(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 627 735**

(51) Int. CI.:

H04N 21/426 (2011.01)
H04N 21/4623 (2011.01)
H04N 7/16 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **22.04.2010 PCT/EP2010/055324**

(87) Fecha y número de publicación internacional: **04.11.2010 WO10124982**

(96) Fecha de presentación y número de la solicitud europea: **22.04.2010 E 10714309 (1)**

(97) Fecha y número de publicación de la concesión europea: **12.04.2017 EP 2425620**

(54) Título: **Método para acceso seguro a un contenido audio/vídeo en una unidad de descodificación**

(30) Prioridad:

27.04.2009 EP 09158878

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
31.07.2017

(73) Titular/es:

NAGRAVISION S.A. (100.0%)
Route de Genève 22-24
1033 Cheseaux-sur-Lausanne, CH

(72) Inventor/es:

CONUS, JOËL y
STRANSKY, PHILIPPE

(74) Agente/Representante:

TOMAS GIL, Tesifonte Enrique

DESCRIPCIÓN

Método para acceso seguro a un contenido audio/vídeo en una unidad de descodificación.

Introducción

[0001] La presente invención se refiere al dominio de TV de pago, en particular al tratamiento de una señal audio/video, en la transmisión y en la recepción de dicha señal, para solo permitir que un abonado con la autorización apropiada acceda el contenido original cuando se usan unidades de descodificación auténticas

Antecedentes de la invención

[0002] En las unidades de descodificación de TV de pago común (conocidas también como decodificador), la unidad de descodificación comprende una ranura para insertar un módulo de seguridad (generalmente en forma de una tarjeta inteligente). El manejo de los derechos, la desencriptación de las claves para acceder el contenido se realiza en tal módulo de seguridad.

[0003] Aquellos módulos de seguridad se pueden implementar de una variedad de maneras tal como en una tarjeta de microprocesador, en una tarjeta inteligente o cualquier módulo electrónico en forma de una insignia o clave. Estos módulos son generalmente portátiles y se pueden separar de la unidad de descodificación. La forma más frecuentemente usada tiene contactos eléctricos pero también existen versiones sin contacto de tipo ISO 14443. Existe otra implementación del módulo de seguridad donde este está directamente soldado dentro de la unidad de descodificación, siendo una variación de este un circuito en una toma de corriente o conector tal como un módulo SIM. Otra implementación más es tener el módulo de seguridad integrado en un chip que tiene otra función, por ejemplo, en el módulo de descodificación o en el módulo del microprocesador de la unidad de descodificación.
El módulo de seguridad puede ser implementarse también en el software.

[0004] La unidad de descodificación podría tener periféricos tales como control remoto, disco duro externo, módulo de acceso condicional (tal como proporcionado por SmarDTV^{tm}) o elementos de seguridad conectados por medio de USB, PCMCIA, ISO7816 o Bluetooth. Aquellos periféricos interactúan con la unidad de descodificación y contienen datos de identificación.

[0005] Algunas unidades de descodificación no contienen un módulo de seguridad y las operaciones de seguridad se realizan directamente por el software - protegidas o no por así llamadas técnicas de protección SW tal como ofuscación de código y/o criptografía de caja blanca - de la unidad de descodificación. En tal caso, la unidad de descodificación inicia regularmente una conexión con un centro de gestión para recibir las claves para descodificar el contenido audio/video. Esta conexión se puede hacer por medio de un módem o por medio de conexión IP (Internet).

[0006] En el caso que no esté disponible una conexión de este tipo, la seguridad reside solo en la verificación de software de los derechos realizados por la unidad de descodificación.

[0007] Es grande la tentación de adquirir una unidad de descodificación de uso general y cargarla en una versión modificada del software que omite la verificación de los derechos.

[0008] El objetivo de la presente solicitud es ofrecer una mejor manera de asegurar el contenido audio/video recibido por una unidad de descodificación.

Breve descripción de la invención

[0009] La presente invención se refiere a la generación de una clave necesaria para desencriptar el contenido audio/video por unidades de descodificación auténticas.

[0010] Se refiere en particular a un método para asegurar la recepción de un contenido de emisión gestionado por un centro de control y encriptado por al menos una clave de transmisión o un dato que permite la recuperación de dicha clave de transmisión y que se transmite a al menos una unidad de descodificación, teniendo dicha unidad de descodificación al menos un parámetro del medio ambiente conocido por el centro de control, y ejecutando los pasos siguientes:

- Recibir desde el centro de control un primer mensaje común a una pluralidad de unidades de descodificación que comprende la clave de transmisión encriptada,
- Recibir desde el centro de control un segundo mensaje que se refiere a dicha unidad de descodificación que comprende datos de corrección,
- Desencriptar la clave de transmisión encriptada usando al menos un parámetro del medio ambiente de dicha unidad de descodificación y los datos de corrección.

[0011] El parámetro del medio ambiente es un dato extraído de la unidad de descodificación o de uno de sus periféricos y enlazado a alguna configuración lógica o física. Ejemplos de un parámetro del medio ambiente son los que siguen:

- Una versión de software de dicha unidad de descodificación o uno de sus periféricos, tal como V3.2c

[0012] La respuesta propuesta por el documento US 2004/0114764 es cargar en todos decodificadores auténticos algunos datos de autentificación y enlazar la desencriptación de una primera clave con la presencia de estos datos. Describe un medio de obtener la primera clave por datos previamente almacenados en el decodificador. Adicionalmente, son almacenados previamente en el decodificador diferentes datos de autentificación y un comando de selección se transmite para usarse como un indicador para seleccionar los datos que permiten para obtener esta primera clave gracias al uso de la segunda clave transmitida.
En este ejemplo, la primera y la segundas clave son comunes a toda unidad de descodificación. El comando es el mismo para toda unidad de descodificación también.

- Datos de configuración de un módulo de hardware, como la versión o designación de un conjunto de chips, la identificación de algunos módulos de hardware (módulo de desencriptación DES, IDEA) presentes en la unidad de descodificación o uno de sus periféricos,

- Información sobre el estado del módulo de hardware, como la información cargada en los registros de estos módulos de hardware mientras la unidad de descodificación o uno de sus periféricos está ejecutando su sistema operativo,

-Un certificado, tal como el certificado que está siendo cargado en el software principal o en los varios periféricos. Algunos de los periféricos de comunicación contienen tal certificado que se usa durante la creación de un canal seguro,

- Una función control de todo o parte del software, este puede utilizarse para calcular una firma en el software y el uso de esta firma como una clave; solo una parte del software por ejemplo el cargador encargado de la operación de seguridad se puede considerar para la generación de la firma (nótese que el resultado de este hash puede ser único por unidad de descodificación o uno de sus periféricos. Este es típicamente el caso cuando se usan técnicas de protección de software; en este caso software único, que incorpora secretos únicos, se puede proporcionar individualmente a cada unidades de descodificación),

- Una indicación de ubicación de la unidad de descodificación, esto se podría hacer por los datos extraídos a partir de un GPS, o los datos extraídos a partir de una red GSM, o la indicación de ubicación almacenada en la memoria de la unidad de descodificación tal como el código postal,

- Una dirección de hardware de una interfaz de red local, tal como una dirección de hardware (dirección MAC) de la interfaz de comunicación,

- Un número de identificación del conjunto de chips, disco duro o tarjeta de vídeo de dicha unidad de descodificación, teniendo estos dispositivos cada uno un número de serie personal,

- Datos de identificación de uno de los periféricos de la unidad de descodificación, donde este periférico podría ser un control remoto, un disco duro desmontable, un teléfono móvil (o smartphone) conectado con la unidad de descodificación por medio de infrarrojo o radiofrecuencia (Bluetooth), una pantalla de televisión.

[0013] Esta invención implica tres elementos, es decir:

- siendo el primero una clave de transmisión encriptada, generada y transmitida por el centro de control hacia una pluralidad de unidades de descodificación,

- El segundo es el parámetro del medio ambiente, extraído por la unidad de descodificación y conocido por el centro de control, siendo este parámetro único para una unidad de descodificación para un grupo de la unidad de descodificación (por grupo se entiende un número de unidades de descodificación menor que las unidades de descodificación que reciben el primer elemento),
- Datos de corrección, generados y transmitidos por el centro de control a una unidad de descodificación o un grupo de unidades de descodificación.

[0014] La idea principal es la necesidad de cooperación del parámetro del medio y los datos de corrección en la unidad de descodificación para extraer la clave de transmisión desde la clave de transmisión encriptada.

Breve descripción de los dibujos

[0015] La invención se entenderá mejor con referencia a la siguiente descripción detallada de la forma de realización preferida cuando se lee conjuntamente con los dibujos anexos, donde:

FIG.1 muestra un diagrama de bloques de los elementos que participan para obtener la clave de transmisión en una unidad de descodificación,
Fig.2 muestra un diagrama de bloques de los elementos que participan para obtener la clave de transmisión con un módulo de seguridad y una unidad de descodificación.

Descripción detallada de la forma de realización preferida

[0016] La presente invención es de relevancia particular para la industria de TV de pago y hace uso de los elementos implementados en una unidad de descodificación genuina para acceder a las claves necesarias para desencriptar un contenido audio/video.
Una unidad de descodificación puede ser una caja electrónica específica tal como un decodificador o un ordenador personal con capacidades para descodificar el contenido encriptado. Más adelante será referido debajo como unidad de descodificación.

[0017] Según el método de la invención, el centro de control manda dos tipos de mensajes, siendo el primero común a una pluralidad de unidades de descodificación y estando previsto el segundo para solo una unidad de descodificación o un grupo de unidades de descodificación.
En el caso de que el segundo mensaje se dirija a un grupo de unidades de descodificación, aquellas unidades comparten al menos algunos parámetros ambientales.

[0018] Diferentes formas de realización pueden utilizarse para obtener la clave de transmisión TK sin codificar, es decir

- Desencriptar la clave de transmisión encriptada (TK)k utilizando el parámetro del medio para obtener la clave de transmisión intermedia TK, y además desencriptar la clave de transmisión intermedia TK por los datos de corrección para obtener la clave de transmisión TK,

- Desencriptar la clave de transmisión encriptada (TK)k utilizando los datos de corrección para obtener la clave de transmisión intermedia TK", y además desencriptar la clave de transmisión intermedia TK" por el parámetro del medio ambiente para obtener la clave de transmisión TK, (nota: la clave de transmisión intermedia TK" es diferente que la clave de transmisión intermedia TK, ambos son información temporal para finalmente obtener la clave de transmisión)

- Calcular la clave de encriptación k por una función de los datos de corrección y el parámetro del medio ambiente, y desencriptar la clave de transmisión encriptada (TK)k utilizando la clave de encriptación k.

[0019] El término "desencriptación" puede ser también una "encriptación" o una función matemática tal como XOR.

[0020] La descripción detallada se focaliza ahora en la primera forma de realización. Las otras aplicaciones son igualmente válidas.

[0021] Una vez que el parámetro del medio ambiente es recogido por la unidad de descodificación, se usa para desencriptar la clave de transmisión encriptada contenida en el primer mensaje. Puesto que los datos del medio ambiente se refieren a una unidad de descodificación particular, el resultado de la desencriptación es diferente para cada unidad de descodificación.

[0022] El objetivo es obtener una clave de transmisión que es la misma para todas las unidades de descodificación auténticas y esto es por qué el segundo mensaje contiene los datos de corrección por aplicar en el resultado de la desencriptación.

[0023] En el centro de control, un primer dato se genera de forma aleatoria y sirve como la clave de transmisión encriptada (TK)k. Este dato se puede introducir en el primer mensaje para difundir todas las unidades de descodificación. Otro dato se genera también por el centro de control y se puede por la clave de encriptación k o la clave de transmisión TK. Si este dato es la clave de encriptación k, la clave de transmisión encriptada (TK)k se descifra para obtener la clave de transmisión TK.

[0024] El segundo paso es calcular los datos de corrección CD para cada unidad de descodificación (RC1). Para una unidad de descodificación dada RC, se usa el parámetro del medio ambiente EP en el proceso de encriptación. El centro de control ejecuta una función criptográfica (encriptación o desencriptación) utilizando el parámetro del medio ambiente y la clave de transmisión encriptada. Puesto que se usará la misma función criptográfica en la unidad de descodificación, la clave de esta función puede ser la clave de transmisión encriptada o el parámetro del medio ambiente.

[0025] El dato resultante de esta función se llama clave de transmisión intermedia TK y sigue siendo sin utilidad en esa fase, puesto que este resultado es diferente para cada unidad de descodificación.

[0026] Según una forma de realización de la invención, el segundo mensaje (dirigido a una persona o grupo) se envía mucho antes de ocurrir un cambio en la clave de transmisión TK con el objetivo de ser capaz de alcanzar todas las unidades de descodificación. El primer mensaje es enviado justo antes del cambio de la clave de transmisión de modo que la unidad de descodificación es capaz de obtener la clave de transmisión poco antes de usarla. Esto reduce el riesgo de que un hacker tenga el tiempo de hackear los mensajes y proporcionar la clave de transmisión a unidades de descodificación no autorizadas.

[0027] La clave de transmisión final TK es generada de forma aleatoria directamente por el centro de control o por un centro de control común en un ambiente Simulcrypt.

[0028] Los datos de corrección CD se calculan por la combinación de la clave de transmisión intermedia TK' y la clave de transmisión TK. Esta combinación es preferiblemente una función XOR o una función criptográfica reversible, sirviendo la clave de transmisión intermedia TK como la clave. En la plataforma abierta, criptografía de caja blanca y software, se pueden usar técnicas de ofuscación para prevenir la ingeniería inversa de la función de combinación y clas laves potenciales en acción. Una implementación incluso más segura aseguraría en el mismo bloque de cifrado de caja blanca la primera fase de descodificación y esta acción correctora.

[0029] Este resultado de la combinación se puede incorporar al segundo mensaje, siendo este mensaje individual (o dedicado a un grupo). La cabecera del segundo mensaje contiene la identificación de la unidad de descodificación o el grupo de unidades de descodificación.

[0030] Según una forma de realización de la invención, el primer o el segundo mensaje contiene adicionalmente la indicación del parámetro del medio ambiente usado para la generación de la clave de transmisión.
Puesto que es posible seleccionar o mezclar dos o más parámetros del medio ambiente, el mensaje describirá que parámetros se usan.

[0031] Esto se podría hacer con un simple mapa de bits, donde el valor resultante de un parámetro se puede combinar matemáticamente con los otros parámetros designados.

[0032] En el lado de la recepción, como ilustrado en la figura 1, la unidad de descodificación recibe el primer mensaje y extrae la clave de transmisión encriptada (TK)k. Para el ejemplo de debajo, suponemos que el parámetro del medio ambiente es un valor hash de una parte de software. La unidad de descodificación calcula el valor hash (H) del software seleccionado y usa este valor en una función criptográfica con la clave de transmisión encriptada (TK)k.
Como explicado anteriormente con respecto al centro de control, la función criptográfica será ejecutada con dos parámetros, es decir la clave de transmisión encriptada (TK)k y el valor hash (H).
Uno se puede usar como datos de entrada y el otro como la clave y viceversa.

[0033] La función criptográfica puede ser una función que ofusca, es decir, el orden de los bits (o bloque de bits) en el mensaje se reorganiza o enmascara o distribuye en la memoria no contigua, o en una de muchas funciones que ofuscan. El parámetro del medio ambiente es una clave para poner los bits del mensaje en el orden apropiado.

[0034] El resultado de esta función criptográfica da la clave de transmisión intermedia TK' y necesita más tratamiento.
Esto se hace gracias a los datos contenidos en el segundo mensaje dedicado a dicha unidad de descodificación.

[0035] Es de notar que el centro de control transmite muchos segundos mensajes, uno por unidad de descodificación o grupo unidades de descodificación. Cada segundo mensaje tiene una zona de dirección que indica la identificación de la unidad de descodificación tal como un número de serie. La unidad de descodificación filtra los segundos mensajes hasta que la identificación encuentra su identificación.

[0036] Este segundo mensaje solo se dedica a dicha unidad de descodificación y contiene CD de datos de corrección para dicha unidad de descodificación.

[0037] Para obtener la clave de transmisión final TK, la unidad de descodificación ejecuta una función XOR con la clave de transmisión intermedia TK y el CD de datos de corrección.
Según otra forma de realización, la clave de transmisión TK se puede obtener por la función inversa de aquella hecha en el centro de control, utilizando esta función la clave de transmisión intermedia TK como una clave y el CD de datos de corrección como datos de entrada.

[0038] Una vez se ha obtenido la clave de transmisión, esta clave puede utilizarse para desencriptar

directamente el contenido audio/video. Esta clave podría ser la palabra de control que permite acceso a una parte del contenido audio/video o una clave de contenido para desencriptar un servicio durante 24 horas.

[0039] La clave de transmisión puede utilizarse para desencriptar mensajes comprendiendo la clave para desencriptar el contenido. Estas claves son las palabras de control que cambian rápidamente. La clave de transmisión es válida durante mucho tiempo en la comparación con la palabra de control, por ejemplo 1 semana.

[0040] Según una forma de realización particular, la función criptográfica que da la clave de transmisión intermedia TK se puede personalizar con datos que se refieren a dicha unidad de descodificación. En el caso de que sea un proceso de encriptación, este proceso podría ser un proceso no estándar que usa datos específicos. Puesto que el centro de control tiene la imagen del proceso de encriptación de dicha unidad de descodificación, el centro de control tendrá en cuenta los datos personalizados mientras calcula la clave de transmisión intermedia TK y a continuación el CD de datos de corrección también tendrá en cuenta estos datos particulares.

[0041] Un ejemplo de tales parámetros es el SBox cargado en un motor de encriptación IdeaNxt.

[0042] El motor de encriptación se puede descargar en la unidad de descodificación por medio ambiente de una conexión a través de una red IP.
Una vez que está encendida la unidad de descodificación, se conecta a un centro de servicio para descargar la encriptación o los parámetros de dicha encriptación válidos para un tiempo limitado (un día, una semana etc..). Durante la conexión, el centro de servicio pide los datos de identificación del abonado para detectar unidades de descodificación falsas.

[0043] La verificación de la identificación se puede hacer adicionalmente con un reto que se genera por el centro de servicio, siendo enviado este reto a la unidad de descodificación.
A su vez, la unidad de descodificación ejecuta alguna operación con el reto, donde estas operaciones utilizan las características de la unidad de descodificación y las envían al centro de servicio.
Este centro puede verificar entonces la unidad de descodificación controlando si los datos de identificación son conformes con la respuesta al reto.

[0044] Como ya se ha explicado, el segundo mensaje se dirige individualmente y por lo tanto aumenta el ancho de banda usado para la información de servicio.
Al mismo tiempo, cuando cambia la clave de transmisión, es necesario actualizar los datos de corrección referentes a la clave de transmisión nueva, llevando así a la transmisión de un segundo mensaje para cada unidad de descodificación.

[0045] Para reducir el ancho de banda usado para los segundos mensajes, el último incorporará más de unos datos de corrección que serán aplicados a diferentes contenidos de primer mensaje.
El primer mensaje contendrá preferiblemente un índice que indica qué datos de corrección tienen que usarse con la clave de transmisión encriptada (TK)k en este mensaje.

[0046] La clave de transmisión TK puede cambiar a un índice definido por el centro de control. En este caso, sería aconsejable incluir en los primeros y segundos mensajes los datos relativamente a la corriente y la siguiente clave de transmisión. En este caso es necesario un proceso sincronizado de modo que se use la clave de transmisión apropiada. Esto se puede conseguir añadiendo unos datos de identificación en los mensajes descifrados por la clave de transmisión para identificar la clave que ha servido para encriptar el mensaje. La unidad de descodificación recibe de antemano la siguiente clave de transmisión y la memoriza. Cuando el mensaje ECM se recibe indicando el identificador de clave de transmisión nueva, esta clave se usa en lugar de la precedente.

[0047] En la forma de realización ilustrada en la figura 2, la obtención de la clave de transmisión final TK se realiza usando dos dispositivos diferentes, es decir, el receptor/decodificador (STB) y el módulo de seguridad (SC). Estos dos dispositivos forman la unidad de descodificación (RC1). Los parámetros del medio ambiente (EP) son preferiblemente extraídos desde el receptor/decodificador (STB) y pasados al módulo de seguridad (SC).
El receptor/decodificador (STB) recibe el flujo de datos entrantes y comprende un filtro (FI) para extraer los datos de gestión relativos al módulo de seguridad (SC).
Estos datos de gestión son los mensajes de gestión (EMM) que contienen la clave de transmisión encriptada (TK)k y el CD de datos de corrección. Puesto que los mensajes de gestión normalmente no son accesibles por el receptor/decodificador (estando la clave para desencriptar tales mensajes solo en el módulo de seguridad), el módulo de seguridad puede interrogar al receptor/decodificador para obtener el parámetro del medio ambiente. Cuando el parámetro del medio ambiente representa una firma en un gran número de datos tal como el hash del código de software, la función hash puede llevarse a cabo por el receptor/decodificador y el resultado puede pasar al módulo de seguridad.

[0048] El parámetro del medio ambiente puede ser luego recogido no solo en el receptor/decodificador sinoi

también en el módulo de seguridad.

[0049] Una vez la clave de transmisión TK se calcula por el módulo de seguridad, se pasa de nuevo al receptor/decodificador para ser aplicado sobre el decodificador DEC.
Es de notar que el canal para transmitir la clave de transmisión TK está protegido, es decir. todos los datos pasan de nuevo al receptor/decodificador se encriptan por una clave que pertenece al par receptor/decodificador y módulo de seguridad.

[0050] Es de notar que el primer o el segundo mensaje transmitidos a la unidad de descodificación pueden comprender condiciones de derecho de acceso. Estas condiciones se verifican en el módulo de seguridad si los derechos correspondientes están presentes. El segundo mensaje, que es dirigido a una unidad de descodificación única, puede contener también la actualización de los derechos del abonado o la actualización de las claves de seguridad, es decir los mensajes de gestión para desencriptar claves.
El segundo mensaje es preferiblemente encriptado por una clave única para la unidad de descodificación prevista.

REIVINDICACIONES

1. Método para asegurar la recepción de un contenido de emisión encriptado por al menos una clave de transmisión (TK) y transmitido a al menos una unidad de descodificación, donde **dicha al menos una clave de transmisión (TK) es generada y transmitida por un centro de control**, donde dicha unidad de descodificación tiene al menos un parámetro del medio ambiente (EP) conocido por el centro de control, donde dicho método comprende los pasos siguientes:

- recepción **por la unidad de descodificación** desde el centro de control de un primer mensaje común a una pluralidad de unidades de descodificación. comprendiendo la clave de transmisión encriptada (TK)k,
- recepción **por la unidad de descodificación** desde el centro de control de un segundo mensaje referente a dicha unidad de descodificación que comprende datos de corrección (CD), donde dichos datos de corrección (CD) se calculan por el centro de control con base en al menos un parámetro del medio ambiente (EP) de la unidad de descodificación, **siendo dicho parámetro del ambiente específico de dicha unidad de descodificación o un grupo de unidades de descodificación, siendo el parámetro del medio ambiente (EP):**

  - una versión de software de dicha unidad de descodificación,
  - datos de configuración de módulo de hardware,
  - información de estado de módulo de hardware,
  - un certificado,
  - una función hash de toda o parte del software,
  - una indicación de ubicación de la unidad de descodificación,
  - una dirección de hardware de una interfaz de red local, o
  - un número de identificación de uno de los dispositivos de hardware de dicha unidad de descodificación

dicho primer o segundo mensaje comprende además una indicación de qué parámetro del medio ambiente tiene que usarse,
- determinar por la unidad de descodificación al menos un parámetro del medio ambiente (EP) de la unidad de descodificación **usando la indicación contenida en el primer o segundo mensaje,**
- desencriptar la clave de transmisión encriptada (TK)k utilizando el parámetro de medio ambiente determinado (EP) y los datos de corrección (CD).

2. Método según la reivindicación 1, que incluye las etapas de recuperar la clave de transmisión:

- aplicación de un proceso de desencriptación en la clave de transmisión encriptada (TK)k usando al menos uno de dichos parámetros del medio ambiente (EP) como una clave para obtener una clave de transmisión intermedia (TK'),
- combinar la clave de transmisión intermedia (TK') con los datos de corrección para obtener la clave de transmisión (TK).

3. Método según la reivindicación 1, que comprende las etapas de recuperar la clave de transmisión:

- aplicación de un proceso de desencriptación en la clave de transmisión encriptada (TK)k utilizando los datos de corrección (CD) como una clave para obtener una segunda clave de transmisión intermedia (TK"),
- combinar la segunda clave de transmisión intermedia (TK') con al menos uno de dichos parámetros del ambiente (EP) para obtener la clave de transmisión (TK).

4. Método según la reivindicación 1, que comprende las etapas de recuperar la clave de transmisión:

- combinar al menos uno de dichos parámetros del medio ambiente (EP) con los datos de corrección (CD) para obtener una clave de encriptación (k),
- aplicación de un proceso de desencriptación en la clave de transmisión encriptada (TK)k utilizando la clave de encriptación (k) para obtener la clave de transmisión (TK).

5. Método según cualquiera de las reivindicaciones 1 a 4, donde el segundo mensaje correspondiente se dirige a un grupo de unidades de descodificación y comprende datos de corrección (CD) acerca del parámetro ambiental de dicho grupo de unidades de descodificación.

6. Método según una de las reivindicaciones 1 a 5, donde el primer mensaje o el segundo mensaje comprende un descriptor del parámetro medioambiental para ser usado por la unidad de descodificación.

7. Método según una de las reivindicaciones 1 a 6, donde la clave de transmisión (TK) se usa directamente para desencriptar dicho contenido.

8. Método según una de las reivindicaciones 1 a 6, donde la clave de transmisión (TK) se utiliza para desencriptar mensajes de control que contienen las claves para desencriptar el contenido.

9. Método según cualquiera de las reivindicaciones 1 a 8, donde la unidad de descodificación comprende una memoria para memorizar todos o parte del software relacionado con el proceso de desencriptación, siendo esta memoria actualizada por la recepción de mensajes de actualización desde el centro de control.

10. Método según cualquiera de las reivindicaciones 1 a 9, donde el segundo mensaje comprende una pluralidad de datos de corrección (CD), siendo cada dato de corrección usado con una clave de transmisión encriptada diferente (TK)k enviada en tiempo diferente.

11. Método según una de las reivindicaciones 1 a 10, donde el segundo mensaje es común a un grupo de unidades de descodificación y donde el parámetro del medio ambiente (EP) se comparte por el grupo de unidades de descodificación.

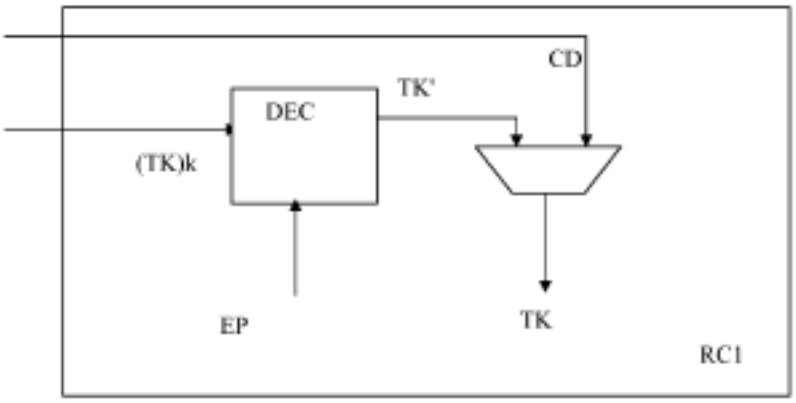

Fig. 1

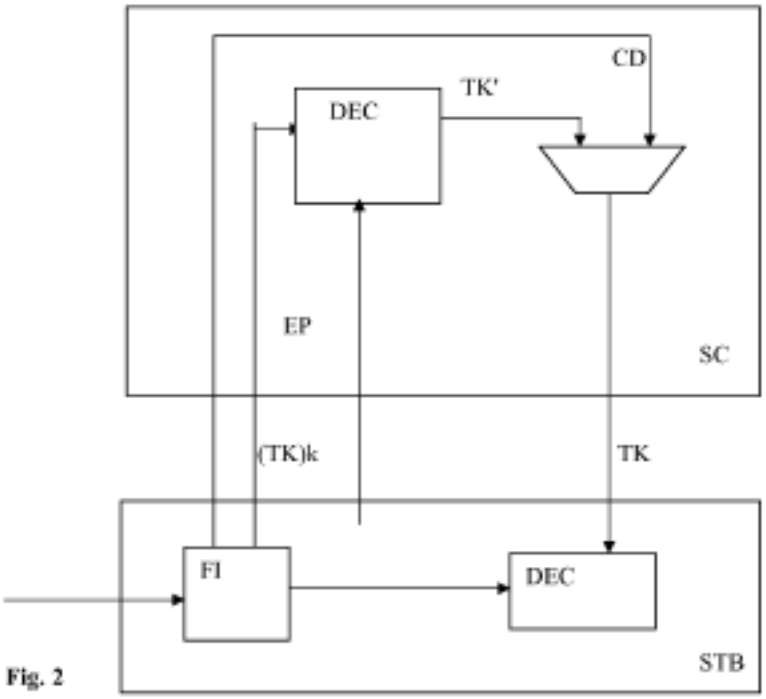

Fig. 2