(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 534 517**

(51) Int. CI.:

H04L 9/08 (2006.01)
H04N 21/258 (2011.01)
H04N 21/418 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **21.03.2011 E 11715718 (0)**

(97) Fecha y número de publicación de la concesión europea: **07.01.2015 EP 2550766**

(54) Título: **Procedimiento para identificar un dispositivo utilizado por un terminal pirata y dispositivo asociado**

(30) Prioridad:

23.03.2010 FR 1052108

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
23.04.2015

(73) Titular/es:

CRYPTOEXPERTS (100.0%)
41 Boulevard des Capucines
75002 Paris , FR

(72) Inventor/es:

DELERABLEE, CÉCILE;
GOUGET, ALINE y
PAILLIER, PASCAL

(74) Agente/Representante:

RUO, Alessandro

DESCRIPCIÓN

Procedimiento para identificar un dispositivo utilizado por un terminal pirata y dispositivo asociado

[0001] La invención se refiere a un procedimiento para prevenir la utilización de un dispositivo electrónico lícitamente adquirido e íntegro, por medio de un terminal pirata. De este modo, la invención permite luchar eficazmente contra la puesta a disposición fraudulenta de contenidos multimedia protegidos.

[0002] La invención se refiere, además, a la adaptación de dichos dispositivos así como a un procedimiento para activar respectivamente la revocación permanente de un dispositivo electrónico o la rehabilitación eventual de este último.

[0003] Un operador de difusión de contenidos digitales opera por lo general un sistema de acceso condicional (*Conditional Access System* - CAS por sus siglas en inglés) para poner un contenido protegido a disposición de un abonado o de una multitud de abonados. Dicho sistema se basa por lo general en dispositivos electrónicos seguros, como tarjetas inteligentes, para alojar las identidades y/o los derechos de los abonados y para realizar operaciones de cifrado, de descifrado o de generación de números.

[0004] Para difundir un contenido multimedia protegido, las palabras de control cifradas *c* y los contenidos codificados *C* se transmiten a través de una red de difusión, a intervalos regulares o, al menos, conocidos y controlados por el operador de difusión. Una palabra de control cifrada se obtiene por lo general por medio de una función de cifrado *E* tal que *c = E(k)*, siendo *k* el valor de dicha palabra de control. Un contenido codificado *C* se obtiene, por su parte, por medio de una función de codificación *enc* y de dicha palabra de control *k*, tal que *C = enc(k,M)*, siendo *M* el contenido multimedia en abierto. A título de ejemplo, la función de codificación puede ser conforme con el estándar DVB-CSA (*Digital Video Broadcasting - Common Scrambling Algorithm*, en inglés). Para poder visualizar o escuchar un contenido protegido, una persona debe abonarse. Un abonado recibe un dispositivo específico, por lo general en forma de una tarjeta inteligente, el cual acoplado a un terminal, por lo general denominado decodificador o “set-top box”, permite que dicho abonado decodifique un contenido protegido. Las palabras de control cifradas *c* se descifran tradicionalmente mediante el dispositivo de abonado el cual envía las palabras de control *k* al terminal. Este último se encarga de realizar la decodificación de un contenido codificado *C* y permite, por medio de una interfaz Hombre-Máquina adaptada -por ejemplo, un televisor doméstico-, acceder al contenido en abierto *M*.

[0005] Es habitual que entidades “piratas” intenten desarrollar un comercio ilícito que busca emitir, en una red pirata, contenidos en abierto *M* o palabras de control descifradas *k* que permiten decodificar un contenido *C* por medio de un terminal adaptado para ello. Las primeras amenazas y ataques han conducido a los piratas a intentar “romper” la seguridad de los dispositivos electrónicos de abonado. Mediante el conocimiento del material criptográfico, de los algoritmos o de secretos, un pirata puede entonces “clonar” o emular a dicho dispositivo y poner algunas de estas “reproducciones” a disposición de abonados deshonestos.

[0006] La robustez creciente y casi inviolable de dichos dispositivos han conducido a los piratas a adquirir lícitamente dispositivos de abonado (como tarjetas inteligentes) y a diseñar terminales piratas, adaptados para cooperar con dichos dispositivos y para emitir las palabras de control descifradas *k* e incluso los contenidos decodificados *M*, en tiempo real, en una red o canal pirata como por ejemplo la red de Internet. Esta amenaza se conoce bajo la denominación inglesa de “*card sharing*” o “*control word sharing*”.

[0007] Para hacer frente a los piratas, los operadores consiguen por lo general conocer la existencia de dicha red pirata. Suscribiendo un abono con un pirata, un operador puede incluso disponer de un dispositivo “clonado” o emulado y estudiarlo. Sin embargo, en el escenario “*control word sharing*”, no existen procedimientos conocidos que permitan identificar a distancia un dispositivo que, aunque legalmente adquirido e íntegro, se utiliza de manera fraudulenta. No existen más procedimientos para eventualmente revocar a distancia dicho dispositivo, sin que sea necesaria una modificación de la arquitectura material y de software de las redes de difusión y/o de parques de terminales lícitos y sin provocar un perjuicio especialmente molesto para los abonados legales en el acceso a los contenidos protegidos.

[0008] La invención permite responder al conjunto de los inconvenientes que plantean las soluciones conocidas. Entre las numerosas ventajas aportadas por la invención, podemos mencionar que la invención permite rastrear, a distancia, cualquier dispositivo de abonado que haya permitido producir una palabra de control cuyo valor se puede transmitir en una red pirata. La invención permite, además y como variante, rastrear cualquier dispositivo de abonado que haya producido una palabra de control que haya permitido decodificar un contenido protegido y cuyo contenido en abierto se emite en dicha red pirata. La invención permite, además, revocar a distancia dicho dispositivo, denominado “dispositivo indeseado”, continuando al mismo tiempo con la difusión de un contenido a través de la red de difusión. De este modo, la invención ofrece, a cualquier operador de difusión de contenidos, una herramienta especialmente simple y eficaz para luchar contra la piratería.

[0009] Con esta finalidad, se prevé un procedimiento para producir una palabra de control *k'*, implementándose dicho procedimiento mediante unos medios de tratamiento de un dispositivo electrónico que coopera con un terminal, constando dicho dispositivo de unos medios para recibir una palabra de control cifrada *c* desde el terminal y de unos medios para enviar dicha palabra de control *k'* producida a dicho terminal. Dicho procedimiento consta de una etapa para aplicar a la palabra de control cifrada *c* una función de descifrado *D* y calcular de este modo una palabra descifrada *k* tal que $k = D(c)$. De acuerdo con la invención, la palabra descifrada *k* consta de una componente *v* y el procedimiento consta, además, de una etapa para producir la palabra de control *k'* respectivamente idéntica o diferente de *k* de acuerdo con el resultado de una operación de comparación entre los valores de *v* y de un identificador *i* específico del dispositivo.

[0010] De acuerdo con una forma de realización ventajosa, la etapa para producir la palabra de control *k'* diferente de *k* puede consistir en producir una palabra $k' = kf$ cuyo valor *kf* es diferente del valor de *k*.

[0011] En una variante, la etapa para producir la palabra de control *k'* diferente de *k* puede consistir en implementar una función de retardo de tal modo que los medios para enviar envíen dicha palabra de control $k' = kd$ cuyo valor *kd* es igual a *k*, tras un intervalo de tiempo determinado.

[0012] De acuerdo con una forma de realización, la etapa para producir la palabra de control *k'* puede consistir en producir una palabra idéntica a *k* si el valor de la componente *v* es estrictamente inferior al valor del identificador *i* y diferente de *k* si el valor de la componente *v* es superior o igual al valor del identificador *i*. En una variante, la invención puede prever que:

- el identificador *i* es un vector de z enteros de valores $i = (i_1,...,i_z)$ comprendidos dentro de un conjunto $[1,m]$, siendo *m* y *z* unos enteros superiores a 1;
- la componente *v* es un vector de z enteros con unos valores $v = (v_1,...,v_z)$ comprendidos dentro de un conjunto $[0,m]$.

[0013] En este caso, la etapa para producir la palabra de control *k'* puede consistir en producir una palabra:

- idéntica a *k* si el valor de cada entero v_l es, respectivamente, estrictamente inferior al valor de cada entero i_l para cualquier *l* comprendido entre 1 y *z*;
- diferente de *k*, en caso contrario.

[0014] Para poder implementar dicho procedimiento, también se prevé un dispositivo electrónico que coopera con un terminal, constando dicho dispositivo de:

- unos medios para recibir una palabra de control cifrada *c* desde el terminal;
- unos medios de tratamiento para producir una palabra de control *k'* a partir de dicha palabra de control cifrada *c*;
- unos medios para enviar, a dicho terminal, dicha palabra de control producida como respuesta a la recepción de la palabra de control cifrada *c*.

[0015] De acuerdo con la invención, dicho dispositivo consta de unos medios para memorizar un identificador *i* y los medios de tratamiento están dispuestos para implementar un procedimiento de acuerdo con la invención para producir la palabra de control *k'*.

[0016] La invención prevé que dicho dispositivo pueda constar de unos medios para implementar una función de retardo que coopera con los medios de tratamiento y que dichos medios de tratamiento puedan estar dispuestos para implementar un procedimiento de acuerdo con la invención de tal modo que la palabra de control *k'* se pueda enviar mediante los medios para enviar tras un intervalo de tiempo determinado.

[0017] También se prevé que el dispositivo electrónico pueda constar de unos medios para memorizar una información R_p que indica una revocación permanente de dicho dispositivo e incluso que pueda constar de unos medios para memorizar o generar una palabra con un valor *kf* diferente del valor de *k*.

[0018] La invención prevé, además, diferentes formas de realización de un procedimiento para identificar un dispositivo electrónico, como el que se ha descrito con anterioridad y que coopera con un terminal pirata adaptado para emitir a través de una red pirata una palabra de control *k'*. Dicho procedimiento consta de:

- una etapa para producir una palabra de control *k* que consiste en determinar el valor de una componente *v* de dicha palabra de control;
- una etapa para producir una palabra de control cifrada *c* cifrando dicha palabra de control *k* por medio de una función de cifrado *E*, tal que $c = E(k)$;
- una etapa para difundir dicha palabra de control cifrada *c* a través de una red de difusión destinada a los terminales entre los cuales se encuentra dicho terminal pirata;
- una etapa para observar la red pirata que consiste en medir la probabilidad $p(k \mid v)$ de constatar la transmisión efectiva de una palabra de control *k'* con un valor *k*, sabiendo el valor de *v*;

- una etapa para identificar que consiste en devolver un valor directamente vinculado al identificador *i* de un dispositivo que ha producido una palabra de control *k'* emitida a través de la red pirata, a partir del valor de *v* y de la medición de dicha probabilidad *p(k| v)*.

[0019] La invención también prevé diferentes formas de realización de un procedimiento para identificar un dispositivo electrónico que coopera con un terminal adaptado para emitir a través de una red pirata un contenido *M'* previamente elaborado, mediante dicho terminal, decodificando un contenido cifrado *C* por medio de una palabra de control *k'* y de una función de decodificación *dec* tal que *M' = dec(k',C)*, habiendo sido producida dicha palabra de control *k'* por dicho dispositivo, de acuerdo con la invención, a partir de una palabra de control cifrada *c* conjuntamente transmitida con *C* por medio de una red de difusión.

[0020] Dicho procedimiento consta de:

- una etapa para producir una palabra de control *k* que consiste en determinar el valor de una componente *v* de dicha palabra de control;
- una etapa para producir una palabra de control cifrada *c* cifrando dicha palabra de control *k* por medio de una función de cifrado *E* tal que *c = E(k)*;
- una etapa para producir un contenido cifrado *C* codificando un contenido *M* por medio de dicha palabra de control *k* y de una función de codificación *enc* tal que *C = enc(k,M)*;
- una etapa para difundir conjuntamente dicha palabra de control cifrada *c* y dicho contenido cifrado *C* a través de la red de difusión destinada a los terminales entre los cuales se encuentra dicho terminal pirata;
- una etapa para observar el flujo de dicha red pirata que consiste en medir la probabilidad *p(M| v)* de constatar la transmisión efectiva de un contenido *M'* con un valor *M*, sabiendo el valor de *v*;
- una etapa para identificar que consiste en devolver un valor directamente vinculado al identificador *i* de un dispositivo que ha producido una palabra de control *k'* que ha utilizado el terminal pirata para elaborar un contenido *M'* emitido a través de la red pirata, a partir del valor de *v* y de la medición de dicha probabilidad *p(M| v)*.

[0021] Se mostrarán otras características y ventajas de forma más clara con la lectura de la descripción que viene a continuación y con el análisis de las figuras que la acompañan, en las que:

- la figura 1 presenta una red de difusión de contenidos multimedia protegidos de acuerdo con el estado de la técnica;
- la figura 2a presenta algunas soluciones para intentar realizar un pirateo de contenidos multimedia protegidos y difundidos por medio de una red de difusión de acuerdo con el estado de la técnica;
- la figura 3 ilustra la arquitectura funcional de un dispositivo electrónico de abonado de acuerdo con la invención;
- las figuras 4a y 4b ilustran respectivamente dos formas de realización de un procedimiento para producir una palabra de control, procedimiento implementado mediante un dispositivo electrónico de acuerdo con la invención;
- las figuras 5, 6 y 7 describen respectivamente tres formas de realización de un procedimiento, de acuerdo con la invención, para observar una red pirata e identificar un dispositivo electrónico utilizado de manera fraudulenta;
- la figura 2b describe la implementación, de acuerdo con la invención, de dicho procedimiento para observar una red pirata e identificar un dispositivo electrónico utilizado de manera fraudulenta.

[0022] La figura 1 permite presentar una red de difusión 4 utilizada por un operador de difusión de contenidos protegidos. De este modo, desde un servidor de contenidos 3, se emiten conjuntamente unas palabras de control *c* y unos contenidos *C* respectivamente cifrados y codificados. El servidor 3 codifica para ello un contenido en abierto *M* por medio de una función de codificación *enc* y de una palabra de control *k*, siendo este último producido por dicho servidor 3. De este modo, se obtiene un contenido codificado *C* tal que *C = enc(k,M)*. Un cifrado *c* de la palabra de control *k* también se emite o "teletransmite" conjuntamente con el contenido codificado *C*. Para ello, el servidor cifra por medio de una función de cifrado *E* dicha palabra de control *k* para obtener *c* tal que *c = E(k)*.

[0023] Las palabras de control cifradas *c* y los contenidos cifrados *C* se transmiten, a través de la red de difusión 4, a unos terminales 2a a 2m. Estos últimos se encargan respectivamente de decodificar en tiempo real los contenidos codificados *C* emitidos por el servidor 3. De este modo, un terminal -como, por ejemplo, el decodificador 2a- implementa una función de decodificación *dec* y la aplica al contenido codificado *C* para obtener el contenido en abierto *M*. Este último se puede visualizar utilizando un televisor doméstico 5 o cualquier otra interfaz adaptada. Para aplicar la función de decodificación *dec*, un terminal debe conocer el valor de la palabra de control *k* que ha utilizado el servidor 3 para codificar el contenido *M*. De acuerdo con el estado de la técnica y de acuerdo con la figura 1, un terminal 2a a 2m recibe una palabra de control cifrada *c* tal que *c = E(k)* y la transmite a un dispositivo electrónico seguro la a 1m, por lo general específico para un abonado. El terminal 2a recibe, a través de la red 4, de forma regular unos pares (*C,c*) y transmite a un dispositivo las palabras de control cifradas *c*. El dispositivo Ia puede descifrar una palabra de control cifrada *c* por medio de una función de descifrado *D* para obtener la palabra de control *k* que se ha utilizado para codificar un contenido *M*. De este modo, *k = D(c)*. Lo mismo sucede para cualquier otro terminal, como 2b a 2m, cooperando respectivamente cada uno con dispositivo 1b a 1m. De acuerdo con una variante de realización, el servidor 3 puede utilizar un secreto, por ejemplo en forma de una clave *Kc* para cifrar una palabra de control *k*. De este modo, *c = E(Kc,k)*. En este caso, un dispositivo, como el dispositivo Ia a 1m,

implementa una función recíproca de descifrado *D*, tal que *k = D(Kd,k)* en la que *Kd* es una clave de descifrado conocida por el dispositivo. De acuerdo con las funciones de cifrado *E* y de descifrado *D*, las claves *Kc* y *Kd* pueden ser idénticas. Es el caso de un cifrado/descifrado simétrico. En una variante, de acuerdo con un esquema denominado de "*broadcast encryption*" - en términos anglosajones- *Kc* es una clave pública o secreta específica del operador y *Kd* es una clave secreta específica para el dispositivo y que conoce el operador. De acuerdo con esta variante, existen de este modo varias claves individuales de descifrado y cada uno de los dispositivos lícitamente emitidos y entregados a los abonados de dicho operador dispone de dicha clave de descifrado individual.

[0024] La figura 2a permite ilustrar un primer escenario para el cual una organización pirata, que llamaremos "pirata" consigue realizar un comercio fraudulento de contenidos protegidos.

[0025] De acuerdo con este primer escenario, el pirata ha contratado de forma completamente normal un abono con el operador de contenidos. De este modo, puede disponer de un dispositivo electrónico de abonado, como una tarjeta inteligente 1a. El pirata pose, además, un terminal 2P, denominado terminal pirata. Este terminal puede recibir unos pares (*C,c*) desde una red de difusión 4 como se ha descrito en relación con la figura 1. El terminal 2P puede cooperar con dicho dispositivo 1a para transmitirle las palabras de control cifradas *c*. A su vez, el dispositivo 1a produce la palabra de control *k* descifrando el cifrado *c* por medio de una función de descifrado *D*. De forma completamente normal, el dispositivo 1a envía al terminal 2P la palabra de control *k*. De acuerdo con este primer escenario, el terminal pirata 2P puede entonces emitir a través de una red pirata 6 las palabras de control *k* en tiempo real. Un usuario deshonesto que ha "suscrito" un abono con el pirata, puede disponer de un terminal 2w. Este último está adaptado para que reciba, por una parte, desde la red de distribución 4, unos contenidos codificados *C* (flecha en línea de puntos) y, por otra parte, desde la red pirata 6, las palabras de control *k* asociadas, en abierto. El terminal 2w puede realizar la decodificación de los contenidos codificados *C* y enviar los contenidos en abierto *M* para que se puedan visualizar.

[0026] De acuerdo con un segundo escenario, el terminal 2P procede a la decodificación de los contenidos codificados *C* y transmite en tiempo real los contenidos en abierto *M* a través de la red pirata 6. El terminal 2w no es entonces más que una simple interfaz para recibir los contenidos *M* y transmitirlos a la interfaz 5 para que el abonado deshonesto pueda disfrutar de forma fraudulenta del contenido protegido.

[0027] Nos encontremos en el primero o en el segundo escenario, un pirata también puede suscribir una multitud de abonos con uno o varios operadores. Un terminal pirata 2P puede entonces cooperar simultáneamente con una multitud de dispositivos de abonados 1a a 1p y utilizar un algoritmo de gestión de dichos dispositivos más o menos complejo. Por ejemplo, el terminal pirata transmite una palabra de control *k* descifrada en su mayor parte por los dispositivos 1a a 1p. En una variante, dicho terminal 2P puede solicitar de manera aleatoria a uno u otro dispositivo electrónico, etc.

[0028] En una variante, un pirata puede eventualmente cifrar o codificar, de acuerdo con un procedimiento propio, las palabras de control *k* y/o los contenidos *M* emitidos en una red pirata. De este modo, se pueden transmitir respectivamente, en dicha red pirata, un cifrado $c_p = E_p(k)$ -siendo E_p una función de cifrado propia del pirata- o $C_p = enc_p(M)$ -siendo enc_p una función de codificación propia del pirata-. Un terminal 2w consta, en este caso, de unas funciones de descifrado D_p y/o de decodificación dec_p recíprocas para enviar finalmente los descifrados $k = D_p(c_p)$ y/o $M = dec_p(C_p)$ esperados.

[0029] La invención permite que estos diferentes escenarios de pirateo fracasen.

[0030] La figura 3 permite ilustrar diferentes formas de realización previstas por la invención, para adaptar un dispositivo electrónico de abonado 1. De acuerdo con el estado de la técnica, dicho dispositivo consta de unos medios R para recibir del mundo exterior -por ejemplo de un terminal 2- un cifrado c. Dicho dispositivo 1 consta de unos medios de tratamiento 10 para implementar 11 una función de descifrado *D* tal que *k = D(c)* y producir una palabra de control *k*. Eventualmente, dicho dispositivo puede implementar una función *D* acoplada a una clave *Kd* de descifrado tal que *k = D(Kd,c)*. La clave *Kd* se memoriza por lo general mediante unos medios de memorización 12. De acuerdo con el estado de la técnica, la palabra de control producida *k* la envía el dispositivo 1, a través de los medios *S*, a un terminal 2. La invención prevé adaptar dicho dispositivo 1 para que envíe una palabra de control *k'* en lugar de la palabra *k*. Para ello, la invención prevé que el servidor 3, descrito en relación con la figura 1, produzca una palabra de control *k* antes del cifrado, que consta de una componente *v* con un valor determinado. De este modo, dicha palabra de control *k* se produce en función de un valor determinado de *v* por medio de una función reversible *F* tal que *k = F(v)*. De acuerdo con algunas formas de realización, la función *F* puede ser un cifrado simétrico que utiliza una clave secreta conocida del servidor 3 y del dispositivo 1.

[0031] Además, la invención prevé que un dispositivo 1 conste de un identificador *i* específico. Por ejemplo, a este identificador lo memorizan los medios de memorización 13 del dispositivo 1. Los medios de tratamiento 10 de este último constan de unos medios para interpretar dicha componente *v* de la palabra de control *k* obtenida tras la implementación 11 de la función de descifrado *D*. De acuerdo con el valor del identificador *i* y de la componente *v* extraída de *k*, el dispositivo 1 envía una palabra de control *k'* idéntica a *k* o diferente de esta. El valor de *k'* puede depender del resultado de una operación de comparación 15 entre los valores de *v* y de *i*. Dicho de otro modo, la

palabra de control *k'* producida y enviada por un dispositivo 1 se elabora 16 a partir de la palabra descifrada *k* y de un identificador *i* específico del dispositivo 1.

[0032] Los medios de tratamiento 10 deciden A que la palabra *k'* sea idéntica a la palabra de control *k* o diferente de esta. A título de ejemplo, para ser diferente de *k*, *k'* puede adoptar un valor *kf* diferente del de *k*. De acuerdo con una forma de realización, la invención prevé que *k'* pueda ser idéntica a *k* si y solo si la componente *v* de la palabra de control *k* es estrictamente inferior al valor del identificador *i*. Se podrían utilizar otras combinaciones o algoritmos de decisión A. Basta con que el valor de la componente *v*, en relación con el valor del identificador *i*, pueda influir en el valor de la palabra de control enviada *k'*. Un valor *kf* puede producirse de forma aleatoria, depender de *k* o leerse desde los medios de memorización 17 del dispositivo 1.

[0033] La invención prevé, además, una variante para la cual en lugar de producir una palabra de control *k'* con un valor *kf* diferente del de *k*, el valor de *k'* sea sistemáticamente igual a *k*, pero que se pueda diferir en el tiempo. En este caso, cuando el valor de *v* es superior o igual a *i*, los medios de tratamiento 10 implementan una función de retardo 18 o equivalente, de tal modo que la palabra de control *k'* se envíe tras un intervalo de tiempo determinado *d*. Se escribe entonces *k' = kd*. En el sentido de la invención, se considera que una palabra *k'* es diferente de *k* si *k' = kf* o *k' = kd*.

[0034] La adaptación de un dispositivo electrónico 1 tiene como objetivo producir una palabra de control *k'* cuyo valor (o el tiempo de respuesta) varía en función del contenido de la palabra de control producida por el servidor 3. De este modo, es posible para un operador revocar de manera momentánea un dispositivo de abonado según su identificador. En efecto, si *k'* es diferente de *k* o se envía tras un intervalo de tiempo suficiente *d*, *k'* no permite decodificar *C*. El contenido *M' = dec(k',C)* no corresponde al contenido *M* emitido por el operador.

[0035] De acuerdo con la figura 2b, se puede observar una red pirata 6 para medir 9 la probabilidad $p(k \mid v)$ de ver circular en tiempo real una palabra de control *k*, sabiendo el valor de *v*. Por medio de la invención, etapa por etapa, revocación momentánea por revocación momentánea, es posible identificar un dispositivo 1 utilizado de manera fraudulenta. Detallaremos más adelante -en relación con las figuras 5 a 7- unas formas de realización de un procedimiento de rastreo de acuerdo con la invención que permiten identificar dicho dispositivo indeseado.

[0036] La figura 4a describe un primer ejemplo de procedimiento para producir una palabra de control *k'*. Este procedimiento se puede implementar mediante los medios de tratamiento de un dispositivo electrónico 1 adaptado de acuerdo con la invención.

[0037] De este modo, dicho procedimiento consta de una primera etapa 501 para descifrar una palabra de control cifrada *c* y obtener un valor *k* de dicha palabra de control. El procedimiento consta de una etapa 502 para comparar el valor de una componente *v* de la palabra *k* y el valor del identificador *i* del dispositivo 1. De acuerdo con el ejemplo de realización ilustrado en la figura 4a, el valor de la palabra de control *k'* es:

- igual 503 al valor de *k*, si $v < i$;
- igual 504 a un valor $kf \neq k$, si $v \geq i$.

[0038] La figura 4a permite, además, ilustrar una variante para la cual el valor de *k'* puede ser igual 505 -si $v \geq i$- a *kd*, es decir igual a *k* pero enviado tras un intervalo de tiempo *d* determinado y característico.

[0039] La invención también prevé una variante para la cual, se puede revocar, a distancia y de manera permanente, un dispositivo electrónico -adaptado de acuerdo con la invención- en particular si este último es considerado por un operador como un dispositivo indeseado, es decir utilizado de forma fraudulenta por un pirata. Las figuras 3 y 4b permiten ilustrar esta variante.

[0040] Para ello, la invención prevé que la palabra de control *k* producida por un servidor 3, tal como se ha descrito en relación con la figura 1, consta, además de una componente *v*, de una segunda componente *t*. De este modo, el valor de la palabra de control *k* se puede obtener mediante la aplicación de una función reversible *F* a las componentes *v* y *t* tal que $k = F(t,v)$. De acuerdo con un ejemplo de realización, la aplicación de dicha función *F* se puede traducir mediante la elaboración de una palabra de control *k* cuyo valor es el resultado de una concatenación de las componentes *v* y *t* tal que $k = t \| v$. Por otra parte, otras componentes se podrían añadir así a dichas componentes *v* y *t*. Como se indica en la figura 3, los medios de tratamiento 10 de un dispositivo de acuerdo con la invención están adaptados, a partir de la palabra de control $k = F(t,v)$, para encontrar e interpretar las componentes *v* y *t*. Una primera forma de realización puede consistir en prever una componente *t* que puede adoptar un valor predeterminado t_p.

[0041] En relación con la figura 4b, un procedimiento para producir una palabra de control *k'* puede entonces constar de una etapa 511, implementada después de la etapa 501 para descifrar el cifrado c, para interpretar el valor de la componente *t*. Si este es igual, por ejemplo a t_p, el procedimiento consta de una etapa 513 para escribir en la memoria una información *Rp (Rp = "1")* para indicar que se revoca al dispositivo 1 de manera permanente. Esta etapa se implementa si y solo si la componente *v* es igual al identificador *i* del dispositivo. Además, de acuerdo con

esta variante, el procedimiento para producir *k'* solo implementa la comparación 502, tal como se describe en la figura 4a, si la información memorizada *Rp* indica (*Rp = "0"*) que no se ha revocado el dispositivo de manera permanente. En caso contrario, el procedimiento produce 504 o 505, *k' = kf* o *k'= kd*, con independencia del valor *v*. Al producir una palabra de control $k = F(t_p,i)$, por ejemplo $k = t_p \| i$, desde el servidor 3, un operador puede revocar al dispositivo cuyo identificador es igual a *i*, sin perjudicar por ello la emisión del contenido protegido destinado a sus abonados legales.

[0042] La invención prevé, además, una variante para la cual se puede rehabilitar un dispositivo revocado de manera permanente -de acuerdo con el procedimiento anterior-.

[0043] De manera recíproca, la invención prevé de este modo que la componente *t* pueda ser igual a un valor característico $t_a \neq t_p$. La etapa 511 permite por tanto interpretar el valor de la componente *t* y activar una etapa 515 para borrar una eventual información *Rp* que indica una revocación permanente del dispositivo (*Rp = "0"*). Esta etapa 515 se implementa si y solo si $t = t_a$ y si $v = i$. De este modo, se puede implementar un procedimiento para rehabilitar un dispositivo revocado produciendo $k = F(t_a,i)$, por ejemplo $k = t_a \| i$, en el servidor 3 del operador.

[0044] En una variante, la invención prevé que la componente *t* pueda adoptar un valor característico t_e, tal que $t_e \neq t_p$ *y* $t_e \neq t_a$, para implementar un procedimiento para producir *k'* de acuerdo con la invención. De este modo, si $t \neq t_e$, $t \neq t_p$ y $t \neq t_a$ entonces el procedimiento para producir *k'* produce *k' = k* sea cual sea el valor de *v*. En este caso, un dispositivo adaptado de acuerdo con la invención, se comporta como un dispositivo conforme con el estado de la técnica.

[0045] De acuerdo con otra variante, la invención permite que un operador pueda activar, para un dispositivo particular o para el conjunto de los dispositivos de abonado considerados, una actualización del identificador *i*. De este modo, la invención prevé poder adaptar dicho dispositivo para que conste de unos medios para detectar un valor particular de la componente *t* y de los medios para actualizar el identificador *i* del dispositivo.

[0046] En el caso de una petición de actualización específica para un dispositivo, dicho valor puede ser igual a un valor determinado $t = t_{iu}$. Si $t = t_{iu}$ y si $v = i$ entonces el dispositivo cuyo identificador es igual a $i = v$ puede actualizar su identificador *i*. A título de ejemplo, dichos medios para actualizar un identificador consisten en sobrescribir el valor actual del identificador *i* con el valor siguiente *i'* comprendido en una lista circular memorizada por dicho dispositivo. En una variante, dichos medios puede estar adaptados para actualizar una función $\Phi(i)$ para producir un nuevo valor *i'* del identificador *i*, tal que $i' = \Phi(i)$.

[0047] Para poder transmitir una petición de actualización global de los identificadores destinados al conjunto de los dispositivos, la invención prevé que dicho dispositivo pueda estar adaptado para que los medios para detectar estén en condiciones de detectar un valor determinado $t = t_{gu}$.

[0048] Cualquier dispositivo activa entonces una actualización de su identificador *i*. De acuerdo con una forma de realización, el valor de la componente *v* lo pueden utilizar dichos medios para actualizar el identificador. De este modo, en el marco de una lista, *v* puede ser un rango en el interior de una lista de identificadores, un índice para seleccionar una lista entre una multitud o incluso un elemento de diversificación para una función Φ, tal que $i' = \Phi(i,v)$. Se podría considerar cualquier otra forma de realización, en el sentido de la invención, desde el momento en que un identificador se puede actualizar mediante un dispositivo desde la red de difusión.

[0049] La figura 2b permite ilustrar la implementación de un procedimiento para observar una red pirata 6 e identificar un dispositivo indeseado 1a a 1p. La figura 2b retoma los elementos descritos en relación con la figura 2a. De este modo, un terminal 2P recibe unos pares (*C,c*) desde una red de difusión 4. El terminal 2P coopera con uno o varios dispositivos 1a a 1p para transmitirle las palabras de control cifradas *c*. A su vez, un dispositivo 1a a 1p produce la palabra de control *k* descifrando el cifrado *c* por medio de una función de descifrado *D* y lo envía al terminal 2P. Este último puede emitir a través de la red pirata 6 las palabras de control *k* en tiempo real. Un terminal 2w puede recibir, por una parte, desde la red de distribución 4, unos contenidos codificados *C* y, por otra parte, desde la red pirata 6 unas palabras de control *k* en abierto. El terminal 2w puede realizar la decodificación de los contenidos codificados *C* y enviar los contenidos en abierto *M* para que se puedan visualizar.

[0050] La invención prevé la utilización de unos medios 9 para observar la red pirata 6. Esta observación consiste en hacer que evolucione el valor de la componente *v* de las palabras de control *k* producidas por el servidor 3, en tiempo real y de acuerdo con un procedimiento descrito en relación con las figuras 5 a 7. Se mide entonces, para cada valor sucesivo de *v*, la probabilidad $p(k \mid v)$ de acuerdo con la cual el canal o la red pirata 6 funciona correctamente -es decir que las palabras de control *k' = k* se transmiten a través de la red 6-. Basándose en esta observación, un operador llega a identificar al menos un dispositivo indeseado utilizado por un decodificador o terminal pirata 2P, entre los dispositivos 1a a 1p. En cuanto se identifica un dispositivo indeseado 1i, se le puede revocar transmitiendo una palabra de control cifrada $c = E(F(t_p,i))$. De este modo, el dispositivo de identificador *i* se revoca de manera permanente. Si la red pirata 6 continúa funcionando correctamente, el procedimiento de rastreo descrito con anterioridad se repite hasta que dicha red 6 quede fuera de funcionamiento -al haberse revocado todos los dispositivos indeseados-.

[0051] Como se ha visto para la figura 2a, un segundo escenario de pirateo puede consistir en emitir ya no palabras de control *k' = k* en la red 6, sino directamente contenidos en abierto *M' = M*. La probabilidad medida es, por lo tanto, para un valor de *v*, la probabilidad $p(M \mid v)$ de ver circular en tiempo real contenidos *M' = M*.

[0052] Además, como también se ha visto para la figura 2a, un tercer escenario de pirateo puede consistir en emitir ya no palabras de control *k' = k* o contenidos en abierto *M' = M* en la red 6, sino unos cifrados $c_p = E_p(k')$ y/o $C_p = enc_p(M')$. Poder medir la probabilidad $p(k,M \mid v)$ para un valor de *v* de ver circular en tiempo real contenidos *M' = M* o palabras de control *k' = k*, sobreentiende que el operador de difusión -o cualquier otra entidad debidamente habilitada por este último para implementar un procedimiento para observar una red pirata- está adaptado para implementar funciones recíprocas D_p y/o dec_p tal que $k' = D_p(c_p)$ y/o $M' = dec_p(C_p)$.

[0053] La figura 5 presenta una primera forma de realización de un procedimiento para identificar un dispositivo electrónico indeseado 1, 1a,…, 1p, de acuerdo con la invención.

[0054] Este procedimiento de rastreo consta de una primera etapa 101 que consiste en inicializar previamente *v* en 0.

[0055] Una etapa 102 permite que el servidor 3 produzca una palabra de control cifrada *c* cifrando dicha palabra de control $k = F(t,v)$, por ejemplo $k = t \| v$, por medio de una función de cifrado *E*, tal que $c = E(k)$. Conjuntamente, se genera un mensaje codificado $C = enc(k,M)$. Un par (*C,c*) se difunde a través de una red de difusión destinada a los terminales entre los cuales se encuentra un terminal pirata.

[0056] Una etapa 103 para observar la red pirata consiste en medir la probabilidad $p(k \mid v)$ de constatar la transmisión efectiva de una palabra de control *k'* idéntica a *k*, sabiendo el valor de *v*. Se entiende por "transmisión efectiva de una palabra de control *k'* idéntica a *k*", la transmisión de dicha palabra, sin ningún desplazamiento temporal vinculado en particular a la implementación de una función de retardo 18 tal como se ha descrito con anterioridad -en relación con la figura 3-. En este caso, en el sentido de la invención, la transmisión retardada de una palabra de control *k' = kd*, no se considera como "una transmisión efectiva de una palabra de control *k'* idéntica a *k*".

[0057] Esta etapa puede, en una variante, consistir en medir la probabilidad $p(M \mid v)$ de constatar la transmisión efectiva de un contenido *M'* con un valor *M*, sabiendo el valor de *v*. Escribiremos $p(k,M \mid v)$ dicha probabilidad que cubre las dos variantes.

[0058] El procedimiento consta, además de una etapa 106 que consiste en incrementar el valor de la componente *v* mientras la probabilidad, sabiendo el valor de *v*, de constatar la transmisión efectiva de una palabra de control *k'* con un valor *k* o de un contenido *M'* con un valor *M* es próxima a 1.

[0059] El procedimiento consta de una etapa 105 para devolver el valor de *v* cuando la medición de la probabilidad $p(k,M \mid v)$ de constatar la transmisión efectiva de una palabra de control *k'* idéntica a *k* o de un contenido *M'* con un valor *M* es próxima a 0 mientras que la medición de dicha probabilidad $p(k,M \mid v\text{-}1)$, sabiendo el valor de *v*-1, es próxima a 1. El dispositivo cuyo identificador es *i = v* se reconoce como un dispositivo indeseado.

[0060] Si *n* es el número de dispositivos emitidos por un operador y los identificadores de dichos dispositivos están comprendidos respectivamente dentro de [1,*n*], entonces dicho procedimiento permite identificar un dispositivo indeseado en *n* mediciones de probabilidades.

[0061] La figura 6 permite ilustrar una segunda forma de realización de un procedimiento para identificar un dispositivo indeseado de acuerdo con la invención.

[0062] De acuerdo con este procedimiento, se va a proceder por dicotomía y obtener un resultado de logaritmo de *n* mediciones de la probabilidad $p(k,M \mid v)$.

[0063] De este modo, dicho procedimiento consta de una primera etapa 200 que consiste en inicializar *a* y *b*, dos números tales que *a* = 1 y *b* = *n*, siendo *n* el valor máximo de la componente *v* de una palabra de control producida por un servidor 3 de un operador.

[0064] El valor de la componente *v* se calcula en 201 tal que $v = (a+b)/2$.

[0065] El procedimiento consta de una etapa 202 para emitir un par (*C,c*) destinado a los terminales. El procedimiento consiste por tanto en medir 203 la probabilidad $p(k,M \mid v)$ de constatar la transmisión efectiva de una palabra de control *k'* idéntica a *k* o de un contenido *M'* con un valor *M*, sabiendo el valor de *v*.

[0066] En 204, el procedimiento consiste en evaluar si $a\text{-}1 = b$.

[0067] En caso afirmativo, entonces el procedimiento vuelve a 205 *i = b*. El dispositivo cuyo identificador es igual a *i* se identifica como un dispositivo indeseado.

[0068] En caso contrario, el procedimiento consiste en evaluar, en 206, la probabilidad $p(k,M| v)$ de constatar la transmisión efectiva, en la red pirata 6, de una palabra de control *k'* idéntica a *k* o de un contenido *M'* con un valor *M*, sabiendo el valor de *v*.

[0069] Si dicha probabilidad es próxima a 1 entonces el procedimiento consiste en asignar, en 207, a *a* el valor de *v* y en volver a la etapa 201. En caso contrario, el procedimiento consiste, en 208, en asignar a *b* el valor de *v* y en volver a la etapa 201.

[0070] La figura 7 permite presentar una tercera forma de realización de un procedimiento de rastreo para identificar un dispositivo indeseado.

[0071] De acuerdo con esta forma de realización, el identificador *i* es un vector de z enteros de valores $i = (i_1,..., i_z)$ comprendidos cada uno dentro de un conjunto [1,*m*], siendo *m* y *z* unos enteros superiores a 1. Además, la componente *v* es un vector de z enteros de valores $v = (v_1,..., v_z)$ comprendidos cada uno dentro de un conjunto [0,*m*].

[0072] Para implementar el procedimiento de rastreo, cualquier dispositivo de abonado produce una palabra de control *k'*:

- idéntica a *k* si el valor de cada entero v_l es, respectivamente, estrictamente inferior al valor de cada entero i_l para cualquier *l* comprendido entre 1 y *z*;
- diferente de *k* (cuyo valor $k' = k_f$ es diferente del de *k*, e incluso emitido con un retardo tal que *k' = kd*), en caso contrario.

[0073] El procedimiento para rastrear un dispositivo indeseado consiste, en primer lugar, en inicializar en 300 un entero *l* tal que *l* = 1 y la componente *v*, como vector de z enteros, tal que *v* = (0,…0).

[0074] El procedimiento consta de una etapa 301 para incrementar v_l, mientras, en 304, la probabilidad sabiendo el valor de *v* de constatar respectivamente la transmisión efectiva de una palabra de control *k'* idéntica a *k* o de un contenido *M'* idéntico a *M* en una red pirata es próxima a 1.

[0075] En caso contrario, el procedimiento consiste, en 305, en disminuir v_l y en incrementar *l* mientras, en 306, el valor de *l* es inferior o igual a *z*. En este caso, el procedimiento consiste en volver a la etapa 301.

[0076] La etapa 307 para identificar un dispositivo indeseado consiste en devolver el valor de *v* cuando, en 305, el valor de *l* se vuelve superior a *z*. El dispositivo cuyo identificador es *i = v* se identifica como un dispositivo indeseado.

[0077] De este modo, de acuerdo con este procedimiento de rastreo, un dispositivo indeseado se reconoce en *z.m* mediciones de probabilidad.

[0078] Para obtener el valor mínimo de *z.m* con $m^z \geq n$, siendo *n* el número de dispositivos, se obtiene *m* = 3, $z = \lceil \log_3 n \rceil$ y $z.m = 3.\lceil \log_3 n \rceil$ mediciones de probabilidades.

[0079] La invención prevé, además, que para identificar un dispositivo indeseado, se pueda transmitir una o varias palabras de control adicionales $k_1,\ldots,k_x$ además de la palabra de control *k*. En este caso, un encabezado de mensaje permite a cualquier dispositivo de abonado tener en cuenta la palabra de control pertinente. De acuerdo con esta variante, un procedimiento para producir una palabra de control de acuerdo con la invención puede constar de una etapa previa de decodificación de dicho encabezado para utilizar la palabra de control pertinente. Estas diferentes palabras de control pueden ser idénticas, válidas, o en parte, no válidas -es decir, que no permiten decodificar un contenido-.

REIVINDICACIONES

1. Procedimiento para producir una palabra de control *k'*, implementándose dicho procedimiento mediante unos medios de tratamiento (10) de un dispositivo electrónico (1) que coopera con un terminal (2), constando dicho dispositivo de unos medios (R) para recibir una palabra de control cifrada *c* desde el terminal (2) y de unos medios (S) para enviar dicha palabra de control *k'* producida a dicho terminal (2), constando dicho procedimiento de una etapa para aplicar (501) a la palabra de control cifrada *c* una función de descifrado *D* y calcular de este modo una palabra descifrada *k* tal que *k = D(c)*, **caracterizado por que** la palabra descifrada *k* consta de una componente *v* y **por que** el procedimiento consta de una etapa para producir (502, 503, 504, 505) la palabra de control *k'* respectivamente idéntica (503) o diferente (504, 505) de *k* de acuerdo con el resultado de una operación de comparación (502) entre el valor de *v* y el de un identificador *i* específico del dispositivo.

2. Procedimiento de acuerdo con la reivindicación anterior, **caracterizado por que** la etapa para producir la palabra de control *k'* diferente de *k* consiste en producir una palabra *k' = kf* cuyo valor *kf* es diferente del valor de *k*.

3. Procedimiento de acuerdo con la reivindicación 1, **caracterizado por que** la etapa para producir la palabra de control *k'* diferente de *k* consiste en implementar una función de retardo (18) de tal modo que los medios (S) para enviar envíen dicha palabra de control *k' = kd* cuyo valor *kd* es igual a *k*, tras un intervalo de tiempo determinado.

4. Procedimiento de acuerdo con la reivindicación 1, **caracterizado por que** la etapa para producir la palabra de control *k'* consiste en producir una palabra:

- idéntica a *k* si el valor de la componente *v* es estrictamente inferior al valor del identificador *i*;
- diferente de *k* si el valor de la componente *v* es superior o igual al valor del identificador *i*.

5. Procedimiento de acuerdo con la reivindicación 1, **caracterizado por que**:

- el identificador *i* es un vector de *z* enteros de valores $i = (i_1,...,i_z)$ comprendidos dentro de un conjunto [1,*m*], siendo *m* y *z* unos enteros superiores a 1;
- la componente *v* es un vector de *z* enteros de valores $v = (v_1,...,v_z)$ comprendidos dentro de un conjunto [0,*m*];

y **por que** la etapa para producir la palabra de control *k'* consiste en producir una palabra:

- idéntica a *k* si el valor de cada entero v_l es, respectivamente, estrictamente inferior al valor de cada entero i_l para cualquier *l* comprendido entre 1 y *z*;
- diferente de *k*, en caso contrario.

6. Procedimiento de acuerdo con una cualquiera de las reivindicaciones anteriores, **caracterizado por que** la palabra de control consta de una componente *t* y **por que** el procedimiento consta de una etapa para interpretar (511) dicha componente *t* para producir la palabra de control *k'* a partir de *v*, *i* y *k*.

7. Procedimiento de acuerdo con la reivindicación anterior, **caracterizado por que** consta de una etapa para memorizar (513) una información *Rp* para indicar una revocación permanente del dispositivo si la componente *t* es igual (511) a un valor predeterminado t_p y si la componente *v* es igual (512) al valor de identificador *i*.

8. Procedimiento de acuerdo con la reivindicación 6 **caracterizado por que** consta de una etapa para borrar (515) una información *Rp* que indica una revocación permanente del dispositivo si la componente *t* es igual (511) a un valor predeterminado t_a y si la componente *v* es igual (514) al valor del identificador *i*.

9. Dispositivo electrónico (1) que coopera con un terminal (2, 2a…., 2P), constando dicho dispositivo de:

- unos medios (R) para recibir una palabra de control cifrada *c* desde el terminal;
- unos medios de tratamiento (10) para producir una palabra de control *k'* a partir de dicha palabra de control cifrada *c*;
- unos medios (S) para enviar, a dicho terminal (2), dicha palabra de control producida como respuesta a la recepción de la palabra de control cifrada *c*,

caracterizado por que el dispositivo consta de unos medios (13) para memorizar un identificador *i* y **por que** dichos medios de tratamiento (10) están dispuestos para implementar un procedimiento de acuerdo con las reivindicaciones 1 o 2 para producir la palabra de control *k'*.

10. Dispositivo electrónico de acuerdo con la reivindicación anterior, **caracterizado por que** consta de unos medios (18) para implementar una función de retardo que coopera con los medios de tratamiento y **por que** dichos medios de tratamiento están dispuestos para implementar un procedimiento de acuerdo con la reivindicación 3 de tal modo que los medios para enviar (S) puedan enviar la palabra de control *k'* tras un intervalo de tiempo determinado.

11. Dispositivo electrónico de acuerdo con las reivindicaciones 9 o 10, **caracterizado por que** consta de unos medios (19) para memorizar una información *Rp* que indica una revocación permanente de dicho dispositivo y **por que** los medios de tratamiento (10) cooperan con dichos medios para memorizar (19) para implementar un procedimiento de acuerdo con las reivindicaciones 7 u 8 para producir la palabra de control *k'*.

12. Dispositivo electrónico de acuerdo con una cualquiera de las reivindicaciones 9 a 11, **caracterizado por que** consta de unos medios (17) para memorizar o generar una palabra con un valor *kf* diferente del valor de *k*.

13. Procedimiento para identificar un dispositivo electrónico (1, 1a,…,1p) de acuerdo con una cualquiera de las reivindicaciones 9 a 12 que coopera con un terminal pirata (2P) adaptado para emitir a través de una red pirata (6) una palabra de control *k'* producida por dicho dispositivo mediante un procedimiento de acuerdo con una cualquiera de las reivindicaciones 1 a 8, **caracterizándose** dicho procedimiento para identificar **por que** consta de:

- una etapa para producir una palabra de control *k* que consiste en determinar (101, 106, 201, 207, 208, 300, 301, 305) el valor de una componente *v* de dicha palabra de control;
- una etapa para producir (102, 202, 302) una palabra de control cifrada *c* cifrando dicha palabra de control *k* por medio de una función de cifrado *E*, tal que $c = E(k)$;
- una etapa para difundir (102, 202, 302) dicha palabra de control cifrada *c* a través de una red de difusión (4) destinada a los terminales (2, 2a, 2b, 2c, 2P) entre los cuales se encuentra dicho terminal pirata (2P);
- una etapa para observar la red pirata (6) que consiste en medir (103, 203, 303) la probabilidad $p(k \mid v)$ de constatar la transmisión efectiva de una palabra de control *k'* con un valor *k*, sabiendo el valor de *v*;
- una etapa para identificar que consiste en devolver (105, 205, 307) un valor directamente vinculado al identificador *i* de un dispositivo que ha producido una palabra de control *k'* emitida a través de la red pirata, a partir (104, 204, 206, 304, 306) del valor de *v* y de la medición de dicha probabilidad $p(k \mid v)$.

14. Procedimiento para identificar un dispositivo electrónico (1, 1a, 1b, 1c) de acuerdo con una cualquiera de las reivindicaciones 9 a 12 que coopera con un terminal pirata (2P) adaptado para emitir a través de una red pirata (6) un contenido *M'* previamente elaborado, mediante dicho terminal, decodificando un contenido cifrado *C* por medio de una palabra de control *k'* y de una función de decodificación *dec* tal que $M' = dec(k',C)$, habiéndose producido dicha palabra de control *k'* por dicho dispositivo mediante un procedimiento de acuerdo con una cualquiera de las reivindicaciones 1 a 8 a partir de una palabra de control cifrada *c* transmitida conjuntamente con *C* por medio de una red de difusión (4), **caracterizándose** dicho procedimiento para identificar **por que** consta de:

- una etapa para producir una palabra de control *k* que consiste en determinar (101, 106, 201, 207, 208, 300, 301, 305) el valor de una componente *v* de dicha palabra de control;
- una etapa para producir (102, 202, 302) una palabra de control cifrada *c* cifrando dicha palabra de control *k* por medio de una función de cifrado *E* tal que $c = E(k)$;
- una etapa para producir (102, 202, 302) un contenido cifrado *C* codificando un contenido *M* por medio de dicha palabra de control *k* y de una función de codificación *enc* tal que $C = enc(k,M)$;
- una etapa para difundir (102, 202, 302) conjuntamente dicha palabra de control cifrada *c* y dicho contenido cifrado *C* a través de la red (4) de difusión destinada a los terminales (2, 2a, 2P) entre los cuales se encuentra dicho terminal pirata (2P);
- una etapa para observar el flujo de dicha red pirata (6) que consiste en medir (103, 203, 303) la probabilidad $p(M \mid v)$ de constatar la transmisión efectiva de un contenido *M'* con un valor *M*, sabiendo el valor de *v*;
- una etapa para identificar que consiste en devolver (105, 205, 307) un valor directamente vinculado al identificador *i* de un dispositivo que ha producido una palabra de control *k'* que ha utilizado el terminal pirata para elaborar un contenido *M'* emitido a través de la red pirata, a partir (104, 204, 206, 304, 306) del valor de *v* y de la medición de dicha probabilidad $p(M \mid v)$.

15. Procedimiento de acuerdo con las reivindicaciones 13 o 14, cuando el procedimiento para producir una palabra de control *k'* es de acuerdo con una cualquiera de las reivindicaciones 1 a 4, **caracterizado por que** consta de una o varias iteraciones para las cuales:

- la etapa para determinar la componente *v* consiste:
  - en inicializar (101) previamente *v* en 0;
  - en incrementar (106) el valor de la componente *v* mientras la probabilidad, sabiendo el valor de *v*, de constatar la transmisión efectiva de una palabra de control *k'* con un valor *k* o de un contenido *M'* con un valor *M* es próxima a 1;
- la etapa para identificar consiste en devolver (105) el valor de *v* cuando (104) la medición de dicha probabilidad, sabiendo el valor de *v*, de constatar la trasmisión efectiva de una palabra de control *k'* con un valor *k* o de un contenido *M'* con un valor *M* es próxima a 0 mientras que la medición de dicha probabilidad, sabiendo el valor de *v*-1, es próxima a 1.

16. Procedimiento de acuerdo con las reivindicaciones 13 o 14, cuando el procedimiento para producir una palabra de control *k'* es de acuerdo con una cualquiera de las reivindicaciones 1 a 4, **caracterizado por que** consta de una o varias iteraciones para las cuales:

- la etapa para determinar la componente *v* consiste:

  - en inicializar (200) previamente *a* y *b*, dos números tales que *a* = 1 y *b* = n, siendo *n* el valor máximo de la componente *v*;
  - en calcular (201) el valor de la componente *v* tal que *v = (a + b) / 2;*
  - en asignar (207) a *a* el valor actual de *v* mientras (206) la probabilidad, sabiendo el valor de *v*, de constatar la transmisión efectiva de una palabra de control *k'* con un valor *k* o de un contenido *M'* con un valor *M* es próxima a 1;
  - en asignar (208) a *b* el valor actual de *v* mientras (206) la probabilidad, sabiendo el valor de *v*, de constatar la transmisión efectiva de una palabra de control *k'* con un valor *k* o de un contenido *M'* con un valor *M* no es próxima a 1;

- la etapa para identificar consiste en devolver (205) el valor de *v* cuando (204) el valor de *a*-1 es igual a *b*.

17. Procedimiento de acuerdo con las reivindicaciones 13 o 14, cuando el procedimiento para producir una palabra de control *k'* es de acuerdo con la reivindicación 5, **caracterizado por que** consta de una o varias iteraciones para las cuales:

- la etapa para determinar la componente *v* consiste:

  - en inicializar (300) previamente un entero *l* tal que *l* = 1 y *v*, como vector de z enteros, tal que *v* = (0,…,0);
  - en incrementar v_l (301) mientras (304) la probabilidad, sabiendo el valor de *v*, de constatar respectivamente la transmisión efectiva de una palabra de control *k'* con un valor *k* o de un contenido *M'* con un valor *M* es próxima a 1;
  - en disminuir v_l (305) y en incrementar *l* mientras (306) la probabilidad, sabiendo el valor de *v*, de constatar la transmisión efectiva de una palabra de control *k'* con un valor *k* o de un contenido *M'* con un valor *M* no es próxima a 0 y el valor de *l* es inferior o igual a *z*;

- la etapa para identificar consiste en devolver (307) el valor de *v* cuando (306) el valor de *l* es superior a *z*.

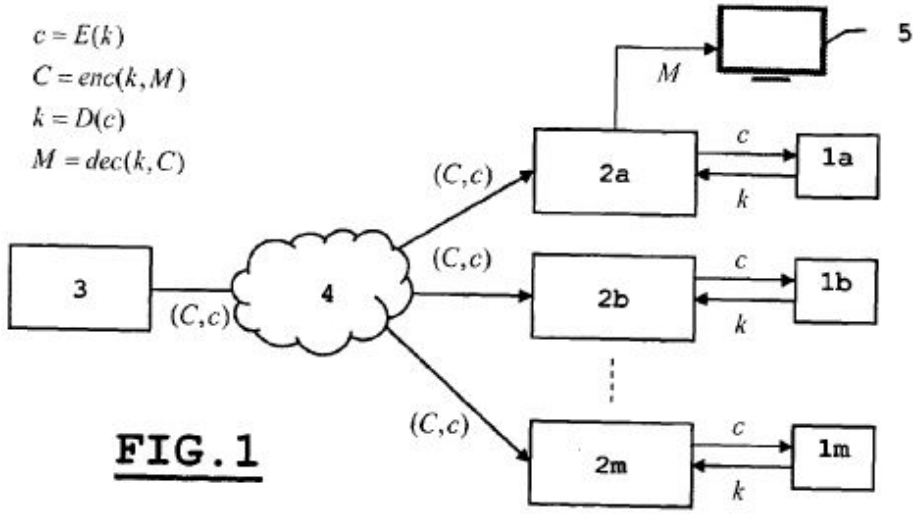

c = E(k)
C = enc(k, M)
k = D(c)
M = dec(k, C)
5
M
c
k
1a
2a
(C,c)
3
4
(C,c)
2b
1b
(C,c)
2m
1m

FIG.1

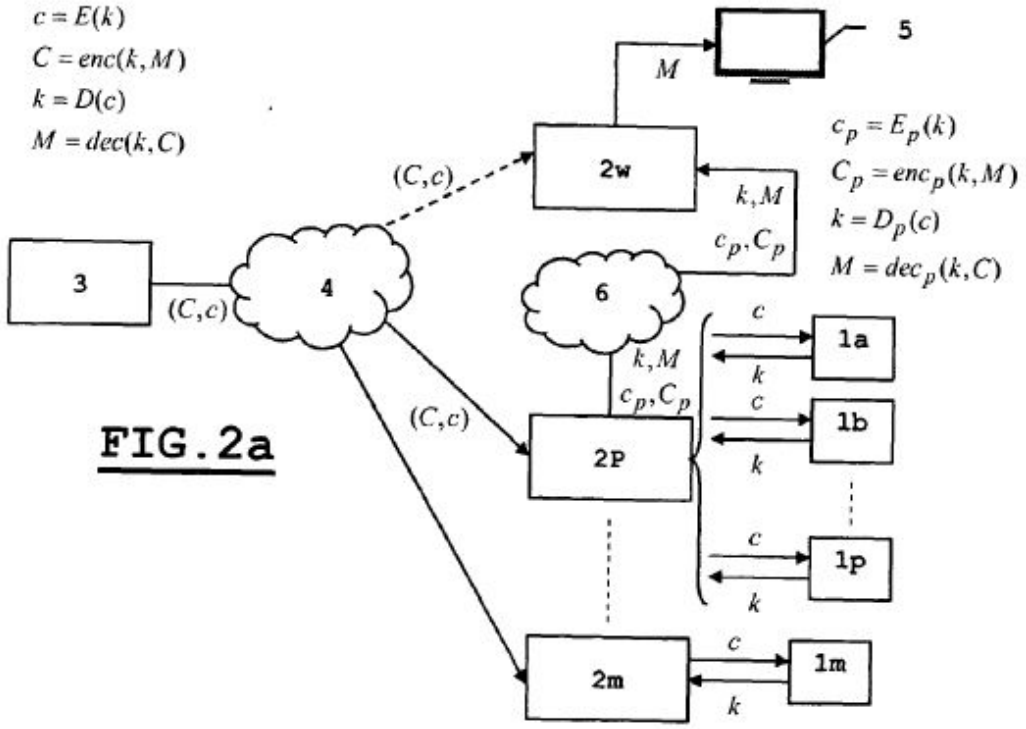

c = E(k)
C = enc(k, M)
k = D(c)
M = dec(k, C)
5
M
2w
k, M
cp, Cp
cp = Ep(k)
Cp = encp(k, M)
k = Dp(c)
M = decp(k, C)
(C,c)
3
4
(C,c)
6
k, M
cp, Cp
c
k
1a
1b
1p
(C,c)
2P
2m
1m

FIG.2a

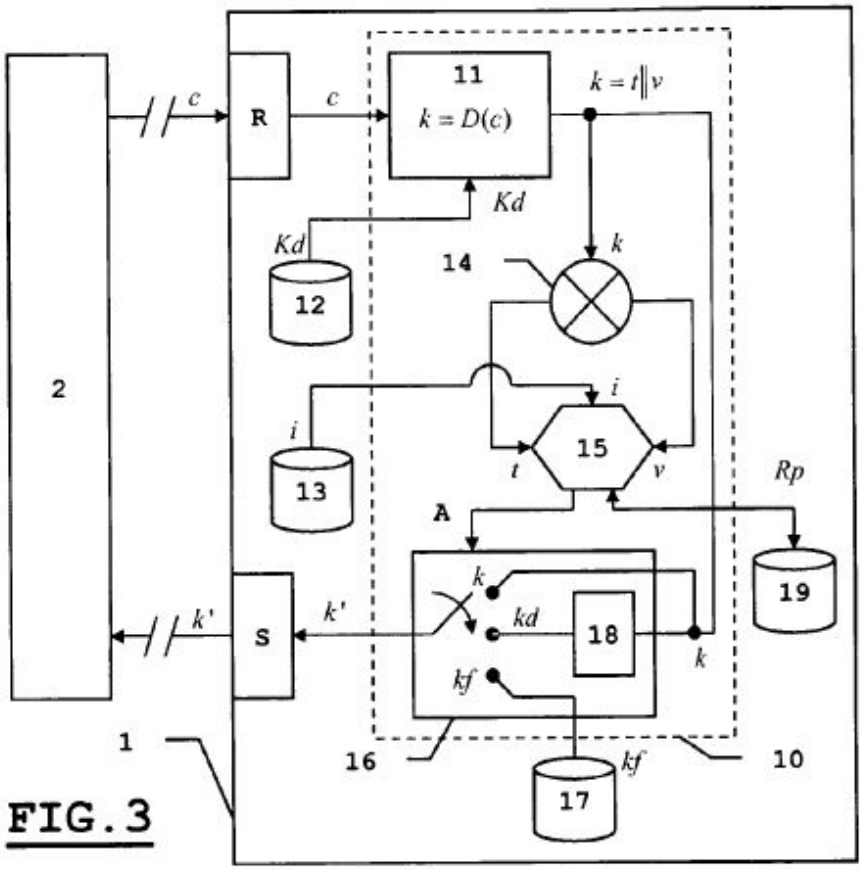

2
c
R
c
11
k = D(c)
k = t||v
Kd
Kd
12
14
k
i
i
13
15
t
v
Rp
A
k
19
k'
S
k'
kd
18
k
kf
1
16
kf
17
10

FIG.3

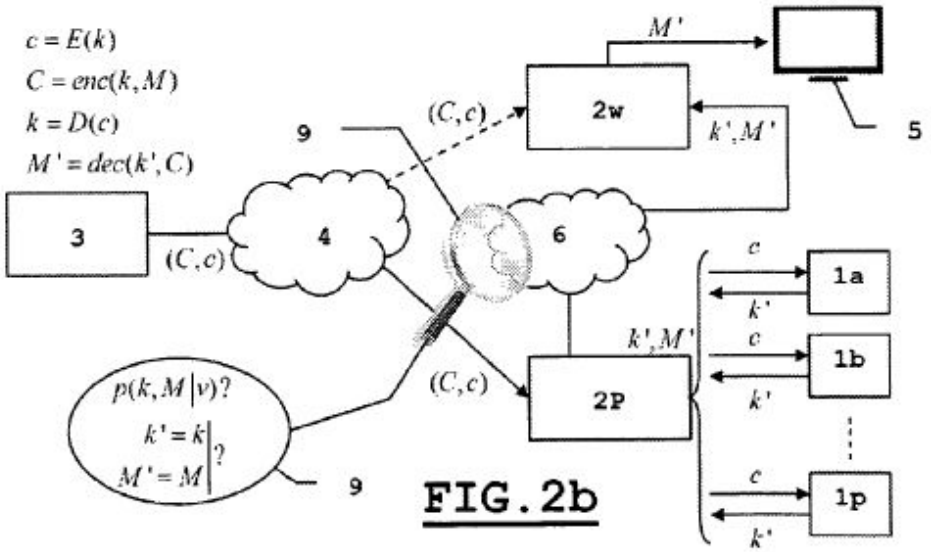

c = E(k)
C = enc(k, M)
k = D(c)
M' = dec(k', C)
M'
2w
(C, c)
9
k', M'
5
3
4
6
(C, c)
c
1a
k'
k', M'
c
1b
k'
p(k, M|v)?
k' = k
M' = M
?
(C, c)
2p
c
1p
k'
9

FIG.2b

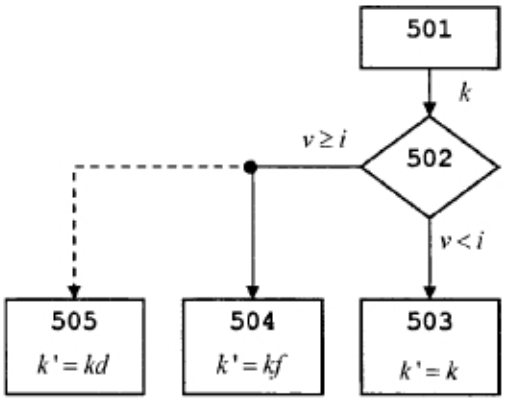

501
k
v ≥ i
502
v < i
505
k' = kd
504
k' = kf
503
k' = k

FIG.4a

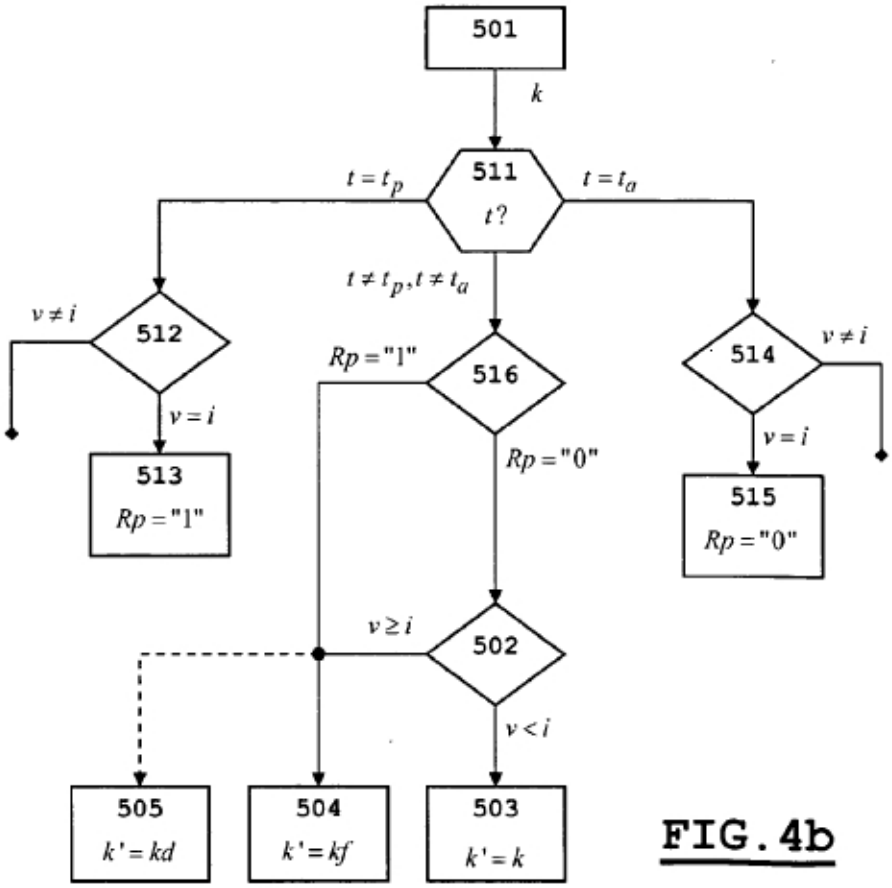

501
k
t = t_p
511
t?
t = t_a
t ≠ t_p, t ≠ t_a
v ≠ i
512
v = i
513
Rp = "1"
Rp = "1"
516
Rp = "0"
v ≠ i
514
v = i
515
Rp = "0"
v ≥ i
502
v < i
505
k' = kd
504
k' = kf
503
k' = k

FIG.4b

FIG. 5

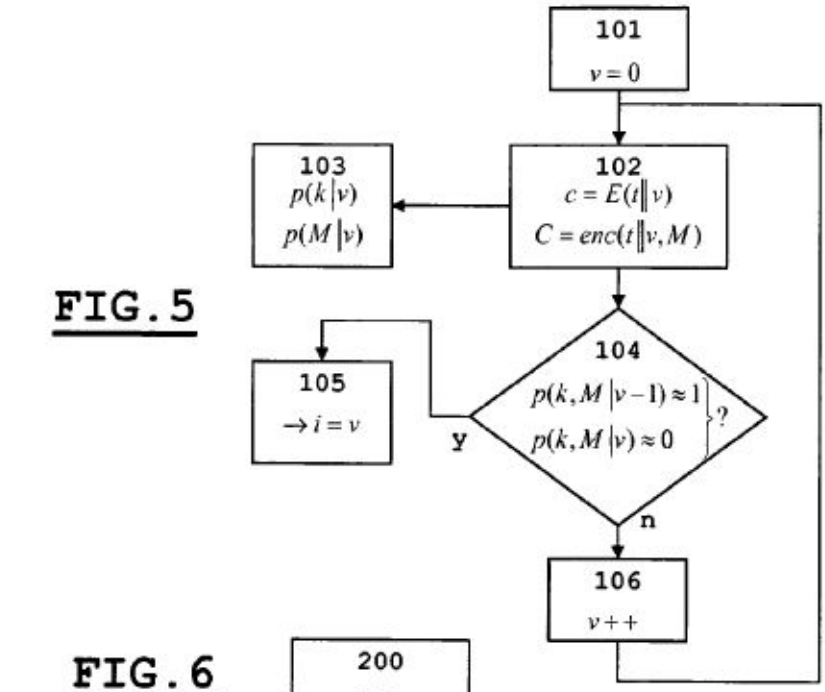
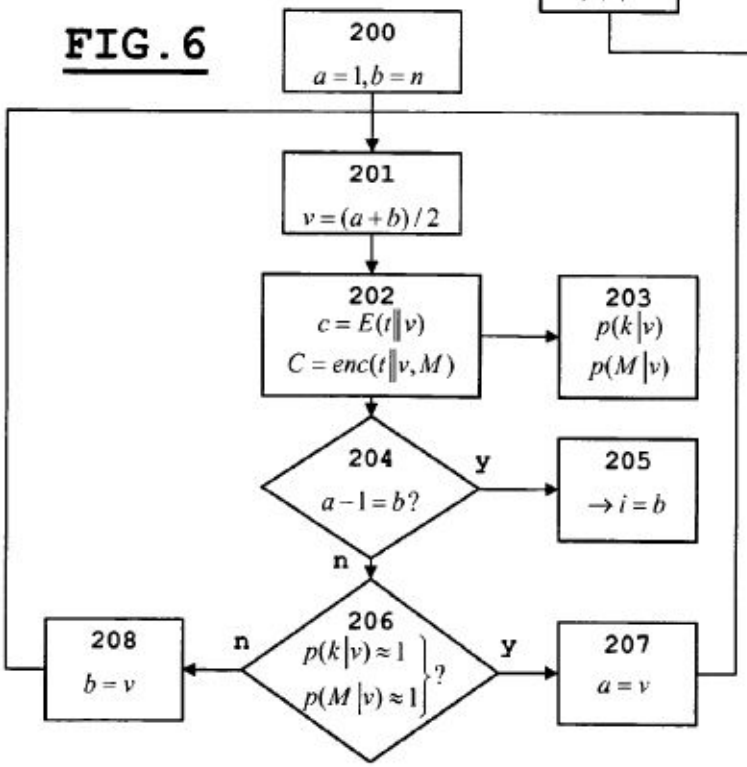

101
$v = 0$
102
$c = E(t \| v)$
$C = enc(t \| v, M)$
103
$p(k|v)$
$p(M|v)$
104
$p(k, M|v-1) \approx 1$
$p(k, M|v) \approx 0$
?
y
n
105
$\rightarrow i = v$
106
$v++$

FIG. 6


200
$a = 1, b = n$
201
$v = (a + b)/2$
202
$c = E(t \| v)$
$C = enc(t \| v, M)$
203
$p(k|v)$
$p(M|v)$
204
$a - 1 = b?$
y
205
$\rightarrow i = b$
n
206
$p(k|v) \approx 1$
$p(M|v) \approx 1$
?
n
y
208
$b = v$
207
$a = v$

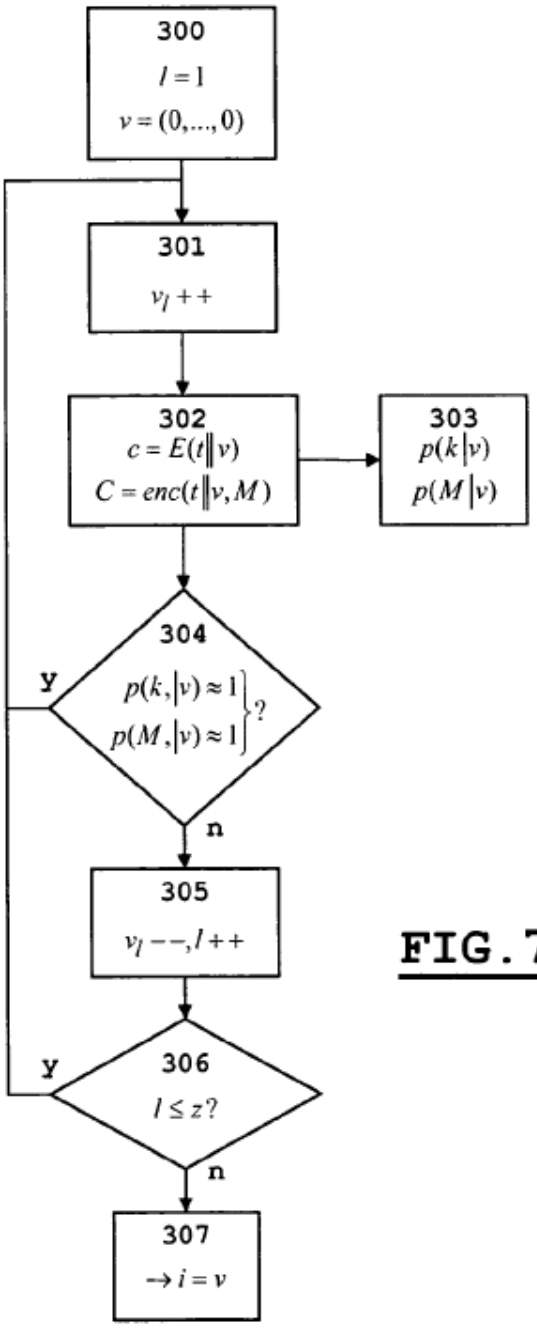

300
$l = 1$
$v = (0,...,0)$
301
$v_l ++$
302
$c = E(t \| v)$
$C = enc(t \| v, M)$
303
$p(k|v)$
$p(M|v)$
304
$p(k,|v) \approx 1$
$p(M,|v) \approx 1$
?
y
n
305
$v_l --, l ++$
306
$l \leq z$?
y
n
307
$\rightarrow i = v$

FIG.7