(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 379 551**

(51) Int. CI.:
G11B 20/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **04708423 .1**
(96) Fecha de presentación: **05.02.2004**
(97) Número de publicación de la solicitud: **1597727**
(97) Fecha de publicación de la solicitud: **23.11.2005**

(54) Título: **Soporte de información que comprende información de acceso**

(30) Prioridad:
20.02.2003 NL 1022743

(45) Fecha de publicación de la mención BOPI:
27.04.2012

(45) Fecha de la publicación del folleto de la patente:
27.04.2012

(73) Titular/es:
KONINKLIJKE PHILIPS ELECTRONICS N.V.
GROENEWOUDSEWEG 1
5621 BA EINDHOVEN, NL

(72) Inventor/es:
STEK, Aalbert;
BLUM, Martinus W.;
VAN ROMPAEY, Bart y
HEEMSKERK, Jacobus P. J.

(74) Agente/Representante:
Zuazo Araluze, Alexander

DESCRIPCIÓN

Soporte de información que comprende información de acceso

La técnica para ocultar información de acceso en un soporte de información que contiene la información de usuario se basa en el hecho de distraer la atención de las personas (los *hackers*) de la información de acceso que se desea ocultar. Al usar esta información de acceso, puede accederse a la información de usuario en el soporte de información. Para fines de protección anticopia algunas veces se desea ocultar este acceso, por ejemplo en la información de usuario se desea proteger u ocultar esta información de acceso en un canal lateral presente en el soporte de información. A partir de soportes de información ópticos tales como CD o DVD, se conoce, por ejemplo, que esta información de acceso puede escribirse en el denominado “canal de oscilación” (algunas veces denominado también “canal de error radial”). Se conoce que la información de acceso puede almacenarse usando técnicas de espectro ensanchado de una manera segura en un soporte de información en una variación de un parámetro, variación que puede detectarse mediante la información de acceso de integración que se almacena en el recorrido radial del presurco oscilante. La amplitud de este recorrido es pequeña, normalmente de algunos 5-10 nm pico a pico. De este modo, la señal de oscilación obtenida, extrayendo mediante lectura de este canal, es muy ruidosa e imposible de copiar directamente. En técnicas de espectro ensanchado, la información de acceso oculta puede detectarse integrando la señal de extracción mediante lectura de una manera especial. Las técnicas de espectro ensanchado se conocen, por ejemplo, a partir de “Digital Modulation and Coding”, Wilson, págs. 247-256 y las referencias en el mismo. La detección de integración se conoce, por ejemplo, a partir de “Digital Baseband Transmission and Recording”, Jan W.M. Bergmans, págs. 122-129. En técnicas de espectro ensanchado el ancho de banda de una señal se hace intencionalmente más grande usando la modulación de espectro ensanchado. La señal modulada puede detectarse usando los métodos de detección de integración que usan, por ejemplo, un receptor de probabilidad máxima hipotético.

El documento WO02/25645 describe un disco óptico que tiene marcas ópticamente legibles que almacenan principales datos digitales y que almacenan adicionalmente datos subdigitales codificados por modulación de fase del reloj. Los datos subdigitales son información para determinar si el disco o contenido es legal. Los principales datos digitales pueden cifrarse por datos subdigitales. Los datos subdigitales pueden estar repetidamente presentes en una pluralidad de áreas de identificación para la reproducción en diferentes velocidades lineales o detección fiable en caso de un área dañada o rayada.

Es un objetivo de la invención realizar un soporte de información que comprende información de acceso en la que se impide además la recuperación ilegal de la información de usuario.

Según la invención, este objetivo se logra mediante el soporte de información tal como se define en la reivindicación 1. Cifrando los bits de información de acceso según un método de cifrado predeterminado no es posible la detección de la información de acceso mientras que no se conozca el método de cifrado. El uso de la técnica de detección de integración sólo da como resultado la información de acceso si uno conoce cómo debe procesarse la señal obtenida tras la extracción mediante lectura del área que comprende los bits de información de acceso.

En otra realización del soporte de información según la invención, los bits de información de acceso se cifran almacenando determinados bits de información de acceso predeterminados invertidos en el soporte de información. En otra realización del soporte de información según la invención, los bits de información de acceso se cifran cambiando la secuencia de los bits de una manera casi aleatoria predeterminada. En estas realizaciones, la señal obtenida por la extracción mediante lectura del área que comprende los bits de información de acceso, debe corregirse en primer lugar según el método de cifrado usado antes de que la técnica de detección de integración, dé como resultado la técnica de información de acceso.

En otra realización del sistema según la invención, en la que el soporte de información comprende además un presurco oscilante, el soporte de información está caracterizado porque los bits de información de acceso se almacenan en la variación del recorrido radial del presurco oscilante.

En otra realización del soporte de información según la invención, el método de cifrado está oculto en el soporte de información. En otra realización del soporte de información según la invención, el método de cifrado está oculto en el recorrido radial del presurco oscilante. Se prefiere que el método de cifrado se mantenga tan secreto como sea posible. Ocultando el método de cifrado en el soporte de información puede impedirse dar a conocer el método de cifrado a las compañías de semiconductor que fabrican IC que van a usarse en un aparato para reproducir el soporte de información según la invención. La información sobre el método de cifrado usado puede entonces, por ejemplo, suministrarse a los mismos mediante una parte de código VERILOG, con una interfaz bien definida, que puede añadirse a su propio diseño de IC y tener en cuenta la detección de método de cifrado usado. Esto tiene como una ventaja adicional que la posición de la información de acceso no debe mencionarse en la especificación estándar que describe el soporte de información según la invención.

Se prefiere poder cambiar el método de cifrado usado si se ha hackeado un método. Para este fin, en otra realización, el soporte de información comprende un área especial que comprende bits del método de cifrado que

indican el método de cifrado predeterminado según el cual se cifran los bits de información de acceso. Preferiblemente, los bits del método de cifrado se almacenan en el soporte de información en una variación de un parámetro, variación que puede detectarse mediante la detección de integración. Preferiblemente, el área especial comprende 8 bits del método de cifrado.

Los bits del método de cifrado pueden usarse para indicar diferentes métodos de cifrado. Por ejemplo, 8 bits del método de cifrado pueden indicar 256 (2^8) posibles secuencias de bits, representando cada una de estas secuencias un método de cifrado. Si se hackea el método de cifrado predeterminado, uno puede cambiar el método de cifrado usado para futuros soportes de información a uno de los otros métodos. Estos bits del método de cifrado pueden, por ejemplo, almacenarse en el soporte de información en una variación de un parámetro, variación que puede detectarse mediante la detección de integración, de modo que estos bits pueden detectarse usando detección de integración. Esto tiene la ventaja de que los bits no son fácilmente detectables por los hackers.

En otra realización, el soporte de información comprende una zona de datos de información y control permanente (PIC), almacenándose la información de acceso en la zona PIC. La información de acceso puede, por ejemplo, ser información que se almacena en la zona PIC en microsurcos/pasos (o marcas/pasos) previamente grabados, pero esta información también puede almacenarse en surcos modulados de alta frecuencia (HFM) previamente grabados que se modulan en la dirección radial con una señal de ancho de banda bastante alta. Esta zona PIC se usa en un nuevo soporte de información óptico, denominado disco *BluRay*.

La invención se refiere además a un aparato para extraer mediante lectura la información a partir del soporte de información tal como se define en la reivindicación 12. En una realización, los medios de control de acceso se integran en un bloque VERILOG. En otra realización, el aparato comprende además una tabla de consulta que comprende una lista de métodos de cifrado predeterminados. Usando esta tabla, el método de cifrado usado puede sustituirse por un diferente método de cifrado si se hackea el método de cifrado.

Estos y otros aspectos de la invención son evidentes a partir de y se aclararán con referencia a las realizaciones descritas a continuación en el presente documento.

En los dibujos:

la figura 1 muestra una primera realización del soporte de información según la invención,

la figura 2 muestra una segunda realización del soporte de información según la invención,

la figura 3 muestra otra realización del soporte de información según la invención,

la figura 4 muestra otra realización del soporte de información según la invención,

la figura 5 muestra una realización de un aparato para extraer mediante lectura la información de acceso de un soporte de información,

la figura 6 muestra una realización del uso de la información de acceso para proporcionar acceso a la información de usuario,

la figura 7 muestra una realización del módulo de detección usado en el aparato.

Es necesario mantener algunas partes del esquema de protección anticopia en secreto, no sólo las claves de encriptación, sino también algún método de modulación o procesamiento de señal para almacenar las claves o números de ID. Entonces, es necesario suministrar una “caja negra” como un formateador para un servicio de elaboración de un original, y suministrar una descripción VERILOG a los desarrolladores de IC de decodificadores. Así, existe (o existen) un secreto(s) en la parte de decodificador, o en un canal lateral, que requiere *hardware* especial para detectarse. En un caso de este tipo, los hackers no pueden tener éxito modificando sólo el *software* de aplicación o el *firmware* de la unidad. Contraria a esta necesidad de secreto, tenemos la necesidad de probar medios en fabricación. Una manera es usar el cifrado en una o más fases en el trayecto de procesamiento de señal, y cambiar el cifrado en algún área de prueba designada. En el área descifrada, puede leerse una “clave de prueba” para probar el margen de recuperación de la información secreta, necesitamos medir alguna señal digital (por ejemplo, tasa de error de bits) o alguna señal analógica (por ejemplo, fluctuación o relación señal a ruido). La clave de prueba puede ser alguna información de disco no confidencial.

Para BD-ROM, el sistema de protección anticopia contendrá una estructura de microsurco oscilado que contiene la información de acceso, por ejemplo, en forma de una clave de encriptación. La modulación en la oscilación representa los bits de la clave. Los bits se cifran con un método de cifrado secreto. Siempre que el método de cifrado no se conozca uno no puede detectar los bits que forman la clave de encriptación. Nos gustaría poder mantener el método de cifrado tan en secreto como sea posible. E incluso tener escenarios de reserva para cambiar posiblemente el método de cifrado si se ha hackeado un método. Estas copias de reserva necesitan ser tan sencillas

como sea posible. En el soporte de información según una realización, el método de cifrado se escribe en una parte (descifrada) de la clave de oscilación.

En la realización del soporte de información tal como se muestra en la figura 1, la información de acceso se almacena en la zona PIC del soporte de información. En esta realización, el soporte de información comprende una denominada zona de datos de información y control permanente (PIC). En esta zona PIC se encuentra almacenada información general sobre el soporte de información y otra información diversa. De esta forma, se crea un canal de datos para información previamente grabada con suficiente capacidad y velocidad de transmisión de datos. En esta realización, la información de PIC se almacena en microsurcos/pasos (o marcas/pasos) previamente grabados, pero esta información también puede almacenarse en surcos modulados de alta frecuencia (HFM) previamente grabados que se modulan en la dirección radial con una señal de ancho de banda bastante alta. Debido al hecho de que la información se almacena en un canal de oscilación, se crea un canal oculto. En la figura 1, se indica la disposición del soporte de información que comprende la zona PIC. El área en el soporte de información más cercana al centro del soporte se denomina el área 6 interna (IA). A lado de ésta está el área 7 de sujeción (CA) que se usa por el aparato de reproducción para sujetar el soporte de información de modo que pueda llevarse a cabo una rotación estable. A lado de ésta está el área 8 de transición (TA). Después de esta área, se sitúa el área de información (IA). Esta área de información comprende la zona de información (IZ) y el área 9 de corte por ráfagas (BCA). El área de corte por ráfagas se usa para añadir información al soporte de información tras la finalización del proceso de fabricación. El código de BCA puede escribirse mediante un sistema láser de alta potencia o mediante el inicializador en caso de discos regrabables. La zona de información (IZ) comprende la zona de línea de entrada (LI), el área 12 de datos y la zona 13 de línea de salida (LO). La zona de línea de entrada comprende la zona 10 PIC y el resto de la zona 11 de línea de entrada. En esta realización, la información de acceso está almacenada en una región predeterminada de la zona PIC.

Con el fin de poder extraer mediante lectura la información de acceso, puede recuperarse una referencia a la posición de la información de acceso en la zona PIC mediante un determinado método. En esta realización este método es de la siguiente manera. La zona PIC comprende un canal de datos principal, con números de unidad de dirección (AUN). Estos AUN se usan para indicar la posición de inicio de la información de acceso en la zona PIC. Esto es posible ya que la señal de canal de oscilación se bloquea para la señal de datos (canal HF). Una dirección es de 4 bytes (sin los bytes de ECC). Ya que la zona PIC sólo se sitúa en una pequeña parte del soporte de información, sólo un número limitado de los bits menos significativos (lsb) de los 32 bits cambian dentro de la zona PIC (generalmente sólo los primeros 16 lsb). Estos 16 bits son suficientes para determinar la posición dentro de la zona PIC. La zona PIC se extiende en unas 2000 pistas; se supone que la información de acceso sólo está presente en 20 pistas consecutivas, determinándose la posición de inicio de esta información de acceso se mediante un AUN de la información de usuario. Los primeros 16 lsb de este AUN se colocan entonces en la zona PIC completa, por ejemplo usando una modulación descifrada. Debido a eso, se hace posible, cuando se llega a una posición aleatoria en la zona PIC, extraer mediante lectura los primeros 16 bits del AUN, para saltar a la posición de inicio de la información de acceso, y extraer mediante lectura la información de acceso. De esta forma, la ubicación exacta de la información de acceso se oculta adicionalmente en la zona PIC, ya que sólo se sitúa en una determinada posición en esta banda, y no en toda la banda completa.

En esta realización, la información de acceso se escribe en la zona PIC del disco BD-ROM que usa una estructura de microsurco oscilado. Los principales datos contenidos en la estructura de microsurco consisten en la información de PIC habitual (información de revocación de unidad, información de disco). La información de acceso puede ser parte de una clave necesaria para descifrar la información de usuario en el disco. La amplitud de la oscilación es pequeña, digamos de 5 -10 nm pico a pico. De esta forma, la señal de oscilación es muy ruidosa e imposible de copiar directamente.

Para unidades de CE incluso una oscilación de gran amplitud es imposible de copiar puesto que la unidad no puede hacer oscilar el actuador. Así, el uso de una oscilación en el soporte de información para contener la clave hace que el copiado bit a bit del contenido sea imposible para la unidad de CE (en la suposición de que en el futuro estarán disponibles unidades de CE avanzadas que podrán hacer oscilar el actuador, no se puede impedir el copiado real de la oscilación). Pero si uno elige que el periodo de la oscilación CPS en BD-ROM sea 69T, la oscilación CPS copiada en el disco BD-RE interferirá con el presurco en este disco que tiene la misma frecuencia de 69 bits de canal. Por tanto, la extracción mediante lectura de la oscilación CPS en el disco copiado es imposible, esto también se menciona en la patente de Philips US 5.724.327 para el caso de CD. Sin embargo, los piratas profesionales que tienen acceso al equipo de elaboración de un original podrían usar esta amplitud de gran oscilación para accionar una señal deflectora para la elaboración de un original de la oscilación en la siguiente estampa hecha ilegalmente. Por tanto, la amplitud de oscilación debe ser lo suficiente pequeña de modo que este método se haga imposible también para estos piratas. La señal de oscilación es entonces demasiado ruidosa para accionar correctamente un deflector en el equipo de elaboración de un original para copiar la oscilación. La detección de los datos en esta oscilación sólo es posible mediante la detección de integración. Naturalmente, los hackers podrían usar todavía este método para obtener los datos por medio de la oscilación. Pero se usa otro método para impedir esto: el cifrado. Esta realización se explica con referencia a la figura 2.

El cifrado de datos puede realizarse de varias formas. Una posibilidad es invirtiendo los bits de la clave de una

manera secreta predefinida. Otra es permutando la secuencia de bits de una manera predefinida que varía durante la integración. En tercer lugar, se puede usar una mezcla de ambos métodos. Mientras que no se conozca el método de cifrado no puede integrarse la señal. Para integrar apropiadamente la señal se necesita producir una señal unipolar por medio de la señal bipolar aplicando la inversa del método de cifrado secreto en los bits detectados. Sólo entonces puede revelarse la información de decisión programada a partir del ruido.

En la realización de la figura 2, en la etapa 22, los 168 bits que comprenden la información de acceso, bits de CRC y bits sobrantes se pasan por XOR con 168 bits aleatorios. Estos bits aleatorios pueden, por ejemplo, recuperarse a partir del soporte de información o pueden presentarse en el aparato que extrae mediante lectura del soporte de información. En los bits resultantes se realiza una permutación aleatoria en la etapa 23. Estos bits permutados se escriben entonces en el soporte 1 de información. Estos bits pueden escribirse en una trama clave tal como se explicará en la figura 3. Los bits aleatorios y la permutación aleatoria usados pueden cambiarse para cada trama clave. La permutación puede repetirse cada bloque de ECC; la semilla de cifrado puede, por ejemplo, derivarse de los AUN, los números de dirección usados en la zona PIC.

La figura 3 muestra otra realización del soporte de información. En esta realización los 168 bits que comprenden los bits de información de acceso cifrados se almacenan en el canal de oscilación presente en las tramas 51 claves. En esta realización, cinco tramas claves más una trama de sincronización sobrante constituyen 1 sector físico. Las cinco tramas claves forman por sí mismas una unidad de dirección (hay 80 tramas claves y por tanto 16 unidades de dirección en cada agrupamiento de ECC). Sólo conociendo la permutación secreta usada en la información de acceso almacenada en el canal de oscilación puede realizarse la integración apropiada de los bits. En una realización, esta permutación secreta permanece en el bloque VERILOG (también denominado paquete LSI). Esto tiene la ventaja de que la posición de la información de acceso no debe mencionarse en la especificación convencional que describe este soporte de información. Esta realización puede usarse cuando no se requiera ninguna opción de reserva para cambiar el método de cifrado usado.

Nos gustaría poder mantener el método de cifrado tan secreto como sea posible. E incluso tener escenarios de reserva para cambiar posiblemente el método de cifrado si se ha hackeado un método. Estas copias de reserva necesitan ser tan sencillas como sea posible. Otra realización del soporte de información según la invención en la que permite el cambio del método de cifrado se muestra en la figura 4. En esta realización el soporte de información comprende cuatro tramas 14 claves. En estas tramas claves, hay 31 tramas de sincronización, estando numeradas desde 0 hasta 30. En el número de tramas de sincronización 3, 7, 11, 15, 19, 23 y 27 (indicados con número de referencia 15) se almacena un número de 8 bits que indica la ubicación exacta de la información de acceso. En el caso en que la información de acceso se almacena en el soporte de información en una variación de un parámetro, variación que puede detectarse mediante la detección de integración, la ubicación exacta de la información de acceso puede cambiarse usando este número de 8 bits. Este número de 8 bits puede entonces, por ejemplo, indicar qué semilla y permutación deben usarse para detectar los bits que constituyen la información de acceso.

También es posible escribir en un área específica en la oscilación en la zona PIC, de una manera descifrada, una secuencia de bits, por ejemplo 8. Estos 8 bits pueden integrarse muy fácilmente de entre el ruido usando la detección de integración puesto que no hay cifrado (podría usarse alternativamente el cifrado, pero entonces debe ser un método fijo conocido por la unidad). La secuencia de bits da $2^8 = 256$ posibles secuencias de bits. Cada una de estas secuencias representa entonces un método de cifrado secreto. Una tabla de consulta que contiene una lista de estos 256 métodos puede estar contenida en la unidad en el circuito de detección de clave de oscilación secreta. Esta secuencia puede leerse fácilmente, se conoce entonces el método de cifrado y así puede detectarse la clave de oscilación. Si se hackea el método de cifrado se cambia simplemente para discos futuros a uno de los otros 256 métodos. Naturalmente, el circuito de detección de oscilación en la unidad debe conocer todos los 256 métodos de cifrado. Normalmente, el circuito de detección de oscilación se pone en código VERILOG y éste se da al fabricante de circuitos. De esta forma, debe hackearse el código VERILOG para descubrir cuáles son los 256 métodos de cifrado. Esto es complicado y no todos tienen acceso a este código VERILOG. Otra ubicación en la que el método de cifrado necesita conocerse es en el equipo de elaboración de un original. Pero en este caso sólo necesita implementarse el método de cifrado actualmente instalado y no todos los 256 métodos de cifrado. Si se hackea un método de cifrado el codificador de oscilación específica en el generador de formato del equipo de elaboración de un original puede sustituirse por otro con un método de cifrado diferente (de los 256 métodos posibles). Esto limita considerablemente el acceso a esta información secreta.

La figura 5 muestra una realización de un aparato para extraer mediante lectura la información de acceso de un soporte de información. El aparato comprende una unidad de lectura para extraer mediante lectura la información de usuario e información de acceso a partir del soporte 1 de grabación. La unidad de lectura comprende un cabezal 41 de lectura para explorar la pista y generar una señal de lectura correspondiente a las marcas físicas en el soporte de grabación, y una unidad 42 de traducción para traducir la señal de lectura en la secuencia de bits, por ejemplo, un decodificador EFM para decodificar en un sistema de CD. La secuencia de bits se acopla a una unidad 43 de corrección de errores para recuperar la información y corregir posibles errores, por ejemplo el corrector CIRC en un sistema de CD. La información recuperada se acopla a medios 47 de control de acceso para controlar el acceso a la información. La información de acceso extraída mediante lectura está disponible para procesar adicionalmente en la salida 48 de los medios 47 de control de acceso. Durante la lectura el cabezal 41 de lectura se coloca en la pista

mediante un servomotor 44 del tipo habitual, mientras el soporte de grabación se rota mediante una unidad 45 de motor. La lectura de la información se controla a través de un controlador 46, controlador que controla la unidad 45 de motor, el servomotor 44 y la unidad 43 de corrección de errores, y se dispone para recibir instrucciones de lectura, por ejemplo a través de una interfaz, para los medios 47 de control de acceso.

La extracción mediante lectura de la información de acceso se realizará de la siguiente manera. Los medios de control de acceso extraerán mediante lectura los bits de información de acceso cifrados desde la zona PIC. Al usar las técnicas de detección de integración y el método de (des)cifrado usado sobre estos bits, los medios de control de acceso pueden recuperar la información de acceso. Al usar esta información de acceso, que puede, por ejemplo, ser una clave de descifrado para descifrar la información de usuario cifrada, se proporciona acceso a la información de usuario. En el caso de que el soporte de información no comprenda la información de acceso, o el aparato no pueda extraer mediante lectura la información de acceso, se rechazará el soporte de información y se prohibirá el acceso a la información de usuario.

La figura 6 muestra una realización del uso de la información de acceso para dar acceso a la información de usuario. Se muestra qué información 16 de usuario se extrae mediante lectura a partir del soporte 1 de información, por ejemplo usando el aparato tal como se muestra en la figura 4. La información 17 de acceso se detecta en un módulo 18 de detección. El módulo de detección tiene conocimiento del método de cifrado usado para cifrar los bits de información de acceso. Los bits de información de acceso cifrados se detectan en primer lugar usando la detección de integración y luego se descifran. Al usar esta información de acceso detectada la clave de descifrado se calcula en el módulo 19. Como una entrada adicional para el método de (des)cifrado, puede usarse un número 20 aleatorio. Este número puede ser el número aleatorio usado para permutar los bits tal como se describe con referencia a la figura 2. Este número puede ser un número oculto en el soporte de información, pero también puede introducirse por el usuario del aparato. La clave calculada se usa en el módulo 21 de descifrado para descifrar la información de usuario. Tras el descifrado de la información de usuario esta información se procesa o emite adicionalmente. Esto puede depender de la detección de la información de acceso correcta. Los módulos 18, 19 y 21 pueden suministrarse a los fabricantes de IC en código VERILOG. Debido a esto, ninguna información sobre la detección de información de acceso o el cálculo de clave deben darse a conocer, ya que esto tiene lugar dentro del bloque 22 VERILOG.

La figura 7 muestra una realización del módulo de detección usado en el aparato. En esta realización se suministra el módulo 18 de detección como un código VERILOG. El inicio de sector y de sincronización de trama se introduce a este módulo de detección ya que éstos se necesitan para encontrar las ubicaciones de bits de clave de oscilación que comprenden los bits de información de acceso. El inicio de bloque de ECC se introduce ya que éste se necesita para conocer la secuencia de permutación de los bits de información de acceso cifrados. El AUN se introduce ya que éste se necesita en la generación de semilla en el método de cifrado. Todas las señales se suministran síncronas con la sincronización de trama en la información de usuario, introducidas en el módulo de detección tras la conversión de A/D. Tras el descifrado de los bits de información de acceso, el módulo de detección emite la información de acceso, por ejemplo como una clave para descifrar la información de usuario.

Aunque la invención se ha aclarado con referencia a las realizaciones descritas anteriormente, será evidente que pueden usarse alternativamente otras realizaciones para lograr el mismo objetivo. El alcance de la invención, por tanto, no se limita a las realizaciones descritas anteriormente, sino también pueden aplicarse a todas las clases de soportes de información, tipos de soportes de regrabación o grabación única, de sólo lectura. El alcance de la invención no se limita además a determinadas clases de información de acceso. Toda la información que está o puede usarse como información de acceso, es decir información usada para proporcionar acceso a la información de usuario almacenada o que va a almacenarse en el soporte de información según la invención, se encuentra dentro del alcance de la invención. El alcance de la invención no se limita además a determinadas técnicas de canal oculto o determinados canales laterales (ocultos). Todas las técnicas y canales que pueden usarse para almacenar información se encuentran dentro del alcance de la invención. Además, la invención no se limita a técnicas de espectro ensanchado en las que la información de acceso se almacena en un pequeño recorrido radial del presurco oscilante. Todos los parámetros físicos pueden usarse para introducir un pequeño cambio en una propiedad detectable para almacenar información detectable de integración en un soporte de información.

La invención puede resumirse de la siguiente manera. La invención se refiere a un soporte de información tal como se define en la reivindicación 1. Cifrando los bits de información de acceso según un método de cifrado predeterminado, la detección de la información de acceso no es posible mientras que no se conozca el método de cifrado. El uso de la técnica de detección de integración sólo da como resultado la información de acceso, si se conoce cómo debe procesarse la señal obtenida tras la extracción mediante lectura del área que comprende los bits de información de acceso. De esta forma, se impide adicionalmente la recuperación ilegal de la información de usuario.

REIVINDICACIONES

1. Soporte de información para contener la información de usuario, comprendiendo el soporte de información la información de acceso en forma de bits de información de acceso para acceder a la información de usuario, estando los bits de información de acceso almacenados en el soporte de información en una variación de un parámetro físico, estando los bits de información de acceso presentes en tramas claves, caracterizado porque la variación tiene una amplitud pequeña, basándose en una técnica de espectro ensanchado, para poder detectarse sólo mediante la detección de integración, y porque los bits de información de acceso se cifran según un método de cifrado predeterminado, método de cifrado que comprende una permutación de los bits de información de acceso, permutación que es diferente para cada trama clave.

2. Soporte de información según la reivindicación 1, en el que los bits de información de acceso se cifran almacenando determinados bits de información de acceso predeterminados invertidos en el soporte de información.

3. Soporte de información según la reivindicación 1, en el que los bits de información de acceso se cifran cambiando la secuencia de los bits de una manera casi aleatoria predeterminada.

4. Soporte de información según la reivindicación 1, 2 ó 3, comprendiendo el soporte de información un presurco oscilante, y los bits de información de acceso se almacenan en la variación del recorrido radial del presurco oscilante.

5. Soporte de información según la reivindicación 1, en el que el método de cifrado está oculto en el soporte de información.

6. Soporte de información según la reivindicación 5, en el que el método de cifrado está oculto en el recorrido radial del presurco oscilante.

7. Soporte de información según la reivindicación 5 ó 6, comprendiendo el soporte de información una área especial que comprende los bits del método de cifrado que indican el método de cifrado predeterminado según el cual se cifran los bits de información de acceso.

8. Soporte de información según la reivindicación 7, en el que los bits del método de cifrado se almacenan en el soporte de información en una variación de un parámetro físico, variación que puede detectarse sólo mediante la detección de integración.

9. Soporte de información según la reivindicación 7 u 8, en el que el área especial comprende 8 bits del método de cifrado.

10. Soporte de información según una cualquiera de las reivindicaciones 1 a 9, comprendiendo el soporte de información una zona de datos de información y control permanente (PIC), la información de acceso se almacena en unidades de dirección en la zona PIC y se deriva una semilla de cifrado a partir de números de dirección (AUN) de respectivas unidades de dirección en la zona PIC.

11. Soporte de información según la reivindicación 10, en el que la información de acceso se almacena en la zona PIC en microsurcos-pasos pregrabados o en surcos modulados de alta frecuencia pregrabados.

12. Aparato para extraer mediante lectura la información de un soporte de información según una cualquiera de las reivindicaciones 1 a 11, comprendiendo el aparato una unidad de lectura para extraer mediante lectura la información de usuario y medios de control de acceso para detectar dicha variación que tiene una pequeña amplitud mediante la detección de integración, recuperando así la información de acceso del soporte de información,

en el que los medios de control de acceso están dispuestos para el descifrado e integración basándose en dicha diferente permutación de los bits de información de acceso en las tramas claves y para proporcionar acceso a la información de usuario en dependencia de la información de acceso descifrada.

13. Aparato según la reivindicación 12, en el que, mientras el soporte de información comprende un presurco oscilante y los bits de información de acceso se almacenan en la variación del recorrido radial del presurco oscilante, la unidad de lectura se adapta para leer dichos bits de información de acceso a partir de dicha variación del recorrido radial del presurco oscilante.

14. Aparato según la reivindicación 12, en el que, mientras el método de cifrado está oculto en el soporte de información, comprendiendo el soporte de información una área especial que comprende bits del método de cifrado que indican el método de cifrado predeterminado según el cual se cifran los bits de información de

acceso, los medios de control de acceso están adaptados para el descifrado de los bits de información de acceso en dependencia de los bits del método de cifrado.

15. Aparato según la reivindicación 12, en el que los medios de control de acceso están integrados en un bloque VERILOG.

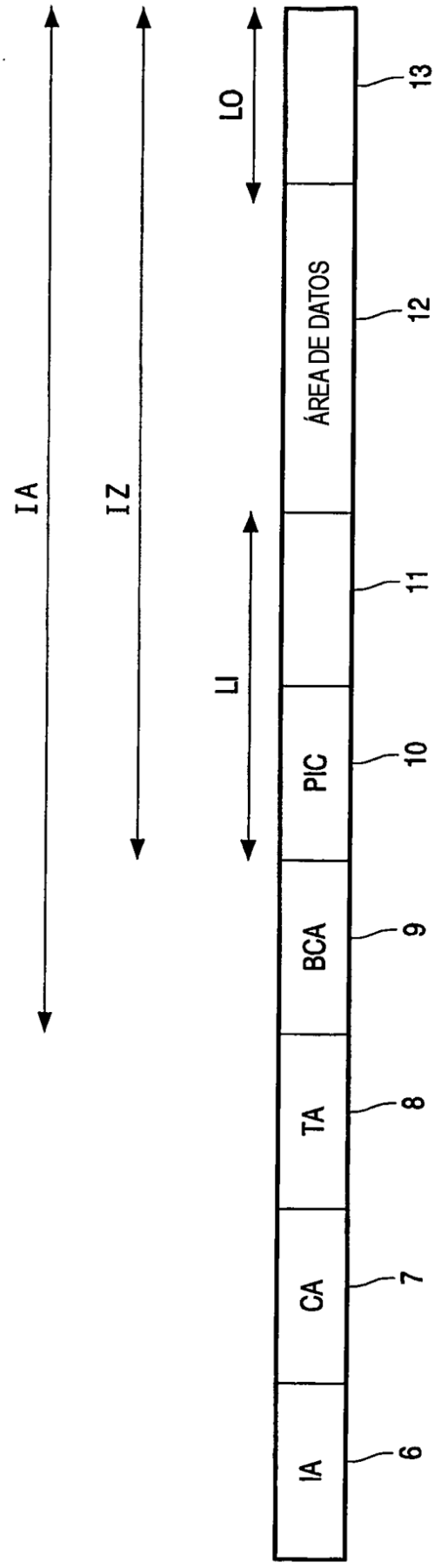

FIG.1

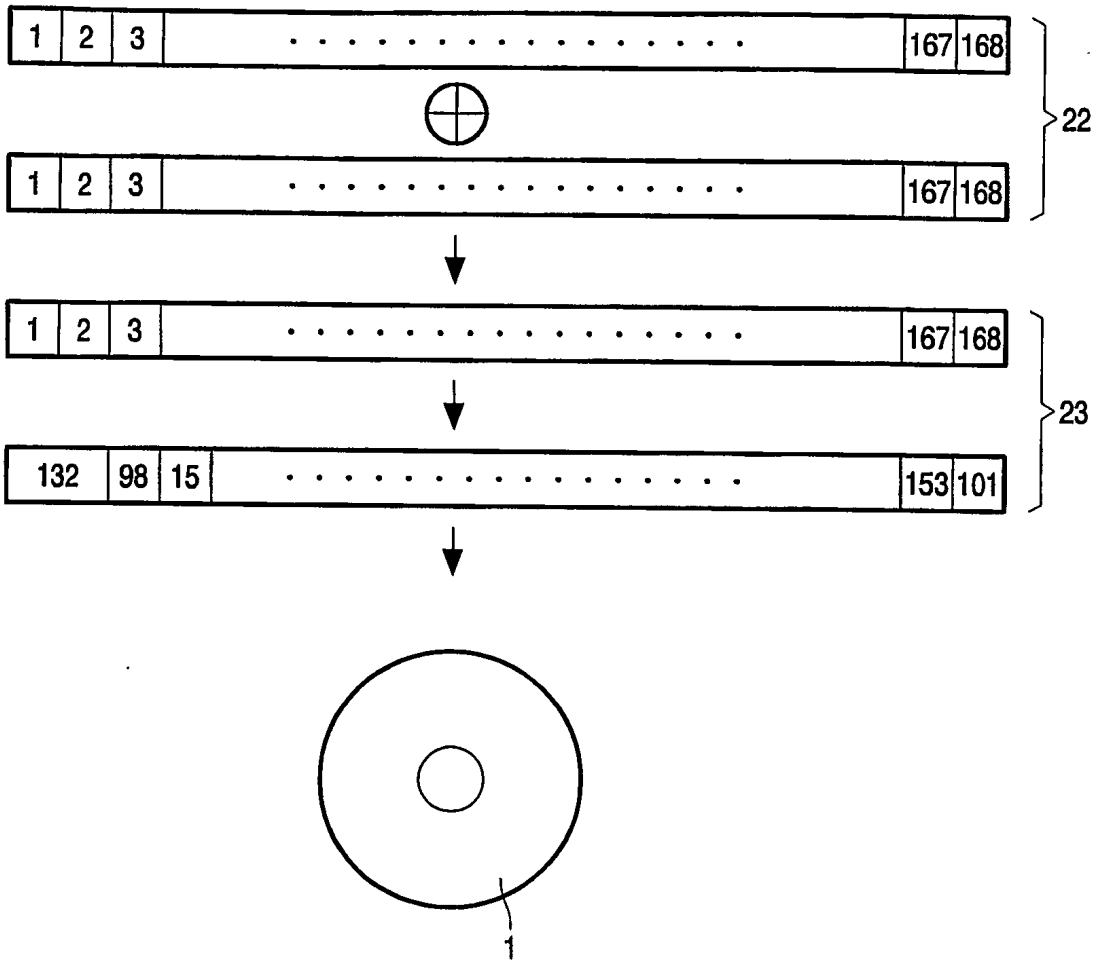

FIG.2

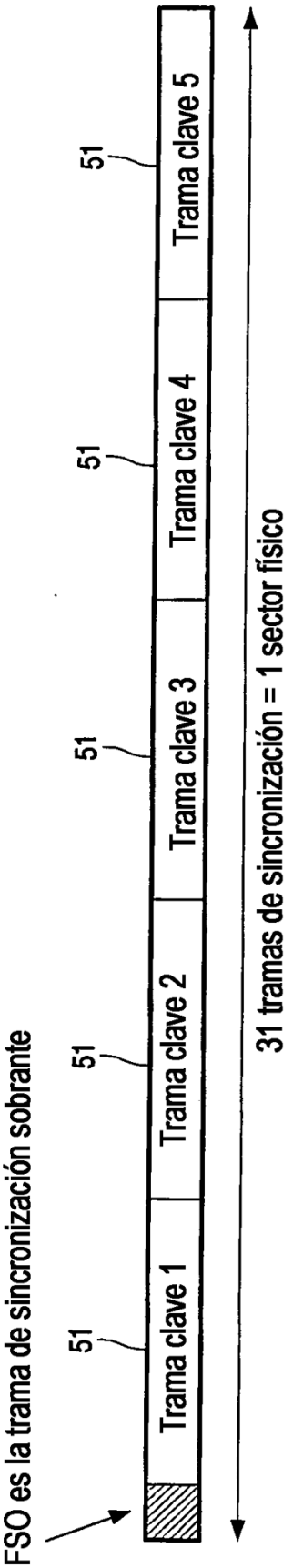
FSO es la trama de sincronización sobrante
Trama clave 1
Trama clave 2
Trama clave 3
Trama clave 4
Trama clave 5
51
51
51
51
51
31 tramas de sincronización = 1 sector físico

FIG.3

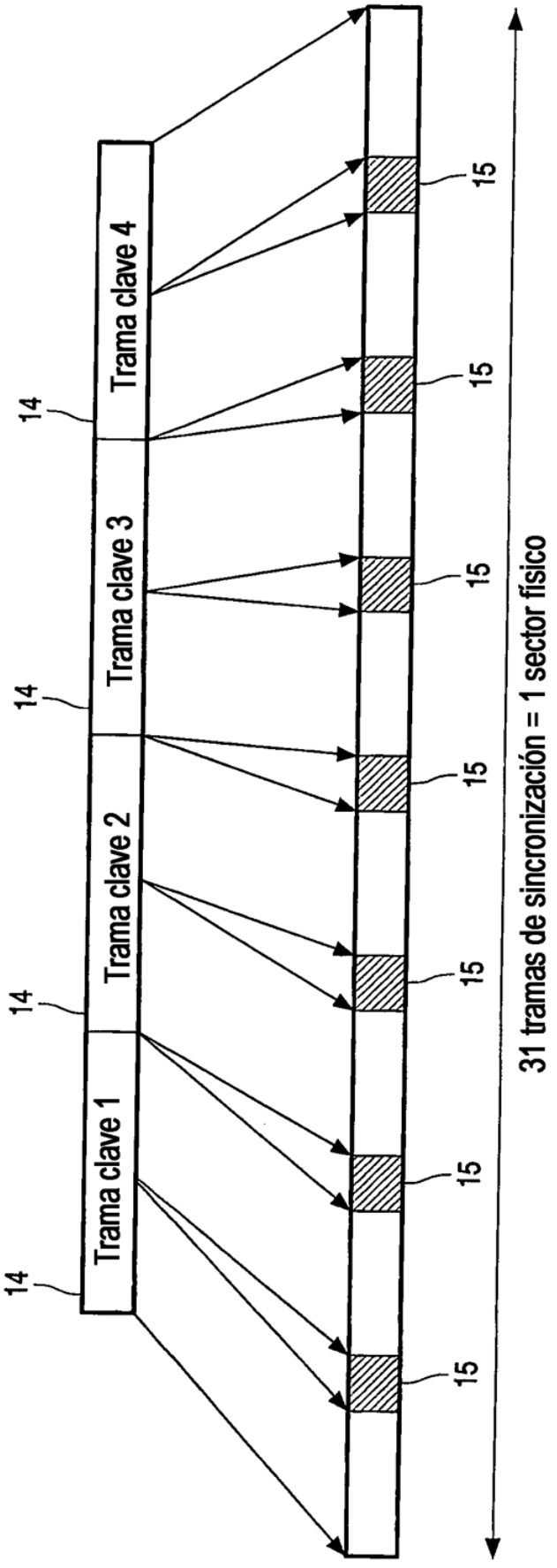
Trama clave 1
Trama clave 2
Trama clave 3
Trama clave 4
14
15
31 tramas de sincronización = 1 sector físico

FIG.4

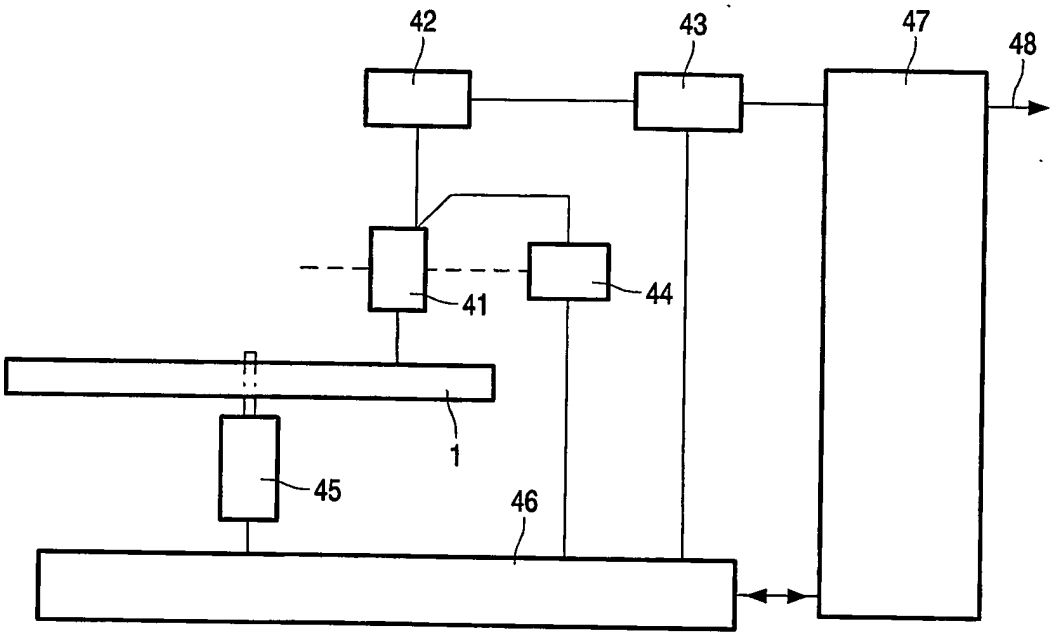

FIG.5

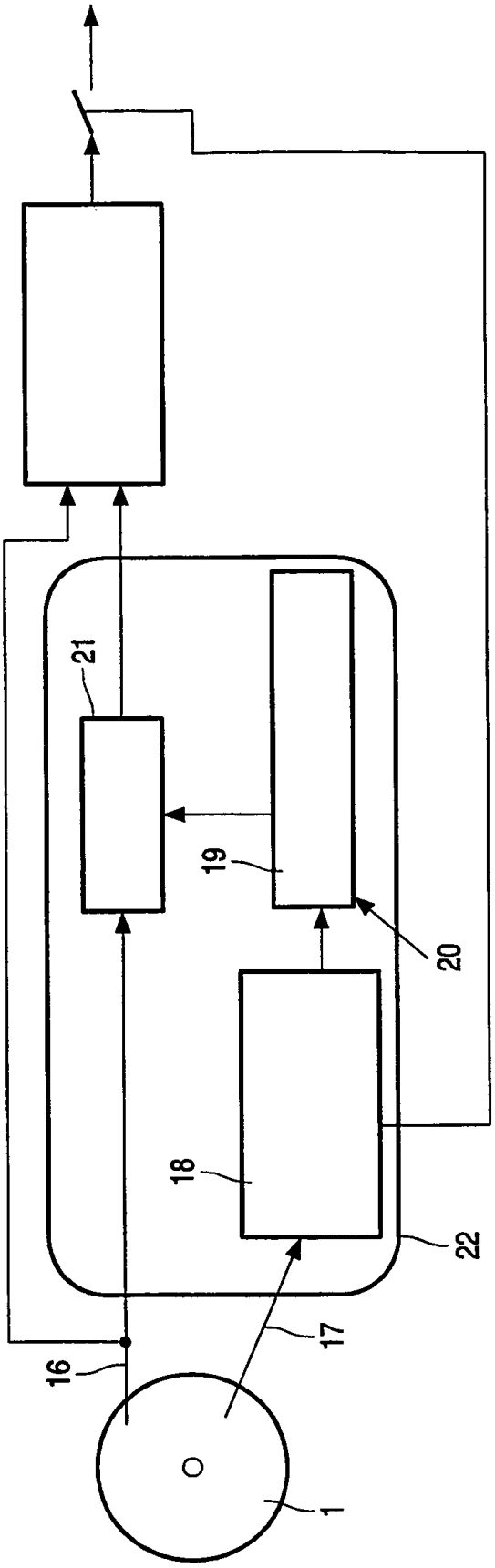

FIG.6

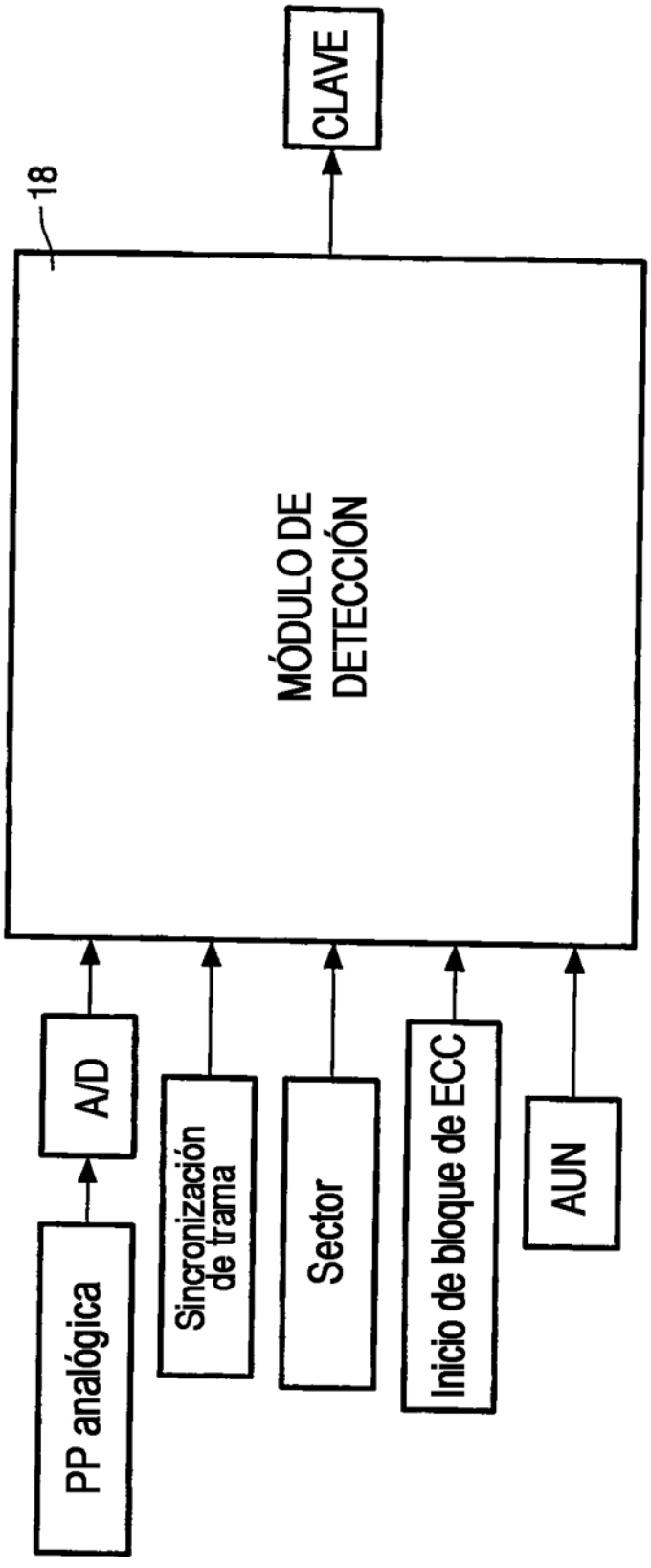
CLAVE
18
MÓDULO DE DETECCIÓN
A/D
PP analógica
Sincronización de trama
Sector
Inicio de bloque de ECC
AUN

FIG.7