(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 523 136**

(51) Int. CI.:

H04L 9/18 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **03.04.2001 E 01917799 (7)**

(97) Fecha y número de publicación de la concesión europea: **03.09.2014 EP 1376922**

(54) Título: **Dispositivo de encriptación**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
21.11.2014

(73) Titular/es:

MITSUBISHI DENKI KABUSHIKI KAISHA (100.0%)
7-3, MARUNOUCHI 2-CHOME CHIYODA-KU
TOKYO 100-8310, JP

(72) Inventor/es:

KASUYA, TOMOMI;
CHIKAZAWA, TAKESHI;
WAKABAYASHI, TAKAO y
UGA, SHINSUKE

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

DESCRIPCIÓN

Dispositivo de encriptación

Campo técnico

La presente invención se refiere a un aparato de encriptación, un aparato de desencriptación y un aparato de comunicación por radio, usados para dispositivos tales como un teléfono celular. En particular, la invención se refiere a un proceso de confidencialidad y de integridad de datos.

Antecedentes de la técnica

La figura 24 muestra un teléfono 500 celular convencional.

En el teléfono 500 celular convencional se proporcionan una unidad 510 IF (interfaz) de terminal, una unidad 520 de control de comunicación por radio y una unidad 530 de comunicación por radio. La unidad 510 IF de terminal realiza una interfaz con un usuario del teléfono 500 celular. La unidad 520 de control de comunicación por radio realiza el control de comunicación del teléfono celular en conjunto, la conversión de datos y el proceso de datos en base a un protocolo. La unidad 530 de comunicación por radio modula y demodula los datos para permitir la comunicación por radio. La unidad 530 de comunicación por radio soporta la capa física (capa 1), que es la capa más inferior de las siete capas definidas por OSI (interconexión de sistemas abiertos). Se proporciona una unidad 540 de proceso de confidencialidad a la unidad 530 de comunicación por radio. La unidad 540 de proceso de confidencialidad encripta o desencripta los datos de la capa física que deben procesarse por la unidad 530 de comunicación por radio. Puesto que los datos enviados/recibidos por una antena 541 se encriptan proporcionando la unidad 540 de proceso de confidencialidad, se evita que conexiones espía obtengan cualquier información significativa a menos que se averigüen los códigos de encriptación.

El teléfono 500 celular convencional tiene la unidad 540 de proceso de confidencialidad dentro de la unidad 530 de comunicación por radio. En consecuencia, los datos que deben procesarse por la unidad 540 de proceso de confidencialidad se almacenan en la capa física (capa 1). En la capa física, es imposible discriminar los datos entre datos de usuario y datos de control. Los datos enviados/recibidos por el teléfono celular incluyen diversos tipos de datos, tales como los datos de usuario o los datos de señalización, y se requiere realizar el proceso de confidencialidad de datos en base a los tipos de datos, o garantizar la integridad de los datos en función de la importancia de los datos. Como se muestra en la arquitectura convencional, aunque la unidad 540 de proceso de confidencialidad se proporciona en la capa 1, no puede realizarse el proceso de confidencialidad ni el proceso de integridad de datos en base al tipo de datos porque es imposible discriminar los tipos de datos en la capa 1.

Además, el proceso de confidencialidad convencional se ha realizado generando una secuencia de números aleatorios de manera sincrónica con los datos de entrada y realizando una operación XOR de los datos y la secuencia de números aleatorios de manera sincrónica con la entrada de los datos.

Aún más, el proceso de integridad convencional se ha realizado generando un código de autenticación de mensajes para cada dato o comprobando la integridad de los datos para cada dato.

El documento US 5 796 836 A desvela un sistema para encriptar bloques de texto legible. Se proporcionan memorias FIFO de salida para desacoplar la generación de vectores pseudoaleatorios con respecto a la encriptación de texto legible. Las FIFO de salida producen el efecto de multiplexación de varios dispositivos criptográficos entre sí y pueden combinarse con memorias FIFO de realimentación con el fin de proporcionar una agilidad de clave y una encriptación de clave secreta paralela. La transferencia de datos también se mejora construyendo libros de códigos extensos, de manera que un bloque de datos pueda cifrarse como un todo.

El documento US 5 345 508 se refiere a una estructura de encriptación digital que permite la variación de la sobrecarga computacional reutilizando selectivamente, de acuerdo con el nivel deseado de seguridad, una secuencia de codificación pseudoaleatoria en el extremo transmisor y almacenando y reutilizando secuencias de decodificación pseudoaleatorias, asociadas con uno o más transmisores en el extremo receptor.

El documento JP 61 22 4531 A describe un dispositivo de cifrado en el que una clave de cifrado y un vector inicial de cifrado actúan en una unidad aritmética de cifrado. Se obtiene una salida de cifrado realimentando una salida cifrada desde la unidad aritmética de cifrado a la entrada. Se almacena el patrón aleatorio para el cifrado obtenido de esta manera. En caso de una transmisión, se realiza una operación OR exclusivamente con el patrón aleatorio almacenado para el cifrado y el bit de información que debe enviarse para cifrar el bit de información y el resultado se envía como unos datos de transmisión.

Por último, el documento US 4 663 500 A muestra un sistema criptográfico que comprende un sumador de módulo 2 con una primera entrada receptiva a una secuencia de dígitos binarios que deben codificarse y una segunda entrada receptiva a una secuencia de dígitos binarios de codificación para generar una secuencia de dígitos binarios codificados. Se proporciona un generador de funciones que tiene una memoria para almacenar una secuencia de predeterminada de dígitos binarios en localizaciones de almacenamiento direccionables y para leer los dígitos

binarios almacenados en respuesta a un código de direcciones representado por los patrones primero y segundo combinados de los dígitos binarios que se generan, respectivamente, por un generador de patrones aleatorios y un registro de desplazamiento que se conecta a la salida del sumador de módulo 2. La salida del generador de funciones son los dígitos binarios de codificación aplicados al sumador de módulo 2.

Una realización preferida de la presente invención pretende realizar un proceso de confidencialidad y de integridad de datos de alta velocidad.

Además, otro objetivo de la realización preferida de la presente invención es realizar el proceso de confidencialidad y de integridad de datos en una capa superior igual a o mayor que la capa 2 (capa de enlace de datos) de las siete capas del OSI.

Aún más, otro objetivo de la realización preferida de la presente invención es realizar el proceso de confidencialidad y de integridad de datos sin carga en la unidad de proceso central y el bus.

Divulgación de la invención

De acuerdo con la presente invención, un aparato de encriptación incluye:

una unidad de proceso central para introducir y emitir una señal de control a usar para generar una secuencia de números aleatorios y los datos de texto legible;

un encriptador para introducir la señal de control desde la unidad de proceso central y generar la secuencia de números aleatorios en base a la señal de control;

una memoria de secuencia de números aleatorios para almacenar la secuencia de números aleatorios generada por el encriptador; y

una unidad de funcionamiento para introducir los datos de texto legible desde la unidad de proceso central, realizar una operación de los datos de texto legible recibidos y la secuencia de números aleatorios almacenada en la memoria de secuencia de números aleatorios y emitir datos de texto cifrado,

en el que la unidad de proceso central está adaptada para emitir la señal de control antes de emitir los datos de texto legible, y el encriptador está adaptado para iniciar la generación de la secuencia de números aleatorios antes de que los datos de texto legible se introduzcan en la unidad de funcionamiento.

El encriptador introduce al menos una clave de encriptación y una longitud de los datos de texto legible, genera la secuencia de números aleatorios que tiene la longitud de los datos de texto legible usando la clave de encriptación, y hace que la memoria de secuencia de números aleatorios almacene la secuencia de números aleatorios generada, y la memoria de secuencia de números aleatorios incluye una memoria intermedia para emitir la secuencia de números aleatorios almacenada en caso de que la unidad de funcionamiento introduzca los datos de texto legible.

La unidad de funcionamiento introduce los datos de texto legible correspondientes a la pluralidad de canales;
el encriptador introduce la información de identificación de canal para identificar un canal y genera la secuencia de números aleatorios para cada uno de la pluralidad de canales;
la memoria de secuencia de números aleatorios almacena la secuencia de números aleatorios generada por el encriptador para cada uno de la pluralidad de canales; y
la unidad de funcionamiento introduce la secuencia de números aleatorios correspondiente a cada uno de la pluralidad de canales desde los que se introducen los datos de texto legible y encripta los datos de texto legible.

De acuerdo con la presente invención, un aparato de desencriptación incluye:

una unidad de proceso central para introducir y emitir una señal de control a usar para generar una secuencia de números aleatorios y los datos de texto cifrado;

un desencriptador para introducir la señal de control desde la unidad de proceso central y generar la secuencia de números aleatorios en base a la señal de control;

una memoria de secuencia de números aleatorios para almacenar la secuencia de números aleatorios generada por el desencriptador; y

una unidad de funcionamiento para introducir los datos de texto cifrado, realizar una operación de los datos de texto cifrado recibidos y la secuencia de números aleatorios almacenada en la memoria de secuencia de números aleatorios, y emitir datos de texto legible,

en el que la unidad de proceso central está adaptada para emitir la señal de control antes de emitir los datos de texto cifrado, y el desencriptador está adaptado para iniciar la generación de la secuencia de números aleatorios antes de introducir los datos de texto cifrado en la unidad de funcionamiento.

El desencriptador introduce al menos una clave de desencriptación y una longitud de los datos de texto cifrado, genera la secuencia de números aleatorios que tiene la longitud de los datos de texto cifrado usando la clave de desencriptación, y hace que la memoria de secuencia de números aleatorios almacene la secuencia de números aleatorios generada, y
la memoria de secuencia de números aleatorios incluye una memoria intermedia para emitir la secuencia de números aleatorios almacenada en caso de que la unidad de funcionamiento introduzca los datos de texto cifrado.

La unidad de funcionamiento introduce los datos de texto cifrado correspondientes a la pluralidad de canales;
el desencriptador introduce la información de identificación de canal para identificar un canal y genera la secuencia de números aleatorios para cada uno de la pluralidad de canales;
la memoria de secuencia de números aleatorios almacena la secuencia de números aleatorios generada por el desencriptador para cada uno de la pluralidad de canales; y
la unidad de funcionamiento introduce la secuencia de números aleatorios correspondiente a cada uno de los canales de los que se introducen los datos de texto cifrado y desencripta los datos de texto cifrado.

De acuerdo con la presente invención, un aparato de comunicación por radio incluye:

una unidad de interfaz de terminal para introducir los datos;

una unidad de control de comunicación por radio para introducir los datos recibidos por la unidad de interfaz de terminal, procesar los datos en base a un protocolo, y emitir un resultado del proceso;

una unidad de proceso de confidencialidad para introducir una señal de control y los datos desde la unidad de control de comunicación por radio, realizar el proceso de confidencialidad encriptando los datos recibidos en base a la señal de control recibida, y emitir los datos procesados a la unidad de control de comunicación por radio; y

una unidad de comunicación por radio para introducir, modular, y enviar los datos emitidos por la unidad de control de comunicación por radio,

en el que la unidad de comunicación por radio está adaptada para emitir la señal de control antes de emitir los datos, y

la unidad de proceso de confidencialidad incluye:

un encriptador para iniciar la generación de una secuencia de números aleatorios a usar para encriptar los datos antes de que los datos se introduzcan, y emitir la secuencia de números aleatorios generada;

una memoria de secuencia de números aleatorios para introducir, antes de que se introduzcan los datos, y almacenar temporalmente la secuencia de números aleatorios emitida por el encriptador; y

una unidad de funcionamiento para introducir los datos y encriptar los datos realizando una operación de los datos recibidos y la secuencia de números aleatorios almacenada en la memoria de secuencia de números aleatorios.

De acuerdo con la presente invención, un aparato de comunicación por radio incluye:

una unidad de comunicación por radio para recibir y demodular los datos;
una unidad de control de comunicación por radio para introducir los datos demodulados por la unidad de comunicación por radio, y procesar y emitir los datos en base al protocolo;

una unidad de proceso de confidencialidad para introducir la señal de control y los datos, realizar un proceso de aleatorización de datos desencriptando los datos para los datos recibidos, y emitir los datos procesados a la unidad de control de comunicación por radio; y

una unidad de interfaz de terminal para introducir y emitir los datos procesados por la unidad de control de comunicación por radio, y

en el que la unidad de comunicación por radio emite la señal de control antes de emitir los datos,

en el que la unidad de proceso de confidencialidad incluye:

un desencriptador para iniciar la generación de una secuencia de números aleatorios a usar para desencriptar los datos recibidos antes de que se introduzcan los datos y emitir la secuencia de números aleatorios generada;

una memoria de secuencia de números aleatorios para introducir, antes de que se introduzcan los datos, y almacenar temporalmente la secuencia de números aleatorios emitida por el desencriptador; y

una unidad de funcionamiento para introducir los datos, realizar una operación de los datos recibidos y la

secuencia de números aleatorios almacenada en la memoria de secuencia de números aleatorios, y emitir datos de texto legible.

Breve explicación de los dibujos

La figura 1 muestra una configuración de un sistema de comunicaciones móviles.
La figura 2 muestra una configuración de un controlador 120 de red de radio (RNC).
La figura 3 muestra una configuración de una estación 100 móvil (MS) de acuerdo con la primera realización.
La figura 4 muestra una configuración de una unidad 40 de proceso de confidencialidad/integridad de acuerdo con la primera realización.
La figura 5 muestra una configuración de una unidad 40 de proceso de confidencialidad/integridad de acuerdo con la primera realización.
La figura 6 muestra una configuración de una unidad 40 de proceso de confidencialidad/integridad de acuerdo con la primera realización.
La figura 7 muestra una configuración de una unidad 40 de proceso de confidencialidad/integridad de acuerdo con la primera realización.
La figura 8 muestra una configuración de una unidad 40 de proceso de confidencialidad/integridad de acuerdo con la primera realización.
La figura 9 muestra una configuración de una estación 100 móvil (MS) de acuerdo con la segunda realización.
La figura 10 muestra una configuración de una unidad 40 de proceso de confidencialidad/integridad de acuerdo con la segunda realización.
La figura 11 muestra una configuración de una unidad 40 de proceso de confidencialidad/integridad de acuerdo con la segunda realización.
La figura 12 muestra un ejemplo de sistemas de encriptación/desencriptación.
La figura 13 muestra una configuración de una unidad 40 de proceso de confidencialidad/integridad de acuerdo con la segunda realización.
La figura 14 es una ilustración mostrada en la ARIB STD-T63 33.102, seguridad 3G; arquitectura de seguridad, sección 6.3.
La figura 15 es una ilustración mostrada en la ARIB STD-T63 33.102, seguridad 3G; arquitectura de seguridad, figura 16b.
La figura 16 es una ilustración mostrada en la ARIB STD-T63 33.102, seguridad 3G; arquitectura de seguridad, figura 16.
La figura 17 muestra una configuración de un módulo 51 de encriptación (o un módulo 71 de desencriptación) empleado en una unidad 421 de encriptación/desencriptación.
La figura 18 muestra una forma de instalación de la unidad 40 de proceso de confidencialidad/integridad.
La figura 19 muestra un caso en el que la unidad 40 de proceso de confidencialidad/integridad se implementa por soporte lógico.
La figura 20 muestra un mecanismo para solicitar un programa 47 de cifrado mediante un programa de aplicación ejecutado en una unidad 20 de control de comunicación por radio.
La figura 21 muestra un ejemplo concreto de los datos 92, 93 en el caso de un modo no transparente RLC.
La figura 22 muestra un ejemplo concreto de datos de voz como un ejemplo de datos 95, 96 transparentes.
La figura 23 muestra un ejemplo concreto de datos digitales restringidos como un ejemplo de datos 95, 96 transparentes.
La figura 24 muestra un teléfono 500 celular convencional.
La figura 25 muestra procedimientos de encriptación y desencriptación para el proceso de confidencialidad de datos de acuerdo con la tercera realización.
La figura 26 muestra procedimientos de encriptación y desencriptación para el proceso de datos de integridad de acuerdo con la tercera realización.
La figura 27 muestra una unidad 20 de control de comunicación por radio y una unidad 40 de proceso de confidencialidad/integridad de acuerdo con la tercera realización.
La figura 28 muestra una configuración de una unidad 420 de proceso de confidencialidad de la tercera realización.
La figura 29 muestra una configuración de la unidad 420 de proceso de confidencialidad de la tercera realización.
La figura 30 muestra una configuración de una unidad 460 de proceso de confidencialidad de la tercera realización.
La figura 31 muestra una configuración de una unidad 430 de proceso de integridad de la tercera realización.
La figura 32 muestra una configuración de la unidad 430 de proceso de integridad de la tercera realización.
La figura 33 muestra una configuración de una unidad 422 de encriptación de la tercera realización que tiene memorias intermedias múltiples.
La figura 34 muestra una configuración de la unidad 422 de encriptación de la tercera realización que tiene memorias intermedias múltiples.
La figura 35 muestra una configuración de la unidad 422 de encriptación de la tercera realización que tiene memorias intermedias múltiples.

Realización preferida para realizar la invención

Realización 1.

La figura 1 muestra una configuración general de un sistema de comunicaciones móviles de acuerdo con esta realización.

Una estación móvil (MS) es un ejemplo del aparato de comunicación por radio de acuerdo con la invención. La estación 100 móvil (MS) es, por ejemplo, un teléfono celular. La estación 100 móvil (MS) está conectada a una estación 110 transceptora base (BTS) por radio. La estación 110 transceptora base (BTS) está conectada a un controlador 120 de red de radio (RNC). El controlador 120 de red de radio (RNC) está conectado a otro controlador 120 de red de radio (RNC). El controlador 120 de red de radio (RNC) también está conectado a una red 130 central (CN), y conectado además a otro controlador 120 de red de radio (RNC) a través de la red 130 central (CN). Una o ambas de las estaciones 110 transceptoras base (BTS) y el controlador 120 de red de radio (RNC) pueden denominarse estación de radio.

La figura 2 muestra una configuración del mismo sistema de comunicaciones móviles como se muestra en la figura 1. En particular, la figura muestra la configuración interna del controlador 120 de red de radio (RNC).

Una unidad 121 IF BTS se conecta con la estación 110 transceptora base (BTS). Una unidad 122 de control de traspaso controla el traspaso en caso de que la estación 100 móvil (MS) se mueva entre las estaciones 110 transceptoras base (BTS).

Una unidad 123 de control de señales para MS realiza el control de comunicación por radio y el proceso de confidencialidad/integridad de datos durante la comunicación con la estación 100 móvil (MS). El siguiente proceso de confidencialidad/integridad de la estación 100 móvil (MS) se realiza en correspondencia con el proceso de confidencialidad/integridad de la unidad 123 de control de señales para MS. Es decir, los datos encriptados por la estación 100 móvil (MS) se desencriptan por la unidad 123 de control de señales para MS. A la inversa, los datos encriptados en la unidad 123 de control de señales para MS se desencriptan en la estación 100 móvil (MS). Un código de autenticación añadido por la estación 100 móvil (MS) para garantizar la integridad de los datos se comprueba por la unidad 123 de control de señales para MS. A la inversa, el código de autenticación añadido por la unidad 123 de control de señales para MS para garantizar la integridad de los datos se comprueba por la estación 100 móvil (MS). El proceso de confidencialidad de datos o el proceso de integridad de datos se realiza en la segunda capa de las siete capas, es decir, la capa 2 (capa de enlace de datos). Una unidad 124 IF CN se interconecta con la red 130 central (CN).

Una unidad 125 IF RNC se interconecta con otro controlador 120 de red de radio (RNC). Una unidad 126 de control de señales para CN realiza el control con una red 130 central (CN). Una unidad 127 de control de señales para RNC realiza el control con otro controlador 120 de red de radio (RNC). Una unidad 128 de control controla el conjunto de controladores 120 de red de radio (RNC). Un conmutador 129 conmuta las señales de control y los datos por paquetes en base a la acción de control de la unidad 128 de control entre la estación 110 de radio (BTS), el controlador 120 de red de radio (RNC) y la red 130 central (CN). Es decir, el conmutador 129 conmuta no solo los datos por paquetes, sino todo tipo de datos, tales como datos de voz, y además el conmutador 129 también conmuta las señales de control.

La figura 3 muestra una configuración de la estación 100 móvil (MS).

La estación 100 móvil (MS) incluye una unidad 10 IF de terminal, una unidad 20 de control de comunicación por radio, una unidad 30 de comunicación por radio y una unidad 40 de proceso de confidencialidad/integridad. Una cámara 1, un video 2, un B/T 3 (bluetooth), un LCD 4, una CLAVE 5, un LED 6, un USIM 7 (módulo de identidad de abonado universal), un RECEPTOR 8, un MIC 9, y un HSJ 0 (conector para auriculares) están conectados a la unidad 10 IF de terminal. Estos dispositivos de la cámara 1 al HSJ 0 realizan un proceso de interfaz con el usuario (una persona) o un dispositivo que va a conectarse, y los dispositivos introducen o emiten información que puede reconocerse por el usuario (persona) o el dispositivo que va a conectarse.

La unidad 10 IF de terminal incluye una unidad 11 IF de módulo para cada módulo, un conversor 12 de formato de datos, una unidad 13 de control IF de terminal, y una unidad 14 de codificación/decodificación de voz. La unidad 11 IF de módulo para cada módulo se interconecta con cada uno de los dispositivos de la cámara 1 al HSJ 0. El conversor 12 de formato de datos convierte los formatos de datos procesados por los dispositivos de la cámara 1 al HSJ 0 en/a partir de los formatos de datos procesados dentro de la estación 100 móvil (MS). La unidad 13 de control IF de terminal controla el funcionamiento de la unidad 10 IF de terminal. La unidad 14 de codificación/decodificación de voz codifica las señales eléctricas de voz recibidas por el MIC 9 en código de voz. Además, la unidad 14 de codificación/decodificación de voz decodifica la señales codificadas para emitir las señales eléctricas de voz al RECEPTOR 8.

La unidad 20 de control de comunicación por radio controla toda la estación 100 móvil (MS). La unidad 20 de control de comunicación por radio está provista de un circuito de soporte físico que incluye una CPU, una ROM, una RAM, un programa fijo de máquina, y similares, o un módulo de soporte lógico. La unidad 20 de control de comunicación por radio procesa los datos entre la unidad 10 IF de terminal y la unidad 30 de comunicación por radio. La unidad 20 de control de comunicación por radio convierte los datos en base a reglas definidas por la norma o el protocolo. En particular, la unidad 20 de control de comunicación por radio procesa los datos de la capa 2 o niveles superiores de

capa, mediante funciones tales como paquetizar o concatenar los datos. La unidad 20 de control de comunicación por radio puede discriminar el tipo de datos, porque la unidad 20 de control de comunicación por radio procesa los datos de la capa 2 o superiores. En consecuencia, la unidad 20 de control de comunicación por radio puede determinar si determinados datos deben someterse al proceso de confidencialidad o al proceso de integridad en base al tipo de datos. Es imposible discriminar el tipo de datos en la capa 1, y por lo tanto es imposible determinar si debe realizarse el proceso de confidencialidad o el proceso de integridad de los datos.

La unidad 30 de comunicación por radio está provista de una unidad 310 de codificación de canal, una unidad 320 de modulación/demodulación de banda base, una unidad 330 de radio, y una antena 34. La unidad 310 de codificación de canal incluye unidades codificación y unidades de decodificación para los canales respectivos. La unidad de codificación incluye una unidad 311 de codificación de detección de errores, una unidad 312 de codificación de corrección de errores, y un conversor 313 de formato físico. Además, la unidad de decodificación incluye un conversor 314 de formato físico, una unidad 315 de decodificación de corrección de errores, y una unidad 316 de detección de errores. La unidad 320 de modulación/demodulación (MODEM) de banda base modula y demodula la banda. La unidad 320 de modulación/demodulación de banda base incluye un modulador 321 de banda base y un demodulador 322 de banda de base. La unidad 330 de radio convierte las señales de banda base en un espectro de transmisión, o invierte la conversión. La unidad 330 de radio incluye un conversor 331 elevador y un conversor 332 reductor.

La unidad 40 de proceso de confidencialidad/integridad está conectada a la unidad 20 de control de comunicación por radio. La unidad 40 de proceso de confidencialidad/integridad recibe datos desde la unidad 20 de control de comunicación por radio y realiza el proceso de confidencialidad de datos. Además, la unidad 40 de proceso de confidencialidad/integridad garantiza la integridad de los datos. La unidad 40 de proceso de confidencialidad/integridad introduce una señal 91 de control desde la unidad 20 de control de comunicación por radio para el proceso de confidencialidad/integridad de los datos. Además, la unidad 40 de proceso de confidencialidad/integridad introduce los datos 92 de una capa arbitraria de 2 o niveles superiores de capa como los datos de proceso del proceso de confidencialidad y/o los datos 92 de una capa arbitraria de 2 o niveles superiores de capa como los datos de proceso del proceso de integridad desde la unidad 20 de control de comunicación por radio. La unidad 40 de proceso de confidencialidad/integridad realiza el proceso de confidencialidad y/o el proceso de integridad de los datos 92 en base a la señal 91 de control de entrada para emitir a la unidad 20 de control de comunicación por radio. La señal 91 de control incluye parámetros tales como una clave, un valor inicial, la selección entre el proceso de confidencialidad y el proceso de integridad.

La figura 4 muestra una configuración de la unidad 40 de proceso de confidencialidad/integridad.

La unidad 40 de proceso de confidencialidad/integridad incluye una unidad 410 IF y un módulo 411. El módulo 411 realiza el proceso de confidencialidad y el proceso de integridad dentro del mismo circuito o usando el mismo algoritmo. La selección entre el proceso de confidencialidad y el proceso de integridad se determina por la señal 91 de control.

En este caso, proceso de confidencialidad significa encriptar o desencriptar los datos. Además, el proceso de integridad significa detectar la manipulación de datos añadiendo códigos de autenticación a los datos o reproduciendo y comparando los códigos de autenticación.

El proceso de confidencialidad y el proceso de integridad pueden realizarse por el mismo circuito o algoritmo, o por un circuito similar o un módulo similar. En consecuencia, como se muestra en la figura 4, el proceso de confidencialidad y el proceso de integridad pueden realizarse por un solo módulo 411. En el caso de la figura 4, es posible reducir los recursos de soporte físico y los recursos de soporte lógico. De lo que sigue en el presente documento, un “módulo” se refiere solo a los implementados o por soporte físico o por soporte lógico, o por la combinación de ambas herramientas.

En este caso, se explicarán ejemplos concretos del proceso de confidencialidad y el proceso de integridad usados para el teléfono celular.

La figura 14 es una figura mostrada en la ARIB STD-T63 33.102, seguridad 3G; arquitectura de seguridad, sección 6.3.

La figura 15 es una figura mostrada en la ARIB STD-T63 33.102, seguridad 3G; arquitectura de seguridad, figura 16b.

La figura 16 es una figura que mostrada en la ARIB STD-T63 33.102, seguridad 3G; arquitectura de seguridad, figura 16.

La figura 14 muestra un procedimiento de encriptación en la línea de radio. Los signos mostrados en la figura 14 significan lo siguiente:

CK: clave de cifrado (clave de encriptación)
F8: función para el proceso de confidencialidad de datos

IK: clave de integridad (clave de autenticación de mensajes)
F9: función para el proceso de integridad de datos

Las compañías de telefonía celular implementan la autenticación usando las funciones f1 a f5. Las claves de encriptación de 128 bits denominadas CK e IK generadas a través de este procedimiento de autenticación se transfieren a la función para el proceso de confidencialidad de datos (f8) y la función para el proceso de integridad de datos (f9).

La figura 15 muestra un procedimiento de encriptación en la línea de radio. Los signos mostrados en la figura 15 significan lo siguiente:

f8: función para el proceso de confidencialidad de datos
CK: clave de cifrado (clave de encriptación)
MENSAJE: datos de texto legible que un emisor quiere enviar a un receptor, tales como datos de usuario e información de señal, antes de la encriptación
CONTADOR-C: datos de valor numérico que muestran el número acumulado de transmisiones/recepciones, aumentado en 1 en cada sesión.
PORTADOR: bit para identificar un canal lógico
DIRECCIÓN: bit para discriminar la dirección de la transmisión de un texto cifrado
LONGITUD: longitud en bits del mensaje o los datos de texto cifrado

Como se muestra en la figura 15, la encriptación/desencriptación de los datos se realiza en base a una secuencia de números aleatorios generada por la función f8 para el proceso de confidencialidad de datos.

La figura 16 muestra un procedimiento para generar un código de autenticación de mensajes. Los signos mostrados en la figura 16 significan lo siguiente:

f9: función para el proceso de integridad de datos
IK: clave de integridad (clave de autenticación de mensajes)
CONTADOR-I: datos de valor numérico que muestran el número acumulado de transmisiones/recepciones, aumentado en 1 en cada sesión
MENSAJE: datos de texto legible que un emisor quiere enviar a un receptor, tales como datos de usuario e información de señal, antes de la encriptación
DIRECCIÓN: bit para discriminar la dirección de transmisión
FRESH: número aleatorio generado para cada usuario
MAC-I: código de autenticación de mensajes para la integridad (código de autenticación de mensajes calculado por el emisor)
XMAC-I: código de autenticación de mensajes esperado para la integridad (código de autenticación de mensajes calculado por el receptor)

Como se muestra en la figura 16, la integridad de los datos puede comprobarse comparando dos códigos de autenticación de mensajes en el lado del receptor.

A continuación, se explicará el funcionamiento.

Para realizar la comunicación cifrada entre el terminal y la red dentro de la red de radio, se requiere un procedimiento de autenticación, en el que una parte confirma que la otra es una parte adecuada, o ambas partes confirman recíprocamente que la otra es adecuada antes del envío/recepción de los datos entre las dos partes.

Como se muestra en la figura 14, durante una serie de procedimientos autenticación, tanto el terminal como la red usan cinco funciones denominadas funciones f1 a f5. En paralelo con el procedimiento de autenticación, la función genera una clave de cifrado (CK) de 128 bits y una clave de autenticación de mensajes (clave de integridad, IK), tanto en el terminal como en la red.

Las dos claves pueden compartirse exclusivamente por el terminal y la red que se han autenticado mutuamente, y las dos claves se usan dentro de las dos funciones f8 y f9 que se describen a continuación. Las dos teclas varían para cada sesión de comunicación y, además, no hay patrones entre las claves generadas. A continuación, se eliminan las claves cuando ha terminado la comunicación.

El mecanismo (protocolo) requerido para este procedimiento de autenticación está normalizado. Sin embargo, como las funciones de f1 a f5 no están normalizadas, los operadores deciden estas funciones de manera independiente.

La seguridad de los datos después del procedimiento de autenticación se mantiene por las técnicas de proceso de confidencialidad y de integridad de datos.

La primera, la técnica de confidencialidad de datos, se aplica para encriptar los datos de usuario y la información de señal incluyendo la voz transferida en la red de radio, y para evitar las captaciones de mensajes. Para implementar este proceso de confidencialidad de datos, se emplea una función llamada función de confidencialidad de datos (en

lo que sigue en el presente documento, denominada f8).

En el caso de los datos de comunicación que se han sometido al proceso de confidencialidad como se muestra en la figura 15, el emisor usa la clave de encriptación (CK) generada en el procedimiento de autenticación. Además, se genera una secuencia de números aleatorios al introducir una longitud en bits (LONGITUD) de los datos de destino para la encriptación/desencriptación, un enlace elevador/reductor (DIRECCIÓN), un contador (CONTADOR-C), un identificador de canal lógico (PORTADOR) para f8.

En este caso, el enlace elevador/reductor significa aquellos bits distintivos que indican la dirección de transmisión de los datos de texto cifrado entre un terminal y una estación base. Además, el contador son los datos que muestran el número acumulado de veces que se envían/reciben los datos. En cada envío/recepción de los datos, se añade un valor fijo al contador. El contador se usa para evitar un ataque que intenta enviar datos de texto cifrado que se han enviado anteriormente. Aún más, el identificador de canal lógico significa un bit para identificar un canal lógico que realiza la encriptación.

Los datos de texto cifrado se generan realizando una operación XOR en la secuencia de números aleatorios generada anteriormente y la información de datos/señales que debe encriptarse y enviarse al receptor.

Los parámetros, excepto CK, se envían desde el emisor al receptor sin encriptación. No es necesario enviar CK porque se genera el mismo parámetro en el lado del receptor en el procedimiento de autenticación.

Incluso si se obtienen otros parámetros distintos de CK por un tercero, puede mantenerse la seguridad del mensaje original, puesto que no puede generarse la secuencia de números aleatorios requerida para desencriptar los datos de texto cifrado, siempre que CK se mantenga en secreto.

En el lado del receptor, la secuencia de números aleatorios se genera usando los parámetros recibidos y CK que ya se ha obtenido, la secuencia de números aleatorios realiza una operación XOR con los datos de texto cifrado recibidos para desencriptar en el mensaje original.

Este procedimiento es una variación del modo OFB (retroalimentación de salida), que es uno de los modos que utilizan el cifrado por bloques definido por ISO/IEC10116. En modo OFB, incluso si el ruido generado en las vías de transmisión se mezcla con los datos de texto cifrado, el proceso de decodificación puede evitar que aumente la parte de ruido. Por esta razón, a menudo se adopta este modo para la comunicación de voz por radio.

La segunda técnica para mantener la seguridad de los datos es la técnica de integridad de datos, que detecta una manipulación en la información de señal añadiendo un código de autentificación de mensajes (código de autenticación de mensajes) a la información de señal en la línea de comunicación por radio. Esto también se llama técnica de autenticación de mensajes. Para implementar esta técnica de integridad de datos, se usa una función para la integridad de datos (en lo que sigue en el presente documento, denominada f9). El mismo algoritmo de encriptación que en F8 se emplea en la parte central de f9.

En primer lugar, en la autenticación, la clave de autentificación de mensajes (IK) se deriva de la función f4 para generar la clave de autenticación de mensajes, y se transfiere a f9 la clave de autentificación de mensajes. Como se muestra en la figura 16, un código de autenticación de mensajes (MAC-I o XMAC-I) se genera al introducir los datos (MENSAJE), el enlace elevador/reductor (DIRECCIÓN), el contador (CONTADOR-C), el número aleatorio (FRESH) generado para cada usuario así como la clave de autenticación de mensajes.

Estos parámetros también se envían al receptor usando un área de formato de datos que no se encripta por el emisor. Incluso si los parámetros se obtienen por un tercero, puede mantenerse la confidencialidad de los datos siempre que se mantenga en secreto la clave de autenticación de mensajes (IK), que es la misma que en el caso de la confidencialidad de datos.

El emisor envía los datos añadiendo este código de autenticación de mensajes (MAC-I) añadido al receptor. El receptor, de manera similar, calcula el código de autenticación de mensajes (XMAC-I) usando f9. Puede confirmarse que no hay manipulación comparando MAC-I y XMAC-I para encontrarlos idénticos.

En este caso, se muestran a continuación, algunos ejemplos de procedimientos posteriores en el caso de una detección de manipulación:

(1) Solicitar la retransmisión de los datos y comprobar si el código de autenticación de mensajes recibido es adecuado o no.
(2) Desconectar la conexión en caso de detección de manipulaciones consecutivas.

De acuerdo con la especificación 3GPP (para más información, acceder a http://www.3gpp.org/About_3GPP/3gpp.htm), el módulo de encriptación/desencriptación tiene la función de encriptar los datos de texto legible de entrada (datos que deben encriptarse) en los datos de texto cifrado (datos encriptados) y emitir los datos de texto cifrado, y la función de desencriptar los datos de texto cifrado en los datos de texto legible y emitir los datos de texto legible. Suponiendo que la realización es compatible con la especificación 3GPP, los

parámetros CONTADOR/PORTADOR/DIRECCIÓN/CK/LONGITUD anteriores se corresponden como ejemplos concretos con la señal 91 de control mostrada en la figura 3.

Además, por ejemplo, “MACSDU” o “RLCPDU (parte de datos)” se corresponden como ejemplos concretos de los datos 92 y 93 mostrados en la figura 3 como se muestra en la figura 21. En este caso, “RLCSDU (parte de datos)” es una parte de RLCPDU, de la que se borra la parte superior (la parte de “DATOS PARA CIFRADO” mostrada en la figura 21) de 1 octeto o 2 octetos (1 byte o 2 bytes). “MACSDU” o “RLCPDU (parte de datos)” es un ejemplo del MENSAJE mostrado en la figura 15. Aún más, MACSDU indica una unidad de datos de servicio de control de acceso al medio. RLCPDU indica una unidad de datos de protocolo de control de enlace de radio. Cada mensaje en el flujo de mensajes se estructura a partir de la RLCPDU en la capa 3, después de borrar la cabecera RLC.

Aunque RLCPDU tiene una parte de 1 octeto o 2 octetos que no se somete al proceso de confidencialidad, la totalidad de la RLCPDU se introduce en la unidad 40 de proceso de confidencialidad/integridad y la unidad decide no realizar el proceso de confidencialidad/integridad en la parte de 1 octeto o 2 octetos. Esto es con el fin de reducir la carga de la unidad 20 de control de comunicación por radio en la que la carga se genera por desplazamiento de 1 octeto o 2 octetos para retirar la parte excluida de 1 octeto o 2 octetos de toda la unidad de datos (RLCPDU).

La figura 5 muestra otro ejemplo de la unidad 40 de proceso de confidencialidad/integridad.

Como se presenta en la figura 5, una unidad 420 de proceso de confidencialidad y una unidad 430 de proceso de integridad se proporcionan por separado. Dentro de la unidad 420 de proceso de confidencialidad, se proporciona una unidad 421 de encriptación/desencriptación. Dentro de la unidad 430 de proceso de integridad, se proporciona una unidad 431 de anexión de códigos de autenticación de mensajes/verificación de integridad. La unidad 421 de encriptación/desencriptación muestra un caso en el que la encriptación y la desencriptación se realizan usando un módulo idéntico. La unidad 431 de anexión de códigos de autenticación de mensajes/verificación de integridad muestra un caso en el que la anexión del código de autenticación de mensajes y la verificación de la integridad se realizan usando un módulo idéntico. Un caso mostrado en la figura 5 es una configuración en la que la encriptación y la desencriptación se realizan por la misma función o en la que la anexión del código de autenticación de mensajes y la verificación de la integridad se realizan por la misma función. En comparación con la figura 6, es posible reducir los recursos de soporte físico y los recursos de soporte lógico dentro de la caja de la figura 5.

La figura 6 muestra otro ejemplo de la unidad 40 de proceso de confidencialidad/integridad.

Como se presenta en la figura 6, dentro de la unidad 420 de proceso de confidencialidad, se proporcionan por separado una unidad 422 de encriptación y una unidad 423 de desencriptación. Además, dentro de la unidad 430 de proceso de integridad, se proporcionan por separado una unidad 432 de anexión de códigos de autenticación de mensajes y una unidad 433 de verificación de integridad. Un caso mostrado en la figura 6 es una configuración en la que la encriptación y la desencriptación se realizan por diferentes funciones o en la que la anexión del código de autenticación de mensajes y la verificación de la integridad se realizan por diferentes funciones. Es posible realizar, respectivamente, la encriptación, la desencriptación, la anexión del código de autenticación de mensajes, la verificación de la integridad y, además, el proceso de confidencialidad de datos o el proceso de integridad pueden realizarse de manera simultánea en paralelo sobre los datos enviados/recibidos. En consecuencia, puede realizarse el proceso de alta velocidad.

La figura 7 muestra un caso en el que se proporcionan múltiples unidades 422 de encriptación y múltiples unidades 423 de desencriptación en la unidad 420 de proceso de confidencialidad. Además, como se muestra en la figura, se proporcionan múltiples unidades 432 de anexión de códigos de autenticación de mensajes y múltiples unidades 433 de verificación de integridad en la unidad 430 de proceso de integridad. Mientras que la estación 100 móvil (MS) está funcionando, podría darse un caso en el que se procesaran los datos en múltiples canales al mismo tiempo. Por ejemplo, cuando se transfieren simultáneamente dos tipos de datos, tales como los datos de voz y los datos de fax, deben procesarse simultáneamente los datos de al menos dos canales. En tal caso, los datos de voz pueden encriptarse por la unidad 1 de encriptación, y los datos de fax pueden encriptarse por la unidad 2 de encriptación. Además, en caso de desencriptación, pueden desencriptarse simultáneamente los datos en múltiples canales. No es necesario tener el mismo número (n en el caso de la figura 7) de unidades 422 de encriptación, unidades 423 de desencriptación, unidades 432 de anexión de códigos de autenticación de mensajes, y unidades 433 de verificación de integridad. El número de cada una de las unidades puede determinarse de acuerdo con el número de canales que deben procesarse simultáneamente por la estación 100 móvil (MS). De otra manera, las unidades anteriores no se corresponden con cada canal, pero cuando un determinado canal necesita procesar una gran cantidad de datos a alta velocidad, es posible hacer que dos unidades de encriptación procesen la gran cantidad de datos asignados al canal. Es decir, el número de cada unidad, como la unidad 422 de encriptación, la unidad 423 de desencriptación, la unidad 432 de anexión de códigos de autenticación de mensajes, y la unidad 433 de verificación de integridad puede determinarse de acuerdo con el número de canales que deben procesarse simultáneamente y/o la cantidad de datos.

Además, el número máximo de las unidades 422 de encriptación y el número máximo de las unidades 423 de desencriptación pueden ser diferentes.

Además, el número máximo de las unidades 432 de anexión de códigos de autenticación de mensajes y el número máximo de las unidades 433 de verificación de integridad pueden ser diferentes.

La figura 8 muestra el caso en el que la unidad 420 de proceso de confidencialidad está provista de múltiples unidades 421 de encriptación/desencriptación. Además, como se muestra en la figura, la unidad 430 de proceso de integridad está provista de múltiples unidades 431 de anexión de códigos de autenticación de mensajes/verificación de integridad.

En la figura 8, la unidad 421 de encriptación/desencriptación y la unidad 431 de anexión de códigos de autenticación de mensajes/verificación de integridad mostradas en la figura 5 son respectivamente múltiples. En el caso de la figura 8, cuando la encriptación y la desencriptación se realizan usando la misma función, se proporcionan múltiples unidades 421 de encriptación/desencriptación correspondientes a múltiples canales. De manera similar, cuando la anexión del código de autenticación de mensajes y la verificación de integridad se realizan usando la misma función, se proporcionan múltiples unidades 431 de anexión de códigos de autenticación de mensajes/verificación de integridad correspondientes a múltiples canales. En comparación con el caso mostrado en la figura 7, la configuración de la figura 8 puede reducir los recursos de soporte físico y los recursos de soporte lógico.

En los casos mostrados en las figuras 4 a 8, la unidad 40 de proceso de confidencialidad/integridad incluye tanto la unidad 420 de proceso de confidencialidad como la unidad 430 de proceso de integridad. Sin embargo, la unidad 40 de proceso de confidencialidad/integridad puede incluir o la unidad 420 de proceso de confidencialidad o la unidad 430 de proceso de integridad. Cuando la unidad 40 de proceso de confidencialidad/integridad incluye o la unidad 420 de proceso de confidencialidad o la unidad 430 de proceso de integridad, el procedimiento de la otra puede realizarse por la unidad 20 de control de comunicación por radio.

Realización 2.

La figura 9 muestra otra configuración de la estación 100 móvil (MS).

A diferencia de la configuración de la figura 3, en la figura 9, los datos se introducen/se emiten entre la unidad 10 IF de terminal y la unidad 40 de proceso de confidencialidad/integridad. Y además, los datos también se introducen/se emiten entre la unidad 30 de comunicación por radio y la unidad 40 de proceso de confidencialidad/integridad. En la figura 9, los datos 97 no transparentes son datos no transparentes, tales como datos por paquetes. Además, los datos 95, 96 son datos transparentes tales como los datos de voz y los datos digitales sin restricciones. Datos transparentes significa que los datos no se cambian a lo largo de la entrada a la salida en cualquiera de las capas o subcapas de las capas de referencia OSI. Mientras que datos no transparentes significa que los datos requieren algún proceso de datos tal como la conversión del formato de datos a lo largo de la entrada a la salida en algunas capas o subcapas de las capas de referencia OSI. Por ejemplo, en una subcapa RLC (control del enlace radio) de la capa 2, cuando la SDU (unidad de datos de servicio) y la PDU (unidad de datos de protocolo) de datos son diferentes, los datos son datos no transparentes. Cuando la SDU y la PDU de datos en la subcapa MAC (control de acceso al medio) de la capa 2 son las mismas, los datos son datos transparentes. En el caso mostrado en la figura 9, los datos transparentes son, por ejemplo, datos de voz que puede transferirse a la unidad 10 IF de terminal sin ningún proceso en los datos de la capa 1 de entrada/salida por la unidad 30 de comunicación por radio. Por otro lado, los datos no transparentes son, por ejemplo, datos por paquetes que requieren algún proceso en los datos de la capa 1 emitidos desde la unidad 30 de comunicación por radio.

Como se ha mencionado anteriormente, los ejemplos concretos de los datos 95 y 96 transparentes en la figura 9 son datos de voz y datos digitales no restringidos, cada uno dividido por la unidad de bloques de transporte definida entre las capas 1 y 2. Estos datos transparentes divididos por la unidad de bloques de transporte es igual a MACPDU (y MACSDU) y, por lo tanto, cada uno de los datos de la unidad de bloques de transporte corresponde a la unidad de proceso de confidencialidad.

Puesto que los tipos datos tales como los datos de voz son datos de usuario que se mantienen transparentes en las subcapas RLC, mediante la implementación de una IF de MT (terminal móvil) - TA (adaptador de terminal) definida por ARIB (figuras 22, 23) como la interfaz serie para este modelo de transporte, se hace posible realizar el proceso de confidencialidad en los formatos en serie de IF de MT-TA sin ninguna conversión.

Además, un ejemplo concreto de los datos 97 no transparentes es, como se ha descrito anteriormente, los datos por paquetes o datos para la señalización, sin embargo, cada uno de los datos se divide en unidades (bloques de transporte) definidas entre las capas 1 y 2.

La unidad 40 de proceso de confidencialidad/integridad mostrada en la figura 9 realiza el proceso de confidencialidad y el proceso de integridad selectivamente sobre los datos no transparentes recibidos/emitidos desde/hacia la unidad 20 de control de comunicación por radio, y al mismo tiempo, la unidad 40 de proceso de confidencialidad/integridad siempre realiza, por ejemplo, el proceso de confidencialidad sobre los datos transparentes recibidos/emitidos entre la unidad 10 IF de terminal y la unidad 30 de comunicación por radio. La unidad 40 de proceso de confidencialidad/integridad no realiza el proceso de integridad en los datos transparentes. Si los datos transparentes incluyen datos que no requieren el proceso de confidencialidad, la unidad 20 de control de comunicación por radio hace que los datos transparentes que no requieren el proceso de confidencialidad no se

introduzcan en la unidad 40 de proceso de confidencialidad/integridad, pero se introduzcan en la unidad 20 de control de comunicación por radio. O es posible hacer que los datos transparentes que no requieren el proceso de confidencialidad se introduzcan en la unidad 40 de proceso de confidencialidad/integridad, pero no realizar el proceso de confidencialidad de los datos transparentes usando la señal de control de la unidad 20 de control de comunicación por radio.

La figura 10 muestra una configuración de la unidad 40 de proceso de confidencialidad/integridad.

A diferencia de la configuración mostrada en la figura 5, la figura 10 incluye como novedad una unidad 460 de proceso de confidencialidad. La unidad 460 de proceso de confidencialidad incluye una unidad 462 de encriptación y una unidad 463 de desencriptación. La unidad 462 de encriptación introduce los datos 95 transparentes desde la unidad 10 IF de terminal, encripta los datos de entrada para emitirlos a la unidad 30 de comunicación por radio como los datos 96 transparentes. Por otro lado, la unidad 463 de desencriptación introduce los datos 96 transparentes desde la unidad 30 de comunicación por radio, desencripta los datos de entrada para emitirlos a la unidad 10 IF de terminal como los datos 95 transparentes. Estos procedimientos de la unidad 460 de proceso de confidencialidad se realizan en base a la señal 99 de control de la unidad 410 IF. La señal 99 de control se deriva de la señal 91 de control. En consecuencia, la unidad 460 de proceso de confidencialidad realiza el proceso de confidencialidad en base a la señal de control emitida desde la unidad 20 de control de comunicación por radio. En la figura 10, los datos 92 se introducen/se emiten usando la interfaz paralela a través del bus. Por otro lado, los datos 95 y 96 transparentes se introducen/se emiten desde/hacia la unidad 460 de proceso de confidencialidad a través de la interfaz serie. Como se ha explicado anteriormente, la figura 10 muestra un caso en el que dos sistemas de interfaz de entrada/salida, es decir, la interfaz paralela y la interfaz serie se proporcionan en la unidad 40 de proceso de confidencialidad/integridad.

La figura 11 muestra una configuración en la que la unidad 460 de proceso de confidencialidad se añade a la unidad 40 de proceso de confidencialidad/integridad mostrada en la figura 7. Es eficaz tener la configuración mostrada en la figura 11 cuando la unidad de encriptación o la unidad de desencriptación generan flujos de claves en los que debe realizarse una operación XOR con los datos en serie como se muestra en la figura 12.

Como se muestra en la figura 11, los datos 95 y 96 transparentes se introducen/se emiten desde/hacia la unidad 460 de proceso de confidencialidad a través de la interfaz serie, y además, los datos en serie que se introducen/se emiten a través de la interfaz serie incluyen datos multiplexados de múltiples canales. Por ejemplo, cuando los datos del canal 2 se introducen como datos en serie después de que se introducen los datos del canal 1, la unidad 1 de encriptación correspondiente al canal 1 genera un flujo de claves para emitir a un multiplexor 481, la unidad 2 de encriptación correspondiente al canal 2 genera otro flujo de claves para emitir al multiplexor 481, y el multiplexor 481 multiplexa estos flujos de claves en el mismo formato que el sistema de datos de los datos 95. Se realiza una operación XOR con el flujo de claves multiplexado y la secuencia de datos de los datos 95 de entrada por el circuito 483 XOR. La unidad 460 de proceso de confidencialidad realiza las operaciones anteriores en base a la señal 99 de control, es decir, la señal 91 de control suministrada desde la unidad 20 de control de comunicación por radio. Mediante el uso de la configuración de la figura 11, el retraso de los datos en serie solo se provoca por la operación del circuito 483 XOR, que permite el proceso de alta velocidad.

La figura 13 muestra otra configuración en la que la unidad 420 de proceso de confidencialidad y la unidad 460 de proceso de confidencialidad de la figura 10 se combinan en una unidad 470 de proceso de confidencialidad.

La unidad 470 de proceso de confidencialidad procesa tanto los datos 92 recibidos/emitidos a través de la interfaz paralela como los datos 95, 96 recibidos/emitidos a través de la interfaz serie. La unidad 420 de proceso de confidencialidad y la unidad 460 de proceso de confidencialidad se unen en la unidad 470 de proceso de confidencialidad, de manera que puede reducirse los recursos de soporte físico. La unidad 470 de proceso de confidencialidad conmuta el procedimiento para los datos transparentes y el procedimiento para los datos no transparentes en base a la señal 99 de control, es decir, la señal 91 de control emitida desde la unidad 20 de control de comunicación por radio.

Realización 3.

La figura 25 muestra procedimientos de encriptación y desencriptación para una unidad de proceso de confidencialidad de acuerdo con la tercera realización. La parte izquierda de la figura 25 muestra un aparato de encriptación del lado del emisor. La parte derecha de la figura 25 muestra un aparato de desencriptación del lado del receptor.

A diferencia de la figura 15, la figura 25 contiene una memoria (memoria intermedia) de secuencia de números aleatorios para almacenar temporalmente una secuencia de números aleatorios generada por una función f8 para el proceso de confidencialidad de datos. La memoria de secuencia de números aleatorios almacena previamente la secuencia de números aleatorios generada por la función f8 para el proceso de confidencialidad de datos. Es decir, tan pronto como se obtiene la información para generar la secuencia de números aleatorios, la función f8 para el proceso de confidencialidad de datos inicia la generación de la secuencia de números aleatorios y emite la secuencia de números aleatorios a la memoria de secuencia de números aleatorios. La memoria de secuencia de

números aleatorios almacena temporalmente la secuencia de números aleatorios hasta que se recibe un mensaje (texto legible), y emite la secuencia de números aleatorios que se almacena de manera sincrónica con la entrada del mensaje (texto legible).

Por otro lado, en caso de desencriptación, tan pronto como se obtiene la información para generar la secuencia de números aleatorios, la función f8 para el proceso de confidencialidad de datos inicia la generación de la secuencia de números aleatorios y emite la secuencia de números aleatorios a la memoria de secuencia de números aleatorios. La memoria de secuencia de números aleatorios almacena temporalmente la secuencia de números aleatorios hasta que se recibe un mensaje (texto legible), y emite la secuencia de números aleatorios que se ha almacenado en la memoria de secuencia de números aleatorios de manera sincrónica con la entrada de los datos de texto cifrado.

Como se ha descrito anteriormente, las características del aparato de encriptación mostrado en la parte izquierda de la figura 25 son la generación de la secuencia de números aleatorios usando la función f8 para el proceso de confidencialidad de datos y la operación asíncrona del mensaje y la secuencia de números aleatorios. Es decir, la función f8 para el proceso de confidencialidad de datos genera la secuencia de números aleatorios antes de la operación de los datos de texto legible y la secuencia de números aleatorios y almacena previamente la secuencia de números aleatorios generada en la memoria de secuencia de números aleatorios.

Las características del aparato de desencriptación mostrado en la parte derecha de la figura 25 son la generación de una secuencia de números aleatorios usando la función f8 para el proceso de confidencialidad de datos y la operación asíncrona de los datos de texto cifrado y la secuencia de números aleatorios. Es decir, la función f8 para el proceso de confidencialidad de datos genera la secuencia de números aleatorios antes de la entrada de los datos de texto cifrado y almacena previamente la secuencia de números aleatorios generada en la memoria de secuencia de números aleatorios.

El aparato de encriptación y el aparato de desencriptación mostrados en la figura 25 realizan, por ejemplo, la encriptación/desencriptación del modo OFB (realimentación de salida), uno de los modos disponibles para el cifrado por bloques definido por ISO/IEC10116. O, puede usarse una variación del modo OFB. O, puede usarse cualquier modo siempre y cuando pueda generarse una secuencia de números aleatorios sin datos de texto legible o datos de texto cifrado. Sin embargo, puesto que el aparato de encriptación y el aparato de desencriptación mostrados en la figura 25 generan por adelantado una secuencia de números aleatorios sin datos de texto legible o datos de texto cifrado, no puede emplearse un modo en el que se genere una secuencia de números aleatorios mediante la entrada de datos de texto legible o datos de texto cifrado para el aparato de encriptación y el aparato de desencriptación mostrados en la figura 25.

En este caso, datos de texto legible significa datos que deben encriptarse y no se limitan a los datos que pueden leerse o escribirse por un ser humano. Por ejemplo, los datos de texto y los datos que consisten en caracteres son datos de texto legible. Los datos de voz, los datos de imagen, los datos de codificación, los datos comprimidos, etc. son datos de texto legible si deben encriptarse.

Los datos de texto cifrado significan datos encriptados. Los datos encriptados son datos de texto cifrado, independientemente del formato de datos de los datos antes de la encriptación, tales como los datos de texto, datos de caracteres, datos de voz, datos de imagen, datos de codificación, datos comprimidos, etc.

La figura 26 muestra un procedimiento de proceso de integridad realizado por una unidad de proceso de integridad de acuerdo con la tercera realización.

A diferencia de la figura 16, la figura 26 se proporciona con una memoria de datos (memoria intermedia) en una etapa anterior de la función f9 para el proceso de integridad de datos. Las memoria de datos introduce y almacena X ($X \geq 2$) piezas de datos y los datos de X señales de control. La función f9 para el proceso de integridad de datos introduce las X piezas de datos y los datos de las X señales de control almacenadas en la memoria de datos, genera X códigos de autenticación de mensajes y emite los X códigos de autenticación de mensajes juntos.

En el caso de que una clave de autenticación de mensajes (clave de integridad, IK) se comparta con las X piezas de datos, la clave de autenticación de mensajes (IK) puede introducirse directamente en la función f9 para el proceso de integridad de datos como se muestra en la figura 26 sin almacenar la clave de autenticación de mensajes (IK) en la memoria de datos. Cuando la clave de autenticación de mensajes (IK) difiere para cada dato, la clave de autenticación de mensajes debe almacenarse en la memoria de datos junto con otros datos de la señal de control.

En lo que sigue en el presente documento, se explicarán ejemplos concretos de una unidad de proceso de confidencialidad y una unidad de proceso de integridad mostradas en la figura 25 con referencia a las figuras.

La figura 27 muestra una unidad 20 de control de comunicación por radio y una unidad 40 de proceso de confidencialidad/integridad de acuerdo con la tercera realización.

La configuración, excepto lo siguiente, es la misma que la de la estación 100 móvil mostrada en la figura 9 de la segunda realización; los puntos diferentes con respecto a la segunda realización se explicarán con referencia a la

figura 27.

Se proporciona una CPU 29 dentro de la unidad 20 de control de comunicación por radio. Dentro de la unidad 40 de proceso de confidencialidad/integridad, se proporciona una unidad 420 de proceso de confidencialidad que tiene una interfaz paralela, otra unidad 460 de proceso de confidencialidad que tiene una interfaz serie, y una unidad 430 de proceso de integridad. La unidad 420 de proceso de confidencialidad incluye una unidad 422 de encriptación y una unidad 423 de desencriptación. La unidad 460 de proceso de confidencialidad incluye una unidad 462 de encriptación y una unidad 463 de desencriptación. La unidad 430 de proceso de integridad incluye una unidad 432 de anexión de códigos de autenticación de mensajes y una unidad 433 de verificación de integridad. La unidad 20 de control de comunicación por radio y la unidad 40 de proceso de confidencialidad/integridad están conectadas con un bus 90. El bus 90 conecta la CPU 29 dentro de la unidad 20 de control de la comunicación por radio, la unidad 420 de proceso de confidencialidad, la unidad 460 de proceso de confidencialidad, y la unidad 430 de proceso de integridad dentro de la unidad 40 de proceso de confidencialidad/integridad, y el bus 90 transfiere una señal 91 de control, los datos 92 y otro tipo de datos. La CPU 29 controla un proceso completo de la unidad 20 de control de comunicación por radio leyendo y ejecutando programas almacenados en el medio de grabación, tal como la memoria de solo lectura. El bus 90 es un bus para uso general que conecta otras unidades de proceso (no ilustrados) localizadas dentro o fuera de la unidad 20 de control de comunicación por radio y la unidad 40 de proceso de confidencialidad/integridad.

La figura 28 muestra en detalle la unidad 422 de encriptación y la unidad 423 de desencriptación de la unidad 420 de proceso de confidencialidad.

La unidad 422 de encriptación incluye un encriptador 610, una memoria 620 intermedia, y una unidad 630 XOR. La unidad 423 de desencriptación incluye un desencriptador 611, una memoria 621 intermedia, y una unidad 631 XOR. El encriptador 610 se corresponde con la función f8 para el proceso de confidencialidad de datos del lado del emisor mostrada en la figura 25. La memoria 620 intermedia se corresponde con la memoria de secuencia de números aleatorios de lado del emisor mostrada en la figura 25. En este caso, se emplea una memoria FIFO para la memoria 620 intermedia. La unidad 630 XOR realiza, por ejemplo, operaciones XOR de los datos en paralelo de 64 bits de manera simultánea. El desencriptador 611 se corresponde con la función f8 para el proceso de confidencialidad de datos del lado del receptor mostrada en la figura 25. La memoria 621 intermedia se corresponde con la memoria de secuencia de números aleatorios de lado del receptor mostrada en la figura 25. La unidad 631 XOR realiza, por ejemplo, operaciones XOR de los datos en paralelo de 64 bits al mismo tiempo.

La unidad 420 de proceso de confidencialidad introduce la señal 91 de control desde la CPU 29 a través del bus 90. En este momento, aún no se han introducido los datos 950 de texto legible. La CPU 29 conoce por adelantado la señal 91 de control y es capaz de transferir la señal 91 de control a la unidad 420 de proceso de confidencialidad desde la CPU 29 antes de la transferencia de los datos 950 de texto legible. La señal 91 de control incluye al menos una clave de encriptación (clave de cifrado, CK) y además, en este ejemplo, otra distinta a CK, una longitud en bits de datos que deben encriptarse/desencriptarse (LONGITUD, la longitud en bits = 256 bits en el caso de la figura 28), un enlace elevador/reductor (DIRECCIÓN), un contador (CONTADOR-C), y un identificador de canal lógico (PORTADOR). La clave de encriptación (CK), la longitud en bits de los datos que deben encriptarse/desencriptarse (LONGITUD), el enlace elevador/reductor (DIRECCIÓN), el contador (COUNT-C), y el identificador de canal lógico (PORTADOR) se introducen en la unidad 422 de encriptación o la unidad 423 de desencriptación como un señal 600 de control u otra señal 601 de control. Al introducir la señal 600 de control, el encriptador 610 empieza a generar una secuencia de números aleatorios y emite la secuencia de números aleatorios a la memoria 621 intermedia. En este caso, se supone que el encriptador 610 genera la secuencia de números aleatorios por una unidad de 64 bits. En este caso, la secuencia de números aleatorios de una unidad de 64 bits se emite desde el encriptador 610 y se almacena temporalmente en la memoria 620 intermedia. Como se ha descrito anteriormente, cuando la longitud en bits de los datos que deben encriptarse (LONGITUD) es de 256 bits, el encriptador 610 genera cuatro secuencias de números aleatorios de 64 bits y compone una secuencia de números aleatorios que tiene una longitud (64 bits x 4) suficiente, adecuada para la longitud en bits de los datos que deben encriptarse (256 bits).

La figura 28 muestra un caso en el que la memoria 620 intermedia almacena cuatro secuencias de números aleatorios que tienen 64 bits.

Posteriormente, la CPU 29 transfiere los datos 950 de texto legible que tienen una longitud en bits de 256 bits por una unidad de 64 bits a la unidad 422 de encriptación a través del bus 90. Cuando la unidad 630 XOR introduce los datos 950 de texto legible por una unidad de 64 bits, la memoria 620 intermedia emite de manera secuencial la secuencia 650 de números aleatorios de 64 bits. La unidad 630 XOR realiza operaciones XOR de los datos 950 de texto legible y la secuencia 650 de números aleatorios por una unidad de 64 bits a la vez y genera los datos 960 de texto cifrado de 64 bits. Los datos 960 de texto cifrado se devuelven a la CPU 29.

Una operación de la unidad 423 de desencriptación es la misma que la de la unidad 422 de encriptación, excepto que la entrada de la unidad 631 XOR son los datos 960 de texto cifrado y la salida son los datos 950 de texto legible, y en este caso se omitirá su explicación.

La unidad 630 XOR no siempre requiere introducir los datos 950 de texto legible después de generar cuatro

secuencias de números aleatorios (que tienen 256 bits) en la memoria 620 intermedia, sino que la unidad 630 XOR puede empezar la operación XOR cuando se almacena al menos una secuencia de números aleatorios de 64 bits en la memoria 620 intermedia. En este caso, la generación de la secuencia de números aleatorios por el encriptador 610 y la operación XOR por la unidad 630 XOR se realizan en paralelo y de manera simultánea. Mientras que la unidad 630 XOR realiza la operación XOR de los datos 950 de texto legible, el encriptador 610 introduce la siguiente señal 600 de control, genera la secuencia de números aleatorios para los datos 950 de texto legible que se introducirán a continuación, y almacena la secuencia de números aleatorios por adelantado para los datos de texto siguientes en la memoria 620 intermedia.

De esta manera, antes de la entrada de los datos 950 de texto legible desde la CPU 29, la unidad 422 de encriptación almacena previamente la secuencia de números aleatorios en la memoria 620 intermedia. En consecuencia, no hay tiempo de espera para la operación en la unidad XOR, lo que permite una encriptación de alta velocidad. De manera similar, puede realizarse una desencriptación de alta velocidad en la unidad 423 de desencriptación.

En cuanto a la capacidad de la memoria 620 intermedia o la memoria 621 intermedia, es suficiente que sea igual a o mayor que el tamaño de unidad de la secuencia de números aleatorios emitida desde el encriptador 610 o el desencriptador 611; sin embargo, es deseable que sea igual a o mayor que el valor máximo de la longitud en bits (LONGITUD) de los datos que deben encriptarse/desencriptarse especificada dentro de este sistema. Por ejemplo, si el tamaño de unidad de la secuencia de números aleatorios emitida desde el encriptador 610 o el desencriptador 611 es de 64 bits y el valor máximo de la longitud en bits (LONGITUD) de los datos que deben encriptarse/desencriptarse es de 5114 bits, es deseable que la capacidad de la memoria 620 intermedia o la memoria 621 intermedia sea igual o mayor que 5120 bits (64 x 80).

Además, la unidad 631 XOR realiza operaciones XOR de, por ejemplo, 64 bits; sin embargo, pueden procesarse datos paralelos de otro tamaño de bit, como 32 bits o 128 bits.

Se ha analizado que el tamaño de unidad de la secuencia de números aleatorios emitida desde el encriptador 610 o el desencriptador 611 es de 64 bits; sin embargo, el tamaño de unidad de la secuencia de números aleatorios puede variar, tal como 32 bits, 128 bits, etc.

No siempre se requiere que el tamaño de unidad de la secuencia de números aleatorios emitida desde el encriptador 610 o el desencriptador 611, el tamaño de lectura/escritura de la memoria 620 o 621 intermedia, y el tamaño de bit de los datos en paralelos de la unidad 631 XOR sean los mismos.

La figura 29 muestra otro ejemplo de la unidad 20 de control de comunicación por radio y la unidad 420 de proceso de confidencialidad.

A diferencia de la figura 28, la unidad 630 XOR y la unidad 631 XOR no están colocadas en la unidad 420 de proceso de confidencialidad, sino en la unidad 20 de control de comunicación por radio en el caso de la figura 29.

La CPU 29 lee la secuencia de números aleatorios (tantas como secuencias múltiples juntas) para los datos 950 de texto legible desde la memoria 620 intermedia a través del bus 90 y suministra las secuencias de números aleatorios a la unidad 630 XOR. En la unidad 630 XOR, se realiza la operación XOR entre los datos 950 de texto legible y la secuencia 650 de números aleatorios para generar los datos 960 de texto cifrado.

De manera similar, en la unidad 631 XOR, se lee la secuencia 651 de números aleatorios desde la memoria 621 intermedia por la CPU 29 a través del bus 90, la operación XOR se realiza con los datos 960 de texto cifrado, y se emiten los datos 950 de texto legible.

En el caso de la figura 29, la operación es tan simple que la CPU 29 lee la secuencia de números aleatorios desde la memoria 620 intermedia, y los datos 950 de texto legible y los datos 960 de texto cifrado no tienen que enviarse/devolverse a través del bus 90. Por lo tanto, en comparación con la configuración de la figura 28, la cantidad de datos que atraviesan el bus 90 puede reducirse a igual o menos de la mitad. Además, puede reducirse el tiempo de espera para usar el bus 90. Aún más, es posible eliminar la competencia para usar el bus 90.

En ambos casos de las figuras 28 y 29, la unidad 630 XOR y la unidad 631 XOR puede implementarse por soporte físico, soporte lógico, o una combinación de soporte físico y soporte lógico.

La figura 30 es un diagrama detallado que muestra la unidad 462 de encriptación y la unidad 463 de desencriptación de la unidad 460 de proceso de confidencialidad que tiene un interfaz serie.

A diferencia de la figura 28, se proporciona una unidad 632 XOR que realiza la operación XOR de los datos en serie de 1 bit en lugar de la unidad 630 XOR que realiza la operación XOR de los datos en paralelo. Y, además, se proporciona una unidad 633 XOR que realiza la operación XOR de los datos en serie de 1 bit en lugar de la unidad 631 XOR que realiza la operación XOR de los datos en paralelo. En la unidad 632 XOR, se introducen los datos 95 transparentes, se realiza en serie por 1 bit la operación XOR con la secuencia 650 de números aleatorios, y se emiten los datos 96 transparentes encriptados. Por otro lado, en la unidad 633 XOR, se introducen los datos 96

transparentes, se realiza en serie por 1 bit la operación XOR con la secuencia 651 de números aleatorios, y se emiten los datos 95 transparentes desencriptados.

En el caso de la figura 30, la secuencia de números aleatorios se genera y se almacena previamente en la memoria 620 intermedia y la memoria 621 intermedia, de manera que se elimina el tiempo de espera en la unidad 632 XOR y la unidad 633 XOR, lo que permite una operación XOR de alta velocidad.

En el caso de la figura 30, la unidad 632 XOR y la unidad 633 XOR también pueden implementarse por soporte físico, soporte lógico, o una combinación del soporte físico y el soporte lógico.

Además, la unidad 632 XOR y la unidad 633 XOR pueden localizarse fuera de la unidad 460 de proceso de confidencialidad.

La figura 31 es un diagrama detallado que muestra la unidad 432 de anexión de códigos de autenticación de mensajes y la unidad 433 de verificación de integridad de la unidad 430 de proceso de integridad.

La unidad 432 de anexión de códigos de autenticación de mensajes está provista de una memoria 660 intermedia, un generador 670 de códigos de autenticación de mensajes, y un anexador 680 de códigos de autenticación de mensajes. La unidad 433 de verificación de integridad está provista de una memoria 661 intermedia, un generador 671 de códigos de autenticación de mensajes, y un verificador 681 de integridad. La memoria 660 intermedia y la memoria 661 intermedia son memorias FIFO. La memoria 660 intermedia y la memoria 661 intermedia se corresponden con la memoria de datos en la figura 26. El generador 670 de códigos de autenticación de mensajes y el generador 671 de códigos de autenticación de mensajes se corresponden con la función f9 para el proceso de integridad de datos en la figura 26. El anexador 680 de códigos de autenticación de mensajes añade el código de autenticación de mensajes a los datos. El verificador 681 de integridad compara el código de autenticación de mensajes recibido desde el lado del emisor y el código de autenticación de mensajes generado en el lado del receptor y, si coinciden, el verificador 681 de integridad verifica la integridad de los datos.

En la figura 31, la CPU 29 envía cuatro piezas de datos 92, que requieren una verificación de integridad, junto a la unidad 432 de anexión de códigos de autenticación de mensajes. La CPU 29 también envía juntas cuatro señales 91 de control correspondientes a las cuatro piezas de datos 92, que requieren una verificación de integridad. La señal 91 de control incluye al menos una clave de autenticación de mensajes (IK), y además un enlace elevador/reductor (DIRECCIÓN), un contador (CONTADOR-C), y un número aleatorio (FRESH) generado para cada usuario. La CPU 29 transfiere, al menos, el enlace elevador/reductor (DIRECCIÓN), el contador (CONTADOR-C), y el número aleatorio (FRESH) generado para cada usuario a la memoria 660 intermedia como la señal 91 de control correspondiente a las cuatro piezas de datos. En cuanto a la clave de autenticación de mensajes (IK), pueden transferirse cuatro claves de autenticación de mensajes (IK) respectivas, correspondientes a las cuatro piezas de datos, a la memoria 660 intermedia, y cuando la clave de autenticación de mensajes (IK) es un valor fijo común a las cuatro piezas de datos, la clave de autenticación de mensajes (IK) no necesita almacenarse en la memoria 660 intermedia, sino que puede introducirse directamente en el generador 670 de códigos de autenticación de mensajes.

La señal 91 de control puede transferirse a través de la línea de señal de control del bus 90 como la señal de control y también puede transferirse a través de la línea de señal de datos del bus 90 como los datos. Las cuatro señales 91 de control pueden enviarse junto con las cuatro piezas de datos y también pueden enviarse por separado. La memoria 660 intermedia introduce y almacena las cuatro piezas de datos y las cuatro señales de control juntas. En este caso, que la CPU 29 transfiera las cuatro piezas de datos o las cuatro señales de control juntas significa que cuatro piezas de datos o cuatro señales de control se transfieren por una instrucción de transferencia. En lo que sigue en el presente documento, “juntos” significa “por una única instrucción” o “tratamiento de cosas múltiples juntas como un grupo, no por separado”. La carga de la CPU 29 y cada unidad de proceso pueden reducirse como resultado de una ejecución de la única instrucción. Además, el número de transferencias que pasan a través del bus 90 o cada línea de transmisión (no ilustradas) pueden reducirse como resultado de una transferencia o una entrada/salida por “tratamiento de cosas múltiples juntas como un grupo, no por separado”.

La memoria 660 intermedia realiza la correspondencia entre los datos y la señal de control y la almacena como datos de correspondencia. El generador 670 de códigos de autenticación de mensajes introduce los datos de correspondencia y genera el código de autenticación de mensajes de los datos en base a la señal de control. El generador 670 de códigos de autenticación de mensajes genera cuatro códigos de autenticación de mensajes a partir de las cuatro piezas de datos de correspondencia usando un algoritmo predeterminado, respectivamente, y emite los cuatro códigos de autenticación de mensajes juntos al anexador 680 de códigos de autenticación de mensajes. El generador 670 de códigos de autenticación de mensajes genera cuatro códigos de autenticación de mensajes que tienen una longitud de 32 bits cada uno. El anexador 680 de códigos de autenticación de mensajes añade los cuatro códigos de autenticación de mensajes a las cuatro piezas de datos, respectivamente, y los transfiere por una instrucción de la CPU 29.

En el caso de la entrada de cuatro piezas de datos que tienen una longitud de 256 bits, la unidad 432 de anexión de códigos de autenticación de mensajes devuelve los datos que tienen (256 + 32) x bits a la CPU 29.

Por otro lado, la unidad 433 de verificación de integridad introduce las cuatro piezas de datos junto con los códigos

de autenticación de mensajes añadidos. La unidad 433 de verificación de integridad también introduce cuatro señales 91 de control juntas. Como se ha analizado anteriormente, la clave de autenticación de mensajes (IK) puede almacenarse en la memoria 661 intermedia o puede introducirse directamente en el generador 671 de códigos de autenticación de mensajes.

La memoria 661 intermedia realiza la correspondencia de las cuatro piezas de datos y la almacena como datos de correspondencia. El generador 671 de códigos de autenticación de mensajes lee las cuatro piezas de datos de correspondencia almacenadas en la memoria 661 intermedia y genera cuatro códigos de autenticación de mensajes usando el mismo algoritmo que el generador 670 de códigos de autenticación de mensajes en el lado del emisor. El verificador 681 de integridad compara los cuatro códigos de autenticación de mensajes añadidos a las cuatro piezas de datos recibidas y los cuatro códigos de autenticación de mensajes generados por el generador 671 de códigos de autenticación de mensajes, respectivamente. Si coinciden, el verificador 681 de integridad envía una respuesta que muestra un estado normal, ya que se ha verificado la integridad.

Cuando la unidad 433 de verificación de integridad introduce los datos que consisten en cuatro piezas de datos que tienen una longitud de 256 bits y cuatro códigos de autenticación de mensajes que tienen una longitud de 32 bits ((256 + 3) bits x 4), el verificador 681 de integridad envía una respuesta de “1 bit x 4” a la CPU 29.

Aunque convencionalmente se transfieren piezas múltiples de datos, respectivamente, a la unidad 430 de proceso de integridad desde la CPU 29, en el caso de la figura 31, pueden transferirse juntas cuatro piezas de datos, lo que mejora la eficacia de utilización del bus 90. Es decir, puede reducirse el tiempo de espera del bus 90, y también puede reducirse la competencia para usar el bus 90.

La figura 31 muestra un caso en el que se transfieren juntas cuatro piezas de datos; sin embargo, el número de piezas de datos no se limita a cuatro. Además, el número de piezas de datos que puede mantener la memoria intermedia tampoco se limita a cuatro.

La longitud en bits de los datos no se limita a 256 bits, por ejemplo, la longitud en bits pueden ser 512 bits o 5114 bits. La capacidad de las memorias 660 y 661 intermedias es suficiente para almacenar los datos si es al menos dos veces la longitud total en bits de la longitud en bits de los datos y la longitud en bits de la señal de control; es decir, la capacidad de las memorias intermedias es suficiente cuando la memoria intermedia puede almacenar al menos dos piezas de datos de correspondencia. Por ejemplo, cuando el valor máximo de la longitud en bits de los datos que puede especificarse dentro de este sistema es de 5114 bits, es preferible que la capacidad de las memorias 660 y 661 intermedias sea al menos (5114 bits + la longitud en bits de la señal de control) x 2, respectivamente.

La figura 32 muestra otro ejemplo de la unidad 20 de control de comunicación por radio y la unidad 430 de proceso de integridad. La unidad 430 de proceso de integridad mostrada en la figura 32 incluye las unidades 434 y 435 de generación de códigos de autenticación de mensajes.

A diferencia de la figura 31, en la figura 32 el anexador 680 de códigos de autenticación de mensajes y el verificador 681 de integridad no están incluidos en la unidad 430 de proceso de integridad sino colocados en la unidad 20 de control de comunicación por radio. En el caso de la figura 32, el generador 670 de códigos de autenticación de mensajes transfiere cuatro códigos de autenticación de mensajes al anexador 680 de códigos de autenticación de mensajes por una instrucción de transferencia emitida desde la CPU 29. Por otro lado, el generador 671 de códigos de autenticación de mensajes transfiere cuatro códigos de autenticación al verificador 681 de integridad por una instrucción de transferencia emitida desde la CPU 29.

En el caso de la figura 32, la cantidad de transferencia de datos del bus 90 desde el generador 670 de códigos de autenticación de mensajes al anexador 680 de códigos de autenticación de mensajes es de 32 bits x 4. Además, la cantidad de transferencia de datos del bus 90 desde el generador 671 de códigos de autenticación de mensajes también es de 32 bits x 4.

La cantidad de transferencia de datos desde la unidad 430 de proceso de integridad a la unidad 20 de control de comunicación por radio mostrada en la figura 32 puede reducirse en gran medida en comparación con la cantidad de datos de transferencia devueltos en el caso de la figura 31, puesto que el generador 670 de códigos de autenticación de mensajes no necesita devolver los datos al anexador 680 de códigos de autenticación de mensajes.

En la unidad 430 de proceso de integridad mostrada en la figura 32, la unidad 434 de generación de códigos de autenticación de mensajes y la unidad 435 de generación de códigos de autenticación de mensajes tienen la misma configuración, de manera que pueden integrarse en una.

En los casos de las figuras 31 y 32, el procedimiento de transferencia de datos del bus 90, el procedimiento de entrada/salida de las memorias 660, 661 intermedias, el procedimiento de generación códigos de autenticación de los generadores 670, 671 de códigos de autenticación de mensajes, el procedimiento de anexión de códigos de autenticación del anexador 680 de códigos de autenticación de mensajes, y el procedimiento de verificación del verificador 681 de integridad se realizan en piezas múltiples de datos “juntas”. Desde el punto de vista de la eficacia de utilización de la CPU 29 y el bus 90, es deseable realizar al menos uno de los procedimientos de envío de datos y los procedimientos de recepción de datos del bus 90 “por una sola instrucción” o por “tratamiento de piezas de datos

múltiples como un grupo, no por separado".

En ambos casos de las figuras 31 y 32, el generador 670 de códigos de autenticación de mensajes, el generador 671 de códigos de autenticación de mensajes, el anexador 680 de códigos de autenticación de mensajes, y el verificador 681 de integridad pueden implementarse por el soporte físico, el soporte lógico, o una combinación del soporte físico y el soporte lógico.

La figura 33 muestra otra configuración de la unidad 422 de encriptación.

La figura 33 muestra un caso en el que se proporcionan memorias intermedias múltiples y que conmutan mediante un conmutador SW. El conmutador SW puede conmutarse, por ejemplo, por un identificador de canal lógico. Es decir, cuando hay n canales lógicos, puede prepararse por adelantado una secuencia de números aleatorios para cada canal lógico, proporcionando n memorias intermedias.

La figura 34 muestra un caso en el que se proporcionan n memorias intermedias y n circuitos XOR.

En el caso de la figura 35, se proporcionan n memorias intermedias y se proporcionan encriptadores múltiples.

De esta manera, al proporcionar memorias intermedias múltiples para los canales lógicos respectivos, el proceso de confidencialidad para cada canal puede realizarse a una alta velocidad.

La unidad de desencriptación puede configurarse para tener memorias intermedias múltiples para los canales respectivos como los casos de las figuras 33, 34, y 35, que no se ilustran. Además, la unidad 432 de anexión de códigos de autenticación de mensajes y la unidad 433 de verificación de integridad pueden estar provistas de memorias intermedias múltiples para los canales respectivos como los casos de las figuras 33, 34, y 35.

La configuración de la tercera realización no se limita a la mostrada en la figura 27, y la configuración puede ser similar a las mostradas en las figuras 4, 5, 6, 7, 8, 10, 11, etc. Por ejemplo, el proceso de confidencialidad y el proceso de integridad pueden realizarse por un módulo como se muestra en la figura 4. La encriptación y la desencriptación pueden realizarse por un módulo. Además, la anexión del código de autenticación de mensajes y la verificación de integridad pueden realizarse por un módulo. Aún más, cada módulo puede ser plural.

Las memorias 620, 621, 660, y 661 intermedias no se limitan a las memorias FIFO, sino que pueden ser memorias de desplazamiento, memorias mapeadas de direcciones, memorias caché, o registros.

Cuando la CPU 29 accede a las memorias 620, 621, 660, y 661 intermedias, dicho acceso puede realizarse usando direcciones de memoria o direcciones de entrada/salida.

El aparato de encriptación, el aparato de desencriptación, la unidad (aparato) de anexión de códigos de autenticación de mensajes, la unidad (aparato) de verificación de integridad, y la unidad (aparato) de generación de códigos de autenticación de mensajes, que se han explicado en la tercera realización, no se limitan a las usadas para el aparato de comunicación por radio, sino que pueden emplearse dentro de un aparato de comunicación por cable, un ordenador, u otros dispositivos electrónicos.

La unidad 40 de proceso de confidencialidad/integridad puede configurarse por el soporte físico. Por ejemplo, la configuración puede implementarse mediante un FPGA o un LSI personalizado. Además, la unidad 40 de proceso de confidencialidad/integridad puede implementarse por el programa de soporte lógico. En caso de que la unidad 40 de proceso de confidencialidad/integridad se implemente por el programa de soporte lógico, la CPU de la unidad 20 de control de comunicación por radio ejecuta el programa de soporte lógico.

Además, la unidad 40 de proceso de confidencialidad/integridad puede implementarse por una combinación del soporte físico y el soporte lógico. Por ejemplo, la unidad 40 de proceso de confidencialidad/integridad puede implementarse por un DSP (procesador de señales digitales) y un microprograma o un programa fijo de máquina ejecutado por el DSP.

En lo que sigue en el presente documento, se explicará un ejemplo concreto con referencia a las figuras 17 a 20.

La figura 17 muestra una configuración del módulo 51 de encriptación (o el módulo 71 de desencriptación) usado para la unidad 421 de encriptación/desencriptación.

El módulo 51 de encriptación incluye un planificador 511 de claves y una unidad 512 de aleatorización de datos. El planificador 511 de claves introduce una clave K y genera n claves extendidas ExtK1 a ExtKn. La unidad 512 de aleatorización de datos genera un número aleatorio usando una función F y un circuito XOR. La función F introduce la clave extendida y realiza una transformación de datos no lineal.

En el módulo 51 de encriptación, pueden emplearse diversos algoritmos de cifrado por bloques, tales como:

(1) DES (norma de encriptación de datos);
(2) MISTY, que es el algoritmo de cifrado por bloques desvelado en la publicación internacional número

WO97/9705 (número de serie US 08/83640);
(3) KASUMI, que es la técnica de cifrado por bloques de 64 bits en base al algoritmo de cifrado por bloques MISTY anterior y se determina para emplearse como cifrado estándar internacional para la próxima generación de teléfonos celulares (IMT2000); y
(4) Camellia, que es el algoritmo de cifrado por bloques desvelado en la solicitud de patente japonesa número 2000-64614 (presentada el 9 de marzo de 2000).

Además, estos algoritmos de cifrado por bloques como DES, MISTY, KASUMI, y Camellia pueden emplearse en el módulo 71 de desencriptación.

La figura 18 muestra la forma de implementación de la unidad 40 de proceso de confidencialidad/integridad.

La figura 18 muestra un caso en el que la unidad 40 de proceso de confidencialidad/integridad se implementa dentro de FPGA, IC o LSI. Es decir, la unidad 40 de proceso de confidencialidad/integridad puede implementarse por el soporte físico. Además, la unidad 40 de proceso de confidencialidad/integridad también puede implementarse por una placa de circuito impreso, que no se muestra en la figura.

La figura 19 muestra un caso en el que la unidad 40 de proceso de confidencialidad/integridad se implementa por el soporte lógico.

La unidad 40 de proceso de confidencialidad/integridad puede implementarse por un programa 47 de cifrado. El programa 47 de cifrado se almacena en una ROM (memoria de solo lectura) 42 (un ejemplo de almacenamiento). El programa 47 de cifrado puede almacenarse en una RAM (memoria de acceso aleatorio) u otro almacenamiento tal como un disco flexible o un disco fijo. Además, el programa 47 de cifrado puede descargarse desde un servidor. El programa 47 de cifrado se hace funcionar como una subrutina. El programa 47 de cifrado se solicita para la ejecución de una subrutina desde un programa 46 de aplicación almacenado en la RAM 45 como una solicitud de subprograma. De otra manera, el programa 47 de cifrado puede activarse por la generación de una interrupción recibida en una unidad 43 de control de interrupción. Una memoria 55 puede ser una parte de la RAM 45. El programa 46 de aplicación y el programa 47 de cifrado son programas ejecutados por la CPU 41.

La figura 20 muestra el mecanismo para solicitar el programa 47 de cifrado por el programa 46 de aplicación que se hace funcionar en la unidad 20 de control de comunicación por radio.

El programa 46 de aplicación solicita el programa 47 de cifrado usando los parámetros de una clave K, un valor IV inicial, datos M de texto legible, y datos C de texto cifrado. El programa 47 de cifrado introduce la clave K, el valor IV inicial, los datos M de texto legible y los datos C de texto cifrado. Si el programa 47 de cifrado y el programa de desencriptación son el mismo, el programa 47 de cifrado se solicita usando los parámetros de la clave K, el valor IV inicial, los datos C de texto cifrado y los datos M de texto legible.

Además, el programa 47 de cifrado puede implementarse por un procesador de señales digitales y un programa leído y ejecutado por el procesador de señales digitales, aunque no se muestra en la figura. Es decir, el programa 47 de cifrado puede implementarse mediante la combinación del soporte físico y el soporte lógico.

La explicación anterior en referencia a las figuras 18, 19, y 20 se aplica a la encriptación, sin embargo, la desencriptación puede implementarse de la misma manera.

El sistema de encriptación o el sistema de desencriptación pueden instalarse en unos dispositivos electrónicos. El sistema puede instalarse en todo tipo de dispositivos electrónicos, por ejemplo, un ordenador personal, una máquina de fax, un teléfono celular, una cámara de vídeo, una cámara digital o una cámara de TV. En particular, la característica de la realización puede conseguirse eficazmente cuando se encriptan/desencriptan los datos de múltiples canales. O la aplicación de la realización puede ser eficaz en caso de que los datos se reciban de manera aleatoria de múltiples usuarios y se desencripten, o los datos de múltiples usuarios se generen de manera aleatoria y se encripten respectivamente en tiempo real. Es decir, la encriptación/desencriptación de la realización anterior puede ser muy eficaz cuando el número de aparatos para encriptar/desencriptar es pequeño en comparación con el número de tipos de datos que deben encriptarse/desencriptarse. Por ejemplo, la encriptación/desencriptación de la realización anterior es muy eficaz cuando se aplica a un servidor que tiene que soportar muchos ordenadores de clientes o una estación base o una unidad de control de línea que tiene que recoger y distribuir datos desde/hacia muchos teléfonos celulares.

En el ejemplo anterior, aunque la unidad 20 de control de comunicación por radio y la unidad 40 de proceso de confidencialidad/integridad se conectan con la interfaz paralela a través del bus, la interfaz serie puede usarse para conectar la unidad 20 de control de comunicación por radio y la unidad 40 de proceso de confidencialidad/integridad. Además, aunque en la explicación anterior, la unidad 10 IF de terminal y la unidad 40 de proceso de confidencialidad/integridad, la 30 y la unidad 40 de proceso de confidencialidad/integridad, se conectan con la interfaz serie, la interfaz paralela puede usarse para el proceso a una velocidad superior en lugar de la interfaz serie.

En el caso de las figuras 9 y 10, aunque la unidad 460 de proceso de confidencialidad se proporciona dentro de la unidad 40 de proceso de confidencialidad/integridad, la unidad 460 de proceso de confidencialidad puede

proporcionarse independientemente de la unidad 40 de proceso de confidencialidad/integridad, y la unidad 460 de proceso de confidencialidad puede colocarse entre la unidad 10 IF de terminal y la unidad 30 de comunicación por radio.

Aplicabilidad industrial

Como se ha descrito, de acuerdo con las realizaciones anteriores, las piezas de datos múltiples se almacenan previamente en la memoria intermedia, lo que permite realizar el proceso de confidencialidad y el proceso de integridad a una alta velocidad.

Además, puede reducirse el número de transferencias de datos para el proceso de confidencialidad y el proceso de integridad, lo que también reduce la carga de la CPU y el bus.

Además, de acuerdo con la realización anterior, se proporcionan múltiples unidades de proceso de confidencialidad y múltiples unidades de proceso de integridad dentro de la unidad de proceso de confidencialidad/integridad de acuerdo con el número de canales o la cantidad de los datos, permitiendo el proceso de datos a alta velocidad mediante el proceso paralelo simultáneo.

REIVINDICACIONES

1. Un aparato de encriptación que comprende:

una unidad (29) de proceso central para introducir y emitir una señal de control a usar para generar una secuencia de números aleatorios y los datos de texto legible;
un encriptador (610) para introducir la señal de control desde la unidad (29) de proceso central y generar la secuencia de números aleatorios en base a la señal de control;
una memoria (620) de secuencia de números aleatorios para almacenar la secuencia de números aleatorios generada por el encriptador (610); y
una unidad (630) de funcionamiento para introducir los datos de texto legible desde la unidad (29) de proceso central, realizar una operación de los datos de texto legible recibidos y la secuencia de números aleatorios almacenada en la memoria (620) de secuencia de números aleatorios y emitir datos de texto cifrado,
la unidad (29) de proceso central está adaptada para emitir la señal de control antes de emitir los datos de texto legible, y el encriptador (610) está adaptado para generar la secuencia de números aleatorios para los datos de texto legible que se introducirán a continuación en la unidad (630) de funcionamiento,
caracterizado porque
la unidad (29) de proceso central está adaptada para, en primer lugar, iniciar la generación de la secuencia de números aleatorios por el encriptador (610) y la memorización de la secuencia de números aleatorios por la memoria (620) de secuencia de números aleatorios y, a continuación, iniciar la operación de los datos de texto legible y la secuencia de números aleatorios por la unidad (630) de funcionamiento,
y para realizar posteriormente la generación de la secuencia de números aleatorios para los siguientes datos de texto legible por el encriptador (610), la memorización de la secuencia de números aleatorios para los siguientes datos de texto legible por la memoria (620) de secuencia de números aleatorios, y la operación de los datos de texto legible y la secuencia de números aleatorios por la unidad (630) de funcionamiento en paralelo.

2. El aparato de encriptación de la reivindicación 1,
en el que el encriptador (610) introduce al menos una clave de encriptación y una longitud de los datos de texto legible, genera la secuencia de números aleatorios que tiene la longitud de los datos de texto legible usando la clave de encriptación, y hace que la memoria (620) de secuencia de números aleatorios almacene la secuencia de números aleatorios generada, y
en el que la memoria de secuencia de números aleatorios incluye una memoria (620) intermedia para emitir la secuencia de números aleatorios almacenada en caso de que la unidad de funcionamiento introduzca los datos de texto legible.

3. El aparato de encriptación de la reivindicación 1, en el que:

la unidad (630) de funcionamiento introduce los datos de texto legible correspondientes a la pluralidad de canales;
el encriptador (610) introduce la información de identificación de canal para identificar un canal y genera la secuencia de números aleatorios para cada uno de la pluralidad de canales;
la memoria (620) de secuencia de números aleatorios almacena la secuencia de números aleatorios generada por el encriptador (610) para cada uno de la pluralidad de canales; y
la unidad (630) de funcionamiento introduce la secuencia de números aleatorios correspondiente a cada uno de la pluralidad de canales desde los que se introducen los datos de texto legible y encripta los datos de texto legible.

4. Un aparato de desencriptación que comprende:

una unidad (29) de proceso central para introducir y emitir una señal de control a usar para generar unas secuencias de números aleatorios y los datos de texto cifrado;
un desencriptador (611) para introducir la señal de control desde la unidad (29) de proceso central y generar la secuencia de números aleatorios en base a la señal de control;
una memoria (621) de secuencia de números aleatorios para almacenar la secuencia de números aleatorios generada por el desencriptador (611); y
una unidad (631) de funcionamiento para introducir los datos de texto cifrado, realizar una operación de los datos de texto cifrado recibidos y la secuencia de números aleatorios almacenada en la memoria (621) de secuencia de números aleatorios, y emitir los datos de texto legible, en el que
la unidad (29) de proceso central está adaptada para emitir la señal de control antes de emitir los datos de texto cifrado, y el desencriptador (611) está adaptado para generar la secuencia de números aleatorios para los datos de texto cifrado que se introducirán a continuación en la unidad (631) de funcionamiento,
caracterizado porque
la unidad (29) de proceso central está adaptada para, en primer lugar, iniciar la generación de la secuencia de números aleatorios por el desencriptador (611) y la memorización de la secuencia de números aleatorios por la memoria (621) de secuencia de números aleatorios y, a continuación, iniciar la operación de los datos de texto cifrado y la secuencia de números aleatorios por la unidad (631) de funcionamiento,
y para realizar posteriormente la generación de la secuencia de números aleatorios para los siguientes datos de

texto cifrado por el desencriptador (611), la memorización de la secuencia de números aleatorios para los siguientes datos de texto cifrado por la memoria (621) de secuencia de números aleatorios, y la operación de los datos de texto cifrado y la secuencia de números aleatorios por la unidad (631) de funcionamiento en paralelo.

5. El aparato de desencriptación de la reivindicación 4,
en el que el desencriptador (611) introduce al menos una clave de desencriptación y una longitud de los datos de texto cifrado, genera la secuencia de números aleatorios que tiene la longitud de los datos de texto cifrado usando la clave de desencriptación, y hace que la memoria (621) de secuencia de números aleatorios almacene la secuencia de números aleatorios generada, y
en el que la memoria de secuencia de números aleatorios incluye una memoria (621) intermedia para emitir la secuencia de números aleatorios almacenada en caso de que la unidad (631) de funcionamiento introduzca los datos de texto cifrado.

6. El aparato de desencriptación de la reivindicación 4, en el que:

la unidad (631) de funcionamiento introduce los datos de texto cifrado correspondientes a la pluralidad de canales;
el desencriptador (611) introduce la información de identificación de canal para identificar un canal y genera la secuencia de números aleatorios para cada uno de la pluralidad de canales;
la memoria (621) de secuencia de números aleatorios almacena la secuencia de números aleatorios generada por el desencriptador (611) para cada uno de la pluralidad de canales; y
la unidad (631) de funcionamiento introduce la secuencia de números aleatorios correspondiente a cada uno de los canales desde los que se introducen los datos de texto cifrado y desencripta los datos de texto cifrado.

7. Un aparato de comunicación por radio que comprende:

una unidad (10) de interfaz de terminal para introducir los datos;
una unidad (20) de control de comunicación por radio para introducir los datos recibidos por la unidad (10) de interfaz de terminal, procesar los datos en base a un protocolo, y emitir un resultado del proceso;
una unidad (420) de proceso de confidencialidad para introducir una señal de control y los datos desde la unidad (20) de control de comunicación por radio, realizar el proceso de confidencialidad encriptando los datos recibidos en base a la entrada de señales de control, y emitir los datos procesados a la unidad (20) de control de comunicación por radio; y
una unidad (30) de comunicación por radio para introducir, modular, y enviar los datos emitidos por la unidad (20) de control de comunicación por radio, en el que la unidad (420) de proceso de confidencialidad incluye un aparato de encriptación de acuerdo con una de las reivindicaciones 1-3.

8. Un aparato de comunicación por radio que comprende:

una unidad (30) de comunicación por radio para recibir y demodular los datos;
una unidad (20) de control de comunicación por radio para introducir los datos demodulados por la unidad (30) de comunicación por radio, y procesar y emitir los datos en base al protocolo;
una unidad (420) de proceso de confidencialidad para introducir la señal de control y los datos, realizar un proceso de aleatorización de datos desencriptando los datos para los datos recibidos, y emitir los datos procesados a la unidad (20) de control de comunicación por radio; y
una unidad (10) de interfaz de terminal para introducir y emitir los datos procesados por la unidad (20) de control de comunicación por radio, en el que la unidad (30) de comunicación por radio está adaptada para emitir la señal de control antes de emitir los datos, y
la unidad (420) de proceso de confidencialidad incluye un aparato de desencriptación de acuerdo con una de las reivindicaciones 4-6.

Fig. 1

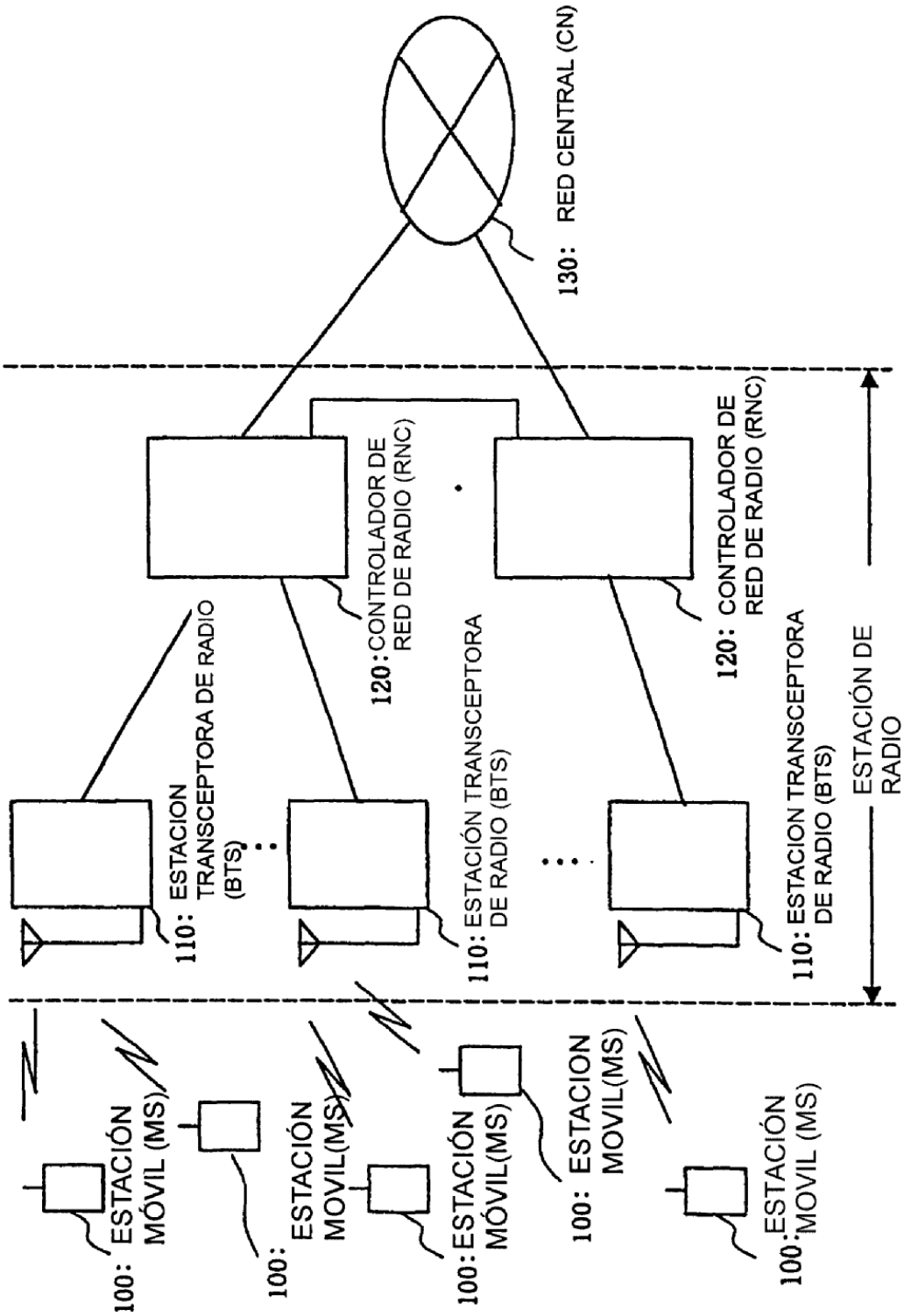

130: RED CENTRAL (CN)
120: CONTROLADOR DE RED DE RADIO (RNC)
120: CONTROLADOR DE RED DE RADIO (RNC)
110: ESTACION TRANSCEPTORA DE RADIO (BTS)
110: ESTACIÓN TRANSCEPTORA DE RADIO (BTS)
110: ESTACION TRANSCEPTORA DE RADIO (BTS)
ESTACIÓN DE RADIO
100: ESTACIÓN MÓVIL (MS)
100: ESTACIÓN MOVIL(MS)
100: ESTACIÓN MÓVIL(MS)
100: ESTACION MOVIL(MS)
100: ESTACIÓN MOVIL (MS)

Fig. 2

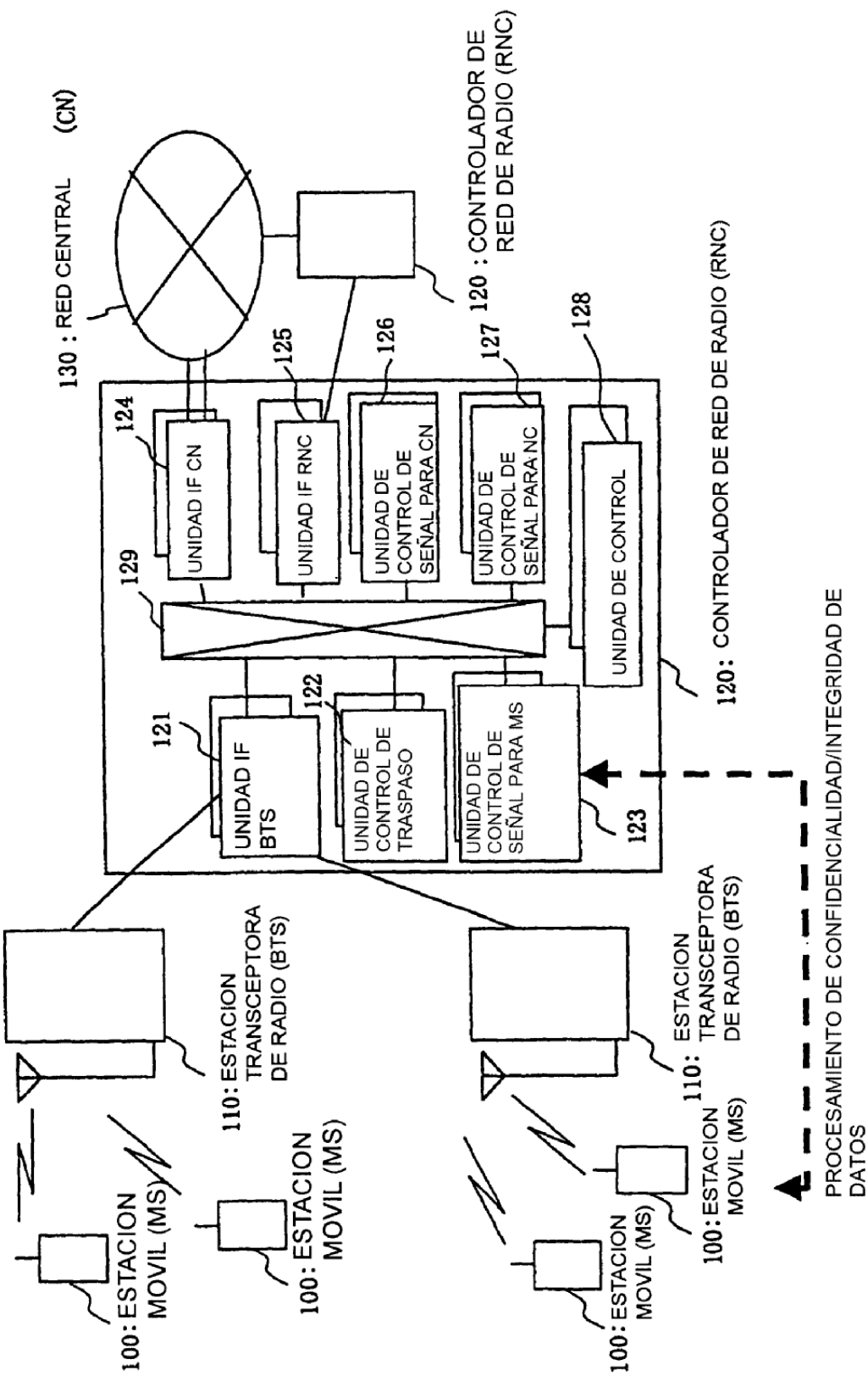

130 : RED CENTRAL (CN)
120 : CONTROLADOR DE RED DE RADIO (RNC)
124
125
126
127
128
129
UNIDAD IF CN
UNIDAD IF RNC
UNIDAD DE CONTROL DE SEÑAL PARA CN
UNIDAD DE CONTROL DE SEÑAL PARA NC
UNIDAD DE CONTROL
121
122
123
UNIDAD IF BTS
UNIDAD DE CONTROL DE TRASPASO
UNIDAD DE CONTROL DE SEÑAL PARA MS
120: CONTROLADOR DE RED DE RADIO (RNC)
110: ESTACION TRANSCEPTORA DE RADIO (BTS)
100: ESTACION MOVIL (MS)
PROCESAMIENTO DE CONFIDENCIALIDAD/INTEGRIDAD DE DATOS

Fig. 3

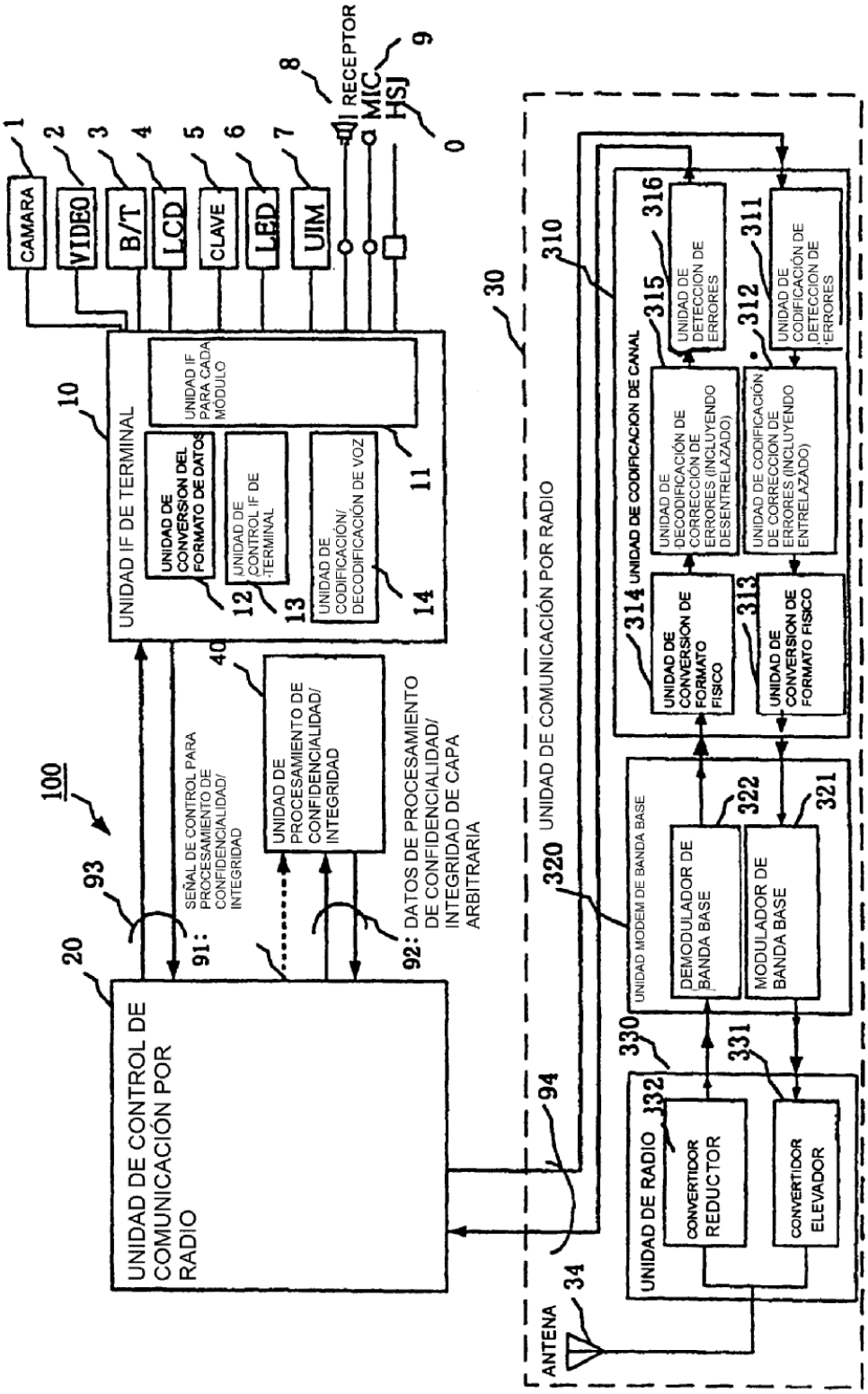

CAMARA
VIDEO
B/T
LCD
CLAVE
LED
UIM
RECEPTOR
MIC
HSJ
UNIDAD IF DE TERMINAL
UNIDAD DE CONVERSION DEL FORMATO DE DATOS
UNIDAD DE CONTROL IF DE TERMINAL
UNIDAD DE CODIFICACIÓN/ DECODIFICACIÓN DE VOZ
UNIDAD IF PARA CADA MÓDULO
UNIDAD DE COMUNICACIÓN POR RADIO
UNIDAD DE CONTROL DE COMUNICACIÓN POR RADIO
SEÑAL DE CONTROL PARA PROCESAMIENTO DE CONFIDENCIALIDAD/ INTEGRIDAD
UNIDAD DE PROCESAMIENTO DE CONFIDENCIALIDAD/ INTEGRIDAD
DATOS DE PROCESAMIENTO DE CONFIDENCIALIDAD/ INTEGRIDAD DE CAPA ARBITRARIA
UNIDAD DE CODIFICACION DE CANAL
UNIDAD DE DECODIFICACIÓN DE CORRECCIÓN DE ERRORES (INCLUYENDO DESENTRELAZADO)
UNIDAD DE DETECCION DE ERRORES
UNIDAD DE CODIFICACIÓN DE CORRECCIÓN DE ERRORES (INCLUYENDO ENTRELAZADO)
UNIDAD DE CODIFICACIÓN DE DETECCION DE ERRORES
UNIDAD DE CONVERSION DE FORMATO FISICO
UNIDAD DE CONVERSION DE FORMATO FISICO
UNIDAD MODEM DE BANDA BASE
DEMODULADOR DE BANDA BASE
MODULADOR DE BANDA BASE
UNIDAD DE RADIO
CONVERTIDOR REDUCTOR
CONVERTIDOR ELEVADOR
ANTENA

Fig. 4

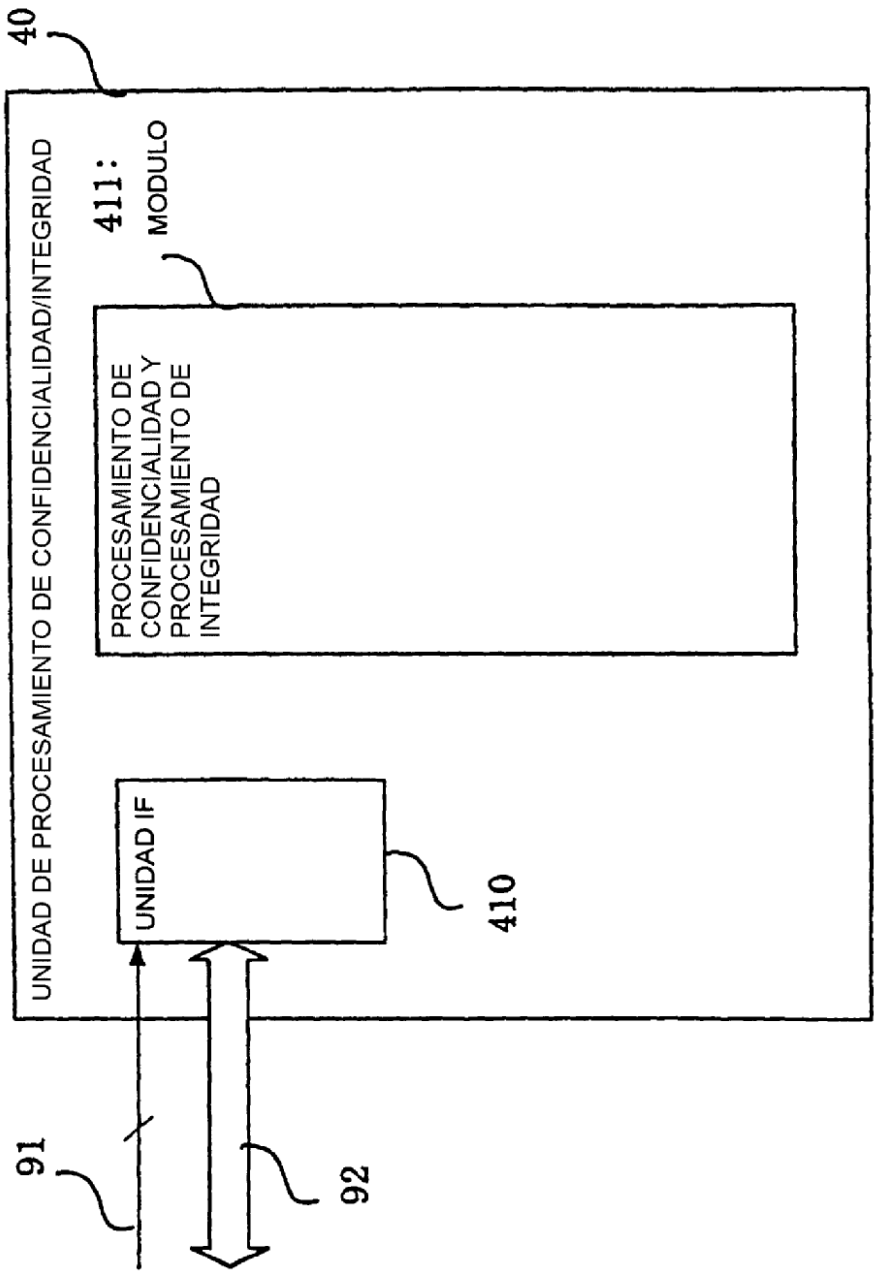

40
UNIDAD DE PROCESAMIENTO DE CONFIDENCIALIDAD/INTEGRIDAD
411: MODULO
PROCESAMIENTO DE CONFIDENCIALIDAD Y PROCESAMIENTO DE INTEGRIDAD
UNIDAD IF
410
91
92

Fig. 5

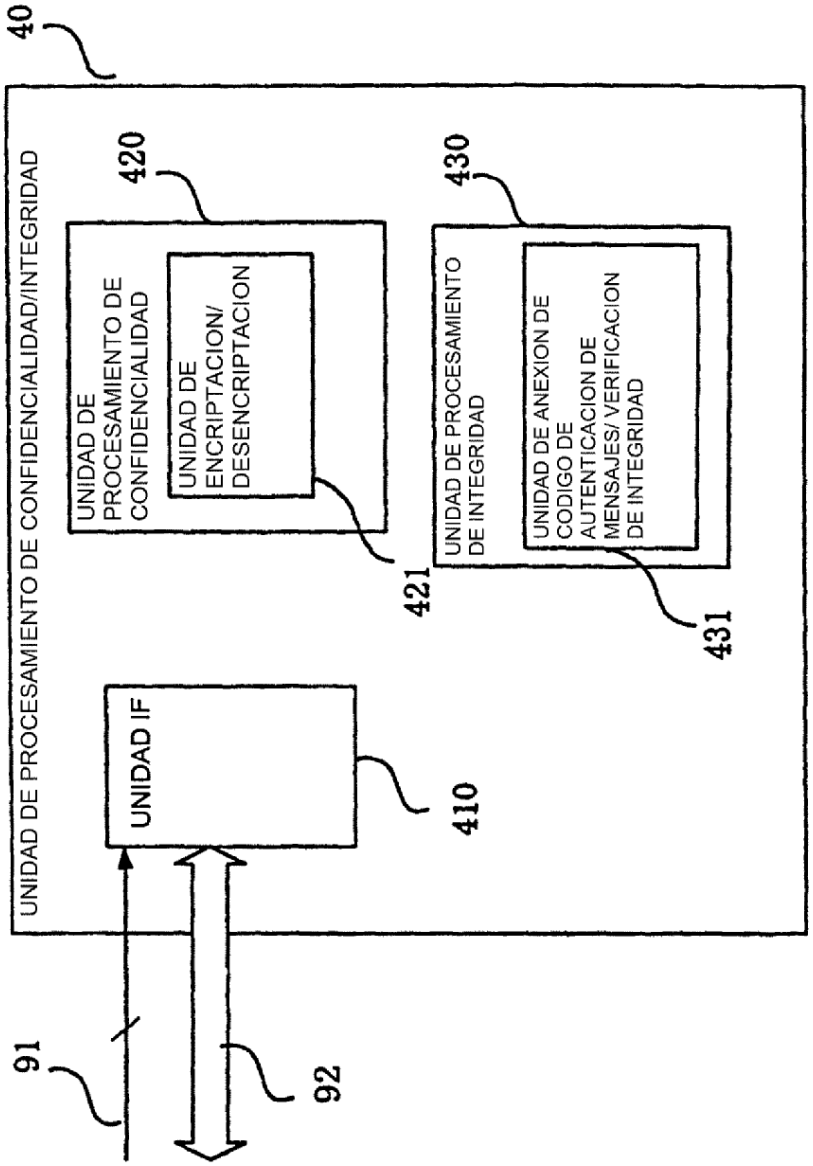

40
UNIDAD DE PROCESAMIENTO DE CONFIDENCIALIDAD/INTEGRIDAD
420
UNIDAD DE PROCESAMIENTO DE CONFIDENCIALIDAD
UNIDAD DE ENCRIPTACION/ DESENCRIPTACION
421
430
UNIDAD DE PROCESAMIENTO DE INTEGRIDAD
UNIDAD DE ANEXION DE CODIGO DE AUTENTICACION DE MENSAJES/ VERIFICACION DE INTEGRIDAD
431
UNIDAD IF
410
91
92

Fig. 6

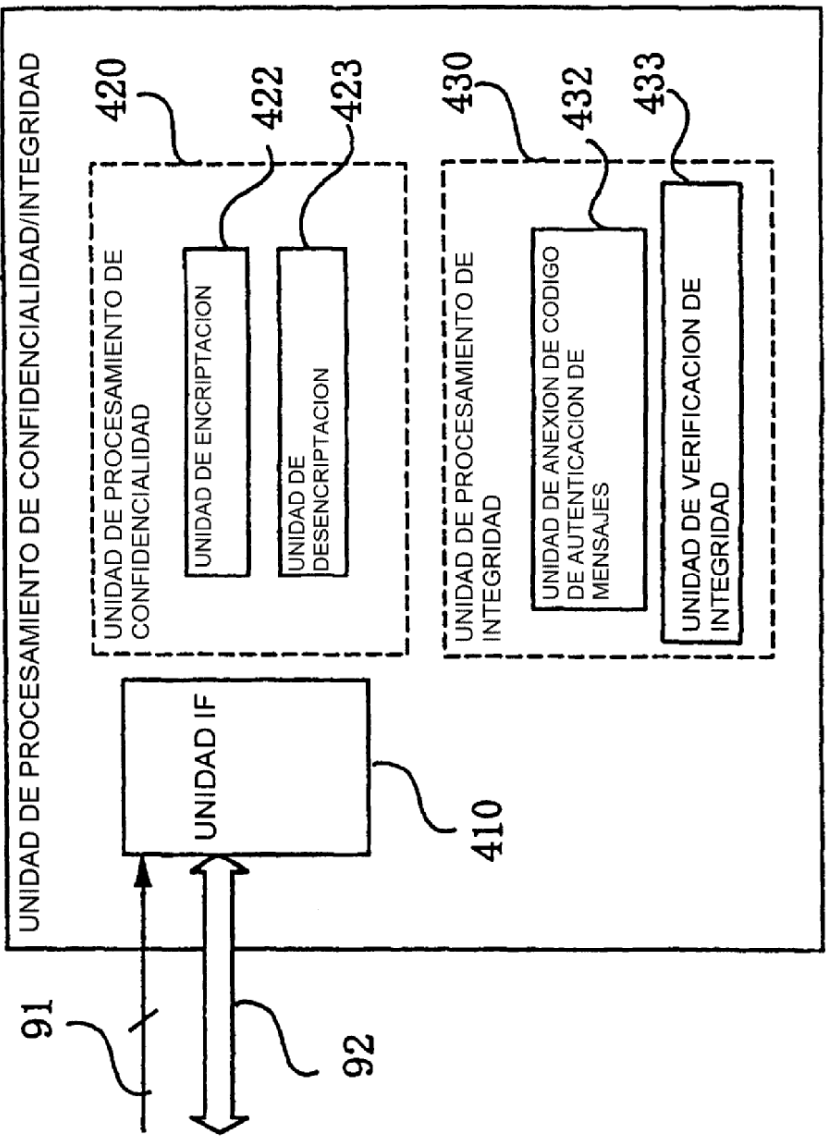

40
UNIDAD DE PROCESAMIENTO DE CONFIDENCIALIDAD/INTEGRIDAD
420
UNIDAD DE PROCESAMIENTO DE CONFIDENCIALIDAD
422
UNIDAD DE ENCRIPTACION
423
UNIDAD DE DESENCRIPTACION
430
UNIDAD DE PROCESAMIENTO DE INTEGRIDAD
432
UNIDAD DE ANEXION DE CODIGO DE AUTENTICACION DE MENSAJES
433
UNIDAD DE VERIFICACION DE INTEGRIDAD
UNIDAD IF
410
91
92

Fig. 7

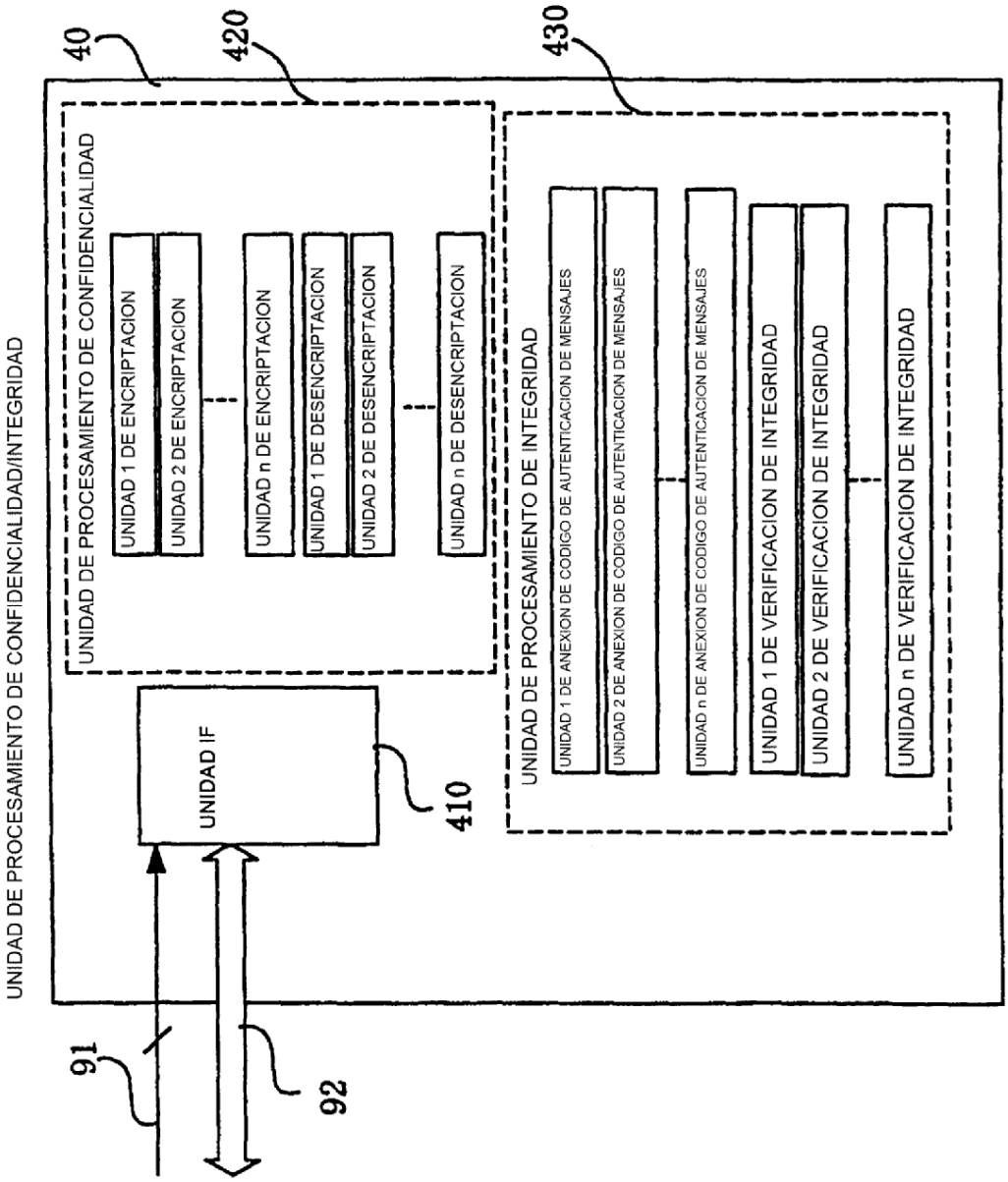

UNIDAD DE PROCESAMIENTO DE CONFIDENCIALIDAD/INTEGRIDAD
40
420
430
UNIDAD DE PROCESAMIENTO DE CONFIDENCIALIDAD
UNIDAD 1 DE ENCRIPTACION
UNIDAD 2 DE ENCRIPTACION
UNIDAD n DE ENCRIPTACION
UNIDAD 1 DE DESENCRIPTACION
UNIDAD 2 DE DESENCRIPTACION
UNIDAD n DE DESENCRIPTACION
UNIDAD IF
410
UNIDAD DE PROCESAMIENTO DE INTEGRIDAD
UNIDAD 1 DE ANEXION DE CODIGO DE AUTENTICACION DE MENSAJES
UNIDAD 2 DE ANEXION DE CODIGO DE AUTENTICACION DE MENSAJES
UNIDAD n DE ANEXION DE CODIGO DE AUTENTICACION DE MENSAJES
UNIDAD 1 DE VERIFICACION DE INTEGRIDAD
UNIDAD 2 DE VERIFICACION DE INTEGRIDAD
UNIDAD n DE VERIFICACION DE INTEGRIDAD
91
92

Fig. 8

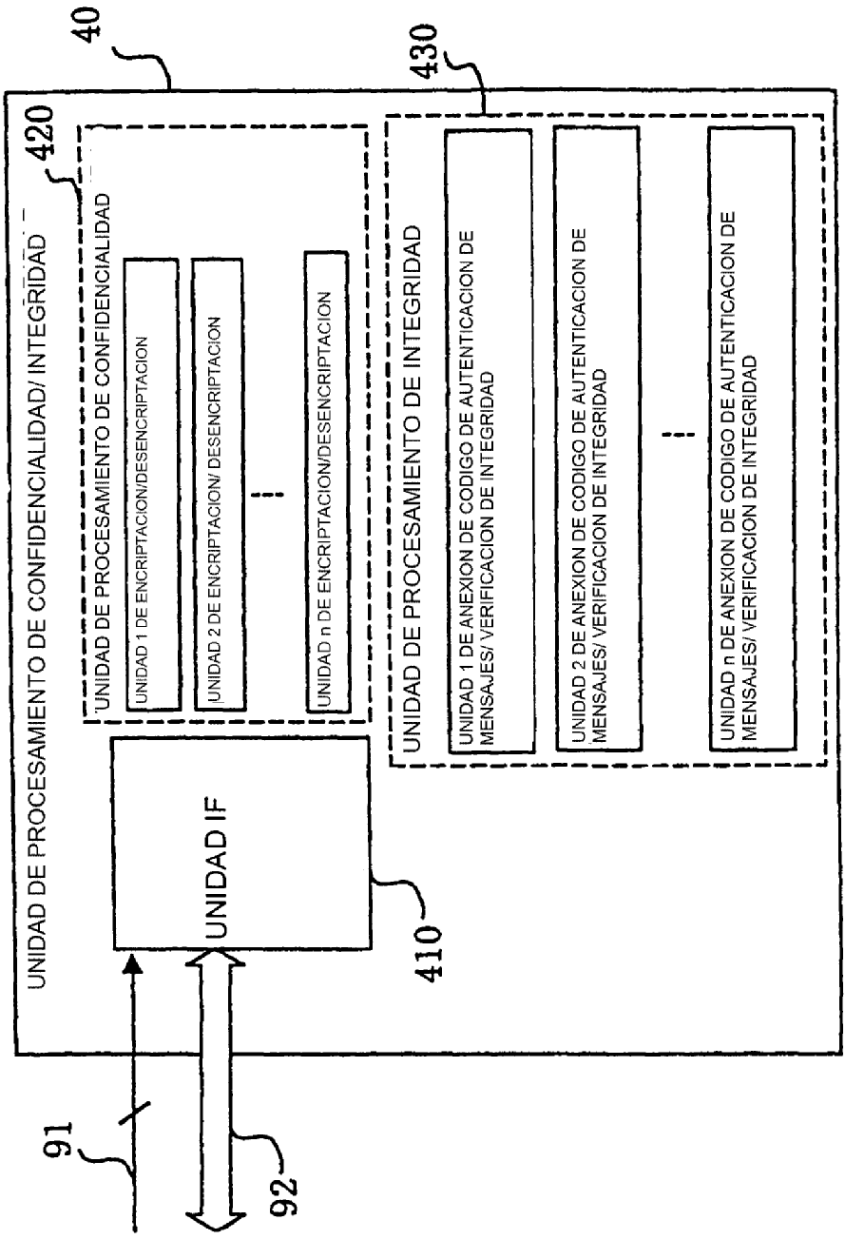

40
430
420
UNIDAD DE PROCESAMIENTO DE CONFIDENCIALIDAD/ INTEGRIDAD
UNIDAD DE PROCESAMIENTO DE CONFIDENCIALIDAD
UNIDAD 1 DE ENCRIPTACION/DESENCRIPTACION
UNIDAD 2 DE ENCRIPTACION/ DESENCRIPTACION
UNIDAD n DE ENCRIPTACION/DESENCRIPTACION
UNIDAD DE PROCESAMIENTO DE INTEGRIDAD
UNIDAD 1 DE ANEXION DE CODIGO DE AUTENTICACION DE MENSAJES/ VERIFICACION DE INTEGRIDAD
UNIDAD 2 DE ANEXION DE CODIGO DE AUTENTICACION DE MENSAJES/ VERIFICACION DE INTEGRIDAD
UNIDAD n DE ANEXION DE CODIGO DE AUTENTICACION DE MENSAJES/ VERIFICACION DE INTEGRIDAD
UNIDAD IF
410
91
92

Fig. 9

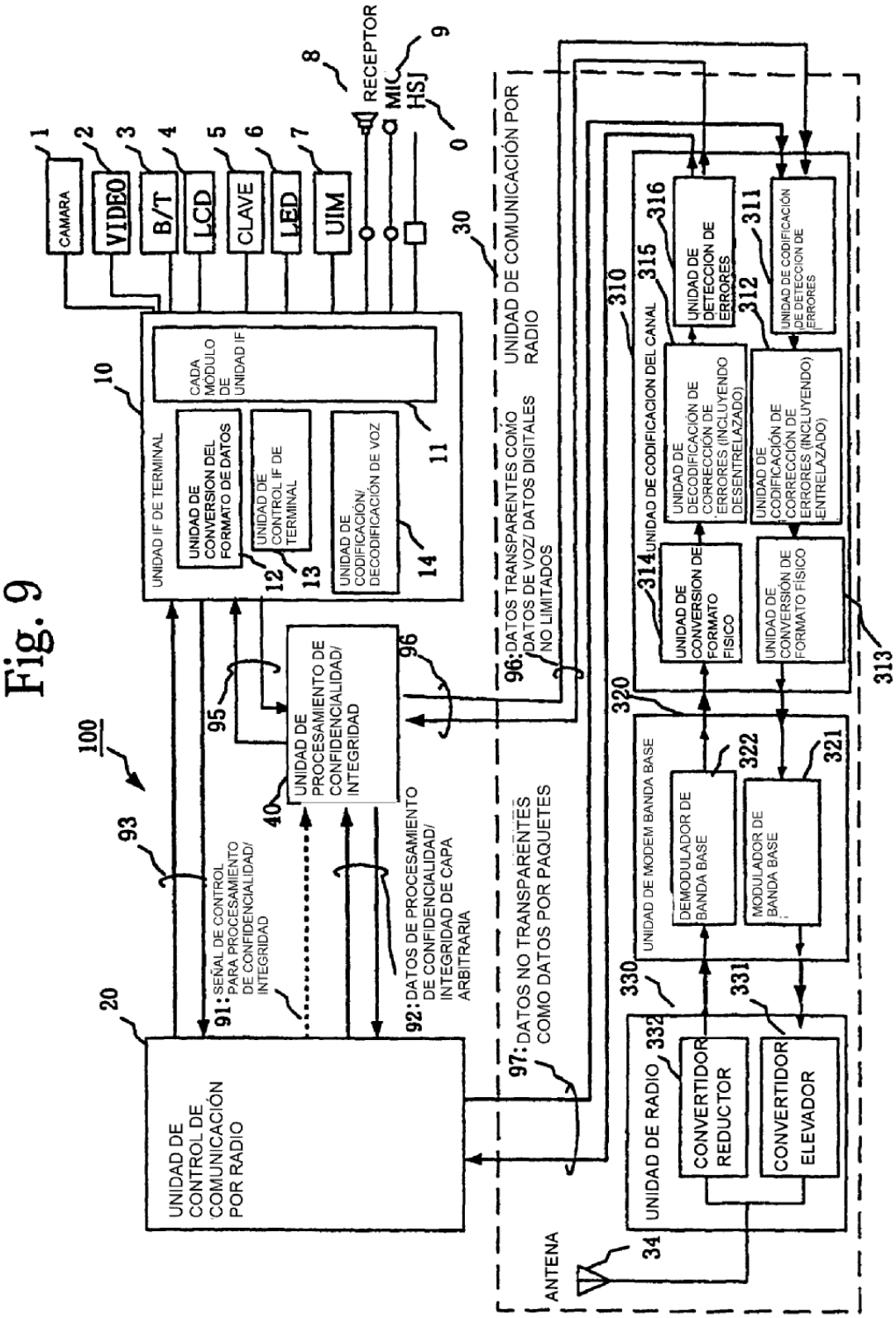

CAMARA
VIDEO
B/T
LCD
CLAVE
LED
UIM
RECEPTOR
MIC
HSJ
UNIDAD IF DE TERMINAL
CADA MODULO DE UNIDAD IF
UNIDAD DE CONVERSION DEL FORMATO DE DATOS
UNIDAD DE CONTROL IF DE TERMINAL
UNIDAD DE CODIFICACIÓN/ DECODIFICACIÓN DE VOZ
UNIDAD DE COMUNICACIÓN POR RADIO
DATOS TRANSPARENTES COMO DATOS DE VOZ/ DATOS DIGITALES NO LIMITADOS
UNIDAD DE PROCESAMIENTO DE CONFIDENCIALIDAD/ INTEGRIDAD
SEÑAL DE CONTROL PARA PROCESAMIENTO DE CONFIDENCIALIDAD/ INTEGRIDAD
DATOS DE PROCESAMIENTO DE CONFIDENCIALIDAD/ INTEGRIDAD DE CAPA ARBITRARIA
DATOS NO TRANSPARENTES COMO DATOS POR PAQUETES
UNIDAD DE CONTROL DE COMUNICACIÓN POR RADIO
UNIDAD DE CODIFICACION DEL CANAL
UNIDAD DE DETECCION DE ERRORES
UNIDAD DE CODIFICACIÓN DE DETECCION DE ERRORES
UNIDAD DE DECODIFICACIÓN DE CORRECCIÓN DE ERRORES (INCLUYENDO DESENTRELAZADO)
UNIDAD DE CODIFICACIÓN DE CORRECCIÓN DE ERRORES (INCLUYENDO ENTRELAZADO)
UNIDAD DE CONVERSION DE FORMATO FISICO
UNIDAD DE CONVERSIÓN DE FORMATO FÍSICO
UNIDAD DE MODEM BANDA BASE
DEMODULADOR DE BANDA BASE
MODULADOR DE BANDA BASE
UNIDAD DE RADIO
CONVERTIDOR REDUCTOR
CONVERTIDOR ELEVADOR
ANTENA

Fig. 10

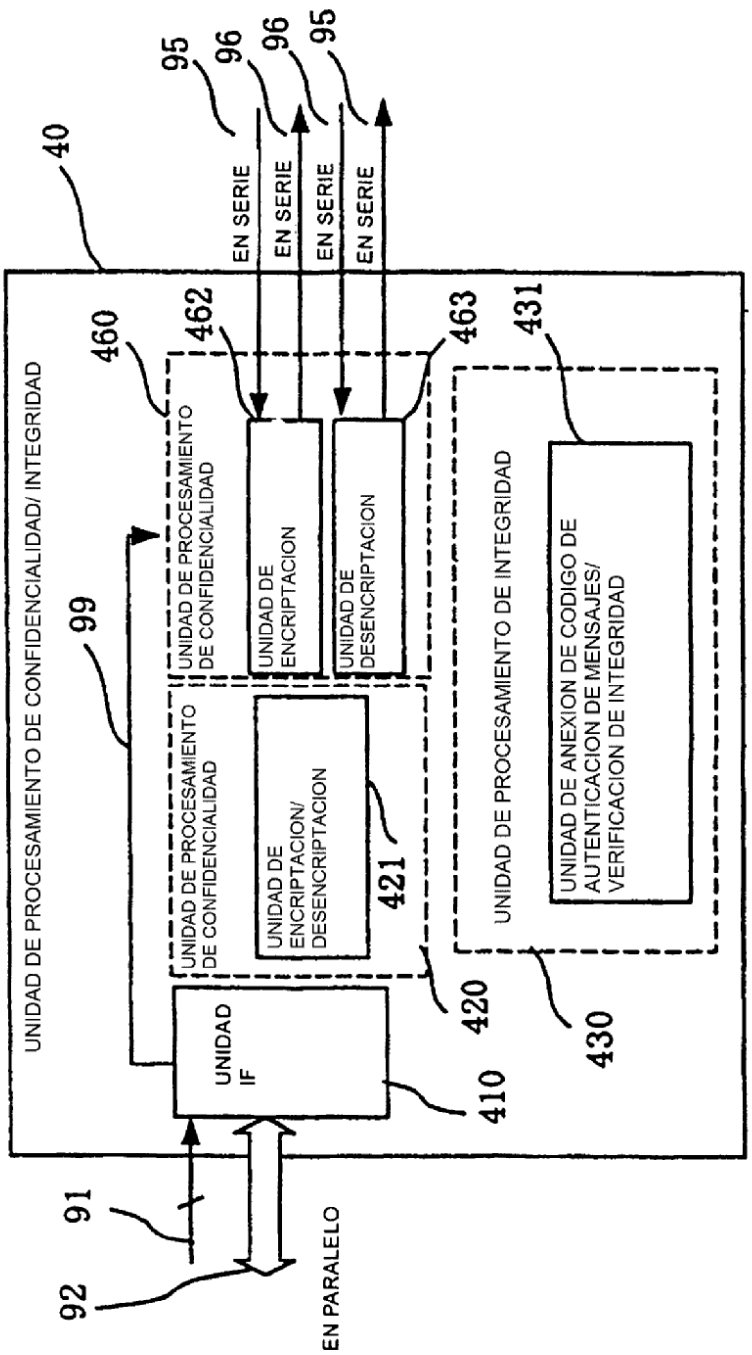

40
UNIDAD DE PROCESAMIENTO DE CONFIDENCIALIDAD/ INTEGRIDAD
95
96
96
95
EN SERIE
EN SERIE
EN SERIE
EN SERIE
460
462
463
431
UNIDAD DE PROCESAMIENTO DE CONFIDENCIALIDAD
UNIDAD DE ENCRIPTACION
UNIDAD DE DESENCRIPTACION
UNIDAD DE PROCESAMIENTO DE INTEGRIDAD
UNIDAD DE ANEXION DE CODIGO DE AUTENTICACION DE MENSAJES/ VERIFICACION DE INTEGRIDAD
99
UNIDAD DE PROCESAMIENTO DE CONFIDENCIALIDAD
UNIDAD DE ENCRIPTACION/ DESENCRIPTACION
421
420
430
UNIDAD IF
410
91
92
EN PARALELO

Fig. 11

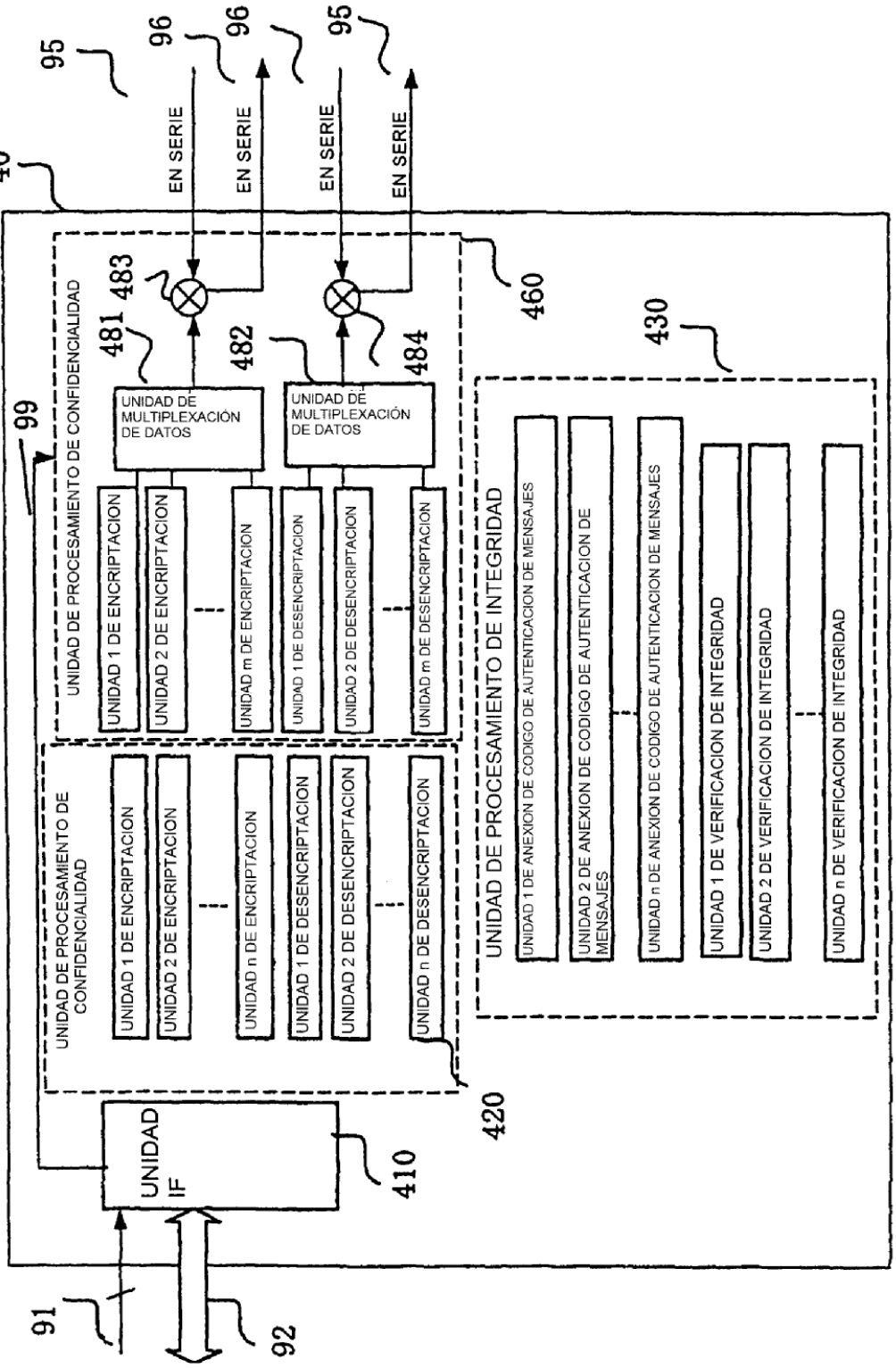

40
95
96
96
95
EN SERIE
EN SERIE
EN SERIE
EN SERIE
460
430
483
481
482
484
99
UNIDAD DE PROCESAMIENTO DE CONFIDENCIALIDAD
UNIDAD DE MULTIPLEXACIÓN DE DATOS
UNIDAD DE MULTIPLEXACIÓN DE DATOS
UNIDAD 1 DE ENCRIPTACION
UNIDAD 2 DE ENCRIPTACION
UNIDAD m DE ENCRIPTACION
UNIDAD 1 DE DESENCRIPTACION
UNIDAD 2 DE DESENCRIPTACION
UNIDAD m DE DESENCRIPTACION
UNIDAD DE PROCESAMIENTO DE CONFIDENCIALIDAD
UNIDAD 1 DE ENCRIPTACION
UNIDAD 2 DE ENCRIPTACION
UNIDAD n DE ENCRIPTACION
UNIDAD 1 DE DESENCRIPTACION
UNIDAD 2 DE DESENCRIPTACION
UNIDAD n DE DESENCRIPTACION
UNIDAD DE PROCESAMIENTO DE INTEGRIDAD
UNIDAD 1 DE ANEXION DE CODIGO DE AUTENTICACION DE MENSAJES
UNIDAD 2 DE ANEXION DE CODIGO DE AUTENTICACION DE MENSAJES
UNIDAD n DE ANEXION DE CODIGO DE AUTENTICACION DE MENSAJES
UNIDAD 1 DE VERIFICACION DE INTEGRIDAD
UNIDAD 2 DE VERIFICACION DE INTEGRIDAD
UNIDAD n DE VERIFICACION DE INTEGRIDAD
420
UNIDAD IF
410
91
92

Fig. 12

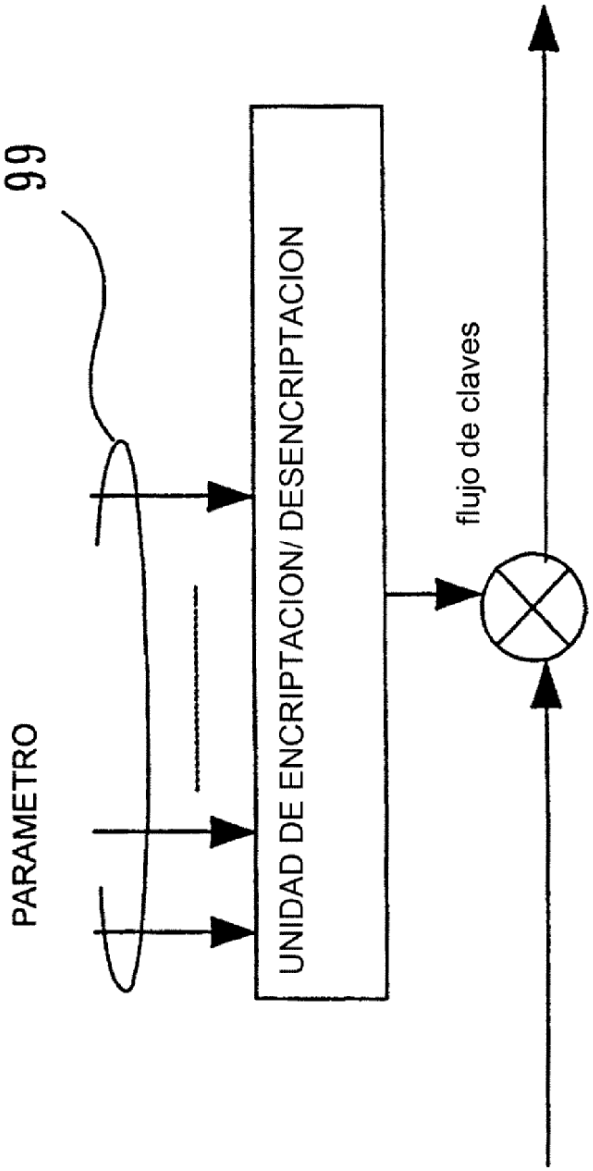

99
PARAMETRO
UNIDAD DE ENCRIPTACION/ DESENCRIPTACION
flujo de claves

Fig.13

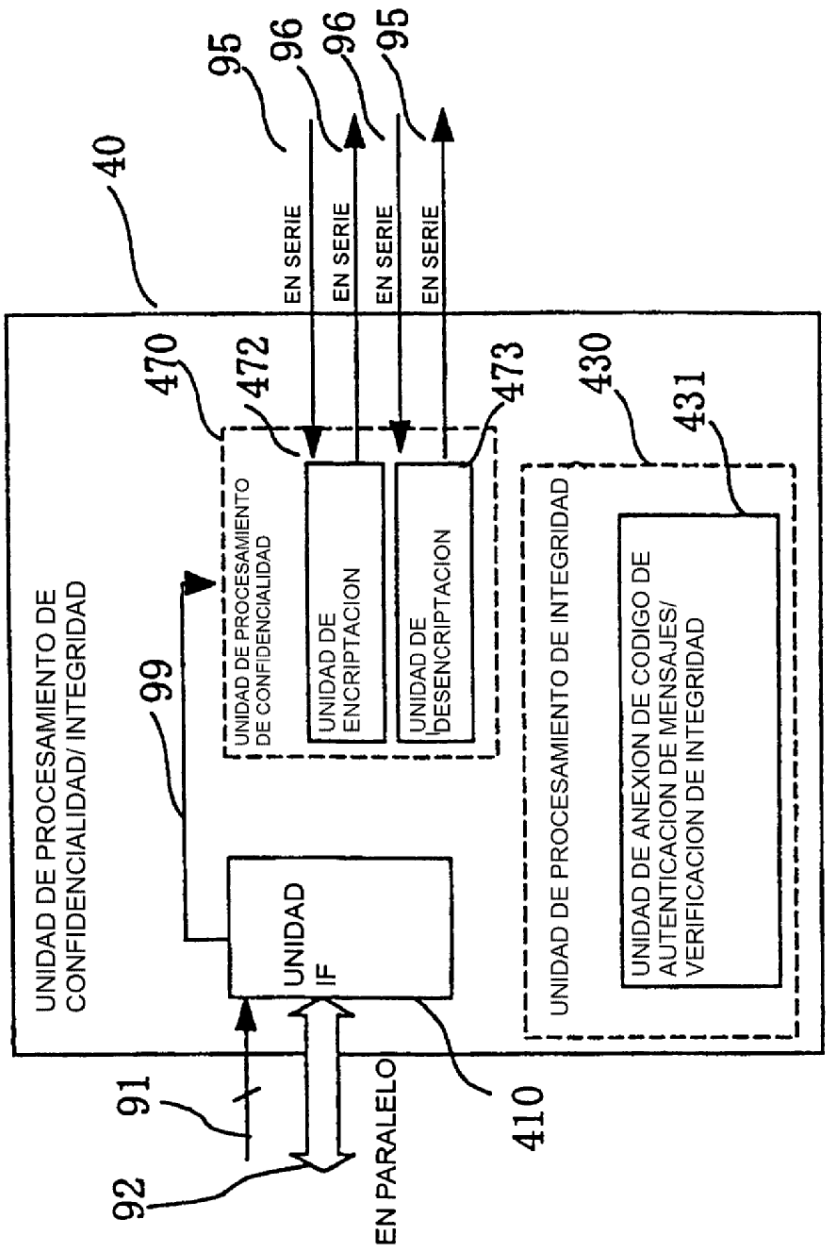

40
95
96
96
95
EN SERIE
EN SERIE
EN SERIE
EN SERIE
470
472
473
430
431
UNIDAD DE PROCESAMIENTO DE CONFIDENCIALIDAD/ INTEGRIDAD
UNIDAD DE PROCESAMIENTO DE CONFIDENCIALIDAD
UNIDAD DE ENCRIPTACION
UNIDAD DE DESENCRIPTACION
UNIDAD DE PROCESAMIENTO DE INTEGRIDAD
UNIDAD DE ANEXION DE CODIGO DE AUTENTICACION DE MENSAJES/ VERIFICACION DE INTEGRIDAD
99
UNIDAD IF
91
92
EN PARALELO
410

Fig. 14

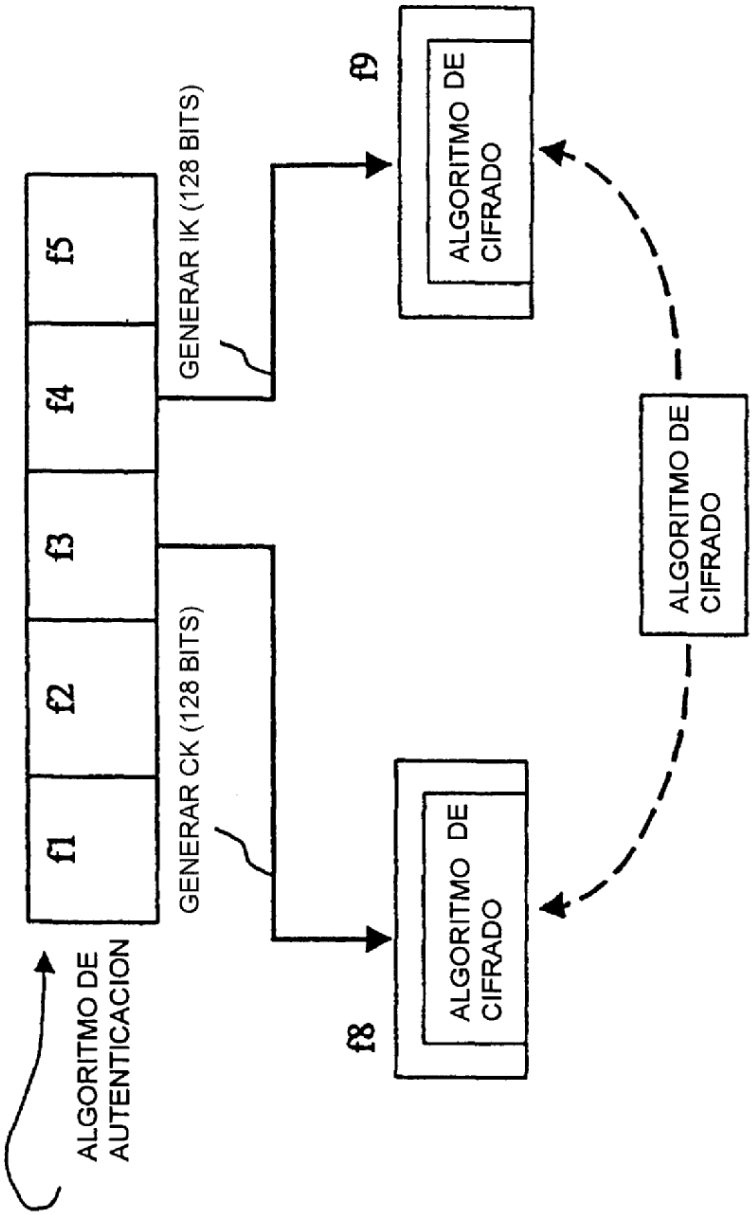

f1
f2
f3
f4
f5
ALGORITMO DE AUTENTICACION
GENERAR CK (128 BITS)
GENERAR IK (128 BITS)
f8
f9
ALGORITMO DE CIFRADO
ALGORITMO DE CIFRADO
ALGORITMO DE CIFRADO

Fig. 15

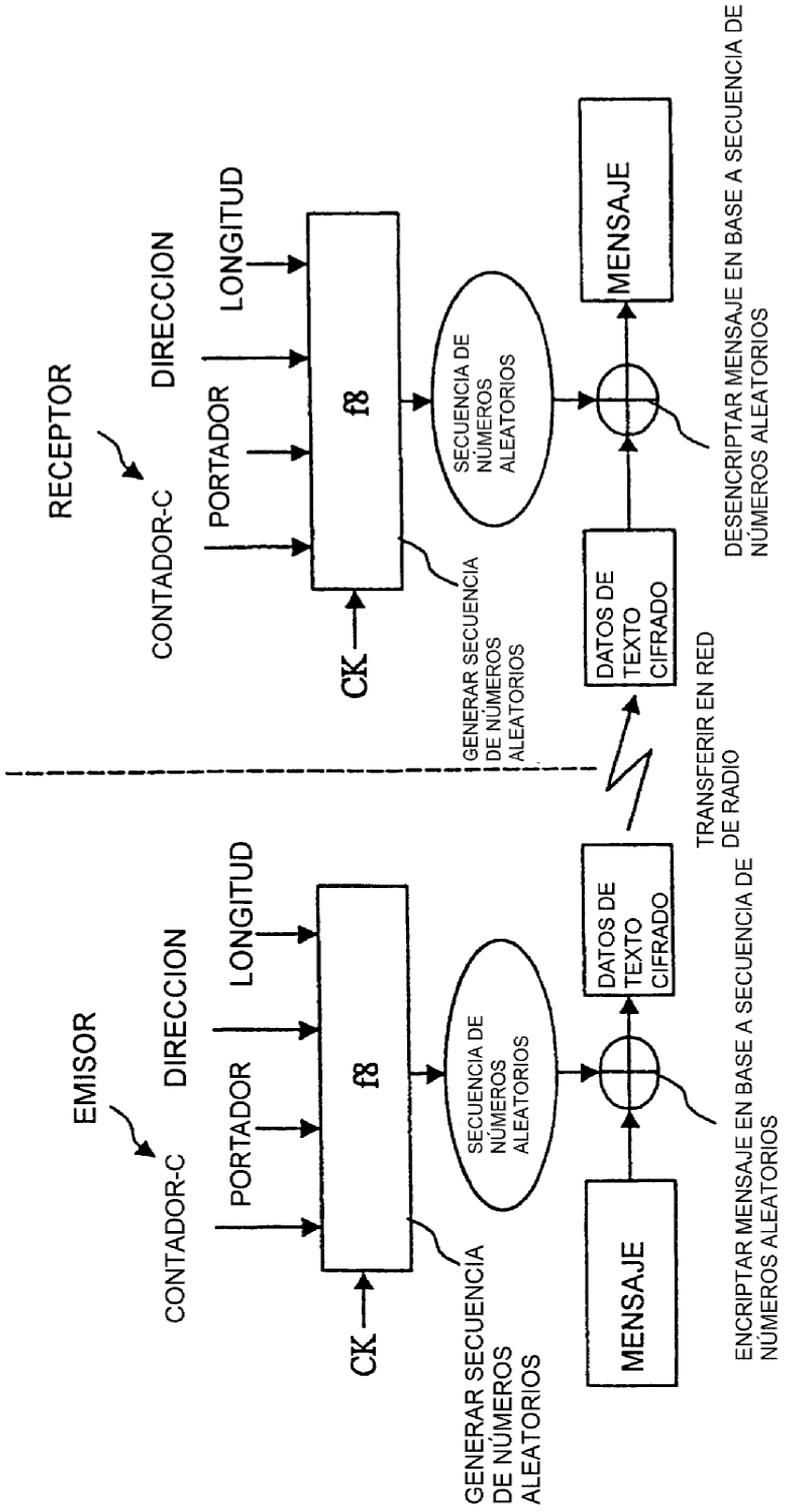

EMISOR
CONTADOR-C
DIRECCION
LONGITUD
PORTADOR
f8
CK
GENERAR SECUENCIA DE NÚMEROS ALEATORIOS
SECUENCIA DE NÚMEROS ALEATORIOS
DATOS DE TEXTO CIFRADO
MENSAJE
ENCRIPTAR MENSAJE EN BASE A SECUENCIA DE NÚMEROS ALEATORIOS
TRANSFERIR EN RED DE RADIO
RECEPTOR
CONTADOR-C
DIRECCION
LONGITUD
PORTADOR
f8
CK
GENERAR SECUENCIA DE NÚMEROS ALEATORIOS
SECUENCIA DE NÚMEROS ALEATORIOS
DATOS DE TEXTO CIFRADO
MENSAJE
DESENCRIPTAR MENSAJE EN BASE A SECUENCIA DE NÚMEROS ALEATORIOS

Fig. 16

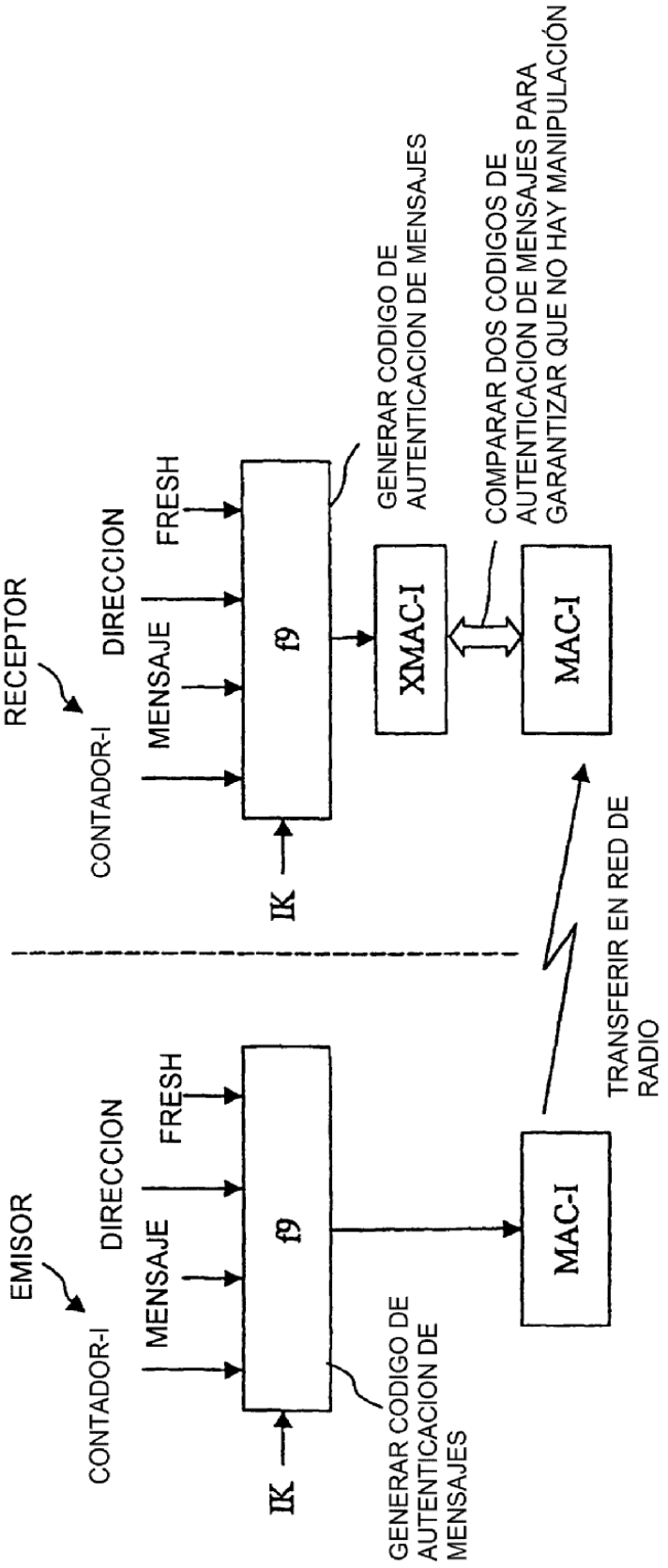

EMISOR
CONTADOR-I
DIRECCION
MENSAJE
FRESH
IK
f9
GENERAR CODIGO DE AUTENTICACION DE MENSAJES
MAC-I
TRANSFERIR EN RED DE RADIO
RECEPTOR
CONTADOR-I
DIRECCION
MENSAJE
FRESH
IK
f9
GENERAR CODIGO DE AUTENTICACION DE MENSAJES
XMAC-I
COMPARAR DOS CODIGOS DE AUTENTICACION DE MENSAJES PARA GARANTIZAR QUE NO HAY MANIPULACIÓN
MAC-I

Fig. 17

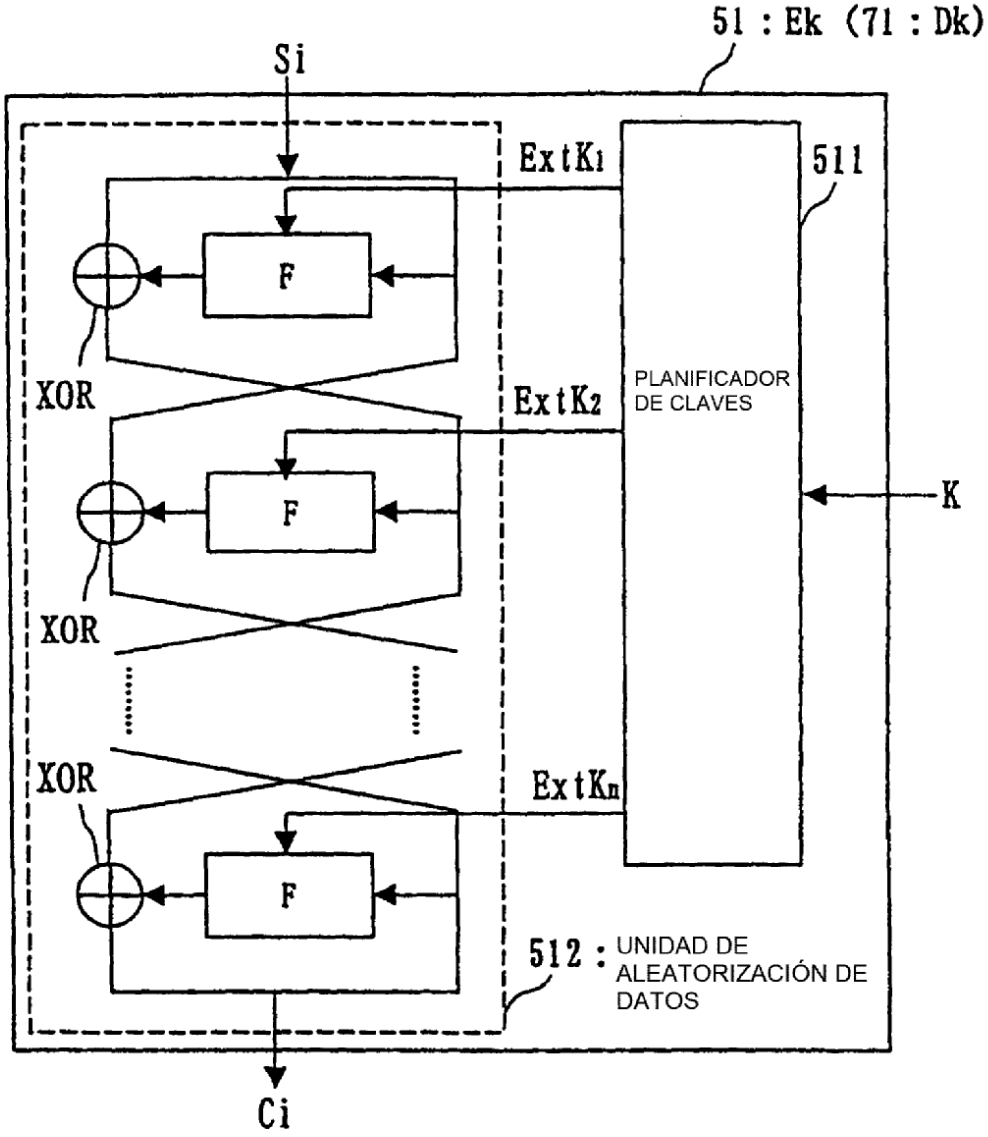

51 : Ek (71 : Dk)
Si
ExtK1
511
F
XOR
ExtK2
PLANIFICADOR DE CLAVES
K
F
XOR
XOR
ExtKn
F
512 : UNIDAD DE ALEATORIZACIÓN DE DATOS
Ci

Fig. 18

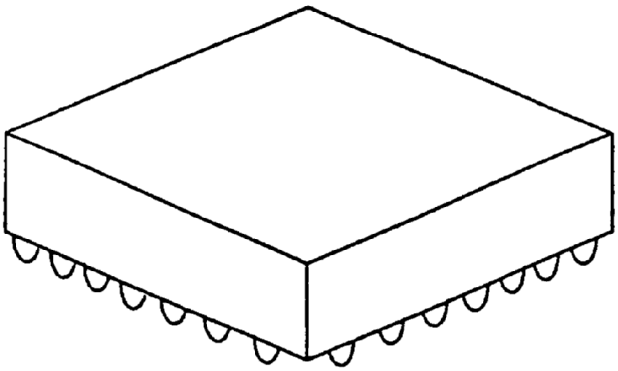


Fig. 19

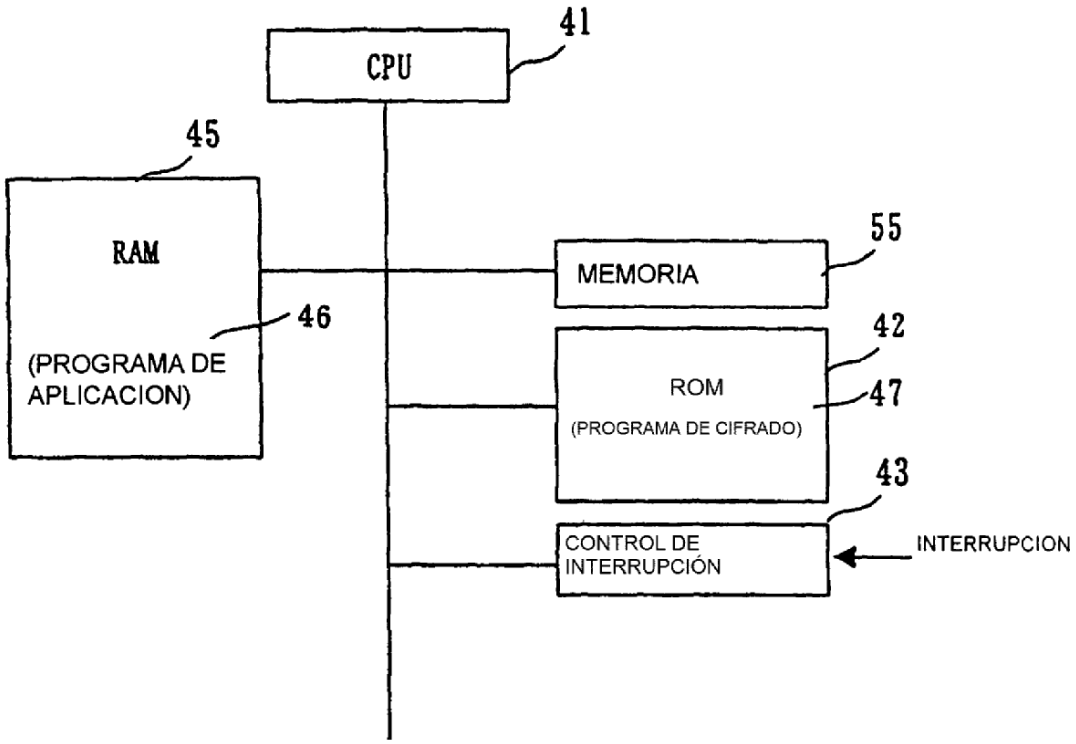

41
CPU
45
RAM
(PROGRAMA DE APLICACION)
46
55
MEMORIA
42
ROM
(PROGRAMA DE CIFRADO)
47
43
CONTROL DE INTERRUPCIÓN
INTERRUPCION

Fig. 20

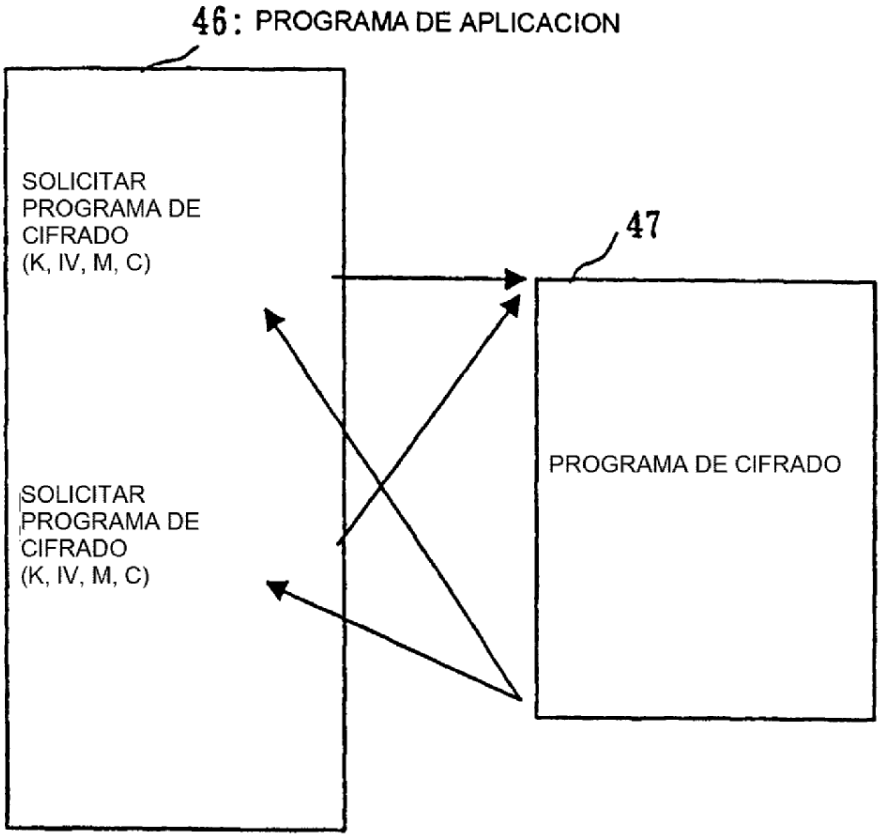

46: PROGRAMA DE APLICACION
SOLICITAR PROGRAMA DE CIFRADO (K, IV, M, C)
SOLICITAR PROGRAMA DE CIFRADO (K, IV, M, C)
47
PROGRAMA DE CIFRADO

Fig. 21

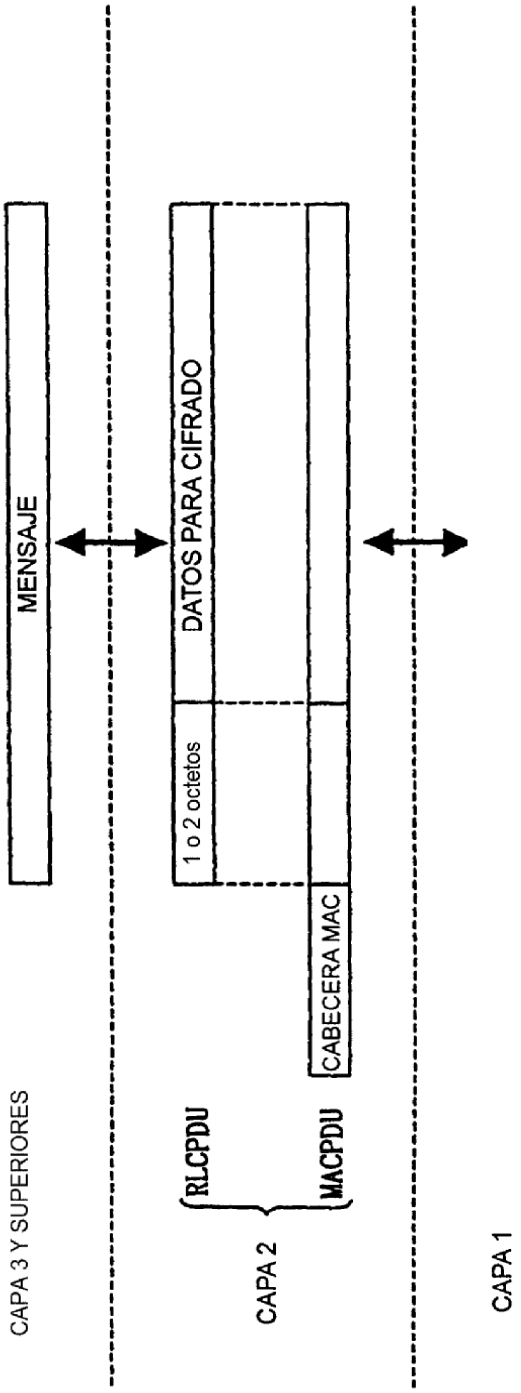

MENSAJE
DATOS PARA CIFRADO
1 o 2 octetos
CABECERA MAC
RLCPDU
MACPDU
CAPA 3 Y SUPERIORES
CAPA 2
CAPA 1

Fig. 22

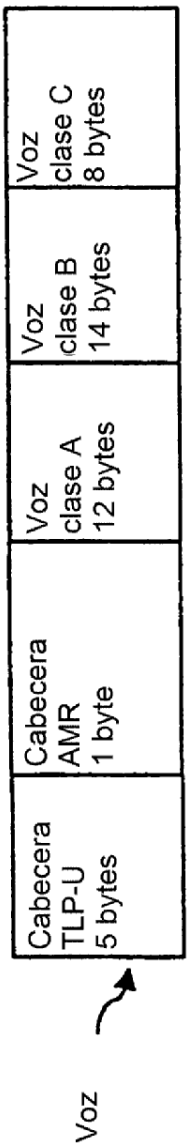

Cabecera TLP-U 5 bytes
Cabecera AMR 1 byte
Voz clase A 12 bytes
Voz clase B 14 bytes
Voz clase C 8 bytes
Voz

Fig. 23

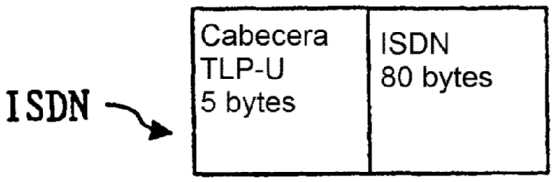


Fig. 24

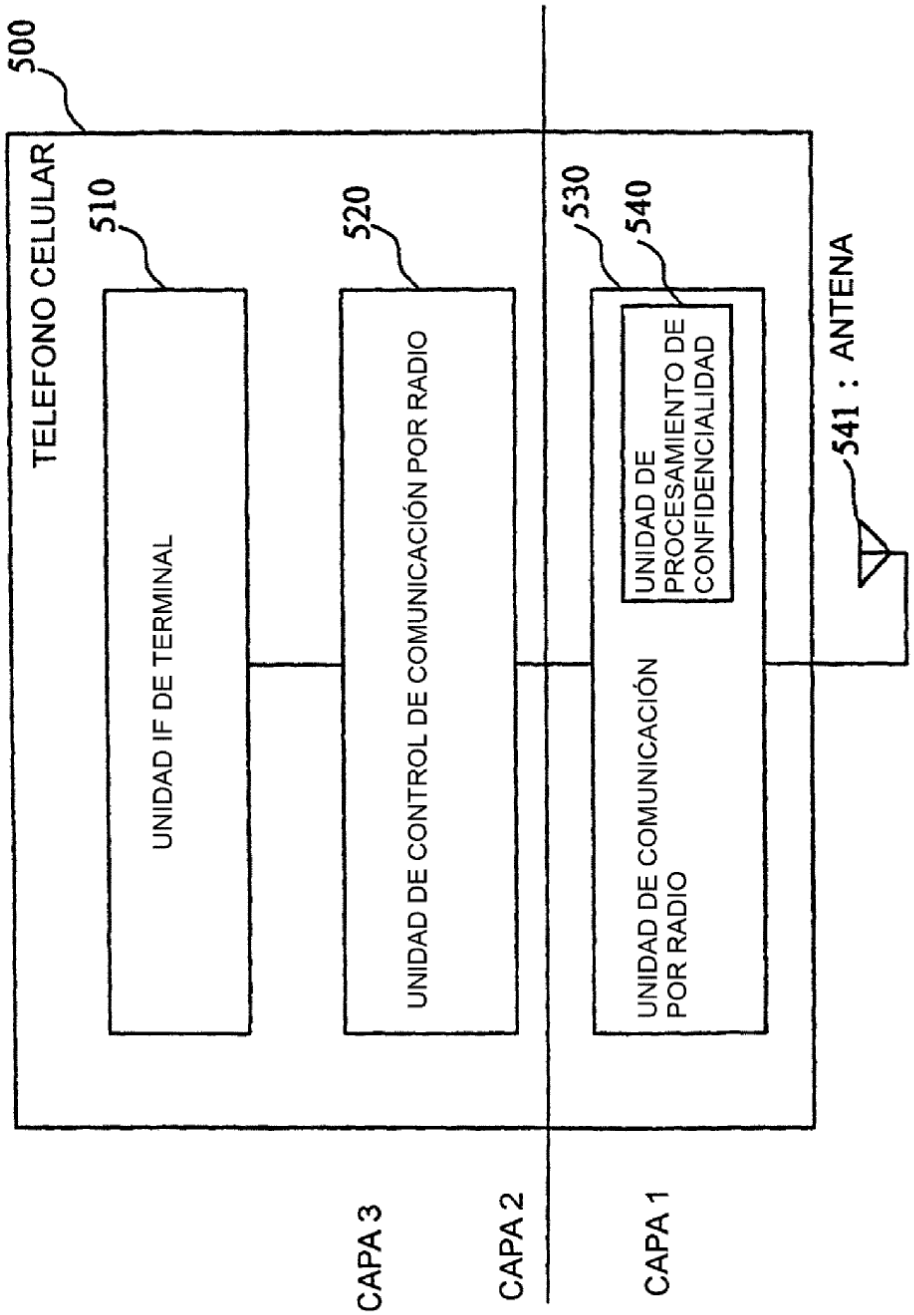

500
TELEFONO CELULAR
510
UNIDAD IF DE TERMINAL
520
UNIDAD DE CONTROL DE COMUNICACIÓN POR RADIO
530
UNIDAD DE COMUNICACIÓN POR RADIO
540
UNIDAD DE PROCESAMIENTO DE CONFIDENCIALIDAD
541 : ANTENA
CAPA 3
CAPA 2
CAPA 1

Fig. 25

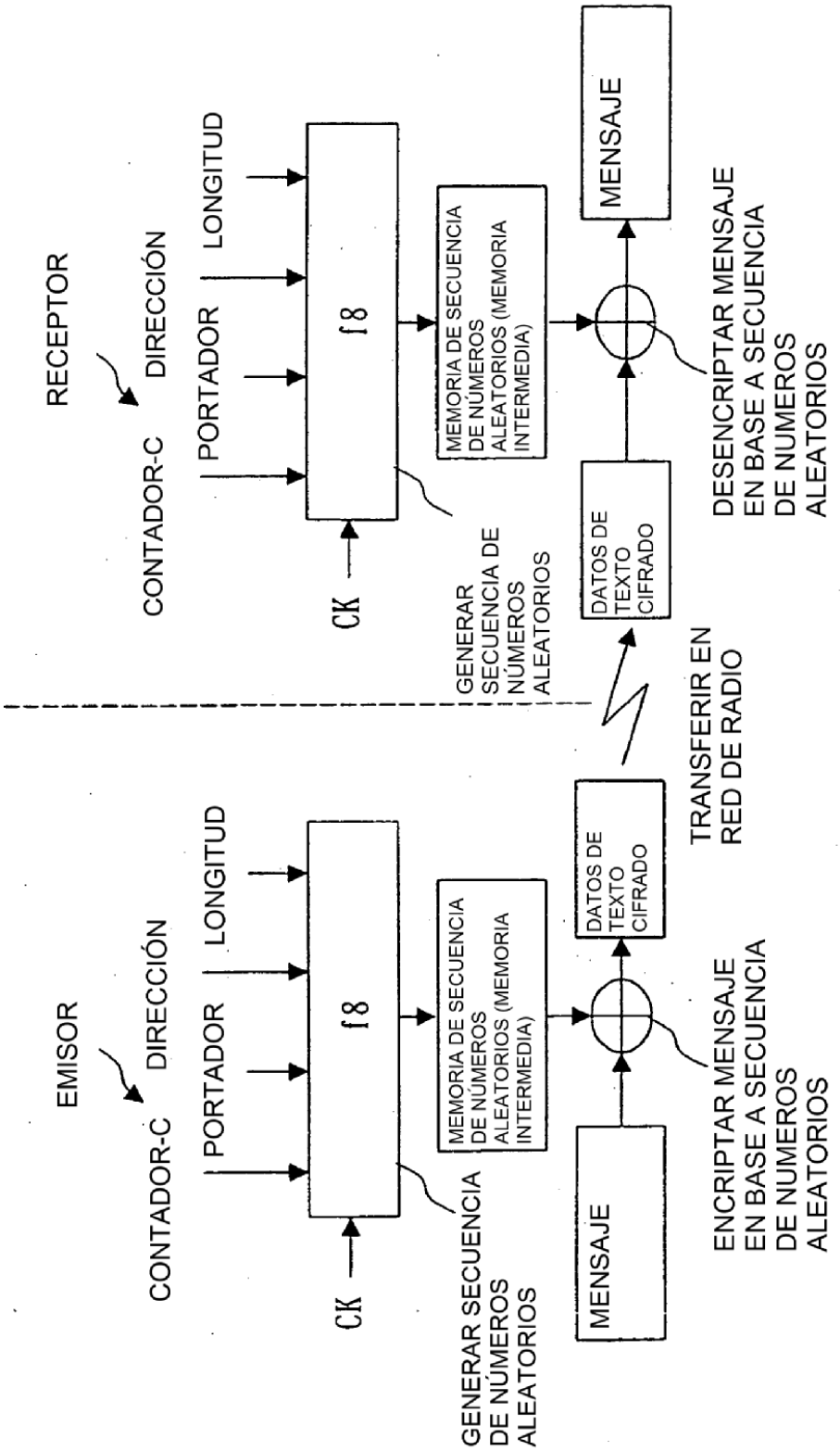

EMISOR
CONTADOR-C
DIRECCIÓN
PORTADOR
LONGITUD
CK
f8
GENERAR SECUENCIA DE NÚMEROS ALEATORIOS
MEMORIA DE SECUENCIA DE NÚMEROS ALEATORIOS (MEMORIA INTERMEDIA)
MENSAJE
ENCRIPTAR MENSAJE EN BASE A SECUENCIA DE NUMEROS ALEATORIOS
DATOS DE TEXTO CIFRADO
TRANSFERIR EN RED DE RADIO
RECEPTOR
CONTADOR-C
DIRECCIÓN
PORTADOR
LONGITUD
CK
f8
GENERAR SECUENCIA DE NÚMEROS ALEATORIOS
MEMORIA DE SECUENCIA DE NÚMEROS ALEATORIOS (MEMORIA INTERMEDIA)
DATOS DE TEXTO CIFRADO
DESENCRIPTAR MENSAJE EN BASE A SECUENCIA DE NUMEROS ALEATORIOS
MENSAJE

Fig. 26

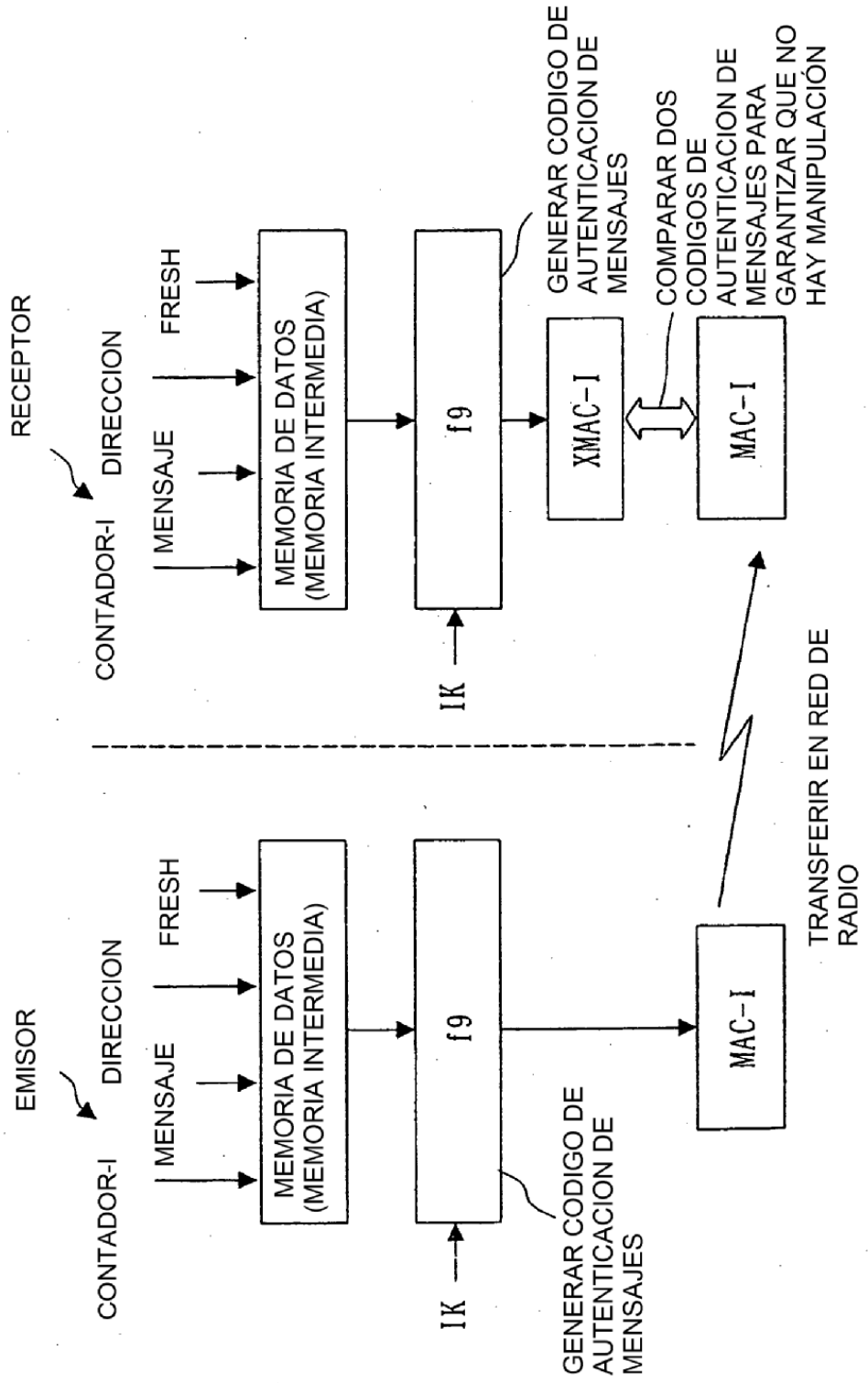

EMISOR
RECEPTOR
CONTADOR-I
DIRECCION
MENSAJE
FRESH
MEMORIA DE DATOS (MEMORIA INTERMEDIA)
f9
IK
GENERAR CODIGO DE AUTENTICACION DE MENSAJES
MAC-I
XMAC-I
COMPARAR DOS CODIGOS DE AUTENTICACION DE MENSAJES PARA GARANTIZAR QUE NO HAY MANIPULACIÓN
TRANSFERIR EN RED DE RADIO

Fig. 27

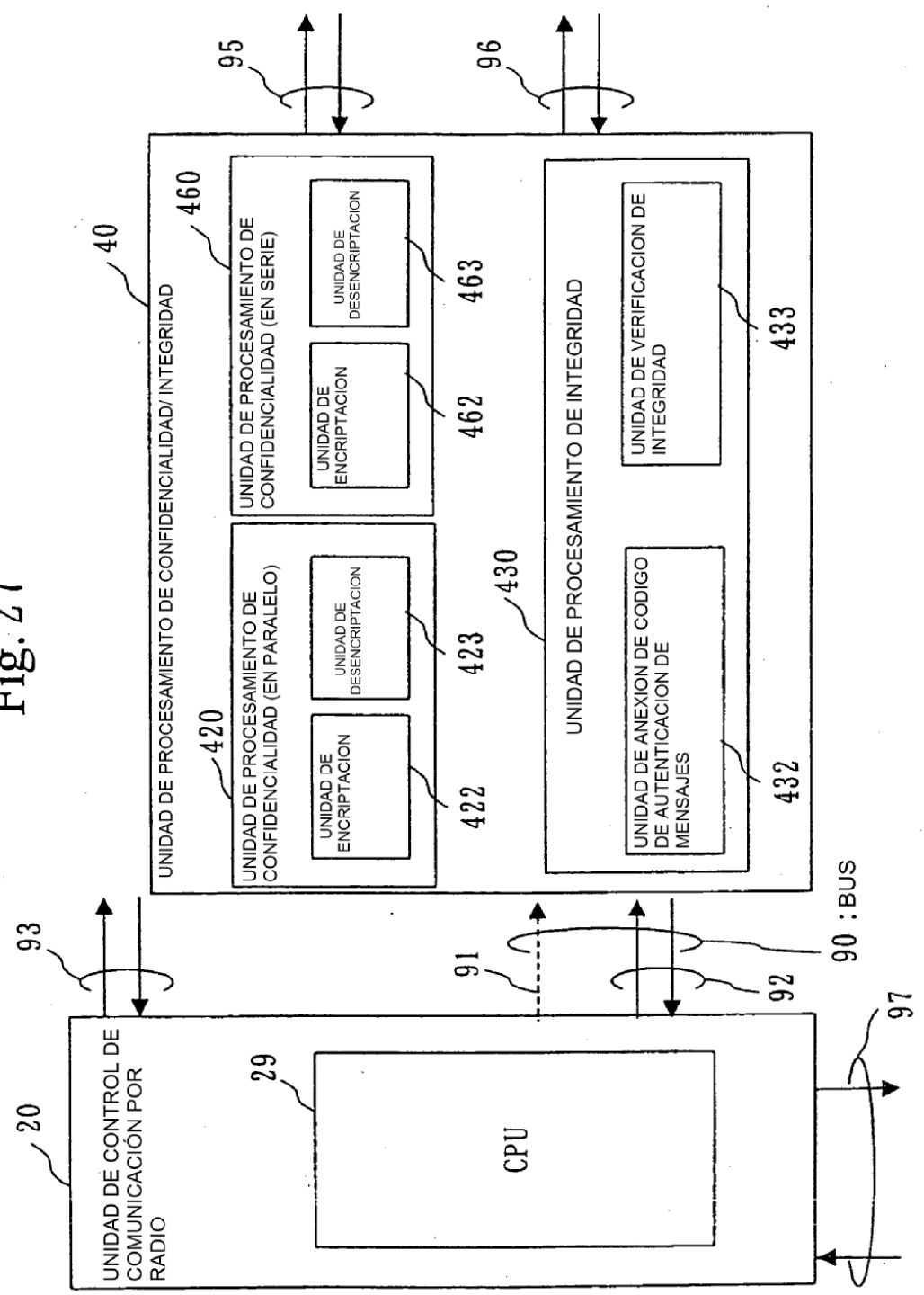

UNIDAD DE CONTROL DE COMUNICACIÓN POR RADIO
20
CPU
29
93
91
92
90 : BUS
97
95
96
40
UNIDAD DE PROCESAMIENTO DE CONFIDENCIALIDAD/ INTEGRIDAD
UNIDAD DE PROCESAMIENTO DE CONFIDENCIALIDAD (EN PARALELO)
420
UNIDAD DE ENCRIPTACION
422
UNIDAD DE DESENCRIPTACION
423
UNIDAD DE PROCESAMIENTO DE CONFIDENCIALIDAD (EN SERIE)
460
UNIDAD DE ENCRIPTACION
462
UNIDAD DE DESENCRIPTACION
463
UNIDAD DE PROCESAMIENTO DE INTEGRIDAD
430
UNIDAD DE ANEXION DE CODIGO DE AUTENTICACION DE MENSAJES
432
UNIDAD DE VERIFICACION DE INTEGRIDAD
433

Fig. 28

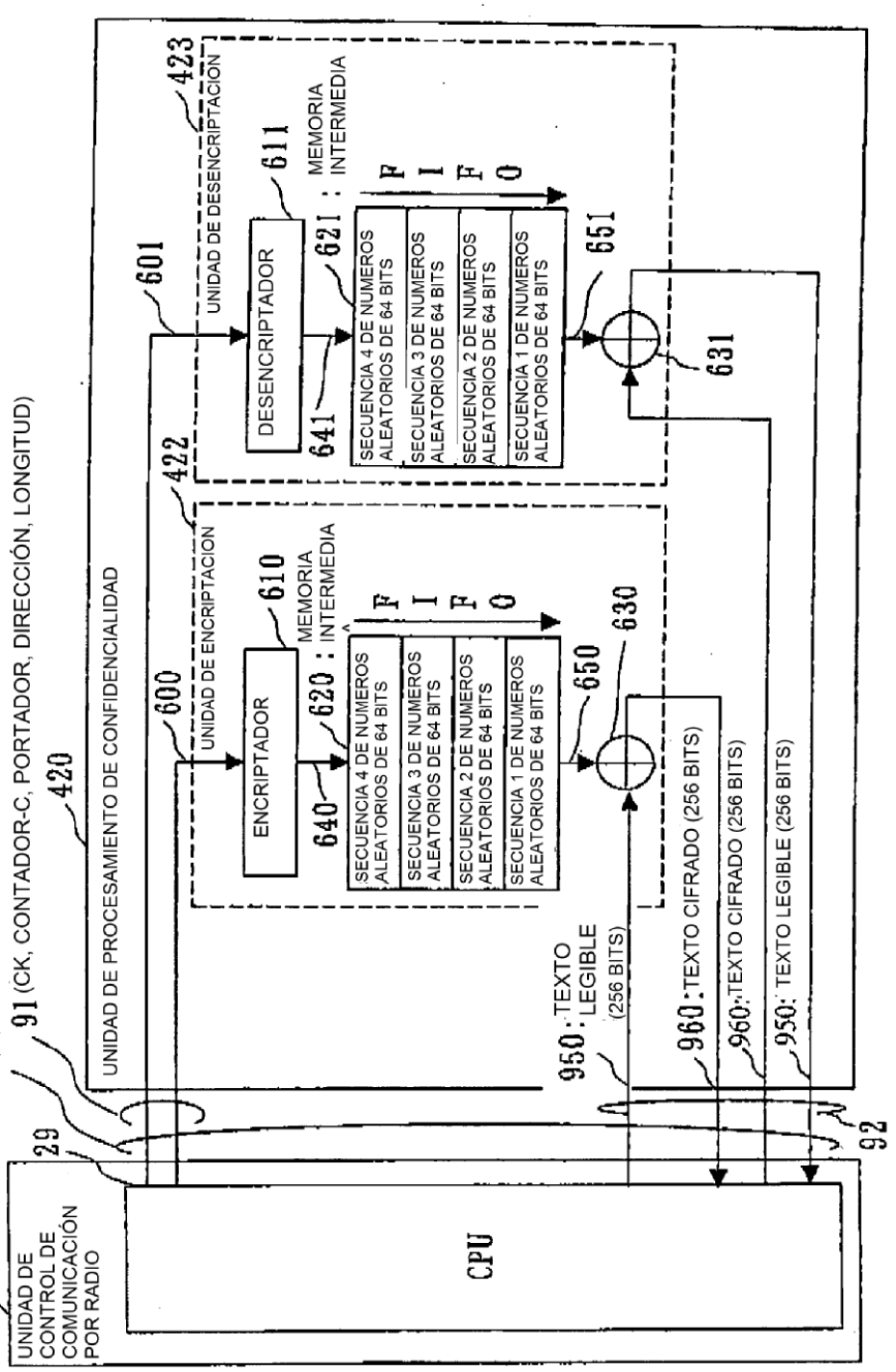

40
UNIDAD DE CONTROL DE COMUNICACIÓN POR RADIO
29
CPU
90 : BUS
91 (CK, CONTADOR-C, PORTADOR, DIRECCIÓN, LONGITUD)
420
UNIDAD DE PROCESAMIENTO DE CONFIDENCIALIDAD
600
UNIDAD DE ENCRIPTACION
ENCRIPTADOR
610
MEMORIA INTERMEDIA
620 :
640
SECUENCIA 4 DE NUMEROS ALEATORIOS DE 64 BITS
SECUENCIA 3 DE NUMEROS ALEATORIOS DE 64 BITS
SECUENCIA 2 DE NUMEROS ALEATORIOS DE 64 BITS
SECUENCIA 1 DE NUMEROS ALEATORIOS DE 64 BITS
FIFO
650
630
422
601
423
UNIDAD DE DESENCRIPTACIÓN
DESENCRIPTADOR
611
MEMORIA INTERMEDIA
621 :
641
SECUENCIA 4 DE NUMEROS ALEATORIOS DE 64 BITS
SECUENCIA 3 DE NUMEROS ALEATORIOS DE 64 BITS
SECUENCIA 2 DE NUMEROS ALEATORIOS DE 64 BITS
SECUENCIA 1 DE NUMEROS ALEATORIOS DE 64 BITS
FIFO
651
631
950 : TEXTO LEGIBLE (256 BITS)
960 : TEXTO CIFRADO (256 BITS)
960 : TEXTO CIFRADO (256 BITS)
950 : TEXTO LEGIBLE (256 BITS)
92

Fig. 29

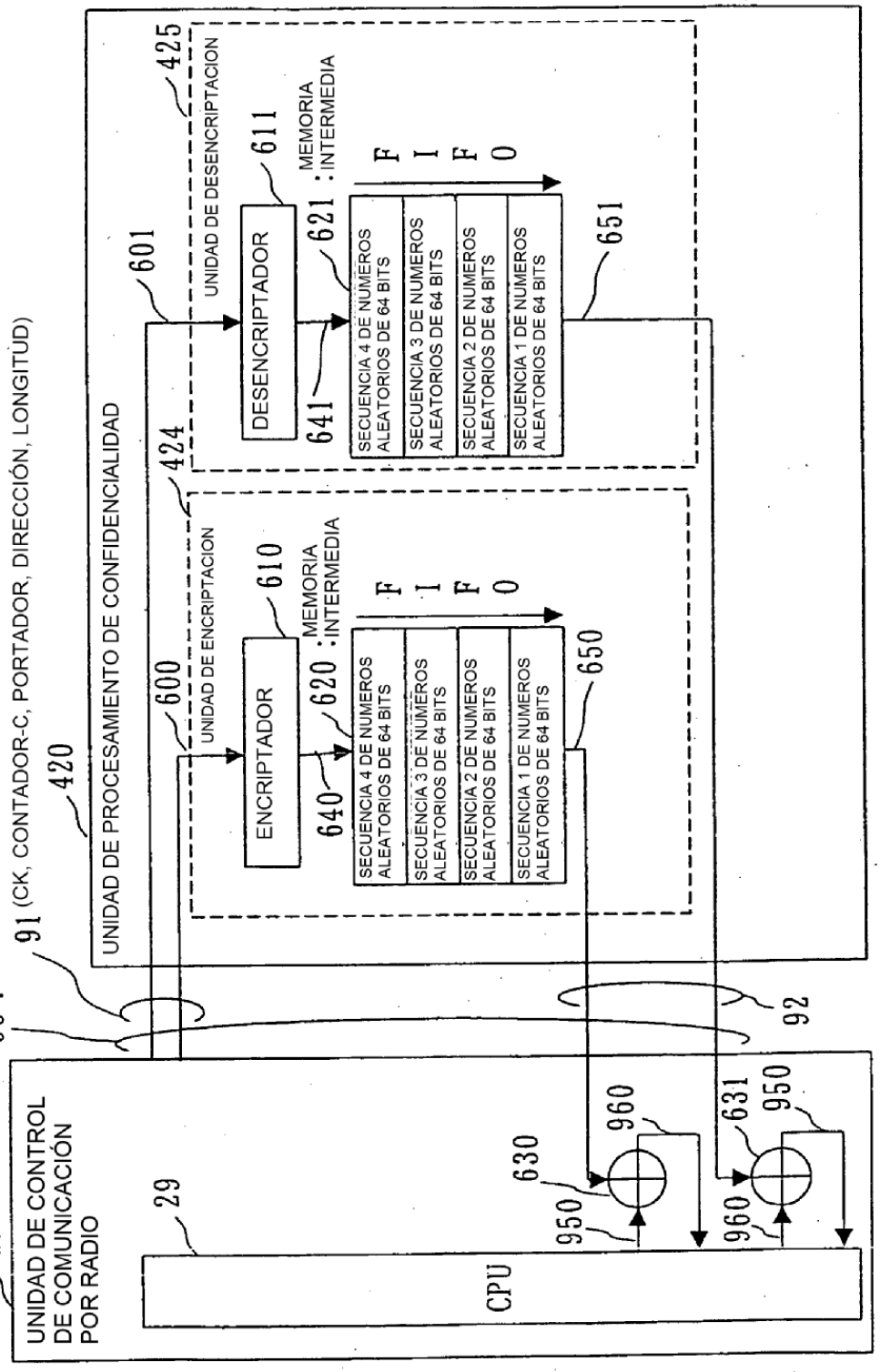

UNIDAD DE CONTROL DE COMUNICACIÓN POR RADIO
40
CPU
29
90 :BUS
91 (CK, CONTADOR-C, PORTADOR, DIRECCIÓN, LONGITUD)
92
UNIDAD DE PROCESAMIENTO DE CONFIDENCIALIDAD
420
UNIDAD DE ENCRIPTACION
600
ENCRIPTADOR
610
640
620 :MEMORIA INTERMEDIA
SECUENCIA 4 DE NUMEROS ALEATORIOS DE 64 BITS
SECUENCIA 3 DE NUMEROS ALEATORIOS DE 64 BITS
SECUENCIA 2 DE NUMEROS ALEATORIOS DE 64 BITS
SECUENCIA 1 DE NUMEROS ALEATORIOS DE 64 BITS
FIFO
650
424
UNIDAD DE DESENCRIPTACION
601
DESENCRIPTADOR
611
641
621 :MEMORIA INTERMEDIA
SECUENCIA 4 DE NUMEROS ALEATORIOS DE 64 BITS
SECUENCIA 3 DE NUMEROS ALEATORIOS DE 64 BITS
SECUENCIA 2 DE NUMEROS ALEATORIOS DE 64 BITS
SECUENCIA 1 DE NUMEROS ALEATORIOS DE 64 BITS
FIFO
651
425
630
631
950
960

Fig.30

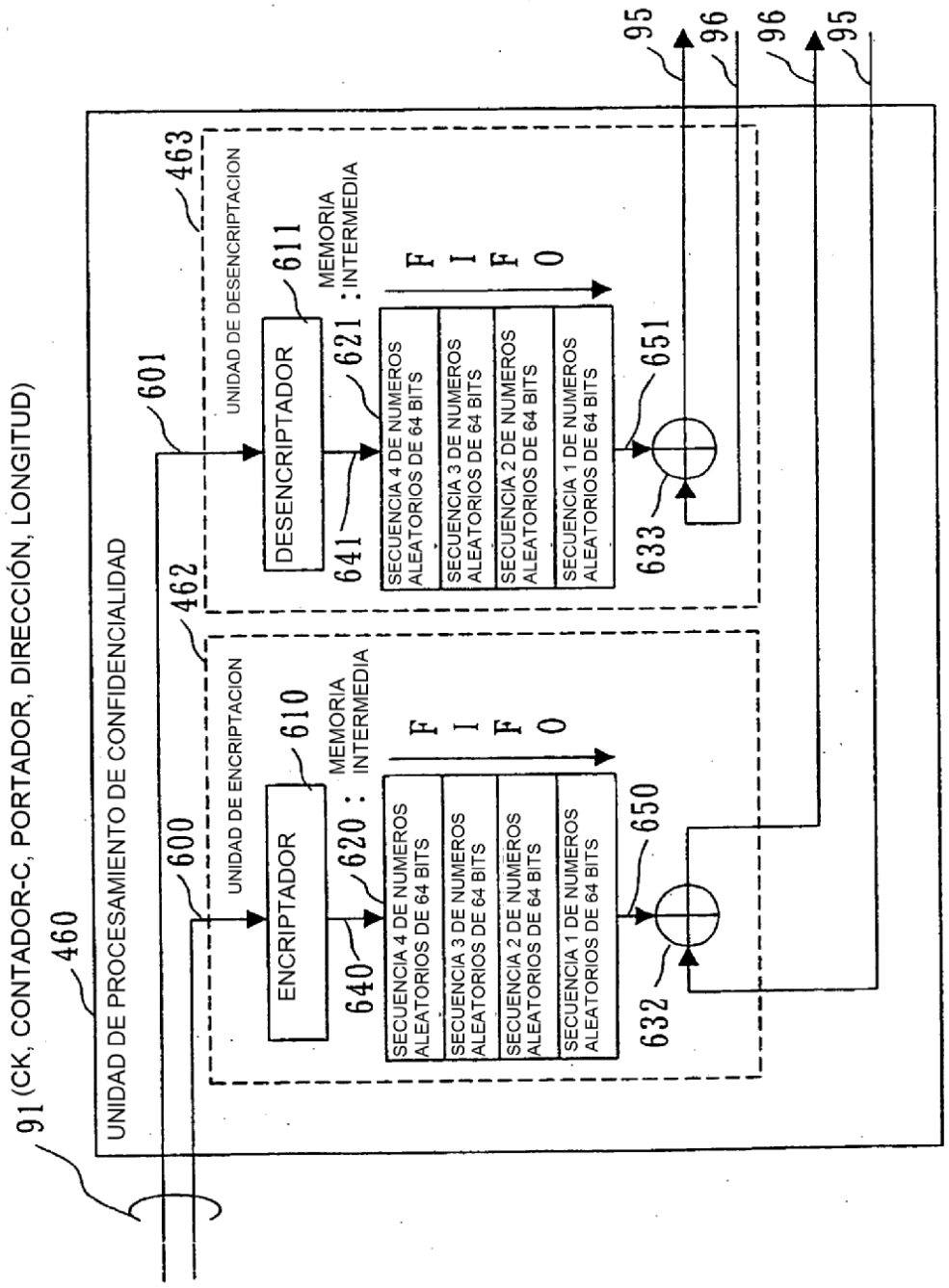

91 (CK, CONTADOR-C, PORTADOR, DIRECCIÓN, LONGITUD)
460
UNIDAD DE PROCESAMIENTO DE CONFIDENCIALIDAD
600
UNIDAD DE ENCRIPTACION
ENCRIPTADOR
610
640
620 : MEMORIA INTERMEDIA
SECUENCIA 4 DE NUMEROS ALEATORIOS DE 64 BITS
SECUENCIA 3 DE NUMEROS ALEATORIOS DE 64 BITS
SECUENCIA 2 DE NUMEROS ALEATORIOS DE 64 BITS
SECUENCIA 1 DE NUMEROS ALEATORIOS DE 64 BITS
FIFO
632
650
462
601
UNIDAD DE DESENCRIPTACION
DESENCRIPTADOR
611
641
621 : MEMORIA INTERMEDIA
SECUENCIA 4 DE NUMEROS ALEATORIOS DE 64 BITS
SECUENCIA 3 DE NUMEROS ALEATORIOS DE 64 BITS
SECUENCIA 2 DE NUMEROS ALEATORIOS DE 64 BITS
SECUENCIA 1 DE NUMEROS ALEATORIOS DE 64 BITS
FIFO
633
651
463
95
96
96
95

Fig. 31

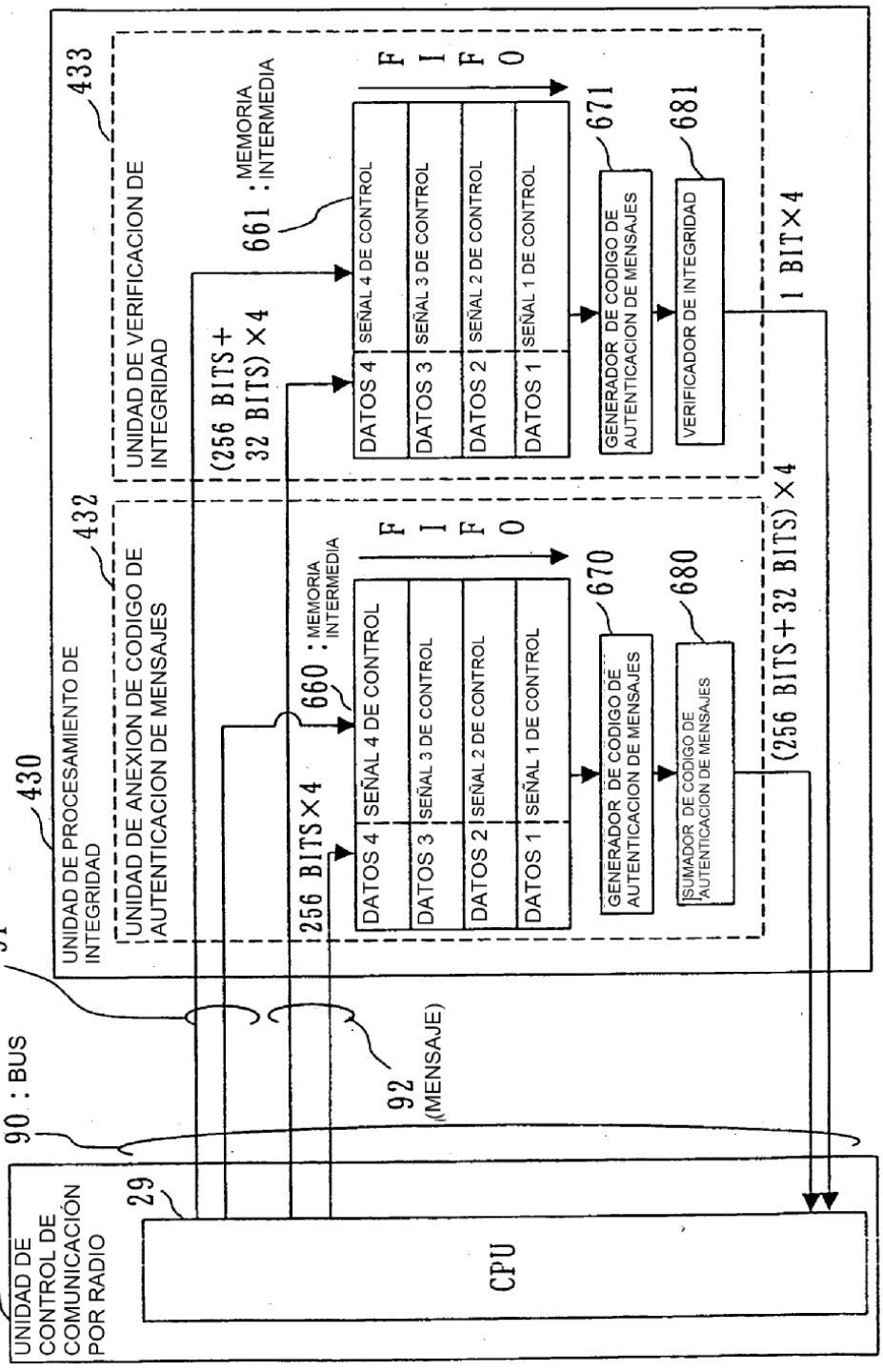

20
UNIDAD DE CONTROL DE COMUNICACIÓN POR RADIO
29
CPU
90 : BUS
91 (IK, CONTADOR-I, DIRECCIÓN, FRESH)
92 (MENSAJE)
430
UNIDAD DE PROCESAMIENTO DE INTEGRIDAD
432
UNIDAD DE ANEXION DE CODIGO DE AUTENTICACION DE MENSAJES
433
UNIDAD DE VERIFICACION DE INTEGRIDAD
256 BITS×4
660 : MEMORIA INTERMEDIA
(256 BITS+ 32 BITS)×4
661 : MEMORIA INTERMEDIA
DATOS 4
DATOS 3
DATOS 2
DATOS 1
SEÑAL 4 DE CONTROL
SEÑAL 3 DE CONTROL
SEÑAL 2 DE CONTROL
SEÑAL 1 DE CONTROL
FIFO
GENERADOR DE CODIGO DE AUTENTICACION DE MENSAJES
670
671
SUMADOR DE CODIGO DE AUTENTICACION DE MENSAJES
680
VERIFICADOR DE INTEGRIDAD
681
(256 BITS+32 BITS)×4
1 BIT×4

Fig. 32

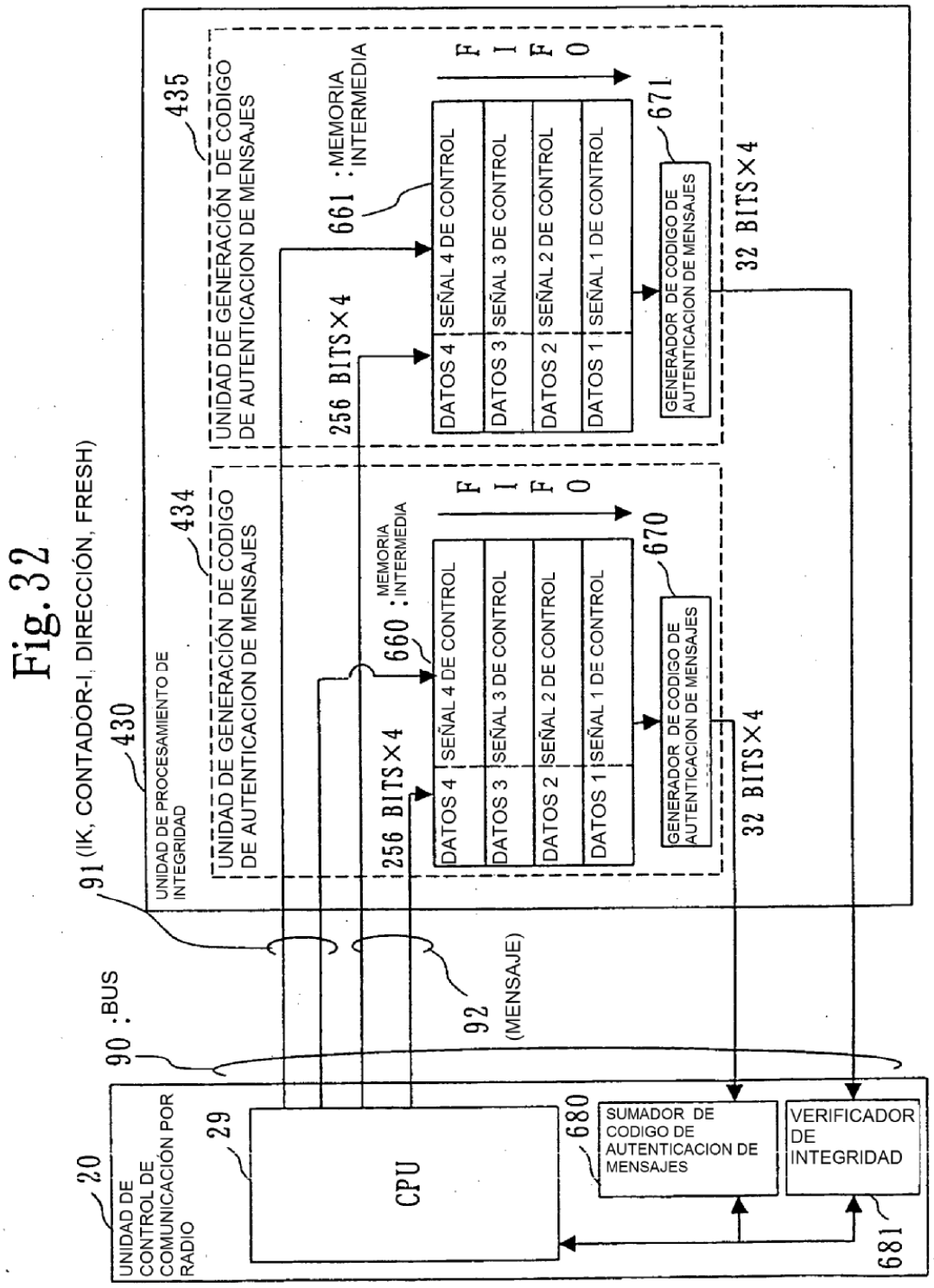

20
UNIDAD DE CONTROL DE COMUNICACIÓN POR RADIO
29
CPU
90 :BUS
91 (IK, CONTADOR-I, DIRECCIÓN, FRESH)
92 (MENSAJE)
430
UNIDAD DE PROCESAMIENTO DE INTEGRIDAD
434
UNIDAD DE GENERACIÓN DE CODIGO DE AUTENTICACION DE MENSAJES
435
UNIDAD DE GENERACIÓN DE CODIGO DE AUTENTICACION DE MENSAJES
660 :MEMORIA INTERMEDIA
661 :MEMORIA INTERMEDIA
256 BITS×4
256 BITS×4
DATOS 4
DATOS 3
DATOS 2
DATOS 1
SEÑAL 4 DE CONTROL
SEÑAL 3 DE CONTROL
SEÑAL 2 DE CONTROL
SEÑAL 1 DE CONTROL
FIFO
670
671
GENERADOR DE CODIGO DE AUTENTICACION DE MENSAJES
GENERADOR DE CODIGO DE AUTENTICACION DE MENSAJES
32 BITS×4
32 BITS×4
680
SUMADOR DE CODIGO DE AUTENTICACION DE MENSAJES
VERIFICADOR DE INTEGRIDAD
681

Fig. 33

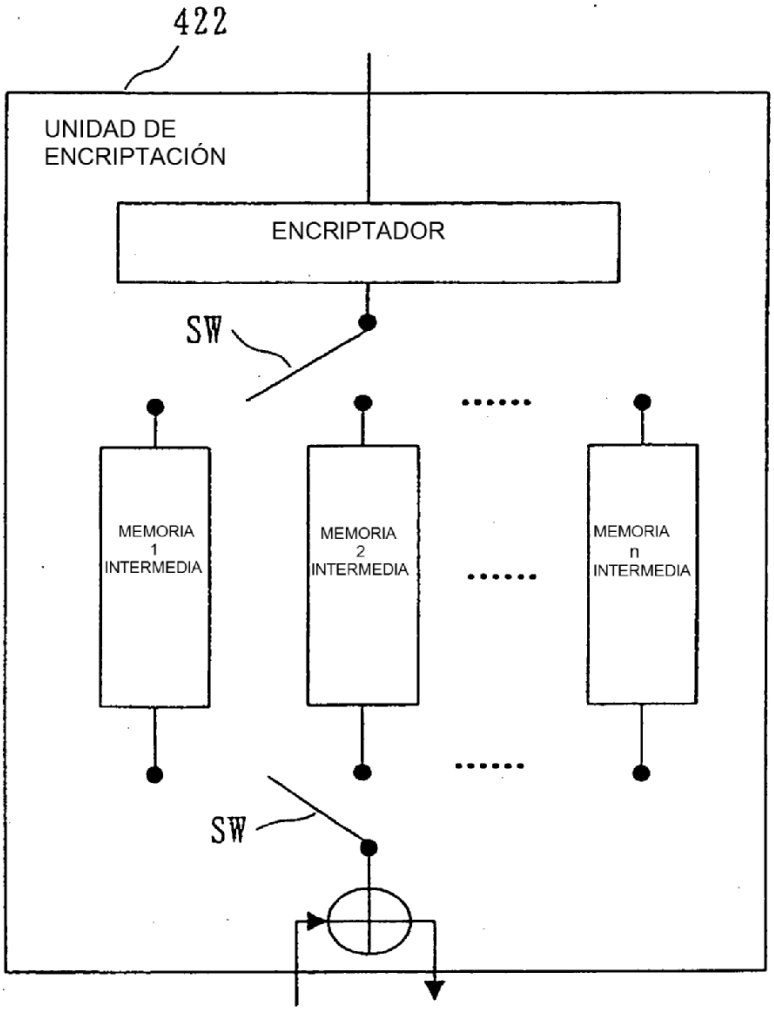

422
UNIDAD DE ENCRIPTACIÓN
ENCRIPTADOR
SW
MEMORIA 1 INTERMEDIA
MEMORIA 2 INTERMEDIA
MEMORIA n INTERMEDIA
SW

Fig. 34

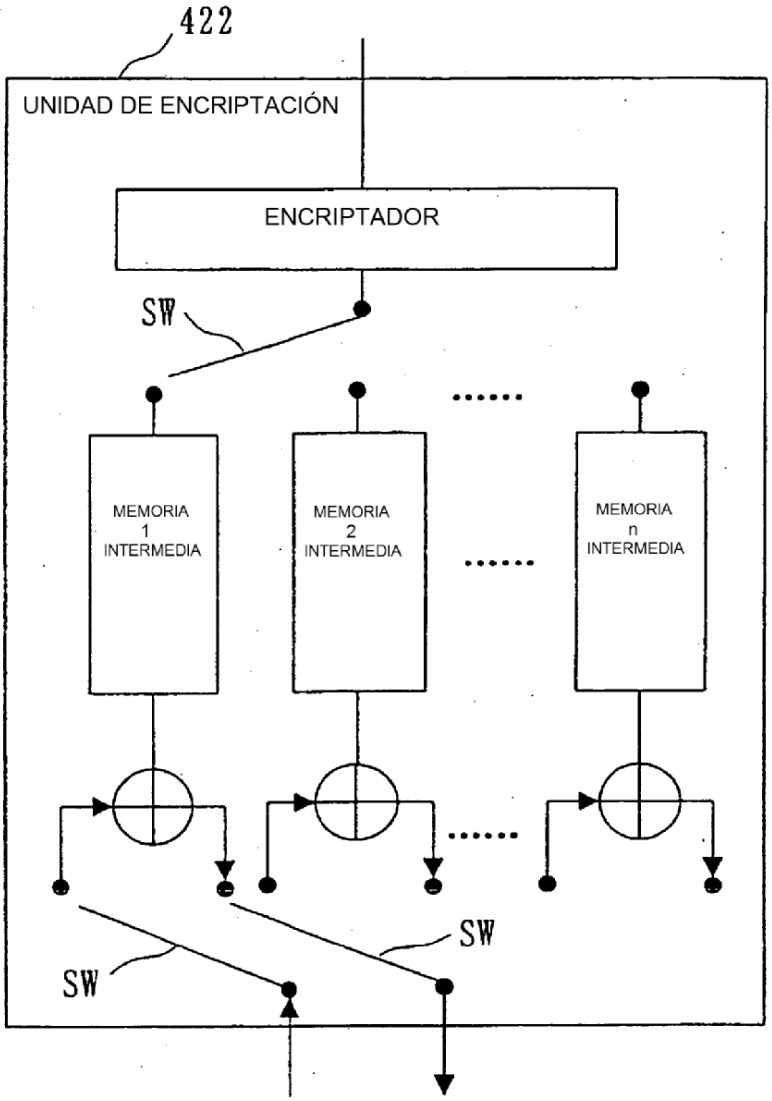
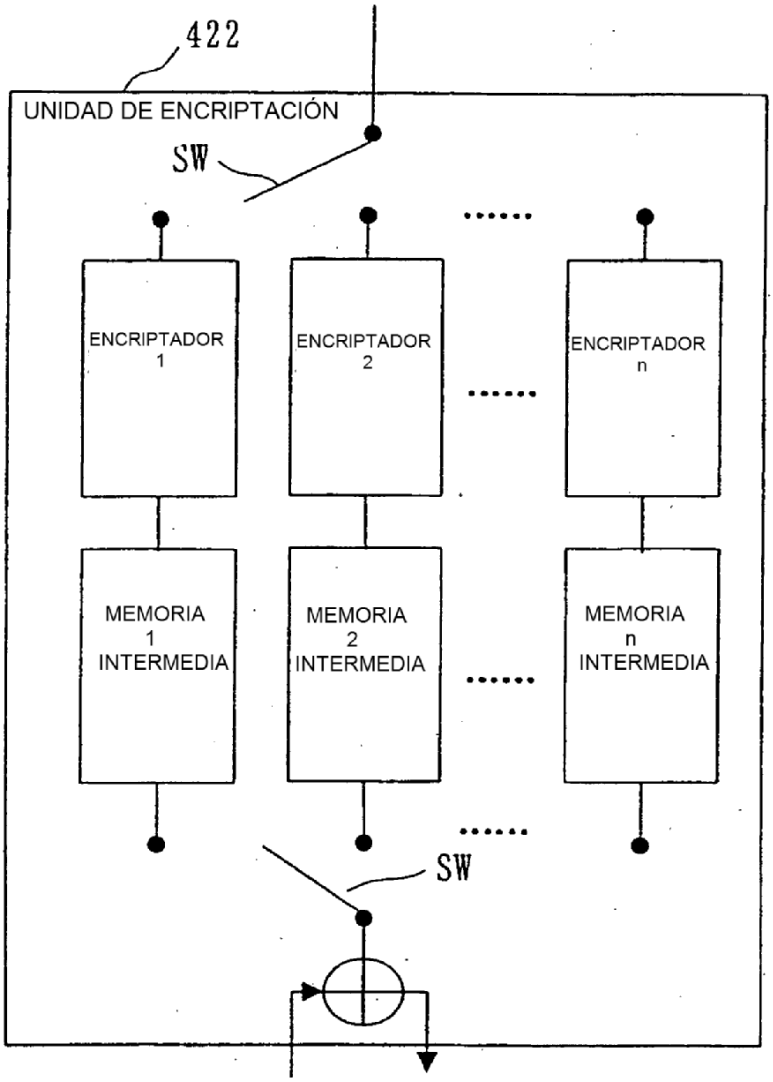

422
UNIDAD DE ENCRIPTACIÓN
ENCRIPTADOR
SW
MEMORIA 1 INTERMEDIA
MEMORIA 2 INTERMEDIA
MEMORIA n INTERMEDIA
SW
SW

Fig. 35


422
UNIDAD DE ENCRIPTACIÓN
SW
ENCRIPTADOR 1
ENCRIPTADOR 2
ENCRIPTADOR n
MEMORIA 1 INTERMEDIA
MEMORIA 2 INTERMEDIA
MEMORIA n INTERMEDIA
SW