(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 334 109**

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

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **02710108 .8**
(96) Fecha de presentación : **23.01.2002**
(97) Número de publicación de la solicitud: **1354443**
(97) Fecha de publicación de la solicitud: **22.10.2003**

(54) Título: **Método para la codificación de transmisiones.**

(30) Prioridad: **26.01.2001 US 770877**

(45) Fecha de publicación de la mención BOPI:
05.03.2010

(45) Fecha de la publicación del folleto de la patente:
05.03.2010

(73) Titular/es:
International Business Machines Corporation
New Orchard Road
Armonk, New York 10504, US

(72) Inventor/es: **Lotspiech, Jeffrey, Bruce;**
Naor, Dalit y
Naor, Simeon

(74) Agente: **Elzaburu Márquez, Alberto**

DESCRIPCIÓN

Método para la codificación de transmisiones.

Antecedentes del invento

1. **Campo del invento**

El invento se refiere en general al cifrado o codificación de datos de transmisión que usa claves de cifrado.

2. **Descripción de la técnica relacionada**

La patente norteamericana nº 6.118.873 describe un sistema para cifrar música, vídeos y otros contenidos transmitidos. Como se ha descrito en ella, solamente reproductores-grabadores autorizados pueden reproducir y/o copiar el contenido y solamente de acuerdo con reglas establecidas por el vendedor del contenido. De este modo, pueden ser impedidas las copias de contenido pirateadas, que comúnmente cuestan a los proveedores de contenidos billones de dólares cada año.

En el método de cifrado descrito en la patente a que antes se ha hecho referencia, los reproductores-grabadores autorizados son provistos de claves para el dispositivo con software implantado desde una matriz de claves del dispositivo. Las claves pueden ser emitidas simultáneamente una con otra o en el trascurso del tiempo, pero en cualquier caso, ningún reproductor-grabador se supone que tiene más de una clave de dispositivo por columna de la matriz. Aunque dos dispositivos podrían compartir la misma clave desde la misma columna, las posibilidades de que cualesquiera dos dispositivos compartan exactamente las mismas claves de conjunto de todas las columnas de la matriz son muy pequeñas cuando las claves son asignadas aleatoriamente. Las claves son usadas para descifrar el contenido.

En el caso de que un dispositivo (y sus claves) resulte comprometido, deliberadamente o por error, es necesario revocar las claves de ese dispositivo. Revocar un conjunto de claves efectivamente convierte al dispositivo comprometido (y cualesquiera clones del mismo) en inoperante para reproducir el contenido que es producido después de la revocación. En la patente antes descrita, para cada revocación se requieren aproximadamente 320 bytes de mensaje. Aunque esto es efectivo, es deseable reducir la longitud del mensaje de revocación incluso más, por eficiencia.

Aunque el sistema descrito en la patente a que antes se ha hecho referencia es efectivo, debido a limitaciones de tamaño del área de encabezamiento del mensaje (denominado como “bloque de clave de medios” en la patente), solamente un número relativamente limitado (10.000 para un encabezamiento de 3M tal como DVD-Audio) de revocaciones puede ser hecho durante la vida del sistema. Este número puede ser incrementado aumentando el tamaño del encabezamiento, pero las revocaciones añadidas serían aplicables sólo a dispositivos hechos de nuevo, y no a dispositivos que hubieran sido hechos antes del aumento de tamaño del encabezamiento. Es deseable ser capaz de ejecutar un gran número de revocaciones tanto de dispositivos “viejos” como “nuevos”, es decir para tener en cuenta receptores sin estado. También, como más de un dispositivo puede compartir cualquier clave particular con el dispositivo comprometido en el invento patentado a que antes se ha hecho referencia, revocar un conjunto de claves de dispositivo podría dar como resultado revocar algunas claves contenidas por dispositivos inocentes. Es deseable reducir adicionalmente las posibilidades de revocar accidentalmente un dispositivo “bueno”, preferiblemente a cero.

Además, el presente invento está dirigido al difícil escenario de los receptores “sin estado”, es decir, receptores que no actualizan necesariamente su estado de cifrado entre transmisiones para aceptar contramedidas contra dispositivos comprometidos. Por ejemplo, una televisión que se suscribe a un canal de pago podría tener su codificador desactivado durante un período de tiempo durante el cual los datos cifrados actualizados podrían ser transmitidos sobre el sistema. Tal dispositivo se convertiría en “sin estado” si sucede que es incapaz de actualizarse por sí mismo después de haber sido vuelto a activar y así no poseería actualizaciones que serían necesarias para un futuro descifrado del contenido.

Además, hay una necesidad creciente de proteger el contenido de medios, tales como los CD y DVD, que son vendidos al público y para los que es deseable impedir una copia no autorizada. Los grabadores en tal sistema corrientemente no interactúan con lo reproductores, y ningún reproductor conseguirá cada posible pieza de actualizaciones de datos de cifrado, ya que ningún reproductor recibe cada disco vendido. Por consiguiente, como se ha comprendido aquí, la protección de contenidos de medios vendidos es un ejemplo del problema de cifrado de transmisión a receptores sin estado.

Además, la presencia de más de unos pocos fabricantes “malvados” (es decir fabricantes que legal o ilegalmente obtienen claves pero que en cualquier caso hacen que muchos dispositivos sin autorización tengan las claves) puede ser problemática. Es deseable tener en cuenta muchos fabricantes potencialmente “malvados”.

Otros métodos para el cifrado de transmisión incluyen los descritos en Fiat y col., *Cifrado de Transmisión*, Crypto ’93 LNCS vol. 839, págs. 257-270 (1994). Este método considera la retirada de cualquier número de receptores mientras como máximo “t” de ellos operen ilegalmente entre sí. Sin embargo, el método de Fiat y col., requiere longitudes de mensaje relativamente grandes, que un número de claves relativamente grandes sea almacenado en el receptor, y que cada receptor debe realizar más de una única operación de descifrado. Además, el método de Fiat y col., no considera el escenario de receptor sin estado. Hay una necesidad de evitar la suposición a priori de cuantos

receptores podrían operar ilegalmente. También, que el tamaño del mensaje y el número de claves almacenadas sean minimizados, y que el número de operaciones de descifrado que deben ser realizadas por un receptor sea minimizado, para optimizar el rendimiento.

Otros sistemas de cifrado o codificado, como el sistema de Fiat y col., no proporcionan medios para el escenario de receptores sin estado, y así no pueden ser aplicados efectivamente en cuanto a la protección de contenido de medios grabados. Ejemplos de tales sistemas incluyen los sistemas de jerarquía de clave lógica a base de árboles descritos en Wallner y col., *Gestión de claves para Multidifusión: Cuestiones y Arquitecturas,* proyecto IETF de clave de Wallner 1997; Wong y col., *Comunicación Segura de Grupo Utilizando Gráficos de Clave*, SIGCOMM 1998; Canetti y col., *Seguridad Multidifusión: Una Taxonomía y Algunas Construcciones Eficientes*, Proc. de INFOCOM '99 vol. 2 págs. 708-716 (1999); Canetti y col., *Intercambios de Comunicación-Almacenamiento para Cifrado Multidifusión*, Eurocrypt 1999, págs. 459-474; y McGraw y col., *Establecimiento de Claves en Grandes Grupos Dinámicos Usando Árboles de Función de Un Sentido,* sometido a Transacciones de IEEE en Ingeniería de Software (1998).

Con más especificidad en relación a los métodos de Wallner y col., y Wong y col., las claves son asignadas por asignación de una etiqueta independiente a cada nodo en un árbol binario. Desgraciadamente, en los métodos referidos alguna de las etiquetas cambia en cada revocación. Claramente, como es, el método sería inapropiado para el escenario del receptor sin estado. Incluso si un lote de revocaciones que ha de ser asociado con una única etiqueta cambia para cada nodo, los métodos referenciados de Wallner y col., y Wong y col., requerirían al menos log N descifrados en el receptor y la transmisión de rlog N cifrados (donde r es el número de dispositivos que ha de ser revocado y N es el número total de receptores en el sistema), desgraciadamente un número relativamente elevado.

Sumario del invento

El presente invento proporciona por consiguiente un método para el cifrado de transmisión, que comprende: asignar a cada usuario en un grupo de usuarios información privada respectiva I_u; seleccionar al menos una clave K de cifrado de sesión; dividir usuarios que no están en un conjunto revocado R en subconjuntos disjuntos $S_{i1},...S_{im}$ que tienen claves de subconjuntos asociadas $L_{i1},...L_{im}$; y cifrar la clave K de sesión con las claves de subconjuntos $L_{i1},...L_{im}$ para hacer m versiones cifradas de la clave K de sesión.

El método comprende preferiblemente además dividir a los usuarios en grupos $S_1,...S_w$ en los que "w" es un entero, y los grupos establecen subárboles en un árbol.

Preferiblemente, el árbol es un árbol binario completo.

El método comprende preferiblemente además usar la información privada I_u para descifrar la clave de sesión.

De modo adecuado, el acto de descifrado incluye utilizar información i_j de tal modo que un usuario pertenece a un subconjunto S_{ij}, y recuperar una clave L_{ij} de subconjunto usando la información privada del usuario.

Preferiblemente, cada subconjunto $S_{i1},...S_{im}$ incluye todas las hojas de un subárbol con raíz en algún nodo v_i, estando asociado al menos cada nodo del subárbol con una clave de subconjunto respectiva.

Preferiblemente, el contenido es proporcionado a los usuarios en al menos un mensaje que define un encabezamiento, y el encabezamiento incluye como máximo r*log(N/r) claves de subconjuntos y cifrados, en los que r es el número de usuarios en el conjunto R revocado y N es el número total de usuarios.

De modo preferible, cada usuario debe almacenar log N claves, en las que N es el número total de usuarios.

Preferiblemente, el contenido es proporcionado a los usuarios en al menos un mensaje, y en el que cada usuario procesa el mensaje usando como máximo log log N operaciones más una única operación de descifrado, en el que N es el número total de usuarios.

Preferiblemente, el conjunto R revocado define un árbol de expansión, y subárboles que tienen raíces unidas a nodos del árbol de expansión definen los subconjuntos.

Preferiblemente, al árbol incluye una raíz y varios nodos, teniendo cada nodo al menos una etiqueta asociada, y en el que cada subconjunto incluye todas las hojas de un subárbol con raíces en algún nodo v_i que no está en el subárbol con raíz en algún otro nodo v_i que desciende de v_i.

Preferiblemente, el contenido es proporcionado a los usuarios en al menos un mensaje que define un encabezamiento, y el encabezamiento incluye como máximo 2r-1 claves del subconjunto y cifrados, donde r es el número de usuarios en el conjunto revocado R.

Preferiblemente, cada usuario debe almacenar $0,5\log^2 N + 0,5\log N + 1$ claves, en las que N es el número total de usuarios.

Preferiblemente, el contenido es proporcionado a los usuarios en al menos un mensaje, y en el que cada usuario procesa el mensaje usando como máximo log N operaciones más una única operación de descifrado, en la que N es el número total de usuarios.

Preferiblemente, el conjunto R revocado define un árbol de expansión, y el método incluye: inicializar un árbol T de cubierta como el árbol de expansión; eliminar iterativamente nodos del árbol de cubierta T y añadir nodos a una cubierta hasta que el árbol de cubierta T tenga como máximo un nodo.

Preferiblemente, cada nodo tiene al menos una etiqueta posiblemente inducida por al menos uno de sus antepasados, y en el que cada usuario tiene etiquetas asignadas de todos los nodos que cuelgan de un trayecto directo entre el usuario y la raíz pero no desde los nodos en el trayecto directo.

Preferiblemente, son asignadas etiquetas a subconjuntos usando un generador de secuencia seudoaleatorio, y el acto de descifrar incluye evaluar el generador de secuencia seudoaleatorio.

Preferiblemente, el contenido es proporcionado a los usuarios en al menos un mensaje que tiene un encabezamiento que incluye una función criptográfica E_L, y el método incluye prefijar-truncar la función criptográfica E_L.

Preferiblemente, el árbol incluye una raíz y varios nodos, teniendo cada nodo una clave asociada, y en el que cada usuario tiene asignadas claves desde todos los nodos en un trayecto directo entre una hoja que representa al usuario y la raíz.

Preferiblemente, el contenido es proporcionado a los usuarios en al menos un mensaje que define varias partes, y cada parte está cifrada con una clave de sesión respectiva.

El presente invento proporciona de modo adecuado un dispositivo de programa de ordenador, que comprende: un dispositivo de almacenamiento del programa de ordenador que incluye un programa de instrucciones utilizable por un ordenador, que comprende: medios lógicos para acceder a un árbol para identificar varias claves de subconjuntos; medios lógicos para cifrar un mensaje con una clave de sesión; medios lógicos para cifrar la clave de sesión al menos una vez con cada una de las claves de subconjuntos para hacer versiones cifradas de la clave de sesión; y medios lógicos para enviar las versiones cifradas de la clave de sesión en un encabezamiento del mensaje a varios receptores sin estado.

El dispositivo del programa de ordenador comprende preferiblemente además medios lógicos para dividir receptores que no están en un conjunto revocado R en subconjuntos disjuntos $S_{i1},...S_{im}$ que tienen claves de subconjuntos asociadas $L_{i1},...L_{im}$.

El dispositivo de programa de ordenador comprende preferiblemente además medios lógicos para dividir a los usuarios en grupos $S_1,...S_w$ en los que "w" es un entero, y los grupos establecen subárboles en un árbol.

El dispositivo de programa de ordenador comprende preferiblemente además medios lógicos para usar información privada I_u para descifrar la clave de sesión.

Preferiblemente, los medios para descifrar incluyen medios lógicos para usar información i_j tal que un receptor pertenece a un subconjunto S_{ij}, y recuperar una clave L_{ij} de la información privada del receptor.

Preferiblemente, cada subconjunto $S_{i1},...S_{im}$ incluye todas las hojas de un subárbol con raíz en algún nodo v_i, estando asociado al menos cada nodo de un subárbol con una clave de subconjunto respectiva.

Preferiblemente, los medios lógicos proporcionan contenido a los receptores en al menos un mensaje que define un encabezamiento, y el encabezamiento incluye como máximo r*log(N/r) claves de subconjuntos y cifrados, en los que r es el número de receptores en el conjunto R revocado y N es el número total de receptores.

Preferiblemente, cada receptor debe almacenar log N claves en las que N es el número total de receptores.

Preferiblemente, los medios lógicos proporcionan el contenido a los receptores en al menos un mensaje, y en el que cada receptor procesa el mensaje usando como máximo log log N operaciones más una única operación de cifrado, en la que N es el número total de receptores.

Preferiblemente, el conjunto R revocado define un árbol de expansión, y subárboles que tienen raíces unidas a nodos del árbol de expansión definen los subconjuntos.

Preferiblemente, el árbol incluye una raíz y varios nodos, teniendo cada nodo al menos una etiqueta asociada, y en el que cada subconjunto incluye todas las hojas de un subárbol con raíces en algún nodo v_i que no están en el subárbol con raíces en algún otro nodo v_j, que desciende de v_i.

Preferiblemente, los medios proporcionan el contenido a los receptores en al menos un mensaje que define un encabezamiento, y el encabezamiento incluye como máximo 2r-1 claves de subconjuntos y cifrados, en los que r es el número de receptores en el conjunto R revocado.

Preferiblemente cada receptor debe almacenar $0,5\log^2 N + 0,5\log N + 1$ claves en las que N es el número total de receptores.

Preferiblemente, los medios lógicos proporcionan el contenido a los receptores en al menos un mensaje, y en el que cada receptor procesa el mensaje usando como máximo log N operaciones más una única operación de descifrado, en la que N es el número total de receptores.

Preferiblemente, el conjunto R revocado define un árbol de expansión, y el dispositivo de programa de ordenador incluye: medios lógicos para inicializar un árbol de cubierta T como el árbol de expansión, y medios lógicos para eliminar iterativamente nodos del árbol de cubierta T y añadir nodos a una cubierta hasta que el árbol de cubierta T tiene como máximo un nodo.

Preferiblemente, unos medios lógicos asignan etiquetas a receptores usando un generador de secuencias seudoaleatorio, y las etiquetas inducen claves de subconjuntos.

Preferiblemente, los medios para descifrar incluyen evaluar el generador de secuencia seudoaleatorio.

Preferiblemente, los medios lógicos proporcionan contenido a los receptores en al menos un mensaje que tiene un encabezamiento que incluye una función criptográfica E_L y el dispositivo de programa de ordenador incluye medios lógicos para prefijar-truncar la función criptográfica E_L.

Preferiblemente, el árbol incluye una raíz y varios nodos, teniendo cada nodo una clave asociada, y en el que medios lógicos asignan a cada receptor claves desde todos los nodos en trayecto directo entre una hoja que representa al receptor y la raíz.

Preferiblemente, los medios lógicos proporcionan contenido a receptores en al menos un mensaje que define varias partes, y cada parte está cifrada con una clave de sesión respectiva.

El presente invento proporciona adecuadamente un ordenador programado con instrucciones para hacer que el ordenador ejecute actos del método que incluyen: cifrar el contenido de transmisión; y enviar el contenido de transmisión a varios receptores buenos sin estado y al menos a un receptor revocado de tal modo que cada receptor bueno sin estado puede descifrar el contenido y el receptor revocado no puede descifrar el contenido.

Preferiblemente, los actos del método comprenden además: asignar a cada receptor en un grupo de información privada I_u respectiva de receptores; seleccionar al menos una clave K de cifrado de sesión; dividir todos los receptores que no están en un conjunto revocado R en subconjuntos disjuntos $S_{i1},...S_{im}$ que tienen claves de subconjuntos asociadas $L_{i1},...L_{im}$; y cifrar la clave de sesión K con las claves de subconjuntos $L_{i1},...L_{im}$ para hacer m versiones cifradas de la clave de sesión K.

Preferiblemente, los actos del método realizados por el ordenador comprenden además dividir a los usuarios en grupos $S_1,...S_w$, en los que "w" es un entero, y los grupos establecen subárboles en un árbol.

Preferiblemente, el árbol es un árbol binario completo.

Preferiblemente, los actos del método incluyen usar información I_u privada para descifrar la clave de sesión.

Preferiblemente, el acto de descifrado realizado por el ordenador incluye usar información i_j de tal modo que un receptor pertenece a un subconjunto S_{ij}, y recuperar una clave L_{ij} usando la información privada del receptor.

Preferiblemente, cada subconjunto $S_{i1},...S_{im}$ incluye todas las hojas de un subárbol con raíces en algún nodo v_i, estando asociado al menos cada nuevo subárbol con una clave de subconjunto respectiva.

Preferiblemente, el contenido es proporcionado a los receptores en al menos un mensaje que define un encabezamiento, y el encabezamiento incluye como máximo r*log(N/r) claves de subconjuntos y cifrados, en los que r es el número de receptores en el conjunto revocado R y en el que N es el número total de receptores.

Preferiblemente, cada receptor almacena log N claves, en las que N es el número total de receptores.

Preferiblemente, el contenido es proporcionado a los receptores en al menos un mensaje, y en el que cada receptor procesa el mensaje usando como máximo log log N operaciones más una única operación de descifrado, en la que N es el número total de receptores.

Preferiblemente, el conjunto revocado R define un árbol de expansión, y subárboles que tienen raíces unidas a nodos del árbol de expansión definen los subconjuntos.

Preferiblemente, al árbol incluye una raíz y varios nodos, teniendo cada nodo al menos una etiqueta asociada, y en el que cada subconjunto incluye todas las hojas de un subárbol con raíces en algún nodo v_i que no están en el subárbol con raíz en algún otro nodo v_j que desciende de v_i.

Preferiblemente, el contenido es proporcionado a los receptores en al menos un mensaje que define un encabezamiento, y el encabezamiento incluye como máximo 2r-1 claves de subconjuntos y cifrados, donde r es el número de receptores en el conjunto revocado R.

Preferiblemente, cada receptor debe almacenar $0,5\log^2 N + 0,5\log N + 1$ claves, en las que N es el número total de receptores.

Preferiblemente, el contenido es proporcionado a los receptores en al menos un mensaje, y en el que cada receptor procesa el mensaje usando como máximo log N operaciones más una única operación de descifrado, en la que N es el número total de receptores.

Preferiblemente, el conjunto revocado R define un árbol de expansión, y en el que los actos del método realizados por el ordenador incluyen además: inicializar un árbol de cubierta T como el árbol de expansión; eliminar iterativamente nodos del árbol de cubierta T y añadir nodos a una cubierta hasta que el árbol de cubierta T tenga como máximo un nodo.

Preferiblemente, el ordenador asigna etiquetas a receptores desde el árbol usando un generador de secuencia seudoaleatorio.

Preferiblemente, el acto de descifrar realizado por el ordenador incluye evaluar el generador de secuencia seudoaleatorio.

Preferiblemente, el contenido es proporcionado a los receptores en al menos un mensaje que tiene un encabezamiento que incluye una función criptográfica E_L, y los actos del método realizados por el ordenador incluyen prefijar-truncar la función criptográfica E_L.

Preferiblemente, el contenido es proporcionado a los receptores en al menos un mensaje que define varias partes, y cada parte es cifrada por el ordenador con una clave de sesión respectiva.

Preferiblemente, cada nodo tiene varias etiquetas con cada antepasado del nodo induciendo una etiqueta respectiva, y en el que cada usuario tiene asignadas etiquetas desde todos los nodos que cuelgan desde un trayecto directo entre el usuario y la raíz pero no desde los nodos en el trayecto directo.

El presente invento comprende adecuadamente un método para el cifrado de transmisión, que comprende: asignar a cada usuario en un grupo de usuarios información privada respectiva I_u; seleccionar al menos una clave K de cifrado de sesión; dividir a todos los usuarios en grupos $S_1,...S_w$, en los que "w" es un entero, y los grupos establecen subárboles en un árbol; dividir usuarios que no están en un conjunto revocado R en subconjuntos disjuntos $S_{i1},...S_{im}$ que tienen claves de subconjuntos asociadas $L_{i1},...L_{im}$; y cifrar la clave K de sesión con las claves de subconjuntos $L_{i1},...L_{im}$ para hacer m versiones cifradas de la clave de sesión K, en que el árbol incluye una raíz y varios nodos, teniendo cada nodo al menos una etiqueta asociada, y en el que cada subconjunto incluye todas las hojas de un subárbol con raíces en algún nodo v_i que no están en el subárbol con raíces en algún otro nodo v_j que desciende de v_i.

El presente invento comprende adecuadamente un receptor potencialmente sin estado en un sistema multidifusión, que comprende: al menos un dispositivo de almacenamiento de datos que almacena varias etiquetas de nodos que no están en un trayecto directo entre el receptor y una raíz de un árbol que tiene una hoja que representa al receptor, pero que cuelga del trayecto directo y que son inducidos por algún nodo v_i, representando un antepasado de la hoja el receptor, estableciendo las etiquetas de información privada I_u del receptor utilizable por el receptor para descifrar claves de subconjuntos derivadas de las etiquetas.

Preferiblemente, el receptor calcula las claves de subconjuntos de todos los conjuntos excepto un conjunto de trayecto directo que tienen raíces en el nodo v_i evaluando una función seudoaleatoria, pero no pueden calcular ninguna otra clave de subconjunto.

Preferiblemente, el receptor descifra una clave de sesión usando al menos una clave de subconjunto, siendo útil la clave de sesión para descifrar el contenido.

El presente invento comprende adecuadamente un receptor de contenido, que comprende: medios para almacenar información derivada respectiva I_u; medios para recibir al menos una clave K de cifrado de sesión cifrada con varias claves de subconjuntos, cifrando la clave de sesión el contenido; y medios para obtener al menos una clave de subconjunto usando la información privada de tal modo que la clave de sesión K puede ser descifrada para reproducir el contenido.

Preferiblemente, el receptor está dividido en uno de un conjunto de grupos $S_i,...S_w$, en los que "w" es un entero, y los grupos establecen subárboles en un árbol definiendo nodos y hojas.

Preferiblemente, subconjuntos $S_{i1},...S_{im}$ derivados del conjunto de grupos $S_i,...S_w$ definen una cubierta.

Preferiblemente, el receptor recibe el contenido en al menos un mensaje que define un encabezamiento, y el encabezamiento incluye como máximo r*log(N/r) claves de subconjuntos y cifrados, en los que r es el número de receptores en un conjunto revocado R y N es el número total de receptores.

Preferiblemente, el receptor debe almacenar log N claves, en las que N es el número total de receptores.

Preferiblemente, el receptor recibe el contenido en al menos un mensaje que define un encabezamiento, y en el que el receptor procesa el mensaje usando como máximo log log N operaciones más una única operación de descifrado, en la que N es el número total de receptores.

Preferiblemente, un conjunto revocado R define un árbol de expansión, y subárboles que tienen raíces unidas a nodos del árbol de expansión definen los subconjuntos.

Preferiblemente, al árbol incluye una raíz y varios nodos, teniendo cada nodo al menos una etiqueta asociada, y en el que cada subconjunto incluye todas las hojas de un subárbol con raíces en algún nodo v_i que no están en el subárbol con raíces en algún otro nodo v_j que desciende de v_i.

Preferiblemente, el receptor recibe el contenido en un mensaje que tiene un encabezamiento que incluye como máximo 2r-1 claves de subconjuntos y cifrados, donde r es el número de receptores en el conjunto revocado R.

Preferiblemente, el receptor debe almacenar $0{,}5\log^2 N + 0{,}5\log N + 1$ claves, en las que N es el número total de receptores.

Preferiblemente, el contenido es proporcionado al receptor en al menos un mensaje, y en el que el receptor procesa el mensaje usando como máximo log N operaciones más una única operación de descifrado, en la que N es el número total de receptores.

Preferiblemente, el receptor descifra la clave de subconjunto evaluando un generador de secuencia seudoaleatorio.

De modo adecuado, el presente invento comprende un receptor de contenido, que comprende: un almacenamiento de datos que almacena información derivada respectiva I_u; un dispositivo de tratamiento que recibe al menos una clave K de cifrado de sesión cifrada con varias claves de subconjuntos, cifrando la clave de sesión el contenido; obteniendo el dispositivo de tratamiento al menos una clave de subconjunto usando la información privada de tal modo que la clave de sesión K puede ser descifrada para reproducir el contenido.

Preferiblemente, el receptor está dividido en uno de un conjunto de grupos $S_1,...S_w$, en los que "w" es un entero, y los grupos establecen subárboles en un árbol.

Preferiblemente, subconjuntos $S_{i1},...S_{im}$ derivados del conjunto de grupos $S_1,...S_w$ definen una cubierta.

Preferiblemente, el receptor recibe el contenido en al menos un mensaje que define un encabezamiento, y el encabezamiento incluye como máximo r*log(N/r) claves de subconjuntos y cifrados, en el que r es el número de receptores en un conjunto revocado R y N es el número total de receptores.

Preferiblemente, el receptor debe almacenar log N claves, en las que N es el número total de receptores.

Preferiblemente, el receptor recibe el contenido en al menos un mensaje que define un encabezamiento, y en el que el receptor procesa el mensaje usando como máximo log log N operaciones más una única operación de descifrado, en la que N es el número total de receptores.

Preferiblemente, un conjunto revocado R define un árbol de expansión, y subárboles que tienen raíces unidas a nodos del árbol de expansión definen los subconjuntos.

Preferiblemente, el árbol incluye una raíz y varios nodos, teniendo cada nodo al menos una etiqueta asociada, y en el que cada subconjunto incluye todas las hojas de un subárbol con raíces en algún nodo v_i que no están en el subárbol con raíces en algún otro nodo v_j que desciende de v_i.

Preferiblemente, el receptor recibe el contenido en un mensaje que tiene un encabezamiento que incluye como máximo 2r-1 claves de subconjuntos y cifrados, donde r es el número de receptores en el conjunto revocado R.

Preferiblemente, el receptor debe almacenar $0{,}5\log^2 N + 0{,}5\log N + 1$ claves, en las que N es el número total de receptores.

Preferiblemente, el contenido es proporcionado al receptor en al menos un mensaje, y en el que el receptor procesa el mensaje usando como máximo log N operaciones más una única operación de descifrado, en la que N es el número total de receptores.

Preferiblemente, el receptor descifra la clave de subconjunto evaluando un generador de secuencia seudoaleatorio.

El presente invento comprende de modo adecuado un medio que contiene un mensaje de contenido de la forma general

$$<[i_1, i_2,...,i_m, E_{Li1}(K), E_{Li2}(K),...,E_{Lim}(K)], F_E(M)>,$$

en la que K es una clave de sesión, F_K es un primitivo cifrado, E_K es un primitivo cifrado, L_i son claves de subconjuntos asociadas con subconjuntos de receptores en un sistema de transmisión de cifrado, M es un cuerpo de mensaje, e $i_1, i_2,...,i_m$ son subconjuntos de nodo de árbol que definen una cubierta.

Preferiblemente, el primitivo cifrado F_K es puesto en práctica mediante la aplicación de XOR al cuerpo de mensaje con una cifra de corriente generada por la clave de sesión K.

Preferiblemente, E_L es una especificación de prefijado-truncado de una cifra de bloques, 1 representa una cadena aleatoria cuya longitud es igual a la longitud del bloque de E_L, y K es una clave corta para F_K, y el mensaje es de la forma

$$<[i_1, i_2,...,i_m, U, [Prefix_{-K-}E_{Li1}(U)]/K,..., [Prefix_{-K-}E_{Lim}(U)]/K], F_E(M)>$$

Preferiblemente, $1/i_1$ está cifrado y el mensaje es de la forma

$$<[i_1, i_2,...,i_m, U, [Prefix_{-L-}E_{Li1}(U/i_1)]/K,..., [Prefix_{-L-}E_{Lim}(U/i_m)]/K], F_E(M)>$$

Preferiblemente, las claves de subconjuntos son derivadas de un árbol que incluye una raíz y varios nodos, teniendo cada nodo al menos una etiqueta asociada, y en el que cada subconjunto incluye todas las hojas de un subárbol con raíces en algún nodo v_i que no están en un subárbol con raíces en algún otro nodo v_j que desciende de v_i.

Preferiblemente, las claves de subconjuntos son derivadas de un árbol que incluye una raíz y varios nodos, teniendo cada nodo al menos una etiqueta asociada, y en el que cada subconjunto incluye todas las hojas de un subárbol con raíces en algún nodo v_i, estando asociado al menos cada nodo del subárbol con una clave de subconjunto respectiva.

Preferiblemente, el acto de dividir es realizado por un ordenador del sistema en un sistema de receptores separado del ordenador del sistema.

Preferiblemente, el acto de dividir es realizado por un ordenador del receptor.

Preferiblemente, el receptor deriva los subconjuntos en la cubierta.

El invento incluye de modo adecuado un sistema de ordenador para realizar la lógica del invento aquí descrita. El invento puede también ser puesto en práctica en un producto de programa de ordenador que almacena la lógica actual y que puede ser accedido por un procesador para ejecutar la lógica. También el invento puede incluir de modo adecuado un método implantado en un ordenador que sigue la lógica descrita a continuación.

El invento incluye de modo adecuado un método para agrupar usuarios en subconjuntos de usuarios (posiblemente solapándolos), teniendo cada subconjunto una única clave de subconjunto preferiblemente de vida larga, y asignando a cada usuario una información privada respectiva I_u. El método incluye también de modo adecuado seleccionar al menos una clave K cifrado de sesión preferiblemente de vida corta, y dividir a los usuarios que no están en un conjunto revocado R en subconjuntos disjuntos $S_{i1},...S_{im}$ que tienen claves de subconjuntos asociadas $L_{i1},...L_{im}$. La clave de sesión K es cifrada adecuadamente con las claves de subconjuntos $L_{i1},...L_{im}$ para hacer m versiones cifradas de la clave de sesión K. En un aspecto, los usuarios pueden establecer hojas en un árbol tal como un árbol binario completo, y los subconjuntos $S_{i1},...S_{im}$ son inducidos por el árbol.

En una realización preferida, los usuarios son inicialmente divididos en grupos $S_1,...S_w$ en los que "w" es un entero. Una transmisión dada selecciona adecuadamente m de tales grupos como una "cubierta" para usuarios no revocados, estando definida la cubierta por el conjunto de usuarios revocados. Los grupos de "cubierta" establecen adecuadamente subárboles (o bien subárboles completos o bien una diferencia entre dos subárboles) en un árbol. Una información privada de usuario I_u es encontrada preferiblemente como información i_j en un mensaje transmitido que indica que un usuario pertenece a un subconjunto S_{ij} de uno de los grupos $S_1,...S_w$. Una clave de subconjunto L_{ij} puede entonces ser obtenida a partir de la información privada del usuario o derivada usando la misma.

En una primera realización, denominada aquí como el método de "subárbol completo", grupos respectivos corresponden a todos los subárboles posibles en el árbol completo. Cada usuario tiene asignadas claves desde todos los nulos que están en un trayecto directo entre una hoja que representar al usuario y la raíz del árbol. En otras palabras, cada subconjunto S_i incluye todas las hojas de un subárbol con raíces en algún nodo v_i, estando asociado al menos cada

nodo del subárbol con una clave de subconjunto respectiva. En esta realización, el contenido es proporcionado a los usuarios en un mensaje que define un encabezamiento, y el encabezamiento incluye como máximo r*log(N/r) claves de subconjuntos y cifrados, en el que r es el número de usuarios en el conjunto revocado R y N es el número total de usuarios. Además, cada usuario debe almacenar log N claves, y cada usuario procesa el mensaje usando como máximo log log N operaciones más una única operación de descifrado.

En una segunda realización, denominada aquí como el método "diferencia de subconjuntos", grupos de usuarios respectivos corresponden a un universo de conjuntos $S_1,...S_w$ que puede ser descrito como "un primer subárbol A menos un segundo subárbol B que está totalmente contenido en A". Cada nodo de este árbol tiene un conjunto de etiquetas, una única al nudo y otras que son inducidas por nodos antepasados. Cada usuario tiene etiquetas asignadas desde todos los nodos que cuelgan desde nodos en un trayecto directo entre el receptor y la raíz (como máximo log N etiquetas para cada uno de tales nodos) pero no desde los nodos en el propio trayecto directo. En otras palabras, cada subconjunto incluye todas las hojas de un subárbol con raíces en algún nodo v_i, que no están en un subárbol con raíces en algún otro nodo v_j que desciende desde v_i. Una de las etiquetas de los nodos de diferencia de subconjuntos para un usuario particular es proporcionada al usuario en una transmisión como esa información privada del usuario. Usando las etiquetas, el usuario puede generar las claves de subconjuntos necesaria para el descifrado.

En esta realización, el encabezamiento del mensaje incluye como máximo 2r-1 (1,25r de promedio) claves de subconjuntos y cifrados, cada usuario debe almacenar $0,5\log^2 N + 0,5\log N + 1$ claves, y cada usuario procesa el mensaje usando como máximo log N operaciones (preferiblemente aplicaciones de un generador seudoaleatorio) más una única operación de descifrado.

Como se ha descrito adicionalmente a continuación con respecto al método de diferencia de subconjuntos, el conjunto revocado R define un árbol de expansión. Un árbol de cubierta T es inicializado como el árbol de expansión, y a continuación el método elimina iterativamente nodos del árbol de cubierta T y añade subárboles al árbol de cubierta T hasta que el árbol de cubierta tiene como máximo un nodo. El árbol de cubierta T es usado para identificar claves de subconjuntos que han de ser usadas en una transmisión particular, con usuarios evaluando el generador de secuencia seudoaleatorio para derivar claves de subconjuntos a partir de las etiquetas. Preferiblemente, para procesar revocaciones con eficiencia son tratados de izquierda a derecha de tal modo que solamente deben ser conservadas en memoria dos revocaciones al mismo tiempo.

En algunas puestas en práctica específicas, el encabezamiento del mensaje incluye una función criptográfica E_L, y el método incluye el prefijado-truncado de la función de prefijo criptográfica E_L. Si se desea, partes del mensaje pueden ser cifradas con claves de sesión respectivas.

En otro aspecto, un dispositivo de programa de ordenador incluye de modo adecuado un dispositivo de almacenamiento de programa de ordenador que a su vez incluye un programa de instrucciones que puede ser usado por un ordenador. El programa incluye medios lógicos para acceder a un árbol para obtener varias claves de subconjuntos, y medios lógicos para cifrar un mensaje con una clave de sesión. Hay también previstos medios lógicos para cifrar la clave de sesión al menos una vez con cada una de las claves de subconjuntos para hacer versiones cifradas de la clave de sesión. A continuación, medios lógicos envían las versiones cifradas de las claves de sesión en un encabezamiento del mensaje a varios receptores sin estado.

Aún en otro aspecto, un ordenador está adecuadamente programado con instrucciones para hacer que el ordenador cifre el contenido de transmisión, y envíe el contenido de transmisión a varios receptores buenos sin estado y al menos a un receptor revocado de tal modo que cada receptor bueno sin estado pueda descifrar el contenido y el receptor revocado no pueda descifrar el contenido.

En otro aspecto, un receptor potencialmente sin estado u en un sistema de cifrado de transmisión incluye de modo adecuado un almacenamiento de datos que almacena información privada respectiva I_u, y un dispositivo de tratamiento que recibe una clave de cifrado de sesión K que está cifrada con varias claves de subconjuntos. La clave en la sesión cifra el contenido, obteniendo el dispositivo de tratamiento al menos una clave de subconjunto usando la información privada de tal modo que la clave de sesión K puede ser descifrada para reproducir el contenido. En una realización preferida, el receptor está dividido en uno de un conjunto de grupos $S_1,...S_w$ en los que "w" es un entero, y los grupos establecen subárboles en un árbol. Subconjuntos $S_{i1},...S_{im}$ derivados del conjunto de grupos $S_1,...S_w$ definen una cubierta que es calculada por el receptor o por un ordenador del sistema. Preferiblemente, el árbol incluye una raíz y varios nodos, teniendo cada nodo al menos una etiqueta asociada. Cada subconjunto incluye todas las hojas de un subárbol con raíces en algún nodo v_i que no están en él subárbol con raíces en algún otro nodo v_j que desciende de v_i.

En otro aspecto, un medio contiene adecuadamente un mensaje de contenido de la forma general $<[i_1, i_2,...,i_m, E_{Li1}(K), E_{Li2}(K),...,E_{Lim}(K)], F_E(M)>$, en el que K es una clave de sesión, F_K es un primitivo cifrado, E_K es un primitivo cifrado, L_i son claves de subconjuntos asociadas con subconjuntos de receptores en un sistema de transmisión de cifrado, M es un cuerpo de mensaje, e $i_1, i_2,...,i_m$ son subconjuntos de nodo de árbol que definen una cubierta.

Breve descripción de los dibujos

A continuación se describirán realizaciones preferidas del presente invento, a modo de ejemplo solamente, con referencia a los dibujos adjuntos, en los que:

La fig. 1 es un diagrama de bloques del sistema actual;

La fig. 2 es un diagrama de flujo de la lógica de cifrado completa;

La fig. 3 es un diagrama de flujo de la lógica de descifrado completa;

La fig. 4 es un diagrama de flujo de la parte de asignación de claves del letrado de subárbol completo;

La fig. 5 es un diagrama de flujo de la parte de cifrado del método de subárbol completo;

La fig. 6 es un diagrama de flujo de la parte de descifrado del método de subárbol completo;

La fig. 7 es un diagrama esquemático de un subconjunto de un subárbol completo;

La fig. 8 es un diagrama esquemático de un subconjunto en el método de diferencia de subconjuntos; y

La fig. 9 es otra forma de un diagrama esquemático del subconjunto en el método de diferencia de subconjuntos;

La fig. 10 es un diagrama de flujo de la lógica para definir una cubierta en el método de diferencia de subconjuntos;

La fig. 11 es un diagrama esquemático de un subconjunto de un árbol en el método de diferencia de subconjuntos, que ilustra asignación de claves;

La fig. 12 es un diagrama de flujo de las partes de descifrado del método de diferencia de subconjuntos;

La fig. 13 es un diagrama de flujo de la lógica para asignar claves en el método de diferencia de subconjuntos; y

La fig. 14 es un diagrama esquemático de un subconjunto de un árbol en el método de diferencia de subconjuntos.

Descripción detallada de las realizaciones preferidas

Con referencia inicialmente a la fig. 1, se ha mostrado un sistema, generalmente designado con 10, para generar conjuntos de claves en un sistema de protección de contenido de transmisión, tal como el sistema descrito en la patente antes referenciada pero no limitado al mismo. Con el término "transmisión" quiere significarse la amplia diseminación de un programa desde un proveedor de contenidos a muchos usuarios simultáneamente sobre cables (desde una fuente de satélite), o hilo, o radiofrecuencia (incluyendo desde una fuente de satélite), o desde discos de contenido ampliamente comercializados.

Como se ha mostrado, el sistema 10 incluye un ordenador 12 de definición del conjunto de claves que accede a un módulo 14 de definición de conjunto de claves que funciona de acuerdo con la descripción siguiente. Los conjuntos de claves definidos por el ordenador 12 son usados por dispositivos 16 reproductores-grabadores potencialmente sin estado, también denominados aquí como "receptores" y "usuarios", que tienen procesadores dentro de ellos para descifrar el contenido. El contenido junto con ciertas claves descritas a continuación es proporcionado a los dispositivos respectivos mediante, por ejemplo fabricantes de dispositivos 16 sobre medios 17. Un dispositivo reproductor-grabador puede acceder a su conjunto de claves para descifrar el contenido en medios o transmisión o hacerlo a través de comunicación inalámbrica. Como se ha usado aquí el término "medios" puede incluir pero no está limitado a los DVD, CD, unidades de disco duro y dispositivos de memoria "flash". En una realización alternativa, cada receptor 16 podría ejecutar el módulo 14 para realizar la operación de calcular la "cubierta" más abajo descrita al dárseles el conjunto de receptores revocados y realizar la lógica descrita a continuación.

Ha de comprenderse que el procesador asociado con el módulo 14 accede a los módulos para emprender la lógica mostrada y descrita a continuación, que puede ser ejecutada por un procesador como una serie de instrucciones ejecutables por ordenador. Dos métodos - el método de subárbol completo, y el método de diferencia de subconjuntos - están descritos aquí para usar el sistema 10 para revocar selectivamente la capacidad de los receptores comprometidos 16 para descifrar el contenido de transmisión sin revocar la capacidad de cualquier receptor 16 no comprometido para descifrar el contenido de transmisión.

Las instrucciones pueden estar contenidas en un dispositivo de almacenamiento de datos con un medio legible por ordenador, tal como un disquete de ordenador que tiene un medio utilizable por ordenador con elementos de código legibles por ordenador almacenados en él. O, las instrucciones pueden estar almacenadas en una agrupación DASD, cinta magnética, unida de disco duro tradicional, memoria electrónica solo de lectura, dispositivo de almacenamiento óptico, u otro dispositivo de almacenamiento de datos apropiado. En una realización ilustrativa del invento, las instrucciones ejecutables por ordenador pueden ser líneas de código compatible C++ compilado.

Además, los diagramas de flujo ilustran aquí la estructura de la lógica de una realización preferida del presente invento como realizada en software de programa de ordenador. Los expertos en la técnica apreciarán que los diagrama de flujo ilustran las estructuras de elementos de código de programa de ordenador que incluyen circuitos lógicos en un circuito integrado, que funciona de acuerdo con este invento. De modo manifiesto, el invento es puesto en práctica

en su realización esencial por un componente de máquina que convierte los elementos de código de programa en una forma que instruye a un aparato de tratamiento digital (es decir un ordenador) a realizar una secuencia de actos de función correspondientes a los mostrados.

La lógica completa de una realización preferida del presente invento como es llevada a cabo tanto por el método de diferencia de subconjuntos como por el método de subárbol completo puede ser vista en referencia a la fig. 2. Con propósitos de la presente exposición, se supone que existen N receptores 16 en el sistema 10, y que es deseable ser capaz de revocar la capacidad de r receptores en un subconjunto receptor revocado R para descifrar el contenido incluso si los receptores revocados actúan en una coalición (compartiendo conocimiento de cifrado), de tal modo que cualquier receptor pueda aún descifrar contenido. Comenzando en el bloque 19, el sistema es iniciado asignando claves de subconjuntos de vida larga $L_1,...L_w$ a subconjuntos correspondientes en un universo de subconjuntos $S_1,...S_w$ en los que los receptores son agrupados de acuerdo con la exposición siguiente, teniendo así cada subconjunto S_j una clave de subconjunto de larga vida L_j asociada con él. En el primer método ("subárbol completo"), los subconjuntos que cubren receptores que no están en un conjunto revocado son simplemente los subconjuntos que son generados por la exposición siguiente. En el segundo método ("diferencia de subconjuntos"), los subconjuntos que cubren los receptores que no están en un conjunto revocado son definidos por la diferencia entre un primer subárbol y un subárbol menor que está totalmente dentro del primer subárbol como se ha descrito adicionalmente a continuación.

En el bloque 20, el sistema es además iniciado suministrando a cada receptor u con información privada L_u que es útil para descifrar el contenido. Detalles de la información privada I_u son descritos adicionalmente a continuación. Si I_u es la información secreta proporcionada al receptor u, entonces cada receptor u en S_j puede deducir L_j de su I_u. Como se ha descrito más completamente a continuación, dado el conjunto revocado R, los receptores no revocados son divididos en m subconjuntos disjuntos $S_{i1},...S_{im}$ y una clave de sesión K de vida corta es cifrada m veces con las claves de subconjuntos de vida larga $L_{i1},...L_{im}$ asociadas con subconjunto respectivos $S_{i1},...S_{im}$. Las claves de subconjuntos son claves de subconjuntos explícitas en el método de subárbol completo y son inducidas por etiquetas de subconjunto en el método de diferencia de subconjuntos.

Específicamente, en el bloque 22 al menos una clave de sesión K es seleccionada con la que cifrar el contenido que es transmitido en un mensaje M, bien mediante trayectos de comunicación inalámbricos o por cable o bien mediante medios de almacenamiento tales como CD y DVD. La clave de sesión K es una cadena aleatoria de bits que es seleccionada de nuevo para cada mensaje. Si se desea, pueden usarse varias claves de sesión para cifrar partes respectivas del mensaje M.

En ambos métodos descritos a continuación, los receptores no revocados son divididos en subconjuntos disjuntos $S_{i1},...S_{im}$ en el bloque 24 usando un árbol. Los subconjuntos son a veces denominados aquí como "subárboles", considerando el primer método explícitamente subárboles y siendo en lo que se refiere al segundo método subárboles de la forma "un primer subárbol menos un segundo subárbol totalmente contenido en el primero". Cada subconjunto $S_{i1},...S_{im}$ está asociado con una clave de subconjunto respectiva $L_{i1},...L_{im}$. Aunque se ha considerado aquí cualquier estructura a modo de árbol de datos, con propósito de exposición se ha supuesto que el árbol es un árbol binario completo.

Continuando al bloque 26, en general la clave de sesión K es cifrada m veces, una vez con cada clave de subconjunto $L_{i1},...L_{im.}$ El texto cifrado resultante que es transmitido puede ser representado como sigue, representando las partes entre paréntesis el encabezamiento del mensaje M y representando i_1, i_2,..., i_m índices de los subconjuntos disjuntos:

$$<[i_1, i_2,...,i_m, E_{Li1}(K), E_{Li2}(K),...,E_{Lim}(K)], F_E(M)>$$

En una realización, el primitivo cifrado F_K es puesto en práctica por aplicación de XOR al mensaje M con una cifra de corriente generada por la clave de sesión K. El primitivo cifrado E_L es un método para entregar la clave de sesión a los receptores 16, usando las claves de subconjuntos de larga vida. Ha de comprenderse que todos los algoritmos de cifrado para F_K, E_L están dentro del marco de una realización preferida del presente invento. Una puesta en práctica preferida de E_L puede ser una especificación de Prefijado-Truncado de una cifra de bloque. Se supone que 1 representa una cadena aleatoria cuya longitud es igual a la longitud del bloque de E_L, y se supone que K es una clave corta para la cifra F_K cuya longitud es por ejemplo de 56 bits. A continuación, $[Prefix_{-K-}E_L(1)/K]$ proporciona un cifrado fuerte. Por consiguiente, el encabezamiento de Prefijo-Truncado resulta:

$$<[i_1, i_2,...,i_m, U, [Prefix_{-K-}E_{Li1}(U)]/K,..., [Prefix_{-K-}E_{Lim}(U)]/K], F_E(M)>$$

Esto reduce ventajosamente la longitud del encabezamiento a aproximadamente m-K- bits en vez de m-L-. En el caso en que la longitud de clave de E_L es mínima, puede usarse lo siguiente para eliminar el factor de ventaja m que un adversario tiene en un ataque con fuerza bruta lo que procede como resultado de cifrar la misma cadena 1 con m claves diferentes. La cadena $1/i_j$ está cifrada. Es decir:

$$<[i_1, i_2,...,i_m, U, [Prefix_{-L-}E_{Li1}(U/i_1)]/K,...,[Prefix_{-L-}E_{Lim}(U/i_m)]/K], F_E(M)>$$

Habiendo descrito modos preferidos, no limitativos para poner en práctica los primitivos E y F de cifrado, la atención se dirige ahora a la fig. 3, que muestra la lógica de descifrado realizada por los receptores 16. Comenzando en el bloque 28, cada receptor u no revocado encuentra un identificador de subconjunto i_j en el texto cifrado de tal modo que pertenece al subconjunto S_{ij}. Como se ha descrito adicionalmente a continuación, si el receptor está en el conjunto revocado R, el resultado del bloque 28 será nulo. A continuación, en el bloque 30 el receptor extrae la clave de subconjunto L_{ij} correspondiente al subconjunto S_{ij} usando su información privada I_u. Usando la clave de subconjunto, la clave de sesión K es determinada en el bloque 32, y a continuación el mensaje es descifrado en el bloque 34 usando la clave de sección K.

A continuación se han descrito dos métodos preferidos para realizar la lógica completa antes descrita. En cada uno, la colección de subconjuntos es especificada, como lo es el modo en que las claves son asignadas a los subconjuntos y un método para cubrir receptores no revocados usando subconjuntos disjuntos de la colección. En cada uno, el conjunto de receptores en el sistema establece las hojas de un árbol, tal como un árbol binario completó pero no estando limitado al mismo.

El primer método que se va a describir es el método de subárbol completo mostrado en las figs. 4-7. Comenzando en el bloque 36 en la fig. 4, una clave de subconjunto independiente y aleatoria L_i es asignada a cada nodo v_i en el árbol. Esta clave de subconjunto L_i corresponde a un subconjunto que contiene todas las hojas con raíces en el nodo v_i. A continuación, en el bloque 38, cada receptor u es provisto con todas las claves de subconjuntos en el trayecto directo desde el receptor a la raíz. Como se ha ilustrado a modo de referencia en la fig. 7, los receptores u en el subconjunto S_i son proporcionados con la clave de subconjunto L_i asociada con el nodo v_i, así como con las claves asociadas con el nodo P, que se encuentra entre los receptores en S_i y la raíz del árbol.

Cuando se desea enviar un mensaje y revocar la capacidad de algunos receptores para descifrar el mensaje, la lógica de la fig. 5 es invocada para la división de receptores no revocados en subconjuntos disjuntos. Comenzando en el bloque 40, un árbol de expansión es descubierto que está definido por las hojas en R, el conjunto de receptores revocados. El árbol de expansión es el subárbol mínimo del árbol binario completo que conecta las hojas "revocadas", y puede ser un árbol de Steiner. Continuando al bloque 42, los subárboles que tienen raíces adyacentes a nodos de grado uno en el árbol (es decir nodos que son directamente adyacentes al árbol mínimo) están identificados. Estos subárboles definen una "cubierta" y establecen los subconjuntos $S_{i1},...S_{im}$. La cubierta abarca a todos los receptores no revocados. Por consiguiente, en el bloque 44 la clave de sesión K es cifrada usando las claves de subconjuntos definidas por la cubierta.

Para descifrar el mensaje, cada receptor invoca a la lógica de la fig 6. Comenzando en el bloque 46, se ha determinado si cualquier nodo antepasado del receptor está asociado con una clave de subconjunto de la cubierta determinando si cualquier nodo antepasado está entre el conjunto $i_1, i_2,..., i_m$ en el encabezamiento del mensaje. La información privada del receptor I_u, que en el método del subárbol completo consiste de su posición en el árbol y claves de subconjuntos asociadas a nodos antepasados, es usada para determinar este. Si se ha encontrado un antepasado en el encabezamiento de mensaje (indicando que el receptor es un receptor no revocado), la clave de sesión K es descifrada en el bloque 48 usando la clave de subconjunto, y a continuación el mensaje es descifrado usando la clave de sesión K en el bloque 50.

En el método del subárbol completo, el encabezamiento incluye como máximo r*log(N/r) claves de subconjuntos y cifrados. Este es también el número de claves y cifrados promedio. Además, cada receptor debe almacenar log N claves, y cada receptor procesa el mensaje usando como máximo log log N operaciones más una única operación de descifrado.

Con referencia ahora a las figs. 8-13, puede ser visto el método de diferencia de subconjuntos para revocar receptores. En el método de diferencia de subconjuntos, cada receptor debe almacenar relativamente más claves ($0{,}5\log^2 N + 0{,}5\log N + 1$ claves)que en el método de subárbol completo, pero el encabezamiento del mensaje incluye sólo como máximo 2r-1 claves de subconjuntos y cifrados (1,25r de promedio), y éste es sustancialmente más corto que en el método de subárbol completo. También, en el método de diferencia de subconjuntos, el mensaje es procesado usando como máximo log N aplicaciones de un generador de números seudoaleatorio más una sola operación de descifrado.

Con referencia a las figs. 8 y 9, el método de diferencia de subconjuntos considera los subconjuntos como la diferencia entre un subconjunto A mayor y un subconjunto B menor que está totalmente contenido en A. Por consiguiente, como se ha mostrado un subárbol mayor tiene raíces en el nodo v_i y un subárbol menor tiene raíces en el nodo v_j que desciende desde v_i. El subconjunto resultante S_{ij} consiste de todas las hojas "sí" bajo v_i excepto para aquellas hojas etiquetadas "no" (y coloreadas más oscuras que las hojas etiquetadas "sí") bajo v_j. La fig. 9 ilustra esto, estando representado el subconjunto $v_{i,j}$ por el área situada dentro del triángulo mayor y fuera del triángulo menor.

Cuando se ha deseado enviar un mensaje y revocar la capacidad de algunos receptores para descifrar el mensaje en el método de diferencia de subconjuntos, la estructura antes descrita es usada como se ha mostrado en la fig. 10. Comenzando en el bloque 52, se ha descubierto que un árbol de expansión está definido por las hojas en R, el conjunto de receptores revocados. El árbol de expansión es el subárbol mínimo del árbol binario completo que conecta las hojas "revocadas", y puede ser un árbol de Steiner. Continuando al bloque 54, un árbol de cubierta T es inicializado como el árbol de expansión. Un bucle iterativo comienza entonces en el que son retirados nodos del árbol de cubierta y son añadidos subárboles a la cubierta hasta que el árbol de cubierta T tiene como máximo un nodo. La salida define la cubierta para los receptores no revocados.

Más específicamente, moviéndose desde el bloque 54 al bloque 56, las hojas v_i y v_j son encontradas en el árbol de cubierta de tal modo que su antepasado menos común v no contiene otras hojas en T. En el diamante de decisión 57 se ha determinado si sólo existe una hoja en el árbol de cubierta T. Si existe más de una sola hoja, la lógica se mueve al bloque 58 para encontrar nodos v_i, v_k en v, de tal modo que v_i desciende desde v_1 y v_j desciende desde v_k y de tal modo que v_1, v_k son hijos de v (es decir descendientes directos de v sin ningún nodo de intervención entre v y v_1, v_k). En contraste, cuando sólo existe una única hoja en T, la lógica se mueve desde el diamante de decisión 57 al bloque 60 para ajustar $v_i = v_j$ = única hoja restante, colocar v en la raíz de T, y ajustar $v_1 = v_k$ = raíz.

Desde el bloque 58 o 60 la lógica se mueve al diamante de decisión 62. En el diamante de decisión 62, se ha determinado si v_1 es igual a v_i. Si v_1 no es igual a v_i la lógica se mueve al bloque 64 para añadir el subconjunto $S_{1,i}$ a T, retirar de T todos los descendientes de v y hacer v una hoja. De modo similar, si v_k no es igual a v_j la lógica se mueve al bloque 64 para añadir el subconjunto $S_{k,j}$ a T, retirar todos los descendientes de v, y hacer v una hoja. Desde el bloque 64 o desde el diamante de decisión 62 cuando no se ha determinado una desigualdad, la lógica forma un bucle de nuevo al bloque 56.

Con la anterior vista completa del método de asignación de claves por diferencia de subconjuntos en mente, se describe a continuación una puesta en práctica particularmente preferida. Mientras el número de subconjuntos total a los que pertenece un receptor es tan grande como N, estos subconjuntos pueden ser agrupados en log N grupos definidos por el primer subconjunto i (desde el que es sustraído otro subconjunto). Para cada $1<i<N$ correspondiente a un nodo interior en el árbol completo, es seleccionada una etiqueta independiente y aleatoria $LABEL_1$, que induce a las etiquetas para todos los subconjuntos legitimados de la forma $S_{i,j}$. A partir de las etiquetas, son derivadas las claves de subconjuntos. La fig. 11 ilustra el método de etiquetado preferido descrito a continuación. El nodo etiquetado L_i es la raíz del subárbol T, y sus descendientes son etiquetados de acuerdo con los principios actuales.

Si G es un generador de secuencia criptográfico seudoaleatorio que triplica la longitud de entrada, G_L(S) indica el tercero por la izquierda de la salida de G en la semilla S, G_R(S) indica el tercero por la derecha, y G_M(S) indica el tercero en el centro. Considerando el subárbol T_i del árbol de cubierta T con raíces en el nodo v_i con etiqueta $LABEL_i$. Si éste nodo está etiquetado S, sus dos hijos son etiquetados G_L(S) y G_R(S) respectivamente. La clave de subconjunto $L_{i,j}$ asignada al conjunto $S_{i,j}$ es la G_M de la etiqueta $LABEL_{i,j}$, de nodo v_j derivada del subárbol T_i. Obsérvese que cada etiqueta S induce tres partes, en particular, las etiquetas para los hijos izquierdo y derecho, y la clave del nodo. Por consiguiente, dada la etiqueta de un nodo es posible calcular las etiquetas y claves de todos sus descendientes. En una realización preferida, la función G es una función de cálculo de clave ("hash") criptográfica tal como el Algoritmo-1 de Cálculo de Clave Seguro (SHA-1), aunque pueden usarse otras funciones.

La fig. 12 muestra cómo los receptores descifran mensajes en el método de diferencia de subconjuntos. Comenzando en el bloque 66, el receptor encuentra el subconjunto $S_{i,j}$ al que pertenece, junto con la etiqueta asociada (que es parte de la información privada del receptor que le permite derivar la $LABEL_{i,j}$ y la clave de subconjuntos $L_{i,j}$). Usando la etiqueta, al receptor calcula la clave de subconjunto $L_{i,j}$ evaluando la función G como máximo N veces en el bloque 68. A continuación, el receptor usa la clave de subconjuntos para descifrar la clave de sesión K en el bloque 70 para un subsiguiente descifrado de mensaje.

La fig. 13 muestra cómo las etiquetas y, por tanto las claves de subconjuntos, son asignadas a receptores en el método de diferencia de subconjuntos. El método de etiquetado descrito aquí es usado para minimizar el número de claves que cada receptor debe almacenar.

Comenzando en el bloque 72, cada receptor está provisto con etiquetas de nodos que no están en el trayecto directo entre el receptor y la raíz pero que "cuelgan" del trayecto directo y que son inducidas por alguno nodo v_i, un antepasado de u. Estas etiquetas establecen la información privada I_u del receptor en el bloque 74, siendo cifradas subsiguientes claves de sesión de mensajes con claves de subconjuntos derivadas de las etiquetas en el bloque 76.

Con referencia brevemente a la fig. 14, se ha ilustrado el principio anterior. Para cada v_i antepasado con etiqueta S de un receptor u, el receptor u recibe etiquetas en todos los nodos 71 que están colgando del trayecto directo desde el nodo v_i al receptor u. Como se ha descrito adicionalmente a continuación, estas etiquetas están derivadas todas preferiblemente desde S. En marcado contraste con el método de subárbol completo, en el método de diferencia de subconjuntos ilustrado en las figs. 8-14 el receptor u no recibe etiquetas desde ningún nodo 73 que está en el trayecto directo desde el receptor u al nodo v_i. Usando las etiquetas, el receptor u puede calcular las claves de subconjuntos de todos los conjuntos (excepto el conjunto de trayecto directo) que tienen raíces en el nodo v_i evaluando la función G antes descrita, pero no puede calcular ninguna otra clave de subconjunto.

Los sistemas multidifusión tradicionales carecen de secreto hacia atrás, es decir un receptor que escucha constantemente que ha sido revocado sin embargo puede grabar todos los contenidos cifrados, y luego alguna vez en el futuro ganar una clave nueva válida (por ejemplo, mediante un nuevo registro) que permite el descifrado del contenido pasado. Una realización preferida del presente invento puede ser usada en tales escenarios para curar la falta de secreto hacia atrás incluyendo, en el conjunto de receptores revocados todas las identidades de receptores que no han sido aún asignadas. Esto puede hacerse si todo los receptores están asignados a hojas en orden consecutivo. En este caso, la revocación de todas las identidades sin asignar da como resultado un aumento moderado en el tamaño del encabezamiento del mensaje, pero no proporcionalmente al número de tales identidades.

Una realización preferida del presente invento también reconoce que es deseable tener codificaciones concisas de los subconjuntos i_j en el encabezamiento de mensaje y proporcionar un modo rápido para que un receptor determine si pertenece a un subconjunto i_j. Se supone que un nodo está indicado por su trayecto a la raíz, con 0 indicando una rama izquierda y 1 indicando una rama derecha. El final del trayecto está indicado por un 1 seguido por cero o más bits 0. Así, la raíz es 1000...000b, el hijo más a la derecha de la raíz es 01000...000b, el hijo más a la izquierda es 11000...000b, y una hoja es xxxx...xxxx1b.

Como se ha reconocido aquí, el trayecto de una raíz de subárbol mayor es un subconjunto del trayecto de una raíz de subárbol menor, de modo que la diferencia de subconjuntos puede ser indicada por la raíz del menor subárbol más la longitud del trayecto a la raíz del mayor subárbol. Con esto en mente, un receptor puede determinar rápidamente si está en un subconjunto dado ejecutando el siguiente bucle del procesador Intel Pentium®.

Fuera del bucle, se ajustan los siguientes registros: ECX contiene el nodo de hoja del receptor, ESI apunta a la memoria tampón del mensaje (el primer byte es la longitud del trayecto a la raíz del mayor subárbol y los siguientes cuatro bytes son la raíz del árbol menor), y una tabla estática emite 32 bits cuando es indexada por la longitud del trayecto, siendo los primeros bits de longitud 1 y siendo los bits restantes 0.

```
bucle: MOV BYTE EBX, [ESI++]
            MOV DWORD EAX, [ESI++]
            XOR EAX, ECX
                AND EAX, TABLE[EBX]
            JNZ bucle
```

Si un receptor cae fuera del bucle, eso no significa necesariamente que pertenezca al subconjunto particular. Podría estar en el subárbol menor excluido, y si es así, debe volver al bucle. Sin embargo, como en la vasta mayoría de casos el receptor no está incluso ni en el subárbol mayor, casi no se gasta tiempo de tratamiento en el bucle.

En otra optimización del método de diferencia de subconjuntos, el servidor del sistema no tiene que recordar cada etiqueta y todas ellas, lo que podría convertirse en millones. En vez de ello la etiqueta del 1er nodo puede ser una función secreta del nodo. La función secreta podría ser un cifrado triple DES que usa una clave secreta para hacer la etiqueta del 1 nodo cuando es aplicada al número i.

REIVINDICACIONES

1. Un método para cifrado o codificado de transmisión, que comprende: asignar a cada usuario en un grupo de usuarios información privada respectiva I_u; seleccionar al menos una clave de cifrado de sesión K; dividir a los usuarios que no están en un conjunto revocado R en subconjuntos disjuntos $S_{i1},...S_{im}$ que tienen claves de subconjuntos asociadas $L_{i1},...L_{im}$; y cifrar la clave de sesión K con las claves de subconjuntos $L_{i1},...L_{im}$ para hacer m versiones cifradas de la clave de sesión K.

2. El método según la reivindicación 1, que comprende además dividir a los usuarios en grupos $S_1,...S_w$, en los que "w" es un entero, y los grupos establecen subárboles en un árbol.

3. El método según la reivindicación 2, en el que cada subconjunto $S_{i1},...S_{im}$ incluye todas las hojas de un subárbol con raíces en algún nodo v_i, estando asociado al menos cada nodo en el subárbol con una clave de subconjunto respectiva.

4. El método según la reivindicación 3, en el que el contenido es proporcionado a los usuarios en al menos un mensaje que define un encabezamiento, y el encabezamiento incluye como máximo r*log(N/r) claves de subconjuntos y cifrados, en los que r es el número de usuarios en el conjunto revocado R y N es el número total de usuarios.

5. El método según la reivindicación 3, en el que el conjunto revocado R define un árbol de expansión, y los subconjuntos que tienen raíces unidas a nodos del árbol de expansión definen los subconjuntos.

6. El método según cualquiera de las reivindicaciones 2 a 5, en el que el árbol incluye una raíz y varios nodos, teniendo cada nodo al menos una etiqueta asociada, y en el que cada subconjunto incluye todas las hojas de un subárbol con raíz en algún nodo v_i que no está en él subárbol con raíces en algún otro nodo v_j que desciende desde v_i.

7. El método según la reivindicación 6, en el que el contenido es proporcionado a los usuarios en al menos un mensaje que define un encabezamiento, y el encabezamiento incluye como máximo 2r-1 claves de subconjuntos y cifrados, en la que r es el número de usuarios en el conjunto revocado R.

8. El método según cualquiera de las reivindicaciones 6 a 7, en el que el conjunto revocado R define un árbol de expansión, y en el que el método incluye: inicializar un árbol de cubierta T como el árbol de expansión; retirar iterativamente nodos desde el árbol de cubierta T y añadir nodos a una cubierta hasta que el árbol de cubierta T tiene como máximo un nodo.

9. El método según cualquiera de las reivindicaciones 6 a 8, en el que cada nodo tiene al menos una etiqueta inducida posiblemente por al menos uno de sus antepasados, y en el que cada usuario tiene asignadas etiquetas desde todos los nodos que cuelgan de un trayecto directo entre el usuario y la raíz pero no desde nodos en el trayecto directo.

10. Un programa de ordenador que comprende un código de programa de ordenador para, cuando es cargado en un sistema de ordenador y ejecutado, hace que dicho sistema de ordenador realice las operaciones de un método según se ha reivindicado en cualquiera de las reivindicaciones 1 a 9.

11. Un aparato para cifrado de transmisión, que comprende: medios para asignar a cada usuario en un grupo de usuarios de información privada I_u respectiva de usuarios; medios para seleccionar al menos una clave de cifrado de sesión K; medios para dividir a los usuarios que no están en un conjunto revocado R en subconjuntos disjuntos $S_{i1},...S_{im}$ que tienen claves de subconjuntos asociadas $L_{i1},...L_{im}$; y medios para cifrar las claves de sesión K con las claves de subconjuntos $L_{i1},...L_{im}$ para hacer m versiones cifradas de la clave de sesión K.

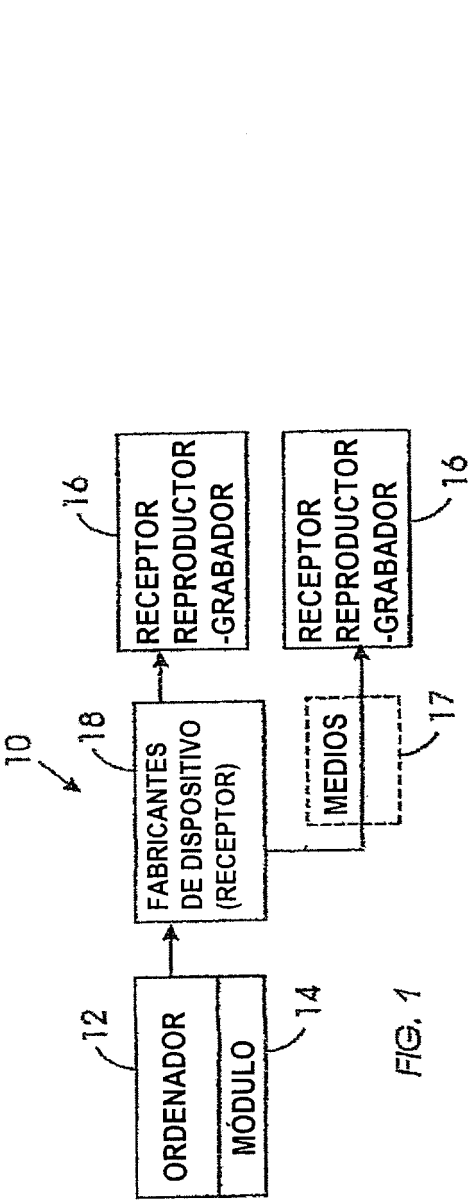

FIG. 1

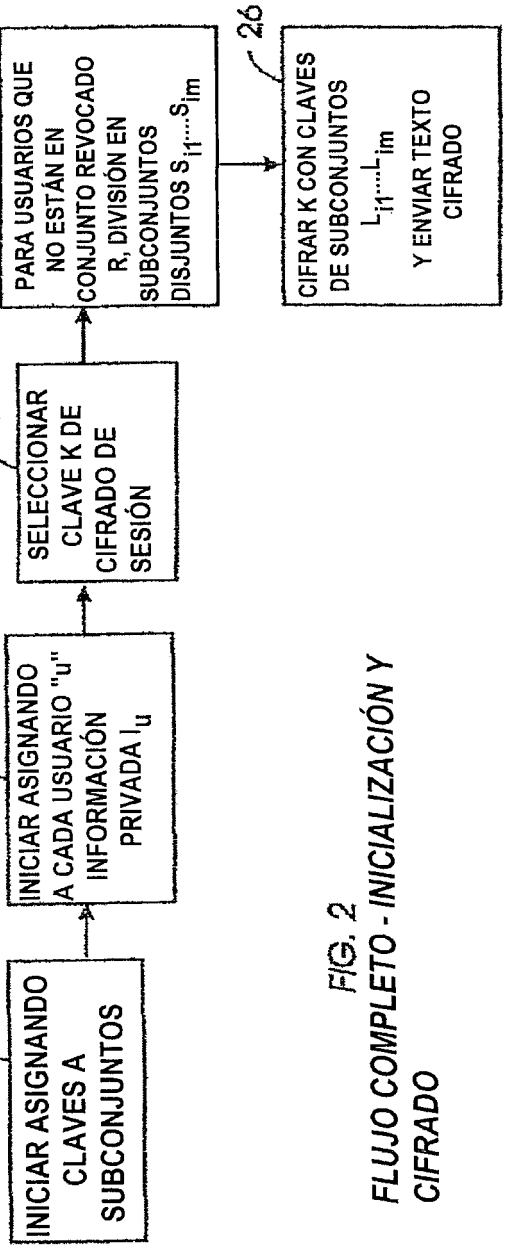

FIG. 2

FLUJO COMPLETO - INICIALIZACIÓN Y CIFRADO

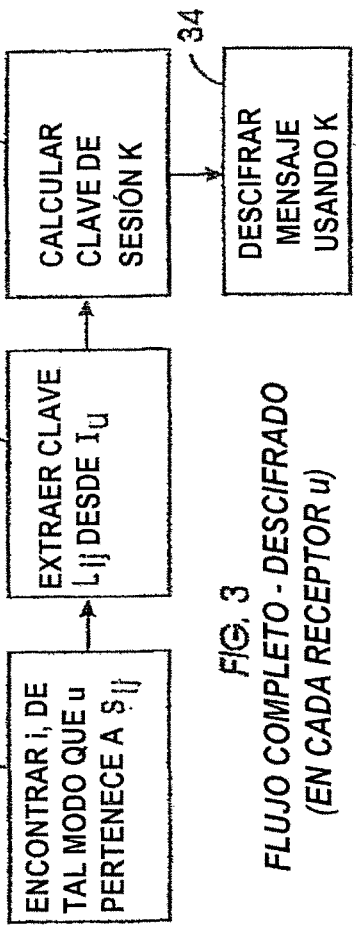

FIG. 3
FLUJO COMPLETO - DESCIFRADO (EN CADA RECEPTOR u)

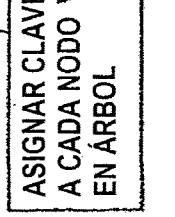

FIG. 4 - ASIGNACIÓN DE CLAVE, SUBÁRBOL COMPLETO

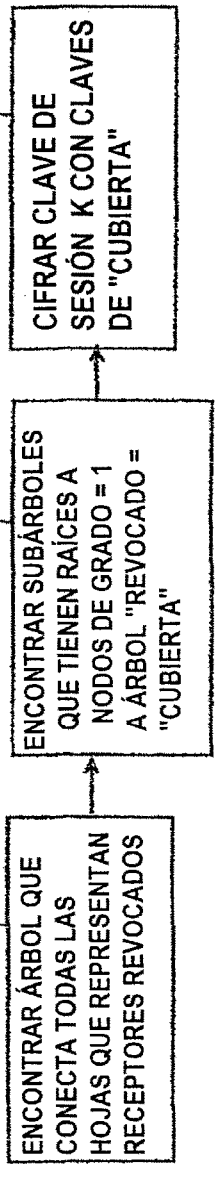

FIG. 5 - SUBÁRBOL COMPLETO CIFRADO USANDO "CUBIERTA"

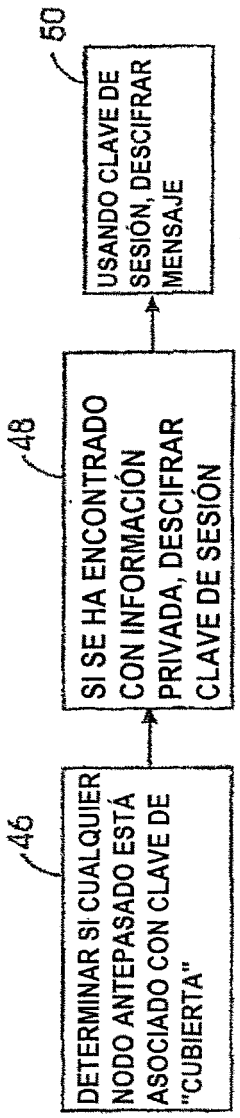

FIG. 6 - DESCIFRADO SUBÁRBOL COMPLETO

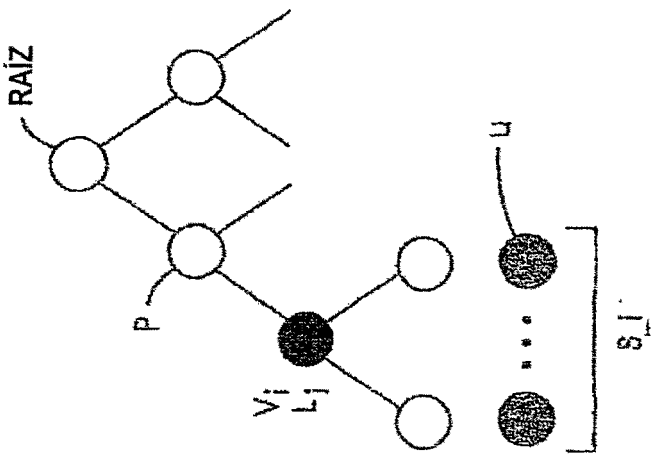

FIG. 7 - SUBÁRBOL COMPLETO

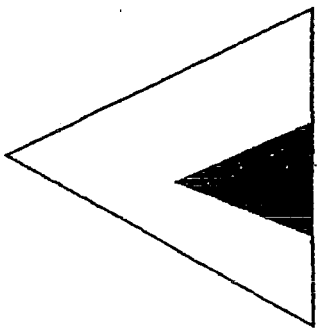

FIG. 9

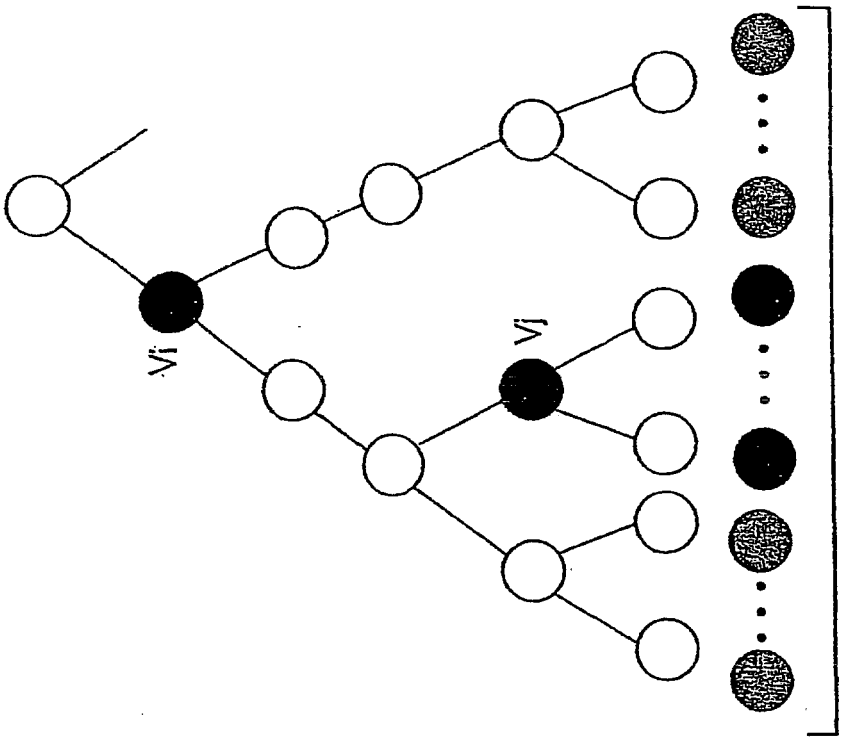

FIG. 8

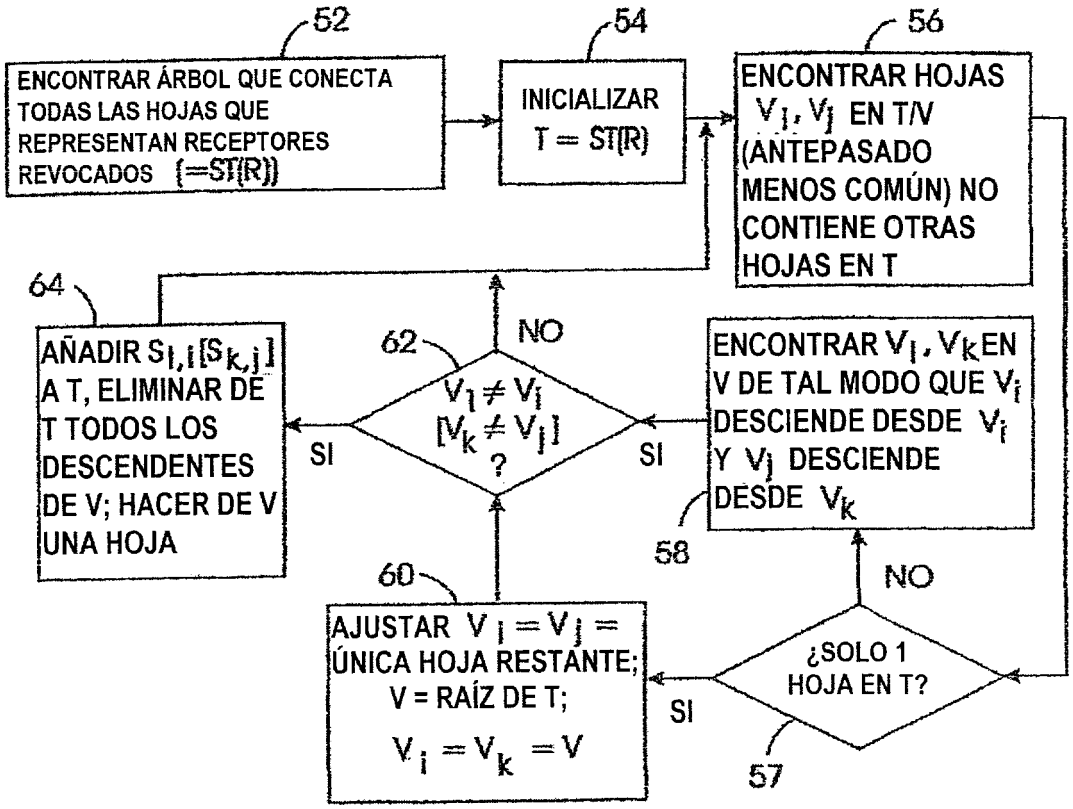

FIG. 10
DEFINICIÓN DE CUBIERTA
DIFERENCIA DE SUBCONJUNTOS

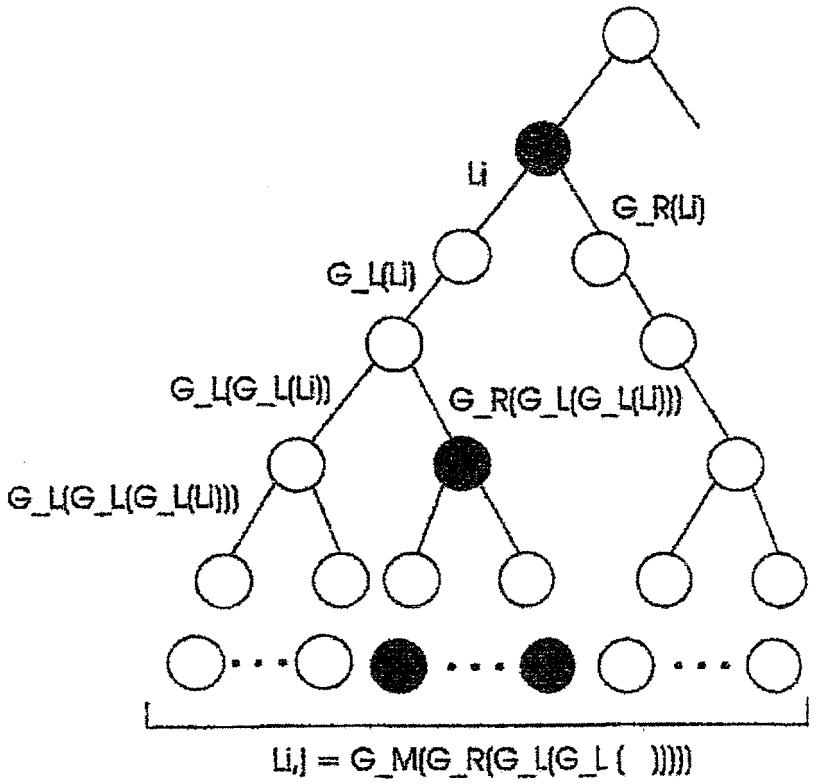

FIG. 11 - ASIGNACIÓN DE CLAVE EN MÉTODO DE DIFERENCIA DE SUBCONJUNTOS

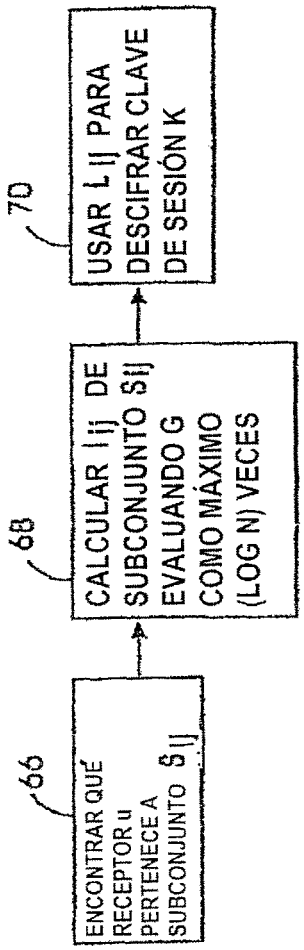

FIG. 12
DESCRIPCIÓN, DIFERENCIA DE SUBCONJUNTOS

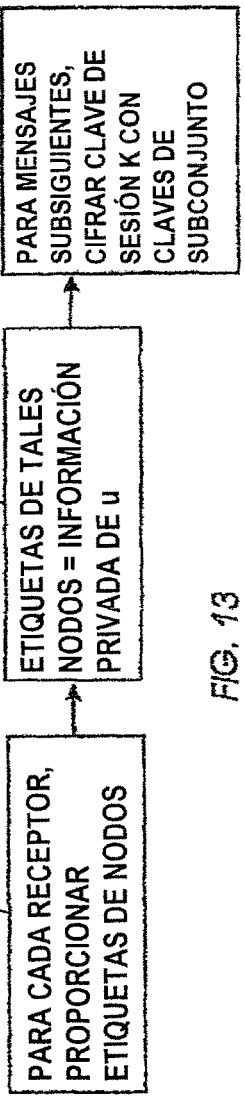

FIG. 13
ASIGNACIÓN DE CLAVES - DIFERENCIA DE SUBCONJUNTOS

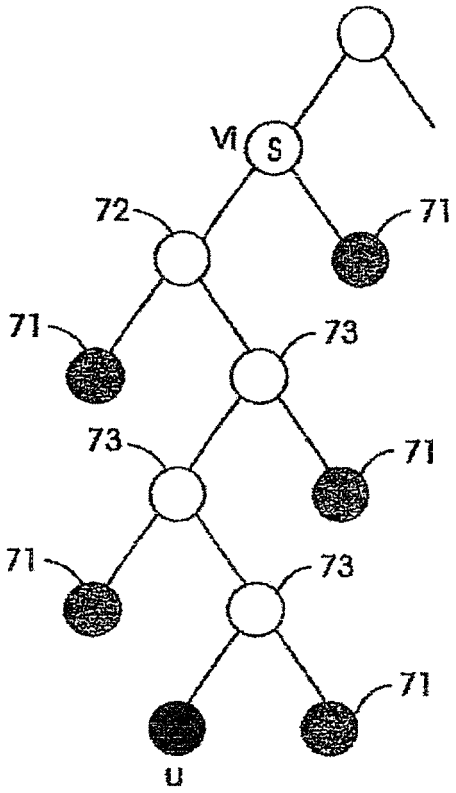

FIG. 14 - ASIGNACIÓN DE ETIQUETAS MÉTODO DE DIFERENCIA DE SUBCONJUNTOS