(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 688 972**

(51) Int. CI.:

H04W 12/04 (2009.01)
H04L 9/08 (2006.01)
H04W 36/00 (2009.01)
H04W 84/04 (2009.01)
H04W 36/14 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **28.06.2010 PCT/US2010/040254**

(87) Fecha y número de publicación internacional: **29.12.2010 WO10151895**

(96) Fecha de presentación y número de la solicitud europea: **28.06.2010 E 10730650 (8)**

(97) Fecha y número de publicación de la concesión europea: **18.07.2018 EP 2446653**

(54) Título: **Derivación de clave para facilitar la seguridad de traspaso**

(30) Prioridad:

26.06.2009 US 220823 P
24.06.2010 US 822700

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
07.11.2018

(73) Titular/es:

QUALCOMM INCORPORATED (100.0%)
International IP Administration 5775 Morehouse Drive
San Diego, California 92121, US

(72) Inventor/es:

ESCOTT, ADRIAN EDWARD;
PALANIGOUNDER, ANAND y
SONG, OSOK

(74) Agente/Representante:

FORTEA LAGUNA, Juan José

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

DESCRIPCIÓN

Derivación de clave para facilitar la seguridad de traspaso

ANTECEDENTES

I. Campo

[0001] La siguiente descripción se refiere a las comunicaciones inalámbricas, en general, y para facilitar la seguridad de traspaso en sistemas de comunicación inalámbrica, en particular.

II. Antecedentes

[0002] Los sistemas de comunicación inalámbrica están ampliamente extendidos para proporcionar diversos tipos de comunicación. Por ejemplo, se pueden proporcionar voz y/o datos a través de dichos sistemas de comunicación inalámbrica. Un sistema, o red, habitual de comunicación inalámbrica puede proporcionar a múltiples usuarios acceso a uno o más recursos compartidos (por ejemplo, ancho de banda, potencia de transmisión). Por ejemplo, un sistema puede usar variadas técnicas de acceso múltiple tales como el multiplexado por división de frecuencia (FDM), el multiplexado por división del tiempo (TDM), el multiplexado por división de código (CDM), el multiplexado por división de frecuencia ortogonal (OFDM) y otras.

[0003] Generalmente, los sistemas de comunicación de acceso múltiple inalámbrica pueden soportar simultáneamente la comunicación para múltiples equipos de usuario (UE). Cada UE puede comunicarse con una o más estaciones base (BS) a través de transmisiones en enlaces directo e inverso. El enlace directo (o enlace descendente (DL)) se refiere al enlace de comunicación de BS a UE, y el enlace inverso (o enlace ascendente (UL)) se refiere al enlace de comunicación de UE a BS.

[0004] En diversos modos de realización, la BS puede ponerse en ubicaciones no fiables que presenten riesgo de violaciones de seguridad durante la comunicación con el UE para el traspaso y otros procesos. Las técnicas de traspaso existentes tienen al menos una vulnerabilidad de seguridad: la repetición de la misma cadena de claves utilizada durante diferentes procesos (por ejemplo, traspaso y otros procesos). Por ejemplo, con respecto a la arquitectura de seguridad de evolución a largo plazo (LTE)/red de acceso de radio terrestre universal (UTRAN) (en conjunto, E-UTRAN) existente (como se define en 3GPP TS 33.401 v8.4.0, "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE): Security architecture (Release 8) [Proyecto de asociación de tercera generación; Aspectos de sistemas y servicios de grupos de memorias descriptivas técnicas; Evolución de arquitectura de sistemas (SAE) 3GPP: Arquitectura de seguridad (Edición 8)]"), la posibilidad de repetición de cadenas de claves para la seguridad del estrato de acceso (AS) durante los escenarios de traspaso de la tecnología de acceso inter-radio (IRAT) es una vulnerabilidad de seguridad.

[0005] Un ejemplo de ello es el traspaso de un sistema global de comunicaciones móviles (GSM) a velocidades de datos mejoradas para la red de acceso de radio de evolución de GSM (EDGE) (en conjunto, GERAN)/UTRAN a una E-UTRAN. Específicamente, cuando el UE está en un modo activo en GERAN/UTRAN, se proporciona seguridad AS usando claves derivadas de uno o más contextos de seguridad previamente establecidos entre el UE y la red. El UE realiza el traspaso a una nueva celda en modo activo y la clave, K_{eNB}, derivada con una función de derivación de clave (KDF) a partir de un contexto de seguridad asignado. La KDF usa un valor indicativo de varias instancias de computación de la clave K_{eNB}, y/o de la información RECUENTO del estrato sin acceso (NAS) como entradas para evitar la repetición de la cadena de claves para un contexto de seguridad dado. El cálculo de K_{eNB} se realiza de acuerdo con la siguiente ecuación: K_{eNB} = KDF (K_{ASME}, S), donde S es una cadena de entrada al KDF junto con la clave K_{ASME}. S puede incluir FC (con un valor FC de 0x11) | RECUENTO UL NAS (con un valor de 0x00 0x00) | longitud de RECUENTO UL NAS (con un valor de 0x00 0x04). FC puede ser un octeto utilizado para distinguir entre diferentes instancias del mismo algoritmo. Las instancias pueden ser indicativas de los diferentes tipos de algoritmos realizados. Por ejemplo, se usan diferentes valores de FC dependiendo del parámetro que se deriva. Los valores de FC actuales pueden estar en el intervalo 0x10 - 0x1F. K_{ASME} es una clave de 256 bits derivada por el UE y por la entidad de gestión de seguridad de acceso (ASME) denominada entidad de gestión de la movilidad (MME). El UE pasa al modo inactivo en la nueva celda, por ejemplo, después de que finaliza una llamada. La función KDF también se aplica cuando se establece un portador de radio E-UTRAN criptográficamente protegido y cuando se realiza un cambio de clave sobre la marcha.

[0006] Después del paso del tiempo, el UE realiza una solicitud de servicio NAS a la misma celda usando procedimientos de modo inactivo a modo activo. Como tal, el K_{eNB} se deriva de nuevo usando la misma fórmula que la fórmula utilizada para derivar K_{eNB} para el traspaso, por ejemplo, K_{eNB} = KDF (K_{ASME}, S), donde S es FC (con un valor FC de 0x11) | RECUENTO UL NAS (con un valor de 0x00 0x00) | longitud del RECUENTO UL NAS (con un valor de 0x00 0x04). Debido a que el UE no ha enviado ningún mensaje NAS antes de la solicitud de servicio NAS, el RECUENTO UL NAS sigue siendo cero. Como resultado, se calcula el mismo valor de K_{eNB}. El cálculo del mismo valor de K_{eNB} da como resultado una repetición de la cadena de claves en la seguridad de nivel AS. Una repetición

de la cadena de claves puede ocasionar una infracción de seguridad grave. Como tal, son deseables sistemas, procedimientos y aparatos para mejorar la seguridad de traspaso.

SUMARIO

[0007] A continuación se ofrece un resumen simplificado de uno o más modos de realización con el fin de proporcionar un entendimiento básico de dichos modos de realización. Este sumario no es una visión general extensiva de todos los modos de realización contemplados y no está previsto para identificar ni elementos clave ni críticos de todos los modos de realización ni delimitar el alcance de algunos o de todos los modos de realización. Su único propósito es presentar algunos conceptos de uno o más modos de realización de una forma simplificada como preludio a la descripción más detallada que se presenta más adelante.

[0008] De acuerdo con uno o más modos de realización y la divulgación correspondiente de los mismos, se describen diversos aspectos en relación con facilitar la seguridad de traspaso.

[0009] En algunos aspectos, se proporciona un procedimiento. El procedimiento puede incluir: derivar un valor de clave para el traspaso desde un sistema GERAN/UTRAN a un sistema E-UTRAN utilizando un primer valor de entrada; y derivar un valor de clave para un establecimiento de conexión usando un segundo valor de entrada, en el que el primer valor de entrada es diferente del segundo valor de entrada y es diferente de los valores de entrada derivados posteriores al segundo valor de entrada, y en el que el primer valor de entrada, el segundo valor de entrada y los valores de entrada derivados posteriores al segundo valor de entrada se configuran para introducirse en una misma función de derivación de claves configurada para emitir una clave para su uso entre una entidad de red y el equipo de usuario.

[0010] En algunos aspectos, se proporciona un producto de programa informático que tiene un medio legible por ordenador. El producto del programa informático puede incluir un primer conjunto de códigos para hacer que un ordenador derive un valor de clave para el traspaso desde un sistema GERAN/UTRAN a un sistema E-UTRAN utilizando un primer valor de entrada. El producto de programa informático puede incluir un segundo conjunto de códigos para hacer que el ordenador derive un valor de clave para un establecimiento de conexión usando un segundo valor de entrada, en el que el primer valor de entrada es diferente del segundo valor de entrada y es diferente de los valores de entrada derivados posteriores al segundo valor de entrada, y en el que el primer valor de entrada, el segundo valor de entrada y los valores de entrada derivados posteriores al segundo valor de entrada se configuran para introducirse en una misma función de derivación de clave configurada para emitir una clave para su uso entre una entidad de red y equipo de usuario.

[0011] En algunos aspectos, se proporciona un aparato. El aparato puede incluir: medios para derivar un valor de clave para el traspaso desde un sistema GERAN/UTRAN a un sistema E-UTRAN utilizando un primer valor de entrada; y derivar un valor de clave para un establecimiento de conexión usando un segundo valor de entrada, en el que el primer valor de entrada es diferente del segundo valor de entrada y es diferente de los valores de entrada derivados posteriores al segundo valor de entrada, y en el que el primer valor de entrada, el segundo valor de entrada y los valores de entrada derivados posteriores al segundo valor de entrada se configuran para introducirse en una misma función de derivación de claves configurada para emitir una clave para su uso entre una entidad de red y un equipo de usuario.

[0012] En algunos aspectos, se proporciona otro aparato. El aparato puede incluir: un módulo de gestión de movilidad configurado para: derivar un valor de clave para el traspaso desde un sistema GERAN/UTRAN a un sistema E-UTRAN utilizando un primer valor de entrada; y derivar un valor de clave para un establecimiento de conexión usando un segundo valor de entrada, en el que el primer valor de entrada es diferente del segundo valor de entrada y es diferente de los valores de entrada derivados posteriores al segundo valor de entrada, y en el que el primer valor de entrada, el segundo valor de entrada y los valores de entrada derivados posteriores al segundo valor de entrada se configuran para introducirse en una misma función de derivación de claves configurada para emitir una clave para su uso entre una entidad de red y un UE.

[0013] En otros aspectos, se proporciona otro procedimiento. El procedimiento puede incluir: derivar un valor de clave para el traspaso desde un sistema GERAN/UTRAN a un sistema E-UTRAN utilizando un primer valor de entrada; y derivar un valor de clave para un establecimiento de conexión usando un segundo valor de entrada, en el que el primer valor de entrada es diferente del segundo valor de entrada, y en el que el primer valor de entrada y el segundo valor de entrada son valores indicativos de instancias de derivación de una clave para su uso entre una entidad de red y un equipo de usuario.

[0014] En algunos aspectos, se proporciona otro producto de programa informático que tiene un medio legible por ordenador. El producto del programa informático puede incluir un primer conjunto de códigos para hacer que un ordenador derive un valor de clave para el traspaso desde un sistema GERAN/UTRAN a un sistema E-UTRAN utilizando un primer valor de entrada. El producto de programa informático también puede incluir un segundo conjunto de códigos para hacer que el ordenador derive un valor de clave para un establecimiento de conexión usando un segundo valor de entrada, en el que el primer valor de entrada es diferente del segundo valor de entrada,

y en el que el primer valor de entrada y el segundo valor de entrada son valores indicativos de instancias de derivación de una clave para su uso entre una entidad de red y un equipo de usuario.

[0015] En algunos aspectos, se proporciona un aparato. El aparato puede incluir: medios para derivar un valor de clave para el traspaso desde un sistema GERAN/UTRAN a un sistema E-UTRAN utilizando un primer valor de entrada. El aparato también puede incluir un medio para derivar un valor de clave para un establecimiento de conexión usando un segundo valor de entrada, en el que el primer valor de entrada es diferente del segundo valor de entrada, y en el que el primer valor de entrada y el segundo valor de entrada son valores indicativos de instancias de derivación de una clave para su uso entre una entidad de red y un equipo de usuario.

[0016] En algunos aspectos, se proporciona otro aparato. El aparato puede incluir: un módulo de gestión de movilidad configurado para: derivar un valor de clave para el traspaso desde un sistema GERAN/UTRAN a un sistema E-UTRAN utilizando un primer valor de entrada; y derivar un valor de clave para un establecimiento de conexión usando un segundo valor de entrada, en el que el primer valor de entrada es diferente del segundo valor de entrada, y en el que el primer valor de entrada y el segundo valor de entrada son valores indicativos de instancias de derivación de una clave para su uso entre una entidad de red y un equipo de usuario.

[0017] Para conseguir el cumplimiento de los fines anteriores y relacionados, el uno o más modos de realización comprenden las características descritas con detalle en lo sucesivo en el presente documento y expuestas particularmente en las reivindicaciones. La descripción siguiente y los dibujos adjuntos exponen con detalle en el presente documento determinados aspectos ilustrativos de uno o más modos de realización. Sin embargo, estos aspectos son indicativos de algunas de las diversas formas en que se pueden emplear los principios de diversos modos de realización, y los modos de realización descritos pretenden incluir todos estos aspectos y sus equivalentes, dentro del alcance de las reivindicaciones independientes.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

[0018] Las características, la naturaleza y las ventajas de la presente divulgación resultarán más evidentes a partir de la descripción detallada expuesta a continuación cuando se considere conjuntamente con los dibujos, en los que los caracteres de referencia similares se identifican de forma correspondiente en toda su extensión, y en los que:

La FIG. 1 es una ilustración de un sistema de comunicación inalámbrica de ejemplo para facilitar la seguridad de traspaso de acuerdo con diversos aspectos expuestos en el presente documento.

La FIG. 2 es una ilustración de otro sistema de comunicación inalámbrica de ejemplo para facilitar la seguridad de traspaso de acuerdo con diversos aspectos expuestos en el presente documento.

La FIG. 3 es una ilustración de un sistema de comunicación inalámbrica de ejemplo donde uno o más femtonodos están desplegados para facilitar la seguridad de traspaso de acuerdo con diversos aspectos expuestos en el presente documento.

La FIG. 4 es una ilustración de un mapa de cobertura de ejemplo en un sistema de comunicación inalámbrica para facilitar la seguridad de traspaso de acuerdo con diversos aspectos expuestos en el presente documento.

Las FIGS. 5A, 5B y 5C son ilustraciones de diagramas de bloques de una jerarquía de claves en una E-UTRAN, una derivación de claves en la red y una derivación de claves en el UE de acuerdo con diversos aspectos expuestos en el presente documento.

Las FIGS. 6 y 7 son ilustraciones de diagramas de flujo de procedimientos de ejemplo para facilitar la seguridad de traspaso de acuerdo con diversos aspectos expuestos en el presente documento.

Las FIGS. 8A y 8B ilustran diagramas de bloques de ejemplo de un sistema de comunicación inalámbrica para facilitar el intercambio de claves de acuerdo con diversos aspectos expuestos en el presente documento.

Las FIGS. 9 y 10 son ilustraciones de diagramas de bloques de sistemas de ejemplo para facilitar la seguridad de traspaso de acuerdo con diversos aspectos expuestos en el presente documento.

La FIG. 11 es una ilustración de un sistema de comunicación inalámbrica de ejemplo en el que los modos de realización descritos en el presente documento pueden emplearse de acuerdo con diversos aspectos expuestos en el presente documento.

DESCRIPCIÓN DETALLADA

[0019] Se describirán ahora diversos modos de realización con referencia a los dibujos, en los que se usan números de referencia similares para referirse a elementos similares de principio a fin. En la descripción siguiente se exponen, para fines explicativos, numerosos detalles específicos con el fin de proporcionar una exhaustiva

comprensión de uno o más modos de realización. Sin embargo, puede resultar evidente que dichos modos de realización pueden llevarse a la práctica sin estos detalles específicos. En otros casos, se muestran estructuras y dispositivos bien conocidos en forma de diagrama de bloques con el fin de facilitar la descripción de uno o más modos de realización.

[0020] Como se usa en esta solicitud, los términos "componente", "módulo", "sistema" y similares pretenden hacer referencia a una entidad relativa al ordenador, ya sea hardware, firmware, una combinación de hardware y software, software o software en ejecución. Por ejemplo, un componente puede ser, pero no se limita a ser, un proceso que se ejecuta en un procesador, un procesador, un objeto, un módulo ejecutable, un hilo de ejecución, un programa y/o un ordenador. A modo de ilustración, tanto una aplicación que se ejecuta en un dispositivo informático como el dispositivo informático puede ser un componente. Uno o más componentes pueden residir dentro de un proceso y/o hilo de ejecución y un componente puede localizarse en un ordenador y/o estar distribuido entre dos o más ordenadores. Además, estos componentes pueden ejecutarse desde diversos medios legibles por ordenador que tengan diversas estructuras de datos almacenadas en los mismos. Los componentes pueden comunicarse mediante procesos locales y/o remotos, tales como de acuerdo con una señal que presenta uno o más paquetes de datos (por ejemplo, datos de un componente que interactúa con otro componente en un sistema local, un sistema distribuido, y/o mediante una red, tal como Internet, con otros sistemas mediante la señal).

[0021] Las técnicas descritas en el presente documento pueden usarse para diversos sistemas de comunicación inalámbrica, tales como sistemas de acceso múltiple por división de código (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 de frecuencia ortogonal (OFDMA), sistemas de acceso múltiple por división de frecuencia de única portadora (SC-FDMA) y otros sistemas. Los términos "sistema" y "red" se usan a menudo indistintamente. Un sistema CDMA puede implementar una tecnología de radio, tal como el acceso de radio terrestre universal (UTRA), CDMA8020, etc. UTRA incluye CDMA de banda ancha (W-CDMA) y otras variantes de CDMA. El CDMA8020 cubre las normas IS-8020, IS-95 e IS-856. Un sistema de OFDMA puede implementar una tecnología de radio tal como el UTRA Evolucionado (E-UTRA), la Banda Ancha Ultra-móvil (UMB), IEEE 802.11 (Wi-Fi), IEEE 802.16 (WiMAX), IEEE 802.20, Flash-OFDM, etc. UTRA y E-UTRA son parte del Sistema Universal de Telecomunicación Móvil (UMTS). La Evolución a Largo Plazo (LTE) del 3GPP es una nueva versión de UMTS que usa E-UTRA, que utiliza OFDMA en el enlace descendente y SC-FDMA en el enlace ascendente. Las tecnologías UTRA, E-UTRA, UMTS, LTE y GSM se describen en los documentos de un organismo denominado "3rd Generation Partnership Project [Proyecto de Colaboración de Tercera Generación]" (3GPP). Adicionalmente, las tecnologías CDMA8020 y UMB se describen en los documentos de un organismo denominado "3rd Generation Partnership Project 2 [Proyecto de asociación de tercera generación 2]" (3GPP2). Además, dichos sistemas de comunicación inalámbrica pueden incluir adicionalmente sistemas de red ad hoc de igual a igual (por ejemplo, de móvil a móvil) que utilizan a menudo espectros sin licencia no emparejados, LAN inalámbrica 802.xx, BLUETOOTH y cualesquiera otras técnicas de comunicación inalámbrica de corto o de largo alcance.

[0022] El acceso múltiple por división de frecuencia de única portadora (SC-FDMA) utiliza modulación de única portadora y ecualización en el dominio de la frecuencia. SC-FDMA puede tener un rendimiento similar y esencialmente la misma complejidad general que un sistema OFDMA. Una señal SC-FDMA puede tener una relación de pico-potencia promedio (PAPR) más baja debido a su estructura de portadora única inherente. SC-FDMA se puede usar, por ejemplo, en comunicaciones de enlace ascendente donde una PAPR menor beneficia en gran medida a los UE en términos de eficiencia de potencia de transmisión. En consecuencia, el SC-FDMA se puede implementar como un esquema de acceso múltiple de enlace ascendente en la Evolución a Largo Plazo (LTE) o en el UTRA Evolucionado del 3GPP.

[0023] Además, en el presente documento se describen diversos modos de realización en relación con los UE. Un UE también se puede llamar sistema, unidad de abonado, estación de abonado, estación móvil, móvil, estación remota, terminal remoto, dispositivo móvil, terminal de acceso, dispositivo de comunicación inalámbrica, agente de usuario o dispositivo de usuario. Un UE puede ser un teléfono móvil, un teléfono sin cables, un teléfono del protocolo de inicio de sesión (SIP), una estación de bucle local inalámbrico (WLL), un asistente digital personal (PDA), un dispositivo manual con capacidad de conexión inalámbrica, un dispositivo informático u otro tipo de dispositivo de procesamiento conectado a un módem inalámbrico. Además, se describen diversos modos de realización en el presente documento en relación con una BS o nodo de acceso (AN). Se puede utilizar una BS para comunicarse con los UE y también se puede hacer referencia a ella como un punto de acceso, BS, Femtonodo, Piconodo, Nodo B, Nodo B evolucionado (eNodoB, eNB) o alguna otra terminología.

[0024] Además, el término "o" pretende referirse a un "o" incluyente en lugar de un "o" excluyente. Es decir, a no ser que se indique lo contrario o que resulte claro a partir del contexto, la frase "X emplea A o B" pretende significar cualquiera de las permutaciones inclusivas naturales. Es decir, la frase "X emplea A o B" se satisface en cualquiera de los siguientes casos: X emplea A; X emplea B; o X emplea tanto A como B. Además, los artículos "un" y "uno", según se utilizan en esta solicitud y en las reivindicaciones adjuntas, deberían ser interpretados, en general, con el significado de "uno o más", a no ser que se especifique lo contrario, o que sea claro a partir del contexto que se orientan a una forma singular.

[0025] Diversos aspectos o características que se describen en el presente documento pueden implementarse como un procedimiento, aparato o artículo de fabricación mediante técnicas de programación y/o de ingeniería convencionales. El término "artículo de fabricación", tal como se usa en el presente documento, pretende abarcar un programa informático accesible desde cualquier dispositivo, soporte o medio legible por ordenador. Por ejemplo, los medios legibles por ordenador pueden incluir, pero sin limitación, dispositivos de almacenamiento magnético (por ejemplo, un disco duro, un disco flexible, cintas magnéticas), discos ópticos (por ejemplo, un disco compacto (CD), un disco versátil digital (DVD)), tarjetas inteligentes y dispositivos de memoria flash (por ejemplo, EPPROM, tarjeta, memoria USB, llave USB). Adicionalmente, diversos medios de almacenamiento descritos en el presente documento pueden representar uno o más dispositivos y/u otros medios legibles por máquina para almacenar información. El término "medio legible por máquina" puede incluir, sin limitación, canales inalámbricos y diversos otros medios (y/o medios de almacenamiento) capaces de almacenar, contener y/o llevar códigos y/o una o más instrucciones y/o datos.

[0026] En algunos aspectos, las enseñanzas del presente documento pueden emplearse en una red que incluya una cobertura a mayor escala (por ejemplo, una red celular de área extensa tal como una red 3G, típicamente denominada red macrocelular) y una cobertura a menor escala (por ejemplo, un entorno de red instalado en un domicilio o en un edificio). Un UE se mueve a través de tal red. El UE puede obtener servicio en ciertas ubicaciones por BS que proporcionan macrocobertura mientras que el UE puede obtener servicio en otras ubicaciones por BS que proporcionan cobertura a menor escala. En algunos aspectos, los nodos de menor cobertura se pueden usar para proporcionar un crecimiento de capacidad incremental, cobertura en edificios y servicios diferentes (por ejemplo, para una experiencia de usuario más robusta). En el análisis del presente documento, un nodo que proporciona cobertura a través de un área relativamente grande puede denominarse macronodo. Un nodo que proporciona cobertura a través de un área relativamente pequeña (por ejemplo, un domicilio) puede denominarse femtonodo. Un nodo que proporciona cobertura a través de un área más pequeña que una macroárea y mayor que una femtoárea puede denominarse piconodo (por ejemplo, que proporciona cobertura en un centro comercial).

[0027] Una celda asociada a un macronodo, un femtonodo o un piconodo puede denominarse macrocelda, femtocelda o picocelda, respectivamente. En algunas implementaciones, cada celda puede estar asociada, además, a (por ejemplo, dividida en) uno o más sectores.

[0028] En diversas aplicaciones, puede usarse otra terminología para hacer referencia a un macronodo, un femtonodo o un piconodo. Por ejemplo, un macronodo se puede configurar o denominarse BS, punto de acceso, eNodoB, macrocelda, etc. Además, un femtonodo puede configurarse o denominarse nodoB local, eNodoB local, nodo de acceso a punto de acceso, BS, femtocelda, etc.

[0029] La FIG. 1 es una ilustración de un sistema de comunicación inalámbrica de ejemplo para facilitar la seguridad de traspaso de acuerdo con diversos aspectos expuestos en el presente documento. En el sistema de comunicación inalámbrica 100, la interferencia causada por transmisiones en el UL puede gestionarse por la BS 102, mientras que la interferencia causada por las transmisiones en el DL puede gestionarse por los UE 116, 122.

[0030] Haciendo referencia ahora a la FIG. 1, se ilustra un sistema de comunicación inalámbrica 100 de acuerdo con diversos modos de realización presentados en el presente documento. El sistema 100 incluye una BS 102 que puede incluir múltiples grupos de antenas. Por ejemplo, un grupo de antenas puede incluir las antenas 104, 106, otro grupo puede comprender las antenas 108, 110, y un grupo adicional puede incluir las antenas 112, 114. Se ilustran dos antenas para cada grupo de antenas; sin embargo, pueden usarse más o menos antenas para cada grupo. La BS 102 puede incluir adicionalmente una cadena de nodos transmisores y una cadena de nodos receptores, cada una de los cuales puede comprender una pluralidad de componentes asociados con la transmisión y recepción de señales (por ejemplo, procesadores, moduladores, multiplexores, demoduladores, demultiplexores, antenas), como se apreciará por un experto en la técnica.

[0031] La BS 102 puede comunicarse con uno o más UE, tal como el UE 116, 122. Sin embargo, debe apreciarse que la BS 102 puede comunicarse sustancialmente con cualquier cantidad de UE similar a los UE 116, 122. Los UE 116, 122 pueden ser, por ejemplo, teléfonos celulares, teléfonos inteligentes, ordenadores portátiles, dispositivos de comunicación portátiles, dispositivos informáticos portátiles, radios por satélite, sistemas de localización global, PDA y/o cualquier otro dispositivo adecuado para la comunicación a través del sistema de comunicación inalámbrica 100. Como se representa, el UE 116 está en comunicación con las antenas 112, 114, donde las antenas 112, 114 transmiten información al UE 116 por DL 118 y reciben información del UE 116 por un UL 120. Además, el UE 122 está en comunicación con las antenas 104, 106, donde las antenas 104, 106 transmiten información al UE 122 por un DL 124 y reciben información del UE 122 por un UL 126. En un sistema de dúplex por división de frecuencia (FDD), el DL 118 puede utilizar una banda de frecuencia diferente a la utilizada por el UL 120, y el DL 124 puede emplear una banda de frecuencia diferente a la empleada por el UL 126, por ejemplo. Además, en un sistema de dúplex por división de tiempo (TDD), el DL 118 y el UL 120 pueden utilizar una banda de frecuencia común, y el DL 124 y el UL 126 pueden utilizar una banda de frecuencia común.

[0032] Cada grupo de antenas y/o el área en la cual estén designadas para comunicarse pueden denominarse sector de BS 102. Por ejemplo, los grupos de antenas pueden diseñarse para comunicarse con los UE en un sector

de las áreas cubiertas por la BS 102. En la comunicación a través del DL 118, 124, las antenas transmisoras de BS 102 pueden utilizar la formación de haces para mejorar la relación señal-ruido de los DL 118, 124 para los UE 116, 122. Además, aunque la BS 102 utiliza la formación de haces para transmitir a los UE 116, 122 dispersos aleatoriamente a través de una cobertura asociada, los UE 116, 122 en las celdas vecinas pueden estar sujetos a menos interferencia en comparación con una BS que transmite a través de una sola antena a todos sus UE. Además, la BS 102 y los UE 116, 122 se pueden configurar para facilitar la seguridad de traspaso tal como se describe en el presente documento.

[0033] La FIG. 2 es una ilustración de otro sistema de comunicación inalámbrica de ejemplo para facilitar la seguridad de traspaso para una serie de usuarios de acuerdo con diversos aspectos expuestos en el presente documento. El sistema 200 proporciona comunicación para múltiples celdas 202, tal como, por ejemplo, macroceldas 202A - 202G, obteniendo atendido cada celda por una BS 204 correspondiente (por ejemplo, BS 204A - 204G). Como se muestra en la FIG. 2, el UE 206 (por ejemplo, UE 206A - 206L) se puede dispersar en diversas ubicaciones a lo largo del sistema a lo largo del tiempo. Cada UE 206 puede comunicarse con una o más BS 204 en un DL o un UL en un momento dado, dependiendo de si el UE 206 está activo y si está en traspaso suave, por ejemplo. El UE 206 puede participar en el traspaso para comunicarse con una nueva BS en una nueva celda. En modos de realización, la seguridad de traspaso puede facilitarse en el sistema 300 como se describe en el presente documento. El sistema de comunicaciones inalámbricas 200 puede prestar servicio en una gran región geográfica. Por ejemplo, las macroceldas 202A-202G pueden incluir algunos bloques en un vecindario.

[0034] La FIG. 3 es una ilustración de un sistema de comunicación inalámbrica de ejemplo en el que uno o más femtonodos están desplegados para facilitar la seguridad de traspaso de acuerdo con diversos aspectos expuestos en el presente documento. Específicamente, el sistema 300 incluye múltiples femtonodos 310 (por ejemplo, los femtonodos 310A y 310B) instalados en un entorno de red de escala relativamente pequeña (por ejemplo, en uno o más domicilios de usuario 330). Cada femtonodo 310 puede estar acoplado a una red de área extensa 340 (por ejemplo, Internet) y a una red central de operador móvil 350 a través de un encaminador DSL, un módem por cable, un enlace inalámbrico u otros medios de conectividad (no mostrados). Como se analizará a continuación, cada femtonodo 310 se puede configurar para dar servicio a UE asociados (por ejemplo, el UE asociado 320A) y, opcionalmente, UE ajenos (por ejemplo, el UE ajeno 320B). En otras palabras, el acceso a los femtonodos 310 se puede restringir, por lo que un UE 320 dado puede obtener servicio por un conjunto de femtonodos 310 designados (por ejemplo, domésticos) pero no puede obtener servicio por cualquier femtonodo 310 no designado (por ejemplo, un femtonodo de un vecino 310).

[0035] Sin embargo, en diversos modos de realización, un UE asociado 320A puede experimentar interferencias en el DL desde un femtonodo 310 que da servicio a un UE ajeno 320B. De forma similar, un femtonodo 310 asociado con el UE asociado 320A puede experimentar interferencias en el UL desde el UE ajeno 320B.

[0036] La FIG. 4 es una ilustración de un mapa de cobertura de ejemplo en un sistema de comunicación inalámbrica para facilitar la seguridad de traspaso de acuerdo con diversos aspectos expuestos en el presente documento. El mapa de cobertura 400 puede incluir varias áreas de seguimiento 402 (o áreas de enrutamiento o áreas de ubicación), cada una de las cuales puede incluir varias macroáreas de cobertura. En el modo de realización mostrado, las áreas de cobertura asociadas con las áreas de seguimiento 402A, 402B y 402C están delineadas por las líneas anchas y las macroáreas de cobertura 404 están representadas por los hexágonos. Las áreas de seguimiento 402A, 402B y 402C pueden incluir femtoáreas de cobertura 406. En este ejemplo, cada una de las femtoáreas de cobertura 406 (por ejemplo, la femtoárea de cobertura 406C) se representa dentro de una macroárea de cobertura 404 (por ejemplo, la macroárea de cobertura 404B). Sin embargo, debe apreciarse que una femtoárea de cobertura 406 puede no situarse completamente dentro de una macroárea de cobertura 404. En la práctica, un gran número de femtoáreas de cobertura 406 pueden definirse con un área de seguimiento 402 o una macroárea de cobertura 404 dadas. Además, una o más picoáreas de cobertura (no mostradas) pueden definirse dentro de un área de seguimiento 402 o de una macroárea de cobertura 404 dadas.

[0037] Haciendo de nuevo referencia a la FIG. 3, el titular de un femtonodo 310 puede abonarse a un servicio móvil tal como, por ejemplo, un servicio móvil 3G, ofrecido a través de la red central de operador móvil 350. Además, un UE 320 puede ser capaz de funcionar tanto en macroentornos como en entornos de red de menor escala (por ejemplo, residencial). En otras palabras, dependiendo de la ubicación actual del UE 320, el UE 320 puede obtener servicio por un nodo de acceso 360 de la red móvil de macrocelda 350 o por uno cualquiera de un conjunto de femtonodos 310 (por ejemplo, los femtonodos 310A y 310B que residen dentro de una residencia de usuario 330 correspondiente). Por ejemplo, cuando un abonado no está en casa, recibe servicio desde un nodo de acceso de macro estándar (por ejemplo, el nodo 360) y cuando el abonado está en casa, recibe servicio desde un femtonodo (por ejemplo, el nodo 310A). Aquí, debe apreciarse que un femtonodo 310 puede ser retrocompatible con los UE existentes 320.

[0038] Un femtonodo 310 puede desplegarse en una única frecuencia o, como alternativa, en múltiples frecuencias. Dependiendo de la configuración particular, la única frecuencia o una o más de las múltiples frecuencias pueden solaparse con una o más frecuencias usadas por un macronodo (por ejemplo, el nodo 360).

[0039] En algunos aspectos, un UE 320 puede configurarse para conectarse a un femtonodo preferido (por ejemplo, el femtonodo local del UE 320) siempre que dicha conectividad sea posible. Por ejemplo, siempre que el UE 320 se encuentre dentro de la residencia del usuario 330, puede desearse que el UE 320 se comunique solamente con el femtonodo local 310.

[0040] En algunos aspectos, si el UE 320 funciona dentro de la red macrocelular 350, pero no reside en su red más preferida (por ejemplo, como la definida en una lista de itinerancia preferida), el UE 320 puede continuar buscando la red más preferida (por ejemplo, el femtonodo 310 preferido) usando la Reselección de Mejor Sistema (BSR), lo que puede implicar una exploración periódica de los sistemas disponibles para determinar si existen sistemas mejores actualmente disponibles y acciones posteriores para su asociación con dichos sistemas preferidos. Con la entrada de adquisición, el UE 320 puede limitar la búsqueda de banda y canal específicos. Por ejemplo, la búsqueda del sistema más preferido puede repetirse periódicamente. Tras el descubrimiento de un femtonodo 310 preferido, el UE 320 selecciona el femtonodo 310 para acampar dentro de su área de cobertura.

[0041] Un femtonodo puede estar limitado en algunos aspectos. Por ejemplo, un femtonodo dado solo puede proporcionar ciertos servicios a ciertos UE. En utilizaciones con la denominada asociación restringida (o cerrada), un UE dado puede recibir servicio solamente desde la red móvil de macroceldas y un conjunto definido de femtonodos (por ejemplo, los femtonodos 310 que residen dentro del domicilio de usuario 330 correspondiente). En algunas implementaciones, un nodo puede estar restringido para no proporcionar, a al menos un nodo, al menos uno de: señalización, acceso a datos, registro, radiolocalización o servicio.

[0042] En algunos aspectos, un femtonodo restringido (que puede denominarse también NodoB Doméstico de Grupo Cerrado de Abonado) es uno que proporciona servicio a un conjunto aprovisionado restringido de UE. Este conjunto se puede ampliar de forma temporal o permanente según sea necesario. En algunos aspectos, un grupo de abonado cerrado (CSG) se puede definir como el conjunto de BS (por ejemplo, femtonodos) que comparten una lista de control de acceso común de UE. Un canal en el cual todos los femtonodos (o todos los femtonodos restringidos) de una región funcionen puede denominarse femtocanal.

[0043] Por lo tanto, pueden existir diversas relaciones entre un femtonodo dado y un UE dado. Por ejemplo, desde la perspectiva de un UE, un femtonodo abierto puede referirse a un femtonodo sin asociación restringida. Un femtonodo restringido puede referirse a un femtonodo que esté restringido de alguna manera (por ejemplo, restringido para la asociación y/o el registro). Un femtonodo local puede referirse a un femtonodo en el cual el UE está autorizado a acceder y funcionar. Un femtonodo invitado puede referirse a un femtonodo en el que un UE está autorizado temporalmente a acceder y funcionar. Un femtonodo ajeno puede referirse a un femtonodo al cual el UE no esté autorizado a acceder ni en el que pueda funcionar, excepto quizá en situaciones de emergencia (por ejemplo, llamadas al 112).

[0044] Desde una perspectiva femtonodo restringido, un UE local puede referirse a un UE autorizado a acceder al femtonodo restringido. Un UE invitado puede denominarse a un UE con acceso temporal al femtonodo restringido. Un UE ajeno puede referirse a un UE que no tiene permiso para acceder al femtonodo restringido, a excepción de situaciones de emergencia, por ejemplo, tal como llamadas al 112 (por ejemplo, un UE que no tiene las credenciales o el permiso para registrarse con el femtonodo restringido).

[0045] Aunque la descripción de la FIG. 4 se ha proporcionado con referencia a un femtonodo, se debe apreciar, que un piconodo puede proporcionar la misma funcionalidad o una similar para un área de cobertura mayor. Por ejemplo, un piconodo puede estar restringido, un piconodo local puede definirse para un UE determinado, etc.

[0046] Un sistema de comunicación de acceso múltiple inalámbrico puede soportar simultáneamente comunicaciones para múltiples UE inalámbricos. Como se mencionó anteriormente, cada UE puede comunicarse con una o más BS a través de transmisiones en el DL o el UL. Estos enlaces de comunicación (es decir, DL y UL) pueden establecerse a través de un sistema de única entrada-única salida, un sistema MIMO (múltiple entrada-múltiple salida), o algún otro tipo de sistema.

[0047] Un sistema MIMO emplea múltiples (N_T) antenas transmisoras y múltiples (N_R) antenas receptoras para la transmisión de datos. Un canal de MIMO formado por las N_T antenas transmisoras y las N_R antenas receptoras puede descomponerse en N_S canales independientes, que también se denominan canales espaciales, donde $N_S \leq \min\{N_T, N_R\}$. Cada uno de los N_S canales independientes corresponde a una dimensión. El sistema MIMO puede proporcionar un rendimiento mejorado (por ejemplo, un caudal de tráfico más alto y/o mayor fiabilidad) si se utilizan las dimensiones adicionales creadas por las múltiples antenas de transmisión y de recepción.

[0048] Un sistema MIMO puede soportar TDD y FDD. En un sistema TDD, las transmisiones DL y UL pueden estar en la misma región de frecuencia de manera que el principio de reciprocidad permita la estimación del canal DL desde el UL. Esto permite que la BS transmita ganancia de formación de haces en el DL cuando hay múltiples antenas disponibles en la BS.

[0049] Las FIG. 5A, 5B y 5C son ilustraciones de diagramas de bloques de una jerarquía de claves en una E-UTRAN, una derivación de claves de la red y una derivación de claves en un UE, respectivamente, de acuerdo con diversos aspectos expuestos en el presente documento. Como se muestra en las FIGS. 5A, 5B y 5C, se introduce un valor RECUENTO UL NAS a la KDF, y la KDF deriva la clave K_{eNB} usando el valor RECUENTO UL NAS. Como se describe con referencia a las FIGS. 6 y 7, el valor para RECUENTO UL NAS que se usa durante el traspaso de un UE desde un sistema UTRAN a un sistema E-UTRAN puede dictarse para evitar, o aumentar las posibilidades de evitar que se genere la repetición de la misma clave K_{eNB}.

[0050] En algunos modos de realización, como se describe en 3GPP TS 33.401 sección 6.2, la jerarquía de claves y derivaciones de claves puede ser como se muestra en las FIGS. 5A, 5B y 5C. Por ejemplo, K_{eNB} puede ser una clave derivada por el UE y una entidad de gestión de movilidad (MME) 524 de K_{ASME} o por el UE y un eNB objetivo de KeNB* durante el traspaso de eNB. En algunos modos de realización, K_{eNB} se usa solo para la derivación de claves para tráfico de control de recursos de radio (RRC) y la derivación de claves para tráfico UP o para derivar una clave de transición K_{eNB}* durante un traspaso de eNB.

[0051] Las claves para el tráfico NAS pueden incluir una clave K_{NASint} que, en algunos modos de realización, sólo se utiliza para la protección del tráfico NAS con un algoritmo de integridad particular. Esta clave puede derivarse por el UE y MME a partir de K_{ASME}, así como por un identificador para el algoritmo de integridad. La clave para el tráfico NAS también puede incluir una clave K_{NASenc}, que en algunos modos de realización, se usa solo para la protección del tráfico NAS con un algoritmo de cifrado particular. Esta clave puede derivarse por el UE y MME a partir de K_{ASME}, así como por un identificador para el algoritmo de cifrado.

[0052] Las claves para el tráfico UP pueden incluir la clave $K_{UPenc,}$ que, en algunos modos de realización, puede usarse solamente para la protección del tráfico UP con un algoritmo de cifrado particular. Esta clave puede derivarse por el UE y el eNB a partir de K_{eNB}, así como por un identificador para el algoritmo de cifrado.

[0053] Las claves para el tráfico RRC pueden incluir la clave K_{RRCint} que, en algunos modos de realización, es una clave que se utiliza para la protección de tráfico RRC con un algoritmo de integridad particular. Esta clave puede derivarse por el UE y el eNB a partir de K_{eNB}, así como por un identificador para el algoritmo de integridad. La clave para el tráfico RRC también puede incluir la clave K_{RRCenc} que, en algunos modos de realización, es una clave utilizada solamente para la protección del tráfico RRC con un algoritmo de cifrado particular. K_{RRCenc} puede derivarse por el UE y el eNB a partir de K_{eNB}, así como un identificador para el algoritmo de cifrado.

[0054] La FIG. 5B ilustra las dependencias entre las diferentes claves, y cómo las diferentes claves se pueden derivar desde el punto de vista de los nodos de red. La FIG. 5C ilustra las dependencias entre las diferentes claves, y cómo el UE puede derivar las diferentes claves. Como se muestra por las FIGS. 5B y 5C, la longitud de K_{ASME} y K_{eNB} puede ser de 256 bits, y las claves NAS, UP y RRC de 256 bits pueden derivarse a partir de K_{ASME} y K_{eNB}, respectivamente. En caso de que el algoritmo de cifrado o integridad utilizado para proteger NAS, UP o RRC requiera una clave de 128 bits como entrada, la clave puede truncarse, y pueden usarse los 128 bits menos significativos. La función, t, puede recibir una entrada de cadena de 256 bits y devolver los 128 bits menos significativos de esa cadena como salida. La entrada Ks, en la derivación de KASME, puede emplearse para la versión de lanzamiento 8 de LTE, o versiones anteriores de los módulos de identidad de abonado universales (USIM), la concatenación de CK e IK. CK e IK pueden ser claves a largo plazo compartidas entre el UE y HSS, donde la K puede ser una clave permanente almacenada en el USIM en una tarjeta de circuito integrado universal (UICC) y en el centro de autenticación (AuC), y CK, IK puede ser el par de claves derivadas en el AuC y en el USIM durante una ejecución de autenticación y acuerdo de claves (AKA). CK, IK se puede manejar de manera diferente dependiendo de si se usan en un contexto de sistema de paquetes evolucionado (EPS) o en un contexto heredado, como se describe en la sección 6.1.2 de 3GPP TS 33.401 y/o 3GPP TS 33.102.

[0055] Las FIGS. 6 y 7 son ilustraciones de diagramas de flujo de procedimientos de ejemplo para facilitar la seguridad de traspaso de acuerdo con diversos aspectos expuestos en el presente documento. Con referencia primero a la FIG. 6, en 610, el procedimiento 600 puede incluir derivar un valor de clave para el traspaso usando un primer valor de entrada. El traspaso puede ser desde un sistema GERAN/UTRAN a un sistema E-UTRAN. En 620, el procedimiento 600 puede incluir derivar un valor de clave para un establecimiento de conexión usando un segundo valor de entrada, en el que el primer valor de entrada es diferente del segundo valor de entrada y es diferente de los valores de entrada derivados posteriores al segundo valor de entrada, y en el que primer valor de entrada, el segundo valor de entrada y los valores de entrada derivados posteriores al segundo valor de entrada están configurados para introducirse en una misma función de derivación de clave configurada para emitir una clave para su uso entre una entidad de red y un UE. En algunos modos de realización, la entidad de red es la BS.

[0056] En algunos modos de realización, el cálculo de K_{eNB} se realiza de acuerdo con la siguiente ecuación: K_{eNB} = KDF (K_{ASME}, S), donde S es una cadena de entrada al KDF junto con la clave K_{ASME}. S puede incluir FC (con un valor FC de 0x11) | RECUENTO UL NAS (con un valor de 0x00 0x00) | longitud de RECUENTO UL NAS (con un valor de 0x00 0x04). FC puede ser un octeto utilizado para distinguir entre diferentes instancias del mismo algoritmo. Las instancias pueden ser indicativas de los diferentes tipos de algoritmos realizados. Por ejemplo, se usan diferentes valores de FC dependiendo del parámetro que se deriva. Los valores de FC actuales pueden estar en el intervalo

0x10 - 0x1F. K_{ASME} es una clave de 256 bits derivada por el UE y por la entidad de gestión de seguridad de acceso (ASME) llamada MME. El UE pasa al modo inactivo en la nueva celda, por ejemplo, después de que finaliza una llamada. La función KDF también se aplica cuando se establece un portador de radio E-UTRAN criptográficamente protegido y cuando se realiza un cambio de clave sobre la marcha.

[0057] En diversos modos de realización, el cálculo de K_{eNB}, uno o más de los aspectos de la derivación de la clave NAS y los procedimientos anteriores para el traspaso pueden ser como se describe con más detalle en 3GPP TS 33.401 v8.4.0 al que se hace referencia anteriormente. Por ejemplo, la MME y el UE pueden derivar las claves NAS de la clave asignada K'_{ASME} como se especifica en el Anexo A de 3GPP TS 33.401 v8.4.0. K_{ASME} es una clave derivada por el UE y se transfiere a la entidad de gestión de seguridad de acceso (ASME).

[0058] En algunos modos de realización, la derivación de claves NAS y K_{eNB} durante el traspaso de UTRAN a E-UTRAN puede ser como se indica a continuación. La MME y el UE pueden derivar claves NAS de una clave asignada, K'_{ASME}, como se especifica en el Anexo A. La MME y el UE pueden derivar la clave, K_{eNB}, aplicando la KDF definida en 3GPP TS 33.401 v8.4.0 Anexo A.3 utilizando la clave asignada K'_{ASME} y 2^{32}-1 como el valor del parámetro RECUENTO UL NAS. En algunos modos de realización, la MME y el UE solamente usan 2^{32}-1 como el valor del RECUENTO UL NAS con el fin de derivar K_{eNB} y no ajustan realmente el RECUENTO UL NAS en 2^{32}-1. La razón para elegir tal valor no en el rango normal de RECUENTO NAS, por ejemplo, [0, 2^{24}-1] es evitar cualquier posibilidad de que el valor pueda usarse para derivar la misma K_{eNB} de nuevo.

[0059] En algunos modos de realización, se puede utilizar un valor RECUENTO UL NAS distinto de cero (por ejemplo, 0x00 0x00) para la derivación de K_{eNB} durante los procedimientos de traspaso. A modo de ejemplo, pero sin limitación, un valor RECUENTO UL NAS puede ser el valor para el que todos los bits están configurados en 1 para RECUENTO UL NAS (por ejemplo, 0xFF 0xFF).

[0060] En diversos modos de realización de los sistemas de evolución a largo plazo (LTE), el valor RECUENTO UL NAS comienza en un valor indicativo de 0, y sigue aumentando con el tiempo. Como tal, en algunos modos de realización, el valor RECUENTO UL NAS utilizado para la derivación de K_{eNB} durante los procedimientos de traspaso puede ser cualquier valor que los valores RECUENTO NAS nunca alcanzarán.

[0061] En algunos modos de realización, el segundo valor de entrada es un valor dentro de un primer rango de posibles valores para los valores de recuento de estrato sin acceso de enlace ascendente, y el primer valor de entrada es un valor fuera del primer rango de posibles valores para los valores de recuento de estrato sin acceso de UL.

[0062] En algunos modos de realización, el primer valor de entrada a la KDF es diferente del segundo valor de entrada a la KDF y es diferente de valores de entrada derivados posteriores al segundo valor de entrada. En algunos modos de realización, el primer valor de entrada, el segundo valor de entrada y los valores de entrada derivados posteriores al segundo valor de entrada están configurados para introducirse en una misma función de derivación de clave configurada para emitir una clave para su uso entre una entidad de red y un UE. El valor de clave puede ser el valor para K_{eNB}. El K_{eNB} puede derivarse en la KDF de la MME y/o el UE. El UE puede estar en comunicación con una entidad de red, incluyendo, pero sin limitación, una BS o una MME. La KDF puede proporcionarse en el módulo de traspaso del UE analizado con referencia a la FIG. 8A y/o la MME analizada a lo largo del presente documento.

[0063] Con referencia de nuevo a la FIG. 6, como tal, en lugar de usar las mismas entradas a la KDF para el primer valor de entrada y el segundo valor de entrada (y valores de entrada derivados del segundo valor de entrada) para diferentes procesos (por ejemplo, traspaso y otros procesos incluyendo, pero sin limitación, una solicitud de servicio NAS), y derivar un mismo valor para K_{eNB} (que puede dar como resultado la repetición de una cadena de claves para los diferentes procesos), en algunos modos de realización, el procedimiento 600 puede ser un procedimiento en el que el primer valor de entrada a la KDF es diferente del segundo valor de entrada a la KDF (y es diferente de los valores de entrada derivados posteriores al segundo valor de entrada). Como tal, se pueden generar dos o más valores diferentes para K_{eNB}. Los valores de entrada pueden ser los indicativos de valores RECUENTO NAS, y/o valores indicativos de un número de instancias de derivación del valor de clave, K_{eNB}.

[0064] Por ejemplo, en algunos modos de realización, el primer valor de entrada, el segundo valor de entrada (y valores de entrada derivados posteriores al segundo valor de entrada) son indicativos de valores RECUENTO UL NAS, y el primer valor de entrada es un valor distinto de cero (por ejemplo, 0x00 0x00) durante el traspaso.

[0065] En algunos modos de realización, con los sistemas de LTE, el valor RECUENTO NAS comienza a 0. Como tal, el valor RECUENTO UL NAS para el traspaso puede ser cualquier valor que el valor RECUENTO NAS nunca alcanzará.

[0066] En algunos modos de realización, el segundo valor de entrada es un valor dentro de un primer rango de posibles valores para los valores de recuento de estrato sin acceso de enlace ascendente, y el primer valor de entrada es un valor fuera del primer rango de posibles valores para los valores de recuento de estrato sin acceso de UL.

[0067] En este modo de realización de ajustar el primer valor de entrada a un valor distinto de cero (por ejemplo, 0x00 0x00) durante el traspaso, el primer valor de entrada es indicativo de ajustar cada bit del primer valor de entrada a uno. Por ejemplo, todos los bits se pueden ajustar a uno para RECUENTO UL NAS (por ejemplo, 0xFF 0xFF).

[0068] En otro modo de realización, se ajusta el primer valor de entrada a un valor distinto de cero (por ejemplo, 0x00 0x00) durante el traspaso.

[0069] En diversos modos de realización de los sistemas de evolución a largo plazo (LTE), el valor RECUENTO UL NAS comienza en un valor indicativo de 0, y sigue aumentando con el tiempo. Como tal, en algunos modos de realización, el valor RECUENTO UL NAS utilizado para la derivación de K_{eNB} durante los procedimientos de traspaso puede ser cualquier valor que los valores RECUENTO NAS nunca alcanzarán.

[0070] La KDF que calcula la K_{eNB} puede situarse en el equipo de usuario. La KDF también se puede ubicar en la red. Por ejemplo, la red puede incluir una MME y una BS. La MME puede derivar el primer valor de entrada, el segundo valor de entrada y/u otros valores de entrada derivados posteriores al segundo valor de entrada.

[0071] Como otro ejemplo del uso de entradas a la KDF que difieren, en algunos modos de realización, el primer valor de entrada y el segundo valor de entrada son indicativos de una serie de instancias de derivación del valor de clave, K_{eNB}. En estos modos de realización, el primer valor de entrada es un valor distinto de 0x11 cuando se deriva la K_{eNB} para el traspaso.

[0072] Como otro ejemplo del uso de las entradas a la KDF que difieren, en algunos modos de realización, el primer valor de entrada y el segundo valor de entrada son indicativos de valores RECUENTO NAS, y el primer valor de entrada es un valor de cero (para el traspaso), y el segundo valor de entrada, y los valores de entrada derivados posteriores al segundo valor de entrada, son distintos de cero (para procesos sin traspaso). En este modo de realización, el segundo valor de entrada se genera inicializando un valor RECUENTO NAS a un valor de uno. En algunos modos de realización, el segundo valor de entrada se genera inicializando un valor de recuento de estrato sin acceso de UL a uno (para el caso en el que el traspaso del UE es a una red de acceso de radio terrestre de sistemas de telecomunicaciones móviles universales (UMTS)).

[0073] Con referencia ahora a la FIG. 7, en 710, el procedimiento 700 puede incluir derivar un valor de clave para el traspaso utilizando un primer valor de entrada. El traspaso puede ser desde un sistema GERAN/UTRAN a un sistema E-UTRAN. En 720, el procedimiento 700 puede incluir derivar un valor de clave para un establecimiento de conexión usando un segundo valor de entrada, en el que el primer valor de entrada es diferente del segundo valor de entrada, y en el que el primer valor de entrada y el segundo valor de entrada son valores indicativos de instancias de derivación de una clave para su uso entre una entidad de red y un UE. En algunos modos de realización, el primer valor de entrada es un valor distinto de 0x11.

[0074] La FIG. 8A es una ilustración de un diagrama de bloques de ejemplo de un sistema de comunicación inalámbrica para facilitar el intercambio de claves de acuerdo con diversos aspectos expuestos en el presente documento. En algunos modos de realización, el intercambio de claves puede emplearse durante el traspaso de un UE desde una red a otra red. Con referencia a las FIGS. 5, 6 y 7, se pueden proporcionar procedimientos para facilitar la seguridad de traspaso, como se describe en el presente documento. Con referencia específicamente a la FIG. 8A, en los modos de realización descritos, las redes 802, 822 pueden incluir los transceptores 806, 816 configurados para transmitir y recibir datos y/o información de control y/o cualquier otro tipo de información descrita ene l presente documento con referencia a cualquiera de los sistemas, procedimientos, aparatos y/o productos de programas informáticos hacia y desde los UE 804, 824, respectivamente. Por ejemplo, los transceptores 806, 816 pueden configurarse para transmitir información para realizar el traspaso y/o facilitar la seguridad con los UE 804, 824 durante el traspaso.

[0075] Las redes 802, 822 también pueden incluir los procesadores 808, 828 y la memoria 810, 830. Los procesadores 808, 828 pueden configurarse para realizar una o más de las funciones descritas en el presente documento con referencia a cualquiera de los sistemas, procedimientos, aparatos y/o productos de programas informáticos. Las redes 802, 822 pueden incluir la memoria 810, 830, respectivamente. La memoria 810, 830 puede ser para almacenar instrucciones ejecutables por ordenador y/o información para realizar las funciones descritas en el presente documento con referencia a cualquiera de los sistemas, procedimientos, aparatos y/o productos de programas informáticos.

[0076] Las redes 802, 822 también pueden incluir módulos de gestión de movilidad 812, 832 configurados para realizar procedimientos para facilitar el intercambio de claves como se describe en el presente documento. En algunos modos de realización, los módulos de gestión de movilidad 812, 832 pueden ser las MME, como se describe en el presente documento. En algunos modos de realización, las redes 802, 822 están configuradas para realizar uno o más de las etapas para facilitar la seguridad de traspaso tal como se describe en el presente documento. En

diversos modos de realización, las redes 802, 822 también pueden incluir BS (no mostradas) configuradas para facilitar el traspaso a/desde los UE 804, 824.

[0077] El UE 804, 824 puede incluir los transceptores 814, 834 configurados para transmitir y recibir datos y/o información de control y/o cualquier otro tipo de información que se describe en el presente documento con referencia a cualquiera de los sistemas, procedimientos, aparatos y/o el ordenador programar productos a y desde las BS (no mostradas) y/o las redes 802, 822, respectivamente. En algunos modos de realización, los transceptores 814, 834 se pueden configurar para recibir y/o transmitir información para realizar el traspaso y/o facilitar la seguridad con las redes 802, 822 antes, después y/o durante el traspaso. A modo de ejemplo, pero sin limitación, la información puede incluir claves de protocolo de seguridad, valores de clave, valores RECUENTO NAS, valores que son indicativos de un número de instancias de derivación o generación de KDF y similares. En algunos modos de realización, el valor indicativo de varias instancias de la derivación o generación de la KDF puede ser un valor de octeto indicado como FC.

[0078] Los UE 804, 824 también pueden incluir los procesadores 816, 836 y la memoria 818, 838. Los procesadores 816, 836 pueden configurarse para realizar una o más de las funciones descritas en el presente documento con referencia a cualquiera de los sistemas, procedimientos, aparatos y/o productos de programas informáticos. Los UE 804, 824 pueden incluir la memoria 818, 838 respectivamente. La memoria 818, 838 puede ser para almacenar instrucciones ejecutables por ordenador y/o información para realizar las funciones descritas en el presente documento con referencia a cualquiera de los sistemas, procedimientos, aparatos y/o productos de programas informáticos.

[0079] Los UE 804, 824 también pueden incluir módulos de gestión de movilidad del UE 820, 840 configurados para realizar procedimientos para facilitar la seguridad de traspaso como se describe en el presente documento. En algunos modos de realización, los módulos de gestión de movilidad del UE 820, 840 configurados para realizar procedimientos para facilitar la seguridad de traspaso como se describe 820, 840 están configurados para realizar uno o más de las etapas de los procedimientos 6 y/o 7. En algunos modos de realización, los módulos de gestión de movilidad del UE 820, 840 pueden incluir o ser MME como se describe en el presente documento. En diversos modos de realización, los UE 804, 824 pueden ser o pueden incluirse dentro de los sistemas 900 y/o 1000 analizados a continuación.

[0080] La FIG. 8B es una ilustración de un diagrama de bloques de ejemplo de un sistema de comunicación inalámbrica para facilitar el intercambio de claves de acuerdo con diversos aspectos expuestos en el presente documento. En algunos modos de realización, el intercambio de claves puede emplearse durante el traspaso de un UE desde una red a otra red. Con referencia a las FIGS. 5, 6 y 7, se pueden proporcionar procedimientos para facilitar la seguridad de traspaso, como se describe en el presente documento. Con referencia específicamente a la FIG. 8B, en los modos de realización descritos, la red de servicio 852 y la red objetivo 854 pueden incluir los transceptores 856, 864 configurados para transmitir y recibir datos y/o información de control y/o cualquier otro tipo de información descrita en el presente documento con referencia a cualquiera de los sistemas, procedimientos, aparatos y/o productos de programas informáticos a y desde las redes 852, 854. Por ejemplo, los transceptores 856, 864 pueden configurarse para transmitir información para realizar el traspaso y/o facilitar la seguridad con los UE durante el traspaso. Con referencia a la FIG. 8A, los UE pueden ser los UE 804, 824. A modo de ejemplo, pero sin limitación, la información puede incluir claves de protocolo de seguridad, valores de clave, valores RECUENTO NAS, valores de FC y similares, y las operaciones pueden incluir las descritas con referencia a las FIGS. 5, 6 y/o 7.

[0081] La red de servicio 852 y la red objetivo 854 también pueden incluir los procesadores 858, 866 y la memoria 860, 868. Los procesadores 858, 866 pueden configurarse para realizar una o más de las funciones descritas en el presente documento con referencia a cualquiera de los sistemas, procedimientos, aparatos y/o productos de programas informáticos. La red de servicio 852 y la red objetivo 854 pueden incluir la memoria 860, 868, respectivamente. La memoria 860, 868 puede ser para almacenar instrucciones ejecutables por ordenador y/o información para realizar las funciones descritas en el presente documento con referencia a cualquiera de los sistemas, procedimientos, aparatos y/o productos de programas informáticos.

[0082] La red de servicio 852 y la red objetivo 854 también pueden incluir los módulos de gestión de movilidad 862, 870 configurados para realizar los procedimientos para facilitar el intercambio de claves, la seguridad de traspaso, etc., como se describe en el presente documento. En algunos modos de realización, los módulos de gestión de movilidad 862, 870 pueden ser o incluir MME como se describe en el presente documento. En algunos modos de realización, la red de servicio 852 y la red objetivo 854 están configuradas para realizar uno o más de las etapas para habilitar los procedimientos 6 y/o 7. En diversos modos de realización, la red de servicio 852 y la red objetivo 854 y/o los módulos de gestión de movilidad 862, 870 pueden ser o pueden estar incluidos dentro de los sistemas 900 y/o 1000 analizados a continuación.

[0083] Las FIGS. 9 y 10 son ilustraciones de diagramas de bloques de sistemas de ejemplo para facilitar la seguridad de traspaso de acuerdo con diversos aspectos expuestos en el presente documento. Se debe apreciar que el sistema 900 se representa incluyendo bloques funcionales, que pueden ser bloques funcionales que representan funciones implementadas por un procesador, hardware, software, firmware o una combinación de los

mismos. El sistema 900 puede incluir un agrupamiento lógico o físico 902 de componentes eléctricos para facilitar la seguridad de traspaso.

[0084] Los componentes eléctricos pueden actuar en conjunto. Por ejemplo, el agrupamiento lógico o físico 902 puede incluir un componente eléctrico 904 para derivar un valor de clave para el traspaso utilizando un primer valor de entrada. El agrupamiento lógico o físico 902 también puede incluir un componente eléctrico 906 para derivar un valor de clave para un establecimiento de conexión usando un segundo valor de entrada, en el que el primer valor de entrada es diferente del segundo valor de entrada y es diferente de los valores de entrada derivados posteriores al segundo valor de entrada, y en el que el primer valor de entrada, el segundo valor de entrada y los valores de entrada derivados posteriores al segundo valor de entrada están configurados para introducirse en una misma función de derivación de clave configurada para emitir una clave para su uso entre una entidad de red y un UE. En algunos modos de realización, la entidad de red puede ser una BS.

[0085] En algunos modos de realización, el primer valor de entrada es diferente del segundo valor de entrada (y es diferente de valores de entrada derivados posteriores al segundo valor de entrada). En algunos modos de realización, el primer valor de entrada, el segundo valor de entrada (y los valores de entrada derivados posteriores al segundo valor de entrada) están configurados para introducirse en una misma función de derivación de clave configurada para emitir una clave para su uso entre una entidad de red y un UE. En algunos modos de realización, la entidad de red es una BS. El valor de clave puede ser el valor para K_{eNB}. El K_{eNB} se puede derivar en la KDF de la MME. La KDF puede proporcionarse en el módulo de traspaso del UE analizado con referencia a la FIG. 8A y/o la MME analizada a lo largo del presente documento.

[0086] Con referencia de nuevo a la FIG. 9, como tal, en lugar de utilizar las mismas entradas en la KDF para el primer valor de entrada y el segundo valor de entrada para diferentes procesos (por ejemplo, traspaso y otros procesos incluyen, pero sin limitación, una solicitud de servicio NAS) y derivar un mismo valor para K_{eNB} (que puede dar como resultado la repetición de una cadena de claves para los diferentes procesos), en algunos modos de realización, el sistema 900 puede ser un sistema en el que el primer valor de entrada a la KDF es diferente del segundo valor de entrada a la KDF (y diferente de otros valores de entrada derivados posteriores al segundo valor de entrada). Como tal, se pueden generar dos valores diferentes para K_{eNB}. Los valores de entrada pueden ser los indicativos de valores RECUENTO NAS, y/o valores indicativos de un número de instancias de derivación del valor de clave, K_{eNB}.

[0087] Por ejemplo, en algunos modos de realización, el primer valor de entrada, el segundo valor de entrada (y valores de entrada derivados posteriores al segundo valor de entrada) son indicativos de valores RECUENTO UL NAS, y el primer valor de entrada es un valor distinto de cero (por ejemplo, 0x00 0x00) durante el traspaso.

[0088] En diversos modos de realización de los sistemas de evolución a largo plazo (LTE), el valor RECUENTO UL NAS comienza en un valor indicativo de 0, y sigue aumentando con el tiempo. Como tal, en algunos modos de realización, el valor RECUENTO UL NAS utilizado para la derivación de K_eNB durante los procedimientos de traspaso puede ser cualquier valor que los valores RECUENTO NAS nunca alcanzarán.

[0089] En algunos modos de realización, el segundo valor de entrada es un valor dentro de un primer rango de posibles valores para los valores de recuento de estrato sin acceso de enlace ascendente, y el primer valor de entrada es un valor fuera del primer rango de posibles valores para los valores de recuento de estrato sin acceso de UL.

[0090] En este modo de realización de ajustar el primer valor de entrada a un valor distinto de cero (por ejemplo, 0x00 0x00) durante el traspaso, el primer valor de entrada es indicativo de ajustar cada bit del primer valor de entrada a uno. Por ejemplo, todos los bits se pueden ajustar a uno para RECUENTO UL NAS (por ejemplo, 0xFF 0xFF).

[0091] En otro modo de realización, se ajusta el primer valor de entrada a un valor distinto de cero (por ejemplo, 0x00 0x00) durante el traspaso.

[0092] La KDF que calcula la K_{eNB} puede situarse en el equipo de usuario. La KDF también se puede ubicar en la red. Por ejemplo, la red puede incluir una MME y una BS.

[0093] Como otro ejemplo del uso de entradas a la KDF que difieren, en algunos modos de realización, el primer valor de entrada y el segundo valor de entrada son indicativos de una serie de instancias de derivación del valor de clave, K_{eNB}. En estos modos de realización, el primer valor de entrada es un valor distinto de 0x11 cuando se deriva la K_{eNB} para el traspaso.

[0094] Como otro ejemplo del uso de las entradas a la KDF que difieren, en algunos modos de realización, el primer valor de entrada y el segundo valor de entrada son indicativos de valores RECUENTO NAS, y el primer valor de entrada es un valor de cero (para el traspaso), y el segundo valor de entrada, y los valores de entrada derivados posteriores al segundo valor de entrada, son distintos de cero (para procesos sin traspaso). En este modo de

realización, el segundo valor de entrada se genera inicializando un valor RECUENTO NAS a un valor de uno. En algunos modos de realización, el segundo valor de entrada se genera inicializando un valor de recuento de estrato sin acceso de UL a uno (para el caso en el que el traspaso del UE es a una red de acceso de radio terrestre de sistemas de telecomunicaciones móviles universales (UMTS)).

[0095] Con referencia ahora a la FIG. 10, el agrupamiento lógico o físico 1002 puede incluir un componente eléctrico 1004 para derivar un valor de clave para el traspaso usando un primer valor de entrada. El agrupamiento lógico o físico 1002 puede incluir un componente eléctrico 1006 para derivar un valor de clave para un establecimiento de conexión usando un segundo valor de entrada, en el que el primer valor de entrada es diferente del segundo valor de entrada, y en el que el primer valor de entrada y la segunda entrada valor son valores indicativos de instancias de derivación de una clave para su uso entre una entidad de red y un UE. En algunos modos de realización, el primer valor de entrada es un valor distinto de 0x11.

[0096] Un sistema de comunicación inalámbrica de acceso múltiple puede soportar simultáneamente comunicaciones para múltiples terminales inalámbricos. Como se mencionó anteriormente, cada terminal puede comunicarse con una o más BS a través de transmisiones en los enlaces directo e inverso. El enlace directo (o enlace descendente) se refiere al enlace de comunicación desde las BS a los terminales, y el enlace inverso (o enlace ascendente) se refiere al enlace de comunicación desde los terminales a las BS. Este enlace de comunicación puede establecerse a través de un sistema de única entrada y única salida, de un sistema de múltiples entradas y múltiples salidas (MIMO) o de algún otro tipo de sistema.

[0097] Un sistema MIMO emplea múltiples (N_T) antenas transmisoras y múltiples (N_R) antenas receptoras para la transmisión de datos. Un canal MIMO formado por las N_T antenas de transmisión y las N_R antenas de recepción puede descomponerse en N_S canales independientes, que también se denominan canales espaciales, donde $N_S \leq \min\{N_T, N_R\}$. Cada uno de los N_S canales independientes corresponde a una dimensión. El sistema MIMO puede proporcionar un rendimiento mejorado (por ejemplo, un mayor rendimiento y/o una mayor fiabilidad) si se utilizan las dimensiones adicionales creadas por las múltiples antenas transmisoras y receptoras.

[0098] Un sistema MIMO puede admitir la duplexación por división de tiempo (TDD) y la duplexación por división de frecuencia (FDD). En un sistema TDD, las transmisiones de enlace directo y de enlace inverso están en la misma región de frecuencia, de modo que el principio de reciprocidad permite la estimación del canal de enlace directo a partir del canal de enlace inverso. Esto permite al punto de acceso extraer una ganancia de formación de haces de transmisión en el enlace directo cuando se dispone de múltiples antenas en el punto de acceso.

[0099] La FIG. 11 muestra un sistema de comunicación inalámbrica de ejemplo en el que los modos de realización descritos en el presente documento pueden emplearse de acuerdo con diversos aspectos expuestos en el presente documento. Las enseñanzas del presente documento pueden incorporarse a un NODO (por ejemplo, un dispositivo) que emplee varios componentes para la comunicación con al menos otro NODO. La FIG. 11 representa varios componentes de ejemplo que pueden utilizarse para facilitar las comunicaciones entre nodos. Específicamente, la FIG. 11 ilustra un dispositivo inalámbrico 1110 (por ejemplo, un punto de acceso) y un dispositivo inalámbrico 1150 (por ejemplo, un terminal de acceso) de un sistema de comunicación inalámbrica 1100 (por ejemplo, sistema MIMO). En el dispositivo 1110, los datos de tráfico para una pluralidad de flujos de datos se proporcionan desde una fuente de datos 1112 hasta un procesador de datos de transmisión (TX) 1114.

[0100] En algunos aspectos, cada flujo de datos se transmite a través de una antena de transmisión respectiva. El procesador de datos TX 1114 da formato, codifica e intercala los datos de tráfico para cada flujo de datos basándose en un esquema de codificación particular seleccionado para que ese flujo de datos proporcione datos codificados.

[0101] Los datos codificados para cada flujo de datos pueden multiplexarse con datos piloto usando técnicas OFDM. Los datos piloto son típicamente un patrón de datos conocido que se procesa de una manera conocida y que puede usarse en el sistema receptor para estimar la respuesta del canal. Los datos piloto y los codificados multiplexados para cada flujo de datos se modulan entonces (es decir, se asignan a símbolos) en base a un sistema de modulación particular (por ejemplo, BPSK, QPSK, M-PSK o M-QAM) seleccionado para que ese flujo de datos proporcione símbolos de modulación. La velocidad, codificación y modulación de datos para cada flujo de datos se puede determinar mediante instrucciones realizadas por un procesador 1130. Una memoria de datos 1132 puede almacenar códigos de programa, datos y otra información usada por el procesador 1130 u otros componentes del dispositivo 1110.

[0102] Los símbolos de modulación para todos los flujos de datos se proporcionan entonces a un procesador MIMO de TX 1120, que puede procesar adicionalmente los símbolos de modulación (por ejemplo, para OFDM). El procesador MIMO de TX 1120 proporciona después N_T flujos de símbolos de modulación a N_T transceptores (XCVR) 1122A a 1122T. En algunos aspectos, el procesador MIMO de TX 1120 aplica ponderaciones de formación de haces a los símbolos de los flujos de datos y a la antena desde la cual se está transmitiendo el símbolo.

[0103] Cada transceptor 1122 recibe y procesa un flujo de símbolos respectivo para proporcionar una o más señales analógicas y acondiciona además (por ejemplo, amplifica, filtra y aumenta en frecuencia) las señales analógicas

para proporcionar una señal modulada adecuada para su transmisión a través del canal MIMO. Después, se transmiten N_T señales moduladas desde los transceptores 1122A a 1122T desde N_T antenas 1124A a 1124T, respectivamente.

[0104] En el dispositivo 1150, las señales moduladas transmitidas se reciben por N_R antenas 1152A a 1152R y la señal recibida desde cada antena 1152 se proporciona a un transceptor respectivo ("XCVR") 1154A a 1154R. Cada transceptor 1154 acondiciona (por ejemplo, filtra, amplifica y disminuye en frecuencia) una señal recibida respectiva, digitaliza la señal acondicionada para proporcionar muestras, y procesa, además, las muestras para proporcionar un flujo de símbolos "recibido" correspondiente.

[0105] Un procesador de datos de recepción (RX) 1160 entonces recibe y procesa los N_R flujos de símbolos recibidos desde N_R transceptores 1154 basándose en una técnica de procesamiento de receptor particular para proporcionar N_T flujos de símbolos "detectados". A continuación, el procesador de datos de RX 1160 desmodula, desintercala y descodifica cada flujo de símbolos detectado para recuperar los datos de tráfico para el flujo de datos. El procesamiento del procesador de datos de RX 1160 es complementario al realizado por el procesador MIMO de TX 1120 y el procesador de datos de TX 1114 en el dispositivo 1110.

[0106] Un procesador 1170 determina periódicamente qué matriz de precodificación utilizar (lo que se describe posteriormente). El procesador 1170 formula un mensaje de enlace inverso que comprende una parte de índice de matriz y una parte de valor de rango. Una memoria de datos 1172 puede almacenar códigos de programa, datos y otra información usada por el procesador 1170 u otros componentes del dispositivo 1150.

[0107] El mensaje de enlace inverso puede comprender diversos tipos de información respecto al enlace de comunicación y/o al flujo de datos recibido. A continuación, el mensaje de enlace inverso se procesa mediante un procesador de datos de TX 1138, que también recibe datos de tráfico para una pluralidad de flujos de datos desde una fuente de datos 1136, se modula mediante un modulador 1180, se acondiciona mediante los transceptores 1154A a 1154R, y se transmite de vuelta al dispositivo 1110.

[0108] En el dispositivo 1110, las señales moduladas del dispositivo 1150 se reciben mediante las antenas 1124, se acondicionan mediante los transceptores 1122, se demodulan mediante un demodulador (DEMOD) 1140, y se procesan mediante un procesador de datos de RX 1142 para extraer el mensaje de enlace inverso transmitido por el dispositivo 1150. Entonces, el procesador 1130 determina la matriz de precodificación que se va a usar para determinar las ponderaciones de formación de haces y entonces procesa el mensaje extraído.

[0109] La FIG. 11 también ilustra que los componentes de comunicación pueden incluir uno o más componentes que realizan operaciones de control de interferencias como se describe en el presente documento. Por ejemplo, un componente de control de interferencias (INTER) 1190 puede actuar conjuntamente con el procesador 1130 y/o con otros componentes del dispositivo 1110 para enviar/recibir señales a/desde otro dispositivo (por ejemplo, el dispositivo 1150), como se describe en el presente documento. Asimismo, un componente de control de interferencias 1192 puede actuar conjuntamente con el procesador 1170 y/o con otros componentes del dispositivo 1150 para enviar/recibir señales a/desde otro dispositivo (por ejemplo, el dispositivo 1110). Debe apreciarse que para cada dispositivo 1110 y 1150, la funcionalidad de dos o más de los componentes descritos puede proporcionarse mediante un único componente. Por ejemplo, un único componente de procesamiento puede proporcionar la funcionalidad del componente de control de interferencias 1190 y del procesador 1130, y un único componente de procesamiento puede proporcionar la funcionalidad del componente de control de interferencias 1192 y del procesador 1170.

[0110] En un aspecto, los canales lógicos se pueden clasificar en canales de control y canales de tráfico. Los canales de control lógico pueden incluir un canal de control de difusión (BCCH), que es un canal de enlace descendente para difundir información de control del sistema. Además, los canales de control lógico pueden incluir un canal de control de radiolocalización (PCCH), que es un canal de enlace descendente que transmite información de radiolocalización. Además, los canales de control lógico pueden incluir un canal de control de multidifusión (MCCH), que es un canal DL punto a multipunto utilizado para transmitir programación de servicios de multidifusión multimedia (MBMS) en información de control para uno o varios canales de tráfico de multidifusión (MTCH)). Por lo general, después de establecer una conexión de control de recursos de radio (RRC), este canal es utilizado únicamente por los UE que reciben el MBMS (por ejemplo, los antiguos MCCH+MSCH). Adicionalmente, los canales de control lógicos pueden incluir un canal de control dedicado (DCCH), que es un canal bidireccional de punto a punto que transmite información de control dedicada y que puede ser utilizada por los UE que tienen una conexión de RRC. En un aspecto, los canales lógicos de tráfico pueden comprender un canal de tráfico dedicado (DTCH), que es un canal bidireccional de punto a punto dedicado a un UE para la transferencia de información de usuario. Además, los canales de tráfico lógico pueden incluir un MTCH para el canal DL punto a multipunto para transmitir datos de tráfico.

[0111] En un aspecto, los canales de transporte se clasifican en DL y UL. Los canales de transporte de DL pueden incluir un canal de difusión (BCH), un canal compartido de datos de enlace descendente (DL-SDCH) y un canal de radiobúsqueda (PCH). El PCH puede dar soporte al ahorro de potencia del UE (por ejemplo, la red puede indicar al

UE un ciclo de recepción discontinua (DRX)) mediante su emisión por una celda completa y su correlación con recursos de capa física (PHY) que pueden ser usados por otros canales de control/tráfico. Los canales de transporte de UL pueden comprender un canal de acceso aleatorio (RACH), un canal de solicitud (REQCH), un canal de datos compartidos de enlace ascendente (UL-SDCH) y una pluralidad de canales PHY.

[0112] Los canales PHY pueden incluir un conjunto de canales de DL y canales de UL. Por ejemplo, los canales PHY de enlace descendente pueden incluir: Canal piloto común (CPICH); Canal de Sincronización (SCH); Canal de Control Común (CCCH); Canal Compartido de Control de Enlace Descendente (SDCCH); Canal de control de multidifusión (MCCH); Canal compartido de Asignación de Enlace Ascendente (SUACH); Canal de confirmación (ACKCH); Canal Físico Compartido de Datos de Enlace Descendente (DL-PSDCH); Canal de Control de Potencia de Enlace Ascendente (UPCCH); Canal Indicador de Radiolocalización (PICH); y/o Canal Indicador de Carga (LICH). A modo de ilustración adicional, los canales PHY de enlace ascendente pueden incluir: Canal Físico de Acceso Aleatorio (PRACH); Canal Indicador de Calidad de Canal (CQICH); Canal de Confirmación (ACKCH); Canal Indicador de Subconjuntos de Antenas (ASICH); Canal compartido de petición (SREQCH); Canal Físico Compartido de Datos de UL (UL-PSDCH); y/o Canal Piloto de Banda Ancha (BPICH).

[0113] Cabe entenderse que los modos de realización descritos en el presente documento pueden implementarse en hardware, software, firmware, middleware, microcódigo o cualquier combinación de los mismos. Para una implementación de hardware, las unidades de procesamiento pueden implementarse dentro de uno o más circuitos integrados específicos de la aplicación (ASIC), procesadores de señales digitales (DSP), dispositivos de procesamiento de señales digitales (DSPD), dispositivos lógicos programables (PLD), formaciones de compuertas programables en el terreno (FPGA), procesadores, controladores, micro-controladores, microprocesadores y/o otras unidades electrónicas diseñadas para realizar las funciones descritas en el presente documento o una combinación de los mismos.

[0114] Cuando los modos de realización se implementan en software, firmware, middleware o microcódigo, código de programa o segmentos de código, se pueden almacenar en un medio legible por máquina (o un medio legible por ordenador), tal como un componente de almacenamiento. Un segmento de código puede representar un procedimiento, una función, un subprograma, un programa, una rutina, una subrutina, un módulo, un paquete de software, una clase o cualquier combinación de instrucciones, estructuras de datos o instrucciones de programa. Un segmento de código puede acoplarse a otro segmento de código o a un circuito de hardware pasando y/o recibiendo información, datos, argumentos, parámetros o contenidos de memoria. La información, los argumentos, los parámetros, los datos, etc., pueden pasarse, remitirse o transmitirse usando cualquier medio adecuado, incluyendo memoria compartida, paso de mensajes, paso de testigos, transmisión en red, etc.

[0115] Para una implementación en software, las técnicas descritas en el presente documento pueden implementarse con módulos (por ejemplo, procedimientos, funciones, etc.) que lleven a cabo las funciones descritas en el presente documento. Los códigos de software pueden almacenarse en unidades de memoria y ejecutarse mediante procesadores. La unidad de memoria puede implementarse dentro del procesador o ser externa al procesador, en cuyo caso puede acoplarse de forma comunicativa al procesador mediante diversos medios, según lo conocido en la técnica.

[0116] Lo que se ha descrito anteriormente incluye ejemplos de uno o más modos de realización. Por supuesto, no es posible describir toda combinación concebible de componentes o metodologías con fines de describir los modos de realización mencionados anteriormente, pero uno medianamente experto en la materia puede reconocer que son posibles muchas otras combinaciones y permutaciones de diversos modos de realización. Por consiguiente, los modos de realización descritos están concebidos para abarcar todas dichas alteraciones, modificaciones y variaciones que entren dentro del alcance de las reivindicaciones adjuntas. Además, en la medida en que se use el término “incluye” en la descripción detallada o en las reivindicaciones, dicho término está previsto para ser inclusivo, de manera similar al término “que comprende” según se interprete “que comprende” cuando se emplee como una palabra de transición en una reivindicación.

[0117] A continuación se describen aspectos adicionales para facilitar el entendimiento de la invención.

[0118] En un primer aspecto adicional, se describe un procedimiento para facilitar la seguridad de traspaso, el procedimiento puede comprender derivar un valor de clave para el traspaso de un sistema global de comunicaciones móviles a velocidades de datos mejoradas para la red de acceso de radio evolución de GSM/red de acceso de radio terrestre universal ("GERAN/UTRAN") a un sistema de red de acceso de radio terrestre universal evolucionado ("E-UTRAN") usando un primer valor de entrada; y derivar un valor de clave para un establecimiento de conexión utilizando un segundo valor de entrada, en el que el primer valor de entrada puede ser diferente del segundo valor de entrada y puede ser diferente de los valores de entrada derivados posteriores al segundo valor de entrada, y en el que el primer valor de entrada el segundo valor de entrada y los valores de entrada derivados posteriores al segundo valor de entrada pueden configurarse para introducirse en una misma función de derivación de clave configurada para emitir una clave para su uso entre una entidad de red y un equipo de usuario. Además, el primer valor de entrada y el segundo valor de entrada pueden ser indicativos de valores de recuento de estrato sin acceso de enlace ascendente. Además, el segundo valor de entrada puede ser un valor dentro de un primer rango de

posibles valores para los valores de recuento de estrato sin acceso de enlace ascendente, y en el que el primer valor de entrada puede ser un valor fuera del primer rango de posibles valores para el valor de recuento de estrato sin acceso de enlace ascendente. Además, el primer valor de entrada puede ser indicativo del ajuste de cada bit del primer valor de entrada a uno. Además, la derivación se puede realizar en el equipo del usuario. Sin embargo, la derivación también puede realizarse en una red que puede comprender una entidad de gestión de movilidad y una estación base, y en la que la entidad de gestión de movilidad puede realizar la derivación del valor de clave y emite un valor de clave derivado a la estación base. Además, el establecimiento de conexión puede incluir una solicitud de servicio de estrato sin acceso. Además, el primer valor de entrada y el segundo valor de entrada pueden ser indicativos de valores de recuento de estrato sin acceso, y en el que el primer valor de entrada puede ser cero, y el segundo valor de entrada y los valores de entrada derivados posteriores al segundo valor de entrada son distintos de cero. Además, el segundo valor de entrada puede generarse inicializando un valor de recuento de estrato sin acceso a un valor de uno. Además, el segundo valor de entrada puede generarse inicializando un valor de recuento de estrato sin acceso de enlace ascendente a uno basado, al menos, en el traspaso que es el traspaso desde un sistema GERAN/UTRAN a un sistema E-UTRAN.

[0119] En otro aspecto adicional, se describe un producto de programa informático, el producto de programa informático puede comprender un medio legible por ordenador que puede comprender un primer conjunto de códigos para hacer que un ordenador derive un valor de clave para el traspaso desde un sistema global de comunicaciones móviles a velocidades de datos mejoradas para la red de acceso de radio de evolución de GSM/red de acceso de radio terrestre universal ("GERAN/UTRAN") a un sistema de red de acceso de radio terrestre universal evolucionado ("E-UTRAN") utilizando un primer valor de entrada; y un segundo conjunto de códigos para hacer que el ordenador derive un valor de clave para un establecimiento de conexión utilizando un segundo valor de entrada, en el que el primer valor de entrada es diferente del segundo valor de entrada y es diferente de los valores de entrada derivados posteriores al segundo valor de entrada, y en el que el primer valor de entrada, el segundo valor de entrada y los valores de entrada pueden derivarse posteriores al segundo valor de entrada pueden configurarse para introducirse en una misma función de derivación de clave que puede configurarse para generar una clave para su uso entre una red entidad y un equipo de usuario. Además, el primer valor de entrada y el segundo valor de entrada pueden ser indicativos de valores de recuento de estrato sin acceso de enlace ascendente. Adicionalmente, el segundo valor de entrada puede ser un valor dentro de un primer rango de posibles valores para los valores de recuento de estrato sin acceso de enlace ascendente, y en el que el primer valor de entrada puede ser un valor fuera del primer rango de posibles valores para los valores de recuento de estrato sin acceso de enlace ascendente. Además, el primer valor de entrada puede ser indicativo del ajuste de cada bit del primer valor de entrada a uno. Adicionalmente, la derivación puede realizarse en el equipo de usuario. Sin embargo, la derivación también puede realizarse en una red que puede comprender una entidad de gestión de movilidad y una estación base, y en la que la entidad de gestión de movilidad puede realizar la derivación del valor de clave y emite un valor de clave derivado a la estación base. Además, el establecimiento de conexión puede incluir una solicitud de servicio de estrato sin acceso. Además, el primer valor de entrada y el segundo valor de entrada pueden ser indicativos de valores de recuento de estrato sin acceso, y en el que el primer valor de entrada puede ser cero, y el segundo valor de entrada y los valores de entrada que pueden derivarse después del segundo valor de entrada son distintos de cero. Además, el segundo valor de entrada puede generarse inicializando un valor de recuento de estrato sin acceso a un valor de uno. Adicionalmente, el segundo valor de entrada puede generarse inicializando un valor de recuento de estrato sin acceso de enlace ascendente a uno basado, al menos, en el traspaso que es el traspaso desde un sistema GERAN/UTRAN a un sistema E-UTRAN.

[0120] En aún otro aspecto adicional se describe un aparato, el aparato puede comprender medios para derivar un valor de clave para el traspaso desde un sistema global de comunicaciones móviles a velocidades de datos mejoradas para la red de acceso de radio evolución de GSM/red de acceso de radio terrestre universal ("GERAN/UTRAN") a un sistema de red de acceso de radio terrestre universal evolucionado ("E-UTRAN") usando un primer valor de entrada; y medios para derivar un valor de clave para un establecimiento de conexión usando un segundo valor de entrada, en el que el primer valor de entrada puede ser diferente del segundo valor de entrada y puede ser diferente de los valores de entrada derivados posteriores al segundo valor de entrada, y en el que el primer valor de entrada, el segundo valor de entrada y los valores de entrada derivados posteriores al segundo valor de entrada pueden configurarse para introducirse en una misma función de derivación de clave configurada para emitir una clave para su uso entre una entidad de red y un equipo de usuario. Además, el primer valor de entrada y el segundo valor de entrada pueden ser indicativos de valores de recuento de estrato sin acceso de enlace ascendente. Adicionalmente, el segundo valor de entrada puede ser un valor dentro de un primer rango de posibles valores para los valores de recuento de estrato sin acceso de enlace ascendente, y en el que el primer valor de entrada puede ser un valor fuera del primer rango de posibles valores para los valores de recuento de estrato sin acceso de enlace ascendente. Además, el primer valor de entrada puede ser indicativo del ajuste de cada bit del primer valor de entrada a uno. Adicionalmente, la derivación puede realizarse en el equipo de usuario. Sin embargo, la derivación también puede realizarse en una red que puede comprender una entidad de gestión de movilidad y una estación base, y en la que la entidad de gestión de movilidad puede realizar la derivación del valor de clave y emite un valor de clave derivado a la estación base. Además, el establecimiento de conexión puede incluir una solicitud de servicio de estrato sin acceso. Además, el primer valor de entrada y el segundo valor de entrada pueden ser indicativos de valores de recuento de estrato sin acceso, y en el que el primer valor de entrada puede ser cero, y el segundo valor de entrada y los valores de entrada derivados posteriores al segundo valor de entrada pueden ser

distintos de cero. Además, el segundo valor de entrada puede generarse inicializando un valor de recuento de estrato sin acceso a un valor de uno. Adicionalmente, el segundo valor de entrada puede generarse inicializando un valor de recuento de estrato sin acceso de enlace ascendente a uno basado, al menos, en el traspaso que es el traspaso desde un sistema GERAN/UTRAN a un sistema E-UTRAN.

[0121] En otro aspecto adicional se describe un aparato, el aparato puede comprender un módulo de gestión de movilidad que puede configurarse para derivar un valor de clave para el traspaso desde un sistema global de comunicaciones móviles a velocidades de datos mejoradas para la red de acceso de radio evolución de GSM/red de acceso de radio terrestre universal ("GERAN/UTRAN") a un sistema de red de acceso de radio terrestre universal evolucionado ("E-UTRAN") usando un primer valor de entrada; y derivar un valor de clave para un establecimiento de conexión usando un segundo valor de entrada, en el que el primer valor de entrada puede ser diferente del segundo valor de entrada y puede ser diferente de los valores de entrada derivados posteriores al segundo valor de entrada, y en el que el primer valor de entrada, el segundo valor de entrada y los valores de entrada derivados posteriores al segundo valor de entrada pueden configurarse para introducirse en una misma función de derivación de clave configurada para emitir una clave para su uso entre una entidad de red y un equipo de usuario. Además, el primer valor de entrada y el segundo valor de entrada pueden ser indicativos de valores de recuento de estrato sin acceso de enlace ascendente. Además, el segundo valor de entrada puede ser un valor dentro de un primer rango de posibles valores para los valores de recuento de estrato sin acceso de enlace ascendente, y en el que el primer valor de entrada puede ser un valor fuera del primer rango de posibles valores para los valores de recuento de estrato sin acceso de enlace ascendente. Además, el primer valor de entrada puede ser indicativo del ajuste de cada bit del primer valor de entrada a uno. Además, el módulo de gestión de movilidad puede ser un módulo de gestión de movilidad del equipo de usuario y la derivación puede realizarse en el equipo de usuario. Además, el módulo de gestión de la movilidad puede ser una entidad de gestión de movilidad y en el que la entidad de gestión de movilidad puede configurarse para realizar la derivación del valor de clave y para emitir un valor de clave derivado a una estación base. Además, el establecimiento de conexión puede incluir una solicitud de servicio de estrato sin acceso. Además, el primer valor de entrada y el segundo valor de entrada pueden ser indicativos de valores de recuento de estrato sin acceso, y en el que el primer valor de entrada puede ser cero, y el segundo valor de entrada y los valores de entrada derivados posteriores al segundo valor de entrada pueden ser distintos de cero. Además, el segundo valor de entrada puede generarse inicializando un valor de recuento de estrato sin acceso a un valor de uno. Sin embargo, el segundo valor de entrada puede generarse también inicializando un valor de recuento de estrato sin acceso de enlace ascendente a uno basado, al menos, en el traspaso que es el traspaso desde un sistema GERAN/UTRAN a un sistema E-UTRAN.

[0122] En otro aspecto adicional se describe un procedimiento para facilitar la seguridad de traspaso, el procedimiento puede comprender derivar un valor de clave para el traspaso desde un sistema global de comunicaciones móviles a velocidades de datos mejoradas para la red de acceso de radio de evolución de GSM/red de acceso de radio terrestre universal ("GERAN/UTRAN") a un sistema de red de acceso de radio terrestre universal evolucionado ("E-UTRAN") utilizando un primer valor de entrada; y derivar un valor de clave para un establecimiento de conexión utilizando un segundo valor de entrada, en el que el primer valor de entrada puede ser diferente del segundo valor de entrada, y en el que el primer valor de entrada y el segundo valor de entrada pueden ser valores indicativos de instancias de derivación de una clave para su uso entre una entidad de red y un equipo de usuario. Adicionalmente, el primer valor de entrada puede ser un valor distinto de 0x11.

[0123] En otro aspecto adicional, se describe un producto de programa informático, el producto de programa informático puede comprender un medio legible por ordenador que puede comprender un primer conjunto de códigos para hacer que un ordenador derive un valor de clave para el traspaso de un sistema global de comunicaciones móviles a velocidades de datos mejoradas para una red de acceso de radio de evolución de GSM/red de acceso de radio terrestre universal ("GERAN/UTRAN") a un sistema de red de acceso de radio terrestre universal evolucionado ("E-UTRAN") utilizando un primer valor de entrada; y un segundo conjunto de códigos para hacer que el ordenador derive un valor de clave para un establecimiento de conexión utilizando un segundo valor de entrada, en el que el primer valor de entrada puede ser diferente del segundo valor de entrada, y en el que el primer valor de entrada y el segundo valor de entrada son valores indicativos de instancias de derivar una clave para su uso entre una entidad de red y el equipo de usuario. Además, el primer valor de entrada puede ser un valor distinto de 0x11.

[0124] En otro aspecto adicional se describe un aparato, el aparato puede comprender medios para derivar un valor de clave para el traspaso de un sistema global de comunicaciones móviles a velocidades de datos mejoradas para la red de acceso de radio de evolución de GSM/red de acceso de radio terrestre universal ("GERAN/UTRAN") a un sistema de red de acceso de radio terrestre universal evolucionado ("E-UTRAN") utilizando un primer valor de entrada; y medios para derivar un valor de clave para un establecimiento de conexión usando un segundo valor de entrada, en el que el primer valor de entrada puede ser diferente del segundo valor de entrada, y en el que el primer valor de entrada y el segundo valor de entrada pueden ser valores indicativos de instancias de derivación de una clave para su uso entre una entidad de red y un equipo del usuario. Adicionalmente, el primer valor de entrada puede ser un valor distinto de 0x11.

[0125] En otro aspecto adicional, se describe un aparato, el aparato puede comprender un módulo de gestión de la movilidad que se puede configurar para derivar un valor de clave para el traspaso de un sistema global de comunicaciones móviles a velocidades de datos mejoradas para la red de acceso de radio de evolución de GSM/red de acceso de radio terrestre universal ("GERAN/UTRAN") a un sistema de red de acceso de radio terrestre universal evolucionado ("E-UTRAN") utilizando un primer valor de entrada; y derivar un valor de clave para un establecimiento de conexión utilizando un segundo valor de entrada, en el que el primer valor de entrada puede ser diferente del segundo valor de entrada, y en el que el primer valor de entrada y el segundo valor de entrada son valores indicativos de instancias de derivar una clave para su uso entre una entidad de red y el equipo de usuario. Además, el primer valor de entrada puede ser un valor distinto de 0x11.

REIVINDICACIONES

1. Un procedimiento para facilitar la seguridad de traspaso, comprendiendo el procedimiento:

derivar (610) un valor de clave para el traspaso desde un sistema global de comunicaciones móviles a velocidades de datos mejoradas para la red de acceso de radio de evolución de GSM/red de acceso de radio terrestre universal, GERAN/UTRAN, a un sistema de red de acceso de radio terrestre universal evolucionada, E-UTRAN, usando un primer valor de entrada; y

derivar (620) un valor de clave para un establecimiento de conexión utilizando un segundo valor de entrada, en el que el primer valor de entrada es diferente del segundo valor de entrada y es diferente de los valores de entrada derivados posteriores al segundo valor de entrada, y en el que el primer valor de entrada, el segundo valor de entrada y los valores de entrada derivados posteriores al segundo valor de entrada se configuran para introducirse en una misma función de derivación de clave configurada para emitir una clave para su uso entre una entidad de red y un equipo de usuario, en el que el primer valor de entrada y el segundo valor de entrada son indicativos de valores de recuento de estrato sin acceso de enlace ascendente, y en el que el segundo valor de entrada es un valor dentro del rango de posibles valores para los valores de recuento de estrato sin acceso de enlace ascendente, y en el que el primer valor de entrada es un valor fuera del rango de posibles valores para los valores de recuento de estrato sin acceso de enlace ascendente.

2. El procedimiento según la reivindicación 1, en el que el primer valor de entrada es indicativo de ajustar cada bit del primer valor de entrada a uno.

3. El procedimiento según la reivindicación 1, en el que la derivación se realiza en el equipo de usuario (804, 824).

4. El procedimiento según la reivindicación 1, en el que la derivación se realiza en una red (802, 822) que comprende una entidad de gestión de movilidad (812, 832) y una estación base, y en el que la entidad de gestión de movilidad (812, 832) realiza la derivación del valor de clave y emite un valor de clave derivado a la estación base.

5. El procedimiento según la reivindicación 1, en el que el establecimiento de conexión incluye una solicitud de servicio de estrato sin acceso.

6. El procedimiento según la reivindicación 1, en el que el primer valor de entrada y el segundo valor de entrada son indicativos de valores de recuento de estrato sin acceso, y en el que el primer valor de entrada es un valor de cero, y el segundo valor de entrada y valores de entrada derivados posteriores al segundo valor de entrada son distintos de cero.

7. El procedimiento según la reivindicación 6, en el que el segundo valor de entrada se genera inicializando un valor de recuento de estrato sin acceso a un valor de uno.

8. El procedimiento según la reivindicación 6, en el que el segundo valor de entrada se genera inicializando un valor de recuento de estrato sin acceso de enlace ascendente a uno basado, al menos, en el traspaso que es un traspaso desde un sistema GERAN/UTRAN a un sistema E-UTRAN.

9. Un aparato, que comprende:

medios para derivar (904) un valor de clave para el traspaso desde un sistema global de comunicaciones móviles a velocidades de datos mejoradas para la red de acceso de radio de evolución de GSM/red de acceso de radio terrestre universal, GERAN/UTRAN, a un sistema de red de acceso de radio terrestre universal evolucionada, E-UTRAN, usando un primer valor de entrada; y

medios para derivar (906) un valor de clave para un establecimiento de conexión utilizando un segundo valor de entrada, en el que el primer valor de entrada es diferente del segundo valor de entrada y es diferente de los valores de entrada derivados posteriores al segundo valor de entrada, y en el que el primer valor de entrada, el segundo valor de entrada y los valores de entrada derivados posteriores al segundo valor de entrada se configuran para introducirse en una misma función de derivación de clave configurada para emitir una clave para su uso entre una entidad de red y un equipo de usuario, en el que el primer valor de entrada y el segundo valor de entrada son indicativos de valores de recuento de estrato sin acceso de enlace ascendente, y en el que el segundo valor de entrada es un valor dentro del rango de posibles valores para los valores de recuento de estrato sin acceso de enlace ascendente, y en el que el primer valor de entrada es un valor fuera del rango de posibles valores para los valores de recuento de estrato sin acceso de enlace ascendente.

10. El aparato de la reivindicación 9, en el que el primer valor de entrada es indicativo de ajustar cada bit del primer valor de entrada a uno.

11. El aparato de la reivindicación 9, en el que la derivación se realiza en el equipo de usuario (804, 824).

12. El aparato según la reivindicación 9, en el que la derivación se realiza en una red (802, 822) que comprende una entidad de gestión de movilidad (812, 832) y una estación base, y en el que la entidad de gestión de movilidad (812, 832) realiza la derivación del valor de clave y emite un valor de clave derivado a la estación base.

13. El aparato de la reivindicación 9, en el que el establecimiento de conexión incluye una solicitud de servicio de estrato sin acceso.

14. El aparato de la reivindicación 9, en el que el primer valor de entrada y el segundo valor de entrada son indicativos de valores de recuento de estrato sin acceso, y en el que el primer valor de entrada es un valor de cero, y el segundo valor de entrada y valores de entrada derivados posteriores al segundo valor de entrada son distintos de cero.

15. Un producto de programa informático, que comprende:

un medio legible por ordenador, que comprende:

código para hacer que un ordenador realice un procedimiento de acuerdo con cualquiera de las reivindicaciones 1 a 8.

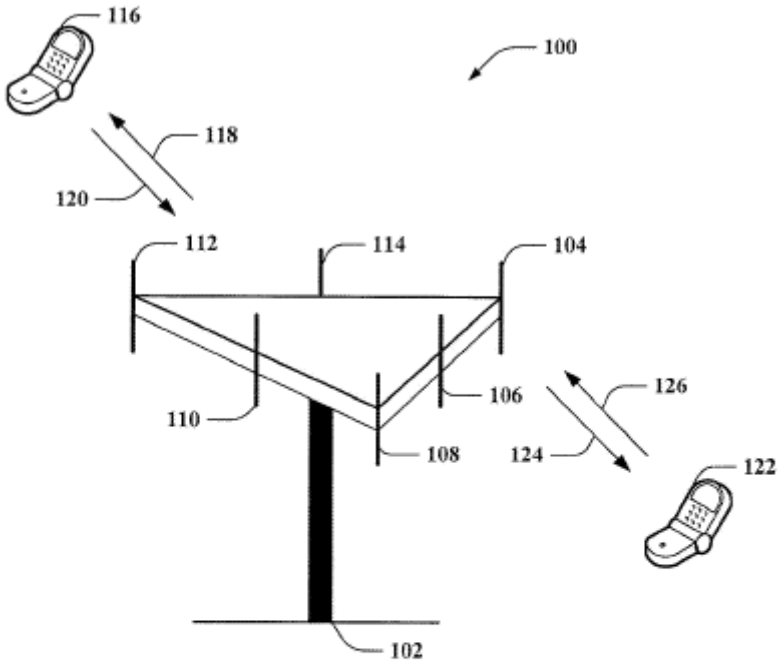


FIG. 1

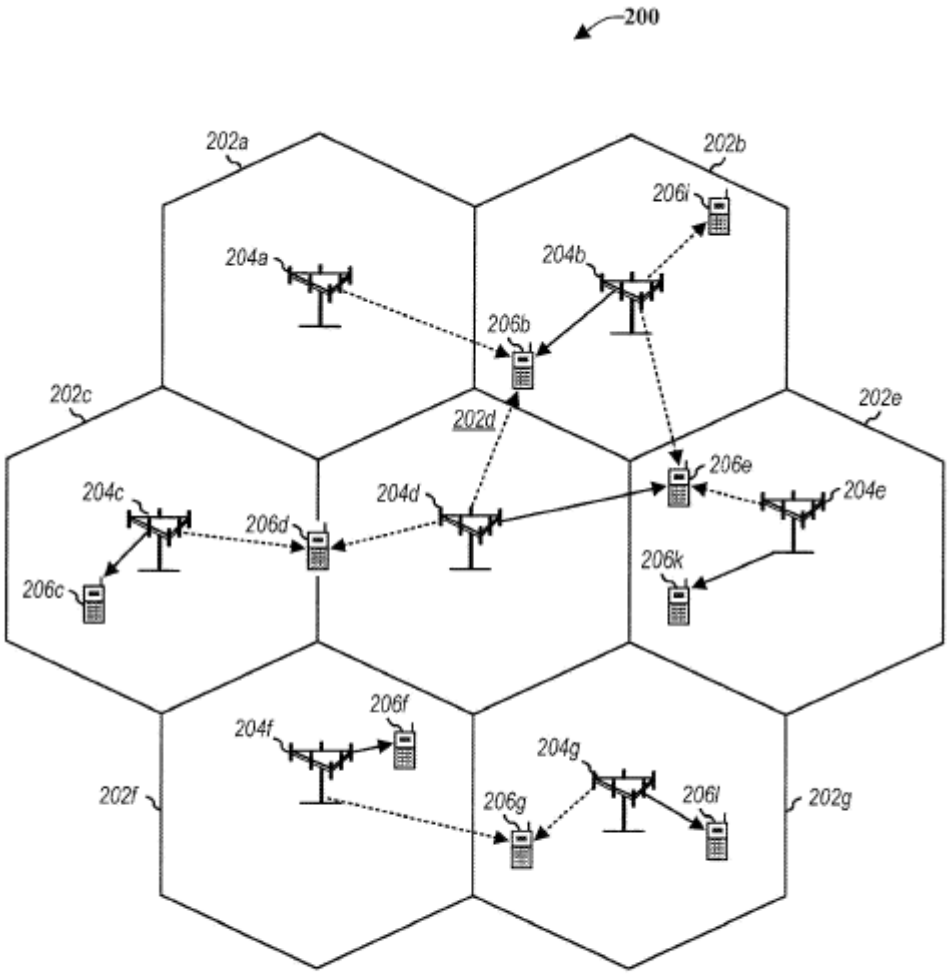

200
202a
202b
206i
204a
204b
206b
202c
202d
202e
206e
204c
204d
204e
206d
206k
206c
206f
204f
204g
202f
206g
206l
202g

FIG. 2

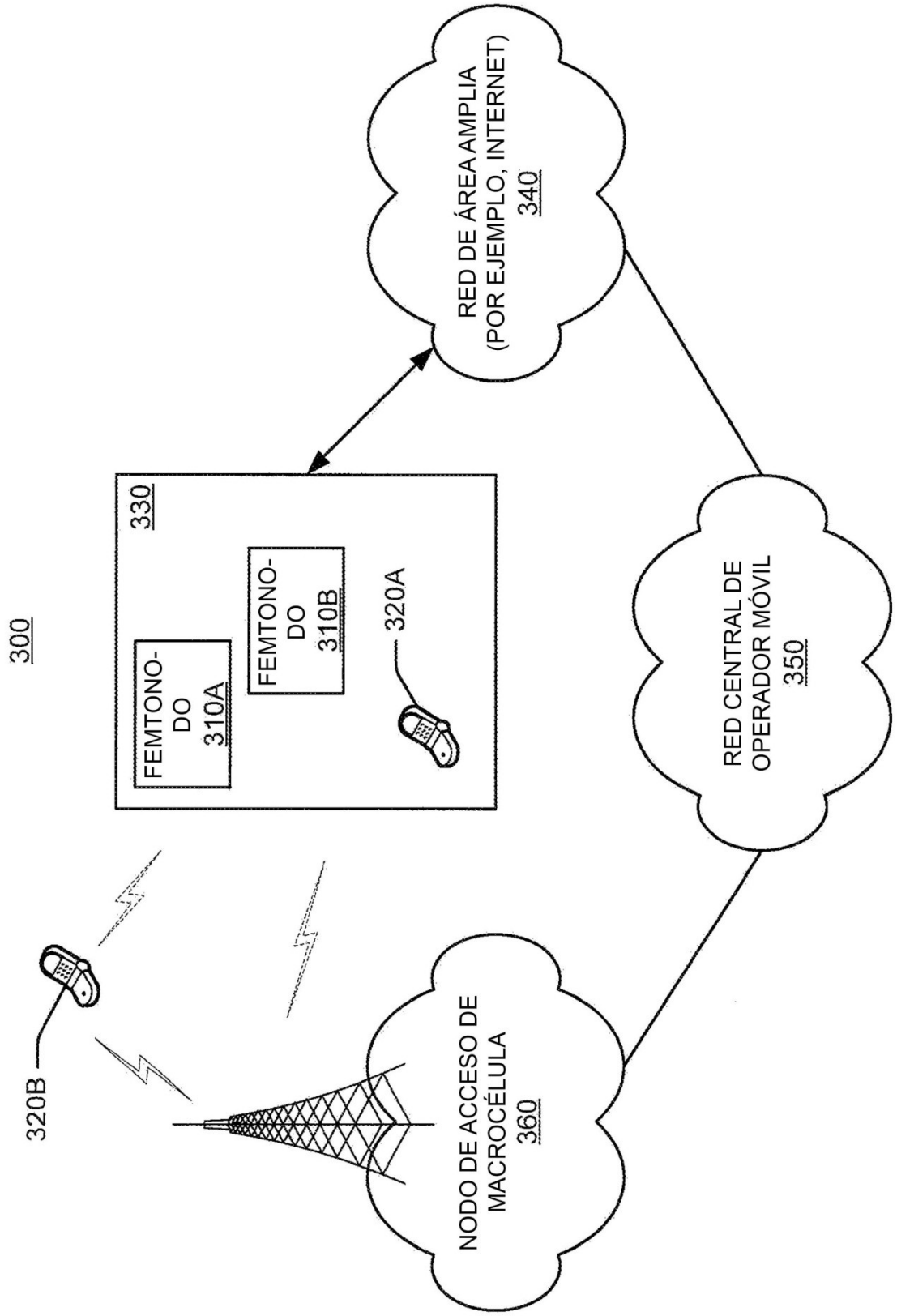

300
330
FEMTONO-DO 310A
FEMTONO-DO 310B
320A
320B
RED DE ÁREA AMPLIA (POR EJEMPLO, INTERNET) 340
RED CENTRAL DE OPERADOR MÓVIL 350
NODO DE ACCESO DE MACROCÉLULA 360

FIG. 3

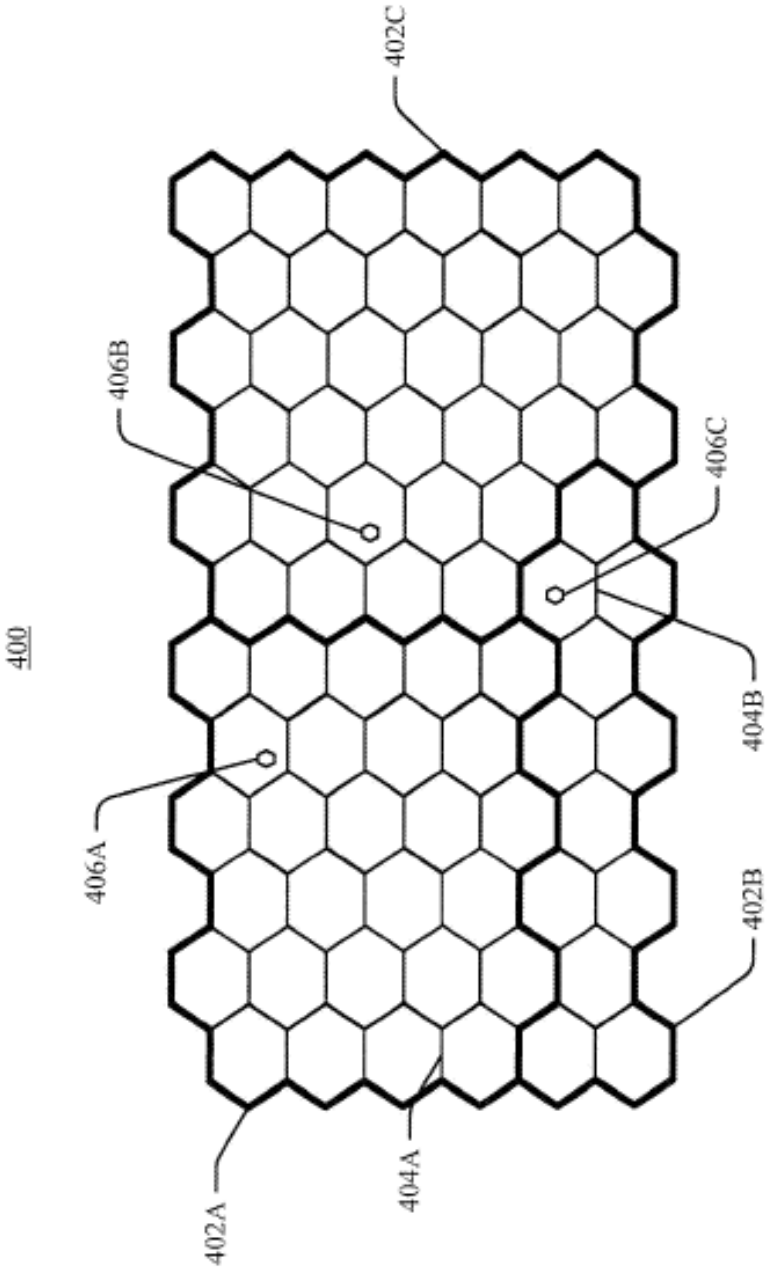


FIG. 4

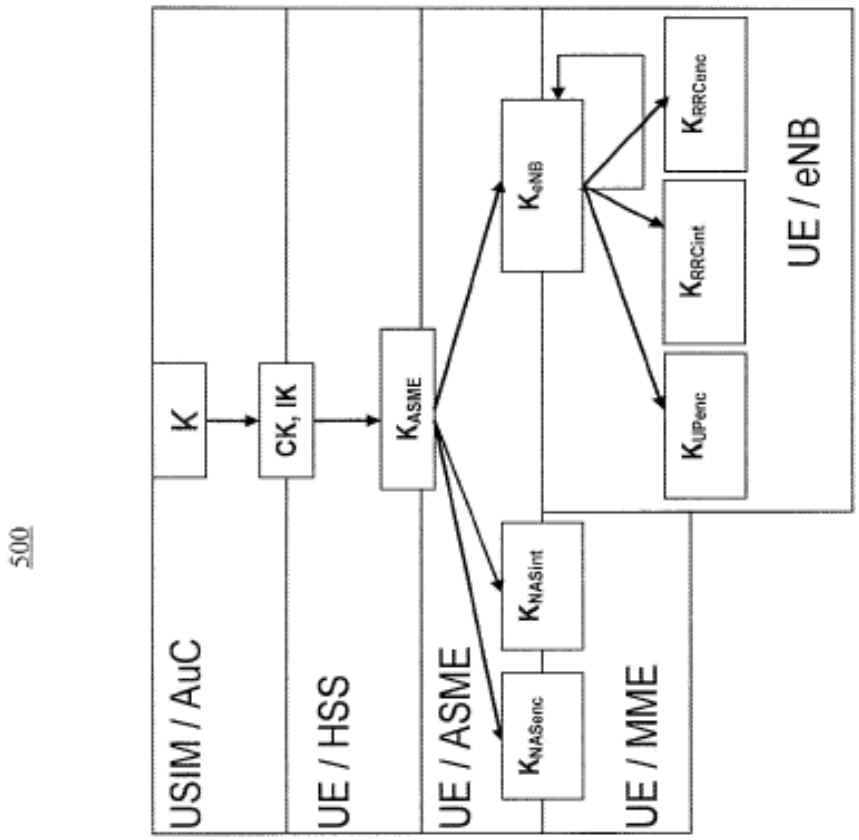

500
USIM / AuC
UE / HSS
UE / ASME
UE / MME
UE / eNB
K
CK, IK
KASME
KeNB
KNASint
KNASenc
KRRCenc
KRRCint
KUPenc

FIG. 5A

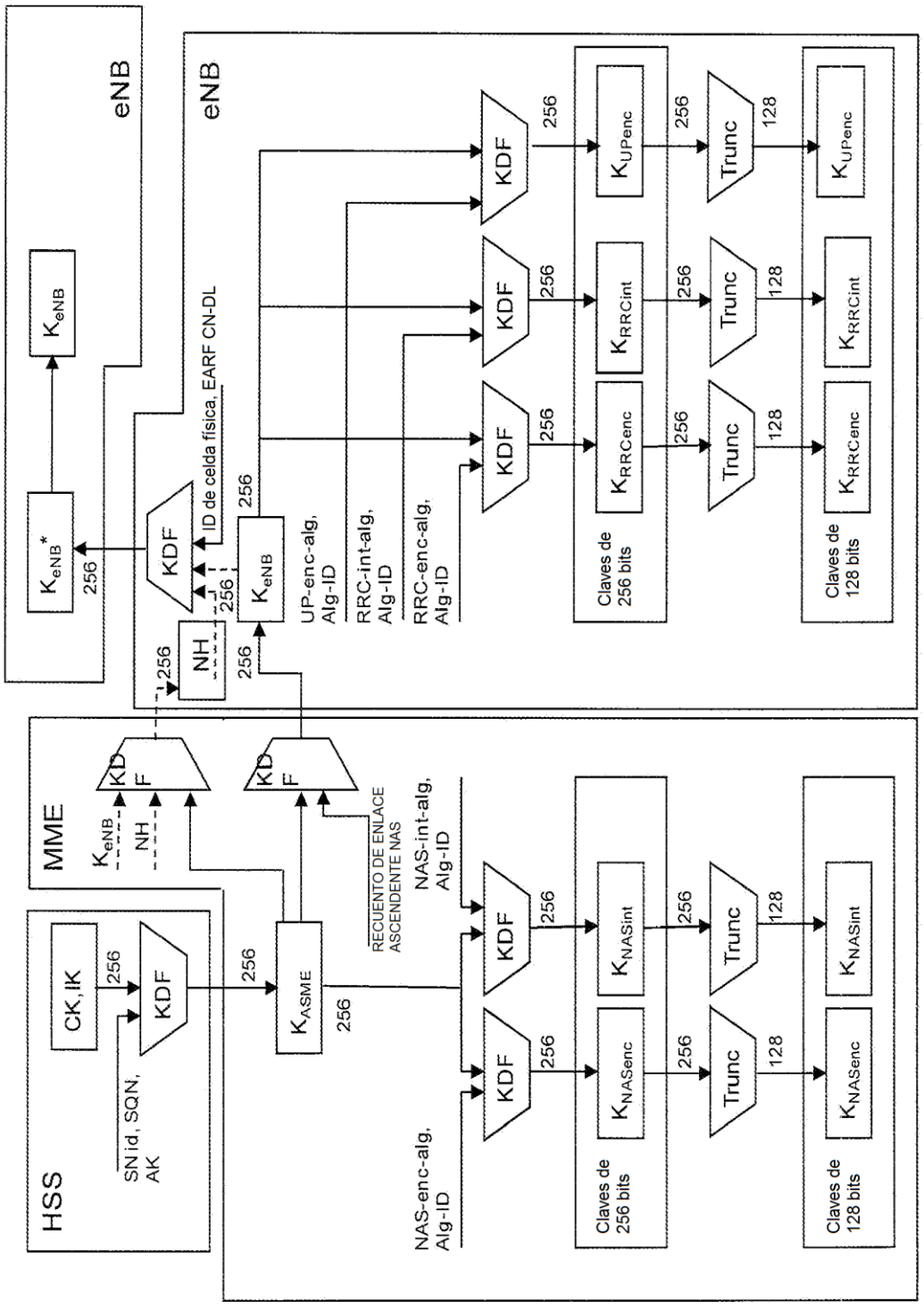

HSS
CK, IK
256
KDF
SNid, SQN, AK
MME
256
K_{ASME}
256
KDF
K_{eNB}
NH
256
K_{eNB}
256
KDF
ID de celda física, EARF CN-DL
256
K_{eNB}
256
NH
256
eNB
K_{eNB}^*
256
K_{eNB}
eNB
RECUENTO DE ENLACE ASCENDENTE NAS
NAS-int-alg, Alg-ID
NAS-enc-alg, Alg-ID
UP-enc-alg, Alg-ID
RRC-int-alg, Alg-ID
RRC-enc-alg, Alg-ID
KDF
256
K_{NASint}
K_{NASenc}
K_{RRCint}
K_{RRCenc}
K_{UPenc}
Claves de 256 bits
Trunc
128
Claves de 128 bits

FIG. 5B

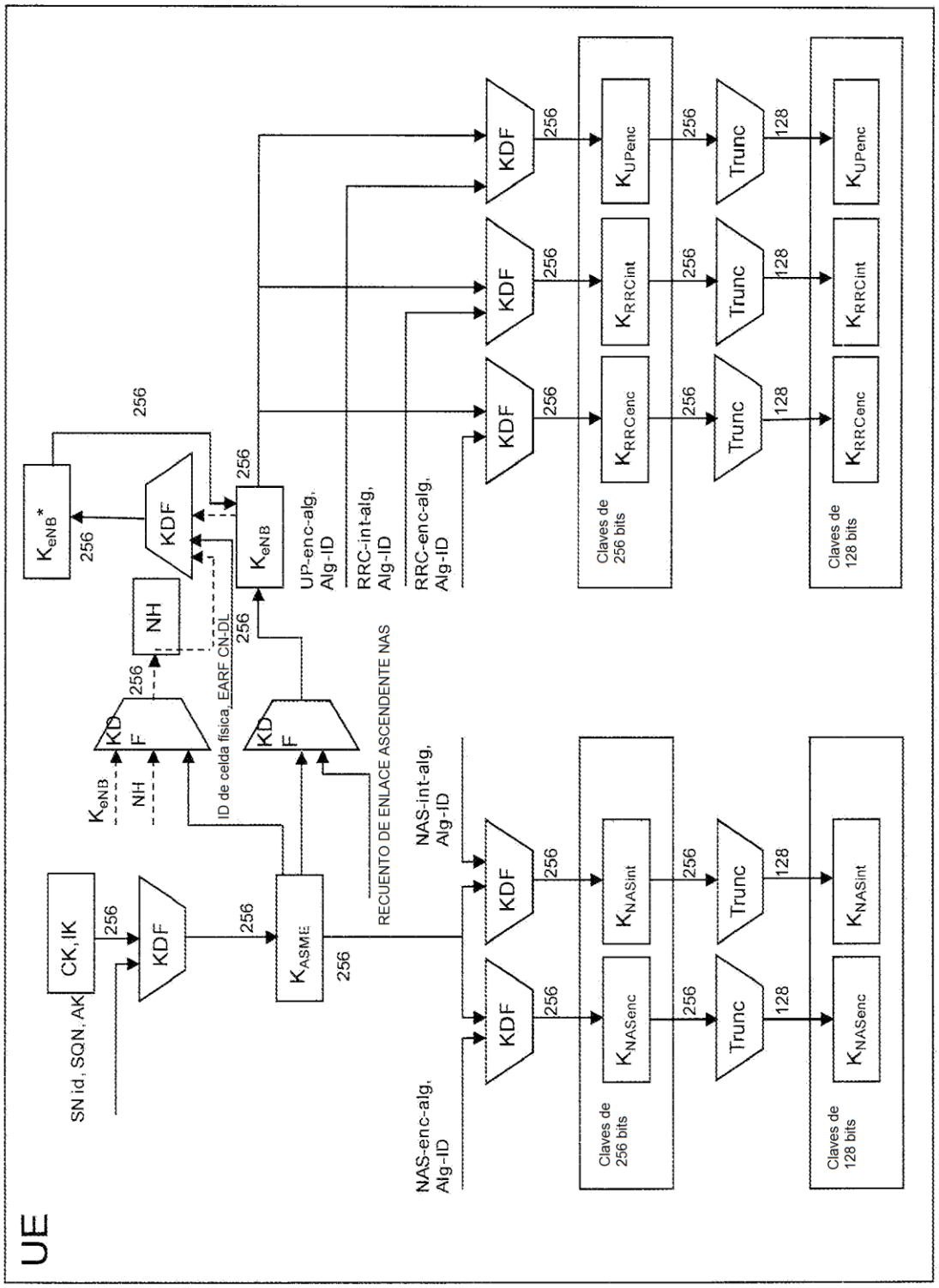

UE
CK, IK
SN id, SQN, AK
KDF
256
K_{ASME}
K_{eNB}
NH
ID de celda física, EARFCN-DL
K_{eNB}*
UP-enc-alg, Alg-ID
RRC-int-alg, Alg-ID
RRC-enc-alg, Alg-ID
NAS-int-alg, Alg-ID
NAS-enc-alg, Alg-ID
RECUENTO DE ENLACE ASCENDENTE NAS
K_{UPenc}
K_{RRCint}
K_{RRCenc}
K_{NASint}
K_{NASenc}
Claves de 256 bits
Claves de 128 bits
Trunc
128

FIG. 5C

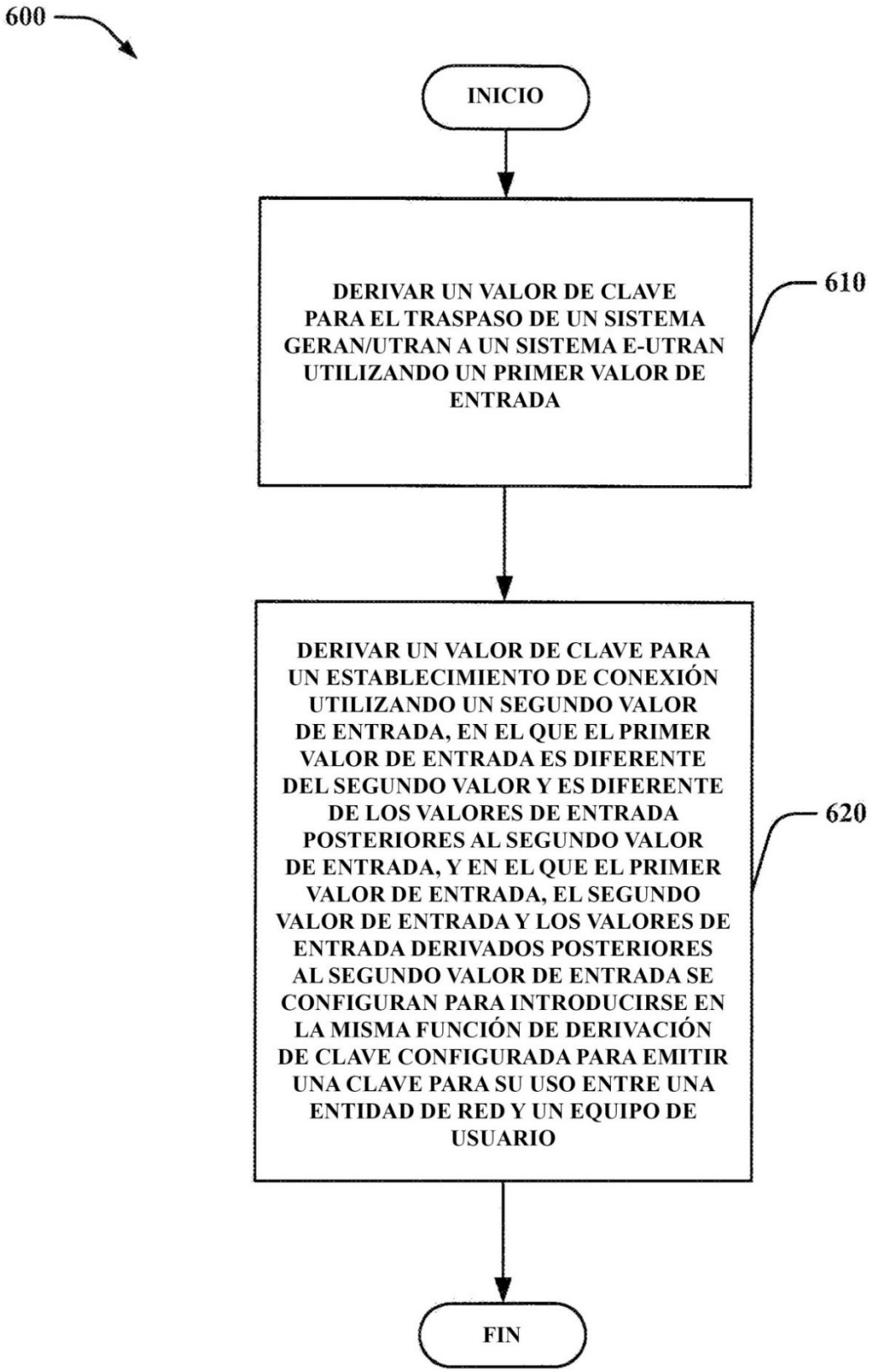

600
INICIO
DERIVAR UN VALOR DE CLAVE PARA EL TRASPASO DE UN SISTEMA GERAN/UTRAN A UN SISTEMA E-UTRAN UTILIZANDO UN PRIMER VALOR DE ENTRADA
610
DERIVAR UN VALOR DE CLAVE PARA UN ESTABLECIMIENTO DE CONEXIÓN UTILIZANDO UN SEGUNDO VALOR DE ENTRADA, EN EL QUE EL PRIMER VALOR DE ENTRADA ES DIFERENTE DEL SEGUNDO VALOR Y ES DIFERENTE DE LOS VALORES DE ENTRADA POSTERIORES AL SEGUNDO VALOR DE ENTRADA, Y EN EL QUE EL PRIMER VALOR DE ENTRADA, EL SEGUNDO VALOR DE ENTRADA Y LOS VALORES DE ENTRADA DERIVADOS POSTERIORES AL SEGUNDO VALOR DE ENTRADA SE CONFIGURAN PARA INTRODUCIRSE EN LA MISMA FUNCIÓN DE DERIVACIÓN DE CLAVE CONFIGURADA PARA EMITIR UNA CLAVE PARA SU USO ENTRE UNA ENTIDAD DE RED Y UN EQUIPO DE USUARIO
620
FIN

FIG. 6

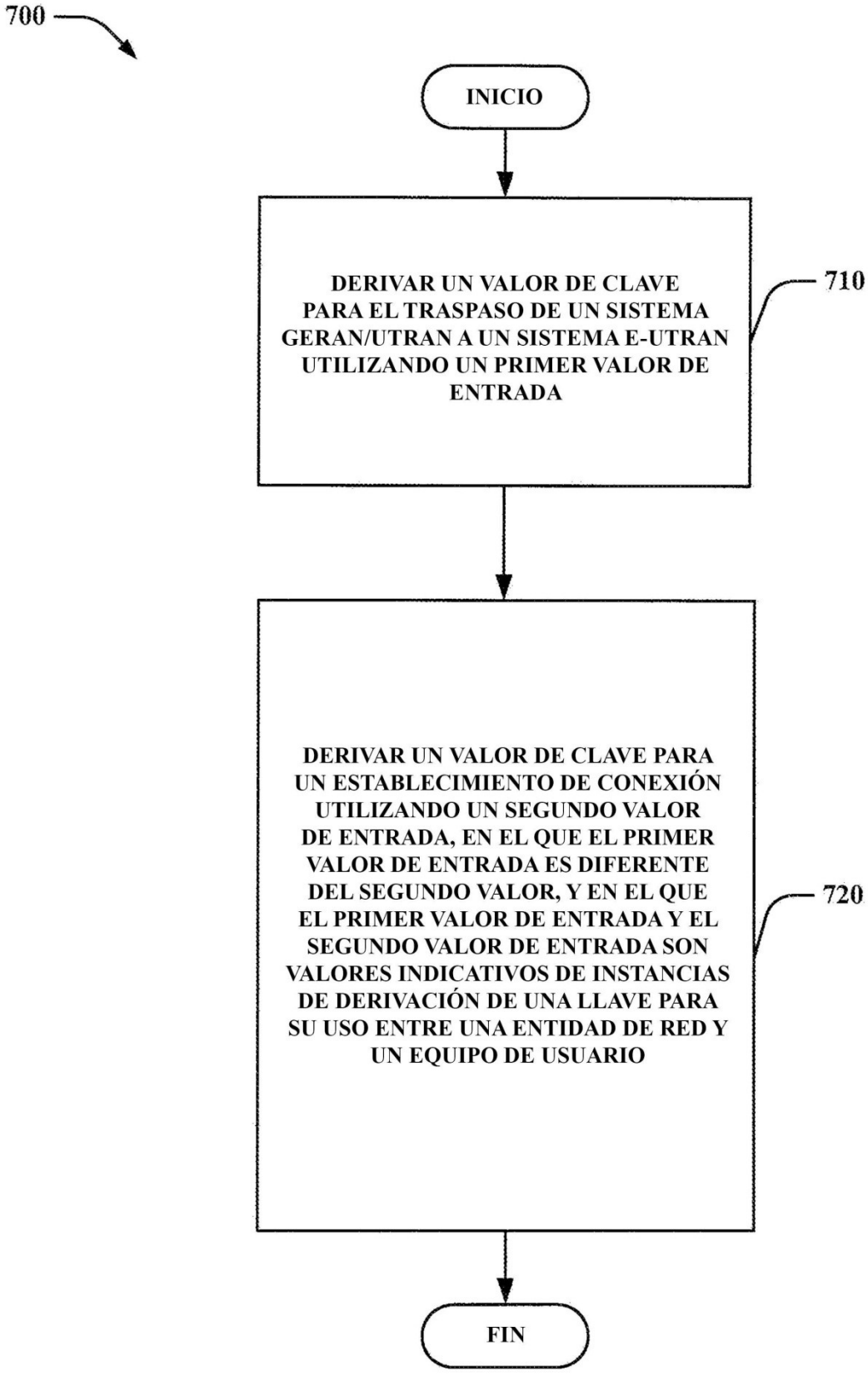

700
INICIO
DERIVAR UN VALOR DE CLAVE PARA EL TRASPASO DE UN SISTEMA GERAN/UTRAN A UN SISTEMA E-UTRAN UTILIZANDO UN PRIMER VALOR DE ENTRADA
710
DERIVAR UN VALOR DE CLAVE PARA UN ESTABLECIMIENTO DE CONEXIÓN UTILIZANDO UN SEGUNDO VALOR DE ENTRADA, EN EL QUE EL PRIMER VALOR DE ENTRADA ES DIFERENTE DEL SEGUNDO VALOR, Y EN EL QUE EL PRIMER VALOR DE ENTRADA Y EL SEGUNDO VALOR DE ENTRADA SON VALORES INDICATIVOS DE INSTANCIAS DE DERIVACIÓN DE UNA LLAVE PARA SU USO ENTRE UNA ENTIDAD DE RED Y UN EQUIPO DE USUARIO
720
FIN

FIG. 7

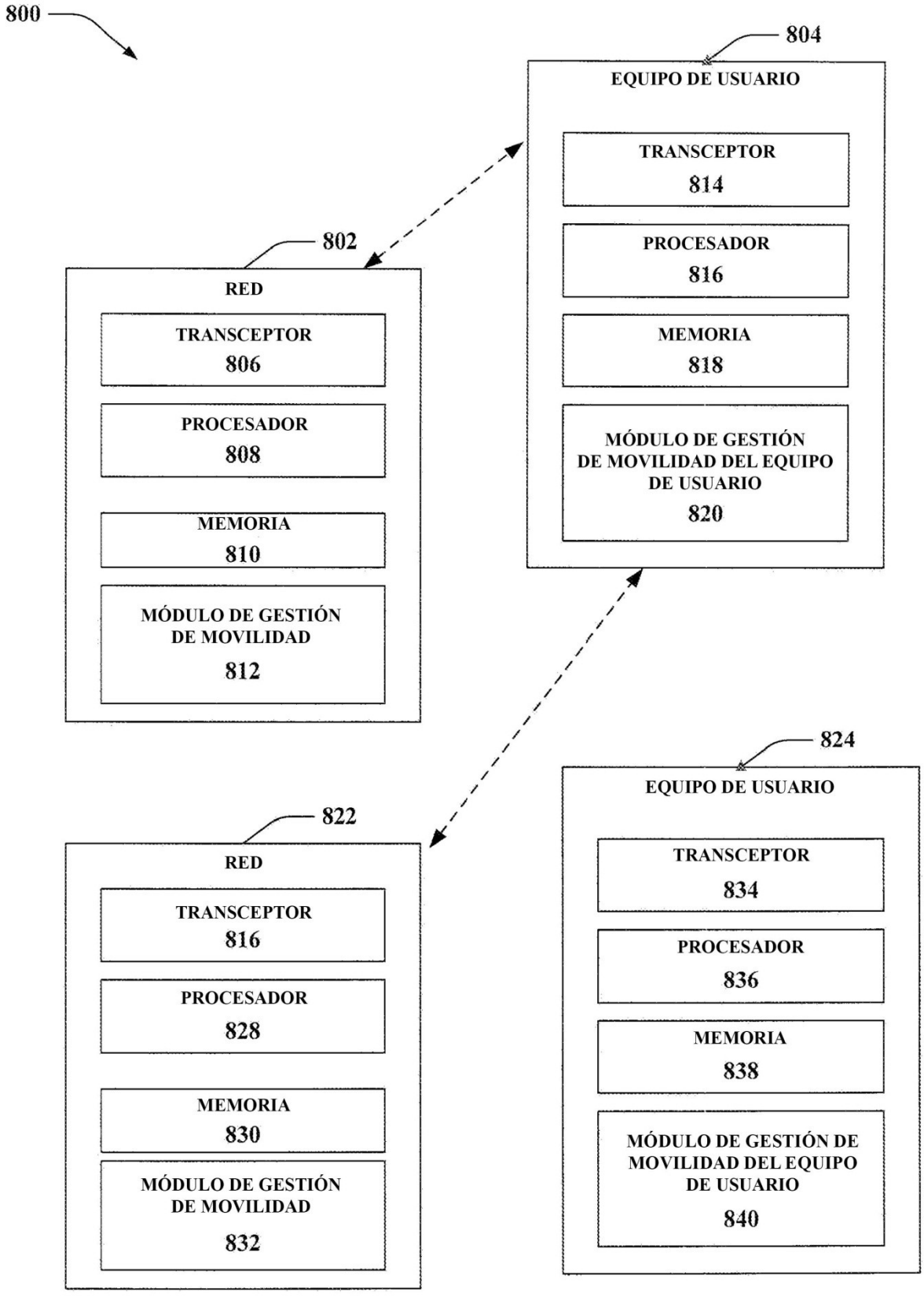

800
804
EQUIPO DE USUARIO
TRANSCEPTOR
814
PROCESADOR
816
MEMORIA
818
MÓDULO DE GESTIÓN DE MOVILIDAD DEL EQUIPO DE USUARIO
820
802
RED
TRANSCEPTOR
806
PROCESADOR
808
MEMORIA
810
MÓDULO DE GESTIÓN DE MOVILIDAD
812
824
EQUIPO DE USUARIO
TRANSCEPTOR
834
PROCESADOR
836
MEMORIA
838
MÓDULO DE GESTIÓN DE MOVILIDAD DEL EQUIPO DE USUARIO
840
822
RED
TRANSCEPTOR
816
PROCESADOR
828
MEMORIA
830
MÓDULO DE GESTIÓN DE MOVILIDAD
832

FIG. 8A

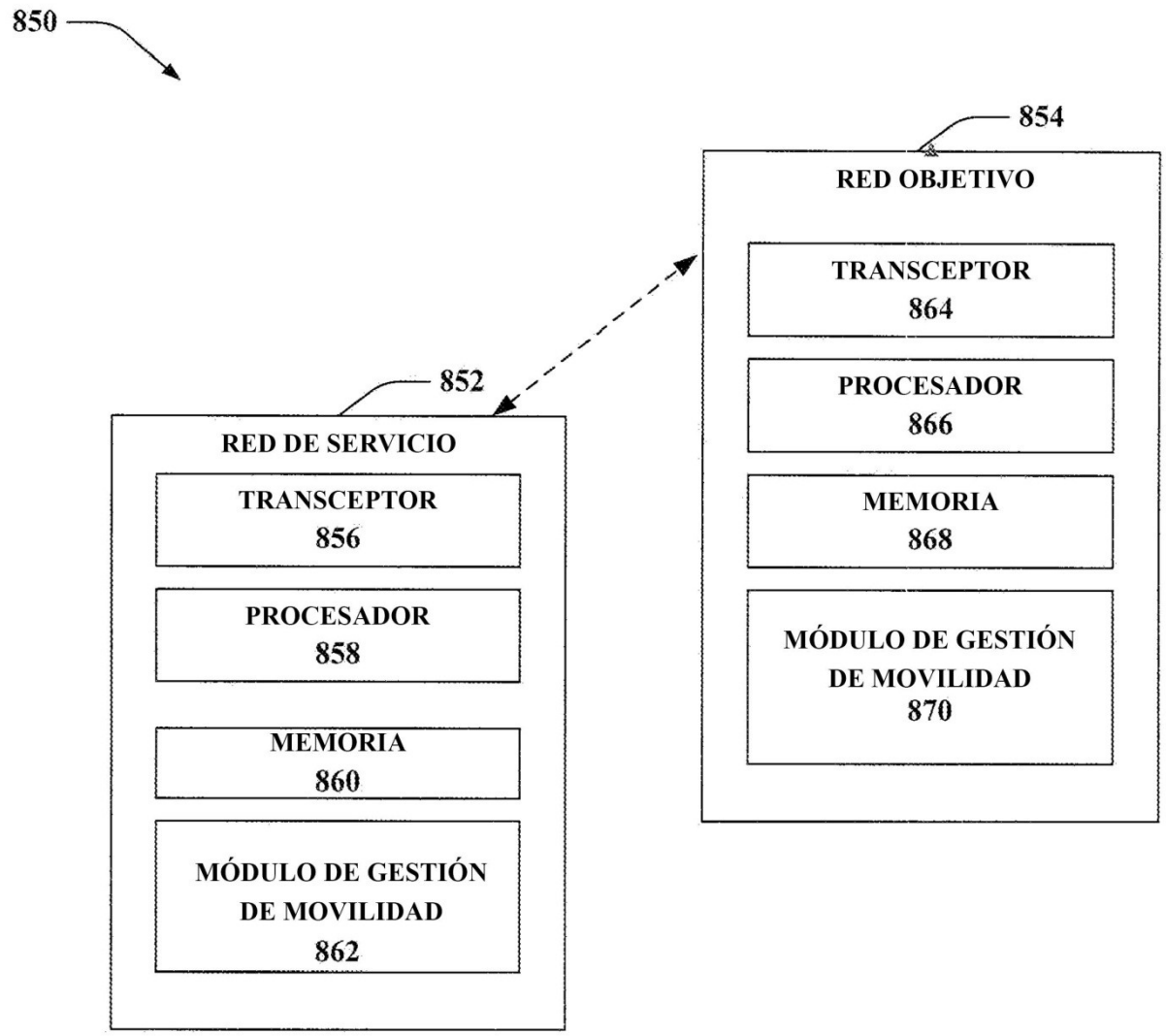

850
854
RED OBJETIVO
TRANSCEPTOR
864
PROCESADOR
866
MEMORIA
868
MÓDULO DE GESTIÓN
DE MOVILIDAD
870
852
RED DE SERVICIO
TRANSCEPTOR
856
PROCESADOR
858
MEMORIA
860
MÓDULO DE GESTIÓN
DE MOVILIDAD
862

FIG. 8B

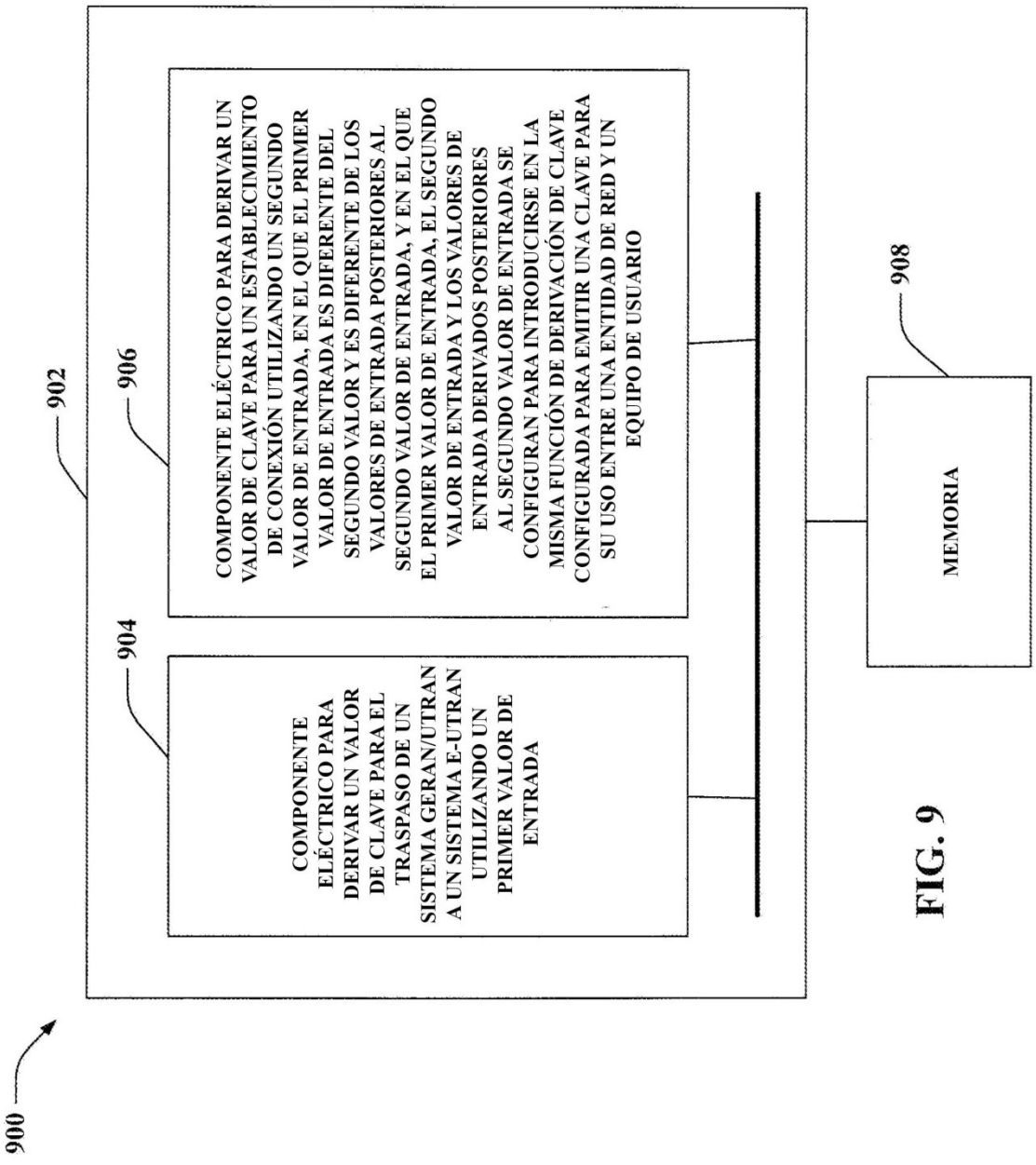

900
902
904
COMPONENTE ELÉCTRICO PARA DERIVAR UN VALOR DE CLAVE PARA EL TRASPASO DE UN SISTEMA GERAN/UTRAN A UN SISTEMA E-UTRAN UTILIZANDO UN PRIMER VALOR DE ENTRADA
906
COMPONENTE ELÉCTRICO PARA DERIVAR UN VALOR DE CLAVE PARA UN ESTABLECIMIENTO DE CONEXIÓN UTILIZANDO UN SEGUNDO VALOR DE ENTRADA, EN EL QUE EL PRIMER VALOR DE ENTRADA ES DIFERENTE DEL SEGUNDO VALOR Y ES DIFERENTE DE LOS VALORES DE ENTRADA POSTERIORES AL SEGUNDO VALOR DE ENTRADA, Y EN EL QUE EL PRIMER VALOR DE ENTRADA, EL SEGUNDO VALOR DE ENTRADA Y LOS VALORES DE ENTRADA DERIVADOS POSTERIORES AL SEGUNDO VALOR DE ENTRADA SE CONFIGURAN PARA INTRODUCIRSE EN LA MISMA FUNCIÓN DE DERIVACIÓN DE CLAVE CONFIGURADA PARA EMITIR UNA CLAVE PARA SU USO ENTRE UNA ENTIDAD DE RED Y UN EQUIPO DE USUARIO
908
MEMORIA

FIG. 9

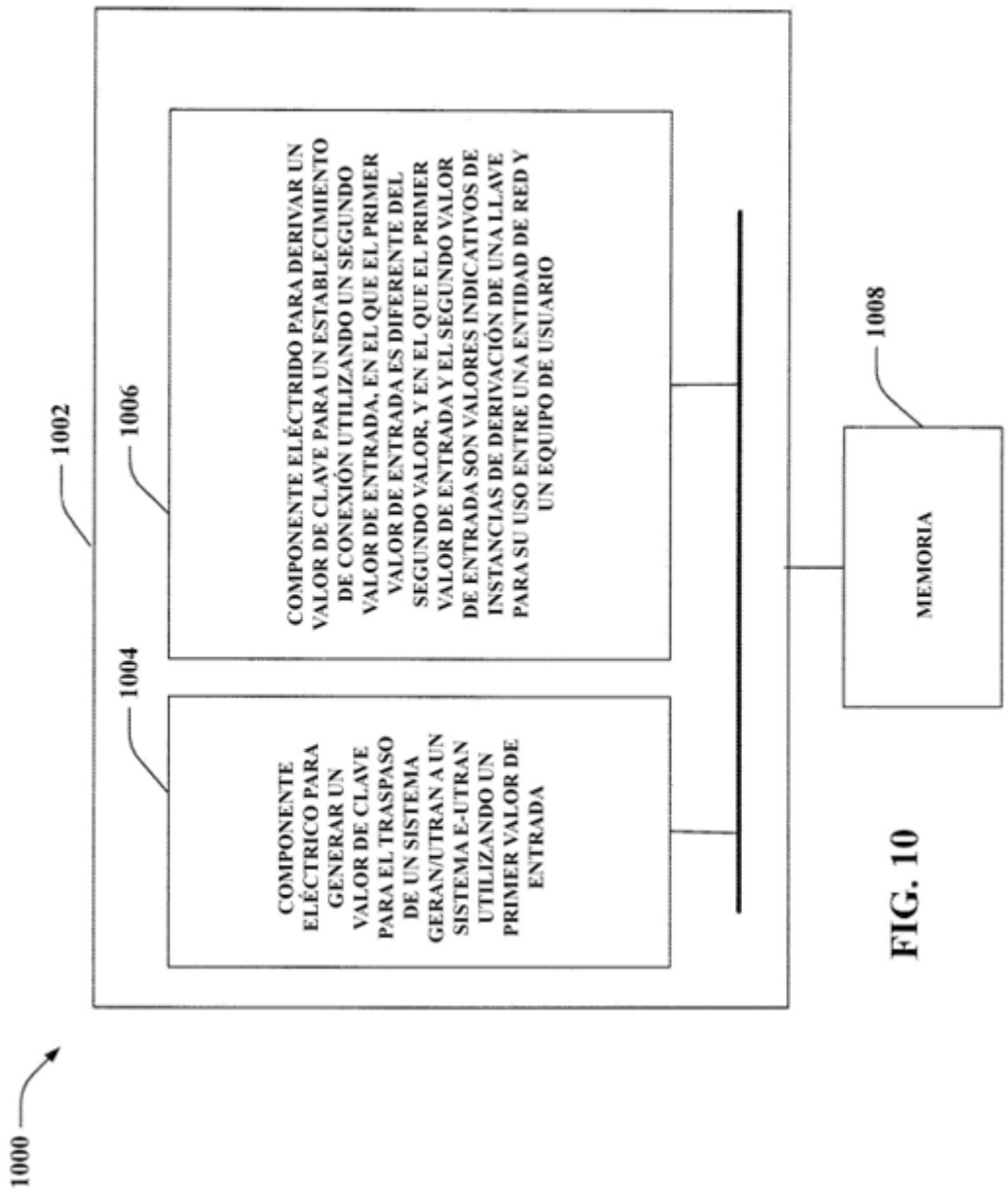

1000
1002
1004
COMPONENTE ELÉCTRICO PARA GENERAR UN VALOR DE CLAVE PARA EL TRASPASO DE UN SISTEMA GERAN/UTRAN A UN SISTEMA E-UTRAN UTILIZANDO UN PRIMER VALOR DE ENTRADA
1006
COMPONENTE ELÉCTRIDO PARA DERIVAR UN VALOR DE CLAVE PARA UN ESTABLECIMIENTO DE CONEXIÓN UTILIZANDO UN SEGUNDO VALOR DE ENTRADA, EN EL QUE EL PRIMER VALOR DE ENTRADA ES DIFERENTE DEL SEGUNDO VALOR, Y EN EL QUE EL PRIMER VALOR DE ENTRADA Y EL SEGUNDO VALOR DE ENTRADA SON VALORES INDICATIVOS DE INSTANCIAS DE DERIVACIÓN DE UNA LLAVE PARA SU USO ENTRE UNA ENTIDAD DE RED Y UN EQUIPO DE USUARIO
1008
MEMORIA

FIG. 10

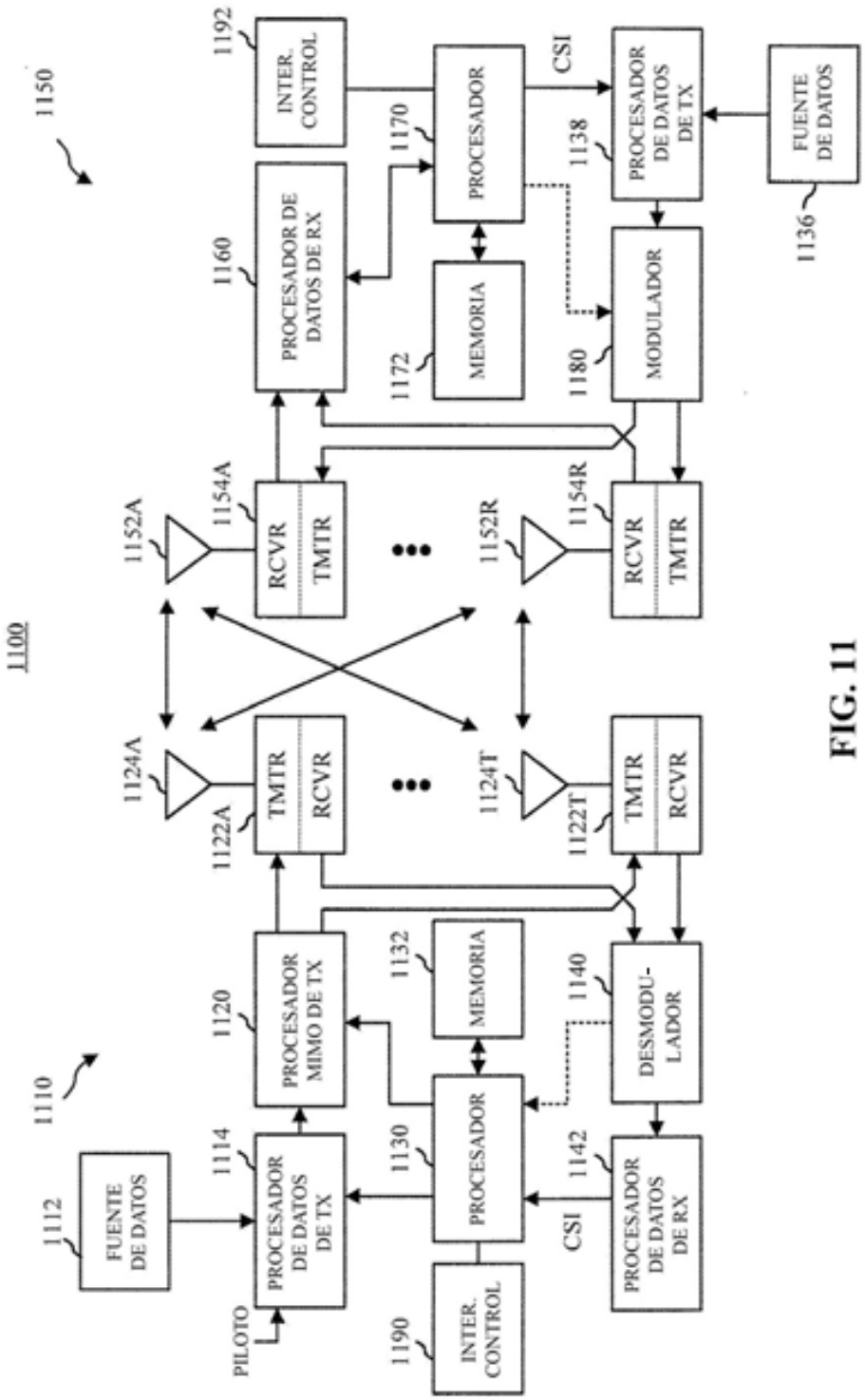

1100
1110
1112
FUENTE DE DATOS
1114
PROCESADOR DE DATOS DE TX
PILOTO
1120
PROCESADOR MIMO DE TX
1122A
TMTR
RCVR
1124A
1124T
1122T
1130
PROCESADOR
1132
MEMORIA
1140
DESMODU-LADOR
1142
PROCESADOR DE DATOS DE RX
CSI
1190
INTER. CONTROL
1150
1152A
1152R
1154A
1154R
RCVR
TMTR
1160
PROCESADOR DE DATOS DE RX
1170
PROCESADOR
1172
MEMORIA
1180
MODULADOR
1138
CSI
1192
INTER. CONTROL
PROCESADOR DE DATOS DE TX
1136
FUENTE DE DATOS

FIG. 11