(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 657 591**

(51) Int. CI.:

H04L 9/06 (2006.01)
H04L 9/28 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **18.01.2012 PCT/EP2012/050671**

(87) Fecha y número de publicación internacional: **26.07.2012 WO12098135**

(96) Fecha de presentación y número de la solicitud europea: **18.01.2012 E 12700355 (6)**

(97) Fecha y número de publicación de la concesión europea: **15.11.2017 EP 2666254**

(54) Título: **Autenticación de bloques de datos cifrados**

(30) Prioridad:

20.01.2011 DE 102011009008

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
06.03.2018

(73) Titular/es:

ROHDE & SCHWARZ GMBH & CO. KG (100.0%)
Mühldorfstrasse 15
81671 München, DE

(72) Inventor/es:

MUELLER, THORSTEN y
EICHLER, STEPHAN

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

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).

DECRIPCIÓN

Autenticación de bloques de datos cifrados

La invención se refiere a una unidad de autenticación y cifrado y a una unidad de autenticación y descifrado así como a un procedimiento para ello.

De gran importancia es el intercambio de datos cifrado a través de un medio común, como Internet, sin tener que dar acceso a personas no autorizadas a los datos que han de ser transmitidos (protección de la confidencialidad). Además de un cifrado suficientemente grande, igualmente es de importancia que quede garantizada la integridad de los datos transmitidos, para garantizar que los datos transmitidos no se hayan modificado en el trayecto de transporte. Una protección de integridad de este tipo se consigue por ejemplo de tal forma que la suma de comprobación se forma a través de los datos cifrados enviados y también se envía.

Por el documento DE102008013785A1 se dieron a conocer un dispositivo y un procedimiento con los que un flujo de datos se divide en bloques individuales, cifrándose los bloques individuales y calculándose a través de los bloques de datos cifrados individuales una suma de comprobación común. Para ello, se utiliza un procedimiento conocido bajo el nombre “Galois Counter Mode” (en español, modo de contaje Galois) y publicado bajo el título “Galois/Counter Mode of Operation” en el National Institute of Standards and Technology (NIST; en español, Instituto nacional de Estandarización y Técnica).

Un inconveniente del documento DE102008013785A1 es que no es posible que bloques de datos cifrados individuales o bits individuales dentro de los bloques de datos cifrados individuales se puedan excluir de la formación de una suma de comprobación. Esto, sin embargo, es deseable precisamente en las aplicaciones en tiempo real, como por ejemplo transmisiones de voz, transmisiones de imágenes o transmisiones de video. En caso de que durante la transmisión de datos de voz, de imagen o de video transmitidos se produzca un error de transmisión y se transmita de forma errónea por ejemplo un bit, este error se nota solo marginalmente o no se nota en caso de faltar una suma de comprobación. En caso de que a través de los bloques de datos cifrados se calcule una suma de comprobación, en caso de una transmisión errónea de un bit se desecha el paquete completo, lo que precisamente en las aplicaciones en tiempo real mencionadas anteriormente conlleva considerables desventajas y repercute de forma muy molesta. Se reduce la “Quality of Experience” (en español, calidad de experiencia) del usuario. Otras propuestas del estado de la técnica se describen en el documento US2004/0039908A1.

Por lo tanto, la invención tiene el objetivo de proporcionar una unidad de autenticación y cifrado y una unidad de autenticación y descifrado así como un procedimiento para ello, con los que sea posible que bloques de datos cifrados o bits individuales de los bloques de datos cifrados puedan excluirse de la formación de una suma de comprobación, teniendo que estar garantizadas al mismo tiempo una velocidad de ejecución y eficiencia elevadas.

El objetivo se consigue con respecto a la unidad de autenticación y cifrado mediante las características de la reivindicación 1 y con respecto a la unidad de autenticación y descifrado mediante las características de la reivindicación 11. Además, el objetivo se consigue con respecto al procedimiento para la unidad de autenticación y cifrado mediante las características de la reivindicación 13 y con respecto al procedimiento para la unidad de autenticación y descifrado mediante las características de la reivindicación 23. La reivindicación 25 contiene un programa informático con medios de código de programa para poder realizar todos los pasos de procedimiento cuando el programa se ejecuta en un ordenador o en un procesador de señales digital o en otro tipo de unidades aritméticas electrónicas. La reivindicación 26 contiene un producto de programa informático con medios de código de programa almacenados en un soporte legible por máquina, para poder realizar todos los pasos de procedimiento cuando el programa se ejecuta en un ordenador o en un procesador de señales digital o en otro tipo de unidades aritméticas electrónicas. En las reivindicaciones subordinadas correspondientes se indican variantes ventajosas del dispositivo según la invención así como del procedimiento según la invención.

La unidad de autenticación y cifrado según la invención presenta al menos una etapa de cifrado. Cada etapa de cifrado cifra un bloque de datos claros y genera durante ello un bloque de datos cifrados, calculándose a través de cada bloque de datos cifrados una suma de comprobación común. A través de una unidad de selección dentro de cada etapa de cifrado se puede seleccionar qué bits de datos han de usarse dentro de cada bloque de datos cifrados para el cálculo de la suma de comprobación común.

La unidad de autenticación y de descifrado según la invención presenta igualmente al menos una etapa de descifrado. Cada etapa de descifrado descifra un bloque de datos cifrados y genera durante ello un bloque de datos claros, estando calculada a través de cada bloque de datos cifrados una suma de comprobación común. A través de una unidad de selección de cada etapa de descifrado se puede seleccionar qué bits de datos han de usarse dentro de cada bloque de datos cifrados para el cálculo de la suma de comprobación común.

En la unidad de autenticación y cifrado según la invención y en la unidad de autenticación y descifrado según la invención resulta especialmente ventajoso que dentro de cada bloque de datos cifrados se pueden seleccionar bits de datos que a continuación han de usarse para un cálculo de la suma de comprobación común. De esta manera, es

posible que se usen únicamente datos de control dentro de los bloques de datos cifrados para el cálculo de una suma de comprobación, y que a través de los datos útiles mismos que contienen por ejemplo datos de voz, de imagen o de video no se forma ninguna suma de comprobación.

El procedimiento según la invención para una unidad de autenticación y cifrado que presenta al menos una etapa de cifrado comprende varios pasos de procedimiento. En un primer paso de procedimiento se cifra un bloque de datos claros dentro de cada etapa de cifrado, de manera que a partir de este se genera un bloque de datos cifrados. En otro paso de procedimiento, por una unidad de selección dentro de cada etapa de cifrado se selecciona qué bits de datos se usan dentro de cada bloque de datos cifrados para el cálculo de la suma de comprobación común, de tal forma que a continuación se calcula una suma de comprobación común a través de cada bloque de datos cifrados.

El procedimiento según la invención para una unidad de autenticación y descifrado que presenta al menos una etapa de descifrado comprende los siguientes pasos de procedimiento. En un primer paso de procedimiento se descifra un bloque de datos cifrados dentro de cada etapa de descifrado, de manera que a partir de este se genera un bloque de datos claros. En otro paso de procedimiento, por una unidad de selección dentro de cada etapa de descifrado se selecciona qué bits de datos dentro de cada bloque de datos cifrados se usan para el cálculo de la suma de comprobación común, de tal forma que a continuación se calcula la suma de comprobación común a través de cada bloque de datos cifrados.

Resulta especialmente ventajoso que en el procedimiento para la unidad de autenticación y cifrado y en el procedimiento para la unidad de autenticación y descifrado, a través de una unidad de selección dentro de cada etapa de cifrado o etapa de descifrado se puede seleccionar qué bits de datos se deben usar dentro de cada bloque de datos cifrados para el cálculo de la suma de comprobación común. De esta manera, se puede garantizar que por ejemplo, al contrario de datos de control, se pueden excluir datos útiles de la formación de una suma de comprobación común. En el resto del documento, datos de control designan la información de cabecera (datos de cabecera) que se usa para la transmisión de los datos útiles en los diferentes protocolos de transmisión – independientemente de si esta información se transmite junto a los datos útiles en un paquete o separadamente en un canal propio.

Otra ventaja de la unidad de autenticación y cifrado según la invención o de la unidad de autenticación y descifrado según la invención se consigue si la unidad de selección dentro de cada etapa de cifrado o etapa de descifrado enlaza una máscara de bits seleccionable libremente, a través de un Y lógico, con el bloque de datos cifrados de la etapa de cifrado o etapa de descifrado. Esta máscara de bits seleccionable libremente y este enlace con un Y lógico se pueden realizar muy fácilmente en una unidad lógica programable, por ejemplo un FPGA (en inglés, field programable gate array, en español, matriz de puertas programables de campo).

Otra ventaja de la unidad de autenticación y cifrado según la invención o de la unidad de autenticación y descifrado según la invención existe si un primer estado lógico está puesto en una posición dentro de la máscara de bits, si el bit correspondiente se ha de usar en la misma posición dentro del mismo bloque de datos cifrados para el cálculo de la suma de comprobación común y/o si un segundo estado lógico está puesto dentro de la máscara de bits en una posición, si el bit correspondiente no ha de usarse en la misma posición dentro del bloque de datos cifrados para el cálculo de la suma de comprobación común. El primer estado lógico es por ejemplo un uno lógico, mientras que el segundo estado lógico es un cero lógico. De esta manera, es posible que los datos útiles y los datos de control se cifran juntos dentro de un bloque de datos cifrados, porque queda garantizado que únicamente los datos de control pueden utilizarse para la formación de una suma de comprobación común, por lo que se consigue una codificación muy eficiente.

Adicionalmente, en el procedimiento según la invención para una unidad de autenticación y cifrado o una unidad de autenticación y descifrado existe una ventaja, si la unidad de autenticación y cifrado o la unidad de autenticación y descifrado trabajan en el procedimiento según la invención según el principio del modo de contaje Galois, porque en el modo de contaje Galois hasta ahora no se han demostrado lagunas de seguridad y porque trabaja de forma muy rápida y se puede implementar con un gasto tolerable tanto en software como en hardware.

Además existe una ventaja en el procedimiento según la invención para una unidad de autenticación y cifrado o una unidad de autenticación y descifrado, si las máscaras de bits se ajustan a discreción e independientemente entre sí en la unidad de selección de cada etapa de cifrado. Esto permite que especialmente no sea necesario el cumplimiento de requisitos especiales en cuanto al número y la disposición de los datos útiles y los datos de control.

Finalmente, existe una ventaja en el procedimiento según la invención para una unidad de autenticación y cifrado o una unidad de autenticación y descifrado, si varios bits de datos dentro del bloque de datos cifrados son seleccionados por la unidad de selección para el cálculo de la suma de comprobación, si una transmisión de los bloques de datos cifrados presenta pocos errores de transmisión y/o si menos bits de datos dentro de los bloques de datos cifrados son seleccionados por la unidad de selección para el cálculo de la suma de comprobación, si una transmisión de los bloques de datos cifrados presenta más errores de transmisión. De esta manera, queda garantizado que únicamente se renuncia a la protección de integración adicional, si las características del trayecto de transmisión no admiten otra cosa.

Dentro de la descripción, la unidad de autenticación y cifrado según la invención y la unidad de autenticación y descifrado se describen únicamente en conjunto con el modo de contaje Galois. Sin embargo, la presente invención es aplicable a cualquier tipo de cifrado en el que se deba cifrar por bloques y proteger la integridad.

Diferentes ejemplos de realización de la invención se describen a título de ejemplo a continuación haciendo referencia al dibujo. Los objetos que son idénticos presentan los mismos signos de referencia. Las figuras correspondientes del dibujo muestran en concreto:

la figura 1 un ejemplo de realización que describe un caso de aplicación para una unidad aritmética;

la figura 2A un ejemplo de realización de un paquete de datos tal como lo pueden enviar por ejemplo los terminales móviles;

la figura 2B un ejemplo de realización de como la unidad aritmética procesa el paquete de datos del terminal móvil;

la figura 3 una vista general de un ejemplo de realización de la unidad aritmética con la unidad de autenticación y cifrado integrada según la invención y de la unidad de autenticación y descifrado integrada según la invención;

la figura 4A un ejemplo de realización de una unidad de autenticación y cifrado utilizada hasta ahora de forma interna;

la figura 4B un ejemplo de realización de una unidad de autenticación y descifrado utilizada hasta ahora de forma interna;

la figura 5A un ejemplo de realización de una unidad de autenticación y cifrado según la invención;

la figura 5B un ejemplo de realización de una unidad de autenticación y descifrado según la invención;

la figura 6 un diagrama de flujo que describe un ejemplo de realización para el procedimiento según la invención con la unidad de autenticación y cifrado;

la figura 7 otro diagrama de flujo que describe un ejemplo de realización para el procedimiento según la invención con la unidad de autenticación y cifrado o la unidad de autenticación y descifrado;

la figura 8 otro diagrama de flujo que describe un ejemplo de realización para el procedimiento según la invención con la unidad de autenticación y cifrado o la unidad de autenticación y descifrado;

la figura 9 otro diagrama de flujo que describe un ejemplo de realización para el procedimiento según la invención con la unidad de autenticación y cifrado o la unidad de autenticación y descifrado; y

la figura 10 otro diagrama de flujo que describe un ejemplo de realización para el procedimiento según la invención con la unidad de autenticación y descifrado;

La figura 1 describe un caso de aplicación para la unidad aritmética 1 con la unidad de autenticación y cifrado 6 integrada según la invención y la unidad de autenticación y descifrado 7 integrada según la invención. Dos terminales móviles 2_1, 2_2 que en el ejemplo de realización de la figura 1 están representados como teléfonos móviles intercambian mutuamente paquetes de datos 8 durante la existencia de una comunicación de voz. En este ejemplo de realización, los paquetes de datos 8 que han de ser intercambiados son paquetes de datos IP (en inglés, Internet Protocol; en español, Protocolo de Internet). En este ejemplo de realización, los terminales móviles 2_1, 2_2 están conectados a la red 3_1 o la red 3_2. La red 3_1 está conectada al router 4_1 y la red 3_2 está conectada al router 4_2. Ambos router 4_1 y 4_2 están conectados entre sí a través de una radiotransmisión 5 por el aire. A una radiotransmisión 5 de este tipo pueden estar heterodinadas perturbaciones de forma especialmente frecuente.

Los dos router 4_1 y 4_2 establecen un enlace VPN (en inglés, virtual private network; en español, red virtual privada). Dicha red VPN que establecen los dos router 4_1 y 4_2 entre sí está basada por ejemplo en IPSEC (en inglés, Internet protocol security; en español, protocolo de seguridad para Internet) interconecta las dos redes 3_1 y 3_2. La unidad aritmética 1 con una unidad de autenticación y cifrado 6 o una unidad de autenticación y descifrado 7 está realizada en el ejemplo de realización de la figura 1 preferentemente en los router 4_1 y 4_2 que preferentemente están integrados en los terminales móviles 2_1 y 2_2. La unidad aritmética 1 según la invención también puede estar realizada en router 4_1 y 4_2 que no estén realizados dentro de los terminales móviles 2_1 y 2_2 y que por ejemplo interconecten las dos redes 3_1 y 3_2 a través de Internet.

La figura 2A muestra un ejemplo de realización de un paquete de datos 8 que se intercambia entre los terminales móviles 2_1 y 2_2. En este ejemplo de realización, el paquete de datos 8 es un paquete de datos IP. El paquete de

datos 8 presenta un área en la que se encuentra una cabecera IP 9 (en inglés, IP-Header; en español cabecera IP), y un área en la que se encuentra los datos útiles 10. En caso de que el paquete de datos 8 de la figura 2A se transmita del terminal móvil 2_1 al terminal móvil 2_2, en la cabecera IP 9 se encuentra por ejemplo la información sobre la dirección de destino en la red 3_2 que también se puede denominar datos de control.

La figura 2B muestra un ejemplo de realización de la unidad aritmética 1 con una unidad de autenticación y cifrado 6 integrada según la invención. En el ejemplo de realización de la figura 2B, la unidad aritmética 1 está integrada en los router 4_1 y 4_2. En caso de que el terminal móvil 2_1 envíe un paquete de datos 8 al terminal móvil 2_2, el paquete de datos 8 que comprende un área con una cabecera IP 9 y un área con los datos útiles 10 se transmite a la unidad de autenticación y cifrado 6 según la invención. La unidad aritmética 1 genera a continuación un nuevo paquete de datos IP 11 que puede ser transmitido a través de un medio común, como por ejemplo Internet 5, y que en su área de datos útiles transporta el paquete de datos 8 cifrado.

Para ello, la unidad aritmética 1 lee de una unidad de memoria 12 la dirección IP pública del 4_2 en el que se encuentra la red de destino 3_2. Esta dirección IP del espacio de direcciones públicas se registra como dirección de destino en una cabecera IP 13 exterior. Esta dirección de destino igualmente se comunica a la unidad de autenticación y cifrado 6 y, como aún se describe en detalle más adelante, se usa dentro de esta preferentemente como datos de autenticación 13. Preferentemente, también el vector de inicialización 14_0 forma parte de los datos de autenticación 13. La unidad de autenticación y cifrado 6 genera también un valor inicial para un vector de inicialización 14_0. Este valor inicial para el vector de inicialización 14_0 se añade al área de datos útiles del paquete de datos IP 11 y no está cifrado. La cabecera IP 9 y los datos útiles 10 del paquete de datos 8 son cifrados por la unidad de autenticación y cifrado 6 y transmitidos al área de datos útiles del paquete de datos IP 11. Además, la unidad de autenticación y cifrado 6 genera una suma de comprobación 15_1 que igualmente se transmite al área de datos útiles del paquete de datos IP 11. Como aún se describe más adelante, la suma de comprobación 15_1 puede ser calculada a partir de datos cifrados o de partes de los datos cifrados.

Como aún se describe en detalle más adelante, el router 4_2 recibe y descifra el paquete de datos IP 11 y transfiere el contenido, compuesto por los datos útiles cifrados así como el valor inicial del vector de inicialización 14_0 y la suma de comprobación 15_1 a una unidad de autenticación y descifrado 7 que descifra los datos cifrados, de modo que a continuación, estos pueden ser transmitidos al terminal móvil 2_2.

La figura 3 muestra un ejemplo de realización de la unidad aritmética 1 con la unidad de autenticación y cifrado 6 integrada según la invención y la unidad de autenticación y descifrado 7 integrada según la invención. La parte esencial de la unidad aritmética 1 es una unidad de procesamiento de datos 20 central. Dicha unidad de procesamiento de datos 20 central puede ser por ejemplo un procesador de señales o una unidad lógica programable. La unidad de procesamiento de datos 20 central está conectada tanto a la unidad de autenticación y cifrado 6 como a la unidad de autenticación y descifrado 7. A la unidad de procesamiento 20 central está conectada además también la unidad de memoria 12.

En el ejemplo de realización según la invención de la figura 3, a la unidad de procesamiento de datos 20 central están conectados al menos un altavoz 21, al menos un micrófono 22, al menos un sistema de cámara 23 y al menos una unidad de pantalla 24. Sin embargo, no necesariamente tienen que estar conectados los cuatro sistemas 21, 22, 23, 24 a la unidad de procesamiento de datos 20 central, pudiendo estar conectadas también solo uno o varios de estos sistemas 21, 22, 23, 24 a la unidad de procesamiento de datos 20 central. La unidad de procesamiento de datos 20 central recibe un flujo de datos del al menos un micrófono 22 o del al menos un sistema de cámara 23 y lo codifica opcionalmente, antes de que el flujo de datos se transfiere a la unidad de autenticación y cifrado 6. En el otro lado, la unidad de procesamiento de datos central recibe un flujo de datos de la unidad de autenticación y descifrado 7 y lo descodifica opcionalmente, antes de que se transfiere al al menos un altavoz 21 o a la al menos una unidad de pantalla 24.

En el ejemplo de realización de la figura 3, la unidad de autenticación y cifrado 6 está conectada a la unidad de emisión 25. En el ejemplo de realización de la figura 3, la unidad de autenticación y descifrado 7 está conectada a la unidad de recepción 26. Según el ejemplo de realización de la figura 1, en la unidad de emisión 25 y la unidad de recepción 26 se puede tratar de un trayecto de transmisión (de datos) por cable, por ejemplo, un enlace de red. Sin embargo, igualmente es posible que en la unidad de emisión 25 y la unidad de recepción 26 se trate de una unidad de comunicación que permita una transmisión de datos inalámbrica. En este caso, la unidad de emisión 25 contiene las etapas de preparación y de amplificación necesarias, conteniendo la unidad de recepción 26 las disposiciones de mezcla correspondientes para la recepción de un flujo de datos en las bandas de frecuencia posibles para ello, como por ejemplo HF (en inglés, high frequency; en español, alta frecuencia), VHF (en inglés, very high frequency; en español, frecuencia muy alta) o UHF (en inglés, ultra high frequency; en español, frecuencia ultraalta) y dispositivos para la digitalización de la señal de banda de base. Errores de transmisión se producen por ejemplo a causa de un mal canal de transmisión.

La figura 4A muestra un ejemplo de realización conocido que describe el modo de funcionamiento de una unidad de autenticación y cifrado que trabaja según el principio del modo de contaje Galois. La unidad de autenticación y cifrado conocida presenta n etapas de cifrado 30_1 a 30_n, con $n \geq 1$, siendo necesaria para el modo de

funcionamiento de la unidad de autenticación y cifrado al menos una etapa de cifrado 30_1. Cada etapa de cifrado 30_1 a 30_n presenta respectivamente una unidad de cifrado 30_1 a 30_n, suministrándose a cada unidad de cifrado 31_1 a 31_n preferentemente la misma clave 32. Dicha clave 32 por ejemplo está almacenada en la unidad de memoria 12. Cada etapa de cifrado 30_1 a 30_n presenta además un enlace XOR 36_1 a 36_n.

Un vector de inicialización 14_0 que puede presentar un valor de 0 a 2^{64}-1, se incrementa en uno mediante una unidad de incrementación 33_1 a 33_n antes de cada etapa de cifrado 30_1 a 30_n, de manera que a la etapa de cifrado 30_1 se suministra el valor del vector de inicialización 14_0 incrementado en uno. Este valor de vector de inicialización 14_0 incrementado en uno se denomina vector de inicialización 14_1 en la primera etapa de cifrado 30_1. Dado que el vector de inicialización 14_0 se incrementa en el valor uno para cada etapa de cifrado 31_1 a 31_nn en total hay n+1 vectores de inicialización 14_0, 14_1 a 14_n. El vector de inicialización 14_0 está almacenado también en el paquete de datos IP 11 y no está cifrado. Los vectores de inicialización 14_1 a 14_n se cifran con la clave 32 por las unidades de cifrado 31_1 a 31_n dentro de las etapas de cifrado 30_1 a 30_n. El vector de incrementación 14_0 debe estar elegido de tal forma que el valor no se repita tampoco después de n unidades de incrementación 33_1 a 33_n. Las distintas unidades de incrementación 33_1 a 33_n se realizan por ejemplo por un contador que está realizado de forma eficiente en el hardware. El valor inicial de dicho contador o el vector de inicialización 14_0 se selecciona de forma aleatoria, pero tiene que quedar garantizado que el contador no rebose. Como algoritmo de cifrado entra en consideración preferentemente un cifrado AES (en inglés, Advanced Encryption Estándar; en español, estándar de cifrado avanzado) con un tamaño de bloque de 128 bits y una longitud de clave de 256 bits, pudiendo usarse también cualquier otro tipo de cifrados de bloques. Un cifrado AES de este tipo puede cifrar bloques con respectivamente 128 bits.

Dentro de cada etapa de cifrado 30_1 a 30_n se encuentra un enlace XOR 36_1 a 36_n que está enlazado respectivamente a la unidad de cifrado 31_1 a 31_n correspondiente. Una segunda entrada de dicho enlace XOR 36_1 a 36_n se enlaza por XOR con el bloque de datos claros 34_1 a 34_n correspondiente que ha de ser cifrado. Para ello, exactamente un bloque de datos claros 34_1 a 34_n se enlaza por XOR dentro de exactamente una etapa de cifrado 30_1 a 30_n con el valor inicial de exactamente una unidad de cifrado 31_1 a 31_n. Los vectores de inicialización 14_0 a 14_n deben presentar con un cifrado AES de 128 bits un tamaño de bloque de 128 bits o menos, teniendo que rellenarse la diferencia entre el tamaño real de los vectores de inicialización 14_0 a 14_n y los 128 bits (en inglés, padding; en español, relleno). Preferentemente, el vector de inicialización 14_0 tiene siempre una longitud de 128 bits, de manera que se puede prescindir del relleno.

La unidad de procesamiento 20 de la figura 3 que está implementada dentro de la unidad aritmética 1 divide el paquete de datos 8 en bloques de 128 bits. Según el tamaño del valor MTU (en inglés, Maximum Transmission Unit; en español, valor de transmisión máximo) que varía según el medio de transmisión (Ethernet, Gigabit-Ethernet, canal de fibra, etc.), tienen que estar realizadas sucesivamente tantas etapas de cifrado 30_1 a 30_n que el tamaño de paquete de datos máximo indicado por el valor MTU se divida en tamaños correspondientemente pequeños, manejables para las unidades de cifrado 31_1 a 31_n. Un tamaño de MTU típico para Ethernet es de 1.500 bitios, de manera que el paquete de datos 8 debe tener como máximo una longitud de 1.500 bitios. En caso de que dentro de las unidades de cifrado 31_1 a 31_n se aplique un cifrado AES de 256, tienen que estar realizadas al menos 1.500 x 8 / 128 etapas de cifrado 30_1 a 30_n, redondeándose el resultado. Para el caso mencionado anteriormente, el número de etapas de cifrado en Ethernet con un valor MTU de 1.500 asciende de forma redondeada a 94. Pero evidentemente, también es posible el uso de otros tipos de cifrado.

En la salida de los etapas de cifrado 30_1 a 30_n, los bloques de datos claros 34_1 a 34_n cifrados se emiten como bloques de datos cifrados 35_1 a 35_n. A causa del enlace XOR 36_1 a 36_n queda garantizado que el orden de bits dentro de los bloques de datos claros 34_1 a 34_n corresponde también al orden de bits en los bloques de cifrado 35_1 a 35_n. Por lo tanto, una información que en los bloques de datos claros 34_1 a 34_n se puede encontrar en una posición de bit determinada dentro de los por ejemplo 128 bits, igualmente se encuentra en la misma posición en los bloques de datos cifrados 35_1 a 35_n. En lo sucesivo, por la unidad de procesamiento 20, los diferentes bloques de datos cifrados 35_1 a 35_n se insertan en el área de datos útiles del paquete de datos IP 11. En este caso, hay tener en cuenta que la longitud de los bloques de datos cifrados 35_1 a 35_n es menor que el valor MTU admisible, porque alrededor del área de datos útiles aún se tiene que establecer una cabecera IP 13 exterior en el paquete de datos IP 11.

Después de que los bloques de datos claros 34_1 a 34_n han sido cifrados por las etapas de cifrado 30_1 a 30_n, por lo que se generan los bloques de datos cifrados 35_1 a 35_n, en un siguiente paso se forma una suma de comprobación 15_1 a través de todos los bloques de datos cifrados 35_1 a 35_n. Para ello, datos de autenticación 13 conocidos se multiplican por el vector de campo de Galois H en la unidad de multiplicación 37, enlazándose el resultado con un enlace XOR 38_1 con el bloque de datos cifrados 35_1. El establecimiento del vector de campo de Galois H se describe en la publicación “Galois/Counter Mode of Operation”, a la que se remite aquí. El resultado de dicho enlace XOR 38_1 se multiplica en una unidad de multiplicación 37 por el vector de campo de Galois H y, a continuación, se enlaza con el enlace XOR 38_2 siguiente con el bloque de datos cifrados 35_2 siguiente que por razones de seguridad no están representados en las figuras del dibujo.

Esto se produce hasta que se haya enlazado el último bloque de datos cifrados 35_n a través del último enlace XOR

38_n. El resultado del último enlace XOR 38_n se multiplica en una unidad de multiplicación 37 por el vector de campo de Galois H y, a continuación, con la unidad de enlace XOR 39 se enlaza con el resultado de una concatenación 41 de una longitud de bits de los datos de autenticación 13 y de una longitud de bits del bloque de datos cifrados 35. Una concatenación 41 de los bits 001 y 10111 da como resultado la secuencia de bits 00110111. Por concatenación se entiende por tanto la adición de secuencias de bits formando una secuencia de bits total.

El resultado de la unidad de enlace XOR 39 se multiplica en la unidad de multiplicación 37 por el vector de campo de Galois H. Este resultado se suministra a la unidad de enlace XOR 40 y se enlaza con el vector inicial 14_0 cifrado con la clave 32 por la unidad de cifrado 31_1. Como resultado, la unidad de enlace XOR 40 proporciona la suma de comprobación 15_1.

La ventaja de la unidad de autenticación y cifrado utilizada hasta ahora de forma interna por la solicitante y que trabaja según la figura 4A, es que las etapas de cifrado 30_1 a 30_n trabajan de forma prácticamente paralela y también la generación de la suma de comprobación 15_1 puede integrarse muy bien en este concepto a través de los bloques de datos cifrados 35_1 a 35_n individuales.

En caso de que la unidad de autenticación y cifrado 6 de la figura 2B esté estructurada conforme al esquema de conexiones de la figura 4A, la unidad aritmética 1 de orden superior integraría la suma de comprobación 15_1 en el área de datos útiles del paquete de datos IP 11. A través de la unidad de emisión 25 conectada a la unidad de autenticación y cifrado 6, el paquete de datos IP se transmitiría al receptor.

Para completar, en la figura 4B está representada una vista general de un esquema de conexiones de una unidad de autenticación y descifrado 7 utilizada hasta ahora de forma interna por la solicitante y que trabaja según el principio del modo de contaje Galois. El modo de funcionamiento de la unidad de autenticación y descifrado de la figura 4B sustancialmente es idéntico a la unidad de autenticación y cifrado de la figura 4A, por lo que se remite además a la descripción relativa a la figura 4A.

La diferencia de la unidad de autenticación y cifrado de la figura 4A y la unidad de autenticación y descifrado de la figura 4B consiste en que en la figura 4B, las unidades de enlace XOR 36_1 a 36_n enlazan la salida de las unidades de cifrado 31_1 a 31_n con los bloques de datos cifrados 35_1 a 35_n recibidos, de manera que en la salida de las unidades de enlace XOR 36_1 a 36_n están presentes los bloques de datos claros 34_1 a 34_n. En este caso, las etapas de cifrado 30_1 a 30_n son etapas de descifrado 29_1 a 29_n, cifrando las etapas de descifrado 29_1 a 29_n un vector de inicialización 14_1 a 14_n con la clave 32 en las unidades de cifrado 31_1 a 31_n. Únicamente la salida de unidades de cifrado 31_1 a 31_n dentro de las etapas de descifrado 29_1 a 29_n se usa junto a las unidades de enlace XOR 36_1 a 36_n y los bloques de datos cifrados 35_1 a 35_n para generar los bloques de datos claros 34_1 a 34_n.

El vector de inicialización 14_0 se comunica a la unidad de autenticación y descifrado a través del paquete de datos IP 11. Por el paquete de datos IP 11, la unidad de autenticación y descifrado conoce también los datos de autenticación 13 que preferentemente se componen de los datos de control (cabecera IP). Según la secuencia descrita con respecto a la figura 4A, también la unidad de autenticación y descifrado calcula una suma de comprobación 15_2 usando para ello los bloques de datos cifrados 35_1 a 35_n y los datos de autenticación 13. En cuanto la unidad de autenticación y descifrado ha calculado la suma de comprobación 15_2, la suma de comprobación 15_2 calculada se compara con la suma de comprobación 15_1 recibida por la unidad de autenticación y descifrado en el paquete de datos IP 11. Si las dos sumas de comprobación 15_1, 15_2 coinciden, es muy probable que en los cifrados 35_1 a 35_n se trate también de los cifrados 35_1 a 35_n generados por la unidad de autenticación y cifrado.

La figura 5A muestra un ejemplo de realización de la unidad de autenticación y cifrado 6 según la invención que está integrada dentro de una unidad aritmética 1. La unidad de autenticación y cifrado 6 según la invención está basada en los principios del modo de contaje Galois tal como ya se ha descrito en detalle en las descripciones de las figuras 4A y 4B anteriores. Por esta razón, con los mismos signos de referencia se remite a las descripciones de las figuras 4A y 4B.

A diferencia, cada etapa de cifrado 30_1 a 30_n presenta además una unidad de selección 52_1 a 52_n, por la que puede seleccionarse qué bits de datos han de usarse dentro de cada bloque de datos cifrados 35_1 a 35_n para el cálculo de la suma de comprobación 15_1 común. Para ello, la unidad de selección 52_1 a 52_n enlaza dentro de cada etapa de cifrado 30_1 a 30_n una máscara de bits 51_1 a 51_n seleccionable libremente, a través de un Y lógico 50_1 a 50_n, con los bloques de datos cifrados 35_1 a 35_n de las etapas de cifrado 30_1 a 30_n individuales. La máscara de bits 51_1 a 51_n se denomina también máscara MAC (en inglés, message authentication code; en español, código de autenticación de mensajes). En el caso de que una primera secuencia de bits 0101 se enlaza con una segunda secuencia de bits 0011 por medio de un enlace de Y lógico, resulta la secuencia de bits 001. La máscara de bits 51_1 a 51_n seleccionable libremente presenta preferentemente la misma longitud de bits que los bloques de datos cifrados 35_1 a 35_n. Respectivamente un Y lógico 50_1 a 50_n y respectivamente una máscara de bits 51_1 a 51_n están integradas en una unidad de selección 51_1 a 51_n.

En cuanto un primer estado lógico que puede ser un uno lógico se ha puesto dentro de una posición dentro de la máscara de bits 51_1 a 51_n, el bit correspondiente se usa en la misma posición dentro del bloque de datos cifrados

35_1 a 35_n para el cálculo de la suma de comprobación 15_1 común. De forma complementaria, en un segundo estado lógico que puede ser un cero lógico y que está puesto en una posición dentro de la máscara de bits 51_1 a 51_n, no se usa el bit correspondiente en la misma posición dentro del bloque de datos cifrados 35_1 a 35_n para el cálculo de la suma de comprobación 15_1 común. Esto permite que un bloque de datos claros 34_1 a 34_n y por tanto un bloque de datos cifrados 35_1 a 35_n contenga tanto datos útiles 10 como datos de control 9, debiendo crearse precisamente solo para los datos de control 9 una suma de comprobación 15_1. De esta manera, los bloques de datos 8 que han de usarse pueden dividirse de manera muy eficiente dentro de la unidad de autenticación y cifrado 6 según la invención. También es especialmente significativo el hecho de que no se modifica el modo de trabajo básico del modo de contaje Galois y que además es posible una realización eficiente en software o hardware.

Las máscaras de bits 51_1 a 51_n individuales de las unidades de selección 52_1 a 52_n dentro de cada etapa de cifrado 30_1 a 30_n pueden ajustarse de forma discrecional y totalmente independiente entre sí. Únicamente en el lado de la unidad de autenticación y descifrado 7 deben aplicarse las mismas máscaras de bits 51_1 a 51_n en las etapas de descifrado 29_1 a 29_n. Preferentemente, precisamente los bits de datos dentro del bloque de datos cifrados 35_1 a 35_n que ya contengan una protección contra errores son excluidos por la unidad de selección 52_1 a 52_n del cálculo de la suma de comprobación 15_1 común. Una protección contra errores de este tipo existe por ejemplo durante la transmisión de datos de video, de imagen o de voz, porque la información en el lado del receptor llegan a una unidad de descodificación robusta, por ejemplo CRC (en inglés, cyclic redundancy check; en español, comprobación de redundancia cíclica). A continuación, un error de bit individual no podría ser notado por el oído humano o no podría ser percibido o apenas podría ser percibido en una unidad de pantalla 24. En cambio, es distinto si la totalidad de los datos útiles 10 dentro del paquete de datos IP 11 se desechan a causa de una suma de comprobación 15_1, 15_n inconsistente, de manera que según el valor MTU y la velocidad de bits faltaría un período de tiempo de por ejemplo 20 ms en el lado del receptor.

Por lo tanto, por las razones mencionadas conviene que la unidad de autenticación y cifrado 6 según la invención así como la unidad de autenticación y descifrado 7 según la invención trabajen según el principio del modo de contaje Galois.

La ventaja es que dentro de cada etapa de cifrado 30_1 a 30_n, una unidad de cifrado 31_1 a 31_n cifre siempre otro vector de inicialización 14_1 a 14_n con la misma clave, de manera que también bloques de datos claros 34_1 a 34_n idénticos que se enlaza con el resultado de las unidades de cifrado 31_1 a 31_n a través de un enlace XOR 36_1 a 36_n, conducen a bloques de datos cifrados 35_1 a 35_n distintos.

El resultado de la primera unidad de selección 52_1 se enlaza, a través de la unidad de enlace XOR 38_1 con el resultado de una unidad de multiplicación 37 que multiplica datos de autenticación 13 con el vector de campo de Galois H. Las demás unidades de selección 52_1 a 52_n se conectan, respectivamente a través de una unidad de multiplicación 37, a la salida de la unidad de enlace XOR 38_1 a 38_n anterior a través de la unidad de enlace XOR 38_2 a 38_n. El cálculo de la suma de comprobación 15_1 se realiza en la figura 5A de forma análoga a las realizaciones en la figura 4A, a lo que se remite en lo sucesivo.

La figura 5B muestra un ejemplo de realización de una unidad de autenticación y descifrado 7 según la invención que preferentemente está integrada en una unidad aritmética 1. La diferencia con el ejemplo de realización según la invención de la figura 5A consiste en que en las etapas de cifrado 30_1 a 30_n se trata ahora de las etapas de descifrado 29_1 a 29_n, enlazando las unidad de enlace XOR 36_1 a 36_n el resultado de las unidades de cifrado 31_1 a 31_n con los bloques de datos cifrados 35_1 a 35_n, de manera que en la salida de las unidades de enlace XOR 36_1 a 36_n están presentes los bloques de datos claros 34_1 a 34_n. En total, cada unidad de autenticación y descifrado 7 presenta al menos una etapa de descifrado 29_1 a 29_n, descifrando cada etapa de descifrado 29_1 a 29_n un bloque de datos cifrados 35_1 a 35_n generando de esta manera un bloque de datos claros 34_1 a 34_n.

Las máscaras de bits 51_1 a 51_n aplicadas en la unidad de selección 52_1 a 52_n por la unidad de autenticación y descifrado 7 tienen que ser idénticas a las máscaras de bits 51_1 a 51_n aplicadas dentro de la unidad de autenticación y cifrado 6 en las unidades de selección 52_1 a 52_n. La máscara de bits 51_1 a 51_n que ha de ser usada puede aplicarse igualmente en la cabecera IP 13 exterior. Para ello, pueden ponerse a disposición por ejemplo tres bits para representar ocho máscaras de bits 51_1 a 52_n diferentes.

Además, dentro de la unidad de autenticación y descifrado 7 según la invención, con la ayuda de los datos de autenticación 13 y los bloques de datos cifrados 35_1 a 35_n conocidos y las máscaras de bits 51_1 a 52_n conocidas se calcula la suma de comprobación 15_2. Para la manera en que se calcula la suma de comprobación 15_2, se remite a la descripción de las figuras 5A y 4A. En el caso de que la suma de comprobación 15_2 calculada por la unidad de autenticación y descifrado 7 no coincida con la suma de comprobación 15_1 que se recibió en el paquete de datos IP 11, se desechan todos los datos de control y datos útiles, cuya integridad no pudo ser verificada. Los datos recibidos que no se utilizaron para el cálculo de la suma de comprobación 15_2 se siguen procesando normalmente después de su descifrado. Esto sirve para que errores de transmisión que pueden producirse dentro de por ejemplo una interfaz aérea no conduzcan a que en caso de un solo error de bit se deseche el paquete de datos IP 11 completo con datos de video y/o datos de voz y/o datos de imagen dentro del área de datos útiles.
Según la calidad de la conexión entre los terminales móviles 2_1 a 2_2 pueden adaptarse las máscaras de bits 51_1 a

52_2. En el caso de que la unión es de alta calidad, todos los bits dentro de los bloques de datos cifrados 35_1 a 35_n pueden utilizarse para el cálculo de la suma de comprobación 15_1,15_n, utilizándose en el caso de que la conexión sea de mala calidad solo los bits para los datos de control para el cálculo de la suma de comprobación 15_1, 15_2.

La figura 6 muestra un ejemplo de realización de un diagrama de flujo del procedimiento según la invención para una unidad de autenticación y cifrado 6 que presenta al menos una etapa de cifrado 30_1 a 30_n. En un primer paso de procedimiento S_1 se cifra un bloque de datos claros 34_1 a 34_n dentro de una etapa de cifrado 30_1 a 30_n, de tal forma que a partir de ello se genera un bloque de datos cifrados 35_1 a 35_n.

En un segundo paso de procedimiento S_2, dentro de una unidad de selección 52_1 a 52_n en cada etapa de cifrado 30_1 a 30_n se selecciona qué bits de datos dentro de cada bloque de datos cifrados 35_1 a 35_n se usan para el cálculo de la suma de comprobación 15_1 común. A continuación, se calcula la suma de comprobación 15_1 común a través de cada bloque de datos cifrados 35_1 a 35_n o a través de cada bit de datos dentro del bloque de datos cifrados 35_1 a 35_n seleccionado por la unidad de selección 52_1 a 52_n.

La figura 7 muestra otro ejemplo de realización de un diagrama de flujo del procedimiento según la invención para una unidad de autenticación y cifrado 6 que presenta un paso de procedimiento S_3 que puede ejecutarse según el paso de procedimiento S_2 del diagrama de flujo anterior. Dentro del paso de procedimiento S_3, una máscara de bits 51_1 a 51_n se enlaza con el bloque de datos cifrados 35_1 a 35_n de cada etapa de cifrado 30_1 a 30_n a través de un Y lógico 50_1 a 50_n dentro de una unidad de selección 52_1 a 52_n. Resulta especialmente ventajoso que un enlace por Y lógico 50_1 a 50_n puede realizarse muy fácilmente en hardware.

La figura 8 muestra otro ejemplo de realización de un diagrama de flujo del procedimiento según la invención para una unidad de autenticación y cifrado 6. El paso de procedimiento S_4 se realiza directamente después del paso de procedimiento S_3 y define que un primer estado lógico que puede contener un uno lógico se usa en una posición de la máscara de bits 51_1 a 51_n, para que el bit correspondiente se use en la misma posición dentro del bloque de datos cifrados 35_1 a 35_n para el cálculo de la suma de comprobación 15_1 y para que un segundo estado lógico que puede contener un cero lógico se use en una posición de la máscara de bits 51_1 a 52_n para que el bit correspondiente no se use en la misma posición dentro del bloque de datos cifrados 35_1 a 35_n para el cálculo de la suma de comprobación 15_1.

El paso de procedimiento S_3 siguiente también puede realizarse directamente después del paso de procedimiento S_3. Dentro del paso de procedimiento S_5, las máscaras de bits 51_1 a 51_n pueden ajustarse a discreción y con total independencia entre sí en la unidad de selección 52_1 a 52_n de cada etapa de cifrado 30_1 a 30_n.

En otro paso de procedimiento S_6 que también puede realizarse según uno de los pasos de procedimiento S_2, S_3 o S_4, se excluyen por la unidad de selección 52_1 a 52_n bloques de datos cifrados 35_1 a 35_n que ya contengan una protección de integridad. Se puede tratar de datos de voz, de imagen o de video.

La figura 9 muestra otro ejemplo de realización de un diagrama de flujo del procedimiento según la invención para una unidad de autenticación y cifrado 6 con el paso de procedimiento 7_7 según la invención. El paso de procedimiento S_7 puede realizarse tanto después del paso de procedimiento S_2 como después de los pasos de procedimiento S_3, S_4 o S_5. El paso de procedimiento S_7 hace que la máscara de bits 51_1 a 51_n se adapte dinámicamente a la calidad del canal de transmisión entre los terminales móviles 2_1 y 2_n. En el caso de que el canal de transmisión esté poco perturbado, por la unidad de selección 52_1 a 52_n son utilizados más bits de datos dentro del bloque de datos de control 35_1 a 35_n para el cálculo de la suma de comprobación 15_1. Por otra parte, en el caso de que el canal de transmisión esté menos perturbado, por la unidad de selección 52_1 a 52_n son utilizados menos bits de datos dentro del bloque de datos cifrados 35_1 a 35_n para el cálculo de la suma de comprobación 15_1.

La figura 10 muestra un ejemplo de realización de un diagrama de flujo para el procedimiento según la invención con una unidad de autenticación y descifrado 7 que presenta los pasos de procedimiento S_8 y S_9. Dentro del paso de procedimiento S_8 se descifra un bloque de datos cifrados 35_1 a 35_n dentro de cada etapa de descifrado 29_1 a 29_n, de manera que a partir de ello se genera respectivamente un bloque de datos claros 34_1 a 34_n.

En el paso de procedimiento S_9, por una unidad de selección 52_1 a 52_n se selecciona dentro de cada etapa de descifrado 29_1 a 29_n qué bits de datos se usan dentro de cada bloque de datos cifrados 35_1 a 35_n para el cálculo de la suma de comprobación 15_2. A continuación, se calcula la suma de comprobación 15_2 a través de cada bloque de datos cifrados 35_1 a 35_n.

A causa del hecho de que el procedimiento para la unidad de autenticación y descifrado 7 se ejecuta de forma sustancialmente análoga al procedimiento para la unidad de autenticación y cifrado 6, los pasos de procedimiento S_3, S_4, S_5, S_6 y S_7, si se refieren a la unidad de autenticación y descifrado 7, pueden usarse junto con los pasos de procedimiento S_8 y S_9. Sobre todo, todas las características que se refieran a una unidad de autenticación y cifrado 6 también pueden aplicarse a una unidad de autenticación y descifrado 7. Como ya se ha descrito, n es siempre un número natural superior o igual a uno.

El procedimiento según la invención para la unidad de autenticación y cifrado 6 y la unidad de autenticación y

descifrado 7 resulta especialmente adecuado para implementarse en un programa que se ejecute en un ordenador o un procesador de señales digital u otras unidades aritméticas electrónicas. El procedimiento para la unidad de autenticación y cifrado 6 y para la unidad de autenticación y descifrado 7 también resulta especialmente adecuado para almacenarse como código de programa especialmente en un soporte legible por máquina, para que posteriormente el programa pueda ejecutarse en un ordenador o un procesador de señales digital u otras unidades aritméticas electrónicas.

En el marco de la invención pueden combinarse entre sí todas las características descritas y/o dibujadas.

REIVINDICACIONES

1. Unidad de autenticación y cifrado (6) que presenta al menos una etapa de cifrado (30_1 a 30_n), estando realizada cada etapa de cifrado (30_1 a 30_n) de tal forma que cifra un bloque de datos claros (34_1 a 34_n) generando durante ello un bloque de datos cifrados (35_1 a 35_n) y calculándose a través de cada bloque de datos cifrados (35_1 a 35_n) una suma de comprobación (15_1) común, **caracterizada porque** a través de una unidad de selección (52_1 a 52_n) dentro de cada etapa de cifrado (30_1 a 30_n) se puede seleccionar qué bits de datos dentro de cada bloque de datos (35_1 a 35_n) han de usarse para el cálculo de la suma de comprobación (15_1) común, para usar únicamente datos de control dentro de los bloques de datos cifrados (35_1 a 35_n) para el cálculo de una suma de comprobación (15_1).

2. Unidad de autenticación y cifrado según la reivindicación 1, **caracterizada porque** la unidad de selección (52_1 a 52_n) dentro de cada etapa de cifrado (30_1 a 30_n) enlaza una máscara de bits (51_1 a 51_n) seleccionable libremente, a través de un Y lógico (50_1 a 50_n), con el bloque de datos cifrados (35_1 a 35_n) de la etapa de cifrado (30_1 a 30_n).

3. Unidad de autenticación y cifrado según la reivindicación 2, **caracterizada porque** un primer estado lógico está puesto en una posición dentro de la máscara de bits (51_1 a 51_n), si el bit correspondiente se ha de usar en la misma posición dentro del bloque de datos cifrados (35_1 a 35_n) para el cálculo de la suma de comprobación (15_1) común y/o porque un segundo estado lógico está puesto dentro de la máscara de bits (51_1 a 51_n) en una posición, si el bit correspondiente no ha de usarse en la misma posición dentro del bloque de datos cifrados (35_1 a 35_n) para el cálculo de la suma de comprobación (15_1) común.

4. Unidad de autenticación y cifrado según las reivindicaciones 2 o 3, **caracterizada porque** las máscaras de bits (51_1 a 51_n) se ajustan de forma discrecional e independiente entre sí en la unidad de selección (52_1 a 52_n) de cada etapa de cifrado (30_1 a 30_n).

5. Unidad de autenticación y cifrado según una de las reivindicaciones anteriores, **caracterizada porque** bits de datos dentro de los bloques de datos cifrados (35_1 a 35_n) que ya contengan una protección de integridad o que no necesiten protección de integridad están exluidos por la unidad de selección (52_1 a 52_n) del cálculo de la suma de comprobación (15_1) común.

6. Unidad de autenticación y cifrado según una de las reivindicaciones anteriores, **caracterizada porque** la unidad de autenticación y cifrado (6) es una unidad de autenticación y cifrado (6) que trabaja según el principio del modo de contaje Galois.

7. Unidad de autenticación y cifrado según una de las reivindicaciones anteriores, **caracterizada porque** varios bits de datos dentro del bloque de datos cifrados (35_1 a 35_n) están seleccionados por la unidad de selección (52_1 a 52_n) para el cálculo de la suma de comprobación (15_1), si una transmisión de los bloques de datos cifrados (35_1 a 35_n) presenta pocos errores de transmisión, o **porque** menos bits de datos dentro de los bloques de datos cifrados (35_1 a 35_n) son seleccionados por la unidad de selección (52_1 a 52_n) para el cálculo de la suma de comprobación (15_1), si una transmisión de los bloques de datos cifrados (35_1 a 35_n) presenta más errores de transmisión.

8. Unidad de autenticación y cifrado según una de las reivindicaciones anteriores, **caracterizada porque** las etapas de cifrado (30_1 a 30_n) individuales están conectadas entre sí de tal forma que incluso a partir de bloques de datos claros (34_1 a 34_n) idénticos resultan después del cifrado bloques de datos cifrados (35_1 a 35_n) distintos.

9. Unidad de autenticación y cifrado según la reivindicación 8, **caracterizada porque** cada etapa de cifrado (30_1 a 30_n) cifra un vector de inicialización (14_1 a 14_n) distinto con una clave (32) idéntica y enlaza los bloques de datos claros (34_1 a 34_n) correspondientes con el vector de inicialización (34_1 a 34_n) cifrado con un enlace XOR (36_1 a 36_n) para generar a partir de ello los bloques de datos cifrados (35_1 a 35_n).

10. Unidad de autenticación y cifrado según una de las reivindicaciones anteriores, **caracterizada porque** datos de autenticación (13) se multiplican en una unidad de multiplicación (37) por el vector de campo de Galois y a través de un enlace XOR (38_1) están enlazados con la salida de la unidad de selección (52_1), multiplicándose el resultado en otra unidad de multiplicación (37) por otro vector de campo de Galois y a través de otro enlace XOR (38_2) se enlaza siempre con una unidad de salida (52_1 a 52_n) de una etapa de cifrado (30_2 a 30_n) siguiente, y la salida del último enlace XOR (38_n) se multiplica en otra unidad de multiplicación (37) por un vector de campo de Galois, estando enlazado el resultado de dicha unidad de multiplicación (37) por medio de un enlace XOR (39) por el resultado de una concatenación (41) de una longitud de bits de los datos de autenticación (13) y de una longitud de bits del bloque de datos cifrados (35_1 a 35_n), multiplicándose el resultado del enlace XOR (39) en otra unidad de multiplicación (37) por el vector de campo de Galois, enlazándose el resultado de esta unidad de multiplicación (37) con un enlace XOR (40) por un vector de inicialización (14_0) cifrado único, a partir de lo cual se calcula la suma de comprobación (15_1).

11. Unidad de autenticación y cifrado (7) que presenta al menos una etapa de descifrado (29_1 a 29_n), estando realizada cada etapa de descifrado (29_1 a 29_n) de tal forma que descifra un bloque de datos cifrados (35_1 a 35_n) generando con ello un bloque de datos claros (34_1 a 34_n) y estando calculada a través de cada bloque de datos

cifrados (35_1 a 35_n) una suma de comprobación (15_2) común, **caracterizada porque** a través de una unidad de selección (52_1 a 52_n) dentro de cada etapa de descifrado (29_1 a 29_n) se puede seleccionar qué bits de datos dentro de cada bloque de datos cifrados (35_1 a 35_n) han de usarse para el cálculo de la suma de comprobación (15_2) común para usar únicamente datos de control dentro de los bloques de datos cifrados (35_1 a 35_n) para el cálculo de una suma de comprobación (15_2).

12. Unidad de autenticación y cifrado según la reivindicación 11, **caracterizada porque** se calcula una suma de comprobación (15_2) que se compara con la suma de comprobación (15_1) recibida por la unidad de autenticación y cifrado (6).

13. Procedimiento para un cifrado con una unidad de autenticación y cifrado (6) que presenta al menos una etapa de cifrado (30_1 a 30_n), con el siguiente paso de procedimiento:

- el cifrado (S_1) de un bloque de datos claros (34_1 a 34_n) dentro de cada etapa de cifrado (30_1 a 30_n), de manera que se genera un bloque de datos cifrados (35_1 a 35_n),

caracterizado por

- la selección (S_2) en una unidad de selección (52_1 a 52_n) dentro de cada etapa de cifrado (30_1 a 30_n), qué bits de datos dentro de cada bloque de datos cifrados (35_1 a 35_n) se usan para el cálculo de la suma de comprobación (15_1) común, y el cálculo de la suma de comprobación (15_1) común a través de cada bloque de datos cifrados (35_1 a 35_n),

usándose solo datos de control dentro de los bloques de datos cifrados (35_1 a 35_n) para el cálculo de una suma de comprobación (15_1).

14. Procedimiento según la reivindicación 13, **caracterizado por** el siguiente paso de procedimiento:

- el enlace (S_3) de una máscara de bits (51_1 a 51_n) seleccionable libremente con el bloque de datos cifrados de la etapa de cifrado (30_1 a 30_n) a través de un Y lógico (50_1 a 50_n) por la unidad de selección (52_1 a 52_n) dentro de cada etapa de cifrado (30_1 a 30_n).

15. Procedimiento según la reivindicación 14, **caracterizado por** el siguiente paso de procedimiento:

- el uso (S_4) de un primer estado lógico en una posición de la máscara de bits (51_1 a 51_n) cuando el bit correspondiente en la misma posición dentro del bloque de datos cifrados (35_1 a 35_n) debe usarse para el cálculo de la suma de comprobación (15_1) común, y

el uso de un segundo estado lógico en una posición de la máscara de bits (51_1 a 51_n) cuando el bit correspondiente en la misma posición dentro del bloque de datos cifrados (35_1 a 35_n) no debe usarse para el cálculo de la suma de comprobación (15_1) común.

16. Procedimiento según las reivindicaciones 14 o 15, **caracterizado por** el siguiente paso de procedimiento:

- el ajuste (S_5) de las máscaras de bits (51_1 a 51_n) en la unidad de selección (52_1 a 52_n) de cada etapa de cifrado (30_1 a 30_n) de forma discrecional e independiente entre sí.

17. Procedimiento según una de las reivindicaciones 13 a 16, **caracterizado por** el siguiente paso de procedimiento:

- la exclusión (S_6) del cálculo de la suma de comprobación (15_1) común dentro del bloque de datos cifrados (35_1 a 35_n), por la unidad de selección (52_1 a 52_n), de los bits de datos que ya contengan una protección de integridad o que no necesiten ninguna protección de integridad.

18. Procedimiento según una de las reivindicaciones 13 a 17, **caracterizado porque** la unidad de autenticación y cifrado (6) trabaja según el principio del modo de contaje Galois.

19. Procedimiento según una de las reivindicaciones 13 a 18, **caracterizado por** el siguiente paso de procedimiento:

- la selección (S_7) de más bits de datos dentro del bloque de datos cifrados (35_1 a 35_n) para el cálculo de la suma de comprobación (15_1) por la unidad de selección (52_1 a 52_n), cuando una transmisión de los bloques de datos cifrados (35_1 a 35_n) presenta menos errores de transmisión y/o

la selección de menos bits de datos dentro del bloque de datos cifrados (35_1 a 35_n) para el cálculo de la suma de comprobación (15_1) por la unidad de selección (52_1 a 52_n), cuando una transmisión de los bloques de datos cifrados (35_1 a 35_n) presenta más errores de transmisión.

20. Procedimiento según una de las reivindicaciones 13 a 19, **caracterizado porque** las etapas de cifrado (30_1 a 30_n) individuales en el procedimiento están conectadas entre sí de tal forma que también a partir de bloques de datos claros (34_1 a 34_n) idénticos resultan después del cifrado bloques de datos cifrados (35_1 a 35_n) distintos.

21. Procedimiento según la reivindicación 20, **caracterizado por** el siguiente paso de procedimiento:

- el cifrado de un vector de inicialización (14_1 a 14_n) distinto por cada etapa de cifrado (30_1 a 30_n) con las mismas claves (32) y
el enlace de los bloques de datos claros (34_1 a 34_n) correspondientes con el vector de inicialización (14_1 a 14_n) cifrado con un enlace XOR, para generar a partir de ello los bloques de datos cifrados (35_1 a 35_n).

22. Procedimiento según una de las reivindicaciones 13 a 21, **caracterizado por** los siguientes pasos de procedimiento:

- la multiplicación de datos de autenticación (13) en una unidad de multiplicación (37) por un vector de campo de Galois y
el enlace de estos con un enlace XOR (38_1) con la salida de la unidad de selección (52_1) y la multiplicación del resultado en otra unidad de multiplicación (37) por un vector de campo de Galois adicional;
- la repetición del paso de procedimiento anterior hasta que se establece un enlace con un enlace XOR (38_n) con la salida de la unidad de selección (52_n) de la última etapa de cifrado (30_n) y
la multiplicación del resultado en otra unidad de multiplicación (37) con un vector de campo de Galois;
- el enlace del resultado de esta unidad de multiplicación (37) por medio de un enlace XOR (39) con el resultado de una concatenación (41) a partir de una longitud de bits de los datos de autenticación (13) y a partir de una longitud de bits del bloque de datos cifrados (35_1 a 35_n) y
la multiplicación del resultado del enlace XOR (39), en una unidad de multiplicación (37) adicional, por el vector de campo de Galois; y
- el enlace del resultado de esta unidad de multiplicación (37) con un enlace XOR (40) con un vector de inicialización (14_0) cifrado único, con lo que se calcula la suma de comprobación (15_1).

23. Procedimiento para un descifrado con una unidad de autenticación y descifrado (7) que presenta al menos una etapa de descifrado (29_1 a 29_n), con el siguiente paso de procedimiento:

- el descifrado (S_8) de un bloque de datos cifrados (35_1 a 35_n) dentro de cada etapa de descifrado (29_1 a 29_n), de manera que se genera un bloque de datos claros (34_1 a 34_n),
caracterizado por
- la selección (S_9) en una unidad de selección (52_1 a 52_n) dentro de cada etapa de descifrado (29_1 a 29_n), de qué bits de datos dentro de cada bloque de datos cifrados (35_1 a 35_n) se usan para el cálculo de la suma de comprobación (15_2) común, y el cálculo de la suma de comprobación (15_2) común a través de cada bloque de datos cifrados (35_1 a 35_n),
usándose únicamente datos de control dentro de los bloques de datos cifrados (35_1 a 35_n) para el cálculo de una suma de comprobación (15_2).

24. Procedimiento según la reivindicación 23, **caracterizado por** el siguiente paso de procedimiento:

- el cálculo de una suma de comprobación (15_2) que se compara con la suma de comprobación (15_1) recibida por la unidad de autenticación y cifrado (6).

25. Programa informático con medios de código de programa para poder realizar todos los pasos según una de las reivindicaciones 13 a 22 y/o 23 o 24, cuando el programa se ejecuta en un ordenador o un procesador de señales digital u otras unidades aritméticas electrónicas.

26. Producto de programa informático con medios de código de programa almacenados especialmente en un soporte legible por máquina, para poder realizar todos los pasos según una de las reivindicaciones 13 a 22 y/o 23 o 24 cuando el programa se ejecuta en un ordenador o en un procesador de señales digital u otras unidades aritméticas electrónicas.

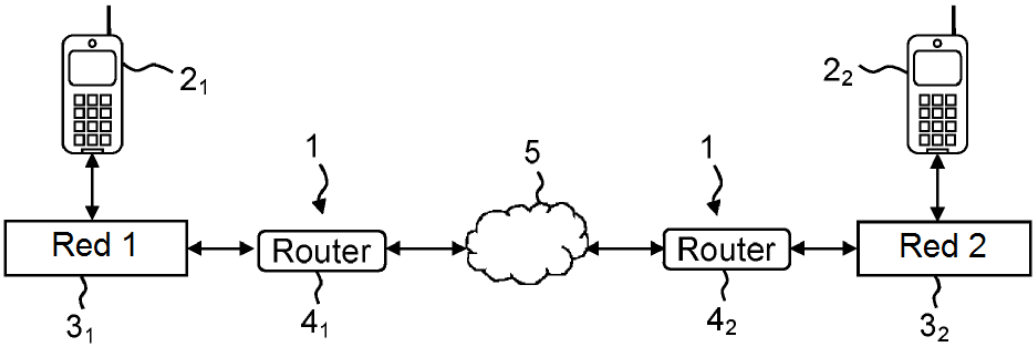


Fig. 1

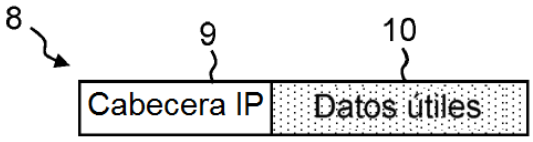


Fig. 2A

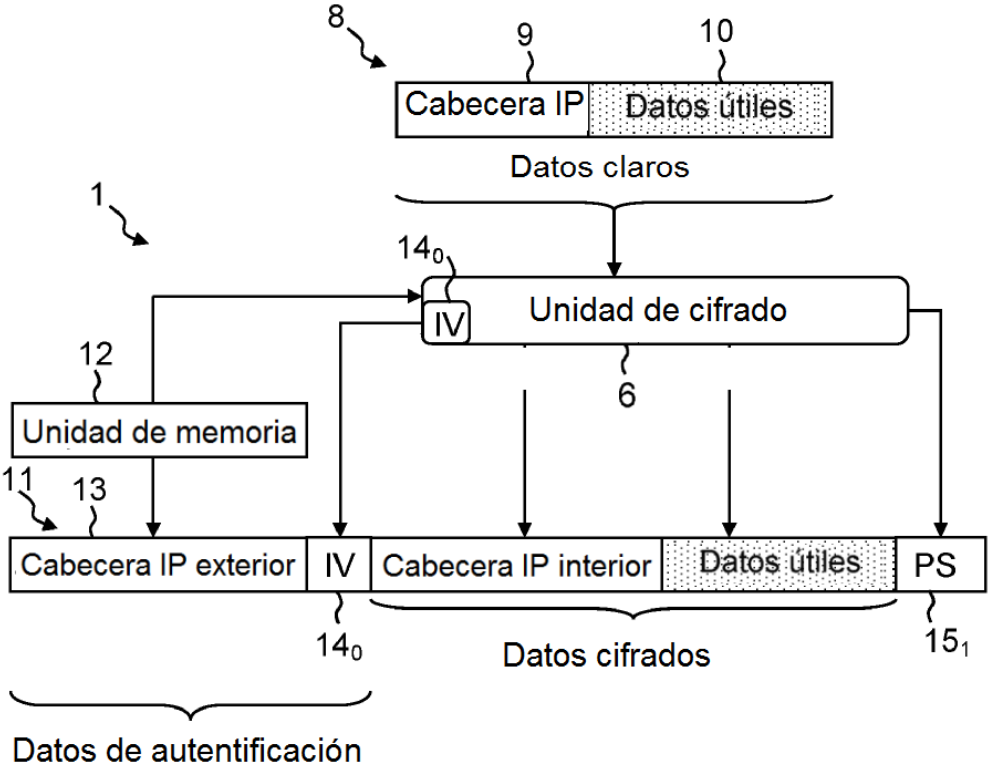


Fig. 2B

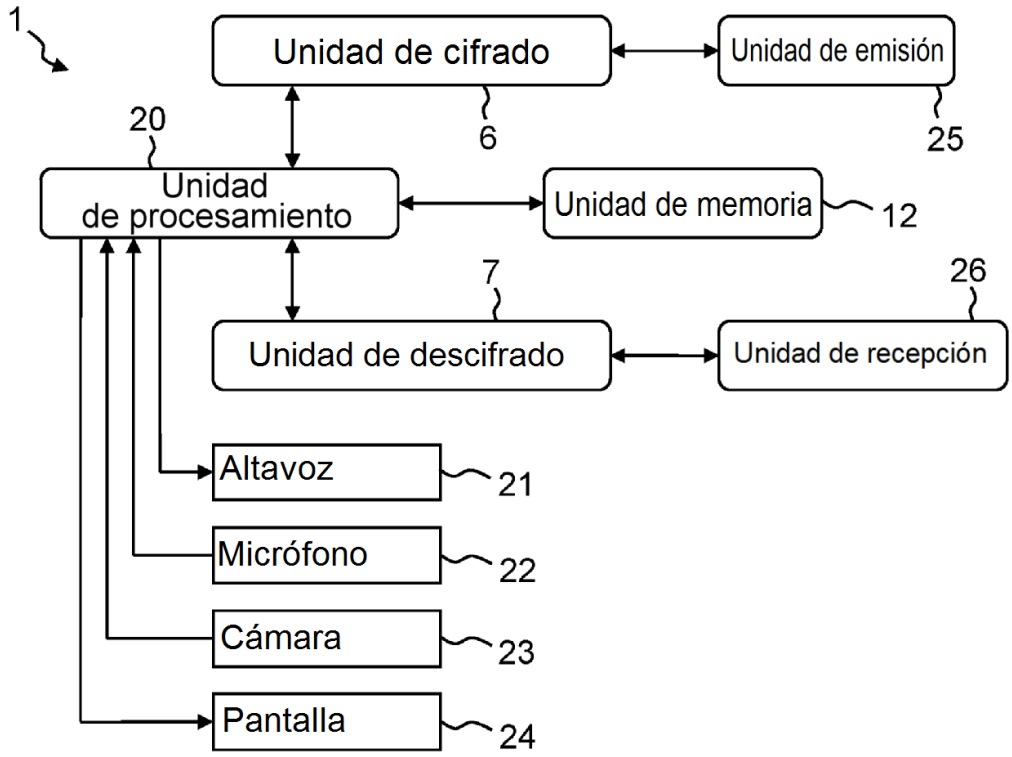

1
Unidad de cifrado
Unidad de emisión
6
25
20
Unidad
de procesamiento
Unidad de memoria
12
7
26
Unidad de descifrado
Unidad de recepción
Altavoz
21
Micrófono
22
Cámara
23
Pantalla
24

Fig. 3

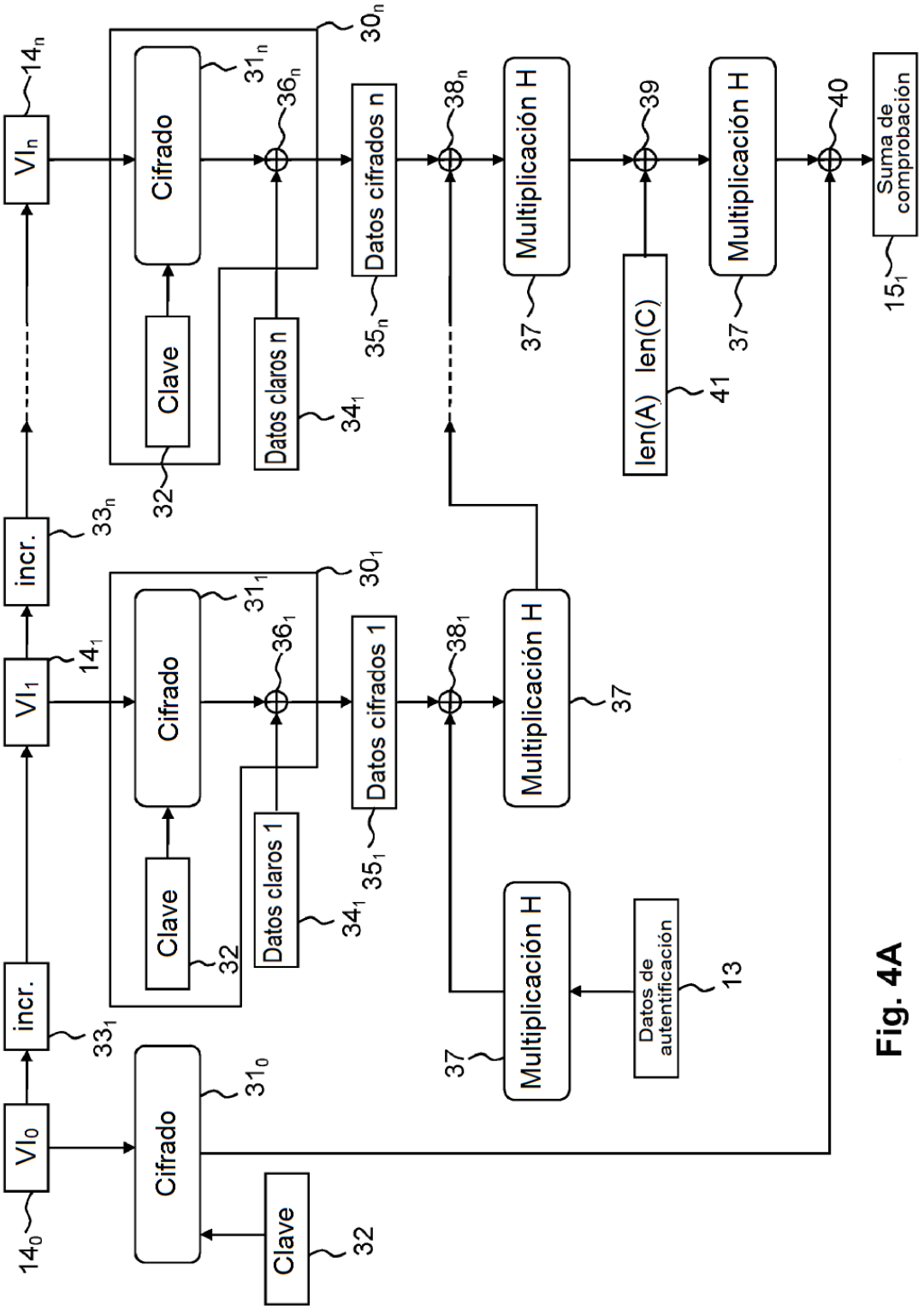

VI0
VI1
VIn
incr.
incr.
Cifrado
Cifrado
Cifrado
Clave
Clave
Clave
Datos claros 1
Datos claros n
Datos cifrados 1
Datos cifrados n
Multiplicación H
Multiplicación H
Multiplicación H
Multiplicación H
Datos de autentificación
len(A) len(C)
Suma de comprobación
14₀
14₁
14n
33₁
33n
31₀
31₁
31n
30₁
30n
32
32
32
34₁
34₁
35₁
35n
36₁
36n
37
37
37
37
38₁
38n
39
40
41
13
15₁

Fig. 4A

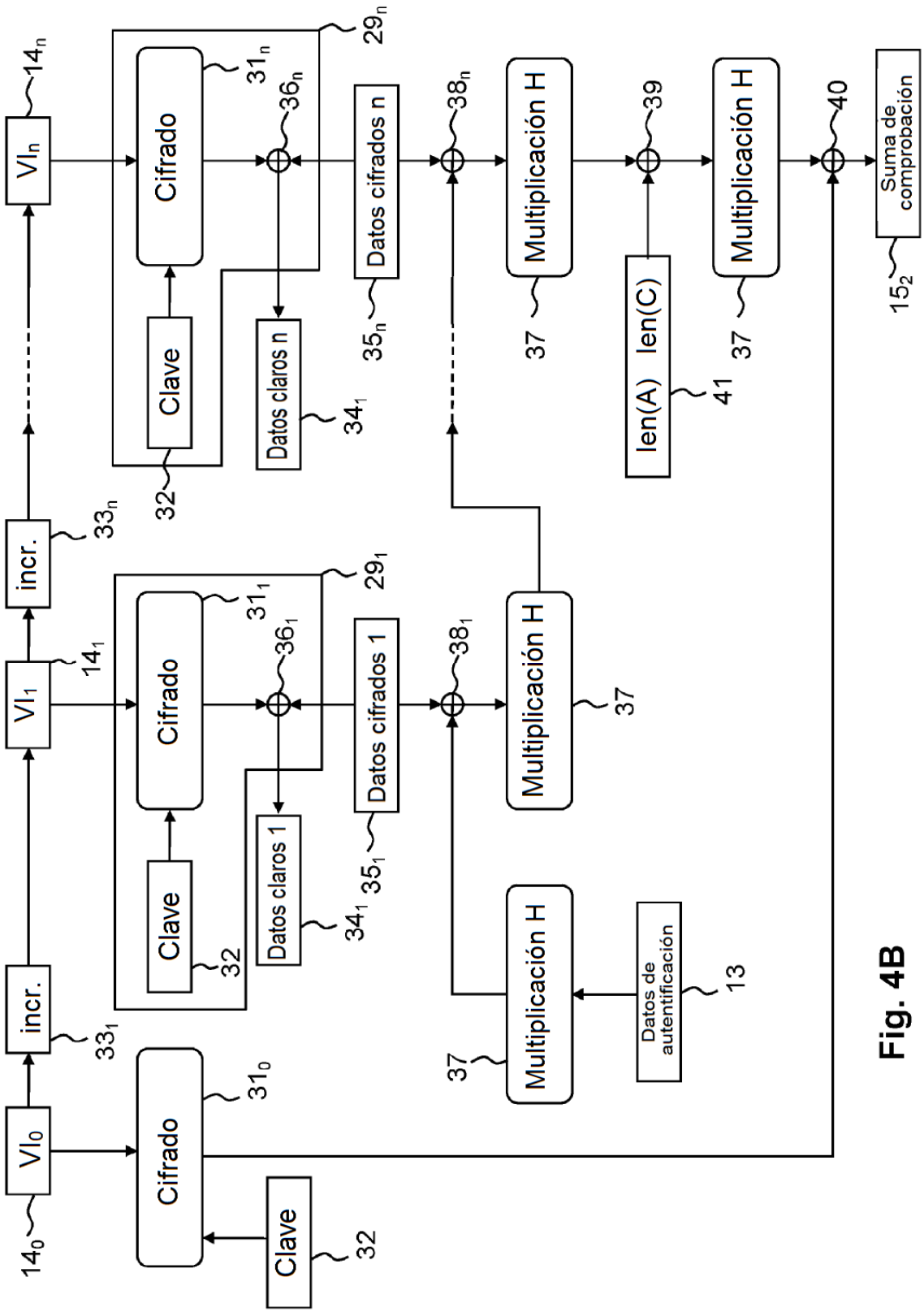
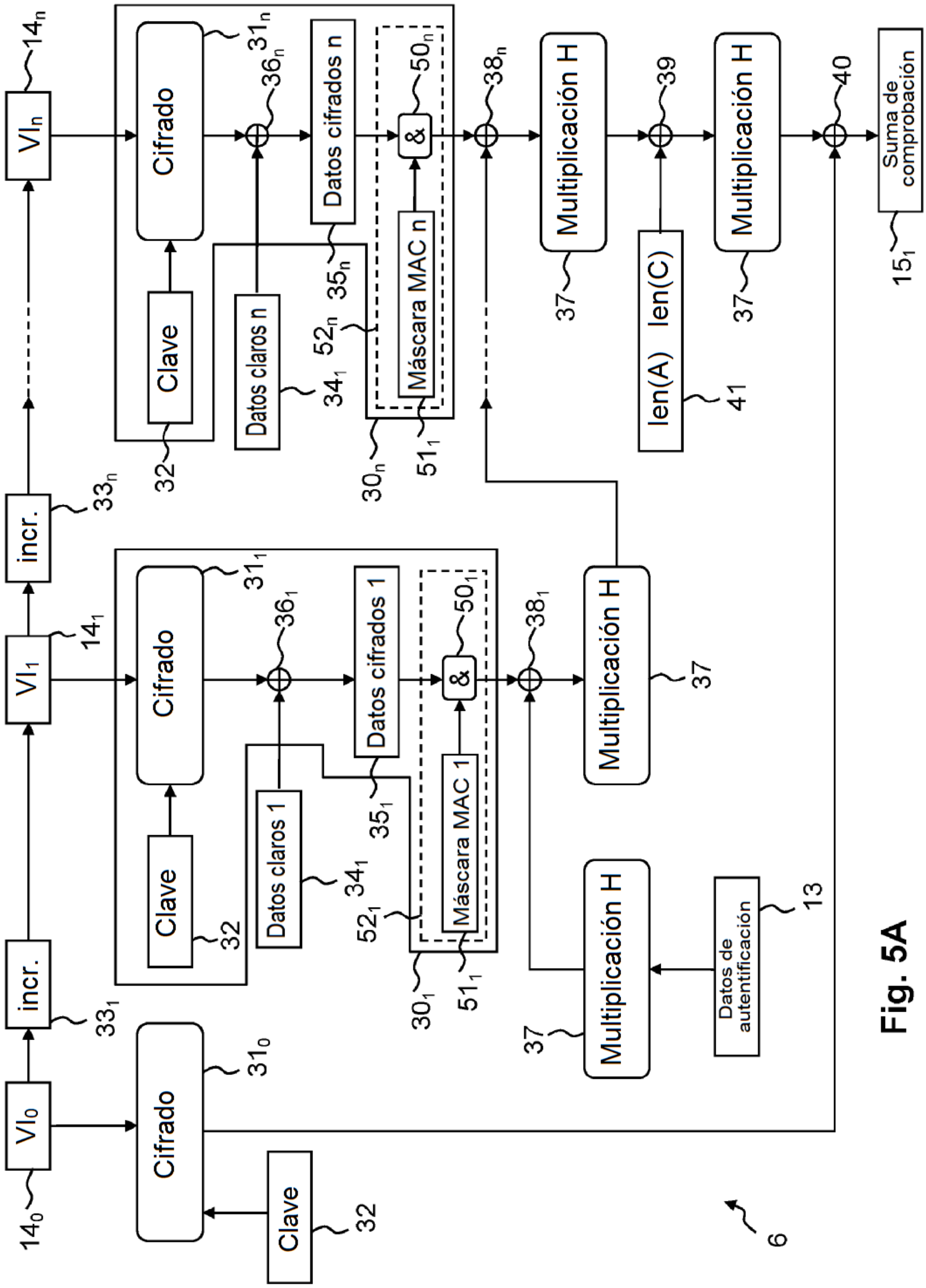
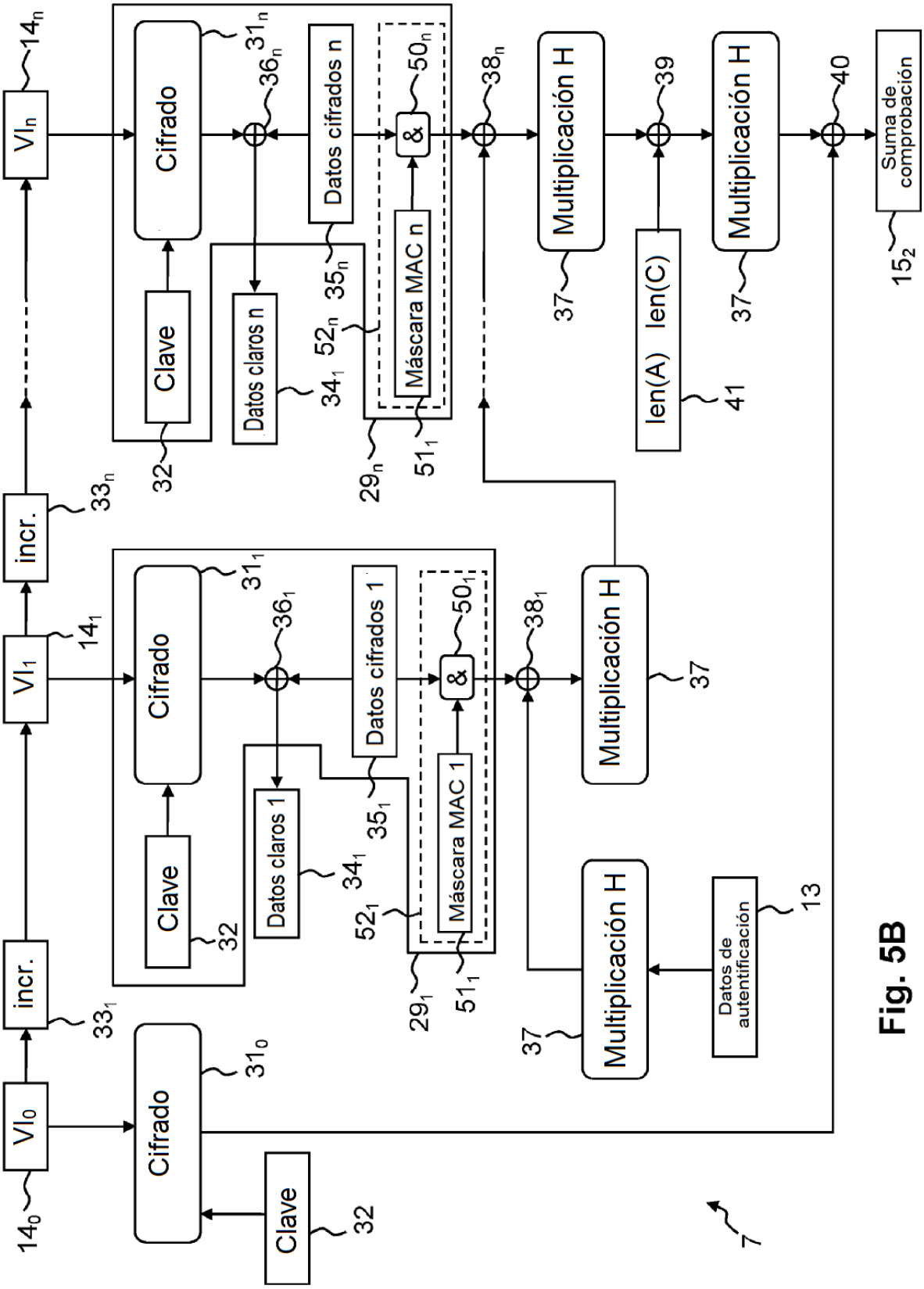

VI0
VI1
VIn
incr.
incr.
Cifrado
Cifrado
Cifrado
Clave
Clave
Clave
Datos claros 1
Datos claros n
Datos cifrados 1
Datos cifrados n
Multiplicación H
Multiplicación H
Multiplicación H
Multiplicación H
Datos de autentificación
len(A) len(C)
Suma de comprobación
14₀
14₁
14n
33₁
33n
31₀
31₁
31n
32
32
32
34₁
34₁
35₁
35n
36₁
36n
29₁
29n
37
37
37
37
38₁
38n
39
40
41
13
15₂

Fig. 4B



VI0
VI1
VIn
14
incr.
33
Cifrado
Clave
32
31
Datos claros 1
Datos claros n
34
Datos cifrados 1
Datos cifrados n
35
36
&
50
Máscara MAC 1
Máscara MAC n
51
52
30
38
Multiplicación H
37
Datos de autentificación
13
len(A)
len(C)
41
39
40
Suma de comprobación
15
6

Fig. 5A


VI0
VI1
VIn
incr.
Cifrado
Clave
32
Datos claros 1
Datos claros n
Datos cifrados 1
Datos cifrados n
Máscara MAC 1
Máscara MAC n
&
Multiplicación H
Datos de autentificación
len(A) len(C)
Suma de comprobación
7
Fig. 5B

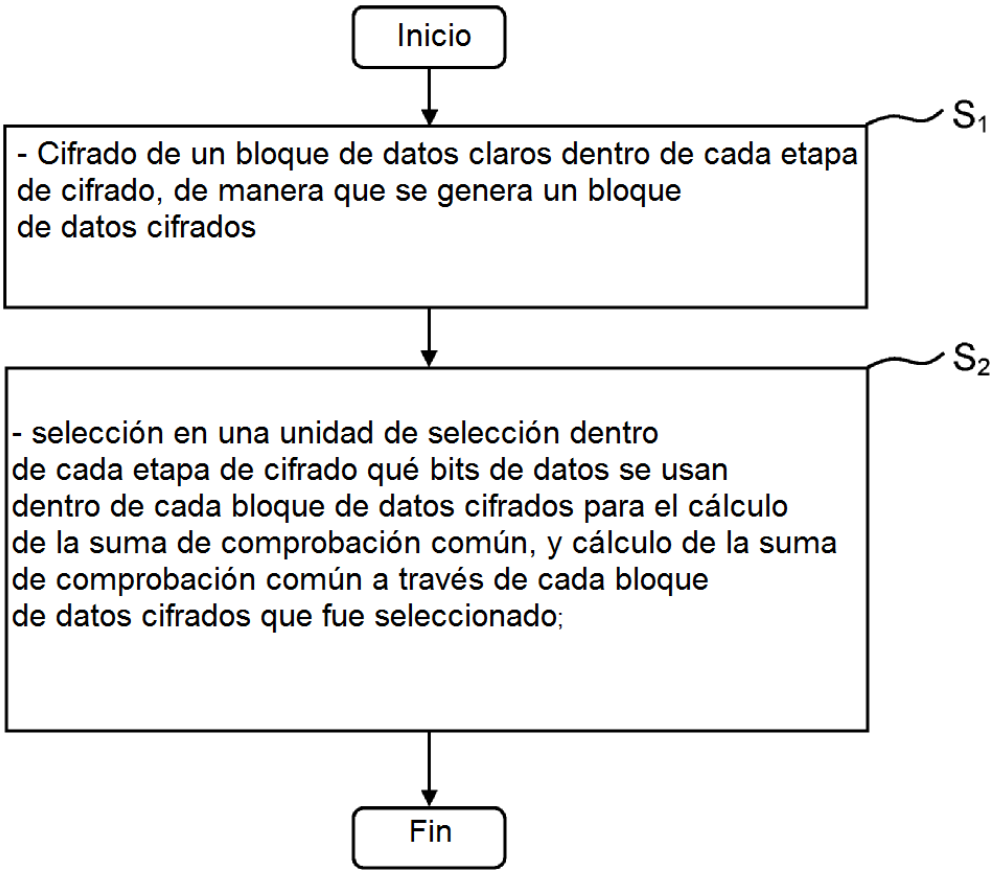

Inicio
S1
- Cifrado de un bloque de datos claros dentro de cada etapa de cifrado, de manera que se genera un bloque de datos cifrados
S2
- selección en una unidad de selección dentro de cada etapa de cifrado qué bits de datos se usan dentro de cada bloque de datos cifrados para el cálculo de la suma de comprobación común, y cálculo de la suma de comprobación común a través de cada bloque de datos cifrados que fue seleccionado;
Fin

Fig. 6

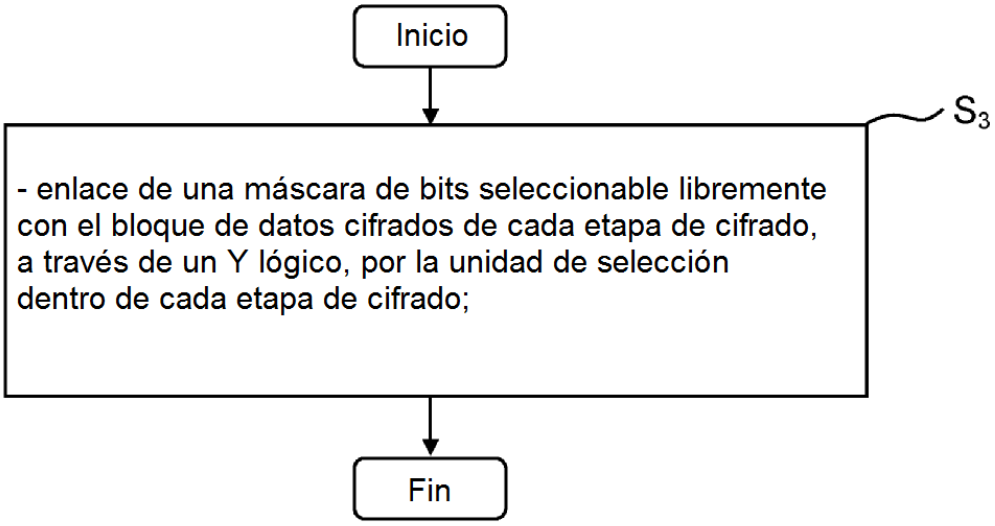

Inicio
S3
- enlace de una máscara de bits seleccionable libremente con el bloque de datos cifrados de cada etapa de cifrado, a través de un Y lógico, por la unidad de selección dentro de cada etapa de cifrado;
Fin

Fig. 7

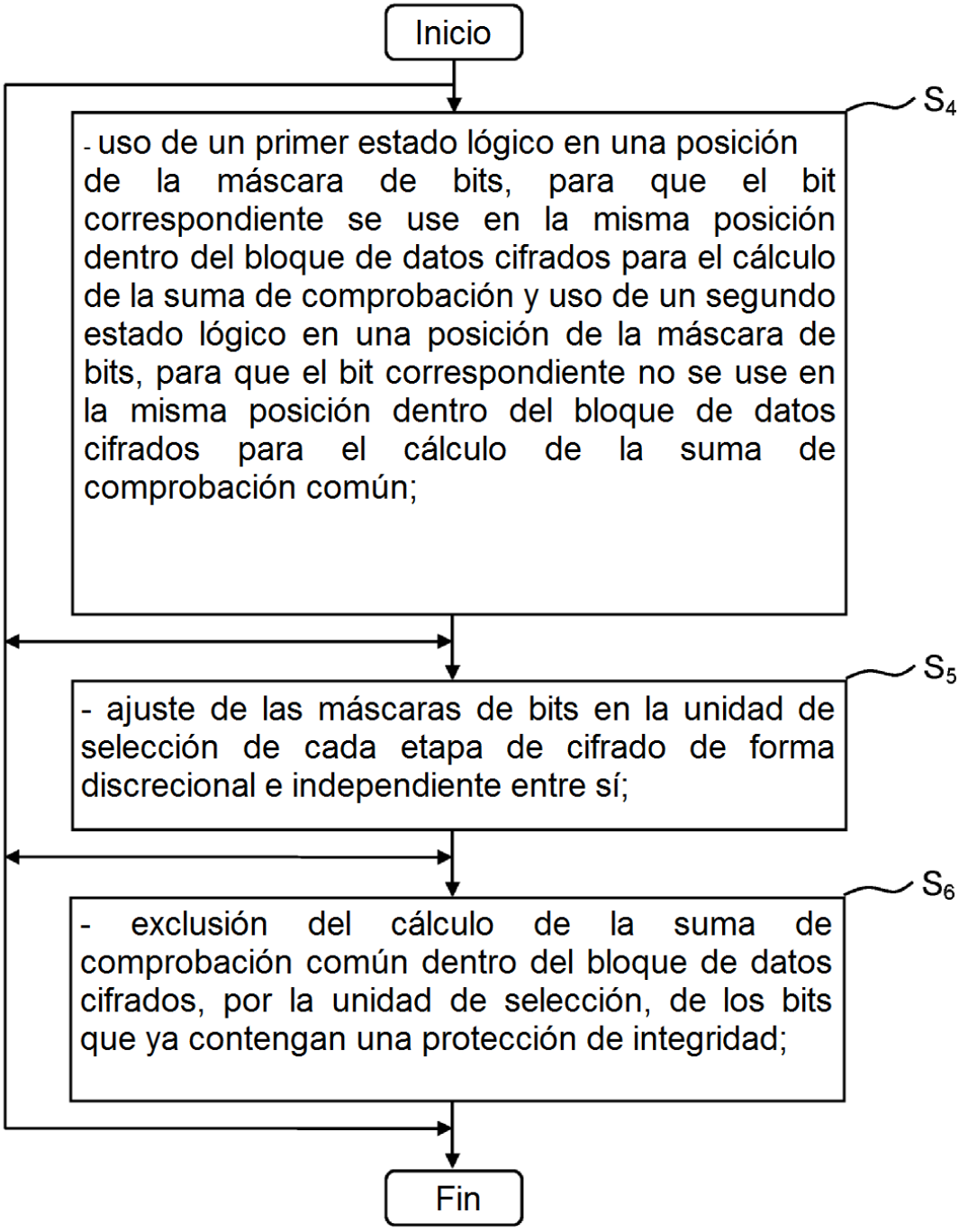

Inicio
S4
- uso de un primer estado lógico en una posición de la máscara de bits, para que el bit correspondiente se use en la misma posición dentro del bloque de datos cifrados para el cálculo de la suma de comprobación y uso de un segundo estado lógico en una posición de la máscara de bits, para que el bit correspondiente no se use en la misma posición dentro del bloque de datos cifrados para el cálculo de la suma de comprobación común;
S5
- ajuste de las máscaras de bits en la unidad de selección de cada etapa de cifrado de forma discrecional e independiente entre sí;
S6
- exclusión del cálculo de la suma de comprobación común dentro del bloque de datos cifrados, por la unidad de selección, de los bits que ya contengan una protección de integridad;
Fin

Fig. 8

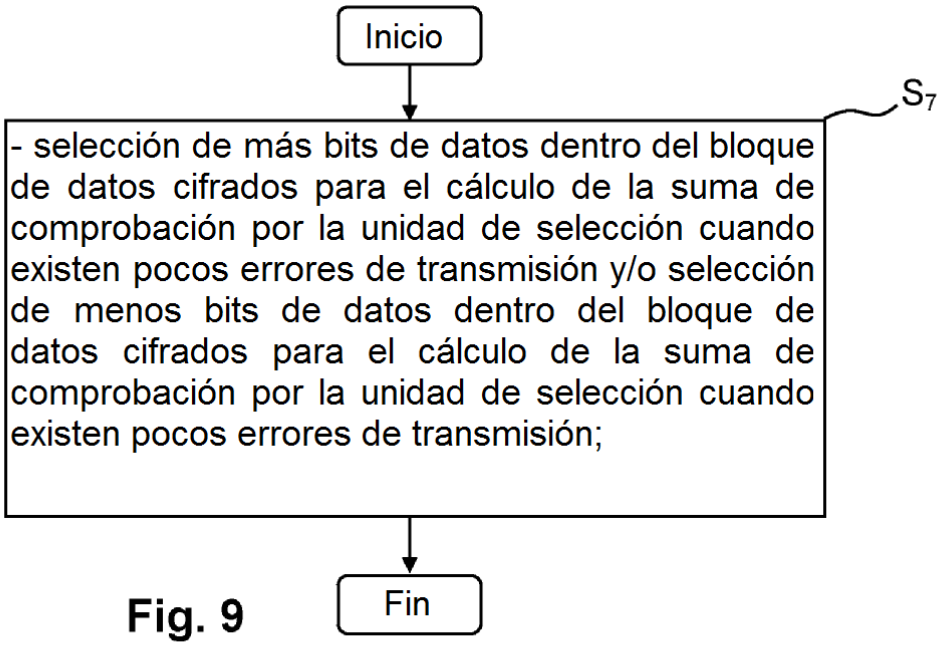

Inicio
S7
- selección de más bits de datos dentro del bloque de datos cifrados para el cálculo de la suma de comprobación por la unidad de selección cuando existen pocos errores de transmisión y/o selección de menos bits de datos dentro del bloque de datos cifrados para el cálculo de la suma de comprobación por la unidad de selección cuando existen pocos errores de transmisión;
Fin

Fig. 9

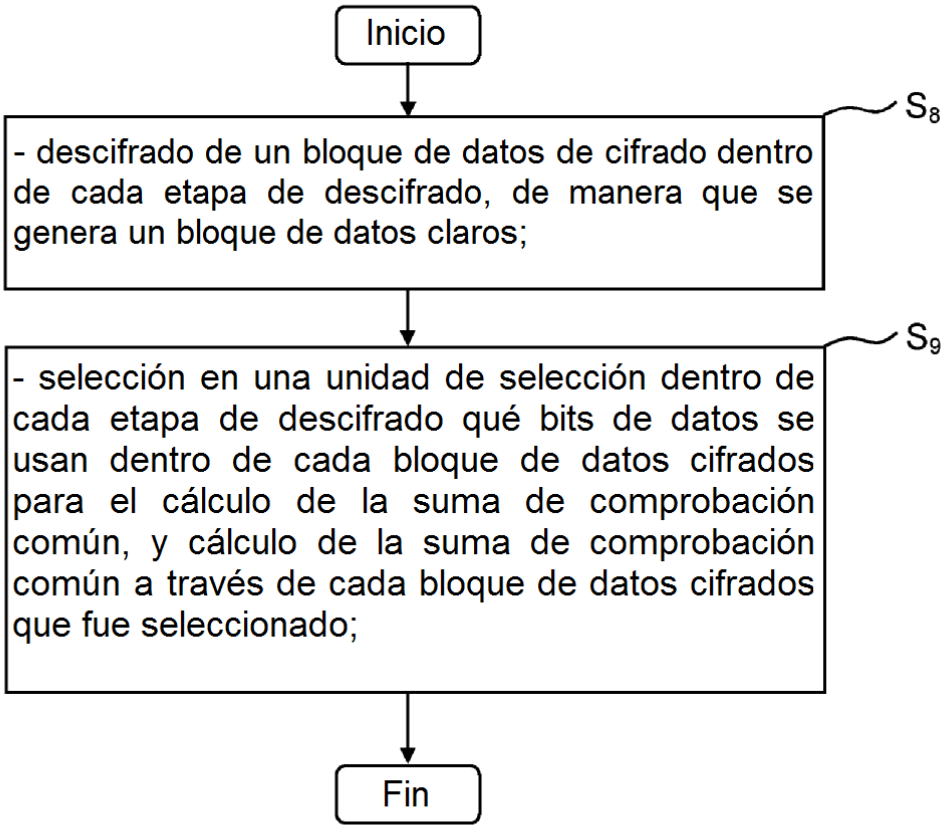

Inicio
S8
- descifrado de un bloque de datos de cifrado dentro de cada etapa de descifrado, de manera que se genera un bloque de datos claros;
S9
- selección en una unidad de selección dentro de cada etapa de descifrado qué bits de datos se usan dentro de cada bloque de datos cifrados para el cálculo de la suma de comprobación común, y cálculo de la suma de comprobación común a través de cada bloque de datos cifrados que fue seleccionado;
Fin

Fig. 10