(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 683 771**

(51) Int. CI.:

H04L 9/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **16.12.2011 PCT/FR2011/053040**

(87) Fecha y número de publicación internacional: **21.06.2012 WO12080683**

(96) Fecha de presentación y número de la solicitud europea: **16.12.2011 E 11817383 (0)**

(97) Fecha y número de publicación de la concesión europea: **23.05.2018 EP 2652899**

(54) Título: **Procedimiento y sistema de acceso condicional a un contenido digital, terminal y dispositivo de abonado asociados**

(30) Prioridad:

17.12.2010 FR 1060770

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
27.09.2018

(73) Titular/es:

CRYPTOEXPERTS SAS (100.0%)
37 Cours de Vincennes
75020 Paris, FR

(72) Inventor/es:

DELERABLEE, CÉCILE;
GOUGET, ALINE y
PAILLIER, PASCAL

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Procedimiento y sistema de acceso condicional a un contenido digital, terminal y dispositivo de abonado asociados

La invención se refiere a un sistema y a un procedimiento de acceso condicional a un contenido digital que permite prevenir la puesta en práctica de un dispositivo electrónico adquirido lícitamente e íntegro, por medio de un terminal pirata. Así, la invención permite luchar eficazmente contra la puesta a disposición fraudulenta de contenidos multimedia protegidos.

La invención se refiere además a la adaptación de tales dispositivos, así como a un procedimiento para desencadenar respectivamente la revocación temporal o permanente de un dispositivo electrónico o la eventual rehabilitación de este último. La invención se refiere además a la adaptación de un terminal para permitir la puesta en práctica del procedimiento de acceso condicional.

Un operador de difusión de contenidos multimedia generalmente opera un sistema de acceso condicional (*Conditional Access System* - CAS en lengua inglesa) para poner un contenido protegido a disposición de un abonado o de una pluralidad de abonados. Tal sistema generalmente estriba en dispositivos electrónicos seguros, tales 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.

De acuerdo con los sistemas de acceso condicional conocidos, para difundir un contenido multimedia protegido, se transmiten palabras de control cifradas *c* y contenidos codificados *C* a través de una red de difusión, a intervalos regulares o criptoperiodos, por lo menos, conocidos y dominados por el operador de difusión. Una palabra de control cifrada generalmente se obtiene por medio de una función de cifrado *E* tal que *c = E(k)*, siendo *k* el valor de dicha palabra de control. Por su parte, un contenido codificado *C* se obtiene 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 claro. A título de ejemplo, la función de codificación puede ser acorde con el estándar DVB-CSA (*Digital Video Broadcasting - Common Scrambling Algorithm*, en lengua inglesa). Para poder visualizar o escuchar un contenido protegido, cualquier persona tiene que contratar una suscripción. Se entrega a un abonado un dispositivo específico, generalmente en forma de una tarjeta inteligente que, acoplado a un terminal, denominado generalmente descodificador o “set-top box”, permite a dicho abonado descodificar un contenido protegido. Convencionalmente, las palabras de control cifradas *c* son descifradas por un dispositivo de abonado que suministra al terminal las palabras de control *k*. Este último es el encargado de realizar la descodificación de un contenido codificado *C* y permite, por medio de una interfaz hombre-máquina adaptada -por ejemplo, un televisor de salón-, acceder al contenido sin cifrar *M*.

Ocurre habitualmente que entidades “piratas” traten de desarrollar un comercio ilícito encaminado a emitir, en una red pirata, palabras de control descifradas *k* que permiten descodificar un contenido protegido *C* con el concurso de un terminal adaptado al efecto. Las primeras amenazas y ataques han movido a los piratas a tratar de “romper” la seguridad de los dispositivos electrónicos de abonado. Mediante el conocimiento del equipo criptográfico, de los algoritmos o de secretos, un pirata, entonces, puede “clonar” o emular un dispositivo de este tipo y poner ciertas “reproducciones” a disposición de abonados desaprensivos.

La creciente y casi inviolable robustez de tales dispositivos ha llevado a los piratas a adquirir lícitamente dispositivos de abonado (tales como tarjetas inteligentes) y a idear terminales piratas, aptos para cooperar con dichos dispositivos y a emitir las palabras de control descifradas *k*, en tiempo real, en una red o canal pirata según técnicas conocidas con el vocablo de “*Control-word sharing*” según una terminología anglosajona. Esta técnica de “*Control-word sharing*” encaminada a emitir palabras de control descifradas es particularmente preciada, ya que permite utilizar una red pirata de escaso ancho de banda, pues el tamaño de las palabras de control es generalmente muy inferior al tamaño de contenidos descodificados.

Para hacer frente a los piratas, los operadores generalmente consiguen enterarse de la existencia de una red pirata de este tipo. Contratando una suscripción con un pirata, un operador puede incluso disponer de un dispositivo “clon” o emulado, y estudiarlo.

Se conocen en el estado de la técnica procedimientos de rastreo de los traidores, tales como el desvelado en el documento US2008/0298582.

No obstante, dado que la palabra de control *k* que permite acceder al contenido multimedia en claro es idéntica para todos los abonados (o para un gran grupo de abonados), no es posible identificar el origen del fraude a partir de una palabra de control que haya sido divulgada en la red pirata. Por lo tanto, no existen procedimientos conocidos que permitan identificar un dispositivo que, aunque adquirido debidamente e íntegro, es explotado de manera fraudulenta.

La invención permite dar respuesta de manera particularmente eficaz a la amenaza del “*Control-word sharing*”. Entre las abundantes ventajas que aporta 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 puede ser transmitido en una red pirata. En efecto, la invención permite prever una palabra de control específica y distinta para

cada dispositivo de abonado. La observación de tal palabra de control emitida en una red pirata permite dar con el dispositivo abonado explotado ilícitamente. La invención permite, además, revocar a distancia un dispositivo de este tipo, llamado “dispositivo traidor”, al propio tiempo que se prosigue la difusión de un contenido a través de la red de difusión. Así, la invención ofrece, para todo operador de difusión de contenidos, una herramienta particularmente simple y eficaz para luchar contra la piratería. Adicionalmente, de acuerdo con una forma preferida de realización, un dispositivo de abonado apenas opera pocos cálculos, siendo efectuados los cálculos costosos en el terminal puesto a disposición del abonado y cooperante con dicho dispositivo de abonado.

Para este fin, se prevé un procedimiento para producir una palabra de control, puesto en práctica por unos medios de procesamiento de un dispositivo electrónico de abonado que coopera con un terminal, incluyendo dicho dispositivo unos medios de recepción para recibir datos desde el terminal y unos medios para suministrar dicha palabra de control producida a dicho terminal. Dicho procedimiento incluye:

- una etapa para recibir datos por intermedio de los medios de recepción que consisten en una etiqueta *t*;
- una etapa para determinar el criptoperiodo en curso explotando la etiqueta *t* recibida;
- una etapa para producir una palabra de control a partir de dicho criptoperiodo en curso *cp* y de un secreto SK_i memorizado por el dispositivo;
- una etapa para suministrar una palabra de control *k’* por intermedio de los medios para suministrar del dispositivo.

Para poder rastrear cualquier dispositivo de abonado que haya producido una palabra de control cuyo valor puede ser transmitido en una red pirata, la etapa para producir la palabra de control de tal procedimiento consiste en elaborar una palabra de control $k_{i,cp}$ rastreable cuyo valor es distinto del de una palabra de control producida, para el criptoperiodo en curso *cp*, por cualquier otro dispositivo de abonado, integrando el valor de un identificador *i* en el cálculo de la palabra $k_{i,cp}$. Dicho valor del identificador *i* es memorizado por el dispositivo y distinto del memorizado por cualquier otro dispositivo de abonado. La etapa para suministrar la palabra de control consiste en suministrar *k’* igual a $k_{i,cp}$.

Para poder revocar o habilitar un dispositivo de abonado que pone en práctica tal procedimiento, este último puede incluir una etapa previa para autorizar el dispositivo a suministrar una palabra de control *k’* igual a la palabra de control producida $k_{i,cp}$.

Eventualmente, para liberar de esta tarea a un servidor de contenido, tal procedimiento puede incluir una etapa para calcular y suministrar una cabecera *H* para, al final, permitir la descodificación del contenido codificado mediante un terminal.

Para llevar a la práctica un procedimiento para producir una palabra de control rastreable, la invención prevé adaptar un dispositivo electrónico de abonado que coopera con un terminal y que incluye:

- unos medios de recepción para recibir datos desde el terminal;
- unos medios de procesamiento para producir una palabra de control a partir de dichos datos;
- unos medios para suministrar dicha palabra de control a dicho terminal.

Tal adaptación consiste en que el dispositivo incluye unos medios de memorización para memorizar un identificador *i*, un secreto SK_i. Los medios de procesamiento y de memorización además están adaptados para producir y suministrar una palabra de control rastreable *k’* según un procedimiento conforme a la invención.

De acuerdo con un segundo objeto, la invención prevé un procedimiento para descodificar un contenido codificado *C* y producir un contenido en claro *M*, siendo puesto en práctica dicho procedimiento por unos medios de procesamiento de un terminal que cooperan con unos medios para recibir datos desde el mundo exterior y unos medios para suministrar dicho contenido en claro *M*. De acuerdo con la invención, dichos datos consisten en dicho contenido codificado *C*, una cabecera *H* y una palabra de control rastreable $k_{i,cp}$ elaborada y suministrada por un dispositivo electrónico de abonado conforme a la invención. Para permitir la descodificación de un contenido, aunque la palabra de control sea rastreable y, por tanto, distinta de un dispositivo de abonado a otro, el procedimiento para descodificar incluye:

- una etapa para aplicar una primera función *F*1 a la cabecera *H* y a la palabra de control $k_{i,cp}$ para producir una palabra *K* independiente del identificador *i* del dispositivo que haya producido y suministrado la palabra de control $k_{i,cp}$ suprimiendo la contribución de dicho identificador específico *i*;
- una etapa para aplicar una segunda función *F*3 a dicha palabra *K* y al contenido codificado *C* para producir el contenido en claro *M*;

- una etapa para suministrar dicho contenido en claro *M* por intermedio de los medios para suministrar del terminal.

Para llevar a la práctica un procedimiento para descodificar un contenido codificado *C* y producir un contenido en claro *M*, la invención prevé adaptar un terminal electrónico que incluye:

- unos medios de recepción para recibir datos desde el mundo exterior;
- unos medios de procesamiento para producir un contenido en claro *M* a partir de dichos datos;
- unos medios para suministrar dicho contenido en claro a una interfaz hombre-máquina adaptada para restituir dicho contenido en claro;
- unos medios para cooperar con un dispositivo electrónico de abonado conforme a la invención.

Los datos recibidos del mundo exterior consisten a partir de entonces en un contenido codificado *C*, una cabecera *H* y una etiqueta *t*. Los medios para cooperar con dicho dispositivo electrónico de abonado transmiten a este último dicha etiqueta *t* y receptan de vuelta una palabra de control rastreable $k_{i,cp}$ elaborada y suministrada según la invención. El terminal incluye además unos medios de procesamiento adaptados para descodificar y suministrar un contenido en claro *M* según un procedimiento conforme a la invención.

De acuerdo con un tercer objeto, la invención prevé un procedimiento para codificar un contenido en claro *M* y producir un contenido codificado *C*, siendo puesto en práctica dicho procedimiento por unos medios de procesamiento de un servidor que incluye unos medios para suministrar dicho contenido codificado *C* a un terminal según la invención y que cooperan con un dispositivo de abonado también conforme a la invención. Tal procedimiento incluye:

- una etapa para producir un contenido codificado *C* a partir de un criptoperiodo *cp* y de un secreto *MK* conocido por el servidor;
- una etapa para producir una etiqueta *t* para caracterizar el criptoperiodo *cp* a partir del cual se ha producido el contenido codificado *C* y permitir al dispositivo producir y suministrar una palabra de control rastreable según la invención;
- una etapa para calcular y suministrar una cabecera *H* para permitir la descodificación del contenido codificado por el terminal según la invención;
- una etapa para suministrar conjuntamente dicho contenido codificado *C*, la cabecera *H* y dicha etiqueta *t*.

Para llevar a la práctica tal procedimiento, la invención prevé adaptar los medios de procesamiento de un servidor para que los mismos pongan en práctica dicho procedimiento para producir y suministrar un contenido codificado *C* a partir de un contenido en claro, de un criptoperiodo *cp* y de un secreto *MK*, una etiqueta *t* y una cabecera *H*.

La invención prevé un sistema de acceso condicional a un contenido digital que incluye un servidor, un terminal y un dispositivo electrónico respectivamente conformes a la invención.

Esta se refiere además a un procedimiento de acceso condicional a un contenido digital que incluye:

- una etapa para elaborar y suministrar, por parte de un servidor, un contenido codificado *C*, una etiqueta *t* y una cabecera *H* de acuerdo con la invención;
- una etapa para receptar, por parte de un terminal, dichos contenido codificado *C*, etiqueta *t* y la cabecera *H*;
- una etapa para transmitir la etiqueta *t* por parte del terminal a un dispositivo que coopera con dicho terminal;
- una etapa para producir y suministrar, por parte de dicho dispositivo al terminal, una palabra de control rastreable $k_{i,cp}$ de acuerdo con la invención;
- una etapa para descodificar, por parte del terminal, el contenido codificado *C* y producir un contenido en claro *M* según la invención;
- una etapa para restituir dicho contenido en claro *M* por medio de una interfaz adaptada a dicho contenido en claro.

Para observar una red pirata e identificar un dispositivo electrónico explotado de manera fraudulenta, la invención prevé un procedimiento para rastrear una palabra de control $k_{p,cp}$ producida por un dispositivo de abonado traidor que pone en práctica un procedimiento para producir una palabra de control rastreable según la invención. Tal procedimiento para rastrear incluye:

- una etapa para recabar la palabra de control $k_{p,cp}$;
- una etapa para recabar una utilidad o programa de descifrado pirata apto para descodificar un contenido codificado con el concurso de dicha palabra de control $k_{p,cp}$;
- una etapa para determinar un identificador $i = p$ de un dispositivo que haya producido $k_{p,cp}$ consistente en:
  i. interpretar la utilidad o programa de descifrado para diseñar un programa equivalente que expresa un conjunto de instrucciones en forma de operaciones algebraicas y anexas incluyendo cada una de ellas al menos una variable de entrada y al menos una variable de salida;
  ii. fijar las variables de entrada a constantes para las cuales el programa equivalente descodifica correctamente el contenido codificado;
  iii. simplificar dicho programa equivalente para que el mismo no incluya más que una secuencia de instrucciones sin salto;
  iv. convertir el programa equivalente simplificado a un sistema de ecuaciones multivariable para la puesta en práctica de transformaciones algebraicas;
  v. invertir en su totalidad o en parte dicho sistema de ecuaciones multivariable para identificar el dispositivo traidor.

Otras características y ventajas se pondrán más claramente de manifiesto con la lectura de la descripción que sigue y con la detenida observación de las figuras que la acompañan, de las cuales:

la figura 1 presenta un sistema de acceso condicional según el estado de la técnica;

la figura 2 presenta un modo de piratería de contenidos multimedia protegidos y difundidos por medio de un sistema de acceso condicional según el estado de la técnica;

las figuras 3 y 3a describen respectivamente dos formas de realización de un sistema de acceso condicional conforme a la invención;

la figura 4 describe la puesta en práctica, según la invención, de un procedimiento para observar una red pirata e identificar un dispositivo electrónico explotado de manera fraudulenta o dispositivo traidor;

la figura 5 ilustra la arquitectura funcional de un dispositivo electrónico de abonado conforme a la invención;

las figuras 5a y 5b ilustran respectivamente dos formas de realización de un procedimiento para producir una palabra de control de acuerdo con la invención;

la figura 6 describe una primera forma preferida de realización de un procedimiento para descodificar un contenido codificado, de acuerdo con la invención;

la figura 7 describe una primera forma preferida de realización de un procedimiento para codificar un contenido en claro, de acuerdo con la invención;

la figura 8 describe una primera forma preferida de realización de un procedimiento para generar un secreto para poner en práctica un sistema de acceso condicional, de acuerdo con la invención; y

la figura 9 describe una forma de realización de un procedimiento de acceso condicional conforme a la invención.

La figura 1 permite presentar un sistema de acceso condicional a un contenido digital según el estado de la técnica. Consiste en una red de difusión 4 puesta en práctica por un operador de difusión de contenidos protegidos. De este modo, desde un servidor de contenidos 3, son emitidos conjuntamente palabras de control *c* y contenidos *C* respectivamente cifrados y codificados. El servidor 3 codifica para ello un contenido en claro *M* por medio de una función de codificación *enc* y de una palabra de control *k*, siendo producida esta última por dicho servidor 3. Se obtiene de este modo un contenido codificado *C* tal que $C = enc(k,M)$. Asimismo, se emite o “radiodifunde” una cifra *c* de la palabra de control *k* junto 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 $c = E(k)$.

Las palabras de control cifradas *c* y los contenidos cifrados *C* son transmitidos, por intermedio de la red de difusión 4, a unos terminales 2a a 2m. Estos últimos son los encargados de respectivamente descodificar en tiempo real los contenidos codificados *C* emitidos por el servidor 3. De este modo, un terminal -tal como por ejemplo el descodificador 2a- pone en práctica una función de descodificación *dec* y la aplica al contenido codificado *C* para obtener el contenido en claro *M*. Este último puede ser visualizado utilizando un televisor de salón 5 o cualquier otra interfaz adaptada para restituir el contenido en claro. Para aplicar la función de descodificación *dec*, un terminal tiene que conocer el valor de la palabra de control *k* que ha sido utilizada por el servidor 3 para codificar el contenido *M*.

De acuerdo con el estado de la técnica y de conformidad 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 1a a 1m, generalmente específico de un abonado. El terminal 2a, a través de la red 4, recibe regularmente parejas *(C,c)* y transmite a un dispositivo 1a las palabras de control cifradas *c*. El dispositivo 1a puede descifrar una palabra de control cifrada *c* por medio de una función de descifrado *D* para obtener la palabra de control *k* que ha servido para codificar un contenido *M*. De este modo, *k = D(c)*. Lo mismo ocurre para cualquier otro terminal, tal como 2b a 2m, cooperando cada uno de ellos respectivamente con un 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, tal como el dispositivo 1a a 1m, pone en práctica una función recíproca de descifrado *D*, tal como *k = D(Kd,k*) donde *Kd* es una clave de descifrado conocida por el dispositivo. Según las funciones de cifrado *E* y de descifrado *D*, las claves *Kc* y *Kd* pueden ser idénticas. Tal es el caso de un cifrado / descifrado simétrico. Como variante, de acuerdo con un esquema llamado de "*broadcast encryption*", *Kc* es una clave pública o secreta específica del operador y *Kd* es una clave secreta específica del dispositivo y conocida por el operador. Así, de acuerdo con esta variante, existen varias claves individuales de descifrado y cada uno de los dispositivos emitidos y entregados de manera lícita a los abonados de dicho operador dispone de tal clave de descifrado individual.

La figura 2 permite ilustrar un escenario por el cual una organización pirata, a la que llamaremos "pirata", consigue realizar un comercio fraudulento de contenidos protegidos.

De acuerdo con este primer escenario, el pirata ha contratado con toda normalidad una suscripción con un operador de contenidos. Así, puede disponer de un dispositivo electrónico de abonado, tal como una tarjeta inteligente 1a. Además, el pirata está en posesión de un terminal 2P, llamado terminal pirata. Este terminal puede recibir parejas *(C,c)* desde una red de difusión 4 tal como la descrita en relación con la figura 1. El terminal 2P puede cooperar con dicho dispositivo 1a para transmitirle las palabras de control cifradas *c*. De vuelta, el dispositivo 1a produce la palabra de control *k* descifrando la cifra *c* por medio de una función de descifrado *D*. Con toda normalidad, el dispositivo 1a suministra al terminal 2P la palabra de control *k*. Según este primer escenario, el terminal pirata 2P puede emitir entonces, a través de una red pirata 6, las palabras de control *k* en tiempo real. Un usuario desaprensivo que haya "contratado" una suscripción 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, contenidos codificados *C* (flecha de puntos) y, por otra, desde la red pirata 6, las palabras de control *k* asociadas, en claro. El terminal 2w puede realizar la descodificación de los contenidos codificados *C* y suministrar los contenidos en claro *M* para que puedan ser restituidos.

Asimismo, un pirata puede contratar una pluralidad de suscripciones con uno o varios operadores. Entonces, un terminal pirata 2P puede cooperar simultáneamente con una pluralidad de dispositivos de abonado 1a a 1z y poner en práctica un algoritmo de gestión de dichos dispositivos más o menos complejo. Por ejemplo, el terminal pirata transmite una palabra de control *k* descifrada mayoritariamente por los dispositivos 1a a 1z. Como variante, tal terminal 2P puede interrogar aleatoriamente uno u otro dispositivo electrónico, etc.

Un pirata, como variante, eventualmente puede cifrar o codificar, según un procedimiento propietario, las palabras de control *k* emitidas en una red pirata. De este modo, se puede transmitir, en dicha red pirata, una cifra $c_p = E_p(k)$ - siendo E_p una función de cifrado propietaria del pirata. Un terminal 2w incluye, en este caso, funciones de descifrado D_p recíprocas para, al final, suministrar los contenidos en claro esperados.

La invención permite frustrar estos diferentes escenarios de piratería.

La figura 3 permite ilustrar una primera forma de realización de un sistema de acceso condicional a un contenido digital tal y como prevé la invención. Al igual que para un sistema conocido, la invención prevé una red de difusión 4 puesta en práctica por un operador de difusión de contenidos protegidos. Desde un servidor de contenidos 3, se emiten contenidos codificados *C*. Para ello, el servidor 3 codifica un contenido en claro *M* por medio de una función de codificación *enc*. Se obtiene de este modo un contenido codificado *C* tal que *C = enc(M)*. Asimismo, se emite o "radiodifunde" una etiqueta *t* junto con el contenido codificado *C*. Esta etiqueta contiene datos relativos especialmente al criptoperiodo en curso. Además puede contener datos referentes al contenido o directrices que el servidor desea emitir por la red 4 con destino a uno o varios dispositivos de abonado 1a a 1m respectivamente cooperantes con unos terminales 2a a 2m aptos para recibir los elementos difundidos por intermedio de la red 4. De acuerdo con esta primera forma de realización, se difunde asimismo una cabecera *H* conjuntamente con el contenido codificado *C* y con la etiqueta *t*. Por su parte, esta cabecera será explotada principalmente por cualquier terminal para descodificar un contenido codificado.

Los descodificadores 2a a 2m son los encargados de respectivamente descodificar en tiempo real los contenidos codificados *C* emitidos por el servidor 3. De este modo, un terminal -tal como por ejemplo el descodificador 2a- pone en práctica una función de descodificación *dec* y la aplica al contenido codificado *C* para obtener el contenido en claro *M*. Este último puede ser visualizado utilizando un televisor de salón 5 o cualquier otra interfaz adaptada para restituir el contenido en claro. Para aplicar la función de descodificación *dec*, un terminal tiene que conocer el valor de la cabecera *H* así como el valor de una palabra de control $k_{a,cp}$ producida y suministrada por el dispositivo electrónico seguro de abonado 1a que coopera con el terminal 2a. Lo mismo ocurre para cualquier otro terminal, tal

como los terminales 2b a 2m, cooperando cada uno de ellos respectivamente con los dispositivos 1b a 1m. Las palabras de control $k_{i,cp}$ suministradas por un dispositivo de abonado 1i son producidas con el concurso de las etiquetas *t* transmitidas desde el servidor 3 por intermedio de los terminales, de un identificador *i* específico del dispositivo de abonado 1i y de un secreto SK_i, estando memorizados *i* y SK_i en el dispositivo de abonado 1i. Así, cada palabra de control es propia de un dispositivo de abonado particular. De este modo, $k_{i,cp}$ es propia de y específica del dispositivo 1i. Además, esta palabra de control $k_{i,cp}$ es diferente de las demás palabras de control específicas de los demás dispositivos de abonado. Así, para descodificar un contenido codificado *C*, un terminal 2i pone en práctica una función de descodificación *dec* tal que $M = dec(k_{i,cp},C,H)$, siendo *M* el contenido en claro.

De acuerdo con una variante de realización ilustrada en relación con la figura 3a, un servidor 3 puede transmitir tan solo, a través de la red 4, el contenido codificado *C* y la etiqueta *t* que caracteriza el criptoperiodo en curso *cp* con destino a unos terminales, entre ellos el terminal 2i. En este caso, la elaboración de la cabecera *H* necesaria para la descodificación la realiza el dispositivo de abonado 1i cooperante con el terminal 2i -de una manera similar a la efectuada por el servidor 3 descrito en relación con la figura 3. Esta variante permite reducir el ancho de banda necesario para la radiodifusión (*broadcast*) de los contenidos codificados.

Cualquiera que sea la forma de realización (descrita en relación con las figuras 3 ó 3a), la invención permite llevar a la práctica un sistema de acceso condicional que previene el riesgo del "*control-word sharing*". En efecto, las palabras de control utilizadas por los descodificadores para descodificar los contenidos codificados son rastreables. Estas, efectivamente, dependen cada una de ellas y respectivamente de un identificador específico del dispositivo de abonado que las ha generado y suministrado. Cada palabra de control así producida es propia y específica de un dispositivo de abonado. Para dos dispositivos de abonado 1i y 1j, son producidas dos palabras de control $k_{i,cp}$ y $k_{j,cp}$ respectivamente por los dispositivos 1i y 1j tales que $k_{i,cp} \neq k_{j,cp}$. La figura 4 permite ilustrar una técnica que permite a un operador detectar la utilización fraudulenta de un dispositivo de abonado al que llamaremos "dispositivo traidor". La figura 4 rescata los elementos descritos en relación con la figura 3. De este modo, un terminal pirata 2P recibe tripletas (*C,H,t*) desde una red de difusión 4. El terminal 2P coopera con uno o varios dispositivos 1a a 1z adquiridos de manera lícita y conformes a la invención. Estos producen y suministran palabras de control que dependen especialmente y respectivamente del identificador de cada dispositivo de abonado. De este modo, un dispositivo 1a suministra una palabra de control $k_{a,cp}$ que depende especialmente de su identificador específico *a*. Más adelante estudiaremos un procedimiento para elaborar tal palabra de control (en relación con las figuras 5a y 5b). Para ilustrar el proceso de observación, consideremos que para un operador en posesión de una palabra de control $k_{i,cp}$, le es posible deducir el identificador *i* del dispositivo que ha producido dicha palabra de control $k_{i,cp}$.

El terminal 2P que ha receptado las palabras de control $k_{a,cp}$, $k_{b,cp}$ o $k_{z,cp}$, respectivamente producidas por los dispositivos 2a, 2b, 2z, puede emitir en tiempo real, a través de una red pirata 6, una o varias palabras de control -que señalaremos con $k_{p,cp}$- igual a una de las palabras $k_{a,cp}$, $k_{b,cp}$ o $k_{z,cp}$. Un terminal 2w puede recibir, por una parte, desde la red de distribución 4, contenidos codificados *C* (acompañados de la cabecera *H* y la etiqueta *t*) y, por otra, desde la red pirata 6, palabras de control $k_{p,cp}$ en claro. El terminal 2w puede realizar la descodificación de los contenidos codificados *C* y suministrar los contenidos en claro *M* para que puedan ser visualizados. Un operador puede disponer de medios 9 para observar la red pirata 6. Esta observación puede consistir en percibir una o varias palabras de control $k_{p,cp}$ que transitan por intermedio de la red pirata 6. Basándose en esta observación, un operador consigue identificar al menos un dispositivo traidor utilizado por un descodificador o terminal pirata 2P, de entre los dispositivos 1a a 1z.

Tan pronto como se identifica un dispositivo traidor 1i, el mismo puede ser revocado transmitiendo una petición de revocación tal y como está previsto por la invención (figura 5b) e incluso tomar cualesquiera medidas que estime útiles para detener la utilización del dispositivo traidor.

Para tratar de complicar la tarea al operador que pretender rastrear un dispositivo traidor, la palabra de control puede, como variante, resultar de una mezcla basada en una de dichas palabras de control $k_{a,cp}$, $k_{b,cp}$ o $k_{z,cp}$ con el fin de producir y emitir una $k_{p,cp}$ distinta de dichas $k_{a,cp}$, $k_{b,cp}$ o $k_{z,cp}$. No obstante, la invención prevé una forma de realización para prevenir el uso de tales combinaciones o mezclas con el fin de garantizar la posibilidad de rastreo de los dispositivos de abonado.

Como indica la figura 9, y en relación con la variante descrita en la figura 3, para poner en práctica la invención, un contenido en claro *M* es codificado por un servidor de contenidos 3 con el concurso de una función *enc* tal y como se describe, por ejemplo, en relación con la figura 7 según un procedimiento 410. Este último permite además elaborar una etiqueta *t* que caracteriza especialmente el criptoperiodo en curso *cp*. Es elaborada además una cabecera *H* por dicho servidor 3 (e incluso por los dispositivos de abonado, según la variante de la figura 3a). Las tripletas (*C,H,t*) -o las parejas (*C,t*) según la figura 3a- se transmiten del servidor 3, por intermedio de la red 4, a al menos un terminal 2i que a su vez transmite a un dispositivo de abonado 1i -con el que coopera- dicha etiqueta *t*. De acuerdo con un procedimiento 100 tal y como se describe en relación con la figura 5a, el dispositivo 1i -adaptado como indica la figura 5- produce y suministra una palabra de control propia $k_{i,cp}$ a dicho terminal 2i. Este último descodifica el contenido codificado *C* según una función de descodificación *dec* conforme a un procedimiento tal como el procedimiento 200 descrito a título de ejemplo mediante la figura 6. El contenido en claro *M* así obtenido se puede suministrar mediante una interfaz hombre-máquina 5. Previamente, tal procedimiento de acceso condicional

conforme a la invención incluye una etapa para definir y distribuir a un grupo de dispositivos de abonado un secreto SK_i específico. De acuerdo con una forma particular de realización, los secretos SK_i tienen un valor común e idéntico al de un secreto *MK* compartido con el servidor. Para inicializar tal secreto común, la invención prevé un procedimiento, tal como el ejemplo 400 descrito en relación con la figura 8.

La invención además prevé que una pluralidad de dispositivos de abonado pueda compartir un mismo identificador *i*. Tal pluralidad de dispositivos se asemeja a partir de entonces a un conjunto de "clones" que comparten un mismo identificador *i* e incluso un mismo SK_i. Por medida de simplificación y en el sentido de la invención, la noción de "dispositivo de abonado" cubre, sin distinción alguna, un dispositivo de abonado en una forma individual (un solo dispositivo electrónico) o en una forma plural (una pluralidad de dispositivos que comparten un mismo identificador *i*).

De acuerdo con una primera forma preferida de realización, la invención estriba en la noción matemática de apareamiento en grupos de orden primo. Tal apareamiento es una aplicación bilineal generalmente utilizada en criptografía, especialmente en el ámbito de las curvas elípticas especialmente.

Sea β un grupo bilineal

$$\beta = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e(.,.))$$

de orden *p* primo tal que $|p| = \lambda$, definiendo λ el tamaño de los elementos como parámetro de seguridad. $\mathbb{G}_1$,$\mathbb{G}_2$ y $\mathbb{G}_T$ son tres grupos cíclicos de orden *p* y

$$e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$$

un apareamiento. Un grupo cíclico es un conjunto algebraico tal que g^{p+1} es igual a *g*, definiendo *p* el orden del grupo cíclico y *g*, un elemento del grupo al que se llama "generador". En el sentido de la invención, no se requiere una relación particular entre los grupos $\mathbb{G}_1$ y $\mathbb{G}_2$. Los dos grupos pueden ser idénticos o, más generalmente, puede definirse un isomorfismo Ψ entre $\mathbb{G}_1$ y $\mathbb{G}_2$. La invención prevé que se priorice cualquier eventual isomorfismo así como cualquier apareamiento calculables eficientemente.

El valor SK_i es común y compartido entre todos los dispositivos de abonado. El valor de SK_i es igual a *MK*, dicho secreto $SK_i = MK$ se puede elaborar como indica a título de ejemplo la figura 8. De este modo, un procedimiento 400 para elaborar tal secreto puede consistir en escoger aleatoriamente 402 un generador *g* del grupo $\mathbb{G}_1$ -como indica la notación

$$g \xleftarrow{R} \mathbb{G}_1\text{-}.$$

En 403, tal procedimiento elige además y aleatoriamente γ_0 perteneciente al conjunto $\mathbb{Z}_p$ de los enteros módulo *p*. El secreto *MK* puede definirse 404 entonces como un conjunto de dos componentes respectivamente iguales a *g* y γ_0 -emplearemos la notación $MK = (g,\gamma_0)$ para describir esto. Este procedimiento 400 puede ser llevado a la práctica por un servidor de contenidos tal como el servidor 3 descrito en relación con las figuras 3 y 3a o, como variante, por un servidor específico, transmitiéndose entonces el secreto *MK* a dicho servidor de contenidos que, así, conoce dicho secreto previamente elaborado.

Los medios de procesamiento de un servidor 3 tal y como se describe en relación con las figuras 3 y 3a pueden llevar a la práctica entonces un procedimiento para codificar un contenido en claro *M* y para producir un contenido codificado *C*. Tal procedimiento puede ser conforme al ejemplo del procedimiento 410 descrito en relación con la figura 7.

Así, dicho procedimiento incluye una etapa 414 para producir un contenido codificado *C* a partir de un criptoperiodo *cp* y del secreto *MK* memorizado por el servidor 3.

Incluye además una etapa (no representada) para producir una etiqueta *t* con el fin de caracterizar el criptoperiodo *cp* a partir del cual se ha producido el contenido codificado *C*. Finalmente, incluye una etapa (no representada) para suministrar conjuntamente dicho contenido codificado *C* y dicha etiqueta *t*. Tal procedimiento puede incluir además una etapa previa a la emisión de la etiqueta *t* para asociar a la misma datos que dan fe de su integridad.

De acuerdo con esta primera forma preferida de realización de la invención, la función *enc* para producir el contenido codificado *C* consiste en calcular 411 en primer lugar $\gamma_{cp} = F_0(\gamma_0, c_p)$, siendo F_0 una función determinada y conocida por el servidor 3. El servidor 3 elige 412 un conjunto $s = \{s_j\}_{j=1}^{n}$ de *n* valores pertenecientes cada uno de ellos a $\mathbb{Z}_p$.

Calcula 413 una palabra $K = \{K_j\}_{j=1}^{n}$ cuyas *n* componentes son cada una de ellas iguales a $K_j = e(g,f)^{\frac{1}{\gamma_{cp}+s_j}}$, para todo *j* comprendido entre 1 y *n*, siendo el generador *f* un generador elegido aleatoriamente del grupo $\mathbb{G}_2$, por ejemplo en la etapa 402 del procedimiento según la figura 8 -como indica la notación

$f \xleftarrow{R} \mathbb{G}_2$-.

El servidor aplica 414 una función $F3^{-1}$ a dicha palabra *K* y al contenido en claro *M* para producir el contenido codificado *C*. De acuerdo con un ejemplo de realización, la función $F3^{-1}$ es la o exclusiva. Las componentes de la palabra *K* previamente son concatenadas o mezcladas de manera determinada.

El procedimiento descrito en relación con la figura 7 puede incluir además una etapa 413a para elaborar la cabecera *H* para permitir la descodificación del contenido codificado. Esta variante la pone en práctica un servidor 3 tal y como se describe en relación con la figura 3, que suministra la cabecera *H* conjuntamente con el contenido codificado *C* y la etiqueta *t*.

De acuerdo con esta forma de realización, la cabecera *H* puede consistir en un conjunto $H = \{h_j\}_{j=1}^{n}$ de *n* componentes respectivamente iguales a un par de magnitudes $\frac{1}{(f^{\gamma_{cp}+s_j}, s_j)}$ para todo *j* comprendido entre 1 y *n*. El conjunto $s = \{s_j\}_{j=1}^{n}$ de *n* valores es idéntico al conjunto *s* utilizado para elaborar la palabra *K* y *f* es el generador elegido -eventualmente aleatoriamente- entre el grupo $\mathbb{G}_2$ durante la etapa 402 para elaborar el secreto *MK*.

Para llevar a la práctica la invención, es necesario adaptar además los dispositivos electrónicos de abonado. De este modo, la figura 5 permite describir un dispositivo de abonado conforme a la invención. Tal dispositivo 1i incluye unos medios R para recibir del mundo exterior -por ejemplo, de un terminal 2i- una etiqueta *t*.

De acuerdo con una forma de realización de la invención, una etiqueta *t* puede incluir datos que dan fe de su integridad. A título de ejemplo, dichos datos pueden consistir en un código de redundancia tal como un resumen o ser elaborados con el concurso de un secreto *Kd* compartido entre el dispositivo y el servidor. De acuerdo con una variante, tal etiqueta se puede transmitir cifrada desde el servidor después de haber sido elaborada por este último con el concurso de un algoritmo de cifrado simétrico o asimétrico. De acuerdo con estas dos formas de realización, el dispositivo 1i incluye medios de procesamiento 10 que pueden comprobar 11 la integridad de la etiqueta recibida e incluso descifrarla. Si para este uso se necesita un secreto *Kd*, se pueden prever unos medios de memorización 21 en el seno de un dispositivo 1i conforme a la invención para memorizar dicho secreto y cooperar con los medios de procesamiento. Para producir 13 una palabra de control $k_{i,cp}$ propia del dispositivo 1i, los medios de procesamiento 10 cooperan con unos medios 22 para memorizar un identificador *i* específico del dispositivo. Para producir la palabra de control, los medios de procesamiento 10 son aptos para deducir 12 de la etiqueta *t* el criptoperiodo en curso *cp*. Estos cooperan además con unos medios de memorización 23 que memorizan un secreto SK_i. Partiendo del identificador *i*, el criptoperiodo *cp* y del secreto SK_i, los medios de procesamiento del dispositivo producen 13 la palabra de control $k_{i,cp}$. Esta última es suministrada por el dispositivo 1i al mundo exterior (por ejemplo, al terminal 2i) por intermedio de los medios para suministrar S.

Para producir una palabra de control, los medios de procesamiento de un dispositivo 1i conforme a la invención pueden poner en práctica un procedimiento 100 tal como se ilustra mediante la figura 5a.

Tal procedimiento para producir una palabra de control incluye una primera etapa para recibir 101 una etiqueta *t* por intermedio de los medios de recepción R del dispositivo 1i. Incluye además una etapa para determinar 103 el criptoperiodo en curso *cp* explotando la etiqueta *t* recibida y, luego, una etapa para producir 105 una palabra de control $k_{i,cp}$ a partir de dicho criptoperiodo en curso *cp*, del identificador *i* específico del dispositivo y del secreto SK_i - siendo memorizados *i* y SK_i por el dispositivo. El procedimiento incluye asimismo una etapa para suministrar una palabra de control *k'* igual a $k_{i,cp}$ por intermedio de los medios para suministrar S del dispositivo.

De acuerdo con la primera forma preferida de realización que estriba en el grupo bilineal

$$\beta = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e(.,.))$$

de orden *p* primo, un dispositivo de abonado, que pone en práctica un procedimiento 100 tal como se ilustra en relación con la figura 5a, recepta 101 una etiqueta *t* -eventualmente valida 102 su integridad- y luego deduce 103 el criptoperiodo en curso *cp*. En 104, dicho dispositivo pone en práctica una función determinada *F0* (idéntica a aquella puesta en práctica por el servidor de contenidos) que, aplicada a la componente γ_0 del secreto $SK_i = MK$ y al criptoperiodo *cp*, permite generar γ_{cp} que pertenece a $\mathbb{Z}_p$.

El procedimiento 100 incluye entonces una etapa 105 para elaborar la palabra de control $k_{i,cp}$. Esta etapa consiste en calcular un par de magnitudes $x_{i,cp}$ y $A_{i,cp}$. $x_{i,cp}$ pertenece a $\mathbb{Z}_p$ y es calculado por los medios de procesamiento del dispositivo de manera determinística a partir del identificador *i* y del criptoperiodo *cp*. $A_{i,cp}$ es calculado por el dispositivo como igual a $\frac{1}{g^{\gamma_{cp}+x_{i,cp}}}$.

Entonces, el dispositivo 1i que pone en práctica un procedimiento 100 puede suministrar 106 al mundo exterior (tal como un terminal 2i con el que coopera) una palabra de control *k'* igual a $k_{i,cp}$.

La invención prevé, de acuerdo con la variante descrita en relación con la figura 3a, que un dispositivo de abonado conforme a la invención pueda -en sustitución del servidor de contenido 3- producir y elaborar la cabecera *H*. El procedimiento 100 incluye entonces una etapa 105a para elaborar las componentes de dicha cabecera y una etapa 106a para suministrar al terminal con el que coopera dicha cabecera. La etapa 105a es similar a la etapa 413a anteriormente descrita y puesta en práctica por un servidor 3 según las figuras 3 y 7.

De este modo, la etapa 105a puesta en práctica por un dispositivo de abonado, tal y como se describe en relación con la figura 3a, puede consistir en calcular un conjunto $H = \{h_j\}_{j=1}^{n}$ de *n* componentes respectivamente iguales a un par de magnitudes $\frac{1}{(f^{\gamma_{cp}+s_j}, s_j)}$ para todo *j* comprendido entre 1 y *n*. Para determinar el conjunto $s = \{s_j\}_{j=1}^{n}$ de *n* valores idéntico al conjunto *s* utilizado para elaborar la palabra *K* por el servidor 3 (etapa 413 de la figura 7) y para elegir el generador *f* entre el grupo $\mathbb{G}_2$ (durante la etapa 402 al margen de la elaboración del secreto *MK*), la invención prevé que la etiqueta *t* incluya datos que caractericen dichas elecciones. Como variante, dichos conjunto $s = \{s_j\}_{j=1}^{n}$ y generador *f* son predeterminados y compartidos entre el servidor y el conjunto de los dispositivos de abonado.

Para descodificar un contenido codificado *C*, los medios de procesamiento de un terminal 2i, tal como se representa en relación con las figuras 3 ó 3a, cooperan con unos medios para memorizar los parámetros del grupo bilineal *β*. Estos ponen en práctica una función de descodificación *dec* -tal como la descrita en relación con la figura 6- para producir un contenido en claro *M*.

Tal procedimiento 200 lo ponen en práctica los medios de procesamiento del terminal a consecuencia de la recepción, desde el mundo exterior, de un contenido codificado *C*, de una cabecera *H* y de una palabra de control $k_{i,cp}$. Incluye una etapa para aplicar 201 una primera función *F*1 a la cabecera *H* y a la palabra de control $k_{i,cp}$ para producir 203 una palabra *K*. El procedimiento 200 incluye además una etapa para aplicar 204 una segunda función *F*3 a dicha palabra *K* y al contenido codificado *C* para producir el contenido en claro *M*. De acuerdo con esta forma de realización, la función $F3^{-1}$, puesta en práctica por el servidor para codificar el contenido, es una función inversa de la función *F*3. Así, el terminal puede suministrar 205 dicho contenido en claro *M*. De acuerdo con una forma de realización, los medios de procesamiento del terminal pueden poner en práctica una función de expansión *F*2 para adaptar el formato de la palabra *K* antes de la aplicación de la función *F*3.

De este modo, de acuerdo con la primera forma de realización preferida de la invención que estriba en un grupo bilineal

$$\beta = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e(.,.))$$

de orden *p* primo, recuérdese que la palabra de control $k_{i,cp}$ incluye dos componentes $x_{i,cp}$ y $A_{i,cp}$, habiéndose calculado $x_{i,cp}$ directamente a partir del identificador *i* del dispositivo de abonado que ha producido y suministrado dicha palabra de control. Recuérdese además que la cabecera *H* consiste en un conjunto de componentes h_j respectivamente iguales a $\frac{1}{(f^{\gamma_{cp}+s_j}, s_j)}$ para todo *j* comprendido entre 1 y *n*. La etapa para producir 203 la palabra *K* consiste a partir de entonces en poner en práctica una aplicación bilineal

$$e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$$

para la cual $\mathbb{G}_1$, $\mathbb{G}_2$ y $\mathbb{G}_T$ son tres grupos cíclicos de orden primo *p*. Esta aplicación bilineal se centra en las componentes de *H* y de $k_{i,cp}$ tal que $K_j = e(A_{i,cp}, (f^{\frac{1}{\gamma_{cp}+s_j}})^{x_{i,cp}-s_j}.f)$ para todo *j* = 1 a *n*, siendo *f* el generador perteneciente al grupo cíclico $\mathbb{G}_2$ de orden *p*.

Mediante la puesta en práctica de la propiedad de bilinealidad, $K_j = e(A_{i,cp}, (f^{\frac{1}{\gamma_{cp}+s_j}})^{x_{i,cp}-s_j}.f) = e(g,f)^{\frac{1}{\gamma_{cp}+s_j}}$. Podemos comprobar que esta propiedad permite suprimir la contribución de la magnitud $x_{i,cp}$ que depende directamente del identificador *i* específico del dispositivo de abonado 1i que ha producido y suministrado la palabra de control $k_{i,cp}$.

Para producir el contenido en claro *M*, la etapa 204 para aplicar la función *F*3 a dichas componentes de la palabra *K* y al contenido codificado *C* consiste en aplicar la función *F*3 a las componentes previamente agregadas 203 -concatenadas o mezcladas de una manera similar a la agregación realizada en la etapa 414 en la codificación del contenido por el servidor. A título de ejemplo, la función *F*3 puede consistir en la o exclusiva -siendo entonces idénticas las funciones *F*3 y $F3^{-1}$.

La eventual puesta en práctica de la función de expansión *F*2 -etapa 202- puede consistir, según el ejemplo de realización preferido de la invención, en adaptar el tamaño de las salidas de cada aplicación de la función *F*1 a una componente K_j para hacerla compatible con la aplicación de la función *F*3 entre la agregación de dichas componentes K_j^* así adaptadas mediante *F*2 y el contenido codificado *C*.

La invención prevé una segunda forma preferida de realización que igualmente estriba en la noción matemática de

apareamiento en grupos de orden primo. De acuerdo con esta segunda forma de realización, el valor del secreto SK_i memorizado en cada dispositivo de abonado es distinto y depende especialmente del valor del identificador *i* de este último.

Sea β un grupo bilineal

$$\beta = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e(.,.))$$

de orden *p* primo tal que $|p| = \lambda$, definiendo λ el tamaño de los elementos como parámetro de seguridad. $\mathbb{G}_1$, $\mathbb{G}_2$ y $\mathbb{G}_T$ son tres grupos cíclicos de orden *p* y

$$e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$$

un apareamiento. No se requiere una relación particular entre los grupos $\mathbb{G}_1$ y $\mathbb{G}_2$. Los dos grupos pueden ser idénticos o, más generalmente, puede definirse un isomorfismo Ψ entre $\mathbb{G}_1$ y $\mathbb{G}_2$. La invención prevé que se priorice cualquier eventual isomorfismo así como cualquier apareamiento calculables eficientemente.

El valor del secreto *MK* conocido por el servidor puede consistir en elegir aleatoriamente dos generadores *g* y *f* respectivamente de los grupos $\mathbb{G}_1$ y $\mathbb{G}_2$ -como indican las notaciones

$$g \xleftarrow{R} \mathbb{G}_1$$

y

$$f \xleftarrow{R} \mathbb{G}_2\text{-}.$$

Se elige, además y aleatoriamente, γ perteneciente al conjunto $\mathbb{Z}_p$ de los enteros módulo *p*. El secreto *MK* puede definirse entonces como un conjunto de tres componentes respectivamente iguales a *g*, γ y *f* -emplearemos la notación $MK = (g,\gamma,f)$ para describir esto.

Para generar una pareja de secretos SK_i y DK_i, destinados a ser memorizados respectivamente en el dispositivo de abonado 1i y en el terminal 2i cooperante con este último, el servidor 3 puede poner en práctica el siguiente procedimiento. Se elige x_i perteneciente a $\mathbb{Z}_p$ y se calcula la magnitud $B_i = f^{\frac{1}{\gamma+x_i}}$. Un secreto SK_i puede definirse como un conjunto de dos componentes respectivamente iguales a x_i y B_i -emplearemos la notación $SK_i = (x_i,B_i)$ para describir esto. Un secreto DK_i se define por ser igual a $DK_i = g^{\frac{x_i}{\gamma+x_i}}$.

Los medios de procesamiento de un servidor 3 tal y como el descrito en relación con las figuras 3 y 3a pueden llevar a la práctica entonces un procedimiento para codificar un contenido en claro *M* y para producir un contenido codificado *C*.

Tal procedimiento puede incluir una etapa para producir un contenido codificado *C* a partir de un criptoperiodo *cp* y del secreto *MK* conocido o memorizado por el servidor 3.

Para un criptoperiodo *cp*, tal procedimiento incluye además una etapa para producir una etiqueta $t = t_{cp}$ con el fin de caracterizar el criptoperiodo *cp* a partir del cual se ha producido el contenido codificado *C*. A título de ejemplo y de acuerdo con la segunda forma preferida de realización, dicha etapa para producir $t = t_{cp}$ consiste en elegir -eventualmente aleatoriamente- y_{cp} entre el conjunto $\mathbb{Z}_p$ y generar una magnitud $f_{cp} = f^{\frac{1}{\gamma+y_{cp}}}$. La etiqueta $t = t_{cp}$ consiste en un par de dos magnitudes respectivamente iguales a y_{cp} y f_{cp}^{-1} tal que $t = t_{cp} = (y_{cp}, f_{cp}^{-1})$. Tal procedimiento puede incluir además una etapa previa a la emisión de la etiqueta *t* para asociar a la misma datos que dan fe de su integridad.

La función *enc* para producir el contenido codificado *C* consiste en elegir en primer lugar -eventualmente aleatoriamente- un conjunto $s = \{s_j\}_{j=1}^{n}$ de *n* valores pertenecientes cada uno de ellos a $\mathbb{Z}_p$. Se calcula a continuación una palabra $K = \{K_j\}_{j=1}^{n}$ cuyas *n* componentes son respectivamente iguales a $K_j = e(g,f_{cp})^{sj}$ para todo *j* comprendido entre 1 y *n*.

El servidor aplica una función $F3^{-1}$ a dicha palabra *K* y al contenido en claro *M* para producir el contenido codificado *C*. De acuerdo con un ejemplo de realización, la función $F3^{-1}$ es la o exclusiva. Las componentes de la palabra *K* previamente son concatenadas o mezcladas de manera determinada.

El procedimiento puesto en práctica por el servidor puede incluir además una etapa para elaborar la cabecera *H* para, al final, permitir la descodificación del contenido codificado por un terminal. Esta variante la pone en práctica un servidor 3 tal y como se describe en relación con la figura 3, que suministra la cabecera *H* conjuntamente con el contenido codificado *C* y la etiqueta *t*.

De acuerdo con esta forma de realización, la cabecera *H* puede consistir en un conjunto $H = \{h_j\}_{j=1}^{n}$ de *n* componentes respectivamente iguales a un par de magnitudes *($h_{j,1}$, $h_{j,2}$)*. Para todo *j* comprendido entre 1 y *n*, $h_{j,1} = g^{s_j \cdot \gamma}$ y $h_{j,2} = f_{cp}^{sj}$, siendo el conjunto $s = \{s_j\}_{j=1}^{n}$ de *n* valores idéntico al conjunto utilizado para elaborar la palabra *K*.

Para poner en práctica la invención según esta segunda forma preferida de realización, es preciso adaptar además los dispositivos electrónicos de abonado. Tal dispositivo 1i -tal y como se describe en relación con la figura 5- incluye unos medios 23 para memorizar el valor del secreto SK_i tal y como es elaborado por el servidor. Incluye además unos medios 13 para producir una palabra de control $k_{i,cp}$ de acuerdo con un procedimiento que, por ejemplo, incluye una primera etapa para recibir una etiqueta *t* por intermedio de los medios de recepción R del dispositivo 1i. Incluye además una etapa para determinar el criptoperiodo en curso *cp* explotando la etiqueta $t = t_{cp}$ recibida y, luego, una etapa para producir una palabra de control $k_{i,cp}$ a partir de dicho criptoperiodo en curso *cp*, del identificador *i* específico del dispositivo y del secreto SK_i -siendo memorizados *i* y SK_i por el dispositivo. El procedimiento incluye asimismo una etapa para suministrar una palabra de control *k'* igual a $k_{i,cp}$ por intermedio de los medios para suministrar S del dispositivo.

De acuerdo con la segunda forma preferida de realización que estriba en el grupo bilineal

$$\beta = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e(.,.))$$

de orden *p* primo, un dispositivo de abonado 1i incluye un secreto $SK_i = (x_i, B_i)$. La etiqueta $t = t_{cp}$ recibida es igual a $t = t_{cp} = (y_{cp}, f_{cp}^{-1})$, siendo c_p el criptoperiodo en curso.

Un procedimiento para producir $k_{i,cp}$ consiste en calcular

$$k_{i,cp} = (B_i . f_{cp}^{-1})^{\frac{1}{y_{cp}-x_i}} = (f^{\frac{1}{\gamma+x_i}} . f^{\frac{-1}{\gamma+y_{cp}}})^{\frac{1}{y_{cp}-x_i}} = f^{\frac{1}{(\gamma+y_{cp}).(\gamma+x_i)}} = f_{cp}^{\frac{1}{(\gamma+x_i)}}.$$

Entonces, el dispositivo 1i que pone en práctica tal procedimiento puede suministrar al mundo exterior (tal como un terminal 2i con el que coopera) una palabra de control *k'* igual a $k_{i,cp}$.

La invención prevé, de acuerdo con la variante descrita en relación con la figura 3a, que un dispositivo de abonado conforme a la invención pueda -en sustitución del servidor de contenido 3- producir y elaborar la cabecera *H* tal y como se ha definido anteriormente.

Para descodificar un contenido codificado *C*, los medios de procesamiento de un terminal 2i, tal como se representa en relación con las figuras 3 ó 3a, ponen en práctica una función de descodificación *dec* para producir un contenido en claro *M*. Tal descodificador 2i incluye además unos medios para memorizar el valor del secreto DK_i elaborado por el servidor así como los parámetros del grupo bilineal *β*.

Un procedimiento puesto en práctica por los medios de procesamiento del terminal a consecuencia de la recepción, desde el mundo exterior, de un contenido codificado *C*, de una cabecera *H* y de una palabra de control $k_{i,cp}$ incluye una primera etapa para producir una palabra $K = \{K_j\}_{j=1}^{n}$. De acuerdo con la segunda forma preferida de realización, recuérdese que la cabecera *H* elaborada por el servidor o, como variante, por el dispositivo de abonado, consiste en un conjunto $H = \{h_j\}_{j=1}^{n}$ de *n* componentes respectivamente iguales a un par de magnitudes ($h_{j,1}$, $h_{j,2}$).

De este modo, la etapa para producir la palabra *K* consiste, para todo *j* comprendido entre 1 y *n*, en elaborar

$$K_j = e(DK_i, h_{j,2}) . e(h_{j,1}, k_{i,cp}) = e\left(g^{\frac{x_i}{\gamma+x_i}}, f_{cp}^{s_j}\right) . e\left(g^{s_j \cdot \gamma}, f_{cp}^{\frac{1}{(\gamma+x_i)}}\right),$$

a saber

$$K_j = e(g, f_{cp})^{\frac{s_j x_i}{\gamma+x_i}} . e(g, f_{cp})^{\frac{s_j \cdot \gamma}{\gamma+x_i}} = e(g, f_{cp})^{s_j}.$$

Podemos comprobar que se suprime la contribución de la magnitud x_i -que depende directamente del identificador *i* específico del dispositivo de abonado 1i que ha producido y suministrado la palabra de control $k_{i,cp}$.

Para producir el contenido en claro *M*, el procedimiento incluye además una etapa para aplicar una función *F*3 a la palabra *K* y al contenido codificado *C*. Esto equivale a aplicar la función *F*3 a las componentes de la palabra $K = \{K_j\}_{j=1}^{n}$ previamente agregadas -concatenadas o mezcladas de una manera similar a la agregación realizada en la codificación del contenido por el servidor. A título de ejemplo, la función *F*3 puede consistir en la o exclusiva -siendo entonces idénticas las funciones *F*3 y $F3^{-1}$.

En relación con la figura 4, para prevenir el uso de una palabra de control $k_{p,cp}$ -emitida por un pirata- resultante de una mezcla basada en una de las palabras de control $k_{a,cp}$, $k_{b,cp}$ o $k_{z,cp}$, la invención prevé una forma preferida de realización que asimismo estriba en la noción matemática de apareamiento en grupos de orden primo.

Sea β un grupo bilineal

$$\beta = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e(.,.))$$

de orden p primo tal que $|p| = \lambda$, definiendo λ el tamaño de los elementos como parámetro de seguridad. $\mathbb{G}_1$, $\mathbb{G}_2$ y $\mathbb{G}_T$ son tres grupos cíclicos de orden p y

$$e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$$

un apareamiento. No se requiere una relación particular entre los grupos $\mathbb{G}_1$ y $\mathbb{G}_2$. Los dos grupos pueden ser idénticos o, más generalmente, puede definirse un isomorfismo Ψ entre $\mathbb{G}_1$ y $\mathbb{G}_2$. La invención prevé que se priorice cualquier eventual isomorfismo así como cualquier apareamiento calculables eficientemente. De acuerdo con esta tercera forma de realización, se define además un parámetro T que determina el tamaño máximo de una coalición autorizada.

Al igual que para la primera forma preferida de realización, cada dispositivo de abonado memoriza un secreto cuyo valor $SK_i = MK$ es común y compartido entre un grupo de dispositivos de abonado y es conocido por el servidor de contenidos.

El valor de dicho secreto MK puede consistir en elegir, eventualmente aleatoriamente, un generador g_0 del grupo $\mathbb{G}_1$. Se elige además -eventualmente aleatoriamente- γ perteneciente al conjunto $\mathbb{Z}_p$ de los enteros módulo p. El secreto MK puede definirse entonces como un conjunto de dos componentes respectivamente iguales a g_0 y γ - emplearemos la notación $MK = (g_0, \gamma)$ para describir esto.

Los medios de procesamiento de un servidor 3, tal y como se describe en relación con las figuras 3 y 3a, pueden poner entonces en práctica un procedimiento para codificar un contenido en claro M y para producir un contenido codificado C a partir de un criptoperiodo cp y del secreto MK conocido o memorizado por el servidor 3.

Para un criptoperiodo cp, tal procedimiento incluye una primera etapa para producir una etiqueta $t = t_{cp}$ con el fin de caracterizar el criptoperiodo cp a partir del cual se va a producir el contenido codificado C. Tal procedimiento puede incluir además una etapa previa a la emisión de la etiqueta t para asociar a la misma datos que dan fe de su integridad.

Para producir un contenido C, el procedimiento incluye una etapa para aplicar una función determinada F_0 al generador g_0 y al criptoperiodo cp para producir $g_{cp} = F_0(g_0, cp)$ perteneciente al grupo $\mathbb{G}_1$. Incluye además una etapa para elegir -eventualmente aleatoriamente- $r = \{r_{j,l}\}_{\substack{j=1 \\ l=1}}^{\substack{j=n \\ l=T}}$ y $s = \{s_j\}_{j=1}^{n}$ dos conjuntos de elementos de $\mathbb{Z}_p$.

Incluye una etapa para calcular una palabra $K = \{K_j\}_{j=1}^{n}$ cuyas n componentes son respectivamente iguales a $K_j = e(g_{cp}, f)^{\frac{s_j}{(\gamma + r_{j,1}) \cdots (\gamma + r_{j,T})}}$ para todo j comprendido entre 1 y n, siendo f un generador de $\mathbb{G}_2$.

El servidor aplica una función $F3^{-1}$ a dicha palabra K y al contenido en claro M para producir el contenido codificado C. De acuerdo con un ejemplo de realización, la función $F3^{-1}$ es la o exclusiva. Las componentes de la palabra K previamente son concatenadas o mezcladas de manera determinada.

El procedimiento puesto en práctica por el servidor puede incluir además una etapa para elaborar una cabecera H para, al final, permitir la descodificación del contenido codificado por un terminal. Esta variante la pone en práctica un servidor 3 tal como el descrito en relación con la figura 3, que suministra la cabecera H conjuntamente con el contenido codificado C y la etiqueta t.

De acuerdo con esta forma de realización, la cabecera H puede consistir en un conjunto $H = \{h_j\}_{j=1}^{n}$ de n componentes respectivamente iguales a una cuaterna de magnitudes $\left(\{P_l\}_{l=1}^{T}, \{r_{j,l}\}_{l=1}^{T}, g_{cp}^{\gamma . s_j}, P_T^{s_j}\right)$. Para todo j comprendido entre 1 y n,

$$P_1 = f^{\frac{1}{\gamma + r_{j,1}}}, \qquad P_2 = f^{\frac{1}{(\gamma + r_{j,1})(\gamma + r_{j,2})}}, \qquad \ldots \qquad P_T = f^{\frac{1}{(\gamma + r_{j,1})(\gamma + r_{j,T})}},$$

siendo el conjunto $r = \{r_{j,l}\}_{\substack{j=1\\l=1}}^{\substack{j=n\\l=T}}$ idéntico al conjunto *r* utilizado para elaborar la palabra *K*. El conjunto *s*, los generadores g_{cp} y *f* así como *T* son igualmente idénticos a los elementos utilizados para elaborar la palabra *K*.

Para poner en práctica la invención según esta tercera forma preferida de realización, es preciso adaptar además los dispositivos electrónicos de abonado. Tal dispositivo 1i -tal y como se describe en relación con la figura 5- incluye unos medios 23 para memorizar el valor del secreto $SK_i = MK$ elaborado por el servidor o simplemente conocido por el mismo. Incluye además unos medios 13 para producir una palabra de control $k_{i,cp}$ de acuerdo con un procedimiento que, por ejemplo, incluye una primera etapa para recibir una etiqueta *t* por intermedio de los medios de recepción R del dispositivo 1i. Incluye además una etapa para determinar el criptoperiodo en curso *cp* explotando la etiqueta $t = t_{cp}$ recibida y, luego, una etapa para producir una palabra de control $k_{i,cp}$ a partir de dicho criptoperiodo en curso *cp*, del identificador *i* específico del dispositivo y del secreto SK_i -siendo memorizados *i* y SK_i por el dispositivo de abonado. El procedimiento incluye asimismo una etapa para suministrar una palabra de control *k'* igual a $k_{i,cp}$ por intermedio de los medios para suministrar S del dispositivo.

De acuerdo con esta tercera forma preferida de realización que estriba en el grupo bilineal

$$\beta = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e(.,.))$$

de orden *p* primo, un dispositivo de abonado 1i incluye un secreto $SK_i = MK = (g_0, \gamma)$. La etiqueta $t = t_{cp}$ recibida permite caracterizar y, por tanto, deducir el criptoperiodo en curso *cp*.

Un procedimiento para producir $k_{i,cp}$ consiste en primer lugar en producir g_{cp} aplicando una función F_0 -idéntica a la función puesta en práctica por el servidor- a g_0 y *cp* tal que $g_{cp} = F_0(g_0, cp)$.

Adicionalmente, dicho procedimiento incluye una etapa para producir -de manera determinística y conocida por el servidor- una magnitud $x_{i,cp}$, elemento de $\mathbb{Z}_p$, que depende del identificador *i* del dispositivo y del criptoperiodo en curso *cp*. Como variante, $x_{i,cp} = x_i$ se calcula para depender del identificador *i* pero no de *cp*. La etapa para producir la palabra de control rastreable $k' = k_{i,cp}$ consiste en producir una tripleta $k_{i,cp} = (x_{i,cp}, A_{i,cp}, B_{i,cp})$ para la cual $A_{i,cp} = g_{cp}^{\frac{x_{i,cp}}{\gamma + x_{i,cp}}}$ y $B_{i,cp} = f^{\frac{1}{\gamma + x_{i,cp}}}$.

Entonces, el dispositivo 1i que pone en práctica tal procedimiento puede suministrar al mundo exterior (tal como un terminal 2i con el que coopera) una palabra de control *k'* igual a $k_{i,cp}$.

La invención prevé, de acuerdo con la variante descrita en relación con la figura 3a, que un dispositivo de abonado conforme a la invención pueda -en sustitución del servidor de contenido 3- producir y elaborar la cabecera *H* tal y como se ha definido anteriormente.

Para descodificar un contenido codificado *C*, los medios de procesamiento de un terminal 2i, tal como se representa en relación con las figuras 3 ó 3a, ponen en práctica una función de descodificación *dec* para producir un contenido en claro *M*. Tal descodificador 2i incluye además unos medios para memorizar los parámetros del grupo bilineal β.

Un procedimiento puesto en práctica por los medios de procesamiento del terminal a consecuencia de la recepción, desde el mundo exterior, de un contenido codificado *C*, de una cabecera *H* y de una palabra de control $k_{i,cp}$ incluye una primera etapa para producir una palabra $K = \{K_j\}_{j=1}^{n}$. De acuerdo con esta tercera forma preferida de realización, recuérdese que la cabecera *H* elaborada por el servidor o, como variante, por el dispositivo de abonado consiste en un conjunto $H = \{h_j\}_{j=1}^{n}$ de *n* componentes respectivamente iguales a una cuaterna de magnitudes $\left(\{P_l\}_{l=1}^{T}, \{r_{j,l}\}_{l=1}^{T}, g_{cp}^{\gamma.s_j}, P_T^{s_j}\right)$. Para todo *j* comprendido entre 1 y *n*, $P_1 = f^{\frac{1}{\gamma + r_{j,1}}}, P_2 = f^{\frac{1}{(\gamma + r_{j,1})(\gamma + r_{j,2})}}$, ... $P_T = f^{\frac{1}{(\gamma + r_{j,1})(\gamma + r_{j,T})}}$, perteneciendo el conjunto $r = \{r_{j,l}\}_{\substack{j=1\\l=1}}^{\substack{j=n\\l=T}}$ a $\mathbb{Z}_p$. Recuérdese además que la palabra de control $k_{i,cp}$ consiste en una tripleta $k_{i,cp} = (x_{i,cp}, A_{i,cp}, B_{i,cp})$ para la cual $A_{i,cp} = g_{cp}^{\frac{x_{i,cp}}{\gamma + x_{i,cp}}}$ y $B_{i,cp} = f^{\frac{1}{\gamma + x_{i,cp}}}$.

De este modo, la etapa para producir la palabra *K* consiste, para todo *j* comprendido entre 1 y *n*, en elaborar $K_j = e\left(g_{cp}^{\gamma.s_j}, B_{i,cp}^{\frac{1}{\prod_{l=1}^{T}(\gamma + r_{j,l})}}\right).e\left(A_{i,cp}, P_T^{s_j}\right)$, a saber:

$$K_j = e(g_{cp}, f)^{\frac{s_j.\gamma}{(\gamma + x_{i,cp})\prod_{l=1}^{T}(\gamma + r_{j,l})}}.e(g_{cp}, f)^{\frac{s_j.x_{i,cp}}{(\gamma + x_{i,cp})\prod_{l=1}^{T}(\gamma + r_{j,l})}} = e(g_{cp}, f)^{\frac{s_j}{\prod_{l=1}^{T}(\gamma + r_{j,l})}}$$

con $B_{i,cp}^{\frac{1}{\prod_{l=1}^{T}(\gamma+r_{j,l})}} = \left(B_{i,cp} \cdot \prod_{l=1}^{T} P_l^{(-1)^{i+T.\prod_{m=1}^{l-1}(x_{i,cp}-r_{j,m})}}\right)^{\frac{1}{\prod_{l=1}^{T}(x_{i,cp}-r_{j,l})}}$.

Podemos comprobar que la contribución de la magnitud $x_{i,cp}$ -que depende directamente del identificador *i* específico del dispositivo de abonado 1i que ha producido y suministrado la palabra de control $k_{i,cp}$- ya no aparece en la palabra *K*.

Para producir el contenido en claro *M*, el procedimiento incluye además una etapa para aplicar una función *F*3 a la palabra *K* y al contenido codificado *C*. Esto equivale a aplicar la función *F*3 a las componentes de la palabra $K = \{K_j\}_{j=1}^{n}$ previamente agregadas -concatenadas o mezcladas de una manera similar a la agregación realizada en la codificación del contenido por el servidor. A título de ejemplo, la función *F*3 puede consistir en la o exclusiva -siendo entonces idénticas las funciones *F*3 y $F3^{-1}$.

De acuerdo con una variante, para un *j* dado, los elementos $\{r_{j,l}\}_{l=1}^{T}$ pueden calcularse de manera determinística a partir de una semilla, de modo que solo se transmita esta semilla en la componente h_j de la cabecera *H*. Dicha componente es entonces de tamaño constante e independiente de *T*. Este parámetro *T* puede estar adaptado al nivel de seguridad y a la eficiencia del sistema que interesen.

Ya se elija una de las tres formas preferidas de realización descritas anteriormente o bien, más generalmente, una forma de realización conforme a la invención, el sistema de acceso condicional así constituido utiliza palabras de control $k_{i,cp}$ rastreables, luego detectables por un operador. Así, tal sistema previene cualquier riesgo de *control-word sharing*.

Para ilustrar un método que permite rastrear una palabra de control $k_{i,cp}$ producida de acuerdo con la invención -aunque la palabra de control $k_{p,cp}$ intercambiada por el pirata sea una palabra mezclada o resultante de una colusión de varias palabras de control $k_{a,cp}$, $k_{b,cp}$ o $k_{z,cp}$- consideremos que un pirata suministra a un “abonado” desaprensivo una utilidad de descifrado o programa acompañado de una palabra de control mezclada emitida por una red pirata. Merced a la invención, es posible dar con la identidad de al menos uno de los dispositivos legítimos (o traidores) que han servido para la fabricación de dicha palabra de control mezclada. Esta capacidad, denominada capacidad de rastreo, se puede realizar por medio de un método general llamado de rastreo en caja blanca.

De acuerdo con este método, el descodificador pirata, en primer lugar, es interpretado como una secuencia de instrucciones formales, componiéndose cada instrucción de una operación, de una o varias variables de entrada y de una variable de salida. De entre las posibles operaciones, se distinguen las operaciones asociadas al sistema bilineal $(p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T)$, a saber, las operaciones de multiplicación y de exponenciación en cada uno de los grupos $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T)$, así como la operación de apareamiento bilineal. Estas operaciones se denominan “algebraicas”, en tanto que todas las demás se calificarán como operaciones “anexas”. En esta misma fase de interpretación, las variables de entrada y de salida de cada instrucción se ponen en una forma llamada SSA (*Static Single-Assignment*, según una terminología anglosajona), en orden a poder deducir con facilidad, de esta representación del descodificador pirata, un grafo de cálculo de toda variable por él manipulada a lo largo de su ejecución formal. La variable de salida del programa representa el dato en claro *K* y dimana de un grafo de cálculo con valor de salida dentro de $\mathbb{G}_T$. Se acota el programa al cálculo de este grafo.

En una segunda etapa llamada de especialización, se pretende fijar todas las variables de entrada del programa en valores constantes para los cuales el programa consigue descifrar correctamente. Esta búsqueda de valores fijos se puede llevar a cabo de manera aleatoria y exhaustiva, y si el descodificador dado en un principio es suficientemente funcional (es decir, descifra en una fracción significativa de los casos en promedio), esta etapa de búsqueda puede culminar rápidamente con algunos intentos. Cuando unos valores son adecuados, se sustituyen por estos las correspondientes variables en el programa, de modo que el nuevo programa obtenido únicamente se compone de instrucciones efectuadas sobre constantes. Entonces se procede a una etapa de simplificación del programa encaminada a obtener una única secuencia de instrucciones sin salto.

Para este fin, se efectúa una propagación de las constantes para suprimir todas las instrucciones anexas cuyas variables de entrada son todas ellas constantes; por lo tanto, esta transformación excluye las operaciones algebraicas. Al término de esta fase, se suprimen los saltos no condicionales yuxtaponiendo extremo con extremo las secuencias lineales de instrucciones por orden cronológico de ejecución. El programa se convierte entonces en una sucesión de instrucciones algebraicas secuenciales sin flujo de control.

En una tercera fase, se aplican al programa obtenido varias transformaciones de simplificaciones algebraicas de manera inductiva y concurrente hasta la estabilización del programa. Estas transformaciones se encaminan a obtener un programa equivalente en el que la salida *K* está calculada como un producto de potencias enteras de apareamiento a partir de los datos de entrada, siendo estas potencias valores constantes debido a las anteriores fases de transformación. A continuación, se identifica el exponente correspondiente a cada elemento algebraico de la cifra dada a la entrada, así como a cada elemento de la palabra de control mezclada dada a la entrada. Por las propiedades matemáticas de la invención, este conjunto de exponentes, cuyos valores son conocidos, forma un

sistema de ecuaciones multivariable conocido de antemano cuyas variables son, por una parte, los elementos $x_1, x_2, \ldots, x_z \in \mathbb{Z}_p$ que componen las palabras de control que han servido para la fabricación de la palabra de control mezclada y, por otra, los parámetros elegidos $s_1, s_2, \ldots, s_z \in \mathbb{Z}_p$ que componen la cifra *C* dada a la entrada por el rastreador. El sistema de ecuaciones multivariable depende de la forma de realización de la invención. Conociendo el valor numérico de las salidas del sistema y los parámetros elegidos $\{s_j\}_{j=1}^{z}$, el sistema puede invertirse parcial o totalmente para dar al menos con uno de los elementos $x_1, x_2, \ldots, x_z$ que componen una de las palabras de control primitivas e identificar así completamente uno de los dispositivos traidores. Esta fase puede necesitar tener $z \leq B$, donde *B* es un extremo que depende de la forma de realización de la invención.

Asimismo, la invención prevé una forma de realización para autorizar o prohibir que un dispositivo electrónico de abonado -conforme a la invención- produzca una palabra de control $k' = k_{i,cp}$. Así, la invención prevé que tal dispositivo tan solo pueda ser autorizado a producir $k' = k_{i,cp}$ si una fecha de puesta a disposición o una fecha de inicialización es anterior al criptoperiodo en curso. De este modo, y a título de ejemplo, al contratar una suscripción, en el dispositivo de abonado entregado a un recién abonado se puede memorizar una fecha de inicialización cp^b. De acuerdo con esta forma de realización, un dispositivo de abonado conforme a la invención incluye unos medios 24 para memorizar tal fecha. Esta puede expresarse como igual al criptoperiodo en curso en el momento de contratar. De este modo, los medios de procesamiento 10 de tal dispositivo pueden estar adaptados para cooperar con dichos medios 24 y suministrar una palabra de control $k' = k_{i,cp}$ tan solo si el criptoperiodo en curso *cp* es superior o igual a cp^b. Esta forma de realización se ilustra mediante las figuras 5 y 5b. De acuerdo con esta última figura, el procedimiento 100, puesto en práctica por los medios de procesamiento 10 de un dispositivo de abonado, incluye una etapa 109 prevista al efecto. En la figura 5, un dispositivo 1 incluye unos medios 14 y 15 para comparar cp^b y *cp* y gobernar A el respectivo suministro $k' = k_{i,cp}$ o $k' = kf$, siendo *kf* un valor distinto de un valor válido de una palabra de control $k_{i,cp}$. De acuerdo con estas mismas figuras, la invención prevé que puedan ser memorizados uno o varios valores *kf* por el dispositivo 1 -medios de memorización 26. Los medios S suministran 106b una palabra de control $k' = kf$ en sustitución de $k' = k_{i,cp}$ si cp^b es superior al criptoperiodo en curso *cp*. Así, esta forma de realización previene toda utilización de un dispositivo de abonado para descodificar un contenido codificado percibido anteriormente al contrato de suscripción. La invención prevé, como complemento o como variante, la utilización de una fecha de expiración cp^e que puede ser memorizada en todo dispositivo de abonado conforme a la invención. Esta fecha se inscribe en unos medios 25 de tal dispositivo en el momento de la rescisión voluntaria o forzada de una suscripción. De este modo, un procedimiento 100, descrito en relación con la figura 5b, puede incluir una etapa 109 que permite comparar el criptoperiodo en curso *cp* deducido de la etiqueta y suministrar 106 $k' = k_{i,cp}$ tan solo si dicho criptoperiodo en curso es inferior a cp^e. En caso contrario, la palabra de control suministrada 106b por el dispositivo puede ser igual a *kf* al igual que en el procesamiento de la fecha de inicialización.

Esta forma de realización se puede aprovechar para, eventualmente, revocar un dispositivo traidor transmitiendo, por intermedio de la red 4, una petición de revocación selectiva y frustrar la utilización de dicho dispositivo traidor.

De acuerdo con esta forma de realización, el servidor de contenidos elabora una etiqueta $t = u\|v\|cp$ que incluye, además de los datos relativos al criptoperiodo en curso *cp*, unas componentes *u* y *v* de valores determinados.

La componente *u* permite indicar una solicitud de revocación con destino a un dispositivo con identificador *i* cuyo valor está contenido en la componente *v*. A la recepción de una etiqueta $t = u\|v\|cp$, los valores *u*, *v* y *cp* son extraídos por los medios 12 del dispositivo 1i según la figura 5. En relación con la figura 5b, los medios 14 comparan 107 el valor de la componente *u* con un valor predeterminado u_r. Si $u = u_r$ y $v = i$ (etapa 110), los medios de procesamiento del dispositivo inicializan 111 una fecha de expiración cp^e igual a *cp*. El dispositivo de abonado ya no está en disposición de suministrar palabras de control válidas. Si el valor de *v* es diferente del valor del identificador *i* del dispositivo, este último prosigue su procesamiento tradicional y produce una palabra de control válida.

La invención prevé una variante a cuyo efecto se pueda remitir a un dispositivo de abonado una petición de rehabilitación. Esta petición puede seguir a una solicitud de revocación previa que se haya remitido, por ejemplo, por error. El objeto de una petición de este tipo consiste en autorizar nuevamente un dispositivo de abonado a producir palabras de control válidas. De la misma manera, la invención prevé un valor predeterminado u_a característico de tal petición. Para anular una revocación de un dispositivo, un servidor de contenidos conforme a la invención transmite una etiqueta $t = u\|v\|cp$, para la cual *u* y *v* son respectivamente iguales a u_a y al identificador *i* del dispositivo al que concierne la petición.

A la recepción de una etiqueta $t = u\|v\|cp$, los valores *u*, *v* y *cp* son extraídos por los medios 12 del dispositivo. Los medios 14 comparan 107 el valor de la componente *u* con el valor predeterminado u_a. Si $u = u_a$ y $v = i$ (etapa 110), los medios de procesamiento del dispositivo reinicializan 111 una fecha de expiración cp^e igual a $\emptyset$ -que denota una ausencia de expiración. El dispositivo de abonado vuelve a estar en disposición de suministrar palabras de control válidas. Si el valor de *v* es diferente del valor del identificador *i* del dispositivo, este último prosigue su procesamiento tradicional o permanece revocado. Tal petición de anulación de revocación o de rehabilitación puede traducirse, como variante, en una petición de inicialización. En este caso, es posible inicializar la fecha de inicialización cp^b al valor en curso de *cp*, traduciéndose así la revocación en la definición de una fecha de inicialización muy superior a los criptoperiodos en curso o infinita.

Aunque se haya ilustrado esencialmente en relación con la primera forma de realización preferida de la invención -figura 5b-, tal procedimiento -para revocar o rehabilitar un dispositivo de abonado- puede ser llevado a la práctica cualquiera que sea la forma de realización de un sistema de acceso condicional conforme a la invención.

REIVINDICACIONES

1. Procedimiento (100) para producir una palabra de control *k'*, siendo puesto en práctica dicho procedimiento por unos medios de procesamiento (10) de un dispositivo electrónico de abonado (1) que coopera con un terminal (2i), poniendo en práctica este último un procedimiento (200) para descodificar un contenido codificado *C* a partir de dicha palabra de control *k'* para producir un contenido en claro *M*, incluyendo dicho dispositivo electrónico de abonado (1) unos medios de recepción (R) para recibir datos desde el terminal (2i) y unos medios (S) para suministrar dicha palabra de control *k'* a dicho terminal (2i), incluyendo dicho procedimiento para producir una palabra de control *k*:

- una etapa para recibir (101) datos por intermedio de los medios de recepción (R) que consisten en una etiqueta *t*;
- una etapa para determinar (103) el criptoperiodo en curso explotando la etiqueta *t* recibida;
- una etapa para producir (105) la palabra de control *k* a partir de dicho criptoperiodo en curso *cp* y de un secreto SK_i memorizado (23) por el dispositivo;
- una etapa para suministrar dicha palabra de control *k'* por intermedio de los medios para suministrar (S) del dispositivo;

caracterizándose el procedimiento por que:

- un valor de un identificador *i* específico del dispositivo electrónico es memorizado previamente (22) por dicho dispositivo electrónico de abonado, siendo el valor de dicho identificador *i* distinto del memorizado por cualquier otro dispositivo de abonado;
- dicho valor del identificador *i* participa en el cálculo de dicha palabra de control $k' = k_{i,cp}$ de la etapa (105) para producir esta última cuyo valor, de este modo, resulta distinto del de cualquier otra palabra de control producida por un segundo dispositivo electrónico de abonado para el mismo criptoperiodo *cp*;

y por que dichos procedimientos para respectivamente producir (100) la palabra de control $k' = k_{i,cp}$ y para descodificar (200) el contenido codificado *C* se establecen mutuamente de modo que este último incluye una etapa (201), dual con la producción de $k' = k_{i,cp}$, para suprimir la contribución del identificador *i* en el seno de la palabra de control $k' = k_{i,cp}$ y producir el contenido en claro *M*.

2. Procedimiento según la reivindicación anterior, caracterizado por que incluye una etapa previa (140) para grabar el secreto SK_i en unos medios de memorización (23) del dispositivo (1i).

3. Procedimiento según las reivindicaciones 1 ó 2, caracterizado por que incluye una etapa previa (109) para autorizar el dispositivo (1i) a producir (105) una palabra de control.

4. Procedimiento según las reivindicaciones 1 ó 2, caracterizado por que incluye una etapa previa (109) para autorizar el dispositivo (1) a suministrar (106) una palabra de control *k'* igual a la palabra de control producida $k_{i,cp}$.

5. Procedimiento según las reivindicaciones 3 ó 4, caracterizado por que la etapa (109) previa para autorizar el dispositivo (1) consiste en comparar el criptoperiodo *cp* deducido de la etiqueta *t* con una fecha de activación (cp^b) memorizada (24) en dicho dispositivo y en autorizar el dispositivo si dicho criptoperiodo *cp* es superior a dicha fecha de activación.

6. Procedimiento según las reivindicaciones 3 ó 4, caracterizado por que la etapa (109) previa para autorizar el dispositivo (1) consiste en comparar el criptoperiodo *cp* deducido de la etiqueta *t* con una fecha de expiración (cp^e) memorizada (25) en dicho dispositivo y en autorizar el dispositivo si dicho criptoperiodo *cp* es inferior a dicha fecha de expiración.

7. Procedimiento según la reivindicación anterior, caracterizado por que incluye una etapa (111) para escribir en unos medios para memorizar (25) del dispositivo un valor de criptoperiodo previamente deducido (103) de la etiqueta *t*, en calidad de fecha de expiración (cp^e), si dicha etiqueta *t* incluye una componente *u* cuyo valor (u_r) es característico de una solicitud de revocación y si dicha etiqueta incluye además una componente *v* que designa el identificador *i* del dispositivo.

8. Procedimiento según las reivindicaciones 6 ó 7, caracterizado por que incluye una etapa (112) parar borrar en unos medios para memorizar (25) una fecha de expiración (cp^e) si dicha etiqueta *t* incluye una componente *u* cuyo valor (u_a) es característico de una solicitud de rehabilitación y si dicha etiqueta incluye además una componente que designa el identificador *i* del dispositivo.

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

- unos medios de recepción (R) para recibir datos desde el terminal (2);
- unos medios de procesamiento (10) para producir una palabra de control a partir de dichos datos;
- unos medios (S) para suministrar dicha palabra de control a dicho terminal (2),

caracterizado por que el dispositivo incluye unos medios de memorización para memorizar un identificador específico *i* (22) cuyo valor es distinto del memorizado por cualquier otro dispositivo de abonado, un secreto SK_i (23), y por que dichos medios de procesamiento (10) y de memorización están adaptados para producir y suministrar una palabra de control rastreable $k' = k_{i,cp}$ según un procedimiento conforme a una cualquiera de las reivindicaciones 1 a 8.

10. Procedimiento (200) para descodificar un contenido codificado *C* y producir un contenido en claro *M*, siendo puesto en práctica dicho procedimiento por unos medios de procesamiento de un terminal (2i) que cooperan con unos medios para recibir datos desde el mundo exterior (3, 4) y unos medios para suministrar dicho contenido en claro *M*, caracterizado por que dichos datos consisten en dicho contenido codificado *C*, una cabecera *H* y una palabra de control $k_{i,cp}$ producida de acuerdo con una cualquiera de las reivindicaciones 1 a 8 por un dispositivo electrónico de abonado (1i) para el cual el valor de un identificador específico *i*, memorizado por dicho dispositivo electrónico de abonado y distinto del memorizado por cualquier otro dispositivo de abonado, participa en el cálculo de la palabra de control $k_{i,cp}$, y por que el procedimiento (200) incluye:

- una etapa (201), dual con la producción de $k' = k_{i,cp}$, para aplicar una primera función *F*1 a la cabecera *H* y a la palabra de control $k_{i,cp}$ para suprimir la contribución de dicho identificador específico *i* en el seno de $k_{i,cp}$ y producir (203) una palabra *K* independiente de dicho identificador *i*;
- una etapa para aplicar (204) una segunda función *F*3 a dicha palabra *K* y al contenido codificado *C* para producir el contenido en claro *M*;
- una etapa para suministrar dicho contenido en claro *M* por intermedio de los medios para suministrar (205) del terminal.

11. Procedimiento según la reivindicación anterior, caracterizado por que incluye una etapa para aplicar (202) una tercera función *F*2 a la palabra *K* producida para adaptar el formato de dicha palabra previamente a la aplicación de la función *F*3 para producir el contenido en claro *M*.

12. Terminal electrónico (2i) que incluye:

- unos medios de recepción para recibir datos desde el mundo exterior (3, 4);
- unos medios de procesamiento (10) para producir un contenido en claro *M* a partir de dichos datos;
- unos medios para suministrar dicho contenido en claro a una interfaz hombre-máquina (5) adaptada para restituir dicho contenido en claro;
- unos medios para cooperar con un dispositivo electrónico de abonado (1i),

caracterizado por que:

- los datos recibidos del mundo exterior consisten en un contenido codificado *C*, una cabecera *H* y una etiqueta *t*;
- los medios para cooperar con dicho dispositivo electrónico de abonado (1i) se establecen para transmitir a este último dicha etiqueta *t* y para recibir de vuelta una palabra de control rastreable $k_{i,cp}$ producida por dicho dispositivo electrónico de abonado con un identificador específico *i* cuyo valor participa en el cálculo de la palabra de control rastreable $k_{i,cp}$, siendo dicho valor del identificador específico *i* memorizado por dicho dispositivo electrónico de abonado y distinto del memorizado por cualquier otro dispositivo electrónico de abonado;
- el terminal incluye unos medios de procesamiento adaptados para descodificar y suministrar un contenido en claro *M* según un procedimiento conforme a las reivindicaciones 10 u 11.

13. Procedimiento (410) para codificar un contenido en claro *M* y producir un contenido codificado *C*, siendo puesto en práctica dicho procedimiento por unos medios de procesamiento de un servidor (3) que incluye unos medios para suministrar dicho contenido codificado *C* a un terminal que coopera con un dispositivo electrónico de abonado, caracterizándose dicho procedimiento por que incluye:

- una etapa para producir (414) un contenido codificado *C* a partir de un criptoperiodo *cp* y de un secreto *MK* conocido por el servidor;

- una etapa para producir una etiqueta *t* para caracterizar el criptoperiodo *cp* a partir del cual se ha producido el contenido codificado *C* y ser explotada por el dispositivo electrónico de abonado para el cual el valor de un identificador específico *i*, memorizado por dicho dispositivo electrónico de abonado y distinto del memorizado por cualquier otro dispositivo de abonado, participa en la producción de una palabra de control rastreable $k_{i,cp}$ según un procedimiento conforme a una cualquiera de las reivindicaciones 1 a 8;

- una etapa (413a) para calcular y suministrar una cabecera *H* explotada por el terminal, siendo este último conforme a la reivindicación 12, para suprimir la contribución del identificador específico *i* en el seno de $k_{i,cp}$ y descodificar el contenido codificado según un procedimiento de descodificación conforme a las reivindicaciones 10 u 11;

- una etapa para suministrar conjuntamente dicho contenido codificado *C*, la cabecera *H* y dicha etiqueta *t*.

14. Servidor (3) caracterizado por que incluye unos medios de procesamiento establecidos para producir y suministrar al mundo exterior (4, 2), según un procedimiento conforme a la reivindicación anterior:

- un contenido codificado *C* a partir de un contenido en claro, de un criptoperiodo *cp* y de un secreto *MK*;

- una etiqueta *t*;

- una cabecera *H*.

15. Procedimiento (100) según una cualquiera de las reivindicaciones 1 a 8, caracterizado por que además incluye una etapa para elaborar (105a) y suministrar (106a) una cabecera *H* para permitir al terminal poner en práctica un procedimiento de descodificación (200) conforme a las reivindicaciones 10 u 11.

16. Dispositivo (1i) según la reivindicación 9, caracterizado por que los medios de procesamiento (10) están adaptados para producir y suministrar además una cabecera *H* según un procedimiento conforme a la reivindicación anterior.

17. Sistema de acceso condicional a un contenido digital, caracterizado por que incluye un servidor (3), un terminal (2i) y un dispositivo electrónico (1i) respectivamente conformes a las reivindicaciones 14, 12 y 9.

18. Sistema de acceso condicional a un contenido digital, caracterizado por que incluye un servidor (3) que incluye unos medios de procesamiento para producir una etiqueta *t*, un contenido codificado *C* a partir de un contenido en claro *M*, de un criptoperiodo *cp* y de un secreto *MK*, un terminal (2i) y un dispositivo electrónico (1i) respectivamente conformes a las reivindicaciones 12, y 16.

19. Procedimiento para rastrear una palabra de control $k_{p,cp}$ producida por un dispositivo de abonado traidor, caracterizándose el procedimiento para rastrear:

- por que dicho dispositivo electrónico de abonado es conforme respectivamente a las reivindicaciones 9 ó 16 poniendo en práctica un procedimiento (100) según una cualquiera de las reivindicaciones 1 a 8 ó 15, para el cual el valor de un identificador específico *i*, memorizado por dicho dispositivo electrónico de abonado y distinto del memorizado por cualquier otro dispositivo electrónico de abonado, participa en la producción de la palabra de control $k_{i,cp}$;

- y por que dicho procedimiento para rastrear incluye:

- una etapa para recabar una palabra de control $k_{p,cp}$;

- una etapa para recabar una utilidad o programa de descifrado pirata establecido para descodificar un contenido codificado con el concurso de dicha palabra de control $k_{p,cp}$;

- una etapa para determinar un identificador $i = p$ de un dispositivo que haya producido $k_{p,cp}$ consistente en:

  i. interpretar la utilidad o programa de descifrado para diseñar un programa equivalente que expresa un conjunto de instrucciones en forma de operaciones algebraicas y anexas incluyendo cada una de ellas al menos una variable de entrada y al menos una variable de salida;

  ii. fijar las variables de entrada a constantes para las cuales el programa equivalente descodifica correctamente el contenido codificado;

  iii. simplificar dicho programa equivalente para que el mismo no incluya más que una secuencia de instrucciones sin salto;

  iv. convertir el programa equivalente simplificado a un sistema de ecuaciones multivariable para la puesta en práctica de transformaciones algebraicas;

v. invertir en su totalidad o en parte dicho sistema de ecuaciones multivariable para identificar el dispositivo traidor.

20. Procedimiento de acceso condicional a un contenido digital que incluye:

- una etapa (410) para elaborar y suministrar, por parte de un servidor (3), un contenido codificado *C*, una etiqueta *t* y una cabecera *H* de acuerdo con la reivindicación 13;
- una etapa para receptar, por parte de un terminal (2i), dichos contenido codificado *C*, etiqueta *t* y la cabecera *H*;
- una etapa para transmitir la etiqueta *t* por parte del terminal a un dispositivo (1i) que coopera con dicho terminal;
- una etapa (100) para producir y suministrar, por parte de dicho dispositivo (1i) al terminal (2i), una palabra de control rastreable $k_{i,cp}$ de acuerdo con una cualquiera de las reivindicaciones 1 a 8;
- una etapa para descodificar (200), por parte del terminal (2i), el contenido codificado y producir un contenido en claro *M* según un procedimiento conforme a las reivindicaciones 10 u 11;
- una etapa para restituir dicho contenido en claro *M* por medio de una interfaz (5) adaptada a dicho contenido en claro.

21. Procedimiento de acceso condicional a un contenido digital que incluye:

- una etapa (410) para elaborar y suministrar, por parte de un servidor, un contenido codificado *C* y una etiqueta *t* que caracteriza el criptoperiodo *cp* a partir del cual se ha producido el contenido codificado *C*;
- una etapa para receptar, por parte de un terminal (2i), dichos contenido codificado *C* y etiqueta *t*;
- una etapa para transmitir la etiqueta *t* por parte del terminal a un dispositivo (1i) que coopera con dicho terminal;
- una etapa (100) para producir y suministrar, por parte de dicho dispositivo (1i) al terminal (2i), una palabra de control rastreable $k_{i,cp}$ y una cabecera *H* de acuerdo con el procedimiento según la reivindicación 15;
- una etapa para descodificar (200), por parte del terminal (2i), el contenido codificado *C* y producir un contenido en claro *M* según un procedimiento conforme a las reivindicaciones 10 u 11;
- una etapa para restituir dicho contenido en claro *M* por medio de una interfaz (5) adaptada a dicho contenido en claro.

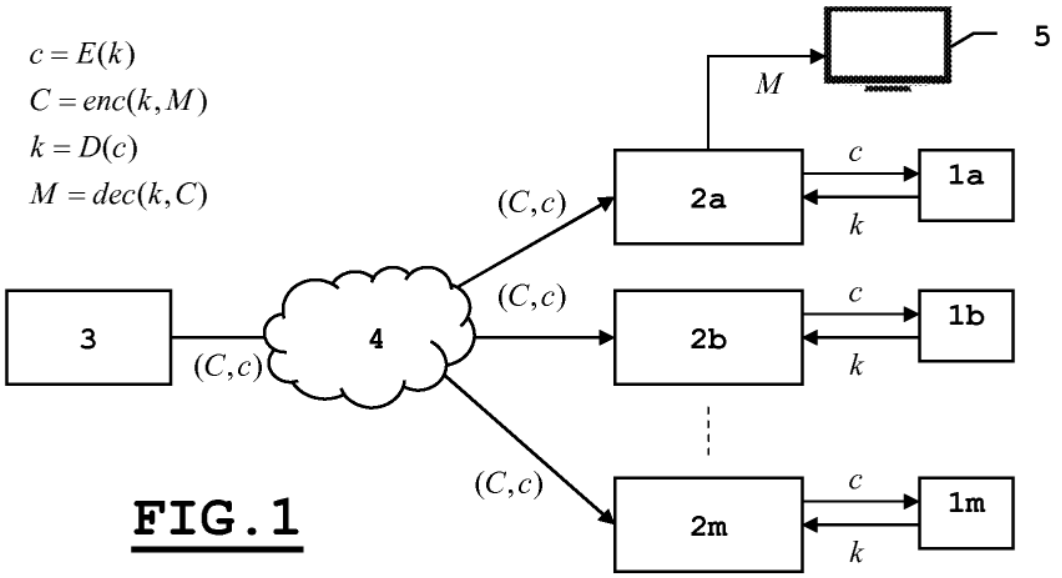

$c = E(k)$
$C = enc(k, M)$
$k = D(c)$
$M = dec(k, C)$
5
M
2a
1a
c
k
(C,c)
3
4
2b
1b
2m
1m

FIG.1

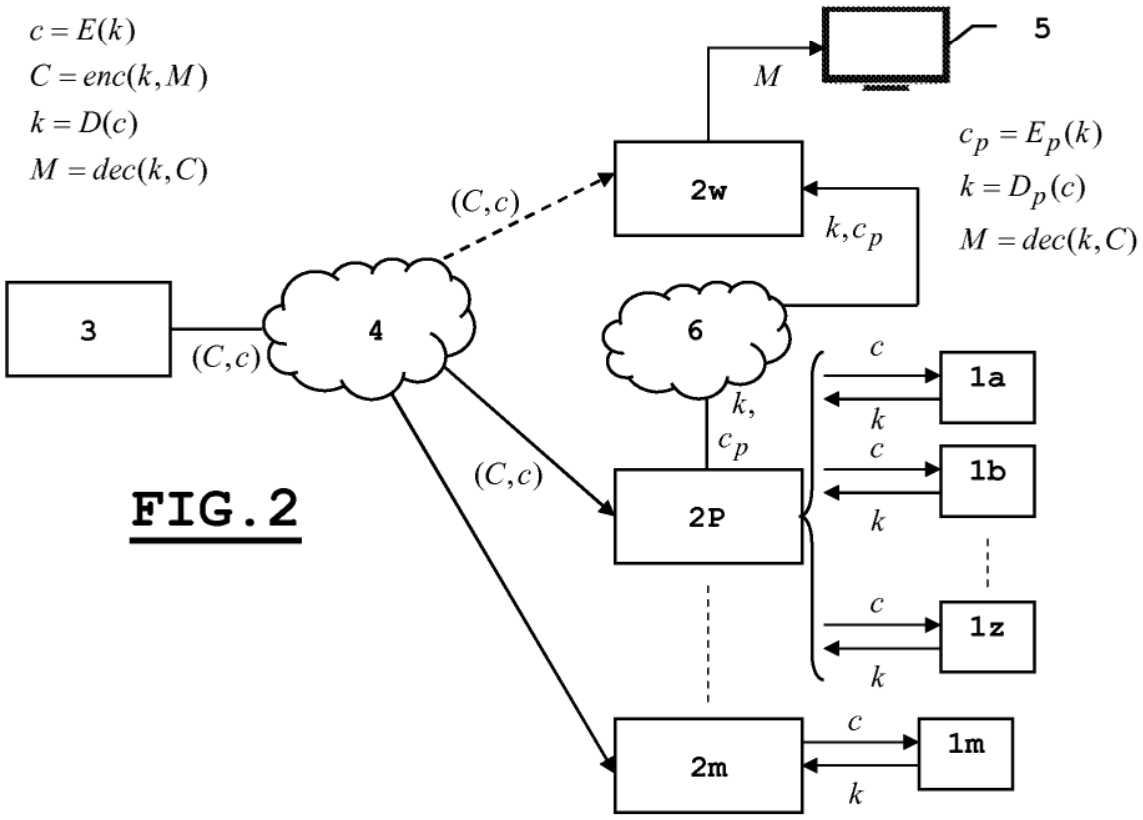

$c = E(k)$
$C = enc(k, M)$
$k = D(c)$
$M = dec(k, C)$
5
M
$c_p = E_p(k)$
$k = D_p(c)$
$M = dec(k, C)$
2w
k, c_p
(C,c)
3
4
6
k, c_p
1a
1b
1z
2P
2m
1m
c
k

FIG.2

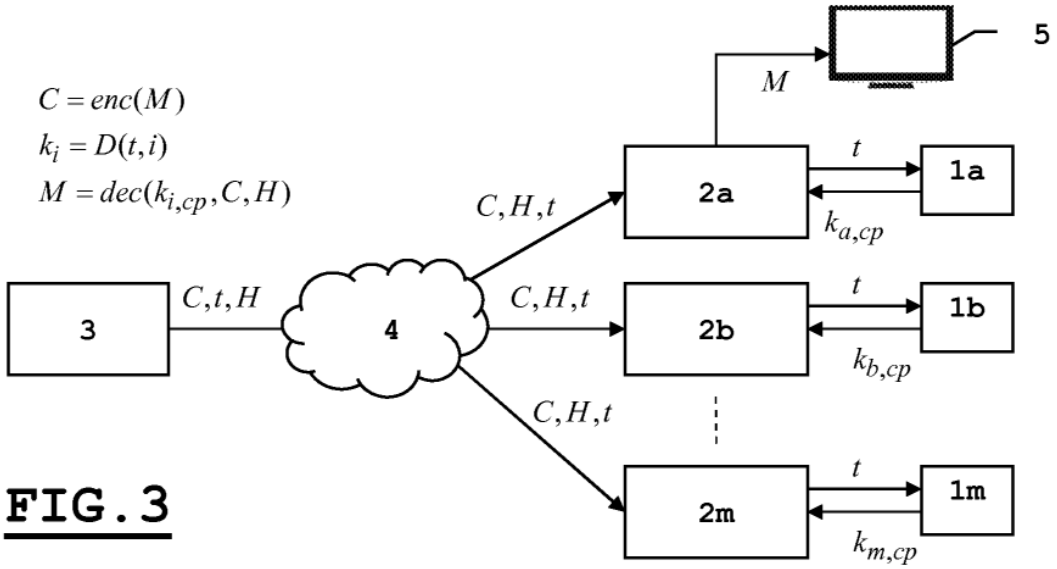
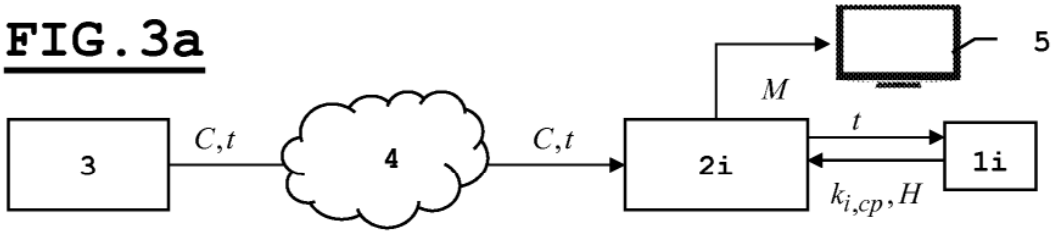


FIG.3

FIG.3a



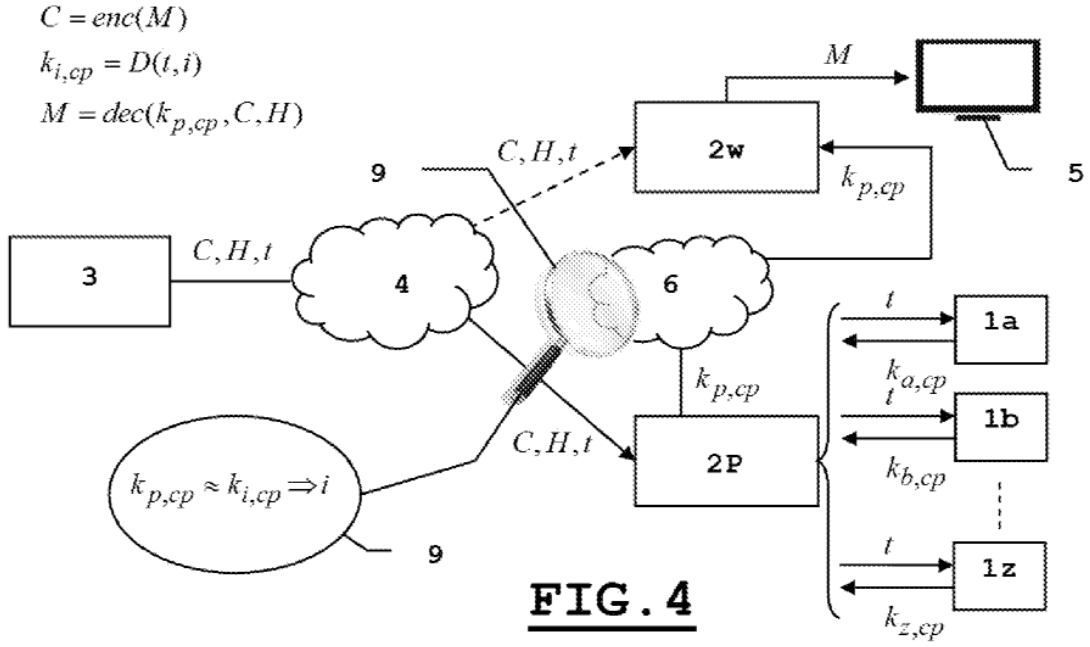


FIG.4

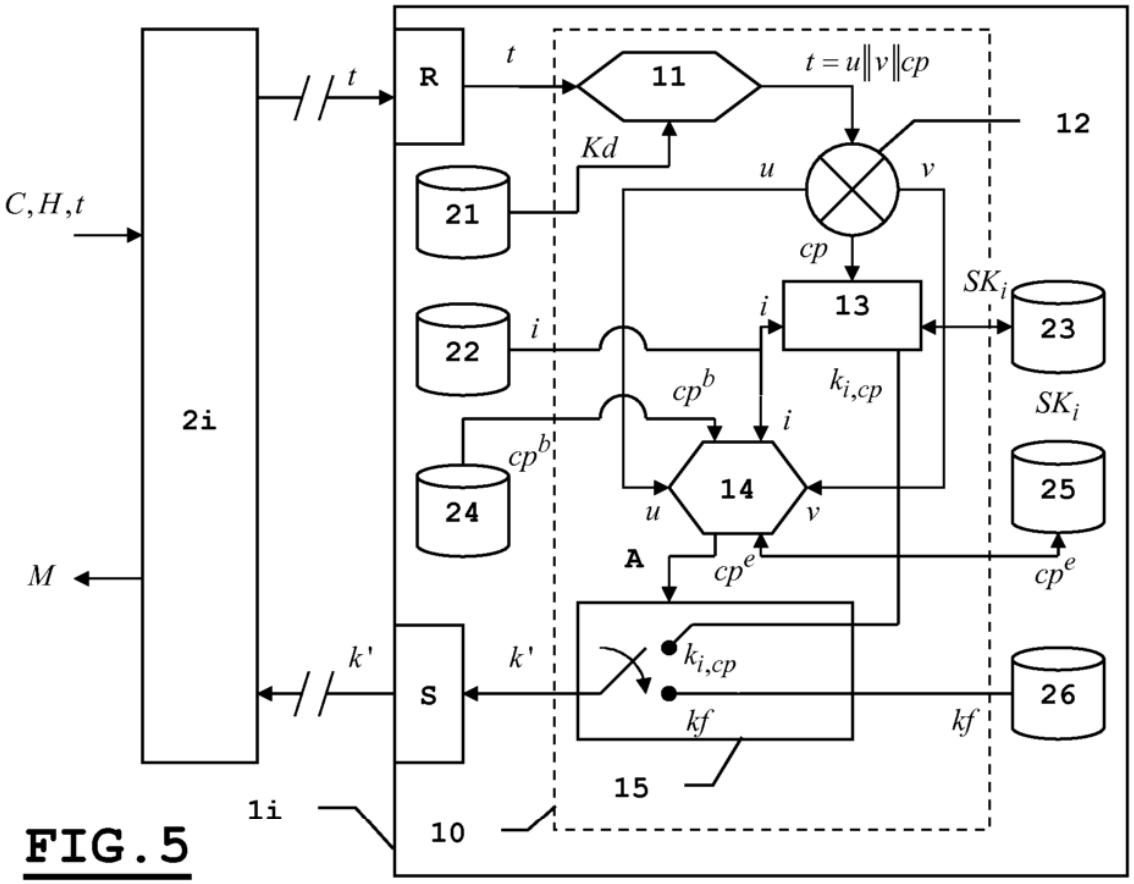

C,H,t
2i
M
t
R
t
11
t = u‖v‖cp
12
Kd
21
u
v
cp
22
i
13
SKi
23
i
kᵢ,cp
SKi
cpᵇ
cpᵇ
24
14
25
u
v
A
cpᵉ
cpᵉ
k'
k'
S
kᵢ,cp
kf
kf
26
15
1i
10

FIG.5

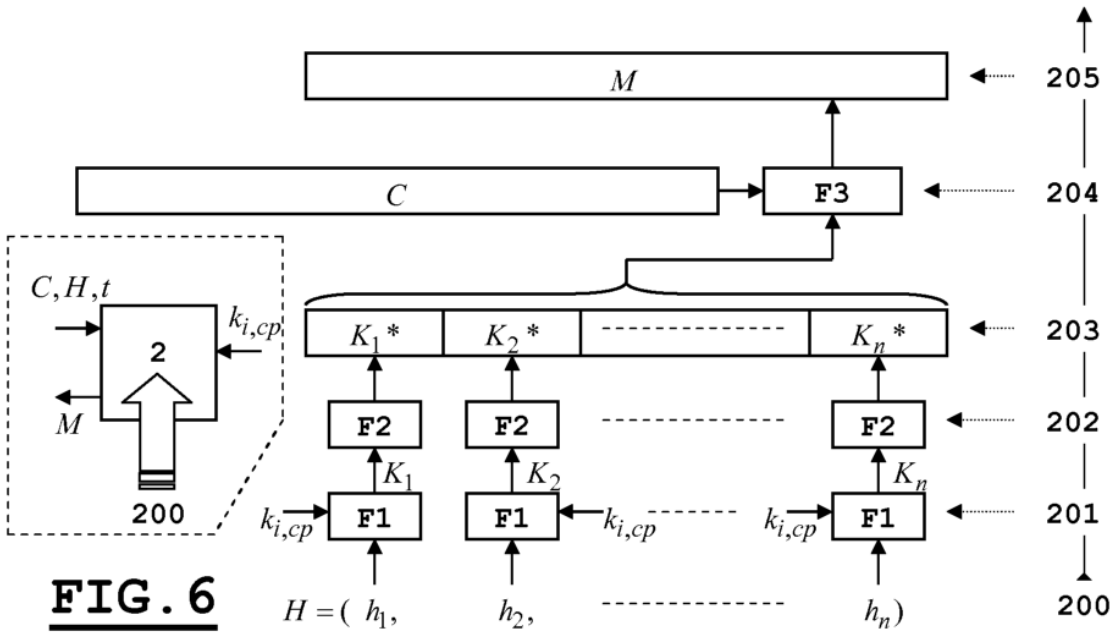

M
205
C
F3
204
C,H,t
kᵢ,cp
2
K₁*
K₂*
Kₙ*
203
M
F2
F2
F2
202
200
K₁
K₂
Kₙ
kᵢ,cp
F1
F1
F1
201
H = (h₁,
h₂,
hₙ)
200

FIG.6

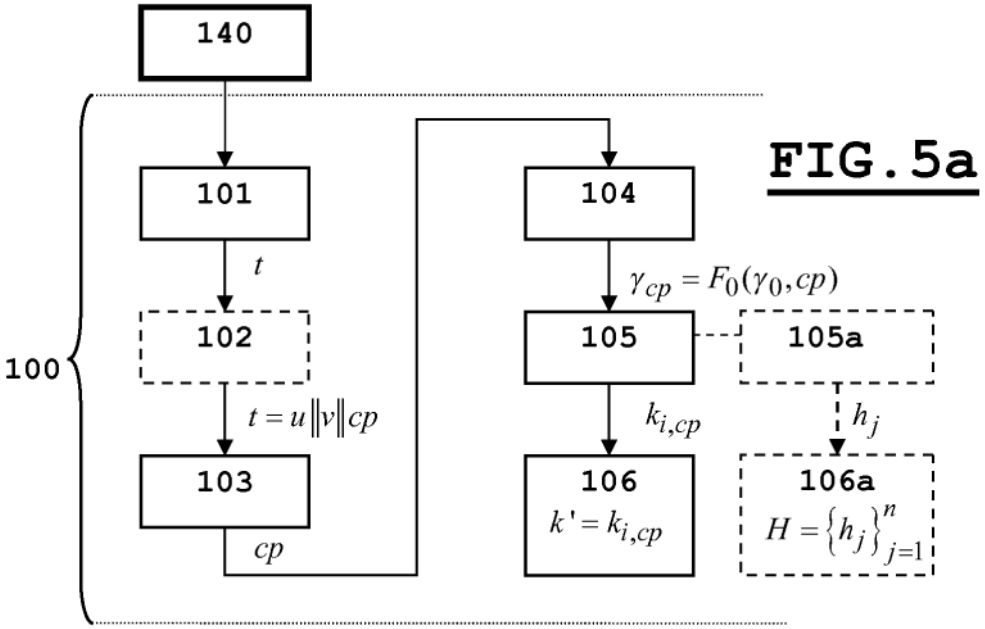

140
101
t
102
$t = u\|v\|cp$
103
cp
104
$\gamma_{cp} = F_0(\gamma_0, cp)$
105
105a
$k_{i,cp}$
h_j
106
$k' = k_{i,cp}$
106a
$H = \{h_j\}_{j=1}^{n}$
100

FIG.5a

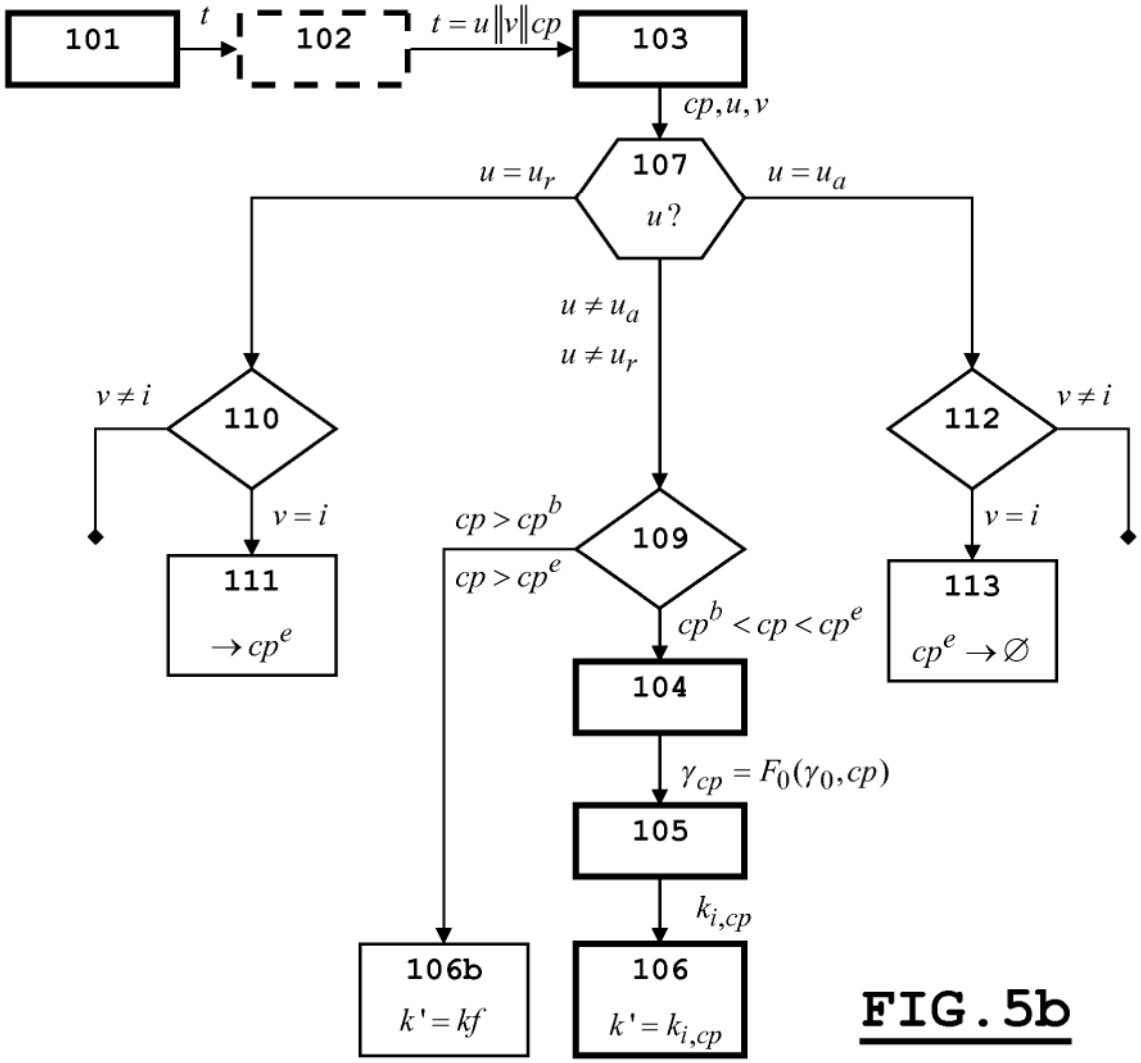

101
t
102
$t = u\|v\|cp$
103
cp, u, v
107
u?
$u = u_r$
$u = u_a$
$u \neq u_a$
$u \neq u_r$
110
$v \neq i$
$v = i$
111
$\rightarrow cp^e$
109
$cp > cp^b$
$cp > cp^e$
$cp^b < cp < cp^e$
112
$v \neq i$
$v = i$
113
$cp^e \rightarrow \varnothing$
104
$\gamma_{cp} = F_0(\gamma_0, cp)$
105
$k_{i,cp}$
106b
$k' = kf$
106
$k' = k_{i,cp}$

FIG.5b

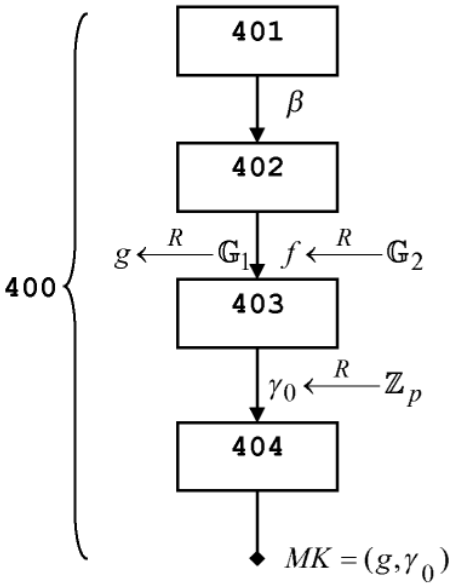


FIG.8

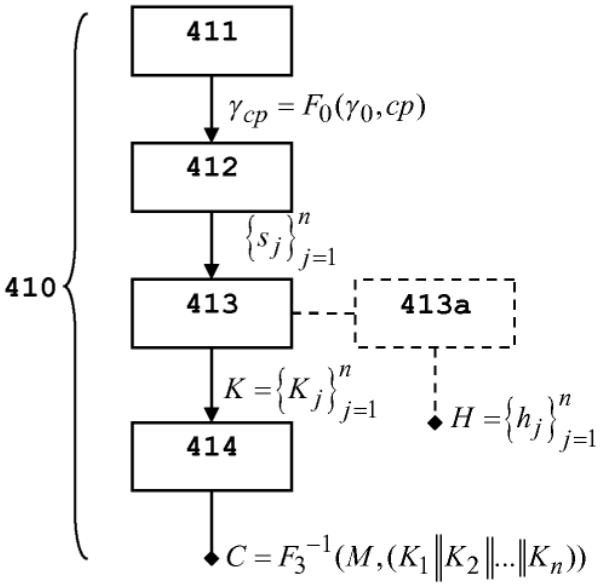


FIG.7

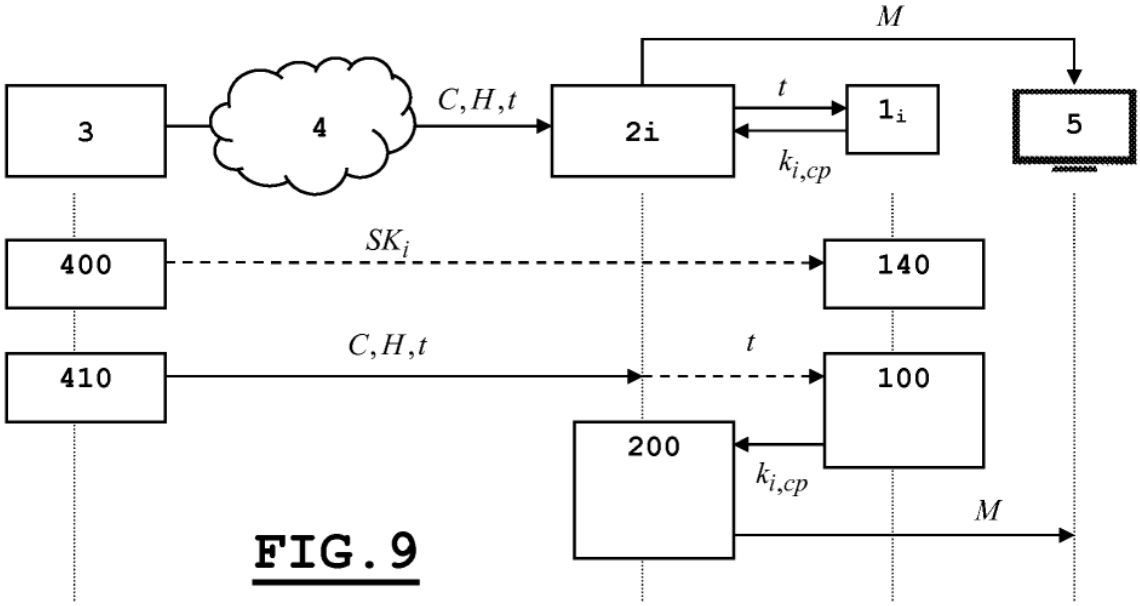


FIG.9