PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 5 : G06F 12/00, 12/06, 12/14

A1

(11) International Publication Number: WO 94/11823

(43) International Publication Date: 26 May 1994 (26.05.94)

(21) International Application Number: PCT/US93/10775

(22) International Filing Date: 9 November 1993 (09.11.93)

(30) Priority data:
07/974,929 12 November 1992 (12.11.92) US

(71) Applicant: SILICON STORAGE TECHNOLOGY, INC. [US/US]; 1208 Apollo Way, Suite 502, Sunnyvale, CA 94086 (US).

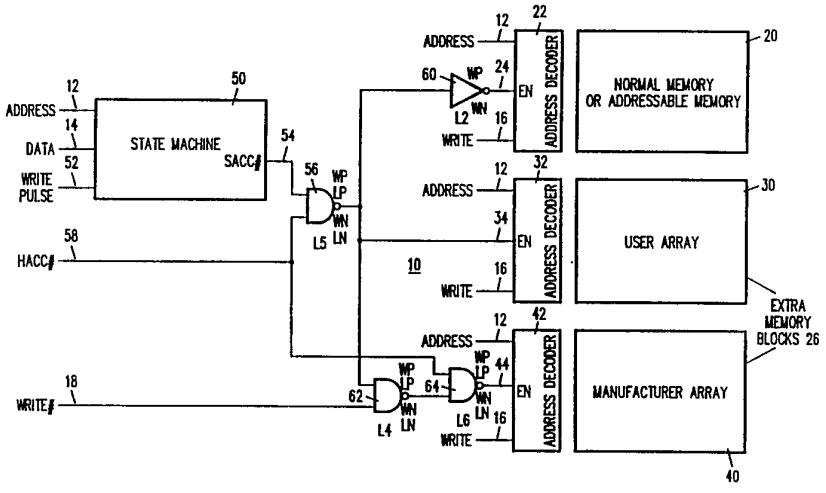
(72) Inventors: WANG, Ping ; 19932 Merribrook Drive, Saratoga, CA 95070 (US). JENQ, Ching-Shi ; 2753 Glauser Drive, San Jose, CA 95133 (US).

(74) Agents: YIN, Ronald, L. et al.; Limbach & Limbach, 2001 Ferry Building, San Francisco, CA 94111 (US).

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

Published
With international search report.

(54) Title: MEMORY STORAGE DEVICE HAVING *IN SITU* COPY PROTECTION AND DATA SECURITY CAPABILITY



ORGANIZATION OF MEMORY

(57) Abstract

A memory card (10) uses two sections of electrically alterable memory cells, such as EEPROM cells. The first section (20) receives an address signal (12), a write signal (16) and a first enable signal (24) for enabling or disabling the first section (2). The second section (26) of the memory card (10) receives the address signal (12), the write signal (16) and a second enable signal (34) for enabling or disabling the second section (26). Logic means (50) generate simultaneously the first enable signal (24) to enable the first signal to read or write data signals therefrom and generates the second enable signal (34) which disables the second section (26). In a second mode of operation, the logic means (50) simultaneously generates a first enable signal (24) to disable the first section (20) and generates a second enable signal (34) which permits the memory in the second section (26) to be read. Finally, in the third mode of operation, the logic means (50) generates the first enable signal (24) to disable the first section (20) and simultaneously generates the second enable signal (34) which permits the memory in the second section (26) to be written into.

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				

MEMORY STORAGE DEVICE HAVING *IN SITU* COPY PROTECTION AND DATA SECURITY CAPABILITY

Technical Field

The present invention relates to a memory storage device and more particularly to a memory storage device comprised of semiconductor integrated memory circuits such as EEPROM and flash EPROM/EEPROM memory circuits. Furthermore, the present invention relates to a memory storage device having *in situ* copy protection and data security features.

Background of the Invention

Electrically alterable non-volatile memory made of integrated circuit devices on a semiconductor substrate is well-known in the art. As the scale of integration increases, i.e. the density of the memory cells in the memory storage device increases per unit area, it becomes commercially possible to manufacture a so-called "memory card" containing megabytes (with each byte equal to 8 bits of data) of storage. Such a memory card in many applications can be used in lieu of a magnetic storage media such as a floppy or a hard disk.

Similar to the magnetic media, the memory card is also designed to be the medium for the distribution of software programs. Thus, software programs can be distributed in memory cards.

Also similar to the magnetic media where copy protection for software programs distributed thereon has become a problem, the copy protection for the software programs distributed in a memory card would also pose a copyright protection problem.

In U.S. Patent No. 4,419,747, a method and an apparatus is disclosed wherein an auxiliary memory array is provided in addition to a primary circuit. The auxiliary memory provides for the storage of processing and test information relating to the manufacture of the integrated circuit device. However, the auxiliary memory is accessed (read and write) only by a high voltage signal.

Summary of the Invention

In the present invention a memory storage device is disclosed. The memory storage device has *in situ* copyright protection and data security feature. The memory storage device has an address port which receives an address signal, a data port which receives an input data signal or provides an output data signal, and a write enable port for receiving a write signal. The storage device comprises an electrically alterable memory storage means for storing information. The storage means has a first section and a second section. The first section of the storage means receives the address signal, the write signal, and has an enable port which receives a first enable signal for enabling or disabling the first section. Similarly, the second section of the storage means receives the address signal and the write signal, and has an enable port which receives a second enable signal for enabling or disabling the second section. Logic means generates simultaneously the first enable signal for enabling the first section to receive the input data signal or for providing an output data signal therefrom and generates the second enable signal to disable the second section. The logic means also comprises means for simultaneously generating the first enable signal

for disabling the first section and generating the second enable signal for enabling the second section to provide an output data signal therefrom in one state. Finally, the logic means in another state has means for simultaneously generating the first enable signal to disable the first section and generates the second enable signal for enabling the second section to receive the input data signal.

Brief Description of the Drawings

Figure 1 is a schematic block level diagram of the storage device 10 of the present invention.

Figure 2 is a schematic logic diagram of one embodiment of a high voltage level detector used in the storage device 10 of the present invention.

Figure 3 is one embodiment of the state machine shown in Figure 1.

Detailed Description of the Drawings

Referring to Figure 1 there is shown a schematic drawing of the memory storage device 10 of the present invention. The memory storage device 10 has an address port for receiving an address signal 12. The device 10 also has a data port for receiving an input data signal 14 or for providing an output data signal 14. As is well known, each of the address signal 12 and data signal 14 is supplied on a plurality of conductors. The device 10 also has a write enable port for receiving a write signal 16. An inverse write signal 18, designated as "write#" is also provided.

The device 10 has a first section 20 of electrically alterable memory for storing information. The first section 20 comprises a first array 20 of memory cells of the type shown and

described in U.S Patent Application No. 07/467,907 filed on January 22, 1990, which is incorporated herein by reference. The first array 20 is also designated as the normal memory array 20. The first array 20 has an address decoder 22 to which the address signal 12 is supplied. The address decoder 22 also has an enable port which receives a first enable signal 24. The first enable signal 24 enables or disables the first section 20 of memory. The write signal 16 is also supplied to the address decoder 22 of the first array 20 of memory.

The device 10 also comprises a second section 26 of electrically alterable memory storage cells. The second section 26 is divided into two arrays of memory cells: second array 30 and third array 40. The second array 30, designated as a user array, has an associated address decoder 32. The address decoder 32 receives the address signal 12 and the write signal 16. In addition, the second array 30 has an enable port which receives a second enable signal 34 for enabling or disabling the second array 30.

The third array 40, designated as the manufacturer array, also has an address decoder 42 associated therewith. The address decoder 42 receives the address signal 12 and the write signal 16. In addition, the address decoder 42 has an enable port which receives a third enable signal 44 which enables or disables the third array 40.

A state machine 50 receives the address signal 12, the data signal 14 and the write pulse signal 52. In response thereto, the state machine 50 generates an output signal SACC# 54. The SACC# 54 is supplied to a NAND gate 56, to which an HACC# signal 58 is also supplied. The HACC# signal 58 is generated by a

high voltage detector for detecting high voltage being supplied to specific pins of the device 10 of the present invention. The output of the NAND gate 56 is then inverted by the inverter 60 and is the first enable signal 24.

The output of the NAND gate 56 is also supplied the second enable signal 34. The output of the NAND gate 56 is also supplied to a second NAND gate 62 to which the WRITE# signal 18 is also supplied. The output of the NAND gate 62 is supplied to a third NAND gate 64 to which the HACC# signal 58 is also supplied. The output of the NAND gate 64 is the third enable signal 44.

Referring to Figure 2 there is shown one embodiment of a high voltage detection circuit 70. The high voltage detection circuit may comprise of a string of four inverters 72, 74, 76 and 78. The first inverter 72 has a suitable threshold for detection of the high voltage signal involved. The signal is then inverted by the second inverter 74, a third and fourth inverters to reach conventional CMOS signal levels. In this manner, the high voltage supplied to the device 10 can be detected and the signal HACC# 58 can be generated.

Referring to Figure 3 there is shown one embodiment of the state machine 50. The state machine 50 serves to detect a combination of the address signal 12, data signal 14 and the write pulse signal 52 to generate the SACC# signal 54. As will be seen, the specific embodiment of the state machine 50 is purely arbitrary. The manner in which the SACC# signal 54 is generated is dictated entirely by the manufacturer of the device 10. It can range from a simple circuit of the type shown in Figure 3 wherein a certain logic combination of the address

signal 12 and data signal 14 sets a flip-flop or register 80 and another certain combination of the address signals 12 and data signals 14 resets the flip-flop 80.

The operation of the device 10 will now be described with reference to a specific example wherein the first array of normal memory 20 comprises one megabytes of storage. Thus, the address signals 12 comprises 20 signal lines. The address signal 12 ranges from "00000" to "FFFFF", where the numbers are expressed in hexadecimal units.

The user array 30 comprises memory cells addressable in the location from "10000" to "30000". The manufacture array 40 comprises memory cells addressable in the location from "00000" to "0FFFF". Thus, no portion of the address of the memory cell in the user array 30 overlaps with the address of the manufacturer array 40, and vice versa. However, as can be seen, collectively, the address space of the memory cells in the second section 26, i.e. the user array 30 and the manufacturer array 40, overlap that of the normal memory array 20.

The device 10 of the present invention is particularly suited to be used as a "memory card". Thus, since the memory cells of the device 10 of the present invention comprise electrically alterable memory cells, the first array 20 of memory cells can be used to store computer programs, such as word processing and spread sheet programs, and distributed on memory card form. The user array 30 is a section in the device 10 which the user can have access to with the storage of his/her data. The manufacturer array 40 is an area of the device 10 containing information such as the production history of the memory cells of the device 10. In addition, and more

importantly, the manufacturer array 40 can be used by the publisher of the computer program that is stored in the first array 20 to provide a key or a copy protect algorithm to thwart the copying of the program that is stored in the first array 20. The specific manner of accomplishing that function will now be explained.

The signals SACC# 54, HACC# 58, and WRITE# 18 are all active low signals. That is, these signals represent a logic "1" state when they are low in voltage and a logic "0" state when they are high in voltage. The first enable signal 24, second enable signal 34, and third enable signal 44 are all active high signals. Thus, a logic table for the various signals is set forth on the attached.

SACC#	HACC#	WRITE#	NORMAL ENABLE	USER ENABLE	MFGR ENABLE
1	1	0	1	0	0
1	0	0	0	1	1
0	1	0	0	1	0
0	0	0	0	1	1
1	1	1	1	0	0
1	0	1	0	1	1
0	1	1	0	1	1
0	0	1	0	1	1

From the foregoing, it can be seen that the first array 20 of normal memory is activated to read or write therefrom when both SACC# 54 and HACC# 58 signals are high. Thus, if no high voltage level is detected and HACC# signal 58 is high and the state machine 50 is not brought to a state where SACC# signal 54 is generated, then the address signals 12 would activate an address in the normal memory array 20. The write signal 16 would cause memory array 20 to be written into or read from and provide the

appropriate signals on the data signal 14. When the first enable signal 24 is generated enabling the first array 20, the second enable signal 34 and the third enable signal 44 serve to disable the second and third memory arrays 30 and 40 respectively.

When either SACC# signal 54 is activated or the HACC# signal 58 is activated and the WRITE# signal 18 is high indicating it is a read state, then both the second enable signal 34 and third enable signal 44 are generated to activate the second array 30 and the third array 40 respectively. In that state, the first enable signal 24 is generated to disable the reading or writing of data from the first array 20. Thus, although there is overlapping of address between the first array 20 and the second and third arrays 30 and 40, respectively, the generation of the enable signals serve to differentiate between the different arrays of the memory. In addition, if SACC# signal 54 is generated and WRITE# signal 18 is active low, then the second memory array 30 can be written into. Thus, in the second state of operation, one could read from the second and third arrays 30 and 40, and one could also write into the second array 30.

Finally, in the last state of operation, in the event HACC# signal 58 is active, and the WRITE# signal 18 is active, then one could write into the third memory array 40.

In the event the device 10 of the present invention is used to store computer program in the first array 20 and the device 10 is used to distribute the computer program, then the thwarting of copying occurs as follows. The manufacturer of the software program would store a key program or data in the third array 40, during the process of

manufacturing the card. There are three potential cases with respect to the copying of data.

The first case is where the copying is from the software manufacturer supplied card 10 (the card 10 of the present invention: hereinafter: "original card") to a copied card (hereinafter: "copied card"), which is identical to the card 10 of the present invention. In that event, during copying, the copied card 10 prohibits the writing of data or program, including the key, into the third array 40. Since normally the HACC# signal 58 is accessible only by the manufacturer, only the program in the first array 20 would be copied into the corresponding first array 20 in the second device 10. The key or the copy protection code that is contained in the third array 40, although could be read by the computer to which the device 10 is attached, could not be copied to the second memory card because the HACC# signal 58 is not available. Thus, the copy protection code would not be copied over to the second device 10. The high voltage signal is normally not supplied to the memory card 10 when the card is used by a user in a "normal" computer. The high voltage signal is present only when the manufacturer publishes the card 10 and stores the key in the third array 30. As a result, during the execution of the program stored in the copied card, the program in the first array 20 or the second array 30, looks to the key in the third array 40. Since the key would be missing in the third array 40, the program would stop executing.

In the second case, the copying is from an original card to a copied card similar to the card 10 of the present invention. The copied card has the three arrays 20, 30 and 40, with the second and third arrays 30 and 40 being writable by the user. Since

the second and the third arrays 30 and 40 are writable by the user, the user can copy the contents of the second and third array 30 and 40 from the original card 10 to the copied card. After the data is copied, during the execution of the program, the program attempts to write into the area in the third array 40 where the key is located. If the card 10 is an original card, the user cannot write into that portion of the third array 40, and the original key would remain. If the card 10 is a copied card, the result would be an altered key. Thus, after an attempt to write into the portion of the third array 40 where the key is stored, the contents of third array 40 would be read. The result would be the original key being read back (if the card 10 were the original card) or would be the altered key (if the card 10 were the copied card). The program can then terminate execution if the key were the altered key.

In the third case, the copied card has the second array 30 and the third array 40 alterable by a programmer, but not by a user. A user, operating as a programmer status, copies the contents of the original card 10, including the contents of all three arrays 20, 30 and 40 into the copied card. Since the user has programmer status, the copied card will contain the contents from the third array 40 of the original card 10. In the execution of the program from the copied card, the program writes a test code into the third array 40 of the copied card 10. Upon read out, if the result is altered from the original key, then the card from which the program was loaded is a copied card and the program terminates its execution. This is the case where the user executes the program of the copied card while maintaining the programmer status.

If the user changes the status to a user status and executes the program from the copied card, then the program writing to the third array 40 would find the key is not altered. The program then writes to a section in the second array 30. If the second section is alterable, then the card from which the program is executing is an original card. If the second array 30 is not alterable, then the card from which the program is executing is a copied card. In that event the program would also terminate its execution.

There are many advantages of the present invention. First and foremost is that the device 10 provides users of the device 10 a way to access extra memory blocks which are not normally addressable by the conventional address pins. As can be seen, the sections of the memory in the second array 30 and the third array 40 are addressed by the same address locations as in the first array 20. The generation of the first enable signal 24, and the second and third enable signals 34 and 44 respectively control whether or not the first array of memory cells 20 is accessed or the second and third memory arrays 30 and 40 are accessed. Further, within the second section 26 of the memory device 10, the memory is further divided into a user array 30 and a manufacturer array 40 to differentiate a user's portion and a manufacture's portion. Through this division, data security can be easily assured and copy protection can be properly enforced.

In another embodiment of the present invention, in lieu of the state machine 50 generating the SACC# signal 54, the SACC# signal 54 can be supplied directly into the memory device 10. In this embodiment, the address signals 12 can be used to

directly address the second and third arrays 30 and 40, respectively. Further, the direct access can be assigned to different user array or manufacturer array. In fact, direct access may permit addressing of a memory space which overlaps areas accessible by other access modes. In each of the overlapping areas, a different access rights, i.e. read only, read/write, or even write only can be defined.

WHAT IS CLAIMED IS:

1. A memory storage device having an address port for receiving an address signal, a data port for receiving an input data signal or for providing an output data signal, and a write enable port for receiving a write signal, said device comprising:

electrically alterable memory storage means for storing information, said storage means having a first section and a second section;

said first section of said storage means for receiving said address signal, said write signal, and having an enable port which receives a first enable signal for enabling or disabling said first section;

said second section of said storage means for receiving said address signal, said write signal, and having an enable port which receives a second enable signal for enabling or disabling said second section;

logic means for simultaneously generating said first enable signal for enabling said first section to receive said input data signal or for providing an output data signal therefrom and generating said second enable signal for disabling said second section;

said logic means further comprising means for simultaneously generating said first enable signal for disabling said first section and generating said second enable signal for enabling said second section to provide an output data signal therefrom in one state; and

said logic means further comprising means for simultaneously generating said first enable signal for disabling said first section and generating said second enable signal for

enabling said second section to receive said input data signal in another state.

2. The device of Claim 1 wherein said second section of said storage means further comprises a user section and a manufacturer section, each for receiving said address signal and said write signal.

3. The device of Claim 2 wherein said user section having an enable port for receiving a user enable signal, and said manufacturer section having an enable port for receiving a manufacturer enable signal.

4. The device of Claim 3 wherein said logic means in said one state simultaneously generates said first enable signal for disabling said first section, and generates said user enable signal for enabling said user section to receive said input data signal therefrom or to provide said input data signal therefrom, and generates said manufacturer enable signal for enabling said manufacturer section to provide said input data signal therefrom.

5. The device of Claim 4 wherein said logic means in another state simultaneously generates said first enable signal for disabling said first section, and generates said manufacturer enable signal for enabling said manufacturer section to receive said input data signal.

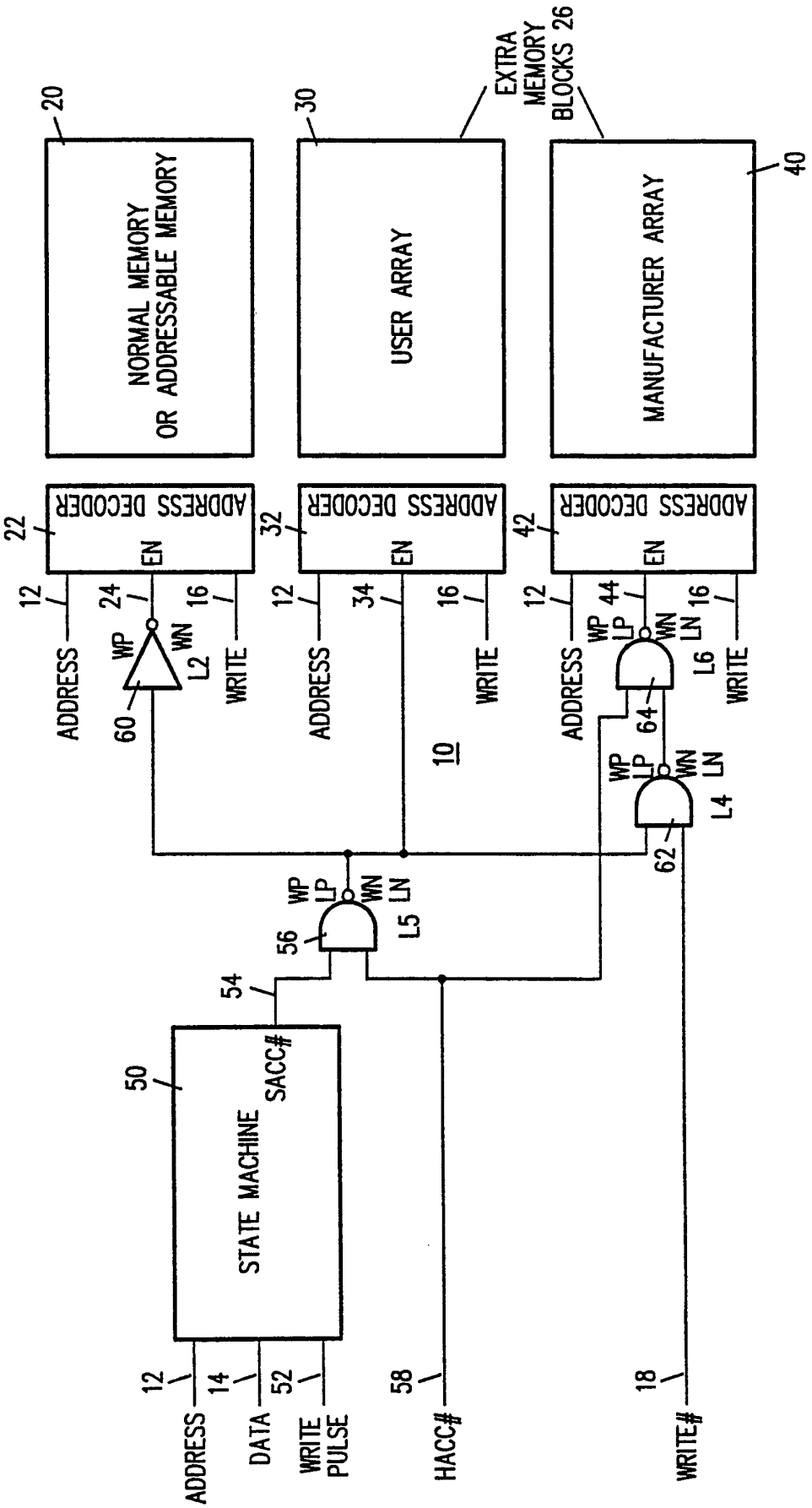
6. The device of Claim 5 wherein said manufacturer section stores a copy protected portion of a software program.

7. The device of Claim 1 wherein said logic means receives said address signal and said input data signal.

8. The device of Claim 7 wherein said logic means generates said first enable signal and said second enable signal in said one state in response to a combination of said address signal and input data signal.

9. The device of Claim 8 wherein said second section of said storage means stores a copy protected portion of a software program.

1/2



ORGANIZATION OF MEMORY

FIG. 1

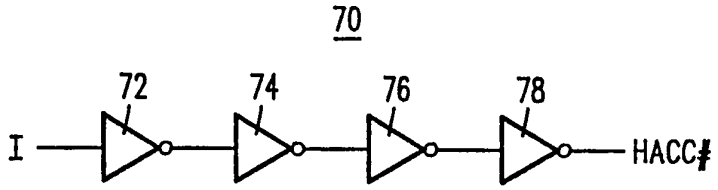


FIG. 2

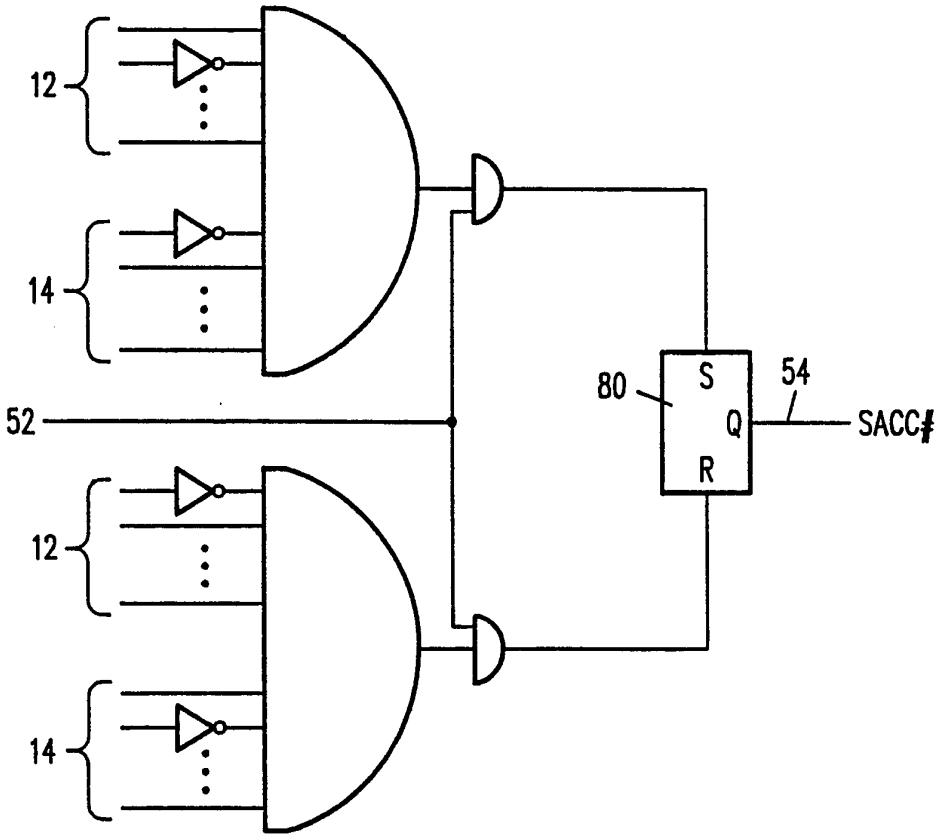


FIG. 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US93/10775

A. CLASSIFICATION OF SUBJECT MATTER

IPC(5) :GO6F 12/00, 12/06, 12/14
US CL : 364/DIG.1, 243, 244, 259, 238.4; 395/425
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)

U.S. : 364/DIG.1, 243, 244, 259, 238.4; 395/425

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 practicable, search terms used)

memory/storage modules, banks, simultaneous/concurrent enable/disable, address, data, protect, and write/copy.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y, E	US, A, 5,265,231 (Nuwayser) 23 November 1993, fig.2 and corresponding sections in the specification of Nuwayser	1-5 and 7-8
Y, P	US, A, 5,226,006 (Wang et al.) 6 July 1993, fig.s 2-5 and corresponding sections in the specification.	1-9
Y	US, A, 5,046,076 (Hill) 3 September 1991, col. 8, line 5 to col. 9, line 41.	1-5 and 7-8
Y	US, A, 3,995,253 (Morrin, II et al.) 30 November 1976, col. 4, line 36 to col. 5, line 22.	1-5 and 7-8
Y	US, A, 3,934,227 (Worst) 20 January 1976, background and summary of invention.	1-5 and 7-8

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"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
"A"	document defining the general state of the art which is not considered to be part of particular relevance	"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
"E"	earlier document published on or after the international filing date	"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
"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)	"&"	document member of the same patent family
"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		

Date of the actual completion of the international search
10 February 1994

Date of mailing of the international search report
FEB 28 1994

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. NOT APPLICABLE

Authorized officer
Matthew M. Kim

Telephone No. (703) 305-9600

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