(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 477 593**

(51) Int. CI.:

G11B 20/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **28.07.2004 E 04744656 (2)**

(97) Fecha y número de publicación de la concesión europea: **21.05.2014 EP 1654732**

(54) Título: **Soporte de registro que comprende información de indicación de encriptación**

(30) Prioridad:

01.08.2003 EP 03102396

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
17.07.2014

(73) Titular/es:

KONINKLIJKE PHILIPS N.V. (100.0%)
HIGH TECH CAMPUS 5
5656 AE EINDHOVEN, NL

(72) Inventor/es:

STARING, ANTONIUS, A., M.;
SKORIC, BORIS;
TREFFERS, MENNO, A. y
MAES, MAURICE, J., J., J-B.

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Soporte de registro que comprende información de indicación de encriptación

La presente invención se refiere a un soporte de registro para almacenar datos de usuario en sectores e información de gestión asociada con dichos sectores. La presente invención se refiere adicionalmente un dispositivo de lectura para leer datos desde un soporte de registro y un método de lectura correspondiente. Aún más, la presente invención se refiere a un dispositivo de registro y un método de registro correspondiente para registrar datos en un soporte de registro. Finalmente, la presente invención se refiere a un programa informático para implementar dichos métodos.

Las unidades de disco óptico se conectan con otros componentes en un ordenador personal (PC) mediante un bus de comunicación, en particular un denominado bus PCI. Es fácil para los hackers escuchar la comunicación a través de este bus árido para obtener acceso a datos de usuario transmitidos. Una denominada encriptación de bus, de acuerdo con la que los datos de usuario se encriptan antes de transmisión a través del bus de comunicación y se desencriptan mediante el componente de recepción después de transmisión, se usa generalmente para proteger transmisión de datos frente a escuchas. Sin embargo, la encriptación de bus requiere esfuerzo computacional significativo que degrada el rendimiento de la aplicación o aumenta los costes de tales sistemas. Los esfuerzos computacionales podrían reducirse no encriptando todos los datos de usuario en todos los sectores, sino únicamente encriptando unos pocos sectores o parte de los datos de usuario en un sector, o eligiendo un algoritmo de encriptación que requiera menos esfuerzo computacional. Sin embargo, tales medidas debilitarían la protección.

Puesto que diferentes aplicaciones tienen diferentes requisitos de seguridad, y una única unidad óptica tiene que leer y proteger datos de muchas aplicaciones diferentes, es por lo tanto un problema fabricar una unidad de disco óptico o, más generalmente, proporcionar un dispositivo de lectura para leer datos de un soporte de registro, que satisfaga todas las necesidades con un único método de encriptación de bus. En particular, deberá proporcionarse este nivel de seguridad flexible para proteger datos de usuario durante transmisión a través del bus de comunicación cuando los datos de usuario se registran en un soporte de registro, tal como un disco óptico registrable.

Muchos métodos de protección de copia se han creado para evitar la copia de datos de usuario. Uno de estos métodos está basado en la denominada re-encriptación de acuerdo con la que algunos sectores del disco se encriptan y que se desencriptarán mediante la unidad antes de transmitirlos mediante un canal de comunicación seguro a otro componente en un PC. La ventaja de la reencriptación es que la clave usada mediante la unidad para desencriptar el sector no deja la unidad y por lo tanto no es fácil de descubrir por los hackers. Sin embargo, la desencriptación del sector encriptado requiere esfuerzo computacional significativo que degrada el rendimiento de la unidad o aumenta los costes de la misma. Aunque el esfuerzo computacional puede reducirse mediante las mismas medidas como se ha mencionado anteriormente, la fortaleza de la protección se debilitará.

Puesto que diferentes aplicaciones tienen diferentes requisitos de seguridad se desea proporcionar por lo tanto un dispositivo de lectura de bajo coste que esté optimizado para el nivel de seguridad de una única aplicación y un dispositivo de lectura de fin general que proporcione el nivel de seguridad correcto para todas las aplicaciones y pueda leer soportes de registro para todas las aplicaciones. Es necesario por lo tanto un método por el que un dispositivo de lectura de fin general pueda determinar si y, preferentemente, qué tipo de encriptación se ha de usar. Preferentemente, debería proporcionarse una información adicional que indica si y qué tipo de desencriptación se requiere antes de encriptación.

La solicitud de patente US 2003/091186 se refiere a un aparato y método para leer o escribir datos de usuario a nivel de bloques en forma encriptada en un medio de almacenamiento. Una lectura desde un bloque obtiene un indicador de encriptación que indica si dichos datos de usuario están encriptados o no, donde un identificador de datos de clave relacionado que especifica qué datos de clave usar para desencriptación de los datos de usuario si el indicador de encriptación indica que los datos de usuario están encriptados. Se devela también encriptación de datos de usuario antes de que se transmitan los datos en un bus.

La memoria descriptiva de la patente US 5.930.358 se refiere a un dispositivo de almacenamiento que tiene una memoria no volátil para almacenar parámetros de operación cambiables por el usuario. Los parámetros que son cambiables en el dispositivo de almacenamiento se refieren a respuestas a la detección de errores en el dispositivo de almacenamiento, algoritmos de encriptación de datos, la detención de giro de un disco, el almacenamiento en caché del dispositivo de almacenamiento y los algoritmos de compresión de datos. Más específicamente, pueden almacenarse diferentes algoritmos de encriptación en la memoria no volátil y el usuario puede seleccionar un parámetro que controla cuál de los algoritmos de encriptación de datos se usa para la encriptación de datos que tiene lugar en el propio conjunto de unidad de almacenamiento.

Es por lo tanto un objeto de la presente invención proporcionar una soporte de registro, un dispositivo de registro y método así como un dispositivo de lectura y método que proporcionen un nivel de seguridad flexible para proteger datos de usuario durante transmisión a través del bus de comunicación, también cuando los datos se registran en un soporte de registro tal como un disco óptico registrable.

Este objeto se consigue de acuerdo con la presente invención mediante un soporte de registro como se reivindica en la reivindicación 1 y un dispositivo de lectura para leer datos de un soporte de registro de este tipo como se define en la reivindicación 6.

Se define un método correspondiente en la reivindicación 8. Se define un programa informático para implementar dichos métodos en la reivindicación 9.

La presente invención está basada en la idea de señalizar al dispositivo de lectura que los datos de usuario particulares deben encriptarse mediante el dispositivo de lectura antes de que puedan transmitirse a través del bus de comunicación, en particular un bus PCI de PC. Una información de indicación de encriptación se proporciona por lo tanto en la información de gestión y se asocia con todos los sectores en los que se almacenan datos de usuario que deberán encriptarse antes de transmisión a través del bus de comunicación. Esta información de indicación de encriptación se leerá y evaluará mediante el dispositivo de lectura que a continuación encripta los datos de usuario asociados antes de que se emitan al bus de comunicación. El dispositivo de registro de acuerdo con la presente invención está adaptado de manera que durante el registro de datos de usuario, tal información de indicación de encriptación se asigna a los datos de usuario y se registra también en el soporte de registro para lectura posterior mediante el dispositivo de lectura. Tal información de indicación de encriptación se escribe basándose en una información de indicación de desencriptación correspondiente incluida en un comando recibido mediante el dispositivo de registro junto con la instrucción para registrar datos de usuario particulares en un soporte de registro. La invención proporciona por lo tanto una solución sencilla, flexible y de bajo coste que proporciona protección de copia durante transmisión de datos de usuario a través de un bus de comunicación que se leen desde un soporte de registro.

Debería observarse que los datos de usuario deben entenderse como que incluyen cualquier tipo de datos que se almacenan en un soporte de registro y que pueden transmitirse a través de un bus de comunicación, es decir no incluyen únicamente datos que se pretenden particularmente para un usuario, tal como audio, vídeo o datos de software, sino que incluyen también cualquier otro tipo de datos tales como datos de gestión o datos de control.

Las realizaciones preferidas de la invención se definen en las reivindicaciones dependientes. De acuerdo con una realización sencilla la información de gestión se almacena en el encabezamiento de sector de cada sector, y la información de indicación de encriptación es un único bit que se usa para desencadenar encriptación de datos de usuario almacenados en el sector asociado. Sin embargo, la información de gestión puede almacenarse también en un canal de sub-código separado (adicional) además del canal de datos normal.

De acuerdo con realizaciones adicionales la información de gestión comprende información adicional que indica qué parte o partes de los datos de usuario se han de encriptar, qué algoritmo de encriptación se ha de usar para encriptación, qué clave-jerarquía se ha de usar para determinación de una clave de encriptación para usarse para encriptación y/o indicar que los datos de usuario almacenados en los sectores asociados han de desencriptarse mediante el dispositivo de lectura antes de que se encripten de nuevo para transmisión. De nuevo, estos indicadores podrían ser bits únicos almacenados en el encabezamiento de sector. Preferentemente, la información de indicación que desencadena encriptación de bus se hace independiente de la información de indicación que desencadena desencriptación de sector debido a que los requisitos de seguridad para ambos métodos pueden ser diferentes. Si los desencadenantes para la encriptación de bus y desencriptación de sectores son independientes, preferentemente se protege la integridad de al menos el desencadenante de encriptación de bus. Esto puede conseguirse mediante, por ejemplo, haciendo la clave de desencriptación de sector dependiente de al menos el desencadenante de encriptación de bus (por ejemplo realizando XOR o troceo del desencadenante en la clave).

La invención se explicará ahora en mayor detalle con referencia a los dibujos en los que

La Figura 1 muestra un diagrama de bloques de un PC,

La Figura 2 muestra un diagrama de bloques de un dispositivo de lectura y registro de acuerdo con la invención,

La Figura 3 ilustra una primera realización de la invención,

La Figura 4 ilustra la primera realización de la invención con un ajuste de parámetro diferente,

La Figura 5 ilustra una segunda realización de la invención,

La Figura 6 ilustra una tercera realización de la invención, y

La Figura 7 ilustra una cuarta realización de la invención.

La Figura 1 muestra un diagrama de bloques de un PC 1 que comprende una unidad 2, por ejemplo una unidad de disco óptico, capaz de leer datos de un soporte 10 de registro y capaz de escribir datos a dicho soporte 10 de registro, una CPU 3 (Unidad de Procesamiento Central), una memoria 4 y una tarjeta 5 de gráficos conectados todos

a un bus 6 de comunicación. Por razones de simplicidad no se muestran detalles adicionales del PC 1 que, por supuesto, puede comprender componentes adicionales y también otros.

La Figura 2 muestra un diagrama de bloques de una unidad 2 de acuerdo con la presente invención. Para leer datos del soporte 10 de registro se proporciona una unidad 21 de lectura; para escribir datos a dicho soporte 10 de registro se proporciona una unidad 22 de escritura. Cuando se leen datos de usuario U del soporte 10 de registro que están almacenados en sectores S, como se muestra en la Figura 3 a modo de ejemplo de un disco óptico que tiene sectores de 2048 bytes de longitud cada uno, se lee la información de gestión asociada M almacenada en el encabezamiento del sector H asociado con cada sector S y teniendo, en este ejemplo, n bytes, así como también se reenvía a un intérprete 23 de datos. En el mismo, la información de gestión M, siendo en el ejemplo mostrado en la Figura 3 un byte que comprende 8 bits, se evalúa para determinar si los datos de usuario leídos almacenados en el sector asociado S deben encriptarse mediante una unidad 24 de encriptación/desencriptación antes de emitirse mediante una unidad 25 de salida y transmisión posterior a través del bus 6 de comunicación.

En la realización mostrada en la Figura 3 la información de gestión M únicamente incluye bits cero que significa que no se requiere encriptación de datos de usuario U antes de transmisión a través del bus de comunicación. Por lo tanto, los datos de usuario se emitirán directamente mediante la unidad 25 de salida al bus 6 de comunicación, es decir los datos de usuario U se comunicarán a través del bus 6 en una forma no encriptada como se muestra en la Figura 3. En la realización mostrada en la Figura 4, la información de indicación de encriptación M1 incluida en la información de gestión M indica, estableciendo un bit uno, que los datos de usuario U almacenados en el sector S se han de encriptar antes de que se emitan. Por lo tanto, los datos de usuario leídos U se reenviarán a la unidad 24 de encriptación/desencriptación donde se encriptan, antes de que se emitan después al bus de comunicación. En esta realización, únicamente se encripta una parte fija Ue de los datos de usuario del sector S mientras que otras partes Uu se comunican en una forma no encriptada.

En la realización mostrada en la Figura 5 ya la parte Se de los datos de usuario U almacenados en el soporte de registro en el sector S está encriptada mientras que otras partes Su del sector S no están encriptadas. En la información de gestión asociada M, además de la información de indicación de encriptación M1, se incluye una información de indicación de desencriptación adicional M2 indicando que (parte de) los datos de usuario U almacenados en el sector S necesitan desencriptarse en primer lugar antes de encriptarse de nuevo (indicado mediante M1) y transmitirse a través del bus de comunicación. Preferentemente, la clave de desencriptación de la parte encriptada Se depende del primer indicador M1 (y opcionalmente también del indicador M2). Por lo tanto, la unidad 24 de encriptación/desencriptación en primer lugar desencripta la porción encriptada Se del sector S antes de que se encripte parte de los datos de usuario U no encriptados completamente del sector S y se transmita a través de bus. Preferentemente, se usan diferentes claves de encriptación/desencriptación y/o algoritmos de encriptación/desencriptación para estas dos etapas de desencriptación/encriptación proporcionadas de acuerdo con esta realización.

La información de gestión puede incluir adicionalmente información adicional, tal como una información que indica la cantidad de datos de usuario que necesitan desencriptarse antes de encriptación, qué algoritmo usar para desencriptación y/o qué clave jerárquica usar para desencriptación.

De acuerdo con otra realización más como se muestra en la Figura 6, se proporciona una información de cantidad de encriptación adicional M3 como información de gestión adicional en el encabezamiento del sector A que indica qué partes del sector S deben encriptarse mediante la unidad 2. Por ejemplo, como se muestra en la Figura 6, tres partes del sector S que deben encriptarse (Ue) se indican mediante la información de cantidad de encriptación M3 mientras que otras partes del sector permanecen no encriptadas (Uu) antes de que se transmitan a través del bus.

Puede incluirse información adicional en la información de gestión, tal como por ejemplo una información de algoritmo de encriptación M4 que indica qué algoritmo de encriptación se ha de usar para encriptación y/o una información jerárquica de clave M5 que indica qué clave-jerarquía se ha de usar para determinación de una clave de encriptación para usarse para encriptación.

La realización de la unidad 2 mostrada en la Figura 2 comprende adicionalmente un intérprete 26 de datos/comandos y una unidad 27 de entrada para recepción de datos del bus 6 de comunicación. Estas unidades se usarán para el registro de datos para el soporte 10 de registro. En este caso se recibe un comando que ordena a la unidad 2 registrar datos de usuario particulares junto con aquellos datos de usuario mediante la unidad 27 de entrada y se evalúan mediante el intérprete 26 de datos/comandos. Esta realización se ilustra en la Figura 7 donde el comando C comprende una información de indicación de desencriptación C2 (similar a M2 mostrada en la Figura 5) que indica que los datos de usuario encriptados Ue recibidos desde el bus 6 necesitan desencriptarse y una información de indicación de encriptación C1 que indica que (parte de) la totalidad de los datos de usuario necesitan encriptarse antes de almacenarse en el soporte de registro. En este caso debe protegerse la integridad de al menos el desencadenante para la encriptación de sector (C1). Esto puede conseguirse, por ejemplo, haciendo la clave de desencriptación de bus dependiente de al menos el desencadenante de encriptación de sector (por ejemplo realizando XOR o troceo del desencadenante en la clave).

Estas etapas de encriptación y desencriptación se harán mediante la unidad 24 de encriptación/desencriptación antes de que los datos de usuario parcialmente encriptados se escriban en el soporte 10 de registro mediante la unidad 22 de escritura. Al mismo tiempo una información de gestión apropiada M que incluye los indicadores M1 y M2 se registra en el encabezamiento de sector H. Por supuesto, más información adicional, similar a la información más adicional ilustrada anteriormente para la información de gestión, puede también incluirse en el comando C.

De acuerdo con la invención se proporciona una solución sencilla, de bajo coste, flexible y segura para protección de datos de usuario almacenados en un soporte de registro antes de transmisión a través de un bus de comunicación de un PC.

REIVINDICACIONES

1. Soporte (10) de registro para almacenar datos de usuario en sectores (S) e información de gestión (M) asociada con dichos sectores (S).
en el que dicha información de gestión (M) comprende una información de indicación de desencriptación (M2) que indica que los datos de usuario almacenados en el sector asociado (S) se han de desencriptar mediante el dispositivo de lectura;
caracterizado por que dicha información de gestión (M) comprende adicionalmente una información de indicación de encriptación de bus que comprende un único bit (M1) asociado con cada uno de dichos sectores (S),
indicando cada bit (M1) a un dispositivo de lectura si los datos de usuario almacenados en el sector asociado (S) se han de encriptar mediante el dispositivo (2) de lectura antes de que se transmitan a través de un bus (6) de comunicación,
siendo la información de indicación de encriptación de bus (M1) independiente de la información de indicación de desencriptación (M2).

2. Soporte de registro como se reivindica en la reivindicación 1, en el que dicha información de gestión (M) se almacena en un encabezamiento (4) de sector.

3. Soporte de registro como se reivindica en la reivindicación 1, en el que dicha información de gestión (M) comprende adicionalmente una información de cantidad de encriptación (M3) que indica qué parte o partes de los datos de usuario almacenados en el sector asociado (S) se han de encriptar.

4. Soporte de registro como se reivindica en la reivindicación 1, en el que dicha información de registro (M) comprende adicionalmente una información de algoritmo de encriptación (M4) que indica qué algoritmo de encriptación se ha de usar para encriptación.

5. Soporte de registro como se reivindica en la reivindicación 1, en el que dicha información de registro (M) comprende adicionalmente una información de clave-jerarquía (M5) que indica qué clave-jerarquía se ha de usar para determinación de una clave de encriptación para encriptación.

6. Dispositivo de lectura para leer datos de un soporte (10) de registro que almacena datos de usuario en sectores (S) e información de gestión (M) asociada con dichos sectores (S), que comprende:

una unidad (21) de lectura para leer dichos datos de usuario y dicha información de gestión (M) de dicho soporte (10) de registro,
un intérprete (23) de datos para interpretar dicha información de gestión (M),
y una unidad (25) de salida para emitir dichos datos de usuario para posterior transmisión a través de un bus (6) de comunicación,
dicha información de gestión (M) comprende una información de indicación de encriptación de bus que comprende un único bit (M1) asociado con cada uno de dichos sectores (S), indicando cada bit (M1) al dispositivo de lectura si los datos de usuario almacenados en el sector asociado (S) se han de encriptar mediante el dispositivo de lectura antes de que se transmitan a través de un bus (6) de comunicación,
en el que dicha información de gestión (M) comprende una información de indicación de desencriptación (M2) que indica que los datos de usuario almacenados en el sector asociado (S) se han de desencriptar mediante el dispositivo (2) de lectura
siendo la información de indicación de encriptación de bus independiente de la información de indicación de desencriptación que desencadena la desencriptación de los datos de usuario mediante el dispositivo de lectura
caracterizado por que
el dispositivo comprende adicionalmente:

una unidad (24) de encriptación/desencriptación para en primer lugar desencriptar los datos de usuario basándose en la información de indicación de desencriptación
la unidad (24) de encriptación/desencriptación para encriptar posteriormente datos de usuario de sectores (S) para los que el respectivo bit (M1) de la información de indicación de encriptación asociada indica que dichos datos de usuario se han de encriptar
emitiendo la unidad (25) de salida los datos de usuario recibidos de la unidad (24) de encriptación/desencriptación a través de un bus (6) de comunicación.

7. Dispositivo de lectura como se reivindica en la reivindicación 1, en el que una clave de desencriptación para desencriptación de los datos de usuario depende de la información de indicación de encriptación de bus (M1).

8. Método de lectura para leer datos de un soporte (10) de registro que almacena datos de usuario en sectores (S) e información de gestión (M) asociada con dichos sectores (S), que comprende las etapas de:

leer dichos datos de usuario y dicha información de gestión (M) de dicho soporte (10) de registro, que interpreta dicha información de gestión (M), y

emitir dichos datos de usuario para posterior transmisión a través de un bus (6) de comunicación,
dicha información de gestión (M) comprende una información de indicación de encriptación de bus que comprende un único bit (M1) asociado con cada uno de dichos sectores (S), indicado cada bit (M1) a un dispositivo de lectura si los datos de usuario almacenados en el sector asociado se han de encriptar mediante el dispositivo de lectura (2) antes de que se transmitan a través de un bus (6) de comunicación,
en el que dicha información de gestión (M) comprende una información de indicación de desencriptación (M2) que indica que los datos de usuario almacenados en el sector asociado (S) se han de desencriptar mediante el dispositivo (2) de lectura
siendo la información de indicación de encriptación de bus (M1) independiente de una información de indicación de desencriptación que desencadena desencriptación de los datos de usuario mediante el dispositivo de lectura
caracterizado por que
el método comprende adicionalmente las etapas de:

en primer lugar desencriptar los datos de usuario basándose en la información de indicación de desencriptación encriptando posteriormente los datos de usuario de sectores (S) para los que el respectivo bit (M1) de la información de indicación de encriptación asociada indica que dichos datos de usuario se han de encriptar,
emitiendo la unidad (25) de salida los datos de usuario recibidos de la unidad (24) de encriptación/desencriptación a través de un bus de comunicación.

9. Programa informático que comprende medios de código de programa para producir a un ordenador que lleve a cabo todas las etapas del método como se reivindica en la reivindicación 8 cuando dicho programa informático se ejecuta en un ordenador.

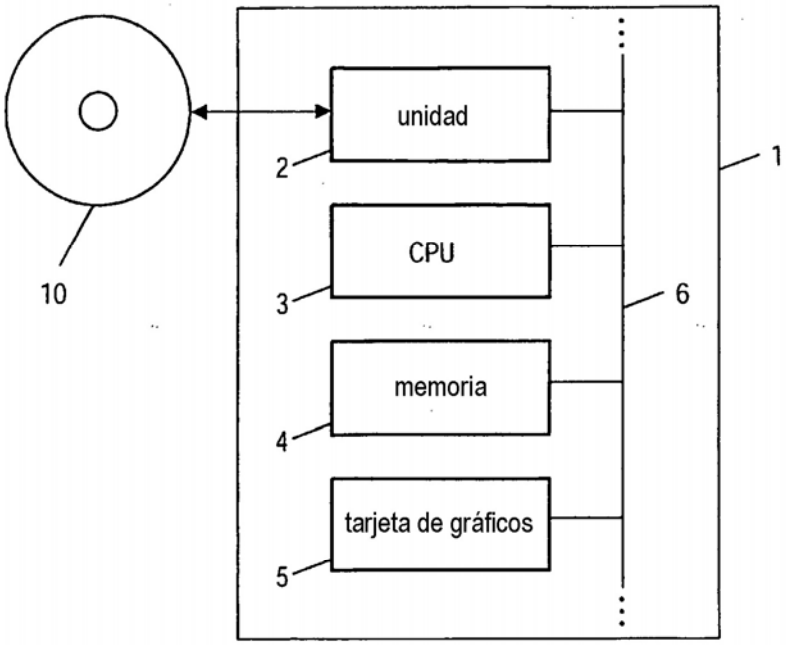

FIG.1

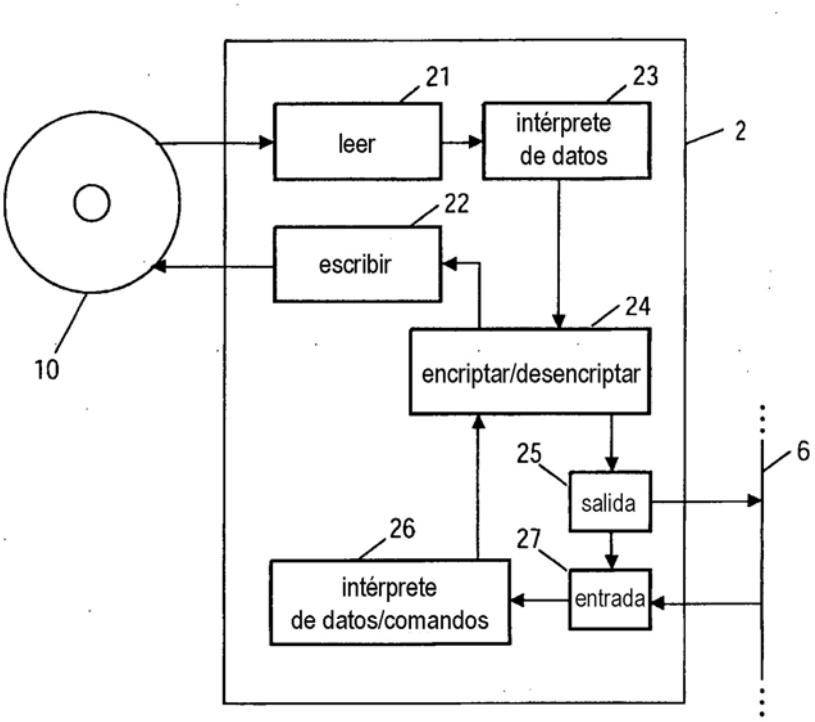
21
23
leer
intérprete
de datos
2
22
escribir
24
encriptar/desencriptar
10
25
6
salida
26
27
intérprete
de datos/comandos
entrada

FIG.2

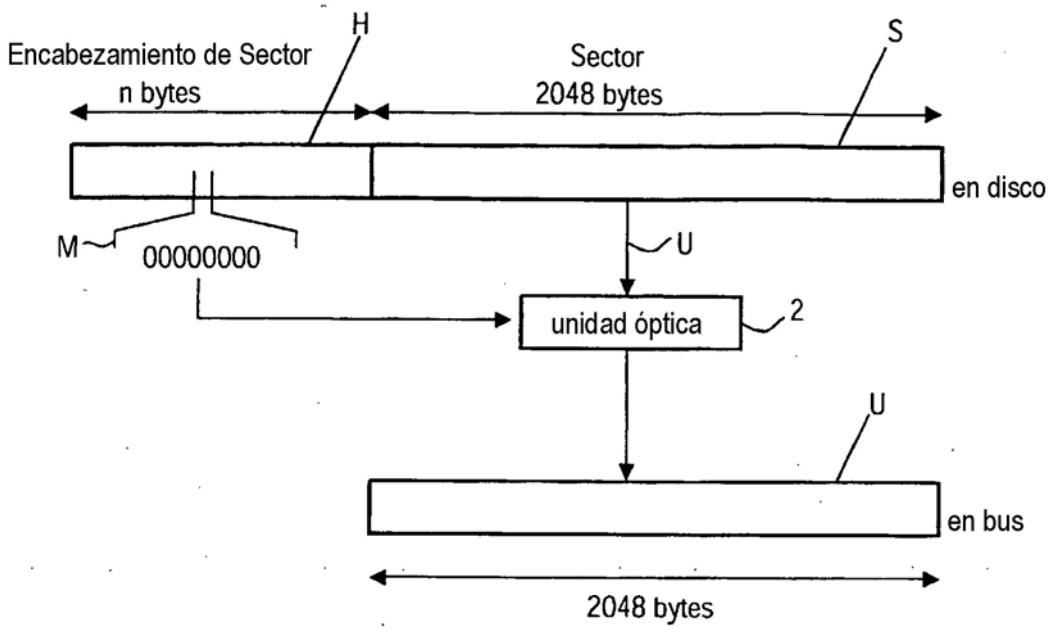
H
S
Encabezamiento de Sector
n bytes
Sector
2048 bytes
en disco
M
00000000
U
unidad óptica
2
U
en bus
2048 bytes

FIG.3

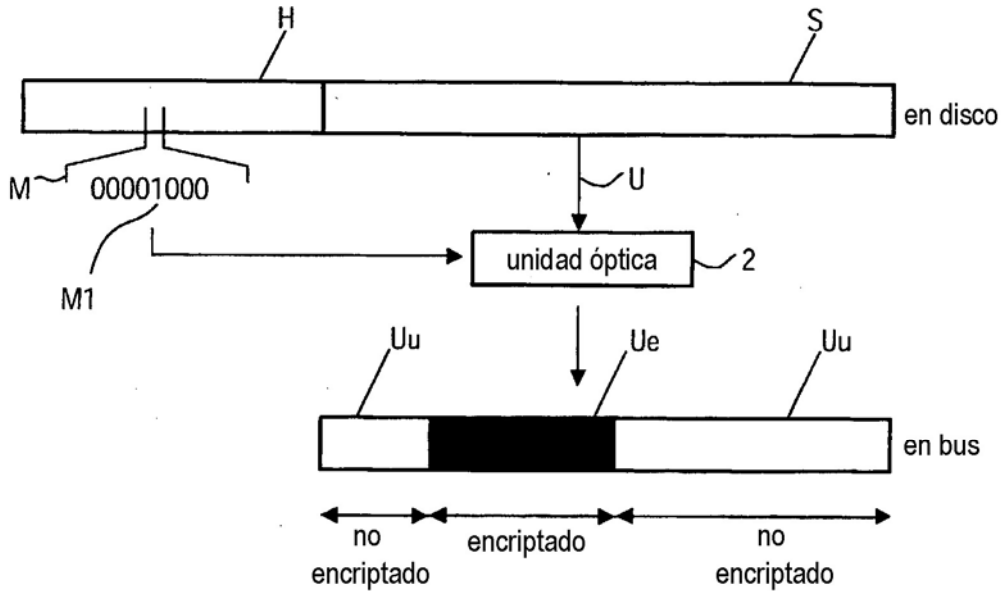
H
S
en disco
M
00001000
U
unidad óptica
2
M1
Uu
Ue
Uu
en bus
no
encriptado
encriptado
no
encriptado

FIG.4

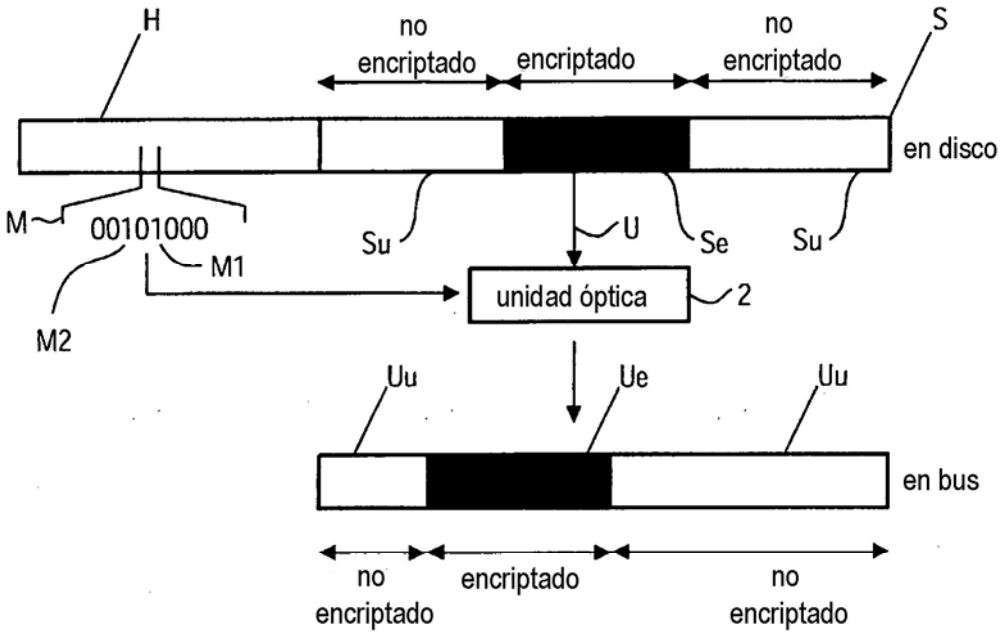
H
no encriptado
encriptado
no encriptado
S
en disco
M
00101000
M1
M2
Su
U
Se
Su
unidad óptica
2
Uu
Ue
Uu
en bus
no encriptado
encriptado
no encriptado

FIG.5

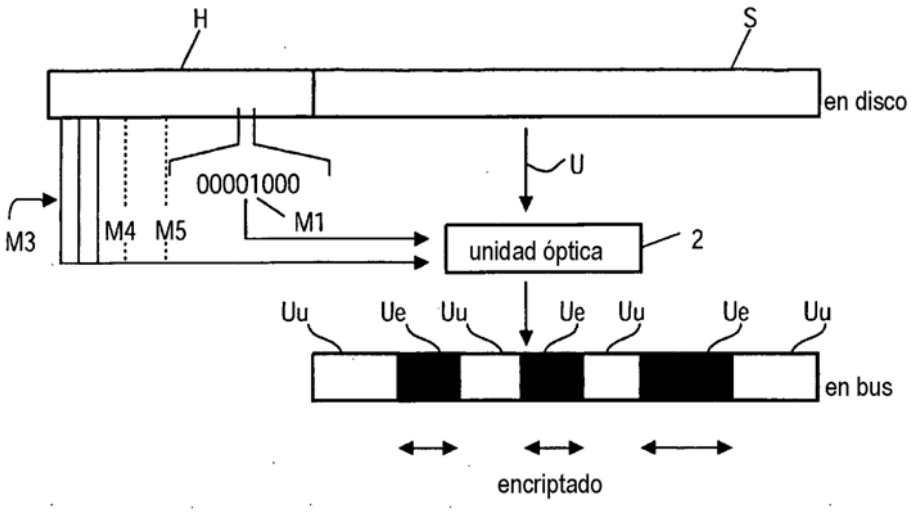
H
S
en disco
U
00001000
M1
M3
M4
M5
unidad óptica
2
Uu
Ue
Uu
Ue
Uu
Ue
Uu
en bus
encriptado

FIG.6

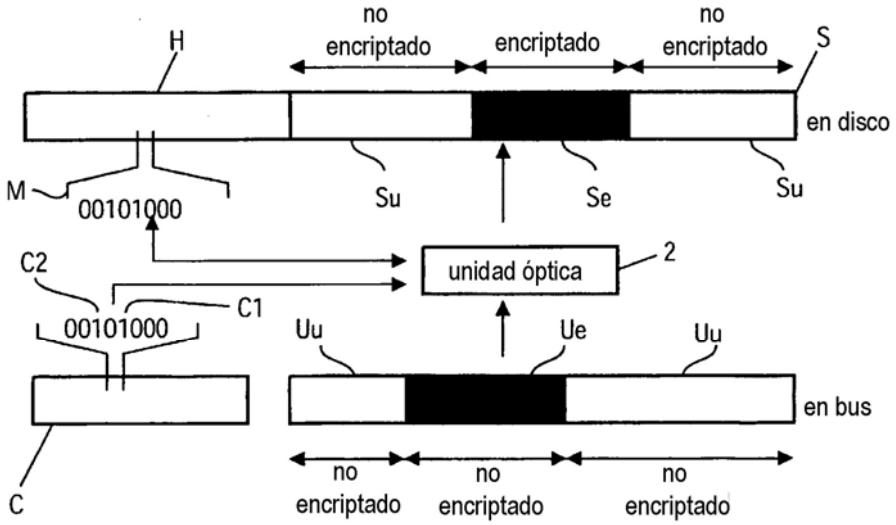
no
encriptado
encriptado
no
encriptado
H
S
en disco
M
00101000
Su
Se
Su
C2
C1
00101000
unidad óptica
2
Uu
Ue
Uu
en bus
C
no
encriptado
no
encriptado
no
encriptado

FIG.7