(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 733 018**

(51) Int. CI.:

H04L 9/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **19.12.2002 PCT/IB2002/05520**

(87) Fecha y número de publicación internacional: **03.07.2003 WO03055131**

(96) Fecha de presentación y número de la solicitud europea: **19.12.2002 E 02788390 (9)**

(97) Fecha y número de publicación de la concesión europea: **10.04.2019 EP 1459474**

(54) Título: **Método anti-pirateo para la distribución de contenido digital**

(30) Prioridad:

20.12.2001 FR 0116585

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
27.11.2019

(73) Titular/es:

GEMALTO SA (100.0%)
6, rue de la Verrerie
92190 Meudon, FR

(72) Inventor/es:

PATARIN, JACQUES y
COURTOIS, NICOLAS

(74) Agente/Representante:

ELZABURU, S.L.P

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

Método anti-pirateo para la distribución de contenido digital

Numerosos canales de televisión de pago actualmente son víctimas de fraude. En particular, las tarjetas piratas se utilizan con frecuencia para ver sus canales. Esta invención propone un nuevo sistema para la transmisión de claves de descifrado de imágenes (o de la imagen en sí) que ofrece numerosas ventajas: el sistema es relativamente sencillo de implementar y puede reaccionar rápidamente si aparecieran tarjetas piratas (flexibilidad).

Si se obtiene una tarjeta pirata, es posible averiguar desde el exterior (es decir, solo observando su funcionamiento) los secretos que guarda, que posiblemente se pueden usar para averiguar de qué tarjeta real obtuvo estos secretos, pero especialmente para desactivar todas las tarjetas piratas sin desactivar las tarjetas legítimas. Esto se conoce como rastreo de traidores y, en particular, rastreo de caja negra (traidor).

El documento de MAYER A ET AL: "Generalized secret sharing and group-key distribution using short keys", COMPRESSION AND COMPLEXITY OF SEQUENCES, 1997, PROCEEDINGS, SALERNO, ITALIA, IEEE COMPUT. SOC, Estados Unidos, 11 de junio de 1997 (11-06-1997), páginas 30-44, XP010274905, ISBN: 0-8186-8132-2, describe un esquema para hacer que una clave de cifrado de grupo esté disponible para varios receptores pertenecientes a un grupo, en donde la clave se define como una función de la información común a todos los receptores y de información diferente para cada receptor y para cada valor de la información común. Obsérvese que la invención propuesta es extremadamente eficiente y segura en comparación con los otros sistemas propuestos en la bibliografía criptográfica. Obsérvese también que esta invención no se limita a la televisión: el método también se puede utilizar siempre que el mismo contenido se deba transmitir a varios receptores autorizados.

El nuevo método se caracteriza por tasas muy razonables que son compatibles con las limitaciones de velocidad impuestas por los canales de comunicación. Además, se destaca de otros métodos debido a la muy corta longitud de los datos K que se transmiten en tiempo real para acceder al contenido protegido: esta longitud puede ser tan corta como solo de 64 bits.

La invención se define por las reivindicaciones adjuntas.

Otros detalles y ventajas de esta invención aparecerán durante la siguiente descripción de un método de ejecución preferido pero no limitante, y en referencia a los dibujos adjuntos en los que:

La figura 1 representa un receptor como un objeto portátil de tipo tarjeta inteligente; y

La figura 2 representa un dispositivo transmisor asociado.

1 Ejemplo de sistema

1.1 Descripción

Consideraremos un sistema para la distribución de la misma información a numerosos receptores válidos. Por ejemplo, un sistema de televisión de pago. K_c representa la clave de descifrado de la información. Esta clave tiene, por ejemplo, una vida útil de 10 minutos y puede requerir entre 64 y 128 bits. Describiremos un método que permite a los receptores recalcular el nuevo valor de K_c cada 10 minutos Obsérvese que aquí, todos los receptores calcularán el mismo valor de K_c, aunque todos ellos tendrán diferentes secretos.

Consideraremos un receptor y lo llamaremos "receptor del índice i". Este receptor tiene, aquí, al menos dos valores específicos para él: una clave de cifrado K_i, y un valor secreto SA_i.

La organización responsable de la transmisión generará una clave secreta K, a continuación calculará, para cada índice i, el siguiente valor:

$$b_i = K_c \oplus E_K(SA_i),$$

donde E designa una función de cifrado, o más generalmente una función unidireccional, usando una clave K, y donde $\oplus$ designa una ley de grupo (por ejemplo XOR bit a bit, o módulo de adición de 256), y transmitirá todos estos valores b_i, cifrados respectivamente con una clave K_i. Por ejemplo, transmitirá regularmente todos los valores b_i varios días con antelación.

En consecuencia, un receptor que estará en modo de recepción podrá, con varios días de antelación, descifrar el valor b_i (usando su clave K_i).

Entonces, solo unos segundos antes de que la clave K_c se vuelva útil, el transmisor enviará la clave secreta K a todos los receptores. Esta clave puede ser muy corta, por ejemplo 64 bits. Ahora podrán calcular K_c calculando $y = E_K(SA_i)$, entonces $K_c = b_i \oplus y^{-1}$ (si la operación de grupo es XOR bit a bit, entonces $y^{-1} = y$).

Obsérvese que el factor "tiempo" desempeña un papel muy importante aquí: antes de transmitir K, ninguno de los receptores puede calcular el valor de K_c, y todos ellos tienen en la memoria diferentes valores b_i y SA_i. A continuación, tan pronto como se haya transmitido K, utilizando este único valor K y sus diferentes valores SA_i y B_i, podrán todos recalcular el mismo valor K_c.

Recuerde que una función unidireccional es aquella que se puede calcular en una dirección sin información particular, pero que no se puede calcular en la dirección inversa, excepto posiblemente si se conocen ciertos parámetros. Es en particular una función de troceo como MD5 o SHA.

1.2 "Rastreo de traidores de caja negra", o cómo reaccionar si aparecieran tarjetas piratas

Si aparecieran tarjetas piratas, es posible reaccionar: en primer lugar, detectando los secretos que se guardan en la tarjeta (véase a continuación), y en segundo lugar desactivando todas las tarjetas que tengan (estos) mismo secreto o secretos (véase a continuación). Esto se puede hacer sin cambiar las otras tarjetas en circulación, que continuarán funcionando.

1.3 Detección de secreto o secretos

En primer lugar, supongamos que los secretos de un único receptor verdadero se guardan en una tarjeta pirata. Las tarjetas válidas se dividirán en dos grupos con aproximadamente el mismo número de elementos: A y B. Los valores reales b_i para A y valores falsos b_i para B, a continuación, se transmiten a la tarjeta pirata para averiguar si aún pueden descifrar las imágenes correctamente. Si es así, su secreto pertenece a A, de lo contrario, pertenece a B. A continuación empezar de nuevo con dos nuevos subgrupos. Si hay aproximadamente 2^n posibles índices i, tomará aproximadamente n intentos encontrar el índice en cuestión.

Obsérvese que no es necesario leer los secretos que se encuentran en la tarjeta: es suficiente observar su funcionamiento. Si varios secretos están presentes en la misma tarjeta, el método indicado se puede usar para detectar un 1er secreto. La transmisión de valores b_i correspondiente a este secreto se detiene entonces, y se detecta un 2º secreto, etc. También es posible que la tarjeta pirata pueda contener los secretos de varios receptores verdaderos, utilizando los secretos de una manera compleja: la detección a continuación se vuelve más difícil, pero aún en general es posible siempre que no haya demasiados secretos mantenidos en la tarjeta pirata.

1.3.1 Desactivar tarjetas con este (estos) secreto o secretos

Simplemente dejar de transmitir los valores b_i que corresponden a estos secretos.

2 Configuración básica general

Se proporcionará un amplio compendio del principio básico en el centro de la invención, y las mejoras más generales, variantes y versiones derivadas de la misma se describirán en los siguientes capítulos. Sea G un grupo de receptores legítimos. El objetivo es transmitirles (y solo a ellos) un contenido K_c, que consiste en todos los tipos de información (datos, programa, clave criptográfica, etc.), especialmente un contenido digital. El contenido K_c en particular, puede ser una clave para acceder a un programa de televisión de pago. El contenido K_c es idéntico para todos los receptores y, por lo general, cambiará muy rápidamente para evitar una redistribución fraudulenta.

El principio básico de la invención es transmitir K_c a todos los receptores legítimos a través de otra clave K enviada en texto claro, de modo que cada receptor tenga un medio para calcular K_c utilizando K, que es completamente diferente de la utilizada por los otros receptores.

En general, este medio será un valor b_i, transmitido con mucha antelación, que se halla en su memoria. Justo antes de que K_c deba estar disponible para los receptores, se transmite un valor único K a todos los receptores del grupo G, de modo que cada receptor pueda calcular K_c usando una función f que tiene y que toma como entrada K, b_i, y un valor SA_i específico para ello. Para cada índice i en el grupo de receptores, por lo tanto tenemos:

$$K_c = f(K, b_i, SA_i).$$

El momento en que K debe transmitirse a los receptores deberá determinarse según las circunstancias, para garantizar que un defraudador no pueda recalcular K_c o al menos usarlo de manera fraudulenta, en el tiempo entre la transmisión de K y el momento en que K_c está disponible. Generalmente, K se transmitirá unos segundos o unos minutos antes de K_c esté disponible.

2.1 Variantes de la configuración básica

Variante 1

Para determinadas aplicaciones, los valores SA_i no tienen que ser secretos: pueden ser públicos.

Variante 2

Para determinadas aplicaciones, cuando los valores SA_i son secretos, los valores b_i se pueden transmitir en texto claro a los receptores.

Variante 3

La función E, en lugar de ser una función de cifrado, puede ser, en general, una función unidireccional que utiliza una clave K, por ejemplo, una función de troceo criptográfico como SHA-1.

Variante 4 - almacenamiento previo de valores b_i

En lugar de transmitir los valores b_i, pueden precalcularse y almacenarse previamente en el receptor, por ejemplo, en la memoria flash, en el disco duro, CD-ROM o DVD. También se pueden transmitir localmente, por ejemplo, a través del cable del edificio o de las microondas.

3 Configuración generalizada.

La configuración anterior con estas variantes se puede duplicar o replicar, lo que ofrece mejoras considerables en términos de rendimiento y detección de bandas de defraudadores. Primero describiremos una versión duplicada y a continuación explicaremos el principio general que permite que el sistema se use varias veces en paralelo, y todos los beneficios resultantes.

3.1 2º ejemplo de sistema

En este caso, cada receptor tiene, en lugar del valor SA_i que era específico para ello, dos valores SA_i y SA_j, para que varios receptores puedan tener el mismo SA_i o el mismo SA_j, pero no el mismo SA_i y el mismo SA_j simultáneamente. Por lo tanto, cada receptor se caracteriza por un par de índices (i, j) específicos para él.

Además, cada receptor puede tener dos claves de cifrado K_i y K_j, de modo que varios receptores puedan tener la misma K_i o la misma K_j, pero no la misma K_i y la misma K_j simultáneamente. Las claves K_i se pueden utilizar para transmitir los valores b_i a los receptores de manera secreta (excepto en la variante donde los valores b_i son públicos).

La organización responsable de las transmisiones generará dos valores secretos K_{c1} y K_{c2}. A continuación se combinan para acceder a la clave principal K_c o para acceder directamente al contenido. Por ejemplo, podríamos tener:

$K_c = K_{c1} \# K_{c2}$, donde # es una ley de grupo.

A continuación genera una clave K y calcula todos los valores.

$$b_{1i} = K_{c1} \oplus E_K(SA_i)$$

y $B_{2j} = K_{c2} \oplus E_K(SA_j)$

donde E designa una función de cifrado o, más generalmente, una función unidireccional, utilizando la clave K y donde $\oplus$ designa una ley de grupo, y a continuación transmitirá todos estos valores b_{1i} cifrados con clave K_{1i} y todos los valores b_{2j} cifrados con K_j. Por ejemplo, transmitirá regularmente todos los valores b_{1i} y b_{2j} con varios días de antelación.

En consecuencia, un receptor que estará en modo de recepción podrá, con varios días de antelación, descifrar el valor b_{1i} (usando su clave K_i) y el valor b_{2j} (usando su clave K_j).

Entonces, solo unos segundos antes de que la clave K_c se vuelva útil, el transmisor enviará la clave secreta K a todos los receptores. Ahora podrán calcular K_c calculando $y = E_K(SA_i)$, $z = E_K(SA_j)$, entonces $K_{c1} = b_{1i} \oplus y^{-1}$, $K_{c2} = b_{2j} \oplus z^{-1}$, a continuación y finalmente $K_c = K_{c1} \# K_{c2}$.

La ventaja de esta 2ª versión es que se transmiten menos valores b_i que con la 1ª versión (ya que varios receptores tienen los mismos valores b_{1i} o b_{2j}). Típicamente, es posible transmitir solamente un número de b_{1i} y de b_{2j} aproximadamente igual a la raíz cuadrada del número de receptores.

3.2 La configuración generalizada replicada.

En lugar de duplicar la configuración básica, se puede replicar más generalmente. Cada valor b_i por lo tanto se compone de uno o más valores: (b_{1i}, b_{2j}, b_{3k}, ...) y cada receptor se caracteriza por una lista de índices (i, j, k, ..) y direcciones correspondientes (SA_i, SA_j, SA_k, ..). El receptor caracterizado por la lista (i, j, k, ..) utiliza los valores correspondientes (b_{1i}, b_{2j}, b_{3k}, ...) con (SA_i, SA_j, SA_k, ...) para descifrar los valores K_{ci} (K_{c1}, K_{c2}, K_{c3}, ...) que deben combinarse para calcular una clave para acceder al contenido K_c, o el contenido en sí.

Cada receptor se identificará mediante una lista de índices, preferiblemente únicos, de la forma (i), (i, j) o (i, j, k, ..) usados para identificarlos (o para identificar un pequeño grupo de receptores sospechosos). Igualmente, podríamos decir que el receptor se caracteriza por su grupo de claves o direcciones según dos interpretaciones posibles, que es su grupo (SA_i, SA_j, SA_k, ...). Por lo tanto, esta configuración se puede combinar con cualquier otra configuración de rastreo de traidores con clave secreta conocida, por ejemplo, la que se describe en el artículo *Tracing Traitors,* Crypto'94, de Benny Chor, Amos Fiat y Moni Naor. En este caso, el protocolo tradicional de rastreo de traidores debe especificar cómo distribuir secretos (SA_i, SA_j, SA_k, ...) a los receptores y cómo calcular la clave principal K_c de las claves K_{ci}. Esto debe llevarse a cabo, dependiendo de la configuración utilizada, de modo que para un cierto número C de receptores que comparten sus claves para construir un decodificador pirata, todavía es posible identificar uno o todos los piratas, o al menos desactivar todos los decodificadores piratas sin impedir que los receptores legítimos que no son piratas accedan al contenido. Según el método de la invención, como ya se explicó anteriormente, hay muchas maneras de averiguar las claves mantenidas en una tarjeta pirata, sin desmontar la tarjeta, simplemente observando su operación en una transmisión en la que solo algunos de los valores b_i son correctos. Esta propiedad de rastreo de caja negra se mantiene en las generalizaciones de la configuración básica y, por lo tanto, es posible dejar de transmitir el valor de b_i correspondiente a uno o más secretos SA_i que se conservan en la tarjeta pirata. Al mismo tiempo, puede tener que enviarse un nuevo valor de SA_i a los receptores legítimos (con antelación, y preferiblemente encriptado con una clave secreta).

3.3 Variantes de la configuración generalizada.

Todas las variantes descritas en el párrafo 2.1 para la configuración básica también pueden aplicarse a la configuración replicada descrita en la sección 3.

Además, hay otros grupos de variantes específicas para la configuración general duplicada o replicada:

Grupo de variantes 1: estas variantes consisten en utilizar otras formas de distribución de secretos (SA_i, SA_j, SA_k, ...) a los receptores.

Grupo de variantes 2: estas variantes consisten en utilizar otras formas de calcular la K_c principal de las claves K_{ci}.

Grupo de variantes 3: variantes donde la clave K utilizada para calcular los diversos valores (b_{1i}, b_{2j}, b_{3k}, ...) no es la misma para todos estos valores. Por ejemplo, se puede usar una clave para todos los valores b_{1i} y otra diferente para los valores b_{2j}.

Grupo de variantes 4: variantes donde la función f (K, b_i, SA_i) usada para los valores b_{1i}, b_{2j} no es la misma para todos estos valores. Por ejemplo, puede usarse una función para los valores b_{1i} usados para calcular K_{c1}, y usarse una función diferente para los valores b_{2j} para calcular K_{c2}.

Grupo de variantes 5: variantes donde la clave secreta K_i usada para transmitir los valores b_{1i} y los valores b_{2j} no es la misma para todos los receptores que usan el mismo i, o difiere para los valores b_{1i} y los valores b_{2i}.

Ahora se dará una breve descripción de la invención en su implementación utilizando dispositivos de procesamiento de información. Se trata de un método para hacer que la misma información (K_c) esté disponible para varios receptores que pertenecen a un grupo (G) de receptores, desde un transmisor que comprende medios de procesamiento de información y medios de almacenamiento de información, comprendiendo cada receptor medios de procesamiento de información y medios de almacenamiento de información, almacenando los medios de almacenamiento del receptor información (SAi) específica para ellos, caracterizado por que comprende los siguientes pasos:

- definir, en los medios de almacenamiento de información de cada receptor, una relación K_c = f (K, b_i, SA_i) donde (f) es una función dada, (K) es información común a todos los receptores, y (b_i) es información diferente para cada receptor y para cada valor de la información (K);

- posibilitar que los medios de procesamiento de cada receptor accedan a la información (b_i), antes de hacer (K_c) disponible; y

- transmitir la información (K) a todos los receptores utilizando los medios de procesamiento del transmisor, justo antes de hacer (K_c) disponible;

de modo que cada receptor pueda calcular la información (K_c) utilizando dicha relación, a través de sus medios de procesamiento.

La figura 1 muestra la estructura general de un receptor 1 de tipo tarjeta inteligente. Comprende medios de procesamiento de información o CPU 2, varios tipos de medios de almacenamiento de información 3, 4, 5 (RAM, EEPROM, ROM), medios de entrada/salida 6 que permiten que la tarjeta se comunique con un terminal lector de tarjetas, y un bus 7 que permite que estas diversas partes se comuniquen juntas. La tarjeta se comunica con un dispositivo transmisor remoto a través del terminal (no mostrado).

La Figura 2 muestra la estructura general de un dispositivo transmisor 10. Comprende medios de procesamiento de información o el procesador 11, medios de almacenamiento de información 12 que pueden ser de varios tipos (RAM,

EEPROM, ROM), medios tradicionales de entrada/salida 13 que permiten que el transmisor se comunique con el exterior, y un bus 14 que permite que estas diversas partes se comuniquen juntas. El transmisor también comprende los medios de transmisión 15 especialmente diseñados para comunicarse según la invención con todos los receptores con los que está asociado. Para un sistema de televisión de pago, estos medios de transmisión están diseñados para transmitir imágenes y al menos la información K mencionada anteriormente, especialmente a través del uso de ondas de radio.

REIVINDICACIONES

1. Método de operación de un grupo (G) de receptores y transmisores para hacer la misma información (K_c) disponible para varios receptores (1) que pertenecen al grupo (G) de receptores, comprendiendo cada receptor i en el grupo (G) una unidad central de procesamiento (2) y medios de almacenamiento de información (3, 4, 5), almacenando los medios de almacenamiento información (SA_i) específica para cada receptor i, respectivamente, caracterizado por que comprende los siguientes pasos:

- permitir a cada receptor acceder a la información (b_i) antes de hacer (K_c) disponible; y

- transmitir una clave secreta (K) a todos los receptores, justo antes de hacer (K_c) disponible;

- operar cada receptor para calcular K_c a partir de una relación predefinida $K_c = f(K, b_i, SA_i)$ donde (f) es una función dada, (K) es una clave secreta común a todos los receptores, y (b_i) es información diferente para cada receptor y para cada valor de la clave secreta (K).

2. Método según la reivindicación 1, caracterizado por que la función (f) es de manera que conociendo un (b_i) y un (SA_i), no se conoce ningún algoritmo que pueda utilizarse para obtener la información (K_c) en un tiempo realista y con probabilidad no despreciable, cuando no se conoce la clave secreta (K).

3. Método según la reivindicación 1, caracterizado por que la función f es de manera que, conociendo un cierto número de ($b_1..b_n$) para un cierto subgrupo (G') de receptores, no se conoce ningún algoritmo que pueda usarse, antes de conocer la K actual, en un tiempo realista y con una probabilidad no despreciable, para producir un par válido (b_i, SA_i) con una (SA_i) legítima, no siendo i uno de los receptores 1..n de (G').

4. Método según la reivindicación 1, caracterizado por que la función f tiene el formato:

$$f(K, b_i, SA_i) = b_i \oplus E_K(SA_i)$$

donde E_K es una función que depende de la clave secreta (K) y donde $\oplus$ designa una ley de grupo.

5. Método según la reivindicación 4, caracterizado por que la función (E_K) es un cifrado criptográfico.

6. Método según la reivindicación 1, caracterizado por que los valores (b_i) se envían cifrados con una clave (K_i) específica para cada receptor de un cierto grupo (G) de receptores.

7. Método según la reivindicación 1, caracterizado por que cada valor (SA_i) es un valor secreto conocido por el receptor del índice i.

8. Método según la reivindicación 1, caracterizado por que cada (b_i) consiste en dos valores b_{1i} y b_{2j} e igualmente la información específica de cada receptor consiste en dos valores SA_i y SA_j, de manera que cada receptor, identificado por el par de índices (i, j), combine los valores correspondientes b_{1i} y b_{2j} con los valores SA_i y SA_j para calcular los valores K_{c1} y K_{c2} utilizando dicha relación, que a su vez se combinan para acceder a la información K_c.

9. Método según la reivindicación 1, caracterizado por que la información K_c es una clave utilizada para descifrar un contenido digital como una imagen de televisión.

10. Método según la reivindicación 1, caracterizado por que la información K_c puede utilizarse durante varios minutos por los receptores, la información K se envía con varios segundos de antelación y los valores b_i se envían regularmente, empezando con varios días de antelación.

11. Método según la reivindicación 1, caracterizado por que ciertos receptores encuentran al menos algunos de sus valores b_i en una lista de valores almacenados previamente en los receptores.

12. Un grupo (G) de objetos receptores portátiles en el que cada objeto receptor portátil (1) del grupo (G) comprende medios de procesamiento de información (2) y medios de almacenamiento de información (3, 4, 5), almacenando los medios de almacenamiento información (SA_i) que es específica para el objeto receptor portátil y una función dada (f), caracterizado por que cada objeto receptor portátil (1) comprende:

- medios para obtener acceso a información (b_i) diferente para cada objeto receptor portátil del grupo (G) y para cada valor de una clave secreta (K) común a todos los objetos receptores portátiles del grupo (G),

- medios para recibir la clave secreta (K) en el objeto receptor portátil (1) de un transmisor justo antes de hacer que (Kc) esté disponible y

- medios para calcular información (K_c) usando una relación $K_c = f(K, b_i, SA_i)$.

13. Dispositivo transmisor (10) para hacer la misma información (K_c) disponible para varios receptores (1) que pertenecen a un grupo (G) de receptores, almacenando cada receptor información (SA_i) específica para ello, caracterizado por que comprende:

- medios de cálculo (11) diseñados para calcular información (b_i) usando una relación K_c= f(K, b_i, SA_i) donde (f) es una función dada, (K) es una clave secreta común a todos los receptores y la información (b_i) es información diferente para cada receptor y para cada valor de la clave secreta (K); y

- medios de transmisión (15) diseñados para transmitir a cada receptor, un cierto tiempo antes de hacer (K_c) disponible, la información (b_i) asociada con los mismos, y para transmitir la clave secreta (K) a todos los receptores, justo antes de hacer (K_c) disponible.

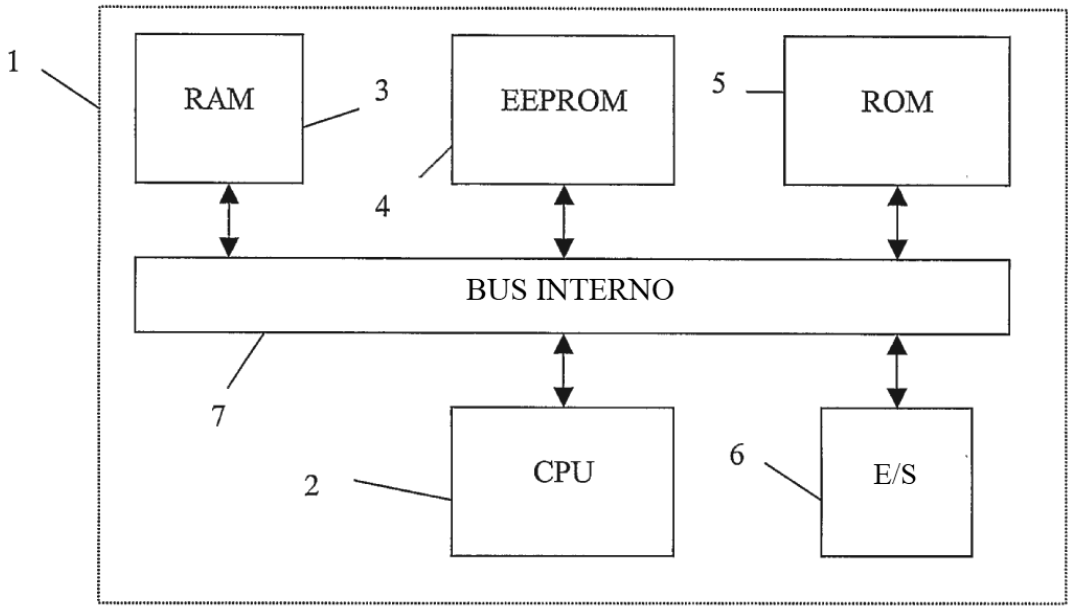
1
RAM
3
EEPROM
5
ROM
4
BUS INTERNO
7
CPU
2
6
E/S

FIG. 1

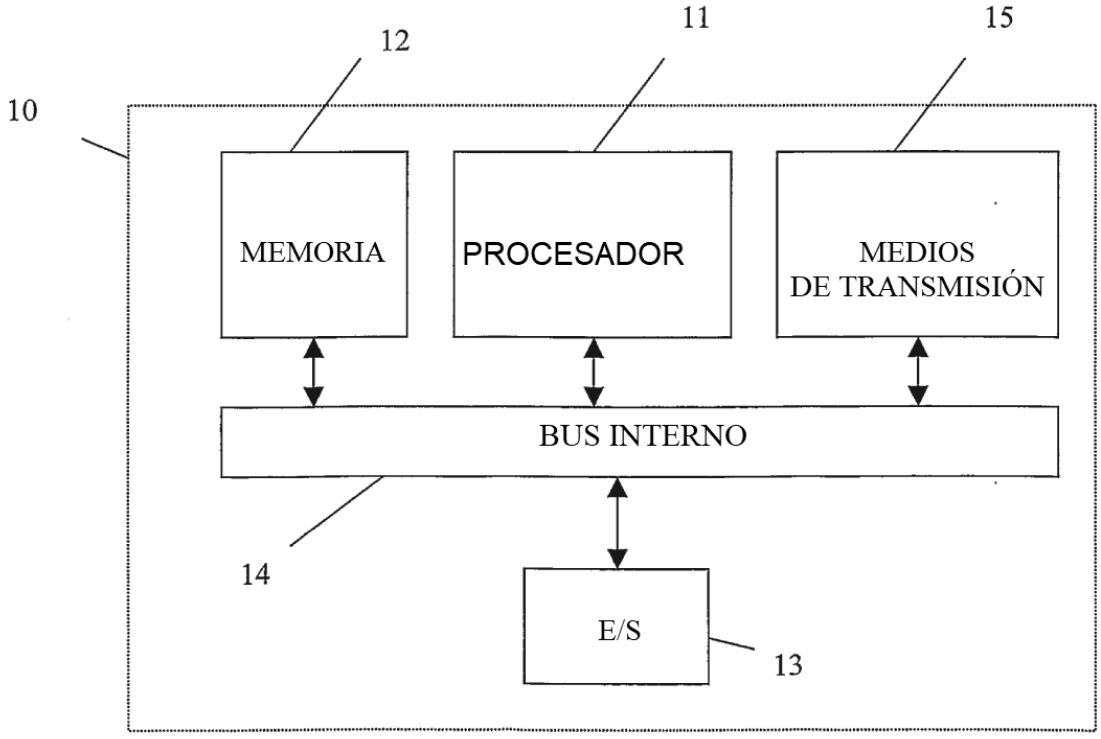
12
11
15
10
MEMORIA
PROCESADOR
MEDIOS
DE TRANSMISIÓN
BUS INTERNO
14
E/S
13

FIG. 2