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

(11) EP 0 987 651 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
01.10.2003 Bulletin 2003/40

(21) Application number: **98901547.4**

(22) Date of filing: **06.02.1998**

(51) Int Cl.[7]: **G06K 19/073**, G07B 15/00

(86) International application number:
PCT/JP98/00512

(87) International publication number:
WO 98/036377 (20.08.1998 Gazette 1998/33)

(54) **PORTABLE POINT STORING MEMBER AND ITS USING METHOD**

TRAGBARES EINHEITEN-SPEICHERELEMENT UND BENUTZUNGSVERFAHREN

ELEMENT PORTABLE DE STOCKAGE D'UNITES ET SON PROCEDE D'UTILISATION

(84) Designated Contracting States:
FR GB

(30) Priority: **13.02.1997 JP 2885997**

(43) Date of publication of application:
22.03.2000 Bulletin 2000/12

(73) Proprietor: **Rohm Co., Ltd.**
Kyoto-shi Kyoto 615-8585 (JP)

(72) Inventors:
- **HIKITA, Junichi**
  Ukyo-ku Kyoto-shi Kyoto 615-0045 (JP)
- **IKEFUJI, Yoshihiro**
  Ukyo-ku Kyoto-shi Kyoto 615-0045 (JP)
- **TAGUCHI, Haruo**
  Ukyo-ku 615-0045 5 (JP)

(74) Representative: **Prüfer, Lutz H., Dipl.-Phys. et al**
Harthauser Strasse 25d
81545 München (DE)

(56) References cited:
EP-A- 0 646 892 **JP-A- 7 105 335**

- **Beutelspacher: Chipkarten als Sicherheitswerkzeug, Springer Verlag Heidelberg, 1991, ISBN 3-540-54140-3**

EP 0 987 651 B1

Printed by Jouve, 75001 PARIS (FR)

Description

Technical Field

[0001] The present invention relates to a portable point storing member and a method of using the same, and particularly a point storing member having improved secrecy and a method of using the same.

Background Art

[0002] It has been proposed to employ a data communication system using IC cards in ticket barriers of a ski lift and a railroad, an automatic cargo sorting system and others.

[0003] Fig. 12 shows a data communication system using IC cards, and particularly a structure of a communication system using non-contact IC cards. This system is formed of an interrogator 40 (e.g., mounted in a gate of a ski lift) and a non-contact IC card 100.

[0004] Interrogator 40 is controlled by a controller 48 to issue a high-frequency carrier wave generated by an oscillator circuit (OSC) 49 from an antenna 41. When non-contact IC card 100 approaches interrogator 40, an antenna 23 of non-contact IC card 100 receives this high-frequency carrier wave. A power producing circuit 25 converts the received high-frequency wave into a DC power, and supplies it to other circuit portions. Thereby, non-contact IC card 100 can start the operation when it approaches interrogator 40.

[0005] Information transmission from interrogator 40 to non-contact IC card 100 is performed by modulating the above high-frequency carrier wave by a modulator-demodulator circuit 46. A controller 35 performs necessary processing such as change of contents of a memory 37 and return of information based on the demodulated information.

[0006] Information is also transmitted from non-contact IC card 100 to interrogator 40. Since an oscillator circuit is not employed in non-contact IC card 100, the information is sent in the following manner. Interrogator 40 issues non-modulated high-frequency carrier wave, and modulator-demodulator circuit 33 in non-contact IC card 100 changes an impedance of resonance circuit 22. Interrogator 40 handles this impedance change as the impedance change of resonance circuit 42 on its own side, and modulator-demodulator circuit 46 detects and demodulates it. Controller 48 obtains the demodulated information, and performs necessary processing.

[0007] When non-contact IC card 100 moves away from interrogator 40, the power supply is interrupted so that non-contact IC card 100 stops the operation.' Since memory 37 is a nonvolatile memory, the stored information is held even when the power supply is interrupted.

[0008] Memory 37 in non-contact IC card 100 described above may store predetermined points, and the data in memory 37 may be changed in accordance with the used points, whereby the IC card can be used as a prepaid card.

[0009] Data is communicated in an encrypted form between the interrogator and the IC card. Thereby, it is possible to prevent unauthorized change of the contents in the IC card which was once used.

[0010] However, the communication system using the IC cards in the prior art suffers from the following problems. Although the communication data is encrypted as described above, the data can be altered if the encryption algorithm is interpreted. Therefore, it is difficult to ensure the secrecy of the system only by the encryption.

[0011] In particular, if the interrogator is located in a place open to the public, and particularly, in a public telephone or the like, the telephone set internally provided with the interrogator may be stolen. When stolen, instructions and commands to be sent between the interrogator and the IC card may be analyzed.

[0012] From EP 0 646 892 A2 a point storing member is known which comprises storing means for storing points and a first cryptogram storing portion for storing a first cryptogram set representing the authorised user, changing means for changing the points stored in the inset storing means, input means for receiving data to be verified and comparing means comparing the data received via said input means with said cryptogram.

[0013] From A. Beutelspacher et a1., "Chipkarten als Sicherheitswerkzeug". Springer Verlag, Heidelberg, 1991, ISBN 3-540-54140-3 it is known to prevent excess to data in a chip card by implementing key hierarchies.

[0014] An object of the invention is to overcome the above problems, and particularly to provide a portable point storing member, which can suppress illegal use, as well as a method of using the same.

[0015] The objet is solved by a portable point storing member according to claim 3 and a method of using a portable point storing member according to claim 1. Further developpments are given in the dependent claims.

Brief Description of the Drawings

[0016]

Fig. 1 shows functional blocks in a point storing member 1 of an embodiment of the invention;

Fig. 2 schematically shows a structure of an IC card 10 of an embodiment of the invention;

Fig. 3 shows a memory 50 and a controller 60 in Fig. 2 in greater detail;

Fig. 4 schematically shows a structure of memory 50;

Fig. 5 shows, by way of example, voltages for reading, writing, erasing and disabling;

Fig. 6 shows relationships between a read change circuit 61, a cryptogram collating portion 63 and a memory area selection detecting circuit 67;

Fig. 7 shows a cryptogram collating portion 63 in greater detail;

Fig. 8 is a flow chart showing operation of IC card

10;
Fig. 9 is a flow chart following Fig. 8;
Fig. 10 is a flow chart following Fig. 9;
Fig. 11 is a flow chart following Fig. 8; and
Fig. 12 is a block diagram.showing structures of IC card 100 and interrogator 40 in the prior art.

Best Mode for Carrying Out the Invention

[0017] The invention will be described in greater detail with reference to the accompanying drawings.

[1. Function Blocks of IC Card]

[0018] Referring to Fig. 1, description will now be given on a point storing member 1 of an embodiment of the invention. Point storing member 1 has portability, and includes a point storing portion 3, a read portion 5, a point changing portion 7, a point rewrite information storing portion 13 and a collating portion 11.

[0019] Point storing portion 3 is a portion for storing points corresponding to moneys, and have data holding portions, which can hold write data and are equal in number to the points. Read portion 5 reads out the points stored in point storing portion 3 in accordance with a read instruction which is externally applied. Point changing portion 7 can change each data holding portion in point storing portion 3 from an unwritten state (first state), where the write data is not held, to a written state (second state), where the write data is held, based on an externally applied point change instruction.

[0020] Point rewrite information storing portion 13 stores point rewrite information, i.e., information for point rewriting. Collating portion 11 collates the applied information with the above point rewrite information. Point changing portion 7 can change each data holding portion from the unwritten state to the written state, and further can change each data holding portion from the written state to the unwritten state based on a result of the collation by collating portion 11.

[0021] Assuming that the data holding portions in the unwritten state correspond in number to remaining points, the data change which increases the points can be reliably prevented, and the points can be increased only when such information is applied that matches with the point rewrite information which has been stored in advance.

[2. Specific Structure of IC Card]

[0022] A non-contact IC card employing the invention will now be described with reference to Fig. 2.

[0023] Non-contact IC card 10 has a whole structure similar to that in the prior art, and includes an antenna 23, a resonance circuit 22, a power producing circuit 25, a modulator-demodulator circuit 33, a controller 60 and a memory 50 which are arranged within a casing 11. The manner of arranging these portions and parts in casing 11 as well as manners of power supply and data transmission are the same as those in the prior art, and therefore will not be discussed below.

[0024] Fig. 3 is a block diagram specifically showing controller 60 and memory portion 50 shown in Fig. 2. Memory 50 has a point area 51, a setting information area 52, a secret information area 53 and a secret data area 54. Point area 51 is an area for storing the points. Setting information area 52 is an area for storing setting information. Secret data area 53 is an area for storing a cryptogram of an IC card user. Secret data area 54 is an area for storing secret data of an IC card manufacturer.

[0025] As shown in Fig. 3, point area 51 can store data of 128 bytes (1024 bits). Setting information area 52 can store data of 32 bytes, secret data area 53 can store data of 3 bytes, and secret data area can store data of 3 bytes.

[2.1 Memory Portion 50]

[0026] The memory structure of memory portion 50 will now be described with reference to Figs. 4 and 5. In this embodiment, an EEPROM is employed as the non-volatile memory. Memory portion 50 is formed of cells C11 (see Fig. 4) arranged in a matrix form (not shown).

[0027] For changing the data of cell C11 (for performing the data writing by placing data "O" therein, and performing the data erasing by placing data "1" therein), and for reading out the data, voltages are applied to a bit line BL, a select line SL and a word line WL as shown in Fig. 5.

[0028] For setting memory cell C11 to the written state (i.e., for keeping data "0" therein), a voltage of 20 V is applied to bit line BL, a voltage of 0 V is applied to select line SL and a voltage of 20 V is applied to word line WL so that a line AG is set to an open state. Thereby, electrons are injected into a floating gate of cell C11 so that cell 11 holds the data "0".

[0029] For setting memory cell C11 to the erased state (i.e., for keeping data "1" in memory cell C11), voltages opposite to those for keeping the data "0" are applied. More specifically, 0 V is applied to bit line BL, 20 V is applied to select line SL and 20 V is applied to word line WL so that line AG is set to the open state (or 0 V). Thereby, electrons are discharged from the floating gate of cell C11, and data "1" is kept therein.

[0030] For reading information from memory cell C11, a voltage of 5 Vis applied to select line SL, a voltage of 5 V is applied to word line WL, and a sense amplifier (not shown) is connected to bit line BL. The result of detection by the sense amplifier changes depending on whether memory cell C11 has stored "0" or "1". Thereby, it is possible to determine whether memory cell C11 has stored data "1" or data "0".

[0031] As described above, each memory cell in point area 51 stores the data "0" or "1", and each of the memory cells forms the data holding portion. Further, point

area 51 has the memory cells equal in number to the points which were set in advance. For 1000 points, point area 51 has memory cells of 1000 bits.

[0032] Setting information area 52, secret data area 53 and secret data area 54 are configured to hold data of ordinary bit lengths, similarly to the prior art.

[2.2 Controller 60]

[0033] Controller 60 will now be described with reference to Fig. 3. Controller 60 has a main controller 69, an address decoder 65, a memory area selection detecting circuit 67, a cryptogram collating portion 63 and a read change circuit 61.

[0034] Main controller 69 designates an address based on the data applied from modulator-demodulator circuit 33, and applies the address to address decoder 65. Further, it applies an instruction for reading, writing or erasing to read change circuit 61. Further, main controller 69 applies a cryptogram to be collated to cryptogram collating portion 63. The address selected by address decoder 65 is detected by memory area selection detecting circuit 67, which applies the selected address to cryptogram collating portion 63 and read changing portion 61.

[2.2.1 Read Changing Circuit 61]

[0035] Read change circuit 61 applies the read voltage, write voltage or erase voltage shown in Fig. 5 or a disabling voltage, which will be described later, to memory portion 50 in accordance with an instruction applied from main controller 69.

[0036] Read change circuit 61 will now be described with reference to Fig. 6. Read change circuit 61 has selected address specifying terminals Ts1 - Ts3, a mode terminal Te and a mode terminal Tf. Selected address specifying terminals Ts1 - Ts3 are supplied with a signal, which specifies the selected area, from memory area selection detecting circuit 67. More specifically, when point area 51 is selected, a voltage "High" is applied to selected address specifying terminal Ts1. When setting information area 52 is selected, the voltage "High" is applied to selected address specifying terminal Ts2. When secret data area 53 is selected, the voltage "High" is applied to selected address specifying terminal Ts3.

[0037] Mode terminals Te and Tf receive signals from cryptogram collating portion 63. In this embodiment, read change circuit 61 selects one from the following three modes in accordance with the voltages applied to the two mode terminals.

[0038] When both mode terminals Tf and Te are supplied with voltages "Low", a mode "0, 0" (normal mode) is selected.

[0039] When mode terminals Tf and Te are supplied with voltages "Low" and "High", respectively, a mode "0,1" (point rewriting mode) is selected.

[0040] When mode terminals Tf and Te are supplied with voltages "High" and "Low", respectively, a mode "1,0" (initializing mode) is selected.

[0041] Read change circuit 61 applies the disabling voltage to each of the area in memory 50 in accordance with the voltages applied to selected address specifying terminals Ts1 - Ts3 and mode terminals Te and Tf.

[0042] In the respective modes, read change circuit 61 can apply the following voltages. In mode "0, 0", if the selected address which is specified by selected address specifying terminals Ts1 - Ts3 is point area 51 or setting information area 52, the write voltage shown in Fig. 5 can be issued. However, the erase voltage cannot be issued.

[0043] In mode "1, 0", if the selected address which is specified by selected address specifying terminals Ts1 - Ts3 is point area 51 or setting information area 52, the write voltage and erase voltage shown in Fig. 5 can be issued. However, if selected address specifying terminals Ts1 - Ts3 specify secret data areas 53 or 54, the write voltage or the erase voltage shown in Fig. 5 cannot be issued. Thus, the writing and erasing shown in Fig. 5 can be performed only by point area 51 or setting information area 52.

[0044] In mode "1,0", if the selected address specified by selected address specifying terminals Ts1- Ts3 is point area 51, setting information area 52 or secret data area 53, the erase voltage shown in Fig. 5 can be issued. However, if the selected address is secret data area 54, the erase voltage cannot be issued. The write voltage cannot be issued for any one of the areas.

[0045] Data lines of secret data areas 53 and 54 are connected to cryptogram collating portion 63 as shown in Fig. 3. Therefore, the cryptogram which is read out is not applied to main controller 69, and the cryptogram stored in secret data areas 53 and 54 can be prevented from being externally read out.

[2.2.2 Cryptogram Collating Portion 63]

[0046] Cryptogram collating portion 63 is enabled when it receives a detection signal from memory area selection detecting circuit 67, and thereby determines whether the cryptogram stored in secret data area 53 or 54 matches with the signal applied from main controller 69. When they match with each other, voltage "High" is applied to mode terminals Te and Tf of read change circuit 61.

[0047] Cryptogram collating portion 63 will now be described in greater detail with reference to Fig. 7. Cryptogram collating portion 63 has comparators 71 and 73, and a data converting circuit 75. Comparator 73 applies the voltage "High" to mode terminal Tf when it receives from main controller 69 the cryptogram which matches with a cryptogram of an IC card manufacturer stored in secret data area 54.

[0048] Comparator 71 applies the voltage "High" to mode terminal Te when it receives from main controller 69 a cryptogram, which matches with a cryptogram

formed by coalescing the data applied from data converting circuit 75 with the data applied from secret data area 53.

[0049] For example, when secret data area 54 has stored a cryptogram "10100000" and the IC card user has stored "1010" in secret data area 53 as his/her own cryptogram or pass word, the collation is performed as follows. Data converting circuit 75 converts the cryptogram "10100000" in secret data area 54. When the result of conversion is "01011111", comparator 71 is supplied with a cryptogram "101001011111") which is a combination of the cryptogram "1010" of the IC card user stored in secret data area 53 and "01011111" following the cryptogram "1010". Comparator 71 determines whether the input data applied from main controller 69 for collation matches with the above cryptogram "101001011111" or not.

[0050] Comparator 71 may be configured such that the cryptogram stored in secret data area 53 is compared with data obtained by removing the data sent from data converting circuit 75 from the data applied from main controller 69.

[0051] In this embodiment, the IC card user is required to obtain the data, which is prepared by converting the cryptogram in secret data area 54 by data converting circuit 75, from the IC card manufacturer, and apply the same, as the cryptogram to be collated, to main controller 69 after adding thereto his/her own cryptogram.

[0052] According to this embodiment, as described above, the cryptogram of secret data area 54 is converted and added to the cryptogram in secret data area 53 for comparison with the cryptogram data applied from main controller 69 for collation. Accordingly, the IC card manufacturer can store the cryptograms, which are different from each other and are dedicated to the IC card users, respectively, in secret data areas 53. Thereby, no confusion occurs even when two IC card users accidentally stored the same cryptogram in secret data areas 53, respectively. Thus, one of the users cannot erase the data in the IC card of the other user.

[0053] The specific comparator actually performing the collation is determined by a signal supplied from memory area selection detecting circuit 67. If the detected area is secret data area 54, the signal enabling the collating operation is applied to comparator 73. If the detected area is secret data area 53, the signal enabling the collating operation is applied to comparators 71 and 73.

[3. Processing in IC Card]

[0054] Processing of reading, writing and erasing the data as well as cryptogram collation will now be described with reference to Figs. 8 to 11. In the initial state (step ST1 which is not shown), mode terminals Te and Tf of read change circuit 61 are supplied with the voltages "Low", and the operation is in the mode "0, 0".

[0055] Then, main controller 69 determines whether the instruction applied from modulator-demodulator circuit 33 is the read instruction, remaining point removing instruction, data changing instruction or initializing instruction (step ST3).

[3.1 Read Operation]

[0056] When the applied instruction is the read instruction, all the addresses in point area 51 are selected (step ST5). The read instruction is issued (step ST7). Thereby, all the data in point area 51 is read and applied to main controller 69 (step ST8). Main controller 69 counts and temporarily stores the bits (remaining points) holding data "1" in the applied data (step ST9). Then, all the addresses in setting information area 52 are selected (step ST11). Then, the read signal is issued to read change circuit 61 (step ST13). Thereby, the setting information stored in setting information area 52 is applied to main controller 69 (step ST14). Main controller 69 temporarily stores the applied setting information (step ST15). Main controller 69 issues the temporarily stored data to modulator-demodulator circuit 33 (step ST17).

[0057] Thereby, it is possible to issue externally the remaining points stored in point area 51 as well as the setting information stored in setting information area 52.

[3.2 Point Removing Processing]

[0058] Description will now be given on the case where the instruction for removing the remaining points is applied in step ST3. In this case, main controller 69 reads out the remaining points which was temporarily stored in step ST9 (step ST19). The leading address of the memory cells in point area 51 holding data "1" is selected (step ST21). Main controller 69 applies the write signal (i.e., signal for holding data "0") to read change circuit 61 (step ST23).

[0059] Read change circuit 61 which received the write signal determines whether the current state allows application of the write voltage or not, in accordance with the voltages applied to the select address specifying, terminals and the mode terminals shown in Fig. 6. In this case, the selected address is point area 51, and the mode terminals were in the mode "0, 0" in step ST1 so that it is determined that the writing can be performed, and the write voltage shown in Fig. 5 is issued (step ST24).

[0060] Then, main controller 69 decrements the remaining points which were temporarily stored in step ST9 (step ST25). Then, a message to the effect that the remaining point removing processing is completed is issued to modulator-demodulator circuit 33 (step ST27). When the instruction of removing the remaining points is issued, therefore, it is possible to change in the decrementing direction the points stored in point area 51 by a specified value. In this manner, the points which have

been stored in point area 51 are read out, or the data can be changed in the direction of reducing the points in accordance with the point removing instruction.

[3.3 Data Changing Processing]

[0061] Description will now be given on the case where the data changing instruction is applied in step ST3. The data changing instruction is an instruction for changing the data in point area 51 or setting information area 52, and includes a collation instruction for collating the cryptogram stored in the secret data area.

[0062] In this case, main controller 69 selects the addresses in secret data areas 53 and 54 (step ST51 in Fig. 9). Then, data to be verified is issued to cryptogram collating portion 63 (step ST53). Main controller 69 issues the read signal to read change circuit 61 (step ST55). Thereby, read change circuit 61 applies the read voltage (step ST56). Cryptogram collating portion 63 collates the cryptogram read from secret data areas 53 and 54 with the verification target data applied from main controller 69 (step ST57).

[0063] More specifically, the cryptogram stored in secret data area 54 is applied to data converting circuit 75 (see Fig. 7). Data converting circuit 75 converts this cryptogram based on a predetermined rile, and applies the result of conversion to comparator 71. Comparator 71 is also supplied with the cryptogram stored in secret data area 53. Comparator 71 coalesces the data applied from data converting circuit 75 with the data applied from secret data area 53, and determines whether the resultant data matches with the applied verification target data. When matching occurs, comparator 71 applies the voltage "High" to mode terminal Te for read change circuit 61. Thereby, read change circuit 61 enters mode "0, 1" (step ST61 in Fig. 10).

[0064] Main controller 69 selects all the addresses in point area 51 and setting information area 52 (step ST63). Then, it issues the erase signal to read change circuit 61 (step ST65). In this case, the erase voltage can be issued from read change circuit 61 because mode "0, 1" is selected, and the addresses in point area 51 and setting information area 52 are selected. Accordingly, read change circuit 61 applies the erase voltage (step ST66). When the erase voltage is applied, all the bits in point area 51 and setting information area 52 hold "1".

[0065] Then, main controller 69 selects only the required bit(s) in point area 51 and setting information area 52 (step ST67). For example, it is necessary to write the data and time of erasing in setting information area 52 again. In this case, the bits holding data "0" are selected.

[0066] Main controller 69 issues the write signal to read change circuit 61 (step ST69). Read change circuit 61 applies the write voltage (step ST70). Thereby, only the selected bits hold the data "0". Main controller 69 applies the end message to modulator-demodulator circuit 33 (step ST71).

[0067] When the verification target data applied in step ST59 shown in Fig. 9 causes mismatching, main controller 69 selects all the addresses in point area 51 and setting information area 52 (step ST73 in Fig. 10). Then, the erase signal is issued to read change circuit 61 (step ST75). Read change circuit 61 does not issue the erase voltage, but issues the disabling voltage (step ST77) because the current mode is mode "0,0". Accordingly, contents of point area 51 and setting information area 52 do not change.

[0068] In the embodiment described above, the disabling voltage is provided by placing the ground potential on line AG, and setting the other lines to the open state.

[0069] Main controller 69 selects only the required bits in point area 51 and setting information area 52 (step ST79). Main controller 69 issues the write signal to read change circuit 61 (step ST 81). Since the current mode is "0, 0", and the selected address relates to point area 51 and setting information area 52, read change circuit 61 does not issue the write voltage, but issues the disabling voltage (step ST83). Accordingly, contents of point area 51 and setting information area 52 do not change. Main controller 69 issues a message to the effect that rewriting could not be performed (step ST85).

[0070] When the cryptogram-mismatching occurs, read change circuit 61 does not apply the write voltage and the erase voltage even if main controller 69 issues the erase signal and the write signal to read change circuit 61.

[0071] As described above, the data in point area 51 and setting information area 52 can be changed only when the applied cryptogram matches with the cryptogram data which has already been entered or applied by the IC card user and the IC card manufacturer. Accordingly, the IC card described above can have high secrecy.

[3.4 Initializing Operation]

[0072] Description will now be given on the case where the initializing instruction is issued in step ST3 shown in Fig. 8 with reference to Fig. 11. The initializing instruction acts to set all the data in point area 51, setting information area 52 and secret data area 53 other than secret data area 54 to "1", and is given from the IC card manufacturer.

[0073] In this case, main controller 69 selects the address of secret data area 54 (step ST31), and issues verification target data to cryptogram collating portion 63 (step ST32). Main controller 69 issues the read signal to read change circuit 61 (step ST33). Read change circuit 61 applies the read voltage (step ST34). The cryptogram is collated in cryptogram collating portion 63 (step ST35). In this case, comparator 73 is supplied with data stored in secret data area 54, and determines whether the verification target data applied from main controller 69 matches with the cryptogram stored in secret data area 54 or not (step ST36).

[0074] When it is determined in step ST36 shown in Fig. 11 that the verification target data matches with the cryptogram, cryptogram collating portion 63 applies the voltage "High" to mode terminal Tf of read change circuit 61 (step ST37). Thereby, read change circuit 61 enters mode "1, 0".

[0075] Then main controller 69 selects all the addresses in point area 51, setting information area 52 and secret data area 53 (step ST38). Further, it issues the erase signal to read change circuit 61 (step ST39). Since read change circuit 61 is in mode "1,0", read change circuit 61 applies the erase voltage (step ST41). Thereby, all the data in point area 51, setting information area 52 and secret data area 53 are initialized. Main controller 69 issues the end message to modulator-demodulator 33 (step ST42).

[0076] When mismatching occurs in the step ST36 shown in Fig. 11, the voltage "High" is not applied to mode terminal Tf of read change circuit 61. Accordingly, read change circuit 61 remains in mode "0, 0". Main controller 69 selects all the addresses in point area 51, setting information area 52 and secret data area 53 (step ST43). Further, it issues the erase signal to read change circuit 61 (step ST44). In this state, since read change circuit 61 is in the mode "0, 0", and the selected addresses relate to point area 51, setting information area 52 and secret data area 53. Therefore, read change circuit 61 applies the disabling voltage (step ST45). Thus, all the data in point area 51, setting information area 52 and secret data area 53 are not initialized. Main controller 69 issues a message to the effect that the initialization is impossible to modulator-demodulator circuit 33 (step ST46).

[0077] As described above, the initialization can be performed only when the applied verification target data matches with the cryptogram stored in secret data area 54, even when the initializing instruction is issued.

[3.5 Cryptogram Storing Processing]

[0078] In this embodiment, the IC card user stores the cryptogram or password in secret data area 53, and for this purpose, the data in secret data area 53 can be changed only one time after the data in secret data area 53 is initialized. When the data change instruction for changing the data in secret data area 53 is applied to main controller 69 after the initialization, main controller 69 allows the data change only one time so that the predetermined cryptogram can be stored in secret data area 53. More specifically, the above processing can be achieved through the steps from step ST61 to step ST70 in Fig. 10.

[0079] Main controller 69 stores whether the data in secret data area 53 is already changed or not, and will ignore the instruction for changing the data in secret data area 53 when this instruction is issued again.

[4. Other Embodiments]

[0080] The embodiment described above relates to the non-contact IC card employing the invention. However, the invention can likewise to applied to contact IC card.

[0081] Main controller 69 may form a CPU, or may be partially or entirely formed of a logic circuit. This is true also with respect to read change circuit 61, cryptogram collating portion 63, memory area selection detecting circuit 67 and others.

[0082] According to the invention, point area 51 is provided with the memory cells corresponding in number to the intended points, as already described. In the mode "0,0", the data change is allowed to change the memory cell of point area 51 only from the unwritten state holding the data "1" to the written state not holding the write data "1". Thereby, forgery of the IC card can be prevented more reliably.

[0083] An ordinary read-out device provides only the instruction, which changes the data in point area 51 only in the decrementing direction, for the IC card side. Therefore, damages caused by so-called "impersonation" can be prevented.

[0084] The structure of memory 50 is not restricted to the foregoing, but may have such a structure that point area 51 and setting information area 52 are in one memory, and secret data areas 53 and 54 are formed in another memory.

[0085] Secret data areas 53 and 54 for providing the cryptograms in two stages are not essential, and only one of them may be employed.

[0086] The embodiment has been described in connection with the case where the EEPROM is used as memory portion 50. However, another structure may be used for memory portion 50 provided that its allows change of data, and a flash memory, a ferroelectric memory or the like may be used.

[0087] Further, the present invention is similarly applicable to any storage other than these to which date is written electrically, for example, a storage to which date is written optically, provided that it allows switching between writing and erasure.

[0088] In this embodiment, if mismatching is found as a result of collation by the cryptogram collating portion, each of mode terminals Te and Tf, which are input terminals of read change circuit 61 with respect to cryptogram collating portion 63, remains in "Low". Accordingly, read change circuit 61 merely applies the disabling voltage to memory portion 50, and there is no possibility that the data is forged.

[0089] When the signal which acts to erase the data in point area 51 is applied, data "0" may be heldin all the bits in point area 51 and setting information area 52 so that the card cannot be reused until the cryptogram is applied to secret data area 54.

[0090] In the above embodiment, the voltages "High" are applied to mode terminals Te and Tf of read change

circuit 61 only when cryptogram collating portion 63 issues the matching signal. Thereby, read change circuit 61 ignores the data change signal sent from main controller 69. Alternatively, the collation mismatching signal may be applied to main controller 69, and main controller 69 may determine, based on this, that the data change cannot be performed so that the data change signal may not be not issued to read change circuit 61. Also, the message to the effect may be displayed.

[0091] In this embodiment, the disabling voltage is applied by placing the ground potential on line AG and setting the other lines in the open state. However, the voltage is not restricted to the above provided that neither writing nor erasing is performed. For example, 0 V may be applied to bit line BL for inhibiting the writing, and 0 V may be applied to selected line SL for inhibiting the erasing.

[0092] In this embodiment, the state where data "0" is written is the written state, the state where data "1" is written is the unwritten state, and the data "0" is the written data. However, the state where data "1" is written is the written state, and thus the data "1" may be the written data.

[0093] In this embodiment, the state where electrons are injected into the floating gate is the state where data "0" is held. Alternatively, the state where the electrons are removed from the floating gate may be the state where the data "0" is held.

[0094] In this embodiment, if the data "1" is held in the initial state, data "0" is set in the bit for reducing the points. Alternatively, data "0" may be held in the initial state, and the data "1" may be set in the bit for reducing the points.

[0095] In this embodiment, the voltages "Low" are usually applied to mode terminals Te and If so that only the rewriting for reducing the points in point area 51 is allowed, and erasing of the write data is allowed when the voltages "High" are applied to mode terminals Te and Tf. Alternatively, the voltages "High" may be usually applied to mode terminals Te and Tf, and erasing of the write data may be allowed when the voltages "Low" are applied to mode terminals Te and Tf.

[0096] In this embodiment, the disabling voltage is provided by placing the ground potential on line AG and setting the other lines in the open state. However, line AG may be kept at the ground potential.

[0097] In the above embodiment, point area 51 forms, e.g., a point storing portion. Main controller 69, address decoder 65 and read change circuit 61 form, e.g., a read portion. Main controller 69, address decoder 65 and read change circuit 61 form, e.g., a point changing portion. Secret data area 53 forms a point rewrite information storing portion. Cryptogram collating portion 63 forms a collating portion.

[0098] In the above embodiment, the expression to the effect that inhibition is performed by the circuit structure means that a specific circuit structure is employed for disabling specific processing. More specifically, a logic circuit or an electric circuit is used for physically inhibiting specific processing.

[0099] In this embodiment, the number of the data holding portions in the unwritten state ("1") is handled as the remaining points. However, the number of the data holding portions in the written state ("0") may be handled as the remaining points. Thus, all the data holding portions may be set to "0" in the all reset state, and "0" may be changed to "1" in accordance with reduction of the points.

Industrial Applicability

[0100] As described above, the invention can provide the point storing member of which illegal use is difficult, and therefore can be advantageously applied to the fields of manufacturing and selling IC cards.

Claims

1. A method of using a portable point storing member (1), comprising the steps of:

   storing, in advance, points corresponding to moneys, a first cryptogram, set by a first person concerned with manufacturing of said point storing member (1), said first cryptogram characterizing secret data of said first person and a second cryptogram, set by a second person different from said first person and concerned with use of said point storing member (1), said second cryptogram characterizing secret data of said second person; collating said first and second cryptograms for generating a third cryptogram and comparing said third cryptogram with an externally applied data to be verified, reading the points stored in said point storing member in accordance with an externally applied read instruction; and
   changing said points in accordance with an externally applied point changing instruction, wherein
   changing of the points in a direction of increasing the points based on said point changing instruction is performed after determining whether said point changing instruction is to be followed or not, based on a result of the comparison between the externally applied data to be verified and said third cryptogram.

2. The method of claim 1, wherein said collating includes converting of said first cryptogram set and adding it to said second cryptogram set.

3. A point storing member (1) comprising:

   storing means (3) for storing points;

a first secret data area (54) storing a first cryptogram, settable by a first person concerned with manufacturing of said point storing member (1), said first cryptogram characterizing secret data of said first person;
a second secret data area (53) storing a second cryptogram, settable by a second person different from said first person and concerned with use of said point storing member (1), said second cryptogram characterizing secret data of said second person;
changing means (7) for changing the points stored in said storing means (3);
input means for receiving data to be verified;
cryptogram collating means (63) for collating said first and second cryptograms for generating a third cryptogram, said cryptogram collating means (63) including
comparing means (71) for comparing said data to be verified received via said input means with said third cryptogram, wherein
it is determined whether said changing means (7) should increase said points or not, based on a result of the comparison by said comparing means (71).

4. The point storing member according to claim 3, wherein said cryptogram collating means converts said first cryptogram set and adds said converted cryptogram set to said second cryptogram set.

Patentansprüche

1. Verfahren zum Verwenden eines tragbaren Punktespeicherteils (1) mit den Schritten:

im voraus Speichern von Punkten, die Geld entsprechen, ein erstes Kryptogramm, das gesetzt ist von einer ersten Person, die mit der Herstellung des Punktespeicherteils (1) zu tun hat, wobei das erste Kryptogramm geheime Daten der ersten Person kennzeichnet, und ein zweites Kryptogramm, das gesetzt ist durch eine zweite Person, die verschieden von der ersten Person ist und die mit der Benutzung des Punktespeicherteils (1) zu tun hat, wobei das zweite Kryptogramm geheime Daten der zweiten Person kennzeichnet; Zusammenfassen des ersten und des zweiten Kryptogramms zum Erzeugen eines dritten Kryptogramms und Vergleichen des dritten Kryptogramms mit einem extern angelegten Datenwert, der verifiziert werden soll, Lesen der Punkte, die in dem Punktespeicherteil gespeichert sind, in Übereinstimmung mit einem extern angelegten Lesebefehl; und Ändern der Punkte in Übereinstimmung mit einem extern angelegten Punkteänderungsbefehl, wobei
das Ändern der Punkte in Richtung auf eine Punktezunahme auf der Grundlage des Punkteänderungsbefehls durchgeführt wird nach dem Bestimmen, ob der Punkteänderungsbefehl befolgt werden soll oder nicht, auf der Grundlage eines Ergebnisses des Vergleichs zwischen dem extern angelegten zu verfizierenden Datenwert und dem dritten Kryptogramm.

2. Verfahren nach Anspruch 1, wobei das Zusammenfassen ein Konvertieren des ersten gesetzten Kryptogramms und des Addierens desselben zu dem zweiten gesetzten Kryptogramm beinhaltet.

3. Punktespeicherteil (1) mit:

einem Speichermittel (3) zum Speichern von Punkten;
einem ersten Bereich für geheime Daten (54), der ein erstes Kryptogramm speichert, das setzbar ist von einer ersten Person, die mit der Herstellung des Punktespeicherteils (1) zu tun hat, wobei das erste Kryptogramm geheime Daten der ersten Person kennzeichnet;
einem zweiten Bereich für geheime Daten (53), der ein zweites Kryptogramm speichert, das setzbar ist durch eine Person, die verschieden von der ersten Person ist, und die mit der Benutzung des Punktespeicherteils (1) zu tun hat, wobei das zweite Kryptogramm geheime Daten der zweiten Person kennzeichnet; einem Änderungsmittel (7) zum Ändern der Punkte, die in dem Speichermittel (3) gespeichert sind;
einem Eingabemittel zum Empfangen von zu verfizierenden Daten; einem Kryptogrammzusammenfassungsmittel (63) zum Zusammenfassen des ersten und des zweiten Kryptogramms zum Erzeugen eines dritten Kryptogramms, wobei das Kryptogrammzusammenfassungsmittel (63) aufweist
ein Vergleichsmittel (71) zum Vergleichen des zu verfizierenden Datenwerts, der von dem Eingabemittel empfangen wird, mit dem dritten Kryptogramm, wobei bestimmt wird, ob das Änderungsmittel (7) die Punkte erhöhen soll oder nicht, auf der Grundlage des Vergleichs durch das Vergleichsmittel (71).

4. Punktespeichermittel nach Anspruch 3, wobei das Kryptogrammzusammenfassungsmittel das erste gesetzte Kryptogramm konvertiert und das konvertierte gesetzte Kryptogramm zu dem zweiten gesetzten Kryptogramm addiert.

Revendications

1. Un procédé d'utilisation d'un élément portable de stockage d'unités (1), comprenant les étapes suivantes :

on stocke, à l'avance, des unités correspondant à des monnaies, un premier cryptogramme, établi par une première personne intervenant dans la fabrication de l'élément de stockage d'unités (1), ce premier cryptogramme caractérisant des données secrètes de la première personne, et un second cryptogramme, établi par une seconde personne différente de la première personne et intervenant dans l'utilisation de l'élément de stockage d'unités (1), le second cryptogramme caractérisant des données secrètes de la seconde personne; on collationne les premier et second cryptogrammes pour générer un troisième cryptogramme et on compare le troisième cryptogramme avec une donnée appliquée de façon externe à vérifier, on lit les unités stockées dans l'élément de stockage d'unités conformément à une instruction de lecture appliquée de façon externe; et on change les unités conformément à une instruction de changement d'unités appliquée de façon externe, dans lequel
le changement des unités dans une direction d'augmentation des unités, sur la base de l'instruction de changement d'unités, est effectué après avoir déterminé si l'instruction de changement d'unités doit être suivie ou non, sur la base d'un résultat de la comparaison entre la donnée appliquée de façon externe à vérifier et le troisième cryptogramme.

2. Le procédé de la revendication 1, dans lequel le collationnement comprend la conversion du premier ensemble de cryptogrammes et l'ajout de celui-ci au second ensemble de cryptogrammes.

3. Un élément de stockage d'unités (1) comprenant :

un moyen de stockage (3) pour stocker des unités;
une première zone de données secrètes (54) stockant un premier cryptogramme, pouvant être établi par une première personne intervenant dans la fabrication de l'élément de stockage d'unités (1), ce premier cryptogramme caractérisant des données secrètes de la première personne;
une seconde zone de données secrètes (53) stockant un second cryptogramme pouvant être établi par une seconde personne différente de la première personne et intervenant dans l'utilisation de l'élément de stockage d'unités (1), le second cryptogramme caractérisant des données secrètes de la seconde personne;
un moyen de changement (7) pour changer les unités stockées dans le moyen de stockage (3);
un moyen d'entrée pour recevoir une donnée à vérifier;
un moyen de collationnement de cryptogrammes (63) pour collationner les premier et second cryptogrammes pour générer un troisième cryptogramme, ce moyen de collationnement de cryptogrammes (63) incluant
un moyen de comparaison (71) pour comparer la donnée à vérifier reçue par l'intermédiaire du moyen d'entrée avec le troisième cryptogramme, dans lequel
il est déterminé si le moyen de changement (7) doit augmenter les unités ou non, sur la base du résultat de la comparaison effectuée par le moyen de comparaison (71).

4. L'élément de stockage d'unités selon la revendication 3, dans lequel le moyen de collationnement de cryptogrammes convertit le premier ensemble de cryptogrammes et ajoute cet ensemble de cryptogrammes converti au second ensemble de cryptogrammes.

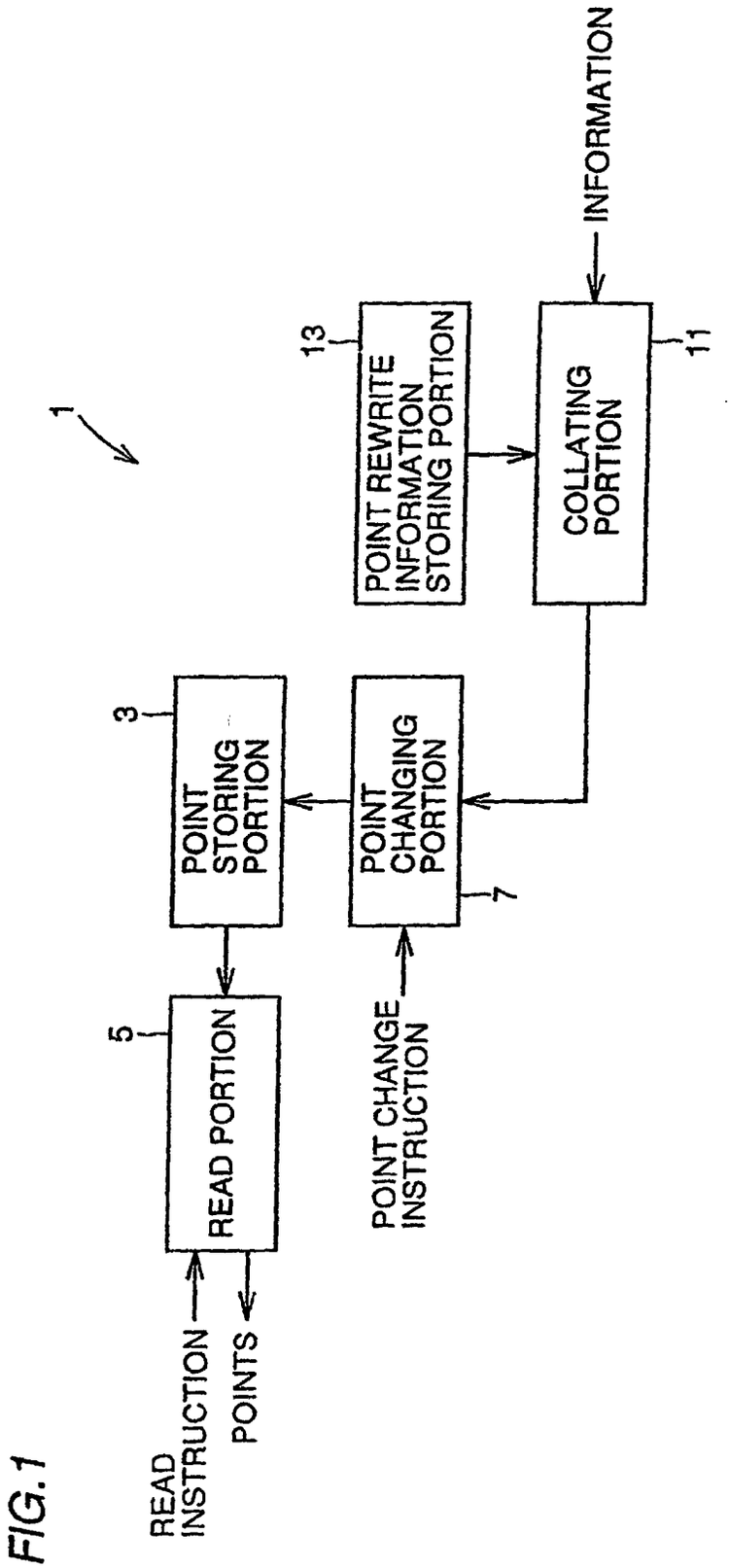
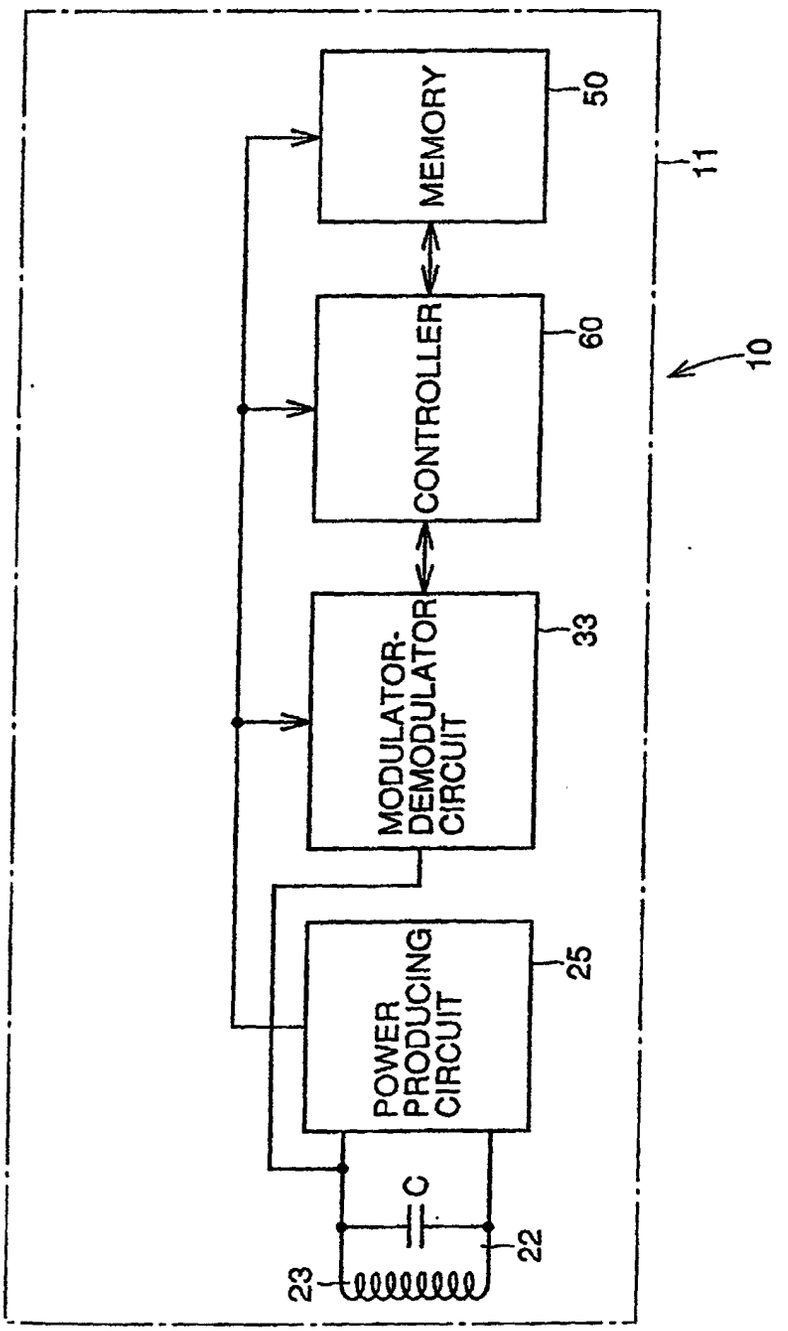

1
13
POINT REWRITE INFORMATION STORING PORTION
COLLATING PORTION
11
INFORMATION
3
POINT STORING PORTION
POINT CHANGING PORTION
7
5
READ PORTION
POINT CHANGE INSTRUCTION
READ INSTRUCTION
POINTS

FIG.1

FIG.2


MEMORY
50
11
CONTROLLER
60
10
MODULATOR-
DEMODULATOR
CIRCUIT
33
POWER
PRODUCING
CIRCUIT
25
C
22
23

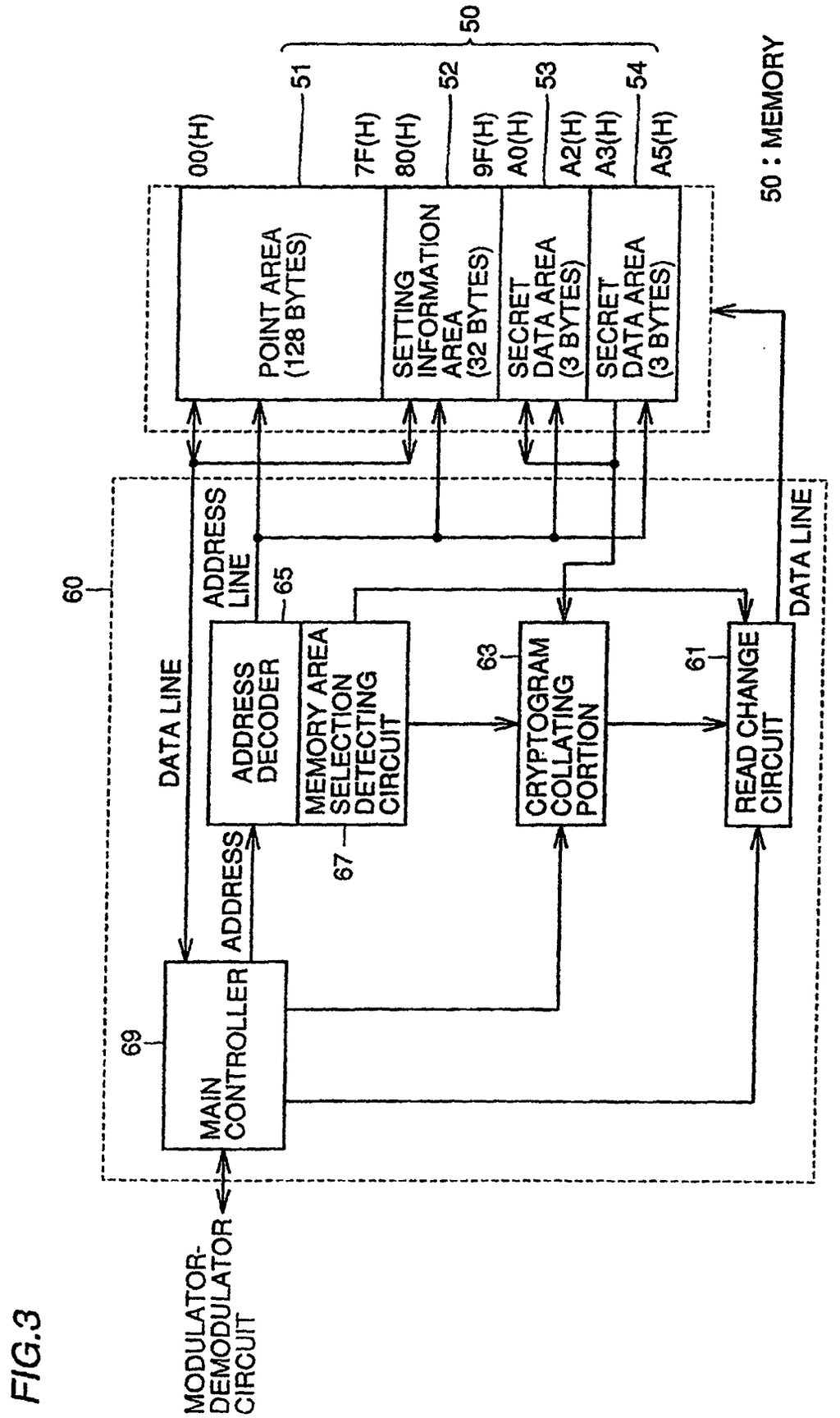

50
51
52
53
54
00(H)
7F(H)
80(H)
9F(H)
A0(H)
A2(H)
A3(H)
A5(H)
POINT AREA (128 BYTES)
SETTING INFORMATION AREA (32 BYTES)
SECRET DATA AREA (3 BYTES)
SECRET DATA AREA (3 BYTES)
50 : MEMORY
60
ADDRESS LINE
65
DATA LINE
ADDRESS DECODER
MEMORY AREA SELECTION DETECTING CIRCUIT
67
63
CRYPTOGRAM COLLATING PORTION
61
READ CHANGE CIRCUIT
DATA LINE
ADDRESS
69
MAIN CONTROLLER
MODULATOR-DEMODULATOR CIRCUIT

FIG.3

FIG.4

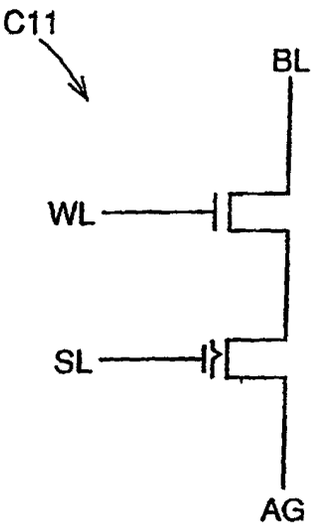


FIG.5

	BL	SL	WL	AG
READ	DATA OUTPUT	5V	5V	0V
WRITE	20V	0V	20V	OPEN
ERASE	0V	20V	20V	OPEN OR 0V

DATA CHANGE { WRITE: CHANGE "1" TO "0"
ERASE: CHANGE "0" TO "1"

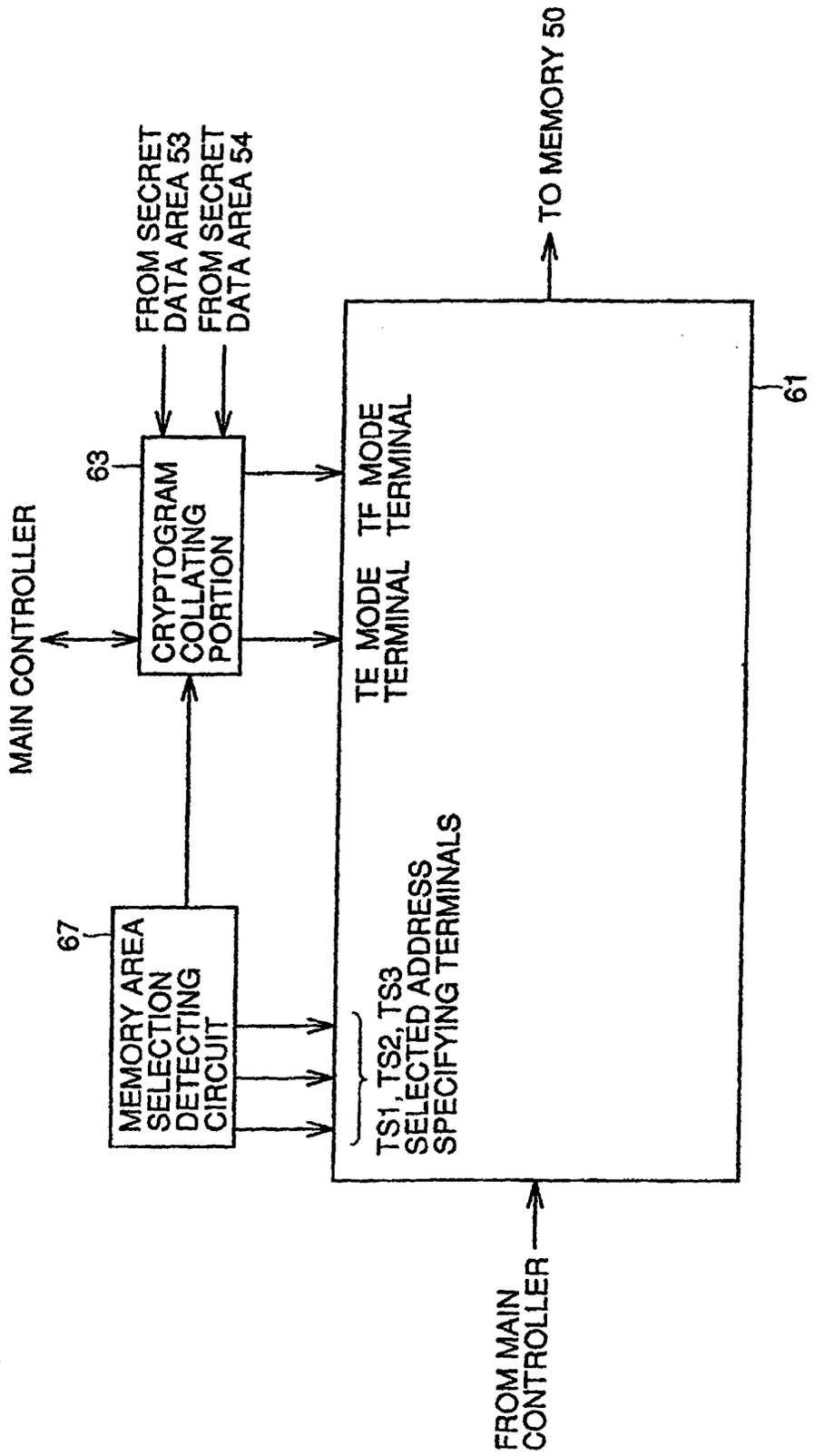

TO MEMORY 50
FROM SECRET DATA AREA 53
FROM SECRET DATA AREA 54
63
CRYPTOGRAM COLLATING PORTION
MAIN CONTROLLER
TE MODE TERMINAL
TF MODE TERMINAL
61
67
MEMORY AREA SELECTION DETECTING CIRCUIT
TS1, TS2, TS3 SELECTED ADDRESS SPECIFYING TERMINALS
FROM MAIN CONTROLLER

FIG.6

FIG.7

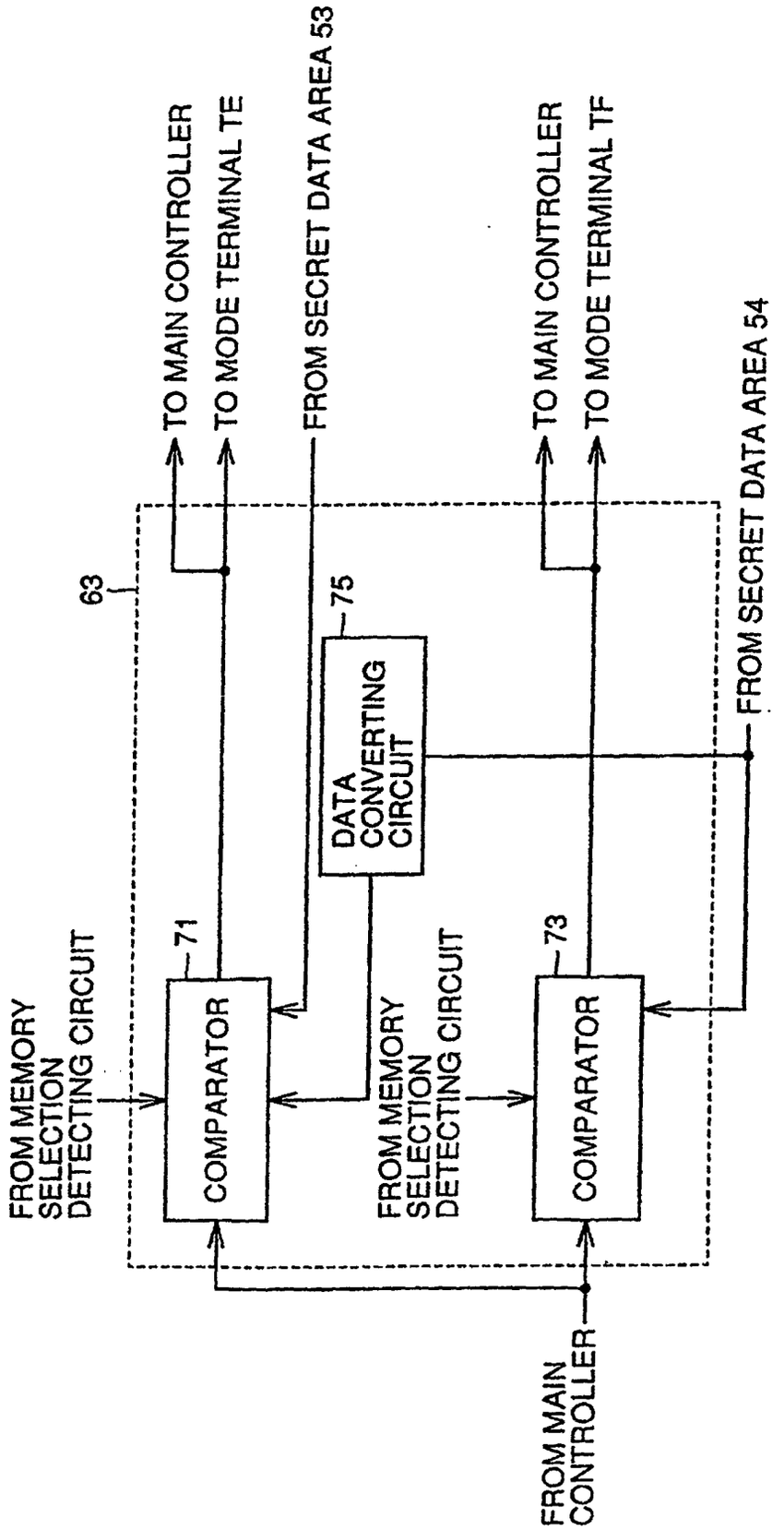

TO MAIN CONTROLLER
TO MODE TERMINAL TE
FROM SECRET DATA AREA 53
TO MAIN CONTROLLER
TO MODE TERMINAL TF
FROM SECRET DATA AREA 54
63
75
DATA CONVERTING CIRCUIT
71
COMPARATOR
73
COMPARATOR
FROM MEMORY SELECTION DETECTING CIRCUIT
FROM MEMORY SELECTION DETECTING CIRCUIT
FROM MAIN CONTROLLER

FIG.8

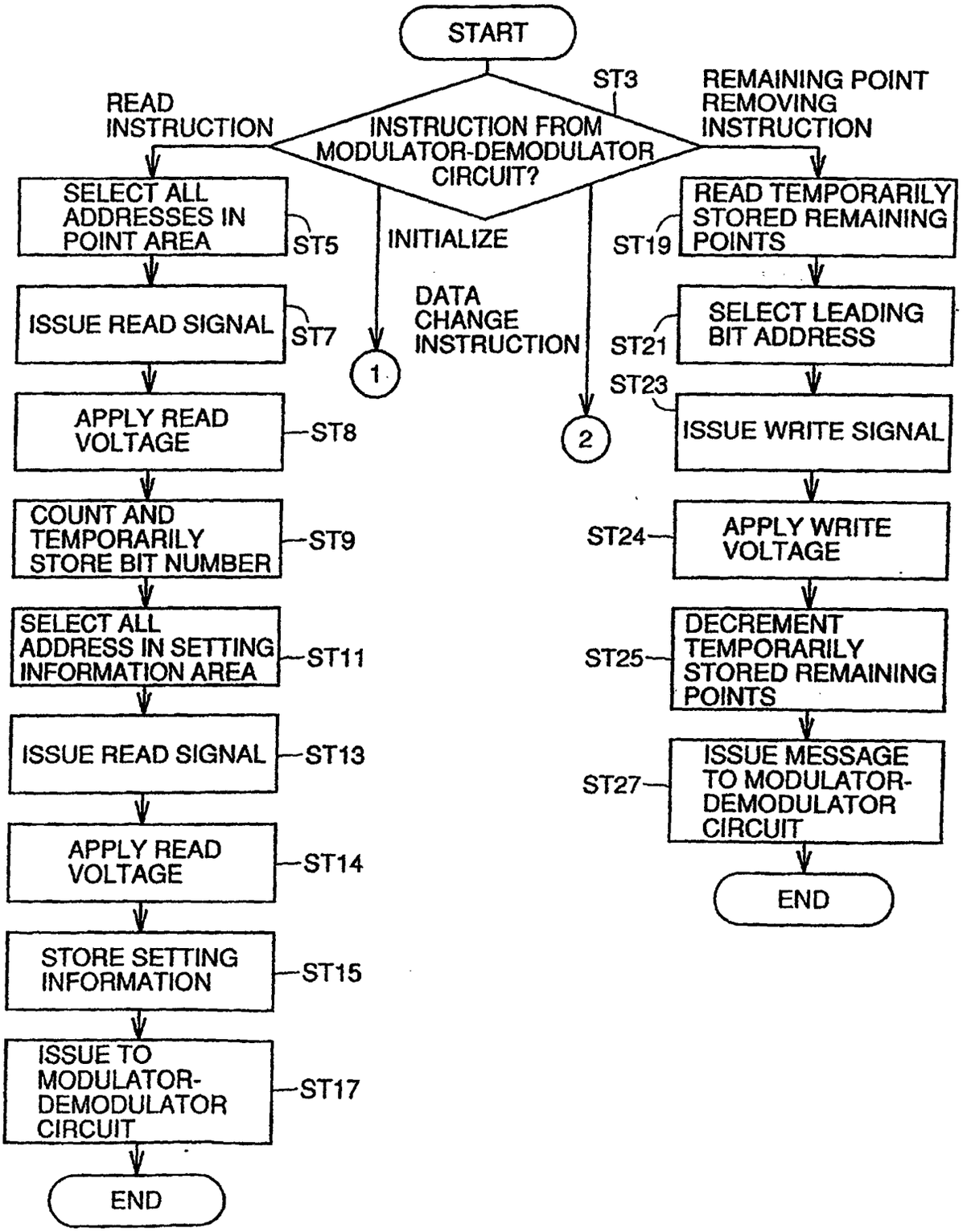

START
ST3
INSTRUCTION FROM MODULATOR-DEMODULATOR CIRCUIT?
READ INSTRUCTION
INITIALIZE
DATA CHANGE INSTRUCTION
REMAINING POINT REMOVING INSTRUCTION
SELECT ALL ADDRESSES IN POINT AREA
ST5
ISSUE READ SIGNAL
ST7
APPLY READ VOLTAGE
ST8
COUNT AND TEMPORARILY STORE BIT NUMBER
ST9
SELECT ALL ADDRESS IN SETTING INFORMATION AREA
ST11
ISSUE READ SIGNAL
ST13
APPLY READ VOLTAGE
ST14
STORE SETTING INFORMATION
ST15
ISSUE TO MODULATOR-DEMODULATOR CIRCUIT
ST17
END
1
2
READ TEMPORARILY STORED REMAINING POINTS
ST19
SELECT LEADING BIT ADDRESS
ST21
ST23
ISSUE WRITE SIGNAL
ST24
APPLY WRITE VOLTAGE
DECREMENT TEMPORARILY STORED REMAINING POINTS
ST25
ISSUE MESSAGE TO MODULATOR-DEMODULATOR CIRCUIT
ST27
END

FIG.9

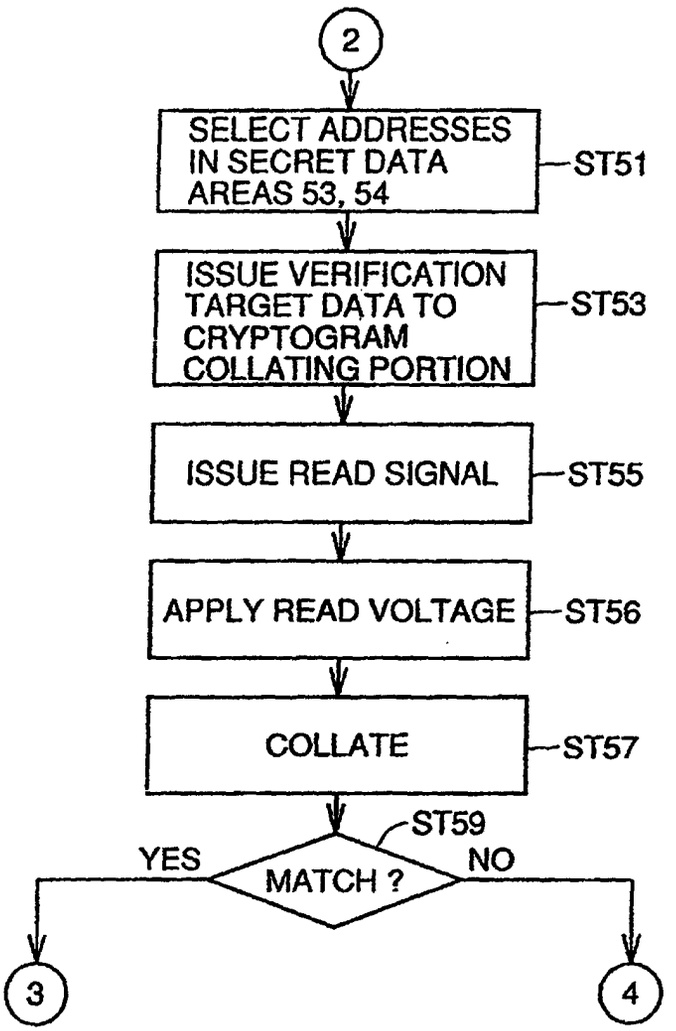

2
SELECT ADDRESSES IN SECRET DATA AREAS 53, 54
ST51
ISSUE VERIFICATION TARGET DATA TO CRYPTOGRAM COLLATING PORTION
ST53
ISSUE READ SIGNAL
ST55
APPLY READ VOLTAGE
ST56
COLLATE
ST57
ST59
YES
MATCH ?
NO
3
4

FIG.10

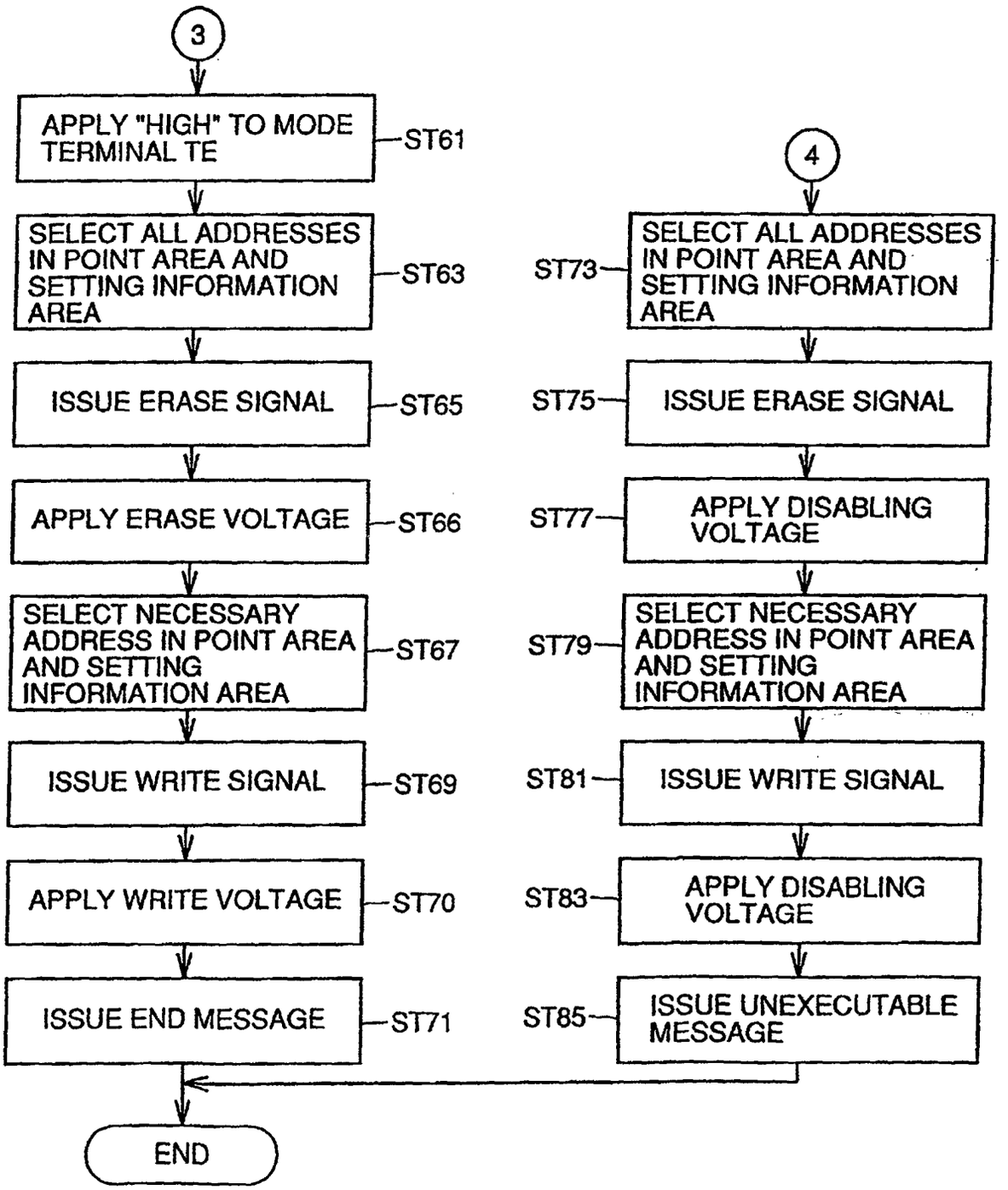

3
APPLY "HIGH" TO MODE TERMINAL TE
ST61
SELECT ALL ADDRESSES IN POINT AREA AND SETTING INFORMATION AREA
ST63
ISSUE ERASE SIGNAL
ST65
APPLY ERASE VOLTAGE
ST66
SELECT NECESSARY ADDRESS IN POINT AREA AND SETTING INFORMATION AREA
ST67
ISSUE WRITE SIGNAL
ST69
APPLY WRITE VOLTAGE
ST70
ISSUE END MESSAGE
ST71
END
4
ST73
SELECT ALL ADDRESSES IN POINT AREA AND SETTING INFORMATION AREA
ST75
ISSUE ERASE SIGNAL
ST77
APPLY DISABLING VOLTAGE
ST79
SELECT NECESSARY ADDRESS IN POINT AREA AND SETTING INFORMATION AREA
ST81
ISSUE WRITE SIGNAL
ST83
APPLY DISABLING VOLTAGE
ST85
ISSUE UNEXECUTABLE MESSAGE

FIG.11

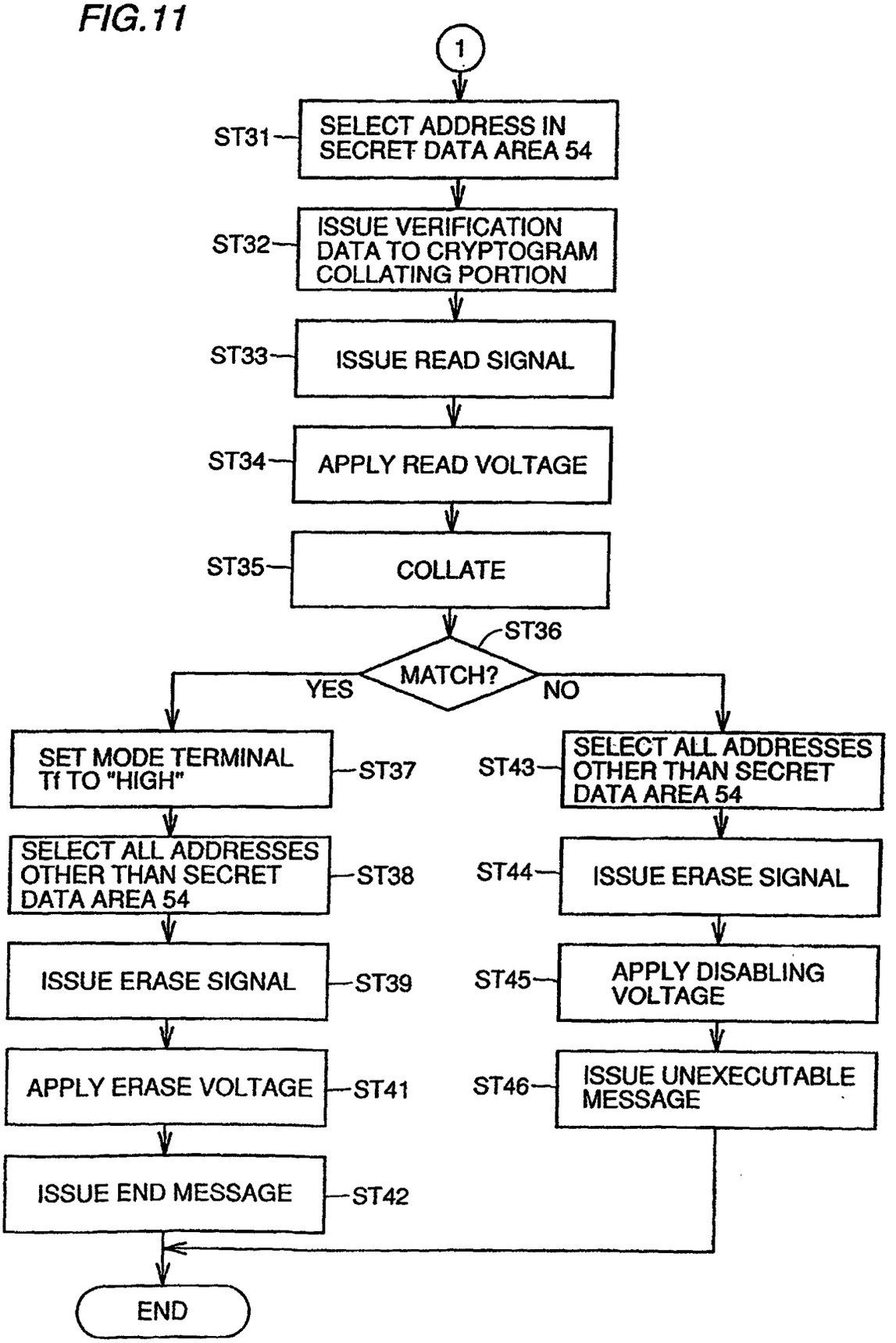
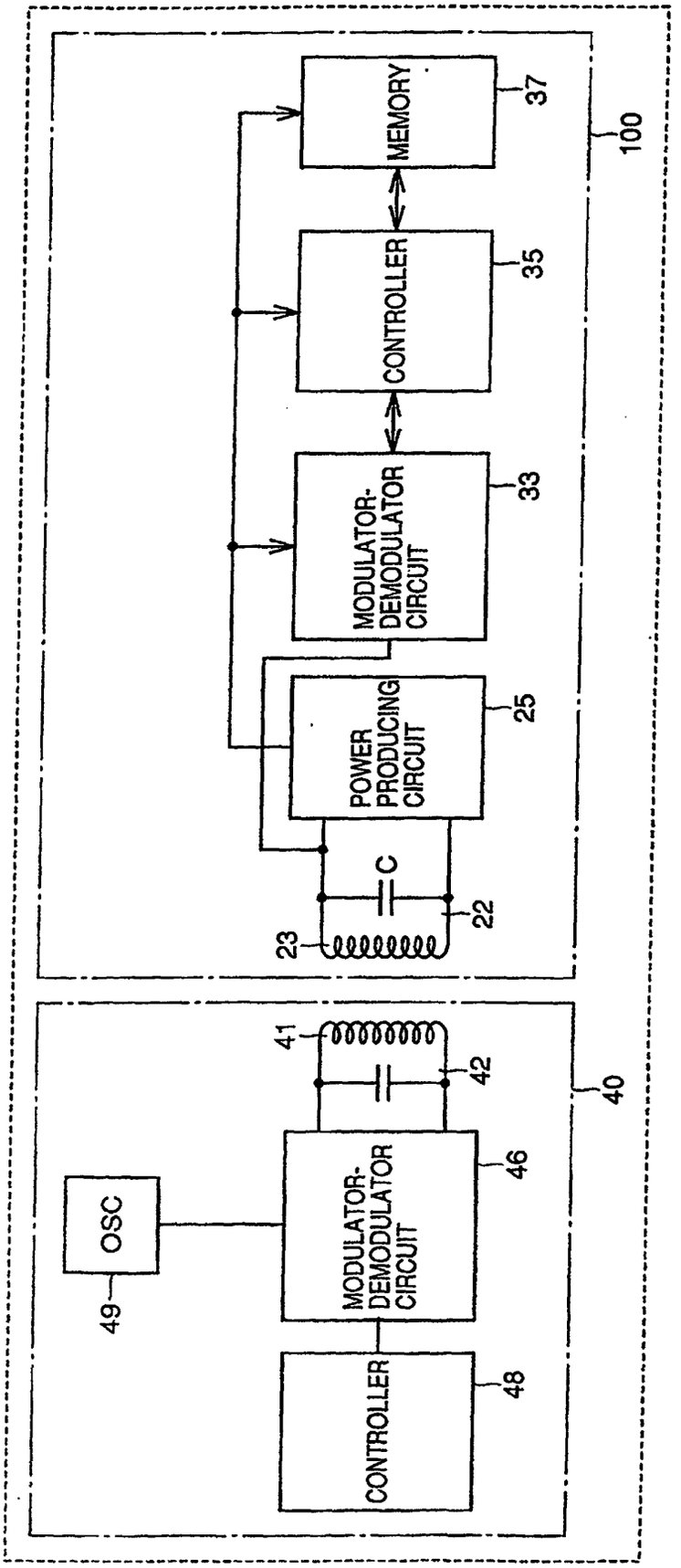

1
ST31
SELECT ADDRESS IN SECRET DATA AREA 54
ST32
ISSUE VERIFICATION DATA TO CRYPTOGRAM COLLATING PORTION
ST33
ISSUE READ SIGNAL
ST34
APPLY READ VOLTAGE
ST35
COLLATE
ST36
MATCH?
YES
NO
SET MODE TERMINAL Tf TO "HIGH"
ST37
SELECT ALL ADDRESSES OTHER THAN SECRET DATA AREA 54
ST38
ISSUE ERASE SIGNAL
ST39
APPLY ERASE VOLTAGE
ST41
ISSUE END MESSAGE
ST42
ST43
SELECT ALL ADDRESSES OTHER THAN SECRET DATA AREA 54
ST44
ISSUE ERASE SIGNAL
ST45
APPLY DISABLING VOLTAGE
ST46
ISSUE UNEXECUTABLE MESSAGE
END

FIG.12


100
MEMORY
37
CONTROLLER
35
MODULATOR-DEMODULATOR CIRCUIT
33
POWER PRODUCING CIRCUIT
25
C
22
23
40
41
42
MODULATOR-DEMODULATOR CIRCUIT
46
OSC
49
CONTROLLER
48