(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 302 979**

(51) Int. Cl.:
H04N 7/167 (2006.01)
H04L 9/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **03810011 .1**
(86) Fecha de presentación : **22.12.2003**
(87) Número de publicación de la solicitud: **1576820**
(87) Fecha de publicación de la solicitud: **21.09.2005**

(54) Título: **Procedimiento y sistema de protección de datos aleatorizados.**

(30) Prioridad: **24.12.2002 FR 02 16650**

(45) Fecha de publicación de la mención BOPI:
01.08.2008

(45) Fecha de la publicación del folleto de la patente:
01.08.2008

(73) Titular/es: **Viaccess**
Les Collines de l'Arche, Tour Opéra C
92057 Paris La Défense Cédex, FR

(72) Inventor/es: **Merle, Gilles y**
Bangui, François

(74) Agente: **Justo Vázquez, Jorge Miguel de**

DESCRIPCIÓN

Procedimiento y sistema de protección de datos aleatorizados.

Campo técnico

La invención se sitúa en el campo del control de acceso a datos aleatorizados.

Se refiere más específicamente a un procedimiento de protección de datos aleatorizados proporcionados a una pluralidad de terminales receptores, estando cada uno de dichos terminales dotado de una pluralidad de módulos de desaleatorización Mj (j=1...M) que tienen cada uno una capacidad de tratamiento y un nivel de seguridad específica, estando previamente dichos datos subdivididos en un número entero de familias Fj (j=1...M) que comprenden cada una un número entero de bloques Bi (i=1...N), estando cada bloque Bi (l=1...N) de una familia Fj aleatorizado por una clave Kj (j=1...M) asociada a la familia Fj.

Los terminales receptores son equipos móviles (ME) (Mobile Equipment en inglés) destinados al público en general tales como, por ejemplo, teléfonos móviles, agendas electrónicas denominadas PDA (Personal Digital Assistant en inglés) o también receptores audiovisuales u ordenadores.

La invención se refiere también a un sistema de protección de datos y/o servicios que comprende una plataforma de aleatorización y una plataforma de desaleatorización destinadas a la aplicación del procedimiento.

Los datos que hay que proteger son obras literarias o artísticas protegidas por un sistema digital de gestión de derechos DRM (Digital Right Management). Estas obras se pueden, por ejemplo, memorizar en un soporte tal, como por ejemplo, un CD-ROM o un DVD, o se pueden transmitir o descargar a partir de un servidor remoto hacia una pluralidad de terminales receptores conectados a una red de transmisión.

Estado de la técnica anterior

En los sistemas de protección de datos de la técnica anterior, el contenido que hay que proteger (audio, vídeo, texto) se aleatoriza en el domicilio del operador y lo descifra durante la recepción en el domicilio del abonado un algoritmo de desaleatorización memorizado en el terminal receptor.

Un inconveniente importante de estos sistemas procede del hecho de que en el momento de la recepción, se desaleatoriza todo el contenido distribuido por un mismo módulo de desaleatorización. Igualmente, en caso de pirateo, la totalidad de este contenido se vuelve accesible y por lo tanto se puede redistribuir de manera fraudulenta en redes ilícitas.

Una primera solución conocida para paliar este problema consiste en confinar el módulo de desaleatorización en un local de acceso protegido. Esta solución no está adaptada a las aplicaciones en las cuales los terminales son de uso destinado al público general.

Una segunda solución, basada en el refuerzo de la seguridad del propio receptor, consiste en impedir la instalación en el terminal de cualquier software sospechoso y autorizar la instalación únicamente de softwares “certificados”, es decir, softwares para los cuales se ha emitido una autorización de descarga.

Esta solución tampoco está adaptada a las aplicaciones mencionadas anteriormente que utilizan receptores “abiertos” provistos de una interfaz de entrada - salida que permiten descargar cualquier tipo de softwares (ordenadores, receptores de audio y de vídeo) por oposición a los terminales “bloqueados” de fábrica, tales como los descodificadores por ejemplo, para impedir que un abonado descargue de manera fraudulenta softwares de desaleatorización. La solicitud europea EP0984630 describe un procedimiento de protección de datos aleatorizados proporcionados a una pluralidad de terminales receptores donde cada terminal está dotado de dos módulos de desaleatorización, un terminal de tipo PC y una tarjeta SIM. En este procedimiento, cada primer bloque de un grupo de x bloques se envía a y lo desaleatoriza la tarjeta SIM mientras que los otros bloques los desaleatoriza el PC.

El objetivo de la invención es paliar los inconvenientes de la técnica anterior anteriormente mencionados.

Exposición de la invención

La invención preconiza un procedimiento de protección de datos aleatorizados proporcionados a una pluralidad de terminales receptores en el cual cada uno de dichos terminales está dotado de una pluralidad de módulos de desaleatorización Mj (J=1...M) que tienen cada uno una capacidad de tratamiento y un nivel de seguridad específicos, y en el cual los datos se subdividen previamente en un número entero de familias Fj (j=1...M) que comprenden cada uno un número entero de bloques Bi (i=1...M), aleatorizándose a continuación cada bloque Bi (i=1...N) de una familia Fj mediante una clave Kj (j=1...M) asociada a la familia Fj.

Según la invención dichos bloques B1 (i=1....N) se organizan previamente en función de las respectivas velocidades de tratamiento de los módulos de desaleatorización Mj.

Según la invención, los módulos Mj (j=1...M) son elementos periféricos diferentes asociados a dicho terminal receptor.

Gracias a la invención, un ataque a uno de los módulos Mj (j=1...M) permite reconstruir un fichero que no está completo ya que falta la parte tratada por los otros módulos. El fichero pirateado se degradará en gran medida respecto del original y por lo tanto no se podrá utilizar.

En una primera realización, los módulos de desaleatorización Mj (j=1...M) comprenden algoritmos Aj (j=1...M) diferentes.

En una segunda realización, los módulos de desaleatorización Mj (j=1...M) comprenden algoritmos Aj (j=1...M) idénticos.

En las dos realizaciones, los datos que se han de distribuir se presentan en forma de un fichero previamente memorizado o en forma de un flujo difundido en tiempo real.

En una aplicación particular del procedimiento según la invención, el flujo de datos representa programas de audio y/o de vídeo o dibujos animados (animación multimedia), o también imágenes de síntesis protegidas por un sistema DRM.

La invención se refiere también a un sistema de protección de datos aleatorizados que comprende una plataforma de aleatorización y una plataforma de desaleatorización.

La plataforma de aleatorización comprende:

- medios para subdividir dicho flujo de m familias distintas de N bloques Bi (i=1...N),

- medios para asignar a cada familia un parámetro específico de identificación pj (j=1...M) asociado a al menos un módulo de desaleatorización Mj que tiene una capacidad de tratamiento y un nivel de seguridad específicos,

- medios para aleatorizar cada bloque Bi por una clave Kj (j=1...M) en relación biunívoca con el parámetro pj.

Según una característica esencial de la invención, dicha plataforma de desaleatorización comprende medios para identificar la familia de cada bloque Bi para desaleatorizar cada bloque Bi de una familia de tipo pj por el módulo Mj que corresponde a dicho parámetro pj.

Según una realización preferida, la plataforma de desaleatorización comprende una pluralidad de módulos distintos de desaleatorización Mj (i=1...M).

En una variante de realización de la invención, los datos que se han de proteger son programas audiovisuales difundidos a una pluralidad de abonados dotados de licencia de utilización gestionada por un sistema DRM.

El equipo móvil puede ser una PDA o un teléfono móvil dotado de una tarjeta inteligente de tipo SIM (Subscriber Identity Module, en inglés).

En este caso, los datos se reparten entre un primer módulo de desaleatorización M1 integrado en la PDA (respectivamente en el teléfono móvil) y un segundo módulo de desaleatorización M2 constituido por la propia tarjeta inteligente.

Breve descripción de los dibujos

Otras características y ventajas de la invención se harán evidentes en la siguiente descripción, tomada a título de ejemplo no limitativo en referencia a las figuras anexas en las cuales:

la figura 1 ilustra esquemáticamente una etapa de tipificación de datos que hay que proteger por el procedimiento según la invención,

la figura 2 ilustra esquemáticamente una etapa de aleatorización de una familia de datos obtenida por la etapa anterior,

la figura 3 ilustra esquemáticamente una primera realización de la primera y la segunda etapa del procedimiento según la invención,

la figura 4 representa esquemáticamente la fase de desaleatorización de las familias de datos obtenidos por las etapas anteriores,

la figura 5 representa una realización preferida de la etapa ilustrada por la figura 4,

la figura 6 representa esquemáticamente un terminal que aplica el procedimiento según la invención,

La figura 7 representa un diagrama temporal que ilustra esquemáticamente el tratamiento por el procedimiento según la invención de un flujo de datos difundidos o descargados en tiempo real por el terminal,

La figura 8 representa un diagrama temporal que ilustra la gestión de las claves de aleatorización del flujo de la figura 7.

Exposición detallada de realizaciones particulares

La siguiente descripción se refiere a una aplicación de la invención en la cual los datos aleatorizados representan programas de audio y/o de vídeo difundidos o descargados hacia una PDA (por Personal Digital Assistant) dotada de una tarjeta inteligente de tipo SIM. La PDA comprende un primer módulo M1 de desaleatorización, siendo un segundo módulo de desaleatorización la propia tarjeta SIM.

Los datos que hay que proteger se pueden descargar a partir de un soporte de grabación (CD, DVD...) o a partir de un servidor especializado (música, vídeo, dibujos animados, tonos telefónicos, libro electrónico E-book...).

También se pueden difundir en una red.

Cualquiera que sea la aplicación considerada y el tipo de datos, antes de la distribución de estos datos, el procedimiento comprende:

- una primera fase de tratamiento que comprende:

una etapa de tipificación que consiste en formar m familias Fj (j=1...M) de datos que comprenden cada una un número nj de bloques de datos Bi (i=1...N), identificándose cada familia mediante un parámetro pj,

una etapa de aleatorización de cada bloque Bi de una familia Fj mediante una clave Kj (j=1...M) en relación biunívoca con el parámetro pj;

- y al recibir los datos mediante un terminal, éstos experimentan una segunda fase de tratamiento que comprende:

una etapa de identificación de la familia de cada bloque Bi recibido,

una etapa de desaleatorización de cada bloque Bi mediante la clave Kj por un módulo Mj (j=1...M) identificado por un parámetro pj.

Según una característica esencial de la invención, los módulos Nj (j=1...M) que permiten desaleatorizar los bloques Bi de dos familias distintas son diferentes.

Estos pueden bien ser diferentes periféricos asociados al terminal receptor, o softwares independientes guardados en la memoria del terminal o de un periférico.

Caso de un fichero de datos previamente memorizado

Tipificación

La figura 1 representa un fichero 2 de datos de audio y/o de vídeo organizados en bloques denominados unidades de acceso AU (Access Unit) según la norma MPEG 4 (Motion Picture Expert Group).

Una primera etapa 4 del procedimiento consistir en recortar el fichero 2 en m familias Fj (j=1...m) que comprenden cada una un número entero nj de bloques Bi (i=1...N); Cada familia Fj está identificada por parámetro pj (j=1...m).

El parámetro pj identifica también el módulo Mj que se encargará de desaleatorizar los bloques Bi de la familia Fj.

En la aplicación descrita, el fichero se recorta en dos familias F_1 y F_2 cuyos respectivos bloques se desaleatorizarán respectivamente por un módulo M1 integrado en la PDA y por la tarjeta SIM que constituye el módulo M2.

Durante la tipificación, se asocia un parámetro p1 a la familia F1 de bloques Bi que se desaleatorizarán por el módulo M1 y se asocia un parámetro p2 a la familia F_2 de bloques B_i que los desleatorizará la tarjeta SIM.

Aleatorización

La figura 2 ilustra una segunda etapa 6 a lo largo de la cual los bloques Bi de una familia F_j se aleatorizan mediante una clave K_j (j=1,2) definida en función de la capacidad de tratamiento y del grado de seguridad respectivos del módulo M_1 integrado en la PDA y de la tarjeta SIM. Los bloques aleatorizados B'_i se guardan en un fichero 8.

En una variante de realización del procedimiento ilustrado esquemáticamente por la figura 3, la tipificación 4 y la aleatorización 6 de un bloque B_i se realizan sucesivamente.

En otra variante de realización no representada, la aleatorización se realiza familia por familia.

El fichero 10 que contiene los bloques B'_i aleatorizados se transmite a continuación a la PDA.

Desaleatorización

La figura 4 ilustra la fase de desaleatorización de un fichero 10 que comprende distintas familias Fj de bloques MPEG previamente aleatorizados.

En la etapa 12, se identifican los bloques B'i mediante su parámetro respectivo Pj y a continuación se encaminan a los módulos de desaleatorización correspondiente M_j.

Los bloques descifrados se reacondicionan para formar el fichero de origen 2 que se proporcionará al usuario.

La figura 5 ilustra esquemáticamente una realización preferida de la aleatorización en la cual los bloques Bi contenidos en el fichero 10 se tratan arbitrariamente bloque por bloque.

Tratamiento temporal de un flujo de datos

La figura 6 representa esquemáticamente los módulos internos de una PDA que permite realizar la desaleatorización.

La PDA ilustrada comprende una etapa de entrada 20 encargada de identificar los bloques B'i en un flujo, una etapa 22 de desmultiplexado, un primer módulo de desaleatorización 24, una tarjeta inteligente que constituye un segundo módulo de desaleatorización 26, una etapa de multiplexado 28 y una etapa de salida 30.

La figura 7a ilustra esquemáticamente un flujo de datos difundido o descargado que comprende bloques Bi en formato MPEG 4.

Un primer tratamiento de este flujo, realizado a nivel del emisor, consiste en reorganizar los bloques MPEG en función de las capacidades y de las velocidades respectivas de tratamiento del módulo M1 y de la tarjeta SIM.

La figura 7b representa el flujo de la figura 7a en la cual se han creado una familia dada por bloques de tipo A y una familia formada por bloques de tipo B.

En este ejemplo, los bloques de tipo A se desaleatorizarán mediante el módulo M1 y los bloques de tipo B por la tarjeta SIM.

Debido al hecho de que la capacidad y la velocidad de tratamiento de la tarjeta SIM son inferiores a las de descodificador, en el momento de la emisión, los bloques de tipo B se desfasan tres bloques corriente arriba para compensar la diferencia de velocidad de tratamiento entre el descodificador y la tarjeta SIM.

La figura 7c representa la repartición temporal de los bloques del flujo difundido después de la aleatorización y la reorganización.

La figura 7d representa la repartición temporal de los bloques del flujo recibido por la PDA antes de la desaleatorización, y la figura 7e representa la repartición temporal de los bloques del flujo desaleatorizado.

La figura 8 ilustra esquemáticamente el mecanismo de cambio de claves para desaleatorizar los bloques del flujo tratado.

Se designa por cripto-periodo, la duración de validez de una clave de desaleatorización. Antes de cada inicio de cripto-periodo se inserta un mensaje en el flujo para prevenir al módulo de desaleatorización del cambio de cripto-periodo. Este mensaje contiene el conjunto de las informaciones necesarias para desaleatorizar el flujo durante el siguiente cripto-periodo (por ejemplo la referencia de la clave de desaleatorización que se ha de utilizar). Este mensaje se inserta en el flujo antes del inicio del cripto-periodo (inicio retrasado) para permitir que el módulo de desaleatorización trate las informaciones del mensaje y esté listo para desaleatorizar en tiempo real los datos del cripto-periodo.

Las aplicaciones

Esta invención se aplica a contenidos donde la pérdida de una parte de la información hace que el contenido no se pueda utilizar. Esto se aplica al conjunto de los contenidos de audio y de vídeo digitales comprimidos donde la pérdida de información se traduce en una degradación rápida de la calidad (audio, vídeo, Ebook, tonos de teléfonos móviles, imagen...).

Los módulos de descifrado apuntados son:

- soportes amovibles de tipo tarjeta inteligente, tarjeta inteligente sin contacto, módulo separable (PCMCIA, serie, ISB, Ethernet);

- terminales de tipo PC, servidor, descodificador digital, receptor móvil (teléfono móvil, PDA).

Los servicios

- VOD (Video On Demand) por difusión o por descarga,

- MOD (Music On Demand) por difusión o por descarga

- Difusión de libro electrónico en línea,

- Difusión de tono para teléfono móvil,

- Difusión de foto/imagen,

- Difusión de texto, documento multimedia.

REIVINDICACIONES

1. Procedimiento de protección de datos aleatorizados proporcionados a una pluralidad de terminales receptores, estando cada uno de dichos terminales dotado de una pluralidad de módulos de desaleatorización Mj (j=1...M), siendo M superior a 1, que tienen cada uno una capacidad de tratamiento y un nivel de seguridad diferente, estando previamente dichos datos subdivididos en un número entero de familias (Fj (j=1...M) que comprenden cada una un número entero de bloques Bi (i=1...N), siendo asignado a cada familia Fj un parámetro específico de identificación pj (j=1...N) asociado a un módulo de desaleatorización Mj que tiene una capacidad de tratamiento y un nivel de seguridad específicos, procedimiento **caracterizado** porque:

- en el momento de la emisión, cada bloque Bi (i=1...N_j) de una familia Fj se aleatoriza mediante una clave Kj (j=1...M) en relación biunívoca con el parámetro pj, definida en función de la capacidad de tratamiento y del grado de seguridad de los respectivos módulos de descifrado Mj (j=1...M), y

- en el momento de la recepción, cada bloque Bi (i=1...Nj) se identifica mediante su parámetro pj y lo desaleatoriza el módulo M_j mediante la clave K_j (j=1...M) asociada a la familia Fj.

2. Procedimiento según la reivindicación 1, **caracterizado** porque los módulos Mj (j=1...M) son elementos periféricos diferentes asociados a dicho terminal receptor.

3. Procedimiento según la reivindicación 2, **caracterizado** porque los módulos de desaleatorización Mj (j=1...M) comprenden algoritmos Aj (j=1...M) diferentes.

4. Procedimiento según la reivindicación 2, **caracterizado** porque los módulos de desaleatorización Mj (j=1...M) comprenden algoritmos Aj (j=1...M) idénticos.

5. Procedimiento según una de las reivindicaciones 1 a 4, **caracterizado** porque los datos que hay que distribuir se presentan en forma de un fichero previamente memorizado.

6. Procedimiento según una de las reivindicaciones 1 a 4, **caracterizado** porque los datos que hay que proteger se presentan en forma de un flujo difundido descargado y tratado en tiempo real por el terminal.

7. Procedimiento según las reivindicaciones 5 ó 6, **caracterizado** porque la duración de utilización del flujo se divide en cripto-periodos que corresponden cada uno a una clave de desaleatorización, y porque antes de cada inicio de cripto-periodo se inserta un mensaje en el flujo para prevenir el módulo de desaleatorización Mj del cambio de cripto-periodo.

8. Procedimiento según la reivindicación 7, **caracterizado** porque dicho mensaje comprende el conjunto de las informaciones necesarias para desaleatorizar el flujo utilizado durante el siguiente cripto-periodo.

9. Procedimiento según una de las reivindicaciones 1 a 8, **caracterizado** porque dichos datos representan programas de audio y/o de vídeo protegidos por un sistema DRM.

10. Procedimiento según una de las reivindicaciones 1 a 8, **caracterizado** porque dichos datos representan imágenes de síntesis o dibujos animados.

11. Sistema de protección de datos aleatorizados proporcionados a una pluralidad de terminales receptores, **caracterizado** porque comprende:

- una plataforma de aleatorización que comprende:

medios para subdividir dicho datos en M>1 familias distintas de N bloques Bi (i=1...N_j),

medios para asignar a cada familia Fj un parámetro específico de identificación pj (j=1...M) asociado a un módulo de desaleatorización Mj que tiene una capacidad de tratamiento y un nivel de seguridad diferentes,

medios para aleatorizar cada bloque Bi por una clave Kj (j=1...M) en relación biunívoca con el parámetro pj; y

- una plataforma de desaleatorización que comprende medios para identificar la familia de cada bloque Bi por su parámetro de identificación para desaleatorizar cada bloque Bi de una familia de tipo pj por el módulo Mj que corresponde a dicho parámetro pj mediante la clave Kj.

12. Sistema según la reivindicación 11, **caracterizado** porque los módulos de desaleatorización distintos Mj (i=1...M) son distintos periféricos asociados al terminal receptor.

13. Plataforma de aleatorización de un flujo de datos, **caracterizada** porque comprende:

- medios para subdividir dicho flujo de datos en M>1 familias distintas Fj (j=1...M) de N bloques Bi (i=1...N_j);

- medios para asignar a cada familia Fj (j=1...M) un parámetro específico de identificación pj (j=1...M) asociado a un módulo de desaleatorización Mj que tiene una capacidad de tratamiento y un nivel de seguridad diferentes;

- medios para definir para cada módulo Mj (j=1...M) una clave Kj (j...1...M) en función de la capacidad de tratamiento y del grado de seguridad de dicho Mj (j=1...M);

- medios para aleatorizar cada bloque Bi que pertenece a una familia Fj (j=1...M) por el módulo M_j mediante una clave Kj (j=1...M) en relación biunívoca con el parámetro pj.

14. Plataforma de desaleatorización de un flujo de datos previamente subdividido en M>1 familias distintas Fj (j=1...M) de N bloques Bi (1=1...N_j) identificadas cada una por un parámetro específico pj (j=1...M) asociado a un módulo de desaleatorización Mj que tiene una capacidad de tratamiento y un nivel de seguridad diferentes, **caracterizándose** dicha plataforma de desaleatorización porque comprende medios para identificar la familia de cada bloque Bi por su parámetro de identificación para desaleatorizar cada bloque Bi de una familia de tipo pj por el módulo Mj que corresponde a dicho parámetro pj mediante la clave Kj.

15. Plataforma de desaleatorización según la reivindicación 14, **caracterizada** porque el terminal receptor es una PDA y porque uno de dichos módulos de desaleatorización Mj (i=1...M) se integra en la PDA y al menos el segundo módulo es una tarjeta inteligente de tipo SIM conectada a dicha PDA.

16. Uso del procedimiento según una de las reivindicaciones 1 a 8 para proteger un servicio de vídeo previa petición (VOD).

17. Uso del procedimiento según una de las reivindicaciones 1 a 8 para proteger un servicio de música previa petición (MOD).

18. Uso del procedimiento según una de las reivindicaciones 1 a 8 para proteger el acceso a un servicio de difusión de libro electrónico en línea o descargado a partir de un soporte amovible.

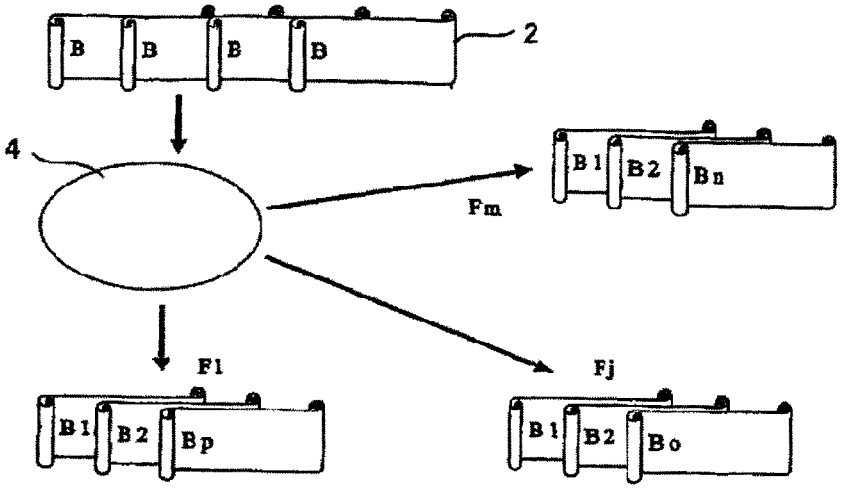
B
B
B
B
2
4
Fm
B1
B2
Bn
Fl
Fj
B1
B2
Bp
B1
B2
Bo

FIG. 1

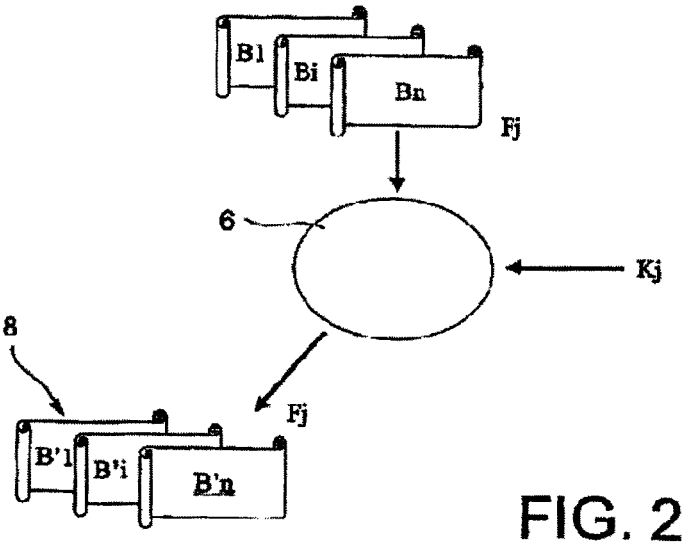
B1
Bi
Bn
Fj
6
Kj
8
Fj
B'1
B'i
B'n

FIG. 2

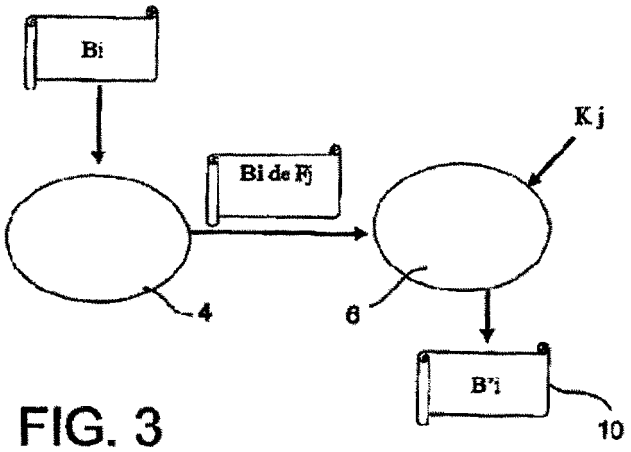
Bi
Bi de Fj
Kj
4
6
B'i
10

FIG. 3

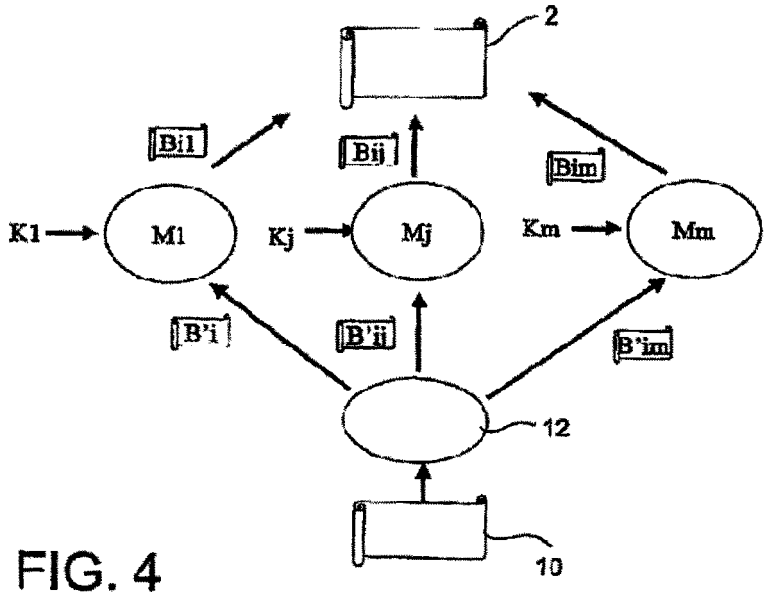
2
Bi1
Bij
Bim
K1
M1
Kj
Mj
Km
Mm
B'i
B'ij
B'im
12
10

FIG. 4

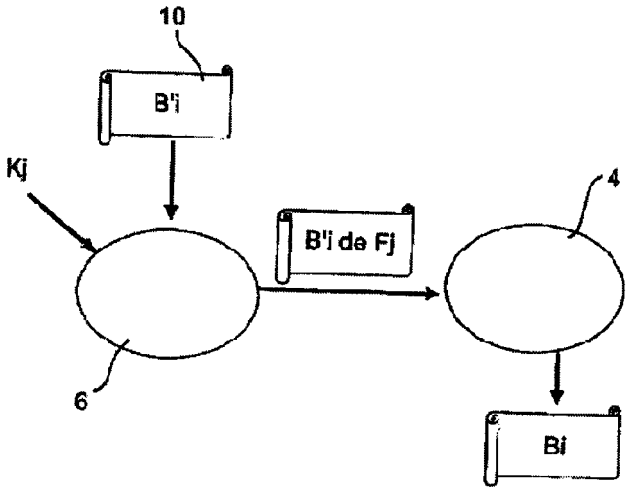

FIG. 5

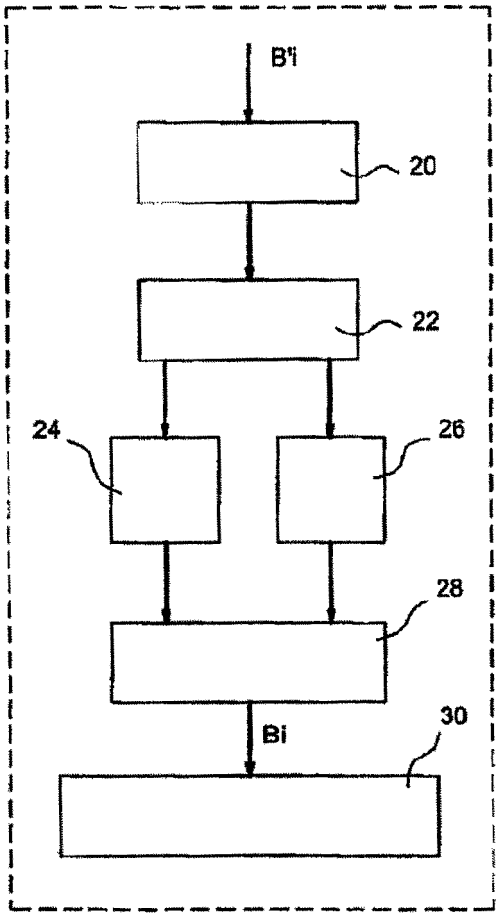

FIG. 6

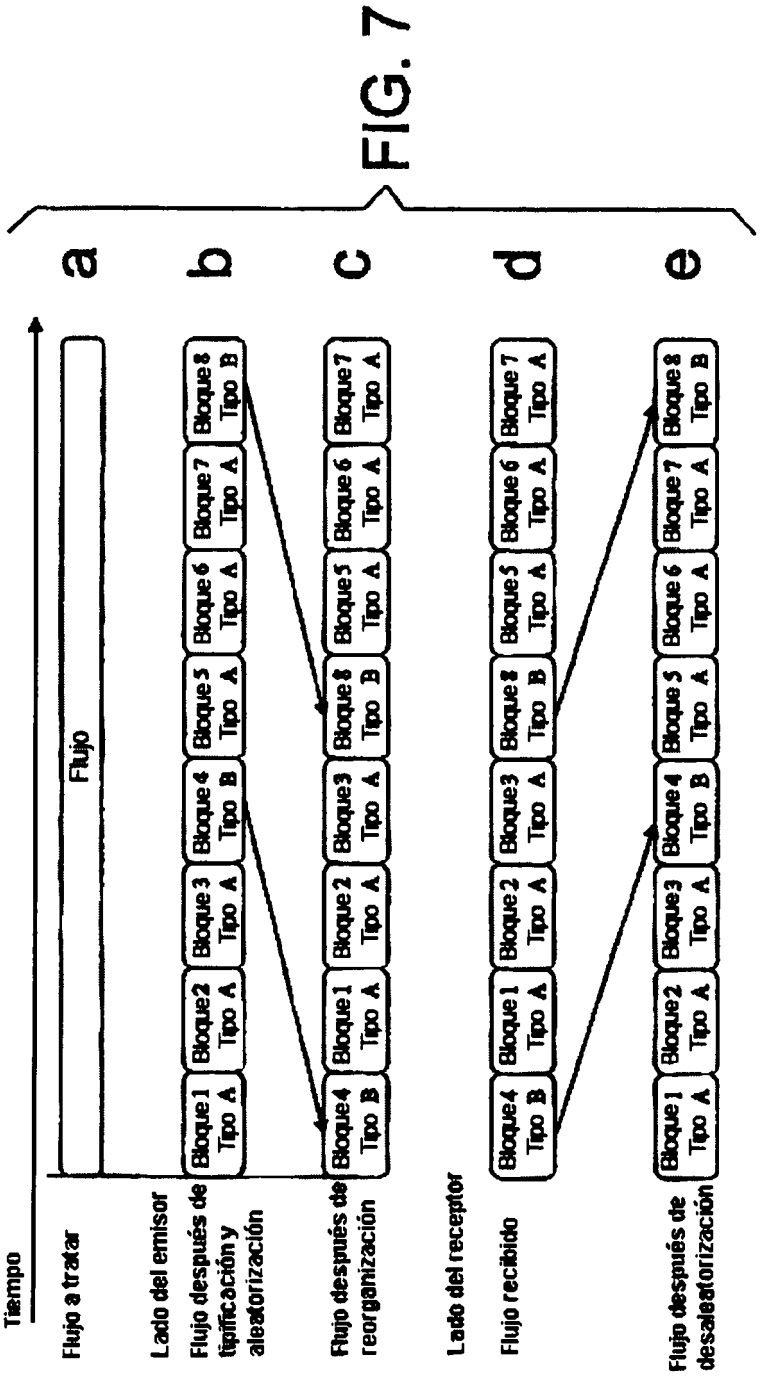
a
b
c
d
e
Tiempo
Flujo a tratar
Flujo
Lado del emisor
Flujo después de tipificación y aleatorización
Flujo después de reorganización
Lado del receptor
Flujo recibido
Flujo después de desaleatorización
Bloque 1 Tipo A
Bloque 2 Tipo A
Bloque 3 Tipo A
Bloque 4 Tipo B
Bloque 5 Tipo A
Bloque 6 Tipo A
Bloque 7 Tipo A
Bloque 8 Tipo B
Bloque 1 Tipo A
Bloque 2 Tipo A
Bloque 3 Tipo A
Bloque 4 Tipo B
Bloque 5 Tipo A
Bloque 6 Tipo A
Bloque 7 Tipo A
Bloque 8 Tipo B
Bloque 4 Tipo B
Bloque 1 Tipo A
Bloque 2 Tipo A
Bloque 3 Tipo A
Bloque 8 Tipo B
Bloque 5 Tipo A
Bloque 6 Tipo A
Bloque 7 Tipo A
Bloque 1 Tipo A
Bloque 2 Tipo A
Bloque 3 Tipo A
Bloque 4 Tipo B
Bloque 5 Tipo A
Bloque 6 Tipo A
Bloque 7 Tipo A
Bloque 8 Tipo B

FIG. 7

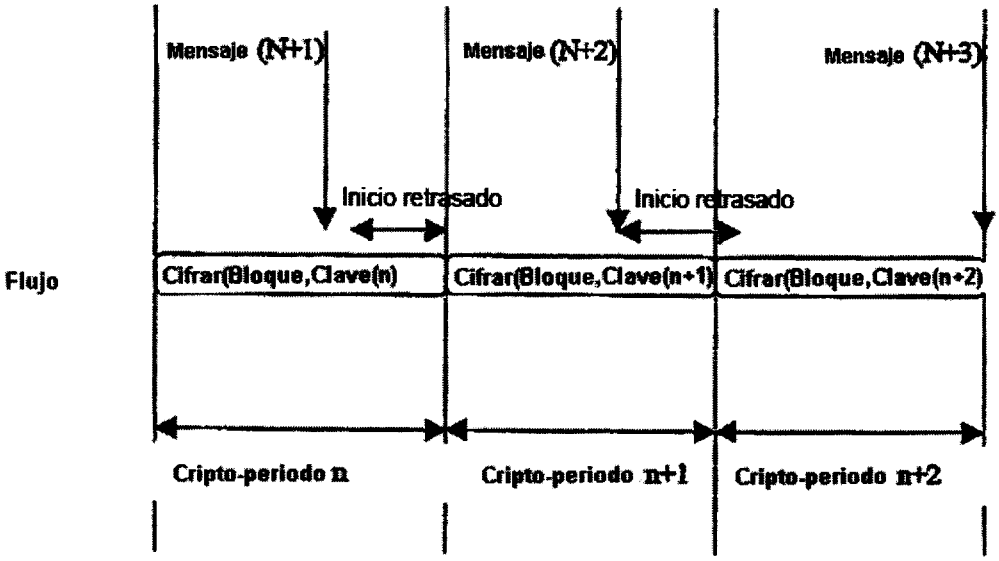
Mensaje (N+1)
Mensaje (N+2)
Mensaje (N+3)
Inicio retrasado
Inicio retrasado
Flujo
Cifrar(Bloque,Clave(n)
Cifrar(Bloque,Clave(n+1)
Cifrar(Bloque,Clave(n+2)
Cripto-periodo n
Cripto-periodo n+1
Cripto-periodo n+2

FIG. 8