(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 764 994**

(51) Int. CI.:

H04W 12/04 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **05.12.2008 E 08021197 (2)**

(97) Fecha y número de publicación de la concesión europea: **06.11.2019 EP 2071885**

(54) Título: **Método de gestión de cambio de clave de seguridad y dispositivo de comunicación relacionado**

(30) Prioridad:

05.12.2007 US 992675 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
05.06.2020

(73) Titular/es:

INNOVATIVE SONIC LIMITED (100.0%)
2nd Floor, The Axis, 26 Cybercity
72201 Ebene , MU

(72) Inventor/es:

KUO, RICHARD LEE-CHEE

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

Método de gestión de cambio de clave de seguridad y dispositivo de comunicación relacionado

3GPP R3-071942 “Key Update in LTE-Active state” de HUAWEI da a conocer procedimientos de actualización de clave para el estado LTE_Active.

3GPP TR 33,821 “Rationale and track of security decisions in Long Term Evolved (LTE) RAN/3GPP System Architecture Evolution” (versión 8) da a conocer diferentes procesos que comprenden acuerdo de autenticación y clave.

3GPP R3-072066 “ACTIVE mode key change” de SA3 da a conocer diferentes procesos para un cambio de clave de AS.

La presente invención se refiere a un método y a un aparato para gestionar un cambio de clave de seguridad para un sistema de comunicación inalámbrico según las partes precaracterizantes de las reivindicaciones independientes.

El sistema de comunicaciones móvil de tercera generación (3G) ha adoptado un método de acceso por interfaz aérea inalámbrica de acceso múltiple por división de código de banda ancha (WCDMA) para una red celular. WCDMA puede proporcionar un uso de espectro a alta frecuencia, cobertura universal y transmisión de datos multimedia con alta calidad y alta velocidad. El método de WCDMA también cumple todas las clases de requisitos de QoS (calidad de servicio) de manera simultánea, proporcionando diversos servicios de transmisión bidireccional flexible y mejor calidad de comunicación para reducir las tasas de interrupción de la transmisión.

Con el fin de proteger los datos de usuarios e información de señalización para que no se intercepte por dispositivos no autorizados, el sistema de comunicaciones móvil de 3G de la técnica anterior puede activar cifrado o protección de integridad (IP) mediante un procedimiento de control de modo de seguridad (SMC) y asegurarse de que la transmisión de datos es más segura. El procedimiento de cifrado calcula datos de secuencia de claves a través de un algoritmo de cifrado, después el transmisor cifra datos de texto claro con los datos de secuencia de claves para generar datos de texto cifrado, y el receptor puede descifrar los datos de texto cifrado recibidos con datos de secuencia de claves iguales que los datos de secuencia de claves usados en el transmisor, para obtener los datos de texto claro.

Con respecto a la seguridad de la transferencia de datos, el proyecto de asociación de 3ª generación, 3GPP, desarrolla una especificación de arquitectura de seguridad para proporcionar un acuerdo de autenticación y clave (AKA) para su uso entre el UE y la red central (CN). Con el acuerdo de autenticación y clave, el UE y la CN pueden autenticarse entre sí y garantizar la seguridad y el cifrado de datos. Es decir, se asignará un nuevo conjunto de claves al UE tras ejecutarse el AKA en una capa de gestión móvil (MM).

Véase la figura 1, que es un diagrama esquemático de una jerarquía de calves para una evolución a largo plazo (LTE) en un sistema de comunicación inalámbrico. Basándose en diferentes niveles de seguridad, el UE incluye una clave permanente K, una clave de cifrado (CK), una clave de integridad (IK), una clave de base KASME, una clave de cifrado de estrato de no acceso K(NAS, enc), una integridad de estrato de no acceso K(NAS, int) y una clave de nivel de estación base KeNB. La clave permanente K existe en un módulo de identidad de abonado universal (USIM). La CK y la IK se usan para el cifrado y la protección de integridad en un sistema de telecomunicación móvil universal (UMTS). La KASME se usa entre el UE y una entidad de gestión de seguridad de acceso (ASME). En cuanto a un estrato de no acceso (NAS), la K(NAS, enc) y la K(NAS, int) se usan para el cifrado y la protección de integridad de un mensaje de estrato de no acceso, respectivamente. Una clave de plano de usuario (UP) KeNB-UP-enc y claves de control de recursos de radio (RRC) KeNB-RRC-int y KeNB-RRC-enc se derivan de la KeNB y se usan para el cifrado para datos de plano de usuario, integridad para mensajes de RRC y cifrado para los mensajes de RRC, respectivamente. La relación de derivación de claves entre cada nivel se ilustra en la figura 1. Por ejemplo, la KeNB puede derivarse a partir de la KASME mediante un algoritmo particular y así sucesivamente. Cuando el UE se hace funcionar en un modo conectado de control de recursos de radio (RRC_CONNECTED) o un modo LTE_ACTIVE, el UE y el eNB derivan las claves de UP y de RRC (es decir, KeNB-UP-enc, KeNB-RRC-int y KeNB-RRC-enc) a partir de la KeNB. Cuando el UE entra en un modo RRC_IDLE o LTE_IDLE, se eliminan la KeNB, KeNB-UP-enc, KeNB-RRC-int, y KeNB-RRC-enc del eNB. Además, como resultado de una ejecución de AKA en el UE, cada clave mostrada en la figura 1 debe actualizarse cuando se realiza un cambio de clave tras la ejecución de AKA.

Cuando el UE se hace funcionar en el modo RRC_CONNECTED o LTE_ACTIVE, los cuatro requisitos referentes al cambio de claves en el eNB se describen de la siguiente manera con el fin de garantizar la seguridad de datos:

(1) Si los números de secuencia que tienen una longitud de bits finitos y usados para el cifrado/protección de integridad de UP o de RRC están a punto de reiniciarse, deben cambiarse las claves respectivas.

(2) Si un UE ha estado en modo LTE_ACTIVE durante un periodo de tiempo prolongado, las claves para cifrado/protección de identidad de UP y de RRC se cambiarán, aunque los números de secuencia no estén próximos a reiniciarse.

(3) Se restringirá la vida útil de KASME.

(4) Si el UE ha realizado un traspaso entre RAT desde UTRAN/GERAN hasta LTE, se actualizarán todas las claves en el plazo de segundos.

Sin embargo, en los casos de (1) y (2), no se necesita ejecutar el AKA para obtener nuevas claves. Cambios de claves de UP y de RRC locales para el eNB son suficientes. Esto puede lograrse, por ejemplo, derivando nuevas claves de UP y de RRC a partir de la KeNB existente en el propio eNB, o derivando una nueva KeNB a partir de la KASME existente. En los casos de (3) y (4), debe actualizarse toda la jerarquía de claves basada en KASME basándose en una nueva ejecución de AKA.

Según las especificaciones relacionadas, aún no se ha decidido el enfoque para activar el cambio de clave en un modo RRC_CONNECTED o LTE_ACTIVE. Un enfoque podría ser un procedimiento de traspaso dentro de una célula. Con respecto al procedimiento de traspaso dentro de una célula, la red realiza un traspaso a la misma célula en la que ya está el UE. Mediante el traspaso dentro de una célula sólo se actualizan las claves de AS (estrato de acceso) de manera similar a un traspaso entre células. Las nuevas claves de AS se derivan a partir de las claves de AS previas.

Cuando el UE se hace funcionar en el modo RRC_CONNECTED o LTE_ACTIVE, hay dos tipos de cambios de clave para considerar: el cambio de clave con la ejecución de AKA y el cambio de clave sin la ejecución de AKA. En la técnica anterior no queda claro cómo debe realizarse el cambio de clave.

Teniendo esto en cuenta, la presente invención tiene como objetivo proporcionar un método y un aparato para un sistema de comunicación inalámbrico, para gestionar un cambio de clave de seguridad para un sistema de comunicación inalámbrico.

Esto se logra mediante los métodos y los dispositivos definidos en las reivindicaciones independientes 1, 3, 7 y 9. Las reivindicaciones dependientes se refieren a desarrollos y mejoras adicionales correspondientes.

Tal como se observará más claramente a partir de la siguiente descripción detallada a continuación, el método reivindicado para gestionar un cambio de clave para un equipo de usuario en un sistema de comunicación inalámbrico. El método incluye usar un procedimiento de RRC para activar el cambio de clave para una primera condición y una segunda condición. La primera condición es un cambio de clave con una ejecución de AKA. La segunda condición es un cambio de clave sin la ejecución de AKA.

Breve descripción de los dibujos

La figura 1 es un diagrama esquemático de una jerarquía de claves para una LTE en sistema de comunicación inalámbrico.

La figura 2 es un diagrama esquemático de un sistema de comunicación inalámbrico.

La figura 3 es un bloque funcional de un sistema de comunicación inalámbrico.

La figura 4 es un diagrama de flujo de un programa mostrado en la figura 3.

La figura 5 es un diagrama de flujo de un proceso según una realización de la presente invención.

Véase la figura 2, que es un diagrama esquemático de un sistema 10 de comunicaciones inalámbrico. Se prefiere que el sistema 10 de comunicaciones inalámbrico sea un sistema de comunicaciones de evolución a largo plazo (LTE), y de manera resumida está formado por un terminal de red y una pluralidad de equipos de usuario. En la figura 2, el terminal de red y los equipos de usuario se usan simplemente para ilustrar la estructura del sistema 10 de comunicaciones inalámbrico. En la práctica, el terminal de red puede incluir una pluralidad de estaciones base evolucionadas (eNB), una red de acceso de radio de UMTS evolucionada (EUTRAN) y así sucesivamente, según demandas reales, y los equipos de usuario (UE) pueden ser aparatos tales como teléfonos móviles, sistemas informáticos, etc.

Véase la figura 3, que es un diagrama de bloques funcionales de un dispositivo 100 de comunicaciones. El dispositivo 100 de comunicaciones puede usarse para realizar los UE en la figura 2. Por motivos de brevedad, la figura 3 sólo muestra un dispositivo 102 de entrada, un dispositivo 104 de salida, un circuito 106 de control, una unidad 108 central de procesamiento (CPU), una memoria 110, un programa 112 y un transceptor 114 del dispositivo 100 de comunicaciones. En el dispositivo 100 de comunicaciones, el circuito 106 de control ejecuta el programa 112 en la memoria 110 a través de la CPU 108, controlando así un funcionamiento del dispositivo 100 de comunicaciones. El dispositivo 100 de comunicaciones puede recibir señales introducidas por un usuario a través del dispositivo 102 de entrada, tal como un teclado, y puede emitir imágenes y sonidos a través del dispositivo 104 de salida, tal como un monitor o altavoces. El transceptor 114 se usa para recibir y transmitir señales inalámbricas, suministrar señales recibidas al circuito 106 de control, y emitir señales generadas por el circuito 106 de control de manera inalámbrica. Desde un punto de vista de un entramado de protocolo de comunicaciones, el transceptor 114 puede considerarse como una parte de la capa 1, y el circuito 106 de control puede usarse para realizar funciones de la capa 2 y la capa 3.

Sígase viendo la figura 4. La figura 4 es un diagrama esquemático del programa 112 mostrado en la figura 3. El programa 112 incluye una capa 200 de aplicación, una capa 202 3 y una capa 206 2, y está acoplado a una capa 208 1. La capa 202 3 incluye una entidad 222 de control de recursos de radio (RRC), que se usa para controlar la capa 1 218 y

la capa 206 2 y realizar comunicación de RRC entre pares con otros dispositivos de comunicaciones, tales como una estación base o un nodo B. La entidad 222 de RRC conmuta el dispositivo 100 de comunicación entre un modo inactivo de control de recursos de radio (RRC_IDLE) y un modo conectado de control de recursos de radio (RRC_CONNECTED).

Cuando el dispositivo 100 de comunicación se hace funcionar en el modo RRC_CONNECTED, se proporciona un programa 220 de gestión de cambio de clave en el programa 112 según una realización de la presente invención y se usa para determinar si el cambio de clave va acompañado de una ejecución de AKA (acuerdo de autenticación y clave) o no. Véase la figura 5, que es un diagrama de flujo de un proceso 40 según una realización de la presente invención. El proceso 40 se usa para gestionar un cambio de clave para el UE en un sistema de comunicación inalámbrico y puede compilarse en el programa 220 de gestión de cambio de clave. El proceso 40 incluye las siguientes etapas:

Etapa 400: Inicio.

Etapa 402: Usar un procedimiento de RRC para activar el cambio de clave.

Etapa 404: Determinar una relación de acompañamiento entre el cambio de clave y la ejecución de AKA.

Etapa 406: Derivar las nuevas claves de AS basándose en el resultado de la etapa 404.

Etapa 408: Fin.

Según el proceso 40, la realización de la presente invención usa un procedimiento de RRC para activar el cambio de clave para las siguientes condiciones asociadas con la relación de acompañamiento entre el cambio de clave y la ejecución de AKA: (1) el cambio de clave con la ejecución de AKA y (2) el cambio de clave sin la ejecución de AKA.

Preferiblemente, cuando el UE se hace funcionar en el modo RRC_CONNECTED o el modo LTE_ACTIVE, el UE recibe un mensaje de RRC a partir del eNB durante el procedimiento de RRC. El mensaje de RRC incluye un indicador para indicar el cambio de clave acompañado de la ejecución de AKA o no.

Preferiblemente, un conjunto de claves de estrato de acceso (AS) incluye una clave de cifrado de plano de usuario KeNB-UP-enc, una clave de integridad de RRC KeNB-RRC-int y una clave de cifrado de RRC KeNB-RRC-enc. La relación de derivación del conjunto de claves de AS anteriormente mencionado puede consultarse en descripciones anteriores y no se describe en el presente documento. Cuando el indicador indica que el cambio de clave va acompañado de una ejecución de AKA, esto significa que la ejecución de AKA se realizó antes que el cambio de clave, y por tanto el UE debe derivar un nuevo conjunto de claves de AS a partir de la nueva clave de base KASME. Por el contrario, cuando el indicador indica que el cambio de clave no va acompañado de la ejecución de AKA, el nuevo conjunto de claves de AS debe derivarse a partir de una KeNB o KASME previa (antigua). Por tanto, el UE puede determinar si el cambio de clave va acompañado de la ejecución de AKA o no, y genera en consecuencia el nuevo conjunto de claves de AS correspondiente.

Por otro lado, el UE puede mantener un estado que indica si el conjunto de claves asociado con la ejecución de AKA más reciente se ha activado o no. Cuando se realiza una ejecución de AKA, el estado se establece a un primer valor, que indica que se ha asignado un nuevo conjunto de claves pero aún no se ha activado. Tras activarse el nuevo conjunto de claves, se establece el estado a un segundo valor que indica que se ha activado el nuevo conjunto de claves. Por ejemplo, el estado puede representarse por un bit binario. Cuando el bit binario se establece a “0”, esto significa que ya se ha activado el conjunto de claves. Cuando el bit binario se establece a “1”, esto significa que se ha asignado el nuevo conjunto de claves asociado con la ejecución de AKA más reciente pero no se ha activado. Tras activarse el nuevo conjunto de claves, se restablece el bit binario a “0”.

Además, cuando el UE en el modo RRC_CONNECTED o el modo LTE_ACTIVE recibe el mensaje de RRC a partir del eNB para activar el cambio de clave, el UE determina la relación de acompañamiento entre el cambio de clave y la ejecución de AKA según el estado. Cuando el estado se establece al primer valor, el UE determina el cambio de clave con la ejecución de AKA. Cuando el estado se establece al segundo valor, el UE determina el cambio de clave sin la ejecución de AKA. Por ejemplo, cuando el estado se establece a “0”, esto significa que ya se ha activado el conjunto de claves y el nuevo conjunto de claves de AS debe derivarse a partir de la clave de base previa KASME o KeNB. Cuando el estado se establece a “1”, esto significa que se ha asignado el nuevo conjunto de claves pero no se ha activado y el nuevo conjunto de claves de AS debe derivarse a partir de la nueva clave de base KASME. Tras el cambio de clave, se restablece el estado a “0”, indicando que se ha activado el nuevo conjunto de claves de AS.

Tal como se conoce anteriormente, el UE puede actualizar el conjunto de claves de AS determinando si el cambio de clave va acompañado de una ejecución de AKA.

En resumen, la presente invención usa un procedimiento de RRC para activar el cambio de clave y determina si el cambio de clave va acompañado de la ejecución de AKA según un indicador comprendido en un mensaje de RRC transmitido durante el procedimiento de RRC, tal como se define en las reivindicaciones adjuntas.

REIVINDICACIONES

1. Método de gestión de un cambio de clave de estrato de acceso, denominado a continuación en el presente documento AS, en un sistema (10) de comunicación inalámbrico, comprendiendo el método:

una estación base que usa un procedimiento de control de recursos de radio, denominado a continuación en el presente documento RRC, para activar el cambio de clave de AS para una primera condición del cambio de clave de AS con una ejecución de acuerdo de autenticación y clave, denominado a continuación en el presente documento AKA, y una segunda condición del cambio de clave de AS sin la ejecución de AKA,

caracterizado por:

enviar un mensaje de RRC para activar el cambio de clave de AS durante un procedimiento de RRC, comprendiendo el mensaje de RRC un indicador para indicar si el cambio de clave de AS va acompañado de la ejecución de AKA o no.

2. Método según la reivindicación 1, caracterizado porque el procedimiento de RRC es un procedimiento de traspaso.

3. Método de gestión de un cambio de clave de estrato de acceso, denominado a continuación en el presente documento AS, para un equipo de usuario, denominado a continuación en el presente documento UE, en un sistema (10) de comunicación inalámbrico,

caracterizado por recibir el UE un mensaje de control de recursos de radio, denominado a continuación en el presente documento RRC, para activar el cambio de clave de AS durante un procedimiento de RRC, comprendiendo el mensaje de RRC un indicador para indicar si el cambio de clave de AS va acompañado de la ejecución de AKA o no, y

derivar el UE un conjunto de claves de AS según el indicador, en el que el conjunto de claves de AS comprende una clave de cifrado de plano de usuario, una clave de integridad de RRC y una clave de cifrado de RRC.

4. Método según la reivindicación 3, que comprende:

según el indicador, determinar si el cambio de clave va acompañado de la ejecución de AKA o no;

derivar el conjunto de claves de AS a partir de una clave de base, correspondiente a la ejecución de AKA, cuando el indicador indica el cambio de clave con la ejecución de AKA; y

derivar el conjunto de claves de AS a partir de una clave de base previa o una clave de nivel de estación base previa cuando el indicador indica el cambio de clave sin la ejecución de AKA.

5. Método según la reivindicación 3, caracterizado porque el UE se hace funcionar en un modo RRC_CONNECTED o un modo LTE_ACTIVE.

6. Método según la reivindicación 3, caracterizado porque el procedimiento de RRC es un procedimiento de traspaso.

7. Estación base para realizar un cambio de clave de estrato de acceso, denominado a continuación en el presente documento AS, para un sistema (10) de comunicación inalámbrico, que comprende medios para:

usar un procedimiento de control de recursos de radio, denominado a continuación en el presente documento RRC, para activar el cambio de clave de AS para una primera condición del cambio de clave de AS con una ejecución de acuerdo de autenticación y clave, denominado a continuación en el presente documento AKA, y una segunda condición del cambio de clave de AS sin la ejecución de AKA,

caracterizada por

medios para enviar un mensaje de RRC para activar el cambio de clave de AS durante el procedimiento de RRC, comprendiendo el mensaje de RRC un indicador para indicar si el cambio de clave de AS va acompañado de la ejecución de AKA o no.

8. Estación base según la reivindicación 7, caracterizada porque el procedimiento de RRC es un procedimiento de traspaso.

9. Dispositivo (100) de comunicación para un equipo de usuario para realizar un cambio de clave de estrato de acceso, denominado a continuación en el presente documento AS, para un sistema (10) de comunicación inalámbrico, comprendiendo el dispositivo (100) de comunicación:

una unidad (108) central de procesamiento, para ejecutar un proceso; y

una memoria (110), para almacenar un programa (112) para ejecutar el proceso,

caracterizado porque el proceso comprende:

recibir un mensaje de control de recursos de radio, denominado a continuación en el presente documento RRC, para activar el cambio de clave de AS durante un procedimiento de RRC, comprendiendo el mensaje de RRC el indicador para indicar si el cambio de clave de AS va acompañado de la ejecución de AKA o no, y

derivar un conjunto de claves de AS según el indicador, caracterizado porque el conjunto de claves de AS comprende una clave de cifrado de plano de usuario, una clave de integridad de RRC y una clave de cifrado de RRC.

10. Dispositivo de comunicación según la reivindicación 9, caracterizado porque el proceso comprende:

según el indicador, determinar si el cambio de clave va acompañado de la ejecución de AKA o no;

derivar el conjunto de claves de AS a partir de una clave de base, correspondiente a la ejecución de AKA, cuando el indicador indica el cambio de clave con la ejecución de AKA; y

derivar el conjunto de claves de AS a partir de una clave de base previa o una clave de nivel de estación base previa cuando el indicador indica el cambio de clave sin la ejecución de AKA.

11. Dispositivo de comunicación según la reivindicación 9, caracterizado porque el UE se hace funcionar en un modo RRC_CONNECTED o un modo LTE_ACTIVE.

12. Dispositivo de comunicación según la reivindicación 9, caracterizado porque el procedimiento de RRC es un procedimiento de traspaso.

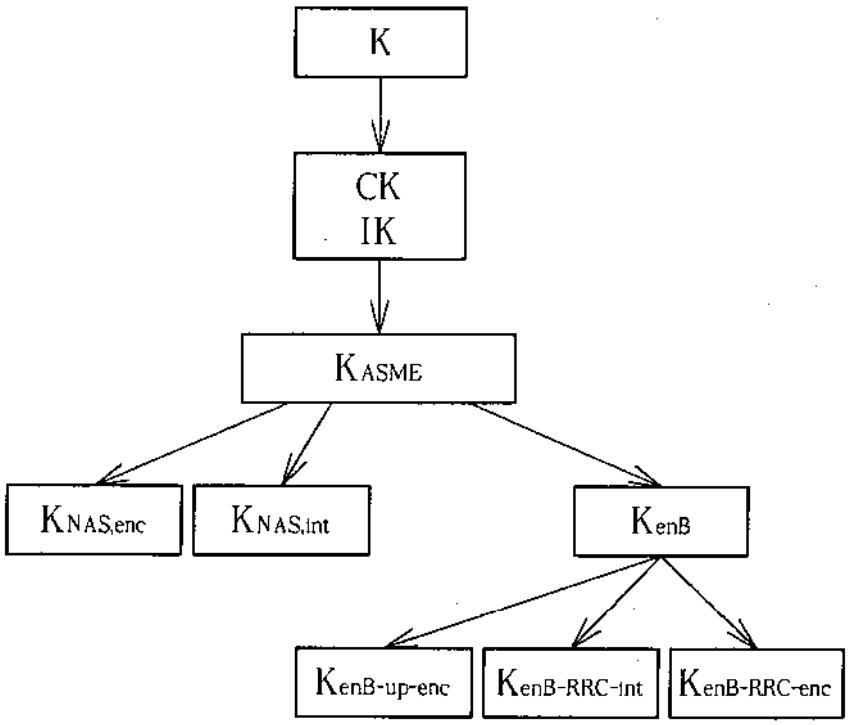
K
CK
IK
KASME
KNAS,enc
KNAS,int
KenB
KenB-up-enc
KenB-RRC-int
KenB-RRC-enc

FIG. 1

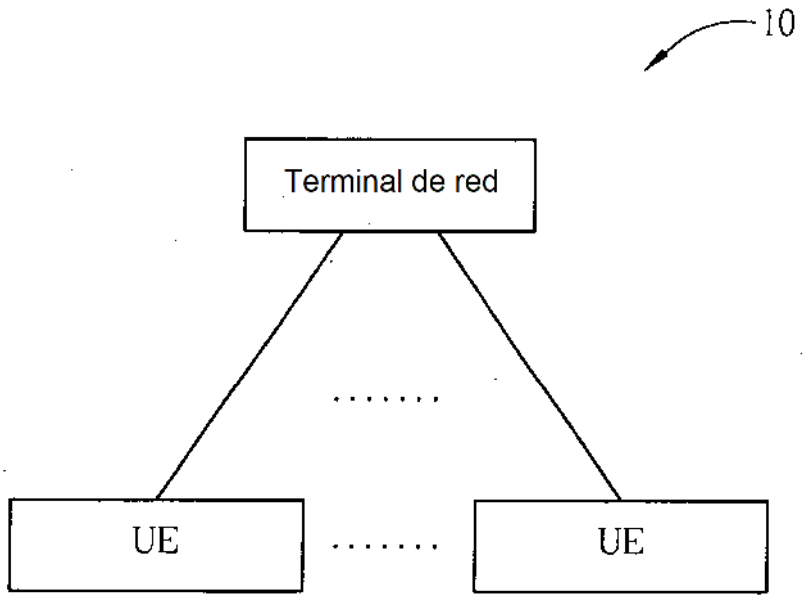

FIG. 2

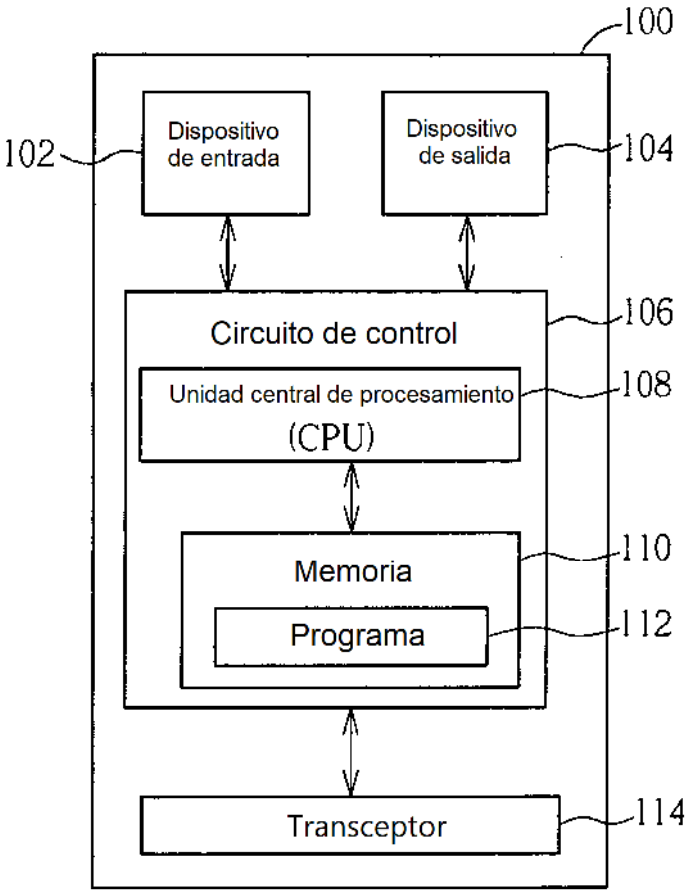
100
102
Dispositivo de entrada
Dispositivo de salida
104
106
Circuito de control
Unidad central de procesamiento (CPU)
108
110
Memoria
Programa
112
Transceptor
114

FIG. 3

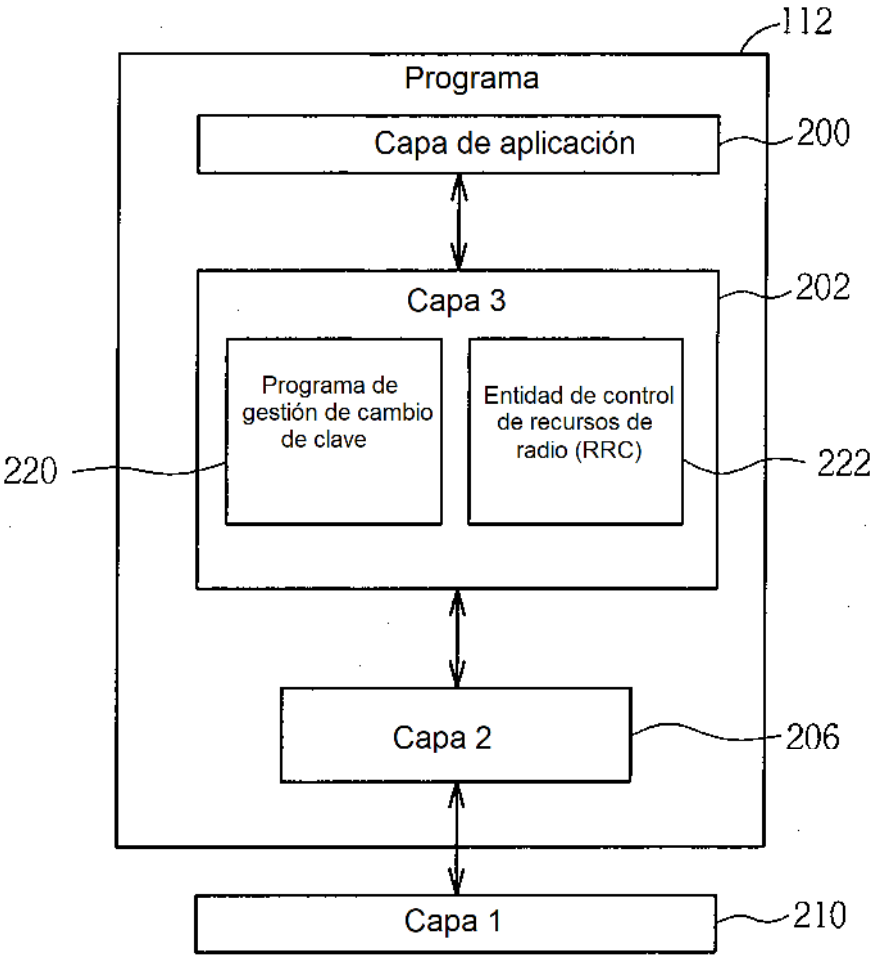
112
Programa
Capa de aplicación
200
Capa 3
202
Programa de gestión de cambio de clave
Entidad de control de recursos de radio (RRC)
220
222
Capa 2
206
Capa 1
210

FIG. 4

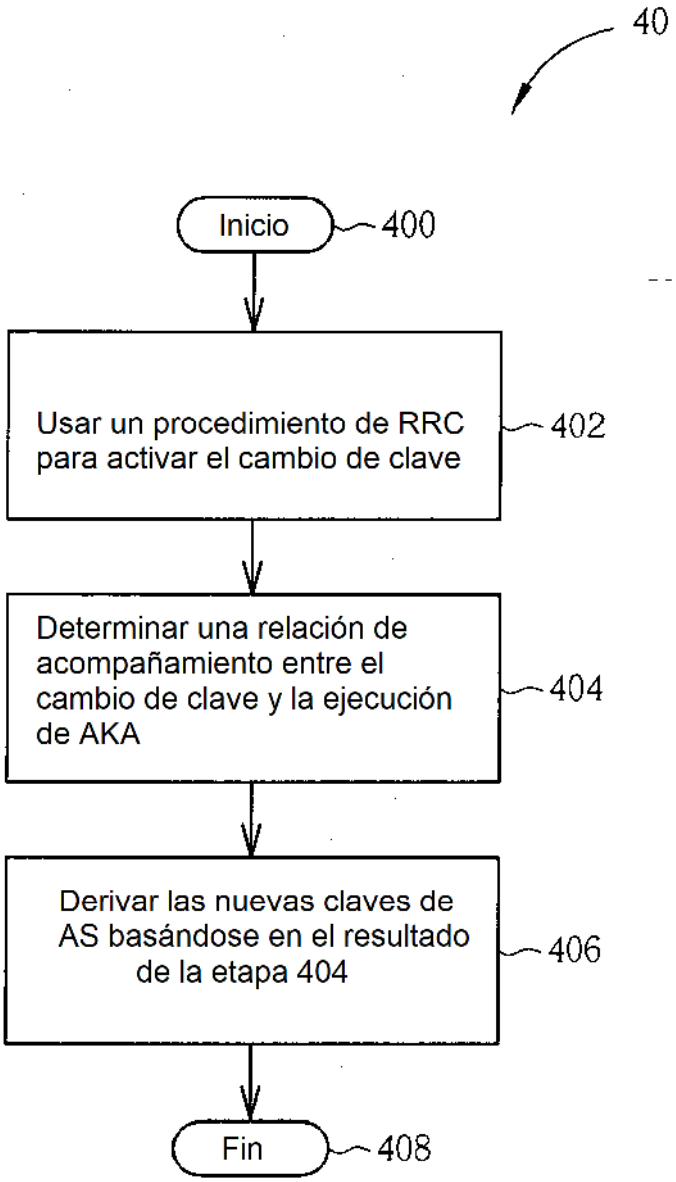
40
Inicio
400
Usar un procedimiento de RRC para activar el cambio de clave
402
Determinar una relación de acompañamiento entre el cambio de clave y la ejecución de AKA
404
Derivar las nuevas claves de AS basándose en el resultado de la etapa 404
406
Fin
408

FIG. 5