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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 February 2005 (10.02.2005)

PCT

(10) International Publication Number
WO 2005/013272 A1

(51) International Patent Classification[7]: G11B 20/00

(21) International Application Number:
PCT/IB2004/051303

(22) International Filing Date: 28 July 2004 (28.07.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
03102396.3 1 August 2003 (01.08.2003) EP

(71) Applicant *(for all designated States except US)*: **KONINKLIJKE PHILIPS ELECTRONICS N.V.** [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **STARING, Antonius, A., M.** [NL/NL]; c/o Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). **SKORIC, Boris** [NL/NL]; c/o Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). **TREFFERS, Menno, A.** [NL/NL]; c/o Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). **MAES, Maurice, J., J., J-B.** [NL/NL]; c/o Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(74) Agent: **BEKKERS, Joost, J., J.**; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(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, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

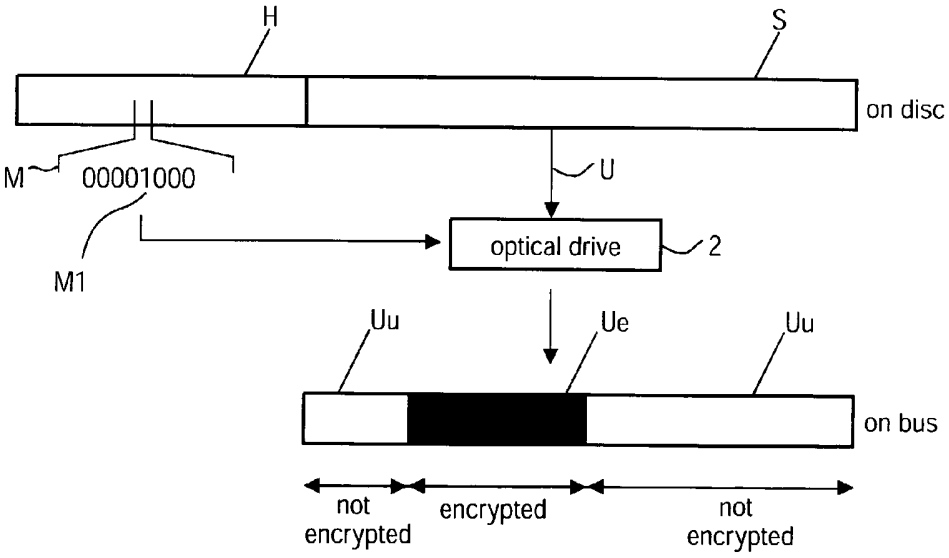
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, 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).

Declaration under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ,*

[Continued on next page]

(54) Title: RECORD CARRIER COMPRISING ENCRYPTION INDICATION INFORMATION



(57) Abstract: The present invention relates to a record carrier (10) for storing user data in sectors (S) and management information (n) associated with said sectors. In order to provide a simple, low-cost, flexible and secure copy protection of the user data when being transmitted over a communication bus (6) of a PC it is proposed according to the present invention that the management information comprises an encryption indication information (M1) indicating that the user data stored in the associated sector (S) are to be encrypted by a read-out device (2) before being transmitted over a communication bus (6).

WO 2005/013272 A1

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, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

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.

Record carrier comprising encryption indication information

The present invention relates to a record carrier for storing user data in sectors and management information associated with said sectors. The present invention relates further to a read-out device for reading data from a record carrier and a corresponding read-out method. Still further, the present invention relates to a recording device and a corresponding recording method for recording data on a record carrier. Finally, the present invention relates to a computer program for implementing said methods.

Optical disc drives connect with other components in a personal computer (PC) via a communication bus, in particular a so-called PCI-bus. It is easy for hackers to listen to the communication over this bus and to get access to transmitted user data. A so-called bus encryption, according to which user data are encrypted before transmission over the communication bus and decrypted by the receiving component after transmission, is generally used to protect data transmission against eavesdropping. However, bus encryption requires significant computational effort which degrades the performance of application or increases the costs of such systems. The computational efforts could be reduced by not encrypting all user data in all sectors, but only encrypting a few sectors or part of the user data in a sector, or by choosing an encryption algorithm that requires less computational effort. Such measures would, however, weaken the protection.

Since different applications have different security requirements, and a single optical drive has to read and to protect data for many different applications, it is thus a problem to make an optical disc drive or, more generally, to provide a read-out device for reading data from a record carrier, that satisfies all needs with a single bus encryption method. In particular, this flexible security level shall be provided to protect user data during transmission over the communication bus when the user data is recorded on a record carrier, such as a recordable optical disc.

Many copy protection methods have been created to prevent copying of user data. One of these methods is based on so-called re-encryption according to which some sectors of the disc are encrypted and which will be decrypted by the drive before transmitting it via a secure communication channel to another component in a PC. The advantage of re-encryption is that the key used by the drive to decrypt the sector does not leave the drive and

is therefore not easily discovered by hackers. However, the decryption of the encrypted sector requires significant computational effort which degrades the performance of the drive or increases the costs thereof. Although the computational effort can be reduced by the same measures as mentioned above, the strength of the protection will be weakened.

Since different applications have different security requirements it is therefore desired to provide a low-cost read-out device that is optimized for the security level of a single application and a general purpose read-out device that provides the right security level for all applications and can read record carriers for all applications. A method is therefore needed by which a general-purpose read-out device can determine if and, preferably, what type of encryption is to be used. Preferably, an additional information indicating if and which kind of decryption is required before encryption, should be provided.

It is thus an object of the present invention to provide a record carrier, a recording device and method as well as a read-out device and method which provide a flexible security level to protect user data during transmission over the communication bus, also when the data is recorded on a record carrier such as a recordable optical disc.

This object is achieved according to the present invention by a record carrier as claimed in claim 1 according to which the management information comprises an encryption indication information indicating that the user data stored in the associated sector are to be encrypted by a read-out device before being transmitted over a communication bus.

A read-out device for reading data from such a record data is defined in claim 7 and comprises a data interpreter for interpreting said management information, an encryption unit for encrypting user data of sectors for which the associated encryption indication information indicates that said user data are to be encrypted and an output unit for outputting said user data.

A recording device for recording data on such a record carrier is defined in claim 10 and comprises:

an input unit for receiving user data and a command to record said user data in sectors on a record carrier from a communication bus,

a command interpreter for interpreting said command so as to identify a decryption indication information included therein indicating which parts of the received user data are encrypted and are to be decrypted before recording on said record carrier,

a decryption unit for decrypting the parts of said user data for which the associated decryption indication information indicates that they are encrypted and are to be decrypted before recording on said record carrier, and

a write unit for recording said user data in sectors on said record carrier and a management information associated with said sectors comprising an encryption indication information indicating that user data stored in sectors associated with said management information are to be encrypted by a read-out device before transmission over a communication bus.

Corresponding methods are defined in claims 9 and 11. A computer program for implementing said methods is defined in claim 13.

The present invention is based on the idea to signal to the read-out device that particular user data shall be encrypted by the read-out device before they can be transmitted over the communication bus, in particular a PCI-bus of PC. An encryption indication information is thus provided in the management information and associated with all sectors in which user data are stored which shall be encrypted before transmission over the communication bus. This encryption indication information will be read and evaluated by the read-out device which then encrypts the associated user data before they are outputted to the communication bus. The recording device according to the present invention is adapted such that during recording of user data such encryption indication information is assigned to the user data and also recorded on the record carrier for later read-out by the read-out device. Such encryption indication information is written based on a corresponding decryption indication information included in a command received by the recording device along with the instruction to record particular user data on a record carrier. The invention thus provides a simple, flexible and low-cost solution providing copy protection during transmission of user data over a communication bus which are read from a record carrier.

It should be noted that user data shall be understood as including any kind of data that are stored on a record carrier and can be transmitted over a communication bus, i.e. not only include data that are particularly meant for a user, such as audio, video or software data, but also include any other kind of data such as management data or control data.

Preferred embodiments of the invention are defined in the dependent claims. According to a simple embodiment the management information is stored in the sector header of each sector and the encryption indication information is a single bit which is used to trigger encryption of user data stored in the associated sector. However, the management information can be also stored in a separate (additional) sub-code channel besides the normal data channel.

According to further embodiments the management information comprises additional information indicating which part or parts of the user data are to be encrypted, which encryption algorithm is to be used for encryption, which key-hierarchy is to be used

for determination of an encryption key to be used for encryption and/or indicating that the user data stored in the associated sectors are to be decrypted by the read-out device before being encrypted again for transmission. Again, these indicators could be single bits stored in the sector header. Preferably, the indication information that triggers bus-encryption is made independent from the indication information that triggers sector decryption because the security requirements for both methods may be different. If the triggers for bus encryption and sector decryption are independent, preferably the integrity of at least the bus encryption trigger is protected. This can be achieved by, e.g., making the sector decryption key dependent on at least the bus encryption trigger (for example XOR or hash the trigger into the key).

The invention will now be explained in more detail with reference to the drawings in which

Fig. 1 shows a block diagram of a PC,

Fig. 2 shows a block diagram of a read-out and recording device according to the invention,

Fig. 3 illustrates a first embodiment of the invention,

Fig. 4 illustrates the first embodiment of the invention with a different parameter setting,

Fig. 5 illustrates a second embodiment of the invention,

Fig. 6 illustrates a third embodiment of the invention and

Fig. 7 illustrates a fourth embodiment of the invention.

Fig. 1 shows a block diagram of a PC 1 comprising a drive 2, for instance an optical disc drive, capable of reading data from a record carrier 10 and capable of writing data to said record carrier 10, a CPU (Central Processing Unit) 3, a memory 4 and a graphics card 5 all connected to a communication bus 6. For simplicity's sake no further details of the PC 1 are shown which may, of course, comprise further and other components as well.

Fig. 2 shows a block diagram of a drive 2 according to the present invention. For reading data from the record carrier 10 a reading unit 21 is provided; for writing data to said record carrier 10 a writing unit 22 is provided. When reading user data U from the record carrier 10 which are stored in sectors S, as shown in Fig. 3 by way of example of an optical

disc having sectors of 2048 bytes length each, associated management information M stored in the sector header H associated to each sector S and, in this example, having n bytes, is read as well and forwarded to a data interpreter 23. Therein, the management information M, in the example shown in Fig. 3 being one byte comprising 8 bits, are evaluated in order to determine if the read user data stored in the associated sector S shall be encrypted by an encryption/decryption unit 24 before output by an output unit 25 and subsequent transmission over the communication bus 6.

In the embodiment shown in Fig. 3 the management information M only includes zero-bits meaning that no encryption of user data U is required before transmission over the communication bus. Thus, the user data will be directly outputted by the output unit 25 to the communication bus 6, i.e. the user data U will be communicated over the bus 6 in unencrypted form as shown in Fig. 3. In the embodiment shown in Fig. 4, the encryption indication information M1 included in the management information M indicates, by setting a one-bit, that the user data U stored in the sector S are to be encrypted before being outputted. Thus, the read user data U will be forwarded to the encryption/decryption unit 24 where they are encrypted, before being afterwards outputted to the communication bus. In this embodiment, only a fixed part Ue of the user data of the sector S is encrypted while other parts Uu are communicated in unencrypted form.

In the embodiment shown in Fig. 5 already part Se of the user data U stored on the record carrier in sector S is encrypted while other parts Su of the sector S are not encrypted. In the associated management information M, besides the encryption indication information M1, an additional decryption indication information M2 is included indicating that (part of) the user data U stored in the sector S need to be decrypted first before again encrypted (indicated by M1) and transmitted over the communication bus. Preferably, the decryption key of the encrypted part Se is dependent on the first indicator M1 (and optionally also on indicator M2). Thus, the encryption/decryption unit 24 first decrypts the encrypted portion Se of the sector S before part of the completely unencrypted user data U of the sector S are encrypted and transmitted over the bus. Preferably, different encryption/decryption keys and/or encryption/decryption algorithms are used for these two steps of decryption/encryption provided according to this embodiment.

The management information may further include additional information, such as an information indicating the amount of user data that needs to be decrypted before encryption, which algorithm to use for decryption and/or which key hierarchy to use for decryption.

According to still another embodiment as shown in Fig. 6 an additional encryption amount information M3 is provided as additional management information in the sector header A indicating which parts of the sector S must be encrypted by the drive 2. For instance, as shown in Fig. 6, three parts of the sector S which shall be encrypted (Ue) are indicated by the encryption amount information M3 while other parts of the sector remain unencrypted (Uu) before being transmitted over the bus.

Further information can be included in the management information, such as for instance an encryption algorithm information M4 indicating which encryption algorithm is to be used for encryption and/or a key hierarchy information M5 indicating which key-hierarchy is to be used for determination of an encryption key to be used for encryption.

The embodiment of the drive 2 shown in Fig. 2 further comprises a data/command interpreter 26 and an input unit 27 for reception of data from the communication bus 6. These units will be used for recording of data to the record carrier 10. In this case a command instructing the drive 2 to record particular user data is received along with that user data by the input unit 27 and is evaluated by the data/command interpreter 26. This embodiment is illustrated in Fig. 7 where the command C comprises a decryption indication information C2 (similar to M2 shown in Fig. 5) indicating that encrypted user data Ue received from the bus 6 need to be decrypted and an encryption indication information C1 indicating that (part of) the whole user data need to be encrypted before storage on the record carrier. In this case the integrity of at least the trigger for sector encryption (C1) must be protected. This can be achieved by, e.g., making the bus decryption key dependent on at least the sector encryption trigger (for example XOR or hash the trigger into the key).

These steps of encryption and decryption will be done by the encryption/decryption unit 24 before the partly encrypted user data are written to the record carrier 10 by the write unit 22. At the same time an appropriate management information M including indicators M1 and M2 is recorded in the sector header H. Of course, additional further information, similar to the additional further information illustrated above for the management information, can also be included in the command C.

According to the invention a simple, low-cost, flexible and secure solution for protection of user data stored on a record carrier before transmission over a communication bus of a PC is provided.

CLAIMS:

1. Record carrier (10) for storing user data in sectors (S) and management information (M) associated with said sectors (S), wherein said management information (M) comprises an encryption indication information (M1) indicating that the user data stored in the associated sector (S) are to be encrypted by a read-out device (2) before being transmitted over a communication bus (6).

2. Record carrier as claimed in claim 1, wherein said management information (M) is stored in a sector header (4) or in an additional sub-code channel.

3. Record carrier as claimed in claim 1, wherein said management information (M) further comprises an encryption amount information (M3) indicating which part or parts of the user data stored in the associated sector (S) are to be encrypted.

4. Record carrier as claimed in claim 1, wherein said management information (M) further comprises an encryption algorithm information (M4) indicating which encryption algorithm is to be used for encryption.

5. Record carrier as claimed in claim 1, wherein said management information (M) further comprises a key-hierarchy information (M5) indicating which key-hierarchy is to be used for determination of an encryption key to be used for encryption.

6. Record carrier as claimed in claim 1, wherein said management information (M) further comprises a decryption indication information (M2) indicating that the user data stored in the associated sector (S) are to be decrypted by the read-out device (2) before being encrypted again for transmission over said communication bus (6).

7. Record carrier as claimed in claim 6, wherein a decryption key for decryption of the user data is dependent on at least the encryption indication information (M1).

8. Read-out device for reading data from a record carrier (10) storing user data in sectors (S) and management information (M) associated with said sectors (S), wherein said management information (M) comprises an encryption indication information (M1) indicating that the user data stored in the associated sector (S) are to be encrypted by a read-out device (2) before being transmitted over a communication bus (6), comprising:
a reading unit (21) for reading said user data and said management information (M) from said record carrier (10),
a data interpreter (23) for interpreting said management information (M),
an encryption unit (24) for encrypting user data of sectors (S) for which the associated encryption indication information (M1) indicates that said user data are to be encrypted and
an output unit (25) for outputting said user data.

9. Read-out method for reading data from a record carrier (10) storing user data in sectors (S) and management information (M) associated with said sectors (S), wherein said management information (M) comprises an encryption indication information (M1) indicating that the user data stored in the associated sector are to be encrypted by a read-out (2) device before being transmitted over a communication bus (6), comprising the steps of:
reading said user data and said management information (M) from said record carrier (10),
interpreting said management information (M),
encrypting user data of sectors (S) for which the associated encryption indication information (M1) indicates that said user data are to be encrypted and
outputting said user data.

10. Recording device for recording data on a record carrier (10) comprising:
an input unit (27) for receiving user data and a command (C) to record said user data in sectors (S) on a record carrier (10) from a communication bus (6),
a command interpreter (26) for interpreting said command (C) so as to identify a decryption indication information (C2) included therein indicating which parts of the received user data are encrypted and are to be decrypted before recording on said record carrier (10),
a decryption unit (24) for decrypting the parts of said user data for which the associated decryption indication information (M2) indicates that they are encrypted and are to be decrypted before recording on said record carrier (10), and
a write unit (22) for recording said user data in sectors (S) on said record carrier (10) and a management information (M) associated with said sectors (S) comprising an encryption

indication information (M1) indicating that user data stored in sectors (S) associated with said management information (M) are to be encrypted by a read-out (2) device before transmission over a communication bus (6).

11. Recording method for recording data on a record carrier (10) comprising the steps of:

receiving user data and a command (C) to record said user data in sectors (S) on a record carrier (10) from a communication bus (6),

interpreting said command (C) so as to identify a decryption indication information (C2) included therein indicating which parts of the received user data are encrypted and are to be decrypted before recording on said record carrier (10),

decrypting the parts of said user data for which the associated decryption indication information (C2) indicates that they are encrypted and are to be decrypted before recording on said record carrier (10), and

recording said user data in sectors (S) on said record carrier (10) and a management information (M) associated with said sectors (S) comprising an encryption indication information (M1) indicating that user data stored in sectors (S) associated with said management information (M) are to be encrypted by a read-out (2) device before transmission over a communication bus (6).

12. Recording method as claimed in claim 11, wherein said command (C) further comprises an encryption indication information (C1) and that a decryption key for decryption of the user data is dependent on said encryption indication information (C1).

13. Computer program comprising program code means for causing a computer to carry out the steps of the methods as claimed in claims 9 and 11 when said computer program is executed on a computer.

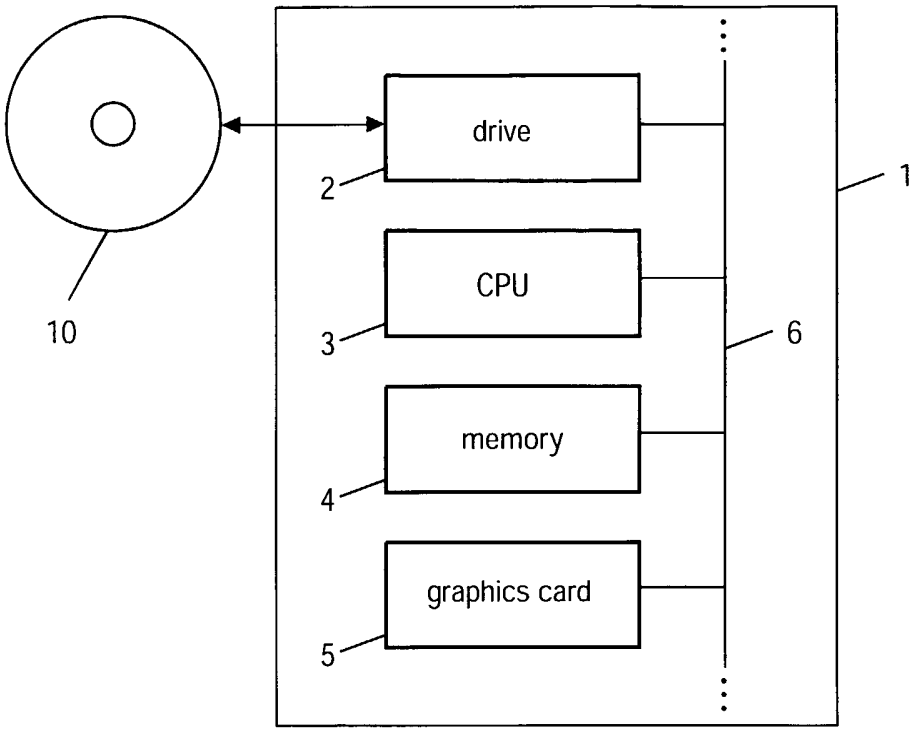


FIG.1

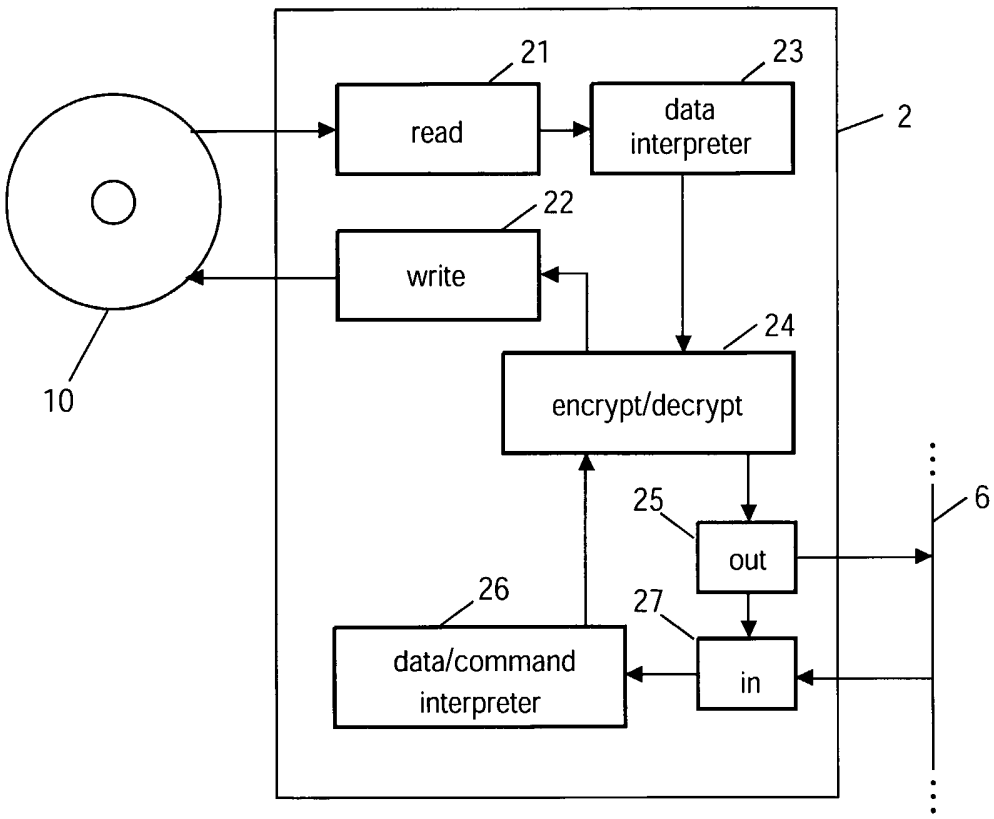

21
23
read
data interpreter
2
22
write
24
encrypt/decrypt
10
25
6
out
26
27
data/command interpreter
in

FIG.2

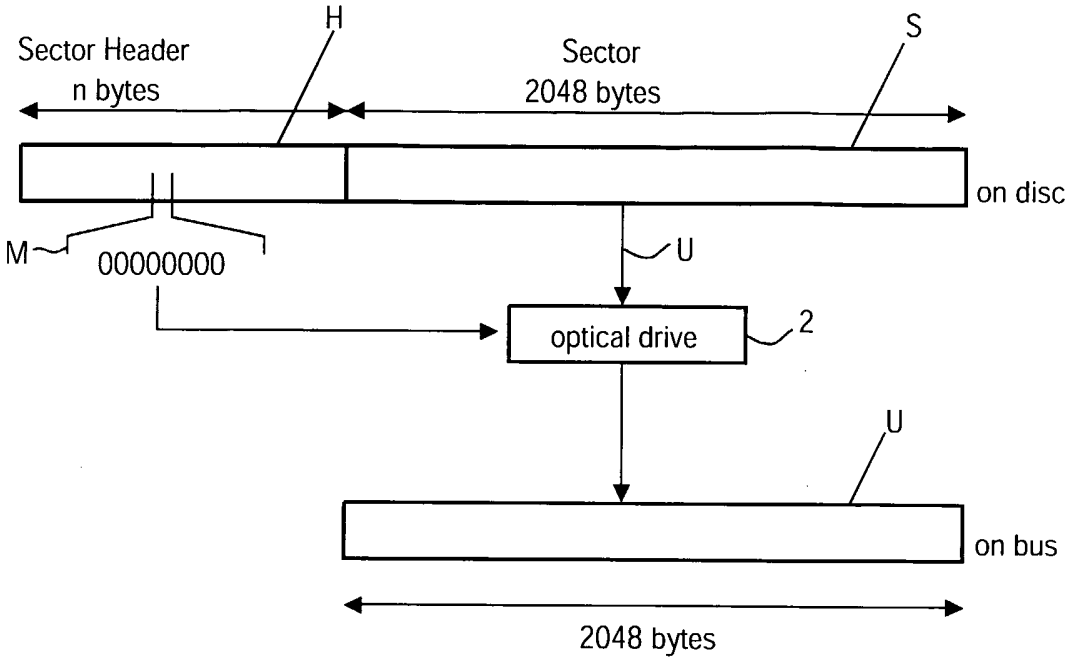

H
S
Sector Header
n bytes
Sector
2048 bytes
on disc
M
00000000
U
optical drive
2
U
on bus
2048 bytes

FIG.3

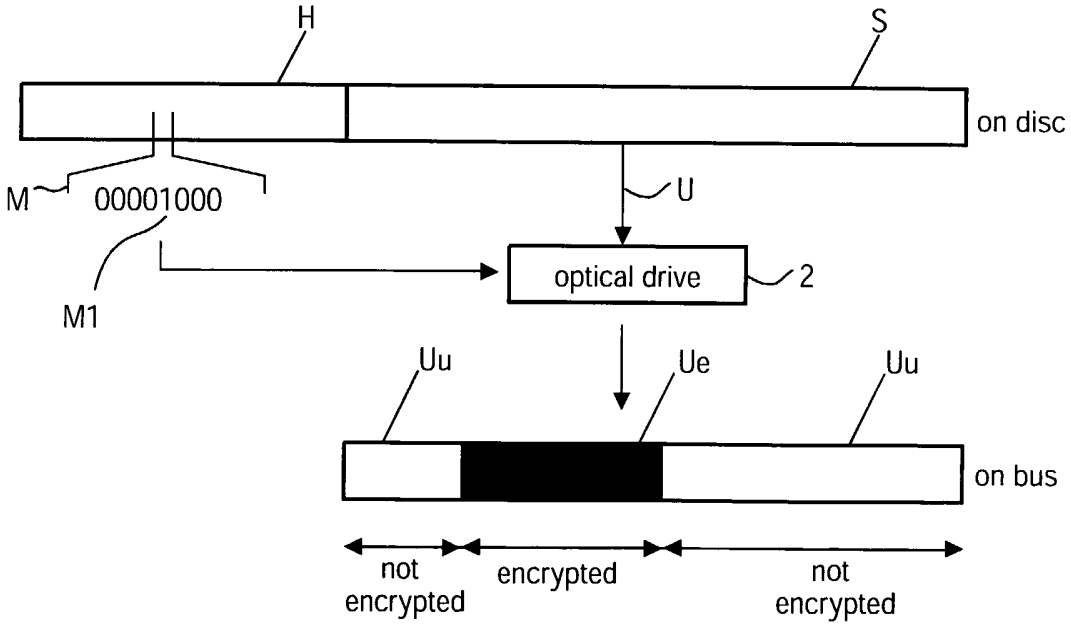

H
S
on disc
M
00001000
U
optical drive
2
M1
Uu
Ue
Uu
on bus
not
encrypted
encrypted
not
encrypted

FIG.4

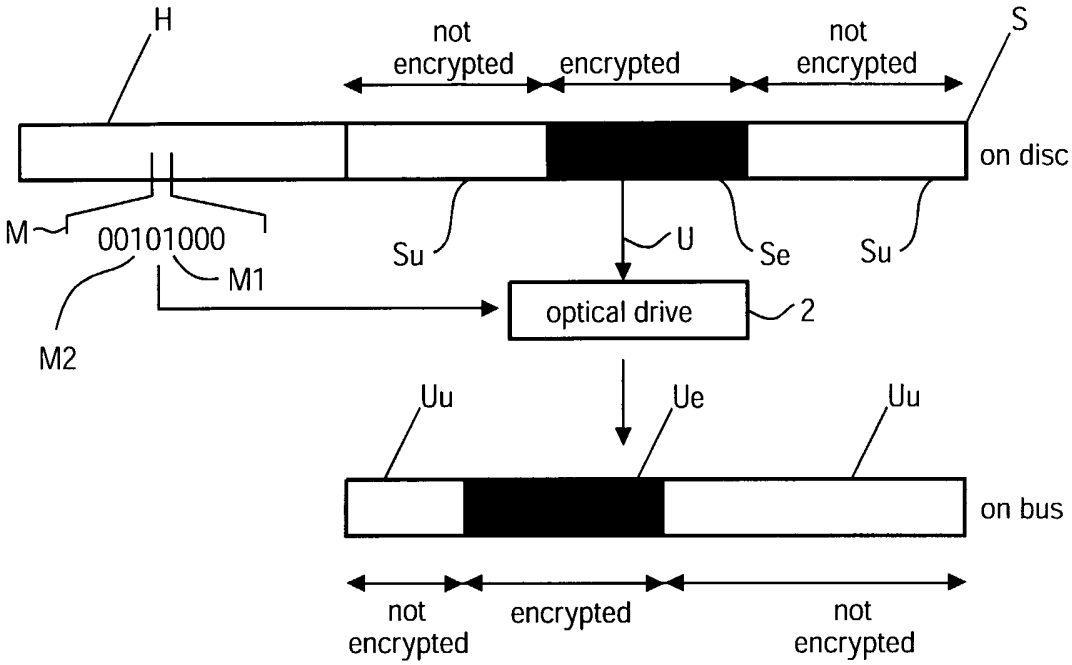

H
not encrypted
encrypted
not encrypted
S
on disc
M
00101000
M1
M2
Su
U
Se
Su
optical drive
2
Uu
Ue
Uu
on bus
not encrypted
encrypted
not encrypted

FIG.5

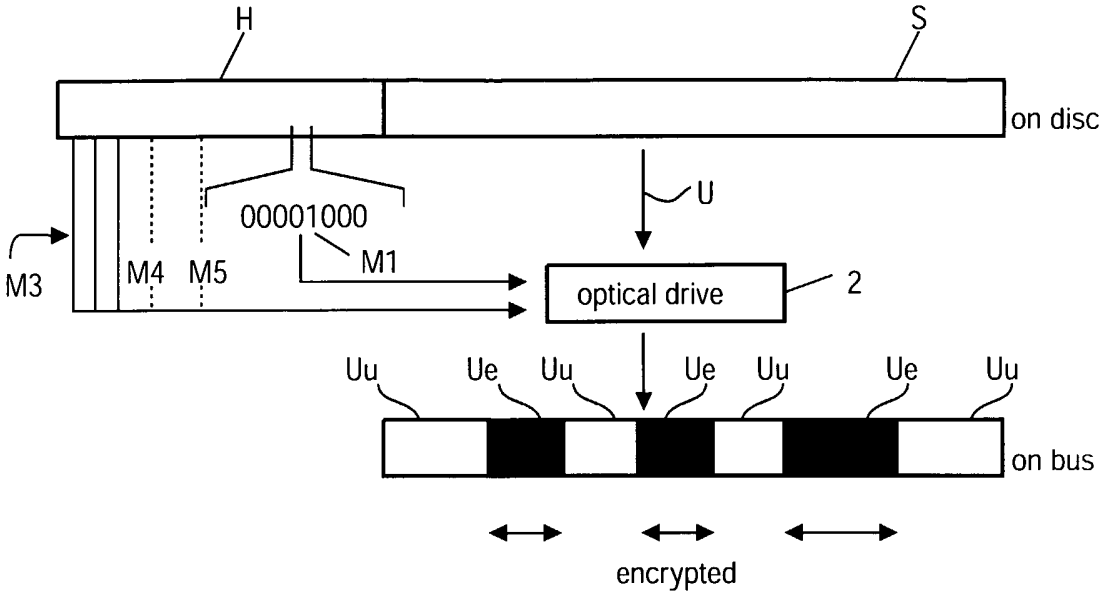

H
S
on disc
U
00001000
M1
M3
M4
M5
optical drive
2
Uu
Ue
Uu
Ue
Uu
Ue
Uu
on bus
encrypted

FIG.6

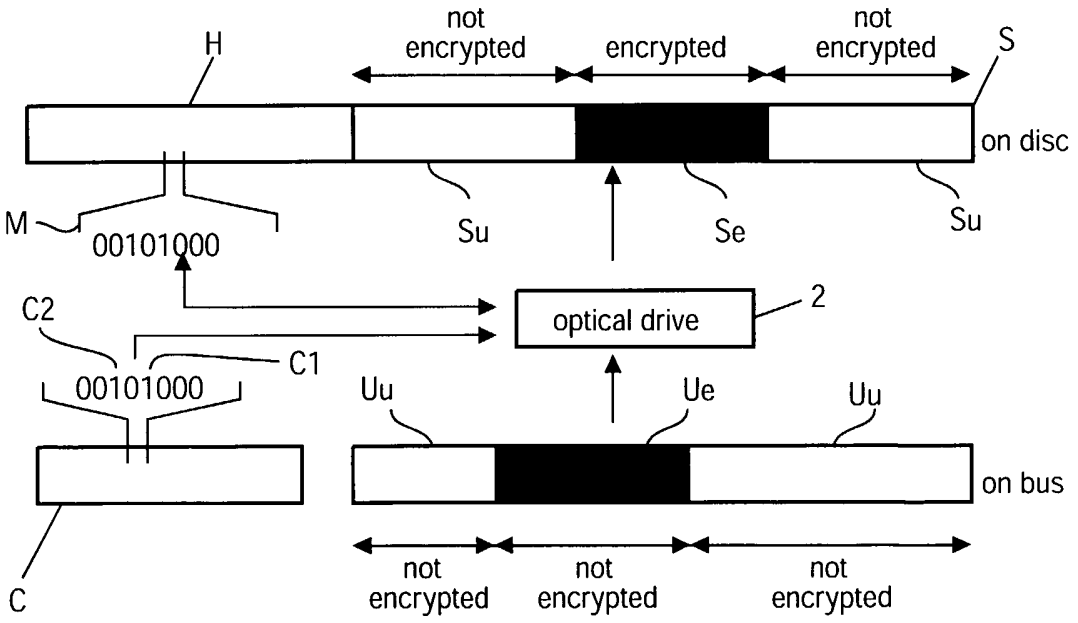

not
encrypted
encrypted
not
encrypted
H
S
on disc
M
00101000
Su
Se
Su
C2
C1
00101000
optical drive
2
Uu
Ue
Uu
on bus
C
not
encrypted
not
encrypted
not
encrypted

FIG.7

INTERNATIONAL SEARCH REPORT

PCT/IB2004/051303

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G11B20/00

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G11B

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2003/091186 A1 (FONTIJN WILHELMUS FRANSISCUS J ET AL) 15 May 2003 (2003-05-15)	1-3,5-13
Y	paragraphs '0003! - '0019! paragraphs '0021!, '0022! paragraph '0024! paragraph '0026! paragraph '0036! - paragraph '0054! paragraph '0057! figures 1-5 figure 7	4
Y	US 5 930 358 A (RAO MAHESH CHANDRA) 27 July 1999 (1999-07-27) column 8, line 37 - line 52 figure 2	4

-/--

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

[X] Patent family members are listed in annex.

° Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
29 November 2004	08/12/2004

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	Barel-Faucheux, C

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 1 327 981 A (SONY CORP) 16 July 2003 (2003-07-16) paragraph '0004! - paragraph '0006! paragraph '0009! paragraph '0053! - paragraph '0055! figures 3,8	1-13
A	US 2002/199099 A1 (HAYASHI SHIGEKAZU ET AL) 26 December 2002 (2002-12-26) paragraph '0106! - paragraph '0107! paragraph '0222! - paragraph '0251! figures 7,8	1-13
A	US 2003/117920 A1 (FURUKAWA SHUNSUKE ET AL) 26 June 2003 (2003-06-26) paragraphs '0129!, '0130! figures 8,9	1-13
A	EP 0 720 166 A (FUJITSU LTD) 3 July 1996 (1996-07-03) column 6, line 33 - line 49 figure 6	1-13
A	EP 1 058 254 A (MATSUSHITA ELECTRIC IND CO LTD) 6 December 2000 (2000-12-06) paragraph '0047! - paragraph '0052! figures 4,5,37,38	1-13
A	EP 1 008 989 A (SONY CORP) 14 June 2000 (2000-06-14) paragraph '0058! paragraphs '0108!, '0109! figure 11	1-13

INTERNATIONAL SEARCH REPORT

PCT/IB2004/051303

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2003091186 A1	15-05-2003	EP 1440439 A1	28-07-2004
		WO 03034425 A1	24-04-2003
US 5930358 A	27-07-1999	US 5812883 A	22-09-1998
		JP 2000500599 T	18-01-2000
		WO 9719406 A1	29-05-1997
EP 1327981 A	16-07-2003	JP 2003208755 A	25-07-2003
		CN 1431638 A	23-07-2003
		EP 1327981 A2	16-07-2003
		US 2003151991 A1	14-08-2003
US 2002199099 A1	26-12-2002	JP 2002132585 A	10-05-2002
US 2003117920 A1	26-06-2003	JP 2002140082 A	17-05-2002
		JP 2002140863 A	17-05-2002
		CN 1401119 T	05-03-2003
		DE 10194725 T0	05-06-2003
		WO 0237493 A1	10-05-2002
EP 0720166 A	03-07-1996	CN 1131852 A ,B	25-09-1996
		DE 69529887 D1	17-04-2003
		DE 69529887 T2	20-11-2003
		EP 0720166 A2	03-07-1996
		JP 8273296 A	18-10-1996
		KR 218995 B1	01-09-1999
		US 5812663 A	22-09-1998
EP 1058254 A	06-12-2000	CN 1355919 T	26-06-2002
		DE 60011958 D1	12-08-2004
		EP 1058254 A2	06-12-2000
		EP 1450362 A2	25-08-2004
		WO 0067257 A2	09-11-2000
		JP 2001189015 A	10-07-2001
		JP 3169366 B1	21-05-2001
		JP 2001189021 A	10-07-2001
		TW 540039 B	01-07-2003
EP 1008989 A	14-06-2000	JP 2000232441 A	22-08-2000
		EP 1008989 A2	14-06-2000