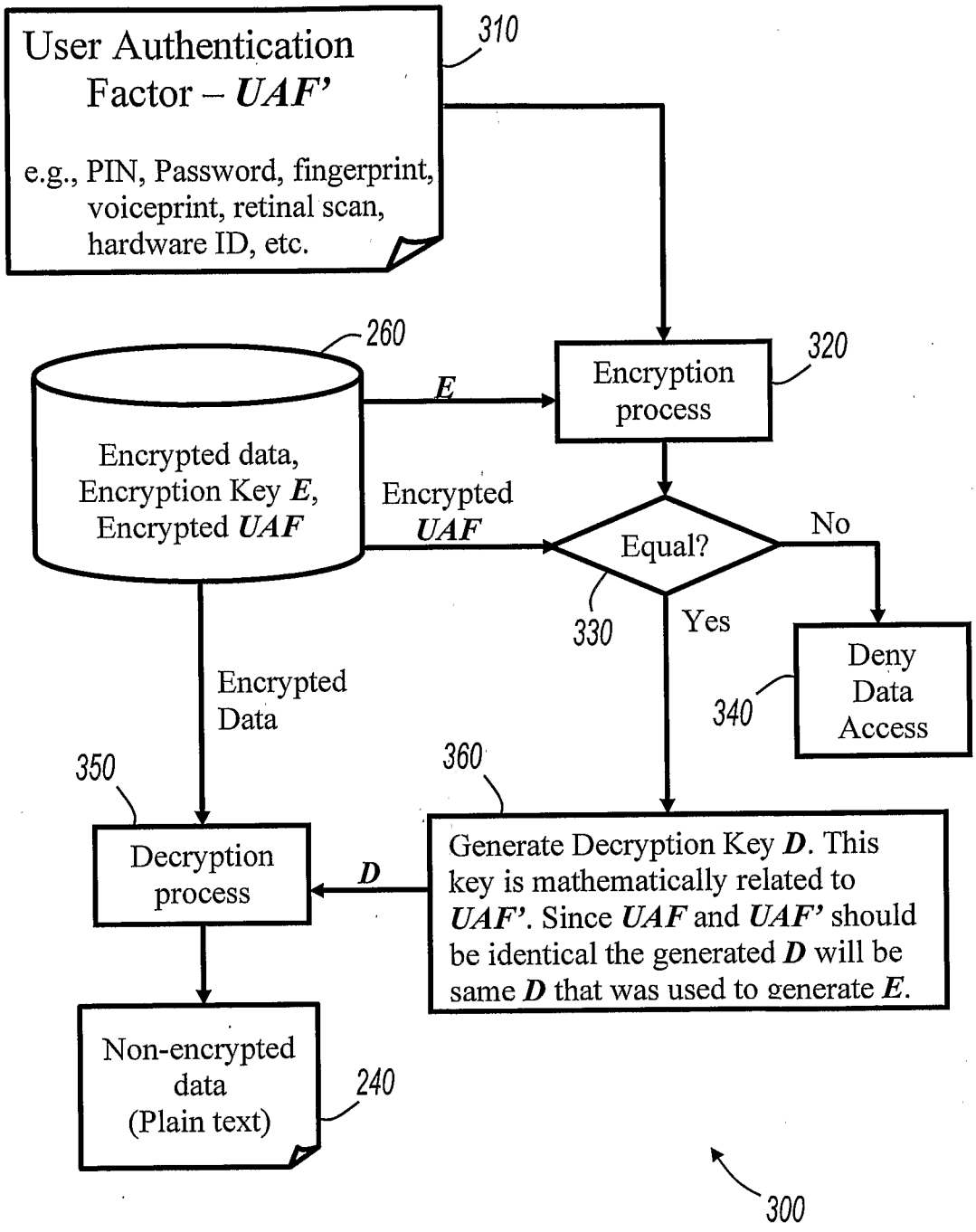

User Authentication Factor – UAF'
e.g., PIN, Password, fingerprint, voiceprint, retinal scan, hardware ID, etc.
310
260
Encrypted data, Encryption Key E, Encrypted UAF
E
Encryption process
320
Encrypted UAF
Equal?
330
No
Yes
Deny Data Access
340
Encrypted Data
350
Decryption process
D
360
Generate Decryption Key D. This key is mathematically related to UAF'. Since UAF and UAF' should be identical the generated D will be same D that was used to generate E.
Non-encrypted data (Plain text)
240
300

FIG. 3

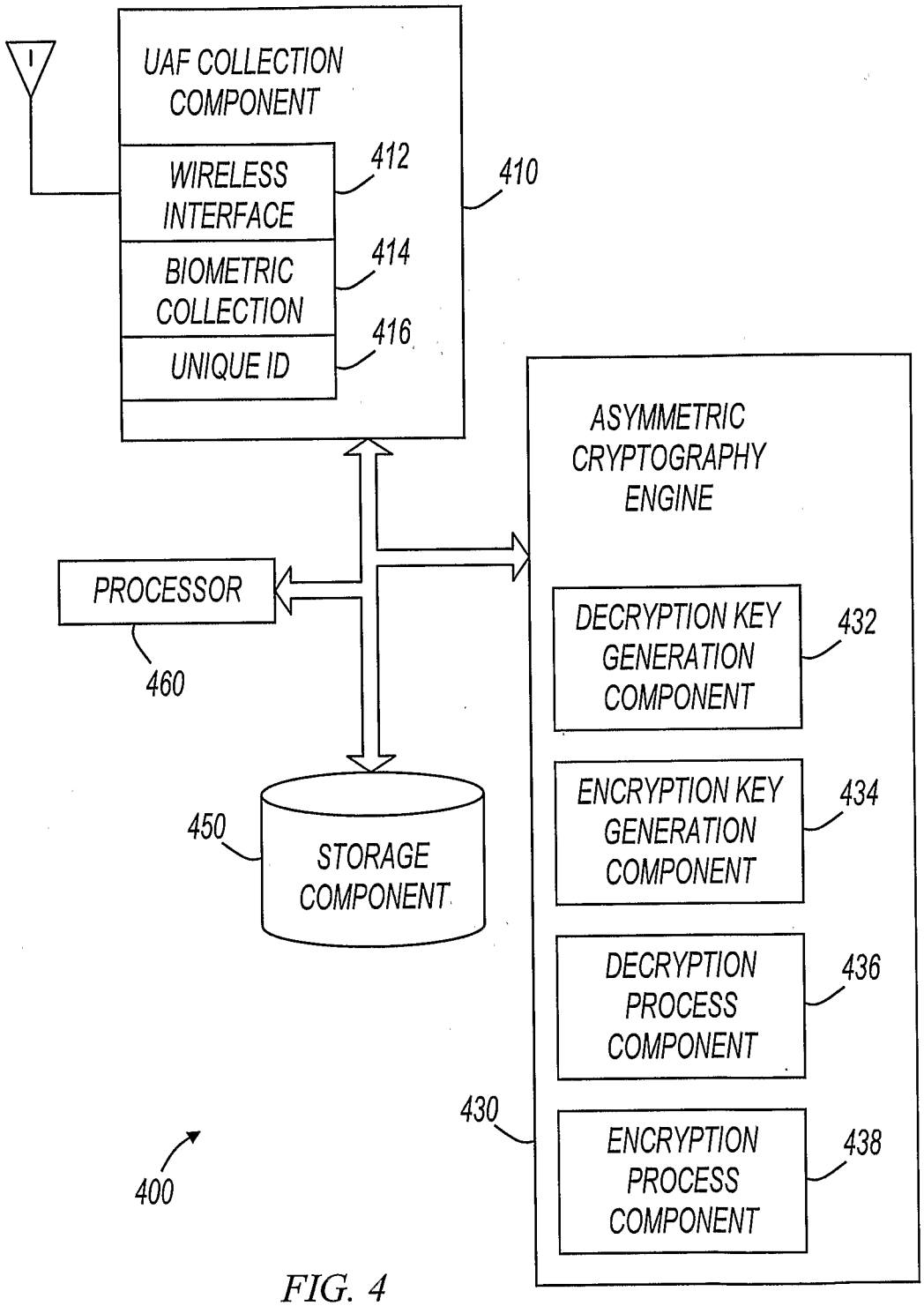

UAF COLLECTION COMPONENT
WIRELESS INTERFACE
412
BIOMETRIC COLLECTION
414
UNIQUE ID
416
410
ASYMMETRIC CRYPTOGRAPHY ENGINE
PROCESSOR
460
DECRYPTION KEY GENERATION COMPONENT
432
ENCRYPTION KEY GENERATION COMPONENT
434
DECRYPTION PROCESS COMPONENT
436
ENCRYPTION PROCESS COMPONENT
438
430
450
STORAGE COMPONENT
400

FIG. 4