PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 4 : **G06F 12/00, 12/14**	**A1**	**(11) International Publication Number:** **WO 88/ 09971** **(43) International Publication Date:** 15 December 1988 (15.12.88)

(21) International Application Number: PCT/US88/01902

(22) International Filing Date: 1 June 1988 (01.06.88)

(31) Priority Application Number: 057,541

(32) Priority Date: 3 June 1987 (03.06.87)

(33) Priority Country: US

(71) Applicant: PERSONAL CAD SYSTEMS, INC. [US/US]; 1290 Parkmoor Avenue, San Jose, CA 95126 (US).

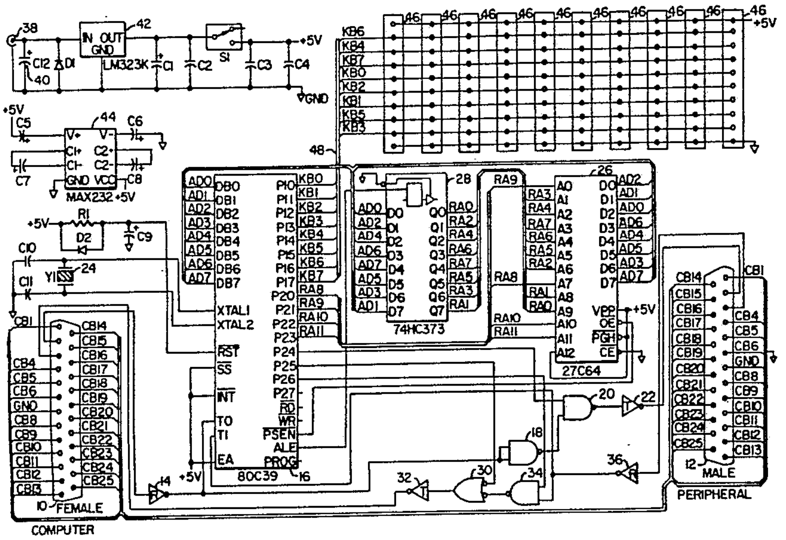
(72) Inventors: KAHL, Tracy ; 5942 Porto Alegre Drive, San Jose, CA 95120 (US). OSANN, Robert ; 4620 Corrida Circle, San Jose, CA 95129 (US).

(74) Agent: HAUGHEY, Paul, C.; Townsend and Townsend, One Market Plaza, 2000 Steuart Tower, San Francisco, CA 94105 (US).

(81) Designated States: AT (European patent), AU, BE (European patent), BR, CH (European patent), DE (European patent), DK, FI, FR (European patent), GB (European patent), IT (European patent), JP, KR, LU (European patent), NL (European patent), NO, SE (European patent).

Published
With international search report.
With amended claims.

(54) Title: SECURITY SYSTEM HAVING SELECTIVE SOFTWARE PROGRAM LOCKS UTILIZING REMOVABLE PLA KEYS TO ALLOW HARDWARE SECURITY LOCK UPDATES



(57) Abstract

A hardware security device enabling the operation of a software program on a computer is disclosed. The security device is coupled to a port (10) of the computer (10) between the computer (10) and a peripheral device (12). A pathway from the computer (10) to the peripheral device (12) through the security device is enabled by a processor (16) in the security device. The processor (16) is coupled to first (46) and second circuit (28, 26) which provide predetermined responses to the processor (16) in response to certain signals from the processor (16). In the preferred embodiment, one of the circuits is a PROM (28, 26) and the other circuit is a PLA (46) (Programmable Logic Array) key. The PLA (46) key (50) couples to a bus (48) connected to the microprocessor (16) which is capable of receiving a number of keys (50). Each key (50) corresponds to a different software program. By using removable and replaceable keys (50), a new program or a program update can be enabled by providing a new key (50) rather than providing an entire new security.

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
AU	Australia
BB	Barbados
BE	Belgium
BG	Bulgaria
BJ	Benin
BR	Brazil
CF	Central African Republic
CG	Congo
CH	Switzerland
CM	Cameroon
DE	Germany, Federal Republic of
DK	Denmark
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
HU	Hungary
IT	Italy
JP	Japan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
LI	Liechtenstein
LK	Sri Lanka
LU	Luxembourg
MC	Monaco
MG	Madagascar
ML	Mali
MR	Mauritania
MW	Malawi
NL	Netherlands
NO	Norway
RO	Romania
SD	Sudan
SE	Sweden
SN	Senegal
SU	Soviet Union
TD	Chad
TG	Togo
US	United States of America

SECURITY SYSTEM HAVING SELECTIVE SOFTWARE PROGRAM LOCKS UTILIZING REMOVABLE PLA KEYS TO ALLOW HARDWARE SECURITY LOCK UPDATES

BACKGROUND OF THE INVENTION

The present invention relates to an external hardware security device for data processing systems.

Software companies often provide elaborate copy protection codes in a software program to prevent unauthorized copying and use of the program. Such codes usually allow only one backup copy of the program to be made and then prevent any further copying of the program. Such codes take advantage of various vagaries of the computer operating system. Unfortunately, such codes are readily removed by copy programs such as "Locksmith". The same operating system vagaries that enable the protection codes to work may also be readily exploited by one knowledgeable with the computer's operating system to circumvent such protection codes. Once the knowledge of such protection code circumvention is available, it is readily disseminated without hesitation to others for the purpose of making additional unauthorized copies of the subject software program.

Security devices presently sold by Personal CAD Systems, Inc. and others connect to a serial port of a computer between the computer and a peripheral device. The security device has a microprocessor which receives an authorization request from the software program running on the computer. An algorithm run by the processor in response to the authorization request produces an encrypted message which is sent back to the software program to provide authorization. The encrypted message is generated with the use of a PROM (programmable read only memory) which is coupled to the microprocessor and is uniquely matched to the program being run. To enable a different software program, a different security device with a different PROM would be used. Thus, the software program cannot be copied and used on another computer without the physical security device.

Another security system uses a PC (printed circuit) board which plugs directly into the computer. The PC board contains a PLA (programmable logic array) device which produces a predetermined output when interrogated by the computer's microprocessor. A different PLA is used for each software program so that the software program will not run without the correct PLA. The microprocessor directly addresses the PLA as it would address any memory location, and the program will not run if the correct response is not provided by the PLA.

SUMMARY OF THE INVENTION

The present invention is a hardware security device enabling the operation of a software program on a computer. The security device is coupled to a port of the computer between the computer and a peripheral device. A pathway from the computer to the peripheral device through the security device is enabled by a processor in the security device. The processer is coupled to first and second circuits which provide predetermined responses to the processor in response to certain signals from the processor.

In the preferred embodiment, one of the circuits is a PROM and the other circuit is a PLA key. The PLA key couples to a bus connected to the microprocessor which is capable of receiving a number of keys. Each key corresponds to a different software program. By using removable and replaceable keys, a new program or a program update can be enabled by providing a new key, rather than providing an entire new security device.

The PLA key improves both the flexibility and the security of a security device of the present invention as compared to the existing security device sold by Personal CAD Systems as described above. The algorithm used by the processor is thus provided with a second degree of complexity. In addition to requiring a coded message from the PROM which is common to all software programs enabled by the security device, the algorithm also requires a coded response specific to a particular software program which is provided by a PLA key and can be easily replaced or updated any time.

In addition, each key is provided with two I/O (input/output) lines through which all data communications to and from the key are passed. A standard PROM would have addresses provided on address lines and data read from separate data lines, enabling a person trying to break the security code to determine what data is being provided to the PROM and what data is being provided to response. By multiplexing data to and from the key on the same I/O lines, a potential security code breaker is prevented from determining whether the data he is monitoring is going to or from the key.

The use of a single bus to receive a plurality of keys enhances the flexibility and expandability of the security device. The addressing data is provided to all keys on the bus, but only the appropriate key will respond to the code directed to that key, thus enabling a number of keys to be connected in parallel. This enables the same computer system, which has the appropriate keys, to run several different software programs. In addition, these software programs can be moved to another computer system by simply moving the associated key, rather than disconnecting the security device and reconnecting it in the new computer system.

For a fuller understanding of the nature and advantages of the invention, reference should be made to the ensuing detailed description taken in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a schematic diagram of an exemplary security device according to the present invention; and

Fig. 2 is a block diagram of a key and the key interface of Fig. 1.

DETAILED DESCRIPTION OF A PREFERRED EMBODIMENT

The present invention is a hardware device that puts a copy/run lock and key on any software package. An exemplary embodiment of the present invention is shown in schematic form in Fig. 1. A connector 10 couples the security device to a host computer serial communications port. The discussion herein is directed to a serial communications line or port, although the present invention is readily adaptable for operation in any computer addressable communications port including parallel and other such ports.

A second connector 12 is provided for coupling the serial communications port directly through to a remote device. Accordingly, the present invention may be operated in a manner transparent to the device remotely connected to the communications port, such as disc drivers, printers, etc. In this way, the device does not limit the communications capability of the computer by tying up a communications port.

Data from the host computer is coupled through connector 10 into an inverter 14 to a microprocessor 16, Data received by microprocessor 16 may be of a type intended for a remote device, in which case the data is coupled through inverter 18 to a NAND gate 20 which is enabled by microprocessor 16. An inverter 22 converts the signal back to its original form and supplies the signal to pin 2 of connector 12, and thereafter to the remote device.

Data received at microprocessor 16 is clocked in at a microprocessor clock rate which is a function of crystal 24. Microprocessor 16 examines a portion of the data to determine if it is a security device read or if the data is intended for the remote device. In the exemplary embodiment of the invention, an 11-MHz clock is provided to an 80C39 microprocessor.

An external PROM 26 is coupled to a microprocessor data bus by means of a latch circuit 28. PROM 26 may be readily replaced with different encryption standards as desired. During a memory addressing operation, a data word is presented to latch 28. The data word is thereafter latched to the address bus of PROM 26. During this interval, the microprocessor turns the data bus (DBO-DB7) around to receive instructions from PROM 26. When clocked appropriately, PROM 26 provides an instruction in the form of data output to the microprocessor data bus.

One or more PLA keys are plugged into connectors 46. Connectors 46 are connected to microprocessor 16 via a bus 48 as shown in more detail with reference to Fig. 2 below.

In response to program instructions received from PROM 26 and one of the keys in connectors 46, a microprocessor data output is provided to NAND gate 30 and thereafter through inverter 32 to the host computer. During intercommunication between the security device and the host computer, any remote device coupled to the host computer is isolated from the serial communications bus by a disabling signal from microprocessor 16. Data from a remote device is thereafter coupled through inverter 36, NAND gate 34, NAND gate 30 and inverter 32 to the host computer.

A local power supply is created by regulating and filtering a 9-volt source supplied through a connector

38. Such filtering is provided by a capacitor 40. Thereafter, voltage regulation is provided by regulator circuits 42 and 44 to produce the required outputs to operate the security device.

Because a minimum number of components are required to produce the security device, it can be provided in a very small container that is readily connected to and removed from a computer. Accordingly, the security device may be taken home by the computer user at the end of the work day, thereby preventing unauthorized operation of the computer.

Fig. 2 shows the keys and key interface in more detail. The plurality of keys 50 can be coupled to bus 48 through connectors 46 shown in Fig. 1. Bus 48 consists of eight signal lines. The clock input 52 for the keys is simply an address port bit of the microprocessor which is toggled under software control. Only two bus lines 54 are used for input and output. These lines are bidirectional so that it will be difficult for an observer to discern which direction signals are flowing during communications between the microprocessor 16 and the keys 50. The other five lines 56 are simply data lines which address the keys and provide information to them.

One of the keys 58 is shown in more detail in Fig. 2. Each key is a single CMOS PLA device having a security fuse which will prevent information from being read from the device. The devices are programmed so that they comprise a sequential machine. Their operation is hidden from the user since most of the signals involved in the sequence are not brought out to the bus connection, but are instead fed back to the internal logic structure. As shown, device 58 has an array 60 of logic which feeds to output flip-flops 62. The output of these flip-flops are fed back via feedback lines 64 to array 60 for most of the outputs. Only two output lines connected to bidirectional lines 54 are used.

In operation, before an authorization request from the host software program, microprocessor 16 scans data bus 48 to determine which keys 50 are present. Upon an authorization request from microprocessor 16, an algorithm is run which requires an appropriate response from PROM 26 and from one of keys 50. The result of the algorithm is then transmitted back to the computer. If the result is the proper one for the program being run, microprocessor 16 will be instructed to enable the data path between connectors 10 and 12 by appropriate signals to NAND gates 20 and 34 and NAND gate 30. The algorithm can either be very simple or fairly complex. The one requirement on the algorithm used is that it access a predetermined response from PROM 26 which is common to all programs which can be authorized and that it access a predetermined response from one of keys 50 for the particular program being used.

As will be understood by those familiar with the art, the present invention may be embodied in other specific forms without departing from the spirit or essential characteristics thereof. For example, a structure in which the keys plug into a single connector with subsequent keys plugging into the first key could be used. In addition, the memory of PROM 26 could be fully contained within the microprocessor. Accordingly, the disclosure of the preferred embodiments of the invention is intended to be illustrative, but not limiting, of the scope of the invention which is set forth in the following claims.

WHAT IS CLAIMED IS:

1. A security device for enabling the operation of one of a plurality of software programs on a computer, comprising:

a first connector for coupling to a port of said computer;

a second connector for coupling to a peripheral device;

means, responsive to a control signal, for coupling said first connector to said second connector;

processor means coupled to said first connector for receiving an authorization request message from one of said software programs and providing an encrypted response and for providing said control signal to said means for coupling;

first circuit means, coupled to said processor means, for providing a first predetermined response to a first plurality of signals from said processor means; and

second circuit means, coupled to said processor means, for providing a second predetermined response to a second plurality of signals from said processor means, said second circuit means enabling said processor means to provide said encrypted message for only a selected one or ones of said software programs.

2. The security device of claim 1 wherein said first circuit means comprises a programmable read only memory.

3. The security device of claim 1 wherein said second circuit means comprises a programmable logic array.

4. The security device of claim 1 wherein said second circuit means receives inputs and provides outputs on one multiplexed input/output line.

5. The security device of claim 1 further comprising a socket for removably coupling said second circuit means to said processor means.

6. The security device of claim 1 further comprising a plurality of sockets and a bus coupling said sockets to said processor means for enabling the connection of a plurality of said second circuit means to said processor means in parallel.

7. The security device of claim 1 wherein said processor means is a microprocessor.

8. The security device of claim 1 wherein said port of said computer is a serial port.

9. A security device enabling the operation of one of a plurality of software programs on a computer, comprising:

a first connector for coupling to a port of said computer;

a second connector for coupling to a peripheral device;

means, responsive to a control signal, for coupling said first connector to said second connector;

processor means coupled to said first connector for receiving an authorization request message from one of said software programs and providing an encrypted response and for providing said control signal to said means for coupling; and

a removable programmable logic array key coupled to said processor means, for providing a second predetermined response to a second plurality of signals from said processor means, said second circuit means enabling said processor means to provide said encrypted message for only a selected one or ones of said software programs.

10. The security device of claim 9 further comprising an external memory, coupled to said processor means, for providing a first predetermined response to a first plurality of signals from said processor means, and

11. A security device for enabling the operation of one of a plurality of software programs on a computer, comprising:

a first connector for coupling to a serial port of said computer;

a second connector for coupling to a peripheral device;

means, responsive to a control signal, for coupling said first connector to said second connector;

a microprocessor coupled to said first connector for receiving an authorization request message from one of said software programs and providing an encrypted response and for providing said control signal to said means for coupling;

a programmable read only memory coupled to said microprocessor, for providing a first predetermined response to a first plurality of signals from said microprocessor;

a removable programmable logic array key coupled to said microprocessor, for providing a second predetermined response to a second plurality of signals from said microprocessor, said key enabling said microprocessor to provide said encrypted message for only a selected one or ones of said software programs, said key receiving inputs and providing outputs on one multiplexed Input-Output line;

a plurality of sockets and

a bus coupling said sockets to said microprocessor for enabling the connection of a plurality of said keys to said microprocessor in parallel.

AMENDED CLAIMS

[received by the International Bureau on 3 October 1988 (03.10.88)
original claims 1.3-7,9 and 10 cancelled: claim 11 replaced by amended
claim 1; claim 2 amended (3 pages)]

1. A security device for enabling access to a peripheral device other than a second computer, during the operation of one of a plurality of software programs on a computer, comprising:

a first connector for coupling to a port of said computer;

a second connector for coupling to said peripheral device;

means, responsive to a control signal, for coupling said first connector to said second connector;

a microprocessor coupled to said first connector for receiving an authorization request message from one of said software programs and providing an encrypted response and for providing said control signal to said means for coupling;

a first memory coupled to said microprocessor, for providing a first predetermined response to a first plurality of signals from said microprocessor;

a removable programmable logic array key coupled to said microprocessor, for providing a second predetermined response to a second plurality of signals from said microprocessor, said key enabling said microprocessor to provide said encrypted response for only a selected one or ones of said software programs, said key receiving inputs and providing outputs on the same multiplexed Input-Output lines;

a plurality of sockets, each capable of receiving said key; and

a bus coupling said sockets to said

microprocessor, thus enabling a plurality of said keys to be connected to said microprocessor in parallel.

2. The security device of claim 1 wherein said first memory comprises a programmable read only memory.

3. The security device of claim 1 wherein said port of said computer is a serial port.

4. The security device of claim 1 further comprising additional, non-multiplexed data input lines to said key from said bus, the input of said key being provided only over said multiplexed Input-Output lines.

5. The security device of claim 1 further comprising a clock line coupled between a clock input of said key and an address output of said microprocessor.

6. A security device for enabling access to a peripheral device other than a second computer, during the operation of one of a plurality of software programs on a computer, comprising:

a first connector for coupling to a serial port of said computer;

a second connector for coupling to said peripheral device;

means, responsive to a control signal, for coupling said first connector to said second connector including first and second NAND gates each having a first input for receiving said control signal, second inputs coupled to said first and second connectors, respectively, and outputs coupled to said second and first connectors, respectively;

a memory coupled to said microprocessor, for providing a first predetermined response to a first plurality of signals from said microprocessor;

a removable programmable logic array key coupled to said microprocessor, for providing a second predetermined response to a second plurality of signals from said microprocessor, said key enabling said microprocessor to provide said encrypted response for only a selected one or ones of said software programs, said key receiving inputs and providing outputs on the same multiplexed Input-Output lines;

a plurality of sockets, each capable of receiving said key;

a bus coupling said sockets to said microprocessor, thus enabling a plurality of said keys to be connected said microprocessor in parallel;

additional, non-multiplexed data input lines to said key from said bus, an output of said key being provided only over said multiplexed Input-Output lines; and

a clock line coupled between a clock input of said key and an address output of said microprocessor.

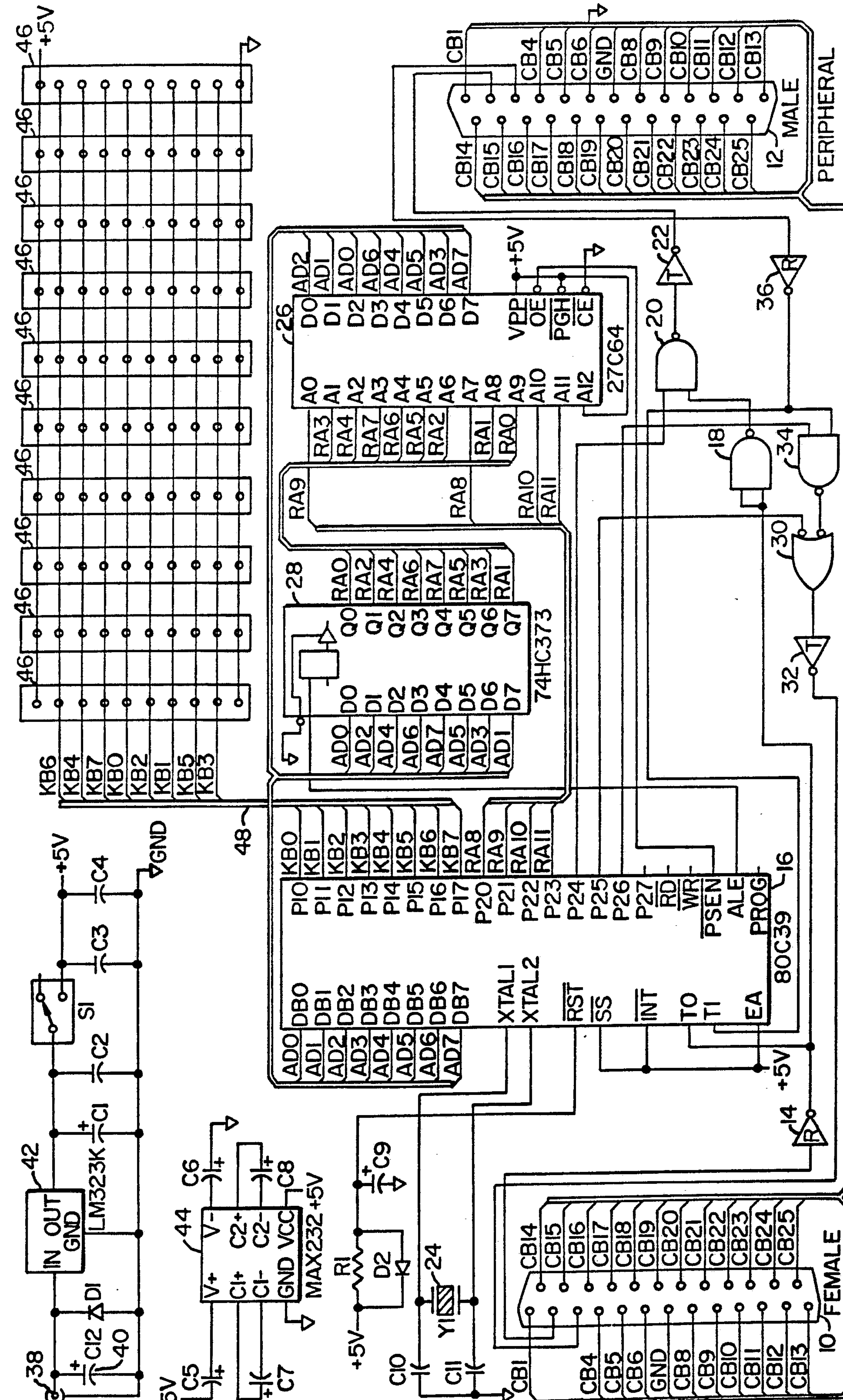


FIG._1.

SUBSTITUTE SHEET

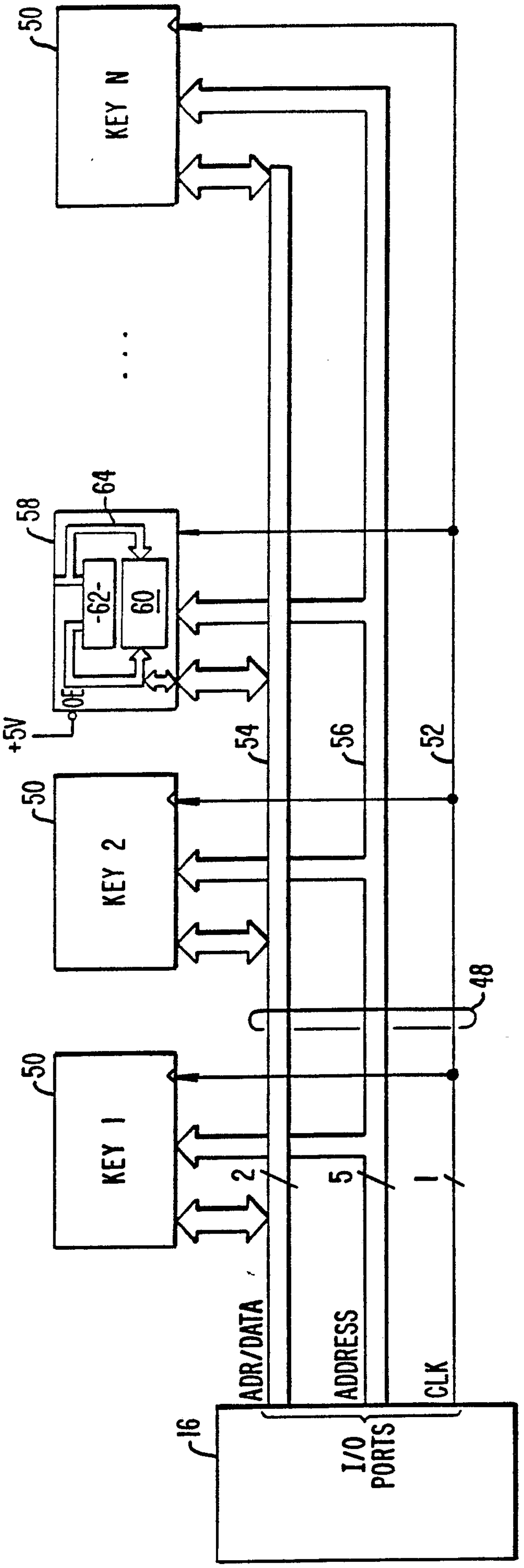

50
KEY N
58
64
-62-
60
+5V
OE
54
56
52
50
KEY 2
48
50
KEY 1
2
5
1
ADR/DATA
ADDRESS
CLK
16
I/O
PORTS

FIG._2.

INTERNATIONAL SEARCH REPORT

International Application No. PCT/US88/01902

I. CLASSIFICATION OF SUBJECT MATTER (if several classification symbols apply, indicate all) [6]

According to International Patent Classification (IPC) or to both National Classification and IPC

IPC(4): G06F 12/00 12/14
U.S. Cl. 364/200

II. FIELDS SEARCHED

Minimum Documentation Searched [7]

Classification System	Classification Symbols
U.S.	364/200, 364/900, 380/4, 380/25 380/28, 380/29, 380/45

Documentation Searched other than Minimum Documentation to the Extent that such Documents are Included in the Fields Searched [8]

III. DOCUMENTS CONSIDERED TO BE RELEVANT [9]

Category *	Citation of Document, [11] with indication, where appropriate, of the relevant passages [12]	Relevant to Claim No. [13]
P, Y	US, A, 4,685,056 (BARNSDALE, JR. ET AL.) 4 August 1987, see entire document.	1-11
A	US, A, 4,493,028 (HEATH) 8 JANUARY 1985, see figure 1.	1-11
A	US, A, 4,646,234 (TOLMAN ET AL.) 24 February 1987, see entire document.	1-11
P, A	US, A, 4,683,968 (APPELBAUM ET AL.) 4 August 1987, see entire document.	1-11
A	US, A, 4,525,599 (CURRAN ET AL.) 25 June 1985 see figure 4.	1-11
A	US, A, 4,562,305 (GAFFNEY, JR.) 31 December 1985, see Abstract, figure 1, col. 3 (line 13 - et seq.).	1-11
Y	US, A, 4,652,990 (PAILEN ET AL.) 24 March 1987, see entire document.	1, 2, 4-11

* Special categories of cited documents: [10]

"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

"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

IV. CERTIFICATION

Date of the Actual Completion of the International Search 15 JULY 1988	Date of Mailing of this International Search Report 29 JUL 1988
International Searching Authority ISA/US	Signature of Authorized Officer ROBERT B. HARRELL