(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 384 953**

(51) Int. CI.:
H04N 7/167 (2011.01)
H04N 5/913 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **01000422 .4**
(96) Fecha de presentación: **05.09.2001**
(97) Número de publicación de la solicitud: **1187477**
(97) Fecha de publicación de la solicitud: **13.03.2002**

(54) Título: **Aparato de recepción y de grabación de información y un procedimiento asociado**

(30) Prioridad:
07.09.2000 FR 0011434

(45) Fecha de publicación de la mención BOPI:
16.07.2012

(45) Fecha de la publicación del folleto de la patente:
16.07.2012

(73) Titular/es:
SAGEMCOM BROADBAND SAS
250, route de l'Empereur
92500 Rueil Malmaison, FR

(72) Inventor/es:
Chevreul, Jean-Jacques

(74) Agente/Representante:
de Elzaburu Márquez, Alberto

DESCRIPCIÓN

Aparato de recepción y de grabación de información y un procedimiento asociado.

La invención tiene por objeto un aparato de recepción y de grabación de información y un procedimiento asociado. El ámbito de la invención es el de los aparatos que pueden recibir informaciones y almacenar estas informaciones. Además tales aparatos deben asegurar un acceso limitado y controlado a las informaciones almacenadas. Tales aparatos son por ejemplo receptores descodificadores de televisión que permiten grabar programas difundidos a través de un flujo de televisión.

Un objetivo de la invención es asegurar un cifrado firme de las informaciones grabadas en medios de almacenamiento de informaciones del aparato. Otro objetivo de la invención es favorecer la utilización de medios de almacenamiento estándares en tales aparatos.

En el estado de la técnica se conocen receptores descodificadores de televisión que comprenden medios que les permiten grabar programas recibidos a través de un flujo de televisión. Estos medios son utilizados en reemplazamiento de un magnetoscopio para grabar un film completo, o bien para evitar que un usuario del receptor descodificador de televisión pierda una parte de la emisión que está viendo si éste se ve obligado a alejarse de su receptor de televisión. En el caso de verse obligado a alejarse, éste activa un modo diferido lo que provoca la grabación por el aparato de la emisión que el usuario está viendo. Cuando éste está de nuevo en condiciones de mirar a su pantalla de televisión, el usuario visualiza entonces la emisión a partir del momento en que éste ha tenido que ausentarse, el aparato continúa grabando la emisión en tiempo real. Así, con respecto a la difusión de la emisión el usuario la visualiza ligeramente con un retardo. El retardo corresponde al tiempo de su ausencia. Si se utiliza el medio de almacenamiento para reemplazar a un magnetoscopio entonces el usuario pone en marcha la grabación y puede elegir revisualizar las informaciones grabadas como bien le parezca.

Los aparatos del estado de la técnica utilizan varias formas de los medios de almacenamiento. Una primera forma consiste en utilizar la memoria flash. En general, este tipo de memoria se presenta en forma de tarjeta inteligente y está directamente soldado al circuito electrónico principal del aparato. La ventaja de este sistema es que no está previsto en el aparato ningún puerto de comunicación para ir a leer el contenido de estas memorias, el contenido de estas memorias solamente es accesible por un microprocesador del aparato. Así, las informaciones contenidas en estas memorias no son disociables del receptor descodificador. El inconveniente de este modo de realización es que este tipo de memoria es muy caro. Así pues, este modo de realización se emplea en general solamente para una aplicación de tipo visualización diferida, y cuando el tiempo de desfase no es demasiado importante. En efecto, para grabar una emisión que dure aproximadamente dos horas, hay que contar aproximadamente con 5 Go de memoria. Actualmente, esto es totalmente inconcebible, económicamente, utilizando memorias flash.

Otro modo de realización del estado de la técnica es utilizar unidades de almacenamiento tradicionales. Por tradicional pueden comprenderse discos duros de tipo disco duro de ordenador personal. Estos discos son relativamente económicos y tienen capacidades compatibles con las aplicaciones que se deseen efectuar. En efecto, la utilización de un disco permite realizar a la vez la aplicación de visualización diferida y la aplicación de magnetoscopio. Además, la utilización de tales discos permite modificar de modo simple la configuración de hardware de un receptor descodificador. En efecto, utilizando discos por ejemplo IDE es muy fácil desmontar una envuelta del aparato y cambiar dicho disco duro, sobre todo si las conexiones con este disco duro son establecidas a través de un controlador IDE estándar y una capa IDE. Esta operación habrá podido ser voluntariamente prevista por el constructor con el fin de permitir por ejemplo la compra posterior de la opción de disco o el reemplazamiento por el usuario del disco inicial cuando unidades de disco de más capacidad estén disponibles.

Sin embargo, esta solución presenta inconvenientes en cuanto a la accesibilidad a los datos grabados en el disco duro. En efecto, como acaba de decirse, el disco duro es fácilmente accesible desmontando la caja del aparato de recepción descodificación. Entonces, resulta fácil extraer el disco duro de la caja de recepción de televisión y conectarle a un ordenador personal para recuperar los datos que están escritos en él. En la medida en que estos datos son digitales y por tanto casi inalterables, el poseedor de tal disco duro está entonces en condiciones de realizar tantas copias como desee de la información que está grabada en él. Además, estas copias serán de una calidad irreprochable con respecto a la original. Se han previsto soluciones de cifrado para cifrar las informaciones grabadas en estos discos duros. Sin embargo, estas soluciones son puestas en práctica por softwares que son ejecutados por lógica de mando de la caja de recepción de televisión. Al cabo de un cierto tiempo, en general relativamente corto, estos softwares son accesibles especialmente a través de Internet. Es entonces posible extraer la información cifrada del disco duro conectándole a un ordenador personal y ejecutar el programa de descifrado en el ordenador personal. Así pues, en el estado de la técnica, una vez grabada una información en un disco duro, no es posible controlarla.

La técnica anterior conoce por la solicitud de patente europea Nº EP-A-0 961 787, un aparato de acuerdo con el preámbulo de la reivindicación 1.

La invención resuelve este problema cifrando las informaciones de una manera apropiada para cada aparato de recepción descodificación de televisión. Esto equivale de hecho a emparejar el aparato y las informaciones

contenidas en un medio de almacenamiento. Además, las informaciones no cifradas no son fácilmente accesibles en el aparato de acuerdo con la invención. La información es recibida por el aparato, a través de una antena por ejemplo, tal como ha sido emitida por el productor de esta información. Esta información recibida es sometida entonces a un cierto número de tratamientos en el aparato. La información, antes de ser escrita en el dispositivo de almacenamiento, por ejemplo un disco duro, pasa por un dispositivo de cifrado. El dispositivo de cifrado está, por una parte, conectado a un bus del aparato, por otra parte conectado por ejemplo a un controlador IDE. El controlador IDE permite utilizar un disco estándar del mercado como medio de almacenamiento. Las informaciones que circulan entonces por el bus IDE están cifradas. Mientras que las informaciones que circulan por el primer bus no lo están. Sin embargo, no es fácil acceder a las informaciones del primer bus. En efecto, para esto habría que manipular la tarjeta electrónica principal del descodificador. El dispositivo de cifrado utiliza una clave propia del aparato para cifrar las informaciones que hay que grabar.

Este dispositivo puede utilizar principios de cifrado de tipo bloque por ejemplo DES (Data Encryption Syste), o incluso “scrambling type DVB”, o de tipo “stream” más simple que utiliza un generador de secuencia seudoaleatoria. La clave que sirve para este cifrado está preferentemente oculta en el descodificador. Por ejemplo, la clave es escrita en una memoria de tipo EEPROM en la fabricación del aparato de recepción descodificación. La EEPROM es bloqueada entonces a fin de que no se pueda leer su contenido. La clave de cifrado específica de cada unidad de este tipo de aparato es preferentemente determinada por un proceso aleatorio, por ejemplo la medición de un ruido blanco. En una variante de la invención, la clave de cifrado es modificada por uno o unos atributos apropiados para las informaciones que hay que cifrar. Esto hace todavía más firme al proceso de cifrado.

Así pues, la invención tiene por objeto un aparato de recepción y de descodificación de información que comprende medios para recibir un flujo de información, medios para extraer de este flujo informaciones, medios para efectuar tratamientos en estas informaciones, medios para almacenar estas informaciones caracterizado porque:

- los medios para tratar comprenden un dispositivo de cifrado para cifrar, antes de la grabación en los medios de almacenamiento, informaciones procedentes del flujo de información,

- el dispositivo de cifrado comprende una memoria no volátil para grabar una clave de cifrado específica de cada aparato.

La invención tiene también por objeto un procedimiento de recepción y de descodificación de información en el cual:

- se recibe un flujo de información,

- se extraen informaciones de este flujo

- se graban estas informaciones en una unidad de almacenamiento, caracterizado porque:

- se lee una clave de cifrado propia de cada aparato poniendo en práctica el procedimiento y pregrabada en una memoria no volátil,

- se cifran informaciones extraídas a partir de la clave de cifrado,

- se graba el resultado del cifrado en la unidad de almacenamiento.

La invención se comprenderá mejor con la lectura de la descripción que sigue, y el examen de las figuras que la acompañan. Las figuras muestran:

- Figura 1: una ilustración de medios útiles para la realización de un aparato de acuerdo con la invención;

- Figura 2: una ilustración de etapa del procedimiento de acuerdo con la invención.

En la descripción que sigue, el dispositivo de cifrado del tipo “stream cyphering” basado en la utilización de un generador de secuencia seudoaleatoria se describe solamente a título de ejemplo de dispositivo de cifrado. La figura 1 muestra un aparato 101 de acuerdo con la invención. En la descripción, se considera que el aparato 101 es una caja 101 de receptor descodificador de televisión. La caja 101 comprende una antena 102 conectada a circuitos 103 de desmodulación y de desmultiplexado. En la ilustración, se considera que la antena 102 permite establecer un enlace 104 hertziano con un satélite 105. Un flujo de información difundido por el satélite 105 a través del enlace 104 es controlado por un operador de televisión. En la práctica, el flujo de información de televisión puede llegar a la caja 101 a través de cualquier otro modo de conexión, por ejemplo una conexión cableada. Las informaciones llegan a la caja 101 a través de la antena 102 en una forma modulada. Los circuitos 103 permiten desmodular estas informaciones y extraer entre todas las presentes en el flujo de información aquéllas que están destinadas al usuario de la caja 101. Estas etapas de extracción de la información son bien conocidas en el ámbito de los receptores descodificadores de televisión.

La antena 102 y el circuito 103 constituyen por tanto medios para recibir un flujo de información.

El circuito 103 está conectado a un primer bus 106. Se recuerda que un bus es un conjunto de hilos o de pistas que comprenden elementos en número suficiente para transportar señales de datos, de direcciones, de mandos, de interrupciones, de reloj y de alimentación.

El bus 106 está también conectado a un dispositivo 107 de cifrado. El dispositivo 107, así como los otros dispositivos de la caja 101 son mandados por un microprocesador 108, a su vez mandado por códigos de instrucciones contenidos en una memoria 109. El microprocesador 108 y la memoria 109 están también conectados al bus 106. La memoria 109 comprende varias zonas. Entre estas zonas, la memoria 109 comprende una zona 109a en la cual están grabados códigos de instrucciones que mandan el microprocesador cuando éste efectúa acciones relativas a la descodificación de informaciones codificadas de acuerdo con la norma MPEG2. En efecto, las informaciones de vídeo recibidas por la caja 101 están generalmente codificadas en el formato MPEG2. La memoria 109 comprende igualmente una zona 109C de vídeo en la cual informaciones de audio y vídeo son almacenadas primero en forma codificada MPEG2 y después en forma descodificada después de su tratamiento por un descodificador de audio y vídeo 110. Este descodificador 110 de audio y vídeo está conectado, por una parte, al bus 106 y, por otra, a un conector 111 que permite conectar una pantalla 112 de televisión a la caja 101. Esta conexión se hace por ejemplo a través de una toma peritelevisión 113. La memoria 109 comprende también códigos de instrucciones que permiten gestionar señales producidas por un dispositivo 114, conectado al bus 106, receptor de infrarrojos. El dispositivo 114 recibe ondas infrarrojas emitidas por el usuario de la caja 101, a través de un mando a distancia 115. El mando a distancia 115 permite al usuario de la caja 101 mandar esta caja. Entre otros, éste le permite elegir qué programa debe descodificar la caja 101 y visualizar en la pantalla 112, elegir grabar informaciones en un disco duro 116 de la caja 101, elegir releer las informaciones en el disco duro 116. El disco duro 116 está conectado al dispositivo 107 de cifrado a través de un segundo bus 117. Por otra parte, el segundo bus 117 está conectado a un controlador IDE que asegura la interfaz entre el bus 117 y el dispositivo de cifrado 107. Así, a través del bus 106 son facilitadas informaciones en claro al dispositivo 107 que las cifra y las coloca a disposición del controlador 118 IDE para que éste envíe las órdenes de escritura al disco 116. De esta manera, todas las informaciones que circulan por el bus 117, el bus que es fácilmente accesible al usuario de la caja 101, están cifradas igual que las informaciones escritas en el disco duro 116. En el ejemplo se considera que se utiliza un disco duro que tiene una interfaz IDE. En la práctica, pueden ser utilizadas otras interfaces, especialmente ultra-DMA o SCSI.

El dispositivo 107 comprende una memoria 119 par grabar una clave de cifrado. Una clave de cifrado es un número que se codifica con un cierto número de bits. La longitud de la clave podrá ser cualquiera, pero en la práctica convendrán perfectamente 32 o 48 bits. El dispositivo 107 comprende varios elementos entre los cuales la memoria 119. Estos elementos han sido representados de manera separada a fin de simplificar la explicación. Pero en la práctica, todos estos elementos están implantados en un solo y mismo componente, por ejemplo de tipo EPLD. Un EPLD es un componente eléctricamente programable. Un componente de este tipo puede ser programado, y en general su programación no puede ser releída, lo que garantiza la confidencialidad de su función. La memoria 119 está por ejemplo escrita con un número generado de manera aleatoria. La generación de este número aleatorio puede hacerse por ejemplo por la medición de un ruido blanco. Dicho ruido blanco puede ser medido con la ayuda de un sensor que mide un ruido ambiente y convierte una medición en un instante dado en una muestra digital. Esta muestra es entonces la clave de cifrado que será grabada en la memoria 119.

La memoria 119 está conectada a un circuito 120 de modificación de clave. El circuito 120 modifica la clave 119 en función de informaciones transmitidas al circuito 120 a través del bus 106. Esta modificación puede ser efectuada en función de un cierto número de elementos. Entre estos elementos, puede citarse un atributo de la grabación que hay que efectuar o un número de bloque grabado. En efecto, el disco 116, o la información que hay que grabar, pueden ser divididos en bloques. Este atributo o el número de bloque pueden servir entonces para producir la clave de cifrado por modificación de la clave 119.

Como se señaló anteriormente, el dispositivo de cifrado 122 puede ser de cualquier naturaleza, la descripción que sigue da el ejemplo simple de un cifrado de flujo (stream cyphering) basado en la utilización de un generador de secuencia seudoaleatoria. La modificación de la clave 119 permite modificar los parámetros de inicialización de un circuito 121 de generación de secuencias seudoaleatorias. El circuito 121 está conectado, por una parte, al circuito 120 y, por otra, a un circuito 125 de mando del dispositivo 122. La utilidad de modificar la clave es que el tratamiento efectuado por el dispositivo 107 varía entonces de un programa de cifrado a otro, lo que hace la determinación de la función del dispositivo 107 y sobre todo de la clave 119, todavía más dura. En este sentido, es posible utilizar un suceso aleatorio, por ejemplo la hora de inicio de grabación, para modificar la clave. Sin embargo, hay que guardar una traza de los parámetros utilizados para realizar el cifrado y esto, a fin de que el cifrado sea posible. En general, los parámetros de modificación de la clave son grabados en un formato conocido y en un encabezamiento no cifrado de la información cifrada.

El circuito 121 genera, a partir de su secuencia de inicialización, una secuencia de números seudoaleatorios. En la práctica, un generador de números seudoaleatorios funciona a partir de un número inicial que se le facilita y de un cierto número de registros diferidos. El resultado de desfases permite producir a la salida un número. Esos registros son reciclados sobre sí mismo de diversas maneras a fin de producir un flujo continuo de números. Este circuito es denominado de generación de secuencias seudoaleatorias porque la secuencia de números que genera depende de sus condiciones de inicialización. Estas condiciones de inicialización dependen a su vez de la clave grabada en la memoria 119 y de los parámetros aplicados al modificador de clave 120. Un circuito de generación de secuencias

aleatorias de este tipo genera una secuencia idéntica para condiciones de inicialización idénticas. Es por esto por lo que se le atribuye este calificativo de seudo.

En el ejemplo elegido, la unidad 122 de cifrado incluye el generador 121 de secuencia seudoaleatoria. La salida del circuito 121 está conectada a una primera puerta XOR (O EXCUSIVO) 123 de la unidad 122. La unidad 122 está también conectada al bus 106. En una segunda entrada de la puerta 123 se aplican señales de datos procedentes del bus 106. Así, la puerta 123 efectúa una operación de O EXCLUSIVO entre elementos procedentes de la parte datos del bus 106, y elementos generados por el circuito 121. La salida de la puerta 123 está conectada a una entrada de datos del controlador 118 IDE. La puerta 123, por otra parte, está conectada al circuito 125 de mando. El circuito 125 está conectado a la parte de mando del bus 106. El circuito 125 asegura por tanto el mando a los diferentes elementos del dispositivo 122, y esto a partir de órdenes recibidas a través del bus 106. El microprocesador 108 manda por tanto el dispositivo 122 a través del bus 106 y el circuito 125. Así, es posible que el microprocesador 108 mande la actividad de la puerta 123. El microprocesador 108 puede así mandar la propia combinación, es decir si la combinación es efectuada o no. En efecto, sigue siendo posible escribir informaciones en el disco 116 sin que éstas sean cifradas por el dispositivo 107. Para esto, basta que el microprocesador 108 desactive la puerta 123, entonces los elementos a la salida de la puerta 123 serán idénticos a los elementos transportados por la parte datos del bus 106.

La figura 1 muestra también que la unidad 122 comprende una segunda puerta 124 XOR. La salida de la puerta 124 está conectada a la parte de datos del bus 106. Una entrada de la puerta 124 está conectada a la salida del circuito 121. Una segunda entrada de la puerta 124 está conectada a la entrada de datos del controlador 118 IDE. Por otra parte, la puerta 124 está conectada al circuito 125. Así, la puerta 124 puede ser mandada de la misma manera que la puerta 123. En la práctica, el microprocesador 108, mandado por los códigos de instrucciones de la memoria 109, activa la puerta 123 cuando éste debe efectuar una escritura en el disco 116. El microprocesador 108 activa la puerta 124 cuando éste debe efectuar una operación de lectura en el disco 116. Para las operaciones de lectura y de escritura, el circuito 125 está conectado al controlador 118 IDE. Naturalmente, el controlador 118 asegura a la vez la traducción de los mandos y la transferencia de los datos del dispositivo 107 hacia el disco 116 y esto a través del bus 117. En una variante de la invención, se prescinde del circuito 125 y se conecta directamente la parte de mando del bus 106 a los elementos 121, 123, 124 y 118.

La figura 2 muestra una etapa 201 preliminar correspondiente a la recepción de un flujo de informaciones por el aparato 101. En la etapa 201, el aparato 101 recibe, a través de la antena 102, informaciones en forma modulada. Estas informaciones son desmoduladas por el circuito 103. Se pasa a una etapa 202 de extracción de los datos. En la etapa 202, el microprocesador 108, mandado por los códigos de instrucciones de la zona 109a, manda el circuito 103 para que éste seleccione, entre las informaciones recibidas, informaciones pertinentes y eventualmente descifre estas informaciones pertinentes.

Estas informaciones seleccionadas son finalmente escritas, a través del bus 106, en la zona 109C en la que éstas quedan a disposición del microprocesador 108. En el ejemplo, se considera que las informaciones pertinentes corresponden a un programa de vídeo. El usuario del aparato 101 ha dado una orden gracias al mando a distancia 115 para que el programa de vídeo actualmente recibido quede grabado en el disco duro 116. Así pues, en la etapa 202 se extrae del flujo de informaciones recibidas por el aparato 101 informaciones que corresponden al programa de audio y vídeo que desea grabar el usuario del aparato 101. Se pasa entonces a una etapa 203 de suministro de la clave de cifrado personalizada a los circuitos de cifrado.

En la etapa 203, el microprocesador 108 mandado por los códigos de instrucciones de la zona 109a envía instrucciones al circuito 120. Estas instrucciones sirven al circuito 120 para modificar la clave grabada en la memoria 119. Estas informaciones comprenden también informaciones propias de las informaciones que acaba de extraer el microprocesador 108 entre las que son producidas por el circuito 103. Esta información caracteriza el programa grabado. Puede tratarse por ejemplo de su título. A partir del titulo, del programa grabado y del contenido de la memoria 119, el circuito 120 produce entonces datos de inicialización que éste envía al circuito 121. En general, este dato de inicialización es una palabra de 16, 32, 48 o más bits. Se considera aquí que el circuito 121 es un operador de secuencia seudoaleatoria.

El circuito 121 acaba de recibir una palabra de inicialización. Éste, por otra parte, recibe a través del bus 106, un mando para generar una secuencia seudoaleatoria a partir de esta palabra de inicialización. El circuito 121 comprende un cierto número de registros interconectados. En un instante dado, estos registros están en un estado dado. El circuito 121 produce entonces a partir del estado de estos registros un número que pertenece a la secuencia seudoaleatoria. Este número es utilizado en la etapa 205 de cifrado en la cual es combinado con los datos extraídos. En la práctica, la actividad del aparato 101 es regulada por un reloj. Lo mismo ocurre para la actividad de la unidad 122 que incluye el circuito 121. El circuito 121 recibe, por tanto, una señal de reloj que le indica que éste debe producir un número de la secuencia seudoaleatoria. Cada vez que el circuito 121 recibe esta señal, éste produce un número y modifica el estado de sus registros internos. El número producido depende de la palabra de inicialización. Así, a cada golpe de reloj el circuito 121 produce un número y modifica el estado de sus registros internos. El conjunto de los números producidos por el circuito 121 constituye la secuencia seudoaleatoria.

En la etapa 205, la unidad 122 combina los números producidos por el circuito 121 con las informaciones extraídas en la etapa 202. Esto está vinculado al modo de cifrado que se ha elegido describir. Otro modo de cifrado implicaría otras acciones en las etapas 203 y 205.

Se considera aquí que se está en un proceso de escritura en el disco 116. Se trata, por tanto, de hecho, de una etapa 205a. Para simplificar la explicación, se considera que el conjunto de la actividad de la unidad 122 es regulada a la misma frecuencia que la actividad del circuito 121, y que el tiempo de propagación de las señales es nulo. Así, cada vez que la unidad 122 tiene a su disposición una palabra producida por el circuito 121, éste tiene también a su disposición una palabra que forma parte de las informaciones de audio y vídeo extraídas por el microprocesador 108. A golpe de reloj, esta informaciones son sometidas a la puerta 123. Como se está en una etapa de escritura en el disco 116, el microprocesador 108 ha mandado la unidad 122 a fin de desactivar la puerta 124 y activar la puerta 123. La puerta 123 es activada en modo cifrado. Se recuerda que la puerta 123 puede ser mandada para dejar pasar las informaciones procedentes de la parte de datos del bus 106 sin cifrarlas. Las informaciones presentes a la entrada de la puerta 123 son combinadas con una función XOR. Esta palabra combinada está por tanto disponible a la salida de la puerta 123. A cada señal de reloj, la puerta 123 produce una nueva palabra combinada a partir de las palabras producidas por el circuito 121 y de las palabras extraídas por el microprocesador 108. Se pasa a una etapa 206 de escritura en el disco. En esta etapa, la actividad del controlador 118 es regulada a la misma frecuencia que la actividad del circuito 121 y que la unidad 122. El controlador 118 escribe por tanto las palabras producidas por la puerta 123 a medida que esta lleva los productos. Estas palabras quedarán escritas entonces en un archivo en el disco 116. El conjunto de estas palabras reunidas en este archivo en el disco 116 constituye el archivo cifrado.

La figura 2 muestra una segunda etapa preliminar 207. La etapa 207 corresponde a un esquema de relectura del contenido del disco 116. Se considera entonces que el contenido del disco 116 está cifrado. En la etapa 207, el microprocesador 108 mandado por los códigos de instrucciones de la memoria 109a envía una orden de lectura en el disco 116. Esta orden de lectura va acompañada de una orden para desactivar la puerta 123 y para activar la puerta 124. En un primer tiempo, la puerta 124 es activada en modo no cifrado. Es decir, que las informaciones leídas en el disco 116 son obtenidas por el procesador en la forma en que están grabadas en el disco 116. Esto permite al microprocesador 108 leer, por ejemplo, el título del programa que el aparato debe 101 debe visualizar en la pantalla 112. En efecto, la etapa 207 inicia en general un proceso de revisualización de las informaciones grabadas en el disco 116. Se trata por tanto de una primera extracción de datos del disco duro pero estos datos extraídos no están sometidos al tratamiento del dispositivo 107. Se pasa entonces de la etapa 207 a la etapa 203. En la etapa 203 el microprocesador utiliza la información que acaba de leer en el disco duro para mandar el circuito 120 que modifica la clave grabada en la memoria 119. Así pues, de esta manera se obtendrá una clave modificada que será utilizada para inicializar el circuito 121 de generación de una secuencia seudoaleatoria.

Se señala aquí que la palabra utilizada para modificar la clave durante la escritura del programa o de su relectura es idéntica. En efecto, ya se ha dicho que el generador 121 producía una secuencia seudoaleatoria función de la palabra utilizada pata inicializarlo. Si se utiliza el mismo modificador de clave, la secuencia producida será por tanto la misma. Esto es útil porque si se aplican a una muestra dada dos combinaciones sucesivas con XOR y con la misma palabra, se obtiene una función IDENTIDAD. Así, la secuencia seudoaleatoria utilizada para el cifrado de los datos y su descifrado es rigurosamente idéntica. De la etapa 203 se pasa a una etapa 205b. En la etapa 205b el microprocesador 108 manda la puerta 124 para que ésta esté en modo descifrado, es decir para que ésta efectúe una combinación entre las palabras producidas por el circuito 121 y las palabras leídas en el disco 116. Así, a la salida de la puerta 124 se tendrán palabras en claro que podrán ser utilizadas por el microprocesador 108 en una etapa 208 para escribir una imagen en la memoria 109C de vídeo.

En una variante de la invención, no se utiliza el circuito 120 sino que se utiliza directamente el contenido de la memoria 119 para inicializar el circuito 121. En este caso, se prescinde por tanto de una relectura de una información en claro en el disco duro. En efecto, no se tiene necesidad de la información que permita modificar la clave para grabar exactamente la secuencia seudoaleatoria que había servido para circular las informaciones grabadas en el disco. Sin embargo, esta variante es ligeramente más sensible al pirateo que la precedente.

REIVINDICACIONES

1. Aparato (101) de recepción y de descodificación de información que comprende medios (102, 103) para recibir un flujo de información, medios (103, 108, 109) para extraer de este flujo informaciones de audio y vídeo que hay que grabar, medios (110) para descodificar estas informaciones de audio y vídeo, medios (118, 116) para almacenar estas informaciones, que comprende:

- un dispositivo (107) de cifrado para cifrar, antes de la grabación en los medios de almacenamiento, las informaciones de audio y vídeo extraídas del flujo de información,

- el dispositivo de cifrado comprende una memoria (119) no volátil para grabar una clave de cifrado específica del aparato, quedando bloqueada la citada memoria de modo que su contenido permanece confidencial,

estando caracterizado el citado aparato porque

- el dispositivo de cifrado comprende medios (121) de generación de una secuencia seudoaleatoria destinada a cifrar las informaciones de audio y vídeo extraídas, siendo generada la citada secuencia seudoaleatoria en función de una clave de cifrado modificada a partir de la clave de cifrado contenida en una memoria bloqueada,

- y porque los parámetros de modificación de la citada clave están grabados en un formato conocido y un encabezamiento no cifrado de una información cifrada.

2. Aparato de acuerdo con la reivindicación precedente, caracterizado porque el dispositivo de cifrado comprende circuitos (120) de modificación de claves conectados a la memoria no volátil, estando configurados los citados circuitos de modo que reciben en entrada la clave de cifrado bloqueada y al menos un atributo propio de las informaciones que hay que cifrar y que facilitan en salida la clave de cifrado modificada.

3. Aparato de acuerdo con una de las reivindicaciones precedentes, caracterizado porque el dispositivo de cifrado comprende un componente (107) programable en el cual queda grabada la clave de cifrado bloqueada.

4. Aparato de acuerdo con una de las reivindicaciones 1 a 3, caracterizado porque la clave de cifrado queda oculta en el aparato en el momento de su fabricación.

5. Aparato de acuerdo con una de las reivindicaciones 1 a 4, caracterizado porque la clave de cifrado bloqueada es generada de manera aleatoria.

6. Aparato de acuerdo con una de las reivindicaciones 1 a 5, caracterizado porque los medios (121) de generación de secuencia seudoaleatoria están conectados a los circuitos de modificación de clave y a un conjunto de puertas lógicas configuradas de modo que combinan el flujo de información extraído con la secuencia seudoaleatoria generada.

7. Aparato de acuerdo con una de las reivindicaciones 1 a 6, caracterizado porque comprende:

- un primer bus (106) de datos conectado, al dispositivo de cifrado y a una pantalla (112) de televisión, por el cual circula el flujo de información no cifrado, y

- un segundo bus (117) de datos, conectado al medio de almacenamiento por intermedio del bus de cifrado, por el cual circula el flujo de información cifrado.

8. Aparato de acuerdo con una de las reivindicaciones 1 a 7, caracterizado porque el aparato es un receptor descodificador de televisión.

9. Procedimiento de recepción y de descodificación de información en el cual:

- se recibe (201) un flujo de información,

- se extraen (202) informaciones de audio y vídeo de este flujo,

- se graban (206) estas informaciones de audio y vídeo en medios de almacenamiento,

caracterizado porque:

- se genera una secuencia seudoaleatoria en función de una clave de cifrado modificada a partir de una clave de cifrado específica de un aparato de recepción y de descodificación y contenida en una memoria no volátil, quedando bloqueada la citada memoria de modo que su contenido permanece confidencial,

- se cifran informaciones de audio y vídeo extraídas a partir de la citada secuencia seudoaleatoria que es generada,

- se graba el resultado del cifrado en los medios de almacenamiento, a través de un bus de datos específico,

- los parámetros de modificación de la citada clave quedan grabados en un formato conocido y en un encabezamiento no cifrado de la información cifrada.

10. Procedimiento de acuerdo con la reivindicación 9, caracterizado porque:

- se releen (207) informaciones de audio y vídeo en la unidad de almacenamiento,

- se descifran (203 - 205) estas informaciones de audio y vídeo aplicándolas el mismo procedimiento que para el cifrado, o un procedimiento simétrico,

- se produce (208) una imagen con la ayuda de las informaciones descifradas.

11. Procedimiento de acuerdo con una de las reivindicaciones 9 a 10, caracterizado porque las informaciones recibidas y descodificadas son informaciones de televisión.

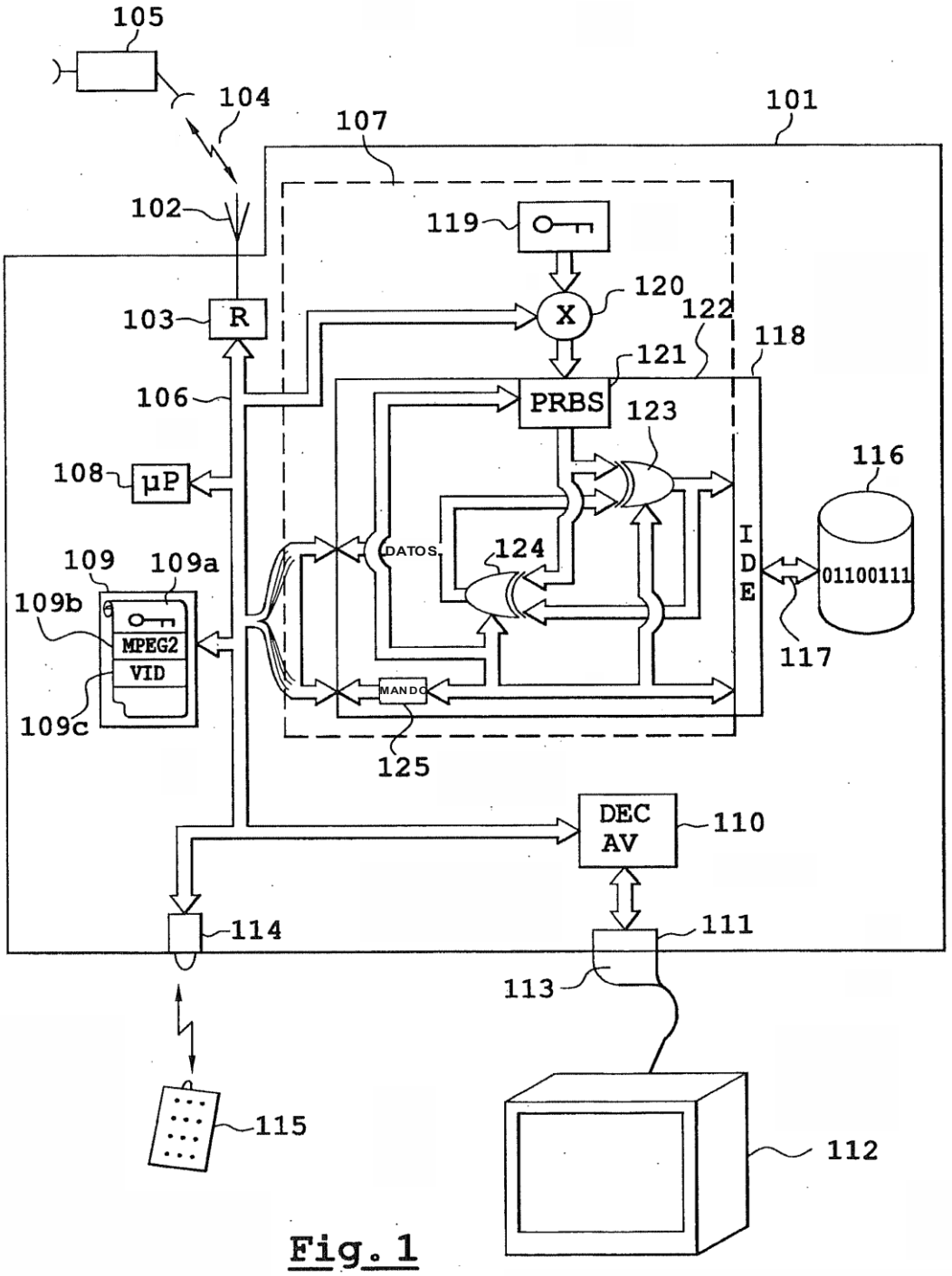
105
104
101
107
102
119
120
103
R
X
122
118
121
106
PRBS
123
116
108
µP
DATOS
124
I
D
E
109
109a
01100111
109b
MPEG2
VID
117
109c
MANDO
125
DEC
AV
110
114
111
113
115
112

Fig. 1

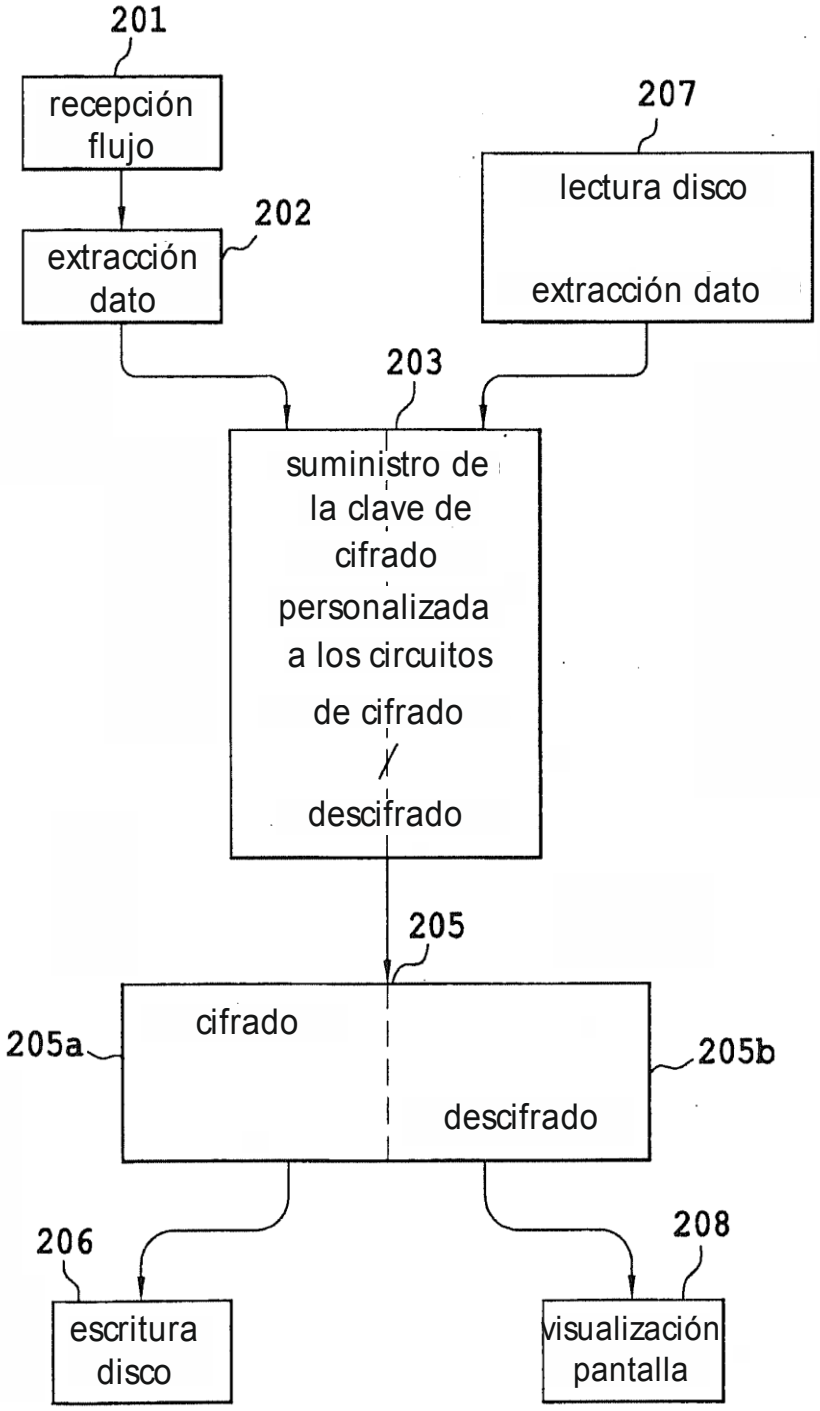
201
recepción flujo
202
extracción dato
207
lectura disco
extracción dato
203
suministro de la clave de cifrado personalizada a los circuitos de cifrado / descifrado
205
205a
cifrado
descifrado
205b
206
escritura disco
208
visualización pantalla

Fig. 2