(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 315 219**

(51) Int. Cl.:
H04N 5/913 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **00201277 .1**
(96) Fecha de presentación : **07.04.2000**
(97) Número de publicación de la solicitud: **1143722**
(97) Fecha de publicación de la solicitud: **10.10.2001**

(54) Título: **Sistema de cifrado y descifrado de datos.**

(73) Titular/es: **Irdeto Access B.V.**
Jupiterstraat 42
2132 HD Hoofddorp, NL

(45) Fecha de publicación de la mención BOPI:
01.04.2009

(72) Inventor/es: **Wajs, Andrew Augustine**

(45) Fecha de la publicación del folleto de la patente:
01.04.2009

(74) Agente: **Durán Moya, Carlos**

DESCRIPCIÓN

Sistema de cifrado y descifrado de datos.

La invención se refiere a sistemas de acceso condicional adecuados para recibir aparatos dotados con dispositivos de almacenamiento de gran capacidad. La invención se refiere específicamente a un sistema para proporcionar contenidos codificados según el preámbulo de la reivindicación 1 y a un sistema para descodificar contenidos codificados según el preámbulo de la reivindicación 3.

Los aparatos receptores de televisión recientes están equipados con dispositivos de almacenamiento de gran capacidad, permitiendo a los usuarios almacenar horas de contenidos de vídeo. De esta manera, el usuario se puede crear una "televisión personal" grabando sus programas favoritos y similares. Dichos aparatos receptores pueden ser un aparato de televisión, un descodificador de televisión o similar.

Los contenidos almacenados en los dispositivos de almacenamiento, tal como discos duros de gran capacidad, pueden incluir contenidos codificados con acceso condicional, en los que se necesitan palabras de control para descodificar los contenidos. Dichos dispositivos de almacenamiento permiten retroceder hacia atrás a través de los contenidos codificados, en los que sin embargo resulta difícil utilizar los mecanismos disponibles actualmente para secuenciar palabras de control. Retroceder hacia atrás es necesario ya que los usuarios querrían utilizar una funcionalidad de rebobinado parecido al del VCR (grabador de videocasete). Sin embargo las técnicas actuales utilizadas para secuenciar palabras de control están diseñadas para señales que avanzan únicamente hacia delante.

El documento EP 0 773 681 da a conocer un método de grabación de contenidos digitales codificados en cinta magnética en el cual se graba la palabra de control una pista por delante de los datos de contenidos a los cuales se aplica. Esto facilita una reproducción a velocidad variable en la dirección hacia delante.

La invención está destinada a dar a conocer un sistema para proporcionar contenidos codificados y un sistema para descodificar contenidos codificados del tipo mencionado anteriormente, en el que se dispone de una función de rebobinado parecida a la del grabador de videocasete.

Según la invención un sistema para proporcionar contenidos codificados comprende un generador de palabras de control, incluyendo cada palabra de control un identificador de palabra de control, un codificador para proporcionar un flujo de paquetes de datos codificados, en el que se codifican uno o más paquetes consecutivos utilizando la misma palabra de control (CW) y en el que cada paquete incluye un identificador de palabra de control que identifica la palabra de control utilizada, y un dispositivo de cifrado para proporcionar mensajes de control de autorización (ECM), incluyendo cada ECM al menos una palabra de control posterior (CW_N), caracterizado porque el dispositivo de cifrado de ECM proporciona mensajes ECM incluyendo una palabra de control anterior (CW_P), una palabra de control actual (CW_C) y una palabra de control posterior (CW_N).

En un segundo aspecto de la invención se da a conocer un sistema para descodificar contenidos codificados, que comprende un descodificador para descodificar los contenidos codificados, un dispositivo de descifrado para descifrar mensajes ECM para obtener palabras de control, en el que el dispositivo de descifrado de ECM suministra palabras de control al descodificador, en el que el descodificador descodifica los paquetes de datos de los contenidos codificados utilizando una palabra de control que tiene un identificador de palabra de control que corresponde con el identificador de palabra de control del paquete de datos a descodificar, comprendiendo además el sistema un dispositivo de almacenamiento para almacenar contenidos codificados y una unidad de procesamiento con medios para controlar la reproducción de los contenidos almacenados, con avance rápido y retroceso, en la que se programa la unidad de procesamiento para extraer mensajes ECM y entregar los mensajes ECM al dispositivo de descifrado de ECM para el descifrado, caracterizado porque la unidad de procesamiento se programa para solicitar al dispositivo de descifrado de ECM que proporcione como mínimo una palabra de control posterior (CW_N) en la reproducción o avance rápido, y que proporcione como mínimo una palabra de control anterior (CW_P) y una palabra de control actual (CW_C) al retroceder.

Proporcionando mensajes de control de autorización con tres palabras de control, es decir, las palabras de control actual, posterior y anterior, el aparato receptor puede reproducir contenidos almacenados desde el disco de un modo normal, en el que además están disponibles funciones de rebobinado y de avance rápido. Cuando el aparato receptor retrocede hacia atrás a través de los contenidos, la unidad de procesamiento coge el primer ECM que encuentra, envía el ECM al dispositivo de descifrado de ECM y solicita al dispositivo de descifrado que entregue las claves actuales y anteriores y cargue dichas claves en el descodificador. Procesar los mensajes ECM y sincronizar el suministro de palabras de control es relativamente sencillo de este modo.

La invención se explicará más detalladamente haciendo referencia a los dibujos en los que se muestra una realización del sistema de la invención.

La figura 1 muestra un diagrama simplificado de realizaciones del sistema para proporcionar contenidos codificados y del sistema para descodificar contenidos codificados según la invención.

La figura 2 muestra un diagrama para explicar el funcionamiento del sistema de la invención.

La figura 1 muestra un sistema (1) para proporcionar contenidos codificados, comprendiendo un generador (2) de palabra de control y un codificador (3). El codificador (3) recibe contenidos sin codificar y entrega contenidos codificados utilizando las palabras de control facilitadas por el generador (2) de palabras de control como claves de cifrado. El generador de palabras de control facilita una nueva palabra de control, por ejemplo, cada diez segundos. Como es bien sabido en esta técnica, las palabras de control se utilizan generalmente como dato o valor inicial para un generador de secuencias binarias pseudoaleatorias, en el que la salida del generador PRBS ("generador de secuencias binarias pseudoaleatorias") se utiliza para codificar los contenidos sin codificar. Por supuesto también se pueden utilizar otros sistemas de codificación tales como un sistema de cifrado de bloque. Como dichos sistemas de codificación son conocidos de por sí, estos no se explican con detalle en esta descripción dado que no es una parte de la presente invención. Cada palabra de control CW tiene un identificador de palabra de control asociado, que en caso del sistema MPEG utilizado generalmente es únicamente un bit, es decir o cero o uno. Correspondientemente, el mismo identificador de palabra de control, es decir un cero o un uno, se asocia con cada paquete de datos codificados o serie de paquetes de datos codificados bajo el control de la palabra de control que tiene el mismo identificador asociado cero o uno.

Las palabras de control CW_0 y CW_1 se entregan también a un dispositivo (4) de cifrado de ECM que cifra las palabras de control utilizando una clave de entrada P. El dispositivo de cifrado (4) puede realizarse como una tarjeta inteligente. Los mensajes ECM cifrados con las palabras de control se insertan en los contenidos codificados y se transmiten o se entregan de cualquier otra manera a un número de abonados teniendo cada uno un sistema (5) para descodificar contenidos codificados.

Se debe observar que la clave P utilizada por el dispositivo (4) de cifrado puede ser transferida a los sistemas (5) a través de los denominados mensajes de gestión de autorización que no se muestran en la figura 1. Los sistemas de acceso condicional que funcionan con tal jerarquía de claves son conocidos de por sí y no se describen adicionalmente en esta descripción.

El sistema de descodificación (5) comprende un descodificador (6) para descodificar los contenidos codificados y un dispositivo (7) de descifrado para descifrar mensajes ECM para obtener las palabras de control CW. Este dispositivo (7) puede realizarse como una tarjeta inteligente. Adicionalmente, el sistema (5) comprende una unidad (8) de procesamiento que controla el funcionamiento del sistema y que tiene medios (9) de control indicados esquemáticamente, permitiendo el control del sistema por parte del usuario. Los contenidos codificados se reciben en la unidad (8) de procesamiento y se pueden almacenar en un dispositivo (10) de almacenamiento, por ejemplo un disco duro de gran capacidad. La unidad (8) de procesamiento entrega los contenidos codificados al descodificador (6) y extrae los mensajes ECM del flujo de datos y entrega los mensajes ECM al dispositivo (7) de descifrado. El dispositivo (7) de descifrado, generalmente realizado como un dispositivo seguro tal como una tarjeta inteligente, descifra los mensajes ECM recibidos y como está controlado por la unidad (8) de procesamiento entrega las palabras de control CW_0, CW_1 al descodificador (6). Si se recibe un paquete de datos con el identificador de palabra de control 0 se utiliza la palabra de control CW_0, si se recibe un paquete de datos que tiene el identificador de palabra de control 1 se utiliza la palabra de control CW_1.

En los sistemas de acceso condicional conocidos se incluye en los mensajes ECM tanto la palabra de control actual CW_C como la palabra de control posterior CW_N o únicamente la palabra de control posterior CW_N. El dispositivo (7) de descifrado descifra las palabras de control y entrega las palabras de control al descodificador (6). Tal como se ha descrito anteriormente, los paquetes de datos que son entregados al descodificador (6) tienen identificadores de palabras de control correspondientes indicando que palabra de control CW_1 o CW_0 utilizar. En utilización normal, cuando únicamente se avanza hacia delante, se extrae un ECM del flujo de datos que contendrá como mínimo la palabra de control CW_1 o CW_0 a utilizar en la siguiente transición del identificador 1 al 0 en el flujo de paquetes de datos. Sin embargo cuando se retrocede a través del flujo de datos, el ECM no tendrá la palabra de control CW_P para el paquete de datos anterior en ninguna ubicación. Esto significa que la unidad (8) de procesamiento debe buscar más atrás que el paquete de datos actual procesado en el descodificador a efectos de encontrar un ECM anterior. Esto requeriría una operación intensiva e implicaría una gran carga en la capacidad de procesamiento del sistema (5).

Según la invención, este problema de localizar un ECM en un flujo de datos se evita incluyendo en los mensajes ECM tres claves, es decir la palabra de control anterior CW_P, la palabra de control actual CW_C y la palabra de control posterior CW_N. De este modo cada ECM extraído del flujo de datos por la unidad (8) de procesamiento en la reproducción de los contenidos almacenados en el disco (10) contiene tres palabras de control, incluyendo la palabra de control requerida para descodificar el paquete de datos anterior. De este modo, se dispone de una función de rebobinado de un modo fácil de manera que el usuario pueda desplazarse hacia atrás a través de los contenidos recuperados del dispositivo (10) de almacenamiento utilizando los medios (9) de control. Por supuesto, dichos medios de control pueden incluir un dispositivo de control remoto.

En la figura 2, se representa de forma esquemática una ilustración del funcionamiento de los sistemas de la invención. Se representa un flujo de contenidos con paquetes de datos A, B, C y D, en el que se supone que el paquete de datos A tiene el identificador de palabra de control 0, el paquete de datos B el identificador 1, el paquete de datos C el identificador 0, etc. El flujo de ECM está representado encima del flujo de paquetes de datos. Tal y como se indica, se extrae un nuevo ECM del flujo de datos de forma breve antes de la transición del paquete de datos A al B, del paquete de datos B al C, etc. El ECM extraído del flujo de datos de forma breve antes del inicio del paquete de datos A, incluye la palabra de control anterior CW_{P1}, la palabra de control actual CW_{A0} y la palabra de control posterior CW_{B1}. El siguiente ECM incluye la palabra de control anterior CW_{A0}, la palabra de control actual CW_{B1}

y la palabra de control posterior CW_{C0}. Durante una reproducción normal, la unidad (8) de procesamiento extraerá posteriormente los mensajes ECM del flujo de datos y enviará los mensajes ECM al dispositivo de descifrado (7). La unidad de procesamiento (8) solicitará al dispositivo (7) de descifrado que le envíe la palabra de control actual CW_{A0} y la palabra de control posterior CW_{B1} al descodificador (6). El descodificador (6) que recibe el paquete de datos A con el identificador 0, utilizará la palabra de control CW_{A0} para descodificar este paquete de datos. En la transición del paquete de datos A al paquete de datos B, el nuevo identificador 1 indica al descodificador (6) que utilice la palabra de control CW_{B1}. Se aplica la misma operación para el modo de avance rápido en el que la unidad (8) de procesamiento solicitará al dispositivo (7) de descifrado que le envíe las palabras de control actual y posterior al descodificador (6).

Si el usuario acciona los medios (9) de control para retroceder hacia atrás, es decir una función de rebobinado parecido al del grabador de videocasete, la unidad (8) de procesamiento ordena al dispositivo (7) de descifrado que le facilite la palabra de control actual CW_{A0} y la palabra de control anterior CW_{P1}. De este modo el descodificador (6) puede descodificar el paquete de datos anterior.

En el ejemplo anterior se indica que los mensajes ECM están almacenados como parte de los contenidos. También es posible almacenar los mensajes ECM de forma separada con información de sincronización. En este caso la información de sincronización en el flujo de contenidos es utilizada por la unidad (8) de procesamiento para extraer o recuperar los mensajes ECM correctos del dispositivo (10) de almacenamiento.

A partir de lo anterior se entenderá que la invención da a conocer sistemas en los que se permite retroceder hacia atrás a través de los contenidos de vídeo almacenados sin ningún incremento significativo en la carga en la unidad de procesamiento en procesar mensajes ECM y sincronizar palabras de control.

La invención no se limita a las realizaciones descritas anteriormente que pueden variar de una serie de maneras dentro del alcance de las reivindicaciones adjuntas.

REIVINDICACIONES

1. Sistema para proporcionar contenidos codificados comprendiendo un generador (2) de palabras de control, incluyendo cada palabra de control un identificador de palabra de control, un codificador (3) para proporcionar un flujo de paquetes de datos codificados, en el que se codifican uno o más paquetes consecutivos utilizando la misma palabra de control (CW) y en el que cada paquete incluye un identificador de palabras de control que identifica la palabra de control utilizada, y un dispositivo (4) de cifrado para proporcionar mensajes de control de autorización (ECM), incluyendo cada ECM al menos una palabra de control posterior (CW_N), **caracterizado** porque el dispositivo de cifrado de ECM proporciona mensajes ECM incluyendo una palabra de control anterior (CW_P), una palabra de control actual (CW_C) y una palabra de control posterior (CW_N).

2. Sistema según la reivindicación 1, en el que el dispositivo (4) de cifrado de ECM está contenido en una tarjeta inteligente.

3. Sistema para descodificar contenidos codificados, comprendiendo un descodificador (6) para descodificar los contenidos codificados, un dispositivo (7) de descifrado para descifrar mensajes ECM para obtener palabras de control, en el que el dispositivo (7) de descifrado de ECM entrega palabras de control al descodificador (6), en el que el descodificador (6) descodifica los paquetes de datos de los contenidos codificados utilizando una palabra de control que tiene un identificador de palabra de control que corresponde con el identificador de palabra de control del paquete de datos a descodificar, comprendiendo además el sistema un dispositivo (10) de almacenamiento para almacenar contenidos codificados y una unidad (8) de procesamiento con medios para controlar la reproducción de los contenidos almacenados, con avance rápido y retroceso, en la que se programa la unidad (8) de procesamiento para extraer mensajes ECM y entregar los mensajes ECM al dispositivo (7) de descifrado de ECM para el descifrado, **caracterizado** porque la unidad (8) de procesamiento se programa para solicitar al dispositivo (7) de descifrado de ECM que proporcione como mínimo una palabra de control posterior (CW_N) en la reproducción o avance rápido, y que proporcione como mínimo una palabra de control anterior (CW_P) y una palabra de control actual (CW_C) al retroceder hacia atrás.

4. Sistema según la reivindicación 3, en el que se programa la unidad (5) de procesamiento para solicitar al dispositivo (7) de descifrado de ECM que le facilite la palabra de control actual (CW_C) junto con una palabra de control posterior (CW_N) en la reproducción o avance rápido y que le proporcione la palabra de control actual (CW_C) junto con una palabra de control anterior (CW_P) al retroceder hacia atrás.

5. Sistema según las reivindicaciones 3 o 4, en el que el dispositivo (7) de descifrado ECM está contenido en una tarjeta inteligente.

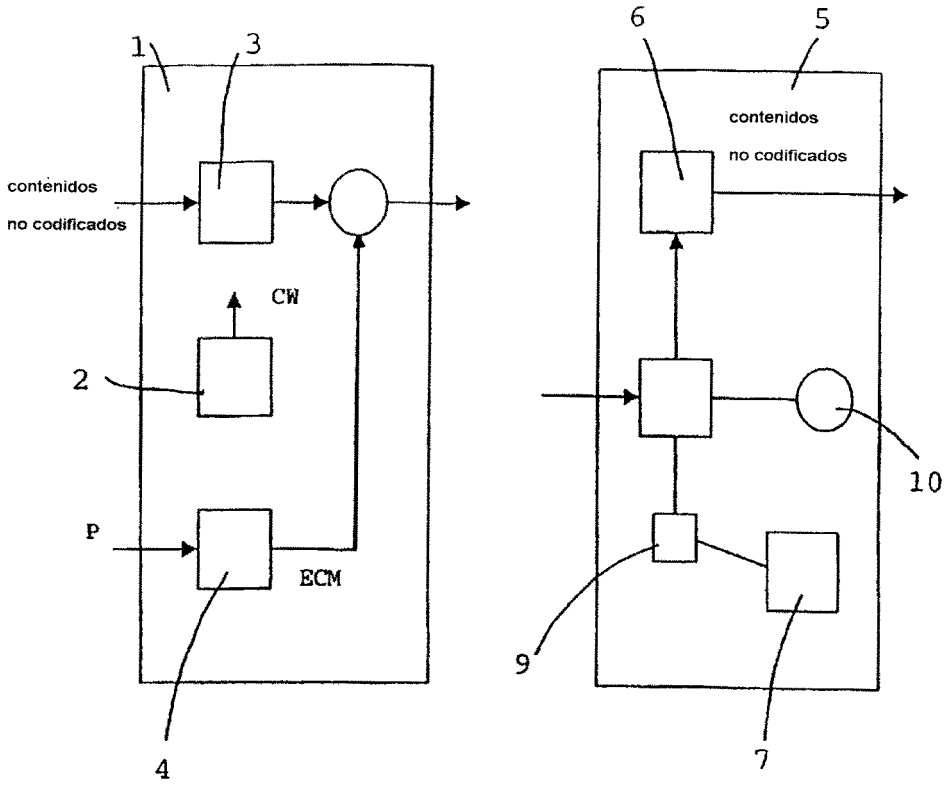
1
3
6
5
contenidos
no codificados
contenidos
no codificados
CW
2
10
P
ECM
9
4
7

Fig. 1

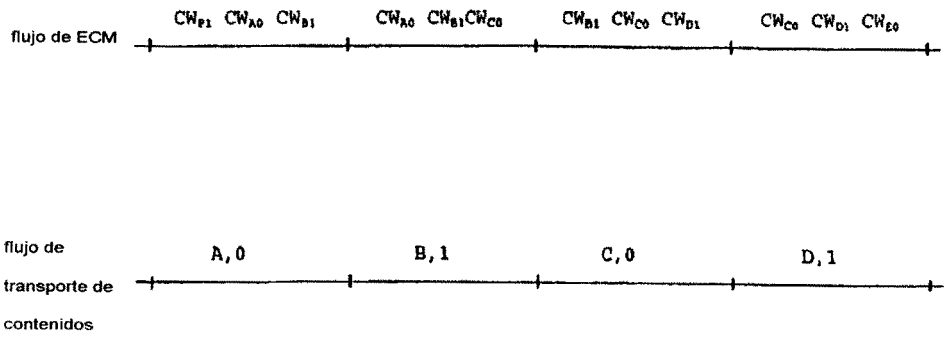
flujo de ECM
CW_{P1} CW_{A0} CW_{B1}
CW_{A0} $CW_{B1}CW_{C0}$
CW_{B1} CW_{C0} CW_{D1}
CW_{C0} CW_{D1} CW_{E0}
flujo de
transporte de
contenidos
A,0
B,1
C,0
D,1

Fig. 2