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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 October 2004 (07.10.2004)

PCT

(10) International Publication Number
WO 2004/085773 A1

(51) International Patent Classification[7]: E05B 37/20

(21) International Application Number:
PCT/CN2004/000249

(22) International Filing Date: 24 March 2004 (24.03.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/394,345 24 March 2003 (24.03.2003) US

(71) Applicant *(for all designated States except US)*: **THE UNIVERSITY OF HONG KONG** [CN/CN]; G18, Eliot Hall, Pokfulam Road, Hong Kong (CN).

(72) Inventors: **WONG, Alfred K.**; Flat A4, Block 3 tam Towers, 25 Sha Wan Drive, Pokfulam, Hong Kong (CN). **YANG, Edward, S.**; 1100 Cotton Street, Menlo Park, CA 94025 (US). **YEUNG, Szeman**; 26H, Loong Shan Mansion, Taikoo Shing, Hong Kong.

(74) Agent: **CHINA PATENT AGENT (H.K.) LTD.**; 22F Great Eagle Centre, 23 Harbour Road, Wanchai, Hong Kong (CN).

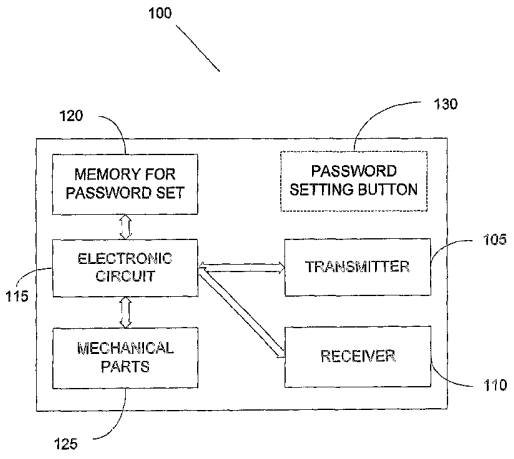
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

[Continued on next page]

(54) Title: AN EFFICIENT LOCK AND KEY SYSTEM



(57) Abstract: A method and system is disclosed for allowing users to consolidate a large number electronic keys (for operating mechanical locks) in electronic key assemblies. These electronic keys are easily duplicated, added to, removed, backed up, or upgraded. The electronic key assemblies are also more resistant to tampering. The lock assembly and electronic key designs taught by the invention are customizable to meet various security needs. The lock assembly includes a transmitter and a receiver operatively coupled to an electronic circuit in communication with a store for keys. The electronic circuit is also coupled to the mechanical levers for operating the lock assembly. The electronic key assembly also has its transmitter, receiver, a control circuit and a user interface for selecting a particular electronic key password.

WO 2004/085773 A1

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

AN EFFICIENT LOCK AND KEY SYSTEM

FIELD OF THE INVENTION

This invention is in the field of security and access control. In particular, the invention has applicability to providing keys that are tampering resistant but are easy to securely duplicate and carry.

BACKGROUND OF THE INVENTION

Mechanical locks based on mechanical types of cylinders have been frequently modified by the addition of electronic security features. Locking elements controlled by electronic-means have been disclosed in combination with non-mechanical types of tumblers, such as in Clarkson et al. U.S. Pat. No. 4,712,398 with an eye to reduce the need to retrofit the traditional locks.

The use of electronic techniques for coding locks offers the possibility of a number of significant advantages as compared with the traditional mechanical bitting. Electronic coding can increase information content with attendant improvements to system capabilities such as more effective new countermeasures against "lock-picking" attempts.

A distinction may be made among purely electronic, magnetic or optical keys; mechanical keys equipped with electronic, magnetic or optical features; and mechanical keys which operate solely by mechanical bittings, whether those bittings be pin tumbler, dimples or other mechanical patterns.

A key comprised of electronic circuitry, magnetic or optical data storage for determining and granting access is an electronic key assembly. Some examples are described in U.S. Pat. Nos. 3,733,862 (Killmeyer), 4,144,523 (Kaplit), 4,326,124 (Faude), 4,562,712 (Wolter), 4,663,952 (Gelhard), 4,686,358 (Seckinger et al.), 5,245,329 (Gokcebay) and 5,140,317 (Hyatt, Jr. et al.). For unlocking a lock, using such a key, data is transferred to a reader associated with a lock, and the reader, in response to recognizing the pattern or code held by the key, activates unlocking. The key , see e.g., U.S. Pat. Nos. 3,797,936 (Dimitriadis), 4,209,782 (Donath et al.), 4,257,030 (Bruhin et al.), 4,620,088 (Flies), 4,659,915 (Flies) and 4,789,859 (Clarkson et al.), does require any mechanical cut or bitting configurations.

Mechanical keys, see, e.g., U.S. Pat. Nos. 480,299 (Voight), 550,111 (Sargent), 564,029 (Sargent), 3,208,248 (Tornoe), 4,723,427 (Oliver), 4,732,022 (Oliver) and 4,823,575 (Florian et al.), directly activate a mechanical device, with a pattern of mechanical bittings, by direct contact with the interpreting device, for instance, the tumblers, such as pin tumblers, lever tumblers, disk tumblers, rotary disk tumblers, slider tumblers, or combinations of several of these incorporated within the same lock, or other pattern-holding apparatus contained in the lock. Typically, access is granted based on the depth and configuration of the key cuts relative to the tumblers, and the keyholder is able to turn the key to lock and unlock the locking device. As a variation, a push or pull action may also be necessary for locking and unlocking. In some instances both mechanical and non-mechanical features of a key are used simultaneously.

Electronic locks and keys are often found in remotely operated devices such as car locks, garage openers and the like. However, each of these remotely operated locks require their own physical key, which typically may be bulkier than the mechanical keys. It is not uncommon to have several such keys, also termed remotes, in combination with mechanical keys. Misplacing or losing such a key is easy while duplicating them continues to be both difficult and expensive.

An example of an electronic lock and key system is the E-Lock™ product marketed by Lista® corporation of Switzerland. While the E-Lock system allows a single key to operate several electronic locks, the keys are designed to be copy proof. Loss or pilfering of a key is handled by reprogramming the system and using a new key corresponding to the reprogrammed setup. In addition, the electronic locks may be configured to relock themselves after a certain amount to further improve security.

Other examples of electronic lock and key systems include the DATAKEY CIP™ smart card. The smart card has the capability of generating keys or of receiving keys generated elsewhere. TRACcess® provides another system of electronic locks, which are operated with an authorized TRACkey™ and is configured to track all activity without relying upon external power or phone lines. The TRACcess® is a large entity solution to provide integrated security that is not suitable for day to day use by individual consumers.

SUMMARY OF THE INVENTION

The invention described below, inter alia, provides a method and system that allows users to carry a large number of passwords, operating as keys, without

the cumbersome clanging keychain weighed down by keys that are easier for a forger rather than the intended possessor to duplicate. The passwords in the electronic key assemblies of the invention are easily duplicated, added to, or removed. In addition, backup versions of the passwords may be stored to guard against accidentally losing the key.

In another aspect, the electronic key assemblies are upgradeable, and do not suffer from the vulnerability of mechanical keys due to the ease of deciphering a master key that operates several mechanical locks by trial and error in relatively few steps.

In another aspect, the lock assembly and password combinations taught by the invention may be reprogrammable or, alternatively, programmed only at the manufacturing stage. These combinations avoid the need to recall a large number of key codes or the security risk associated with mechanical keys. Specifying the password at the manufacturing stage allows customization to meet various security needs as is described briefly next.

Conventional mechanical locks are opened by one or more keys that are determined in the course of manufacturing the lock. In such mechanical locks, sometimes manufactured so as to admit of a 'master key,' the use of cyptographic techniques is known to lead to a key capable of duplicating the function of even the master key, thus posing a security risk since all keys to locks admitting of the master key necessarily share many characteristics. This draw back is not universal since mechanical locks, such as 'number locks' requiring a particular number combination, allow for choosing alternative combinations. Such number locks however require memorization of many combinations.

In an illustrative embodiment of the invention, the lock assembly includes a transmitter and a receiver that are operatively coupled to an electronic circuit, which is preferably programmable, in communication with a memory or other store for identifiers and keys. The electronic circuit is also coupled to the mechanical levers that need to be moved to lock or unlock the lock assembly.

The electronic lock assembly is preferably a part of an electronic lock system comprising a lock assembly and an electronic key assembly. The electronic key assembly also has its transmitter and receiver so that it may communicate with the electronic lock assembly and other electronic key assemblies. In a preferred embodiment of the invention, a user interface is presented to the key user so that the user may select a password for a particular electronic lock assembly or duplication to another key. The key electronic control circuit coordinates the

activities of the various key sub-parts. One or more passwords are stored on a typical electronic key assembly, which may operate one or more lock assemblies. Additionally, a stored password on the electronic key assembly may be used to set the password for a lock assembly using a password-setting button on the lock assembly to be set. Preferably such a button may be activated only during the manufacturing of the lock assembly or a limited number of times after the manufacturing.

Preferably the user interface has a display or a scroll button. Alternatively, one or more of a clickable button, an infrared port, or a pressure sensitive surface may be used to either input or view desired information on the user interface. Thus, a password is copied from one electronic key assembly to another electronic key assembly by activating a password duplication feature, establishing a link between the electronic key assemblies; receiving a specified password to be duplicated followed by storing the duplicate password. The password duplication feature is preferably accessed via the user interface, although automated duplication procedures may also be implemented in alternative embodiments. In such procedures, over a secure link, a particular transmission pattern may result in duplication of a password or in view of previously transacted information, receiving a transmitted password may automatically result in its duplication. Or, instead of copying a password, a property of the password is communicated and replicated in a generated password.

Additionally, a password-setting button in the lock assembly allows setting of the password during manufacturing. Preferably in response to pressing of the password-setting button a random sequence is stored as a password for unlocking the lock assembly. This random sequence is also transmitted to the electronic key assembly for storage as the password for unlocking the lock assembly. A password setting function is activated in the key to enable receiving the random sequence as the password for the lock assembly. In an aspect designed to improve security the password-setting button is inactivated after setting the password of the lock assembly during manufacturing.

It should be noted that the lock assembly may correspond to more than one password for unlocking the lock assembly. Indeed, a particular password may unlock more than one lock assembly. However, in contrast to the typical lock and key systems with master keys, the various passwords need not be related since they can be chosen independently. Thus, several passwords for unlocking a lock assembly may be stored on a single key, or the key may store passwords for unlocking more than one lock assembly.

Although there is no limit on the number of passwords that may be stored on a key except that imposed by the available memory, it is preferred that several passwords be stored on a single key. For instance, an electronic key assembly may store at least five passwords, at least ten passwords, at least twenty passwords, at least fifty passwords, and at least one hundred passwords. With a large number of passwords, their relative organization is preferably implemented with the passwords organized with the help of navigable folders. Preferably, the password corresponding to the lock assembly is transmitted from a key in response to a selection made via the user interface.

In response to receiving a password the control circuit in a lock assembly determines if there is a match. The match may be a common hash value , which in combination with a public-private key setup provides secure communications. Alternatively, directed communication between keys and a key and a lock assembly may reduce the likelihood of eavesdropping. To this end there is considerable flexibility since either or both of the lock assembly transmitter and the key transmitter may be coupled to one or more of an antenna and a light emitting diode and the like with corresponding receivers.

In another aspect, the lock assembly electronic control circuit is configured, at a time point following unlocking, to instruct the lock assembly mechanical parts to relock in a default mode.

The invention also encompasses designing an electronic lock assembly system. Typically, a method for designing such an electronic lock system include providing a lock assembly transmitter and a lock assembly receiver; storage for one or more passwords; and a control circuit coupled to mechanical parts for locking and unlocking the electronic lock assembly. The control circuit unlocks the electronic lock assembly in response to receiving a password matching the stored password.

The electronic key assembly has a key transmitter and a key receiver as well as password storage locations. A control circuit determines whether to transmit a password, its required encryption, implementation of various functions, and the like. The control circuit also interacts with a user via a user interface, for instance to provide functionality such as that for password duplication function for transmitting a password from one electronic key assembly to another electronic key assembly followed by storing of the transmitted password.

In another aspect, the electronic lock preferably has a password-setting button. In response to activating the button, a password is stored by the electronic lock assembly such that receiving the password operates the lock assembly.

Preferably, the button is operated during the manufacturing of the lock assembly and the stored password is transmitted to an electronic key assembly for operating the lock assembly. In another aspect, the electronic key assembly has a password-setting function so that the password received from the electronic lock assembly is stored on the electronic key assembly.

In another aspect, preferably the transmissions between electronic key assemblies or with the electronic lock assembly are encrypted. An exemplary method uses a private-public key system to encrypt messages, including passwords sent to each device. By the optional use of digital signatures in some embodiments of the invention, secure communication channels may be established for transmission of the password and related information using hashing. It should be noted that such use of public-private keys is not required for practicing the invention, and any encryption scheme may be deployed to meet the particular security needs. In some embodiments, no encryption may be employed. In addition, directed communication using narrow beams, key cards, and the like may be employed with or without encryption technology.

DETAILED DESCRIPTION OF THE FIGURES

FIGURE 1 is a schematic diagram illustrating an electronic lock assembly according to the invention.

FIGURE 2 is a block diagram of an electronic key assembly according to the invention.

FIGURE 3 illustrates a method for duplicating a password using the electronic key assemblies according to the invention

FIGURE 4 illustrates interactions between two electronic key assemblies during password duplication.

FIGURE 5 illustrates interactions between a lock assembly and a key assembly while setting a password.

FIGURE 6 illustrates interactions between a lock assembly and a key assembly for mechanically operating the lock assembly.

FIGURE 7 illustrates a method for operation of a lock assembly in response to a key assembly.

FIGURE 8 illustrates a method for operation of a lock assembly to revert to a default state, for instance staying locked, in the absence of alternative instructions.

FIGURE 9 illustrates interactions between a lock assembly and a key assembly during a dynamic key assignment and distribution process.

DETAILED DESCRIPTION OF THE INVENTION

The invention encompasses embodiments that allow users to carry a large number of keys, actually passwords to electronic locks, without the cumbersome clanging keychain weighed down by mechanical keys. Moreover, the passwords are easily and securely duplicated, added to, or removed using friendly user interfaces. In addition, backup versions of the passwords can be stored to guard against accidentally losing a password.

In another aspect, the electronic key assembly is upgradeable, and do not suffer from the vulnerability of mechanical keys due to easy deciphering of a master key that operates several locks by trial and error in relatively few steps.

In another aspect, the lock assembly and key combinations taught by the invention may be reprogrammable or, alternatively, programmed only at the manufacturing stage. These combinations avoid the need to recall a large number of key codes or the risk of reverse engineering of mechanical keys including master keys. Optional, fixing of the key at the manufacturing stage allows customization for particular applications. Conventional mechanical locks are opened by one or more keys that are determined in the course of manufacturing the lock. In such mechanical locks, sometimes manufactured so as to admit of a 'master key,' the use of cryptographic techniques is known to lead to a key capable of duplicating the function of even the master key, thus posing a security risk since all keys to locks admitting of the master key necessarily share many characteristics. This draw back is not universal since mechanical locks, such as 'number locks' requiring a particular number combination, allow for choosing alternative combinations, but with the drawback of remembering particular combinations.. Electronic locks, however, often are reprogrammable, although this could be a security risk if the lock could be compromised by merely reprogramming it.

In an illustrative embodiment of the invention in **FIGURE 1**, the lock assembly **100** includes transmitter **105** and receiver **110** that are operatively coupled to electronic circuit **115**, which is preferably programmable, in communication

with a memory **120** or other store for identifiers and keys. The electronic circuit is also coupled to mechanical levers **125** that are operated to lock or unlock the lock assembly **100**.

Electronic lock assembly **100** is preferably a part of an electronic lock system comprising lock assembly **100** and electronic key assembly **200**, illustrated in **FIGURE 2**. Electronic key assembly 200 also has its transmitter **205** and receiver **210** so that it may communicate with electronic lock assembly **100** and other electronic key assemblies. In a preferred embodiment of the invention, user interface **220** is presented to the key user so that the user may select a password for a particular electronic lock or duplication to another key. Key electronic control circuit **215** coordinates the activities of the various key sub-parts. On electronic key assembly **200** one or more passwords are stored in a memory **225**, which may operate one or more locks. Additionally, a stored password on electronic key assembly **200** may be used to set the password for a lock using optional password-setting button **230**. Similarly, optional password-setting button **130** on the lock assembly allows setting of the password for a particular lock assembly. Preferably password-setting button **230** may be activated only during the manufacturing of the lock assembly or a limited number of times after the manufacturing.

Preferably user interface 220 has display 221 and is operated with the aid of one or more buttons, such as a physical scroll button **222** or a clickable displayed simulated button **223**, which may be operated with a pointing device **224** or other means. In addition, one or more of a clickable button, an infrared port, or a pressure sensitive surface may be used to either input or view desired information on user interface **220**.

A password is copied from one electronic key assembly to another electronic key assembly, as illustrated in **FIGURES 3** and **4**, by activating password duplication feature **400** on user interface **405** during step **300**, establishing link **410** between electronic key assemblies **415** and **420** during step **305**; receiving, via receiver **435** from transmitter **440**, a specified password to be duplicated at electronic key assembly **420** during step **310**; followed by storing the duplicate password on electronic key assembly **420** during step **315**. The password duplication feature is preferably accessed via user interfaces **405** and **430**, although automated duplication procedures may also be implemented in alternative embodiments. In such procedures the user need not expressly select the key duplication feature for a specific key and instead all of the passwords in a particular group of passwords on an electronic key assembly may be copied to another electronic key assembly. Or, instead of copying a password itself, a

property of the password is communicated and replicated in a generated password. Examples include algorithms for generating passwords using one or more seeds or parameters, which may be replicated by copying the parameters rather than a particular password.

Additionally, as mentioned previously, password-setting button **130** in lock assembly **100** allows setting of the password during manufacturing. Preferably in response to pressing of password-setting button **130** a random sequence is stored as a password for unlocking lock assembly **100**. This random sequence is also transmitted to an electronic key assembly for storage. Password setting function **230** is activated in key **200** to enable receiving and storing the random sequence as the password for lock assembly **100**. In an aspect designed to improve security password-setting button **130** is inactivated after setting the password of lock assembly **100** during manufacturing.

FIGURE 5 illustrates these interactions in additional detail. Password set button **500** of lock assembly **505** is activated resulting in electronic circuit **510** activating transmitter **515** to transmit a selected key sequence to receiver **520** of electronic key assembly **525**. Receiver **520** communicates with user interface **530**, possibly via electronic circuit **535**, to complete the process of password acceptance and storage on electronic key assembly **525**.

It should be noted that lock assembly **100** may correspond to more than one password for operating lock assembly **100**. Indeed, a particular password may unlock more than one lock. However, in contrast to typical lock and key systems with master keys, the various passwords need not be related, thus providing additional security compared to mechanical lock systems. This follows from the unrestricted choice available for selecting one or more passwords. Thus, several passwords for unlocking lock assembly **100** may be stored on a single key, or multiple keys, or a particular key may store passwords for unlocking more than one lock.

FIGURE 6 illustrates typical unlocking interactions between electronic key assembly **600** and electronic lock assembly **605**. User interface **610** receives instructions to unlock lock assembly **605** resulting electronic circuit **615** activating transmitter **620** of electronic key assembly **600** to send unlocking information to lock assembly **605** via receiver **625**, which is interpreted and/or processed by electronic circuit **630** resulting in operating mechanical parts **635** for unlocking or locking lock assembly **605**.

Although there is no limit on the number of passwords that may be stored on a key, it is preferred that several passwords be stored on a single key. For

instance, an electronic key assembly may store at least five passwords, preferably at least ten passwords, more preferably at least twenty passwords, even more preferably at least fifty passwords, and most preferably at least one hundred passwords. With a large number of passwords, their relative organization is preferably implemented with the passwords organized with the help of navigable folders accessible via the user interface corresponding to a key. Preferably, the password corresponding to the lock is transmitted from a key in response to a selection made via the user interface.

As illustrated in **FIGURE 7**, during step 700 a determination is made if a signal has been received. In response to receiving a signal control passes to step **705** for receiving a password. The control circuit in a lock assembly determines if there is a match between a password required by the lock assembly and the received password during step **710**. The match may be a common hash value and a public-private key setup to provide for secure communications. Alternatively, directed communication between keys and a key and a lock assembly may reduce the likelihood of eavesdropping. To this end there is considerable flexibility since either or both of the lock assembly transmitter and the key transmitter is coupled to one or more of an antenna and a light emitting diode and the like with corresponding receivers.

If there is a match, then, during step 715 the mechanical parts of the electronic lock assembly are operated to unlock or lock it. On the other hand, if there is no match then control passes to step **700**.

In another aspect, the lock assembly electronic control circuit is configured to, at a time point following unlocking, instruct the lock assembly mechanical parts to relock in a default mode. As shown in **FIGURE 8**, during step **800** a determination is made as to whether the electronic lock assembly is open. In effect, in response to the electronic lock assembly being open, an estimate of the time period for which the electronic lock assembly has been open is made. If a time threshold is satisfied during step **805** then control passes to step **810** for locking the electronic lock assembly. Otherwise, control stays at step **805**.

The invention also includes illustrative examples for designing an electronic lock assembly system. Typically, a method for designing such an electronic lock assembly system include providing a lock assembly transmitter and a lock assembly receiver; storage for one or more passwords; and a control circuit coupled to mechanical parts for locking and unlocking the electronic lock assembly. The control circuit unlocks the electronic lock assembly in response to receiving a password matching the stored password.

The electronic key assembly has a key transmitter and a key receiver as well as password storage locations. A control circuit may determine whether to transmit a password, its required encryption, implementation of various functions, and the like. The control circuit also interacts with a user via a user interface, for instance to provide functionality such as that for password duplication function for transmitting a password from one electronic key assembly to another electronic key assembly followed by storing of the transmitted password.

In another aspect, the electronic lock assembly preferably has a password-setting button. In response to activating the button, a password is stored by the electronic lock assembly such that receiving the password operates the lock assembly. Preferably, the button is operated during the manufacturing of the lock assembly and the stored password is transmitted to an electronic key assembly for operating the lock assembly. In another aspect, the electronic key assembly has a password-setting function so that the password received from the electronic lock assembly is stored on the electronic key assembly.

In another aspect, preferably the transmissions between electronic key assemblies or with the electronic lock are encrypted. An exemplary method may use a public key with the private key held on each device. By the optional use of digital signatures in some embodiments of the invention, secure communication channels may be established for transmission of the password and related information. It should be noted that the use of public-private keys is not required for practicing the invention, and any encryption scheme may be deployed to meet the particular security needs. In some embodiments, no encryption may be employed, or directed communication using narrow beams, key cards, and the like, may be used for additional security.

In an illustrative embodiment of the invention, a cellular phone, personal digital assistant, or other devices equipped with an infra red transmitter and receiver, with a programmable central processing unit, and a numerical keypad, can be operated as an electronic key assembly **200** to lock or unlock the lock assembly **100.** The non-volatile memory available on the above devices can be used to store different electronic keys with different key length for different security implementation levels. An embedded software application is programmed in the above devices to transmit the password, in a plain or encrypted format, over an unencrypted or encrypted digital data channel for key authentication.

In another aspect, the electronic lock assembly preferably operated with a dynamic electronic key assignment and redistribution functionality to enhance security. As illustrated in **Figure 9**, after an electronic key is send **900** over the

established link **410** between electronic key assemblies **415** and **420** during step **305**, and the correct electronic key is fully authenticated **905** on the electronic lock assembly **415**, a new electronic key is being generated **910** on the electronic circuit in lock assembly. The old key on the lock assembly will be disposed and deleted **910**. The key modification command with new key is being sent to the key assembly **915**. The old key will be overwritten by the new key on the key assembly **920**. The key assembly write new key on its memory and use for next authentication **925**.

Those of ordinary skill in the art will understand that other system architectures can be used to implement the methods of the present invention described above. While the discussion herein focuses on electronic key assemblies and electronic lock assemblies, those of ordinary skill in the art will recognize that the scope of the discussion is not so limited but applies equally to designing security systems and user friendly security devices. Although an illustrative embodiment of the invention has been described herein, various modifications may be made without departing from the spirit and scope of the invention described by the following claims.

CLAIMS

1. An electronic lock system comprising:

at least one lock assembly having a lock assembly transmitter, a lock assembly receiver, a lock assembly password setting button, a lock assembly electronic control circuit operatively coupled to lock assembly mechanical parts for locking and unlocking;

a first electronic key assembly having a key transmitter and a key receiver; a user interface presented to the key user; and a key electronic control circuit for coordinating the activities of the various key sub-parts; and

wherein the one or more passwords are stored on the electronic key assembly to operate the at least one lock assembly.

2. The electronic lock system of claim 1, wherein the user interface has a display and one or more of a scroll button, clickable button, infrared port, or pressure sensitive surface.

3. The electronic lock system of claim 1, wherein a password is copied from the first electronic key assembly to a second electronic key assembly by activating a password duplication feature in at least one of the first and second electronic key assemblies; establishing a link between the first and second electronic key assemblies; receiving a specified password at the second electronic key assembly; and finishing the duplication process by storing a new password in the second electronic key assembly.

4. The electronic lock system of claim 1, wherein the password duplication feature is accessed via the user interface.

5. The electronic lock system of claim 1 further comprising a password-setting button in the lock assembly, whereby during manufacturing responsive to pressing of the password-setting button a random sequence is stored as a password for unlocking the lock assembly; and the random sequence is also transmitted to the first key for storage as the password for unlocking the lock assembly.

6. The electronic lock system of claim 1, wherein the password-setting button is inactivated after setting the password of the lock during manufacturing.

7. The electronic lock system of claim 5, wherein a password setting function is activated in the first key, whereby the random sequence is received as the password for the lock assembly.

8. The electronic lock system of claim 5 wherein the lock assembly corresponds to a plurality of passwords for unlocking the lock assembly.

9. The electronic lock system of claim 8 wherein the plurality of passwords for unlocking the lock assembly are stored on the first key.

10. The electronic lock system of claim 9 wherein the first key also stores at least one password for unlocking at least one additional lock.

11. The electronic lock system of claim 9 wherein a number of passwords stored on the first key belongs to the set consisting of at least five passwords, at least ten passwords, at least twenty passwords, at least fifty passwords, and at least one hundred passwords.

12. The electronic lock system of claim 8 wherein at least one password for unlocking the lock assembly is stored on a second key assembly.

13. The electronic lock system of claim 1 wherein in response to receiving a password corresponding to the lock assembly, the lock assembly unlocks.

14. The electronic lock system of claim 1 wherein the password corresponding to the lock assembly is transmitted from the first key in response to a selection made via the user interface.

15. The electronic lock system of claim 1 wherein the lock assembly electronic control circuit is configured to, at a time point following unlocking, instruct the lock assembly mechanical parts to relock in a default mode.

16. The electronic lock system of claim 1 wherein at least one of the lock assembly transmitter and the key transmitter is coupled to one or more of an antenna and a light emitting diode.

17. A method for designing an electronic lock system, the method comprising the steps of:

providing a lock assembly transmitter and a lock assembly receiver in an electronic lock assembly having at least one stored password and a control circuit coupled to mechanical parts for locking and unlocking the electronic

lock assembly, wherein the control circuit unlocks the electronic lock assembly in response to receiving a password matching the stored password;

providing a key transmitter and a key receiver in a first electronic key assembly having at least one password storage location and a control circuit coupled to mechanical parts for locking and unlocking the electronic lock assembly;

providing a user interface for the first electronic key assembly, whereby a user selects at least one password stored on the first electronic key assembly to unlock the electronic lock assembly; and

implementing a password duplication function for transmitting a password from the first electronic key assembly to a second electronic key assembly followed by storing of the transmitted password on the second electronic key assembly.

18. The method of claim 17 further comprising providing a password-setting button in the electronic lock assembly, whereby a password is stored by the electronic lock assembly in response to operation of the password-setting button during the manufacturing of the lock assembly and the stored password is transmitted to the first electronic key assembly.

19. The method of claim 18 further comprising providing a password-setting function in the first electronic key assembly, whereby the password received from the electronic lock assembly is stored on the first electronic key assembly.

20. The method of claim 17, wherein at least one transmission between the first electronic key assembly and one or more of the electronic lock assembly and the second electronic key assembly is encrypted using a public key.

21. A method for designing an dynamic key assignment and distribution system, the method comprising the steps of:

providing a key assembly transmitter send a electronic key over an established data link for lock authentication;

providing a lock assembly receiver receive the key and authenticate the key and generate a new electronic key after successful authentication.

providing a lock assembly dispose, delete and expire the old key

providing a lock assembly transmitter send the newly generated key to the key assembly; and

the key assembly delete the old key and write the new key to its memory

providing the key assembly use the newly received key for next authentication

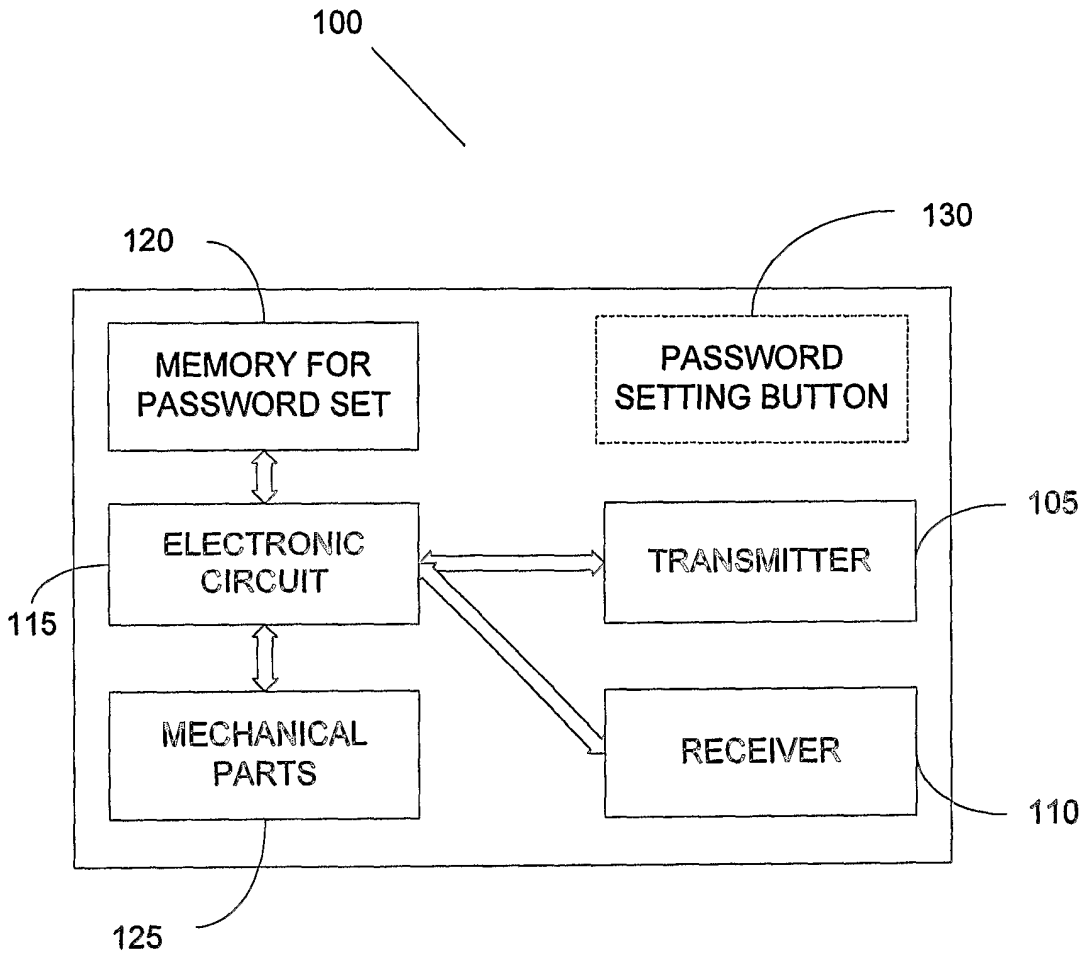

100
120
130
MEMORY FOR PASSWORD SET
PASSWORD SETTING BUTTON
ELECTRONIC CIRCUIT
TRANSMITTER
105
115
MECHANICAL PARTS
RECEIVER
110
125

FIG.1

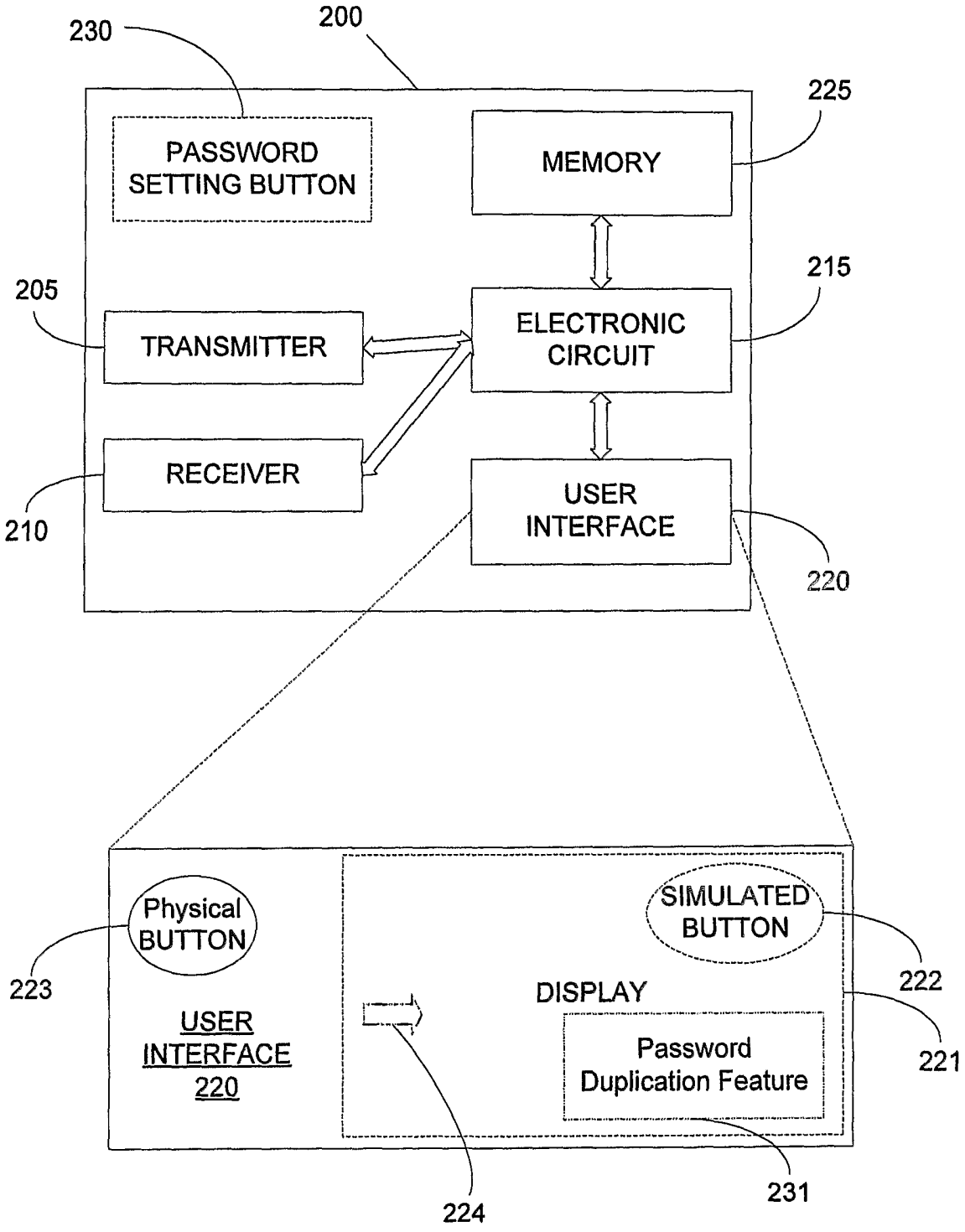

230
200
225
PASSWORD SETTING BUTTON
MEMORY
215
205
TRANSMITTER
ELECTRONIC CIRCUIT
RECEIVER
210
USER INTERFACE
220
Physical BUTTON
223
SIMULATED BUTTON
222
DISPLAY
USER INTERFACE 220
Password Duplication Feature
221
224
231

FIG.2

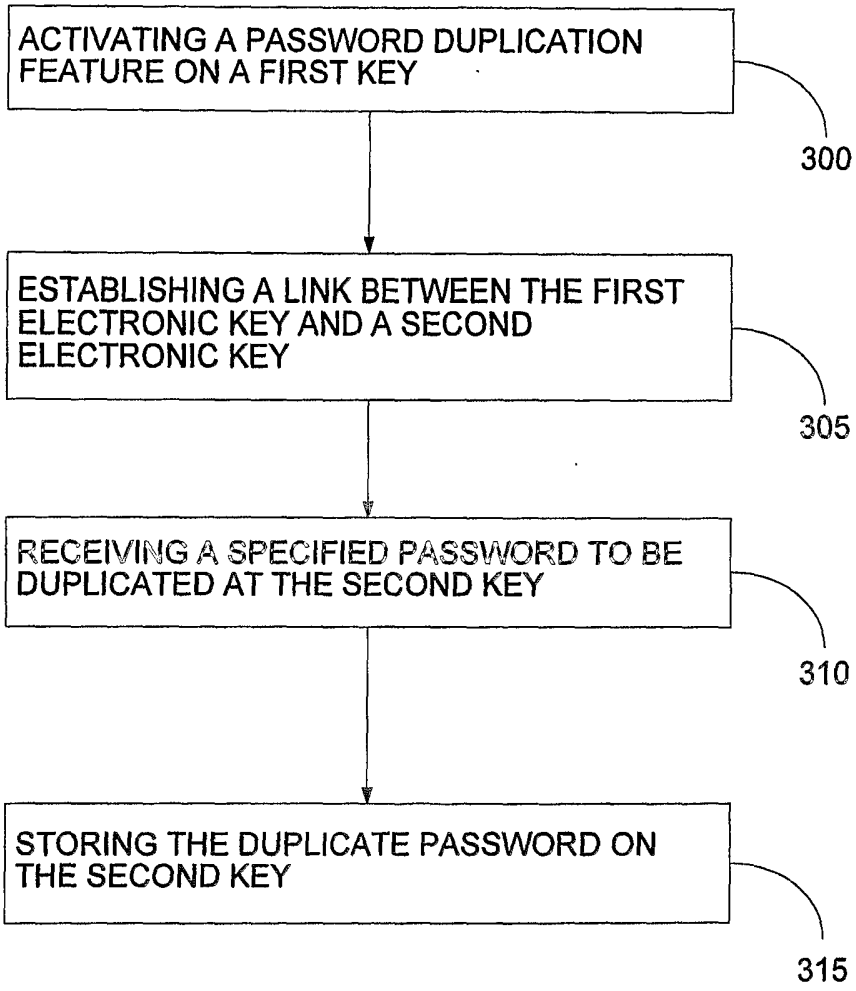

ACTIVATING A PASSWORD DUPLICATION FEATURE ON A FIRST KEY
300
ESTABLISHING A LINK BETWEEN THE FIRST ELECTRONIC KEY AND A SECOND ELECTRONIC KEY
305
RECEIVING A SPECIFIED PASSWORD TO BE DUPLICATED AT THE SECOND KEY
310
STORING THE DUPLICATE PASSWORD ON THE SECOND KEY
315

FIG.3

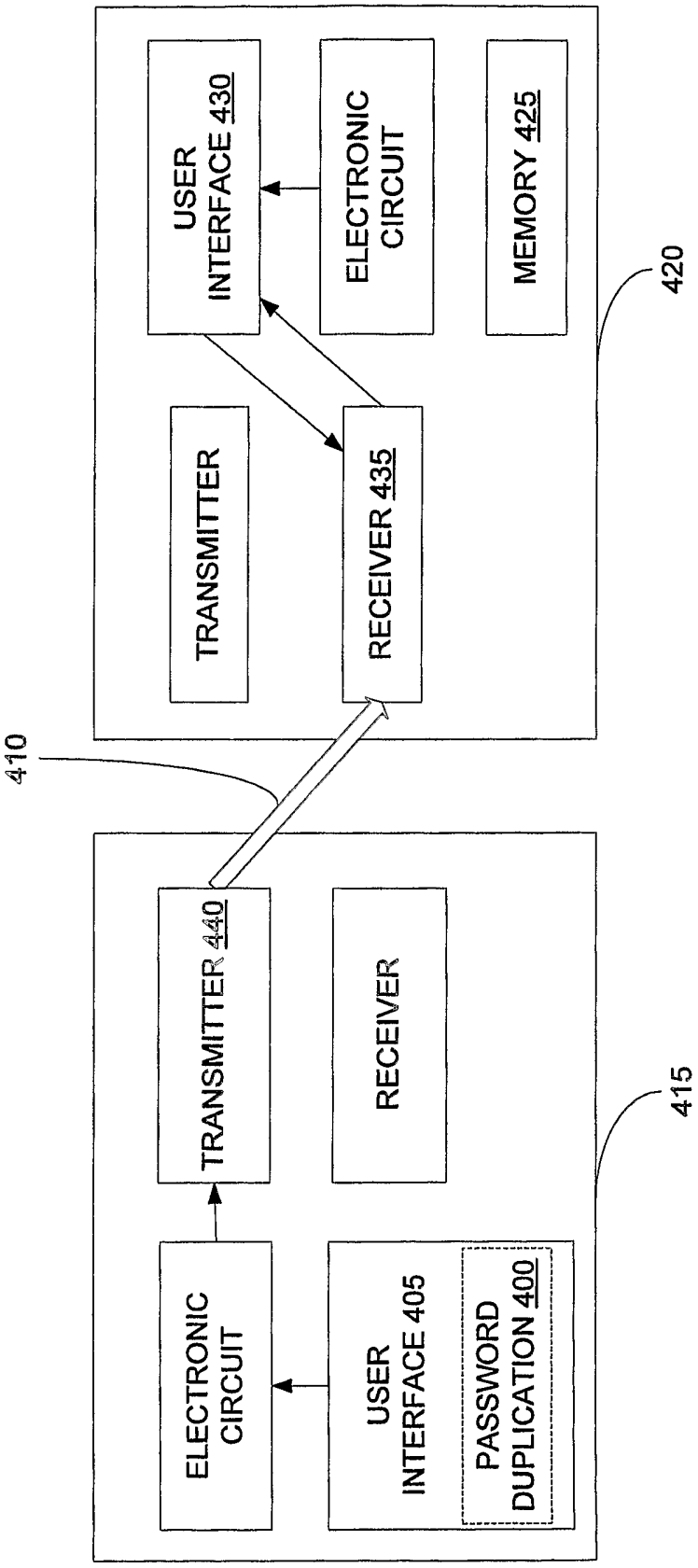

USER INTERFACE 430
ELECTRONIC CIRCUIT
MEMORY 425
420
TRANSMITTER
RECEIVER 435
410
TRANSMITTER 440
RECEIVER
415
ELECTRONIC CIRCUIT
USER INTERFACE 405
PASSWORD DUPLICATION 400

FIG. 4

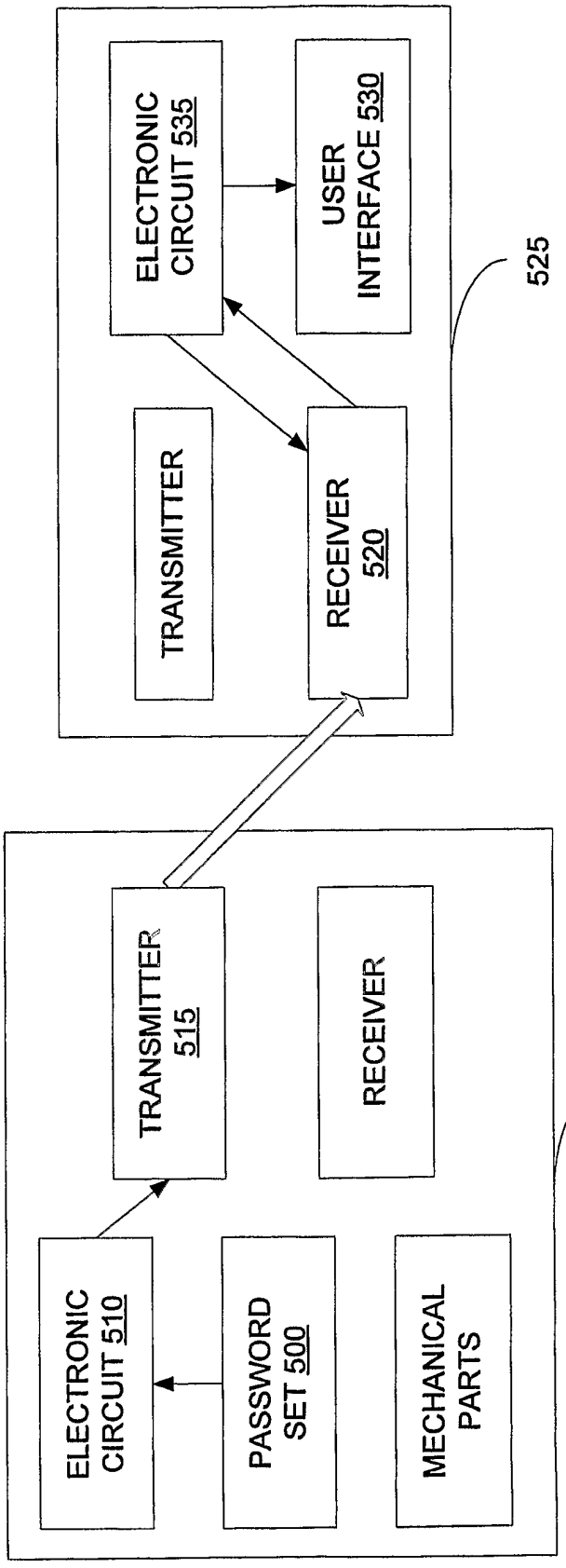

ELECTRONIC CIRCUIT 535
USER INTERFACE 530
525
TRANSMITTER
RECEIVER 520
TRANSMITTER 515
RECEIVER
505
ELECTRONIC CIRCUIT 510
PASSWORD SET 500
MECHANICAL PARTS

FIG. 5

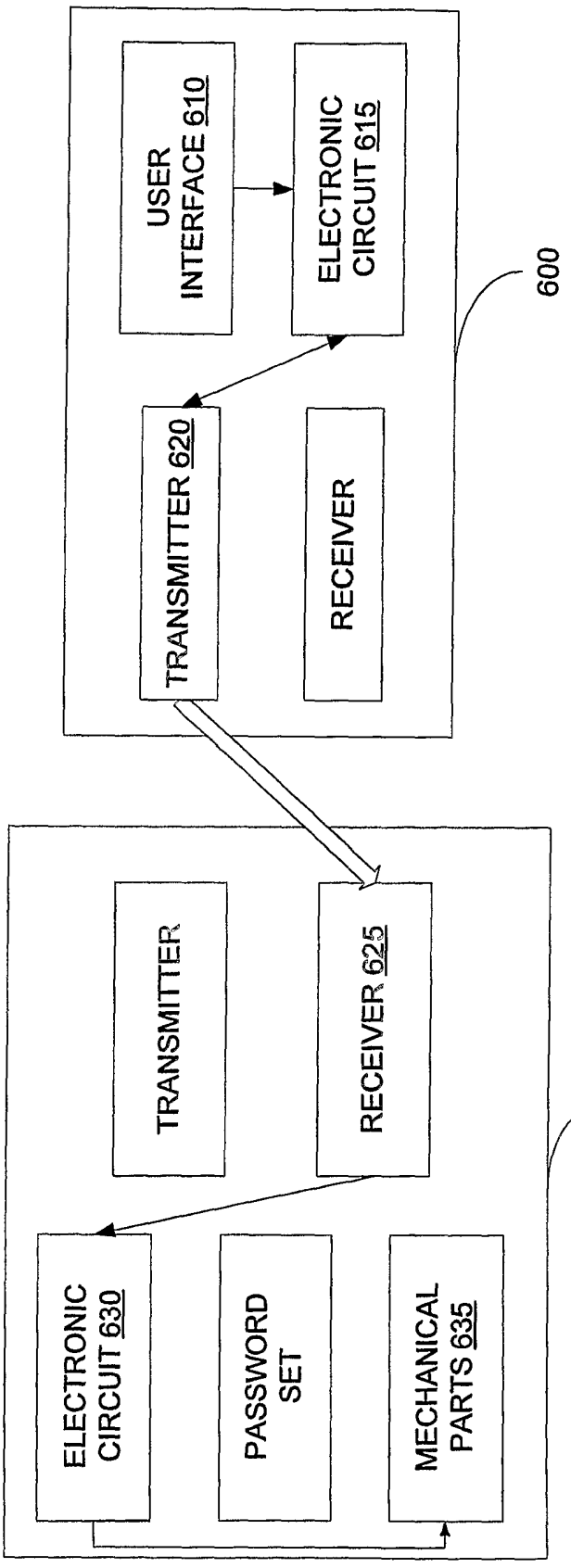

USER INTERFACE 610
ELECTRONIC CIRCUIT 615
600
TRANSMITTER 620
RECEIVER
TRANSMITTER
RECEIVER 625
605
ELECTRONIC CIRCUIT 630
PASSWORD SET
MECHANICAL PARTS 635

FIG. 6

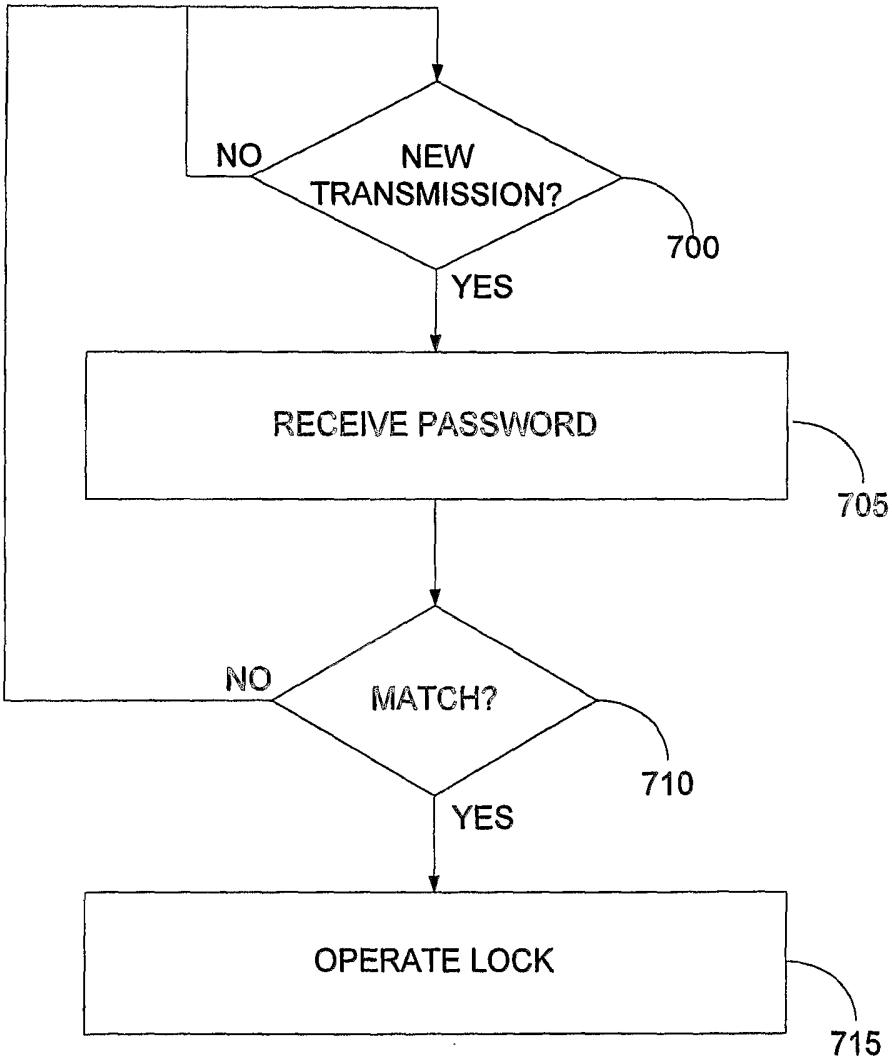

NO
NEW TRANSMISSION?
700
YES
RECEIVE PASSWORD
705
NO
MATCH?
710
YES
OPERATE LOCK
715

FIG. 7

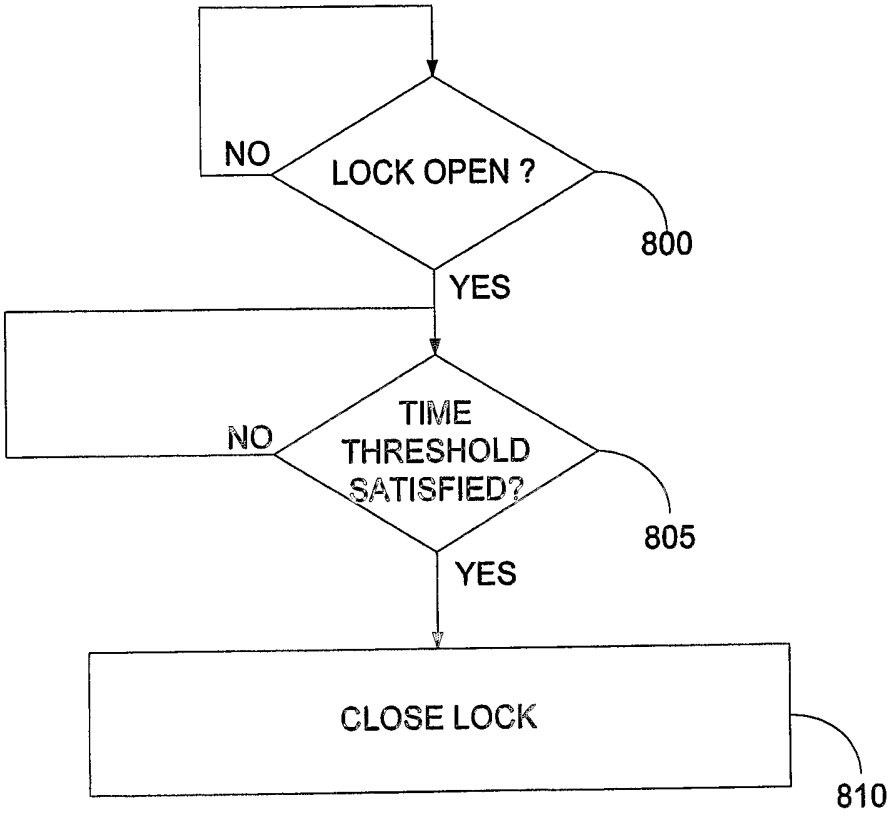

NO
LOCK OPEN ?
800
YES
NO
TIME
THRESHOLD
SATISFIED?
805
YES
CLOSE LOCK
810

FIG. 8

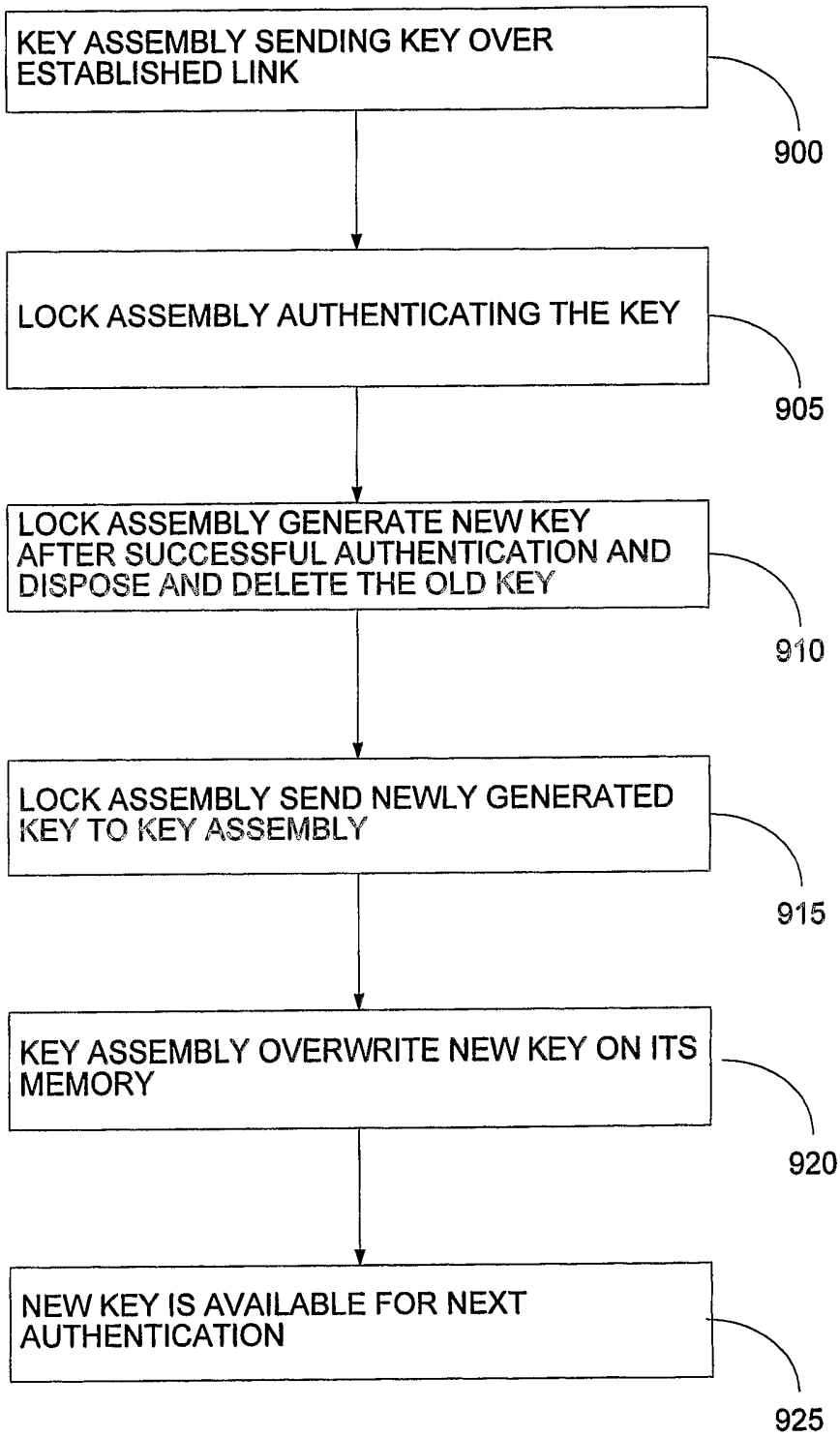

KEY ASSEMBLY SENDING KEY OVER ESTABLISHED LINK
900
LOCK ASSEMBLY AUTHENTICATING THE KEY
905
LOCK ASSEMBLY GENERATE NEW KEY AFTER SUCCESSFUL AUTHENTICATION AND DISPOSE AND DELETE THE OLD KEY
910
LOCK ASSEMBLY SEND NEWLY GENERATED KEY TO KEY ASSEMBLY
915
KEY ASSEMBLY OVERWRITE NEW KEY ON ITS MEMORY
920
NEW KEY IS AVAILABLE FOR NEXT AUTHENTICATION
925

FIG.9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2004/000249

A. CLASSIFICATION OF SUBJECT MATTER

IPC[7]E05B37/20

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)

IPC[7]E05B37/20, E05B49/04

Documentation searched other than minimum documentation to the extent that such documents are included in the field searched

Chinese patent document(1985~)

Electronic data base consulted during the international search(name of data base and, where practicable, search terms used)
CNPAT, WPI, PAJ, EPODOC
Circuit,key,pasword

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant claim No.
A	CN2075238U (HUANG,Weijie) 17 Apr.1991(17.04.91) Claim 1; figure1	1-21
A	CN1221846A (YU,Yilun) 7 Jul.1999(07.07.99) Claim 1; figure1	1-21
A	US5164718(Stig Cedergren) 17 Nov. 1992(17.11.92) Claim 1; figure1	1-21
A	JP8-277664(OKI ELECTRIC IND CO LTD) 22 Oct. 1996(22.10.96) Claim 1; figure1	1-21
A	JP2003-27788(BIONICS KK) 29 Jan. 2003(29.01.03) Claim 1; figure1	1-21

☐ 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 document 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	Date of mailing of the international search report
13 Jul. 2004 (13.07.04)	29 JUL 2004 (29.07.2004)
Name and mailing address of the ISA/ The Chinese Patent Office 6, Xitucheng Road, Haidian District, Beijing, 100088, China Facsimile No. 86-10-62019451	Authorized officer XIA,Dong Telephone No. (86-10)62084843

Form PCT/ISA/210(second sheet)(July 1992)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2004/000249

Patent document cited in search report	Publication date	Patent family members	Publication date
US5164718	17.11.92	SE8703775	1989-03-31
		WO89029689	1989-04-06
		AU2529988	1989-04-18
		DK79890	1990-03-29
		DK169389B	1994-10-17
		SE462174	1990-05-14
		EP0389495	1990-10-03
		EP19880908772	1988-09-27
		JP3500312T	1991-01-24
		AU618034	1991-12-12
		AT100516	1994-02-15
		DE3887341D	1994-03-03
		DE3887341T	1994-05-11