(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 June 2006 (22.06.2006)

PCT

(10) International Publication Number
WO 2006/064318 A1

(51) International Patent Classification:
G11C 16/10 (2006.01) *G06F 11/00* (2006.01)
G06F 11/14 (2006.01) *G11C 16/22* (2006.01)

(21) International Application Number:
PCT/IB2005/003476

(22) International Filing Date:
21 November 2005 (21.11.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
04292970.3 13 December 2004 (13.12.2004) EP

(71) Applicant *(for all designated States except US)*: **AXALTO SA** [FR/FR]; 50 AVENUE JEAN JAURES, F-92120 MONTROUGE (FR).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **GIRAUD, Nicolas** [FR/FR]; C/O AXALTO SA, INTELLECTUAL PROPERTY DPT, 36-38 Rue de la Princesse, BP 45, F-78431 LOUVECIENNES (FR).

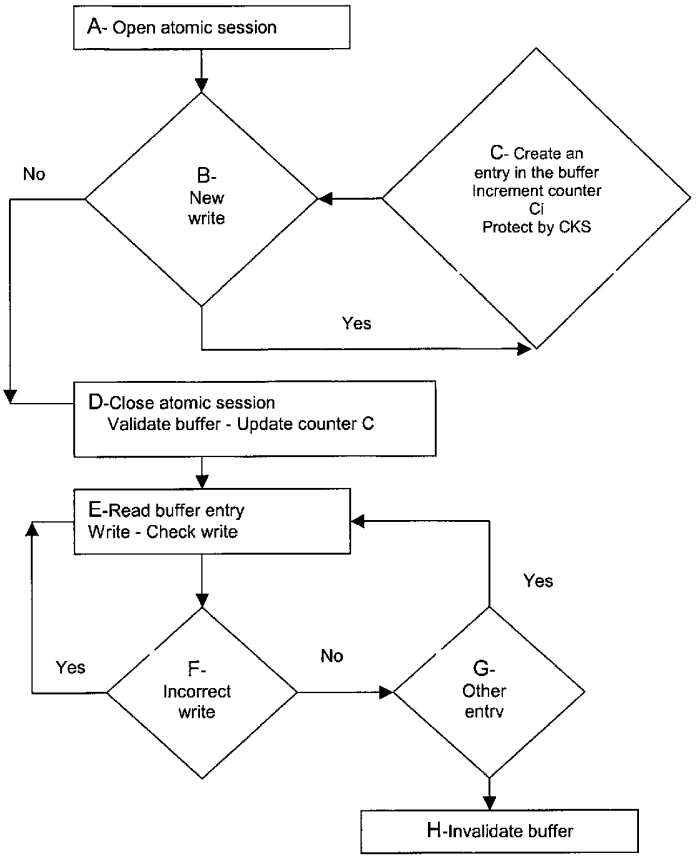
(74) Common Representative: **AXALTO SA**; IP & Licensing Department, 6, rue de la Verrerie, F-92197 Meudon Cedex (FR).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: METHOD TO SECURE WRITING IN MEMORY AGAINST ATTACKS BY RADIATION OR OTHER MEANS



(57) Abstract: The method according to this invention concerns a method to secure the write in storage means of an electronic assembly comprising information processing means, said method comprising an atomic write process to write data recorded in a write log. The method consists in checking a sequence of atomic writes in said storage means by setting in said write log one or more indicators in memory as proof of one of more successive writes recorded in said log. This invention also concerns the electronic module in which said method is implemented and the card comprising said module.

WO 2006/064318 A1

Declaration under Rule 4.17:

— *of inventorship (Rule 4.17(iv))*

Published:

— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

METHOD TO SECURE WRITING IN MEMORY AGAINST ATTACKS BY RADIATION OR OTHER MEANS

This invention concerns a method and a device to secure an electronic assembly implementing a program to be protected. More precisely, the purpose of the method is to propose a defence against attacks by radiation, flash, light, laser, glitch or other and more generally against any attack disturbing the execution of the program instructions. These attacks modify the instructions to be executed, resulting in non-execution or incorrect execution of certain parts of the program.

TECHNICAL FIELD

When a program is executed by a microprocessor, attacks for example by injecting faults via laser, glitch or electromagnetic radiation modify the instruction codes executed by the processor: the program instructions may be replaced by instructions producing a different effect. Consequently, a security processing sequence in an operating system for smart cards may be made inoperative by an attacker. Applied during an instruction sequence designed to write in non volatile memory of the card, these attacks may disable security writes used, for example, to count a number of incorrect authentications. Through this type of attack, the attacker also prevents the card from storing security-related events.

Amongst the known defences, one solution consists in setting flags in a byte of the RAM (Random Access Memory) at regular intervals and in checking, at a particular point in the execution of the software, that all flags which should be set have actually been set. Setting up this type of defence is tedious, however, since specific volatile memory areas must be allocated and processing added in the code to be protected, wherever this is required. In addition, since attacks of this type are becoming shorter and more precise, the known solutions are becoming less effective. Firstly, the attack may be too short to have any effect on the setting of flags: the flags in RAM may

indicate to the program that all writes have been made correctly, even if this is not the case. Secondly, the flag verification software may itself be disturbed.

One purpose of this invention is to protect all writes contained in the program.

Another purpose of this invention is to propose efficient protection even for very short attacks.

SUMMARY OF THE INVENTION

This invention concerns a method to secure the write in storage means of an electronic assembly comprising information processing means, said method comprising an atomic write process to write data recorded in a write log, characterised in that it consists in checking a sequence of atomic writes in said storage means by setting in said write log one or more indicators in memory as proof of one of more successive writes recorded in said log.

This invention also concerns an electronic module in which said method is implemented, a card comprising said module and a program to implement said method.

BRIEF DESCRIPTION OF THE DRAWINGS

Other purposes, features and advantages of the invention will appear on reading the description which follows of the implementation of the method according to the invention and of a mode of realisation of an electronic system designed for this implementation, given as a non-limiting example, and referring to the attached drawings in which:

- figure 1 is a diagrammatic representation of an example of a device in which the method according to this invention is implemented;

- figure 2 is a diagrammatic representation of the content of part of the memory of a device in which the known atomic write process is implemented;
- figure 3 is a graph representing the various steps of a known atomic write process;
- figure 4 is a graph representing the various steps of one form of realisation of the method according to this invention;
- figure 5 is a diagrammatic representation of the content of part of the memory of a device according to a first form of realisation in which the method according to this invention is implemented;
- figure 6 is a diagrammatic representation of the content of part of the memory of a device according to a second form of realisation in which the method according to this invention is implemented.

WAY OF REALISING THE INVENTION

The purpose of the method according to the invention is to secure an electronic assembly and for example a portable object such as a smart card implementing a program. The electronic assembly comprises at least processing means such as a processor and storage means such as a memory. The program to be secured is installed in the memory, for example ROM (Read Only Memory) type, of said assembly.

As a non-limiting example, the electronic assembly described below corresponds to an onboard system comprising an electronic module 1 illustrated on figure 1.This type of module is generally realised as a monolithic integrated electronic microcircuit, or chip, which once physically protected by any known means can be assembled on a portable object such as for example a smart card, microcircuit or integrated circuit card (microprocessor card, etc.) or other card which can be used in various fields.

The electronic module 1 comprises a microprocessor CPU 3 with a two-way connection via an internal bus 5 to a non volatile memory 7 of type

ROM, EEPROM (Electrical Erasable Programmable Read Only Memory), Flash, FeRam or other containing the program PRO 9 to be executed and a transaction buffer 10 containing a write log used for temporary data storage, a volatile memory 11 of type RAM, input/output means I/O 13 to communicate with the exterior.

The method according to the invention consists in checking that each write in non volatile memory while executing the program 9 is executed correctly.

The method according to the invention consists in checking the atomic write of data in non volatile memory by setting in a write log, when executing a program 9, an indicator in memory as proof of a write. The "write log" means the list of all write operations to be made atomically on the memory, the log containing control data and/or data to be written and/or any other type of information. A sequence of "atomic" writes means all writes recorded in the write log such that, if the log is validated (sequence closed), all the writes are made, even in the event of attack; if the log is not validated, none of said writes is made. According to this invention, writing the indicator in memory is made atomic with the write of the planned data in the write log.

Each write in the log and the indicator are atomic, so the fact that the proof indicator is in memory guarantees that the data has actually been written. By checking that the proof indicator is present, the program ensures a posteriori that the write was made. If the write was not made, various measures can then be taken, such as, for example, triggering by program 9 of a security defence, interruption of program execution or setting of a fraud indicator in non volatile memory 7 to indicate that a fraudulent attack has taken place and for example to prohibit any future use of the operating system.

The methods used to make several atomic writes in the memory and more especially in the non volatile memory 7 of a microprocessor card as an anti-tearing mechanism are known. They use for example, as shown on figure 2, the transaction buffer 10; the transaction buffer 10 is located in the non volatile memory 7 and acts as log for the writes to be made.

The known atomic write process may consist of the following sequence (refer to figure 3):

After opening the atomic session (step A), for each write (step B), the process consists in creating (step C) an entry in the write log of the transaction buffer 10 comprising the control data (Control Data) (address Adr1, Adr2, Adr3,..., length of useful data, L1, L2, L3, ..., ...) and the useful data (Data) (Data1, Data2, Data3, ...) (see figure 2).

When closing the atomic session (step D), the process validates the transaction buffer to indicate that it contains an atomic write sequence.

The method then consists in reading (steps E, G) each entry in the log and making, then checking the corresponding write, repeating each incorrect write (step F). Then in step H, the method invalidates the transaction buffer to indicate that it contains no atomic write sequence.

If the writes of the atomic sequence are interrupted, the process resumes at step E as long as the transaction buffer has not been invalidated.

This type of atomic write process protects against an interruption in the atomic session in progress: it guarantees that

- either the writes recorded in the write log of the transaction buffer are ignored and none of the writes recorded is made if the session has not been closed;
- or all the writes recorded in the log of the transaction buffer are made if the session has been closed.

However, this type of process does not protect against disturbances in system operation which allow the session to continue: one of the writes planned in the atomic session could be prevented without being detected by the atomicity mechanism.

The method according to this invention therefore consists in combining the known atomic data write process with the write of a write indicator. The indicator is entered in the write log. The data and indicator writes are made atomic...

The mode of realisation of this invention described below and illustrated on figure 4 combines the atomicity process like that described

above and a counter acting as indicator of the successive writes in non volatile memory during a command, and for example a counter of the number of writes which is incremented on each new write.

As shown on figure 5, according to one form of realisation of the invention, the value (Counter) of the write counter (C1, C2, C3) in EEPROM is included in the block of control data of the write log of the atomicity process (Control Data). According to another form of realisation illustrated on figure 6, the value of the write counter is included in the atomicity data of the write log of the atomicity process (Atomicity Data). For each new write in the atomic session, the counter is incremented (step C- figure 4) and the control and atomicity data are updated in the same block, under the protection of a checksum (CKS1, CKS2, CKS3 on figure 5 or CKS on figure 6, depending on the form of realisation) on part or all of the data (step C). The counter is incremented on each new write in the atomic session. The atomicity process guarantees that once the atomic session has been closed, all the writes recorded in the log will be made completely. This mode of realisation guarantees that each incrementation of the counter is atomic with the corresponding write in the log. When closing the atomic session in progress, each incrementation of the counter during the atomic session corresponds to a write actually made when closing the atomic session.

As shown on figure 4 therefore, after opening the atomic session, on each new write, i.e. on each new entry in the write log of the transaction buffer 10, the counter is incremented (step C). Depending on the form of realisation, the new value of the counter is written with the control data of the entry concerned (C1, figure 5) or in the atomicity data (Ci, figure 6). The value of the counter before opening the atomic session is stored in the atomicity data (C, figure 6). When closing the atomic session, the value of the counter is compared with the expected value and if they match and the other checks planned in the known atomic write processes are also correct, the buffer is validated. The value of the counter C before opening the session is then assigned the value of the counter at closure.

This form of realisation implementing a counter provides a means of

checking during program execution and/or when closing the atomic session that the writes planned in the log have been made by comparing the actual value of the counter with the expected value.

The method according to the invention consists in incrementing said counter and making each atomic write simultaneously. If an attack occurs during the write, the write will not be made correctly, the counter will not be incremented and the value of the counter will be different from the expected value; the attack is therefore detected and a specific action is carried out by the program or the processor.

Two methods can be used to make the recording of a new write in the write log of the transaction buffer and the incrementation of the write counter in non volatile memory atomic:

- the counter is placed in the same block as all or some of the control and/or atomicity data and/or the useful data of the atomicity process; and/or
- the counter and all or some of the control and/or atomicity data and/or the useful data are protected by the same checksum which validates this write,

either of the two methods alone is sufficient to guarantee atomicity. The writes in the non volatile memory 7 of type EEPROM generally encountered in smart cards, are made in blocks (usually 64 or 128 bytes). All the bytes programmed in a given block are written simultaneously, making the write of several bytes in the same block atomic. The programming duration is the same, whether for a single byte in the block or for all bytes in the block, of the order of 1 to 5 ms. This duration must be multiplied by the number of blocks to be written.

Atomicity can be achieved by using this intrinsic property of EEPROM. By placing the proof indicator of a write in the same block as the data to be written in the write log, if the proof indicator is present we can be certain that the data has actually been written.

Placing the write counter in the same block as the control and/or atomicity data and/or the useful data of the atomicity process helps improve

the performance of the protection mechanism. No extra block writes are required, which helps to limit the number of writes.

The method according to the invention consists according to the second method in calculating a checksum (CKS1, CKS2, CKS3 on figure 5, CKS on figure 6) on the value of the counter and on all or some of the control and/or atomicity data and/or the useful data and making the write in the log simultaneously and in writing the value obtained for the checksum in the log. The method according to the invention then consists in verifying the checksum by comparing it with the precalculated value written in memory. Note that the checksum may concern the indicator and all or some of the useful data, and/or one or more items of atomicity data and/or one or more items of control data depending on the form of realisation chosen. The protection of the write counter and of the control data by a checksum guarantees the efficiency of the mechanism with any non volatile memory and for example with memory types other than EEPROM.

CLAIMS

1- Method to secure the write in storage means (7) of an electronic assembly comprising information processing means, said method comprising an atomic write process to write data recorded in a write log, characterised in that it consists in checking a sequence of atomic writes in said storage means by setting in said write log one or more indicators in memory as proof of one or more successive writes recorded in said log.

2- Method according to claim 1, characterised in that it consists in making the write of the data in the log and that of the indicator are atomic.

3- Method according to claim 1 or 2, characterised in that it consists in protecting said indicator and the data in the write log with the same checksum when writing said indicator and said data.

4- Method according to one of claims 1 to 3, characterised in that the atomicity of the writes is increased by using a property of some memories according to which the writes are made in blocks, said indicator being placed in the same block as the data to be written in the log.

5- Method according to one of claims 1 to 4, characterised in that it consists in setting said indicator by incrementing a counter on each new write.

6- Method according to claim 5, characterised in that it consists in placing the value of said counter in the same block of data to be written as the control and/or atomicity data and/or the useful data of the write log.

7- Method according to one of claims 1 to 6, characterised in that it consists in triggering an action if the write of said data is not made.

8- Electronic module including information processing means and storage means containing a program to be executed and a write log recording the writes of an atomic write process, characterised in that the information processing means include means, when executing the program, to set in said write log one or more indicators in memory as proof of one or more successive writes recorded in said log.

9- Card characterised in that it comprises the electronic module according to claim 8.

10- Computer program comprising program code instructions to execute the steps of the method according to one of claims 1 to 7 when said program is run in an electronic assembly.

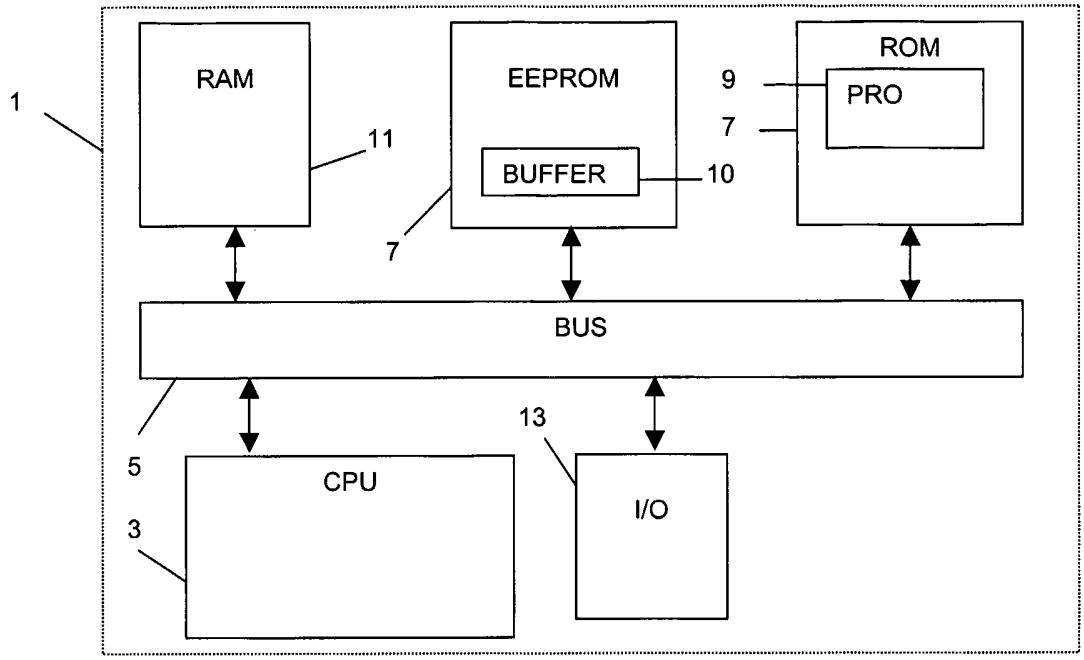

1
RAM
11
EEPROM
BUFFER
10
7
ROM
9
PRO
7
BUS
5
3
CPU
13
I/O

FIG. 1

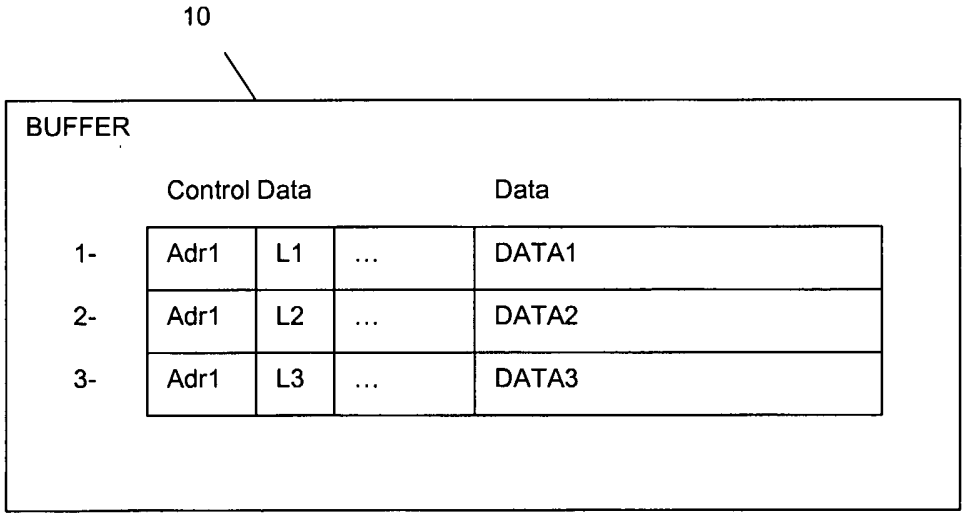

10
BUFFER
Control Data
Data
1- Adr1 L1 ... DATA1
2- Adr1 L2 ... DATA2
3- Adr1 L3 ... DATA3

FIG.2

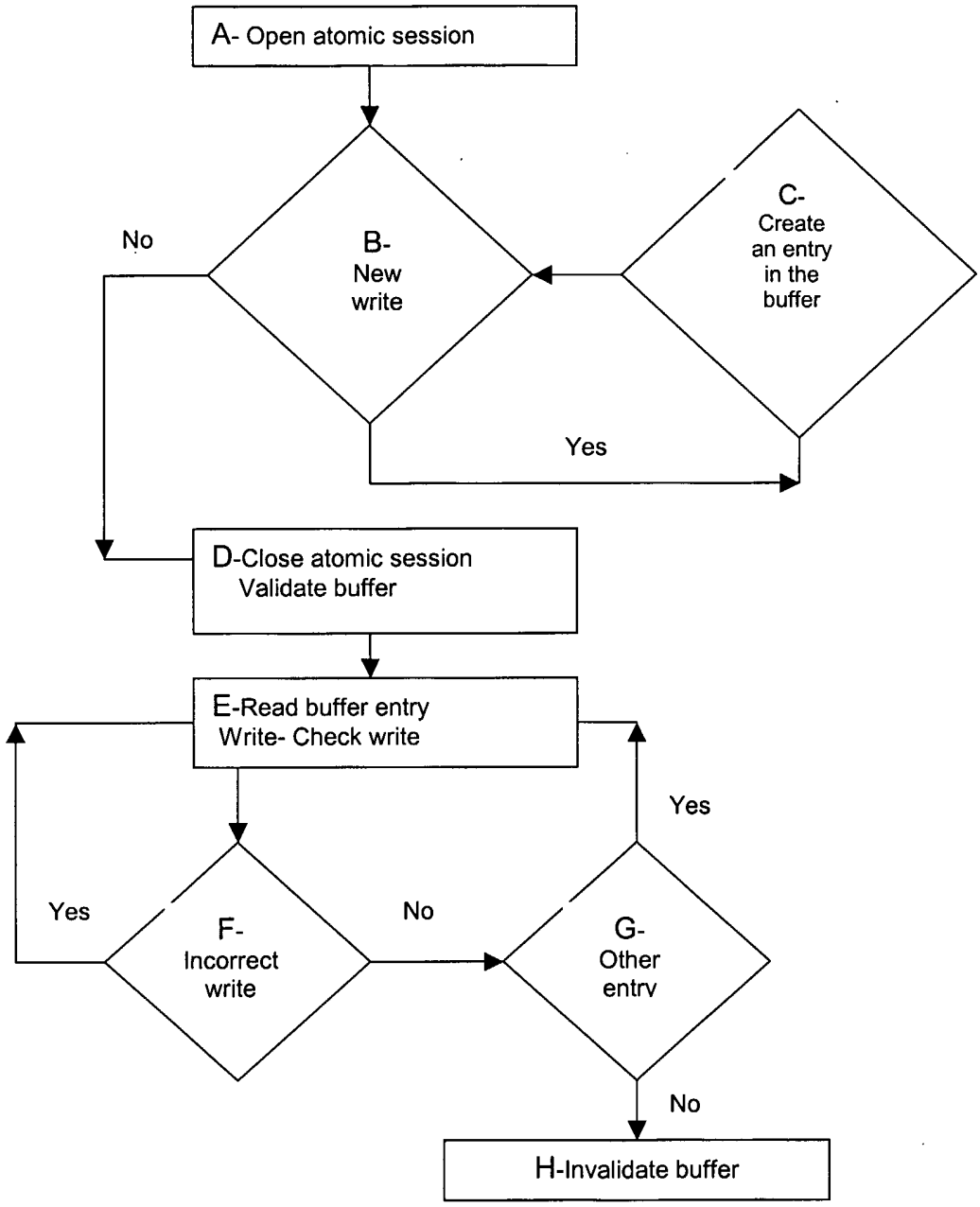

A- Open atomic session
B- New write
C- Create an entry in the buffer
No
Yes
D-Close atomic session Validate buffer
E-Read buffer entry Write- Check write
F- Incorrect write
G- Other entrv
Yes
No
Yes
No
H-Invalidate buffer

FIG.3

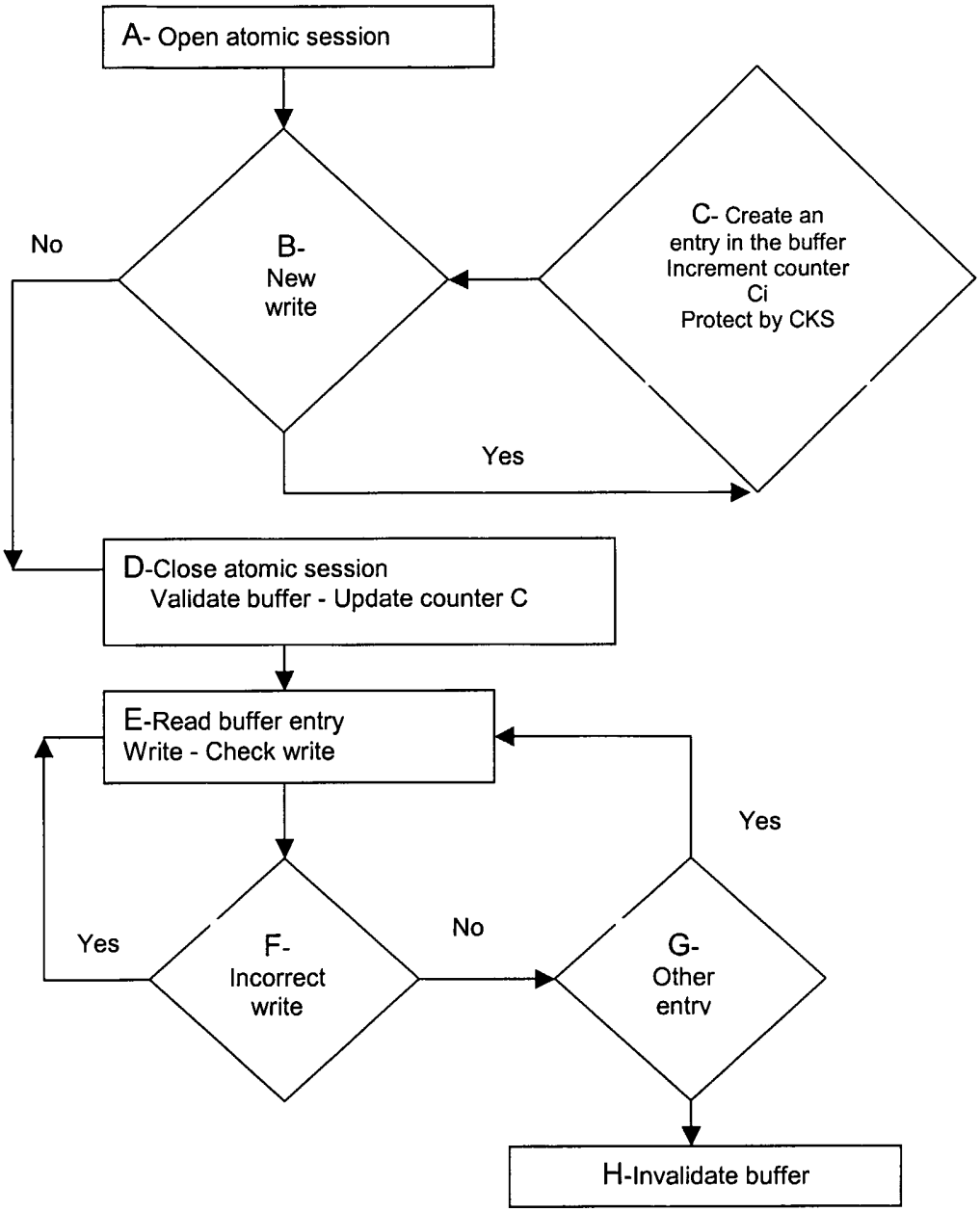

A- Open atomic session
B-
New
write
No
C- Create an
entry in the buffer
Increment counter
Ci
Protect by CKS
Yes
D-Close atomic session
Validate buffer - Update counter C
E-Read buffer entry
Write - Check write
F-
Incorrect
write
Yes
No
G-
Other
entry
Yes
H-Invalidate buffer

FIG.4

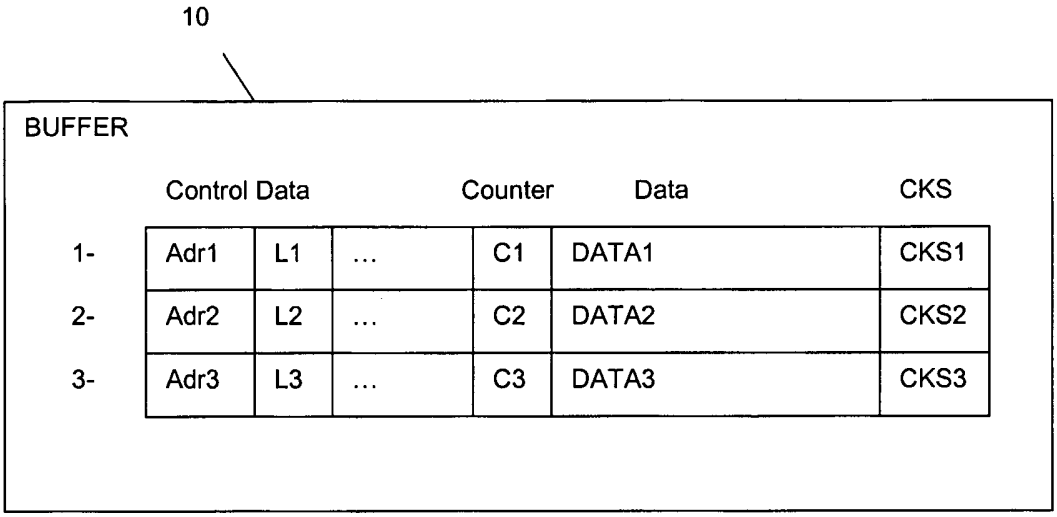

10
BUFFER
Control Data
Counter
Data
CKS
1-
Adr1
L1
...
C1
DATA1
CKS1
2-
Adr2
L2
...
C2
DATA2
CKS2
3-
Adr3
L3
...
C3
DATA3
CKS3

FIG.5

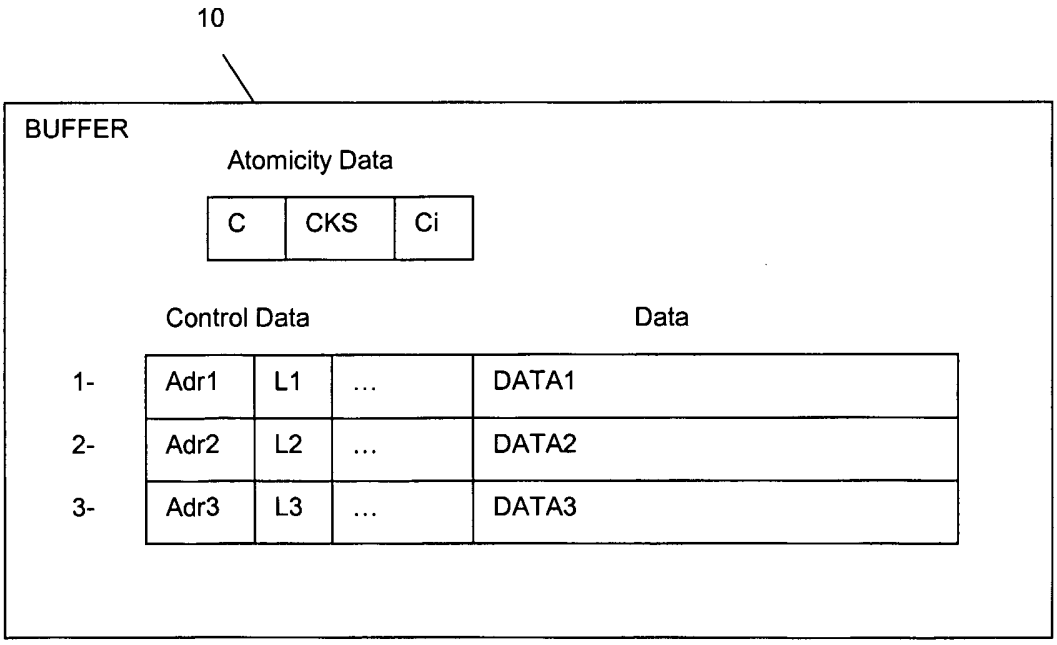

10
BUFFER
Atomicity Data
C
CKS
Ci
Control Data
Data
1-
Adr1
L1
...
DATA1
2-
Adr2
L2
...
DATA2
3-
Adr3
L3
...
DATA3

FIG.6

INTERNATIONAL SEARCH REPORT

Int onal application No
PCT/IB2005/003476

A. CLASSIFICATION OF SUBJECT MATTER
G11C16/10 G06F11/14 G06F11/00 G11C16/22

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)
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)
EPO-Internal, PAJ, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 715 431 A (EVERETT ET AL) 3 February 1998 (1998-02-03) column 7, line 5 - column 8, line 21; figures 1,5,6	1-3,5, 7-10
A	FR 2 742 893 A (SCHLUMBERGER INDUSTRIES SA) 27 June 1997 (1997-06-27) page 7, line 1 - line 7; claims 10,11; figure 3	1,3-6, 8-10
A	US 5 532 463 A (DEBELLEIX ET AL) 2 July 1996 (1996-07-02) figure 1	1,8-10
A	US 4 507 751 A (GAWLICK ET AL) 26 March 1985 (1985-03-26) column 4, line 10 - column 5, line 33; figures 1-3	1,8-10

-/--

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

[X] See patent family 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
20 March 2006	29/03/2006

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Cummings, A

INTERNATIONAL SEARCH REPORT

Int ional application No
PCT/IB2005/003476

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	"WRITE ATOMICITY WITH STORAGE HARDWARE" IBM TECHNICAL DISCLOSURE BULLETIN, IBM CORP. NEW YORK, US, vol. 33, no. 2, 1 July 1990 (1990-07-01), pages 422-425, XP000123669 ISSN: 0018-8689	

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int ional application No
PCT/IB2005/003476

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5715431 A	03-02-1998	AT 219857 T	15-07-2002
		AU 676731 B2	20-03-1997
		AU 6507794 A	08-11-1994
		BR 9404989 A	15-06-1999
		CA 2137683 A1	27-10-1994
		CN 1110488 A	18-10-1995
		DE 69430859 D1	01-08-2002
		EP 0645046 A1	29-03-1995
		WO 9424673 A1	27-10-1994
		JP 7508120 T	07-09-1995
		MD 960344 A	30-06-1997
		PL 306763 A1	18-04-1995
		RU 2146399 C1	10-03-2000
		ZA 9402553 A	05-06-1995
FR 2742893 A	27-06-1997	NONE	
US 5532463 A	02-07-1996	AT 192602 T	15-05-2000
		DE 69424223 D1	08-06-2000
		DE 69424223 T2	04-01-2001
		EP 0630027 A1	21-12-1994
		ES 2146642 T3	16-08-2000
		FR 2705820 A1	02-12-1994
US 4507751 A	26-03-1985	DE 3379754 D1	01-06-1989
		EP 0098928 A2	25-01-1984
		JP 58223856 A	26-12-1983