(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 376 158**

(51) Int. Cl.:
***H04M 7/16*** (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **00901474 .7**
(96) Fecha de presentación: **09.02.2000**
(97) Número de publicación de la solicitud: **1254556**
(97) Fecha de publicación de la solicitud: **06.11.2002**

(54) Título: **DESCODIFICADOR, PROCEDIMIENTO DE DESCODIFICACIÓN Y TARJETA DE CHIP.**

(45) Fecha de publicación de la mención BOPI:
**09.03.2012**

(45) Fecha de la publicación del folleto de la patente:
**09.03.2012**

(73) Titular/es:
**SWISSCOM AG**
**ALTE TIEFENAUSTRASSE 6**
**3050 BERN, CH**

(72) Inventor/es:
**LAUPER, Eric;**
**RITTER, Rudolf y**
**BISCHOFF, Jean-Claude**

(74) Agente/Representante:
**Sugrañes Moliné, Pedro**

**ES 2 376 158 T3**

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

## DESCRIPCIÓN

Descodificador, procedimiento de descodificación y tarjeta de chip

Campo técnico

La presente invención se refiere a un descodificador, por ejemplo un descodificador que descodifica datos digitales codificados, así como a un procedimiento de descodificación y a una tarjeta de chip correspondiente.

Estado de la técnica

En un sistema de televisión de pago (Pay-TV), el receptor selecciona los programas o los datos que quiere recibir, y paga para la descodificación de estos datos, que son enviados de modo encriptado. Entre otros, se conocen sistemas en los que los receptores cierran un abono con el emisor de televisión para el uso ilimitado de los datos, y sistemas en los que los usuarios sólo han de pagar por los datos descodificados que realmente se han descodificado a partir de una tarjeta de chip insertada en el descodificador (pay-per-view).

Para descodificar los datos, el receptor necesita por lo general un descodificador con el que los datos emitidos por el emisor son descodificados, y que también son responsables de la determinación del tiempo de uso y, dado el caso, para cargar la tarjeta de chip con el importe que se ha de facturar. Sólo los usuarios que disponen del descodificador adecuado y de la clave de descodificación adecuada pueden descodificar los datos emitidos en modo broadcast, y reproducirlos en una forma que se pueda comprender.

Los descodificadores también se usan en otros sistemas en los que los datos emitidos, entre otros los datos emitidos en el modo de broadcast, sólo pueden ser reproducidos por los receptores autorizados, por ejemplo conjuntamente con Internet o con sistemas de comunicaciones móviles.

Con el sistema DAB o DVB (Digital Audio o Digital Video Broadcasting), se pueden emitir, adicionalmente al programa, también datos que acompañen al programa y datos que no acompañen al programa en el modo de broadcast. Habitualmente se desea poder acceder a estos datos, para que sólo puedan ser descodificados por los receptores autorizados con un descodificador y una clave de descodificación.

La Figura 1 muestra de modo esquemático un sistema de descodificación conocido con un emisor 1, que envía datos, por ejemplo datos de imágenes, a un gran número de descodificadores 5, como por ejemplo receptores de televisión. Cada descodificador 5 comprende una parte de recepción 2, por ejemplo un sintonizador de televisión, un módem, etc. Los datos x recibidos por la parte de recepción 2 son depositados en una memoria de buffer 3, y son descodificados por un módulo de descodificación 4. El módulo de descodificación 4 descodifica los datos x (por ejemplo permutando para ello líneas de la imagen y/o bloques digitales y/o combinándolos), y de este modo conforma una imagen descodifica y, que se reproduce por medio de medios de reproducción 8. Las reglas de permutación y de combinación se definen por medio de una clave de descodificación secreta, que es generada por un generador de claves 6. En el caso más sencillo, la clave de descodificación K se fija en el módulo de descodificación 4, y con ello no se puede modificar.

La Figura 2 muestra un ejemplo de un módulo de descodificación 4 digital, en este caso un descifrador. El módulo de descodificación 4 comprende en este ejemplo un registro de desplazamiento 40 con un gran número de celdas, en las que se almacenan, por ejemplo, los siguientes bits, bytes, grupos de bytes (de modo correspondiente, por ejemplo, a una línea de una señal de televisión o a un bloque de imágenes) de la señal x(i) codificada. Cada celda del registro de desplazamiento 40 está unida con una conexión AND 41, cuya segunda entrada está unida con un elemento (por ejemplo un bit) de una clave de descodificación $K=\{k_n k_{n-1} k_{n-2}..k_1 k_0\}$. La salida de cada conexión AND 41 se deriva a una conexión XOR 42, cuya segunda entrada está unida con la salida de la conexión XOR 42 anterior. La primer celda del registro de desplazamiento 40 y la primera conexión XOR 42 están unidas con la señal x(i) codificada. La última conexión XOR 42 entrega la señal y(i) descodificada.

Este módulo de descodificación 4 puede descodificar con la clave de descodificación $K=\{k_n k_{n-1} k_{n-2}..k_1 k_0\}$ una señal x codificada con un polinomio $k_n x^n + k_{n-1} x^{n-1} + k_{n-2} x^{n-1} +.. k_1 x + k_o$, y generar la señal y descodificarla.

No se ha definido ninguna arquitectura estandarizada para descodificadores y para módulos de descodificación. En particular, la longitud de la clave de descodificación K o bien del registro de desplazamiento 40 y el formato del bloque digital en las celdas del registro de desplazamiento dependen del sistema de emisión, e incluso del emisor. En muchos sistemas de emisión se usan módulos de descodificación más complejos con otra arquitectura, por ejemplo módulos de descodificación que emplean varios registros de desplazamiento, o se usan otras conexiones lógicas y algoritmos de descodificación más complejos. Cada emisor 1, con ello, selecciona un sistema de descodificación, con el que se puede cumplir con sus requerimientos de seguridad.

Esto, sin embargo, para el usuario del receptor 5 tiene la desventaja de que por lo general se han de comprar varios descodificadores 5 cuando quiere recibir datos de varios emisores (por ejemplo emisores de televisión) que emplean

diferentes algoritmos de codificación (por ejemplo varias disposiciones diferentes de registros de desplazamiento y conexiones lógicas).

Adicionalmente, un emisor no puede reemplazar el algoritmo de codificación usado sin sustituir todo el parque de receptores distribuido a los usuarios finales. Cuando el algoritmo de codificación empleado ya no cumple con los requerimientos de seguridad deseados, con ello, sólo se puede sustituir con un coste elevado.

La clave de descodificación K usada por el módulo de descodificación 4 puede ser fijada, por ejemplo, por el emisor 1, y puede ser depositada en el descodificador. Esto, sin embargo, tiene la desventaja de que cada uno que haya encontrado la clave de descodificación K puede seguir usando ésta durante un tiempo ilimitado para descodificar datos recibidos.

Se conoce ya que este problema puede ser evitado cuando la clave se reemplaza de modo periódico. En este caso, el emisor ha de fijar una nueva clave K, y transmitirla a través de un canal seguro adecuado al descodificador 5.

El documento WO-A1-94/08408 describe, por ejemplo, un dispositivo de comunicación con una estación central que, cuando se cumplen ciertas condiciones, envía claves de descifrado a través de una red móvil a descodificadores móviles. Este documento, sin embargo, no aporta ninguna solución a la problemática de la invención.

El documento EP-A1-0 626 793 describe un descodificador para imágenes de televisión con dos procesadores. Un primer procesador realiza el descifrado de los datos con una clave, que es enviada de modo encriptado por el emisor, y que es desencriptada por un segundo procesador en una tarjeta de chip. Esta solución, sin embargo, tiene la desventaja de que para el descifrado de datos de imágenes animadas con una elevada resolución se requieren procesadores muy rápidos (por ejemplo DSP). Este tipo de procesadores son caros y requieren mucha corriente, de manera que no están indicados para ser integrados en terminales portátiles (por ejemplo en tarjetas de chip).

El documento WO-A1-90/10354 describe un descodificador en el que se genera una tabla de claves de descodificación por medio de un generador aleatorio. El generador aleatorio se inicializa con un valor de inicialización KINI secreto fijo, para generar las tablas correctas.

El documento EP-A2-0 723 373 describe un descodificar equipado con un generador de pseudoruido (pseudo-noise, PN), en el que las señales codificadas son descodificadas a partir de la señal PN. En una variante, la señal PN generada depende de una clave de descifrado y de una lógica de conversión, que pueden ser parametrizadas de modo aleatorio. El propio algoritmo de descodificación, sin embargo, permanece siempre igual.

La seguridad que es garantizada por este tipo de sistemas conocidos, en los que se conoce la estructura del módulo de descodificación 4, y en los que sólo es secreta la clave de descifrado, es sólo tan buena como la seguridad que se garantiza por la clave de descodificación. Cualquier que conoce una posibilidad de identificar la clave de descodificación (por ejemplo por medio de escuchas de la clave durante la transmisión o por medio de la prueba de todas las posibles claves) puede descodificar también los datos recibidos.

Resumen de la invención

Un objetivo de la invención es proporcionar un nuevo descodificador y un nuevo procedimiento de descodificación que permitan una codificación más segura.

Otro objetivo es proporcionar un nuevo descodificador y un nuevo procedimiento de descodificación que se puedan adaptar a diferentes algoritmos de codificación.

Otro objetivo es proporcionar un nuevo descodificador potente y un procedimiento de descodificación con los que también se puedan descodificar flujos de datos rápidos.

Según la presente invención, estos objetivos se consiguen, en particular, por medio de las características de las reivindicaciones independientes. Otras formas de realización ventajosas se derivan además de las reivindicaciones dependientes y de la descripción.

En particular, estos objetivos se consiguen por medio de un descodificador y por medio de un procedimiento de descodificación, en los que se usa una conexión FPGA programable, y en los que la descodificación de los datos de imagen depende de la programación de esta conexión FPGA.

Las conexiones FPGA (Field Programmable Gate Arrays) están formadas por varios bloques lógicos dentro de un único circuito integrado, cuya disposición y conexiones se determina por medio del contenido de una memoria. La funcionalidad de una conexión FPGA se puede variar muy rápidamente escribiendo nuevos datos en la memoria FPGA.

Se describen diferentes conexiones con FPGA, entre otras, en los documentos de patente clasificados en el grupo

H03K-19/177 de la clasificación internacional de patentes. Según esto, ya no describiremos estas conexiones en detalle.

El descodificador conforme a la invención tiene la ventaja de que se puede adaptar a un nuevo algoritmo de descodificación escribiendo en la memoria de la FPGA. Estos nuevos datos pueden ser transmitidos, por ejemplo, desde el emisor a través de diferentes canales posibles. Esto tiene la ventaja de que un emisor puede sustituir el algoritmo de descodificación de un modo muy sencillo en todos los descodificadores, enviando para ello nuevos datos para la programación del circuito FPGA. El algoritmo de descodificación se puede cambiar incluso varias veces dentro de una emisión y durante la transmisión de una única página.

Representa una ventaja la posibilidad de transmitir datos para la programación de la conexión FPGA a través de otro canal de transmisión y/o en otro momento como la clave de descodificación. Los datos para la programación de la conexión FPGA, con ello, se pueden vender, con ello, por ejemplo, como una especie de vale de autorización en tarjetas de chip, en applets, etc., que han de ser adquiridos por los usuarios finales, y que se pueden usar por primera vez cuando se conoce la clave de descodificación adecuada.

Breve descripción de la invención

A continuación se describen con más detalle a partir de los dibujos anexos ejemplos de realización de la invención, en los que

Fig. 1 muestra de modo esquemático un sistema con un descodificador 5 conocido,

Fig. 2 muestra de modo esquemático un módulo de descodificación,

Fig. 3 muestra de modo esquemático un sistema con un descodificador y

Fig. 4 muestra de modo esquemático un sistema con un descodificador según la invención.

Modos para la realización de la invención

La Figura 3 ilustra la arquitectura de un sistema con un descodificador. En este ejemplo, el sistema comprende un emisor 1, preferentemente un emisor de los datos en modo broadcast. En emisor 1 comprende un codificador no representado, para codificar al menos una parte de los datos emitidos, para que sólo los receptores autorizados (que disponen de la clave de descodificación adecuada), puedan reproducir estos datos en una forma reconocible.

El emisor 1 puede estar formado, por ejemplo, por un emisor DAB o DVB (Digital Audio Broadcasting o Digital Video Broadcasting). También se pueden emplear en el marco de esta invención otros procedimientos de emisión y protocolos, por ejemplo con ADSL, UMTS (Universal Mobile Telephone System), PLC (Power Communication Line), FTTH (Fiber to the Home) u otros procedimientos ópticos.

Los datos emitidos por el emisor 1 a través del canal de transmisión A son recibidos por uno o varios receptores 5. En esta variante de realización, el receptor 5 contiene una parte de recepción 2, por ejemplo un receptor DAB, DVB, ADSL, UMTS o PLC, que recibe los datos recibidos (por ejemplo secuencias de imágenes, páginas de Internet, tarjetas WAP, datos que acompañan al DAB, etc.), y los transforma en un formato digital adecuado. Los datos x digitales transformados se depositan entonces en un buffer 3.

El descodificador 5 conforme a la invención comprende un módulo de descodificación 4 (por ejemplo un descifrador según la Figura 2) que usa una clave de descodificación K, para convertir datos x en datos y descodificados, que pueden ser reproducidos por medio de medios de reproducción 8.

En esta primera variante, la clave de descodificación K es generada por un generador de claves 6, que comprende una conexión FPGA. La arquitectura del generador de claves 6, es decir, la conexión de los componentes lógicos en la conexión FPGA, se define por medio de una memoria FPGA 7, por ejemplo una RAM o una ROM o una EEPROM en un módulo reemplazable (por ejemplo en una tarjeta de chip que se puede retirar).

En esta variante, el generador de claves 6 determina la clave de descodificación K tomando como base un valor KINI transmitido por el emisor 1, tal y como se explica posteriormente. El generador de claves 6 puede estar formado en una primera variante posible a partir de un generador aleatorio, que genera una serie de claves, en el que la serie depende del valor de inicialización KINI y de la estructura del generador aleatorio. El emisor 1 (o el usuario del descodificador 5) puede generar, con ello, diferentes series de claves del descodificador, depositando a la entrada del generador de claves 6 un nuevo valor KINI y/o programando de nuevo el contenido P de la memoria FPGA 7. En otra variante, el generador de claves 6 está formado por un descodificador que puede desencriptar los datos de clave encriptadas emitidos por el emisor 1, para reconstruir la clave de descodificación. El descodificador, por ejemplo, puede usar un algoritmo de descodificación asimétrico (por ejemplo según RSA, ECC, El-Garnal, DSA, ESIGN, etc.).

Un usuario no autorizado que sólo conoce el valor de inicialización KINI, si bien no conoce el contenido P de la memoria FPGA 7, con ello, no puede reconstruir la serie generada de claves de descodificación. Al contrario, el conocimiento del contenido P de la memoria FPGA 7 no es suficiente para descodificar los datos x recibidos cuando no se conoce el valor de inicialización KINI.

El receptor 5 comprende de modo ventajoso una segunda parte de recepción 9 para una segunda red de comunicaciones 10 (por ejemplo una pieza de comunicaciones móviles GSM o UMTS, un terminal PLC, un cliente de Internet, etc.). Los datos del emisor 1, entre otros el valor de inicialización KINI y/o el contenido P de la memoria 7, se pueden transmitir preferentemente a través de un canal de transmisión B por medio de esta segunda red de comunicación 10 al receptor 5 (por ejemplo como Applet, como programa ME-XE, como aplicación WAP, etc.). Estos datos, por ejemplo, pueden ser cargados de modo remoto desde un servidor, por ejemplo desde un servidor WAP (Wireless Application Protocol), o un servidor http, en la red de comunicaciones 10, por ejemplo por medio del pago a través de procedimientos electrónicos conocidos de transacción de dinero (por ejemplo con el procedimiento de flexmart descrito en la solicitud de patente WO-A1-98/28900).

El valor de inicialización KINI y/o el contenido de la memoria FPGA 7 se pueden transmitir como variante también a través del mismo canal de transmisión A que los datos codificados, por ejemplo como datos desencriptados que acompañan al programa o que no acompañan al programa (PAD o bien NPAD) de un emisor DAB o bien de un emisor DVB.

Como otra variante, el valor de inicialización KINI y/o el contenido P de la memoria FPGA 7 también pueden ser copiados desde el emisor 1 en las tarjetas de chip 12, que se venden, por ejemplo, a todos los abonados autorizados, o que pueden ser adquiridas comercialmente en quioscos, tiendas, etc. Por ejemplo, se pueden adquirir tarjetas de chip 12 que autorizan al propietario a reproducir datos de una emisora 1 determinada, de una emisión determinada, de un programa del día determinado, o durante una duración determinada.

Es ventajosa la posibilidad de transmitir el valor de inicialización KINI y el contenido de la memoria P a través de dos canales diferentes, para evitar que una escucha que averigüe sólo el KINI o sólo P pueda descodificar datos sin estar autorizado. Estos dos datos KINI y P se pueden actualizar, además, en diferentes instantes de tiempo (por ejemplo, el valor KINI se puede reemplazar varias veces durante cada emisión a través del canal de transmisión A o B, y el contenido de la memoria FPGA 7 por medio de la adquisición de una nueva tarjeta de chip 12).

Con ello se abre también la posibilidad de usar el valor de inicialización KINI o el contenido de la memoria P como vale de autorización para permitir el acceso a determinadas emisoras, a determinadas emisiones o a determinados datos. Estos vales de autorización se pueden comercializar, por ejemplo, a través de diferentes canales; sin embargo, una descodificación es posible sólo cuando el usuario también conoce el otro valor adecuado (KINI o bien P), que se reemplaza automáticamente, por ejemplo, en todos los abonados.

El generador de claves 6 y/o la memoria 7 FPGA se pueden encontrar en una tarjeta de chip 12 intercambiable, por ejemplo en una tarjeta de chip en formato ISO. El especialista entenderá que también se pueden integrar otros componentes del receptor 5 en la tarjeta de chip 12, entre otros también el módulo de descodificación 4. La tarjeta de chip se comunica con el receptor 5 por medio de una interfaz API preferentemente estandarizado. La tarjeta de chip 12 es preferentemente una JavaCard (marca de Sun Corporation), que puede ejecutar Java-Applets (marca de Sun Corporation).

Con ello se abre la posibilidad de adaptar el generador de claves 6 de un modo muy sencillo a otro emisor 1 o a una emisión determinada, reemplazando para ello la tarjeta de chip 12.

También se pueden depositar varios juegos de contenidos de la memoria FPGA en el descodificador 5, en el que se selecciona automáticamente el juego adecuado cuando el usuario selecciona otro canal de emisión o una emisión determinada. Los contenidos de la memoria FPGA se pueden usar en este caso como módulos plug-in, permitiendo cada módulo plug-in el acceso a datos determinados.

La tarjeta de chip 12 comprende además preferentemente una región de memoria 120 con una identificación del usuario, por ejemplo una IMSI (International Mobile Subscriber Identity), que también puede ser usada por la segunda parte de recepción 9 para identificar al usuario del receptor 5 en la red de comunicaciones móviles 10. Esta identificación también se puede usar por parte de un centro de cálculo 11 que puede ser accedido a través de la segunda red de comunicaciones 10, para facturar al usuario la reproducción de los datos o la carga remota del vale de autorización. El importe facturado se puede facturar, por ejemplo, de modo mensual con la factura de teléfono, cuando el centro de facturación sea administrado por el operador de la red de comunicaciones 10, o por medio de mecanismos conocidos a una cuenta prepagada en la tarjeta de chip 12.

El importe facturado puede ser dependiente, por ejemplo, de la duración de la reproducción de datos y/o de los datos reproducidos. Los importes dependientes de los datos se pueden indicar, por ejemplo, como datos que acompañan al programa en un programa DAB ó DVB. La duración de reproducción se puede determinar, por

ejemplo, por un módulo temporal 13 en el receptor 5. En una variante preferida, el módulo temporal se integra en la tarjeta de chip 12, tal y como se describe en la solicitud de patente WO-A1-99/25111.

A continuación se describe la invención a partir de la Figura 4. Las características iguales o correspondientes se designaron los mismos símbolos de referencia en todas las figuras, y sólo se describen de nuevo cuando sea necesario.

El descodificador 5 conforme a la invención comprende un módulo de descodificación 4, que comprende una conexión FPGA, o que está hecho a partir de una conexión FPGA. La arquitectura del módulo de descodificación 4, es decir, la conexión de los componentes lógicos en la conexión FPGA, se define por medio de una memoria FPGA 7 que se puede sobreescribir, por ejemplo una RAM, una ROM o una EEPROM en un módulo que se puede reemplazar, por ejemplo en una tarjeta de chip 12 que se puede extraer.

El módulo de descodificación 4 usa una clave de descodificación K determinada por el generador de claves 6, para convertir datos codificados x en datos descodificados y, que pueden ser reproducidos por los medios de reproducción 8. El generador de claves 6 determina la clave de descodificación K tomando como base un valor KINI transmitido por el emisor 1, como se explica posteriormente. Como en la primera variante, el generador de claves 6, por ejemplo, puede estar formado por un generador aleatorio o por un descodificador, que puede desencriptar los datos encriptadas emitidos por el emisor 1, para reconstruir la clave del descodificador. En el caso más sencillo, la clave de descodificación K o el valor de inicialización KINI está fijado en el módulo de descodificación 4 y no se puede transmitir de modo separado. En otra variante, la clave de descodificación está formada por una región de memoria sencilla en la que se copia la clave.

Esta variante permite programar todo el módulo de descodificación 4 haciendo que la memoria del FPGA 7 registre nuevos datos. Gracias a ello, el descodificación 5 se puede adaptar muy rápidamente y sin mucho coste a diferentes emisores o emisiones.

Además, con esta variante se pueden fabricar módulos de descodificación 4 reprogramables muy complejos, que se pueden volver a programar completamente, y que pueden procesar, por ejemplo, varios bits en paralelo, por ejemplo palabras de 512 bits o más. De este modo, los datos proporcionados por la parte de recepción 2 se pueden mecanizar en tiempo real, sin ser almacenados previamente en la memoria de buffer 3. Con ello, es posible prescindir totalmente a la memoria de buffer 3, o reducir fuertemente su tamaño.

Además, se pueden llevar a cabo modificaciones muy complejas de la estructura del módulo de descodificación 4, con las que se pueden programar diferentes módulos de descodificación 4 completamente diferentes desde el punto de vista estructural. Con la misma conexión FPGA se pueden programar, por ejemplo, módulos de descodificación que mueven líneas completas, u otros módulos de descodificación que descodifican o desplazan bits o bytes individuales.

El módulo de descodificación 4, el generador de claves 6 y/o la memoria FPGA 7 se pueden encontrar en una tarjeta de chip 12 reemplazable, por ejemplo en una tarjeta de chip en formato ISO. El especialista entenderá que también se pueden integrar otros componentes del receptor 5 en la tarjeta de chip 12. La tarjeta de chip se comunica con el receptor 5 por medio de un interfaz API preferentemente estandarizado. La tarjeta de chip es preferentemente una JavaCard (marca de Sun Corporation), que puede ejecutar Java-Applets (marca de Sun Corporation).

Como en la primera variante, el contenido de la FPGA y el valor de inicialización KINI pueden ser modificados independientemente entre sí y a través de diferentes canales de transmisión por parte del emisor 1. También es posible actualizar automáticamente de modo periódico un valor (por ejemplo el valor de inicialización KINI) mientras que el otro valor, por ejemplo el contenido de la FPGA, se ha de adquirir como vale de autorización en tarjetas de chip o en applets, para poder acceder a datos determinados o a emisoras determinadas.

En las dos variantes se pueden usar, además, vales de autorización P y/o KINI dependientes del tiempo, que, por ejemplo, sólo son válidos durante una determinada duración, o sólo a determinadas horas del día o días de la semana. Esta invención permite además conceder diferentes calidades de autorizaciones. Por ejemplo, se pueden comprar “buenos” contenidos de FPGA, que hacen posible una descodificación óptima y una buena reproducción de los datos, y por un precio inferior “peores” contenidos de FPGA, que no programan de modo óptimo el módulo de descodificación, de manera que la calidad, por ejemplo, sólo es suficiente para pequeños anuncios o sólo para el archivo o indexación de los datos.

También es posible distribuir vales de autorización que sólo permiten la descodificación de determinadas partes de la imagen, por ejemplo sólo la descodificación de determinadas ventanas en un sistema con una superficie de usuario gráfica (GUI), o sólo la descodificación de los datos transmitidos durante el intervalo de barrido de líneas de un programa de televisión.

## REIVINDICACIONES

1. Descodificador (5) con un módulo de descodificación (4), para descodificar datos de imagen codificados digitales de un emisor de broadcast (1) que son recibidos con una primera parte de recepción (2), en el que el módulo de descodificación (4) usa una clave de descodificación (K) para convertir datos codificados en datos descodificados,

en el que el módulo de descodificación (4) mencionado contiene una conexión FPGA programable con un gran número de bloques lógicos, cuya conexión se puede modificar por medio de la modificación de una memoria FPGA (7), dependiendo la descodificación de los datos de imagen mencionados de la programación de esta conexión FPGA, y en el que la memoria FPGA (7) se encuentra en una tarjeta de chip (12), caracterizado porque el módulo de descodificación (4) se encuentra en la tarjeta de chip (12), y el descodificador (5) comprende una segunda parte de recepción (9) para una red de comunicaciones móviles (10), de manera que la memoria FPGA (7) mencionada se puede actualizar a través de la red de comunicaciones móviles (10).

2. Descodificador (5) según una de las reivindicaciones anteriores, caracterizado porque el módulo de descodificación (4) mencionado usa una clave de descodificación (K) que se determina con una conexión FPGA (6) programable.

3. Descodificador (5) según la reivindicación anterior, caracterizado porque la clave de descodificación (K) mencionada se determinada con un generador aleatorio (6) realizado con una conexión FPGA programable.

4. Descodificador (5) según la reivindicación anterior, caracterizado porque el generador aleatorio (6) usa un valor de inicialización (KINI) que está almacenado en la tarjeta de chip (12).

5. Descodificador (5) según una de las reivindicaciones 3 ó 4, caracterizado porque el generador aleatorio (6) mencionado usa un valor de inicialización (KINI) que se transmite a través una red de comunicaciones móviles (10) al descodificador (5) mencionado.

6. Descodificador (5) según una de las reivindicaciones 3 ó 4, caracterizado porque el generador aleatorio (4) mencionado usa un valor de inicialización (KINI) que se transmite de modo encriptado a través de un canal de broadcast y se desencripta en la tarjeta de chip (12) en el descodificador mencionado.

7. Descodificador (5) según la reivindicación anterior, caracterizado porque la tarjeta de chip (12) mencionada comprende una conexión FPGA (6) para el desencriptado del valor de inicialización (KINI) mencionado.

8. Descodificador (5) según la reivindicación 2, caracterizado porque la clave de descodificación (K) mencionada se almacena en la tarjeta de chip (12).

9. Descodificador (5) según la reivindicación 2, caracterizado porque la clave de descodificación (K) mencionada se transmite a través de la red de comunicaciones móviles (10) al descodificador mencionado.

10. Descodificador (5) según la reivindicación 2, caracterizado porque la clave de descodificación (K) mencionada se transmite encriptada a través de un canal de broadcast, y se desencripta en la tarjeta de chip (12) en el descodificador (5) mencionado.

11. Descodificador (5) según la reivindicación anterior, caracterizado porque la tarjeta de chip (12) mencionada comprende una conexión FPGA para el desencriptado de la clave de descodificación (K) mencionada.

12. Descodificador (5) según una de las reivindicaciones anteriores, caracterizado porque comprende un receptor DAB o DVB (2), para recibir los datos mencionados de imágenes animadas.

13. Descodificador (5) según una de las reivindicaciones 1 a 11, caracterizado porque comprende un receptor de PLC (2) para recibir los datos mencionados de imágenes animadas.

14. Descodificador (5) según una de las reivindicaciones 1 a 11, caracterizado porque comprende un receptor ADSL (2) para recibir los datos mencionados de imágenes animadas.

15. Descodificador (5) según una de las reivindicaciones 1 a 11, caracterizado porque comprende un receptor UMTS (2) para recibir los datos mencionados de imágenes animadas.

16. Descodificador (5) según una de las reivindicaciones 1 a 15, caracterizado porque comprende un módulo de identificación (12), en el que está depositada la identidad (120) del usuario para identificar el usuario en la red de comunicaciones móviles (10).

17. Procedimiento para descodificar datos de imágenes animadas codificados de un emisor de broadcast (1) con un

descodificador (5) que comprende una primera parte de recepción (2) para el emisor de broadcast (1) y un módulo de descodificación (4), en el que el módulo de descodificación (4) usa una clave de descodificación (K) para convertir datos codificados en datos descodificados, con los siguientes pasos:

- los datos de imagen mencionados se desencriptan a partir del módulo de descodificación (4), que se realiza como una conexión FPGA con una pluralidad de bloques lógicos, cuya conexión se puede modificar por medio de la variación de una memoria FPGA (7) que se encuentra en una tarjeta de chip (12),

- descodificación de los datos de imagen mencionados a partir de la conexión FPGA mencionada

caracterizado porque el módulo de descodificación (4) mencionado se encuentra en la tarjeta de chip (12), y el descodificador (5) comprende una segunda parte de recepción (9) para una red de comunicaciones móviles (10), y la memoria FPGA (7) mencionada se actualiza a través de la red de comunicaciones móviles (10).

18. Procedimiento según la reivindicación 17, caracterizado porque los datos de imagen mencionados se desencriptan a partir de una clave de descodificación (K) que se determina con un circuito FPGA programable (6).

19. Procedimiento según la reivindicación anterior, caracterizado porque la clave de descodificación (K) mencionada se determina con un generador aleatorio (6) fabricado por medio de una conexión FPGA programable.

20. Procedimiento según la reivindicación anterior, caracterizado porque el generador aleatorio (6) mencionado usa un valor de inicialización (KINI) que se vende por tarjeta de chip (12).

21. Procedimiento según una de las reivindicaciones 18 ó 20, caracterizado porque el generador aleatorio (6) mencionado usa un valor de inicialización (KINI) que se transmite a través de la red de comunicaciones móviles (10) al descodificador (5) mencionado.

22. Procedimiento según una de las reivindicaciones 18 ó 20, caracterizado porque el generador aleatorio (4) mencionado usa un valor de inicialización (KINI) que se transmite encriptado a través de un canal de broadcast, y se encripta en la tarjeta de chip (12) en el descodificador (5) mencionado.

23. Procedimiento según la reivindicación 20, caracterizado porque la clave de descodificación (K) mencionada se transmite a través de la red de comunicaciones móviles (10) al descodificador (5) mencionado.

24. Procedimiento según la reivindicación 18, caracterizado porque la clave de descodificación (K) mencionada se transmite a través de un canal de broadcast, y se desencripta en la tarjeta de chip (12) en el descodificador (5) mencionado.

25. Procedimiento según una de las reivindicaciones 17 a 24, caracterizado porque los datos de imagen mencionados se transmiten a través de un canal de transmisión DAB o DVB.

26. Procedimiento según una de las reivindicaciones 17 a 24, caracterizado porque los datos de imagen mencionados se transmiten a través de un canal de transmisión PLC.

27. Procedimiento según una de las reivindicaciones 17 a 24, caracterizado porque los datos de imagen mencionados se transmiten a través de un canal de transmisión ADSL.

28. Procedimiento según una de las reivindicaciones 17 a 24, caracterizado porque los datos de imagen mencionados se transmiten a través de un canal de transmisión UMTS.

29. Procedimiento según una de las reivindicaciones 17 a 28, caracterizado porque la identidad del usuario (120) en la red de comunicaciones móviles (10) se determina a partir de un módulo de identificación (12).

30. Procedimiento según una de las reivindicaciones 17 a 29, caracterizado porque el algoritmo de descodificación, que es usado por un emisor de broadcast (1) determinado se modifica varias veces, y porque la conexión FPGA mencionada (4; 6) se programa de nuevo varias veces de modo correspondiente.

31. Procedimiento según una de las reivindicaciones anteriores, caracterizado porque el emisor de broadcast (1) mencionado modifica la capacidad de reconocimiento de diferentes emisiones por medio de la adaptación del algoritmo de codificación mencionado.

32. Tarjeta de chip (12) para su uso en un descodificador (5) según una de las reivindicaciones 1 a 16, para descodificar datos de imagen codificados digitales de un emisor de broadcast (1), caracterizada porque comprende un módulo de descodificación (4) que contiene una conexión FPGA programable con una pluralidad de bloques lógicos, cuya conexión se puede modificar por medio de la variación de una memoria FPGA (7) que se encuentra en la tarjeta de chip (12), usándose la conexión FPGA mencionada para la adaptación de un algoritmo para la

descodificación de datos de imagen, y pudiéndose actualizar la memoria FPGA (7) mencionada a través de una red de comunicaciones móviles (10).

33. Tarjeta de chip (12) según la reivindicación 32, caracterizada porque la conexión FPGA mencionada es un generador aleatorio (6).

34. Tarjeta de chip (12) según la reivindicación 32, caracterizada porque la conexión FPGA mencionada permite la determinación de un valor de inicialización (KINI) para un generador aleatorio (6).

35. Tarjeta de chip (12) según una de las reivindicaciones 32 a 34, caracterizada porque contiene además datos de identificación de usuario (120), para modificar el usuario en la red de comunicaciones móviles (10).

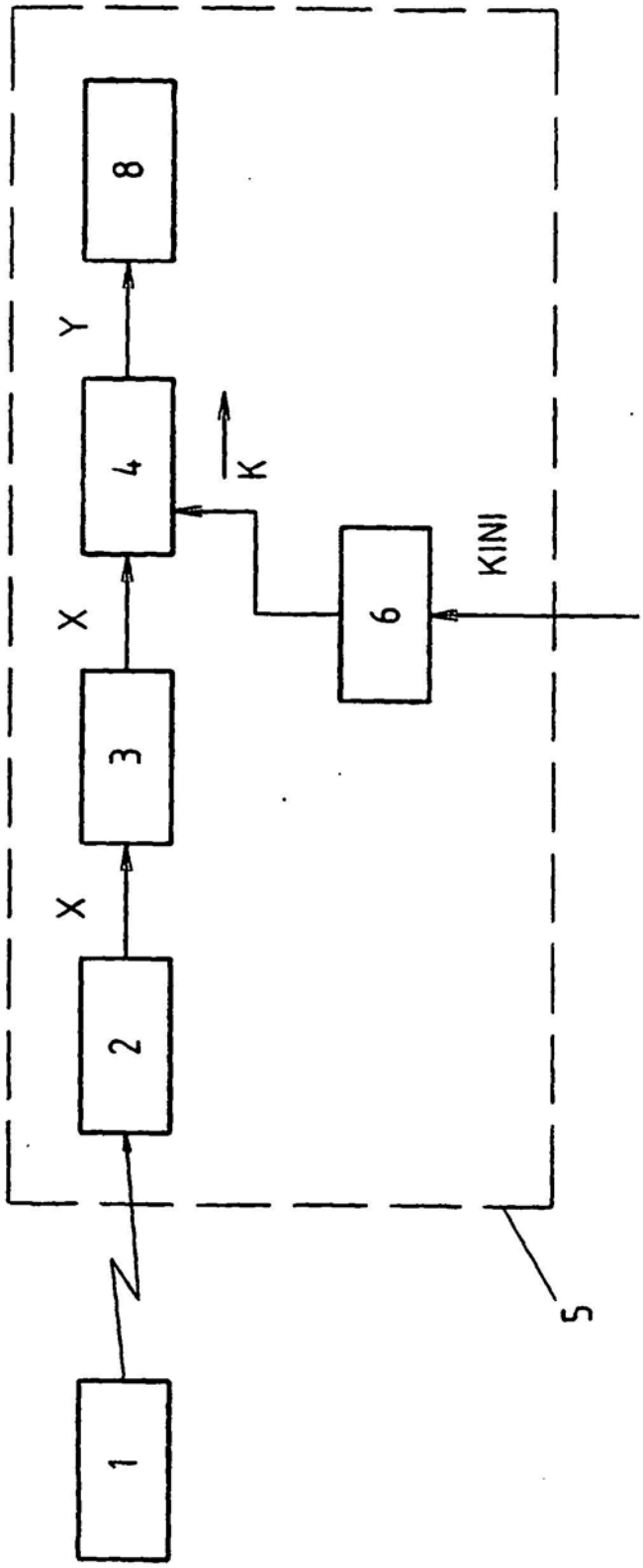


Fig. 1

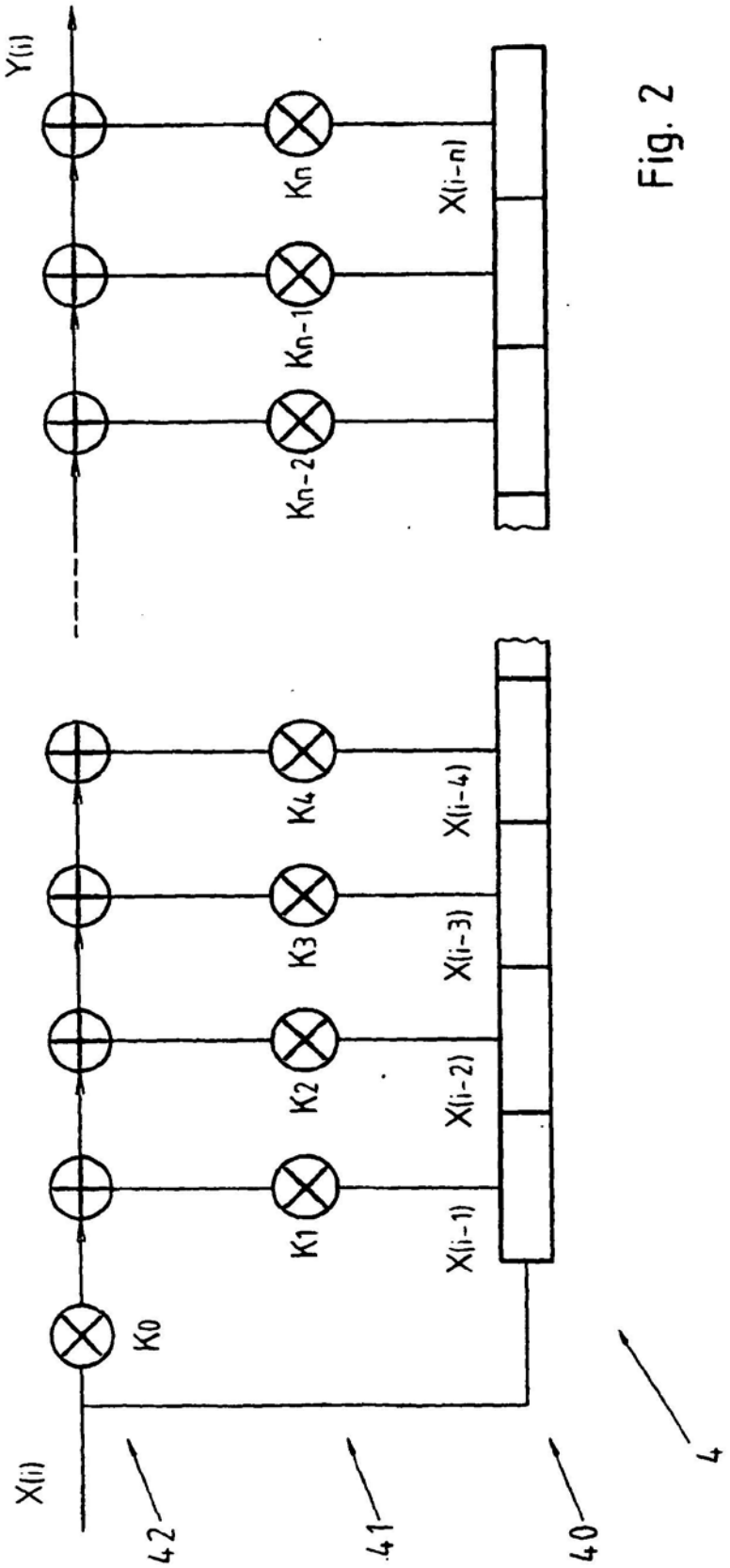


Fig. 2

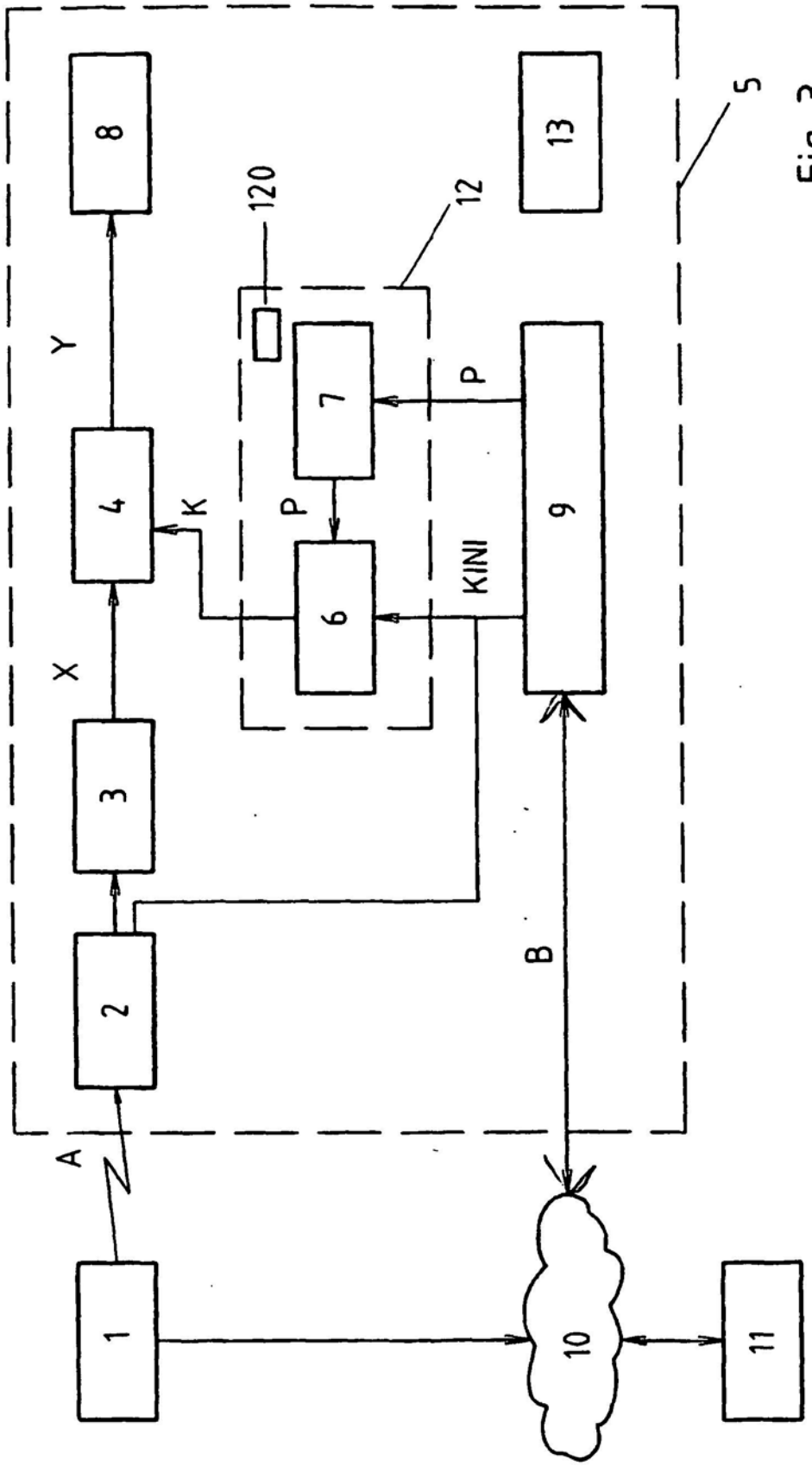


Fig. 3

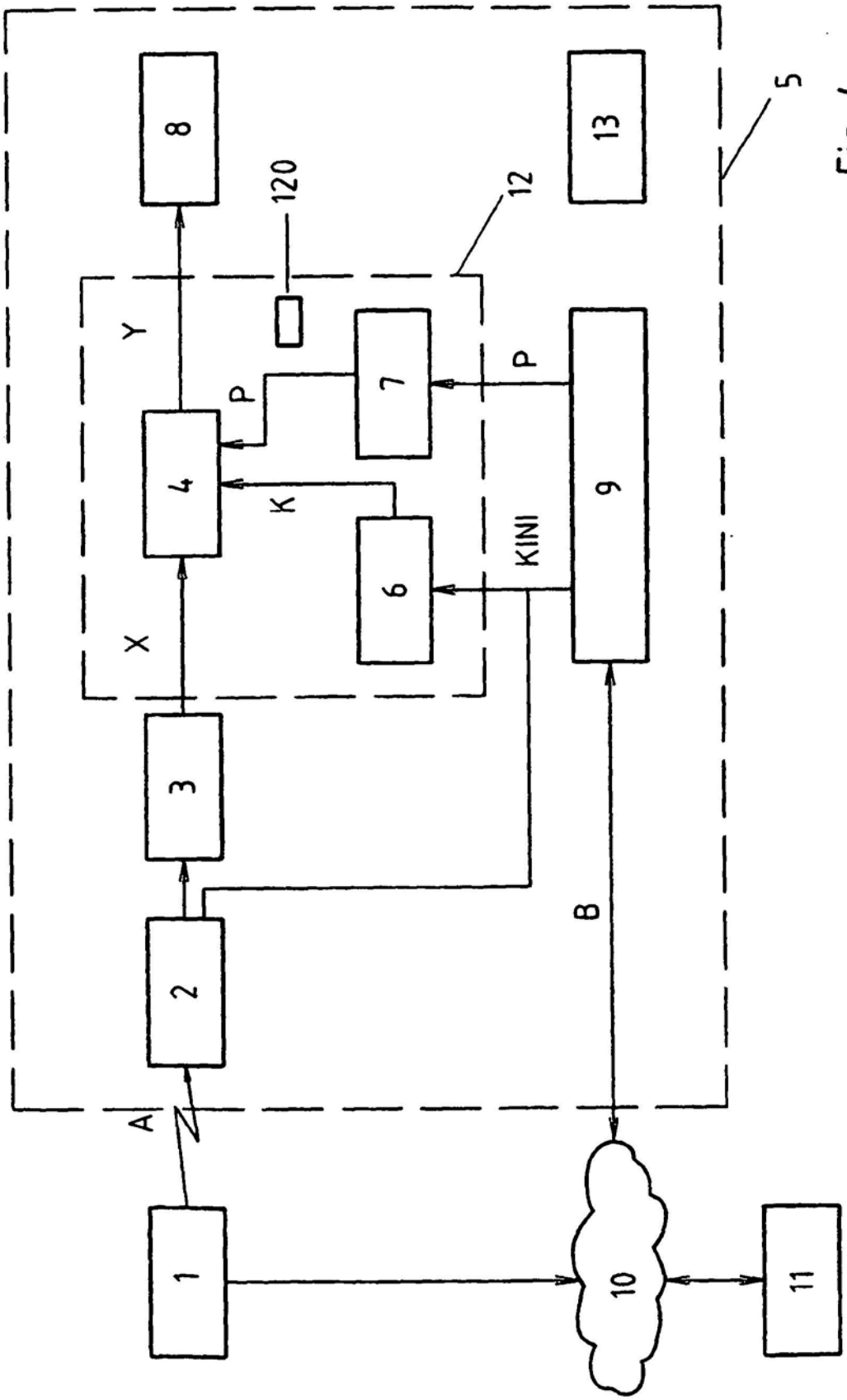


Fig. 4