(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 337 920**

(51) Int. Cl.:
H04N 7/167 (2006.01)
H04L 9/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **06100043 .6**
(96) Fecha de presentación : **03.01.2006**
(97) Número de publicación de la solicitud: **1804508**
(97) Fecha de publicación de la solicitud: **04.07.2007**

(54) Título: **Método de descifrado de un objeto de datos de contenido cifrado.**

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

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

(74) Agente: **Tomás Gil, Tesifonte Enrique**

(45) Fecha de publicación de la mención BOPI:
30.04.2010

(45) Fecha de la publicación del folleto de la patente:
30.04.2010

DESCRIPCIÓN

Método de descifrado de un objeto de datos de contenido cifrado.

La invención se refiere a un método de descifrado de un objeto de datos de contenido cifrado según el preámbulo de la reivindicación 1.

La invención también se refiere a un dispositivo para descifrado de unos datos de contenido cifrado según el preámbulo de la reivindicación 12.

La invención también se refiere a un método de acceso condicional para proporcionar un objeto de datos de contenido, según el preámbulo de la reivindicación 13.

La invención también se refiere a un sistema para suministrar acceso condicional a un objeto de datos de contenido, según el preámbulo de la reivindicación 17.

La invención también se refiere al uso de un dispositivo para cifrar un objeto de datos de contenido en un sistema para proporcionar acceso condicional.

La invención también se refiere a un programa informático.

Ejemplos respectivos de métodos de este tipo, dispositivos y tal sistema se conocen a partir de WO 97/38530. Esta publicación describe un descodificador para un sistema de TV de pago, donde señales de información digital son cifradas usando una palabra de control conforme al Eurocript estándar. El descodificador comprende un módulo de acceso condicional (CAM) y una tarjeta inteligente. El CAM está provisto con una unidad descifradora. Durante la operación, el CAM transfiere mensajes de control de derecho hacia un microprocesador de la tarjeta inteligente de modo que el microprocesador puede procesar el mensaje de control de derecho y extraer la palabra de control. Luego la tarjeta inteligente devuelve la palabra de control descifrada hacia el CAM de modo que se permite que el descifrador descifre una corriente de datos digital recibida de un desmodulador. Para proporcionar una comunicación segura entre el CAM y la tarjeta inteligente, el CAM genera una clave aleatoria Ci y transfiere la clave a la tarjeta inteligente en un primer mensaje codificado usando una clave pública de la tarjeta inteligente. La clave aleatoria Ci se utiliza para codificar y descodificar transmisiones entre los dispositivos.

Un problema del sistema conocido es que es posible sustituir la tarjeta inteligente por otro dispositivo, establecer una sesión de comunicación con el descifrador del CAM, y después suministrar palabras de control obtenidas ilícitamente al descifrador. El descifrador se diseña para trabajar con cualquier sistema de acceso condicional, de modo que es posible para un pirata informático simular un sistema de acceso condicional para proporcionar palabras de control al descifrador desde una fuente no controlada por el proveedor de la corriente de datos de contenido.

WO 99/09743 expone un sistema de televisión por cable que proporciona acceso condicional a servicios. El sistema de televisión por cable incluye una cabecera desde la cual son radiotransmitidos “ejemplos” de servicio, o programas, y una pluralidad de unidades de cajas descodificadoras para recibir los ejemplos y selectivamente descodificar los ejemplos para ser visualizados por los abonados del sistema. Los ejemplos de servicio son codificados usando claves públicas y/o privadas provistas por proveedores de servicio o agentes de autorización central. Las claves usadas por las cajas descodificadoras para la descodificación selectiva pueden también ser públicas o privadas en naturaleza, y claves de este tipo pueden ser reatribuidas a tiempos diferentes para proporcionar un sistema de televisión por cable donde las preocupaciones sobre piratería son minimizadas.

Es un objeto de la invención proporcionar métodos, dispositivos, un sistema y un programa informático de los tipos definidos arriba que permiten que un proveedor de acceso condicional fuerce el uso de un subsistema de acceso condicional particular para un objeto de datos de contenido.

Este objeto se consigue por el método de descifrado de un objeto de datos de contenido cifrado según la invención, que se caracteriza por el hecho de que al menos la sección del objeto de datos de contenido cifrado se descifra aplicando una operación de descodificación bajo una clave al menos parcialmente derivable desde la primera clave.

Puesto que al menos la sección del objeto de datos de contenido es descifrada aplicando una operación de descodificación bajo una clave al menos parcialmente derivable de una clave de descifrado de contenido, se requiere la implicación de un subsistema de acceso condicional. El subsistema de acceso condicional, sucesivamente, debe poseer información para derivar la primera clave o una clave que forma un par de claves con la primera clave, con el objetivo de poder formar los criptogramas para los mensajes a partir de los cuales la clave o claves de descifrado de contenido es/son obtenible/s. Esto es también cierto para el proveedor del objeto de datos de contenido cifrado, debido al hecho de que es descifrado aplicando una operación de descodificación bajo una clave al menos parcialmente derivable de la primera clave. Este requisito común enlaza el subsistema de acceso condicional con el proveedor del objeto de datos de contenido cifrado, previniendo el uso de una fuente diferente de mensajes que lleva las claves de descifrado de contenido. Una ventaja añadida es que esta variación en el cifrado del objeto de datos de contenido es alcanzable por el uso tanto de una clave de descifrado de contenido como de una primera clave. La primera clave no necesita, en consecuencia variar tan rápidamente como la clave de descifrado de contenido para conseguir una variación suficiente

en la información de la clave usada para descifrar el objeto de datos de contenido. Esto es ventajoso si no es posible proporcionar información de la clave al subsistema de acceso condicional frecuentemente para formar los criptogramas. Por otro lado, con cada cambio de clave de descifrado de contenido requerido, otro intercambio de mensajes con el subsistema de acceso condicional es requerido. Cada intercambio funciona también como una comprobación de la presencia continuada del subsistema de acceso condicional adecuado.

Se observa que la primera clave, o una clave que forma un par de claves con ella, podría corresponder a la clave de canal, dependiendo de la implementación del método. El, o uno de los criptogramas puede ser una firma, basada en una cantidad suficiente del contenido del mensaje al cifrador para enlazar la firma con el contenido de mensaje. Aunque el término subsistema de acceso condicional deriva de aplicaciones donde el objeto de datos de contenido cifrado es una corriente de datos de contenido, debe entenderse también como comprendiendo aquello que se llama de forma convencional un agente de gestión de derechos digitales.

En una forma de realización, donde la primera clave es una clave pública de un par de claves asimétricas, una operación criptográfica que incluye un cifrado asimétrico bajo la primera clave se aplica en datos intercambiados por el subsistema de acceso condicional.

Esta forma de realización permite el uso de un descifrador particular por diferentes proveedores de subsistemas de acceso condicional, al ser más fáciles de distribuir correspondientemente muchas primeras claves diferentes. Las primeras claves no necesitan ser mantenidas secretas. No es posible suplantar un subsistema de acceso condicional, puesto que requiere posesión de la clave secreta correspondiente para permitir que el descifrador establezca la clave de canal correcta.

En una forma de realización, al menos la sección del objeto de datos de contenido cifrado es descifrada aplicando una operación de descodificación bajo una clave basada en la primera clave y la clave de descifrado de contenido.

Así, la sección es descifrada aplicando una única función con una única clave derivada de al menos la primera clave y una clave de descifrado de contenido. Ésta es una vía eficaz de asegurar que el enlace entre el objeto de datos de contenido cifrado y el subsistema de acceso condicional no puede fácilmente ser circunvenido aplicando una descodificación bajo la primera clave a una sección del objeto de datos de contenido cifrado antes de suministrarla al descifrador para descodificación bajo una clave derivada de la clave de descifrado de contenido y/o aplicando una descodificación bajo la primera clave a los datos obtenidos como salida de tal descifrador.

En una forma de realización, al menos la sección del objeto de datos de contenido cifrado se descifra al menos aplicando una primera operación de descodificación en la sección del objeto de datos de contenido cifrado bajo una clave al menos parcialmente derivable de una clave de descifrado de contenido y aplicando otra operación de descodificación bajo una clave al menos derivable desde la primera clave a la salida de la primera operación de descodificación.

Así, aunque la primera clave no es secreta, el enlace entre el objeto de datos de contenido cifrado y un subsistema de acceso condicional particular no puede ser circunvenido descodificando en primer lugar el objeto de datos de contenido cifrado bajo la primera clave y luego suministrándola al descifrador.

En una forma de realización, al menos la sección del objeto de datos de contenido cifrado se descifra aplicando al menos una segunda operación de descodificación bajo una clave al menos parcialmente derivable de una clave de descifrado de contenido para datos obtenidos como salida de otra operación de descodificación bajo una clave al menos derivable desde la primera clave.

Así, aunque la primera clave no es secreta, el enlace entre el objeto de datos de contenido cifrado y un subsistema de acceso condicional particular no puede ser circunvenido descodificando la salida del descifrador bajo la primera clave y después proporcionándolo a un receptor. En esta forma de realización, es el descifrador el que debe desempeñar al menos ambas operaciones, es decir descifrar bajo una clave al menos parcialmente derivable de una clave de descifrado de contenido y al menos otra descodificación bajo una clave al menos derivable desde la primera clave.

Una variante incluye derivar al menos dos claves a partir de una única clave de descifrado de contenido, donde la primera de las claves derivadas se usa en la primera operación de descodificación y la segunda de las claves derivadas se usa en la segunda operación de descodificación.

Ésta es una manera eficaz de prevenir que un hacker circunvenga el enlace entre el objeto de datos de contenido cifrado y el subsistema de acceso condicional aplicando una descodificación bajo la primera clave al objeto de datos de contenido cifrado antes de suministrarla al descifrador para descodificación bajo una clave derivada de la clave de descifrado de contenido y/o aplicando una descodificación bajo la primera clave a los datos obtenidos de este descifrador.

Una forma de realización incluye aplicar una operación de descodificación que implica un cifrado simétrico de clave bajo una clave obtenida como función de al menos la primera clave.

Esta forma de realización tiene el efecto de permitir el uso de una clave pública como la primera clave, mientras que además se obtiene una velocidad de procesamiento mejorada asociada a los cifrados simétricos de clave.

Una forma de realización incluye generar una clave de canal, codificar la clave de canal generada bajo la primera clave y comunicar la clave de canal codificada al subsistema de acceso condicional, y descodificar al menos parte del mensaje recibido desde el subsistema de acceso condicional bajo la clave de canal, preferiblemente usando un cifrado simétrico.

Esta forma de realización tiene el efecto de permitir un uso más prolongado de la primera clave sin ofrecer mejores oportunidades para el criptoanálisis. Especialmente cuando la primera clave es una clave asimétrica, la aleatoriedad de los criptogramas se mejora para evitar su uso directo. Otro efecto es que es posible cambiar las claves de canal sin la cooperación inmediata del proveedor del objeto de datos de contenido cifrado, puesto que la clave que forma un par de claves con la primera clave y usada en una operación de codificación que forma parte del cifrado no necesita ser cambiada.

En una forma de realización, una clave de canal nueva se establece al recibir una versión nueva de la primera clave.

Por lo tanto, el recibo de una versión nueva de la primera clave desencadena una comprobación renovada de que el subsistema de acceso condicional está asociado con el proveedor del objeto de datos de contenido cifrado.

Una forma de realización incluye obtener una firma digital del mensaje recibido del subsistema de acceso condicional, usando al menos la primera clave para verificar la firma digital, y descifrar al menos la sección del objeto de datos de contenido cifrado dependiendo del resultado de la verificación.

Esta forma de realización tiene el efecto de que el descifrador verifica la identidad del subsistema de acceso condicional mediante una firma.

Una variante incluye generar una clave de canal, preferiblemente como un número aleatorio, codificar la clave de canal generada bajo la primera clave y comunicar la clave de canal codificada al subsistema de acceso condicional, y además usar la clave de canal para verificar la firma digital.

Esta variante tiene la ventaja de que la primera clave no se usa directamente para formar la firma. Por lo tanto, es menos fácilmente comprometida. Además, la verificación de la firma puede ser terminada de forma más rápida que una descodificación completa del mensaje del subsistema de acceso condicional.

Según otro aspecto de la invención, se proporciona un dispositivo para descifrar un objeto de datos de contenido cifrado, incluyendo una entrada para recibir el objeto de datos de contenido cifrado y una entrada para recibir mensajes de un subsistema de acceso condicional sobre un canal de comunicación de datos, donde el dispositivo se configura para ejecutar un método de descifrado de un objeto de datos de contenido cifrado según la invención.

El dispositivo puede ser implementado como un dispositivo monolítico para incorporación en los receptores. Tiene un control incorporado de la asociación entre el proveedor de los datos de contenido cifrado y el subsistema de acceso condicional.

Según otro aspecto, el método para suministrar acceso condicional a un objeto de datos de contenido según la invención se caracteriza por suministrar información de la clave a los subsistemas de acceso condicional representativa de la segunda clave y por suministrar al cifrador de la información de clave representativa de una primera clave que forma un par de claves con la segunda clave, donde el cifrador está dispuesto para cifrar al menos la sección del objeto de datos de contenido aplicando una operación de codificación bajo una clave al menos parcialmente derivable desde la primera clave.

Así, los subsistemas de acceso condicional se enlazan al objeto de datos de contenido cifrado. Sólo los subsistemas de acceso condicional provistos de la información de la clave representativa de la segunda clave son capaces de proporcionar el mensaje al descifrador de un receptor autorizado que incluye datos que permiten al descifrador obtener al menos una clave de descifrado del contenido. El descifrador es forzado a controlar que el subsistema de acceso condicional tiene la información de clave, porque usa datos representativos de una primera clave que forma un par de claves con la segunda clave para descifrar el objeto de datos de contenido y para establecer la clave de canal.

En una forma de realización, donde la segunda clave es una clave secreta de un par de claves asimétricas, una primera clave correspondiente a una clave pública del par de claves asimétricas es suministrada a un transmisor dispuesto para comunicar al receptor autorizado la primera calve en un mensaje.

Puesto que la primera clave es pública, la distribución de la misma es relativamente simple. Esto permite que diferentes proveedores de objetos de datos de contenido cifrado usen el mismo descifrador con diferentes subsistemas de acceso condicional respectivos. La segunda clave es secreta, pero es suministrada sólo a los subsistemas de acceso condicional asociados a un proveedor particular.

En una forma de realización, donde el objeto de datos de contenido comprende una corriente de datos de contenido, una secuencia de palabras de control está provista al cifrador, el cifrador está dispuesto para usar una actual de la secuencia de palabras de control como la clave de cifrado de contenido, y el método además incluye transmitir la primera clave en un mensaje de control de autorización que además incluye al menos una de la secuencia de palabras de control.

Esto tiene el efecto de que los cambios en la palabra de control y primera clave pueden ser sincronizados de forma relativamente fácil.

Una forma de realización incluye suministrar al menos un dispositivo portátil protegido que comprende una unidad de procesamiento, memoria, una interfaz a un descifrador de un receptor autorizado y al menos uno de los subsistemas de acceso condicional.

El dispositivo portátil protegido que es el resultado directo inevitable de aplicar esta forma de realización puede ser asociado a un proveedor particular de objetos de datos de contenido cifrado, incluso interactúa con un descifrador de un receptor autorizado que es potencialmente adecuado para el uso en la descifrado de objetos de datos de contenido de diferentes proveedores. Tal descifrador coopera con el dispositivo portátil protegido de manera que puede controlar la asociación de este último con el proveedor del objeto de datos de contenido cifrado que debe ser descifrado.

Según otro aspecto, el sistema para suministrar acceso condicional a un objeto de datos de contenido se caracteriza por el hecho de que el cifrador está dispuesto para cifrar al menos la sección del objeto de datos de contenido aplicando una operación de codificación bajo una clave al menos parcialmente derivable de una primera clave que forma un par de claves con la segunda clave.

De esta manera, el cifrador y los subsistemas de acceso condicional son cada uno capaces de obtener la segunda clave. El descifrador puede controlar que éste es el caso descodificando el criptograma y descifrando el objeto de datos de contenido cifrado.

En una forma de realización, donde la segunda clave es una clave secreta de un par de claves asimétricas, el sistema se configura para proporcionar una primera clave correspondiente a una clave pública del par de claves asimétricas a un transmisor dispuesto para comunicar la primera clave en un mensaje al receptor autorizado.

Esto tiene el efecto de que el descifrador de un receptor autorizado puede ser habilitado para comprobar la asociación entre cualquier subsistema de acceso condicional y un objeto de datos de contenido cifrado sin tener que ser preprogramado con la información de la clave necesaria. Como primera clave es una clave pública, no hay ninguna necesidad de mantenerla secreta cuando se permite al descifrador realizar la comprobación de esta manera.

En una forma de realización, configurada para cifrar un objeto de datos de contenido que comprende una corriente de datos de contenido, el sistema está dispuesto para efectuar un cambio de valor de la segunda clave, donde el sistema además comprende un sistema para sincronizar un cambio de suministro de la segunda clave a un valor nuevo con una transición de uso de una actual para usar la siguiente de una secuencia de palabras de control como clave de cifrado del contenido.

De esta manera, es posible cambiar la segunda clave sin tener que indicar todas las combinaciones posibles de la actual y la siguiente palabra de control y clave que forman un par de claves con la segunda clave en el punto aplicable en la corriente de datos de contenido cifrado al descifrador de un receptor autorizado.

En una forma de realización, el cifrador se configura para cifrar al menos la sección del objeto de datos de contenido al menos aplicando una primera operación de codificación en la sección del objeto de datos de contenido bajo una clave al menos parcialmente derivable de una clave de cifrado de contenido y aplicando otra operación de codificación bajo una clave al menos parcialmente derivable de una primera clave que forma un par de claves con la segunda clave a la salida de la primera operación de codificación.

Esto significa que un hacker no puede circunvenir un control en la asociación entre el subsistema de acceso condicional y el objeto de datos de contenido cifrado descodificando la salida del descifrador bajo la clave que forma un par de claves con la segunda clave, incluso si esta clave está disponible para él.

En una forma de realización, el cifrador se configura para cifrar al menos la sección del objeto de datos de contenido al menos aplicando una segunda operación de codificación bajo una clave al menos parcialmente derivable de una clave de cifrado de contenido para datos obtenidos como salida de otra operación de codificación bajo una clave al menos parcialmente derivable de una primera clave que forma un par de claves con la segunda clave.

El efecto es que un hacker no puede circunvenir un control en la asociación entre el subsistema de acceso condicional y los datos de contenido cifrado descodificando los datos de contenido cifrado bajo la clave que forma un par de claves con la segunda clave, antes de pasarla al descifrador, incluso si la clave está disponible para él.

Una variante se configura para derivar al menos dos claves de una única clave de cifrado, y para usar una primera de las claves derivadas en la primera operación de codificación y una segunda de las claves derivadas en la segunda operación de codificación.

Esta es una implementación eficaz de un sistema que implementa el uso de un descifrador que controla la asociación entre un subsistema de acceso condicional y el proveedor del objeto de datos de contenido cifrado, incluso cuando la clave que forma un par de claves con la segunda clave no es mantenida secreta.

En una forma de realización, la operación de codificación bajo una clave al menos parcialmente derivable desde la primera clave implica un cifrado simétrico de clave bajo una clave obtenida como función de al menos la primera clave.

Esta forma de realización tiene la ventaja de una eficiencia y aleatoriedad aumentadas. Las claves simétricas pueden ser obtenidas más aleatorias que las claves asimétricas.

Según otro aspecto de la invención, se proporciona un dispositivo para cifrar un objeto de datos de contenido, presentando todas las características del cifrador en el sistema para suministrar el acceso condicional descrito arriba y estando así construido y evidentemente destinado para el uso en el sistema para suministrar acceso condicional según la invención.

Según otro aspecto de la invención, se proporciona un programa de ordenador, que incluye un conjunto de instrucciones capaz, cuando se incorpora en un medio legible por máquina, de provocar que un sistema que tiene capacidades de tratamiento de la información ejecute un método según la invención y/o que funcione como un cifrador o subsistema de acceso condicional en un sistema según la invención.

La invención ahora será explicada con más detalle con referencia a los dibujos anexos, donde

La Fig. 1 da una visión de conjunto esquemática de un sistema para cifrar, transmitir y descifrar corrientes de datos de contenido;

La Fig. 2 es un diagrama esquemático que detalla las funciones proporcionadas en una implementación en hardware de un descifrador;

La Fig. 3 es un flujograma que ilustra un cambio de clave pública en el sistema ilustrado en la Fig. 1;

La Fig. 4 es un diagrama esquemático que ilustra períodos de clave asociados a una corriente de datos de contenido cifrado; y

La Fig. 5 es un diagrama esquemático que detalla funciones proporcionadas en una implementación en hardware de un cifrador.

En un ejemplo, ilustrado en la Fig. 1, el acceso condicional está provisto para la radiotransmisión de datos de contenido de un sistema de cabecera 1 a un receptor autorizado 2. El receptor 2 interactúa con un subsistema de acceso condicional 3, implementado como un dispositivo desmontable protegido. Los datos de contenido son radiotransmitidos por medio de una red de radiotransmisión terrestre, por cable o por satélite o una cadena de tales redes. El ejemplo donde datos de contenido cifrado son radiotransmitidos se usa a lo largo de toda esta descripción. No obstante, los métodos perfilados en la presente pueden también ser usados para proporcionar acceso condicional al contenido diseminado en soportes de datos tales como discos digitales versátiles (DVDs), discos compactos (CDS), o medios de grabación magnéticos. Además, los métodos encuentran aplicación para proporcionar acceso condicional al contenido distribuido sobre redes de ordenador, tales como Internet, en un modo de unidifusión, de multidifusión o de radiotransmisión. Esto incluye objetos de datos de contenido que no comprenden una corriente de datos de contenido, tales como documentos digitales. En una implementación alternativa a aquella descrita aquí con detalle, el subsistema de acceso condicional puede ser un módulo de software protegido ejecutado por un procesador en el receptor 2. Este software protegido puede, por ejemplo, ser protegido por el uso de técnicas de ofuscación de código, etc.

Una o más corrientes de datos de contenido se obtienen del almacenamiento de datos 4, y de manera simultánea por un multiplexor 5 en una única corriente. En el ejemplo ilustrado, el multiplex entero de corrientes elementales es cifrado por un cifrador 6 y es radiotransmitido por un transmisor 7. Se observa que una o más corrientes seleccionadas elementales pueden ser individualmente cifradas en otra forma de realización, mejor que el multiplex entero.

Un sistema de autorización de abonado (SAS) 8 es responsable de autorizar y facturar a abonados individuales. Proporciona datos de autorización - incluyendo una clave a un alto nivel en una jerarquía de claves - a un generador de mensajes de gestión de derechos (EMM) 9 en cierto modo conocido como tal. Un generador de palabras de control (CW) 10 genera continuamente la siguiente de una secuencia de palabras de control (CWs), que varía de una a la siguiente. Las palabras de control son codificadas bajo una clave, por ejemplo la clave proporcionada por el SAS 8, para formar mensajes de control de derechos (ECMs). Los ECMs se generan por un generador de ECM 11. Las palabras de control son también proporcionadas al cifrador 6, que las usa en cierto modo que será descrito con más detalle abajo para cifrar la corriente de datos de contenido recibido del multiplexor 5. Como se ha descrito hasta aquí, el sistema

de cabecera 1 corresponde a aquellos conocidos, por ejemplo, de "Digital Video Broadcasting (DVB); Implementation Guidelines of the DVB Simulcrypt Standard", ETSI Technical Report 102 035, European Telecommunications Standards Institute.

El sistema de cabecera 1 ilustrado además comprende un generador de par de claves pública/privada 12. En la forma de realización ilustrada, la primera clave del par de claves pública/privada, es decir la clave pública, está provista al generador de ECM 11. El generador de ECM 11 la incluye en mensajes de claves proporcionados al receptor 2 de forma intencionada. En otra forma de realización (no ilustrada), cada primera clave está provista para receptores autorizados en un ECM.

Las primeras claves pueden ser distribuidas al receptor 2 por una vía diferente a la corriente de datos de contenido cifrado, por ejemplo sobre una red de ordenadores, en un soporte de datos, como un ajuste de fábrica, etc. En el ejemplo, será asumido que las primeras claves se proveen en mensajes de claves en una corriente elemental separada dentro del multiplex que comprende la corriente de datos de contenido cifrado.

La segunda clave del par de claves pública/privada, la clave secreta, está provista al subsistema de acceso condicional 3. En la forma de realización ilustrada, será asumido que la segunda clave está provista en un mensaje codificado, codificado bajo una clave accesible sólo para el dispositivo que comprende el subsistema de acceso condicional 3. En una forma de realización alternativa, la segunda clave puede ser estática, o derivada en una manera predeterminada de una clave estática almacenada en el dispositivo que comprende el subsistema de acceso condicional 3 antes de la distribución de la misma a abonados autorizados.

El receptor 2 es ilustrado sólo en la medida que es considerada necesaria para explicar la invención. Es ilustrativo para una gama de dispositivos incluyendo entradas a una red interna, ordenadores privados provistos de funcionalidad adicional, cajas descodificadoras, conjuntos de televisión digital, etc. Comprende una interfaz de receptor 13 para recibir una señal de radiotransmisión a través de la red de radiotransmisión. Además comprende un sintonizador/desmodulador 14 para obtener la corriente de datos de contenido cifrado desde la señal de radiotransmisión. Se ilustra esquemáticamente un descifrador 15 en la Fig. 1 y en detalle en la Fig. 2. El descifrador 15 descifra la corriente de datos de contenido cifrado. La corriente de datos de contenido claro está provista a un demultiplexor 16, que proporciona corrientes elementales seleccionadas que forman un programa para una salida del receptor 2, de modo que el programa puede ser restituido. Aunque la Fig. 1 muestra unidades funcionales mejor que los componentes de hardware actuales, el descifrador 15 generalmente corresponderá a un dispositivo específico, un circuito integrado de aplicación específica, o concebiblemente un procesador de señal digital programada o matriz de puertas programables de campo.

El receptor 2 incluye una interfaz 17 para el subsistema de acceso condicional 3. La interfaz 17 es de un tipo estandarizado para volver al receptor 2, y en particular al descifrador 15 interoperable con cualquier pluralidad de diferentes subsistemas de acceso condicional, cada uno asociado a un proveedor de acceso condicional diferente. El subsistema de acceso condicional 3 incluye una interfaz correspondiente 18. El subsistema de acceso condicional 3 recibe los ECMs y EMMs del demultiplexor 16 a través de las interfaces 17,18. En la forma de realización ilustrada, también recibe cualquier mensaje que lleva una nueva segunda clave secreta, según es generada por el generador de par de claves pública/privada 12.

El subsistema de acceso condicional 3 incluye al menos tres unidades funcionales: una primera unidad criptográfica 19 para descodificar EMMs, una segunda unidad criptográfica 20 para descodificar ECMs y codificar mensajes para el receptor 2, y un procesador protegido 21 para controlar la operación del subsistema de acceso condicional 3. Tras el recibo exitoso y la descodificación de un EMM autorizando la descodificación de un servicio particular, el procesador protegido 21 habilita la segunda unidad criptográfica 20 para derivar palabras de control de ECMs recibidas a través de la interfaz 18. Las palabras de control son comunicadas al descifrador 15 en mensajes pasados a través de las interfaces 17,18. En la forma de realización ilustrada, la primera unidad criptográfica 19 también dispone la segunda clave del par de claves pública/privada para el uso en la instalación de un canal de comunicaciones protegido y/o autentificado entre el subsistema de acceso condicional 3 y el descifrador 15.

La operación del descifrador 15 se ilustra por ejemplo en las Figs. 2 y 3. El descifrador 15 tiene una primera interfaz 22 para recibir la corriente de datos de contenido cifrado para ser descifrada y una unidad 23 para recuperar una primera clave 24 de un par de claves pública/privada en un mensaje de claves del sistema de cabecera (fase 25 en la Fig. 3). La recepción de un mensaje de clave que indica una nueva primera clave es un desencadenante para que un generador de números aleatorios 26 en el descifrador 15 genere un número aleatorio como una clave de sesión 27 en una siguiente fase 28. En la forma de realización ilustrada, la clave de sesión 27 se utiliza para configurar un canal de comunicaciones protegidas al subsistema de acceso condicional 3 a través de una segunda interfaz 29. La clave de sesión 27 se utiliza para descodificar criptogramas soportados en mensajes recibidos del subsistema de acceso condicional 3. Estos criptogramas incluyen al menos uno de una firma digital y un criptograma de una o más palabras de control.

Una unidad de codificación 30 codifica (fase 31) la clave de sesión 27 bajo la nueva primera clave 24 recibida en la primera fase 25. Con este fin, un cifrado asimétrico bajo la primera clave 24 se aplica a la clave de sesión 27. La clave de sesión 27 es establecida como la clave para asegurar el canal de comunicaciones al subsistema de acceso condicional 3 para comunicar (fase 32) un mensaje que incluye la clave de sesión codificada 27 al subsistema de acceso condicional 3.

Cuando el descifrador 15 recibe un mensaje de palabra de control 33 del subsistema de acceso condicional 3 (fase 34), se pasa a una unidad de descodificación 35, que usa la clave de sesión 27 para descodificar (fase 36) al menos un criptograma soportado en el mensaje de palabra de control 33. En la forma de realización ilustrada, la descodificación se realiza usando un cifrado simétrico bajo la clave de sesión 27. La codificación bajo la clave de sesión (aleatoria) 27 tiene el efecto de que no es posible "alimentar" el descifrador 15 con mensajes de palabra de control 33 obtenidos de un subsistema de acceso condicional operativo conjuntamente con otro receptor autorizado 2.

Se señala que la primera clave 24 se utiliza para autentificar el mensaje de palabra de control 33 en el misma fase 36. Según una manera conocida, el subsistema de acceso condicional 3 usa la segunda clave para firmar el mensaje de palabra de control 33, por ejemplo codificando una porción de al menos parte del mensaje de palabra de control 33 bajo la segunda clave para formar un criptograma llevado en el mensaje. En otra forma de realización, la clave de sesión 27 se utiliza para formar la firma digital.

En estas formas de realización donde una firma digital es obtenida del mensaje de palabra de control 33 y la primera clave 24 se utilizan para verificar la firma digital, el método se detiene (no ilustrado con detalle) si el resultado de la verificación indica que la firma no es correcta. Es decir, que la descifrado de la corriente de datos de contenido cifrado es abortada. En una variante adicional de esta forma de realización donde una firma digital es verificada, el contenido del mensaje de palabra de control 33 no se codifica por el subsistema de acceso condicional 3. Sólo se utiliza la firma, formada usando el número aleatorio generado por el descifrador 15 o usando la primera clave 24 como una clave de codificación para la codificación de, por ejemplo, una porción de parte o todo el contenido del mensaje de palabra de control 33, para prevenir la sustitución del subsistema de acceso condicional 3.

En consecuencia se señala que pueden haber dos denominadas "claves de canal", es decir la primera clave y la clave de sesión, dependiendo de si la comunicación entre el descifrador 15 y el subsistema de acceso condicional 3 es protegido, autentificado, o ambos. Cada clave de canal es establecida usando la primera clave. Por una parte, la clave usada para la autentificación es idéntica a la primera clave 24, de modo que se establece por su gran recuperación en la primera fase 25. En cambio, la clave de sesión 27 se establece por un intercambio de mensajes, del cual al menos uno es codificado bajo parte o toda la primera clave 24.

Como resultado de la realización de la fase de descodificación y/o de autentificación 36, el descifrador 15 obtiene al menos una palabra de control 37 en la secuencia generada por el generador de CW 10.

Una primera unidad de función 38 aplica una primera función f_a a la palabra de control 37 para generar (fase 39) una primera clave de descodificación de contenido 40. Una segunda unidad de función 41 aplica una segunda función f_b a la primera clave 24 para generar (fase 42) una segunda clave de descodificación de contenido 43. Una tercera unidad de función 44 aplica una tercera función f_c a la misma palabra de control 37 que es usada por la primera unidad de función 38, para generar (fase 45) una tercera clave de descodificación de contenido 46.

Para descifrar la corriente de datos de contenido cifrado, una primera unidad de descodificación 47 aplica un primer cifrado de descodificación a la corriente de datos de contenido cifrado bajo la primera clave de descodificación de contenido 40. El resultado de la aplicación del primer cifrado de descodificación está provisto como entrada a una segunda unidad de descodificación 48, que aplica un cifrado de descodificación bajo la segunda clave de descodificación de contenido 43. El resultado de la aplicación del segundo cifrado de descodificación está provisto como entrada a una tercera unidad de descodificación 49, que aplica un tercer cifrado de descodificación bajo la tercera clave de descodificación de contenido 46.

De esta manera, se requiere una versión particular de la primera clave 24 para descifrar la corriente de datos de contenido cifrado. Aunque haya sido posible establecer una clave de sesión 27 usando un par de claves pública/privada diferentes de aquellas generadas por el generador de par de claves pública/privada 12, la descifrado por el descifrador 15 fallará, puesto que la segunda unidad de descodificación 48 usará una segunda clave de descodificación de contenido basada en la primera clave incorrecta. Como la segunda clave de descodificación de contenido 43 se usa en un cifrado entremedias de dos cifrados que usan claves basadas en la palabra de control 37, no es posible descodificar la corriente de datos de contenido cifrado bajo la primera clave correcta fuera del descifrador 15 y proporcionar el descifrador 15 con mensajes de palabras de control 33 procedentes de otra fuente. Por esta razón, la primera clave 24 no necesita ser mantenida secreta, ni tampoco la segunda función f_b.

En una forma de realización alternativa (no ilustrada en detalle), un efecto similar es conseguido usando una única unidad de descodificación que recibe una clave basada en la palabra de control 37 y la primera clave 24. Una unidad de función es empleada de forma ventajosa para formar la única clave. Como un ejemplo, la unidad de descodificación podría aplicar un cifrado AES. Una clave AES de 128 bits podría ser obtenida concatenando 64 bits de información desde la clave de la palabra de control 37 y 64 bits de información de clave desde la primera clave 24. De forma alternativa, la unidad de función podría implementar una función de mezcla. En esta forma alternativa, los 128 bits son generados conteniendo la palabra de control 37 y la primera clave 24 es sometida a la función de mezcla. Se señala que la clave AES en estas formas de realización es derivable parcialmente desde la primera clave 24 y parcialmente desde la palabra de control 37.

Volviendo a la forma de realización ilustrada, la segunda función f_b convierte la primera clave 24 en una clave para el uso en un cifrado simétrico. En una forma de realización, la segunda función f_b se utiliza para derivar una clave

para un cifrado AES desde una clave pública para el uso en un algoritmo RSA. Esta segunda función f_b puede ser una clase de porción para reducir la longitud de clave de, por ejemplo, 1024 bits a una longitud de clave de 128 bits. En vez de un cifrado AES, un cifrado simétrico para un objetivo especial puede ser implementado en la segunda unidad de descodificación 48. Como es conocido, las claves usadas en cifrados asimétricos de clave son generalmente menos aleatorias que aquellas usadas en cifrados simétricos.

La Fig. 4 ilustra cómo los cambios de clave son efectuados, usando una corriente de transporte MPEG-2 conforme a la norma internacional ISO/IEC 13818-1 como un ejemplo de una corriente de datos de contenido cifrado. Por supuesto, los métodos perfilados aquí son igualmente aplicables a una corriente de datos de contenido cifrado compuesta de paquetes IP o paquetes RTP. Volviendo al presente ejemplo, cada uno de una secuencia de paquetes TS de MPEG-2 50a-50j comprende una cabecera 51 y una carga útil 52. La carga útil 52 es descifrada por el descifrador 15. La cabecera 51 indica que la carga útil 52 está codificada, y cual de una palabra de control par o impar 37 es conveniente para el uso para generar la primera y tercera claves de descodificación de contenido 40,46. Paralelamente, los mensajes de clave 53-57 son continuamente transmitidos. Los mensajes de clave 53-57 se sincronizan con la corriente de datos de contenido cifrado por el sistema de cabecera 1.

En la Fig. 4, cinco períodos de palabras de control son mostrados. Una palabra de control siguiente 37 en una secuencia se vuelve válida con cada transición a un periodo de palabra de control posterior. El periodo para el que una primera clave 24 es válida es más largo que la longitud de un periodo de palabra de control. En la Fig. 4 una transición de una primera primera clave P_{k0} a una segunda primera clave P_{k0} ocurre después de tres períodos de palabra de control. En los dos primeros períodos de palabra de control, el primer y segundo mensajes de clave 53,54 son enviados. Cada uno contiene información correspondiente a la primera primera clave P_{k0}, al igual que los datos que indican que la siguiente primera clave es también la primera primera clave P_{k0}. Un tercer mensaje de clave 55 es enviado dentro de un periodo de palabra de control que precede un periodo de palabra de control cuyo inicio coincide con el inicio del uso de una nueva primera clave. Al menos una copia del tercer mensaje de clave 55 es enviado dentro del tercer periodo de palabra de control. La nueva primera clave se utiliza para descifrar aquellas de los paquetes TS de MPEG-2 50 cifradas usando la palabra de control asociada al cuarto periodo de palabra de control.

El tercer mensaje de clave 55 incluye una cabecera 58, un campo 59 en referencia a la primera corriente clave, es decir la primera primera clave P_{k0}, un campo 60 en referencia a la siguiente primera clave - ésta es la segunda primera clave P_{k1} en este caso - y lleva información de la clave 61 correspondiente a la primera clave actualmente en uso apta para descifrar la corriente de datos de contenido cifrado, la primera primera clave P_{k0} El tercer mensaje de clave 55 también lleva información 62 correspondiente a la primera clave válida dentro del periodo de la palabra de control posterior, la segunda primera clave P_{k1}, desde el campo 60 en referencia a la siguiente primera clave se refiere a una clave diferente que el campo 59 referente a la primera clave actual. Los cuarto y quinto mensajes de clave 56,57 se refieren sólo a la segunda primera clave P_{k1}, porque la primera clave no cambia tras la siguiente transición a una palabra de control nueva. Esta manera de señalar la primera clave para el periodo de palabra de control actual y siguiente, si éste difiere de la primera clave actual, en mensajes de clave 53-55 enviados al mismo tiempo y en sincronización con los paquetes TS de MPEG-2 actuales 50, que identifican la palabra de control actual, tiene el efecto de que los paquetes de datos que llevan la corriente de datos de contenido cifrado no necesitan referirse directamente a la primera clave pertinente 24 para la descifrado de la carga útil del paquete de datos. Para claridad, la Fig. 4 muestra sólo un mensaje de clave 53-57 para cada uno de los cinco períodos de palabra de control. En otras formas de realización, diferentes copias del mensaje de clave aplicable a un periodo de palabra de control particular son enviadas dentro de este periodo de palabra de control. El efecto es permitir que el descifrador comience la operación anteriormente.

Si la primera clave pública 24 es cambiada, entonces la clave privada correspondiente, la segunda clave, en el subsistema de acceso condicional 3 debe también cambiar. En formas de realización donde el subsistema de acceso condicional 3 recibe la segunda clave en un mensaje codificado, es ventajoso usar un ECM. De esta manera, la sincronización entre el inicio del uso de una segunda clave siguiente también coincide con el inicio del uso de una palabra de control siguiente, debido a que está siendo soportada en forma codificada en el mismo mensaje del sistema de cabecera. Por lo tanto, las transiciones de la primera y la segunda clave coinciden con la transición de una palabra de control a una palabra de control posterior en una secuencia. En otra forma de realización, los EMMs se utilizan para llevar las segundas claves codificadas. Cuando el descifrador 15 ejecuta la fase 32 de envío de una clave de sesión codificada 27 al subsistema de acceso condicional 3, el recibo de este mensaje informa al subsistema de acceso condicional 3 que está listo para cambiar a una segunda clave siguiente previamente recibida en un EMM. En una forma de realización, el subsistema de acceso condicional se configura para limitar el nivel en el que nuevas claves de canal, es decir claves de sesión y/o segundas claves, se establecen a un nivel inferior o en uno predeterminado. Esto asegura que el subsistema de acceso condicional 3 no puede ser usado con más de un número predeterminado de descifradores 15. En caso de que el subsistema de acceso condicional 3 se limite al uso conjuntamente con un descifrador y cada mensaje al descifrador lleva una palabra de control, el nivel más rápido en el que el subsistema de acceso condicional se configura para aceptar mensajes que establecen una clave nueva para proteger y/o autentificar la información transferida por medio del canal de comunicación al descifrador corresponderá al nivel en el que ocurren las transiciones a la palabra de control posterior.

Bloques funcionales de una forma de realización del cifrador 6 implementado en hardware se muestran en la Fig. 5. Un ejemplo de tal implementación es un circuito integrado específico de aplicación, o conjunto de puertas programables de campo. El descifrador incluye una interfaz de entrada 63 para recibir una corriente de datos de contenido claro, por ejemplo una sucesión de paquetes TS de MPEG-2, paquetes IP, paquetes RTP o paquetes de

corriente elemental de programa (PES) tal y como se define en la norma internacional ISO/IEC 13818-1. El cifrador 6 además incluye una interfaz de entrada 64 para recibir una secuencia de palabras de control del generador de CW 10. El descifrador 6 también incluye una interfaz de entrada 65 para recibir la primera clave 24 del generador de par de claves pública/privada 12.

La primera clave 24 es una clave pública de un par de claves asimétricas, pero se convierte a una segunda clave de codificación de contenido para el uso en un algoritmo de codificación simétrica, dicha conversión se realiza por una segunda unidad de función 66. Esta segunda unidad de función 66 corresponde a la segunda unidad de función 41 del descifrador 15.

Una actual de una secuencia de palabras de control recibida a través de la interfaz de entrada 64 está provista para las primera y tercera unidades de función 67,68. Las primera y tercera unidades de función 67,68 corresponden a las primera y tercera unidades de función 38,44 del descifrador 15. Éstas generan las primera y tercera claves de codificación de contenido, que se suministran a las primera y tercera unidades de codificación de contenido 69,70. La segunda clave de codificación de contenido, generada por la segunda unidad de función 66 se usa en un cifrado simétrico de clave, aplicado por una segunda unidad de codificación de contenido 71. La corriente de datos de contenido cifrado proporcionada como salida por la tercera unidad de codificación de contenido 70 está provista a una interfaz de salida 72.

La segunda unidad de codificación de contenido 71 aplica la operación de codificación bajo una clave al menos derivable de una clave que forma un par de claves con la clave que se proporciona al subsistema de acceso condicional 3, como será aclarado a partir de la descripción de arriba. El término "par de claves" se refiere a un par de claves del cual una es utilizable para descodificar datos codificados bajo la otra. En el caso de un cifrado simétrico, las dos claves de un par de claves son por supuesto idénticas. La secuencia de la primera, segunda y tercera unidades de codificación de contenido 69,71,70 fuerza al descifrador a usar una secuencia correspondiente de unidades de descodificación 47-49, donde una unidad de descodificación intermedia usa una clave derivada de la primera clave 24. Tal y como se menciona, el efecto es que la primera clave 24 no necesita necesariamente ser mantenida secreta para forzar al uso de un subsistema de acceso condicional particular 3.

Cuando los receptores emplean el descifrador alternativo perfilado arriba que usa una única unidad de descodificación que recibe una clave basada en la palabra de control 37 y la primera clave 24, el cifrador 6 comprenderá una única unidad de codificación complementaria (no mostrada). Una unidad de función es empleada de forma ventajosa para formar la única clave usada por el cifrador 6. La clave usada en esta forma de realización, que es preferiblemente simétrica, se deriva parcialmente de la primera clave 24 y parcialmente de la palabra de control 37. Obviamente, esta derivación puede ocurrir bien dentro del cifrador 6 o en una unidad externa.

El cifrador ilustrado 6 se configura para asegurar que un cambio en la primera clave 24 a un valor nuevo coincide con un cambio a una siguiente de una secuencia de palabras de control. En el caso de una corriente de datos de contenido claro compuesta por una secuencia de paquetes, se utiliza una palabra de control 37 de la secuencia para derivar la primera y tercera claves de codificación de contenido para codificar un número determinado de cargas útiles de paquete, antes de que ocurra una transición a una palabra de control posterior 37 de la secuencia, es decir el inicio de un periodo de palabra de control nuevo. Un valor particular de la primera clave 24 se usa sobre varios períodos de palabra de control, antes de ser sustituidos por un valor nuevo a una transición de un periodo de palabra de control al siguiente.

La invención no está limitada a las formas de realización anteriormente descritas, pero pueden ser variadas dentro del campo de las reivindicaciones anexas. Por ejemplo, aunque el descifrador ha sido descrito como un componente integral del receptor 2, o un descifrador similar adicional, puede también ser comprendido en un módulo despegable con una interfaz al receptor 2. Puede incluso ser comprendida en una tarjeta inteligente, con el subsistema de acceso condicional 3. En vez de usar los mensajes de clave 53-57, una señalización más compleja del estado de cifrado puede ser usada tal como aquella descrita en ISMA, ISMA Encryption and Authentication Specification 1.0, Feb. 2004, disponible por Internet Streaming Media Alliance.

Aunque la descripción se ha centrado en una implementación en un sistema para suministrar y obtener acceso condicional a una radiotransmisión cifrada o corriente de datos de contenido de multidifusión, un sistema para la gestión de derechos digitales puede de forma similar comprender el cifrador y descifrador descritos en detalle anteriormente. El subsistema de acceso condicional en tal forma de realización es más comúnmente denominado agente DRM. En tal forma de realización, el objeto de datos de contenido cifrado comprende un fichero de datos. Un fichero de datos de contenido cifrado puede ser serializado en una corriente de datos de contenido cifrado, a la que se pueden aplicar las técnicas perfiladas arriba. Se señala que tal forma de realización puede hacer uso de una única clave de descifrado de contenido para el fichero entero, en efecto usando una palabra de control única mejor que una secuencia de palabras de control.

Referencias citadas en la descripción

Esta lista de referencias citada por el solicitante ha sido recopilada exclusivamente para la información del lector. No forma parte del documento de patente europea. La misma ha sido confeccionada con la mayor diligencia; la OEP sin embargo no asume responsabilidad alguna por eventuales errores u omisiones.

Documentos de patente citados en la descripción

- WO 9738530 A [0007]
- WO 9909743 A [0009]

Bibliografia distinta de patentes citada en la descripción

- **ISMA**. *ISMA encryption and Authentication Specification 1.0*, February 2004, [0092]

REIVINDICACIONES

1. Método de descifrado de un objeto de datos de contenido cifrado (50a-50j),

donde al menos una sección del objeto de datos de contenido cifrado (50a-50j) se descifra aplicando al menos una operación de descodificación bajo una clave (40,46) al menos parcialmente derivable de una clave de descifrado de contenido,

donde la clave de descifrado de contenido (37) se obtiene de un mensaje (33) recibido de un subsistema de acceso condicional (3) sobre un canal de comunicación de datos,

donde al menos un criptograma de datos obtenible de la clave de descifrado de contenido (37) en el mensaje (33), cada criptograma de los mismos es llevado en el mensaje (33), es descifrado bajo una clave de canal asociada (24,27), y

donde una primera clave (24) se utiliza para establecer cada clave de canal (24,27), **caracterizado** por el hecho de que

al menos la sección del objeto de datos de contenido cifrado (50a-50j) es descifrada aplicando una operación de descodificación bajo una clave (43) al menos parcialmente derivable de la primera clave (24).

2. Método según la reivindicación 1, donde la primera clave (24) es una clave pública de un par de claves asimétricas,

donde una operación criptográfica que incluye un cifrado asimétrico según la primera clave (24) se aplica en datos intercambiados por el subsistema de acceso condicional (3).

3. Método según la reivindicación 1 o 2, donde al menos la sección del objeto de datos de contenido cifrado (50a-50j) es descifrada aplicando una operación de descodificación bajo una clave basada en la primera clave (24) y la clave de descifrado de contenido (37).

4. Método según cualquiera de las reivindicaciones 1-3, donde al menos la sección del objeto de datos de contenido cifrado (50a-50j) se descifra al menos aplicando una primera operación de descodificación en la sección del objeto de datos de contenido cifrado bajo una clave (40) al menos parcialmente derivable de una clave de descifrado de contenido y aplicando otra operación de descodificación bajo una clave (43) al menos derivable de la primera clave (24) a la salida de la primera operación de descodificación.

5. Método según cualquiera de las reivindicaciones 1-4, donde al menos la sección del objeto de datos de contenido cifrado se descifra al menos aplicando una segunda operación de descodificación bajo una clave (46) al menos parcialmente derivable de una clave de descifrado de contenido (37) para datos obtenidos como salida de otra operación de descodificación bajo una clave (43) al menos derivable de la primera clave (24).

6. Método según las reivindicaciones 4 y 5, que incluye la derivación de al menos dos claves (40,46) de una única clave de descifrado de contenido (37), donde una primera de las claves derivadas (40,46) se usa en la primera operación de descodificación y una segunda de las claves derivadas se usa en la segunda operación de descodificación.

7. Método según cualquiera de las reivindicaciones 1-6, que incluye la aplicación de una operación de descodificación que implica un cifrado simétrico de clave bajo una clave (43) obtenida como función de al menos la primera clave (24).

8. Método según cualquiera de las reivindicaciones 1-7, que incluye

la generación de una clave de canal (27),

la codificación de la clave de canal generada (27) bajo la primera clave (24) y la comunicación de la clave de canal codificada al subsistema de acceso condicional (3), y

la descodificación de al menos parte del mensaje (33) recibido del subsistema de acceso condicional (3) bajo la clave de canal (27), preferiblemente usando un cifrado simétrico.

9. Método según la reivindicación 8, donde una clave de canal nueva (24,27) se establece al recibir una versión nueva de la primera clave (24).

10. Método según cualquiera de las reivindicaciones 1-9, que incluye

la obtención de una firma digital del mensaje (33) recibido del subsistema de acceso condicional,

el uso de al menos la primera clave (24) para verificar la firma digital, y

la descifrado de al menos la sección del objeto de datos de contenido descifrado (50a-50j) en función del resultado de la verificación.

11. Método según la reivindicación 10, que incluye

la generación una clave de canal, preferiblemente como un número aleatorio,

la codificación de la clave de canal generada (27) bajo la primera clave (24) y la comunicación de la clave de canal codificada al subsistema de acceso condicional (3), y

además la utilización de la clave de canal (27) para verificar la firma digital.

12. Dispositivo para descifrar un objeto de datos de contenido cifrado (50a-50j), que incluye una entrada (22) para recibir el objeto de datos de contenido cifrado y una entrada (29) para recibir mensajes de un subsistema de acceso condicional (3) sobre un canal de comunicación de datos **caracterizado** por el hecho de que el dispositivo se configura para ejecutar un método según cualquiera de las reivindicaciones 1-11.

13. Método para acceso condicional a un objeto de datos de contenido, que incluye

el suministro de al menos una clave de cifrado de contenido a un cifrador (6), dispuesto para cifrar al menos una sección del objeto de los datos aplicando al menos una operación de codificación bajo una clave (40,46) al menos parcialmente derivable de la clave de cifrado de contenido (37),

el suministro de un mensaje de derecho a al menos un subsistema de acceso condicional (3) para suministrar un mensaje (33) sobre un canal de comunicación de datos a un descifrador (15) de un receptor autorizado (2), dicho mensaje (33) incluye los datos que permiten que el descifrador (15) obtenga la clave de descifrado de contenido (37) y que el mensaje (33) lleve al descifrador (15) al menos un criptograma,

el subsistema de acceso condicional (3) estando configurado para generar el criptograma codificando bajo una clave de canal (27) datos obtenibles de la clave de descifrado de contenido (37) en el mensaje (33),

donde el subsistema de acceso condicional (3) se configura para usar una segunda clave para establecer la clave de canal (27), **caracterizado** por,

el suministro de los subsistemas de acceso condicional (3) con información de la clave representativa de la segunda clave y el suministro de la información de la clave del cifrador representativa de una primera clave (24) formando un par de claves con la segunda clave, donde el cifrador (6) está dispuesto para cifrar al menos la sección del objeto de datos de contenido aplicando una operación de codificación bajo una clave (43) al menos parcialmente derivable desde la primera clave (24).

14. Método según la reivindicación 13, donde la segunda clave es una clave secreta de un par de claves asimétricas,

donde una primera clave (24) correspondiente a una clave pública del par de claves asimétricas está provista a un transmisor (7) dispuesto para comunicar la primera clave (24) en un mensaje al receptor autorizado (2).

15. Método según la reivindicación 14, donde el objeto de datos de contenido comprende una corriente de datos de contenido, donde una secuencia de palabras de control está provista al cifrador (6), el cifrador (6) estando dispuesto para usar una actual de la secuencia de palabras de control como la clave de cifrado de contenido, que además incluye transmitir la primera clave (24) en un mensaje de control de derecho adicional que incluye al menos una de la secuencia de palabras de control.

16. Método según cualquiera de las reivindicaciones 13-15, que incluye el suministro de al menos un dispositivo portátil protegido que comprende una unidad de procesamiento (21), memoria, una interfaz (18) a un descifrador (15) de un receptor autorizado (2) y al menos uno de los subsistemas de acceso condicional (3).

17. Sistema para suministrar acceso condicional a un objeto de datos de contenido, que incluye

un cifrador (6), dispuesto para cifrar al menos una sección del objeto de datos de contenido aplicando al menos una operación de codificación

bajo una clave (40,46) al menos parcialmente derivable de una clave de cifrado de contenido (37),

al menos un subsistema de acceso condicional (3) para suministrar un mensaje (33) sobre un canal de comunicación de datos a un descifrador (15) de un receptor autorizado (2), dicho mensaje (33) incluye datos que permiten que el descifrador (15) obtenga la clave de descifrado de contenido (37) y el mensaje (33) que lleva al menos un criptograma,

donde el subsistema de acceso condicional (3) se configura para generar el criptograma codificando bajo una clave de canal (27) de datos obtenibles a partir de la clave de descifrado de contenido (37) en el mensaje (33) al descifrador (15),

donde el subsistema de acceso condicional (3) se configura para usar una segunda clave para establecer la clave de canal (27), **caracterizado** por el hecho de que,

el cifrador (6) está dispuesto para cifrar al menos la sección del objeto de datos de contenido aplicando una operación de codificación bajo una clave (43) al menos parcialmente derivable a partir de una primera clave (24) formando un par de claves con la segunda clave.

18. Sistema según la reivindicación 17, donde la segunda clave es una clave secreta de un par de claves asimétricas, y donde el sistema se configura para suministrar una primera clave (24) correspondiente a una clave pública del par de claves asimétricas a un transmisor (7) dispuesto para comunicar la primera clave (24) en un mensaje (53-57) al receptor autorizado (2).

19. Sistema según la reivindicación 17 o 18, configurado para cifrar un objeto de datos de contenido que comprende una corriente de datos de contenido, donde el sistema está dispuesto para efectuar un cambio en valor de la segunda clave, donde el sistema además comprende un sistema (8-12) para sincronizar un cambio en el suministro de la segunda clave a un valor nuevo con una transición de uso de una actual para al uso de una siguiente de una secuencia de palabras de control como clave de cifrado de contenido.

20. Sistema según cualquiera de las reivindicaciones 17-19, donde el cifrador (6) se configura para cifrar al menos la sección del objeto de datos de contenido al menos aplicando una primera operación de codificación en la sección del objeto de datos de contenido bajo una clave (40) al menos parcialmente derivable de una clave de cifrado de contenido y aplicando otra operación de codificación bajo una clave (43) al menos parcialmente derivable de una primera clave (24) formando un par de claves con la segunda clave a la salida de la primera operación de codificación.

21. Sistema según cualquiera de las reivindicaciones 17-20 donde el cifrador (6) se configura para cifrar al menos la sección del objeto de datos de contenido al menos aplicando una segunda operación de codificación bajo una clave (46) al menos parcialmente derivable de una clave de cifrado de contenido para datos obtenidos como salida de otra operación de codificación bajo una clave (43) al menos parcialmente derivable de una primera clave (24) formando un par de claves con la segunda clave.

22. Sistema según las reivindicaciones 20 y 21, configurado para derivar al menos dos claves (40,46) de una única clave de cifrado de contenido (37), y para usar una primera de las claves derivadas en la primera operación de codificación y una segunda de las claves derivadas en la segunda operación de codificación.

23. Sistema según cualquiera de las reivindicaciones 17-22, donde la operación de codificación bajo una clave (43) al menos parcialmente derivable desde la primera clave (24) implica un cifrado simétrico de clave bajo una clave (43) obtenida como función de al menos la primera clave (24).

24. Uso de un dispositivo para cifrar un objeto de datos de contenido en un sistema según las reivindicaciones 17-23.

25. Programa informático, que incluye un conjunto de instrucciones capaz, cuando se incorpora en un medio legible por máquina, de provocar que un sistema que tiene capacidades de procesamiento de la información ejecute un método según cualquiera de las reivindicaciones 1-11 o reivindicaciones 13-15.

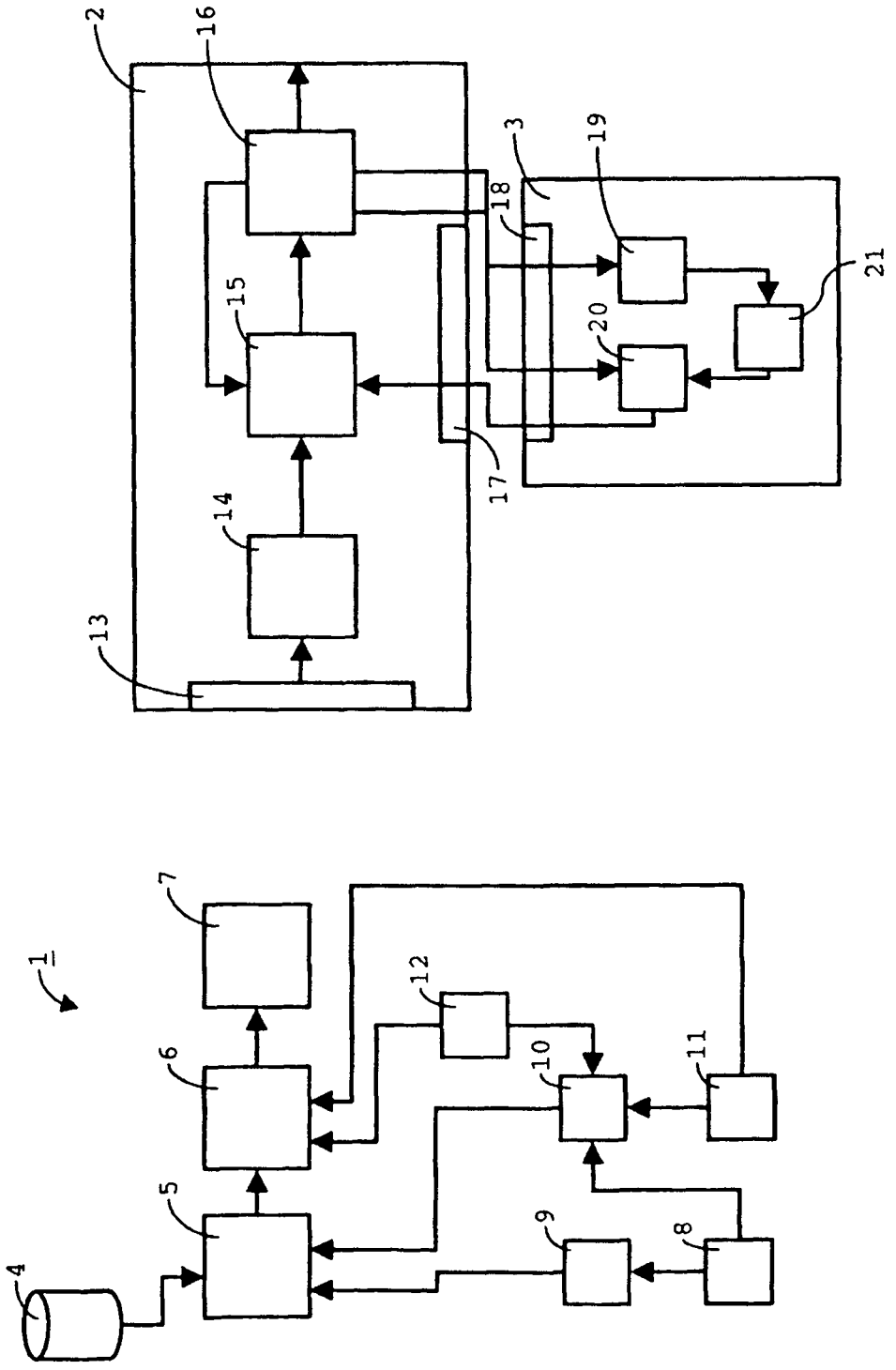

Fig. 1

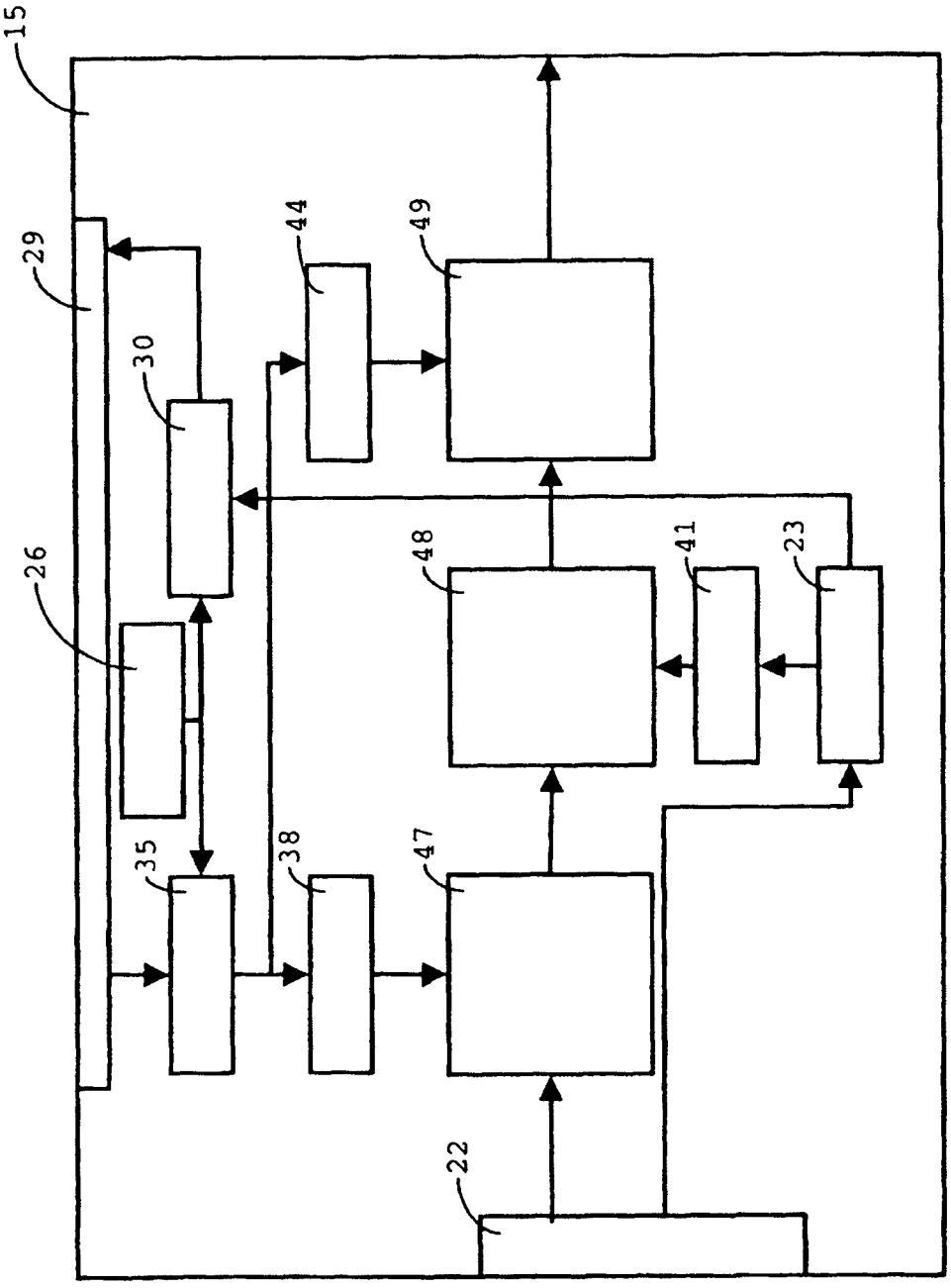

Fig. 2

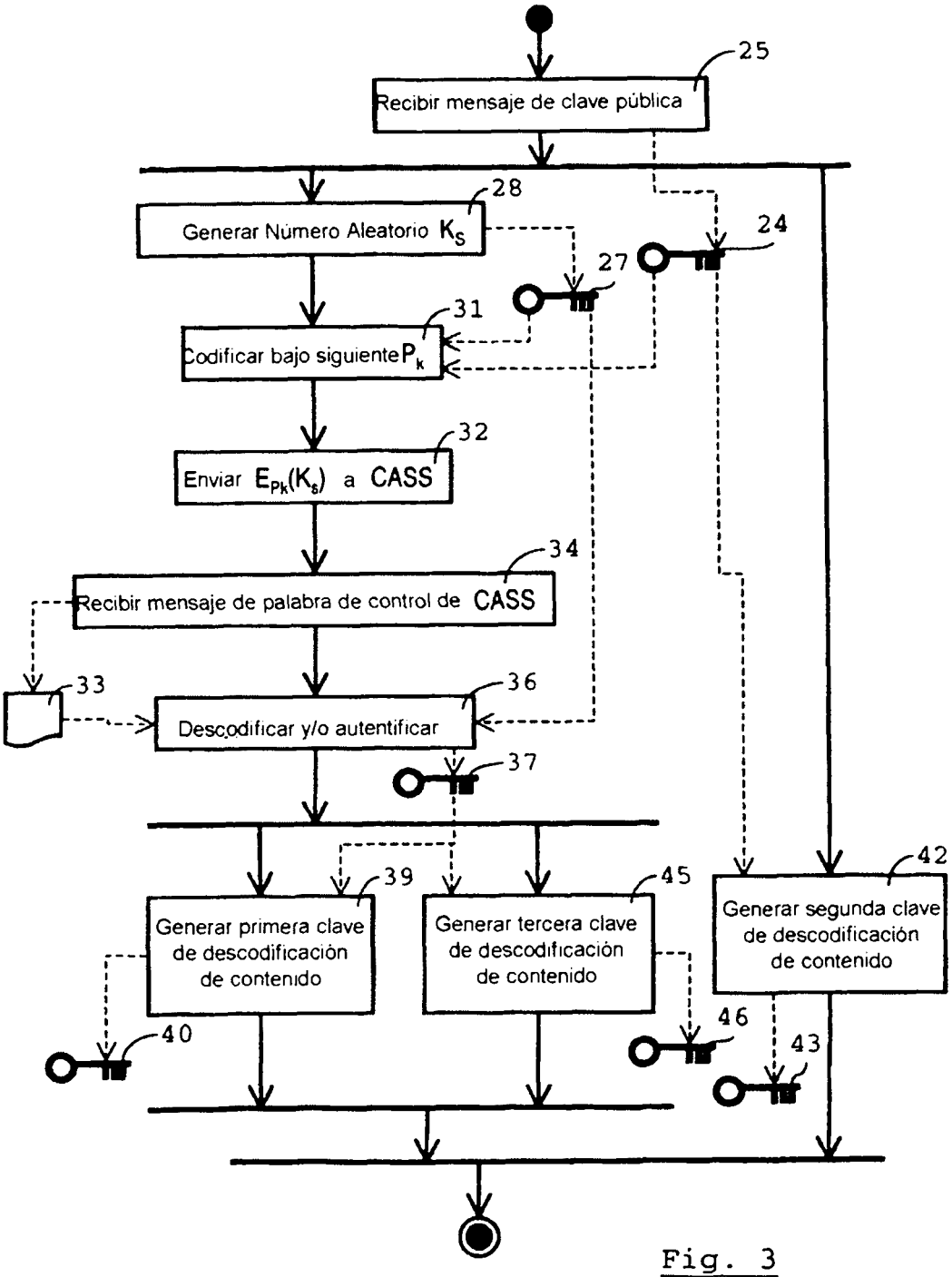
25
Recibir mensaje de clave pública
28
Generar Número Aleatorio K_S
24
27
31
Codificar bajo siguiente P_k
32
Enviar $E_{Pk}(K_s)$ a CASS
34
Recibir mensaje de palabra de control de CASS
33
36
Descodificar y/o autentificar
37
39
Generar primera clave de descodificación de contenido
45
Generar tercera clave de descodificación de contenido
42
Generar segunda clave de descodificación de contenido
40
46
43

Fig. 3

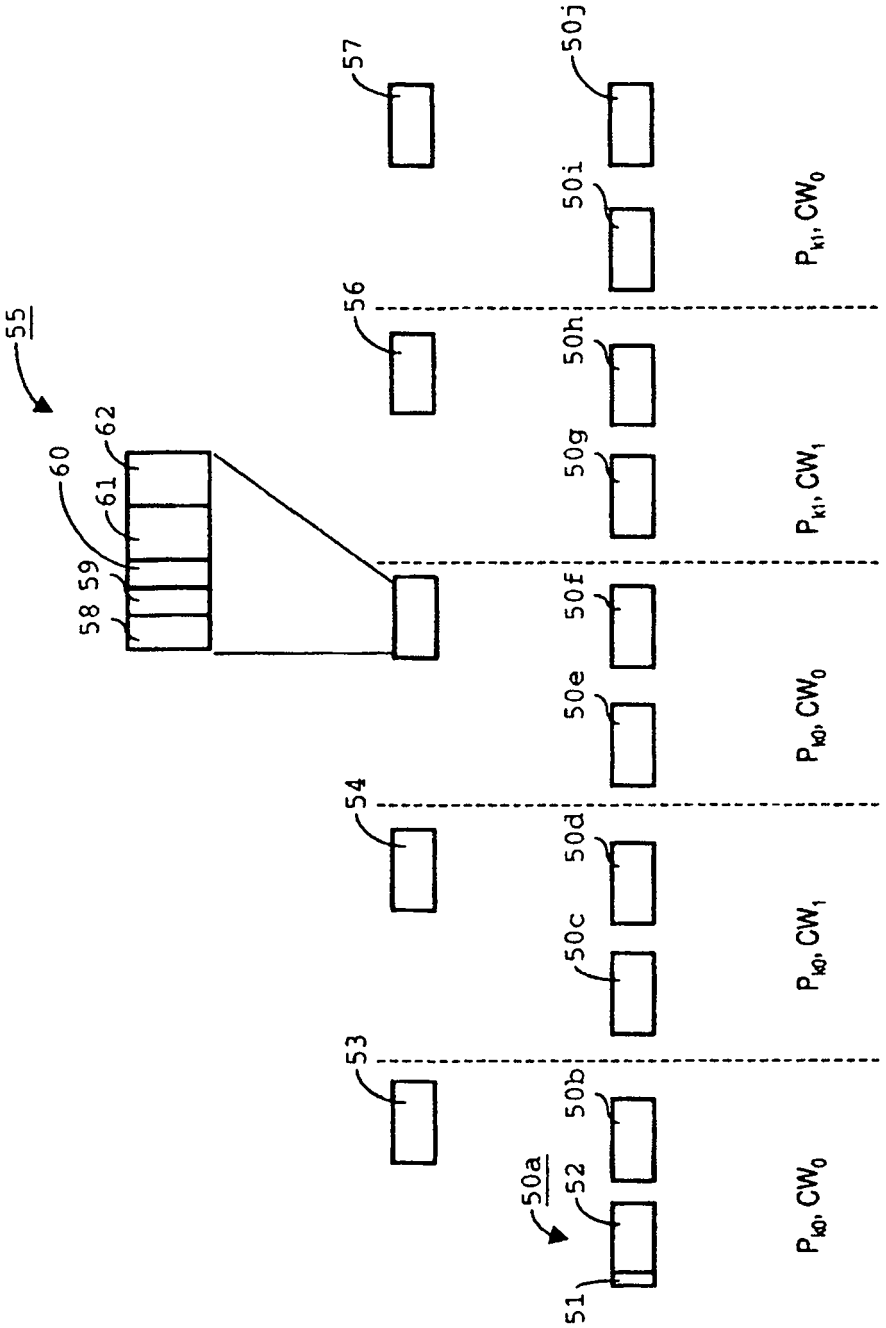
55
60
62
61
58 59
57
56
54
53
50a
52
51
50b
50c
50d
50e
50f
50g
50h
50i
50j
P_{k0}, CW_0
P_{k0}, CW_1
P_{k0}, CW_0
P_{k1}, CW_1
P_{k1}, CW_0

Fig. 4

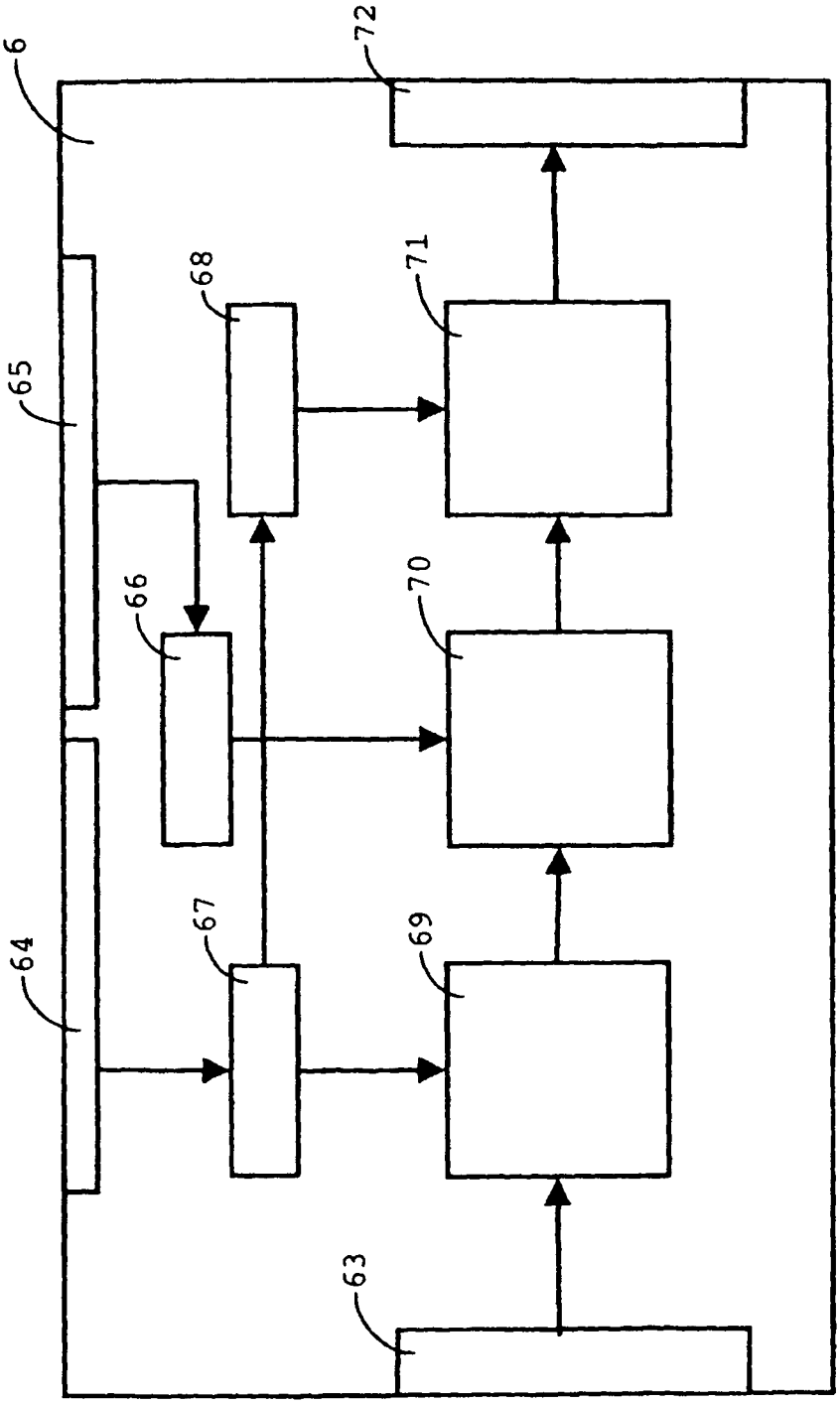

Fig. 5