(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 807 733 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
19.11.1997 Bulletin 1997/47

(51) Int Cl.^{6}: E05B 49/00

(21) Application number: 97303313.7

(22) Date of filing: 15.05.1997

(84) Designated Contracting States:
DE FR GB

(30) Priority: 16.05.1996 JP 121869/96
13.09.1996 JP 243555/96

(71) Applicant: SONY CORPORATION
Tokyo 141 (JP)

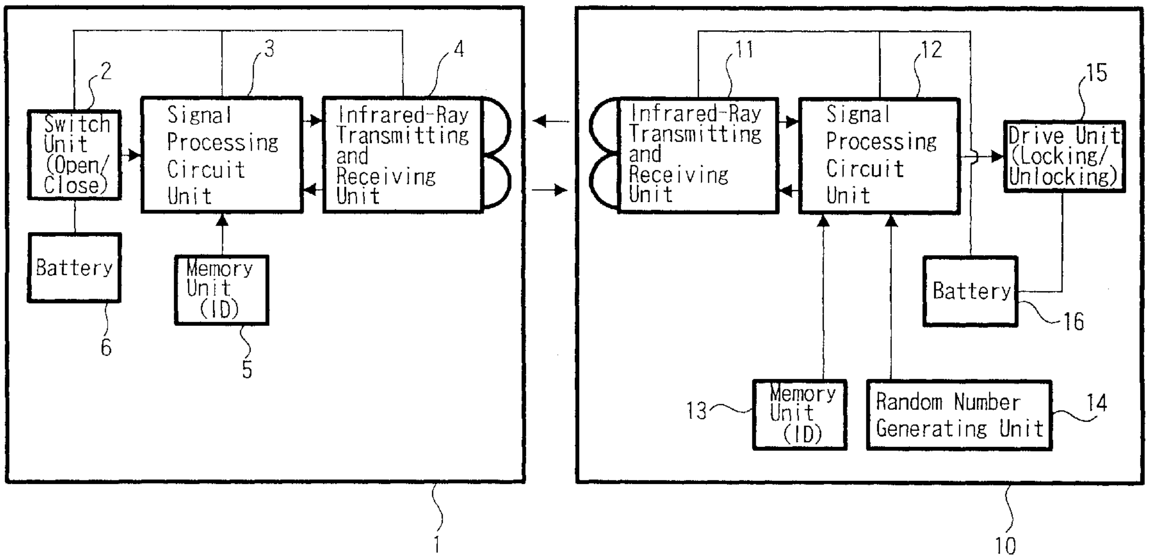
(72) Inventors:
- Takamatsu, Hiroyuki,
  Sony Corp. Intell. Prop. Div.
  Tokyo 141 (JP)
- Harada, Yoshio, Sony Corp. Intell. Prop. Div.
  Tokyo 141 (JP)

(74) Representative: Pilch, Adam John Michael et al
D. YOUNG & CO.,
21 New Fetter Lane
London EC4A 1DA (GB)

(54) Identification signal checking apparatus and methods

(57) An identification signal checking apparatus includes an apparatus (1) to be detected having a first wireless transmitting and receiving unit (4) , a first signal processing unit (3) and a first memory unit (5) for storing an identification signal. A detecting apparatus (10) has a second wireless transmitting and receiving unit (11), a second signal processing unit (12), a second memory unit (13) for storing an identification signal, and a random number generating unit (14). When the detecting apparatus (10) receives a response request signal from the apparatus (1) to be detected, the detecting apparatus (10) transmits a random number signal obtained from the random number generating unit (14). When receiving the random number signal, the apparatus (1) to be detected encrypts the identification signal stored in the first memory unit (5) by using the random number signal and transmits the encrypted identification signal to the detecting apparatus (10). The detecting apparatus (10) decrypts the encrypted identification signal and checks whether or not it coincides with the identification signal stored in the second memory unit (13).

FIG. 1


Switch Unit (Open/Close)
2
Signal Processing Circuit Unit
3
Infrared-Ray Transmitting and Receiving Unit
4
Battery
6
Memory Unit (ID)
5
1
Infrared-Ray Transmitting and Receiving Unit
11
Signal Processing Circuit Unit
12
Drive Unit (Locking/Unlocking)
15
Battery
16
Memory Unit (ID)
13
Random Number Generating Unit
14
10

Printed by Jouve, 75001 PARIS (FR)

Description

The present invention relates to identification signal checking apparatus and methods, such as those suitable for use in a keyless entry system.

A keyless entry system has been proposed. In this keyless entry system, infrared rays or radio waves are used to transmit an identification signal from a key apparatus side to a lock apparatus side for the locking or the unlocking thereof.

Such keyless entry system employs a one-way communication in which the key apparatus side constantly transmits the same identification signal. Therefore, when this communication is intercepted, the identification signal may disadvantageously be stolen easily.

Particularly when the identification signal is transmitted by using the infrared rays, it is possible to copy the identification signal easily by a so-called learning remote controller, which has already been developed into a social problem.

Moreover, since in the above keyless entry system it is possible to detect a specific identification signal by using each of various identification signals to detect whether or not the identification signal coincides with the specific identification signal, there is the critical disadvantage in security.

Therefore, a keyless entry system has been proposed in which a portable apparatus (key apparatus) transmits an encryption value to a main apparatus (lock apparatus) and the main apparatus determines whether or not an encryption value which it obtains by itself by calculation of a value signal coincides with the received encryption value (see Japanese laid-open patent publication No. 7-269196 and Japanese laid-open patent publication No. 7-274258).

In such proposed keyless entry system, since the main apparatus determines whether or not the encryption value which it obtains by itself by calculation of the value signal coincides with the received encryption value, the security is improved.

However, in the previously proposed keyless entry system with a satisfactory security, since the main apparatus determines whether or not the encryption value which it obtains by itself by calculation of the value signal coincides with the received encryption value, except when the portable apparatus (key apparatus) and the main apparatus (lock apparatus) are manufactured, it is impossible that, after the portable apparatus and the main apparatus are manufactured, a specific identification signal is registered in both of the key apparatus and the main apparatus by transmitting the same specific identification signal from the portable apparatus to the main apparatus.

Therefore, in such system, when the portable apparatus (key apparatus) and the main apparatus (lock apparatus) are manufactured, the same specific identification signal is registered in both of them. Therefore, it is necessary to manage both of the portable apparatus (key apparatus) and the main apparatus (lock apparatus) as a pair of objects to be managed until the lock apparatus is finally built in a door, for example. This necessity leads to the disadvantage in effective management and in physical distribution.

In view of such aspects, it is therefore an aim of the present invention to improve the security with a comparatively simple arrangement and to make it unnecessary to manage the key apparatus (apparatus to be detected) and the lock apparatus (detecting apparatus) as a pair of separate items to be managed.

According to an aspect of the present invention, an identification signal checking apparatus includes an apparatus to be detected having a first wireless transmitting and receiving unit, a first signal processing unit and a first memory unit for storing an identification signal and includes a detecting apparatus having a second wireless transmitting and receiving unit, a second signal processing unit, a second memory unit for storing an identification signal, and a communication permission signal generating means. When the detecting apparatus receives a response request signal from the apparatus to be detected, the detecting apparatus transmits a random number signal obtained from the random number generating unit. When receiving the random number signal, the apparatus to be detected encrypts said identification signal stored in the first memory unit by using the random number signal and transmits the encrypted identification signal to the detecting apparatus. The detecting apparatus decrypts the encrypted identification signal and checks whether or not the decrypted identification signal coincides with the identification signal stored in the second memory unit.

According to the present invention, the detecting (lock apparatus) transmits the random number signal and the apparatus to be detected (key apparatus) encrypts the identification signal by using the random number signal and transmits it to the detecting apparatus. Therefore, since the identification signal transmitted from the apparatus to be detected to the detecting apparatus is the encrypted signal obtained by encryption employing the random number signal and hence is always an unique signal, the security is improved.

According to the present invention, since the detecting apparatus decrypts the encrypted identification signal, even if the apparatus to be detected and the detecting apparatus are separately manufactured and distributed on the market, when the detecting apparatus is built in a door or the like, the detecting apparatus (lock apparatus) decrypts the encrypted signal transmitted from the apparatus to be detected (key apparatus) to obtain the specific identification signal. If the identification signal obtained by decryption is registered in the detecting apparatus, then it is possible to register the same identification signal in both of the apparatus to be detected (key apparatus) and the detecting apparatus (lock apparatus) .

The invention will now be described by way of example with reference to the accompanying drawings, throughout which like parts are referred to by like references, and in which:

FIG. 1 is a block diagram showing an arrangement of an identification signal checking apparatus according to a first embodiment of the present invention;

FIG. 2 is a flowchart used to explain an operation of the identification signal checking apparatus according to the first embodiment of the present invention;

FIGS. 3A to 3D are timing charts used to explain communication between a key apparatus and a lock apparatus according to the first embodiment of the present invention;

FIG. 4 is a block diagram showing an arrangement of an identification signal checking apparatus according to a second embodiment of the present invention;

FIG. 5 is a flowchart used to explain an operation of the identification signal checking apparatus according to the second embodiment of the present invention;

FIG. 6 is a block diagram showing an arrangement of an identification signal checking apparatus according to a third embodiment of the present invention; and

FIG. 7 is a flowchart used to explain an operation of the identification signal checking apparatus according to the third embodiment of the present invention.

An identification signal checking apparatus and an identification signal checking method according to a first embodiment of the present invention will be described with reference to the accompanying drawings. In this embodiment, the identification signal checking apparatus and method are applied to a keyless entry system for opening and closing a door.

As shown in FIG. 1, a portable key apparatus 1 (an apparatus to be detected) has a switch unit 2 for issuing commands to open and close a door, a signal processing circuit unit 3, an infrared-ray transmitting and receiving unit 4 for communicating with a lock apparatus 10 described later on, and a memory unit 5 for storing a specific (own) identification signal ID.

The signal processing circuit unit 3 is formed of a microcomputer. When the switch unit 2 issues a commend to open or close the door by operating a switch thereof, the signal processing circuit unit 3 generates a response request signal including a lock/unlock command signal and supplies this response request signal to the infrared-ray transmitting and receiving unit 4. The infrared-ray transmitting and receiving unit 4 transmits the response request signal to the lock apparatus 10.

When the key apparatus 1 receives a random number signal X formed of 24 bits, for example, from the lock apparatus 10, the signal processing circuit unit 3 encrypts a specific identification signal ID of 24 bits, for example, stored in the memory unit 5 to convert it into a code signal of 24 bits, for example, in accordance with a predetermined function f(X, ID) by using the 24-bit random number signal X, for example. Then, the signal processing circuit unit 3 transmits the encrypted signal f(X, ID) to the lock apparatus 10.

This function f(X, ID) is defined as shown below, for example, such that if respective corresponding bits of the random number signal X and the identification signal ID have the same value of "1" or "0", then the value of a corresponding bit in the function f(X, ID) is set to "1" and if the respective corresponding bits have the values different from each other, then the value thereof in the function f(X, ID) is set to "0".

Table 1

ID	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
X	1	1	0	1	1	1	0	1	1	1	0	1	1	1	0	1	1	1	0	1	1	1	0	1
f (X, ID)	0	1	1	1	0	1	1	1	0	1	1	1	0	1	1	1	0	1	1	1	0	1	1	1

The infrared-ray transmitting and receiving unit 4 according to this embodiment is arranged so as to carry out communication in accordance with a known base band system. The base band system permits high-speed communication at a lower consumed power and simplifies a circuit arrangement as compared with other modulation systems such as an amplitude shift keying (ASK), a frequency shift keying (FSK) or the like.

The lock apparatus 10 is provided at a predetermined position in association with the door. The lock apparatus 10 has an infrared-ray transmitting and receiving unit 11 for communicating with the key apparatus 1, a signal processing circuit unit 12, a memory unit 13 for storing a specific (own) identification signal ID, a random number generating unit 14 for generating the random number signal X, and a drive unit 15 for controlling a door locking or unlocking operation based on a command signal from the signal processing circuit unit 12.

A binary counter for processing 24 bits, for example, is employed as the random number generating unit 14. This 24-bit binary counter carries out a count operation in accordance with a predetermined clock signal regardless of the communication. When the lock apparatus 10 receives the response request signal from the key apparatus 1, the operation of the 24-bit binary counter is stopped and then a count value of the binary counter at this time is read, thereby the 24-bit random number signal X, for example, being obtained.

The signal processing circuit unit 12 is formed of a microcomputer. When the lock apparatus 10 receives the response request signal from the key apparatus 1, the signal processing circuit unit 12 transmits the random number signal X generated by the random number generating unit 14 from the lock apparatus 10 to the key apparatus 1.

When the lock apparatus 10 receives from the key apparatus 1 the encrypted signal f(X, ID) obtained by encrypting the identification signal ID with the random number signal X, the signal processing circuit unit 12 decrypts the received encrypted signal f(X, ID) in accordance with a predetermined function f^{-1}\{f(x, ID), X\} by using the previously transmitted 24-bit random number signal X, for example, and checks whether or not the identification signal ID obtained by this decryption coincides with the specific (own) identification signal ID previously stored (registered) in the memory unit 13.

As a result of the check processing, if the decrypted identification signal ID coincides with the identification signal ID previously stored (registered), then the signal processing circuit unit 12 supplies a locking/unlocking command signal based on a door opening/closing command included in the response request signal to the drive unit 15. Then, under the operation of the drive unit 15, the door is opened or closed.

The infrared-ray transmitting and receiving unit 11 according to this embodiment is arranged similarly to the above-mentioned infrared-ray transmitting and receiving unit 4, and arranged so as to carry out communication in accordance with the known base band system. In FIG. 1, batteries 6 and 16 are used for energizing the key apparatus 1 and the lock apparatus 10, respectively.

An operation of the keyless entry system for opening and closing a door according to this embodiment will be described with reference to FIG. 2 which is a flowchart therefor and with reference to FIGS. 3A to 3D which are timing charts therefor. In this embodiment, it is assumed that the same specific (own) identification signals ID, e.g., the identification signals ID formed of codes of 24 bits, for example, are previously registered (stored) in the memory units 5 and 13.

In step S1 of the flowchart shown in FIG. 2, the switch unit 2 of the key apparatus 1 is operated and the switch thereof is set in its on-state, thereby a command to open or close a door being issued. In step S2, as shown in FIG. 3A, for example, the key apparatus 1 transmits the response request signal including the door opening/closing command signal to the lock apparatus 10 for a period of 100 ms. Then, the processing proceeds to step S3.

In step S3, the lock apparatus 10 receives the response request signal as shown in FIG. 3D. Then, the processing proceeds to step S4, wherein the lock apparatus 10 obtains the 24-bit random number signal X, for example, generated by the random number generating unit 14. In step S5, as shown in FIG. 3C, the lock apparatus 10 transmits the random number signal X to the key apparatus 1 for a period of 30 ms. Then, the processing proceeds to step S6.

In step S6, the key apparatus 1 receives the random number signal X as shown in FIG. 3B. Then, the processing proceeds to step S7, wherein the key apparatus 1 encrypts the specific (own) identification signal ID registered in the memory unit 5 to convert it into the 24-bit code signal, in accordance with the predetermined function f(X, ID) by using the 24-bit random number signal X, for example, and obtains the encrypted signal f(X, ID). Then, the processing proceeds to step S8, wherein the key apparatus 1 transmits the encrypted signal f(X, ID) to the lock apparatus 10 during the period of 30 ms, for example, as shown in FIG. 3A. Then, the processing proceeds to step S9.

In step S9, the lock apparatus 10 receives the encrypted signal f(X, ID) as shown in FIG. 3D. Then, the processing proceeds to step S10, wherein the lock apparatus 10 decrypts the received encrypted signal f(X, ID) in accordance with the predetermined function f^{-1}\{f(x, ID), X\} by using the previously transmitted random number signal X. Then, the processing proceeds to step S11, wherein the lock apparatus 10 checks whether or not the decrypted identification signal ID coincides with the specific (own) identification signal ID previously registered in the memory unit 13. In step S12, as a result of the check processing, if the decrypted identification signal ID coincides with the specific (own) identification signal ID previously registered (stored) in the memory unit 13, then, in accordance with the door opening or closing command signal of the response request signal, the signal processing circuit unit 12 supplies the unlocking or locking command signal to the drive unit 15 for carrying out the unlocking or locking operation of the door. Then, under the control of the drive unit 15, the door is opened or closed.

According to this embodiment, every time when the operation of opening or closing the door is attempted, the lock apparatus 10 generates the random number signal X and the key apparatus 1 encrypts the identification signal ID by using the random number signal X and transmits the encrypted signal f(X, ID) to the lock apparatus 10. Therefore, since the signals transmitted in this both-way communication are constantly different from each other, even if these communication signals are intercepted, the specific (own) identification signal ID is prevented from being stolen.

According to this embodiment, even if the operation of opening or closing the door is attempted any times, the possibility that the code signals coincide with each other by accident is constant, e.g., the possibility is constantly about one over 16.7 million in a case of the 24-bit code signal. Therefore, it is advantageously possible to realize the extremely high security with ease.

Since the lock apparatus 10 decrypts the encrypted identification signal f(X, ID), even if the key apparatus 1 and the lock apparatus 10 are separately manufactured and distributed on a market, when the lock apparatus 10 is built in a door or the like, the lock apparatus 10 decrypts the encrypted signal f(X, ID) transmitted from the key apparatus 1 to obtain the specific (own) identification signal ID. Therefore, if the identification signal ID obtained by decryption is registered in the memory unit 13 of the lock apparatus 10, then it is possible to register the same identification signal ID in both of the key apparatus 1 and the lock apparatus 10.

Therefore, according to the first embodiment, it is not necessary to manage both of the key apparatus 1 and the lock apparatus 10 as a pair of the objects to be managed, which leads to the advantages in effective management and physical distribution.

An identification signal checking apparatus according to a second embodiment of the present invention will be described with reference to FIGS. 4 and 5. In FIG. 4, parts corresponding to those in FIG. 1 are marked with the same reference numerals and hence need not be described.

In the second embodiment, a nonvolatile memory unit 5 of a key apparatus 1 stores a plurality of, e.g., sixteen identification signals ID_1, ID_2, ..., ID_{16}.

When a key apparatus 1 receives a random number signal X of 24 bits, for example, from a lock apparatus 10, a signal processing circuit unit 3 of the key apparatus 1 determines which of random number signals X_1, X_2, ..., X_{16} a random number signal formed of lower 4 bits of the 24 bits of the received random number signal X is, and, if the lower 4-bit random number signal is a random number signal X_1, selects one of sixteen identification signals ID_1, ID_2, ..., ID_{16} stored in the memory unit 5, e.g., the identification signal ID_1 in response to the random number signal X_1.

In this embodiment, as shown in Table 2, the random number signals X_1, X_2,..., X_{16} formed of the lower 4 bits of the above 24-bit random number signal X respectively correspond to sixteen identification signals ID_1, ID_2, ..., ID_{16} stored in the memory unit 5.

Table 2

lower 4-bit random number	identification signal	encrypted signal
X_1 = 0000	ID_1	f(X, ID_1)
X_2 = 0001	ID_2	f(X, ID_2)
:	:	:
:	:	:
X_{16} = 1111	ID_{16}	f(X, ID_{16})

In this second embodiment, each of the sixteen identification signals ID_1, ID_2, ..., ID_{16} stored in the memory unit 5 is formed of 24 bits, for example.

In this second embodiment, the signal processing circuit unit 3 encrypts one of the identification signals ID_1, ID_2, ..., ID_{16} selected as shown in Table 2 in response to the received one of the lower 4-bit random number signal X_1, X_2, ..., X_{16} of the random number signal X by using the received random number signal X, and obtains one of the encrypted signals f(X, ID_1), f(X, ID_2), ..., f(X, ID_{16}) shown in Table 2. The key apparatus 1 transmits the obtained one of the encrypted signals f(X, ID_1), f(X, ID_2), ..., f(X, ID_{16}) to the lock apparatus 10.

The same identification signals, e.g., the sixteen identification signals ID_1, ID_2, ..., ID_{16} stored in the memory unit 5 of the key apparatus 1 are also stored in the memory unit 13 of the lock apparatus 10 shown in FIG. 4.

The signal processing circuit unit 12 of the lock apparatus 10 stores the 24-bit random number signal X, for example, generated by the random number generating unit 14 and transmitted therefrom in response to the response request signal from the key apparatus 1, and selects one of, for example, the sixteen identification signals ID_1, ID_2, ..., ID_{16} stored in the memory unit 13 similarly to the key apparatus 1 in response to the selected one of the lower 4-bit random number signals X_1, X_2, ..., X_{16} of the random number signal X.

In this case, the identification signal selected by the key apparatus 1 in response to one of the lower 4-bit random number signal X_1, X_2, ..., X_{16} of the random number signal X is set the same as the identification signal selected by the lock apparatus 10 in response to the same one of the lower 4-bit random number signal X_1, X_2, ..., X_{16} of the random number signal X.

When the lock apparatus 10 receives from the key apparatus 1 one of the encrypted signals f(X, ID_1), f(X, ID_2), ..., f(X, ID_{16}) obtained by encrypting the selected one of the identification signals ID_1, ID_2, ..., ID_{16}, e.g., the encrypted signal f(X, ID1) by using the random number signal X, the signal processing circuit unit 12 decrypts the encrypted signals f(X, ID_1) in accordance with a predetermined function f^{-1}{f(X, ID_1), X} by using the identification signal ID_1 selected in response to the random number signal X_1, for example, selected from the lower 4-bit random number signals X_1, X_2,..., X_{16} of the random number signal X, and checks whether or not the identification signal ID_1 obtained by the decryption coincides with the one of the identification signals ID_1, ID_2,..., ID_{16} previously selected in response to the lower 4-bit random number signals X_1, X_2, ..., X_{16} of the random number signal X, e.g., the identification signal ID_1.

Other parts and units of the identification signal checking apparatus according to the second embodiment shown in FIG. 4 are arranged similarly to those of the identification signal checking apparatus according to the first embodiment shown in FIG. 1.

An operation of the keyless entry system for opening and closing a door according to the second embodiment shown in FIG. 4 will be described with reference to FIG. 5 which is a flowchart therefor. In this second embodiment, it is assumed that the same sixteen identification signals ID_1, ID_2, ..., ID_{16} formed of codes of 24 bits, for example, are previously stored (registered) in both of the memory units 5 and 13.

In step S21 of the flowchart shown in FIG. 5, the switch unit 2 of the key apparatus 1 is operated, thereby a command to open or close a door being issued. In step S22, as shown in FIG. 3A, for example, the key apparatus 1 transmits the response request signal including the door opening/closing command signal to the lock apparatus 10 for a period of 100 ms. Then the processing proceeds to step S23.

In step S23, the lock apparatus 10 receives the response request signal as shown in FIG. 3D. Then, the processing proceeds to step S24, wherein the lock apparatus 10 obtains the 24-bit random number signal X, for example, generated by the random number generating unit 14. In step S25, as shown in FIG. 3C, the lock apparatus 10 transmits the random number signal X to the key apparatus 1 for the period of 30 ms, for example. Then, the processing proceeds to step S26.

In step S26, the key apparatus 1 receives the random number signal X as shown in FIG. 3B. Then, the processing proceeds to step S27, wherein the key apparatus 1 selects one of the sixteen identification signals ID_1, ID_2, ..., ID_{16} registered in the memory unit 5, e.g., the identification signal ID_1 in response to one of the lower 4-bit random number signals X_1, X_2, ..., X_{16} of the random number signal X. Then, the processing proceeds to step S28.

In step S28, the key apparatus 1 encrypts the selected identification signal ID_1 to convert it into the 24-bit code signal, in accordance with a predetermined function f(X, ID_1) by using the 24-bit random number signal X, for example, and then obtains the encrypted signal f(X, ID_1). Then, the processing proceeds to step S29, wherein the key apparatus 1 transmits the encrypted signal f(X, ID_1) to the lock apparatus 10 during the period of 30 ms, for example, as shown in FIG. 3A. Then, the processing proceeds to step S30.

In step S30, the lock apparatus 10 receives the encrypted signal f(X, ID_1) as shown in FIG. 3D. Then, the processing proceeds to step S31, wherein the lock apparatus 10 decrypts the received encrypted signal f(X, ID_1) in accordance with a predetermined function f^{-1}{f(X, ID_1), X} by using the previously transmitted random number signal X. Then, the processing proceeds to step S32.

In step S32, the lock apparatus 10 checks whether or not the decrypted identification signal ID_1 coincides with the one of the sixteen identification signals ID_1, ID_2, ..., ID_{16} registered in the memory unit 13, e.g., the identification signal ID_1 selected in response to the selected one of the lower 4-bit random number signals X_1, X_2, ..., X_{16} of the random number signal X. In step S33, as a result of the check processing, if the decrypted identification signal ID_1 coincides with the selected identification signal ID_1, then, in accordance with the door opening or closing command signal of the response request signal, the signal processing circuit unit 12 supplies the unlocking or locking command signal to the drive unit 15 for carrying out the unlocking or locking operation of the door. Under the control of the drive unit 15, the door is opened or closed.

Since the identification signal checking apparatus according to the second embodiment shown in FIG. 4 is arranged as described above, it can easily be understood that it is possible to achieve the same effect as that of the identification signal checking apparatus according to the embodiment shown in FIG. 1. According to the second embodiment shown in FIG. 4, since one of the sixteen identification signals ID_1, ID_2, ..., ID_{16} is selected in response to one of the lower 4-bit random number signals X1, X_2, ..., X_{16} of the random number signal X, it is advantageously possible to improve the security further.

The identification signal checking apparatus according to a third embodiment of the present invention will be described with reference to FIGS. 6 and 7. In FIG. 6, parts and units corresponding to those in FIG. 1 are marked with the same reference numerals and hence need not to be described in detail.

In the third embodiment shown in FIG. 6, a nonvolatile memory unit 5 of a portable key apparatus 1 stores a specific (own) identification signal ID and a plurality of, e.g., sixteen functions f_1, f_2,..., f_{16}.

When the key apparatus 1 receives a random number signal X of 24 bits, for example, from a lock apparatus 10, a signal processing circuit unit 3 of the key apparatus 1 determines which of random number signals X_1, X_2,..., X_{16} a random number signal formed of lower 4 bits of the 24 bits of the received random number signal X is, and, if the lower 4-bit random number signal is a random number signal X_1, for example, selects one of sixteen functions f_1, f_2,..., F_{16} stored in a memory unit 5, e.g., the function f_1 in response to the random number signal X_1.

In this third embodiment, as shown in Table 3, the random number signals X_1, X_2,..., X_{16} formed of the lower 4 bits of the above 24-bit random number signal X respectively correspond to the sixteen functions f_1, f_2,..., F_{16} stored in the memory unit 5.

Table 3

lower 4-bit random number	function	encrypted signal
X_1 = 0000	f_1	f_1(X, ID)
X_2 = 0001	f_2	f_2(X, ID)
:	:	:
:	:	:
X_{16} = 1111	f_{16}	f_{16}(X, ID)

In this third embodiment, the identification signal ID stored in the memory unit 5 is formed of 24 bits, for example.

In this embodiment, the signal processing circuit unit 3 encrypts the identification signal ID by using the received random number signal X and one of the functions f_1, f_2, ..., f_{16} selected in response to one of the lower 4-bit random number signal X_1, X_2, ..., X_{16} of the random number signal X, and obtains one of the encrypted signals f_1(X, ID), f_2(X, ID),..., f_{16}(X, ID) shown in Table 3. The key apparatus 1 transmits the obtained one of the encrypted signals f_1(X, ID), f_2(X, ID), ..., f16(X, ID) to the lock apparatus 10.

The same identification signal and the same plurality of, e.g., sixteen functions f_1, f_2,..., f_{16} stored in the memory unit 5 of the key apparatus 1 are also stored in the memory unit 13 of the lock apparatus 10 shown in FIG. 6.

The signal processing circuit unit 12 of the lock apparatus 10 stores the 24-bit random number signal X, for example, generated by the random number generating unit 14 and transmitted therefrom in response to the response request signal from the key apparatus 1, and selects one of, for example, the sixteen functions f_1, f_2, ..., f_{16} stored in the memory unit 13 similarly to the key apparatus 1 in response to the received one of the lower 4-bit random number signals X_1, X_2, ..., X_{16} of the random number signal X.

In this case, one of the functions f_1, f_2,..., f_{16} selected by the key apparatus 1 in response to one of the lower 4-bit random number signal X_1, X_2, ..., X_{16} of the random number signal X is set the same as one of the functions f_1, f_2,..., f_{16} selected by the lock apparatus 10 in response to one of the lower 4-bit random number signals X_1, X_2,..., X_{16} of the random number signal X.

When the lock apparatus 10 receives from the key apparatus 1 one of the encrypted signals f_1(X, ID), f_2(X, ID, ..., f_{16}(X, ID) obtained by encrypting the identification signal ID by using the selected one of the functions f_1, f_2,..., f_{16} and the random number signal X, e.g., the encrypted signal f_1(X, ID), the signal processing circuit unit 12 decrypts the encrypted signals f1(X, ID) in accordance with a predetermined function $f_1^{-1}\{f_1(X, ID), X\}$ by using the previously transmitted 24-bit random number signal X and the function f_1 selected in response to one of the lower 4-bit random number signals X_1, X_2, ..., X_{16} of the random number signal X, e.g., selected in response to the random number signal X_1, and checks whether or not the identification signal ID obtained by the decryption coincides with the identification signal ID previously registered in the memory unit 13.

Other parts of the identification signal checking apparatus according to the third embodiment shown in FIG. 6 are arranged similarly to those of the identification signal checking apparatus according to the first embodiment shown in FIG. 1.

An operation of the keyless entry system for opening and closing a door according to the third embodiment shown in FIG. 6 will be described with reference to FIG. 7 which is a flowchart therefor. In this third embodiment, it is assumed that the identification signal and the sixteen functions f_1, f_2, ..., f_{16} are previously registered (stored) in both of the memory units 5 and 13.

In step S41 of the flowchart shown in FIG. 7, the switch unit 2 of the key apparatus 1 is operated, thereby a command to open or close a door being issued. In step S42, as shown in FIG. 3A, for example, the key apparatus 1 transmits the response request signal including the door opening/closing command signal to the lock apparatus 10 for a period of 100 ms. Then, the processing proceeds to step S43.

In step S43, the lock apparatus 10 receives the response request signal as shown in FIG. 3D. Then, the processing proceeds to step S44, wherein the lock apparatus 10 obtains the 24-bit random number signal X, for example, generated by the random number generating unit 14. In step S45, as shown in FIG. 3C, the lock apparatus 10 transmits the random number signal X to the key apparatus 1 for a period of 30 ms, for example. Then, the processing proceeds to step S46.

In step S46, the key apparatus 1 receives the random number signal X as shown in FIG. 3B. Then, the processing proceeds to step S47, wherein the key apparatus 1 selects one of the sixteen functions f_1, f_2,..., f_{16} registered in the memory unit 5, e.g., the function f_1 in response to one of the lower 4-bit random number signals X_1, X_2, ..., X_{16} of the random number signal X. Then, the processing proceeds to step S48.

In step S48, the key apparatus 1 encrypts the identification signal ID to convert it into the 24-bit code signal, by using the selected function f1 and the 24-bit random number signal X, for example, and then obtains the encrypted signal f_1(X, ID). Then, the processing proceeds to step S49, wherein the key apparatus 1 transmits the encrypted signal f_1(X, ID) to the lock apparatus 10 during the period of 30 ms, for example, as shown in FIG. 3A. Then, the processing proceeds to step S50.

In step S50, the lock apparatus 10 receives the encrypted signal f_1(X, ID) as shown in FIG. 3D. Then, the processing proceeds to step S51, wherein the lock apparatus 10 decrypts the received encrypted signal f_1(X, ID) in accordance with a predetermined function $f_1^{-1}\{f_1(X, ID), X\}$ by using the previously transmitted random number signal X and the corresponding one of the random number signals X_1, X_2, ..., X_{16} of the random number signal X. Then, the processing proceeds to step S52.

In step S52, the lock apparatus 10 checks whether or not the decrypted identification signal ID coincides with the identification signal ID registered in the memory unit 13. In step S53, as a result of the check processing, if the decrypted identification signal ID coincides with the identification signal ID registered in the memory unit 13, then, in accordance with the door opening or closing command signal of the response request signal, the signal processing circuit unit 12 supplies the unlocking or locking command signal to the drive unit 15 for carrying out the unlocking or locking operation of the door. Under the control of the drive unit 15, the door is opened or closed .

Since the identification signal checking apparatus according to the third embodiment shown in FIG. 6 is arranged as described above, it can easily be understood that it is possible to achieve the same effect as that of the identification signal checking apparatus according to the first embodiment shown in FIG. 1. According to the third embodiment shown in FIG. 6, since one of the sixteen functions f_1, f_2,..., f_{16} is selected in response to one of the lower 4-bit random number signals X_1, X_2, ...,X_{16} of the random number signal X, it is advantageously possible to improve the security further.

While in the first to third embodiments the communication between the key apparatus 1 and the lock apparatus 10 is carried out in accordance with the base band system by using the infrared rays, the communication may be carried out in accordance with some other modulation systems such as the ASK, the FSK or the like by using the infrared rays. It is needless to say that the communication may be carried out by using a radio wave or a supersonic wave instead of the infrared rays.

It is not necessary that each of the random number signal, the identification signal and the encrypted signal is formed of 24 bits. It is sufficient to determine the number of bits thereof in response to a required degree of the security.

While in the first to third embodiments the response request signal includes the locking or unlocking command signal, the locking or unlocking command signal may be added to the above encrypted signal or may be transmitted individually.

In the above embodiments, the number of the identification signals ID_1, ID_2, ..., ID_{16} or the functions f_1, f_2,..., f_{16} is set to 16, it is not necessary to set the number to 16, and hence the number may be set to any value depending upon a desired degree of security.

While in the above embodiments one of the identification signals ID_1, ID_2, ..., ID_{16} or one of the functions f_1, f_2, ..., f_{16} is selected in response to one of the lower 4-bit random number signals X_1, X_2, ..., X_{16} of the random number signal X, it is not necessary to use the lower 4 bits of the random number signal X and one of the identification signals ID_1, ID_2, ..., ID_{16} or one of the functions f_1, f_2,...,f_{16} may be selected by using any bits of the random number signal X.

According to the first to third embodiments of the present invention, the detecting apparatus (lock apparatus) transmits the random number signal, and the apparatus to be detected (key apparatus) encrypts the identification signal by using the random number signal and transmits the encrypted identification signal to the detecting apparatus (lock apparatus). Therefore, since the identification signal transmitted from the apparatus to be detected (key apparatus) to the detecting apparatus (lock apparatus) is the encrypted signal obtained by encryption using the random number signal and hence is always a unique signal, the security is advantageously improved.

According to the embodiments of the present invention, since it is not necessary to manage the apparatus to be detected (key apparatus) and the detecting apparatus (lock apparatus) as a pair of items or objects to be managed, this leads to advantages in effective management and physical distribution.

Having described preferred embodiments of the present invention with reference to the accompanying drawings, it is to be understood that the present invention is not limited to the above-mentioned embodiments and that various changes and modifications can be effected therein by one skilled in the art without departing from the scope of the present invention as defined in the appended claims.

Claims

1. An identification signal checking apparatus comprising:

an apparatus to be detected having a first wireless transmitting and receiving unit, a first signal processing unit and a first memory unit for storing an identification signal; and
a detecting apparatus having a second wireless transmitting and receiving unit, a second signal processing unit, a second memory unit for storing an identification signal, and a random number generating unit, wherein when said detecting apparatus receives a response request signal from said apparatus to be detected, said detecting apparatus transmits a random number signal obtained from said random number generating unit, when receiving said random number signal, said apparatus to be detected encrypts said identification signal stored in said first memory unit by using said random number signal and transmits said encrypted identification signal to said detecting apparatus, and said detecting apparatus decrypts said encrypted identification signal and checks whether or not said decrypted identification signal coincides with the identification signal stored in said second memory unit.

2. An identification signal checking apparatus according to claim 1, wherein in accordance with a predetermined function, said identification signal is encrypted by using said random number signal.

3. An identification signal checking apparatus according to claim 2, wherein said identification signal is composed of plurality of identification signals each corresponding to plurality of random number signals, said identification signals being stored in both of said first memory unit and said second memory unit and said identification signals are encrypted by corresponding random number signals, respectively.

4. An identification signal checking apparatus according to claim 2, wherein said function is composed of plurality of functions each corresponding to plurality of random number signals, and a function is used for encryption in response to the corresponding random number signal.

5. An identification signal checking apparatus according to claim 1, wherein said first and second wireless transmitting and receiving units are respectively infrared-ray transmitting and receiving units.

6. An identification signal checking method of an identification signal checking apparatus having an apparatus to be detected having a first wireless transmitting and receiving unit, a first signal processing unit and a first memory unit for storing an identification signal, and a detecting apparatus having a second wireless transmitting and receiving unit, a second signal processing unit, a second memory unit for storing an identification signal, and a random number generating unit, comprising the steps of:

transmitting a response request signal from said apparatus to be detected;
transmitting, when said detecting apparatus receives said response request signal from said apparatus to be detected, a random number signal obtained from said random number generating unit from said detecting apparatus;
encrypting, when said apparatus to be detected receives said random number signal, said identification signal stored in said first memory unit of said apparatus to be detected by using said random number signal;
transmitting said encrypted identification signal from said apparatus to be detected to said detecting apparatus; and
decrypting said encrypted identification signal by said detecting apparatus to check whether or not said decrypted identification signal coincides with the identification signal stored in said second memory unit.

7. An identification signal checking method according to claim 6, wherein in accordance with a predetermined function, said identification signal is encrypted by using said random number signal.

8. An identification signal checking method according to claim 7, wherein said identification signal is composed of plurality of identification signals each corresponding to plurality of random number signals, said identification signals being stored in both of said first memory unit and said second memory unit and said identification signals are encrypted by corresponding random number signals, respectively.

9. An identification signal checking method according to claim 7, wherein said function is composed of plurality of functions each corresponding to plurality of random number signals, and a function is used for encryption in response to the corresponding random number signal.

10. An identification signal checking method according to claim 6, wherein said first and second wireless transmitting and receiving units are respectively infrared-ray transmitting and receiving units.

11. An identification signal checking apparatus according to claim 1, wherein said apparatus to be detected is a key apparatus, said detecting apparatus is a lock apparatus, said lock apparatus is provided with a locking means and/or an unlocking means, said lock apparatus controls said locking means and/or said unlocking means based on a check output indicative of whether or not said decrypted identification signal coincides with the identification signal stored in said second memory unit.

12. An identification signal checking method according to claim 6, wherein said apparatus to be detected is a key apparatus, said detecting apparatus is a lock apparatus, said lock apparatus is provided.with a locking means and/or an unlocking means, said lock apparatus controls said locking means and/or said unlocking means based on a check output indicative of whether or not said decrypted identification signal coincides with the identification signal stored in said second memory unit.

FIG. 1

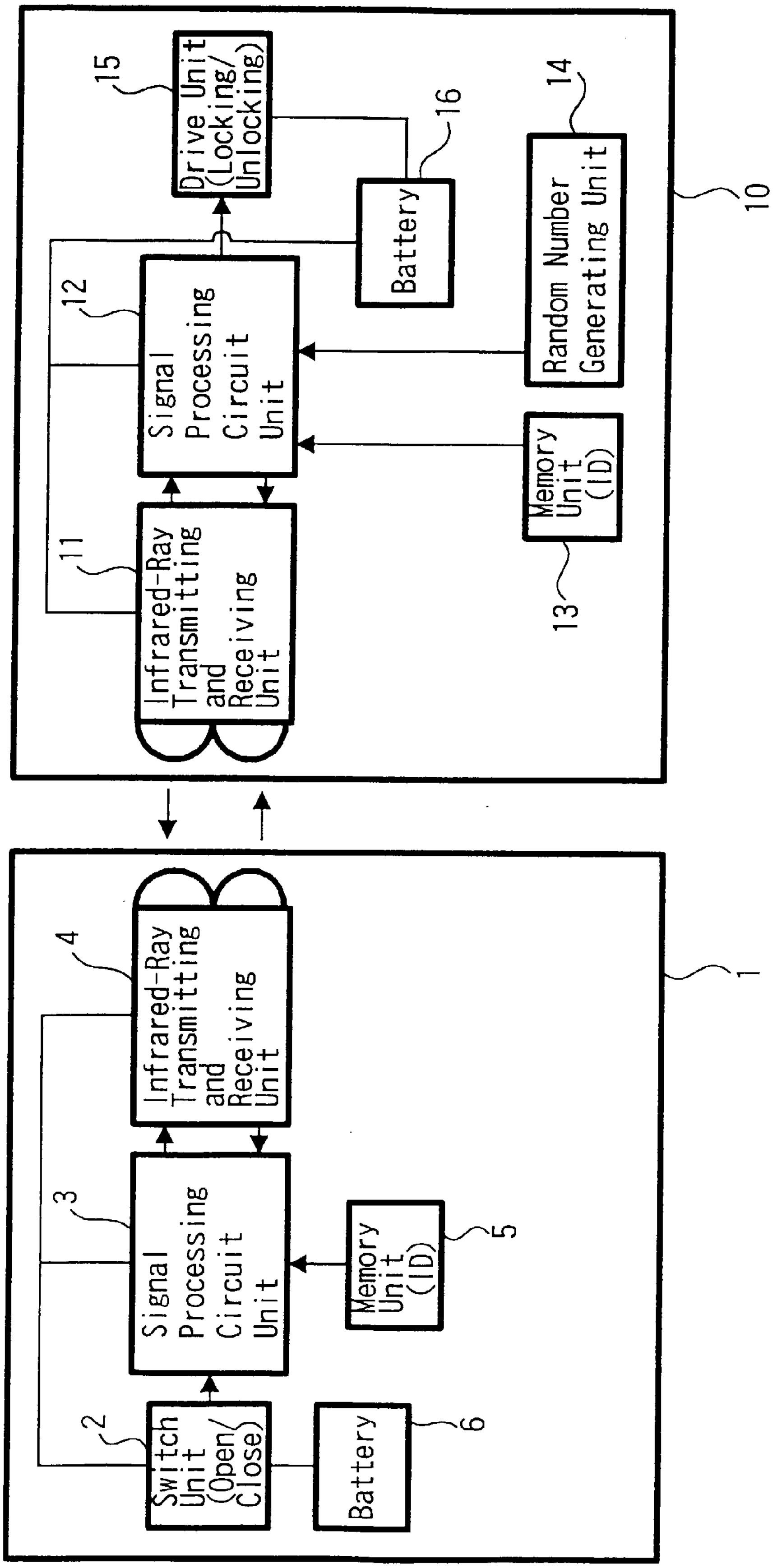
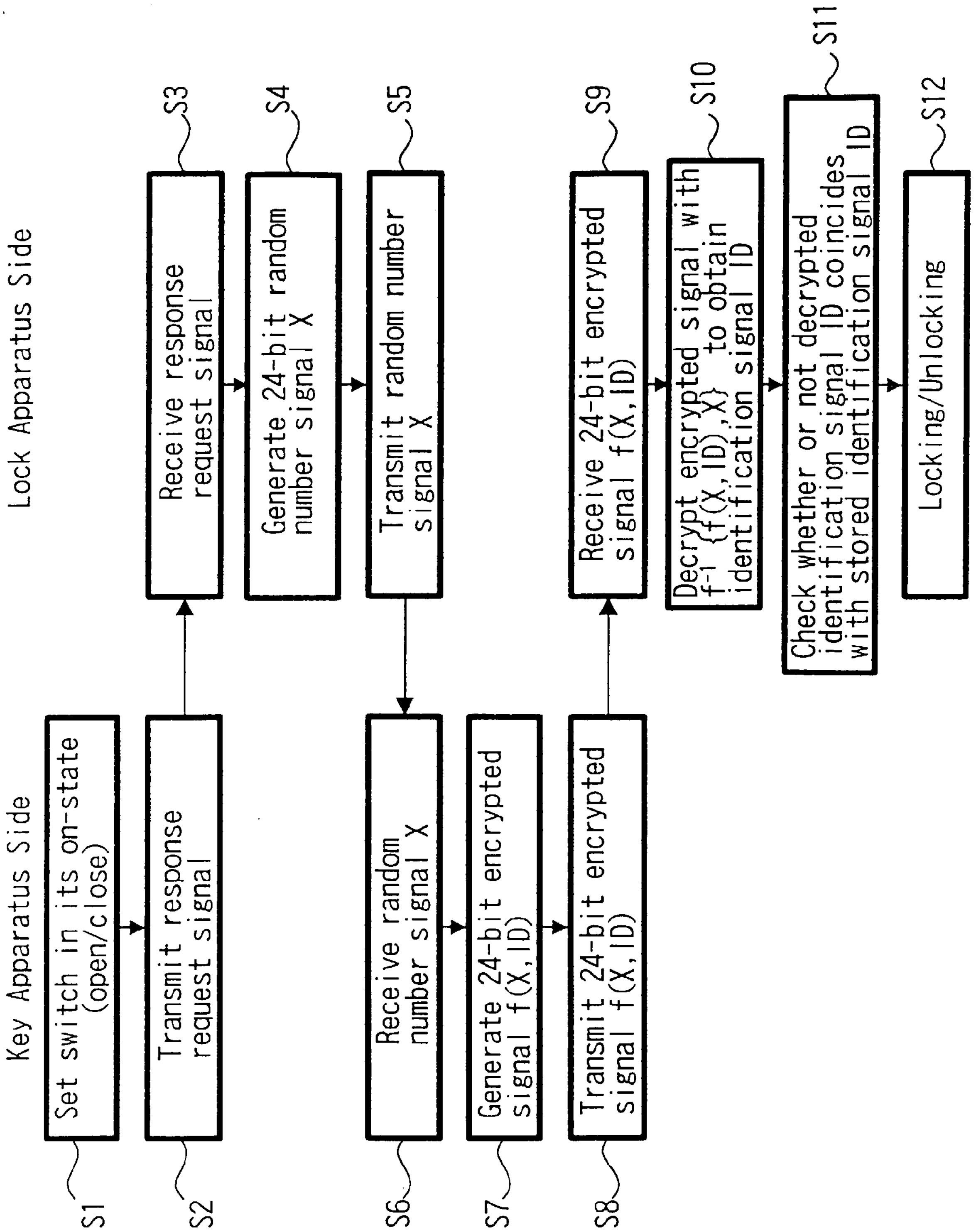

Switch Unit (Open/Close)
2
Battery
6
Signal Processing Circuit Unit
3
Memory Unit (ID)
5
Infrared-Ray Transmitting and Receiving Unit
4
1
Infrared-Ray Transmitting and Receiving Unit
11
Signal Processing Circuit Unit
12
Memory Unit (ID)
13
Random Number Generating Unit
14
Battery
16
Drive Unit (Locking/Unlocking)
15
10

FIG. 2


Key Apparatus Side
Lock Apparatus Side
S1
Set switch in its on-state (open/close)
S2
Transmit response request signal
S3
Receive response request signal
S4
Generate 24-bit random number signal X
S5
Transmit random number signal X
S6
Receive random number signal X
S7
Generate 24-bit encrypted signal f(X,ID)
S8
Transmit 24-bit encrypted signal f(X,ID)
S9
Receive 24-bit encrypted signal f(X,ID)
S10
Decrypt encrypted signal with f⁻¹ {f(X,ID),X} to obtain identification signal ID
S11
Check whether or not decrypted identification signal ID coincides with stored identification signal ID
S12
Locking/Unlocking

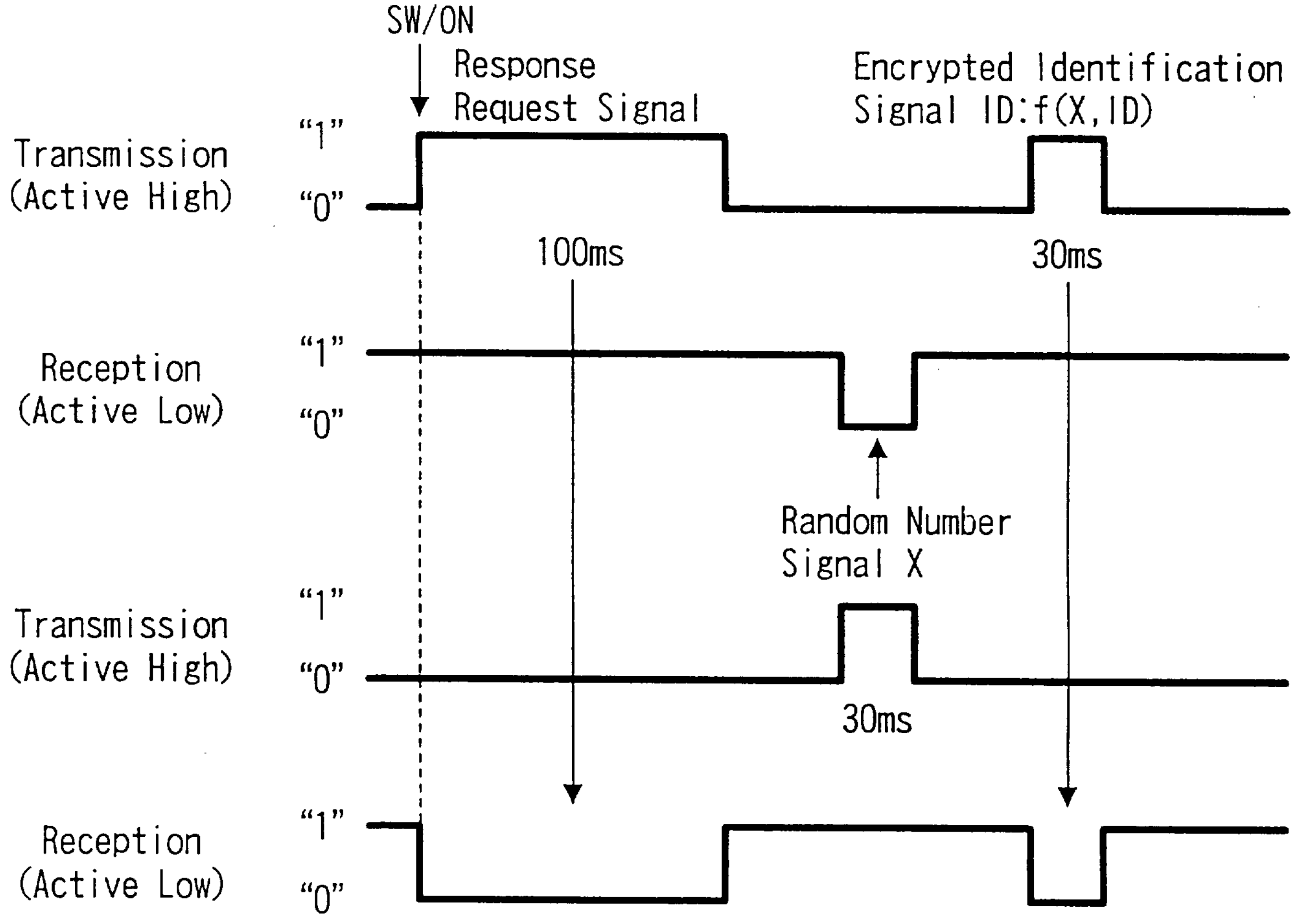


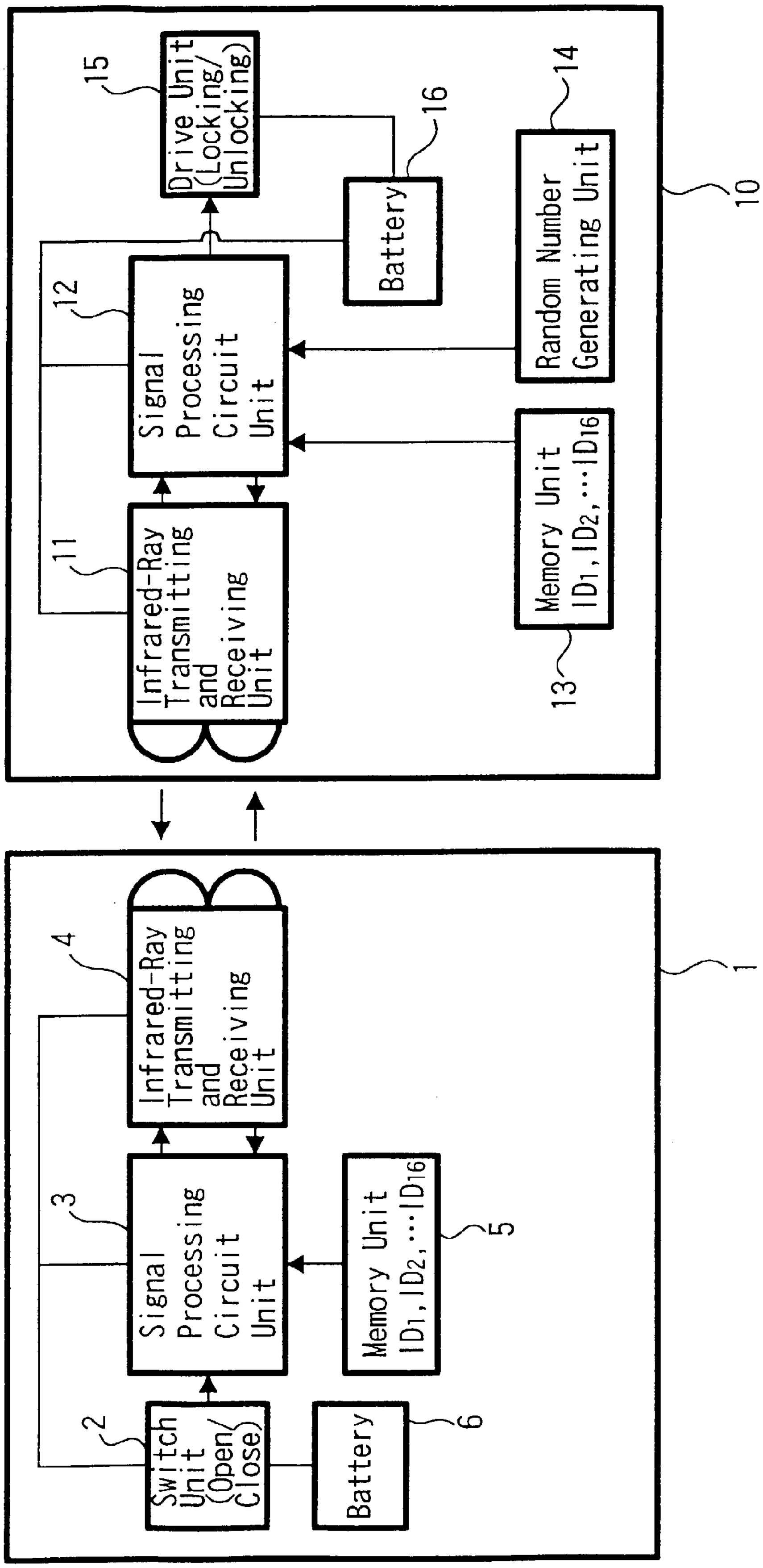
FIG. 3A

FIG. 3B

FIG. 3C

FIG. 3D

FIG. 4


1
2
Switch Unit (Open/Close)
6
Battery
3
Signal Processing Circuit Unit
5
Memory Unit ID1, ID2, ···ID16
4
Infrared-Ray Transmitting and Receiving Unit
10
11
Infrared-Ray Transmitting and Receiving Unit
12
Signal Processing Circuit Unit
13
Memory Unit ID1, ID2, ···ID16
14
Random Number Generating Unit
15
Drive Unit (Locking/Unlocking)
16
Battery

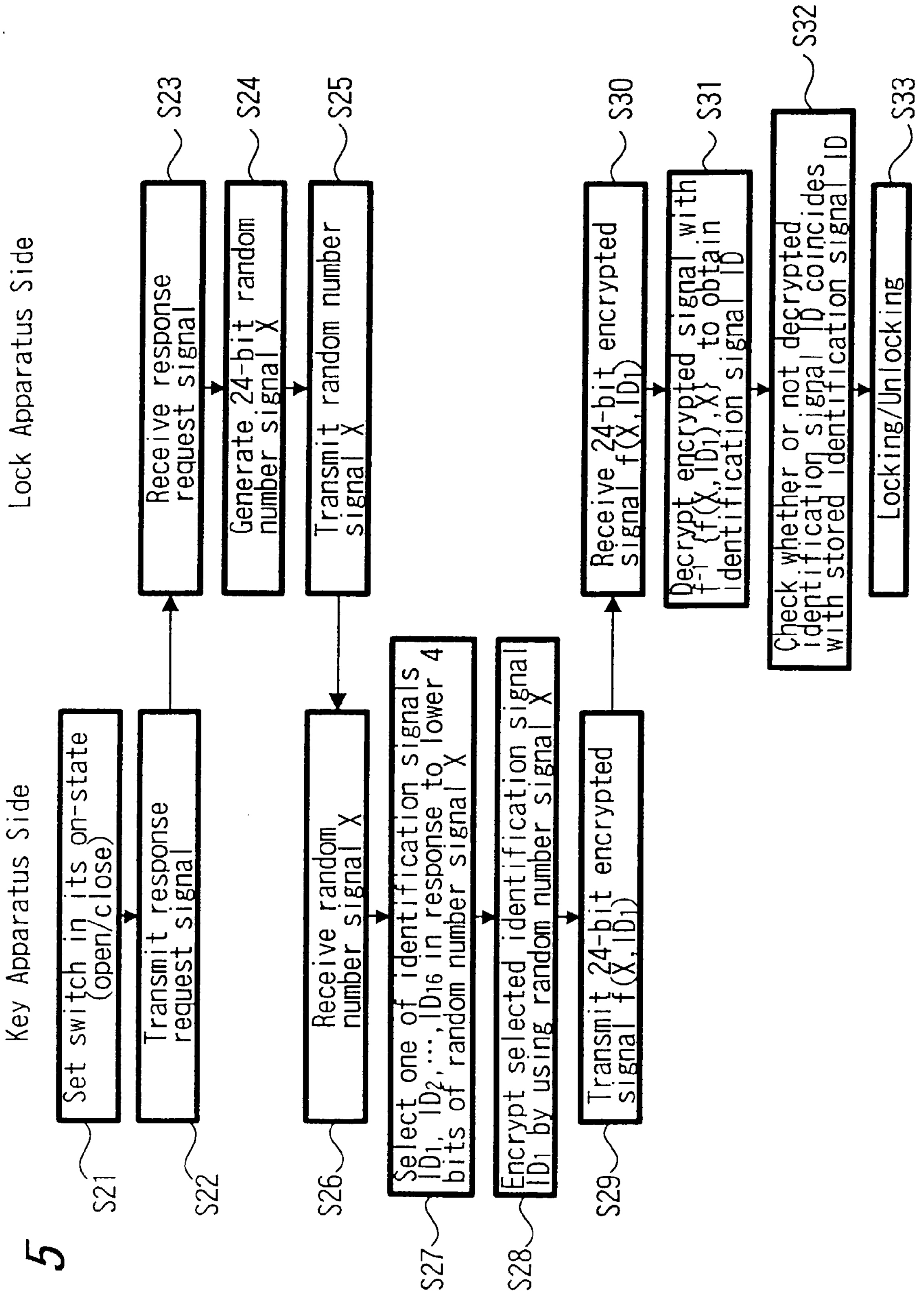

Key Apparatus Side
Lock Apparatus Side
Set switch in its on-state (open/close)
S21
Transmit response request signal
S22
Receive response request signal
S23
Generate 24-bit random number signal X
S24
Transmit random number signal X
S25
Receive random number signal X
S26
Select one of identification signals ID₁, ID₂,···,ID₁₆ in response to lower 4 bits of random number signal X
S27
Encrypt selected identification signal ID₁ by using random number signal X
S28
Transmit 24-bit encrypted signal f(X, ID₁)
S29
Receive 24-bit encrypted signal f(X, ID₁)
S30
Decrypt encrypted signal with f⁻¹ {f(X, ID₁), X} to obtain identification signal ID
S31
Check whether or not decrypted identification signal ID coincides with stored identification signal ID
S32
Locking/Unlocking
S33

FIG. 5

FIG. 6

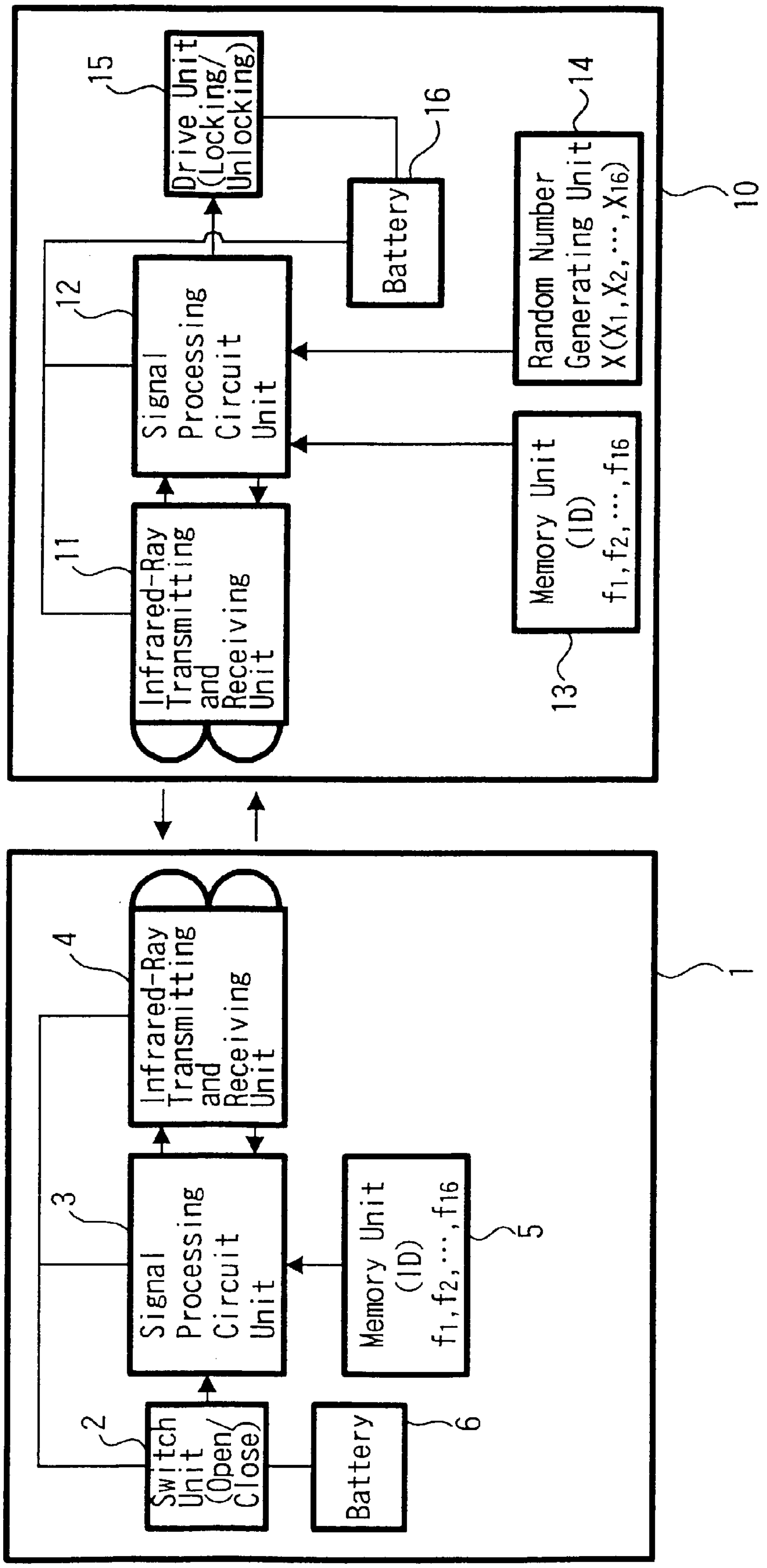
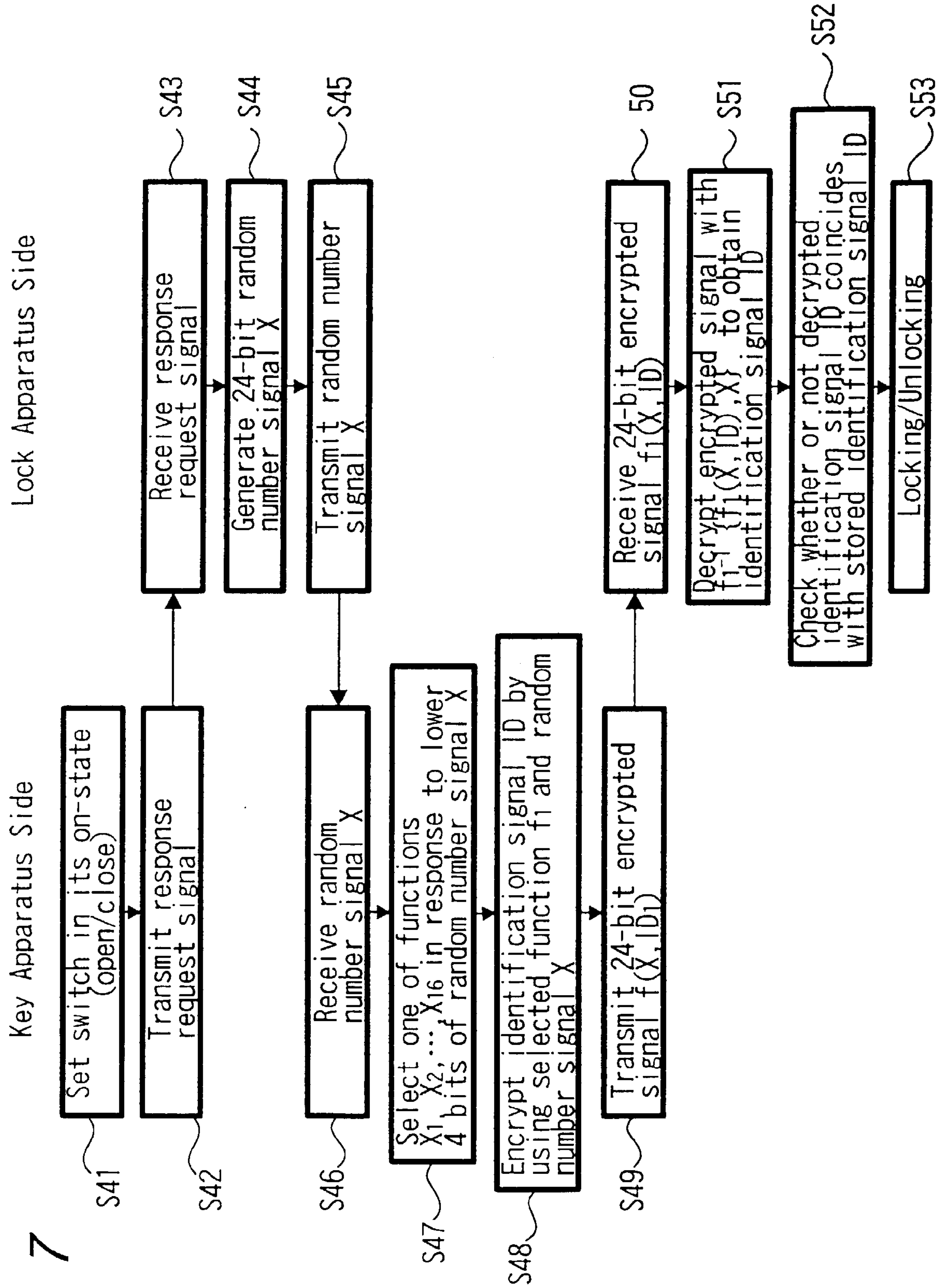

1
2
Switch Unit (Open/ Close)
6
Battery
3
Signal Processing Circuit Unit
5
Memory Unit (ID) $f_1, f_2, \cdots, f_{16}$
4
Infrared-Ray Transmitting and Receiving Unit
10
11
Infrared-Ray Transmitting and Receiving Unit
12
Signal Processing Circuit Unit
13
Memory Unit (ID) $f_1, f_2, \cdots, f_{16}$
14
Random Number Generating Unit $X(X_1, X_2, \cdots, X_{16})$
15
Drive Unit (Locking/ Unlocking)
16
Battery

FIG. 7


Key Apparatus Side
Lock Apparatus Side
S41
Set switch in its on-state (open/close)
S42
Transmit response request signal
S43
Receive response request signal
S44
Generate 24-bit random number signal X
S45
Transmit random number signal X
S46
Receive random number signal X
S47
Select one of functions X1, X2, …, X16 in response to lower 4 bits of random number signal X
S48
Encrypt identification signal ID by using selected function f1 and random number signal X
S49
Transmit 24-bit encrypted signal f(X,ID1)
50
Receive 24-bit encrypted signal f1(X,ID)
S51
Decrypt encrypted signal with f1⁻¹ {f1(X,ID),X} to obtain identification signal ID
S52
Check whether or not decrypted identification signal ID coincides with stored identification signal ID
S53
Locking/Unlocking