(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 731 856**

(51) Int. CI.:

H04L 9/06 (2006.01)
H04L 9/32 (2006.01)
H04L 29/06 (2006.01)
H04W 12/10 (2009.01)
H04W 88/02 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **13.02.2014 PCT/US2014/016285**

(87) Fecha y número de publicación internacional: **28.08.2014 WO14130341**

(96) Fecha de presentación y número de la solicitud europea: **13.02.2014 E 14708382 (8)**

(97) Fecha y número de publicación de la concesión europea: **20.03.2019 EP 2959630**

(54) Título: **Autenticación de mensajes mediante una función hash universal calculada con multiplicación sin acarreo**

(30) Prioridad:

20.02.2013 US 201313771531

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
19.11.2019

(73) Titular/es:

QUALCOMM INCORPORATED (100.0%)
5775 Morehouse Drive
San Diego, CA 92121, US

(72) Inventor/es:

BRUMLEY, BILLY B. y
DENT, ALEXANDER W.

(74) Agente/Representante:

FORTEA LAGUNA, Juan José

DESCRIPCIÓN

Autenticación de mensajes mediante una función *hash* universal calculada con multiplicación sin acarreo

CAMPO TÉCNICO

[0001] La presente divulgación se refiere, en general, a sistemas de comunicación inalámbrica. Más específicamente, la presente divulgación se refiere a sistemas y procedimientos para la autenticación de mensajes utilizando una función *hash* universal con multiplicación sin acarreo.

ANTECEDENTES

[0002] Los sistemas de comunicación inalámbrica están ampliamente distribuidos para proporcionar diversos tipos de contenido de comunicación, tal como voz, vídeo, datos, etc. Estos sistemas pueden ser sistemas de acceso múltiple capaces de admitir una comunicación simultánea de múltiples dispositivos móviles con una o más estaciones base.

[0003] Para proporcionar seguridad adicional a las comunicaciones inalámbricas, se pueden utilizar técnicas de cifrado. El cifrado es el proceso de codificación de mensajes para evitar que los intrusos/piratas informáticos lean los mensajes y/o alteren el mensaje. Solo una parte autorizada puede descodificar los mensajes cifrados utilizando un algoritmo de descifrado. Incluso con las técnicas de cifrado/descifrado, pueden ser necesarias otras técnicas para proteger la integridad y autenticidad de un mensaje. Las soluciones de la técnica anterior se divulgan en los documentos: LONG HOANG NGUYEN ET AL: "On the construction of digest functions for manual authentication protocols [Sobre la creación de funciones de resumen para protocolos de autenticación manual]", ASOCIACIÓN INTERNACIONAL PARA LA INVESTIGACIÓN CRIPTOLÓGICA, vol. 20120404: 154833, 8 de marzo de 2011 (08-03-2011), páginas 1 a 24, XP061004718; y KAZUMARO AOKI ET AL: "The Security and Performance of GCM when Short Multiplications Are Used Instead [La seguridad y el rendimiento de GCM cuando se utilizan multiplicaciones cortas]", 28 de noviembre de 2012 (28-11-2012), SEGURIDAD DE LA INFORMACIÓN Y CRIPTOLOGÍA, SPRINGER BERLIN HEIDELBERG, BERLÍN, HEIDELBERG, PÁGINA(S) 225 - 245, XP047028051, ISBN : 978-3-642-38518-*6*. Pueden obtenerse beneficios mediante procedimientos mejorados de autenticación de mensajes cifrados.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

[0004]

La figura 1 muestra un sistema de comunicación inalámbrica con múltiples dispositivos inalámbricos;

la figura 2 es un diagrama de bloques que ilustra procedimientos de autenticación entre un dispositivo inalámbrico de transmisión y un dispositivo inalámbrico de recepción;

la figura 3 es un diagrama de flujo de un procedimiento que permite autenticar un mensaje de transmisión;

la figura 4 es un diagrama de flujo de un procedimiento de autenticación de un mensaje recibido;

la figura 5 es un diagrama de bloques que ilustra un módulo 128-EIA3 para su uso en los presentes sistemas y procedimientos;

la figura 6 es un diagrama de flujo de un procedimiento de cálculo de un código de autenticación de mensaje (MAC) utilizando un mensaje de entrada (M);

la figura 7 es un diagrama de bloques que ilustra el cálculo del código de autenticación de mensaje (MAC) utilizando multiplicación sin acarreo;

la figura 8 ilustra diversos componentes que pueden incluirse en un dispositivo de comunicación inalámbrica, y

la figura 9 ilustra ciertos componentes que pueden estar incluidos en una estación base.

DESCRIPCIÓN DETALLADA

[0005] La autenticación de mensajes se puede utilizar en las comunicaciones inalámbricas para proporcionar garantías de integridad y autenticidad para un mensaje transmitido de forma inalámbrica como se define en las reivindicaciones adjuntas. Esta autenticación de mensajes puede incluir generar un código de autenticación de mensaje (MAC) utilizando una función *hash* universal. La función *hash* universal actúa como una clave (en un flujo de claves) para autenticar el mensaje de entrada. Sin embargo, tal autenticación puede requerir un número significativo de instrucciones máquina. Al utilizar la multiplicación sin acarreo para calcular la función *hash* universal, el número de instrucciones máquina requeridas puede reducirse considerablemente, lo que da como resultado operaciones más eficientes. Esto puede a su vez mejorar el rendimiento del algoritmo de integridad. Además, el cálculo de la función

hash universal mediante la multiplicación sin acarreo puede ejecutarse en un tiempo de reloj que es independiente de los valores de bits de mensaje.

[0006] En la siguiente descripción, por razones de brevedad y claridad, se utiliza la terminología asociada con las normas LTE, promulgada en virtud del Proyecto de Asociación de Tercera Generación (3GPP) por la Unión Internacional de Telecomunicaciones (UIT). Cabe señalar que la invención también es aplicable a otras tecnologías, como las tecnologías y las normas asociadas relacionadas con el Acceso múltiple por división de código (CDMA), el Acceso múltiple por división de tiempo (TDMA), el Acceso múltiple por división de frecuencia (FDMA), el Acceso múltiple por división ortogonal de frecuencia (OFDMA), etc. Las terminologías asociadas con diferentes tecnologías pueden variar. Por ejemplo, dependiendo de la tecnología considerada, un dispositivo inalámbrico puede denominarse en algunas ocasiones equipo de usuario, estación móvil, terminal móvil, unidad de abonado, terminal de acceso, etc., por nombrar solo algunos ejemplos. Del mismo modo, una estación base puede denominarse en algunas ocasiones punto de acceso, Nodo B, Nodo B evolucionado, etc. Cabe señalar que diferentes terminologías se aplican a diferentes tecnologías cuando corresponda.

[0007] La figura 1 muestra un sistema de comunicación inalámbrica 100 con múltiples dispositivos inalámbricos. Los sistemas de comunicación inalámbrica 100 están ampliamente distribuidos para proporcionar diversos tipos de contenido de comunicación, tal como voz, datos, etc. Un dispositivo inalámbrico puede ser una estación base 102 o un dispositivo de comunicación inalámbrica 104. Tanto la estación base 102 como el dispositivo de comunicación inalámbrica 104 pueden configurarse para autenticar mensajes cifrados (por ejemplo, para proporcionar autenticación a los mensajes transmitidos y para obtener autenticación para mensajes recibidos). Durante la autenticación, una función *hash* universal puede calcularse utilizando multiplicación sin acarreo. El cálculo de la función *hash* universal mediante la multiplicación sin acarreo se describe con más detalle posteriormente en relación con la figura 5 y la figura 6.

[0008] Una estación base 102 es una estación que se comunica con uno o más dispositivos de comunicación inalámbrica 104. Una estación base 102 también puede denominarse como, y puede incluir parte de o toda la funcionalidad de, un punto de acceso, un transmisor de radiodifusión, un NodoB, un NodoB evolucionado, etc. En el presente documento se utilizará el término "estación base". Cada estación base 102 proporciona cobertura de comunicación para un área geográfica particular. Una estación base 102 puede proporcionar cobertura de comunicación para uno o más dispositivos de comunicación inalámbrica 104. El término "célula" puede referirse a una estación base 102 y/o a su área de cobertura, dependiendo del contexto en el que se use el término.

[0009] Las comunicaciones en un sistema inalámbrico (por ejemplo, un sistema de acceso múltiple) se pueden lograr a través de transmisiones mediante un enlace inalámbrico. Dicho enlace de comunicación puede establecerse a través de un sistema de única entrada y única salida (SISO), de múltiples entradas y única salida (MISO) o de múltiples entradas y múltiples salidas (MIMO). Un sistema MIMO incluye un(os) transmisor(es) y receptor(es) equipado(s), respectivamente, con múltiples (N_T) antenas de transmisión y múltiples (N_R) antenas de recepción para la transmisión de datos. Los sistemas SISO y MISO son ejemplos particulares de un sistema MIMO. El sistema MIMO puede proporcionar un rendimiento mejorado (por ejemplo, mayor caudal de tráfico, mayor capacidad o mejor fiabilidad) si se utilizan las dimensiones adicionales creadas por las múltiples antenas de transmisión y de recepción.

[0010] El sistema de comunicación inalámbrica 100 puede utilizar el sistema MIMO. Un sistema MIMO puede admitir sistemas de duplexación por división de tiempo (TDD) y duplexación por división de frecuencia (FDD). En un sistema TDD, las transmisiones de enlace ascendente y de enlace descendente están en la misma región de frecuencia de modo que el principio de reciprocidad permite la estimación del canal de enlace descendente a partir del canal de enlace ascendente. Esto permite a un dispositivo inalámbrico que transmite obtener una ganancia de formación de haces de transmisión de las comunicaciones recibidas por el dispositivo inalámbrico que transmite.

[0011] El sistema de comunicación inalámbrica 100 puede ser un sistema de acceso múltiple capaz de permitir una comunicación con múltiples dispositivos de comunicación inalámbrica 104 compartiendo los recursos de sistema disponibles (por ejemplo, ancho de banda y potencia de transmisión). Entre los ejemplos de dichos sistemas de acceso múltiple se incluyen sistemas de acceso múltiple por división de código (CDMA), sistemas de acceso múltiple por división de código de banda ancha (W-CDMA), sistemas de acceso múltiple por división de tiempo (TDMA), sistemas de acceso múltiple por división de frecuencia (FDMA), sistemas de acceso múltiple por división ortogonal de frecuencia (OFDMA), sistemas de acceso múltiple por división de frecuencia de única portadora (SC-FDMA), sistemas de Evolución a Largo Plazo (LTE) del Proyecto de Asociación de Tercera Generación (3GPP) y sistemas de acceso múltiple por división espacial (SDMA).

[0012] Los términos "redes" y "sistemas" se usan a menudo de forma intercambiable. Una red CDMA puede implementar una tecnología de radio, tal como el Acceso Radioeléctrico Terrestre Universal (UTRA), cdma2000, etc. El UTRA incluye W-CDMA y Baja Velocidad de Chip (LCR), mientras que cdma2000 abarca las normas IS-2000, IS-95 e IS-856. Una red de TDMA puede implementar una tecnología de radio tal como el Sistema Global de Comunicaciones Móviles (GSM). Una red OFDMA puede implementar una tecnología de radio tal como UTRA Evolucionado (E-UTRA), IEEE 802,11, IEEE 802.16, IEEE 802.20, Flash-OFDMA, etc. UTRA, E-UTRA y GSM son parte del Sistema Universal de Telecomunicaciones Móviles (UMTS). La Evolución a Largo Plazo (LTE) es una versión

de UMTS que usa E-UTRA. UTRA, E-UTRA, GSM, UMTS y Evolución a Largo Plazo (LTE) se describen en documentos de una organización denominada "Proyecto de Asociación de Tercera Generación" (3GPP). cdma2000 se describe en documentos de una organización denominada "Segundo Proyecto de Asociación de Tercera Generación" (3GPP2).

[0013] El Proyecto de Asociación de Tercera Generación (3GPP) es una colaboración entre grupos de asociaciones de telecomunicaciones que tiene como objetivo definir una especificación de telefonía móvil de tercera generación (3G) aplicable a nivel mundial. La Evolución a Largo Plazo (LTE) de 3GPP es un proyecto de 3GPP que tiene como objetivo mejorar la norma de telefonía móvil del Sistema Universal de Telecomunicaciones Móviles (UMTS). El 3GPP puede definir especificaciones para la próxima generación de redes móviles, sistemas móviles y dispositivos móviles.

[0014] En la Evolución a Largo Plazo (LTE) de 3GPP, un dispositivo de comunicación inalámbrica 104 puede denominarse "equipo de usuario" (UE). Un dispositivo de comunicación inalámbrica 104 también puede denominarse, y puede incluir parte de o toda la funcionalidad de, un terminal, un terminal de acceso, una unidad de abonado, una estación, etc. Un dispositivo de comunicación inalámbrica 104 puede ser un teléfono celular, un asistente personal digital (PDA), un dispositivo inalámbrico, un módem inalámbrico, un dispositivo portátil, un ordenador portátil, etc.

[0015] Un dispositivo de comunicación inalámbrica 104 puede comunicarse con ninguna, una o múltiples estaciones base 102 en el enlace descendente 106 y/o el enlace ascendente 108 en cualquier momento dado. El enlace descendente 106 (o enlace directo) se refiere al enlace de comunicación desde una estación base 102 hasta un dispositivo de comunicación inalámbrica 104, y el enlace ascendente 108 (o enlace inverso) se refiere al enlace de comunicación desde un dispositivo de comunicación inalámbrica 104 hasta una estación base 102.

[0016] Tanto el dispositivo de comunicación inalámbrica 104 como la estación base 102 pueden incluir un módulo de cifrado/descifrado 110a-b. Un módulo de cifrado/descifrado 110 puede permitir el cifrado y descifrado de mensajes enviados de forma inalámbrica entre el dispositivo de comunicación inalámbrica 104 y la estación base 102. Por ejemplo, el módulo de cifrado/descifrado 110a puede permitir que el dispositivo de comunicación inalámbrica 104 cifre un mensaje. El mensaje cifrado puede transmitirse entonces a través del enlace ascendente 108 a la estación base 102. La estación base 102 puede usar el módulo de cifrado/descifrado 110b para descifrar el mensaje.

[0017] Cuando se utilizan mensajes cifrados, se pueden usar procedimientos de autenticación para autenticar un mensaje y detectar falsificaciones. Los procedimientos de autenticación pueden incluir la inserción de la autenticación en un mensaje antes de la transmisión y la verificación de la autenticación de los mensajes recibidos. Un módulo de cifrado/descifrado 110 puede incluir un módulo 128-EIA3 112a-b. El módulo 128-EIA3 112 puede realizar procedimientos de autenticación para mensajes cifrados (por ejemplo, insertar la autenticación antes de la transmisión y obtener la autenticación para los mensajes recibidos) utilizando multiplicación sin acarreo. Por lo tanto, el módulo 128-EIA3 112 puede usar una función *hash* universal para el algoritmo de integridad que usa una función de multiplicación sin acarreo 139a-b. La función de multiplicación sin acarreo 139 se describe en mayor detalle posteriormente en relación con la figura 5 y la figura 6.

[0018] Dentro de la arquitectura de seguridad del sistema LTE, existen algoritmos normalizados para la confidencialidad y la integridad. Ya se han especificado dos conjuntos de algoritmos (128-EEA1/128-EIA1 y 128-EEA2/128-EIA2) (en la especificación de los algoritmos de confidencialidad e integridad de 3GPP; Documento 1: especificaciones f8 y f9; (3GPP TS35.201 versión 6) y Evolución de Arquitectura de Sistema (SAE); Arquitectura de Seguridad; (3GPP TS33.401 versión 9)). 128-EIA3 aplica un tercer algoritmo de integridad (es decir, autenticación) basado en un cifrado de flujo (ZUC). El algoritmo 128-EIA3 puede calcular un código de autenticación de mensaje (MAC) de 32 bits de un mensaje de entrada dado usando una clave de integridad (IK). Los algoritmos principales adoptados por el código de autenticación de mensaje (MAC) son *hash* universal y cifrado de flujo (ZUC). El algoritmo 128-EIA3 calcula por tanto el código de autenticación de mensaje (MAC) en software que requiere una instrucción OR exclusiva (XOR) de 32 bits por bit de mensaje.

[0019] La figura 2 es un diagrama de bloques que ilustra procedimientos de autenticación entre un dispositivo inalámbrico de transmisión 214a y un dispositivo inalámbrico de recepción 214b. El dispositivo inalámbrico de transmisión 214a puede ser un dispositivo de comunicación inalámbrico 104 o una estación base 102. El dispositivo inalámbrico de recepción 214b puede ser un dispositivo de comunicación inalámbrico 104 o una estación base 102. Los procedimientos de autenticación tanto en el dispositivo inalámbrico de transmisión 214a como en el dispositivo inalámbrico de recepción 214b pueden usar el algoritmo 128-EIA3.

[0020] El dispositivo inalámbrico de transmisión 214a puede obtener un mensaje de transmisión 218 (es decir, generando el mensaje de transmisión 218). En una configuración, un procesador en el dispositivo inalámbrico de transmisión 214a puede generar el mensaje de transmisión 218. El mensaje de transmisión 218 se puede proporcionar a un módulo 128-EIA3 212a. El módulo 128-EIA3 212a puede incluir una función de multiplicación sin acarreo 239a (que se describe a continuación en relación con la figura 5 y la figura 7). Usando el mensaje de transmisión 218, el módulo 128-EIA3 212a puede emitir un código de autenticación de mensaje (MAC) de transmisión 220a. Tanto el mensaje de transmisión 218 como el código de autenticación de mensaje (MAC) de transmisión 220a pueden proporcionarse a un transmisor 222. El transmisor 222 puede combinar el mensaje de transmisión 218 y el código de

autenticación de mensaje (MAC) de transmisión 220a para obtener un mensaje 224. El transmisor 222 puede entonces transmitir el mensaje 224 (junto con el código de autenticación (MAC) de mensaje de transmisión 220b).

[0021] El dispositivo inalámbrico de recepción 214b puede obtener el mensaje 224 (por ejemplo, al recibir el mensaje 224 usando un receptor 228). En una configuración, el dispositivo inalámbrico de recepción 214b puede obtener el mensaje 224 usando una antena. El receptor 228 puede extraer el código de autenticación de mensaje (MAC) de transmisión 220c a partir del mensaje 224. El receptor 228 puede proporcionar el código de autenticación de mensaje (MAC) de transmisión 220c a un módulo de autenticación 226. El receptor 228 también puede proporcionar el mensaje recibido 230 a un módulo 128-EIA3 212b. El módulo 128-EIA3 212b puede usar el mensaje recibido 230 para calcular un código de autenticación de mensaje (MAC) de recepción 220d. El módulo 128-EIA3 212b puede incluir una función de multiplicación sin acarreo 239b (que se describe posteriormente en relación con la figura 5 y la figura 7). El módulo 128-EIA3 212b puede proporcionar el código de autenticación de mensaje (MAC) de recepción 220d al módulo de autenticación 226. El módulo de autenticación 226 puede entonces comparar el código de autenticación de mensaje (MAC) de transmisión 220c y el código de autenticación de mensaje (MAC) de recepción 220d para determinar si el mensaje 224 recibido es auténtico.

[0022] Un algoritmo de código de autenticación de mensaje (MAC) (como el algoritmo 128-EIA3) también se puede denominar función *hash* con clave (criptográfica). Un algoritmo de código de autenticación de mensaje (MAC) puede aceptar como entrada una clave secreta y un mensaje de longitud arbitraria a autenticar (por ejemplo, el mensaje de transmisión 218 o el mensaje recibido 230) y emitir una etiqueta de código de autenticación de mensaje (MAC) 220. El uso de un algoritmo de código de autenticación de mensaje (MAC) puede proteger tanto la integridad de los datos como la autenticidad de un mensaje 224, ya que el dispositivo inalámbrico de recepción 214b puede detectar cualquier cambio en el contenido del mensaje (como falsificaciones).

[0023] La figura 3 es un diagrama de flujo de un procedimiento 300 que permite autenticar un mensaje de transmisión 218. El procedimiento 300 puede realizarse mediante un dispositivo inalámbrico de transmisión 214a (tal como una estación base 102 o un dispositivo de comunicación inalámbrica 104). El dispositivo inalámbrico de transmisión 214a puede generar 302 un mensaje de transmisión 218. El dispositivo inalámbrico de transmisión 214a puede aplicar 304 un algoritmo 128-EIA3 al mensaje de transmisión 218 para obtener un código de autenticación de mensaje (MAC) de transmisión 220a. El dispositivo inalámbrico de transmisión 214a puede transmitir 306 el mensaje de transmisión 218 y el código de autenticación de mensaje (MAC) de transmisión 220a en un único mensaje 224 a un dispositivo inalámbrico de recepción 214b.

[0024] La figura 4 es un diagrama de flujo de un procedimiento 400 para autenticar un mensaje recibido 224. El procedimiento 400 puede ser realizado por un dispositivo inalámbrico de recepción 214b (tal como una estación base 102 o un dispositivo de comunicación inalámbrica 104). El dispositivo inalámbrico de recepción 214b puede recibir 402 un mensaje 224 que incluye un código de autenticación de mensaje (MAC) de transmisión 220b. El dispositivo inalámbrico de recepción 214b puede extraer 404 el código de autenticación de mensaje (MAC) de transmisión 220c a partir del mensaje recibido 224. El dispositivo inalámbrico de recepción 214b puede aplicar 406 un algoritmo 128-EIA3 al mensaje recibido 230 para obtener un código de autenticación de mensaje (MAC) de recepción 220d. El dispositivo inalámbrico de recepción 214b puede comparar 408 el código de autenticación de mensaje (MAC) de recepción 220d con el código de autenticación de mensaje (MAC) de transmisión 220c para determinar una autenticación del mensaje 224. Por ejemplo, si el código de autenticación de mensaje (MAC) de recepción 220d es el mismo que el código de autenticación de mensaje (MAC) de transmisión 220c, el mensaje 224 puede considerarse auténtico. Como otro ejemplo, si el código de autenticación de mensaje (MAC) de recepción 220d es diferente del código de autenticación de mensaje (MAC) de transmisión 220c, el mensaje 224 puede considerarse no auténtico.

[0025] La figura 5 es un diagrama de bloques que ilustra un módulo 128-EIA3 512 para su uso en los presentes sistemas y procedimientos. El módulo 128-EIA3 512 de la figura 5 puede ser una configuración de los módulos 128-EIA3 112a-b de la figura 1. El módulo 128-EIA3 512 puede recibir un mensaje de entrada (M) 532 y emitir un código de autenticación de mensaje (MAC) 520 que se calcula utilizando el mensaje de entrada (M) 532, un flujo de claves 552 y una función *hash* universal H 535 que usa una función de multiplicación sin acarreo 539. El flujo de claves 552 se puede calcular utilizando un cifrado de flujo (ZUC) 544. El módulo 128-EIA3 512 puede por lo tanto aplicar un algoritmo 128-EIA3 al mensaje de entrada (M) 532 para obtener un código de autenticación de mensaje (MAC) 520 (y así proporcionar/obtener autenticación para el mensaje de entrada (M) 532).

[0026] El módulo 128-EIA3 512 puede incluir un contador CONTADOR 534 que es de 32 bits. El módulo 128-EIA3 512 también puede incluir una identidad de portadora PORTADORA 536 que es de 5 bits. El módulo 128-EIA3 512 puede incluir además la dirección de transmisión DIRECCIÓN 538, que es de 1 bit. El módulo 128-EIA3 512 también puede incluir una clave de integridad (IK) 540 que es de 128 bits. La LONGITUD 542 del mensaje de entrada (M) 532 puede ser de 32 bits (es decir, la LONGITUD 542 de 32 bits puede usar 32 bits para indicar la longitud del mensaje de entrada (M) 532). Por ejemplo, la LONGITUD 542 indica el número de bits del mensaje de entrada (M) 532 (entre 1 y 65.504 bits). El código de autenticación de mensaje (MAC) 520 generado por el módulo 128-EIA3 512 puede ser de 32 bits.

[0027] El módulo 128-EIA3 512 puede incluir una función *hash* universal H 535. La función *hash* universal H 535 se

refiere a una subrutina en el algoritmo 128-EIA3 que correlaciona grandes conjuntos de datos (es decir, el mensaje de entrada (M) 532) con conjuntos de datos más pequeños de longitud fija (es decir, el flujo de claves 552). La función *hash* universal H 535 se puede calcular utilizando una función de multiplicación sin acarreo 539. El uso de la función de multiplicación sin acarreo 539 puede permitir que el módulo 128-EIA3 calcule la función *hash* universal H 535 de manera más eficiente.

[0028] El módulo 128-EIA3 512 también puede incluir un cifrado de flujo (ZUC) orientado a palabras 544. El cifrado de flujo (ZUC) 544 puede tomar una clave inicial (CLAVE) de 128 bits 546 y un vector inicial (IV) de 128 bits 548 como entradas y generar un flujo de claves z[*i*] 552 de palabras de 32 bits (donde cada palabra de 32 bits se llama palabra clave). El número de palabras clave generadas por el cifrado de flujo (ZUC) 544 puede definirse por la variable L 550. El flujo de claves 552 se puede utilizar para el cifrado/descifrado. El cálculo del código de autenticación de mensaje (MAC) 520 utilizando el mensaje de entrada (M) 532 se describe a continuación en mayor detalle en relación con la figura 6 y la figura 7.

[0029] La Figura 6 es un diagrama de flujo de un procedimiento 600 para calcular un código de autenticación de mensaje (MAC) 520 utilizando un mensaje (M) de entrada 532. El procedimiento 600 puede ser realizado por un módulo 128-EIA3 512 en un dispositivo inalámbrico 214 tal como una estación base 102 o un dispositivo de comunicación inalámbrica 104.

[0030] El dispositivo inalámbrico 214 puede inicializar 602 la clave inicial (CLAVE) 546 e inicializar 604 el vector inicial (IV) 548 con la clave de integridad (IK) 540 y las variables de inicialización antes de la generación del flujo de claves 552. Cuando una variable se divide en varias subcadenas (como se usa en las siguientes ecuaciones), la subcadena más a la izquierda es [0], la siguiente subcadena más significativa es [1] y así sucesivamente hasta la subcadena menos significativa. El subíndice 2 (por ejemplo, 000_2) se usa para indicar un número en representación binaria. La notación *a* || *b* se utiliza para indicar la concatenación de subcadenas *a* y *b.* La notación $\lceil x \rceil$ se refiere al entero más pequeño, no menor que *x.*

[0031] La clave de integridad (IK) de 128 bits 540 se puede definir utilizando la ecuación (1):

$$IK = IK[0] \| IK[1] \| IK[2] \| ... \| IK[15] . \quad (1)$$

[0032] En la ecuación (1), *IK*[*i*] ($0 \leq i \leq 15$) son octetos. La clave inicial (CLAVE) de 128 bits 546 para el cifrado de flujo (ZUC) 544 se puede configurar mediante la ecuación (2):

$$CLAVE = CLAVE[0] \| CLAVE[1] \| CLAVE[2] \| ... \| CLAVE[15] . \quad (2)$$

[0033] En la ecuación (2), *CLAVE*[*i*] ($0 \leq i \leq 15$) son octetos. Por lo tanto, la clave inicial (CLAVE) 546 se puede inicializar 602 usando la ecuación (3):

$$CLAVE[i] = IK[i], i = 0,1,2,..., 15. \quad (3)$$

[0034] En la ecuación (3), cada subcadena de la clave inicial (CLAVE) 546 se establece igual a cada subcadena correspondiente de la clave de integridad (IK) 540. El contador CONTADOR de 32 bits 534 se puede definir mediante la ecuación (4):

$$CONTADOR = CONTADOR[0] \| CONTADOR[1] \| CONTADOR[2] \| CONTADOR[3] . \quad (4)$$

[0035] En la ecuación (4), *CONTADOR*[*i*], $i = 0,1,2,3$ son octetos. El vector inicial (IV) de 128 bits 548 se puede definir utilizando la ecuación (5):

$$IV = IV[0] \| IV[1] \| IV[2] \|... \| IV[15] . \quad (5)$$

[0036] En la ecuación (5), *IV*[*i*] ($0 \leq i \leq 15$) son octetos. Entonces, el vector inicial (IV) 548 puede inicializarse 604 utilizando la ecuación (6):

$$\begin{aligned} &IV[0] = CONTADOR[0], IV[1] = CONTADOR[1], \\ &IV[2] = CONTADOR[2], IV[3] = CONTADOR[3], \\ &IV[4] = PORTADORA \| 000_2, IV[5] = 00000000_2, \\ &IV[6] = 00000000_2, IV[7] = 00000000_2, \\ &IV[8] = IV[0] \oplus (DIRECCIÓN << 7), IV[9] = IV[1], \\ &IV[10] = IV[2], IV[11] = IV[3], \\ &IV[12] = IV[4], IV[13] = IV[5], \\ &IV[14] = IV[6] \oplus (DIRECCIÓN << 7), IV[15] = IV[7] \end{aligned} \quad (6)$$

[0037] En la ecuación (6), $\oplus$ se refiere a una operación OR exclusiva y *a « t se* refiere a un desplazamiento a la izquierda en *t* bits de números enteros *a*. Por lo tanto, *DIRECCIÓN* << 7 se refiere a desplazar 7 bits a la izquierda la

DIRECCIÓN 538.

[0038] El dispositivo inalámbrico 214 puede entonces generar 606 el flujo de claves 552. En una configuración, el flujo de claves 552 puede ser generada por un procesador en el dispositivo inalámbrico 214. En otra configuración, el flujo de claves 552 se puede generar usando la memoria en el dispositivo inalámbrico 214. El cifrado de flujo (ZUC) 544 puede generar un flujo de claves 552 con L palabras clave 550, donde $L = \left\lceil \frac{LONGITUD}{32} \right\rceil + 2\ palabras$. el flujo de claves 552 se puede denotar como $z[0], z[1],..., z[32 \times (L - 1)]$, donde $z[0]$ es el bit más significativo de la primera palabra de salida de la secuencia el cifrado (ZUC) 544 y z[31] es el bit menos significativo. Para cada $i = 0,1,2,...,32\times(L -1)$, se puede aplicar la ecuación (7):

$$z_i = z[i] \| z[i+1] \| ... \| z[i+31] . \quad (7)$$

[0039] Por lo tanto, cada z_i del flujo de claves 552 es una palabra de 32 bits. El dispositivo inalámbrico 214 puede entonces calcular 608 la función *hash* universal antes de calcular el código de autenticación de mensaje (MAC) 520. T puede definirse como una palabra de 32 bits. T puede establecerse inicialmente igual a 0. Para cada $i = 0,1,2,...,$ *LONGITUD*-1, si $M[i] = 1$, se aplica la ecuación (8):

$$T = T \oplus z_i . \quad (8)$$

[0040] La ecuación (8) se puede denominar función *hash* universal H. Sin embargo, la ecuación (8) es tediosa (ya que el cálculo de la función *hash* universal H debe realizarse para cada bit individual en el mensaje de entrada (M) 532). En su lugar, se puede usar una multiplicación sin acarreo para procesar 32 bits a la vez del mensaje de entrada (M) 532 para calcular 608 de manera eficiente la función *hash* universal H.

[0041] En la multiplicación sin acarreo, los polinomios se multiplican. Una iteración de multiplicación sin acarreo puede reemplazar 32 iteraciones de la ecuación (8). Una multiplicación sin acarreo CLMUL (F,G) toma como entrada una palabra F de 32 bits y una palabra G de 32 bits y genera una palabra E de 64 bits, donde los bits de F y G se toman como coeficientes (de grado máximo 31) de polinomios en GF(2)[x] y donde E es el producto polinomial resultante (de grado máximo 62) en GF(2)[x]. Este concepto puede aplicarse a todas las funciones de multiplicación sin acarreo para cualquier tamaño de palabra wlog dado. Para simplificar, se puede suponer que el tamaño de palabra wlog es un entero divisible por 32.

[0042] Para calcular la función *hash* universal H mediante la multiplicación sin acarreo, la palabra T de 32 bits se puede fijar primero a 0. Una palabra de 32 bits del mensaje de entrada (M) 532 $M_i...M_j$, donde $j = i + 31$, puede invertirse de acuerdo con la ecuación (9):

$$r0 = M_j...M_i . \quad (9)$$

[0043] Se puede encontrar una primera palabra E de 64 bits utilizando la ecuación (10):

$$E = CLMUL(r0,Z\_i...Z\_j) . \quad (10)$$

[0044] En la ecuación (10), *Z_ i... Z_j se* refiere a los bits del flujo de claves 552 y *CLMUL* se refiere a la función de multiplicación sin acarreo, que está cada vez más presente en los procesadores comerciales modernos. Una segunda palabra F de 64 bits se puede encontrar usando la ecuación (11):

$$F = CLMUL(r0,Z\_k...Z\_l) . \quad (11)$$

[0045] En la ecuación (11), $k = j + 1$ y $l = k + 31$ (por lo tanto, la palabra de 32 bits *Z_k... Z_l* sigue inmediatamente la palabra de 32 bits *Z_i... Z_ j*). La variable *m* se puede fijar a la palabra de 32 bits más baja de E. La variable n se puede fijar a la palabra de 32 bits más alta de F. La ecuación (12) se puede realizar entonces:

$$r1 = m \oplus n . \quad (12)$$

[0046] Entonces, la función *hash* universal se calcula 608 utilizando la ecuación (13):

$$T = T \oplus r1 . \quad (13)$$

[0047] Entonces, el código de autenticación de mensaje (MAC) de salida 520 se calcula 610 de acuerdo con la ecuación (14):

$$MAC = T \oplus z_{32(L-1)} . \quad (14)$$

[0048] El coste, en instrucciones máquina, por cada 32 bits del mensaje puede ser fijo. En procedimientos anteriores para la especificación 128-EIA3, se requiere al menos una instrucción (es decir, una XOR condicional) por bit de

mensaje. Por lo tanto, se requieren 32 instrucciones por cada 32 bits de mensaje. Usar una multiplicación sin acarreo para calcular 608 la función *hash* requiere 5 instrucciones por cada 32 bits de mensaje: una inversión de bit de una palabra, dos multiplicaciones sin acarreo y dos XOR. Al usar una multiplicación sin acarreo para calcular 608 la función *hash* universal se reduce significativamente el número de instrucciones máquina necesarias para evaluar la función *hash* H. Esto mejora el rendimiento del algoritmo de integridad 128-EIA3 de LTE. Además, el uso de una multiplicación sin acarreo para calcular 608 la función *hash* universal se ejecuta en un tiempo de reloj que es independiente de los valores de bit de mensaje (la solución existente depende de los valores de bit de mensaje, ya que la ecuación (8) solo se aplica cuando un bit de mensaje = 1). Por lo tanto, al usar la multiplicación sin acarreo para calcular 608 la función *hash* universal se puede proporcionar protección adicional contra una gran variedad de ataques de canal lateral, como los ataques de análisis de tiempo y de potencia, lo que mejora la seguridad física del sistema. Un tiempo de ejecución de reloj de la multiplicación sin acarreo puede ser independiente del peso de Hamming de los operandos, lo que aumenta la seguridad del canal lateral.

[0049] La figura 7 es un diagrama de bloques que ilustra el cálculo del código de autenticación de mensaje (MAC) 220 utilizando la multiplicación sin acarreo. En una configuración, el código de autenticación de mensaje (MAC) 220 se puede calcular utilizando un procesador y/o una memoria en un dispositivo inalámbrico 214. Se recibe una palabra de 32 bits del mensaje de entrada (M) 732 $M_i...M_{i+31}$. Como se describe en la ecuación (9), los bits en el mensaje de entrada (M) 732 pueden invertirse 754 para formar $M_{i+32}...M_i$. Los bits en el mensaje de entrada (M) 732 pueden invertirse correlacionando las palabras del mensaje de entrada (M) 732 con su representación en el anillo de polinomios.

[0050] Los bits de mensaje invertidos $M_{i+32}...M_i$ pueden proporcionarse entonces a una primera etapa de multiplicación sin acarreo 752a y a una segunda etapa de multiplicación sin acarreo 752b. Cada una de las etapas de multiplicación sin acarreo 752 puede ser una función de multiplicación sin acarreo 739a-b. Como se describe en la ecuación (10) anterior, se proporcionan 32 bits del flujo de claves 752a $Z_i...Z_{i+31}$ a la primera etapa de multiplicación sin acarreo 752a para formar la primera palabra E de 64 bits. Del mismo modo, 32 bits del flujo de claves 752b $Z_{i+32}...Z_{i+63}$ se proporcionan a la segunda etapa de multiplicación sin acarreo 752b para formar la segunda palabra F de 64 bits (como se describe en la ecuación (11) anterior).

[0051] La primera palabra E de 64 bits se puede separar en una palabra de 32 bits más altos y una palabra de 32 bits más bajos. Del mismo modo, la segunda palabra F de 64 bits se puede separar en una palabra de 32 bits más altos y una palabra de 32 bits más bajos. La palabra de 32 bits más bajos de la primera palabra E de 64 bits se puede denotar como la variable *m*. La palabra de 32 bits más altos de la segunda palabra F de 64 bits se puede denotar como la variable n. Una OR exclusiva (XOR) 756 se puede realizar entonces entre *m* y *n,* como se describe anteriormente en la ecuación (12). La función *hash* universal T 735 se calcula entonces de acuerdo con la ecuación (13) anterior.

[0052] La figura 8 muestra parte de una implementación de hardware de un dispositivo de comunicación inalámbrica 804 para ejecutar los esquemas o procesos como se describió anteriormente. El dispositivo de comunicación inalámbrica 804 comprende un sistema de circuitos como se describe a continuación. En esta memoria descriptiva y en las reivindicaciones adjuntas, debe quedar claro que el término "sistema de circuitos" se interpreta como un término estructural y no como un término funcional. Por ejemplo, el sistema de circuitos puede ser un conjunto de componentes de circuito, tal como una multiplicidad de componentes de circuito integrado, en forma de celdas de procesamiento y/o memoria, unidades, bloques y similares, como se muestra y describe en la figura 8.

[0053] El dispositivo de comunicación inalámbrica 804 incluye un bus de datos central 883 que enlaza varios circuitos entre sí. Los circuitos incluyen una CPU (unidad central de procesamiento) o un controlador 885, un circuito de recepción 881, un circuito de transmisión 873 y una memoria 879.

[0054] El circuito de recepción 881 y el circuito de transmisión 873 pueden estar conectados a un circuito de RF (radiofrecuencia) (no mostrado en el dibujo). El circuito de recepción 881 procesa y almacena temporalmente las señales recibidas antes de enviar las señales al bus de datos 883. Por otro lado, el circuito de transmisión 873 procesa y almacena temporalmente los datos del bus de datos 883 antes de enviar los datos desde el dispositivo de comunicación 804. La CPU/el controlador 885 realiza la función de gestión de datos del bus de datos 883 y además la función de procesamiento general de datos, que incluye ejecutar los contenidos de instrucción de la unidad de memoria 879.

[0055] La unidad de memoria 879 incluye un conjunto de módulos y/o instrucciones representados de manera genérica con el número de referencia 875. En este modo de realización, los módulos/instrucciones incluyen, entre otras cosas, un *hash* universal que utiliza una función de multiplicación sin acarreo 877 que lleva a cabo los esquemas y procesos descritos anteriormente. La función 877 incluye instrucciones de ordenador o código para ejecutar las etapas de proceso mostradas y descritas en las figuras 1 a 6. Instrucciones específicas particulares de una entidad pueden implementarse de manera selectiva en la función 877.

[0056] En este modo de realización, la unidad de memoria 879 es una RAM (memoria de acceso aleatorio). Las funciones a modo de ejemplo, tales como la función 877, incluyen una o más rutinas de software, módulos y/o

conjuntos de datos. La unidad de memoria 879 puede vincularse a otro circuito de memoria (no mostrado) que puede ser volátil o no volátil. Como alternativa, la unidad de memoria 879 puede estar compuesta por otros tipos de circuitos, tales como una EEPROM (memoria de solo lectura programable y borrable eléctricamente), una EPROM (memoria de solo lectura programable eléctrica), una ROM (memoria de solo lectura), un ASIC (circuito integrado específico de la aplicación), un disco magnético, un disco óptico y otros bien conocidos en la técnica.

[0057] La figura 9 muestra parte de una implementación en hardware de una estación base 902 para ejecutar los esquemas o procesos descritos anteriormente. La estación base 902 comprende un sistema de circuitos como el descrito a continuación. En esta memoria descriptiva y en las reivindicaciones adjuntas, debe quedar claro que el término "sistema de circuitos" se interpreta como un término estructural y no como un término funcional. Por ejemplo, el sistema de circuitos puede ser un conjunto de componentes de circuito, tal como una multiplicidad de componentes de circuito integrado, en forma de celdas de procesamiento y/o memoria, unidades, bloques y similares, como se muestra y describe en la figura 9.

[0058] La estación base 902 incluye un bus de datos central 983 que enlaza varios circuitos entre sí. Los circuitos incluyen una CPU (unidad central de procesamiento) o un controlador 985, un circuito de recepción 981, un circuito de transmisión 973 y una memoria 979.

[0059] El circuito de recepción 981 y el circuito de transmisión 973 pueden estar conectados a un circuito de RF (radiofrecuencia) (no mostrado en el dibujo). El circuito de recepción 981 procesa y almacena temporalmente las señales recibidas antes de enviar las señales al bus de datos 983. Por otro lado, el circuito de transmisión 973 procesa y almacena temporalmente los datos del bus de datos 983 antes de enviar los datos desde la estación base 902. La CPU/el controlador 985 realiza la función de gestión de datos del bus de datos 983 y además la función de procesamiento general de datos, que incluye ejecutar los contenidos de instrucción de la unidad de memoria 979.

[0060] La unidad de memoria 979 incluye un conjunto de módulos y/o instrucciones representados de manera genérica con el número de referencia 975. En este modo de realización, los módulos/instrucciones incluyen, entre otras cosas, un *hash* universal que utiliza una función de multiplicación sin acarreo 977 que lleva a cabo los esquemas y procesos descritos anteriormente. La función 977 incluye instrucciones de ordenador o código para ejecutar las etapas de proceso mostradas y descritas en las figuras 1 a 6. Instrucciones específicas particulares de una entidad pueden implementarse de manera selectiva en la función 977.

[0061] En este modo de realización, la unidad de memoria 979 es una RAM (memoria de acceso aleatorio). Las funciones a modo de ejemplo, tales como la función 977, incluyen una o más rutinas de software, módulos y/o conjuntos de datos. La unidad de memoria 979 puede vincularse a otro circuito de memoria (no mostrado) que puede ser volátil o no volátil. Como alternativa, la unidad de memoria 979 puede estar compuesta por otros tipos de circuitos, tales como una EEPROM (memoria de solo lectura programable y borrable eléctricamente), una EPROM (memoria de solo lectura programable eléctrica), una ROM (memoria de solo lectura), un ASIC (circuito integrado específico de la aplicación), un disco magnético, un disco óptico y otros bien conocidos en la técnica.

[0062] El término "determinar" abarca una amplia variedad de acciones y, por lo tanto, "determinar" puede incluir calcular, computar, procesar, obtener, investigar, consultar (por ejemplo, consultar una tabla, una base de datos u otra estructura de datos), verificar y similares. Además, "determinar" puede incluir recibir (por ejemplo, recibir información), acceder, (por ejemplo, acceder a datos de una memoria) y similares. Asimismo, "determinar" puede incluir resolver, seleccionar, elegir, establecer y similares.

[0063] La expresión "en función de/basándose en" no significa "en función de únicamente/basándose únicamente en", a menos que se especifique expresamente lo contrario. Dicho de otro modo, la expresión "en función de/basándose en" describe tanto "en función de únicamente/basándose únicamente en" como "en función de al menos/basándose al menos en".

[0064] Ningún elemento de reivindicación debe interpretarse según las provisiones del artículo 35 U.S.C. § 112, párrafo seis, a no ser que el elemento sea referido expresamente usando la expresión "medios para" o que, en el caso de una reivindicación de procedimiento, el elemento se mencione usando la expresión "etapa para".

[0065] En esta memoria descriptiva y en las reivindicaciones adjuntas, debe quedar claro que el término "sistema de circuitos" se interpreta como un término estructural y no como un término funcional. Por ejemplo, el sistema de circuitos puede ser un conjunto de componentes de circuito, tal como una multiplicidad de componentes de circuito integrado, en forma de celdas de procesamiento y/o memoria, unidades, bloques y similares, como se muestra y describe en la figura 8 y la figura 9.

[0066] El término «procesador» debería interpretarse en sentido amplio para abarcar un procesador de propósito general, una unidad de procesamiento central (CPU), un microprocesador, un procesador de señales digitales (DSP), un controlador, un microcontrolador, una máquina de estados, etc. En algunas circunstancias, un "procesador" puede referirse a un circuito integrado específico de la aplicación (ASIC), un dispositivo lógico programable (PLD), una formación de compuertas programables en el terreno (FPGA), etc. El término "procesador" puede referirse a una

combinación de dispositivos de procesamiento, por ejemplo, una combinación de un DSP y un microprocesador, una pluralidad de microprocesadores, uno o más microprocesadores junto con un núcleo DSP o cualquier otra configuración de este tipo.

[0067] El término "memoria" debería interpretarse en sentido amplio para abarcar cualquier componente electrónico capaz de almacenar información electrónica. El término memoria puede referirse a diversos tipos de medios legibles por procesador tales como memoria de acceso aleatorio (RAM), memoria de solo lectura (ROM), memoria de acceso aleatorio no volátil (NVRAM), memoria de solo lectura programable (PROM), memoria de solo lectura programable borrable (EPROM), PROM borrable eléctricamente (EEPROM), memoria flash, almacenamiento de datos magnéticos u ópticos, registros, etc. Se dice que la memoria está en comunicación electrónica con un procesador si el procesador puede leer información de y/o escribir información en la memoria. La memoria que es parte integrante de un procesador está en comunicación electrónica con el procesador.

[0068] Los términos "instrucciones" y "código" deberían interpretarse en sentido amplio para incluir cualquier tipo de sentencia(s) legible(s) por ordenador. Por ejemplo, los términos "instrucciones" y "código" pueden referirse a uno o más programas, rutinas, subrutinas, funciones, procedimientos, etc. "Instrucciones" y "código" pueden comprender una única secuencia legible por ordenador o muchas secuencias legibles por ordenador.

[0069] Las funciones descritas en el presente documento pueden implementarse en software o firmware que se ejecuta mediante hardware. Las funciones pueden almacenarse como una o más instrucciones en un medio legible por ordenador. Los términos "medio legible por ordenador" o "producto de programa informático" se refieren a cualquier medio de almacenamiento tangible al que se pueda acceder mediante un ordenador o un procesador. A modo de ejemplo, y no de manera limitativa, un medio legible por ordenador puede incluir RAM, ROM, EEPROM, CD-ROM u otros dispositivos de almacenamiento de disco óptico, almacenamiento de disco magnético u otros dispositivos de almacenamiento magnético, o cualquier otro medio que pueda usarse para transportar o almacenar código de programa deseado en forma de instrucciones o estructuras de datos y al que pueda accederse mediante un ordenador. Los discos, tal y como se usan en el presente documento, incluyen un disco compacto (CD), un disco láser, un disco óptico, un disco versátil digital (DVD), un disco flexible y un disco Blu-ray®, donde algunos discos habitualmente reproducen datos magnéticamente y otros discos reproducen datos ópticamente con láseres. Debería apreciarse que un medio legible por ordenador puede ser tangible y no transitorio. El término "producto de programa informático" se refiere a un dispositivo o procesador informático en combinación con código o instrucciones (por ejemplo, un "programa") que se pueden ejecutar, procesar o computar mediante el dispositivo o procesador informático. Como se usa en el presente documento, el término "código" puede referirse a software, instrucciones, código o datos que son ejecutables por un dispositivo o procesador informático.

[0070] El software o las instrucciones pueden transmitirse también por un medio de transmisión. Por ejemplo, si el software se transmite desde un sitio web, un servidor u otra fuente remota usando un cable coaxial, un cable de fibra óptica, un par trenzado, una línea de abonado digital (DSL) o tecnologías inalámbricas tales como infrarrojos, radio y microondas, entonces el cable coaxial, el cable de fibra óptica, el par trenzado, la DSL o las tecnologías inalámbricas tales como infrarrojos, radio y microondas se incluyen en la definición de medio de transmisión.

[0071] Los procedimientos divulgados en el presente documento comprenden una o más etapas o acciones para lograr el procedimiento descrito. Las etapas y/o acciones de procedimiento se pueden intercambiar entre sí sin apartarse del alcance de las reivindicaciones. Dicho de otro modo, a menos que se requiera un orden específico de etapas o acciones para un funcionamiento adecuado del procedimiento que se describe, el orden y/o el uso de etapas y/o acciones específicas puede modificarse sin apartarse del alcance de las reivindicaciones.

[0072] Además, debería apreciarse que un dispositivo puede descargar y/u obtener de otra manera módulos y/u otros medios adecuados para realizar los procedimientos y las técnicas descritos en el presente documento, tales como los ilustrados en las figuras 3, 4 y 6. Por ejemplo, un dispositivo puede estar acoplado a un servidor para facilitar la transferencia de medios para realizar los procedimientos descritos en el presente documento. De forma alternativa, diversos procedimientos descritos en el presente documento pueden proporcionarse a través de medios de almacenamiento (por ejemplo, memoria de acceso aleatorio (RAM), memoria de solo lectura (ROM), un medio de almacenamiento físico tal como un disco compacto (CD) o un disco flexible, etc.), de tal manera que un dispositivo puede obtener los diversos procedimientos tras acoplarse o proporcionar los medios de almacenamiento al dispositivo. Además, se puede utilizar cualquier otra técnica adecuada para proporcionar a un dispositivo los procedimientos y técnicas descritos en el presente documento.

[0073] Se ha de entender que las reivindicaciones no están limitadas a la configuración y a los componentes precisos ilustrados anteriormente. Pueden hacerse diversas modificaciones, cambios y variantes en la disposición, operación y detalles de los sistemas, procedimientos y aparatos descritos en el presente documento sin apartarse del alcance de las reivindicaciones.

[0074] A continuación se describen ejemplos adicionales para facilitar el entendimiento de la invención:

1. Un dispositivo inalámbrico configurado para autenticar un mensaje, que comprende:

medios para obtener el mensaje;

medios para generar un flujo de claves; y

medios para calcular un código de autenticación de mensaje utilizando el flujo de claves y una función *hash* universal, donde la función *hash* universal se calcula utilizando una multiplicación sin acarreo.

2. El dispositivo inalámbrico del ejemplo 1, en el que calcular la función *hash* universal comprende:

invertir una palabra de 32 bits del mensaje;

calcular una primera palabra de 64 bits utilizando una multiplicación sin acarreo entre la palabra invertida de 32 bits del mensaje y una primera palabra de 32 bits del flujo de claves;

calcular una segunda palabra de 64 bits utilizando una multiplicación sin acarreo entre la palabra invertida de 32 bits del mensaje y una segunda palabra de 32 bits del flujo de claves;

realizar una operación OR exclusiva entre una palabra de 32 bits más bajos de la primera palabra de 64 bits y una palabra de 32 bits más altos de la segunda palabra de 64 bits para obtener una primera variable de 32 bits; y

realizar una operación OR exclusiva entre una segunda variable de 32 bits y la primera variable de 32 bits.

3. El dispositivo inalámbrico del ejemplo 2, en el que la segunda variable de 32 bits se fija inicialmente a 0.

4. El dispositivo inalámbrico del ejemplo 2, en el que la segunda palabra de 32 bits del flujo de claves sigue inmediatamente a la primera palabra de 32 bits del flujo de claves.

5. El dispositivo inalámbrico del ejemplo 1, en el que la función *hash* universal se calcula utilizando menos de 32 instrucciones máquina por cada 32 bits de mensaje.

6. El dispositivo inalámbrico del ejemplo 1, en el que la función *hash* universal se calcula utilizando 5 instrucciones máquina por cada 32 bits de mensaje.

7. El dispositivo inalámbrico del ejemplo 1, en el que el código de autenticación de mensaje se calcula utilizando un algoritmo 128-EIA3.

8. El dispositivo inalámbrico del ejemplo 7, en el que los medios para obtener el mensaje comprenden medios para generar un mensaje de transmisión, y además comprenden medios para transmitir el mensaje de transmisión y el código de autenticación de mensaje en un único mensaje.

9. El dispositivo inalámbrico del ejemplo 7, en el que los medios para obtener el mensaje comprenden medios para recibir un único mensaje que comprende el mensaje y el código de autenticación de mensaje, y que además comprenden:

medios para extraer un código de autenticación de mensaje de transmisión a partir del único mensaje; y

medios para comparar el código de autenticación de mensaje de transmisión con el código de autenticación de mensaje para determinar una autenticación del único mensaje.

10. El dispositivo inalámbrico del ejemplo 1, en el que el flujo de claves se genera utilizando un cifrado de flujo.

11. El dispositivo inalámbrico del ejemplo 1, donde el dispositivo inalámbrico es un dispositivo de comunicación inalámbrica.

12. El dispositivo inalámbrico del ejemplo 1, donde el dispositivo inalámbrico es una estación base.

13. El dispositivo inalámbrico del ejemplo 1, en el que el tiempo de ejecución de reloj de la multiplicación sin acarreo es independiente del peso de Hamming de los operandos.

14. Un aparato configurado para autenticar un mensaje, que comprende:

un sistema de circuitos configurado para obtener el mensaje, para generar un flujo de claves y para calcular un código de autenticación de mensaje utilizando el flujo de claves y una función *hash* universal, donde la función *hash* universal se calcula utilizando una multiplicación sin acarreo.

15. El aparato del ejemplo 14, en el que calcular la función *hash* universal comprende:

invertir una palabra de 32 bits del mensaje;

calcular una primera palabra de 64 bits utilizando una multiplicación sin acarreo entre la palabra invertida de 32 bits del mensaje y una primera palabra de 32 bits del flujo de claves;

calcular una segunda palabra de 64 bits utilizando una multiplicación sin acarreo entre la palabra invertida de 32 bits del mensaje y una segunda palabra de 32 bits del flujo de claves;

realizar una operación OR exclusiva entre una palabra de 32 bits más bajos de la primera palabra de 64 bits y una palabra de 32 bits más altos de la segunda palabra de 64 bits para obtener una primera variable de 32 bits; y

realizar una operación OR exclusiva entre una segunda variable de 32 bits y la primera variable de 32 bits.

16. El aparato del ejemplo 15, en el que la segunda variable de 32 bits se fija inicialmente a 0.

17. El aparato del ejemplo 15, en el que la segunda palabra de 32 bits del flujo de claves sigue inmediatamente a la primera palabra de 32 bits del flujo de claves.

18. El aparato del ejemplo 14, en el que la función *hash* universal se calcula utilizando menos de 32 instrucciones máquina por cada 32 bits de mensaje.

19. El aparato del ejemplo 14, en el que la función *hash* universal se calcula utilizando 5 instrucciones máquina por cada 32 bits de mensaje.

20. El aparato del ejemplo 14, en el que el código de autenticación de mensaje se calcula utilizando un algoritmo 128-EIA3.

21. El aparato del ejemplo 20, en el que el sistema de circuitos configurado para obtener el mensaje comprende un sistema de circuitos configurado para generar un mensaje de transmisión, y además comprende un sistema de circuitos configurado para transmitir el mensaje de transmisión y el código de autenticación de mensaje en un único mensaje.

22. El aparato del ejemplo 20, en el que el sistema de circuitos configurado para obtener el mensaje comprende un sistema de circuitos configurado para recibir un único mensaje que comprende el mensaje y el código de autenticación de mensaje, y que además comprende un sistema de circuitos configurado para extraer un código de autenticación de mensaje de transmisión a partir del único mensaje, y un sistema de circuitos configurado para comparar el código de autenticación de mensaje de transmisión con el código de autenticación de mensaje para determinar la autenticación del único mensaje.

23. El aparato del ejemplo 14, en el que el flujo de claves se genera usando un cifrado de flujo.

24. El aparato del ejemplo 14, en el que el aparato es un dispositivo de comunicación inalámbrica.

25. El aparato del ejemplo 14, en el que el aparato es una estación base.

26. El aparato del ejemplo 14, en el que el tiempo de ejecución de reloj de la multiplicación sin acarreo es independiente de un peso de Hamming de operandos.

27. Un procedimiento de autenticación de un mensaje mediante un dispositivo inalámbrico, que comprende:

obtener el mensaje;

generar un flujo de claves; y

calcular un código de autenticación de mensaje utilizando el flujo de claves y una función *hash* universal, donde la función *hash* universal se calcula utilizando una multiplicación sin acarreo.

28. El procedimiento del ejemplo 27, en el que calcular la función *hash* universal comprende:

invertir una palabra de 32 bits del mensaje;

calcular una primera palabra de 64 bits utilizando una multiplicación sin acarreo entre la palabra invertida de

32 bits del mensaje y una primera palabra de 32 bits del flujo de claves;

calcular una segunda palabra de 64 bits utilizando una multiplicación sin acarreo entre la palabra invertida de 32 bits del mensaje y una segunda palabra de 32 bits del flujo de claves;

realizar una operación OR exclusiva entre una palabra de 32 bits más bajos de la primera palabra de 64 bits y una palabra de 32 bits más altos de la segunda palabra de 64 bits para obtener una primera variable de 32 bits; y

realizar una operación OR exclusiva entre una segunda variable de 32 bits y la primera variable de 32 bits.

29. El procedimiento del ejemplo 28, en el que la segunda variable de 32 bits se fija inicialmente a 0.

30. El procedimiento del ejemplo 28, en el que la segunda palabra de 32 bits del flujo de claves sigue inmediatamente a la primera palabra de 32 bits del flujo de claves.

31. El procedimiento del ejemplo 27, en el que la función *hash* universal se calcula utilizando menos de 32 instrucciones máquina por cada 32 bits de mensaje.

32. El procedimiento del ejemplo 27, en el que la función *hash* universal se calcula utilizando 5 instrucciones máquina por cada 32 bits de mensaje.

33. El procedimiento del ejemplo 27, en el que el código de autenticación de mensaje se calcula utilizando un algoritmo 128-EIA3.

34. El procedimiento del ejemplo 33, en el que obtener el mensaje comprende generar un mensaje de transmisión, y además comprende transmitir el mensaje de transmisión y el código de autenticación de mensaje en un único mensaje.

35. El procedimiento del ejemplo 33, en el que obtener el mensaje comprende recibir un único mensaje que comprende el mensaje y el código de autenticación de mensaje, y que comprende además:

extraer un código de autenticación de mensaje de transmisión a partir del único mensaje; y

comparar el código de autenticación de mensaje de transmisión con el código de autenticación de mensaje para determinar una autenticación del único mensaje.

36. El procedimiento del ejemplo 27, en el que el flujo de claves se genera utilizando un cifrado de flujo.

37. El procedimiento del ejemplo 27, en el que el dispositivo inalámbrico es un dispositivo de comunicación inalámbrica.

38. El procedimiento del ejemplo 27, en el que el dispositivo inalámbrico es una estación base.

39. El procedimiento del ejemplo 27, en el que el tiempo de ejecución de reloj de la multiplicación sin acarreo es independiente de un peso de Hamming de operandos.

40. Un producto de programa informático de autenticación de un mensaje, donde el producto de programa informático comprende un medio legible por ordenador no transitorio que tiene instrucciones en el mismo, comprendiendo las instrucciones:

código para hacer que un dispositivo inalámbrico obtenga el mensaje;

código para hacer que el dispositivo inalámbrico genere un flujo de claves; y

código para hacer que el dispositivo inalámbrico calcule un código de autenticación de mensaje utilizando el flujo de claves y una función *hash* universal, donde la función *hash* universal se calcula utilizando una multiplicación sin acarreo.

41. El producto de programa informático del ejemplo 40, en el que calcular la función *hash* universal comprende:

invertir una palabra de 32 bits del mensaje;

calcular una primera palabra de 64 bits utilizando una multiplicación sin acarreo entre la palabra invertida de 32 bits del mensaje y una primera palabra de 32 bits del flujo de claves;

calcular una segunda palabra de 64 bits utilizando una multiplicación sin acarreo entre la palabra invertida de 32 bits del mensaje y una segunda palabra de 32 bits del flujo de claves;

realizar una operación OR exclusiva entre una palabra de 32 bits más bajos de la primera palabra de 64 bits y una palabra de 32 bits más altos de la segunda palabra de 64 bits para obtener una primera variable de 32 bits; y

realizar una operación OR exclusiva entre una segunda variable de 32 bits y la primera variable de 32 bits.

42. El producto de programa informático del ejemplo 41, en el que la segunda variable de 32 bits se fija inicialmente a 0.

43. El producto de programa informático del ejemplo 41, en el que la segunda palabra de 32 bits del flujo de claves sigue inmediatamente a la primera palabra de 32 bits del flujo de claves.

REIVINDICACIONES

1. Un dispositivo inalámbrico (104) configurado para autenticar un mensaje, que comprende:

medios para obtener el mensaje;

medios para generar un flujo de claves; y

medios para calcular un código de autenticación de mensaje utilizando el flujo de claves y una función *hash* universal, donde la función *hash* universal se calcula utilizando una multiplicación sin acarreo, y donde calcular la función *hash* universal comprende:

invertir (754) una palabra de 32 bits del mensaje;

calcular (752a) una primera palabra de 64 bits utilizando una multiplicación sin acarreo entre la palabra invertida de 32 bits del mensaje y una primera palabra de 32 bits del flujo de claves;

calcular (752b) una segunda palabra de 64 bits utilizando una multiplicación sin acarreo entre la palabra invertida de 32 bits del mensaje y una segunda palabra de 32 bits del flujo de claves;

realizar una operación OR exclusiva (756) entre una palabra de 32 bits más bajos de la primera palabra de 64 bits y una palabra de 32 bits más altos de la segunda palabra de 64 bits para obtener una primera variable de 32 bits; y

realizar una operación OR exclusiva entre una segunda variable de 32 bits y la primera variable de 32 bits.

2. El dispositivo inalámbrico según la reivindicación 1, en el que la segunda variable de 32 bits se fija inicialmente a 0, o en el que la segunda palabra de 32 bits del flujo de claves sigue inmediatamente a la primera palabra de 32 bits del flujo de claves, o en el que la función *hash* universal se calcula utilizando menos de 32 instrucciones máquina por cada 32 bits de mensaje, o en el que la función *hash* universal se calcula utilizando 5 instrucciones máquina por cada 32 bits de mensaje.

3. El dispositivo inalámbrico según la reivindicación 1, en el que el código de autenticación de mensaje se calcula utilizando un algoritmo 128-EIA3, o en el que los medios para obtener el mensaje comprenden medios para generar un mensaje de transmisión, y además comprenden medios para transmitir el mensaje de transmisión y el código de autenticación de mensaje en un único mensaje, o en el que los medios para obtener el mensaje comprenden medios para recibir un único mensaje que comprende el mensaje y el código de autenticación de mensaje, y que comprenden además:

medios para extraer un código de autenticación de mensaje de transmisión a partir del único mensaje; y

medios para comparar el código de autenticación de mensaje de transmisión con el código de autenticación de mensaje para determinar una autenticación del único mensaje.

4. El dispositivo inalámbrico según la reivindicación 1, en el que el flujo de claves se genera utilizando un cifrado de flujo, o en el que el dispositivo inalámbrico es un dispositivo de comunicación inalámbrica, o en el que el dispositivo inalámbrico es una estación base, o en el que un tiempo de ejecución de reloj de la multiplicación sin acarreo es independiente de un peso de Hamming de operandos.

5. Un aparato (104) configurado para autenticar un mensaje, que comprende:

un sistema de circuitos configurado para obtener el mensaje, para generar un flujo de claves y para calcular un código de autenticación de mensaje utilizando el flujo de claves y una función *hash* universal, donde la función *hash* universal se calcula utilizando una multiplicación sin acarreo, y donde el cálculo de la función *hash* universal comprende:

invertir (754) una palabra de 32 bits del mensaje;

calcular (752a) una primera palabra de 64 bits utilizando una multiplicación sin acarreo entre la palabra invertida de 32 bits del mensaje y una primera palabra de 32 bits del flujo de claves;

calcular (752b) una segunda palabra de 64 bits utilizando una multiplicación sin acarreo entre la palabra invertida de 32 bits del mensaje y una segunda palabra de 32 bits del flujo de claves;

realizar una operación OR exclusiva (756) entre una palabra de 32 bits más bajos de la primera palabra de

64 bits y una palabra de 32 bits más altos de la segunda palabra de 64 bits para obtener una primera variable de 32 bits; y

realizar una operación OR exclusiva entre una segunda variable de 32 bits y la primera variable de 32 bits.

6. El aparato según la reivindicación 5, en el que la segunda variable de 32 bits se fija inicialmente a 0, o en el que la segunda palabra de 32 bits del flujo de claves sigue inmediatamente a la primera palabra de 32 bits del flujo de claves, o en el que la función *hash* universal se calcula utilizando menos de 32 instrucciones máquina por cada 32 bits de mensaje, o en el que la función *hash* universal se calcula utilizando 5 instrucciones máquina por cada 32 bits de mensaje.

7. El aparato según la reivindicación 5, en el que el código de autenticación de mensaje se calcula utilizando un algoritmo 128-EIA3, o en el que el sistema de circuitos configurado para obtener el mensaje comprende un sistema de circuitos configurado para generar un mensaje de transmisión, y que comprende además un sistema de circuitos configurado para transmitir el mensaje de transmisión y el código de autenticación de mensaje en un único mensaje, o en el que el sistema de circuitos configurado para obtener el mensaje comprende un sistema de circuitos configurado para recibir un único mensaje que comprende el mensaje y el código de autenticación de mensaje, y que comprende además un sistema de circuitos configurado para extraer un código de autenticación de mensaje de transmisión a partir del único mensaje, y un sistema de circuitos configurado para comparar el código de autenticación de mensaje de transmisión con el código de autenticación de mensaje para determinar la autenticación del único mensaje.

8. El aparato según la reivindicación 5, en el que el flujo de claves se genera usando un cifrado de flujo, o en el que el aparato es un dispositivo de comunicación inalámbrica, o en el que el aparato es una estación base, o en el que el tiempo de ejecución de reloj de la multiplicación sin acarreo es independiente de un peso de Hamming de los operandos.

9. Un procedimiento de autenticación de un mensaje mediante un dispositivo inalámbrico (104), que comprende:

obtener el mensaje;

generar un flujo de claves; y

calcular un código de autenticación de mensaje utilizando el flujo de claves y una función *hash* universal, donde la función *hash* universal se calcula utilizando una multiplicación sin acarreo, y donde calcular la función *hash* universal comprende:

invertir (754) una palabra de 32 bits del mensaje;

calcular (752a) una primera palabra de 64 bits utilizando una multiplicación sin acarreo entre la palabra invertida de 32 bits del mensaje y una primera palabra de 32 bits del flujo de claves;

calcular (752b) una segunda palabra de 64 bits utilizando una multiplicación sin acarreo entre la palabra invertida de 32 bits del mensaje y una segunda palabra de 32 bits del flujo de claves;

realizar una operación OR exclusiva (756) entre una palabra de 32 bits más bajos de la primera palabra de 64 bits y una palabra de 32 bits más altos de la segunda palabra de 64 bits para obtener una primera variable de 32 bits; y

realizar una operación OR exclusiva entre una segunda variable de 32 bits y la primera variable de 32 bits.

10. El procedimiento según la reivindicación 9, en el que la segunda variable de 32 bits se fija inicialmente a 0, o en el que la segunda palabra de 32 bits del flujo de claves sigue inmediatamente a la primera palabra de 32 bits del flujo de claves, o en el que la función *hash* universal se calcula utilizando menos de 32 instrucciones máquina por cada 32 bits de mensaje, o en el que la función *hash* universal se calcula utilizando 5 instrucciones máquina por cada 32 bits de mensaje.

11. El procedimiento según la reivindicación 9, en el que el código de autenticación de mensaje se calcula utilizando un algoritmo 128-EIA3, o en el que obtener el mensaje comprende generar un mensaje de transmisión, y que comprende además transmitir el mensaje de transmisión y el código de autenticación de mensaje en un único mensaje, o en el que obtener el mensaje comprende recibir un único mensaje que comprende el mensaje y el código de autenticación de mensaje, y que comprende además:

extraer un código de autenticación de mensaje de transmisión a partir del único mensaje; y

comparar el código de autenticación de mensaje de transmisión con el código de autenticación de mensaje para determinar una autenticación del único mensaje.

12. El procedimiento según la reivindicación 9, en el que el flujo de claves se genera utilizando un cifrado de flujo, o en el que el dispositivo inalámbrico es un dispositivo de comunicación inalámbrica, o en el que el dispositivo inalámbrico es una estación base, o en el que un tiempo de ejecución de reloj de la multiplicación sin acarreo es independiente de un peso de Hamming de operandos.

13. Un producto de programa informático de autenticación de un mensaje, donde el producto de programa informático comprende un medio legible por ordenador no transitorio que tiene instrucciones en el mismo, comprendiendo las instrucciones:

código para hacer que un dispositivo inalámbrico (104) obtenga el mensaje;

código para hacer que el dispositivo inalámbrico genere un flujo de claves; y

código para hacer que el dispositivo inalámbrico calcule un código de autenticación de mensaje utilizando el flujo de claves y una función *hash* universal, donde la función *hash* universal se calcula utilizando una multiplicación sin acarreo, y donde calcular la función *hash* universal comprende:

invertir (754) una palabra de 32 bits del mensaje;

calcular (752a) una primera palabra de 64 bits utilizando una multiplicación sin acarreo entre la palabra invertida de 32 bits del mensaje y una primera palabra de 32 bits del flujo de claves;

calcular (752b) una segunda palabra de 64 bits utilizando una multiplicación sin acarreo entre la palabra invertida de 32 bits del mensaje y una segunda palabra de 32 bits del flujo de claves;

realizar una operación OR exclusiva (756) entre una palabra de 32 bits más bajos de la primera palabra de 64 bits y una palabra de 32 bits más altos de la segunda palabra de 64 bits para obtener una primera variable de 32 bits; y

realizar una operación OR exclusiva entre una segunda variable de 32 bits y la primera variable de 32 bits.

14. El producto de programa informático según la reivindicación 13, en el que la segunda variable de 32 bits se fija inicialmente a 0.

15. El producto de programa informático según la reivindicación 13, en el que la segunda palabra de 32 bits del flujo de claves sigue inmediatamente a la primera palabra de 32 bits del flujo de claves.

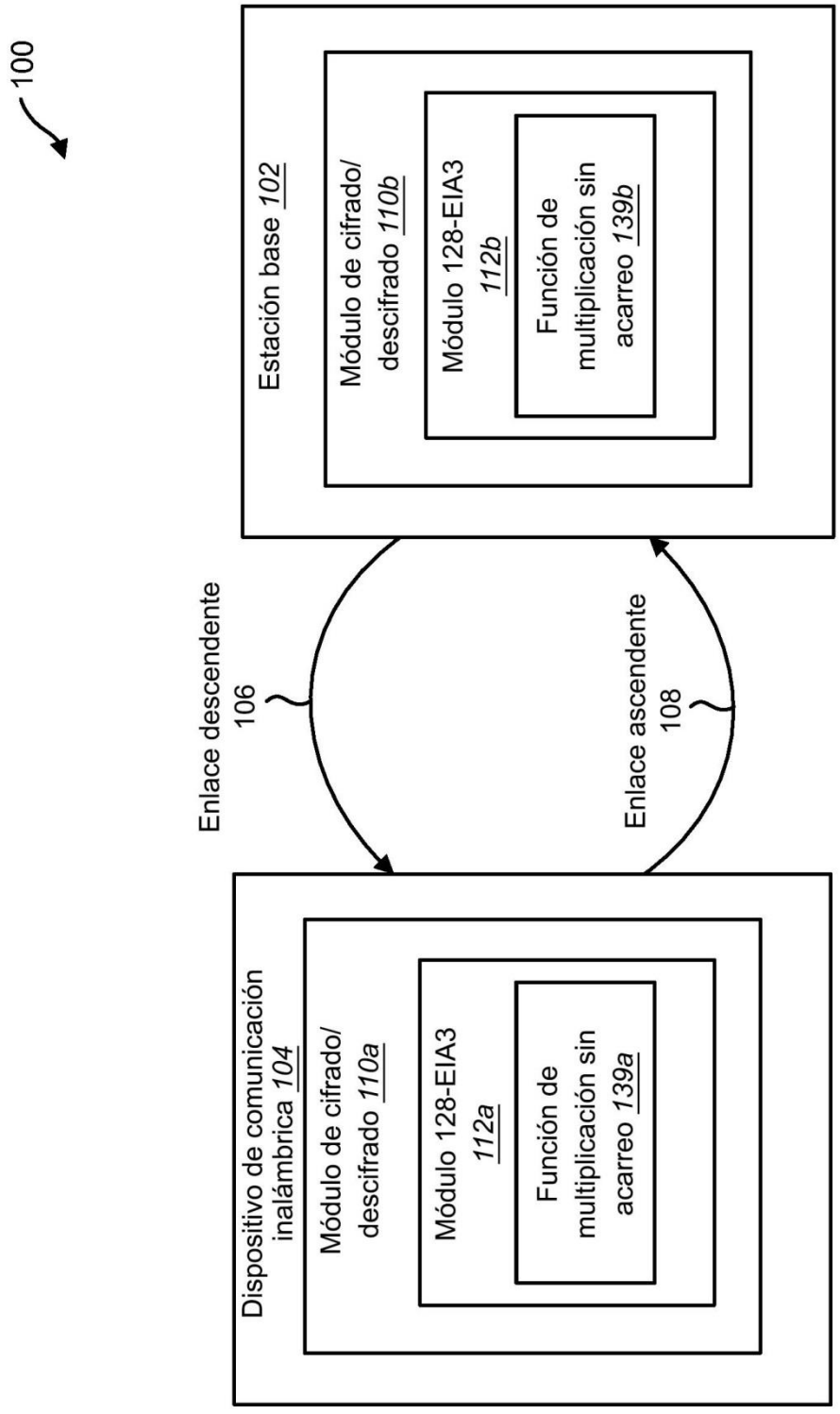
100
Estación base 102
Módulo de cifrado/ descifrado 110b
Módulo 128-EIA3 112b
Función de multiplicación sin acarreo 139b
Enlace descendente 106
Enlace ascendente 108
Dispositivo de comunicación inalámbrica 104
Módulo de cifrado/ descifrado 110a
Módulo 128-EIA3 112a
Función de multiplicación sin acarreo 139a

FIG. 1

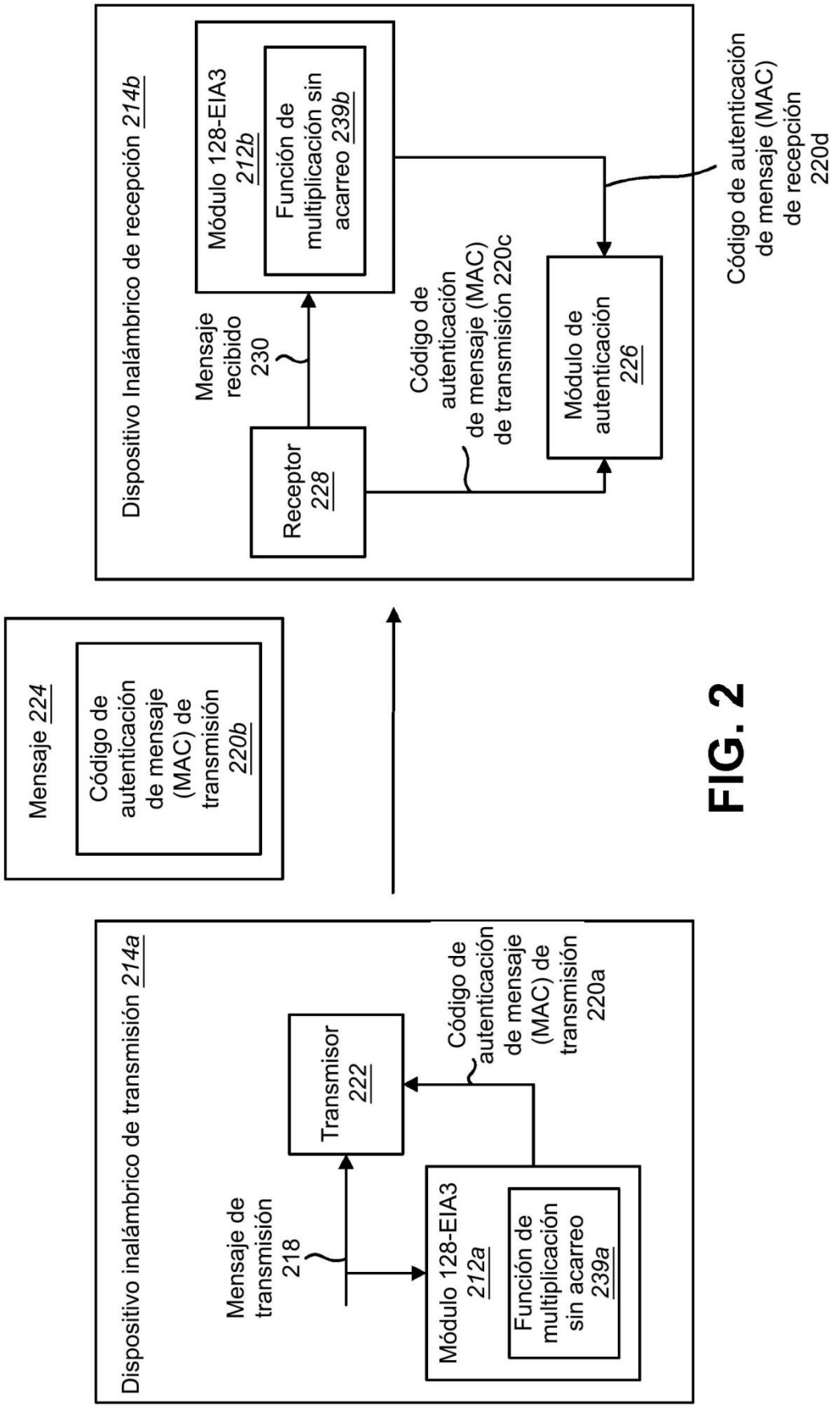
Dispositivo inalámbrico de transmisión 214a
Mensaje de transmisión 218
Módulo 128-EIA3 212a
Función de multiplicación sin acarreo 239a
Transmisor 222
Código de autenticación de mensaje (MAC) de transmisión 220a
Mensaje 224
Código de autenticación de mensaje (MAC) de transmisión 220b
Dispositivo Inalámbrico de recepción 214b
Mensaje recibido 230
Receptor 228
Módulo 128-EIA3 212b
Función de multiplicación sin acarreo 239b
Código de autenticación de mensaje (MAC) de transmisión 220c
Módulo de autenticación 226
Código de autenticación de mensaje (MAC) de recepción 220d

FIG. 2

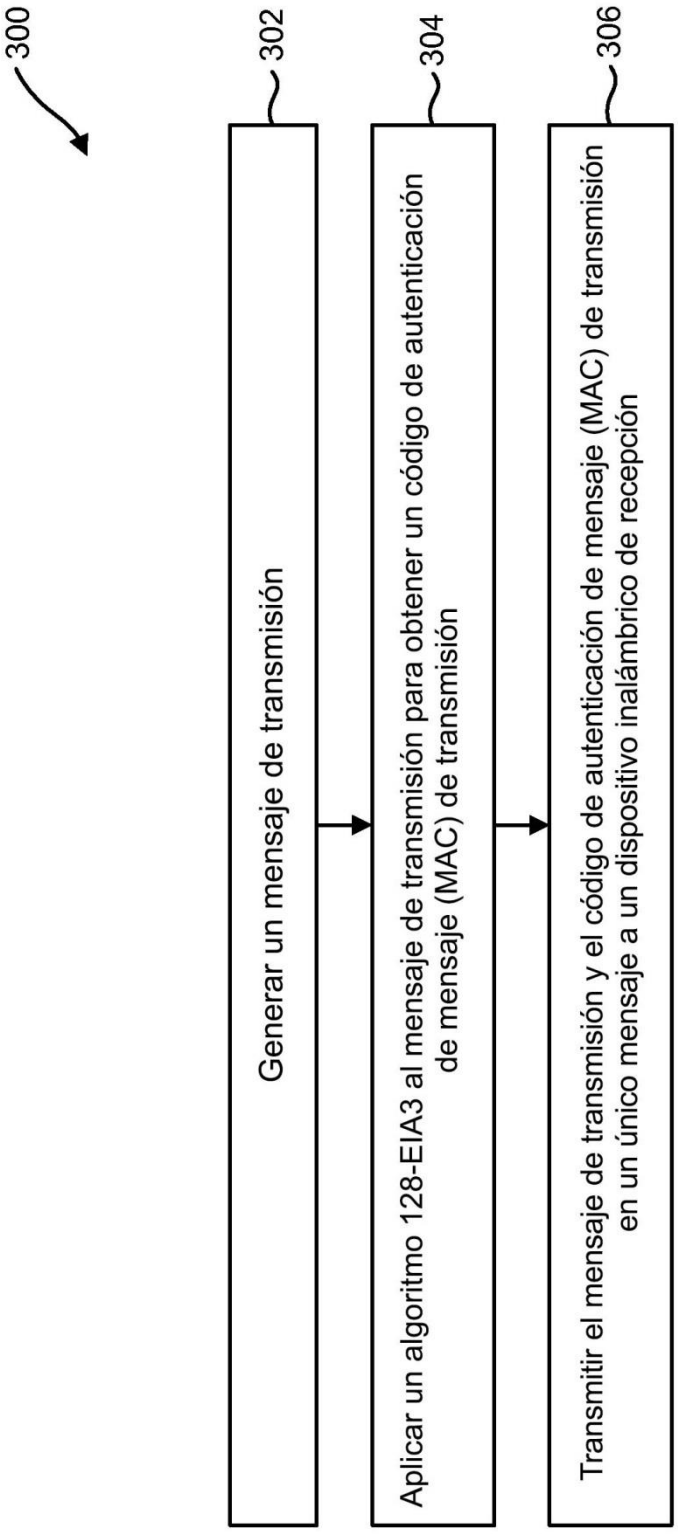
300
302
Generar un mensaje de transmisión
304
Aplicar un algoritmo 128-EIA3 al mensaje de transmisión para obtener un código de autenticación de mensaje (MAC) de transmisión
306
Transmitir el mensaje de transmisión y el código de autenticación de mensaje (MAC) de transmisión en un único mensaje a un dispositivo inalámbrico de recepción

FIG. 3

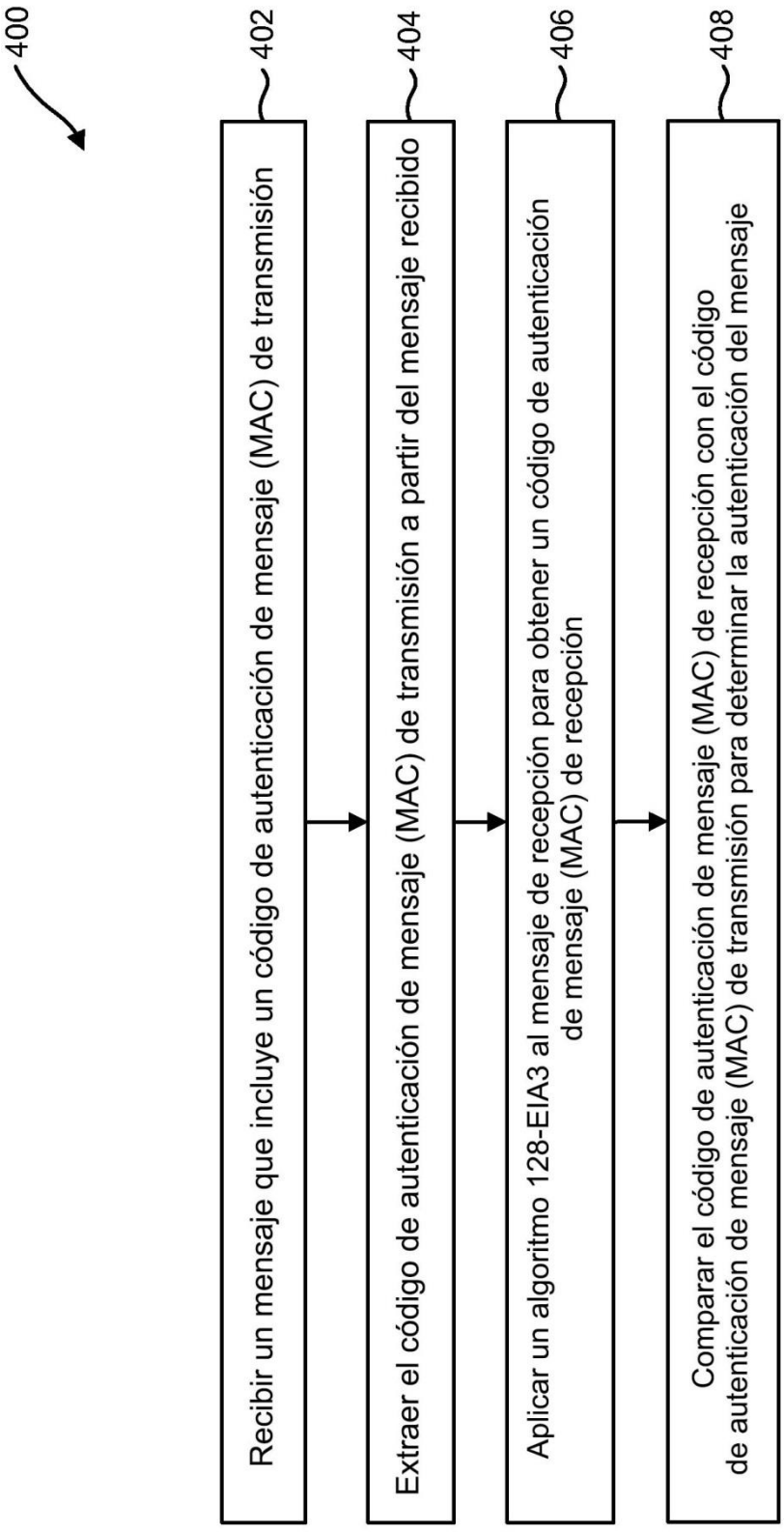
400
402
Recibir un mensaje que incluye un código de autenticación de mensaje (MAC) de transmisión
404
Extraer el código de autenticación de mensaje (MAC) de transmisión a partir del mensaje recibido
406
Aplicar un algoritmo 128-EIA3 al mensaje de recepción para obtener un código de autenticación de mensaje (MAC) de recepción
408
Comparar el código de autenticación de mensaje (MAC) de recepción con el código de autenticación de mensaje (MAC) de transmisión para determinar la autenticación del mensaje

FIG. 4

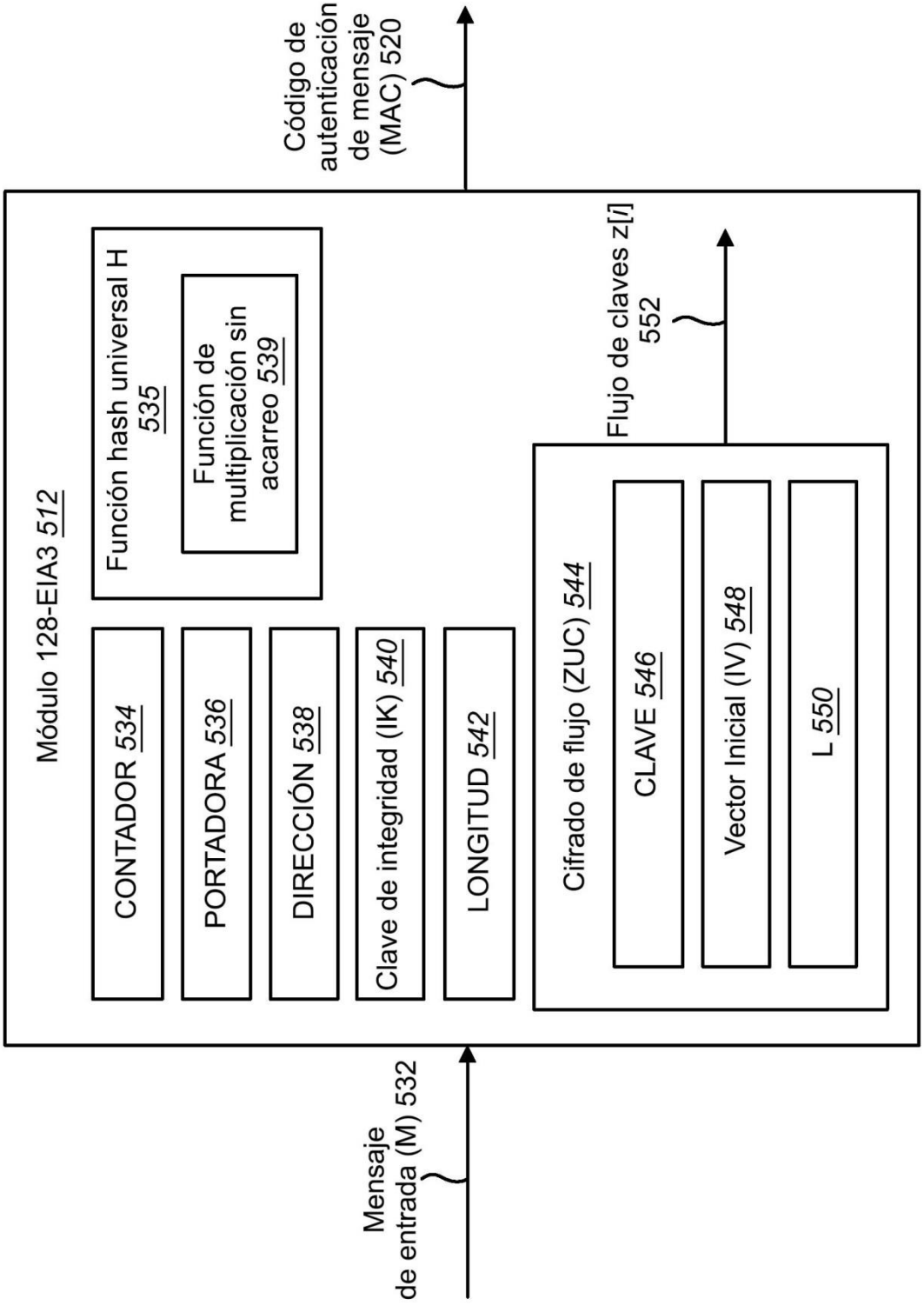
Código de autenticación de mensaje (MAC) 520
Módulo 128-EIA3 512
Función hash universal H 535
Función de multiplicación sin acarreo 539
CONTADOR 534
PORTADORA 536
DIRECCIÓN 538
Clave de integridad (IK) 540
LONGITUD 542
Cifrado de flujo (ZUC) 544
CLAVE 546
Vector Inicial (IV) 548
L 550
Flujo de claves z[i] 552
Mensaje de entrada (M) 532

FIG. 5

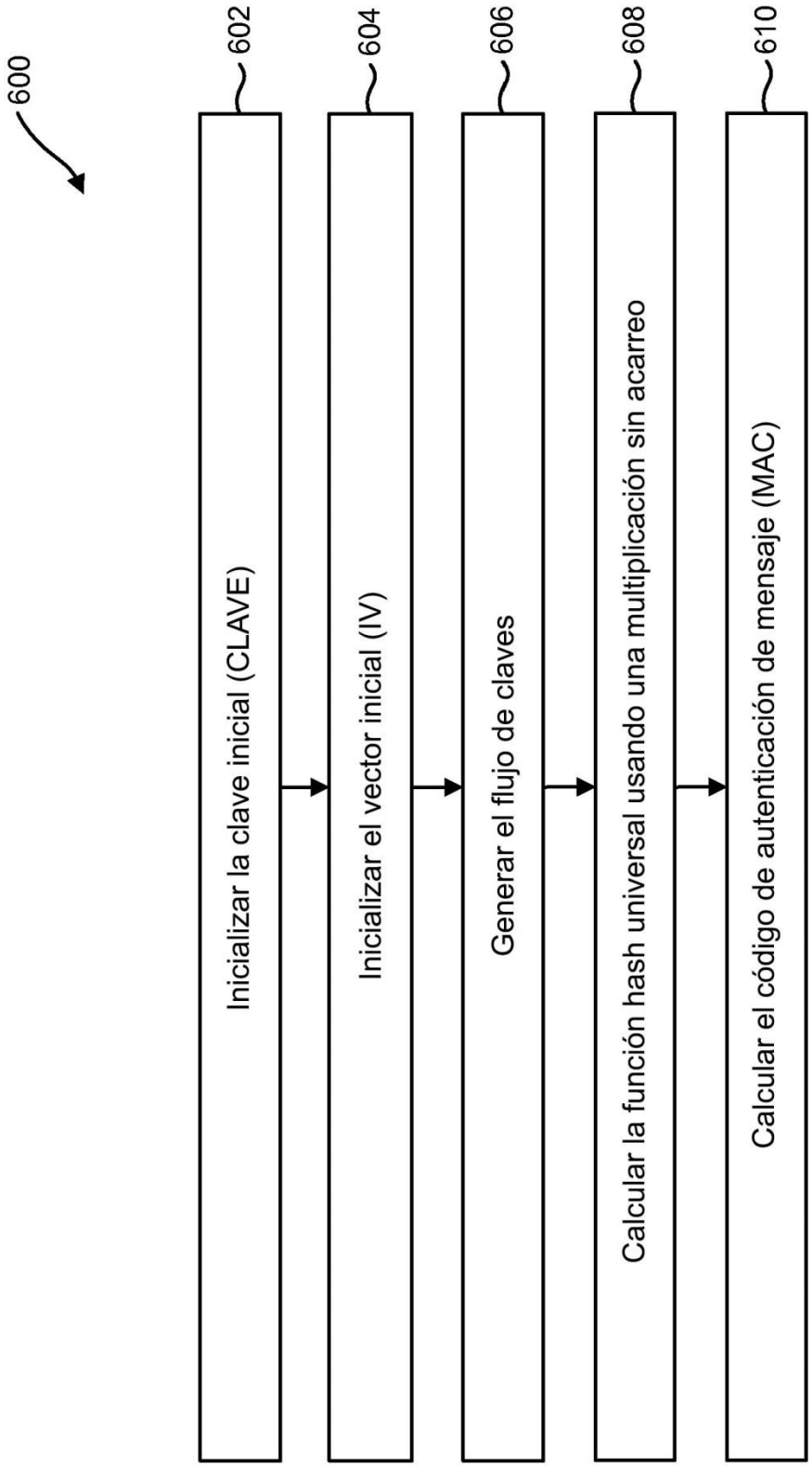
600
602
Inicializar la clave inicial (CLAVE)
604
Inicializar el vector inicial (IV)
606
Generar el flujo de claves
608
Calcular la función hash universal usando una multiplicación sin acarreo
610
Calcular el código de autenticación de mensaje (MAC)

FIG. 6

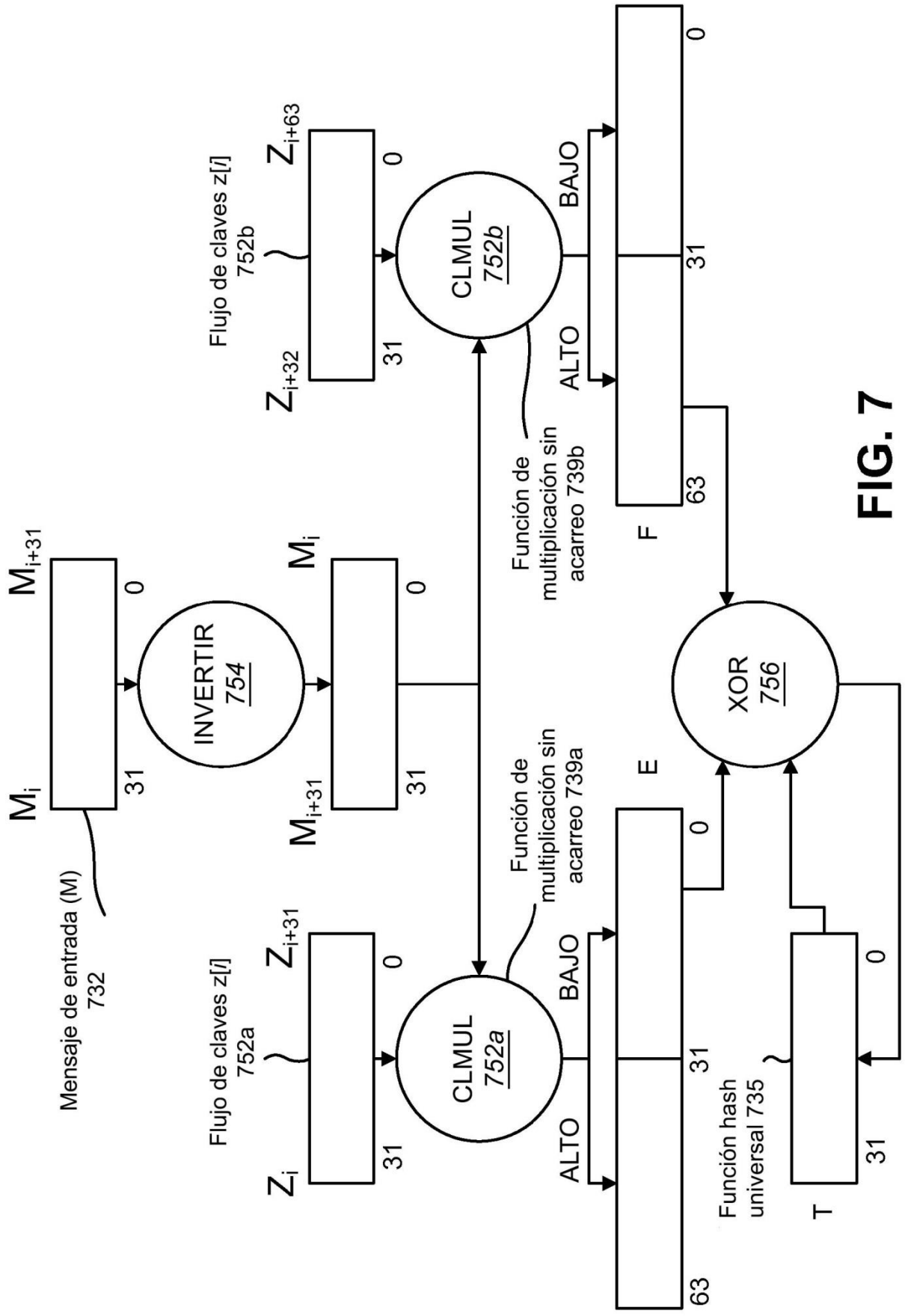
Mensaje de entrada (M)
732
M_i
M_{i+31}
INVERTIR
754
M_i
M_{i+31}
Flujo de claves z[i]
752a
Z_i
Z_{i+31}
CLMUL
752a
Función de multiplicación sin acarreo 739a
Flujo de claves z[i]
752b
Z_{i+32}
Z_{i+63}
CLMUL
752b
Función de multiplicación sin acarreo 739b
BAJO
ALTO
E
F
XOR
756
Función hash universal 735
T
0
31
63

FIG. 7

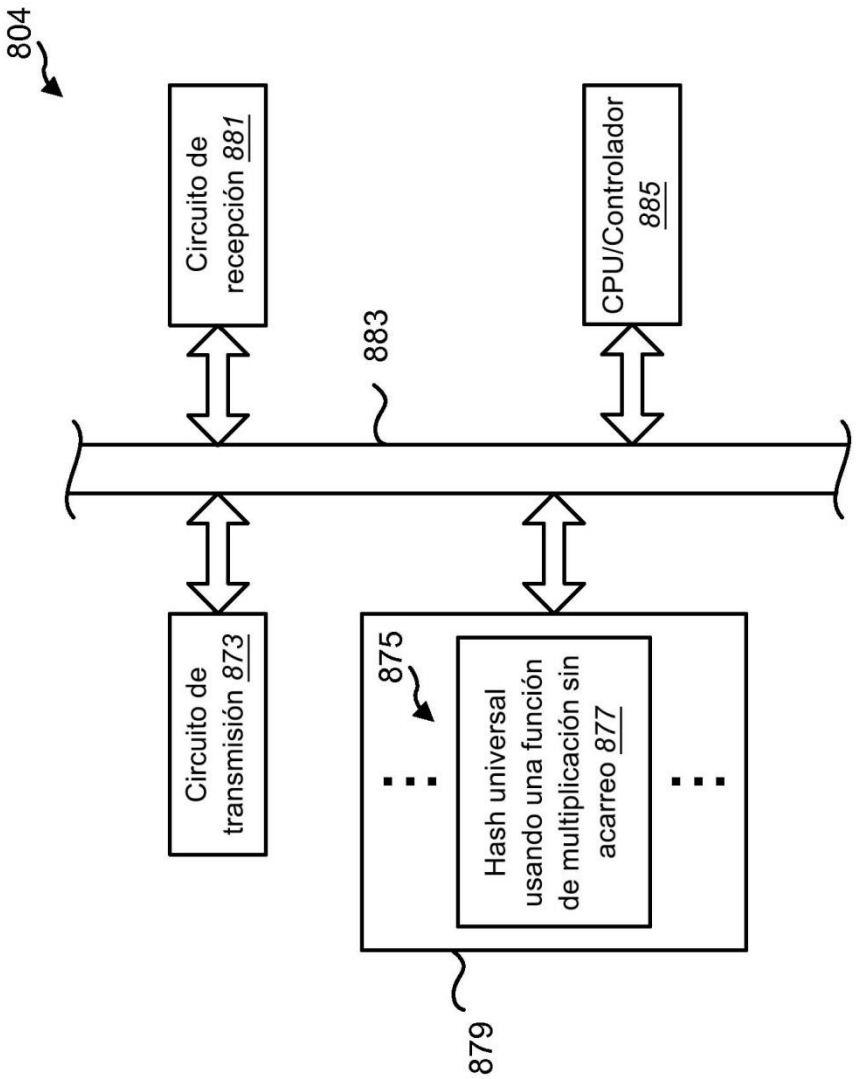
804
Circuito de recepción 881
CPU/Controlador 885
883
Circuito de transmisión 873
875
Hash universal usando una función de multiplicación sin acarreo 877
879

FIG. 8

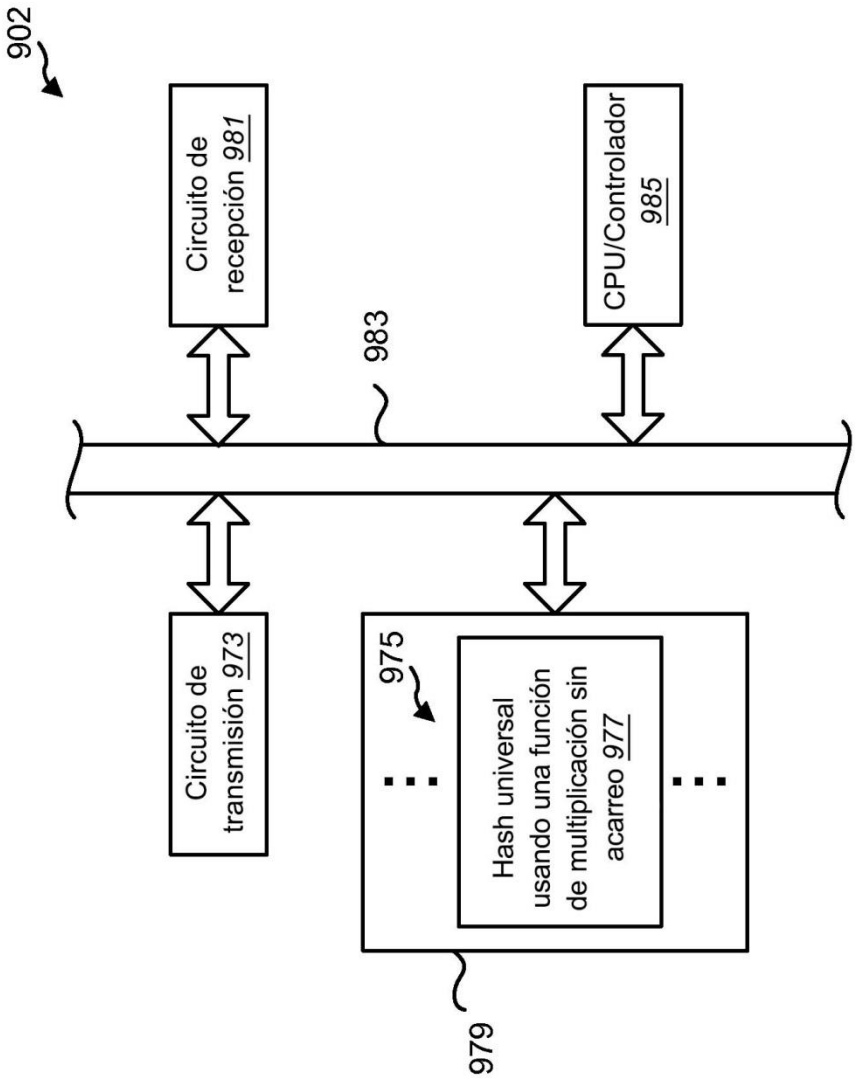
902
Circuito de recepción 981
CPU/Controlador 985
983
Circuito de transmisión 973
975
Hash universal usando una función de multiplicación sin acarreo 977
979

FIG. 9