**PCT** WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

| (51) International Patent Classification 5 : | | (11) International Publication Number: | WO 94/10687 |
|---|---|---|---|
| G11C 16/06, 7/00, G06F 12/14 | A1 | (43) International Publication Date: | 11 May 1994 (11.05.94) |

(21) International Application Number: PCT/US93/10189

(22) International Filing Date: 25 October 1993 (25.10.93)

(30) Priority data:
07/965,635 23 October 1992 (23.10.92) US

(71) Applicant: VLSI TECHNOLOGY, INC. [US/US]; 1109 McKay Drive, San Jose, CA 95131 (US).

(72) Inventors: DOI, Bryan, C. ; 4414 MacBeth Circle, Fremont, CA 94555 (US). THOMAS, Steven, Dion ; 3209 Comestoga Canyon Road, Palm Dale, CA 93550 (US). COLI, Vincent, J. ; 971 Dana Avenue, San Jose, CA 95126 (US). DI GIGLIO, Vito ; 7255 Quartz Avenue, Canoga Park, CA 91306 (US).

(74) Agent: WELLER, Douglas, L.; 431 Magnolia Lane, Santa Clara, CA 95051 (US).

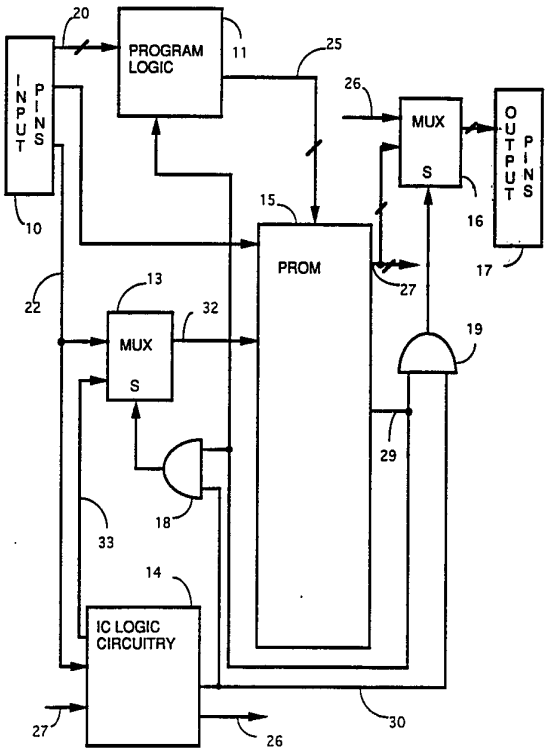
(81) Designated States: JP, KR, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

**Published**
*With international search report.*
*Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.*

(54) Title: VERIFIABLE SECURITY CIRCUITRY FOR PREVENTING UNAUTHORIZED ACCESS TO PROGRAMMED READ ONLY MEMORY

(57) Abstract

A security system is used for programmable read-only memory locations within a VLSI circuit. In a first security bit memory location there is stored a first security data bit. The first security data bit has a first value when the first security bit memory location is unprogrammed and a second value when the first security bit memory location is programmed. In a second security bit memory location there is stored a second security data bit. The second security data bit has the first value when the second security bit memory location is unprogrammed and the second value when the second security bit memory location is programmed. A selection means is electrically coupled to the first security bit memory location and the second security bit memory location. The selection means selects no security data bit, the first security data bit or the second security data bit to be used to generate a security access signal. An access means allows and prevents direct access, by any device outside the VLSI circuit, to the programmable read-only memory locations in response to the security access signal. The access means prevents any device outside the VLSI circuit direct access to the programmable read-only memory locations when the selection means selects no security data bit, when the selection means selects the first security bit and the first security data bit has the second value, or when the selection means selects the second security bit and the second security data bit has the second value.



*FOR THE PURPOSES OF INFORMATION ONLY*

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

| | | | | | |
|---|---|---|---|---|---|
| **AT** | Austria | **GB** | United Kingdom | **MR** | Mauritania |
| **AU** | Australia | **GE** | Georgia | **MW** | Malawi |
| **BB** | Barbados | **GN** | Guinea | **NE** | Niger |
| **BE** | Belgium | **GR** | Greece | **NL** | Netherlands |
| **BF** | Burkina Faso | **HU** | Hungary | **NO** | Norway |
| **BG** | Bulgaria | **IE** | Ireland | **NZ** | New Zealand |
| **BJ** | Benin | **IT** | Italy | **PL** | Poland |
| **BR** | Brazil | **JP** | Japan | **PT** | Portugal |
| **BY** | Belarus | **KE** | Kenya | **RO** | Romania |
| **CA** | Canada | **KG** | Kyrgystan | **RU** | Russian Federation |
| **CF** | Central African Republic | **KP** | Democratic People's Republic of Korea | **SD** | Sudan |
| **CG** | Congo | | | **SE** | Sweden |
| **CH** | Switzerland | **KR** | Republic of Korea | **SI** | Slovenia |
| **CI** | Côte d'Ivoire | **KZ** | Kazakhstan | **SK** | Slovakia |
| **CM** | Cameroon | **LI** | Liechtenstein | **SN** | Senegal |
| **CN** | China | **LK** | Sri Lanka | **TD** | Chad |
| **CS** | Czechoslovakia | **LU** | Luxembourg | **TG** | Togo |
| **CZ** | Czech Republic | **LV** | Latvia | **TJ** | Tajikistan |
| **DE** | Germany | **MC** | Monaco | **TT** | Trinidad and Tobago |
| **DK** | Denmark | **MD** | Republic of Moldova | **UA** | Ukraine |
| **ES** | Spain | **MG** | Madagascar | **US** | United States of America |
| **FI** | Finland | **ML** | Mali | **UZ** | Uzbekistan |
| **FR** | France | **MN** | Mongolia | **VN** | Viet Nam |
| **GA** | Gabon | | | | |

# VERIFIABLE SECURITY CIRCUITRY FOR PREVENTING UNAUTHORIZED ACCESS TO PROGRAMMED READ ONLY MEMORY

## Technical Field

The present invention is related to the field of programmable read-only memory (PROM) and particurlarly concerns the provision of a method and circuitry to protect a programmable read-only memory (PROM) or programmable logic array within an integrated circuit from unauthorized access.

## Background Art

Once a PROM or programmable array of logic within a VLSI circuit has been programmed and verified, it is often desirable to prevent further access by other than logic internal to the VLSI circuit. The restriction of access may be, for example, to prevent further programming of the PROM or to prevent examination of the contents of the PROM.

In the prior art, the burning of a security fuse has been used after programming a PAL to prevent further programming. However, the use of such a security fuse could cause difficulty when applied to a PROM within an integrated circuit. Particularly, in the prior art, there is no way for a manufacture to test the integrity of the security which implements the security fuse prior to use by a user. The inability to test the security logic would, if the security logic were utilized in a PROM, result in a manufacturer being required to develop a very reliable manufacturing process in order to guarantee the shipment of a high yield of working products.

## Disclosure of the Invention

In accordance with the preferred embodiment of the present invention, a security system for programmable read-only memory locations within a VLSI circuit is presented. In a first security bit memory location there is stored

a first security data bit. The first security data bit has a first value when the first security bit memory location is unprogrammed and a second value when the first security bit memory location is programmed. In a second security bit memory location there is stored a second security data bit. The second security data bit has the first value when the second security bit memory location is unprogrammed and the second value when the second security bit memory location is programmed. A selection means is electrically coupled to the first security bit memory location and the second security bit memory location. The selection means selects no security data bit, the first security data bit or the second security data bit to be used to generate a security access signal. An access means allows and prevents direct access, by any device outside the VLSI circuit, to the programmable read-only memory locations in response to the security access signal. The access means prevents any device outside the VLSI circuit direct access to the programmable read-only memory locations when the selection means selects no security data bit, when the selection means selects the first security bit and the first security data bit has the second value, or when the selection means selects the second security bit and the second security data bit has the second value.

In the preferred embodiment of the present invention, the VLSI circuit includes additional logic circuitry. Additionally, the selection means includes a first multiplexor which selects between data on address lines from the additional logic circuitry and data on input pins of the VLSI circuit to be connected to input address lines for the programmable read only memory locations. The selection means additionally includes a second multiplexor which selects between data lines for the additional logic circuitry and output pins of the VLSI circuit to receive data from the programmable read only memory locations.

Also in the preferred embodiment of the present invention, the additional logic circuitry generates a test bit. Additionally, the access means does not allow any device outside the VLSI circuit direct access to the programmable read-only memory locations when the test bit has the second value.

In one embodiment of the security system, the programmable read-only memory locations are arranged in a memory array within a PROM. The PROM additionally includes an address decoder, a test row, a test column, the first security bit memory location and the second security bit memory location. Also, the VLSI circuit may additionally include program logic which provides a programming voltage to the programmable read-only memory locations. The program logic includes an enable/disable means for preventing programming when the selection means selects no security data bit, when the selection means selects the first security bit and the first security data bit has the second value, or when the selection means selects the second security bit and the second security data bit has the second value.

The security system has the advantage of being testable. For example, once the test memory locations have been programmed, the first security memory bit may be programmed. Once the first security memory bit is programmed, the first security memory bit is selected and it is verified that no device outside the VLSI circuit can access the programmable read-only memory locations. The end user then can program and protect the programmable read-only memory locations by first selecting the second security memory bit. Then, the programmable read-only memory locations may be programmed. Afterwards, the second security memory bit is programmed, thereby preventing subsequent unauthorized access to the programmable read-only memory locations.

## Brief Description of the Drawings

Figure 1 shows implementation of security logic in an integrated circuit, in accordance with the preferred embodiment of the present invention.

Figure 2 shows the arrangement of a testable programmable read only memory in accordance with the preferred embodiment of the present invention.

Figure 3 is a flowchart which describes a process for testing the security feature of a VLSI circuit in accordance with a preferred embodiment of the present invention.

Figure 4 is a flowchart which describes a process which a customer follows to program and test a part in accordance with a preferred embodiment of the present invention.

## Description of the Preferred Embodiment

Figure 1 shows a block diagram of circuitry which implements security for a programmable read only memory (PROM) 15 which is within a VLSI circuit. Integrated circuit (IC) logic circuitry 14 within the VLSI circuit controls operation of the VLSI circuit. Under normal operating conditions, when PROM 15 is accessed, a multiplexor 13 selects an address on lines 33 to be forwarded to PROM 15 on address lines 32. In response, IC logic circuitry 14 receives data from PROM 15 through PROM output lines 27.

Also, under normal operating conditions, IC logic circuitry 14 controls the interface of the VLSI circuit to other devices. IC logic circuitry 14 receives data through input pins 10 via lines 22. A multiplexor 16 selects data on logic output lines 26 to be connected to output pins 17.

When PROM 15 is programmed and verified, multiplexor 13 selects an address on lines 22 from input pins 10 to be forwarded to PROM 15 on address lines 32. Multiplexor 16 selects data on PROM output lines 27 to be connected

to output pins 17. In response to values placed on input pins 10 and forwarded to program logic 11 through lines 20, program logic 11 provides programming voltages to PROM 15 through lines 25.

A selection input to multiplexor 13 and a selection input to multiplexor 16 are controlled respectively by a logical AND gate 18 and a logical AND gate 19. Alternately, as will be understood by persons of ordinary skill in the art, the function of logical AND gate 18 and logical AND gate 19 may be accomplished by a single logical AND gate. Logical AND gate 18 and logical AND gate 19 each performs a logical AND operation on a test/program bit and a security bit. The test/program bit is generated by IC logic circuitry 14 and placed on a line 30. The security bit is supplied by PROM 15 and placed on a line 29. Program logic 11 also receives the security bit on line 29 which serves to enable/disable program logic 11.

In the circuitry shown in Figure 1, when both the test/program bit and the security bit are at logic 1, multiplexor 13 selects an address on lines 22 to be connected to address lines 32 and multiplexor 16 selects data on PROM output lines 27 to be connected to output pins 17. Therefore, memory locations within PROM 15 may be programmed and accessed by devices outside the VLSI circuit. When either the test/program bit or the security bit is at logic 0, multiplexor 13 selects the address on lines 33 to be connected to address lines 32 and multiplexor 16 selects the data on logic output lines 26 to be connected to output pins 17. Therefore, memory locations within PROM 15 cannot be programmed or accessed by devices outside the VLSI circuit.

As may be understood by a person of ordinary skill in the art, while the logic shown assumes the security bit and the test/program bit are active high, the logic shown may be easily modified to accommodate the situation where the security bit and/or the test/program bit are active low.

In the preferred embodiment of the present invention, two locations within PROM 15 are able to provide the security bit on line 29. Security bit address lines 21 are used to access the first security bit, the second security bit or no security bit.

Figure 2 shows a simplified block diagram of PROM 15. Memory array 50 contains, for example, 64 rows of 8 one-bit memory locations. An address decoder 53 receives an address on address lines 32 and generates a row select activating a selected row. In normal operation, data values stored by the selected row appear on data lines 40, 41, 42, 43, 44, 45, 46 and 47. This data is then forwarded to PROM output lines 27. When memory location in memory array 50 are being programmed, address decoder 53 receives an address on address lines 32 and generates a row select activating a selected row. A programming voltage through lines 25 is placed on various of programming lines 60, 61, 62, 63, 64, 65, 66 and 67. A programming voltage on one of the programming lines results in the corresponding memory cell in the selected row being programmed. In one embodiment of the present invention, unprogrammed memory cells store a data value of logic 1 and programmed memory cells store a data value of logic 0. In an alternate embodiment of the present invention, unprogrammed memory cells store a data value of logic 0 and programmed memory cells store a data value of logic 1.

In order to aid in the factory test of the VLSI circuit, PROM 15 may include a test row 52 and a test column 51. In a test mode, the integrity of programming lines 60, 61, 62, 63, 64, 65, 66 and 67 and data lines 40, 41, 42, 43, 44, 45, 46 and 47 may be checked by programming and verifying values in test row 52. Likewise, the operation of address decoder 53 may be checked by programming and verifying values in test column 51. Test column 51 is

programmed using a programming line 68. For more complete testing, an additional test row may be placed below memory array 50.

In the preferred embodiment of the present invention, two memory cells within PROM 15 are used to store security bits. One or none of the security bit locations are selected by a security bit decoder 70, based on a value on security bit address lines 21. When a first memory location is selected, security bit decoder activates a security bit selection line 23. When a second memory location is selected, security bit decoder activates a security bit selection line 24. The value in the selected memory location appears on line 29. The selected memory bit location may also be programmed using a programming line 69. In the disclosed embodiment of the present invention, when unprogrammed, each security bit memory cell stores a data value of logic 1. When programmed, each security bit memory cell stores a data value of logic 0. In an alternate embodiment of the present invention, when unprogrammed, each security bit memory cell stores a data value of logic 0. When programmed, each security bit memory cell stores a data value of logic 1. The actual position of the security bit memory location within PROM 15 should be concealed as well as possible to prevent defeat of the security feature by an unauthorized person.

The use of two separate memory locations for the security bit allows for the manufacturer to test the security features of the VLSI circuit. For example, Figure 3 is a flowchart which describes a process for testing the security feature of a VLSI circuit by a device external to the VLSI circuit in accordance with a preferred embodiment of the present invention. During testing, IC logic circuitry 14 sets the test/program bit on line 30 to logic 1.

In a step 80, no security bit is selected by the address on security bit address lines 21. In a step 81, an attempt is made to access and program memory locations within memory array 50. In a step 82, the first security bit is

selected and program memory locations are checked to see if any were programmed or accessed in step 81.

A step 83 is a branching step. If any memory locations were successfully programmed, in a step 89 the VLSI circuit is rejected. Otherwise, in a step 84, the first security bit location is selected by the address on security bit address lines 21. In a step 85, an attempt is made to access and program memory locations within the test row(s) and/or test column(s). In a step 86, the programmed memory locations are checked to see if they were successfully programmed in step 85.

A step 87 is a branching step. If any memory locations were not successfully programmed, in step 89 the VLSI circuit is rejected. Otherwise, in a step 88, the first security bit is programmed. In a step 90, the first security bit location is selected by the address on security bit address lines 21. In a step 91, an attempt is made to access and program memory locations within memory array 50. In a step 92, the second security bit is selected and program memory locations are checked to see if any were programmed or accessed in step 91.

A step 93 is a branching step. If any memory locations were successfully programmed, in step 89 the VLSI circuit is rejected. Otherwise, in a step 94, the second security bit location is selected by the address on security bit address lines 21. In a step 95, an attempt is made to access and program memory locations within memory array 50. In a step 96, program memory locations are checked to see if any were programmed or accessed in step 95.

A step 97 is a branching step. If any memory locations were not successfully programmed, in step 89 the VLSI circuit is rejected. Otherwise, in a step 98, after all other testing is complete, the VLSI circuit may be shipped to the customer.

Figure 4 describes a process by which a customer programs and tests the shipped part. In a step 101, the customer selects the second security bit. In a

step 102, the customer programs memory locations within memory array 50. In a step 103, the customer verifies the programmed data.

A step 104 is a branching step. If any memory locations were not successfully programmed, in a step 110, the VLSI circuit is rejected. Otherwise, in a step 105, the second security bit is programmed. In a step 106, the second security bit is selected. In a step 107, an attempt is made to access memory locations within memory array 50.

A step 108 is a branching step. If any memory locations were successfully accessed, in step 110, the VLSI circuit is rejected. Otherwise, in a step 109, the VLSI circuit is ready for further testing or to be utilized in a computing system.

The foregoing discussion discloses and describes merely exemplary methods and embodiments of the present invention. As will be understood by those familiar with the art, the invention may be embodied in other specific forms without departing from the spirit or essential characteristics thereof. Accordingly, the disclosure of the present invention is intended to be illustrative, but not limiting, of the scope of the invention, which is set forth in the following claims.

## Claims

We Claim:

1. A security system for programmable read-only memory locations within a VLSI circuit, the security system comprising:

a first security bit memory location in which is stored a first security data bit, the first security data bit having a first value when the first security bit memory location is unprogrammed and the first security data bit having a second value when the first security bit memory location is programmed;

a second security bit memory location in which is stored a second security data bit, the second security data bit having the first value when the second security bit memory location is unprogrammed and the second security data bit having the second value when the second security bit memory location is programmed;

selection means, electrically coupled to the first security bit memory location and the second security bit memory location, for selecting no security data bit, the first security data bit or the second security data bit to be used to generate a security access signal; and,

access means for allowing and preventing direct access, by any device outside the VLSI circuit, to the programmable read-only memory locations in response to the security access signal;

wherein the access means prevents any device outside the VLSI circuit direct access to the programmable read-only memory locations when the selection means selects no security data bit, when the selection means selects the first security bit and the first security data bit has the second value, or when the selection means selects the second security bit and the second security data bit has the second value.

2. A security system as in claim 1

wherein the VLSI circuit includes additional logic circuitry; and,

wherein the selection means includes

a first multiplexor which selects between data on address lines from the additional logic circuitry and data on input pins of the VLSI circuit to be connected to input address lines for the programmable read only memory locations, and

a second multiplexor which selects between data lines for the additional logic circuitry and output pins of the VLSI circuit to receive data from the programmable read only memory locations.

3. A security system as in claim 2 wherein the additional logic circuitry generates a test bit and wherein the access means does not allow any device outside the VLSI circuit direct access to the programmable read-only memory locations when the test bit has the second value.

4. A security system as in claim 1 wherein the programmable read-only memory locations are arranged in a memory array within a PROM, the PROM additionally including an address decoder, a test row, a test column, the first security bit memory location and the second security bit memory location.

5. A security system as in claim 1 wherein the VLSI circuit additionally includes program logic for providing a programming voltage to the programmable read-only memory locations, the program logic including enable/disable means for preventing programming when the selection means selects no security data bit, when the selection means selects the first security bit and the first security data bit has the second value, or when the selection means selects the second security bit and the second security data bit has the second value.

6. A method for providing security for programmable read-only memory locations within a VLSI circuit, the method comprising the steps of:

(a) providing a testable security system which prevents a device outside the VLSI circuit from accessing the programmable read-only memory locations except when a first security bit is selected and unprogrammed or when a second security bit is selected and unprogrammed;

(b) programming test memory locations;

(c) programming the first security memory bit; and,

(d) selecting the first security memory bit and verifying that no device outside the VLSI circuit can access the programmable read-only memory locations.

7. A method as in claim 6 additionally comprising the steps of:

(e) selecting the second security memory bit;

(f) programming the programmable read-only memory locations; and,

(g) programming the second security memory bit.

8. A method for providing security for programmable read-only memory locations within a VLSI circuit, the method comprising the steps of:

(a) providing a first security bit memory location in which is stored a first security data bit, the first security data bit having a first value when the first security bit memory location is unprogrammed and the first security data bit having a second value when the first security bit memory location is programmed;

(b) providing a second security bit memory location in which is stored a second security data bit, the second security data bit having the first value when the second security bit memory location is unprogrammed and the

second security data bit having the second value when the second security bit memory location is programmed; and,

(c) allowing and preventing direct access, by any device outside the VLSI circuit, to the programmable read-only memory locations including the substep of:

(c.1) preventing any device outside the VLSI circuit from directly accessing the programmable read-only memory locations when a selection means selects no security data bit, when the selection means selects the first security bit and the first security data bit has the second value, or when the selection means selects the second security bit and the second security data bit has the second value.

9. A method as in claim 8 wherein step (c) additionally comprises the substep of:

(c.2) preventing any device outside the VLSI circuit from directly accessing the programmable read-only memory locations when a test bit has the second value.

10. A method as in claim 8 additionally comprising the step of:

(d) preventing a programming voltage from being provided to the programmable read-only memory locations when the selection means selects no security data bit, when the selection means selects the first security bit and the first security data bit has the second value, or when the selection means selects the second security bit and the second security data bit has the second value.

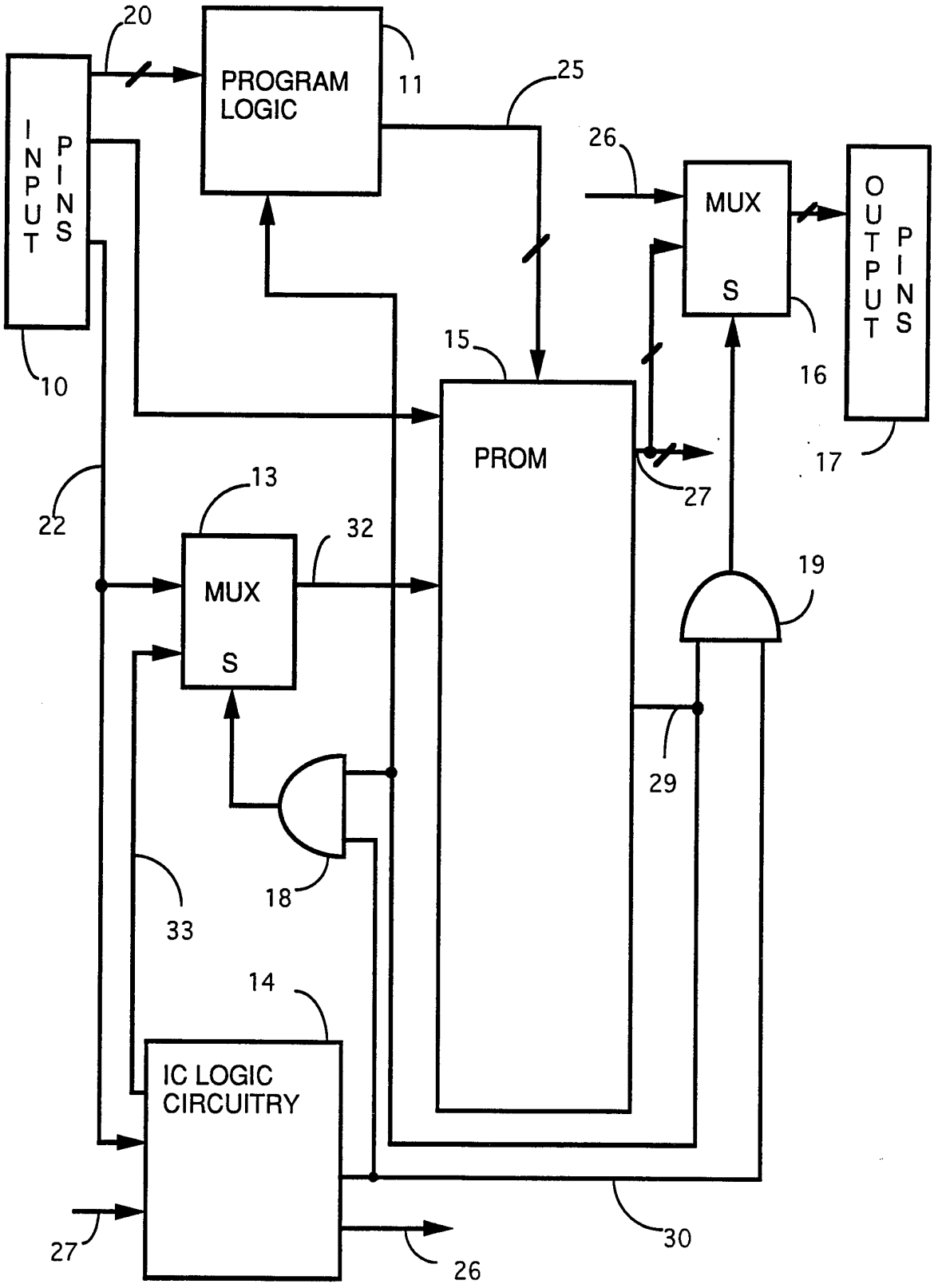

20
PROGRAM LOGIC
11
25
INPUT PINS
26
MUX
S
OUTPUT PINS
10
15
16
PROM
17
27
22
13
32
MUX
S
19
29
18
33
14
IC LOGIC CIRCUITRY
27
26
30

FIGURE 1

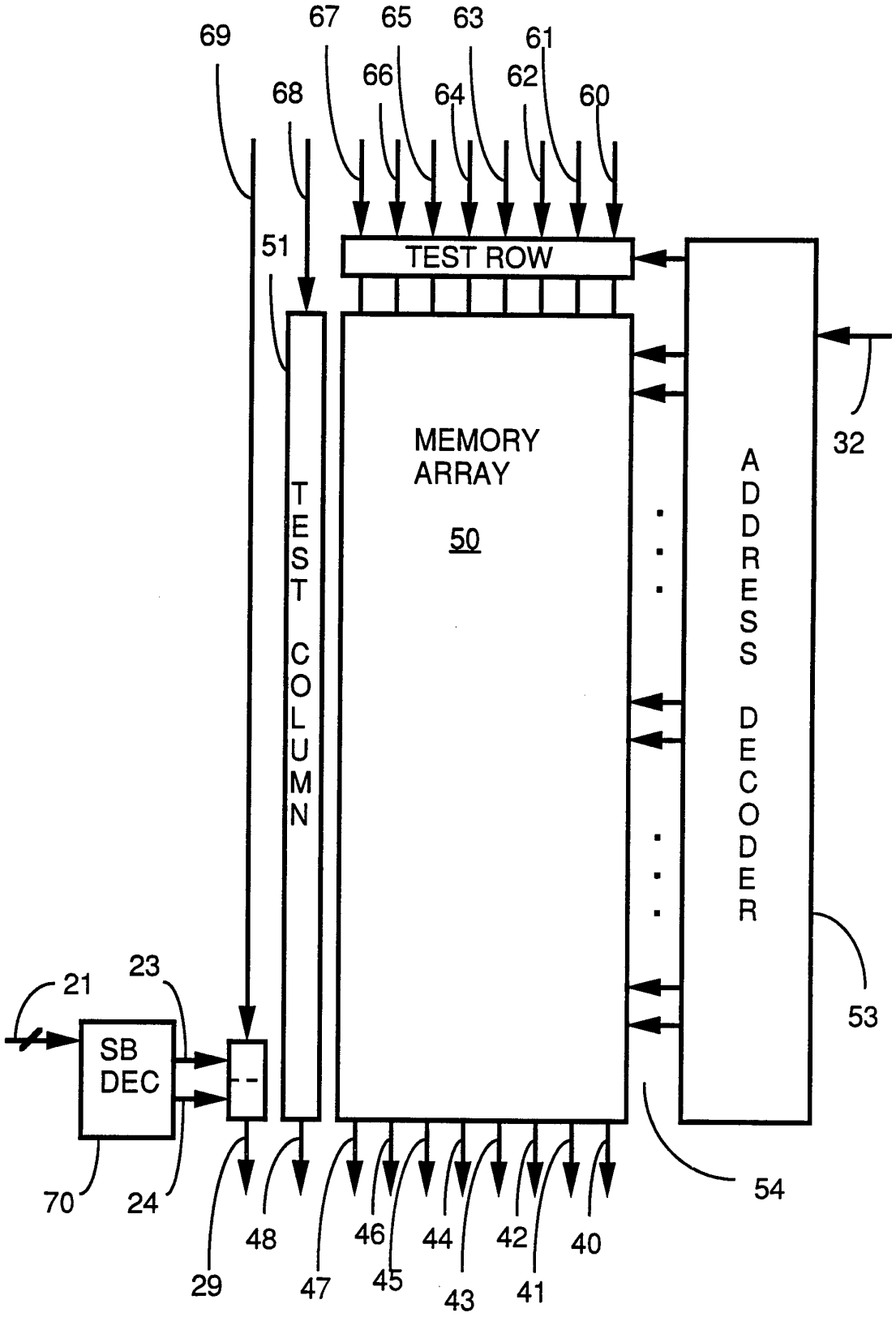

69
67
65
63
61
66
62
68
64
60
51
TEST ROW
32
MEMORY
ARRAY
50
TEST COLUMN
ADDRESS DECODER
53
21
23
SB
DEC
70
24
48
46
44
42
40
54
29
47
45
43
41

FIGURE 2

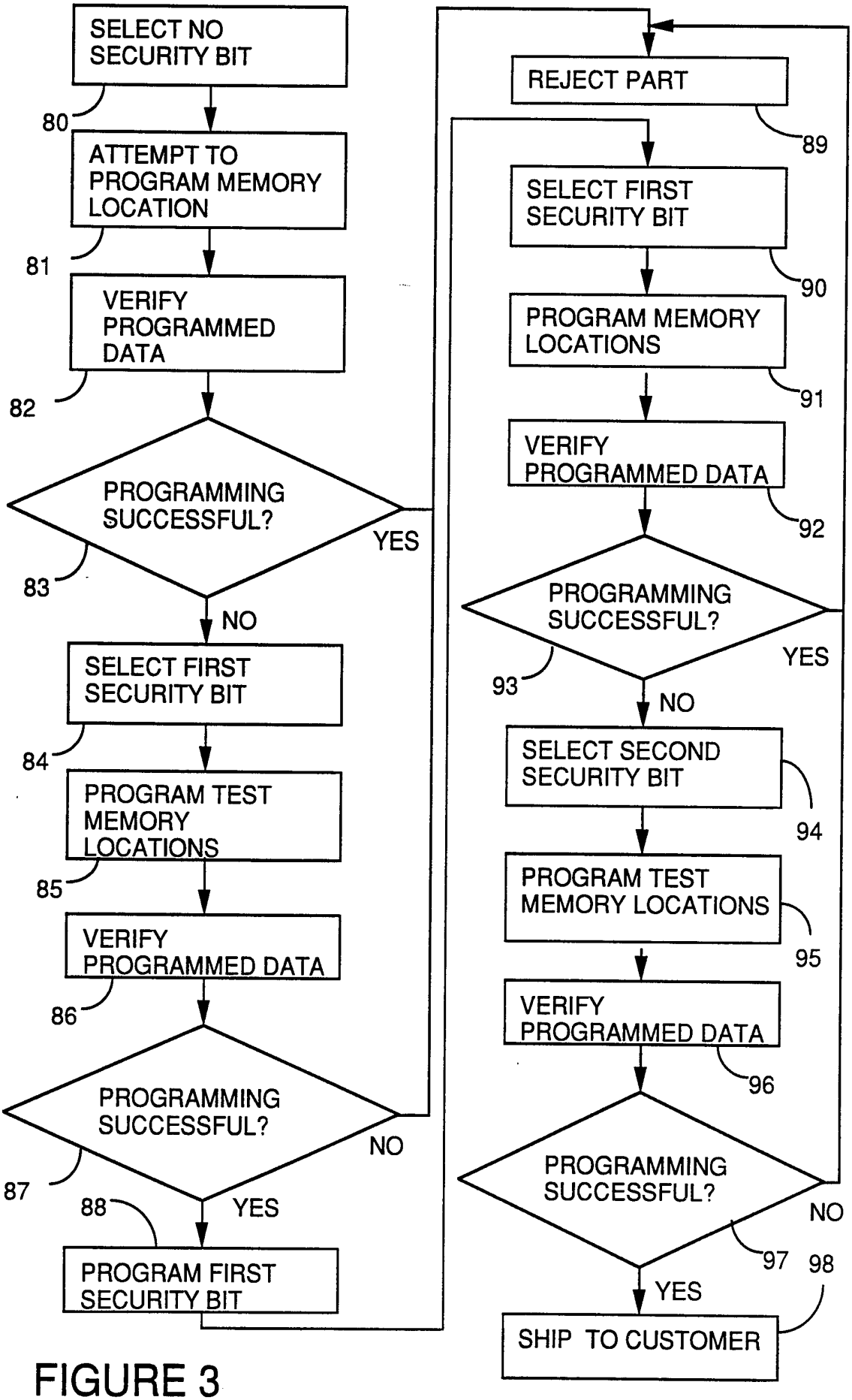

SELECT NO SECURITY BIT
80
ATTEMPT TO PROGRAM MEMORY LOCATION
81
VERIFY PROGRAMMED DATA
82
PROGRAMMING SUCCESSFUL?
83
YES
NO
SELECT FIRST SECURITY BIT
84
PROGRAM TEST MEMORY LOCATIONS
85
VERIFY PROGRAMMED DATA
86
PROGRAMMING SUCCESSFUL?
87
NO
YES
88
PROGRAM FIRST SECURITY BIT
REJECT PART
89
SELECT FIRST SECURITY BIT
90
PROGRAM MEMORY LOCATIONS
91
VERIFY PROGRAMMED DATA
92
PROGRAMMING SUCCESSFUL?
93
YES
NO
SELECT SECOND SECURITY BIT
94
PROGRAM TEST MEMORY LOCATIONS
95
VERIFY PROGRAMMED DATA
96
PROGRAMMING SUCCESSFUL?
97
NO
YES
98
SHIP TO CUSTOMER

FIGURE 3

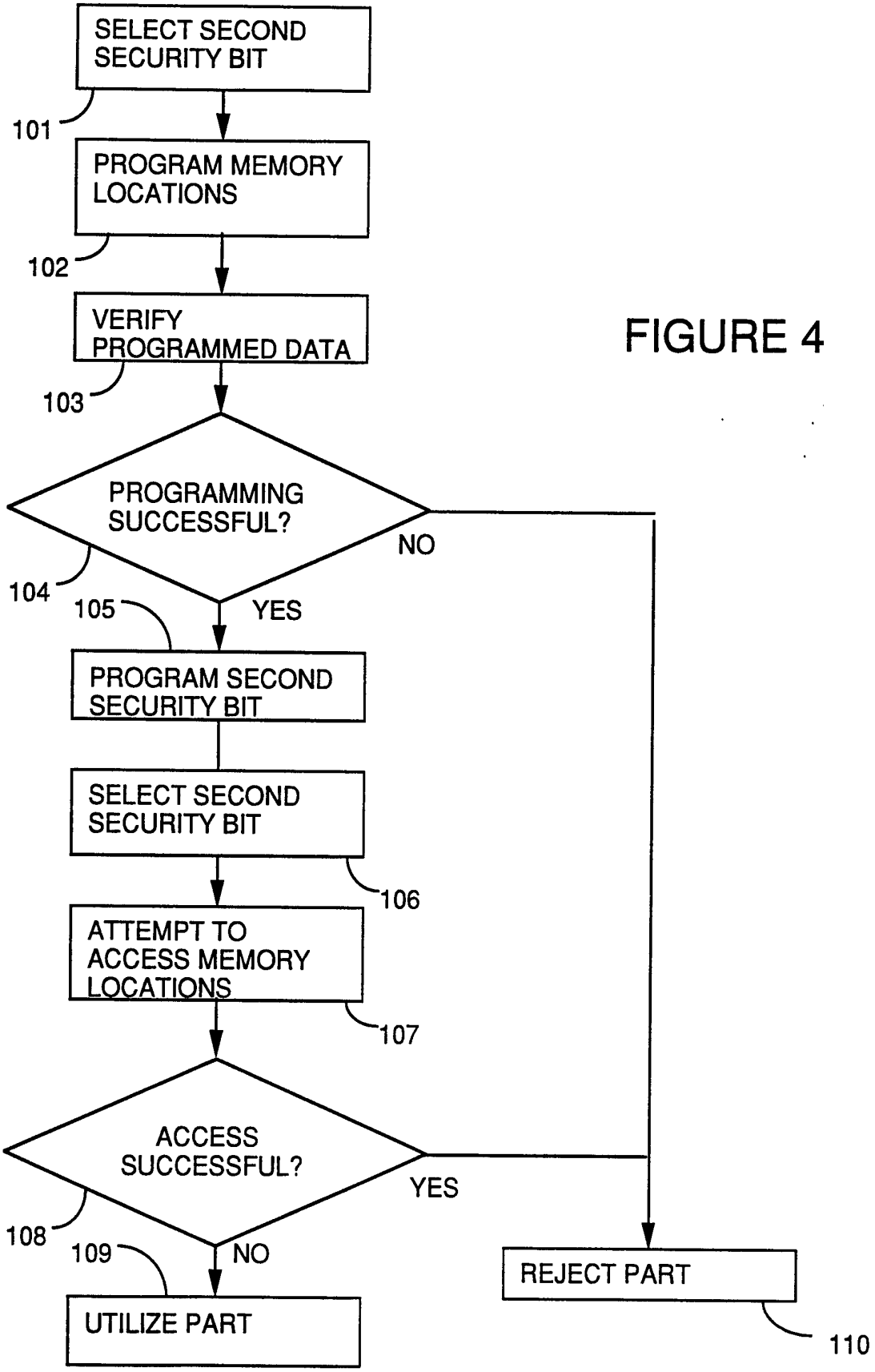

SELECT SECOND SECURITY BIT
101
PROGRAM MEMORY LOCATIONS
102
VERIFY PROGRAMMED DATA
103
PROGRAMMING SUCCESSFUL?
NO
104
YES
105
PROGRAM SECOND SECURITY BIT
SELECT SECOND SECURITY BIT
106
ATTEMPT TO ACCESS MEMORY LOCATIONS
107
ACCESS SUCCESSFUL?
YES
108
NO
109
UTILIZE PART
REJECT PART
110

FIGURE 4

# INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 93/10189

A. CLASSIFICATION OF SUBJECT MATTER
IPC 5 G11C16/06 G11C7/00 G06F12/14

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 5 G11C G06F

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

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category * | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| Y | EP,A,0 378 306 (GENERAL INSTRUMENT CORP.) 18 July 1990<br>see column 4, line 25 - line 46<br>see column 10, line 41 - column 13, line 55<br>see figures 1,9,10<br>--- | 1-10 |
| Y | ELECTRONIQUE RADIO PLANS<br>no. 527 , October 1991 , PARIS FR<br>pages 69 - 74<br>D.PARET 'Microcontroleurs et Protection de Code'<br>see figure 7<br>see page 73, centre column, line 1 - line 25<br>--- | 1-10 |
| Y | EP,A,0 231 041 (PHILIPS) 5 August 1987<br>see abstract; figure 1<br>---<br>-/-- | 4 |

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 16 February 1994 | - 9. 03. 94 |

| Name and mailing address of the ISA | Authorized officer |
|---|---|
| European Patent Office, P.B. 5818 Patentlaan 2<br>NL - 2280 HV Rijswijk<br>Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,<br>Fax: (+31-70) 340-3016 | Powell, D |

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

# INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 93/10189

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

| Category * | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| A | PROC. 10TH. ANNUAL INTL. CONF. ON COMPUTER ARCHITECTURE, 1983 , STOCKHOLM, SE; pages 334 - 339 L.PHILIPSON ET AL 'A Communication Structure for a Multiprocessor Computer with Distributed Global Memory' see figures 1,3 see page 335, left column, line 7 - right column, line 5 ----- | 2,3 |

1

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/US 93/10189

| Patent document cited in search report | Publication date | Patent family member(s) | | Publication date |
|---|---|---|---|---|
| EP-A-0378306 | 18-07-90 | US-A- | 4933898 | 12-06-90 |
| | | AU-B- | 617026 | 14-11-91 |
| | | AU-A- | 4766990 | 19-07-90 |
| | | CA-A- | 2007469 | 12-07-90 |
| | | JP-A- | 2232960 | 14-09-90 |
| EP-A-0231041 | 05-08-87 | NL-A- | 8600099 | 17-08-87 |
| | | DE-A- | 3772062 | 19-09-91 |
| | | JP-A- | 62172600 | 29-07-87 |
| | | US-A- | 4862418 | 29-08-89 |