



(51) International Patent Classification:

H04L 29/06 (2006.01) H04W 4/80 (2018.01)

H04W 4/70 (2018.01) H04W 12/02 (2009.01)

H04W 12/04 (2021.01) H04W 12/06 (2021.01)

(21) International Application Number:

PCT/EP2021/068238

(22) International Filing Date:

01 July 2021 (01.07.2021)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

20186200.0 16 July 2020 (16.07.2020) EP

(71) Applicant: SIGNIFY HOLDING B.V. [NL/NL]; High Tech Campus 48, 5656 AE Eindhoven (NL).

(72) Inventors: VAN DEURSEN, Ton, Frederik, Petrus; c/o High Tech Campus 7, 5656 AE Eindhoven (NL). KUMAR, Sandeep, Shankaran; c/o High Tech Campus 7, 5656 AE Eindhoven (NL).

(74) Agent: VAN EEUWIJK, Alexander, Henricus, Walterus et al.; Signify Netherlands B.V., High Tech Campus 7, 5656 AE Eindhoven (NL).

(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, IT, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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).

Declarations under Rule 4.17:

— as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))

(54) Title: LOCATION-BASED ENCRYPTION AND DECRYPTION

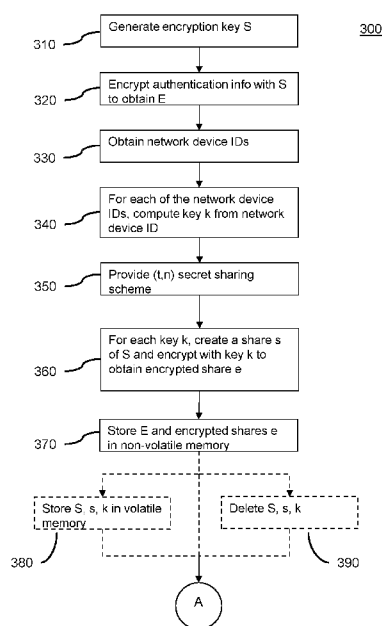


Fig. 3

(57) Abstract: An enrolment method for encrypting authentication information by a wireless device is disclosed. The method comprises generating an encryption key and encrypting the authentication information with the encryption key, to obtain an encrypted authentication information. A plurality of network device identifiers corresponding to a respective plurality of network devices detected within radio range of the wireless device is obtained. From each network device identifier, a key is computed. The method further comprises providing a (t, n) secret sharing scheme. For each computed key, the method comprises creating a share, s, of the encryption key S using the (t,n) secret sharing scheme and encrypting said share s symmetrically with said computed key k to produce an encrypted share, e, to obtain n encrypted shares. The method further comprises storing the encrypted authentication information and the encrypted shares in a non-volatile memory of the wireless device.

Published:

- *with international search report (Art. 21(3))*
- *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

Location-based encryption and decryption

TECHNICAL FIELD

The invention relates to encrypting and decrypting authentication information by a wireless device. More particularly, the invention relates to an enrolment method for encrypting authentication information by a wireless device, a reconstruction method for decrypting authentication information by a wireless device, a method of protecting authentication information by a wireless device, a wireless device for encrypting authentication information, a wireless device for decrypting authentication information, and a transitory or non-transitory computer-readable medium.

10 BACKGROUND

In recent years, research and consumer interest in Internet of Things (IoT) devices has been steadily increasing. The concept of a smart home, with multiple networked devices that can be easily controlled centrally and automated, has become increasingly mainstream. IoT devices typically have wireless interfaces which are used to store key material enabling them to connect to their provisioned wireless network. For example, a wireless speaker or lighting element can use its wireless interface to connect to a home network. Many of these IoT devices connect to their provisioned wireless network, e.g. their home network, using a wireless interface such as a Wi-Fi interface, using authentication information such as the Wi-Fi passphrase associated with their provisioned wireless network. The authentication information is then stored in a non-volatile memory of the IoT device in order to enable the device to reconnect to the network after a reboot or disconnection.

In the example of a Wi-Fi-enabled device, during commissioning or provisioning, the Wi-Fi passphrase is sent to the device through one of a multitude of means, such as by putting the device in Access Point mode, by transfer via Bluetooth or Bluetooth Low Energy (BLE) or the like, or through the use of a covert channel. The device stores the Wi-Fi passphrase in a non-volatile memory for future use so that the device can reuse the Wi-Fi passphrase for subsequent reconnections, for example after a power reset or connection loss, without having to be re-provisioned. Many IoT devices use low-cost Wi-Fi systems on chip (SoCs) without any means to secure the passphrase in storage. The passphrase is often

stored in non-volatile memory, such as flash memory. In some cases, the security features that are present in a low-cost SoC can be easily bypassed.

If the device is broken, returned, sold or stolen, the authentication information, such as the Wi-Fi passphrase, is often still stored in the memory of the device. In many cases, the network's authentication information has not changed, meaning that the authentication information stored on the device can be salvaged and used to gain access to the network where the device was previously commissioned. That is, an attacker can extract the Wi-Fi passphrase from the non-volatile memory of the device and gain access to a secure network and attack other devices of value on the network. Therefore, old devices pose a threat to a network if the authentication information is accessible after disposal, including theft, of the device.

In addition, new security best-practices and regulations demand that credentials and security-sensitive data that are used by the device are stored securely on the device. There is therefore a need to protect authentication information on IoT devices.

US 2019/253243A1 discloses preparation and distribution of keys to be applied for authentication reasons in an Internet of Things (IoT) configuration in order to allow secure communication between a host device and the IoT device.

SUMMARY

It would be advantageous to have a method of encrypting and decrypting authentication information which allows the wireless device to successfully access the authentication information when necessary but which protects the authentication information from attackers, especially after a disposal or theft of the wireless device. An enrolment method, a reconstruction method, a wireless device for encrypting authentication information and a wireless device for decrypting authentication information are set out herein and are claimed that aim to address these and other concerns.

The presently disclosed subject matter includes an enrolment method for encrypting authentication information, a reconstruction method for decrypting authentication information, a method for protecting authentication information, a wireless device for encrypting authentication information, a wireless device for decrypting authentication information and a computer-readable medium.

The enrolment method for encrypting authentication information comprises generating an encryption key *S* and encrypting authentication information with the generated encryption key, to obtain an encrypted authentication information, *E*. For example a random

symmetric encryption key may be generated and used to encrypt the authentication information. The enrolment method further comprises obtaining a plurality of network device identifiers corresponding to a respective plurality of network devices detected within radio range of the wireless device. For each of the obtained plurality of network device identifiers, the enrolment method comprises computing a key from the network device identifier. A (t,n) secret sharing scheme is provided, in which n represents the number of computed keys and t represents a threshold number of shares. The secret sharing scheme is used to divide the encryption key S into a number of shares depending on the number of network device identifiers obtained. For each computed key, a share s of the encryption key S is created and then encrypted with the computed key using a symmetric encryption algorithm, to obtain an encrypted share, e . The encrypted authentication information E and the encrypted shares e are stored in the non-volatile memory of the wireless device.

The reconstruction method for decrypting authentication information comprises obtaining, from a non-volatile memory of a wireless device, an encrypted authentication information E , the encrypting authentication information being authentication information encrypted with an encryption key S , and a plurality of encrypted shares e , each encrypted share being a share of the encryption key S encrypted with a respective key k . The reconstruction method further comprises obtaining a plurality of network device identifiers corresponding to a respective plurality of network devices detected within radio range of the wireless device. For each of at least a subset of the obtained plurality of network device identifiers, the method comprises computing a key k from the network device identifier and performing a decryption of at least one of the plurality of encrypted shares e using the computed key. If the decryption of an encrypted share e successfully decrypts the encrypted share to obtain a decrypted share s , the decrypted share is stored in a memory of the wireless device. The decrypted share may be stored in a volatile memory or in a non-volatile memory of the wireless device. By repeating the operations of computing a key and performing a decryption of an encrypted key for at least a subset of the network device identifiers, a plurality of decrypted shares may be obtained. The reconstruction further comprises reconstructing the encryption key S using the decrypted shares s , and decrypting the encrypted authentication information E using the reconstructed encryption key S to recover the authentication information.

A method of protecting authentication information is further provided, comprising the enrolment method and the reconstruction method.

In an environment with a large number of network devices, such as access points, stations, beacons and the like, the encryption key S may be divided into a larger number of shares than in an environment with fewer such devices. The use of a (t,n) secret sharing scheme in which a threshold number t of shares are needed to reconstruct the encryption key S allows for the encryption key S to be reconstructed even if some of the network devices are not detected or if some of the network device identifiers have changed at the time of a future reconstruction. Moreover, the network device identifiers of network devices within radio range of the wireless device are unlikely to be identified if the wireless device is removed or disposed of before an attacker attempts to obtain the authentication information. An attacker would also need to obtain a sufficient number (e.g. the threshold number) of network device identifiers in order to decrypt enough encrypted shares to reconstruct the encryption key S . If the wireless device is removed from its environment, the decryption of the authentication information becomes substantially more difficult, thereby protecting the authentication information and the network to which it allows access in the event that a wireless device is stolen, sold or otherwise disposed of. This prevents unauthorized access to the network based on information obtained from a stolen or discarded wireless device. During the reconstruction method, it is not required for the wireless device to be aware of the threshold number t of shares in the secret sharing scheme in all embodiments. In some embodiments, for example, the wireless device may attempt to reconstruct the encryption key S each time an encrypted share is decrypted.

In an embodiment, encrypting each share s symmetrically with the respective computed key k comprises generating a corresponding authentication tag and storing the corresponding authentication tag. The use of an authentication tag enables the wireless device to authenticate the decryption of the encrypted share during the reconstruction method. Since each computed key is used to attempt to decrypt an encrypted share, e.g. a single computed key is used in attempted decryptions of possibly multiple encrypted shares, it is beneficial to provide a simple and straightforward means to authenticate the decryption.

In an embodiment, the obtained plurality of network device identifiers comprises at least one of:

- WiFi access point identifiers of WiFi access points detected by a WiFi receiver of the wireless device, the WiFi access point identifiers preferably comprising at least one of a basic service set identifier (BSSID) of a WiFi access point, a service set identifier (SSID) of the WiFi access point, a supported rates indication of the WiFi access point and a country information of the WiFi access point; and

- a MAC address of a station sending data to an access point.

The above identifiers provide information identifying a network device which is unique or near-unique to the network device and remains static. This enables the same key to be computed during reconstruction as was computed during the encryption, as the network device identifier is static and therefore is unlikely to have changed.

In an embodiment, obtaining the plurality of network device identifiers comprises detecting network device identifiers with a received signal strength greater than a threshold. Using network device identifiers of network devices with at least a threshold signal strength prevents identifiers of devices with poor signal strength from being considered and used in the encryption method and corresponding reconstruction method. Devices with poor signal strength pose a risk of not being identified in the future, for example during reconstruction. Ensuring that the identifiers used in the encryption method correspond to network devices with sufficiently strong signal strength improves the likelihood of the same network devices being detected during the reconstruction method when the encryption key is being reconstructed.

In an embodiment, obtaining the plurality of network device identifiers comprises at least one of scanning wireless channels such as WiFi channels, listening to wireless traffic and sending probe requests and receiving probe responses. These options provide a variety of means for obtaining the plurality of network device identifiers, which may be based on the circumstances of the wireless device. In some cases, for example, it may be advantageous to constantly monitor wireless traffic whilst in other cases it may be more suitable to periodically or aperiodically obtain network device identifiers. Periodically or sporadically obtaining network device identifiers may prevent unnecessary power and resource consumption associated with unnecessarily monitoring, particularly in environments in which the network devices are unlikely to frequently change. Constant or near-constant monitoring may be advantageous in other cases, such as in environments when the network devices are likely to change more frequently.

In an embodiment, the enrolment method may further comprise obtaining a new network device identifier, generating a new key using the new network device identifier, attempting to decrypt each of the encrypted shares using the new key, and if the new key does not successfully decrypt any of the encrypted shares, e:

- generating a new share s of the encryption key S using a function of the (t,n) secret sharing scheme;

- encrypting the new share s with the new key to obtain a new encrypted share; and

- storing the new encrypted share in the non-volatile memory of the wireless device.

5 Identifying a new network device identifier, in other words identifying a new network device within radio range of the wireless device, and using the new network device identifier to encrypt a new share of the encryption key S , improves the freshness of the encrypted shares and ensures that the encryption key S can be reconstructed during the reconstruction method. In environments where network devices leave the vicinity and/or when new network devices
10 enter the vicinity, it is advantageous to ensure that the encrypted shares can be decrypted with keys computed from network device identifiers of network devices that are still in the vicinity of the wireless device. Adding new encrypted shares encrypted with keys computed from the identifiers of new network devices increases the number of encrypted shares in the non-volatile memory, which ensures that a sufficient number of encrypted shares can be
15 successfully decrypted during the reconstruction method based on the network device identifiers obtained during the reconstruction method.

In an embodiment, the authentication information comprises a WiFi passphrase. Encrypting a WiFi passphrase is beneficial as it prevents unauthorized access to a WiFi network, through which sensitive data and applications may be accessible. As IoT
20 devices such as WiFi-enabled lighting elements and home appliances become increasingly popular, home and office network security becomes an increasing concern. By encrypting the WiFi passphrase as detailed in the enrolment method, unauthorized access to a WiFi network may be avoided.

In an embodiment, the reconstruction method further comprises obtaining,
25 from the non-volatile memory of the wireless device, a threshold number t denoting a threshold number of shares for a (t, n) secret sharing scheme, and wherein the number of network identifiers in the subset of the obtained plurality of network device identifiers is equal to or greater than the threshold number t . When the threshold number t is available to the wireless device during the reconstruction method, the wireless device can continue to
30 decrypt encrypted shares of the encryption key S until at least the threshold number of decrypted shares are obtained. In this way, attempting to reconstruct the encryption key S with too few decrypted shares is avoided, which prevents unnecessary resource and power consumption.

In an embodiment, the method of protecting authentication information further comprises detecting a refresh event and repeating the enrolment method. The refresh event comprises at least one of:

- an expiry of a rekeying timer, the rekeying timer being an indication of freshness of the encrypted shares;
- a change in the network device identifiers detected within radio range of the wireless device, the change exceeding a predetermined threshold; and
- a number of times the authentication information has been recovered since the enrolment phase.

A refresh event may be used to ensure that the encrypted shares remain fresh, and to ensure that the wireless device is able to successfully reconstruct the encryption key and therefore access the authentication information even in an environment in which the network devices change frequently. A rekeying timer alleviates the need to constantly monitor the network devices, which may be advantageous in a low-power environment or an environment in which network devices are not prone to leaving and entering frequently.

In some IoT-connected (e.g. 'smart') environments, sensitive information is frequently protected using multi-party computation, in which sensitive information is distributed among multiple parties. Restoring the sensitive information then requires the cooperation and computation of at least some number of these multiple parties. However, it is not always practical to require the use of multiple parties to decrypt information. Particularly in the context of home or work networks, there may not be a large number of parties available to take part in a multi-party computation in this manner. Particularly if the sensitive information is authentication information, it may be not be feasible to communicate with other devices without being already connected to the other devices, for example over a network. If the sensitive information is required in order to connect to the network and therefore to the other devices, the parties involved in the multi-party computation approach may not be accessible.

Requiring such an interaction from multiple devices may not be a realistic requirement in many applications, such as in a home network with a small pool of connected or accessible devices, or in a remote setting. It is therefore advantageous to securely protect authentication information without requiring computational input from multiple external devices.

Aspects of the presently disclosed subject matter include a computer implemented method.

Executable code for an embodiment of the method may be stored on a computer program product. Examples of computer program products include memory devices, optical storage devices, integrated circuits, servers, online software, etc. Preferably, the computer program product comprises non-transitory program code stored on a computer readable medium for performing an embodiment of the method when said program product is executed on a computer.

The devices of claims 12 and/or 13 may exist as a single device or as a plurality of devices which are communicatively coupled, such as in a network. One or more components of the devices of claims 12 and/or 13 may be provided within a single device whilst other components are provided in one or more further devices communicatively coupled to the single device.

In an embodiment, the computer program comprises computer program code adapted to perform all or part of the steps of an embodiment of the method when the computer program is run on a computer. Preferably, the computer program is embodied on a computer readable medium.

Another aspect of the presently disclosed subject matter provides a method of making the computer program available for downloading. This aspect is used when the computer program is uploaded into, e.g., Apple's App Store, Google's Play Store, or Microsoft's Windows Store, and when the computer program is available for downloading from such a store.

BRIEF DESCRIPTIONS OF DRAWINGS

These and other aspects of the invention are apparent from and will be elucidated with reference to the embodiments described hereinafter. In the drawings, Fig. 1 schematically shows an example of an embodiment of a wireless device and a plurality of network devices within a radio range of the wireless device;

Fig. 2 schematically shows an example of an embodiment of a wireless device and a plurality of network devices within a radio range of the wireless device;

Fig. 3 schematically shows an example of an embodiment of an enrolment method for encrypting authentication information;

Fig. 4 schematically shows an example of an embodiment of an enrolment method for encrypting authentication information;

Fig. 5 schematically shows an example of an embodiment of a reconstruction method for decrypting authentication information;

Fig. 6 schematically shows an example of an embodiment of a method for protecting authentication information;

Fig. 7 schematically shows an example of an embodiment of a method for protecting authentication information;

5 Fig. 8a schematically shows an example of an embodiment of a wireless device for encrypting authentication information;

Fig. 8b schematically shows an example of an embodiment of a wireless device for decrypting authentication information;

10 Fig. 8c schematically shows an example of an embodiment of a lighting element for encrypting and/or decrypting authentication information;

Fig. 9 schematically shows a computer readable medium having a writable part comprising a computer program according to an embodiment; and

Fig. 10 schematically shows a representation of a processor system according to an embodiment.

15 It should be noted that items which have the same reference numbers in different Figures, have the same structural features and the same functions, or are the same signals. Where the function and/or structure of such an item has been explained, there is no necessity for repeated explanation thereof in the detailed description.

20 **Reference signs list**

The following list of references signs is provided for facilitating the interpretation of the drawings and shall not be construed as limiting the claims.

	10	radio range of a wireless device
25	100	a wireless device
	100-b	a wireless device
	110	processor circuitry
	110-b	processor circuitry
	120	memory
30	120-b	memory
	122	non-volatile memory
	122-b	non-volatile memory
	124	volatile memory
	124-b	volatile memory

	130	wireless communication interface
	130-b	wireless communication interface
	132	wireless receiver
	132-b	wireless receiver
5	134	wireless transmitter
	134-b	wireless transmitter
	200	access point(s)
	250	association(s)
	300	station(s)
10	900	a computer readable medium
	910	a writable part
	920	a computer program
	1010	an integrated circuit
	1020	a processing unit
15	1022	a memory
	1024	a dedicated integrated circuit
	1026	a communication element
	1030	an interconnect
	1040	a processor system

20

DESCRIPTION OF EMBODIMENTS

While the presently disclosed subject matter is susceptible of embodiment in many different forms, there are shown in the drawings and will herein be described in detail one or more specific embodiments, with the understanding that the present disclosure is to be
 25 considered as exemplary of the principles of the presently disclosed subject matter and not intended to limit it to the specific embodiments shown and described.

In the following, for the sake of understanding, elements of embodiments are described in operation. However, it will be apparent that the respective elements are arranged to perform the functions being described as performed by them.

30 Further, the presently disclosed subject matter is not limited to the embodiments, as features described herein or recited in mutually different dependent claims may be combined.

In order to overcome the disadvantages described above, methods and devices are described herein which use information obtained from the vicinity of the wireless device

in order to securely store authentication information. Authentication information used to permit the wireless device to access a network, such as a wireless local area network (WLAN), may be encrypted using a generated encryption key. The encryption key may then be divided into a plurality of shares, based on a secret-sharing scheme. The number of shares
5 into which the encryption is divided may be based on the number of network devices detected. Identification information of network devices within radio range of the wireless device may be used to encrypt the shares of the encryption key. The encryption of authentication information may be referred to as the enrolment phase. When the wireless device is, e.g. rebooted or restarted, and needs to reconnect to the network, the identification
10 information of the network devices within radio range of the wireless device can be obtained and used to decrypt the encrypted shares of the encryption key. The decryption of the authentication information may be referred to as the reconstruction phase. In many embodiments, the same wireless device performs both phases, although this is not always the case. In some embodiments, for example when replacing the wireless device with a new
15 device (for example following damage to the wireless device), the saved information, e.g. the encrypted authentication information E and the encrypted shares e, may be transferred to the non-volatile memory of the new device and the step of provisioning or commissioning may be bypassed.

For wireless devices in a typically fixed environment, such as a Wi-Fi-enabled
20 device in a home or work network such as a smart network, use of information obtained from the vicinity of the device in the encryption of sensitive information such as authentication information offers several security advantages. If the device is removed from its environment, such as if the device is sold, stolen, broken or otherwise disposed of, reconstructing the authentication information becomes substantially more complicated and
25 difficult. However, these difficulties are not present when the device remains in its fixed environment, meaning that the complexities in decrypting the authentication information do not hinder the standard operation of the wireless device.

With reference to Figs. 1 and 2, overviews of two example environments in which the wireless device may be used are described, highlighting various types of network
30 device identification information used to encrypt and decrypt the encryption key. The methods of encrypting, decrypting and protecting authentication information will be described in detail with reference to Figs. 3 to 7, whilst the wireless device will be described in detail with reference to Figs. 8a-8c.

Fig. 1 schematically shows an example of an embodiment of a wireless device and a plurality of network devices within a radio range of the wireless device.

As shown in Fig. 1, a wireless device 100 is provided, configured to connect to a wireless network provided by an access point 200-1. The access point 200-1 may be a router, for example of a home or office WLAN network, and may provide a Wi-Fi network. The wireless device 100 may be enrolled in the wireless network by providing authentication information, such as a Wi-Fi passphrase, a password or the like. The access point 200-1 may be an access point of a wireless local area network (WLAN), such as a home network, office network or the like, and may be referred to as a beacon. Although a Wi-Fi access point is referred to in the examples provided herein, it is to be understood that this is not a limitation, and other communication standards such as Bluetooth, Zigbee, and the like may be equivalently used.

The wireless device 100 may detect a plurality of network devices 200, 300 within radio range 10 of the wireless device 100. The plurality of network devices may comprise at least one access point 200 and/or at least one station 300 sending data to an access point 200.

In the embodiment shown in Fig. 1, the wireless device 100 may use authentication information in the form of a Wi-Fi passphrase to connect to the network provided by access point 200-1. The Wi-Fi passphrase should be stored in the non-volatile memory of the wireless device 100 in order to ensure that, after a restart or reboot of the wireless device 100, the wireless device 100 is able to reconnect to the wireless network without requiring re-enrolment, although in a secured manner to prevent attackers from accessing the Wi-Fi passphrase directly. For example, the Wi-Fi passphrase may be encrypted before being stored in the non-volatile memory of the device.

Fig. 2 schematically shows an example of an embodiment of a wireless device and a plurality of network devices within a radio range of the wireless device.

The embodiment depicted in Fig. 2 is similar to that of Fig. 1, but further illustrates associations 250 between stations 300 and access points 200. Such associations, indicated by arrows, indicate a relationship between a station and an access point in which the station sends data to the access point.

The wireless device 100 may obtain identifiers of the stations sending data to one or more access points, for example by monitoring or listening to wireless traffic. The identifier of a station 300 may be, for example, a media access control (MAC) address of the station 300, but is not limited thereto.

In some situations, the wireless device 100 may be an environment with relatively few access points 200, for example when the wireless device 100 is used in a building in a remote area. In such a situation, the number of access points 200 detected within radio range of the wireless device 100 may provide relatively few keys to use to protect shares of the encryption key. The identifiers of the stations 300 sending data to the detected access points 200 may then be used, either in addition to the identifiers of the access points or as an alternative to the identifiers of the access points, in the same manner as described with regard to Fig. 1 and detailed below with reference to Figs. 3 to 7. The stations 300 may be, for example, mobile phones, laptops, tablets or any wireless device that is sending data to an access point 200. Stations 300 may be less constant than access points 200. The choice of whether to use only station identifiers, only access point identifiers or a combination of station identifiers and access point identifiers is dependent on the situation. For example, in a public or highly trafficked network such as a university campus where the stations 300 sending data to an access point tend to fluctuate, the use of station identifiers may be less reliable, as students typically carry mobile phones and laptops which send data to access points, but cannot be relied upon to be present in the event that the wireless device is rebooted. Conversely, in a home network where the stations 300 that connect to the access point 200 are relatively constant, the use of station identifiers may increase the number of shares into which the encryption key may be divided without a significant impact on the reconstructability of the encryption key.

Enrolment phase

Fig. 3 schematically shows an example of an embodiment of an enrolment method for encrypting authentication information.

In operation 310, the wireless device 100 may generate an encryption key, S. The encryption key may be generated randomly, or may be based on a seed value, such as a system parameter or current time. The encryption key S may be a symmetric key.

In operation 320, the wireless device 100 may be configured to encrypt the authentication information, such as the Wi-Fi passphrase, with the generated encryption key S to obtain encrypted authentication information E.

In operation 330, the wireless device 100 may be further configured to obtain network device identifiers of the network devices, such as access points 200 and stations 300, within radio range of the wireless device 100. As described above with reference to Figs. 1 and 2, the wireless device 100 may be enrolled in the network provided by access point 200-

1, and the wireless device 100 may detect additional access points 200 within radio range of the wireless device 100, including access points 200 other than the access point 200-1 providing the network in which the wireless device 100 is enrolled. By detecting these additional access points 200, the wireless device 100 may obtain identifiers of the access
5 points. The network device identifiers may comprise access point identifiers and/or station identifiers of stations sending data to an access point, as described with reference to Figs. 1 and 2. The identifiers of the access points may comprise one or more of a basic service set identifier (BSSID), a service set identifier (SSID), a supported rates indication, a country information, or any of the static parameters of the Wi-Fi (IEEE 802.11) standard or any static
10 vendor-specific parameter. In other words, the identifier of an access point should be a static parameter of the access point which can be used to identify the access point. The identifier of a station may comprise, for example, a MAC address of the station.

In some embodiments, obtaining the network device identifiers may comprise detecting a plurality of network devices 200 whose signal strength exceeds a threshold. In
15 other words, the network device identifiers of network devices having a sufficiently high signal strength may be obtained. The threshold may be a predetermined threshold value of signal strength, such as a received signal strength indicator (RSSI). The threshold may be a relative threshold, such as the top-K network devices, indicating the K network devices with the best signal strength or the like. The RSSI may be used to indicate the signal strength of
20 each network device.

The network device identifiers may be obtained by, for example, scanning wireless channels such as Wi-Fi channels, listening to wireless traffic, and/or sending probe requests and receiving probe responses.

In operation 340, the wireless device 100 may be configured to compute a key
25 k from the each of the obtained identifiers. The keys k may be deterministically computed. That is, for each network device detected within radio range of the wireless device 100, the wireless device 100 may compute a key using the identifier of that network device. Thus, if the identifiers of n network devices are obtained, n keys are computed by the wireless device 100.

30 In operation 350, the wireless device 100 may provide or employ a (t,n) secret sharing scheme, also known as a threshold secret sharing scheme. A (t,n) secret sharing scheme is a scheme which distributes a secret into a number (n) of shares (s) in such a way as to ensure that if fewer than a threshold number (t) of shares (s) is obtained, the secret cannot be reconstructed. However, if at least the threshold number (t) of shares is available, the

secret can be reconstructed. In the present embodiment, the encryption key S may be distributed into n shares – that is, the number of shares into which the encryption key S is distributed may be equal to the number of keys computed, and therefore the number of obtained identifiers of the detected network devices.

5 The (t,n) secret sharing scheme may be one of any known such secret sharing scheme, such as a Shamir secret sharing scheme, Blakely secret sharing scheme, a sharing scheme based on Chinese remainder theorem or the like. The (t,n) secret sharing scheme may use a function to construct shares from the encryption key S .

10 The value of the threshold number (t) of shares that would enable reconstruction of the encryption key S may be predetermined as an absolute value, or may be determined from the number n of obtained network device identifiers. For example, the value of the threshold number t may be determined as $n/2$, $n/3$, $n-5$, $n-10$, or similar. In some embodiments, the value of the threshold number t may have a condition to ensure that the value of the threshold number t is not less than 2. Ensuring that the value of the threshold
15 number t is not less than 2 ensures that the encryption key S cannot be reconstructed from a single share. In some embodiments, the threshold number (t) may be stored in the non-volatile memory of the wireless device 100.

 In operation 360, the wireless device 100 may divide the encryption key into a plurality of shares s , according to the provided (t,n) secret sharing scheme. The wireless
20 device 100 may then encrypt each share s of the encryption key S using a computed key k to obtain an encrypted share, e . In other words, each computed key k is used to encrypt a respective share s , to obtain an encrypted share e . Each share s is encrypted symmetrically, such that a single key is required to encrypt or decrypt the share. Thus, if n network device identifiers are obtained, n keys k are computed, the encryption key S is distributed into n
25 shares s , which are encrypted with the computed keys to obtain n encrypted shares e . In some embodiments, encrypting each share s comprises generating a corresponding authentication tag. The authentication tag may then be stored, for example in the non-volatile memory of the wireless device 100.

 The wireless device 100 may then be configured to store the encrypted
30 authentication information, E , as well as the encrypted shares e in the non-volatile memory of the wireless device 100. In some embodiments, the encryption key S , the shares s and the computed keys k may be stored in a volatile memory of the wireless device, such that when the wireless device 100 is rebooted or restarted, the encryption key S , shares s and computed

keys k are deleted. In some embodiments, the encryption key S , the shares s and the computed keys k may be permanently deleted directly.

Optionally, the wireless device 100 may either store the encryption key S , the shares s and the computed keys k in a volatile memory of the wireless device 100, as shown in operation 380, or delete the encryption key S , the shares s and the computed keys k , as shown in operation 390. By so doing, these values are not available if the wireless device 100 is rebooted.

Optionally, the method may continue to the method illustrated in Fig. 4, as indicated by the letter 'A'.

10 In other words, the enrolment phase may be performed as follows:

```

S = GenerateKey();
E = Encrypt(S, authentication_info);
A = AuthTagGen(S, authentication_info); // optional
15 networkIDs[] = GetNetworkIDs();
s[] = ComputeShares(size(networkIDs));
for (int i = 0; i < size(networkIDs); i++)
    k[i] = GenerateKey(networkIDs[i])
e[i] = Encrypt(s[i], k[i])
20 a[i] = AuthTagGen(s[i], k[i]) // optional
Store(E, e); // and optionally Store(A, a)

```

The Encrypt() function may comprise an authenticated encryption algorithm, such as AES-GCM-256(), which may comprise encrypting a quantity (such as the encryption key S or a share s) and generating an authentication tag. In some embodiments, the encryption operation may be followed by a separate authentication tag generation operation, AuthTagGen, such as a message authentication code (MAC) generation operation, checksum function or the like, to obtain an authentication tag corresponding to the encrypted quantity, such as the encryption key and/or the shares. Depending on the encryption scheme used, for each encrypted share, an authentication tag may also be stored in non-volatile memory. In some embodiments, an authentication code or tag may be appended to the share s (e.g. the plaintext) before encryption. In these cases, it is not necessary to separately store authentication tags as each encrypted share e is a ciphertext of the share s and the corresponding authentication tag.

Fig. 4 schematically shows an example of an embodiment of an enrolment method for encrypting authentication information. In particular, the method of Fig. 4 may follow the method of Fig. 3. The additional operations of the method of Fig. 4 improves the effectiveness of the encryption method, which may be hampered by changes in the network devices within a radio range of the wireless device 100. For example, when an access point is added, removed or when the identifier of an access point is changed, for example after an update or reconfiguration, keys generated from identifiers of the new or changed access points may not successfully decrypt encrypted shares. Moreover, stations 300 sending data to access points 200 have a high likelihood of being removed from the vicinity of the wireless device 100 and there is a high likelihood of new stations entering the vicinity of the wireless device 100 and sending data to access points in the vicinity. By adapting to changes in the network devices within the vicinity of the wireless device 100, e.g. within radio range of the wireless device 100, unnecessary re-enrolment, or re-commissioning can be avoided.

In operation 410, the wireless device 100 obtains a new network device identifier. The new network device identifier may be obtained by, for example, scanning wireless channels such as Wi-Fi channels, listening to wireless traffic, and/or sending probe requests and receiving probe responses. In some embodiments, the wireless device 100 obtains the new network device identifier as a result of periodically monitoring for changes, for example by periodically scanning wireless channels, periodically listening to wireless traffic, and/or periodically sending probe requests and receiving probe responses.

In operation 420, the wireless device 100 computes a new key k from the obtained new network identifier. The new key k may be symmetrically generated in the same manner as the keys generated in operation 340.

In operation 430, the wireless device 100 performs a decryption of the encrypted shares e stored in the non-volatile memory of the wireless device 100. In some cases, for example, an access point previously visible has been removed or hidden temporarily, and upon its re-introduction is detected as a new access point. In such cases, the access point identifier may have been previously used to encrypt a share s of the encryption key S . This is shown to be the case if the key generated from the new network identifier successfully decrypts one of the stored encrypted shares e .

In operation 440, the wireless device 100 determines if the new key successfully decrypts any encrypted share e stored in the non-volatile memory of the wireless device 100. In some embodiments, the encrypted shares e stored in the non-volatile memory

of the wireless device 100 have associated authentication tags which enable the decryption to be authenticated.

If the new key does not decrypt any of the stored encrypted shares e , the method proceeds to operation 450, in which the wireless device 100 generates a new share s of the encryption key S using a function associated with the (t,n) secret sharing scheme. The new share s may be generated using at least t existing shares, for example using a polynomial function corresponding to the (t,n) secret sharing scheme.

In operation 460, the wireless device 100 encrypts the new share s with the new key to obtain a new encrypted share e . The encryption of the new share s may be performed in the same manner as described in operation 360.

In operation 470, the wireless device 100 stores the new encrypted share in the non-volatile memory of the wireless device 100. The new share s and the new key k may be stored in volatile memory of the device, or the new share s and the new key k may be deleted.

The method of Fig. 4 may be repeated periodically, or when a change in network devices is detected, for example.

Reconstruction phase

When the wireless device 100 needs to reconnect to the network provided by access point 200-1, for example after a reboot, the wireless device 100 may be configured to decrypt at least a threshold number of encrypted shares e to obtain shares s , and to reconstruct the encryption key S using the obtained decrypted shares s , as described presently. The wireless device 100 may then use the reconstructed encryption key S to decrypt the encrypted authentication information E to obtain the authentication information. This is described in detail with reference to Fig. 5.

Fig. 5 schematically shows an example of an embodiment of a reconstruction method for decrypting authentication information.

In operation 510, the wireless device 100 obtains the encrypted authentication information E and the encrypted shares e from the non-volatile memory of the wireless device 100.

In operation 520, the wireless device 100 obtains a plurality of network device identifiers corresponding to a respective plurality of network devices 200, 300 detected within radio range 10 of the wireless device 100. The network device identifiers may be obtained in a similar manner as that used in the enrolment phase described above. Following

the examples depicted in Figs. 1 and 2, the network devices may comprise access points 200 and/or stations 300 sending data to an access point 200.

In operation 530, the wireless device 100 computes a key k from each of at least a subset of the obtained network device identifiers. In some embodiments, the wireless device 100 computes a key from a subset of the obtained network device identifiers. That is, it may not be necessary to compute a key from every obtained network device identifier, as will be elucidated presently. Preferably, a subset comprises at least two network device identifiers. In some embodiments, the number of network device identifiers in the at least a subset of network device identifiers may be greater than or equal to the threshold number t of the (t,n) secret-sharing scheme used in the enrolment phase. In some embodiments, network device identifiers may be added to the at least a subset of the network device identifiers until the encryption key S can be reconstructed, e.g. until a sufficient number of encrypted shares are decrypted in order to allow the encryption key S to be reconstructed.

Once a key has been computed from a network device identifier, the wireless device 100 performs a decryption of an encrypted share e , as indicated by operation 540. The decryption may be authenticated, for example through the use of an authentication tag generated when the encrypted share was encrypted. In this case, the wireless device 100 may further obtain the authentication tag corresponding to the encrypted share from the non-volatile memory of the wireless device 100.

If the decryption is successful, a decrypted share s is obtained, and the decrypted share s may be stored in a memory of the wireless device 100 as indicated by operation 550. Preferably, the decrypted share s is stored in the volatile memory of the wireless device 100. If the decryption is not successful, the computed key may be used to perform a decryption of a different encrypted share e , until the wireless device 100 successfully decrypts one of the encrypted shares e , or until the wireless device has attempted to decrypt all of the encrypted shares using the generated key without success.

The computation of a key from a network device identifier, the subsequent performance of the decryption of the encrypted share(s) e and the storing of a decrypted share s may be repeated for each obtained network device identifier. In some embodiments, these steps are repeated until at least a threshold number (t) of shares have been successfully decrypted. This may be determined by retrieving or determining a threshold number of shares based on the (t,n) secret sharing scheme employed, or by attempting to reconstruct the authentication key S each time a decrypted share s is stored in the memory until the reconstruction is successful. The reconstruction may be considered successful, for example if

the result of the reconstruction successfully decrypts the encrypted authentication information E.

In some embodiments, operations 530 to 550 are performed until the threshold number of shares have been successfully decrypted, as outlined below. Although steps 'a' and 'b' are expressed in a sequential manner, it is to be understood that these operations may be performed concurrently. For example, the wireless device 100 may continue scanning, listening or detecting network device identifiers whilst already performing the operations of step 'b' for a network device identifier already obtained, until a sufficient number of decrypted shares are obtained.

10

a. obtain plurality of network device identifiers (IDs);

b. while number of stored decrypted shares $< t$:

b1. select network device ID of the plurality of network device IDs

b2. compute key k from network device ID;

15

b3. perform decryption of encrypted share(s);

b4. if successful:

store decrypted share

In order to determine if an encrypted share e has been successfully decrypted, an authentication tag corresponding to the encrypted share e may be retrieved, for example from the non-volatile memory of the wireless device 100, and used to authenticate the decryption. However, this is merely exemplary. Any other known means of determining whether a decryption is successful may be additionally or alternatively employed. As an alternative, the wireless device 100 may use a computed key to obtain decryption results from each encrypted share.

Once a sufficient number of shares have been decrypted and are stored in the memory of the wireless device 100, for example at least a threshold number (t) of shares, or once each of the computed keys have been used to attempt to decrypt all of the stored encrypted shares, the wireless device 100 may reconstruct the encryption key S using the decrypted shares s , as indicated in operation 560.

In operation 570, the wireless device 100 decrypts the encrypted authentication information E with the reconstructed encryption key S to obtain the authentication information. Using the obtained authentication information, the wireless device 100 may reconnect to the network.

Although the flowchart of method 500 illustrates operations 520 to 550 in a sequential manner, it is to be understood that these operations may be performed at least partially simultaneously, concurrently or overlappingly. For example, once a first network device identifier is obtained, the wireless device 100 may proceed to computing a key from the obtained network device identifier, attempt to decrypt the encrypted shares etc. whilst continuing to obtain further network device identifiers, for example by scanning wireless channels in the background. In some embodiments, the wireless device 100 may continue to obtain network device identifiers until a sufficient number of decrypted shares has been obtained.

10 **Fig. 6** schematically shows an example of an embodiment of a method 600 for protecting authentication information.

The method 600 for protecting authentication information may comprise a combination of the methods of Figs. 3 and 5, and optionally Fig. 4.

15 The method 600 comprises an enrolment phase comprising method 300 and a reconstruction phase comprising method 500. The enrolment phase may further comprise method 400.

20 In some embodiments, both the enrolment phase 300 and the reconstruction phase 500 may be performed by the same wireless device 100. In some embodiments, however, the enrolment phase 300 may be performed by a first wireless device, whilst the reconstruction phase 500 may be performed by a second wireless device. For example, the encrypted authentication information E and the encrypted shares may be stored on a removable non-volatile memory by the first wireless device. The removable non-volatile memory may be provided to the second wireless device prior to the second wireless device performing the reconstruction phase 500. This may be advantageous when the first wireless device is being replaced by the second wireless device, for example in the case of an upgrade or replacement of a damaged or broken first wireless device.

25 **Fig. 7** schematically shows an example of an embodiment of a method 700 for protecting authentication information.

30 The method 700 of Fig. 7 may be implemented on the same wireless device 100 to improve the freshness of the encrypted shares, which reduces the risk of having too few decrypted shares when reconstructing the encryption key S.

The method 700 comprises the enrolment phase 300 as described above, and may optionally also include method 400. The method 700 may further comprise operation 710, in which the wireless device 100 may detect a refresh event. Upon detection of the

refresh event, the method 700 may proceed to operation 500 to reconstruct the encryption key S. In operation 720, the wireless device 100 may repeat the encryption phase 300.

In some embodiments, the refresh event may comprise a rekeying timer. A rekeying timer may be used as an indication of the freshness of the encrypted shares. For example, the rekeying timer may be started during or after the enrolment phase 300. In some examples, the rekeying timer may be restarted when a new encrypted share is stored, such as during or after method 400. The refresh event may then comprise an expiry of the rekeying timer.

In some embodiments, the refresh event may correspond to a change in the network devices detected within radio range of the wireless device 100. The wireless device 100 may be configured to detect a change in the network device identifiers detected within radio range of the wireless device 100. For example, the wireless device 100 may be configured to monitor the network device identifiers of network devices detected within radio range of the wireless device 100. The refresh event may comprise a change in the network device identifiers. In some embodiments, the refresh event corresponds to a threshold change in network device identifiers detected. For example, the refresh event may specify a number of network device identifiers that are removed or added. That is, the refresh event may correspond to a change in at least a predetermined number of network devices within radio range of the wireless device 100. This type of refresh event reduces a risk of being unable to reconstruct the encryption key S. For example, when attempting to reconstruct the authentication information, if there are fewer than the threshold number t of network devices available whose identifiers were used in the encryption of the shares of the encryption key S, the wireless device 100 may not be able to reconstruct the encryption key S. By repeating the encryption phase when there is a change in the network device identifiers of the network devices detected within radio range of the wireless device 100, there is an increased likelihood that there will be sufficient identifiers available when the wireless device 100 reconstructs the encryption key S.

In some embodiments, the refresh event may correspond to a number of times the authentication information has been recovered since the enrolment phase. For example, the enrolment phase may be repeated each time the authentication information is recovered, or after the authentication information has been recovered a predetermined number of times.

By repeating the enrolment phase 300, a new encryption key is generated, the authentication information is newly encrypted with the new encryption key and the new encryption key is divided into new shares. This improves the freshness of the encrypted

information, which further reduces the risk of the authentication information being accessed by an attacker whilst ensuring that the wireless device 100 can recover the authentication information when necessary.

Fig. 8a schematically shows an example of an embodiment of a wireless device 100 for encrypting authentication information. The wireless device 100 shown in Fig. 8a may be configured to perform the enrolment phase as described above. The wireless device 100 comprises processor circuitry 110, a memory 120 and a wireless communication interface 130.

In an embodiment, the wireless communication interface 130 comprises a wireless receiver 132. In some embodiments, the wireless communication interface 130 may further comprise a wireless transmitter 134. In some embodiments, the wireless receiver 132 and the wireless transmitter 134 may be incorporated as a wireless transceiver. In other embodiments, the wireless receiver 132 and the wireless transmitter 134 may be separate components.

In an embodiment, the wireless receiver 132 is configured to obtain a plurality of network device identifiers corresponding to a respective plurality of network devices detected within radio range of the wireless device 100. In some embodiments, the wireless receiver 132 is configured to obtain the plurality of network device identifiers corresponding to the respective plurality of network devices by scanning wireless channels, such as Wi-Fi channels, and receiving identification information broadcasted by network devices, such as access points, beacons, stations and/or the like. In some embodiments, the wireless receiver 132 is configured to obtain the plurality of network device identifiers by listening to wireless traffic. In some embodiments, the wireless transmitter 134 is configured to send one or more probe requests and the wireless receiver 132 is configured to receive one or more probe responses. Information received from network devices within range of the wireless device 100 may comprise identification information identifying the respective network device. The identification information may comprise, for example, a MAC address of a station, a base service set identifier (BSSID), a service set identifier (SSID), an internet protocol (IP) address, and/or any static information identifying a network device and/or unique to a network device.

In some embodiments, the wireless communication interface may be configured to detect network devices within radio range of the wireless device 100 with at least a threshold signal strength. In some embodiments, the wireless communication interface

130 is configured to detect the received signal strength indicator (RSSI) of each network device detected within radio range of the wireless device 100.

The wireless communication interface 130 may be configured to operate using Wi-Fi, ZigBee, Bluetooth and the like. The wireless communication interface 130 may be arranged to communicate with any other subsystem of wireless device 100 as needed. For example, the wireless communication interface may comprise a connector, e.g. a wired connector, e.g. an Ethernet connector, an optical connector, etc., or a wireless connector, e.g. an antenna, e.g. a Wi-Fi, 4G or 5G antenna. The wireless communication interface 130 may be configured to communicate with and/or connect to a computer network. The computer network may comprise additional elements, such as a router, a hub and the like.

In an embodiment, the memory 120 may comprise a non-volatile memory 122. The non-volatile memory 122 is configured to store information persistently, such that the stored information even after the wireless device 100 has been rebooted. The non-volatile memory 122 may comprise an electronic memory, such as a flash memory, a magnetic memory, e.g. a hard disk, or the like, or optical memory, e.g. a DVD or CD-ROM. The non-volatile memory 122 may comprise a removable memory, such as an SD-card or the like, and/or a non-removable memory, such as a hard disk. The memory 120 may further comprise volatile memory 124. The volatile memory 124 may be used to temporarily store information, such as intermediate values. The volatile memory 124 is configured to store information whilst power is being received. Information stored in the non-volatile memory 124 will be lost in the event of an interruption to the power supply, such as during a reboot, or after removal of the wireless device 100 from its installation. The volatile memory 124 may comprise a temporary memory, such as random access memory (RAM).

The wireless device 100 comprises processor circuitry 110. The processing circuitry 110 may be electrically coupled, either wirelessly or wired, to the memory 120 and the wireless communication interface 130.

The processor circuitry 110 may comprise at least one processor, also referred to as at least one processor circuit.

In an embodiment, the processor circuitry 110 may be configured to generate an encryption key, S. The processor circuitry 110 may generate the encryption key S as a random encryption key. The encryption key S may be generated symmetrically. The processor circuitry 110 may be configured to encrypt authentication information, such as a passphrase, e.g. a Wi-Fi passphrase, using the generated encryption key S, to obtain encrypted authentication information E. The authentication information may be encrypted

using an authenticated encryption algorithm, such as an AES-GCM algorithm. The authentication information may be input by a user via any known means, or may be obtained via the wireless communication interface 130 by any known means. The authentication information may be used by the wireless device 100 to access a network, server, device or the like, within radio range of the wireless device 100. For example, the authentication information may comprise a Wi-Fi passphrase enabling the wireless device 100 to connect to a network provided by access point 200-1.

The processing circuitry 110 may be configured to compute a key from each of the network device identifiers obtained via the wireless communication interface 130. For example, if the wireless communication interface 130 receives or obtains identification information or unique information from N network devices, the processing circuitry 110 may compute a respective N keys from the N network devices. In some embodiments, the wireless communication interface 130 may obtain network device identifier information from a plurality of network devices having a signal strength above a threshold signal strength. For example, the wireless communication interface 130 may obtain network identifier information from network devices with an RSSI above a threshold RSSI. For each network device having a sufficiently high RSSI, the processing circuitry 110 may be configured to compute a corresponding key from the network device identifier. For example, the wireless communication interface 130 may detect N network devices within radio range of the wireless device 100, of which M network devices have a sufficiently high signal strength. In this case, the processing circuitry 110 may be configured to compute M keys, corresponding to the M network devices having sufficiently high signal strength, from their respective network device identifiers.

The processing circuitry 110 may be configured to provide a (t,n) secret sharing scheme, wherein n represents the number of computed keys and t represents a threshold number of shares. In some embodiments, the value of t is stored in the non-volatile memory 124 of the wireless device 100. The threshold number may indicate a minimum number of shares required to reconstruct the encryption key S.

The processing circuitry 110 may be configured to create a share s of the encryption key S for each computed key, according to the (t,n) secret sharing scheme. The processing circuitry 110 may then encrypt each share s with the respective key to obtain an encrypted share e. That is, for each of a plurality of network devices detected within radio range of the wireless device 100, for example for network devices having a sufficiently high

signal strength, a key is computed from the network device identifier, a share of the encryption key is created and encrypted using the computed key.

The encryption of each created share s may be a symmetric encryption. Each created share s may be encrypted using an authenticated encryption algorithm, such as an
5 AES-GCM encryption algorithm. In an example in which n keys are computed, n shares s may be created and encrypted with the respective n keys, to obtain n encrypted shares.

The processing circuitry 110 may be further configured to store the encrypted authentication information E and the encrypted shares e in the non-volatile memory 122 of the wireless device 100. In some embodiments, the authentication information, the encryption
10 key S , the computed keys and/or the created shares s may be stored in the volatile memory 124 of the wireless device 100 or may be deleted.

The processing circuitry 110 may be configured to perform any of the methods of Figs. 3 to 7.

Fig. 8b schematically shows an example of an embodiment of a wireless
15 device 100-b for decrypting authentication information. The wireless device 100-b may be configured to perform the methods of the reconstruction phase, as described above. In many embodiments, the wireless device 100-b is the same wireless device 100 as that of Fig. 8a. That is, the same wireless device 100 may be used to encrypt and then subsequently decrypt the authentication information, for example at a later time or after a connection interruption.
20 In some embodiments, the wireless device 100-b may be a different device than wireless device 100 of Fig. 8a. For example, the wireless device 100-b may be a replacement device arranged to replace wireless device 100 in an installation or environment. In such a case, the memory 120-b may comprise a removable memory in which the encrypted authentication information, E , and the encrypted shares e are stored. For example, the wireless device 100 of
25 Fig. 8a may store the encrypted authentication information E and the encrypted shares e on a removable drive such as an SD card, Flash drive or the like, which may be inserted into a replacement device such as wireless device 100-b.

Wireless device 100-b comprises a processing circuitry 110-b, a memory 120-b and a wireless communication interface 130-b.

30 In an embodiment, the wireless communication interface 130-b comprises a wireless receiver 132-b. In some embodiments, the wireless communication interface 130-b may further comprise a wireless transmitter 134-b. In some embodiments, the wireless receiver 132-b and the wireless transmitter 134-b may be incorporated as a wireless

transceiver. In other embodiments, the wireless receiver 132-b and the wireless transmitter 134-b may be separate components.

In an embodiment, the wireless receiver 132-b is configured to obtain a plurality of network device identifiers corresponding to a respective plurality of network devices detected within radio range of the wireless device 100-b. In some embodiments, the wireless receiver 132-b is configured to obtain the plurality of network device identifiers corresponding to the respective plurality of network devices by scanning wireless channels, such as Wi-Fi channels, and receiving identification information broadcasted by network devices, such as access points, beacons, stations and/or the like. In some embodiments, the wireless receiver 132-b is configured to obtain the plurality of network device identifiers by listening to wireless traffic. In some embodiments, the wireless transmitter 134-b is configured to send one or more probe requests and the wireless receiver 132-b is configured to receive one or more probe responses. Information received from network devices within range of the wireless device 100-b may comprise identification information identifying the respective network device. The identification information may comprise, for example, a MAC address of a station, a base service set identifier (BSSID), a service set identifier (SSID), an internet protocol (IP) address, and/or any static information identifying a network device and/or unique to a network device.

In some embodiments, the wireless communication interface may be configured to detect network devices within radio range of the wireless device 100-b with at least a threshold signal strength. In some embodiments, the wireless communication interface 130-b is configured to detect the received signal strength indicator (RSSI) of each network device detected within radio range of the wireless device 100-b.

The wireless communication interface 130-b may be configured to operate using Wi-Fi, ZigBee, Bluetooth and the like. The wireless communication interface 130-b may be arranged to communicate with any other subsystem of wireless device 100-b as needed. For example, the wireless communication interface may comprise a connector, e.g. a wired connector, e.g. an Ethernet connector, an optical connector, etc., or a wireless connector, e.g. an antenna, e.g. a Wi-Fi, 4G or 5G antenna. The wireless communication interface 130-b may be configured to communicate with and/or connect to a computer network. The computer network may comprise additional elements, such as a router, a hub and the like.

In an embodiment, the memory 120-b may comprise a non-volatile memory 122-b. The non-volatile memory 122-b is configured to store information persistently, such

that the stored information even after the wireless device 100-b has been rebooted. The non-volatile memory 122-b may comprise an electronic memory, such as a flash memory, a magnetic memory, e.g. a hard disk, or the like, or optical memory, e.g. a DVD or CD-ROM. The non-volatile memory 122-b may comprise a removable memory, such as an SD-card or the like, and/or a non-removable memory, such as a hard disk. The memory 120-b may further comprise volatile memory 124-b. The volatile memory 124-b may be used to temporarily store information, such as intermediate values. The volatile memory 124-b is configured to store information whilst power is being received. Information stored in the non-volatile memory 124-b will be lost in the event of an interruption to the power supply, such as during a reboot, or after removal of the wireless device 100-b from its installation. The volatile memory 124-b may comprise a temporary memory, such as random access memory (RAM).

The non-volatile memory 124-b may be configured to store the encrypted authentication information E and the encrypted shares e, obtained during the enrolment phase.

The wireless device 100-b comprises processor circuitry 110-b. The processing circuitry 110-b may be electrically coupled, either wirelessly or wired, to the memory 120-b and the wireless communication interface 130-b.

The processor circuitry 110-b may comprise at least one processor, also referred to as at least one processor circuit.

For each of at least a subset of the network device identifiers obtained via the wireless communication interface 130-b, the processing circuitry 110-b is configured to compute a key k from the network device identifier and perform a decryption of each of the plurality of encrypted shares e using the computed key k. The key k may be computed using a symmetric key generation algorithm. The processing circuitry 110-b may be configured to perform a decryption of one of the encrypted shares e stored in the non-volatile memory 122-b of the wireless device 100-b. If the decryption of the encrypted share is successful, the processing circuitry 110-b is configured to store the decrypted share and the network device identifier from which the key was computed in the volatile memory 124-b of the wireless device 100-b. If, however, the decryption was not successful, a different, or next, encrypted share may be selected from the non-volatile memory 122-b and the processing circuitry 110-b may perform a decryption on the next encrypted share. This may be repeated until either the computed key successfully decrypts an encrypted share, in which case the processing circuitry 110-b is configured to store the decrypted share and the network device identifier

from which the key was computed in the volatile memory 122-b of the wireless device 100-b, or until the key has been used to attempt to decrypt each of the encrypted shares stored in the non-volatile memory 122-b of the wireless device 100-b unsuccessfully.

5 A decryption may be determined to be successful or unsuccessful based on, for example, the use of a corresponding authentication tag generated when the encryption of the share occurred. In this case, an authentication tag corresponding to each encrypted share may be stored in the non-volatile memory 122-b of the wireless device 100-b.

Once an encrypted share has been successfully decrypted, the processing circuitry 110-b may be configured to compute a next key from a next network device
10 identifier, and again attempt to decrypt an encrypted share from the non-volatile memory 122-b.

In some embodiments, after an encrypted share has been successfully decrypted, for example after each successful decryption, the processing circuitry 110-b may be configured to determine how many decrypted shares are stored in the volatile memory
15 124-b. If the number of decrypted shares stored in the volatile memory 124-b meets or exceeds a threshold number t of shares, the processing circuitry 110-b may be configured to reconstruct the encryption key S using the decrypted shares. The threshold number t may be stored in the non-volatile memory 122-b of the wireless device 100-b, or the threshold number t may be hardcoded in the wireless device 100-b, for example as a function of the
20 number of encrypted shares e stored in the non-volatile memory 122-b. For example, if the non-volatile memory 122-b is storing n encrypted shares e , the value of the threshold number t may be a function of n , such as $n/2$ or the like. If the number of decrypted shares stored in the volatile memory 124-b does not meet the threshold number t , the processing circuitry 110-b may be configured to repeat the above process of computing a key and decrypting an
25 encrypted share for a next network device identifier obtained via the wireless communication interface 130-b.

In some embodiments, after an encrypted share has been successfully decrypted, for example after each successful decryption, the processing circuitry 110-b may be configured to attempt to reconstruct the encryption key S using the decrypted shares s . The
30 reconstruction may be evaluated, for example to determine whether the reconstruction is successful, by attempting to decrypt the encrypted authentication information E using the result of the reconstruction attempt. The decryption of the encrypted authentication information E may be confirmed using, for example, an authentication tag generated when the authentication information was encrypted. If the decryption of the encrypted

authentication information E is not successful, then the processing circuitry 110-b may be configured to compute a next key from a next network device identifier of the plurality of network device identifiers obtained via the wireless communication interface 130, attempt to decrypt an encrypted share from the plurality of encrypted shares stored in the non-volatile memory 122-b of the wireless device 100-b, as described above, until another share is successfully decrypted.

Although the above description of Fig. 8b refers to storing the decrypted shares in the volatile memory 124-b of the wireless device 100-b, the decrypted shares may additionally or alternatively be stored in an area of the non-volatile memory 122-b. In embodiments in which the decrypted shares are stored in the non-volatile memory 122-b, it is preferable for the decrypted shares to be deleted from the non-volatile memory 122-b once the authentication information is decrypted.

Fig. 8c schematically shows an example of an embodiment of a lighting element for encrypting and/or decrypting authentication information. In some embodiments, the wireless device 100 and/or the wireless device 100-b may be a lighting element, such as a luminaire or a lightbulb.

For example, the wireless device 100 may comprise a wireless-enabled lightbulb or luminaire, configured to wirelessly connect to a network, such as a home or office network. The network may be a smart network, and may include additional IoT or smart devices.

Fig. 9 shows a computer readable medium 900 having a writable part 910 comprising a computer program 920, the computer program 920 comprising instructions for causing a processor system to perform a method, such as any or all of the methods of Figs. 4 through 8. The computer program 920 may be embodied on the computer readable medium 900 as physical marks or by magnetization of the computer readable medium 900. However, any other suitable embodiment is conceivable as well. Furthermore, it will be appreciated that, although the computer readable medium 900 is shown here as an SD card, the computer readable medium 900 may be any suitable computer readable medium, such as a compact disk, a hard disk, solid state memory, flash memory, etc., and may be non-recordable or recordable. The computer program 920 comprises instructions for causing a processor system to perform said method of encrypting and/or decrypting authentication information.

Fig. 10 shows in a schematic representation of a processor system 1040, an example of processor subsystem 110, according to an embodiment of the wireless device shown in Figs. 8a, 8b and/or 8c.. The processor system comprises one or more integrated

circuits 1010. Circuit 1010 comprises a processing unit 1020, e.g., a CPU, for running computer program components to execute a method according to an embodiment and/or implement its modules or units. Circuit 1010 comprises a memory 1022 for storing programming code, data, etc. Part of memory 1022 may be read-only. Circuit 1010 may
5 comprise a communication element 1026, e.g., an antenna, connectors or both, and the like. Circuit 1010 may comprise a dedicated integrated circuit (IC) 1024 for performing part or all of the processing defined in the method. Processor 1020, memory 1022, dedicated IC 1024 and communication element 1026 may be connected to each other via an interconnect 1030, for example a bus. The processor system 1010 may be arranged for contact and/or contact-
10 less communication, using an antenna and/or connectors, respectively.

For example, in an embodiment, processor system 1040, e.g., the wireless device of Figs. 8a, 8b and/or 8c may comprise a processor circuit and a memory circuit, the processor being arranged to execute software stored in the memory circuit. For example, the processor circuit may be an Intel Core i7 processor, ARM Cortex-R8, etc. In an embodiment,
15 the processor circuit may be ARM Cortex M0. The memory circuit may be an ROM circuit, or a non-volatile memory, e.g., a flash memory. The memory circuit may be a volatile memory, e.g., an SRAM memory. In the latter case, the device may comprise a non-volatile software interface, e.g., a hard drive, a network interface, etc., arranged for providing the software.

20 While wireless device 100 is shown as including one of each described component, the various components may be duplicated in various embodiments. For example, the processor 1020 may include multiple microprocessors that are configured to independently execute the methods described herein or are configured to perform steps or subroutines of the methods described herein such that the multiple processors cooperate to
25 achieve the functionality described herein. Further, where the wireless device 100 is implemented in a cloud computing system, the various hardware components may belong to separate physical systems. For example, the processor 1020 may include a first processor in a first server and a second processor in a second server.

It should be noted that the above-mentioned embodiments illustrate rather than
30 limit the invention, and that those skilled in the art will be able to design many alternative embodiments.

In the claims, any reference signs placed between parentheses shall not be construed as limiting the claim. Use of the verb "comprise" and its conjugations does not exclude the presence of elements or steps other than those stated in a claim. The article "a" or

"an" preceding an element does not exclude the presence of a plurality of such elements. Expressions such as "at least one of" when preceding a list or group of elements represent a selection of all or of any subset of elements from the list or group. For example, the expression, "at least one of A, B, and C" should be understood as including only A, only B, only C, both A and B, both A and C, both B and C, or all of A, B, and C. The invention may be implemented by means of hardware comprising several distinct elements, and by means of a suitably programmed computer. In the device claim enumerating several means, several of these means may be embodied by one and the same item of hardware. The mere fact that certain measures are recited in mutually different dependent claims does not indicate that a combination of these measures cannot be used to advantage.

CLAIMS:

1. An enrolment method for encrypting authentication information by a wireless device, the method comprising:
 - generating an encryption key, S ;
 - encrypting the authentication information with the encryption key, S , to
 - 5 obtain an encrypted authentication information, E ;
 - obtaining a plurality of network device identifiers corresponding to a respective plurality of network devices detected within radio range of the wireless device;
 - for each of the obtained plurality of network device identifiers, computing a key from the network device identifier;
 - 10 - providing a (t, n) secret sharing scheme, wherein n represents the number of computed keys and t represents a threshold number of shares;
 - for each computed key, creating a share, s , of the encryption key S using the (t, n) secret sharing scheme and encrypting said share s symmetrically with said computed key k to produce an encrypted share, e , to obtain n encrypted shares; and wherein the number of
 - 15 shares into which the encryption is divided is based on the number of network devices detected and wherein the threshold number (t) of shares is predetermined as an absolute value, or determined from the number n ;
 - storing the encrypted authentication information and the encrypted shares in a non-volatile memory of the wireless device.
 - 20
2. The method of claim 1, further comprising, for each share, generating an authentication tag from the share and the corresponding computed key, and storing the corresponding authentication tag.
- 25 3. The method of any preceding claim, wherein the obtained plurality of network device identifiers comprises at least one of:
 - WiFi access point identifiers of WiFi access points detected by a WiFi receiver of the wireless device, the WiFi access point identifiers preferably comprising at least one of a basic service set identifier, BSSID, of a WiFi access point, a service set

identifier, SSID, of the WiFi access point, a supported rates indication of the WiFi access point and a country information of the WiFi access point; and

- a MAC address of a station sending data to an access point.

5 4. The method of any preceding claim, wherein obtaining the plurality of network device identifiers comprises detecting network device identifiers with a received signal strength greater than a threshold.

10 5. The method of any preceding claim, wherein obtaining the plurality of network device identifiers comprises at least one of:

- scanning wireless channels such as Wi-Fi channels,
- listening to wireless traffic, and
- sending probe requests and receiving probe responses.

15 6. The method of any preceding claim, further comprising:

- obtaining a new network device identifier;
 - generating a new key using the new network device identifier;
- attempting to decrypt each of the encrypted shares e using the new key;
- if the new key does not successfully decrypt any of the encrypted shares e :

20 - generating a new share s of the encryption key S using a function of the (t, n) secret sharing scheme;

- encrypting the new share s with the new key to obtain a new encrypted share; and

25 - storing the new encrypted share in the non-volatile memory of the wireless device.

7. The method of any preceding claim, wherein the authentication information comprises a Wi-Fi passphrase.

30 8. A reconstruction method for decrypting authentication information by a wireless device, the method comprising:

- obtaining, from a non-volatile memory of the wireless device:

- an encrypted authentication information E, the encrypted authentication information E being authentication information encrypted with an encryption key S;

- a plurality of encrypted shares e, each encrypted share
5 being a share of the encryption key S encrypted with a respective key k;

- obtaining a plurality of network device identifiers corresponding to a respective plurality of network devices detected within radio range of the wireless device;

- for each of at least a subset of the obtained plurality of network device identifiers:

10 - computing a key k from the network device identifier;

- performing a decryption of at least one of the plurality of encrypted shares e using the key;

- if the decryption of an encrypted share e of the plurality of encrypted shares successfully decrypts the encrypted share to obtain a decrypted share s, storing the
15 decrypted share s in a memory of the wireless device;

- reconstructing the encryption key S using the decrypted shares s;

- decrypting the encrypted authentication information E using the reconstructed encryption key S to recover the authentication information.

20

9. The method of claim 8, further comprising obtaining, from the non-volatile memory of the wireless device, a threshold number t denoting a threshold number of shares for a (t,n) secret sharing scheme, and wherein the number of network identifiers in the subset of the obtained plurality of network device identifiers is at least equal to the threshold

25 number t.

10. A method of protecting authentication information by a wireless device, the method comprising an enrolment phase corresponding to the method as defined in any one of claims 1 to 7, and a reconstruction phase corresponding to the method as defined in claim 8
30 or claim 9.

11. The method of claim 10, further comprising:

- detecting a refresh event;

- repeating the enrolment phase of any one of claims 1 to 7;

wherein the refresh event comprises at least one of:

- an expiry of a rekeying timer, the rekeying timer being an indication of freshness of the encrypted shares;
- a change in the network device identifiers detected within radio range of the wireless device, the change exceeding a predetermined threshold; and
- a number of times the authentication information has been recovered since the enrolment phase.

12. A wireless device for encrypting authentication information, the wireless device comprising:

- a wireless receiver configured to:
 - obtain a plurality of network device identifiers corresponding to a respective plurality of network devices detected within radio range of the wireless device; and
 - processing circuitry, configured to:
 - generate an encryption key, S;
 - encrypt the authentication information with the encryption key, S, to obtain an encrypted authentication information, E;
 - for each of the detected plurality of network device identifiers, compute a key from the network device identifier;
- provide a (t, n) secret sharing scheme, wherein n represents the number of computed keys and t represents a threshold number of shares; and wherein the number of shares into which the encryption is divided is based on the number of network devices detected and the threshold number (t) of shares is predetermined as an absolute value, or determined from the number n; and
- for each computed key, create a share, s, of the encryption key S using the (t,n) secret sharing scheme and encrypt said share s symmetrically with said computed key k to produce an encrypted share, e, to obtain n encrypted shares; and
- non-volatile memory configured to store the encrypted authentication information and the encrypted shares.

30

13. A wireless device for decrypting authentication information, the wireless device comprising:

- a wireless receiver configured to obtain a plurality of network device identifiers corresponding to a respective plurality of network devices detected within radio range of the wireless device;
- a volatile memory;
- 5 - non-volatile memory configured to store:
 - encrypted authentication information E, the encrypted authentication information E being authentication information encrypted with an encryption key S;
 - a plurality of encrypted shares e, each encrypted share being a share of the encryption key S encrypted with a respective key k;
 - 10 - a threshold number t denoting a threshold number of shares for a (t, n) secret sharing scheme;
 - processing circuitry, configured to:
 - for each of at least a subset of the obtained plurality of network device identifiers:
 - 15 - compute a key k from the network device identifier; and
 - perform a decryption of each of the plurality of encrypted shares e using the computed key k;
 - if the decryption of an encrypted share e of the plurality of encrypted shares successfully decrypts the encrypted share to obtain a decrypted share s, store the network device identifier and the decrypted share s in the volatile memory of the wireless device;
 - 20 - reconstruct the encryption key S using the decrypted shares s;
 - decrypt the encrypted authentication information E using the reconstructed encryption key S.
 - 25

14. The wireless device of claim 12 and/or claim 13, wherein the wireless device comprises at least one of a Wi-Fi-enabled lighting element, a Wi-Fi-enabled light bulb and a Wi-Fi-enabled luminaire.

30

15. A transitory or non-transitory computer-readable medium comprising data representing instructions which, when executed by a processor system, cause the processor system to carry out the method of any of claims 1 to 11.

1/8

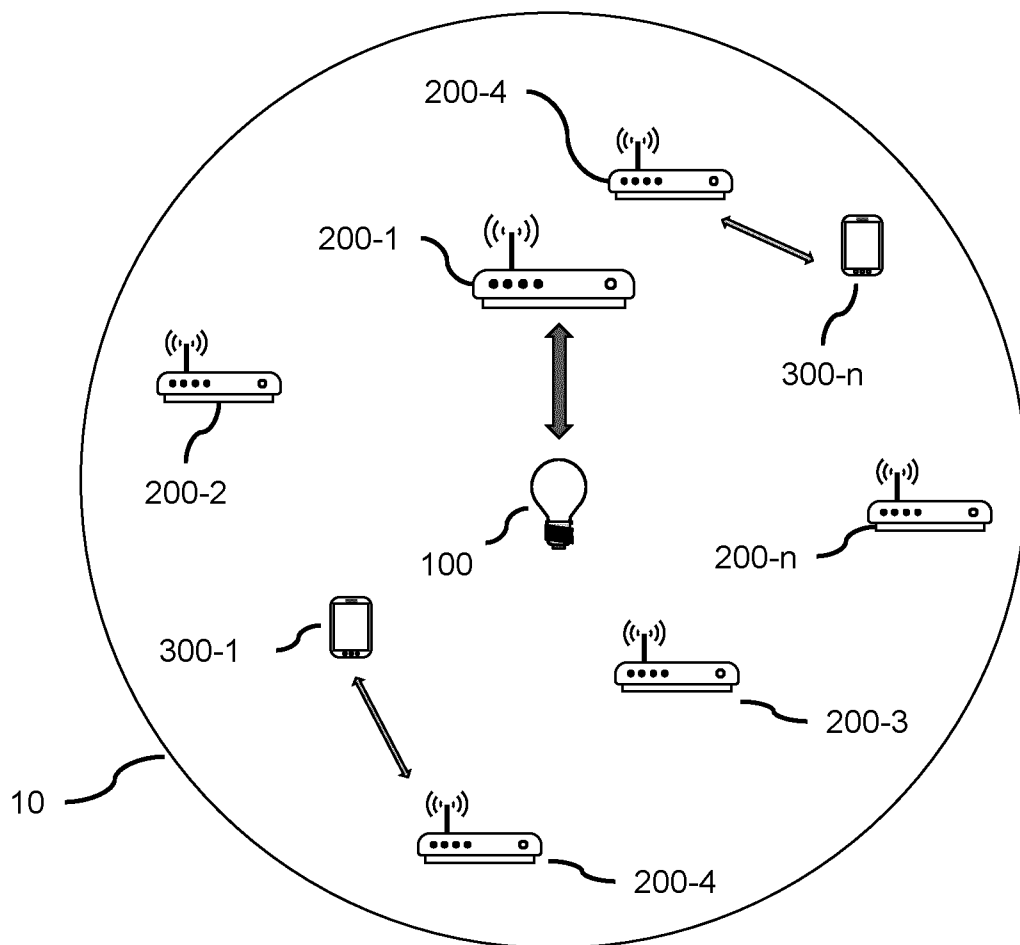


Fig. 1

2/8

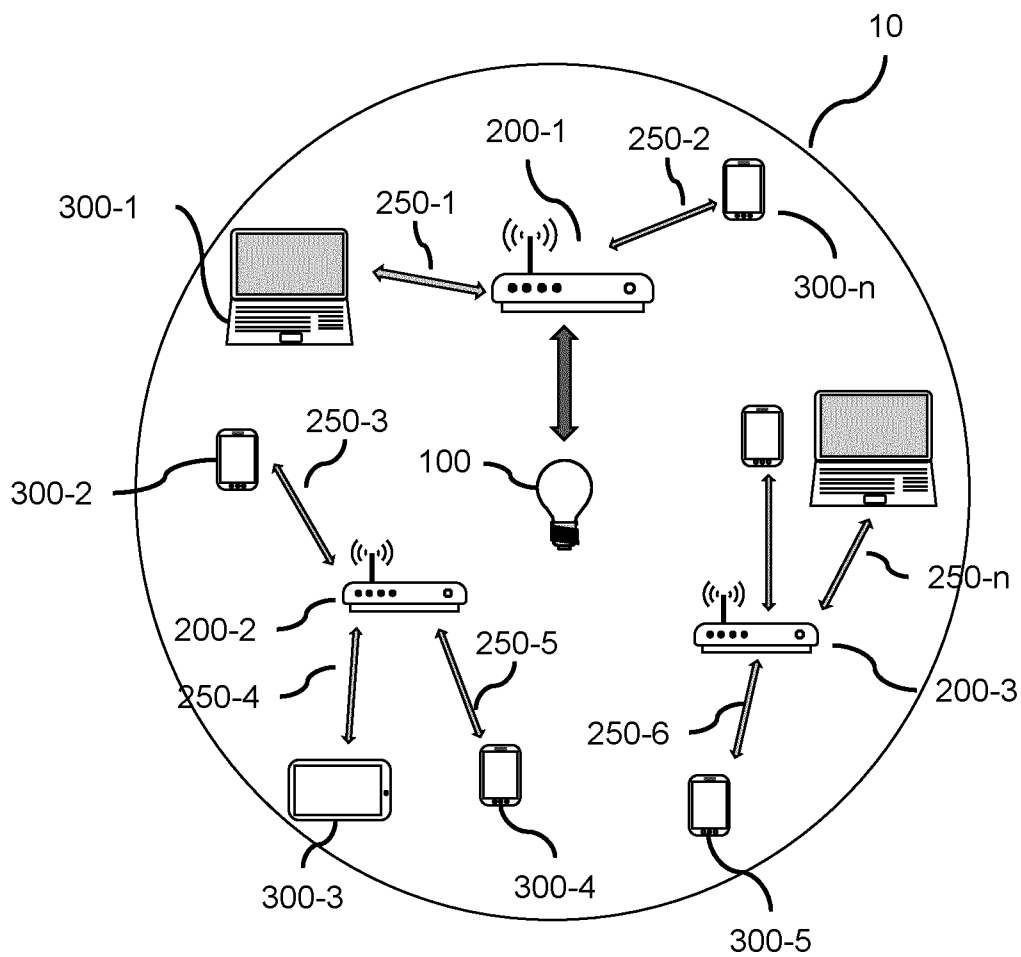


Fig. 2

3/8

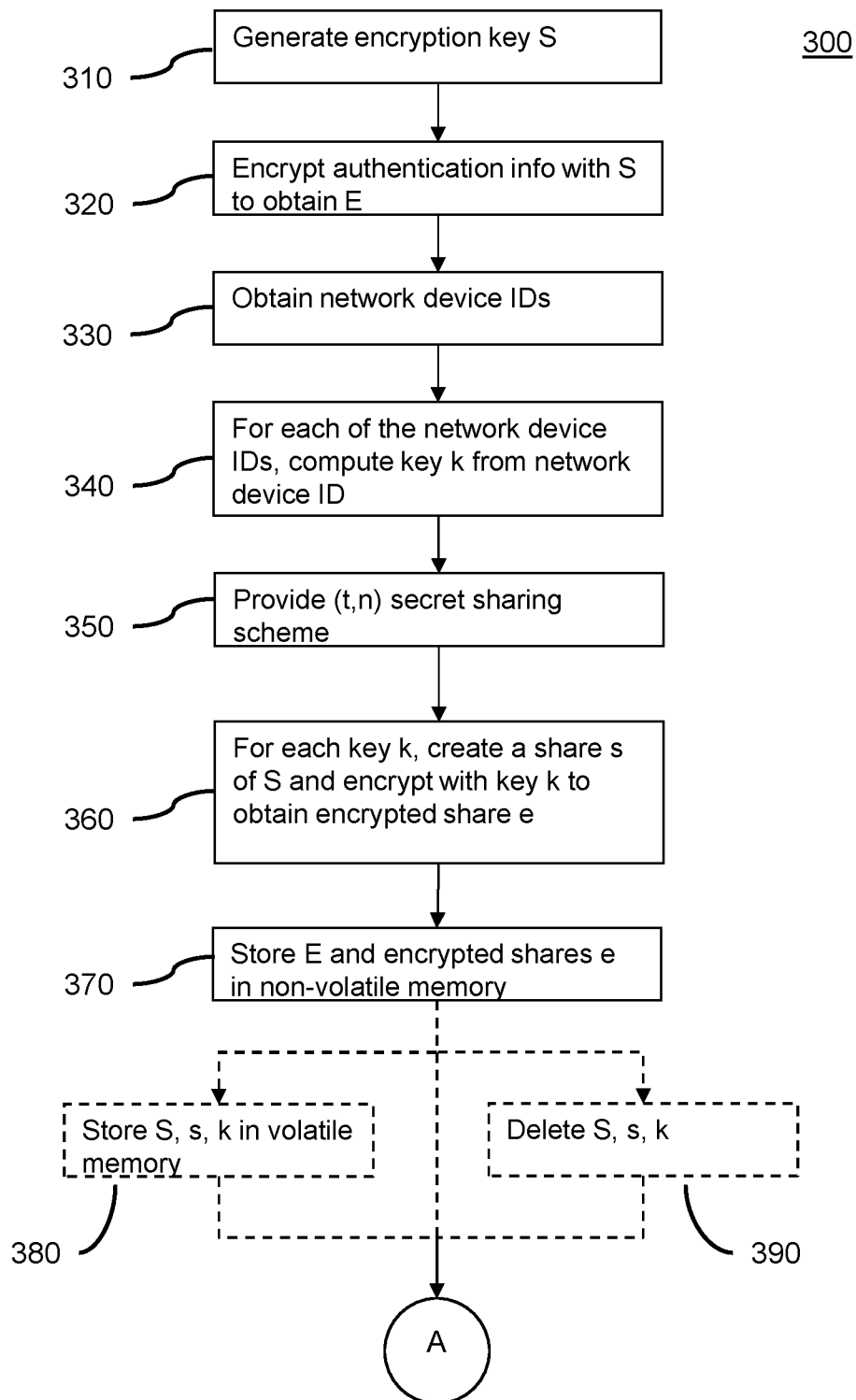
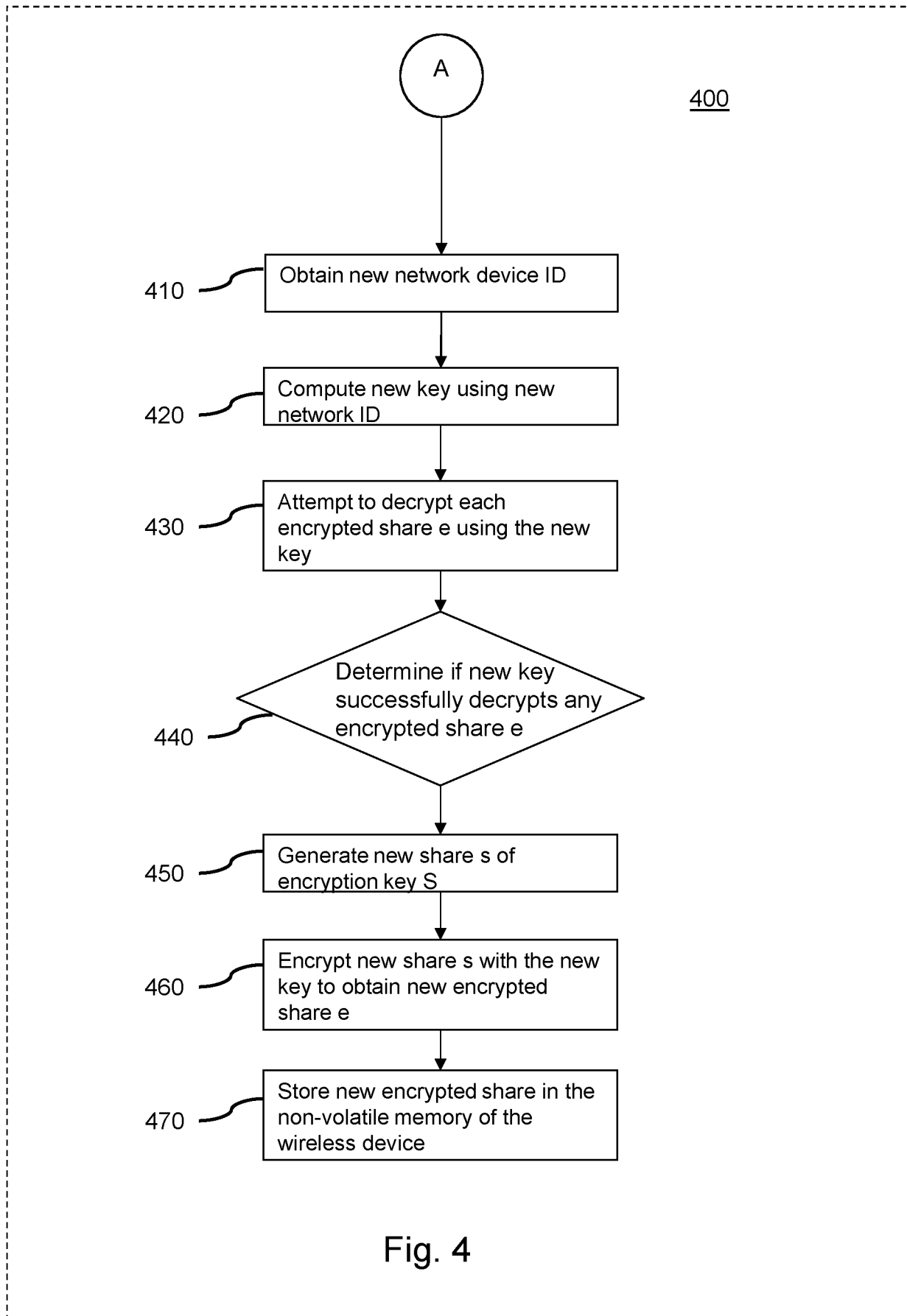
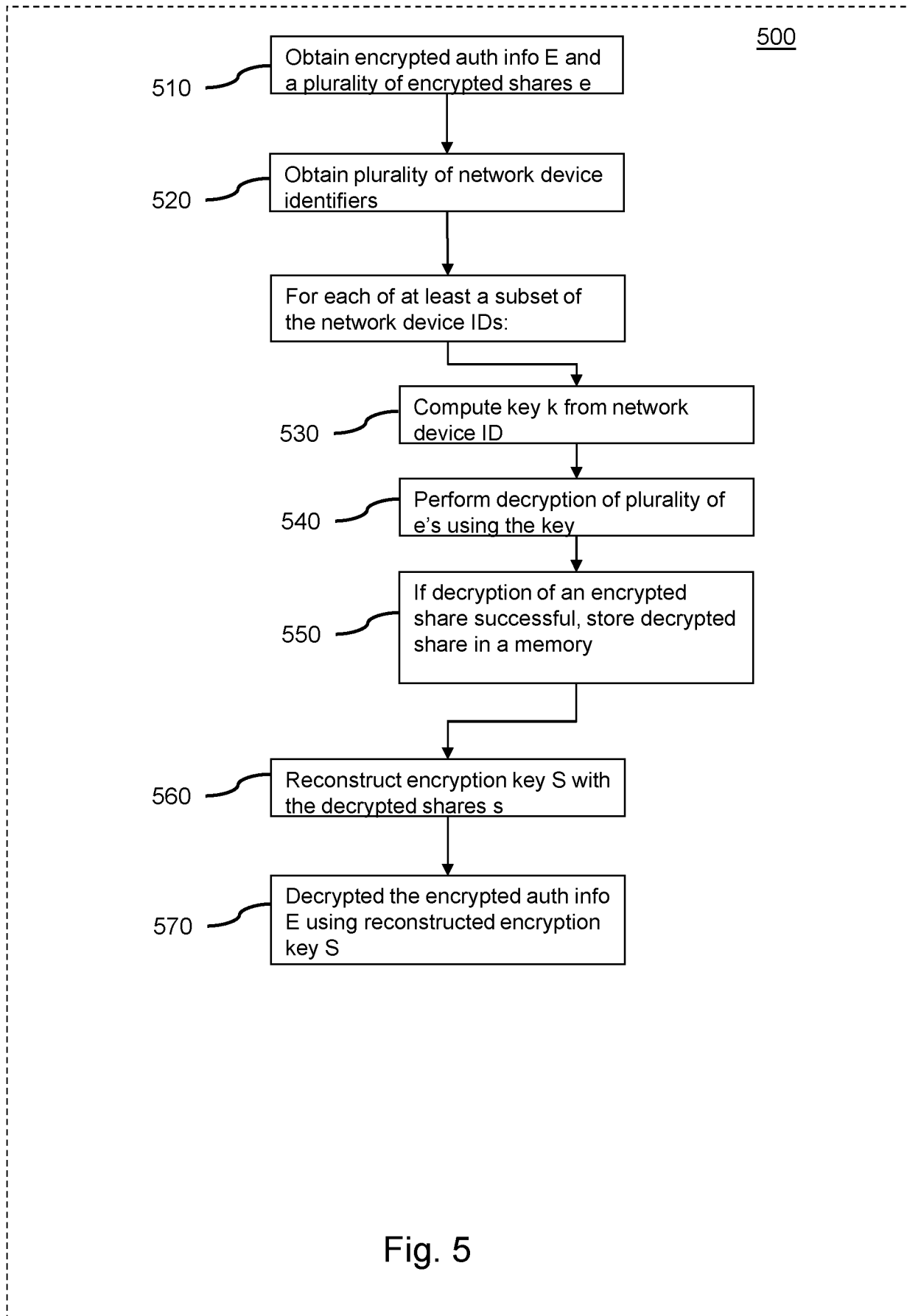


Fig. 3

4/8



5/8

6/8

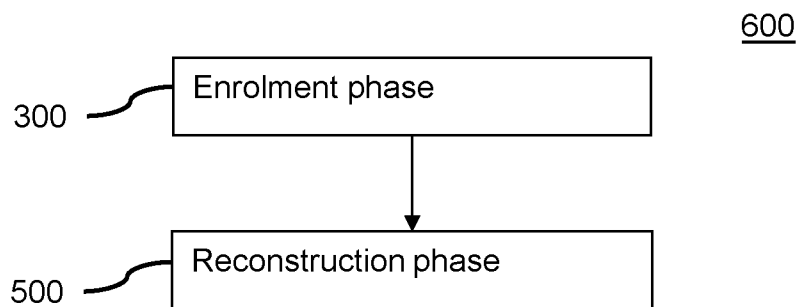


Fig. 6

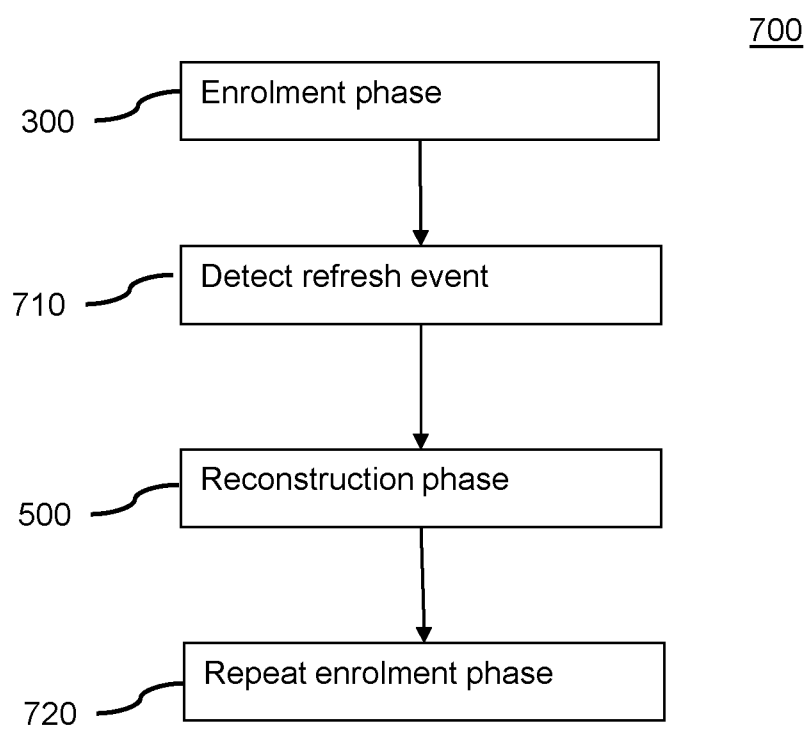


Fig. 7

100

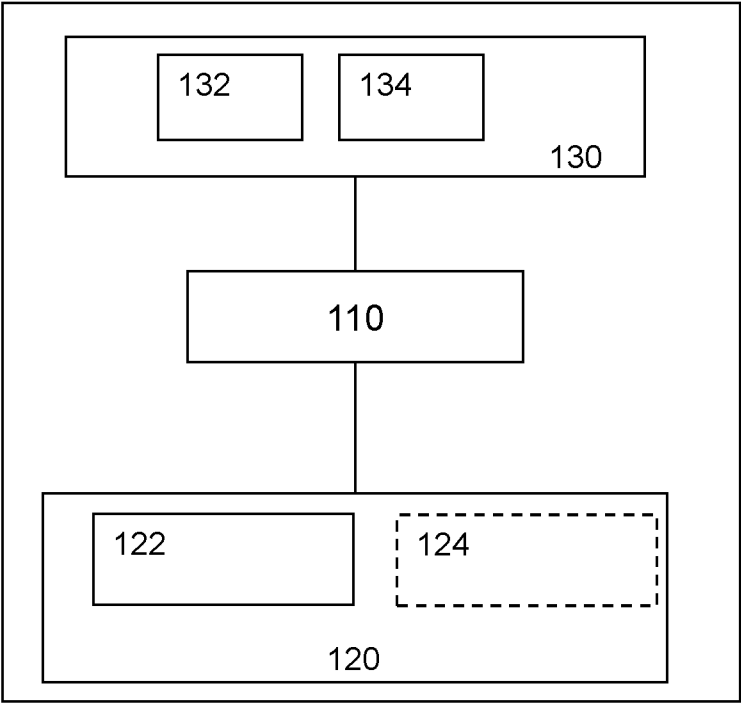


Fig. 8a

100-b

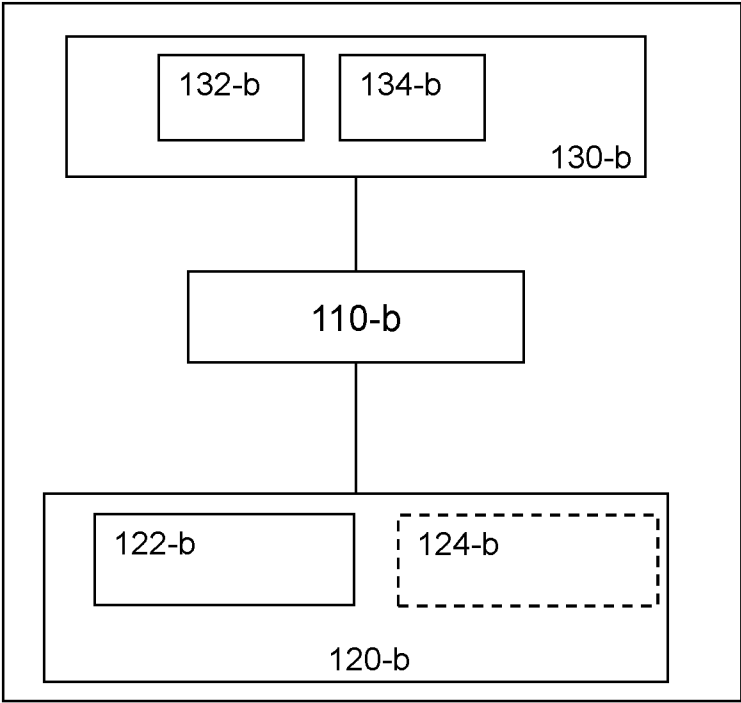


Fig. 8b

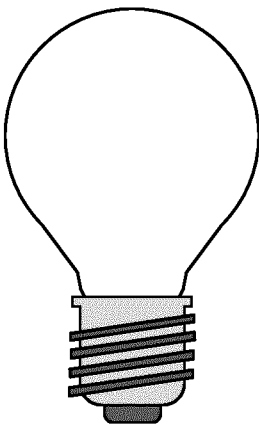


Fig. 8c

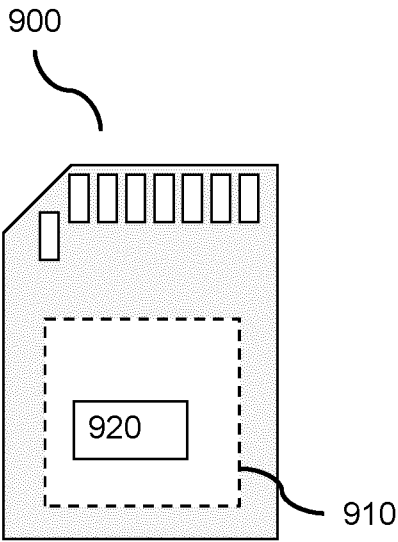


Fig. 9

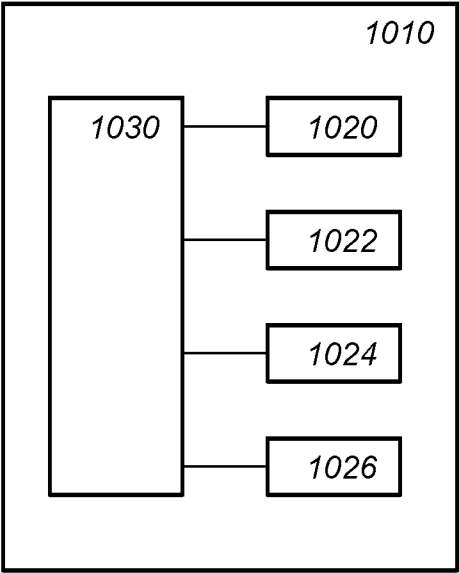


Fig. 10

1040

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2021/068238

A. CLASSIFICATION OF SUBJECT MATTER INV. H04L29/06 H04W4/70 H04W12/04 H04W4/80 H04W12/02 H04W12/06 ADD. According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) H04L H04W Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) EPO-Internal, WPI Data		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 2 937 802 A1 (SAMSUNG ELECTRONICS CO LTD [KR]) 28 October 2015 (2015-10-28) paragraph [0001] - paragraph [0031] paragraph [0049] - paragraph [0059] paragraph [0213] - paragraph [0215]; figures 19-21 -----	1-15
Y	EP 3 633 913 A1 (CLOVER NETWORK INC [US]) 8 April 2020 (2020-04-08) paragraphs [0012], [0032] ----- -/--	1-15
☒ Further documents are listed in the continuation of Box C. ☒ See patent family annex.		
* Special categories of cited documents : "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family		
Date of the actual completion of the international search 29 November 2021		Date of mailing of the international search report 07/12/2021
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016		Authorized officer Wuillème, Cédric

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2021/068238

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2019/253243 A1 (ZIMMERMAN SCOTT [US] ET AL) 15 August 2019 (2019-08-15) paragraph [0047] - paragraph [0049] paragraph [0099] - paragraph [0112] paragraph [0127] - paragraph [0144] paragraph [0201] - paragraph [0206] paragraph [0220] - paragraph [0243] paragraph [0259] - paragraph [0270]; claims 1,9,17; figures 1B,8A-11, 16A-18,23A-28 -----	1-15

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2021/068238

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 2937802	A1	28-10-2015	EP 2937802 A1 28-10-2015
			US 2015312759 A1 29-10-2015
			WO 2015163735 A1 29-10-2015

EP 3633913	A1	08-04-2020	AU 2019202163 B1 31-10-2019
			BR 102019015369 A2 18-02-2020
			CA 3061233 A1 03-04-2020
			CN 110995642 A 10-04-2020
			EP 3633913 A1 08-04-2020
			US 10326797 B1 18-06-2019

US 2019253243	A1	15-08-2019	US 2019253243 A1 15-08-2019
			US 2020213101 A1 02-07-2020
			WO 2019157433 A1 15-08-2019
