PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G07B 17/04 | A1

(11) International Publication Number: **WO 99/48055**

(43) International Publication Date: 23 September 1999 (23.09.99)

(21) International Application Number: PCT/US99/05891

(22) International Filing Date: 18 March 1999 (18.03.99)

(30) Priority Data:
60/078,489 18 March 1998 (18.03.98) US

(71) Applicant *(for all designated States except US)*: ASCOM HASLER MAILING SYSTEMS INC. [US/US]; 19 Forest Parkway, Shelton, CT 06484–6140 (US).

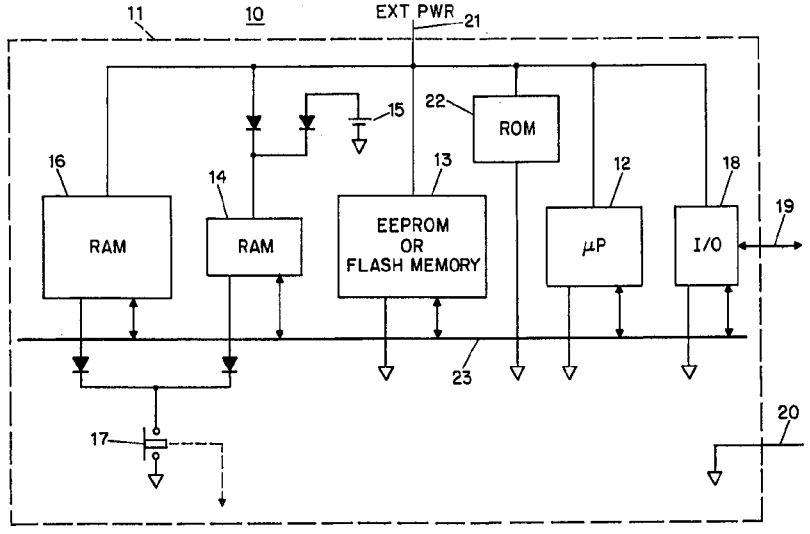
(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: NACLERIO, Edward, J. [US/US]; 49 Scenic Road, Madison, CT 06443 (US).

(74) Agents: OPPEDAHL, Carl et al.; Oppedahl & Larson, P.O. Box 5270, Frisco, CO 80443–5270 (US).

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

Published
With international search report.

(54) Title: TAMPER RESISTANT POSTAL SECURITY DEVICE WITH LONG BATTERY LIFE



(57) Abstract

In accordance with the invention, a postal security device (PSD) (10) contains a non–volatile memory (13) which does not depend on battery power such as an EEPROM (13), and contains a nonvolatile memory (14, 16) which does depend on battery power, such as a static RAM. The PSD (10) also contains an encryption engine (12, 14, 22). An encryption key is developed and is stored in the static RAM (14), which is sized to be only large enough to contain the encryption key. A large body of data, too large to fit in the static RAM, is encrypted by means of the encryption engine (12, 14, 22) and with reference to the encryption key, and is stored in the EEPROM (13). This body of data typically includes cryptographic keys and sensitive bit–images. When the PSD is powered, a large RAM (typically a dynamic RAM) (16) is available to receive the large body of data, decrypted using the encryption key. A tamper switch (17) cuts power to both RAMs (14, 16) in the event of tampering.

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.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

TAMPER RESISTANT POSTAL SECURITY DEVICE WITH LONG BATTERY LIFE

The invention relates generally to postage meters (franking machines), and relates particularly to systems in which postage value is stored in a postal security device (PSD) so as to be protected against undetected tampering. The application claims priority from US application no. 60/078,489, filed March 18, 1998, which application is incorporated herein by reference to the extent permitted by the designated and elected States hereto.

Background

In recent years it has been proposed to print postal indicia by means of conventional nonsecure printers such as laser printers, ink-jet printers, and thermal transfer printers. Such printers are termed "nonsecure" because the printer itself is not in a secure housing and because the communications channel linking the printer to other apparatus is nonsecure. Under such a proposal, the question naturally arises what would prevent a user from printing the same postal indicium repeatedly, thereby printing postal indicia for which no money has been paid to the post office. The proposed anti-fraud measure is to store information within the indicia which would permit detecting fraud. The indicium would include not only human-readable text such as a date and a postage amount, but would also include machine-readable information, for example by means of a two-dimensional bar code. The machine-readable information would be cryptographically signed, and would include within it some information intended to make fraud more difficult. The information would typically include an identification of the postage meter license (granted by the meter manufacturer or by the postal authorities, depending on the country), an indication of the number of mail pieces franked, the postage amount, a postal security device identifier about which more will be said later, the date and time, and a zip code or post code of the mail piece addressee.

The typical apparatus for printing such "encrypted indicia" postage includes what is called a postal security device or PSD. The PSD has a secure housing, and within the secure housing are the accounting registers as well as a cryptographic engine. The engine permits cryptographic authentication and signing for communication with an external device such as

the computer of the meter manufacturer or of the post office. The engine also permits creation of postal indicia which contain specified information and which are cryptographically signed. The PSD may well be physically small as compared to traditional postage meters. The PSD may be the size of a PCMCIA card or the size of a smart card.

Within the PSD the memory must be protected against inadvertent damage due to malfunction of the processor of the PSD, for example as set forth in US Pat. No. 5668973, *Protection system for critical memory information* owned by the same assignee as the assignee of the present application. The PSD must handle power failure in a graceful fashion, for example as set forth in US Pat. No. 5712542, *Postage meter with improved handling of power failure*, also owned by the same assignee as the assignee of the present application.

To reduce smudging, the printer may preferably be that described in PCT publication no. 97-46389, *Printing apparatus,* also owned by the same assignee as the assignee of the present application. While it has been proposed that the PSD contain a real-time clock which is keeping time continuously, desirably this requirement may be avoided as described in PCT publication no. 98-08325, *Printing postage with cryptographic clocking security*, also owned by the same assignee as the assignee of the present application. PSDs can form part of a network with multiple printers as described in PCT publication no. 98-13790, *Proof of postage digital franking*, also owned by the same assignee as the assignee of the present application.

The postal authorities face the question how the PSD can be protected from tampering. For example, the entire system of PSDs depends on the use of cryptographic keys. The keys are used for authenticating communications between the PSD and the manufacturer's system or the postal authority's system. Such communications are used to set up and maintain the PSDs, and are used to refill or "reset" the PSDs to reflect the ability to print more postage. The keys are also used to cryptographically "sign" information printed in the postal indicia. If the cryptographic keys were compromised, a user might be able to defraud the post office or the PSD manufacturer or both.

Many approaches have been proposed for protection of such cryptographic keys from compromise. The usual approach is to place the cryptographic keys in a RAM (random access memory) of a type which keeps its contents only so long as the RAM receives power from a battery. The secure housing of the PSD is designed to include a tamper switch, so that if the secure housing is tampered with, the switch opens. The switch interrupts power to the RAM (and, in particular, interrupts battery power to the RAM) and its contents are lost. In this way the information in the RAM (for example, the cryptographic keys) is protected from tampering. Another proposed approach is to employ commercial memory chips (such as the Dallas Semiconductor DS1283 and Benchmarq bq3283) offer a pin on the package which will clear the memory based on a predetermined input voltage level. The tamper switch is set up to apply the predetermined voltage upon detection of tampering.

Many approaches have also been proposed for detection of the tampering. In EP 820 041, for example, it is suggested that the secure housing of an old-style mechanical or electromechanical postage meter be set up to contain an air pressure that is distinctively higher than or lower than normal atmospheric pressure. If the secure housing is violated, the pressure within the secure housing changes to match the ambient pressure. A sensor within the housing detects the pressure change and thus the violation. The sensor disables further function of the postage meter.

The approach of cutting power to a volatile memory such as the RAM discussed above has a drawback in that during periods of power-down, the RAM depends on an internal battery to avoid loss of the information in the RAM. Depending on the requirements of the postal authority, and on design decisions made by the PSD manufacturer, the quantity of data requiring protection may be quite large. The data to be protected may include cryptographic keys used for PSD configuration, keys used for remote resetting (refilling), keys used for signing postal indicia, and keys used for the management of the other keys. In addition it may be desired to protect the bit-images used to generate the human-readable portion of the printed indicia. A RAM big enough to hold all of these important items of data will also draw a non-negligible current from the internal battery. This may lead to a limited and commercially unacceptable battery life.

It would thus be desirable to have a PSD design which protects the many important items of data stored within, and yet which does not draw very much battery power and so permits a commercially acceptable battery life.

Summary of the invention

In accordance with the invention, a postal security device (PSD) contains a nonvolatile memory which does not depend on battery power, such as an EEPROM, and contains a nonvolatile memory which does depend on battery power, such as a static RAM. The PSD also contains an encryption engine. An encryption key is developed and is stored in the static RAM, which is sized to be only large enough to contain the encryption key. A large body of data, too large to fit in the static RAM, is encrypted by means of the encryption engine and with reference to the encryption key, and is stored in the EEPROM. This body of data typically includes cryptographic keys and sensitive bit-images. When the PSD is powered, a large RAM (typically a dynamic RAM) is available to receive the large body of data, decrypted using the encryption key. A tamper switch cuts power to both RAMs in the event of tampering. In this way, the battery power required to maintain the PSD during power-off periods is minimal, and yet the large body of data will be inaccessible in the event of tampering.

Description of the drawing

The invention will be described with respect to a drawing, of which:

Fig. 1 is a schematic functional block diagram of a system according to the invention.

Detailed description

Fig. 1 shows a postal security device (PSD) in accordance with the invention. The PSD has a microprocessor 12 which communicates on a bus 22 with an input/output (I/O) device 18, a memory which does not require battery backup 13 which may be for example an EEPROM or

flash memory, a relatively small RAM 14, a ROM 22, and a larger RAM 16. The I/O device 18 communicates with external apparatus by means of communications channel 19 which may be a serial asynchronous data line. External power 21 and ground 20 are also defined. The larger RAM 16, and most of the other active components, receive external power. The smaller RAM 14 is additionally able to receive power from a backup battery 15, preferably a lithium cell with a very long (e.g. ten year) life. A tamper switch 17 is provided which, when triggered, can cut power to both the small RAM 14 and the large RAM 16.

A large body of data is assumed to require protection from a tampering user. The EEPROM is selected to be large enough to hold this body of data after it has been encrypted. When power is applied and the system is stable, the body of data (or selected portions thereof) is decrypted and transferred to RAM 16. This decryption is performed by the microprocessor 12 executing a decryption routine stored in the ROM 22, and the decryption is done with respect to a decryption key in the RAM 14. Alternatively the decryption may be performed by an optional engine omitted for clarity in Fig. 1. The decrypted data in RAM 16 are used as needed for the ordinary functions of the PSD, which include communicating via the communications channel 19 with a user computer, with a manufacturer's system, or with a postal authority system, and can include generating postal indicia which are to be printed by means of a printer.

When external power 21 is cut off, or when the PSD undergoes a normal power-down routine, the information in the RAM 16 is lost. In contrast, the information in the RAM 14 is preserved even when external power 21 is lost, because of battery 15.

During normal operation the body of data that requires protection from a tampering user (or some portion of it) may be located "in the clear", that is, unencrypted, in the RAM 16. In the event that this data has changed, it may be necessary to encrypt the data and to store it again in the memory 13. This encryption is performed by the processor 12 executing encryption software in the ROM 22, or may optionally be performed by an encryption engine omitted for clarity in Fig. 1.

The power-down condition for the PSD 10 assumes that no power is present at line 21. In that event, the only powered device is RAM 14. RAM 14 was purposefully selected to be large enough to hold the encryption key but not much larger, and in any event is smaller than the large body of data that is understood to require protection from a tampering user. Because of the limited size of the RAM 14, it does not draw as much current from the battery 15 as would be drawn by a larger RAM such as RAM 16. Thus, the battery life is optimized, especially as compared with the shorter battery life that would result if the large body of data were all in battery-backed-up RAM.

Tampering may happen during a time when external power 21 is present. At a minimum, the tamper switch should cut power to the RAM 14. (Or, alternatively, the tamper switch should apply to RAM 14 the predetermined voltage that clears the RAM.) Preferably the tamper switch will also cut power to the RAM 16 (or clear the RAM 16), for the reason that some of the body of sensitive data may be present "in the clear" in the RAM 16, and should not fall into the hands of the tampering user. Alternatively the tamper switch might trigger an interrupt in the processor 12 which would cause the processor 12 to clear the sensitive portions of the RAM 16.

Tampering may also happen during a time when external power 21 is absent. In such a case, the RAM 16 is already, by definition, empty, as it is unpowered. The tamper switch causes the RAM 14 to be cleared. If the tampering user extracts the contents of the memory 13, this is of little significance, because the contents are useless unless decrypted with the assistance of the key that is no longer present in the RAM 14. If the PSD 10 is powered up again after the tampering, the decryption routine will not work because the key of RAM 14 is gone. In addition, desirably the processor 12, under program control, will note the fact that RAM 14 is empty and will immediately attempt to send a message via communications channel 19 to the manufacturer or to the postal authority.

Those skilled in the art will readily appreciate that design considerations may prompt the use of electrical components in addition to or instead of those shown in Fig. 1, none of which depart in any way from the invention. For example, dedicated cryptographic chips may be

employed which take some of the computational burden from the microprocessor. As another example, the particular way in which the tamper switch cuts power to the RAM may be varied, and the particular type of tamper switch may be selected among several types, all without departing in any way from the invention. Those skilled in the art will indeed have no difficulty devising obvious variations and improvements to the invention, all of which are intended to be encompassed by the claims that follow.

Claims

1. A postal security device comprising a secure housing, and within the secure housing a body of data having a size, said postal security device also having within the secure housing means for generating print data for printing of postage indicia, said generating of said print data relying in part on the body of data, said postal security device also having within the secure housing a first memory sized to accommodate the body of data, said first memory of a type not requiring electrical power to maintain the contents thereof, said postal security device also having within the secure housing a second memory not large enough to accommodate the body of data, said second memory of a type requiring electrical power to maintain the contents thereof, said postal security device also comprising a battery powering the second memory and a tamper switch mechanically coupled with the secure housing so that upon tampering with the secure housing the second memory is disconnected from the battery, said postal security device further comprising an encryption key stored within said second memory, said postal security device further comprising a cryptographic engine, said body of data encrypted by the cryptographic engine with respect to the encryption key.

2. A method for use with a postal security device comprising a secure housing, and within the secure housing a body of data having a size, said postal security device also having within the secure housing means for generating print data for printing of postage indicia, said generating of said print data relying in part on the body of data, said postal security device also having within the secure housing a first memory sized to accommodate the body of data, said first memory of a type not requiring electrical power to maintain the contents thereof, said postal security device also having within the secure housing a second memory not large enough to accommodate the body of data, said second memory of a type that requires electric power to maintain its contents, said postal security device also comprising a battery powering the second memory and a tamper switch mechanically coupled with the secure housing so that upon tampering with the secure housing the second memory is disconnected from the battery, said postal security device further comprising an encryption key stored within said second memory, said postal security device further comprising a cryptographic engine; the method comprising the steps of:

storing the encryption key within the second memory;

encrypting the body of data by the cryptographic engine with respect to the encryption key;

storing the encrypted body of data in the first memory; and

in the event of tampering, removing power from the second memory.

3. A method for use with a postal security device comprising a secure housing, and within the secure housing a body of data having a size, said postal security device also having within the secure housing means for generating print data for printing of postage indicia, said generating of said print data relying in part on the body of data, said postal security device also having within the secure housing a first memory sized to accommodate the body of data, said first memory of a type not requiring electrical power to maintain the contents thereof, said postal security device also having within the secure housing a second memory not large enough to accommodate the body of data, said second memory of a type that clears its contents upon a predetermined electrical condition, said postal security device also comprising a tamper switch mechanically coupled with the secure housing so that upon tampering with the secure housing the second memory has said predetermined electrical condition, said postal security device further comprising an encryption key stored within said second memory, said postal security device further comprising a cryptographic engine; the method comprising the steps of:

storing the encryption key within the second memory;

encrypting the body of data by the cryptographic engine with respect to the encryption key;

storing the encrypted body of data in the first memory; and

in the event of tampering, causing said predetermined electrical condition.

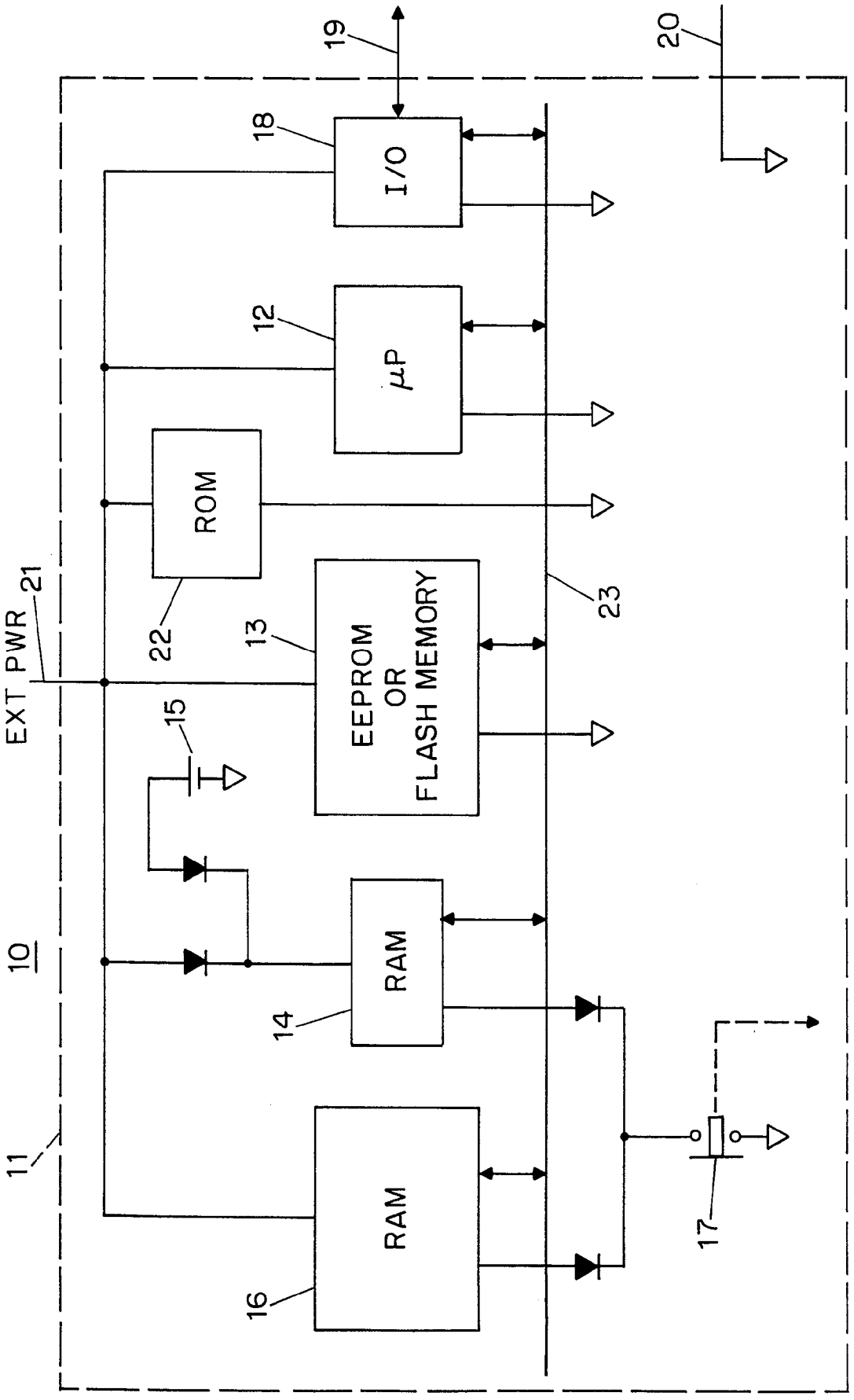

19
20
18
I/O
12
μP
ROM
22
EXT PWR
21
13
EEPROM
OR
FLASH MEMORY
23
15
10
RAM
14
11
RAM
16
17

FIG. 1

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/05891

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :G07B 17/04
US CL :705/405

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. : 380/3, 4, 23, 25; 705/401, 405, 410

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

None

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

None

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 4,575,621 A (DREIFUS) 11 March 1986, see abstract.	1-3
A	US 4,882,752 A (LINDMAN et al) 21 November 1989, see abstract.	1-3
A	US 5,097,253 A (ESCHBACH et al 17 March 1992, see abstract.	1-3
A	US 5,249,227 A (BERGUM et al) 28 September 1993, see abstract.	1-3

☐ 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 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	Date of mailing of the international search report
15 MAY 1999	28 MAY 1999
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer EDWARD R COSIMANO Telephone No. (703) 308-3800

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