Description

The present invention relates to a method of manufacturing an IC card including a semiconductor chip comprising the steps of forming memory means having data input/output terminals, test address terminals and test data terminals on the semiconductor chip; testing the memory means by using the test address terminals and the test data terminals.

The recent years have been called "the cashless era.". Many things can be bought by using personal identification (ID) cards issued by credit companies and the like, eliminating the need to pay in cash.

Various kinds of ID cards are available at present, such as plastic cards, embossed cards, and cards with a magnetic stripe. From a structural point of view, these cards are easy to forge. Further, the data recorded on them can be easily read. Many cases of their illegal use have been reported, and this has become a great social problem.

To resolve this problem, IC cards with a built-in CPU and a built-in IC memory have been developed. The IC memory stores various data about the card owner, such as his or her personal identification number. The data cannot be easily read from the IC memory. Recently, an IC card system comprising such IC cards and terminals has been put to practical use.

Fig. 1 is a perspective view of an IC card. As shown in this figure, eight connection pads 12 are arranged on plastic card body 10 in two vertical rows, each consisting of four pads. When the IC card is inserted in a terminal, connection pads 12 contact the corresponding pins provided in the terminal. thereby electrically connecting the IC card to the terminal. Of these eight pads. only six are actually used at present. Magnetic stripe 14 is adhered to the surface of card body 10.

An integrated circuit (IC) of the structure shown in Fig. 2 is formed within card body 10. This IC comprises CPU (Central Processing Unit) 20 and EEP-ROM (Electrically Erasable Programmable - Read Only Memory) 22. The six connection pads, i.e., input/output terminal I/O, clock terminal CLOCK, reset terminal RESET, power supply terminal Vcc, ground terminal GND and datawriting power supply terminal Vpp, are provided in the IC. Due to its specific use, the IC must be greatly reliable. Therefore, it is subjected to an extremely strict test before delivery. EEP-ROM 22 is tested by inputting data to it, and outputting data from it, through input/output terminal I/O, bit by bit. Obviously, this method of testing EEP-ROM 22 requires too long a time. To save time, data pads D1 to Dn are coupled to n-bit data bus 24 connecting CPU 20 and EEP-ROM 22, and address pads A1 to Am are coupled to m-bit address bus 26 connecting CPU 20 and EEP-ROM 22. The test probe designed to test EEP-ROM 22 is put into contact with data pads D1 to Dn and address pads A1 to Am, whereby EEP-ROM 22 can be tested within a short time.

After EEP-ROM 22 has been tested, only leads 30 are bonded to eight pads 12 as illustrated in Fig. 3, but no process is performed on data pads D1 to Dn or address pads A1 to Am. Thereafter, the IC is incorporated into card body 10. More precisely, IC pellet 32 containing the IC (Fig. 2) is put within recess 34a made in base plate 34 of card body 10, and is then so positioned to have eight pads 12 aligned with leads 30, respectively. Leads 30 are then bonded to pads 12.

If the IC card happens to fall into the hands of a person other than the card owner, either by theft or loss, and if the IC is removed from card body 10, the data including secret data stored in EEP-ROM 22 could be read merely by touching a test probe to data pads D1 to Dn and address pads Al to Am, which remained intact. In other words, the IC card could be forged based on the data thus read from EEP-ROM 22. This greatly reduces the security of the IC card. In the worst possible case, the technical aspects of the IC card system as a whole can be analyzed and unlawfully utilized on a large scale.

From WO 83/00244 it is already known to disable direct access to a memory, particularly in connection with credit or security cards, by providing connection pads to the memory bus, which are only usable during test operations after manufacturing the integrated circuit chip on a wafer, but which connections are separated or destroyed when the wafer is cut into separate chips. This is particularly done by placing the connection pads connected to a memory bus of one chip on the area of the adjacent chip, so that the connections are automatically destroyed when cutting the wafer into chips. Moreover, it is indicated that these connections could also be separated if they were formed as fusible poly links, or the separation could be performed by laser beams.

It is an object of the invention to provide a method of manufacturing an IC card in which this step of separating the connections to test address terminals and test data terminals is more flexibly performed, so that the internal data cannot be illegally read, thereby maintaining the security of not only the card but also the system in which the card is used.

According to the invention, as defined by claim 1, a method of manufacturing an IC card including a semiconductor chip is characterized by the steps of storing a specified address which is not used in the memory means in a fixed address unit formed on the semiconductor chip; supplying the specific address to the memory means after the testing of the integrated circuit card is completed; comparing the address input to the memory

means with the specific address stored in the fixed address unit; and electrically disconnecting by logic gate means the test data terminals from the data bus of the memory means upon detecting the input of the specific address.

Preferable embodiments are defined in the dependent claims.

This invention can be more fully understood from the following detailed description when taken in conjunction with the accompanying drawings, in which:

Figure 1 is a perspective view of an IC card;
Figure 2 shows the internal circuit of the IC card shown in figure 1;
Figure 3 is a diagram representing the connection between the IC pellet and base plate of a conventional IC card;
Figure 4 is a flow chart explaining the process of manufacturing an IC card with mechanical disconnection of the test pads;
Figure 5 is a perspective view of the IC pellet used in the IC card according to the solution of figure 4;
Figure 6 is a diagram illustrating the connection between the IC pellet and base plate of the IC card according to the solution of figures 4 and 5;
Figure 7 is a cross-sectional view of the IC card according to the solution of figures 4 and 5;
Figure 8 is a cross-sectional view of the IC card which is a modification;
Figure 9 shows the internal circuit of the IC card
Figure 10 is a flow chart explaining the process of manufacturing the IC card according to an embodiment of the invention; and
Figure 11 is a flow chart explaining the operation of the IC card.

First, it will be explained how the IC card, e.g., a credit card, is manufactured with reference to the flow chart of figure 4.

To manufacture an IC card and bring it into a usable condition, a card manufacturer, a card issuer and a cardholder all take part in the process. In step S1, the card manufacturer forms an IC on a wafer. This IC is similar to the one shown in Fig. 2.

In step S2, the manufacturer tests the IC. To be more precise, a test probe is put into contact with the exposed test data pads and test address pads of the IC, thereby accomplishing various tests. (As described above, the test data pads are coupled to the data bus connecting the CPU and EEP-ROM both included in the IC, and the test address pads are coupled to the address bus connecting the CPU and EEP-ROM.) In the next step, step S3, the wafer is diced into a plurality of IC pellets. In step S4, the test data pads and test address pads, which are no longer necessary, are removed from each IC pellet, or disconnected from the data bus and address bus formed in the IC pellet. Now, only one terminal i.e., input/output terminal I/O, through which data in the EEP-ROM can be read out, is connected to the IC. This prevents an illegal access to the EEP-ROM. Test(data pads D1 to Dn and test address pads A1 to Am are removed by cutting the opposing edge portions of IC pellet 32, on which test pads D1 to Dn and test address pads A1 to Am are formed, along the one-dot-one-dash lines shown in Fig. 5. Eight connection pads 38, which will be electrically connected to pads 12 (Fig. 1), are formed on other opposing edge portions of IC pellet 32. IC pellet can be cut to remove the test data pads and test address pads, by applying a laser beam or an etching solution to IC pellet 32.

Thereafter, in step S5, die-bonding is carried out to bond IC pellet 32 to base plate 34, and wire-bonding is performed to bond leads 30 to pads 38. More specifically, as shown in Fig. 6, IC pellet 32 is placed in recess 34a made in base plate 34 and is positioned to have pads 38 aligned with the ends (30a) of leads 30. IC pellet 32 is then die-bonded-to-base plate 34, and pins 38 of IC pellet 32 are connected to ends 30a of leads 30 by hot-pressing or pulse-heating process.

In the next step, step S6, a resin is applied onto the major surface of base plate 34, in which IC pellet 32 is now provided, thereby achieving the plasticsealing of IC pellet 32. Then, test data is written in the test data area of the memory section of IC pellet 32, in step S7, through input/output terminal I/O. The test data is a minimal amount of data that is required for the fundamental operation of the IC card.

Then, in step S8, the IC pellet is subjected to the final test. Namely, basic tests on codes such as PIN (later described) are carried out.

In step S9, the unit consisting of IC pellet 32, base plate 34 and leads 30 is built in an IC card body. As shown in Fig. 7, the IC card body comprises upper sheet 42, intermediate sheet 44 and lower sheet 46, which are put one upon another and bonded together. To be more precise, intermediate sheet 44 made of hardy PVC is bonded to lower sheet 46 made of soft PVC. Sheet 44 has an opening. This opening forms a recess 44a when sheet 44 and 46 are bonded. The base plate 34 is bonded to sheet 42, forming an IC assembly. Upper sheet 42 made of soft PVC has eight through holes. arranged in two rows, each row consisting of four holes. Eight contacts 42a are formed in these holes. The IC assembly is positioned within recess 44a such that the IC unit contacts lower sheet 46. Then, upper shect 42 is bonded to intermediate sheet 44, such that contacts

42a are connected to base plate 34. As a result, the IC card body is formed. A magnetic stripe (not shown in Fig. 7) is bonded on upper sheet 42. As a result, an IC card is manufactured. This IC card has the same outer appearance as the conventional IC card shown in Fig. 1.

Thereafter, in step S10, the card manufacturer inserts the IC card into a manufacturer's card terminal, and operates the manufacturer's card terminal, thereby writing codes CA (Card Authenticator), IPIN (Initialization Personal Identification Number), PMK (Production Master Key) and PRK (Private Key) into EEP-ROM 22. Code CA will be used to encrypt and decrypt messages. Code IPIN is a 6-bit code which remains valid until code PIN (Personal Identification Number) is written into EEP-ROM 22. Code PMK represents the number assigned to IC cards of the same lot. Code PRK will be used to decrypt an encrypted message.

After codes CA, IPIN, PMK and PRK have been written into EEP-ROM 22, the manufacturer's card terminal prints code PMK on a sheet of paper. In step S11, the card manufacturer mails the IC card and the PMK-printed paper to the card issuer under separate cover. Here, the card manufacturer has finished all work required of him.

The card issuer inserts the IC card into an issuer's card terminal, and operates the issuer's card terminal, thereby inputting code PAN representing the primary account number assigned to the cardholder, and also inputting code PMK printed the sheet of paper mailed from the card manufacturer. Code PAN is written into EEP-ROM 22 in step S12 only when code PMK is identical with code PMK written in EEP-ROM 22 in step S10. When code PAN is written into EEP-ROM 22, the issuer's card terminal reads code IPIN from EEP-ROM 22 and prints this code on a sheet of paper. In step S13, the card issuer mails the IC card and the IPIN-printed paper to the cardholder.

The cardholder takes the IC card and the IPIN-printed paper to the card issuer's office. In step S14, the cardholder inserts the IC card in the card terminal installed in the card issuer's office, and then operates the card terminal, thereby inputting his or her personal identification number (PIN) and also code IPIN printed on the paper mailed from the card issuer. Code PIN is written into EEP-ROM 22 only when code IPIN is identical with code IPIN already written in EEP-ROM 22. After code PIN has been thus written into EEP-ROM 22, the IC card can be used.

Before delivery the test data pads and test address pads are removed from the IC pellet after the IC chip has been tested. Therefore, if the IC card containing this IC pellet chances to fall into the hands of anyone other than the cardholder by theft or loss, and if the IC pellet is removed from the IC card, the data stored in EEP-ROM 22 can by no means be read. This prevents a forgery of the IC card, and ultimately maintains not only the security of the IC card, but also the security of the IC card system. Not all the test pads need be removed after the test of the IC pellet. For instance, it suffices to remove only the test data pads, only the test address pads or only some of the test data pads or test address pads.

A modification will now be described. In the first solution, pads 38 are wirebonded to leads 30 in step S5. Without such wirebonding, pads 38 can be connected to leads 30 as in the modification (i.e., an IC pellet) shown in Fig. 8. As illustrated in Fig. 8. which is a cross-sectional view, this IC pellet comprises silicon substrate 52, active region 54 formed in the surface of substrate 52, insulation layer 56 formed on the surface of substrate 52 and having contact holes, inner contact pad 58 formed on insulation layer 56 and electrically connected to active region 54 through the contact holes of insulation layer 56, insulation layer 60 formed on inner contact pad 58 and having contact holes, and outer contact pad 62 formed on insulation layer 60 and electrically connected to inner contact pad 58 through the contact holes of insulation layer 60. This IC pellet (Fig. 8) is adhered to a base plate with an anisotropically conducive adhesive. The unit consisting of the IC pellet and base plate is incorporated into an IC card body, thereby forming an IC card. The anisotropically conductive adhesive consists of a hot-melt insulative adhesive and electrically conductive particles of nickel, silver or carbon, dispersed within the adhesive. It allows the passage of an electric current only in the direction in which it is compressed by hot-pressing. When outer contact pad 62 is extremely narrow, no conductive particles contained in the anisotropically conductive adhesive can contact pad 62. If this is the case, no electrical connection is accomplished between the IC pellet (Fig. 8) and the base plate. Therefore, in the modification of Fig. 8, outer contact pad 62 is broad enough to ensure the electrical connection between the IC pellet and the base plate. Since no wirebonding is required in connecting the IC pellet to the base plate, the IC pellet can be efficiently connected to the base plate.

As shown in Fig.9, the internal circuit comprises a system bus 151 comprising an address bus 26 and a data bus 24. Data ROM 152, application ROM 153, system program ROM 154, working RAM 155, system controller 156, decryption unit 157, and read/write controller 158 are coupled to system bus 151. Input buffer 159 is connected to system bus 151, and input controller 160 is coupled to input buffer 159. Output buffer 161 is connected to system bus 151, and output controller 162 is connected to output buffer 161. Data input/output terminal I/O is connected to input controller 160 and also to output controller 162.

Data ROM 152 stores data representing all operation conditions of the IC cards, such as data-writing vol-

tage, current tolerance, maximum application time, maximum data transmission capacity, and maximum response-waiting time. When the IC card is initialized, the condition data is supplied as "answer-to-reset" data to a card terminal (not shown) in conformance with a preset format. Application RON 153 stores code APN (Application Name) showing the classification of the IC card. Code APN is put into a specified format and then supplied to the card terminal when an attribute exchange takes place in the card- terminal after initial parameters have been set in the card terminal in accordance with the answerto-reset data. System program ROM 154 stores codes ACK (acknowledgment) and NAC (non-aknowledgment), as well as every kind of system program. Code ACK indicates that the signal transmitted from the card terminal to the IC card is correct, and code NAC shows that this signal is incorrect. System controller 156 has an internal decision area. Controller 156 outputs commands to the associated components included in the internal circuit of the IC card, in accordance with the data supplied from input buffer 159 and in accordance with the operation status of the IC card. Decryption unit 157 decrypts the input data supplied from the card terminal through input buffer 159, in accordance with an RSA algorithm. It uses the decryption key code (the card issuer's private key) stored in key code memory 157a. Unit 157 outputs the decrypted data to comparator 163. The output data of comparator 163 is supplied to system controller 156 through system control line 156a. System control line 156a is connected to flag 164. Flag 164 is set or reset by the output data of comparator 163. Read/ write controller 158 controls the data-writing and data-reading from data memory 165 in accordance with the command supplied from system controller 156. The data read from data memory 165 under the control of read/write controller 158 is. input to comparator 163, system bus 151 or card status buffer 166. Read/write controller 158 has a tri-state gate 181. Tri-state gate 181 is connected on data lines 182 to which the test data pads (not shown in Fig. 9) of the IC card are connected.

Flag section 183 comprised of a one-bit memory is connected to read/write controller 158. The output of comparator 168 is coupled to a set terminal of flag section 183 as a fetch signal. The output signal of flag-setting section 183 is supplied to inverter 184. The output of inverter 184 is supplied to the control terminal of tri-state gate 181 and also to the input terminal of flag section 183.

Data memory 165 is, for example, an EEP-ROM. Secret codes CA, IPIN, PAN, CHN, EPD, PRK and RTN, and status data ST are written in this memory. Code CHN represents the cardholder's name, and code EPD shows the expiration data of the IC card Code RTN indicates the number of times any incorrect data has been input to the IC card. Status data ST represents the present status of the IC card. More precisely, data ST shows whether the IC card has been completely manufactured, duly issued, or made usable by entering code PIN. Status data ST is in the same format as code APN (Application Name) stored in application ROM 153. Data ST is. transmitted to the card terminal. Data memory 165 is not limited to an EEP-ROM; it can be comprised of an EP-ROM (Erasable Programmable - Read Only Memory), for instance.

System controller 156 is connected to timer 167. This timer 167 counts a predetermined period of time during the normal data exchange between the IC card and the card terminal, when a start data write voltage supply message is output by the card terminal. If a positive response code ACK is not supplied from the card terminal to the IC card during said period of time, system controller 156 stops the data exchange between the IC card and the card terminal.

Read/write controller 158 is connected to system bus 151 by a bus line. This bus line is coupled to one of the two input terminals of address comparator 168. Fixed address unit 169 is connected to the other input terminal of address comparator 168. Unit 169 stores a specific address of memory 165 that is not used. Address comparator 168 compares any address supplied to it via system bus 151, with the address stored in fixed address unit 169. The output data of comparator 168 is supplied to read/write controller 158 and also to the set terminal of flag section 183. When the two addresses compared by address comparator 168 are the same, that is, when the card terminal has input an illegal address, address comparator 168 generates a coincidence signal and read/write controller 158 clears all data stored in data memory 165 thereby preventing secret data from being read out of the card.

When the IC card is electrically coupled to the card terminal, a reset signal RESET and a system clock signal are supplied from the card terminal to the IC card through connection pads. Voltages Vcc and Vpp are applied from the card terminal to the IC card. Voltage Vcc is used to drive both the IC card and the card terminal, and voltage Vpp is used to write data into data memory 165. The card terminal starts applying these voltages to the IC card in response to the answer-to-reset data read from data ROM 152. The system clock signal supplied to the IC card is frequency-divided by frequency divider 170.

The data exchange between the IC card shown in Fig. 9 and the card terminal will now be explained. When the IC card is inserted into the card terminal and thus electrically connected thereto, the card terminal supplies an initialization signal to the IC card. In response to the initialization signal, system controller 156 reads the answer-to-reset data from data ROM 152. The answer-to-reset data is supplied to the card terminal through output buffer 161, output controller 162 and input/output terminal I/O.

If the answer-to-reset data is found to be correct. the card terminal sends an enquiry code (ENQ) to the IC card. Code ENQ is input to working RAM 155 through input-output terminal I/O, input controller 160 and input buffer 159. System controller 156 determines whether or not code ENQ has been correctly written into working RAM 155. If it determines that code ENQ has been corretly written. system controller 156 suoplies code ACK to the card terminal through output buffer 161, output controller 162 and input/output terminal I/O. If system controller 156 determines that code ENQ has been incorrectly written, it supplies code NAC to the card terminal.

In response to code ACK, the card terminal sends terminal code TC representing the type of the card terminal to the IC card. In response to code NAC. the card terminal ejects the IC card, thereby electrically disconnecting the IC card from it.

When terminal code TC is supplied to the IC card, code APN (Application Name) showing the type of the IC card is read from application ROM 153 under the control of system controller 156. Code APN is temporarily latched in output buffer 161 and is then sent to the card terminal.

The card terminal determines, from code APN, whether or not the IC card is compatible with the card terminal. If the IC card is found to be compatible, the card terminal sends a command code to the IC card. Conversely, if the IC card is found to be incompatible, the card terminal ejects the IC card, thereby electrically disconnecting the IC card from it.

When the command code is supplied to the IC card, code PIN (Personal Identification Number) stored in the IC card is compared with code PIN input through the keyboard of the card terminal. If these compared codes are identical, data will be exchanged between the IC card and the card terminal, thereby enabling a financial transaction.

With reference to the flow chart of Fig. 10, it will be briefly explained how the IC card is manufactured. First, in step S100, data memory 165 is tested for its function. More specifically, a test probe is put into contact with the test data pads connected to data lines 182 and the test address pads connected to address lines 150, as in the test of the IC pellet built in the IC card of the solution of figures 4 and 5. Since flag section 183 is set to "0," the output of inverter 184 is "1." Tri-state gate 181 is therefore conductive. Hence, the data stored in those addresses of data memory 165 which have been designated by the signals supplied from the test probe through the test address pads, address lines 150 and system bus 151, is read out to the test data pads coupled to data lines 182, through tri-state gate 181 of read/write controller 158. Data memory 165 is thereby tested.

Upon completion of the test of data memory 165, the address data identical with the address stored in fixed address unit 169 is input to comparator 168 through system bus 151 in step S102. As a result. the output of comparator 168 becomes "1," whereby a signal for reading the output of inverter 184 is supplied to flag-setting section 183 through fine 185 connecting compa-rator 168 to flag section 183. Then, in step S104, the output of inverter 184. i.e., "1," is sent to flag section 183. The output of inverter 184 therefore changes to "0", and tri-state gate 181 becomes inconductive. Consequently, data lines 182 are electrically cut, and the test data pads, which are coupled to these data lines 182, are electrically disconnected from data memory 165. Thereafter, the IC pellet is built in an IC card body, whereby the IC card is completed.

If any person other than the cardholder receives this IC card by theft or by chance, he or she has no way to access to data memory 165 since the data pads have been disconnected from data lines 182. In short, an illegal reading of the data from data memory 165 can be prevented. This ensures not only the security of the IC card but also that of the IC card system as a whole.

Furthermore, some security measures are taken during the use of the IC card, as will be explained with reference to the flow chart of Fig 11. In step S110, it is determined whether or not a command for an access to data memory 165 has been supplied to the IC card. If YES, a data memory address is generated in step S112. In the next step, step S114, it is determined whether or not address comparator 168 has found that this address is identical with the address stored in fixed address unit 169. If NO in step S114, an access is made to data memory 165, in step S116. If YES in step S114, read/ write controller 158 clears the data stored in data memory 165 in step S118. The two addresses compared by comparator 168 can be identical also when tri-state gate 181 is rendered inconductive after the IC pellet has been tested. Nonetheless, when the data set in flag section 183 is "0" and tri-state gate 181 is made conductive, the data stored in memory 165 is not cleared. Data memory 165 is cleared only when both the output of comparator 168 and the data set in flag section 183 are "1."

All data stored in data memory 165 is cleared when the address set in fixed address unit 169 which is not provided in data memory 165 is supplied to the IC card. Therefore, the data cannot be illegally read from data memory 165.

In the embodiment, tri-state gate 181 is used to electrically cut data lines 182, thereby electrically disconnecting the test data pads from data memory 165. Any other means, such as a gate or a switch, can be used for the same purpose. Further, tri-state gate 181 can be replaced by a fuse which is physically cut, thereby to

permanently cut data lines 182. Still further, a tri-state gate can be connected between address lines 150 and system bus 151 for electrically connecting or disconnecting the test address pads to or from data memory 165, either in place of, or in addition to, tristate gate 181. Further, plural unused memory addresses may be stored in fixed address unit 169.

As described above, in the present invention, the test data pads are disconnected from the data lines 182 or the test address pads are cut from the address lines 150, after the IC pellet has been tested. Alternatively, all test pads are disconnected from the data lines and address lines after the test of the IC pellet. Therefore, an illegal access to the data memory provided within the IC card is prevented, ensuring not only the security of the IC card, but also that of the IC card system.

Claims

1. A method of manufacturing an IC card including a semiconductor chip comprising the steps of: forming memory means (22,165) having data input/output terminals (I/O), test address terminals (A1-Am) and test data terminals (D1-Dn) on the semiconductor chip (32); testing the memory means (22,165) by using the test address terminals (A1-Am) and the test data terminals (D1-Dn), characterized by the steps of: storing a specified address which is not used in the memory means (22,165) in a fixed address unit (169) formed on the semiconductor chip (32); supplying the specific address to the memory means (22,165) after the testing of the integrated circuit card is completed; comparing the address input to the memory means (22,165) with the specific address stored in the fixed address unit (169); and electrically disconnecting by logic gate means (181) the test data terminals (D1-Dn) from the data bus (24) of the memory means upon detecting the input of the specific address.

2. A method according to claim 1, characterized by
using said memory means (22, 165) for storing secret data, generating a coincidence signal and setting a flag section (183) upon detecting the input of said specific address and the output of said flag section (183) turning off said gate means (181) when set.

3. A method according to claim 2,
characterized by
providing data clearing means (158, 168, 169) for clearing said secret data stored in said memory means (22, 165).

4. A method according to claim 3
characterized by
providing data clearing means (158, 168, 169) for clearing said secret data stored in said memory means (22, 165), when said input address is found to be identical with said unused address stored in said fixed address unit (169) and when said flag section (183) is set.

Patentansprüche

1. Verfahren zur Anfertigung einer IC-Karte mit einem Halbleiterchip, bestehend aus folgenden Schritten:
Ausbildung von Speichervorrichtungen (22, 165) mit Daten-Eingabe-/Ausgabe-Terminals (I/O), Testadressenterminals (A1-Am) und Testdatenterminals (D1-Dn) auf dem Halbleiterchip (32);
Prüfung der Speichervorrichtungen (22, 165) unter Verwendung der Testadressenterminals (A1-Am) und der Testdatenterminals (D1-Dn),
gekennzeichnet durch die Schritte:
Speicherung einer spezifizierten Adresse, die nicht in den Speichervorrichtungen (22, 165) verwendet wird, in einer Festadresseneinheit (169), welche auf dem Halbleiterchip (32) ausgebildet ist;
Zuführung der spezifischen Adresse zu den Speichervorrichtungen (22, 165) nach Abschluß des Tests der IC-Karte;
Vergleich der den Speichervorrichtungen (22, 165) eingegebenen Adresse mit der in der Festadresseneinheit (169) gespeicherten spezifischen Adresse; und
elektrische Unterbrechung der Verbindung der Testdatenterminals (D1-Dn) mit dem Datenbus (24) der Speichervorrichtung mittels logischer Gattervorrichtungen, nachdem eine Eingabe der spezifischen Adresse ermittelt wurde.

permanently cut data lines 182. Still further, a tri-state gate can be connected between address lines 150 and system bus 151 for electrically connecting or disconnecting the test address pads to or from data memory 165, either in place of, or in addition to, tristate gate 181. Further, plural unused memory addresses may be stored in fixed address unit 169.

As described above, in the present invention, the test data pads are disconnected from the data lines 182 or the test address pads are cut from the address lines 150, after the IC pellet has been tested. Alternatively, all test pads are disconnected from the data lines and address lines after the test of the IC pellet. Therefore, an illegal access to the data memory provided within the IC card is prevented, ensuring not only the security of the IC card, but also that of the IC card system.

Claims

1. A method of manufacturing an IC card including a semiconductor chip comprising the steps of: forming memory means (22,165) having data input/output terminals (I/O), test address terminals (A1-Am) and test data terminals (D1-Dn) on the semiconductor chip (32); testing the memory means (22,165) by using the test address terminals (A1-Am) and the test data terminals (D1-Dn), characterized by the steps of: storing a specified address which is not used in the memory means (22,165) in a fixed address unit (169) formed on the semiconductor chip (32); supplying the specific address to the memory means (22,165) after the testing of the integrated circuit card is completed; comparing the address input to the memory means (22,165) with the specific address stored in the fixed address unit (169); and electrically disconnecting by logic gate means (181) the test data terminals (D1-Dn) from the data bus (24) of the memory means upon detecting the input of the specific address.

2. A method according to claim 1, characterized by
using said memory means (22, 165) for storing secret data, generating a coincidence signal and setting a flag section (183) upon detecting the input of said specific address and the output of said flag section (183) turning off said gate means (181) when set.

3. A method according to claim 2,
characterized by
providing data clearing means (158, 168, 169) for clearing said secret data stored in said memory means (22, 165).

4. A method according to claim 3
characterized by
providing data clearing means (158, 168, 169) for clearing said secret data stored in said memory means (22, 165), when said input address is found to be identical with said unused address stored in said fixed address unit (169) and when said flag section (183) is set.

Patentansprüche

1. Verfahren zur Anfertigung einer IC-Karte mit einem Halbleiterchip, bestehend aus folgenden Schritten:
Ausbildung von Speichervorrichtungen (22, 165) mit Daten-Eingabe-/Ausgabe-Terminals (I/O), Testadressenterminals (A1-Am) und Testdatenterminals (D1-Dn) auf dem Halbleiterchip (32);
Prüfung der Speichervorrichtungen (22, 165) unter Verwendung der Testadressenterminals (A1-Am) und der Testdatenterminals (D1-Dn),
gekennzeichnet durch die Schritte:
Speicherung einer spezifizierten Adresse, die nicht in den Speichervorrichtungen (22, 165) verwendet wird, in einer Festadresseneinheit (169), welche auf dem Halbleiterchip (32) ausgebildet ist;
Zuführung der spezifischen Adresse zu den Speichervorrichtungen (22, 165) nach Abschluß des Tests der IC-Karte;
Vergleich der den Speichervorrichtungen (22, 165) eingegebenen Adresse mit der in der Festadresseneinheit (169) gespeicherten spezifischen Adresse; und
elektrische Unterbrechung der Verbindung der Testdatenterminals (D1-Dn) mit dem Datenbus (24) der Speichervorrichtung mittels logischer Gattervorrichtungen, nachdem eine Eingabe der spezifischen Adresse ermittelt wurde.

* C L M S *

2. Verfahren nach Anspruch 1,
gekennzeichnet durch
die Verwendung der Speichervorrichtungen (22, 165) zum Speichern von Geheimdaten, Erzeugung eines Koinzidenzsignals und Setzen eines Flagbereiches (183), nachdem die Eingabe der spezifischen Adresse ermittelt wurde, und der Ausgang des Flagbereiches (183) die Gattervorrichtung (181) abschaltet, wenn er gesetzt ist.

3. Verfahren nach Anspruch 2,
gekennzeichnet durch
die Bereitstellung von Datenlöschvorrichtungen (158, 168, 169) zur Löschung der in den Speichervorrichtungen (22, 165) gespeicherten Geheimdaten.

4. Verfahren nach Anspruch 3,
gekennzeichnet durch
die Bereitstellung von Datenlöschvorrichtungen (158, 168, 169) zum Löschen der in den Speichervorrichtungen (22, 165) gespeicherten Geheimdaten, wenn festgestellt wird, daß die eingegebene Adresse mit der nichtverwendeten, in der Festadresseneinheit (169) gespeicherten Adresse identisch ist und wenn der Flagbereich (183) gesetzt ist.

Revendications

1. Un procédé de fabrication d'une carte à circuit intégré contenant une puce de semiconducteur, qui comprend les étapes suivantes :
on établit des moyens de mémoire (22, 165) ayant des bornes d'entrée/sortie de données (I/O), des bornes d'adresse de test (A1-Am) et des bornes de données de test (D1-Dn), sur la puce de semiconducteur (32) ;
on teste les moyens de mémoire (22, 165) en utilisant les bornes d'adressse de test (A1-Am) et les bornes de données de test (D1-Dn) ;
caractérisé par les étapes suivantes :
on enregistre dans une unité d'adresse fixée (169), formée sur la puce de semiconducteur (32), une adresse spécifiée qui n'est pas utilisée dans les moyens de mémoire (22, 165) ;
on applique l'adresse spécifique aux moyens de mémoire (22, 165) après l'achèvement du test de la carte à circuit intégré ;
on compare l'adresse qui est appliquée aux moyens de mémoire (22, 165) avec l'adresse spécifique qui est enregistrée dans l'unité d'adresse fixée (169) ; et
on déconnecte électriquement les bornes de données de test (D1-Dn) vis-à-vis du bus de données (24) des moyens de mémoire, à l'aide de moyens de transmission sélective à portes logiques (181), sous l'effet de la détection de l'adresse spécifique.

2. Un procédé selon la revendication 1, caractérisé par l'opération consistant à utiliser lesdits moyens de mémoire (22, 165) pour enregistrer des données secrètes, générer un signal de coïncidence et instaurer une section d'indicateur (183) sous l'effet de la détection du signal d'entrée de ladite adresse spécifique et du signal de sortie de ladite section d'indicateur (183) plaçant les moyens de transmission sélective (181) dans l'état de blocage lorsque la section d'indicateur est instaurée.

3. Un procédé selon la revendication 2, caractérisé par l'opération consistant à prévoir des moyens d'effacement de données (158, 168, 169) qui sont destinés à effacer les données secrètes enregistrées dans les moyens de mémoire (22, 165).

4. Un procédé selon la revendication 3, caractérisé par l'opération consistant à prévoir des moyens d'effacement de données (158, 168, 169) qui sont destinés à effacer les données secrètes enregistrées dans lesdits moyens de mémoire (22, 165), lorsque l'adresse d'entrée est trouvée identique à l'adresse inutilisée qui est enregistrée dans l'unité d'adresse fixée (169) et lorsque la section d'indicateur (183) est instaurée.