(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 759 428**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04W 12/04 (2009.01)
H04L 9/08 (2006.01)
H04W 36/00 (2009.01)
H04W 36/06 (2009.01)
H04W 88/08 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **28.01.2014 PCT/CN2014/071675**

(87) Fecha y número de publicación internacional: **06.08.2015 WO15113207**

(96) Fecha de presentación y número de la solicitud europea: **28.01.2014 E 14881066 (6)**

(97) Fecha y número de publicación de la concesión europea: **25.09.2019 EP 3099029**

(54) Título: **Método de cambio de clave de seguridad y equipo de usuario**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.05.2020

(73) Titular/es:

HUAWEI TECHNOLOGIES CO., LTD. (100.0%)
Huawei Administration Building, Bantian, Longgang District
Shenzhen, Guangdong 518129, CN

(72) Inventor/es:

CHANG, JUNREN;
BI, HAO;
GUO, YI;
ZHANG, DONGMEI y
LIN, BO

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Método de cambio de clave de seguridad y equipo de usuario

Campo técnico

Las realizaciones de la presente invención se refieren al área de comunicaciones y, en particular, a un método de cambio de clave de seguridad, una estación base y equipo de usuario.

Antecedentes

En la actualidad, para mejorar una velocidad de transmisión de una red inalámbrica, la organización Proyecto de asociación de 3ª generación (en inglés, 3rd Generation Partnership Project - 3GPP) está analizando la creación de un nuevo proyecto de investigación en la mejora de células pequeñas.

Durante el despliegue de células pequeñas en la técnica anterior, se utilizan, a menudo, un portador de banda de baja frecuencia y un portador de banda de alta frecuencia. Por ejemplo, como un portador de banda de baja frecuencia, una frecuencia F1 presenta un área de gran cobertura, pero recursos relativamente escasos; como un portador de banda de alta frecuencia, F2 presenta un área pequeña de cobertura, pero recursos relativamente abundantes. En una red celular existente, se utiliza generalmente un portador de banda de baja frecuencia; por ejemplo, la F1 se utiliza para proporcionar un servicio para usuarios. Sin embargo, con la popularización de los teléfonos inteligentes, un usuario establece un requisito más estricto en una velocidad de transmisión inalámbrica. Para cumplir con el requisito del usuario, los recursos de portador de banda de alta frecuencia abundantes necesitan utilizarse paso a paso para proporcionar un servicio para usuarios. Dado que un portador de banda de alta frecuencia presenta una pequeña cobertura, una estación base (Nodo B evolucionado, abreviado en inglés - eNB) que utiliza un portador de banda de alta frecuencia para pequeña cobertura se denomina generalmente una estación base micro y un área de cobertura de la estación base micro se denomina generalmente una célula pequeña. Generalmente, una estación base macro se selecciona como un eNodoB maestro (NodoB evolucionado Macro, abreviado en inglés - MeNB), y una estación base micro se selecciona como un eNodoB secundario (NodoB evolucionado pequeño, abreviado en inglés - SeNB). Puede haber múltiples células para un MeNB. Una célula se selecciona a partir de las múltiples células como una célula primaria (en inglés, Primary Cell - PCell) para proporcionar un servicio para equipo de usuario (en inglés, User Equipment - UE) y otra célula puede ser una célula secundaria (en inglés, Secondary Cell - SCell). Además, una célula de un eNodoB secundario se selecciona generalmente como una célula secundaria para proporcionar un servicio para el UE. Un modo en la que el UE puede llevar a cabo la comunicación mediante el uso de recursos de radio proporcionados por el MeNB y el SeNB se define como comunicación de conectividad dual. La comunicación de conectividad dual se utiliza cada vez más en la transmisión de datos entre una estación base y un UE debido a la alta eficiencia de transmisión de datos y un alto rendimiento.

Normalmente se necesita una clave de seguridad durante la transmisión de datos entre una estación base y un UE. Sin embargo, en algunos casos, la clave de seguridad debe ser cambiada. En un sistema de evolución a largo plazo (en inglés, Long Term Evolution - LTE), un proceso para cambiar una clave de seguridad puede completarse en un proceso de traspaso intracelular, donde el proceso de traspaso intracelular se refiere a que una célula de origen y una célula objetivo son la misma célula de una estación base cuando el UE lleva a cabo el traspaso, es decir, las células primarias antes y después del traspaso son una misma célula, y no cambian.

En un proceso para implementar la presente invención, el inventor de la presente invención descubre que al menos la siguiente desventaja existe en la técnica anterior: un método de cambio de clave de seguridad existente es aplicable a un cambio de clave de seguridad cuando un UE lleva a cabo la transmisión de datos con solamente una estación base, pero una solución de implementación relacionada para cambiar una clave de seguridad no se proporciona para un escenario de aplicación en el que el UE realiza la comunicación de conectividad dual con un MeNB y un SeNB.

HUAWEI ET ÁL, "Security for SCE arc.1A", vol. SA WG3, no. Taipei; 20140120 - 20140124, (20140119), PROYECTO 3GPP; S3-140026 SECURITY FOR SCE ARC.1A, PROYECTO DE ASOCIACIÓN DE 3ª GENERACIÓN (3GPP), MOBILE COMPETENCE CENTRE; 650, ROUTE DES LUCIOLES; F-06921SOPHIA-ANTIPOLISCEDEX; FRANCIA URL: http://www.3gpp.org/ftp/Meetings_3GPP_SYNC/SA/SA3/Docs/, (20140119), XP050745165, proporciona solución de seguridad para mejoras de células pequeñas de la arquitectura 1A, en donde el UE actualiza todas las claves AS y simultáneamente libera la conexión con MeNB y SeNB.

SAMSUNG, "Discussion on Security Aspects of SCE UP Architecture", vol. RAN WG2, no. San Francisco; EE.UU.; 20131111 - 20131115, (20131101), PROYECTO 3GPP; R2-134278-SCE-SECURITY, PROYECTO DE ASOCIACIÓN DE 3ª GENERACIÓN (3GPP), MOBILE COMPETENCE CENTRE; 650, ROUTE DES LUCIOLES; F-06921 SOPHIA-ANTIPOLIS CEDEX;FRANCIA,URL:http://www.3gpp.org/ftp/tsg_ran/WG2_RL2/TSGR2_84/Docs/, (20131101), XP050753167, presenta el análisis de seguridad en las arquitecturas seleccionadas hacia abajo de RAN2 y proporciona vistas sobre la viabilidad de estas soluciones respecto a aspectos de seguridad. En la sección 2.1, se analiza la conectividad dual con PDCP distribuido (Opción 1A).

WO 2013/185579 A1 describe un método de actualización de la clave, en donde el eNB macro actualiza una clave de acuerdo con la solicitud de actualización de clave o la información de valor de CONTEO PDCP de enlace ascendente

y enlace descendente del plano de usuario.

Compendio

La presente invención proporciona un método de cambio de clave de seguridad en la reivindicación 1, y un equipo de usuario en la reivindicación 8 para implementar un cambio de clave de seguridad cuando el UE lleva a cabo la comunicación de conectividad dual con un MeNB y un SeNB.

Según un primer aspecto, una realización de la presente invención proporciona un método de cambio de clave de seguridad, que incluye:

recibir, mediante el equipo de usuario UE, un mensaje de comando de cambio de clave desde un eNodoB maestro, MeNB, donde el mensaje de comando de cambio de clave incluye información de indicación de que un cambio de clave de seguridad puede realizarse entre el UE y un eNodoB secundario, SeNB, en donde UE está configurado con una conectividad dual entre el MeNB y el SeNB;
realizar, mediante el UE según el mensaje de comando de cambio de clave, el cambio de clave de seguridad entre el UE y el SeNB;
determinar, mediante el UE según el mensaje de comando de cambio de clave, si mantener la información de configuración de estrato de acceso entre el UE y el SeNB; y
enviar, mediante el UE, un mensaje de cambio de clave completado al MeNB;
en donde la información de configuración de estrato de acceso entre UE y el SeNB comprende al menos uno de los siguientes:

información de configuración del protocolo de convergencia de datos por paquetes, PDCP, entre el UE y el SeNB;
información de configuración del Control de Radio Enlace, RLC, entre el UE y el SeNB;
información de configuración del Control de Acceso al Medio, MAC, entre el UE y el SeNB;
un estado activo de una célula secundaria, SCell, activada entre el UE y el SeNB;
un identificador temporal de red de radio celular, C-RNTI, utilizado para comunicación entre el UE y el SeNB.

Según un segundo aspecto, una realización de la presente invención proporciona un equipo de usuario UE, que incluye:

un módulo de recepción de mensajes, configurado para recibir un mensaje de comando de cambio de clave desde un eNodoB maestro, MeNB, donde el mensaje de comando de cambio de clave incluye información de indicación de que un cambio de clave de seguridad puede llevarse a cabo entre el UE y un eNodoB secundario, SeNB, en donde el UE está configurado con una conectividad dual entre el MeNB y el SeNB;
un módulo de cambio de clave, configurado para llevar a cabo, según el mensaje de comando de cambio de clave, el cambio de clave de seguridad entre el UE y el SeNB;
un módulo de determinación, configurado para determinar, según el mensaje de comando de cambio de clave, si mantener la información de configuración de estrato de acceso entre el UE y el SeNB; y
un módulo de envío de mensajes, configurado para enviar un mensaje de cambio de clave completado al MeNB
en donde la información de configuración de estrato de acceso entre el UE y el SeNB comprende al menos uno de los siguientes:

información de configuración del protocolo de convergencia de datos por paquetes, PDCP, entre el UE y el SeNB;
información de configuración del Control de Radio Enlace, RLC, entre el UE y el SeNB;
información de configuración del Control de Acceso al Medio, MAC, entre el UE y el SeNB;
un estado activo de una célula secundaria, SCell, activada entre el UE y el SeNB;
un identificador temporal de red de radio celular, C-RNTI, utilizado para la comunicación entre el UE y el SeNB.

Se puede observar a partir de las soluciones técnicas que las realizaciones de la presente invención tienen las siguientes ventajas:

En las realizaciones de la presente invención, un eNodoB maestro determina en primer lugar que necesita realizarse un cambio de clave de seguridad entre una primera estación base y un UE, donde la primera estación base incluye al menos uno del eNodoB maestro y un eNodoB secundario; luego de que el eNodoB maestro determina que el cambio de clave de seguridad debe realizarse entre la primera estación base y el UE, el eNodoB maestro envía un mensaje de comando de cambio de clave al UE de manera que el UE realiza, según el mensaje de comando de cambio de clave, el cambio de clave de seguridad entre el UE y la primera estación base, y determina, según el mensaje de comando de cambio de clave, si mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o el eNodoB secundario y/o si mantener la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario; y luego de que el UE completa el cambio de clave de seguridad, el UE envía un mensaje de cambio de clave completado al eNodoB maestro, el eNodoB maestro puede recibir el mensaje de cambio de clave completado enviado por el UE de manera que la primera estación base puede determinar, al utilizar el eNodoB maestro, que se complete el cambio de clave de seguridad entre el UE y la primera estación base, y además, la primera estación base y el UE pueden usar una nueva clave de seguridad para llevar a cabo la transmisión de datos.

Por lo tanto, según las realizaciones de la presente invención, puede implementarse un cambio de clave de seguridad cuando un UE lleva a cabo la comunicación de conectividad dual con MeNB y un SeNB.

Breve descripción de los dibujos

La Figura 1 es un diagrama de bloques esquemático de un proceso de un método de cambio de clave de seguridad según una realización de la presente invención.

La Figura 2 es un diagrama de flujo esquemático de otro método de cambio de clave de seguridad según una realización de la presente invención.

La Figura 3-a es un diagrama de flujo esquemático de una interacción entre un eNodoB maestro, un eNodoB secundario y un UE según una realización de la presente invención.

La Figura 3-b es un diagrama de flujo esquemático de otra interacción entre un eNodoB maestro, un eNodoB secundario, y un UE según una realización de la presente invención.

La Figura 3-c es un diagrama de flujo esquemático de otra interacción entre un eNodoB maestro, un eNodoB secundario, y un UE según una realización de la presente invención.

La Figura 3-d es un diagrama de flujo esquemático de otra interacción entre un eNodoB maestro, un eNodoB secundario, y un UE según una realización de la presente invención.

La Figura 3-e es un diagrama de flujo esquemático de otra interacción entre un eNodoB maestro, un eNodoB secundario, y un UE según una realización de la presente invención.

La Figura 4-a es un diagrama estructural esquemático de una estación base según una realización de la presente invención.

La Figura 4-b es un diagrama estructural esquemático de un módulo de determinación de cambio de clave según una realización de la presente invención;

La Figura 5-a es un diagrama estructural esquemático de un UE según una realización de la presente invención.

La Figura 5-b es un diagrama estructural esquemático de otro UE según una realización de la presente invención.

La Figura 5-c es un diagrama estructural esquemático de otro UE según una realización de la presente invención.

La Figura 5-d es un diagrama estructural esquemático de un módulo de cambio de clave según una realización de la presente invención.

La Figura 5-e es un diagrama estructural esquemático de otro UE según una realización de la presente invención.

La Figura 6 es un diagrama estructural esquemático de otra estación base según una realización de la presente invención; y

La Figura 7 es un diagrama estructural esquemático de otro UE según una realización de la presente invención.

Descripción de las realizaciones

Las realizaciones de la presente invención proporcionan un método de cambio de clave de seguridad, una estación base y equipo de usuario para implementar un cambio de clave de seguridad cuando el UE lleva a cabo la comunicación de conectividad dual con un MeNB y un SeNB.

Para aclarar y comprender mejor los objetivos, características y ventajas de la presente invención, a continuación, se describen clara y completamente las soluciones técnicas en las realizaciones de la presente invención con referencia a los dibujos adjuntos en las realizaciones de la presente invención. Aparentemente, las realizaciones descritas a continuación son solamente una parte más que la totalidad de las realizaciones de la presente invención. Todas las otras realizaciones obtenidas por expertos en la técnica con base en las realizaciones de la presente invención estarán dentro del alcance de protección de la presente invención.

En la memoria descriptiva, reivindicaciones y dibujos adjuntos de la presente invención, se pretende que los términos “primero”, “segundo”, y así sucesivamente, distingan entre objetos similares, pero no necesariamente indican un orden o secuencia específica. Deberá entenderse que los términos utilizados de esta manera son intercambiables en circunstancias adecuadas y son simplemente maneras distintivas que se utilizan cuando los objetos de un mismo atributo se describen en las realizaciones que describen la presente invención. Además, los términos “incluye”, “contiene” y cualquier otra variante significa que abarcan la inclusión no exclusiva de manera que un proceso, método, sistema, producto o dispositivo que incluye una lista de unidades no se limita necesariamente a esas unidades, pero puede incluir otras unidades no mencionadas expresamente o inherentes a dicho proceso, método, sistema, producto o dispositivo.

Los detalles se ilustran de forma separada a continuación.

Una realización de un método de cambio de clave de seguridad de la presente invención puede aplicarse a una estación base, y es particularmente aplicable a un eNodoB maestro de al menos dos estaciones base con las que un UE lleva a cabo la comunicación de conectividad dual al mismo tiempo. El método puede incluir las siguientes etapas: determinar, mediante el eNodoB maestro, que se debe realizar un cambio de clave de seguridad entre una primera estación base y el equipo de usuario UE, donde la primera estación base incluye al menos uno del eNodoB maestro y un eNodoB secundario; enviar, mediante el eNodoB maestro, un mensaje de comando de cambio de clave al UE de manera que el UE realice, según el mensaje de comando de cambio de clave, el cambio de clave de seguridad entre el UE y la primera estación base, y determine, según el mensaje de comando de cambio de clave, si mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o el eNodoB secundario y/o si mantener la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario; y recibir, mediante el eNodoB maestro, un mensaje de cambio de clave completado enviado por el UE, de manera que la primera estación base determina que se complete el cambio de clave de seguridad entre el UE y la primera estación base.

Con respecto a la Figura 1, un método de cambio de clave de seguridad según una realización de la presente invención puede incluir las siguientes etapas:

101. Un eNodoB maestro determina que se necesita realizar un cambio de clave de seguridad entre una primera estación base y equipo de usuario UE.

La primera estación base incluye al menos uno del eNodoB maestro y un eNodoB secundario.

En esta realización de la presente invención, normalmente se necesita una clave de seguridad durante la transmisión de datos entre una estación base y un UE y en algunos casos, debe cambiarse la clave de seguridad. Asimismo, cuando un UE lleva a cabo la comunicación al utilizar al menos dos nodos de red, normalmente existe un requisito de aplicación de cambiar una clave de seguridad utilizada por el UE que lleva a cabo la comunicación de conectividad dual. Por ejemplo, se debe cambiar una clave de seguridad cuando un UE lleva a cabo la comunicación al utilizar recursos de radio proporcionados por un MeNB y un SeNB. Sin embargo, cuando el UE lleva a cabo la comunicación de conectividad dual, los dos nodos de red están conectados al utilizar una red de transmisión no ideal (es decir, existe un retardo). En un escenario de aplicación de transmisión de datos entre el UE y la estación base, cuando el UE anterior lleva a cabo la comunicación de conectividad dual con el MeNB y el SeNB, si no se considera una característica especial de comunicación de conectividad dual, al menos existen los siguientes problemas: Por ejemplo, una capa PDCP y una capa RLC de una RB establecida en un lado del SeNB deben ser reestablecidas y el MAC debe reconfigurarse; como resultado, la transmisión de datos entre el UE y el SeNB debe interrumpirse. Adicionalmente, un estado de una SCell en el lado SeNB se cambia a un estado desactivado y luego de completarse un cambio de clave de seguridad, la SCell en el lado SeNB debe activarse nuevamente, lo que provoca un retardo de la transmisión de datos innecesario. Además, hay una gran diferencia entre una célula primaria y una célula secundaria. Por ejemplo, una diferencia principal radica en que la célula primaria es una célula con la que un UE establece una conexión de control de recursos de radio (en inglés, Radio Resource Control - RRC) durante la conexión inicial o traspaso y la célula primaria proporciona parámetros relacionados con gestión de seguridad y movilidad para el UE, y también se utiliza para transmitir datos de plano de usuario del UE; la célula secundaria es responsable principalmente de transmitir datos de plano de usuario para el UE. Dadas estas características de comunicación de conectividad dual, un experto en la técnica debe llevar a cabo una investigación más exhaustiva en cómo cambiar una clave de seguridad cuando un UE realiza una comunicación de conectividad dual.

En esta realización de la presente invención, para resolver un problema de cambio de clave de seguridad cuando el UE realiza la comunicación de conectividad dual, el eNodoB maestro puede determinar primero si el cambio de clave de seguridad debe realizarse entre el eNodoB maestro y el UE y si el cambio de clave de seguridad debe realizarse entre el SeNB y el UE. Es decir, el eNodoB maestro detecta un proceso de transmisión de datos entre el eNodoB maestro y el UE y un proceso de transmisión de datos entre el eNodoB secundario y el UE cuando el UE utiliza recursos de radio proporcionados por el eNodoB maestro y el eNodoB secundario para realizar la comunicación de conectividad dual, y luego el eNodoB maestro determina si el cambio de clave de seguridad debe realizarse entre el eNodoB maestro y el UE y si el cambio de clave de seguridad debe realizarse entre el eNodoB secundario y el UE. Además, el eNodoB maestro puede determinar una manera para realizar el cambio de clave de seguridad entre el eNodoB maestro y el UE y el eNodoB maestro puede determinar además un modo para realizar el cambio de clave de seguridad entre el eNodoB secundario y el UE.

Debería observarse que, en esta realización de la presente invención, una manera de cambio de clave de seguridad incluye la regeneración de clave (en inglés, Key Re-key) y la actualización de clave (en inglés, Key Refresh). Tanto la regeneración de clave como la actualización de clave se utilizan esencialmente para realizar el cambio de clave de seguridad. Una diferencia radica en que un proceso de implementación de regeneración de clave se inicia por una entidad de gestión de movilidad (en inglés, Mobility Management Entity - MME) y la MME proporciona una nueva clave intermedia (que puede representarse por un símbolo K_{eNB}) para llevar a cabo un proceso de cambio de clave de seguridad. La actualización de clave se inicia por un eNB. La actualización de clave se acciona generalmente mediante el ajuste automático de un conteo (en inglés, Count) de protocolo de convergencia de datos por paquetes (en inglés, Packet Data Convergence Protocol - PDCP) y luego se realiza un proceso de cambio de clave de seguridad. Los

detalles se describen a continuación:

En algunas realizaciones de la presente invención, la etapa 101 de la determinación, mediante un eNodoB maestro, de que se debe realizar un cambio de clave de seguridad entre una primera estación base y un UE puede incluir las siguientes etapas:

A1. El eNodoB maestro recibe un comando de indicación de clave enviado por la MME, donde el comando de indicación de clave se utiliza para ordenar que se realice la regeneración de clave entre el eNodoB maestro y el UE y/u ordenar que se realice la regeneración de clave entre el eNodoB secundario y el UE; y

A2. El eNodoB maestro determina, según el comando de indicación de clave, que la regeneración de clave debe realizarse entre la primera estación base y el UE.

Es decir, la MME puede determinar cuál del eNodoB maestro y el eNodoB secundario realiza el cambio de clave de seguridad con el UE, y la MME puede determinar además que el cambio de clave de seguridad se realiza específicamente entre el UE y la primera estación base de un modo de regeneración de clave. Luego de que la MME determina la estación base que realiza el cambio de clave de seguridad con el UE y determina el modo a ser utilizado, la MME envía el comando de indicación de clave al eNodoB maestro, y el eNodoB maestro puede adquirir, al analizar el comando de indicación de clave, una indicación específica para realizar el cambio de clave de seguridad desde la MME. En esta realización de la presente invención, un resultado determinado por el eNodoB maestro se describe en la realización del cambio de clave de seguridad entre la primera estación base y el UE, es decir, llevar a cabo la etapa A2 de la determinación, mediante el eNodoB maestro, de que el cambio de clave de seguridad se debe realizar entre la primera estación base y el UE y determinar que debe usarse un modo de regeneración de clave. La primera estación base representa una estación base que se determina por el eNodoB maestro y debe realizar el cambio de clave de seguridad con el UE. En esta realización de la presente invención, la primera estación base se determina específicamente de tres modos: 1. La primera estación base es el eNodoB maestro; 2. La primera estación base es el eNodoB secundario; y 3. La primera estación base es el eNodoB maestro y el eNodoB secundario. Es decir, el eNodoB maestro puede seleccionar, al utilizar el comando de indicación de clave, uno de los tres modos de implementación de la primera estación base. Por ejemplo, si la MME indica, al utilizar el comando de indicación de clave, que se debe realizar el cambio de clave de seguridad solamente entre el eNodoB maestro y el UE y que se debe usar un modo de regeneración de clave, el eNodoB maestro puede determinar que la primera estación base específicamente se refiere al eNodoB maestro.

En otras realizaciones de la presente invención, si la primera estación base determinada por el eNodoB maestro incluye el eNodoB secundario, luego de la etapa 101 de la determinación, mediante un eNodoB maestro de que se debe realizar un cambio de clave de seguridad entre una primera estación base y un UE, esta realización de la presente invención puede incluir además la siguiente etapa:

enviar, mediante el eNodoB maestro, un mensaje de indicación de cambio de clave al eNodoB secundario, donde el mensaje de indicación de cambio de clave se utiliza para ordenar al eNodoB secundario a que realice el cambio de clave de seguridad y el mensaje de indicación de cambio de clave incluye una clave intermedia del lado del eNodoB secundario generada por el eNodoB maestro según una clave intermedia del lado del eNodoB maestro actualizada e información de célula, asociado con el cambio de clave de seguridad del eNodoB secundario o información de estación base, asociado con el cambio de clave de seguridad del eNodoB secundario, o el mensaje de indicación de cambio de clave incluye una clave intermedia del lado del eNodoB secundario generada por la MME para el eNodoB secundario.

Que el eNodoB maestro determine que la primera estación base incluya el eNodoB secundario específicamente significa que la primera estación base es el eNodoB secundario o significa que la primera estación base es el eNodoB maestro y el eNodoB secundario. Es decir, cuando el eNodoB maestro determina que una estación base que debe realizar el cambio de clave de seguridad con el UE incluye el eNodoB secundario, el eNodoB maestro debe enviar el mensaje de indicación de cambio de clave al eNodoB secundario para ordenar que el eNodoB secundario realice el cambio de clave de seguridad y el eNodoB maestro agregue la siguiente información al mensaje de indicación de cambio de clave: la clave intermedia del lado del eNodoB secundario generada por el eNodoB maestro según la clave intermedia del lado del eNodoB maestro actualizada y la información de célula, asociada con el cambio de clave de seguridad del eNodoB secundario o la información de estación base, asociada con el cambio de clave de seguridad del eNodoB secundario. De manera alternativa, el mensaje de indicación de cambio de clave porta la siguiente información: la clave intermedia del lado del eNodoB secundario generada por la MME para el eNodoB secundario. Es decir, cuando el cambio de clave de seguridad debe realizarse entre el eNodoB secundario y el UE, el eNodoB secundario debe utilizar la clave intermedia del lado del eNodoB secundario, donde la clave intermedia del lado del eNodoB secundario puede determinarse por el eNodoB maestro, o puede determinarse por la MME. Cuando la clave intermedia del lado del eNodoB secundario se determina por el eNodoB maestro, el eNodoB maestro puede generar la clave intermedia del lado del eNodoB maestro según la clave intermedia del lado del eNodoB secundario actualizada y la información de célula, asociada con el cambio de clave de seguridad del eNodoB secundario o la información de estación base, asociada con el cambio de clave de seguridad del eNodoB secundario. Cuando la clave intermedia del lado del eNodoB secundario se determina por la MME, el comando de indicación de clave enviado por la MME al eNodoB maestro puede transmitir la clave intermedia del lado del eNodoB secundario y el eNodoB maestro agrega la

clave intermedia del lado del eNodoB secundario al mensaje de indicación de cambio de clave y envía el mensaje de indicación de cambio de clave al eNodoB secundario.

Específicamente, en otras realizaciones de la presente invención, si el eNodoB maestro determina que una manera para realizar el cambio de clave de seguridad entre la primera estación base y el UE es la regeneración de clave, un mensaje de comando de cambio de clave porta la información de célula asociada con el cambio de clave de seguridad del eNodoB secundario o información de estación base asociada con el cambio de clave de seguridad del eNodoB secundario. Es decir, si una clave intermedia del lado del eNodoB secundario se va a generar en un lado del eNodoB maestro, el mensaje de comando de cambio de clave enviado por el eNodoB maestro al UE necesita transmitir además la información de célula, asociada con el cambio de clave de seguridad del eNodoB secundario o la información de estación base asociada con el cambio de clave de seguridad del eNodoB secundario, la UE puede adquirir, al utilizar el mensaje de comando de cambio de clave enviado por el eNodoB maestro, la información de célula, asociada con el cambio de clave de seguridad del eNodoB secundario o la información de estación base, asociada con el cambio de clave de seguridad del eNodoB secundario, y la UE puede generar la clave intermedia del lado del eNodoB secundario al utilizar la información de célula y una clave intermedia del lado del eNodoB maestro actualizada.

El contenido que antecede describe que la manera para realizar el cambio de clave de seguridad es la regeneración de clave y lo siguiente describe que la manera para realizar el cambio de clave de seguridad es la actualización de clave. Con referencia a la siguiente descripción, en algunas realizaciones de la presente invención, la etapa 101 de la determinación, mediante un eNodoB maestro, de que se debe realizar un cambio de clave de seguridad entre una primera estación base y un UE puede incluir las siguientes etapas:

B1. El eNodoB maestro determina si un conteo PDCP actual del UE en un eNodoB maestro se ajusta automáticamente dentro de los tiempos preestablecidos, y si el conteo PDCP del UE en el eNodoB maestro se ajusta automáticamente dentro de los tiempos preestablecidos, el eNodoB maestro determina que el cambio de clave de seguridad debe realizarse entre la primera estación base y el UE, y determina que se utilizará un modo de actualización de clave, donde la primera estación base es el eNodoB maestro;

y/o

B2. Cuando el eNodoB maestro recibe información de indicación que es enviada por el eNodoB secundario y que indica que un conteo PDCP en un eNodoB secundario se ajusta automáticamente dentro de los tiempos preestablecidos, o el eNodoB maestro recibe información de indicación que es enviada por el eNodoB secundario y que indica que el eNodoB secundario debe realizar la actualización de clave, o el eNodoB maestro recibe información de indicación que es informada por el UE y que indica que un conteo PDCP actual en un lado del eNodoB secundario se ajusta automáticamente dentro de los tiempos preestablecidos, el eNodoB maestro determina que el cambio de clave de seguridad debe realizarse entre la primera estación base y el UE y determina que debe utilizarse un modo de actualización de clave, donde la primera estación base es el eNodoB secundario.

Es decir, si el conteo PDCP actual del UE en el eNodoB maestro se ajusta automáticamente dentro de los tiempos preestablecidos, los tiempos preestablecidos pueden determinarse por el eNodoB maestro y el eNodoB maestro puede fijar un valor de los tiempos según un escenario de aplicación específico, que no se limita en la presente memoria. Además, que el conteo PDCP actual del UE en el lado del eNodoB maestro se ajuste automáticamente dentro de los tiempos preestablecidos puede describirse simplemente a continuación: el conteo PDCP actual del UE en el lado del eNodoB maestro está a punto de ajustarse automáticamente; que el conteo PDCP actual del UE en el eNodoB maestro no se ajuste automáticamente dentro de los tiempos preestablecidos puede describirse simplemente a continuación: el conteo PDCP actual del UE en el lado del eNodoB maestro no está a punto de ajustarse automáticamente. En la etapa B1, el eNodoB maestro determina, luego de determinar que el conteo PDCP está a punto de ajustarse automáticamente, que el cambio de clave de seguridad debe realizarse entre el eNodoB maestro y el UE y que se utilizará el modo de actualización de clave; en este caso, la primera estación base puede referirse al eNodoB maestro.

Para la etapa B2, si se presentan cualquiera de las siguientes tres condiciones, el eNodoB maestro puede determinar que el cambio de clave de seguridad debe realizarse entre el eNodoB secundario y el UE y que el cambio se debe realizar en el modo de actualización de clave. Las tres condiciones son respectivamente las siguientes: 1. El conteo PDCP en el lado del eNodoB secundario se ajusta automáticamente dentro de los tiempos preestablecidos y el eNodoB secundario envía al eNodoB maestro la información de indicación de que el conteo PDCP en el lado del eNodoB secundario se ajusta automáticamente dentro de los tiempos preestablecidos; 2. El eNodoB secundario debe realizar la actualización de clave y el eNodoB secundario envía al eNodoB maestro la información de indicación de que el eNodoB secundario debe realizar la actualización de clave; y 3. El UE descubre que el conteo PDCP actual en el lado del eNodoB secundario se ajusta automáticamente dentro de los tiempos preestablecidos y el UE informa al eNodoB maestro, que el conteo PDCP actual en el lado del eNodoB secundario se ajusta automáticamente dentro de los tiempos preestablecidos. Los tiempos preestablecidos pueden determinarse mediante el eNodoB secundario y el eNodoB secundario puede fijar un valor del período según un escenario de aplicación específico que no se limita en la presente memoria. Además, que el conteo PDCP en el lado del eNodoB secundario se ajuste automáticamente dentro de los tiempos preestablecidos puede describirse simplemente a continuación: el conteo PDCP en el lado del eNodoB secundario está a punto de ajustarse automáticamente. En la etapa B2, el eNodoB maestro determina, luego

de determinar que el conteo PDCP está a punto de ajustarse automáticamente, que el cambio de clave de seguridad debe realizarse entre el eNodoB secundario y el UE y que se utilizará el modo de actualización de clave; en este caso, la primera estación base puede referirse al eNodoB secundario. Además, al menos uno de la etapa B1 y la etapa B2 debe realizarse. Cuando se implementan la etapa B1 y etapa B2, el eNodoB maestro puede determinar que el cambio de clave de seguridad debe realizarse entre el eNodoB maestro y el UE, el eNodoB puede determinar además que se debe realizar el cambio de clave de seguridad entre el eNodoB secundario y el UE y el eNodoB maestro determina que los cambios de clave de seguridad se realicen en el modo de actualización de clave.

102. El eNodoB maestro envía un mensaje de comando de cambio de clave al UE de manera que el UE realice, según el mensaje de comando de cambio de clave, el cambio de clave de seguridad entre el UE y la primera estación base, y determina, según el mensaje de comando de cambio de clave, si mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o un eNodoB secundario y/o si mantener la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario.

En esta realización de la presente invención, en la etapa 101, el eNodoB maestro puede determinar cuál del eNodoB maestro y el eNodoB secundario debe realizar el cambio de clave de seguridad con el UE, el eNodoB maestro determina que el cambio de clave de seguridad debe realizarse entre la primera estación base y el UE y luego el eNodoB maestro envía el mensaje de comando de cambio de clave al UE para activar al UE para realizar el cambio de clave de seguridad, donde el mensaje de comando de cambio de clave porta información de identificación de la estación base, entre el eNodoB maestro y el eNodoB secundario, con el que el UE debe realizar el cambio de clave de seguridad, y el mensaje de comando de cambio de clave puede transmitir además información de indicación que indica un modo en el que el UE realiza el cambio de clave de seguridad.

En algunas realizaciones de la presente invención, el mensaje de comando de cambio de clave enviado por el eNodoB maestro al UE incluye una primera información de indicación y una segunda información de indicación, donde:

la primera información de indicación se utiliza para indicar que el cambio de clave de seguridad debe realizarse entre el eNodoB maestro y el UE; y
la segunda información de indicación se utiliza para indicar que el cambio de clave de seguridad debe realizarse entre el eNodoB secundario y el UE.

Es decir, el mensaje de comando de cambio de clave generado por el eNodoB maestro porta la primera información de indicación y la segunda información de indicación, y las dos piezas de información de indicación se utilizan separadamente para indicar, al UE, si realizar el cambio de clave de seguridad. La primera información de indicación indica el eNodoB maestro y la segunda información de indicación indica el eNodoB secundario. El eNodoB maestro puede establecer específicamente dos áreas en el mensaje de comando de cambio de clave para representar respectivamente valores de la primera información de indicación y la segunda información de indicación. Por ejemplo, cuando la primera información de indicación indica que el cambio de clave de seguridad debe realizarse entre el eNodoB maestro y el UE y la segunda información de indicación indica que el cambio de clave de seguridad debe realizarse entre el eNodoB secundario y el UE, el eNodoB maestro puede determinar que la primera estación base se refiere al eNodoB maestro y el eNodoB secundario; por lo tanto, el UE puede descubrir a partir de la primera información de indicación y la segunda información de indicación que el cambio de clave de seguridad debe realizarse de forma separada entre el UE y el eNodoB maestro y entre el UE y el eNodoB secundario.

Además, en otras realizaciones de la presente invención, la primera información de indicación se utiliza además para indicar que un modo para realizar el cambio de clave de seguridad entre el eNodoB maestro y el UE es la regeneración de clave o la actualización de clave; la segunda información de indicación se utiliza además para indicar que un modo para realizar el cambio de clave de seguridad entre el eNodoB secundario y el UE es la regeneración de clave o la actualización de clave. Es decir, luego de agregar la primera información de indicación y la segunda información de indicación al mensaje de comando de cambio de clave generado, el eNodoB puede utilizar además la primera información de indicación y la segunda información de indicación para indicar un modo para realizar el cambio de clave de seguridad. La primera información de indicación indica el eNodoB maestro y la segunda información de indicación indica el eNodoB secundario. El eNodoB maestro puede establecer específicamente dos áreas en el mensaje de comando de cambio de clave para representar respectivamente valores de la primera información de indicación y la segunda información de indicación. Por lo tanto, cuando la primera información de indicación indica que un modo para realizar el cambio de clave de seguridad entre el eNodoB maestro y el UE es la regeneración de clave, y la segunda información de indicación indica que un modo para realizar el cambio de clave de seguridad entre el eNodoB secundario y el UE es la actualización de clave, el UE puede descubrir, a partir de la primera información de indicación, que el modo para realizar el cambio de clave de seguridad entre el UE y el eNodoB maestro es la regeneración de clave, y el UE puede descubrir, a partir de la segunda información de indicación, que el modo para realizar el cambio de clave de seguridad entre el UE y el eNodoB secundario es la actualización de clave.

En otras realizaciones de la presente invención, el mensaje de comando de cambio de clave enviado por el eNodoB maestro al UE incluye una primera información de contexto de clave de seguridad y una segunda información de contexto de clave de seguridad, donde:

la primera información de contexto de clave de seguridad se utiliza para indicar que el cambio de clave de

seguridad debe realizarse entre el eNodoB maestro y el UE; y
la segunda información de contexto de clave de seguridad se utiliza para indicar que el cambio de clave de seguridad debe realizarse entre el eNodoB secundario y el UE.

Es decir, el mensaje de comando de cambio de clave generado por el eNodoB maestro porta la primera información de contexto de clave de seguridad y la segunda información de contexto de clave de seguridad y las dos piezas de la información de contexto de clave de seguridad se utilizan separadamente para indicar, al UE, si se realiza el cambio de clave de seguridad. La primera información de contexto de clave de seguridad indica el eNodoB maestro y la segunda información de contexto de clave de seguridad indica el eNodoB secundario. El eNodoB maestro puede establecer específicamente dos áreas en el mensaje de comando de cambio de clave para representar respectivamente valores de la primera información de contexto de clave de seguridad y la segunda información de contexto de clave de seguridad. Por lo tanto, cuando la primera información de contexto de clave de seguridad indica que el cambio de clave de seguridad debe realizarse entre el eNodoB maestro y el UE y la segunda información de contexto de clave de seguridad indica que el cambio de clave de seguridad debe realizarse entre el eNodoB secundario y el UE, el eNodoB maestro puede determinar que la primera estación base se refiere al eNodoB maestro y el eNodoB secundario; por lo tanto, el UE puede descubrir, a partir de la primera información de contexto de clave de seguridad y la segunda información de contexto de clave de seguridad que el cambio de clave de seguridad debe realizarse de forma separada entre el UE y el eNodoB maestro y entre el UE y el eNodoB secundario.

Además, en otras realizaciones de la presente invención, la primera información de contexto de clave de seguridad se utiliza además para indicar que un modo para realizar el cambio de clave de seguridad entre el eNodoB maestro y el UE es la regeneración de clave o la actualización de clave; la segunda información de contexto de clave de seguridad se utiliza además para indicar que un modo para realizar el cambio de clave de seguridad entre el eNodoB secundario y el UE es la regeneración de clave o la actualización de clave. Es decir, luego de agregar la primera información de contexto de clave de seguridad y la segunda información de contexto de clave de seguridad al mensaje de comando de cambio de clave, el eNodoB puede utilizar además la primera información de contexto de clave de seguridad y la segunda información de contexto de clave de seguridad para indicar un modo para realizar el cambio de clave de seguridad. La primera información de contexto de clave de seguridad indica el eNodoB maestro y la segunda información de contexto de clave de seguridad indica el eNodoB secundario. El eNodoB maestro puede establecer específicamente dos áreas en el mensaje de comando de cambio de clave para representar respectivamente valores de la primera información de contexto de clave de seguridad y la segunda información de contexto de clave de seguridad. Por lo tanto, cuando la primera información de contexto de clave de seguridad indica que un modo para realizar el cambio de clave de seguridad entre el eNodoB maestro y el UE es la regeneración de clave, y la segunda información de contexto de clave de seguridad indica que un modo para realizar el cambio de clave de seguridad entre el eNodoB secundario y el UE es la actualización de clave, el UE puede descubrir, a partir de la primera información de contexto de clave de seguridad, que el modo para realizar el cambio de clave de seguridad entre el UE y el eNodoB maestro es la regeneración de clave, y el UE puede descubrir, a partir de la segunda información de contexto de clave de seguridad, que el modo para realizar el cambio de clave de seguridad entre el UE y el eNodoB secundario es la actualización de clave.

En otras realizaciones de la presente invención, el mensaje de comando de cambio de clave enviado por el eNodoB maestro al UE incluye un indicador de cambio de clave (en inglés, Key Change Indicator). El eNodoB maestro puede indicar, al utilizar un valor de un campo del indicador de cambio de clave, que un modo para realizar el cambio de clave de seguridad entre la primera estación base y el UE es la regeneración de clave o la actualización de clave. Por ejemplo, el eNodoB maestro puede establecer el valor del campo del indicador de cambio de clave en verdadero (en inglés, True) para representar que la regeneración de clave debe realizarse entre la primera estación base y el UE; el eNodoB maestro puede establecer el valor del campo del indicador de cambio de clave a falso (en inglés, False) para representar que la actualización de clave debe realizarse entre la primera estación base y el UE.

En otras realizaciones de la presente invención, el mensaje de comando de cambio de clave enviado por el eNodoB maestro al UE incluye, además: información de indicación que indica la transmisión de datos entre el UE y la primera estación base o una segunda estación base. El contenido de la información de indicación puede estar en cualquiera de las siguientes tres condiciones: 1. que indica que el UE mantiene la transmisión de datos entre el UE y la segunda estación base; 2. que indica que el UE suspende la transmisión de datos entre el UE y la primera estación base; y 3. que indica que el UE detiene la transmisión de datos entre el UE y la primera estación base. Cuando la segunda estación base es el eNodoB maestro, la primera estación base es el eNodoB secundario; o cuando la segunda estación base es el eNodoB secundario, la segunda estación base es el eNodoB maestro. Específicamente, cuando el contenido de la información de indicación anterior está en la condición 1 o 2, el UE realiza, según la información de indicación anterior, el cambio de clave de seguridad en un modo de actualización de clave; cuando el contenido de la información de indicación anterior está en la condición 3, el UE realiza, según la información de indicación anterior, el cambio de clave de seguridad de un modo de regeneración de clave.

Debería apreciarse que, en algunas realizaciones de la presente invención, el mensaje de comando de cambio de clave enviado por el eNodoB maestro al UE es específicamente un mensaje de comando de traspaso (en inglés, Handover - HO) intracelular. Es decir, en esta realización de la presente invención, un proceso para cambiar una clave de seguridad cuando el UE realiza la comunicación de conectividad dual, puede completarse en un proceso de traspaso intracelular, donde el proceso de traspaso intracelular se refiere a que una célula de origen y una célula

objetivo son la misma célula de una estación base cuando el UE lleva a cabo el traspaso, es decir, las células primarias antes y después del traspaso son una misma célula, y no cambian.

103. El eNodoB maestro recibe un mensaje de cambio de clave completado enviado por el UE de manera que la primera estación base determina que se completa el cambio de clave de seguridad entre el UE y la primera estación base.

En esta realización de la presente invención, luego de que el UE recibe el mensaje de comando de cambio de clave enviado por el eNodoB maestro, el UE puede realizar el cambio de clave de seguridad entre el UE y la primera estación base según el mensaje de comando de cambio de clave. Luego de que el UE completa el cambio de clave de seguridad entre el UE y la primera estación base, el UE envía el mensaje de cambio de clave completado al eNodoB maestro y el eNodoB maestro puede recibir el mensaje de cambio de clave completado enviado por el UE. Luego de que el eNodoB maestro recibe el mensaje de cambio de clave completado enviado por el UE, la primera estación base puede determinar, al utilizar el mensaje de cambio de clave completado recibido por el eNodoB maestro, que se complete el cambio de clave de seguridad entre el UE y la primera estación base. La primera estación base puede utilizar una nueva clave de seguridad para continuar realizando la transmisión de datos con el UE. Debería apreciarse que puede aprenderse de las descripciones anteriores que la primera estación base puede referirse al eNodoB maestro o puede referirse al eNodoB secundario o puede referirse al eNodoB maestro y el eNodoB secundario; por lo tanto, luego de obtener una retroalimentación desde el UE de que se completó el cambio de clave de seguridad, la estación base que debe realizar el cambio de clave de seguridad con el UE debe instruirse para continuar realizando la transmisión de datos con el UE. Por lo tanto, el cambio de clave de seguridad entre el eNodoB maestro y el UE no afecta la transmisión de datos entre el eNodoB secundario y el UE; asimismo, el cambio de clave de seguridad entre el eNodoB secundario y el UE no afecta la transmisión de datos entre el eNodoB maestro y el UE.

Debería apreciarse que, en otras realizaciones de la presente invención, si la primera estación base determinada por el eNodoB maestro incluye el eNodoB secundario, luego de la etapa 103 de la recepción, mediante un eNodoB maestro, de un mensaje de cambio de clave completado enviado por el UE, esta realización de la presente invención puede incluir además la siguiente etapa:

reenviar, mediante el eNodoB maestro, el mensaje de cambio de clave completado al eNodoB secundario, de manera que el eNodoB secundario determina que se complete el cambio de clave de seguridad entre el UE y el eNodoB secundario.

Es decir, si el UE realiza el cambio de clave de seguridad entre el UE y el eNodoB secundario, cuando el eNodoB maestro recibe una retroalimentación desde el UE de que se completó el cambio de clave de seguridad entre el UE y el eNodoB secundario, el eNodoB maestro puede reenviar el mensaje de cambio de clave completado al eNodoB secundario. El eNodoB secundario determina, al utilizar el mensaje de cambio de clave completado, que se complete el cambio de clave de seguridad entre el UE y el eNodoB secundario, y luego el eNodoB secundario puede restaurar la transmisión de datos entre el UE y el eNodoB secundario según el mensaje de cambio de clave completado.

En algunas realizaciones de la presente invención, el mensaje de comando de cambio de clave enviado por el eNodoB maestro al UE puede transmitir además información de indicación que indica si el UE realiza acceso aleatorio a la primera estación base. Es decir, el eNodoB maestro puede notificar específicamente al UE de una estación base a la que se le realiza acceso aleatorio y el UE puede iniciar acceso aleatorio según la indicación del eNodoB maestro. Además, si el mensaje de comando de cambio de clave indica que el UE realiza acceso aleatorio a la primera estación base y la primera estación base incluye el eNodoB maestro, etapa 102 del envío, mediante el eNodoB maestro, un mensaje de comando de cambio de clave al UE específicamente incluye:

enviar, mediante el eNodoB maestro, al UE un mensaje de comando de cambio de clave que incluye información sobre un recurso de acceso aleatorio de manera que el UE realiza acceso aleatorio a la primera estación base según la información sobre el recurso de acceso aleatorio.

Es decir, si el eNodoB maestro le ordena al UE que realice acceso aleatorio al eNodoB maestro, el eNodoB maestro puede asignar un recurso de acceso aleatorio al UE y agregar información sobre el recurso de acceso aleatorio al mensaje de comando de cambio de clave. Cuando el UE envía una solicitud de acceso aleatorio al eNodoB maestro, el eNodoB maestro envía una respuesta de acceso aleatorio al UE para ordenar al UE a realizar acceso aleatorio al eNodoB maestro de manera de completar todo un proceso de acceso aleatorio. Debería apreciarse que el eNodoB maestro ordena al UE a realizar acceso aleatorio al eNodoB secundario, el UE y el eNodoB secundario pueden completar todo un proceso de acceso aleatorio según el método que antecede. Por supuesto, el eNodoB maestro también puede ordenar al UE a que realice acceso aleatorio al eNodoB maestro y al eNodoB secundario. Cuando el UE realiza acceso aleatorio al eNodoB maestro y al eNodoB secundario, los dos procesos de acceso aleatorio pueden realizarse simultáneamente. Además, cuando el UE realiza acceso aleatorio al eNodoB secundario, el eNodoB secundario puede determinar, luego de determinar que el UE realiza exitosamente un proceso de acceso aleatorio, que se completó el cambio de clave de seguridad. Por lo tanto, en este caso, el eNodoB maestro puede no enviar el mensaje de cambio de clave completado al eNodoB secundario.

Se puede aprender de las descripciones anteriores en esta realización de la presente invención que: un eNodoB

maestro determina que se debe realizar un cambio de clave de seguridad entre una primera estación base y un UE, donde la primera estación base incluye al menos uno del eNodoB maestro y un eNodoB secundario; luego de que el eNodoB maestro determina que se debe realizar el cambio de clave de seguridad entre la primera estación base y el UE, el eNodoB maestro envía un mensaje de comando de cambio de clave al UE, de manera que el UE realiza, según el mensaje de comando de cambio de clave, el cambio de clave de seguridad entre el UE y la primera estación base, y determina, según el mensaje de comando de cambio de clave, si mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o el eNodoB secundario y/o si mantener la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario; y luego de que el UE completa el cambio de clave de seguridad, el UE envía un mensaje de cambio de clave completado al eNodoB maestro, el eNodoB maestro puede recibir el mensaje de cambio de clave completado enviado por el UE, de manera que la primera estación base pueda determinar, al utilizar el eNodoB maestro, que se complete el cambio de clave de seguridad entre el UE y la primera estación base, y la primera estación base y el UE pueden utilizar una nueva clave de seguridad para realizar la transmisión de datos. Por lo tanto, según esta realización de la presente invención, puede implementarse un cambio de clave de seguridad cuando un UE lleva a cabo la comunicación de conectividad dual con un MeNB y un SeNB.

La realización anterior describe el método de cambio de clave de seguridad proporcionado en las realizaciones de la presente invención desde la perspectiva de un eNodoB maestro y lo siguiente describe el método de cambio de clave de seguridad proporcionado en las realizaciones de la presente invención en detalle desde la perspectiva del equipo de usuario. Otra realización del método de cambio de clave de seguridad de la presente invención puede aplicarse al equipo de usuario, y es particularmente aplicable a un UE que lleva a cabo la comunicación de conectividad dual con al menos dos estaciones base. El método puede incluir las siguientes etapas: recibir, mediante el UE, un mensaje de comando de cambio de clave enviado por un eNodoB maestro, donde el mensaje de comando de cambio de clave incluye información de indicación de que el eNodoB maestro ordena que puede realizarse un cambio de clave de seguridad entre el UE y una primera estación base, donde la primera estación base incluye al menos uno del eNodoB maestro y un eNodoB secundario; realizar, mediante el UE según el mensaje de comando de cambio de clave, el cambio de clave de seguridad entre el UE y la primera estación base; determinar, mediante el UE según el mensaje de comando de cambio de clave, si mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o el eNodoB secundario y/o si mantener la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario; y enviar, mediante el UE, un mensaje de cambio de clave completado al eNodoB maestro, de manera que la primera estación base determina que se complete el cambio de clave de seguridad entre el UE y la primera estación base.

Con respecto a la Figura 2, un método de cambio de clave de seguridad según otra realización de la presente invención puede incluir las siguientes etapas:

201. Un UE recibe un mensaje de comando de cambio de clave enviado por un eNodoB maestro.

El mensaje de comando de cambio de clave incluye información de indicación de que el eNodoB maestro ordena que se realice un cambio de clave de seguridad entre el UE y una primera estación base, donde la primera estación base incluye al menos uno del eNodoB maestro y un eNodoB secundario.

En esta realización de la presente invención, normalmente se necesita una clave de seguridad durante la transmisión de datos entre una estación base y el UE. En algunos casos, la clave de seguridad debe ser cambiada. Asimismo, cuando un UE lleva a cabo la comunicación al utilizar dos nodos de red, normalmente existe un requisito de aplicación de cambiar una clave de seguridad utilizada por el UE que lleva a cabo la comunicación de conectividad dual. En esta realización de la presente invención, para resolver un problema de cambio de clave de seguridad cuando el UE realiza la comunicación de conectividad dual, el eNodoB maestro puede determinar primero si el cambio de clave de seguridad debe realizarse entre el eNodoB maestro y el UE y si el cambio de clave de seguridad debe realizarse entre el eNodoB secundario y el UE. Es decir, el eNodoB maestro detecta un proceso de transmisión de datos entre el eNodoB maestro y el UE y un proceso de transmisión de datos entre el eNodoB secundario y el UE cuando el UE utiliza recursos de radio proporcionados por el eNodoB maestro y el eNodoB secundario para realizar la comunicación de conectividad dual, y luego el eNodoB maestro determina si el cambio de clave de seguridad debe realizarse entre el eNodoB maestro y el UE y si el cambio de clave de seguridad debe realizarse entre el eNodoB secundario y el UE. Además, el eNodoB maestro puede determinar una manera para realizar el cambio de clave de seguridad entre el eNodoB maestro y el UE y el eNodoB maestro puede determinar además un modo para realizar el cambio de clave de seguridad entre el eNodoB secundario y el UE.

Luego de que el eNodoB maestro determina que el cambio de clave de seguridad debe realizarse entre el eNodoB maestro y el UE y/o el cambio de clave de seguridad debe realizarse entre el eNodoB secundario y el UE, el eNodoB maestro puede enviar el mensaje de comando de cambio de clave al UE para indicar que el cambio de clave de seguridad debe realizarse entre el UE y la primera estación base, donde la primera estación base representa una estación base que está determinada por el eNodoB maestro y que debe realizar el cambio de clave de seguridad con el UE. En esta realización de la presente invención, la primera estación base se determina específicamente de tres modos: 1. La primera estación base es el eNodoB maestro; 2. La primera estación base es el eNodoB secundario; y 3. La primera estación base es el eNodoB maestro y el eNodoB secundario. Es decir, el eNodoB maestro puede seleccionar uno de tres modos de implementación de la primera estación base al utilizar un comando de indicación de clave. Por ejemplo, si una MME indica, al utilizar el comando de indicación de clave, que se debe realizar el cambio

de clave de seguridad solamente entre el eNodoB maestro y el UE y que se debe usar un modo de regeneración de clave, el eNodoB maestro puede determinar que la primera estación base específicamente se refiera al eNodoB maestro. El eNodoB maestro agrega un identificador del eNodoB maestro al mensaje de comando de cambio de clave enviado al UE, y el UE puede descubrir, a partir del mensaje de comando de cambio de clave, que el cambio de clave de seguridad debe realizarse entre el UE y el eNodoB maestro.

Cabe destacar que el eNodoB maestro puede agregar, además, al mensaje de comando de cambio de clave, información de indicación que indica un modo en el que el UE realiza el cambio de clave de seguridad. Específicamente, el modo que es indicado por el eNodoB maestro y en el que el UE realiza el cambio de clave de seguridad incluye la regeneración de clave y la actualización de clave. Tanto la regeneración de clave como la actualización de clave se utilizan esencialmente para realizar el cambio de clave de seguridad. El UE puede descubrir, a partir del mensaje de comando de cambio de clave enviado por el eNodoB maestro, el modo para realizar el cambio de clave de seguridad. Los detalles se describen a continuación:

En algunas realizaciones de la presente invención, si la información de indicación incluida en el mensaje de comando de cambio de clave recibido por el UE incluye una primera información de indicación y segunda información de indicación, donde la primera información de indicación se utiliza para indicar que el cambio de clave de seguridad debe realizarse entre el eNodoB maestro y el UE y la segunda información de indicación se utiliza para indicar que el cambio de clave de seguridad debe realizarse entre el eNodoB secundario y el UE, el UE determina, según la primera información de indicación y/o la segunda información de indicación, que la primera estación base se encuentra en una de las siguientes tres condiciones: la primera estación base es el eNodoB maestro, la primera estación base es el eNodoB secundario y la primera estación base es el eNodoB maestro y el eNodoB secundario.

Es decir, el mensaje de comando de cambio de clave generado por el eNodoB maestro porta la primera información de indicación y la segunda información de indicación y las dos piezas de la información de indicación se utilizan separadamente para indicar, al UE, si se realiza el cambio de clave de seguridad. La primera información de indicación indica el eNodoB maestro y la segunda información de indicación indica el eNodoB secundario. Por ejemplo, cuando la primera información de indicación indica que el cambio de clave de seguridad debe realizarse entre el eNodoB maestro y el UE y la segunda información de indicación indica que el cambio de clave de seguridad debe realizarse entre el eNodoB secundario y el UE, el UE puede determinar que la primera estación base se refiera al eNodoB maestro y al eNodoB secundario; por lo tanto, el UE puede aprender de la primera información de indicación y la segunda información de indicación, que el cambio de clave de seguridad debe realizarse de forma separada entre el UE y el eNodoB maestro y entre el UE y el eNodoB secundario.

Además, en otras realizaciones de la presente invención, la primera información de indicación se utiliza además para indicar que un modo para realizar el cambio de clave de seguridad entre el eNodoB maestro y el UE es la regeneración de clave o la actualización de clave; la segunda información de indicación se utiliza además para indicar que un modo para realizar el cambio de clave de seguridad entre el eNodoB secundario y el UE es la regeneración de clave o la actualización de clave. Es decir, luego de agregar la primera información de indicación y la segunda información de indicación al mensaje de comando de cambio de clave, el eNodoB maestro puede utilizar además la primera información de indicación y la segunda información de indicación para indicar un modo para realizar el cambio de clave de seguridad. La primera información de indicación indica el eNodoB maestro y la segunda información de indicación indica el eNodoB secundario. El eNodoB maestro puede establecer específicamente dos áreas en el mensaje de comando de cambio de clave para representar respectivamente valores de la primera información de indicación y la segunda información de indicación. Por lo tanto, cuando la primera información de indicación indica que un modo para realizar el cambio de clave de seguridad entre el eNodoB maestro y el UE es la regeneración de clave, y la segunda información de indicación indica que un modo para realizar el cambio de clave de seguridad entre el eNodoB secundario y el UE es la actualización de clave, el UE puede aprender, a partir de la primera información de indicación, que el modo para realizar el cambio de clave de seguridad entre el UE y el eNodoB maestro es la regeneración de clave, y el UE puede aprender, a partir de la segunda información de indicación, que el modo para realizar el cambio de clave de seguridad entre el UE y el eNodoB secundario es la actualización de clave.

En otras realizaciones de la presente invención, si la información de indicación incluida en el mensaje de comando de cambio de clave recibido por el UE incluye una primera información de contexto de clave de seguridad y segunda información de contexto de clave de seguridad, donde la primera información de contexto de clave de seguridad se utiliza para indicar que el cambio de clave de seguridad debe realizarse entre el eNodoB maestro y el UE y la segunda información de contexto de clave de seguridad se utiliza para indicar que el cambio de clave de seguridad debe realizarse entre el eNodoB secundario y el UE, el UE determina, según la primera información de contexto de clave de seguridad y/o la segunda información de contexto de clave de seguridad, que la primera estación base se encuentra en una de las siguientes tres condiciones: la primera estación base es el eNodoB maestro, la primera estación base es el eNodoB secundario y la primera estación base es el eNodoB maestro y el eNodoB secundario.

Es decir, el mensaje de comando de cambio de clave generado por el eNodoB maestro porta la primera información de contexto de clave de seguridad y la segunda información de contexto de clave de seguridad, y las dos piezas de información de contexto de clave de seguridad se utilizan separadamente para indicar, al UE, si realizar el cambio de clave de seguridad. La primera información de contexto de clave de seguridad indica el eNodoB maestro y la segunda información de contexto de clave de seguridad indica el eNodoB secundario. Por ejemplo, cuando la primera

información de contexto de clave de seguridad indica que el cambio de clave de seguridad debe realizarse entre el eNodoB maestro y el UE y la segunda información de contexto de clave de seguridad indica que el cambio de clave de seguridad debe realizarse entre el eNodoB secundario y el UE, el UE puede determinar que la primera estación base se refiere al eNodoB maestro y al eNodoB secundario; por lo tanto, el UE puede aprender, de la primera información de contexto de clave de seguridad y la segunda información de contexto de clave de seguridad que el cambio de clave de seguridad debe realizarse de forma separada entre el UE y el eNodoB maestro y entre el UE y el eNodoB secundario.

Además, en otras realizaciones de la presente invención, la primera información de contexto de clave de seguridad se utiliza además para indicar que un modo para realizar el cambio de clave de seguridad entre el eNodoB maestro y el UE es la regeneración de clave o la actualización de clave; la segunda información de contexto de clave de seguridad se utiliza además para indicar que un modo para realizar el cambio de clave de seguridad entre el eNodoB secundario y el UE es la regeneración de clave o la actualización de clave. Es decir, luego de agregar la primera información de contexto de clave de seguridad y la segunda información de contexto de clave de seguridad al mensaje de comando de cambio de clave, el eNodoB maestro puede utilizar además la primera información de contexto de clave de seguridad y la segunda información de contexto de clave de seguridad para indicar un modo para realizar el cambio de clave de seguridad. La primera información de contexto de clave de seguridad indica el eNodoB maestro y la segunda información de contexto de clave de seguridad indica el eNodoB secundario. El eNodoB maestro puede establecer específicamente dos áreas en el mensaje de comando de cambio de clave para representar respectivamente valores de la primera información de contexto de clave de seguridad y la segunda información de contexto de clave de seguridad. Por lo tanto, cuando la primera información de contexto de clave de seguridad indica que un modo para realizar el cambio de clave de seguridad entre el eNodoB maestro y el UE es la regeneración de clave, y la segunda información de contexto de clave de seguridad indica que un modo para realizar el cambio de clave de seguridad entre el eNodoB secundario y el UE es la actualización de clave, el UE puede aprender, a partir de la primera información de contexto de clave de seguridad, que el modo para realizar el cambio de clave de seguridad entre el UE y el eNodoB maestro es la regeneración de clave, y el UE puede aprender, a partir de la segunda información de contexto de clave de seguridad, que el modo para realizar el cambio de clave de seguridad entre el UE y el eNodoB secundario es la actualización de clave.

En otras realizaciones de la presente invención, si la información de indicación incluida en el mensaje de comando de cambio de clave es un campo del indicador de cambio de clave (Key Change Indicator), el UE aprende, desde un valor del campo del indicador de cambio de clave que es la información de indicación incluida en el mensaje de comando de cambio de clave, un modo para realizar el cambio de clave de seguridad entre el UE y la primera estación base. Por ejemplo, el eNodoB maestro puede establecer el valor del campo del indicador de cambio de clave en verdadero para representar que la regeneración de clave debe realizarse entre la primera estación base y el UE, y el UE aprende, del valor establecido de verdadero del indicador de cambio de clave, que se debe realizar la regeneración de clave. El eNodoB maestro puede establecer el valor del campo del indicador de cambio de clave en falso para representar que la regeneración de clave debe realizarse entre la primera estación base y el UE, y el UE aprende, del valor establecido de falso del indicador de cambio de clave, que se debe realizar la actualización de clave.

En algunas realizaciones de la presente invención, el mensaje de comando de cambio de clave enviado por el eNodoB maestro al UE puede transmitir además información de indicación que indica si el UE realiza acceso aleatorio a la primera estación base. Luego de la etapa 201 de la recepción, mediante un UE, de un mensaje de comando de cambio de clave enviado por un eNodoB maestro, esta realización de la presente invención puede incluir además la siguiente etapa:

determinar, mediante el UE según la información de indicación que es transmitida en el mensaje de comando de cambio de clave y que indica si el UE realiza acceso aleatorio a la primera estación base, si se debe realizar acceso aleatorio a la primera estación base.

Es decir, el eNodoB maestro puede notificar especialmente al UE de una estación base a la cual se le deba realizar acceso aleatorio, y el UE puede determinar, según la indicación del eNodoB maestro, si iniciar acceso aleatorio y la estación base a la cual se le deba realizar acceso aleatorio. Si el mensaje de comando de cambio de clave indica que el UE realiza acceso aleatorio a la primera estación base, etapa 201 del receptor, mediante un UE, un mensaje de comando de cambio de clave enviado por un eNodoB maestro incluye:

recibir, mediante el UE, un mensaje de comando de cambio de clave que es enviado por el eNodoB maestro y que incluye información sobre un recurso de acceso aleatorio, y realizar acceso aleatorio a la primera estación base según la información sobre el recurso de acceso aleatorio.

Es decir, si el eNodoB maestro le ordena al UE a realizar acceso aleatorio al eNodoB maestro, el eNodoB maestro puede asignar un recurso de acceso aleatorio al UE y agregar información sobre el recurso de acceso aleatorio al mensaje de comando de cambio de clave. Cuando el UE envía una solicitud de acceso aleatorio al eNodoB maestro, el eNodoB maestro envía una respuesta de acceso aleatorio al UE para ordenar al UE a realizar acceso aleatorio al eNodoB maestro de manera de completar todo un proceso de acceso aleatorio. Debería apreciarse que el eNodoB maestro ordena al UE a realizar acceso aleatorio al eNodoB secundario, el UE y el eNodoB secundario pueden completar todo un proceso de acceso aleatorio según el método que antecede. Por supuesto, el eNodoB maestro

también puede ordenar al UE a que realice acceso aleatorio al eNodoB maestro y el eNodoB secundario. Cuando el UE realiza acceso aleatorio al eNodoB maestro y al eNodoB secundario, los dos procesos de acceso aleatorio pueden realizarse simultáneamente.

202. El UE realiza, según el mensaje de comando de cambio de clave, un cambio de clave de seguridad entre el UE y una primera estación base.

En esta realización de la presente invención, luego de que el UE recibe el mensaje de comando de cambio de clave enviado por el eNodoB maestro, el UE realiza el cambio de clave de seguridad entre el UE y la primera estación base según la indicación del eNodoB maestro. Específicamente, si la primera estación base es el eNodoB maestro, el UE debe realizar un cambio de clave de seguridad entre el UE y el eNodoB maestro; si la primera estación base es el eNodoB secundario, el UE debe realizar un cambio de clave de seguridad entre el UE y el eNodoB secundario; si la primera estación base es el eNodoB maestro y el eNodoB secundario, el UE debe realizar un cambio de clave de seguridad entre el UE y el eNodoB maestro y un cambio de clave de seguridad entre el UE y el eNodoB secundario.

En algunas realizaciones de la presente invención, si el mensaje de comando de cambio de clave recibido por el UE incluye la primera información de indicación y la segunda información de indicación, y el eNodoB maestro indica, al UE al utilizar la primera información de indicación, que el cambio de clave de seguridad debe realizarse entre el eNodoB maestro y el UE, y si la primera información de indicación desde el eNodoB maestro indica además que un modo para realizar el cambio de clave de seguridad entre el eNodoB maestro y el UE es la regeneración de clave o la actualización de clave, etapa 202 de la realización, mediante el UE según el mensaje de comando de cambio de clave, un cambio de clave de seguridad entre el UE y la primera estación base es específicamente: realizar, mediante el UE según la primera información de indicación, el cambio de clave de seguridad entre el UE y el eNodoB maestro en el modo de regeneración de clave o actualización de clave. Es decir, si el eNodoB maestro indica, al UE en la primera información de indicación, que se va a utilizar la regeneración de clave, el UE debe realizar, según la primera información de indicación, el cambio de clave de seguridad entre el UE y el eNodoB maestro en el modo de regeneración de clave; si el eNodoB maestro indica al UE en la primera información de indicación, que se va a utilizar la actualización de clave, el UE debe realizar, según la primera información de indicación, el cambio de clave de seguridad entre el UE y el eNodoB maestro en el modo de actualización de clave.

Además, en algunas realizaciones de la presente invención, si el mensaje de comando de cambio de clave recibido por el UE incluye la primera información de indicación y la segunda información de indicación, y el eNodoB maestro indica, al UE al utilizar la segunda información de indicación, que el cambio de clave de seguridad debe realizarse entre el eNodoB secundario y el UE, y si la segunda información de indicación desde el eNodoB maestro indica además que un modo para realizar el cambio de clave de seguridad entre el eNodoB secundario y el UE es la regeneración de clave o la actualización de clave, etapa 202 de la realización, mediante el UE según el mensaje de comando de cambio de clave, un cambio de clave de seguridad entre el UE y la primera estación base es específicamente: realizar, mediante el UE según la primera información de indicación, el cambio de clave de seguridad entre el UE y el eNodoB secundario en el modo de regeneración de clave o actualización de clave. Es decir, si el eNodoB maestro indica, al UE en la primera información de indicación, que se va a utilizar la regeneración de clave, el UE debe realizar, según la primera información de indicación, el cambio de clave de seguridad entre el UE y el eNodoB secundario en el modo de regeneración de clave; si el eNodoB maestro indica al UE en la primera información de indicación, que se va a utilizar la actualización de clave, el UE debe realizar, según la primera información de indicación, el cambio de clave de seguridad entre el UE y el eNodoB secundario en el modo de actualización de clave.

En algunas realizaciones de la presente invención, si el mensaje de comando de cambio de clave recibido por el UE incluye la primera información de contexto de clave de seguridad y la segunda información de contexto de clave de seguridad, y el eNodoB maestro indica, al UE al utilizar la primera información de contexto de clave de seguridad, que el cambio de clave de seguridad debe realizarse entre el eNodoB maestro y el UE, y si la primera información de contexto de clave de seguridad desde el eNodoB maestro indica además que un modo para realizar el cambio de clave de seguridad entre el eNodoB maestro y el UE es la regeneración de clave o la actualización de clave, etapa 202 de la realización, mediante el UE según el mensaje de comando de cambio de clave, un cambio de clave de seguridad entre el UE y la primera estación base es específicamente: realizar, mediante el UE según la primera información de contexto de clave de seguridad, el cambio de clave de seguridad entre el UE y el eNodoB maestro en el modo de regeneración de clave o actualización de clave. Es decir, si el eNodoB maestro indica, al UE en la primera información de contexto de clave de seguridad, que se va a utilizar la regeneración de clave, el UE debe realizar, según la primera información de contexto de clave de seguridad, el cambio de clave de seguridad entre el UE y el eNodoB maestro en el modo de regeneración de clave; si el eNodoB maestro indica al UE en la primera información de contexto de clave de seguridad, que se va a utilizar la actualización de clave, el UE debe realizar, según la primera información de contexto de clave de seguridad, el cambio de clave de seguridad entre el UE y el eNodoB maestro en el modo de actualización de clave.

Además, en otras realizaciones de la presente invención, si el mensaje de comando de cambio de clave recibido por el UE incluye la primera información de contexto de clave de seguridad y la segunda información de contexto de clave de seguridad, y el eNodoB maestro indica, al UE al utilizar la segunda información de contexto de clave de seguridad, que el cambio de clave de seguridad debe realizarse entre el eNodoB secundario y el UE, y si la segunda información de contexto de clave de seguridad desde el eNodoB maestro indica además que un modo para realizar el cambio de

clave de seguridad entre el eNodoB secundario y el UE es la regeneración de clave o la actualización de clave, etapa 202 de la realización, mediante el UE según el mensaje de comando de cambio de clave, un cambio de clave de seguridad entre el UE y la primera estación base es específicamente: realizar, mediante el UE según la segunda información de contexto de clave de seguridad, el cambio de clave de seguridad entre el UE y el eNodoB secundario en el modo de regeneración de clave o actualización de clave. Es decir, si el eNodoB maestro indica, al UE en la segunda información de contexto de clave de seguridad, que se va a utilizar la regeneración de clave, el UE debe realizar el cambio de clave de seguridad entre el UE y el eNodoB secundario en el modo de regeneración de clave según la segunda información de contexto de clave de seguridad; si el eNodoB maestro indica al UE en la segunda información de contexto de clave de seguridad, que se va a utilizar la actualización de clave, el UE debe realizar el cambio de clave de seguridad entre el UE y el eNodoB secundario en el modo de actualización de clave según la segunda información de contexto de clave de seguridad.

En algunas realizaciones de la presente invención, si la información de indicación incluida en el mensaje de comando de cambio de clave recibido por el UE es el campo del indicador de cambio de clave Key Change Indicator, etapa 202 de la realización, mediante el UE según el mensaje de comando de cambio de clave, un cambio de clave de seguridad entre el UE y la primera estación base es específicamente: determinar, mediante el UE al utilizar el valor del campo del indicador de cambio de clave, la realización del cambio de clave de seguridad entre el UE y la primera estación base en un modo de regeneración de clave o actualización de clave. Por ejemplo, si el valor del campo del indicador de cambio de clave en el mensaje de comando de cambio de clave desde el eNodoB maestro está en verdadero, el UE realiza el cambio de clave de seguridad entre el UE y la primera estación base en un modo de regeneración de clave; si el valor del campo del indicador de cambio de clave en el mensaje de comando de cambio de clave desde el eNodoB maestro está en falso, el UE realiza el cambio de clave de seguridad entre el UE y la primera estación base en un modo de actualización de clave.

203.El UE determina, según el mensaje de comando de cambio de clave, si mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o un eNodoB secundario y/o si mantener la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario.

En esta realización de la presente invención, el UE puede descubrir, del mensaje de comando de cambio de clave, una estación base que debe realizar el cambio de clave de seguridad con el UE y puede aprender además que un modo para realizar el cambio de clave de seguridad es la regeneración de clave o la actualización de clave. Por lo tanto, el UE puede determinar si mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o el eNodoB secundario y/o si mantener la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario. Específicamente, la etapa 203 puede implementarse en los siguientes tres modos: 1. El UE determina si mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o el eNodoB secundario; 2. El UE determina si mantener la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario; y 3. El UE determina si mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o el eNodoB secundario y si mantener la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario. La condición 1 descrita anteriormente incluye dos modos de implementación: en un primer modo, el UE determina si se mantiene la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o el eNodoB secundario; en un segundo modo, el UE determina reconfigurar la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o el eNodoB secundario. Que el UE mantenga la información de configuración de estrato de acceso entre la UE y el eNodoB maestro o el eNodoB secundario puede implementarse específicamente de dos modos: en un primer modo, el UE mantiene la información de configuración de estrato de acceso entre el UE y el eNodoB maestro; en un segundo modo, el UE mantiene la información de configuración de estrato de acceso entre el UE y el eNodoB secundario. La condición 2 descrita anteriormente incluye dos modos de implementación: en un primer modo, el UE determina mantener la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario; en un segundo modo, el UE determina suspender o detener la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario. Que el UE mantenga la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario puede implementarse específicamente de dos modos: en un primer modo, el UE mantiene la transmisión de datos entre el UE y el eNodoB maestro; en un segundo modo, el UE mantiene la transmisión de datos entre el UE y el eNodoB secundario. Que el UE suspenda o detenga la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario puede implementarse de cuatro modos: En un primer modo, el UE suspende la transmisión de datos entre el UE y el eNodoB maestro; en un segundo modo, el UE suspende la transmisión de datos entre el UE y el eNodoB secundario; en un tercer modo, el UE detiene la transmisión de datos entre el UE y el eNodoB maestro; en un cuarto modo, el UE detiene la transmisión de datos entre el UE y el eNodoB secundario.

Cabe destacar que, en algunas realizaciones de la presente invención, el modo de implementación 1 de la etapa 203 en el que el UE determina, según la información de comando de cambio de clave, si mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o el eNodoB secundario incluye la siguiente etapa:

determinar, mediante el UE según la primera información de indicación y la segunda información de indicación que están incluidas en el mensaje de comando de cambio de clave, si mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o el eNodoB secundario, donde la primera información de indicación se utiliza para indicar que el cambio de clave de seguridad debe realizarse entre el eNodoB maestro y

el UE y la segunda información de indicación se utiliza para indicar que el cambio de clave de seguridad debe realizarse entre el eNodoB secundario y el UE;
o
determinar, mediante el UE según la primera información de contexto de clave se seguridad y la segunda información de contexto de clave de seguridad que están incluidas en el mensaje de comando de cambio de clave, si mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o el eNodoB secundario, donde la primera información de contexto de clave de seguridad se utiliza para indicar que el cambio de clave de seguridad debe realizarse entre el eNodoB maestro y el UE y la segunda información de contexto de clave de seguridad se utiliza para indicar que el cambio de clave de seguridad debe realizarse entre el eNodoB secundario y el UE;
o
determinar, mediante el UE según el campo del indicador de cambio de clave Key Change Indicator incluida en el mensaje de comando de cambio de clave, si mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o el eNodoB secundario;
o
determinar, mediante el UE según la información de indicación que está incluida en el mensaje de comando de cambio de clave y que indica que el UE mantiene la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario, si mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o el eNodoB secundario.

Los modos de implementación en los que el UE determina si mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o el eNodoB secundario se describe anteriormente en esta realización. Puede haber otro modo de implementación en función de la inspiración de los modos de implementación proporcionados en esta realización de la presente invención. Solamente se proporciona descripción ilustrativa en la presente.

Específicamente, determinar, mediante el UE según el campo del indicador de cambio de clave incluida en el mensaje de comando de cambio de clave, si mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o el eNodoB secundario incluye:

al determinar, según el campo del indicador de cambio de clave, que se debe realizar la regeneración de clave, determinar no mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o el eNodoB secundario;
o
al determinar, según el campo del indicador de cambio de clave, que se debe realizar la actualización de clave en función de una clave intermedia del lado de UE que corresponde al eNodoB maestro, determinar mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o el eNodoB secundario;
o
al determinar, según el campo del indicador de cambio de clave, que se debe realizar la actualización de clave en función de un NH de siguiente salto, determinar mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o el eNodoB secundario.

Cabe destacar que, en algunas realizaciones de la presente invención, el modo de implementación 2 de la etapa 203 en el que el UE determina, según el mensaje de comando de cambio de clave, si mantener la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario, incluye la siguiente etapa:

determinar, mediante el UE según la primera información de indicación y la segunda información de indicación que están incluidas en el mensaje de comando de cambio de clave, si mantener la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario, donde la primera información de indicación se utiliza para indicar que el cambio de clave de seguridad debe realizarse entre el eNodoB maestro y el UE y la segunda información de indicación se utiliza para indicar que el cambio de clave de seguridad debe realizarse entre el eNodoB secundario y el UE;
o
determinar, mediante el UE según la primera información de contexto de clave de seguridad y la segunda información de contexto de clave de seguridad que están incluidas en el mensaje de comando de cambio de clave, si mantener la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario, donde la primera información de contexto de clave de seguridad se utiliza para indicar que el cambio de clave de seguridad debe realizarse entre el eNodoB maestro y el UE y la segunda información de contexto de clave de seguridad se utiliza para indicar que el cambio de clave de seguridad debe realizarse entre el eNodoB secundario y el UE;
o
determinar, mediante el UE según el campo del indicador de cambio de clave incluida en el mensaje de comando de cambio de clave, si mantener la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario;
o
el UE determina, según la información de indicación que está incluida en el mensaje de comando de cambio de clave y que indica que el UE mantiene la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario, si mantiene la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario.

Los modos de implementación en los que el UE determina si mantener la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario se describen anteriormente en esta realización. Puede haber otro modo de implementación en función de la inspiración de los modos de implementación proporcionados en esta realización de la presente invención. Solamente se proporciona descripción ilustrativa en la presente.

Específicamente, determinar, mediante el UE según el campo del indicador de cambio de clave incluida en el mensaje de comando de cambio de clave, si mantener la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario incluye:

al determinar, según el campo del indicador de cambio de clave, que se debe realizar la regeneración de clave, determinar no mantener la transmisión de datos entre el UE y el eNodoB maestro o entre el UE y el eNodoB secundario; o

al determinar, según el campo del indicador de cambio de clave, que se debe realizar la actualización de clave en función de una clave intermedia del lado de UE que corresponde al eNodoB maestro, determinar mantener la transmisión de datos entre el UE y el eNodoB secundario;

o

al determinar, según el campo del indicador de cambio de clave, que se debe realizar la actualización de clave en función de un NH, determinar mantener la transmisión de datos entre el UE y el eNodoB secundario.

En algunas realizaciones de la presente invención, cuando el UE determina, según la información de comando de cambio de clave, que la información de configuración de estrato de acceso entre el UE y el eNodoB maestro debe mantenerse, y/o que la transmisión de datos entre el UE y el eNodoB maestro debe mantenerse, mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro y/o mantener la transmisión de datos entre el UE y el eNodoB maestro puede incluir específicamente al menos una de las siguientes etapas:

mantener, mediante el UE, configuraciones del protocolo de convergencia de datos por paquetes PDCP de todas las portadoras de radio RB establecidas entre el UE y el eNodoB maestro;

mantener, mediante el UE, configuraciones de Control de Enlace de Radio RLC de todas las RB establecidas entre el UE y el eNodoB maestro;

mantener, mediante el UE, configuraciones de Control de Acceso al Medio MAC de todas las RB establecidas entre el UE y el eNodoB maestro;

mantener, mediante el UE, un estado activo de una célula secundaria, SCell, activada entre el UE y el eNodoB maestro;

mantener, mediante el UE, un identificador temporal de red de radio celular, C-RNTI, utilizado para la comunicación entre el UE y el eNodoB maestro; y

mantener o suspender, mediante el UE, la transmisión de datos entre el UE y el eNodoB maestro.

En algunas realizaciones de la presente invención, cuando el UE determina, según la información de comando de cambio de clave, que la información de configuración de estrato de acceso entre el UE y el eNodoB secundario debe mantenerse, y/o que la transmisión de datos entre el UE y el eNodoB secundario debe mantenerse, mantener la información de configuración de estrato de acceso entre el UE y el eNodoB secundario y/o mantener la transmisión de datos entre el UE y el eNodoB secundario puede incluir específicamente al menos una de las siguientes etapas:

mantener, mediante el UE, configuraciones de PDCP de todas las RB establecidas entre el UE y el eNodoB secundario;

mantener, mediante el UE, configuraciones de todas las RB establecidas entre el UE y el eNodoB secundario;

mantener, mediante el UE, configuraciones de MAC de todas las RB establecidas entre el UE y el eNodoB secundario;

mantener, mediante el UE, un estado activo de una SCell activada entre el UE y el eNodoB secundario;

mantener, mediante el UE, un C-RNTI utilizado para la comunicación entre el UE y el eNodoB secundario; y

mantener o suspender, mediante el UE, la transmisión de datos entre el UE y el eNodoB secundario.

En algunas realizaciones de la presente invención, si el mensaje de comando de cambio de clave indica que el cambio de clave de seguridad debe realizarse entre el eNodoB maestro y el UE, el UE puede determinar reconfigurar la información de configuración de estrato de acceso entre el eNodoB maestro y el UE, y el UE puede determinar suspender o detener la transmisión de datos entre el eNodoB maestro y el UE; si el mensaje de comando de cambio de clave indica que el cambio de clave de seguridad debe realizarse entre el eNodoB secundario y el UE, el UE puede determinar reconfigurar la información de configuración de estrato de acceso entre el eNodoB secundario y el UE y el

UE puede determinar suspender o detener la transmisión de datos entre el eNodoB secundario y el UE. Cabe destacar que en esta realización de la presente invención, luego de que el UE determina si mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o el eNodoB secundario y/o si mantener la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario, el UE puede procesar la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o el eNodoB secundario según un resultado de la determinación, y puede controlar la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario según el resultado de la determinación. Las descripciones se proporcionan de forma separada en los siguientes ejemplos.

En algunas realizaciones de la presente invención, etapa 202 de la determinación, mediante el UE según el mensaje de comando de cambio de clave, un cambio de clave de seguridad entre el UE y la primera estación base incluye la siguiente etapa:

C1. Cuando la primera estación base es el eNodoB maestro, si el UE determina, según el mensaje de comando de cambio de clave, que un modo para realizar el cambio de seguridad entre el eNodoB maestro y el UE es la actualización de clave, el UE realiza el cambio de clave de seguridad entre el UE y el eNodoB maestro en un modo de actualización de clave.

Es decir, si el UE determina, según el mensaje de comando de cambio de clave, que el eNodoB maestro indica que se debe realizar el cambio de clave de seguridad entre el UE y el eNodoB maestro, y un modo para realizar el cambio de clave de seguridad es la actualización de clave, el UE puede realizar el cambio de clave de seguridad entre el UE y el eNodoB maestro en el modo de actualización de clave.

Específicamente, la etapa C1 de la determinación, mediante el UE según el mensaje de comando de cambio de clave, de que un modo para realizar el cambio de clave de seguridad entre el eNodoB maestro y el UE es la actualización de clave, es específicamente:

determinar, mediante el UE según la primera información de indicación o la primera información de contexto de clave de seguridad o información de contexto de seguridad que es transmitida en el mensaje de comando de cambio de clave, que el modo para realizar el cambio de clave de seguridad entre el eNodoB maestro y el UE es la actualización de clave.

Es decir, el eNodoB maestro puede utilizar la primera información de indicación o la información de contexto de clave de seguridad que es transmitida en el mensaje de comando de cambio de clave para indicar que un modo para realizar el cambio de clave de seguridad entre el eNodoB maestro y el UE es la actualización de clave, y luego de recibir el mensaje de comando de cambio de clave, el UE puede descubrir, desde la primera información de indicación o la primera información de contexto de clave de seguridad, que el modo para realizar el cambio de clave de seguridad entre el eNodoB maestro y el UE es la actualización de clave. Además, en algunas realizaciones de la presente invención, el mensaje de comando de cambio de clave puede ser específicamente un mensaje de comando de traspaso intracelular, y en este caso, un contexto de seguridad transmitido en el mensaje de comando de traspaso intracelular se utiliza para indicar que un modo para realizar el cambio de clave de seguridad entre el eNodoB maestro y el UE es la actualización de clave.

Cabe destacar que, en otras realizaciones de la presente invención, luego de la etapa 203 de la determinación, mediante el UE según el mensaje de comando de cambio de clave, si mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o un eNodoB secundario y/o si mantener la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario, el método de cambio de clave de seguridad proporcionado en esta realización de la presente invención incluye además al menos una de las siguientes etapas:

C2. El UE mantiene las configuraciones de PDCP de todas las portadoras de radio (en inglés, Radio Bearer - RB) establecidas entre el UE y el eNodoB secundario.

C3.El UE mantiene las configuraciones del Control de Enlace de Radio (en inglés, Radio Link Control - RLC) de todas las RB establecidas entre el UE y el eNodoB secundario.

C4.El UE mantiene las configuraciones del Control de Acceso al Medio (en inglés, Medium Access Control - MAC) de todas las RB establecidas entre el UE y el eNodoB secundario.

C5. El UE, mantiene el estado activo de la SCell activada entre el UE y el eNodoB secundario.

C6.El UE mantiene el identificador temporal de red de radio celular (en inglés, Cell-Radio Network Temporary Identity - C-RNTI) utilizado para la comunicación entre el UE y el eNodoB secundario.

C7. El UE mantiene o suspende la transmisión de datos entre el UE y el eNodoB secundario.

En la etapa C1, el UE realiza el cambio de clave de seguridad entre el UE y el eNodoB maestro en un modo de actualización de clave, que indica que el cambio de clave de seguridad debe realizarse entre el UE y el eNodoB maestro. En este caso, durante la ejecución de al menos uno de la etapa C2 a la etapa C7, uno o más de la etapa C2

a la etapa C7 pueden ejecutarse según un requerimiento específico. Se mantiene la información de configuración de estrato de acceso entre el UE y el eNodoB secundario y el UE mantiene la transmisión de datos entre el UE y el eNodoB secundario. Por lo tanto, puede evitarse que el cambio de clave de seguridad entre el UE y el eNodoB maestro provoque la reconfiguración de la información de configuración de estrato de acceso de todas las RB y puede asegurarse la transmisión de datos normal en las RB entre el UE y el eNodoB secundario, lo que evita la interrupción de transmisión de datos innecesaria entre el UE y el eNodoB secundario causada por el cambio de clave de seguridad entre el UE y el eNodoB maestro y reduce un retardo de la transmisión de datos innecesario. Cabe destacar que, al mantener el UE las configuraciones de PDCP de todas las RB establecidas entre el UE y el eNodoB secundario descritas en la etapa anterior, significa que el UE mantiene las configuraciones actuales para la información de configuración de las configuraciones de PDCP. Adicionalmente, mantener las configuraciones de RLC y las configuraciones de MAC tiene un significado similar. Mantener el estado activo de la SCell activada entre el UE y el eNodoB secundario significa que el estado activo de la SCell activada permanece el estado activo. Mantener el C-RNTI utilizado para la comunicación entre el UE y el eNodoB secundario significa que el UE utiliza el valor de C-RNTI actual.

Además, la etapa C1 de la realización, mediante el UE, el cambio de clave de seguridad entre el UE y el eNodoB maestro en el modo de actualización de clave puede incluir específicamente las siguientes etapas:

C11. El UE actualiza, en función de un valor de un conteo de encadenamiento de siguiente salto (en inglés, Next Hop Chaining Count) indicado por el mensaje de comando de cambio de clave y mediante el uso de una clave intermedia del lado del UE actual que corresponde al eNodoB maestro o un salto siguiente (en inglés, Next Hop - NH), la clave intermedia del lado del UE que corresponde al eNodoB maestro.

C12. El UE genera, al utilizar una clave intermedia del lado del UE actualizada que corresponde al eNodoB maestro y un algoritmo de seguridad del eNodoB maestro, una nueva clave de seguridad que corresponde al eNodoB maestro, donde la nueva clave de seguridad que corresponde al eNodoB maestro incluye: una clave de cifrado y una clave de protección de integridad que se utilizan para la comunicación entre el UE y el eNodoB maestro.

Cuando se genera la clave de seguridad que corresponde al eNodoB maestro, el UE primero actualiza la clave intermedia del lado del UE que corresponde al eNodoB maestro, y luego utiliza la clave intermedia del lado del UE actualizada que corresponde al eNodoB maestro y el algoritmo de seguridad del eNodoB maestro para generar la nueva clave de seguridad que corresponde al eNodoB maestro.

Específicamente, luego de la etapa 203 de la determinación, mediante el UE según el mensaje de comando de cambio de clave, de si mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o el eNodoB secundario y/o de si mantener la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario, esta realización de la presente invención puede incluir además la siguiente etapa:

determinar, mediante el UE, que la realización del cambio de clave de seguridad entre el UE y el eNodoB maestro en el modo de actualización de clave se basa en la clave intermedia del lado del UE actual que corresponde al eNodoB maestro.

Es decir, si se determina que el UE realice el cambio de clave de seguridad entre el UE y el eNodoB maestro en función de la clave intermedia del lado del UE actual que corresponde al eNodoB maestro, en la etapa C11, la clave intermedia del lado del UE que corresponde al eNodoB maestro puede utilizarse para actualizar la clave intermedia del lado del UE que corresponde al eNodoB maestro, de manera de obtener una clave intermedia del lado del UE actualizada que corresponda al eNodoB maestro.

En algunas realizaciones de la presente invención, etapa 202 de la determinación, mediante el UE según el mensaje de comando de cambio de clave, un cambio de clave de seguridad entre el UE y la primera estación base incluye la siguiente etapa:

D1. Cuando la primera estación base es el eNodoB maestro, si el UE determina, según el mensaje de comando de cambio de clave, que un modo para realizar el cambio de seguridad entre el eNodoB maestro y el UE es la regeneración de clave, el UE realiza el cambio de clave de seguridad entre el UE y el eNodoB maestro en el modo de regeneración de clave.

Es decir, si el UE determina, según el mensaje de comando de cambio de clave, que el eNodoB maestro indica que se debe realizar el cambio de clave de seguridad entre el UE y el eNodoB maestro, y el modo para realizar el cambio de clave de seguridad es la regeneración de clave, el UE puede realizar el cambio de clave de seguridad entre el UE y el eNodoB maestro en el modo de regeneración de clave.

Cabe destacar que, en otras realizaciones de la presente invención, luego de la etapa 203 de la determinación, mediante el UE según el mensaje de comando de cambio de clave, si mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o un eNodoB secundario y/o si mantener la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario, el método de cambio de clave de seguridad proporcionado en esta realización de la presente invención incluye además al menos una de las siguientes etapas:

D2. El UE reconfigura las configuraciones de PDCP de todas las RB establecidas entre el UE y el eNodoB maestro.

D3. El UE reconfigura las configuraciones de PDCP de todas las RB establecidas entre el UE y el eNodoB secundario.

D4. El UE reconfigura las configuraciones de RLC de todas las RB establecidas entre el UE y el eNodoB maestro.

D5. El UE reconfigura las configuraciones de RLC de todas las RB establecidas entre el UE y el eNodoB secundario.

D6. El UE reconfigura las configuraciones de MAC de todas las RB establecidas entre el UE y el eNodoB maestro.

D7. El UE reconfigura las configuraciones de MAC de todas las RB establecidas entre el UE y el eNodoB secundario.

D8. El UE detiene la transmisión de datos entre el UE y el eNodoB maestro.

D9. El UE detiene la transmisión de datos entre el UE y el eNodoB secundario.

En la etapa D1, el UE realiza el cambio de clave de seguridad entre el UE y el eNodoB maestro en el modo de regeneración de clave, que indica que el cambio de clave de seguridad debe realizarse entre el UE y el eNodoB maestro. En este caso, durante la ejecución de al menos uno de la etapa D2 a la etapa D9, uno o más de la etapa D2 a la etapa D9 pueden ejecutarse según un requerimiento específico. La información de configuración de estrato de acceso entre el UE y el eNodoB maestro o el eNodoB secundario está reconfigurada y el UE detiene la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario; por lo tanto, puede evitarse una falla de la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario. Cabe destacar que cuando el UE reconfigura las configuraciones de PDCP descritas en la etapa anterior significa que el UE reconfigura la información de configuración de las configuraciones de PDCP. Adicionalmente, reconfigurar las configuraciones de RLC y las configuraciones de MAC tiene un significado similar.

Además, la etapa D1 de la realización, mediante el UE, del cambio de clave de seguridad entre el UE y el eNodoB maestro en el modo de regeneración de clave puede incluir específicamente las siguientes etapas:

D11. El UE actualiza una clave intermedia del lado del UE entre el UE y el eNodoB maestro en función de una clave intermedia de entidad de gestión de seguridad de acceso actualizada (en inglés, Access Stratum Management Entity - ASME).

D12. El UE genera, según una clave intermedia del lado del UE actualizada que corresponde al eNodoB maestro y un algoritmo de seguridad del eNodoB maestro, una nueva clave de seguridad que corresponde al eNodoB maestro, donde la nueva clave de seguridad que corresponde al eNodoB maestro incluye: una clave de cifrado y una clave de protección de integridad que se utilizan para la comunicación entre el UE y el eNodoB maestro.

Cuando se genera la clave de seguridad que corresponde al eNodoB maestro, el UE primero actualiza la clave intermedia del lado del UE que corresponde al eNodoB maestro, y luego utiliza la clave intermedia del lado del UE actualizada que corresponde al eNodoB maestro y el algoritmo de seguridad del eNodoB maestro para generar la nueva clave de seguridad que corresponde al eNodoB maestro.

Además, en algunas realizaciones de la presente invención, luego de la etapa D11 de la actualización de una clave intermedia del lado del UE entre el UE y el eNodoB maestro en función de una clave intermedia de la entidad de gestión de seguridad de acceso actualizada ASME, el método de cambio de clave de seguridad proporcionado en esta realización de la presente invención puede incluir además las siguientes etapas:

E1. El UE actualiza, según la clave intermedia del lado del eNodoB maestro e información de célula, asociado con el cambio de clave de seguridad, del eNodoB secundario o información de estación base, asociado con el cambio de clave de seguridad, del eNodoB secundario, una clave intermedia del lado del UE que corresponde al eNodoB secundario.

E2. El UE genera, según una clave intermedia del lado del UE actualizada que corresponde al eNodoB secundario y un algoritmo de seguridad del eNodoB secundario, una nueva clave de seguridad que corresponde al eNodoB secundario, donde la nueva clave de seguridad que corresponde al eNodoB secundario incluye una clave de cifrado utilizada para la comunicación entre el UE y el eNodoB secundario.

Cuando el UE genera la clave de seguridad que corresponde al eNodoB secundario, el UE debe utilizar la clave intermedia del lado del eNodoB maestro actualizada, que puede adquirirse en la etapa D11, para actualizar la clave intermedia del lado del UE que corresponde al eNodoB secundario, y luego utilizar la clave intermedia del lado del UE actualizada que corresponde al eNodoB secundario y al algoritmo de seguridad del eNodoB secundario para generar la nueva clave de seguridad que corresponde al eNodoB secundario. Cabe destacar que el algoritmo de seguridad del eNodoB secundario utilizado por el UE en la etapa E2 puede ser el mismo que el algoritmo de seguridad del eNodoB maestro utilizado por el UE en la etapa D11; ciertamente, el algoritmo de seguridad del eNodoB secundario utilizado por el UE en la etapa E2 puede ser diferente del algoritmo de seguridad del eNodoB maestro utilizado por el UE en la etapa D11, que puede determinarse específicamente según un escenario de aplicación y con fines meramente descriptivos y no se pretende que sea taxativo.

Específicamente, la etapa D1 de la determinación, mediante el UE según el mensaje de comando de cambio de clave, de que un modo para realizar el cambio de clave de seguridad entre el eNodoB maestro y el UE es la regeneración de clave, es específicamente:

determinar, mediante el UE según la primera información de indicación de la primera información de contexto de clave de seguridad o información de contexto de seguridad que es transmitida en el mensaje de comando de cambio de clave, que el modo para realizar el cambio de clave de seguridad entre el eNodoB maestro y el UE es la actualización de clave.

Es decir, el eNodoB maestro puede utilizar la primera información de indicación o la primera información de contexto de clave de seguridad que es transmitida en el mensaje de comando de cambio de clave para indicar que un modo para realizar el cambio de clave de seguridad entre el eNodoB maestro y el UE es la regeneración de clave, y luego de recibir el mensaje de comando de cambio de clave, el UE puede descubrir, desde la primera información de indicación o la primera información de contexto de clave de seguridad, que el modo para realizar el cambio de clave de seguridad entre el eNodoB maestro y el UE es la regeneración de clave. Además, en algunas realizaciones de la presente invención, el mensaje de comando de cambio de clave puede ser específicamente un mensaje de comando de traspaso intracelular, y en este caso, un contexto de seguridad transmitido en el mensaje de comando de traspaso intracelular se utiliza para indicar que un modo para realizar el cambio de clave de seguridad entre el eNodoB maestro y el UE es la regeneración de clave.

En algunas realizaciones de la presente invención, si la información de indicación incluida en el mensaje de comando de cambio de clave indica que el UE mantiene la transmisión de datos entre el UE y una segunda estación base, luego de la etapa 203 de la determinación, mediante el UE según el mensaje de comando de cambio de clave, de si mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o un eNodoB secundario y/o de si mantener la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario, el método de cambio de clave de seguridad proporcionado en esta realización de la presente invención incluye además al menos una de las siguientes etapas:

F1. El UE mantiene las configuraciones de PDCP de todas las RB establecidas entre el UE y la segunda estación base.

F2. El UE mantiene las configuraciones de RLC de todas las RB establecidas entre el UE y la segunda estación base.

F3. El UE mantiene las configuraciones de MAC de todas las RB establecidas entre el UE y la segunda estación base.

F4. El UE mantiene un estado activo de una SCell activada entre el UE y la segunda estación base.

F5. El UE mantiene un C-RNTI utilizado para la comunicación entre el UE y la segunda estación base.

F6. El UE mantiene la transmisión de datos entre el UE y la segunda estación base.

La información de indicación incluida en el mensaje de comando de cambio de clave indica que el UE mantiene la transmisión de datos entre el UE y la segunda estación base. Cuando la segunda estación base es el eNodoB maestro, la primera estación base es el eNodoB secundario; o cuando la segunda estación base es el eNodoB secundario, la segunda estación base es el eNodoB maestro. Cuando la información de indicación incluida en el mensaje de comando de cambio de clave indica que el UE mantiene la transmisión de datos entre el UE y la segunda estación base, este indica que el cambio de clave de seguridad debe realizarse entre el UE y la primera estación base. En este caso, durante la ejecución de al menos uno de la etapa F1 a la etapa F6, uno o más de la etapa F1 a la etapa F6 pueden ejecutarse según un requerimiento específico. Se mantiene la información de configuración de estrato de acceso entre el UE y la segunda estación base y el UE mantiene la transmisión de datos entre el UE y la segunda estación base. Por lo tanto, puede evitarse que el cambio de clave de seguridad entre el UE y la primera estación base provoque la reconfiguración de la información de configuración de estrato de acceso de todas las RB y puede asegurarse la transmisión de datos normal en las RB entre el UE y la segunda estación base, lo que evita la interrupción de transmisión de datos innecesaria entre el UE y la segunda estación base causada por el cambio de clave de seguridad entre el UE y la primera estación base y reduce un retardo de transmisión de datos innecesario.

En algunas realizaciones de la presente invención, si el mensaje de comando de cambio de clave porta información de indicación que indica que el UE suspende la transmisión de datos entre el UE y la primera estación base, luego de la etapa 203 de la determinación, mediante el UE según el mensaje de comando de cambio de clave, si mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o un eNodoB secundario y/o si mantener la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario, el método de cambio de clave de seguridad proporcionado en esta realización de la presente invención incluye además al menos una de las siguientes etapas:

G1.El UE mantiene las configuraciones de PDCP de todas las RB establecidas entre el UE y la primera estación base.

G2.El UE mantiene las configuraciones de RLC de todas las RB establecidas entre el UE y la primera estación base.

G3.El UE mantiene las configuraciones de MAC de todas las RB establecidas entre el UE y la primera estación base.

G4.El UE mantiene un estado activo de una SCell activada entre el UE y la primera estación base.

G5.El UE mantiene un C-RNTI utilizado para la comunicación entre el UE y la primera estación base.

G6.El UE suspende la transmisión de datos entre el UE y la primera estación base.

La información de indicación incluida en el mensaje de comando de cambio de clave indica que el UE suspende la transmisión de datos entre el UE y la primera estación base. En este caso, durante la ejecución de al menos uno de la etapa G1 a la etapa G6, uno o más de la etapa G1 a la etapa G6 pueden ejecutarse según un requerimiento específico. La información de configuración de estrato de acceso entre el UE y la primera estación base se mantiene y el UE suspende la transmisión de datos entre el UE y la primera estación base; por lo tanto, la reconfiguración de la información de configuración de estrato de acceso entre el UE y la primera estación base puede evitarse.

En algunas realizaciones de la presente invención, si el mensaje de comando de cambio de clave porta información de indicación que indica que el UE detiene la transmisión de datos entre el UE y la primera estación base, luego de la etapa 203 de la determinación, mediante el UE según el mensaje de comando de cambio de clave, si mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o un eNodoB secundario y/o si mantener la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario, el método de cambio de clave de seguridad proporcionado en esta realización de la presente invención incluye además al menos una de las siguientes etapas:

H1.El UE reconfigura las configuraciones de PDCP de todas las RB establecidas entre el UE y la primera estación base.

H2. El UE reconfigura las configuraciones de RLC de todas las RB establecidas entre el UE y la primera estación base.

H3. El UE reconfigura las configuraciones de MAC de todas las RB establecidas entre el UE y la primera estación base.

H4. El UE detiene la transmisión de datos entre el UE y la primera estación base.

La información de indicación incluida en el mensaje de comando de cambio de clave indica que el UE detiene la transmisión de datos entre el UE y la primera estación base. En este caso, este indica que el cambio de clave de seguridad debe realizarse entre el UE y la primera estación base. En este caso, durante la ejecución de al menos uno de la etapa H1 a la etapa H4, uno o más de la etapa H1 a la etapa H4 pueden ejecutarse según un requerimiento específico. La información de configuración de estrato de acceso entre el UE y la primera estación base está reconfigurada y el UE detiene la transmisión de datos entre el UE y la primera estación base; por lo tanto, una falla de la transmisión de datos entre el UE y la primera estación base puede evitarse.

204. El UE envía un mensaje de cambio de clave completado al eNodoB maestro de manera que la primera estación base determina que se complete el cambio de clave de seguridad entre el UE y la primera estación base.

En esta realización de la presente invención, luego de que el UE completa el cambio de clave de seguridad entre el UE y la primera estación base, el UE envía el mensaje de cambio de clave completado al eNodoB maestro y el eNodoB maestro puede recibir el mensaje de cambio de clave completado enviado por el UE. Luego de que el eNodoB maestro recibe el mensaje de cambio de clave completado enviado por el UE, la primera estación base puede determinar, al utilizar el mensaje de cambio de clave completado recibido por el eNodoB maestro, que se complete el cambio de clave de seguridad entre el UE y la primera estación base. La primera estación base puede utilizar una nueva clave de seguridad para continuar realizando la transmisión de datos con el UE. Debería apreciarse que puede descubrirse de las descripciones anteriores que la primera estación base puede referirse al eNodoB maestro o puede referirse al eNodoB secundario o puede referirse al eNodoB maestro y el eNodoB secundario; por lo tanto, luego de obtener una retroalimentación desde el UE de que se completó el cambio de clave de seguridad, una estación base que debe realizar el cambio de clave de seguridad con el UE debe instruirse para continuar realizando la transmisión de datos con el UE. El cambio de clave de seguridad entre el eNodoB maestro y el UE no afecta la transmisión de datos entre el eNodoB secundario y el UE; asimismo, el cambio de clave de seguridad entre el eNodoB secundario y el UE no afecta la transmisión de datos entre el eNodoB maestro y el UE.

Se puede aprender de las descripciones anteriores en esta realización de la presente invención que: un eNodoB maestro envía un mensaje de comando de cambio de clave a un UE, y el UE realiza, según el mensaje de comando de cambio de clave, un cambio de clave de seguridad entre el UE y una primera estación base, y determina, según el mensaje de comando de cambio de clave, si mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o un eNodoB secundario y/o si mantener la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario; luego de que el UE completa el cambio de clave de seguridad, el UE envía un mensaje de cambio de clave completado al eNodoB maestro, el eNodoB maestro puede recibir el mensaje de cambio de clave completado enviado por el UE, la primera estación base puede determinar, al utilizar el eNodoB maestro,

que se complete el cambio de clave de seguridad entre el UE y la primera estación base, y la primera estación base y el UE pueden utilizar una nueva clave de seguridad para realizar la transmisión de datos. Por lo tanto, según esta realización de la presente invención, puede implementarse un cambio de clave de seguridad cuando un UE lleva a cabo la comunicación de conectividad dual con un MeNB y un SeNB.

Para una mejor comprensión e implementación de las soluciones anteriores en las realizaciones de la presente invención, se proporcionan descripciones específicas más adelante mediante el uso de escenarios de aplicación correspondientes como ejemplos.

En un escenario de aplicación de la presente invención, con referencia a la Figura 3-a, la Figura 3-a es un diagrama de flujo esquemático de una interacción entre un eNodoB maestro, un eNodoB secundario y un UE según una realización de la presente invención, que puede incluir específicamente las siguientes etapas:

S01. El MeNB determina que debe realizarse un cambio de clave de seguridad, y deben realizarse tanto la actualización de clave como la regeneración de clave.

Específicamente, cuando el MeNB recibe un comando de indicación de clave, desde una MME, que requiere realizar la regeneración de clave, el MeNB determina que debe realizarse la regeneración de clave. Cuando el MeNB determina que debe realizarse la actualización de clave, por ejemplo, cuando determina que un valor de conteo PDCP actual del UE está a punto de ajustarse automáticamente, el MeNB determina que debe realizarse la actualización de clave.

S02. Cuando el MeNB determina que debe realizarse la regeneración de clave, el MeNB puede enviar un mensaje de indicación de cambio de clave al SeNB para ordenar al SeNB a realizar el cambio de clave de seguridad.

Específicamente, el MeNB puede agregar, al mensaje de indicación de cambio de clave, una o más claves intermedias del lado del eNodoB secundario generadas en función de una nueva clave intermedia del lado del eNodoB maestro del MeNB, y una frecuencia/frecuencias e información de PCI de una o más células del SeNB o un parámetro de seguridad específico del SeNB, por ejemplo, un valor de conteo PDCP. La o las células del SeNB son una célula/células asociadas con la generación de una clave de seguridad del SeNB y la o las claves intermedias del lado del eNodoB secundario se utilizan para generar una clave de cifrado de plano de usuario en un lado del SeNB.

S03. El MeNB envía un mensaje de comando HO intracelular al UE de manera que el UE realiza un proceso de cambio de clave de seguridad según el mensaje de comando HO intracelular.

Específicamente, cuando debe realizarse la regeneración de clave, un indicador de cambio de clave en el mensaje de comando HO intracelular se fija en verdadero; de lo contrario, cuando se debe realizar la actualización de clave, el indicador de cambio de clave en el mensaje de comando HO intracelular se fija en falso. Si se debe realizar la regeneración de clave, el mensaje de comando HO intracelular puede incluir además información de célula actualizada, asociada con una clave de seguridad, en el lado del SeNB o un parámetro de seguridad actualizado de la estación base, asociada con una clave de seguridad, en el lado del SeNB.

S04. Luego de que el UE recibe el mensaje de comando de traspaso intracelular enviado por el MeNB, el UE realiza el cambio de clave de seguridad y determina, según un indicador de cambio de clave en el mensaje de comando HO intracelular, si mantener la información de configuración de estrato de acceso entre el UE y el SeNB y/o si mantener la transmisión de datos entre el UE y el SeNB.

Específicamente, al determinar, según el indicador en el mensaje de comando HO intracelular, que debe realizarse la actualización de clave o el indicador de cambio de clave está en falso, el UE debe realizar una o más de las siguientes operaciones:

(1) mantener las configuraciones de PDCP de todas las RB establecidas entre el UE y el SeNB;

(2) mantener las configuraciones de RLC de todas las RB establecidas entre el UE y el SeNB;

(3) mantener las configuraciones de MAC de todas las RB establecidas entre el UE y el SeNB;

(4) mantener un estado activo de una SCell activada entre el UE y el SeNB;

(5) mantener un C-RNTI utilizado para la comunicación entre el UE y el SeNB;

(6) mantener/suspender la transmisión de datos entre el UE y el SeNB; y

(7) realizar un proceso de actualización de clave entre el UE y el MeNB. Específicamente, realizar la actualización de clave entre el UE y el MeNB es actualizar una clave intermedia del lado del UE que corresponde al MeNB al utilizar un valor de un conteo de encadenamiento de siguiente salto indicado en el mensaje de comando HO intracelular y se basa en una clave intermedia del lado del UE actual que corresponde al MeNB o un NH, y genera además, al utilizar una clave intermedia del lado del UE que corresponde al MeNB y un algoritmo de seguridad del MeNB, una nueva clave de cifrado y una nueva clave

de protección de integridad que se utilizan para la comunicación con el MeNB.

Si se determina, según el mensaje de comando HO intracelular, que debe realizarse la regeneración de clave, el UE debe realizar una o más de las siguientes operaciones:

(1) Reconfigurar MAC en un lado del MeNB;

(2) Reconfigurar MAC en el lado del SeNB;

(3) Para todas las RB establecidas en un lado del MeNB y el lado del SeNB, reestablecer PDCP de estas RB;

(4) Para todas las RB establecidas en un lado del MeNB y el lado del SeNB, reestablecer RLC de estas RB;

(5) Detener la transmisión de datos entre el UE y el MeNB y entre el UE y el SeNB; y

(6) Actualizar las claves de seguridad para el MeNB y el SeNB según la información de contexto de seguridad en el mensaje de comando HO intracelular. Específicamente, para el MeNB, el UE genera la nueva clave intermedia del lado del UE entre el UE y el MeNB en función de la clave intermedia ASME actualizada, y genera, según la clave intermedia del lado del UE recientemente generada entre el UE y el MeNB y el algoritmo de seguridad del MeNB, la nueva clave de cifrado y la nueva clave de protección de integridad que se utilizan para la comunicación con el MeNB. Además, el UE genera una clave intermedia del lado del UE entre el UE y el lado del SeNB según la nueva clave intermedia del lado del UE entre el UE y el MeNB y la información de célula, asociada con el cambio de clave de seguridad, en el lado del SeNB o el parámetro específico de la estación base, asociado con seguridad, en el lado del SeNB, por ejemplo, el conteo PDCP, y luego el UE genera, en función de la nueva clave intermedia del lado del UE entre el UE y el SeNB y un algoritmo de seguridad del SeNB o el algoritmo de seguridad del MeNB, una nueva clave de cifrado utilizada para la comunicación con el SeNB. La información de célula, asociada con seguridad, del SeNB es información de célula, asociada con seguridad, entre el UE y el SeNB antes del cambio de clave de seguridad o información de célula actualizada, asociada con seguridad y obtenida desde el mensaje de comando HO intracelular, del SeNB. Específicamente, la información de célula incluye un identificador de célula física (en inglés, Physical Cell Identity - PCI) y una frecuencia (en inglés, Frequency).

S05. La MME envía un mensaje de traspaso completado al MeNB. Específicamente, luego de realizar exitosamente acceso aleatorio al MeNB, el UE puede enviar el mensaje de traspaso completado al MeNB; o luego de realizar exitosamente acceso aleatorio al MeNB y el SeNB, el UE puede enviar el mensaje de traspaso completado al MeNB.

Específicamente, cuando el UE determina realizar la actualización de clave, el UE no necesita realizar acceso aleatorio al SeNB. Cuando el UE determina realizar la regeneración de clave, el UE puede realizar acceso aleatorio al MeNB y el SeNB, donde se puede realizar acceso aleatorio al MeNB y al SeNB simultáneamente.

S06. El MeNB envía un mensaje de cambio de clave completado al SeNB.

Específicamente, si se debe realizar la regeneración de clave, cuando el UE no realiza acceso aleatorio al SeNB, el MeNB debe enviar el mensaje de cambio de clave completado al SeNB para notificar al SeNB que el proceso de cambio de clave de seguridad del UE se completó satisfactoriamente, y la transmisión de datos entre el UE y el SeNB puede realizarse al utilizar una nueva clave de seguridad. En el caso de la actualización de clave, si el UE suspende la transmisión de datos con el SeNB, el mensaje de cambio de clave completado enviado por el MeNB al SeNB se utiliza para indicar que la transmisión de datos suspendida entre el UE y el SeNB puede recuperarse.

Debería observarse que en el escenario de aplicación descrito en la Figura 3-a, la generación de la clave intermedia del lado del SeNB por el SeNB depende del MeNB. En este caso, cuando el MeNB realiza la regeneración de clave, el SeNB también debe realizar un cambio de clave de seguridad. En otro escenario de aplicación de la presente invención, con referencia a la Figura 3-b, la Figura 3-b es un diagrama de flujo esquemático de otra interacción entre un eNodoB maestro, un eNodoB secundario y un UE según una realización de la presente invención, que puede incluir específicamente las siguientes etapas:

Etapa S11: El MeNB determina que debe realizarse un cambio de clave de seguridad, y deben realizarse la actualización de clave como la regeneración de clave.

Específicamente, cuando el MeNB recibe un comando de indicación de clave, desde una MME, que requiere realizar la regeneración de clave en un lado del MeNB y/o en un lado del SeNB, el MeNB determina que debe realizarse la regeneración de clave. Cuando el MeNB determina que un valor de conteo PDCP actual del UE en el lado del MeNB está a punto de ajustarse automáticamente, el MeNB puede determinar que el UE debe realizar la actualización de clave para el MeNB. Debería apreciarse que antes de la etapa S11, esta realización de la presente invención puede incluir además la etapa S10: el SeNB envía información de indicación de actualización de clave al MeNB. Luego de que el MeNB recibe información de indicación que es enviada por el SeNB y que indica que un valor de conteo PDCP en el lado del SeNB está a punto de ajustarse automáticamente o información de indicación que es enviada por el

SeNB y que indica que el SeNB debe realizar la actualización de clave, o cuando el MeNB recibe información de indicación que es informada por el SeNB o el UE y que indica que un valor de conteo PDCP actual en el lado del SeNB está a punto de ajustarse automáticamente, el MeNB puede determinar que el UE debe realizar la actualización de clave en claves de seguridad para el MeNB y/o el SeNB.

Etapa S12: Cuando el MeNB recibe una indicación que es enviada por una MME y que requiere realizar la regeneración de clave de una clave de seguridad en un lado del SeNB, el MeNB debe enviar un mensaje de indicación de cambio de clave al SeNB para ordenar al SeNB a realizar un proceso de regeneración de clave.

Etapa S13a: Al determinar que debe realizarse un cambio de clave de seguridad entre el UE y el MeNB, el MeNB envía un mensaje de comando HO intracelular al UE, donde el mensaje de comando HO intracelular incluye información de indicación que indica si el UE realiza la regeneración de clave o la actualización de clave en una clave de seguridad para el MeNB, por ejemplo, al utilizar un indicador de cambio de clave en el mensaje de comando HO intracelular.

Etapa S13b: Al determinar que debe cambiarse la clave de seguridad entre el UE y el SeNB, el MeNB envía un mensaje de comando de cambio de clave al UE, donde el mensaje de comando de cambio de clave incluye información de indicación que indica si el UE realiza la regeneración de clave o la actualización de clave en la clave de seguridad en el lado del SeNB.

Etapa S14. Luego de que el UE recibe el mensaje de comando HO intracelular enviado por el MeNB, si se determina, según el indicador del mensaje de comando HO intracelular, que debe realizarse el cambio de clave de seguridad en un lado del MeNB, el UE debe realizar una o más de las siguientes operaciones:

(1) realizar solamente un proceso de cambio de clave de seguridad entre el UE y el MeNB;

(2) mantener las configuraciones de PDCP de todas las RB establecidas entre el UE y el SeNB;

(3) mantener las configuraciones de RLC de todas las RB establecidas entre el UE y el SeNB;

(4) mantener las configuraciones de MAC de todas las RB establecidas entre el UE y el SeNB;

(5) mantener un estado activo de una SCell activada entre el UE y el SeNB;

(6) mantener un C-RNTI utilizado para la comunicación entre el UE y el SeNB; y

(7) mantener/suspender la transmisión de datos entre el UE y el SeNB.

Si el UE recibe el mensaje de comando de cambio de clave además del mensaje de comando HO intracelular, el UE debe realizar una o más de las siguientes operaciones:

(1) reconfigurar MAC en el lado del SeNB;

(2) reestablecer PDCP para RB establecidas en el SeNB;

(3) reestablecer RLC para RB establecidas en el SeNB;

(4) detener la transmisión de datos entre el UE y el SeNB; y

(5) cambiar, según la información de contexto de seguridad transmitida en el mensaje de comando de cambio de clave y la información de indicación de cambio de clave, la clave de seguridad utilizada para la comunicación con el SeNB. Específicamente, al determinar, según la información de indicación de cambio de clave que debe realizarse la regeneración de clave, el UE actualiza una clave intermedia del lado del UE entre el UE y el SeNB en función de una clave intermedia ASME actualizada entre el UE y el SeNB, y genera, en función de una clave intermedia del lado del UE actualizada entre el UE y el SeNB y un algoritmo de seguridad del SeNB, una nueva clave de cifrado utilizada para la comunicación con el SeNB; al determinar, según la información de indicación de clave, que debe realizarse la actualización de clave, el UE actualiza, en función de una clave intermedia del lado del UE actual que corresponde al SeNB o a un valor NH, una clave intermedia del lado del UE que corresponde al SeNB, y luego genera una nueva clave de cifrado en función de una clave intermedia del lado del UE actualizada que corresponde al SeNB y un algoritmo de seguridad del SeNB.

S15a. El UE envía un mensaje de traspaso completado al MeNB. Esta etapa es una respuesta a la etapa S13a. Específicamente, el UE puede enviar el mensaje de traspaso completado al MeNB luego de realizar exitosamente acceso aleatorio al MeNB; o el UE puede enviar el mensaje de traspaso completado al MeNB luego de realizar exitosamente acceso aleatorio al MeNB y al SeNB.

Específicamente, cuando el UE determina realizar la actualización de clave, el UE no necesita realizar acceso aleatorio al SeNB. Cuando el UE determina realizar la regeneración de clave, el UE puede realizar acceso aleatorio al MeNB y

el SeNB, donde se puede realizar acceso aleatorio al MeNB y el SeNB simultáneamente.

S15b. El UE envía un mensaje de cambio de clave completado al MeNB; esta etapa es una respuesta a la etapa S13b.

S16. El MeNB envía el mensaje de cambio de clave completado al SeNB. Específicamente, si se debe realizar la regeneración de clave, cuando el UE no realiza acceso aleatorio al SeNB, el MeNB debe enviar el mensaje de cambio de clave completado al SeNB para notificar al SeNB que el proceso de cambio de clave de seguridad del UE se completó satisfactoriamente, y la transmisión de datos entre el UE y el SeNB puede realizarse al utilizar una nueva clave de seguridad. En el caso de la actualización de clave, si el UE suspende la transmisión de datos con el SeNB, el mensaje de cambio de clave completado enviado por el MeNB al SeNB se utiliza para indicar que la transmisión de datos suspendida entre el UE y el SeNB puede recuperarse.

En otro escenario de aplicación de la presente invención, con referencia a la Figura 3-c, la Figura 3-c es un diagrama de flujo esquemático de otra interacción entre un eNodoB maestro, un eNodoB secundario y un UE según una realización de la presente invención, que puede incluir específicamente las siguientes etapas:

Etapa S21. El MeNB determina que debe realizarse un cambio de clave de seguridad, y deben realizarse tanto la actualización de clave o la regeneración de clave.

Específicamente, cuando el MeNB recibe un comando de indicación de clave, desde una MME, que requiere realizar la regeneración de clave en un lado del MeNB o un lado del SeNB, el MeNB determina que debe realizarse la regeneración de clave. Cuando el MeNB determina que un valor de conteo PDCP actual del UE en el lado del MeNB está a punto de ajustarse automáticamente, el MeNB puede determinar que el UE debe realizar la actualización de clave para el MeNB. Debería apreciarse que antes de la etapa S21, esta realización de la presente invención puede incluir además la etapa S20: El SeNB envía información de indicación de actualización de clave al MeNB. Luego de que el MeNB recibe información de indicación que es enviada por el SeNB y que indica que un valor de conteo PDCP en el lado del SeNB está a punto de ajustarse automáticamente o información de indicación que es enviada por el SeNB y que indica que el SeNB debe realizar la actualización de clave, o cuando el MeNB recibe información de indicación que es informada por el SeNB o el UE y que indica que un valor de conteo PDCP actual en el lado del SeNB está a punto de ajustarse automáticamente, el MeNB puede determinar que el UE debe realizar la actualización de clave en una clave de seguridad para el SeNB.

S22. Cuando el MeNB determina que debe realizarse la regeneración de clave, el MeNB puede enviar un mensaje de indicación de cambio de clave al SeNB para indicar que el SeNB debe realizar el cambio de clave de seguridad.

Específicamente, si una clave intermedia que corresponde al SeNB se genera en función de una clave intermedia del MeNB, una o más claves intermedias que corresponden al SeNB que son generadas en función de una nueva clave intermedia del MeNB, y una frecuencia/frecuencias e información de PCI de una o más células del SeNB, o un parámetro de seguridad específico del SeNB, por ejemplo, un valor conteo PDCP, pueden transmitirse en la información de indicación de cambio de clave. La o las células del SeNB son una célula/células asociadas con la generación de una clave de seguridad del SeNB y la o las claves intermedias que corresponden al SeNB se utilizan para generar una clave de cifrado de plano de usuario en el lado del SeNB.

Si la clave intermedia que corresponde al SeNB se genera desde una clave intermedia ASME, la información de indicación de cambio de clave porta una nueva clave intermedia que corresponde al SeNB que se genera por la MME para el SeNB.

S23. El MeNB envía un mensaje de comando de cambio de clave al UE de manera que el UE realiza un proceso de cambio de clave de seguridad según el mensaje de comando de cambio de clave.

Específicamente, el mensaje de comando de cambio de clave incluye una primera información de indicación y segunda información de indicación. La primera información de indicación se utiliza para ordenar al UE a cambiar una clave de seguridad entre el UE y el MeNB y la segunda información de indicación se utiliza para ordenar al UE a cambiar una clave de seguridad entre el UE y el SeNB.

Además, la primera información de indicación puede incluir además información de indicación que indica si se debe realizar la regeneración de clave o la actualización de clave, y la segunda información de indicación puede incluir además información de indicación que indica si se debe realizar la regeneración de clave o la actualización de clave.

Especialmente, el mensaje de comando de cambio de clave anterior puede ser un mensaje de comando HO intracelular.

S24. Luego de recibir el mensaje de comando de cambio de clave enviado por el MeNB, el UE determina, según la primera información de indicación y segunda información de indicación en el mensaje de comando de cambio de clave, cómo realizar el proceso de cambio de clave de seguridad.

Específicamente, al determinar, según la indicación del mensaje de comando de cambio de clave, que solamente debe realizarse un cambio de clave de seguridad entre el UE y el MeNB, por ejemplo, cuando la primera información

de indicación está en verdadero y la segunda información de indicación está en falso, el UE debe realizar una o más de las siguientes operaciones:

(1) mantener las configuraciones de PDCP de todas las RB establecidas entre el UE y el SeNB;

(2) mantener las configuraciones de RLC de todas las RB establecidas entre el UE y el SeNB;

(3) mantener las configuraciones de MAC de todas las RB establecidas entre el UE y el SeNB;

(4) mantener un estado activo de una SCell activada entre el UE y el SeNB;

(5) mantener un C-RNTI utilizado para la comunicación entre el UE y el SeNB;

(6) mantener/suspender la transmisión de datos entre el UE y el SeNB; y

(7) realizar un proceso de cambio de clave de seguridad entre el UE y el MeNB. Específicamente, al determinar, según la primera información de indicación (por ejemplo, la primera información de indicación incluye indicación de realizar la actualización de clave) o información de contexto de seguridad transmitida en el mensaje de comando de cambio de clave (por ejemplo, el mensaje de comando de cambio de clave incluye un valor de un conteo de encadenamiento de siguiente salto), que debe realizarse la actualización de clave entre el UE y el MeNB, el UE genera una nueva clave intermedia del lado del MeNB en función de una clave intermedia del lado del MeNB actual o un NH, y utiliza además una clave intermedia del lado del MeNB actualizada y un algoritmo de seguridad del MeNB para generar una nueva clave de cifrado y una nueva clave de protección de integridad que se utilizan para la comunicación con el MeNB. Al determinar, según la primera información de indicación (por ejemplo, la primera información de indicación incluye la indicación de realizar la regeneración de clave otra vez) o información de contexto de seguridad transmitida en el mensaje de comando de cambio de clave (por ejemplo, el mensaje de comando de cambio de clave no incluye un valor de un conteo de encadenamiento de siguiente salto, o el valor está vacío), que debe realizarse un proceso la regeneración de clave entre el UE y el MeNB, el UE genera una nueva clave intermedia del lado del MeNB en función de una clave intermedia ASME nueva entre el UE y el MeNB, y luego utiliza una clave intermedia del lado del MeNB actualizada y un algoritmo de seguridad del MeNB para generar una nueva clave de cifrado y una nueva clave de protección de integridad que se utilizan para la comunicación con el MeNB.

Al determinar, según la indicación del mensaje de comando de cambio de clave, que solamente debe realizarse un cambio de clave de seguridad entre el UE y el SeNB, por ejemplo, cuando la primera información de indicación está en falso y la segunda información de indicación está en verdadero, el UE debe realizar una o más de las siguientes operaciones:

(1) mantener las configuraciones de PDCP, RLC y MAC de todas las RB establecidas entre el UE y el MeNB;

(2) mantener un estado activo de una SCell activada entre el UE y el MeNB;

(3) mantener la comunicación entre el UE y el MeNB;

(4) reconfigurar MAC en el lado del SeNB;

(5) para todas las RB establecidas en un lado del SeNB, reestablecer PDCP de estas RB;

(6) para todas las RB establecidas en un lado del SeNB, reestablecer RLC de estas RB;

(7) detener la transmisión de datos entre el UE y el SeNB; y

(8) realizar un proceso de cambio de clave de seguridad entre el UE y el SeNB. Específicamente, al determinar, según la segunda información de indicación (por ejemplo, la segunda información de indicación incluye indicación de realizar la actualización de clave) o información de contexto de seguridad transmitida en el mensaje de comando de cambio de clave (por ejemplo, el mensaje de comando de cambio de clave incluye un valor de un conteo de encadenamiento de siguiente salto), que debe realizarse la actualización de clave entre el UE y el SeNB, el UE genera una nueva clave intermedia del lado del SeNB en función de una clave intermedia del lado del SeNB actual o un NH, y utiliza además una clave intermedia del lado del SeNB actualizada y un algoritmo de seguridad del SeNB para generar una nueva clave de cifrado para la comunicación con el SeNB. Al determinar, según la segunda información de indicación (por ejemplo, la segunda información de indicación incluye indicación de realizar la regeneración de clave otra vez) o información de contexto de seguridad transmitida en el mensaje de comando de cambio de clave (por ejemplo, el mensaje de comando de cambio de clave no incluye un valor de un conteo de encadenamiento de siguiente salto, o el valor está vacío), que debe realizarse un proceso de regeneración de clave entre el UE y el SeNB, el UE genera una nueva clave intermedia del lado del SeNB en función de una clave intermedia ASME nueva entre el UE y el SeNB, y luego utiliza una clave intermedia del lado del SeNB

actualizada y un algoritmo de seguridad del SeNB para generar una nueva clave de cifrado utilizada para la comunicación con el SeNB.

Al determinar, según la indicación del mensaje de comando de cambio de clave, que deben realizarse procesos de cambio de clave de seguridad entre el UE y el MeNB y entre el UE y el SeNB, por ejemplo, cuando la primera información de indicación y la segunda información de indicación están en verdadero, el UE debe realizar una o más de las siguientes operaciones:

(1) reconfigurar MAC en el lado del MeNB;

(2) reconfigurar MAC en el lado del SeNB;

(3) para todas las RB establecidas en un lado del MeNB y el lado del SeNB, reestablecer PDCP de estas RB;

(4) para todas las RB establecidas en el lado del MeNB y el lado del SeNB, reestablecer RLC de estas RB;

(5) detener la transmisión de datos entre el UE y el MeNB y entre el UE y el SeNB; y

(6) realizar los procesos de cambio de clave de seguridad entre el UE y el MeNB y entre el UE y el SeNB, que es específicamente lo siguiente:

Al determinar, según la primera información de indicación (por ejemplo, la primera información de indicación incluye indicación de realizar la actualización de clave) o información de contexto de seguridad transmitida en el mensaje de comando de cambio de clave (por ejemplo, el mensaje de comando de cambio de clave incluye un valor de Un conteo de encadenamiento de siguiente salto), que debe realizarse la actualización de clave entre el UE y el MeNB, el UE genera una nueva clave intermedia del lado del MeNB en función de una clave intermedia del lado del MeNB actual o un NH, y utiliza además una clave intermedia del lado del MeNB actualizada y un algoritmo de seguridad del MeNB para generar una nueva clave de cifrado y una nueva clave de protección de integridad que se utilizan para la comunicación con el MeNB. Al determinar, según la primera información de indicación (por ejemplo, la primera información de indicación incluye indicación de realizar la regeneración de clave otra vez) o información de contexto de seguridad transmitida en el mensaje de comando de cambio de clave (por ejemplo, el mensaje de comando de cambio de clave no incluye un valor de un conteo de encadenamiento de siguiente salto, o el valor está vacío), que debe realizarse un proceso de regeneración de clave entre el UE y el MeNB, el UE genera una nueva clave intermedia del lado del MeNB en función de una clave intermedia ASME nueva entre el UE y el MeNB, y luego utiliza una clave intermedia del lado del MeNB actualizada y un algoritmo de seguridad del MeNB para generar una nueva clave de cifrado y una nueva clave de protección de integridad para la comunicación con el MeNB.

De forma específica, al determinar, según la segunda información de indicación (por ejemplo, la segunda información de indicación incluye indicación de realizar la actualización de clave) o información de contexto de seguridad transmitida en el mensaje de comando de cambio de clave (por ejemplo, el mensaje de comando de cambio de clave incluye un valor de un conteo de encadenamiento de siguiente salto), que debe realizarse la actualización de clave entre el UE y el SeNB, el UE genera una nueva clave intermedia del lado del SeNB en función de una clave intermedia del lado del SeNB actual o un NH, y utiliza además una clave intermedia del lado del SeNB actualizada y un algoritmo de seguridad del SeNB para generar una nueva clave de cifrado utilizada para la comunicación con el SeNB. Al determinar, según la segunda información de indicación (por ejemplo, la segunda información de indicación incluye indicación de realizar la regeneración de clave otra vez) o información de contexto de seguridad transmitida en el mensaje de comando de cambio de clave (por ejemplo, el mensaje de comando de cambio de clave no incluye un valor de Un conteo de encadenamiento de siguiente salto, o el valor está vacío), que debe realizarse un proceso de regeneración de clave entre el UE y el SeNB, el UE genera una nueva clave intermedia del lado del SeNB en función de una clave intermedia ASME nueva entre el UE y el SeNB, y luego utiliza una clave intermedia del lado del SeNB actualizada y un algoritmo de seguridad del SeNB para generar una nueva clave de cifrado utilizada para la comunicación con el SeNB.

S25. El UE envía un mensaje de cambio de clave completado al MeNB.

Específicamente, según si el MeNB y el SeNB realizan el cambio de clave de seguridad, el UE puede enviar el mensaje de cambio de clave completado al MeNB luego de realizar satisfactoriamente acceso aleatorio al MeNB o al SeNB (si solo se cambia una clave de MeNB o del SeNB); o el UE puede enviar el mensaje de cambio de clave completado al MeNB luego de realizar satisfactoriamente acceso aleatorio al MeNB y al SeNB (las claves de MeNB y del SeNB están cambiadas). Cuando el UE realiza acceso aleatorio al MeNB y al SeNB, los dos procesos de acceso aleatorio pueden realizarse simultáneamente.

Específicamente, el UE puede estar especialmente notificado, en el mensaje de comando de cambio de clave anterior, de si el UE realiza acceso aleatorio al MeNB y/o al SeNB. Es decir, el mensaje de comando de cambio de clave anterior incluye información de indicación que indica si se realiza acceso aleatorio al MeNB y/o al SeNB.

S26. El MeNB envía el mensaje de cambio de clave completado al SeNB. Excepcionalmente, cuando el UE realiza

acceso aleatorio al SeNB, el SeNB puede determinar, luego de determinar que el UE realiza satisfactoriamente un proceso de acceso aleatorio, que se completó el cambio de clave de seguridad. Por lo tanto, en este caso, el MeNB puede no enviar el mensaje de cambio de clave completado al SeNB.

En otro escenario de aplicación de la presente invención, con referencia a la Figura 3-d, la Figura 3-d es un diagrama de flujo esquemático de otra interacción entre un eNodoB maestro, un eNodoB secundario y un UE según una realización de la presente invención, que puede incluir específicamente las siguientes etapas:

S31. El MeNB determina que debe realizarse un cambio de clave de seguridad, y deben realizarse tanto Key-fresh o la regeneración de clave.

Específicamente, cuando el MeNB recibe un comando de indicación de clave, desde una MME, que requiere realizar la regeneración de clave en un lado del MeNB o un lado del SeNB, el MeNB determina que debe realizarse la regeneración de clave. Cuando el MeNB determina que un valor de conteo PDCP actual del UE en el lado del MeNB está a punto de ajustarse automáticamente, el MeNB puede determinar que el UE debe realizar la actualización de clave para el MeNB. Debería apreciarse que antes de la etapa S31, esta realización de la presente invención puede incluir además la etapa S30: El SeNB envía información de indicación de actualización de clave al MeNB. Luego de que el MeNB recibe información de indicación que es enviada por el SeNB y que indica que un valor de conteo PDCP en el lado del SeNB está a punto de ajustarse automáticamente o información de indicación que es enviada por el SeNB y que indica que el SeNB debe realizar la actualización de clave, o cuando el MeNB recibe información de indicación que es informada por el SeNB o el UE y que indica que un valor de conteo PDCP actual en el lado del SeNB está a punto de ajustarse automáticamente, el MeNB puede determinar que el UE debe realizar la actualización de clave en una clave de seguridad para el SeNB.

S32. Cuando el MeNB determina que debe realizarse la regeneración de clave, el MeNB puede enviar un mensaje de indicación de cambio de clave al SeNB para indicar que el SeNB debe realizar el cambio de clave de seguridad.

Específicamente, si una clave intermedia que corresponde al SeNB se genera en función de una clave intermedia del MeNB, una o más claves intermedias que corresponden al SeNB que son generadas en función de una nueva clave intermedia del MeNB, y una frecuencia/frecuencias e información de PCI de una o más células del SeNB, o un parámetro de seguridad específico del SeNB, por ejemplo, un valor de conteo PDCP, pueden transmitirse en la información de indicación de cambio de clave. La o las células del SeNB son una célula/células asociadas con la generación de una clave de seguridad del SeNB y la o las claves intermedias que corresponden al SeNB se utilizan para generar una clave de cifrado de plano de usuario en el lado del SeNB.

Si la clave intermedia que corresponde al SeNB se genera desde una clave intermedia ASME, la información de indicación de cambio de clave porta una nueva clave intermedia que corresponde al SeNB que se genera por la MME para el SeNB.

S33. El MeNB envía un mensaje de comando de cambio de clave al UE de manera que el UE realiza un proceso de cambio de clave de seguridad según el mensaje de comando de cambio de clave.

Específicamente, el mensaje de comando de cambio de clave incluye una primera información de contexto de clave de seguridad y segunda información de contexto de clave de seguridad. La primera información de contexto de clave de seguridad se utiliza para ordenar al UE a cambiar una clave de seguridad entre el UE y el MeNB y la segunda información de contexto de clave de seguridad se utiliza para ordenar al UE a cambiar una clave de seguridad entre el UE y el SeNB.

Especialmente, el mensaje de comando de cambio de clave anterior puede ser un mensaje de comando HO intracelular.

S34. Luego de recibir el mensaje de comando de cambio de clave enviado por el MeNB, el UE determina, según la primera información de contexto de clave de seguridad y segunda información de contexto de clave de seguridad en el mensaje de comando de cambio de clave, cómo realizar el proceso de cambio de clave de seguridad.

Específicamente, si el mensaje de comando de cambio de clave incluye solamente la primera información de contexto de clave de seguridad, el UE determina, según el mensaje de comando de cambio de clave, que se debe realizar solamente un cambio de clave de seguridad entre el UE y el MeNB, y el UE debe realizar una o más de las siguientes operaciones:

(1) mantener las configuraciones de PDCP de todas las RB establecidas entre el UE y el SeNB;

(2) mantener las configuraciones de RLC de todas las RB establecidas entre el UE y el SeNB;

(3) mantener las configuraciones de MAC de todas las RB establecidas entre el UE y el SeNB;

(4) mantener un estado activo de una SCell activada entre el UE y el SeNB;

(5) mantener un C-RNTI utilizado para la comunicación entre el UE y el SeNB;

(6) mantener/suspender la transmisión de datos entre el UE y el SeNB; y

(7) realizar un proceso de cambio de clave de seguridad entre el UE y el MeNB. Específicamente, al determinar, según la primera información de contexto de clave de seguridad (por ejemplo, la primera información de contexto de clave de seguridad incluye un valor de Un conteo de encadenamiento de siguiente salto), que debe realizarse la actualización de clave entre el UE y el MeNB, el UE genera una nueva clave intermedia del lado del MeNB en función de una clave intermedia del lado del MeNB actual o un NH, y utiliza además una clave intermedia del lado del MeNB actualizada y un algoritmo de seguridad del MeNB para generar una nueva clave de cifrado y una nueva clave de protección de integridad que se utilizan para la comunicación con el MeNB. Al determinar, según la primera información de contexto de clave e seguridad (por ejemplo, la primera información de contexto de clave de seguridad incluye indicación de realizar la regeneración de clave), que debe realizarse la regeneración de clave entre el UE y el MeNB, el UE genera una nueva clave intermedia del lado del MeNB en función de una nueva clave intermedia ASME nueva entre el UE y el MeNB, y luego utiliza una clave intermedia del lado del MeNB actualizada y un algoritmo de seguridad del MeNB para generar una nueva clave de cifrado y una nueva clave de protección de integridad que se utilizan para la comunicación con el MeNB.

Si el mensaje de comando de cambio de clave incluye solamente la segunda información de contexto de clave de seguridad, el UE determina, según el mensaje de comando de cambio de clave, que solamente debe realizarse un cambio de clave de seguridad entre el UE y el SeNB, y el UE debe realizar una o más de las siguientes operaciones:

(1) mantener las configuraciones de PDCP, RLC y MAC de todas las RB establecidas entre el UE y el MeNB;

(2) mantener un estado activo de una SCell activada entre el UE y el MeNB;

(3) mantener la transmisión de datos entre el UE y el MeNB;

(4) reconfigurar MAC en el lado del SeNB;

(5) para todas las RB establecidas en el lado del SeNB, restablecer PDCP de estas RB;

(6) para todas las RB establecidas en el lado del SeNB, restablecer RLC de estas RB;

(7) detener la transmisión de datos entre el UE y el SeNB; y

(8) realizar un proceso de cambio de clave entre el UE y el SeNB.

Específicamente, al determinar, según la segunda información de contexto de clave de seguridad (por ejemplo, la segunda información de contexto de clave de seguridad incluye un valor de Un conteo de encadenamiento de siguiente salto), que debe realizarse la actualización de clave entre el UE y el SeNB, el UE genera una nueva clave intermedia del lado del SeNB en función de una clave intermedia del lado del SeNB actual o un NH, y utiliza además una clave intermedia del lado del SeNB actualizada y un algoritmo de seguridad del SeNB para generar una nueva clave de cifrado que se utiliza para la comunicación con el SeNB. Al determinar, según la segunda información de contexto de clave de seguridad (por ejemplo, la segunda información de contexto de clave de seguridad incluye una indicación para realizar la regeneración de clave otra vez), que debe realizarse un proceso de regeneración de clave entre el UE y el MeNB, el UE genera una nueva clave intermedia del lado del SeNB en función de una nueva clave intermedia ASME entre el UE y el SeNB, y luego utiliza una clave intermedia del lado del SeNB actualizada y un algoritmo de seguridad del SeNB para generar una nueva clave de cifrado utilizada para la comunicación con el SeNB.

Si se determina, según la primera información de contexto de clave de seguridad y la segunda información de contexto de clave de seguridad, que deben realizarse los cambios de clave entre el UE y el MeNB y entre el UE y el SeNB, por ejemplo, cuando el mensaje de comando de cambio de clave incluye la primera información de contexto de clave de seguridad y la segunda información de contexto de clave de seguridad, el UE debe realizar una o más de las siguientes etapas:

(1) reconfigurar MAC en el lado del MeNB;

(2) reconfigurar MAC en el lado del SeNB;

(3) para todas las RB establecidas en un lado del MeNB y el lado del SeNB, reestablecer PDCP de estas RB;

(4) para todas las RB establecidas en el lado del MeNB y el lado del SeNB, reestablecer RLC de estas RB;

(5) detener la transmisión de datos entre el UE y el MeNB y entre el UE y el SeNB; y

(6) realizar los procesos de cambio de clave de seguridad entre el UE y el MeNB y entre el UE y el SeNB, que es específicamente lo siguiente:

Al determinar, según la primera información de contexto de clave de seguridad (por ejemplo, la primera información de contexto de clave de seguridad incluye un valor de Un conteo de encadenamiento de siguiente salto), que debe realizarse la actualización de clave entre el UE y el MeNB, el UE genera una nueva clave intermedia del lado del MeNB en función de una clave intermedia del lado del MeNB actual o un NH, y utiliza además una clave intermedia del lado del MeNB actualizada y un algoritmo de seguridad del MeNB para generar una nueva clave de cifrado y una nueva clave de protección de integridad que se utilizan para la comunicación con el MeNB. Al determinar, según la primera información de contexto de clave de seguridad (por ejemplo, la primera información de contexto de clave de seguridad incluye indicación de realizar la regeneración de clave), que debe realizarse la regeneración de clave entre el UE y el MeNB, el UE genera una nueva clave intermedia del lado del MeNB en función de una nueva clave intermedia ASME nueva entre el UE y el MeNB, y luego utiliza una clave intermedia del lado del MeNB actualizada y un algoritmo de seguridad del MeNB para generar una nueva clave de cifrado y una nueva clave de protección de integridad que se utilizan para la comunicación con el MeNB.

Al determinar, según la segunda información de contexto de clave de seguridad (por ejemplo, la segunda información de contexto de clave de seguridad incluye un valor de Un conteo de encadenamiento de siguiente salto), que debe realizarse la actualización de clave entre el UE y el SeNB, el UE genera una nueva clave intermedia del lado del SeNB en función de una clave intermedia del lado del SeNB actual o un NH, y utiliza además una clave intermedia del lado del SeNB actualizada y un algoritmo de seguridad del SeNB para generar una nueva clave de cifrado que se utiliza para la comunicación con el SeNB. Al determinar, según la segunda información de contexto de clave de seguridad (por ejemplo, la segunda información de contexto de clave de seguridad incluye una indicación de realizar la regeneración de clave otra vez), que debe realizarse un proceso de regeneración de clave entre el UE y el MeNB, el UE genera una nueva clave intermedia del lado del SeNB en función de una nueva clave intermedia ASME nueva entre el UE y el SeNB, y luego utiliza una clave intermedia del lado del SeNB actualizada y un algoritmo de seguridad del SeNB para generar una nueva clave de cifrado que se utiliza para la comunicación con el SeNB.

S35. El UE envía un mensaje de cambio de clave completado al MeNB.

Específicamente, según si el MeNB y el SeNB realizan el cambio de clave de seguridad, el UE puede enviar el mensaje de cambio de clave completado al MeNB luego de realizar satisfactoriamente acceso aleatorio al MeNB o al SeNB (si solo se cambia una clave de MeNB o del SeNB); o el UE puede enviar el mensaje de cambio de clave completado al MeNB luego de realizar satisfactoriamente acceso aleatorio al MeNB y al SeNB (las claves de MeNB y del SeNB están cambiadas). Cuando el UE realiza acceso aleatorio al MeNB y al SeNB, los dos procesos de acceso aleatorio pueden realizarse simultáneamente.

Específicamente, el UE puede estar especialmente notificado, en el mensaje de comando de cambio de clave anterior, de si el UE realiza acceso aleatorio al MeNB y/o al SeNB. Es decir, el mensaje de comando de cambio de clave anterior incluye información de indicación que indica si se realiza acceso aleatorio al MeNB y/o al SeNB.

S36. El MeNB envía el mensaje de cambio de clave completado al SeNB. Excepcionalmente, cuando el UE realiza acceso aleatorio al SeNB, el SeNB puede determinar, luego de determinar que el UE realiza satisfactoriamente un proceso de acceso aleatorio, que se completó el cambio de clave de seguridad. Por lo tanto, en este caso, el MeNB puede no enviar el mensaje de cambio de clave completado al SeNB.

En otro escenario de aplicación de la presente invención, con referencia a la Figura 3-e, la Figura 3-e es un diagrama de flujo esquemático de otra interacción entre un eNodoB maestro, un eNodoB secundario y un UE según una realización de la presente invención, que puede incluir específicamente las siguientes etapas:

S41. El MeNB determina que debe realizarse un cambio de clave de seguridad, y deben realizarse tanto la actualización de clave o la regeneración de clave.

Específicamente, cuando el MeNB recibe un comando de indicación de clave, desde una MME, que requiere realizar la regeneración de clave, el MeNB determina que debe realizarse la regeneración de clave. Cuando el MeNB determina que debe realizarse la actualización de clave, por ejemplo, cuando determina que un valor de conteo PDCP actual del UE está a punto de ajustarse automáticamente, el MeNB determina que debe realizarse la actualización de clave.

S42. Cuando el MeNB determina que debe realizarse la regeneración de clave, el MeNB puede enviar un mensaje de indicación de cambio de clave al SeNB para ordenar al SeNB a realizar el cambio de clave de seguridad. Específicamente, el MeNB puede agregar, al mensaje de indicación de cambio de clave, una o más claves intermedias del lado del eNodoB secundario generadas en función de una nueva clave intermedia del lado del eNodoB maestro del MeNB, y una frecuencia/frecuencias e información de PCI de una o más células del SeNB o un parámetro de seguridad específico del SeNB, por ejemplo, un valor de conteo PDCP. La o las células del SeNB son una célula/células asociadas con la generación de una clave de seguridad del SeNB y la o las claves intermedias del lado del eNodoB secundario se utilizan para generar una clave de cifrado de plano de usuario en un lado del SeNB.

S43. El MeNB envía un mensaje de comando HO intracelular al UE de manera que el UE realiza un proceso de cambio de clave de seguridad según el mensaje de comando HO intracelular. El mensaje de comando HO intracelular incluye información de indicación que indica la transmisión de datos en el lado del SeNB, donde la información de indicación

puede incluir información de indicación que indica mantener la transmisión entre el UE y el SeNB, o información de indicación que indica detener la transmisión de datos entre el UE y el SeNB, o información de indicación que indica suspender la transmisión de datos entre el UE y el SeNB, de manera que el UE determina, según la información de indicación, cómo realizar la transmisión de datos en el lado del SeNB.

S44. Luego de recibir el mensaje de comando de traspaso HO intracelular enviado por el MeNB, el UE determina, según la información de indicación en el comando HO intracelular, cómo manejar la transmisión de datos entre el UE y el SeNB.

Si el MeNB indica que el UE mantiene la transmisión de datos entre el UE y el SeNB, el UE debe realizar una o más de las siguientes operaciones:

(1) mantener las configuraciones de PDCP de todas las RB establecidas entre el UE y el SeNB;

(2) mantener las configuraciones de RLC de todas las RB establecidas entre el UE y el SeNB;

(3) mantener las configuraciones de MAC de todas las RB establecidas entre el UE y el SeNB;

(4) mantener un estado activo de una SCell activada entre el UE y el SeNB;

(5) mantener un C-RNTI utilizado para la comunicación entre el UE y el SeNB;

(6) mantener la transmisión de datos entre el UE y el SeNB; y

(7) realizar un proceso de actualización de clave entre el UE y el MeNB.

Específicamente, realizar la actualización de clave entre el UE y el MeNB es actualizar una clave intermedia del lado del UE que corresponde al MeNB al utilizar un valor de un conteo de encadenamiento de siguiente salto indicado en el mensaje de comando HO intracelular y se basa en una clave intermedia del lado del UE actual que corresponde al MeNB o un NH, y genera además, al utilizar una clave intermedia del lado del UE que corresponde al MeNB y un algoritmo de seguridad del MeNB, una nueva clave de cifrado y una nueva clave de protección de integridad que se utilizan para la comunicación con el MeNB.

Si El MeNB indica que suspende la transmisión de datos entre el UE y el SeNB, el UE debe realizar una o más de las siguientes operaciones:

(1) mantener las configuraciones de PDCP de todas las RB establecidas entre el UE y el SeNB;

(2) mantener las configuraciones de RLC de todas las RB establecidas entre el UE y el SeNB;

(3) mantener las configuraciones de MAC de todas las RB establecidas entre el UE y el SeNB;

(4) mantener un estado activo de una SCell activada entre el UE y el SeNB;

(5) mantener un C-RNTI utilizado para la comunicación entre el UE y el SeNB;

(6) suspender la transmisión de datos entre el UE y el SeNB; y

(7) realizar un proceso de actualización de clave entre el UE y el MeNB. Específicamente, realizar la actualización de clave entre el UE y el MeNB es actualizar una clave intermedia del lado del UE que corresponde al MeNB al utilizar un valor de un conteo de encadenamiento de siguiente salto indicado en el mensaje de comando HO intracelular y se basa en una clave intermedia del lado del UE actual que corresponde al MeNB o un NH, y genera además, al utilizar una clave intermedia del lado del UE que corresponde al MeNB y un algoritmo de seguridad del MeNB, una nueva clave de cifrado y una nueva clave de protección de integridad que se utilizan para la comunicación con el MeNB.

Si el MeNB indica que el UE detiene la transmisión de datos entre el UE y el SeNB, el UE debe realizar una o más de las siguientes operaciones:

(1) reconfigurar MAC en un lado del MeNB y MAC en el lado del SeNB;

(2) restablecer PDCP y RLC para las RB del MeNB y el SeNB;

(3) detener la transmisión de datos entre el UE y el MeNB y entre el UE y el SeNB; y

(4) actualizar las claves de seguridad para el MeNB y el SeNB según la información de contexto de seguridad en el mensaje de comando HO intracelular. Para un proceso específico, referirse a la descripción en la realización anterior.

Puede aprenderse de las descripciones de la presente invención en las realizaciones anteriores que según las

realizaciones de la presente invención, un efecto impuesto por un proceso de cambio de clave de seguridad de un MeNB en la transmisión de datos entre un UE y un SeNB puede reducirse, y se evita que el proceso de cambio de clave de seguridad del MeNB cause restablecimiento innecesario de PDCP y RLC de las RB y reconfiguración de MAC, lo que así asegura la normal transmisión de datos en las RB entre el UE y el SeNB.

Cabe destacar que, a efectos de una breve descripción, las realizaciones del método anterior están representadas como una serie de acciones. Sin embargo, un experto en la técnica debe comprender que la presente invención no se limita al orden de las acciones descrito, dado que, según la presente invención, algunas etapas pueden realizarse en otros órdenes o simultáneamente. Además, un experto en la técnica también comprenderá que las realizaciones descritas en esta memoria descriptiva pertenecen todas a realizaciones ilustrativas y las acciones y módulos implicados no son necesariamente obligatorios respecto a la presente invención.

Para implementar de una mejor manera las soluciones anteriores en las realizaciones de la presente invención, los aparatos relacionados utilizados para implementar las soluciones anteriores se proporcionan además a continuación.

Con respecto a la Figura 4-a, una realización de la presente invención proporciona una estación base 400. La estación base 400 es específicamente un MeNB de eNodoB maestro, que puede incluir un módulo de determinación de cambio de clave 401, un módulo de envío de mensajes 402 y un módulo de recepción de mensajes 403.

El módulo de determinación de cambio de clave 401 está configurado para determinar que se debe realizar un cambio de clave de seguridad entre una primera estación base y el equipo de usuario UE, donde la primera estación base incluye al menos uno del eNodoB maestro y un eNodoB secundario.

El módulo de envío de mensajes 402 está configurado para enviar un mensaje de comando de cambio de clave al UE de manera que el UE realiza, según el mensaje de comando de cambio de clave, el cambio de clave de seguridad entre el UE y la primera estación base, y determina, según el mensaje de comando de cambio de clave, si mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o el eNodoB secundario y/o si mantener la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario.

El módulo de recepción de mensajes 403 está configurado para recibir un mensaje de cambio de clave completado enviado por el UE de manera que la primera estación base determina que se completa el cambio de clave de seguridad entre el UE y la primera estación base.

En algunas realizaciones de la presente invención, si la primera estación base determinada por el eNodoB maestro incluye el eNodoB secundario, el módulo de envío de mensajes 402 está configurado además para: luego de que el módulo de recepción de mensajes recibe el mensaje de cambio de clave completado enviado por el UE, reenvia el mensaje de cambio de clave completado al eNodoB secundario, de manera que el eNodoB secundario determina que se complete el cambio de clave de seguridad entre el UE y el eNodoB secundario.

En algunas realizaciones de la presente invención, el mensaje de comando de cambio de clave porta además información de indicación que indica si el UE realiza acceso aleatorio a la primera estación base.

En algunas realizaciones de la presente invención, si el mensaje de comando de cambio de clave indica que el UE realiza acceso aleatorio a la primera estación base, el módulo de envío de mensajes 402 está específicamente configurado para enviar al UE el mensaje de comando de cambio de clave que incluye información sobre un recurso de acceso aleatorio de manera que el UE realiza acceso aleatorio a la primera estación base según la información sobre el recurso de acceso aleatorio.

Específicamente, en algunas realizaciones de la presente invención, como se muestra en la Figura 4-b, el módulo de determinación de cambio de clave 401 incluye:

un submódulo de recepción de comando 4011, configurado para recibir un comando de indicación de clave enviado por una entidad de gestión de movilidad MME, donde el comando de indicación de clave se utiliza para ordenar que se realice la regeneración de clave entre el eNodoB maestro y el UE y/u ordenar que se realice la regeneración de clave entre el eNodoB secundario y el UE; y

un submódulo de determinación de cambio de clave 4012, configurado para determinar, según el comando de indicación de clave, que la regeneración de clave debe realizarse entre la primera estación base y el UE.

Además, en otras realizaciones de la presente invención, si el eNodoB maestro determina que un modo para realizar el cambio de clave de seguridad entre la primera estación base y el UE es la regeneración de clave, un mensaje de comando de cambio de clave porta la información de célula asociada con el cambio de clave de seguridad del eNodoB secundario o información de estación base asociada con el cambio de clave de seguridad del eNodoB secundario.

En algunas realizaciones de la presente invención, si la primera estación base determinada por el eNodoB maestro incluye el eNodoB secundario, el módulo de envío de mensajes 402 está configurado además para: luego de que el submódulo de determinación de cambio de clave determine, según el comando de indicación de clave, que debe realizarse el cambio de clave de seguridad entre la primera estación base y el UE, enviar un mensaje de indicación

de cambio de clave al eNodoB secundario, donde el mensaje de indicación de cambio de clave se utiliza para ordenar al eNodoB secundario a que realice el cambio de clave de seguridad y el mensaje de indicación de cambio de clave incluye una clave intermedia del lado del eNodoB secundario generada por el eNodoB maestro según una clave intermedia del lado del eNodoB maestro actualizada e información de célula, asociado con el cambio de clave de seguridad del eNodoB secundario o información de estación base, asociado con el cambio de clave de seguridad del eNodoB secundario, o el mensaje de indicación de cambio de clave incluye una clave intermedia del lado del eNodoB secundario generada por la MME para el eNodoB secundario.

En algunas realizaciones de la presente invención, el módulo de determinación de cambio de clave 401 está especialmente configurado para: determinar si un conteo de protocolo de convergencia de datos por paquetes, conteo PDCP, del UE en un lado del eNodoB maestro se ajusta automáticamente dentro de los tiempos preestablecidos, y si el conteo PDCP actual del UE en el lado del eNodoB maestro se ajusta automáticamente dentro de los tiempos preestablecidos, determinar que debe realizarse el cambio de clave de seguridad entre la primera estación base y el UE, y determinar que se va a utilizar un modo de actualización de clave (Key Refresh), donde la primera estación base es el eNodoB maestro; y/o cuando el eNodoB maestro recibe información de indicación que es enviada por el eNodoB secundario y que indica que un conteo PDCP en un lado del eNodoB secundario se ajusta automáticamente dentro de los tiempos preestablecidos, o el eNodoB maestro recibe información de indicación que es enviada por el eNodoB secundario y que indica que el eNodoB secundario debe realizar la actualización de clave, o el eNodoB maestro recibe información de indicación que es informada por el UE y que indica que un conteo PDCP actual en un lado del eNodoB secundario se ajusta automáticamente dentro de los tiempos preestablecidos, determinar que debe realizarse el cambio de clave de seguridad entre la primera estación base y el UE, y determinar que se va a utilizar un modo de actualización de clave, donde la primera estación base es el eNodoB secundario.

En algunas realizaciones de la presente invención, el mensaje de comando de cambio de clave incluye una primera información de indicación y segunda información de indicación, la primera información de indicación se utiliza para indicar que el cambio de clave de seguridad debe realizarse entre el eNodoB maestro y el UE y la segunda información de indicación se utiliza para indicar que el cambio de clave de seguridad debe realizarse entre el eNodoB secundario y el UE.

En algunas realizaciones de la presente invención, la primera información de indicación se utiliza además para indicar que un modo de realizar el cambio de clave de seguridad entre el eNodoB maestro y el UE es la regeneración de clave o la actualización de clave.

La segunda información de indicación se utiliza además para indicar que un modo para realizar el cambio de clave de seguridad entre el eNodoB secundario y el UE es la regeneración de clave o la actualización de clave.

En algunas realizaciones de la presente invención, el mensaje de comando de cambio de clave incluye una primera información de contexto de clave de seguridad y segunda información de contexto de clave de seguridad, donde la primera información de contexto de clave de seguridad se utiliza para indicar que el cambio de clave de seguridad debe realizarse entre el eNodoB maestro y el UE y la segunda información de contexto de clave de seguridad se utiliza para indicar que el cambio de clave de seguridad debe realizarse entre el eNodoB secundario y el UE.

En algunas realizaciones de la presente invención, la primera información de contexto de clave de seguridad se utiliza además para indicar que un modo de realizar el cambio de clave de seguridad entre el eNodoB maestro y el UE es la regeneración de clave o la actualización de clave.

La segunda información de contexto de clave de seguridad se utiliza además para indicar que un modo para realizar el cambio de clave de seguridad entre el eNodoB secundario y el UE es la regeneración de clave o la actualización de clave.

En algunas realizaciones de la presente invención, el mensaje de comando de cambio de clave indica, al utilizar un valor de un campo del indicador de cambio de clave Key Change Indicator, que un modo para realizar el cambio de clave de seguridad entre la primera estación base y el UE es la regeneración de clave o la actualización de clave.

En algunas realizaciones de la presente invención, el mensaje de comando de cambio de clave porta información de indicación que indica que el UE mantiene la transmisión de datos entre el UE y una segunda estación base o indica que el UE suspende la transmisión de datos entre el UE y la primera estación base o indica que el UE detiene la transmisión de datos entre el UE y la primera estación base, donde cuando la segunda estación base es el eNodoB maestro, la primera estación base es el eNodoB secundario o cuando la segunda estación base es el eNodoB secundario, la segunda estación base es el eNodoB maestro.

En algunas realizaciones de la presente invención, el mensaje de comando de cambio de clave es específicamente un mensaje de comando de traspaso HO intracelular.

Puede aprenderse de las descripciones anteriores en esta realización de la presente invención que: un módulo de determinación de cambio de clave determina que debe realizarse un cambio de clave de seguridad entre una primera estación base y un UE, donde la primera estación base incluye al menos uno del eNodoB maestro y un eNodoB secundario; luego de que el eNodoB maestro determina que el cambio de clave de seguridad debe realizarse entre la

primera estación base y el UE, un módulo de envío de mensajes envía un mensaje de comando de cambio de clave al UE, de manera que el UE realiza, según el mensaje de comando de cambio de clave, el cambio de clave de seguridad entre el UE y la primera estación base, y determina, según el mensaje de comando de cambio de clave, si mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o el eNodoB secundario y/o si mantener la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario; y luego de que el UE completa el cambio de clave de seguridad, el UE envía un mensaje de cambio de clave completado al eNodoB maestro, el eNodoB maestro puede recibir el mensaje de cambio de clave completado enviado por el UE de manera que la primera estación base pueda determinar, al utilizar el eNodoB maestro, que se complete el cambio de clave de seguridad entre el UE y la primera estación base, y la primera estación base y el UE pueden usar una nueva clave de seguridad para llevar a cabo la transmisión de datos. Por lo tanto, según esta realización de la presente invención, puede implementarse un cambio de clave de seguridad cuando un UE lleva a cabo la comunicación de conectividad dual con un MeNB y un SeNB.

Con respecto a la Figura 5-a, una realización de la presente invención proporciona UE 500, que puede incluir un módulo de recepción de mensajes 501, un módulo de cambio de clave 502, un módulo de determinación 503 y un módulo de envío de mensajes 504.

El módulo de recepción de mensajes 501 está configurado para recibir un mensaje de comando de cambio de clave enviado por el eNodoB maestro, donde el mensaje de comando de cambio de clave incluye información de indicación de que el eNodoB maestro ordena que se realice un cambio de clave de seguridad entre el UE y una primera estación base, donde la primera estación base incluye al menos uno del eNodoB maestro y un eNodoB secundario.

El módulo de cambio de clave 502 está configurado para llevar a cabo, según el mensaje de comando de cambio de clave, el cambio de clave de seguridad entre el UE y la primera estación base.

El módulo de determinación 503 está configurado para determinar, según el mensaje de comando de cambio de clave, si mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o el eNodoB secundario y/o si mantener la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario.

El módulo de envío de mensajes 504 está configurado para enviar un mensaje de cambio de clave completado al eNodoB maestro, de manera que la primera estación base determina que se complete el cambio de clave de seguridad entre el UE y la primera estación base.

En algunas realizaciones de la presente invención, el mensaje de comando de cambio de clave porta información de indicación que indica si el UE realiza acceso aleatorio a la primera estación base y el módulo de determinación 503 está configurado además para: luego de que el módulo de recepción de mensajes recibe el mensaje de comando de cambio de clave enviado por el eNodoB maestro, determinar, según la información de indicación que es transmitida en el mensaje de comando de cambio de clave y que indica si el UE realiza acceso aleatorio a la primera estación base, si realiza acceso aleatorio a la primera estación base.

En otras realizaciones de la presente invención, si el mensaje de comando de cambio de clave indica que el UE realiza acceso aleatorio a la primera estación base, como se muestra en la Figura 5-b, el UE 500 incluye también un módulo de acceso aleatorio 505.

El módulo de recepción de mensajes 501 está específicamente configurado para recibir un mensaje de comando de cambio de clave que es enviado por el eNodoB maestro y que incluye información sobre un recurso de acceso aleatorio.

El módulo de acceso aleatorio 505 está configurado para realizar acceso aleatorio a la primera estación base según la información sobre el recurso de acceso aleatorio.

En algunas realizaciones de la presente invención, si la información de indicación incluida en el mensaje de comando de cambio de clave recibida por el UE incluye una primera información de indicación y segunda información de indicación, donde la primera información de indicación se utiliza para indicar que el cambio de clave de seguridad debe realizarse entre el eNodoB maestro y el UE y la segunda información de indicación se utiliza para indicar que el cambio de clave de seguridad debe realizarse entre el eNodoB secundario y el UE, el módulo de cambio de clave 502 está configurado además para determinar, según la primera información de indicación y/o la segunda información de indicación, que la primera estación base se encuentra en una de las siguientes tres condiciones: la primera estación base es el eNodoB maestro, la primera estación base es el eNodoB secundario y la primera estación base es el eNodoB maestro y el eNodoB secundario.

En algunas realizaciones de la presente invención, la primera información de indicación se utiliza además para indicar que un modo para realizar el cambio de clave de seguridad entre el eNodoB maestro y el UE es la regeneración de clave o la actualización de clave y el módulo de cambio de clave 502 está específicamente configurado para realizar, según la primera información de indicación, el cambio de clave de seguridad entre el UE y el eNodoB maestro en el modo de regeneración de clave o actualización de clave.

La segunda información de indicación se utiliza además para indicar que un modo para realizar el cambio de clave de

seguridad entre el eNodoB secundario y el UE es la regeneración de clave o la actualización de clave y el módulo de cambio de clave 502 está específicamente configurado para realizar, según la segunda información de indicación, el cambio de clave de seguridad entre el UE y el eNodoB secundario en el modo de regeneración de clave o actualización de clave.

En algunas realizaciones de la presente invención, si el mensaje de comando de cambio de clave recibido por el UE incluye una primera información de contexto de clave de seguridad y segunda información de contexto de clave de seguridad, donde la primera información de contexto de clave de seguridad se utiliza para indicar que el cambio de clave de seguridad debe realizarse entre el eNodoB maestro y el UE y la segunda información de contexto de clave de seguridad se utiliza para indicar que el cambio de clave de seguridad debe realizarse entre el eNodoB secundario y el UE, el módulo de cambio de clave 502 está configurado además para determinar, según la primera información de contexto de clave de seguridad y/o la segunda información de contexto de clave de seguridad, que la primera estación base se encuentra en una de las siguientes tres condiciones: la primera estación base es el eNodoB maestro, la primera estación base es el eNodoB secundario y la primera estación base es el eNodoB maestro y el eNodoB secundario.

En algunas realizaciones de la presente invención, la primera información de contexto de clave de seguridad se utiliza además para indicar que un modo para realizar el cambio de clave de seguridad entre el eNodoB maestro y el UE es la regeneración de clave o la actualización de clave y el módulo de cambio de clave 502 está específicamente configurado para realizar, según la primera información de contexto de clave de seguridad, el cambio de clave de seguridad entre el UE y el eNodoB maestro en el modo de regeneración de clave o actualización de clave.

La segunda información de contexto de clave de seguridad se utiliza además para indicar que un modo para realizar el cambio de clave de seguridad entre el eNodoB secundario y el UE es la regeneración de clave o la actualización de clave y el módulo de cambio de clave está específicamente configurado para realizar, según la segunda información de contexto de clave de seguridad, el cambio de clave de seguridad entre el UE y el eNodoB secundario en el modo de regeneración de clave o actualización de clave.

En algunas realizaciones de la presente invención, si la información de indicación incluida en el mensaje de comando de cambio de clave es un campo del indicador de cambio de clave Key Change Indicator, el módulo de cambio de clave 502 está específicamente configurado para determinar, al utilizar un valor del campo del indicador de cambio de clave, la realización del cambio de clave de seguridad entre el UE y la primera estación base en un modo de regeneración de clave o actualización de clave.

En algunas realizaciones de la presente invención, el módulo de determinación 503 está específicamente configurado para:

determinar, según la primera información de indicación y segunda información de indicación que están incluidas en el mensaje de comando de cambio de clave, si mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o el eNodoB secundario, donde la primera información de indicación se utiliza para indicar que el cambio de clave de seguridad debe realizarse entre el eNodoB maestro y el UE y la segunda información de indicación se utiliza para indicar que el cambio de clave de seguridad debe realizarse entre el eNodoB secundario y el UE;

o

determinar, según la primera información de contexto de clave de seguridad y segunda información de contexto de clave de seguridad que están incluidas en el mensaje de comando de cambio de clave, si mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o el eNodoB secundario, donde la primera información de contexto de clave de seguridad se utiliza para indicar que el cambio de clave de seguridad debe realizarse entre el eNodoB maestro y el UE y la segunda información de contexto de clave de seguridad se utiliza para indicar que el cambio de clave de seguridad debe realizarse entre el eNodoB secundario y el UE;

o

determinar, según un campo del indicador de cambio de clave Key Change Indicator incluida en el mensaje de comando de cambio de clave, si mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o el eNodoB secundario;

o

determinar, según la información de indicación que está incluida en el mensaje de comando de cambio de clave y que indica que el UE mantiene la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario, si mantiene la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario.

En algunas realizaciones de la presente invención, el módulo de determinación 503 está específicamente configurado para:

al determinar, según el campo del indicador de cambio de clave, que se debe realizar la regeneración de clave, determinar no mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o el eNodoB secundario;

o

al determinar, según el campo del indicador de cambio de clave, que se debe realizar la actualización de clave en función de una clave intermedia del lado de UE que corresponde al eNodoB maestro, determinar mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o el eNodoB secundario;

o

al determinar, según el campo del indicador de cambio de clave, que se debe realizar la actualización de clave en función de un siguiente salto NH, determinar mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o el eNodoB secundario.

En algunas realizaciones de la presente invención, el módulo de determinación 503 está específicamente configurado para:

determinar, según la primera información de indicación y la segunda información de indicación que están incluidas en el mensaje de comando de cambio de clave, si mantener la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario, donde la primera información de indicación se utiliza para indicar que el cambio de clave de seguridad debe realizarse entre el eNodoB maestro y el UE y la segunda información de indicación se utiliza para indicar que el cambio de clave de seguridad debe realizarse entre el eNodoB secundario y el UE;

o

determinar, según la primera información de contexto de clave de seguridad y la segunda información de contexto de clave de seguridad que están incluidas en el mensaje de comando de cambio de clave, si mantener la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario, donde la primera información de contexto de clave de seguridad se utiliza para indicar que el cambio de clave de seguridad debe realizarse entre el eNodoB maestro y el UE y la segunda información de contexto de clave de seguridad se utiliza para indicar que el cambio de clave de seguridad debe realizarse entre el eNodoB secundario y el UE;

o

determinar, según el campo del indicador de cambio de clave incluida en el mensaje de comando de cambio de clave, si mantener la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario;

o

determinar, según la información de indicación que está incluida en el mensaje de comando de cambio de clave y que indica que el UE mantiene la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario, si mantener la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario.

En algunas realizaciones de la presente invención, el módulo de determinación 503 está específicamente configurado para:

al determinar, según el campo del indicador de cambio de clave, que se debe realizar la regeneración de clave, determinar no mantener la transmisión de datos entre el UE y el eNodoB maestro o entre el UE y el eNodoB secundario; o

al determinar, según el campo del indicador de cambio de clave, que se debe realizar la actualización de clave en función de una clave intermedia del lado de UE que corresponde al eNodoB maestro, determinar mantener la transmisión de datos entre el UE y el eNodoB secundario;

o

al determinar, según el campo del indicador de cambio de clave, que se debe realizar la actualización de clave en función de un NH, determinar mantener la transmisión de datos entre el UE y el eNodoB secundario.

En algunas realizaciones de la presente invención, cuando el UE determina, según la información de comando de cambio de clave, que la información de configuración de estrato de acceso entre el UE y el eNodoB maestro debe mantenerse, y/o que la transmisión de datos entre el UE y el eNodoB maestro debe mantenerse, el módulo de determinación 503 está específicamente configurado para determinar al menos uno de las siguientes:

mantener, mediante el UE, configuraciones de protocolo de convergencia de datos por paquetes PDCP de todas las portadoras de radio RB establecidas entre el UE y el eNodoB maestro;

mantener, mediante el UE, configuraciones de Control de Enlace de Radio RLC de todas las RB establecidas entre el

UE y el eNodoB maestro;

mantener, mediante el UE, configuraciones de Control de Acceso al Medio MAC de todos las RB establecidas entre el UE y el eNodoB maestro;

mantener, mediante el UE, un estado activo de una célula secundaria, SCell, activada entre el UE y el eNodoB maestro;

mantener, mediante el UE, un identificador temporal de red de radio celular, C-RNTI, utilizado para la comunicación entre el UE y el eNodoB maestro; y

mantener o suspender, mediante el UE, la transmisión de datos entre el UE y el eNodoB maestro.

En algunas realizaciones de la presente invención, cuando el UE determina, según la información de comando de cambio de clave, que la información de configuración de estrato de acceso entre el UE y el eNodoB secundario debe mantenerse, y/o que la transmisión de datos entre el UE y el eNodoB secundario debe mantenerse, al mantener la información de configuración de estrato de acceso entre el UE y el eNodoB secundario y/o al mantener la transmisión de datos entre el UE y el eNodoB secundario, el módulo de determinación 503 está específicamente configurado para determinar al menos uno de los siguientes:

mantener, mediante el UE, configuraciones de PDCP de todas las RB establecidas entre el UE y el eNodoB secundario;

mantener, mediante el UE, configuraciones de RLC todas las RB establecidas entre el UE y el eNodoB secundario;

mantener, mediante el UE, configuraciones de MAC de todas las RB establecidas entre el UE y el eNodoB secundario;

mantener, mediante el UE, un estado activo de una SCell activada entre el UE y el eNodoB secundario;

mantener, mediante el UE, un C-RNTI utilizado para la comunicación entre el UE y el eNodoB secundario; y

mantener o suspender, mediante el UE, la transmisión de datos entre el UE y el eNodoB secundario.

En algunas realizaciones de la presente invención, el módulo de cambio de clave 502 está específicamente configurado para: cuando la primera estación base es el eNodoB maestro, si el UE determina, según el mensaje de comando de cambio de clave, que el modo para realizar el cambio de seguridad entre el eNodoB maestro y el UE es la actualización de clave, realizar el cambio de clave de seguridad entre el UE y el eNodoB maestro en el modo de actualización de clave.

Luego de que el módulo de determinación 503 determina, según el mensaje de comando de cambio de clave, si mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o el eNodoB secundario y/o si mantener la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario, en comparación con el UE 500 que se muestra en la Figura 5-a, el UE 500 que se muestra en la Figura 5-c incluye además al menos uno de los siguientes módulos:

un módulo de mantenimiento de PDCP 506, configurado para mantener las configuraciones de protocolo de convergencia de datos por paquetes PDCP de todas las portadoras de radio RB establecidas entre el UE y el eNodoB secundario;

un módulo de mantenimiento de RLC 507, configurado para mantener las configuraciones del Control de Enlace de Radio RLC de todas las RB establecidas entre el UE y el eNodoB secundario;

un módulo de mantenimiento de MAC 508, configurado para mantener las configuraciones de Control de Acceso al Medio MAC de todas las RB establecidas entre el UE y el eNodoB secundario;

un módulo de mantenimiento de activación 509, configurado para mantener el estado activo de la célula secundaria, SCell, activada entre el UE y el eNodoB secundario;

un módulo de mantenimiento de C-RNTI 510, configurado para mantener el identificador temporal de red de radio celular, C-RNTI, utilizado para la comunicación entre el UE y el eNodoB secundario; y

un primer módulo de control de transmisión 511, configurado para mantener o suspender la transmisión de datos entre el UE y el eNodoB secundario.

En algunas realizaciones de la presente invención, como se muestra en la Figura 5-d, el módulo de cambio de clave 502 incluye:

un primer submódulo de actualización de clave intermedia 5021, configurado para actualizar, en función de un valor de un conteo de encadenamiento de siguiente salto (Next Hop Chaining Count) indicado por el mensaje de comando de cambio de clave y mediante el uso de una clave intermedia del lado del UE actual que corresponde al eNodoB

maestro o un siguiente salto NH, la clave intermedia del lado del UE que corresponde al eNodoB maestro; y

un primer submódulo de cambio de clave 5022, configurado para generar, al utilizar una clave intermedia del lado del UE actualizada que corresponde al eNodoB maestro y un algoritmo de seguridad del eNodoB maestro, una nueva clave de seguridad que corresponde al eNodoB maestro, donde la nueva clave de seguridad que corresponde al eNodoB maestro incluye: una clave de cifrado y una clave de protección de integridad que se utilizan para la comunicación entre el UE y el eNodoB maestro.

En algunas realizaciones de la presente invención, el módulo de determinación 503 está configurado además para: luego de determinar, según el mensaje de comando de cambio de clave, si mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o el eNodoB secundario y/o si mantener la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario, determinar que la realización del cambio de clave de seguridad entre el UE y el eNodoB maestro y en el modo de actualización de clave, está basada en la clave intermedia del lado del UE actual que corresponde al eNodoB maestro.

En algunas realizaciones de la presente invención, el módulo de cambio de clave 502 está específicamente configurado para determinar, según la primera información de indicación o la primera información de contexto de clave de seguridad o información de contexto de seguridad que es transmitida en el mensaje de comando de cambio de clave, que el modo para realizar el cambio de clave de seguridad entre el eNodoB maestro y el UE es la actualización de clave.

En algunas realizaciones de la presente invención, el módulo de cambio de clave 502 está específicamente configurado para: cuando la primera estación base es el eNodoB maestro, si el UE determina, según el mensaje de comando de cambio de clave, que el modo para realizar el cambio de seguridad entre el eNodoB maestro y el UE es la regeneración de clave, realizar el cambio de clave de seguridad entre el UE y el eNodoB maestro en el modo de regeneración de clave.

En algunas realizaciones de la presente invención, luego de que el módulo de determinación determina, según el mensaje de comando de cambio de clave, si mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o el eNodoB secundario y/o si mantener la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario, en comparación con el UE 500 que se muestra en la Figura 5-a, el UE 500 que se muestra en la Figura 5-e incluye además al menos uno de los siguientes módulos:

un módulo de reconfiguración de PDCP 512 configurado para: reconfigurar las configuraciones de PDCP de todas las RB establecidas entre el UE y el eNodoB maestro y reconfigurar las configuraciones de PDCP de todas las RB establecidas entre el UE y el eNodoB secundario;

un módulo de reconfiguración de RLC 513 configurado para: reconfigurar las configuraciones de RLC de todas las RB establecidas entre el UE y el eNodoB maestro y reconfigurar las configuraciones de RLC de todas las RB establecidas entre el UE y el eNodoB secundario;

un módulo de reconfiguración de MAC 514, configurado para: reconfigurar las configuraciones de MAC de todas las RB establecidas entre el UE y el eNodoB maestro y reconfigurar las configuraciones de MAC de todas las RB establecidas entre el UE y el eNodoB secundario; y

un segundo módulo de control de transmisión 515, configurado para: detener la transmisión de datos entre el UE y el eNodoB maestro y detener la transmisión de datos entre el UE y el eNodoB secundario.

En algunas realizaciones de la presente invención, el módulo de cambio de clave 502 incluye:

un segundo submódulo de actualización de clave intermedia, configurado para actualizar una clave intermedia del lado del UE entre el UE y el eNodoB maestro en función de una clave intermedia de entidad de gestión de seguridad de acceso actualizada ASME; y

un primer submódulo de cambio de clave, configurado para generar, según una clave intermedia del lado del UE actualizada que corresponde al eNodoB maestro y un algoritmo de seguridad del eNodoB maestro, una nueva clave de seguridad que corresponde al eNodoB maestro, donde la nueva clave de seguridad que corresponde al eNodoB maestro incluye: una clave de cifrado y una clave de protección de integridad que se utilizan para la comunicación entre el UE y el eNodoB maestro.

En algunas realizaciones de la presente invención, el módulo de cambio de clave incluye, además:

un tercer submódulo de actualización de clave intermedia, configurado para: luego de que el segundo submódulo de actualización de clave intermedia actualiza la clave intermedia del lado del UE que corresponde al eNodoB maestro en función de la clave intermedia de entidad de gestión de seguridad de acceso ASME, actualizar, según la clave intermedia del lado del eNodoB maestro actualizada e información de célula, asociado con el cambio de clave de seguridad, del eNodoB secundario o información de estación base, asociado con el cambio de clave de seguridad del eNodoB secundario, una clave intermedia del lado del UE que corresponde al eNodoB secundario; y

un submódulo de cambio de clave, configurado para generar, según una clave intermedia del lado del UE actualizada que corresponde al eNodoB secundario y un algoritmo de seguridad del eNodoB secundario, una nueva clave de seguridad que corresponde al eNodoB secundario, donde la nueva clave de seguridad que corresponde al eNodoB secundario incluye una clave de cifrado utilizada para la comunicación entre el UE y el eNodoB secundario.

En algunas realizaciones de la presente invención, el módulo de cambio de clave 502 está específicamente configurado para determinar, según la primera información de indicación o la primera información de contexto de clave de seguridad o información de contexto de seguridad que es transmitida en el mensaje de comando de cambio de clave, que el modo para realizar el cambio de clave de seguridad entre el eNodoB maestro y el UE es la regeneración de clave.

En algunas realizaciones de la presente invención, si el mensaje de comando de cambio de clave porta información de indicación que indica que el UE mantiene la transmisión de datos entre el UE y la segunda estación base, luego de que el módulo de determinación determina, según el mensaje de comando de cambio de clave, si mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o el eNodoB secundario y/o si mantener la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario, el UE incluye además al menos uno de los siguientes módulos:

un módulo de mantenimiento de PDCP, configurado para mantener las configuraciones de PDCP de todas las RB establecidas entre el UE y la segunda estación base;

un módulo de mantenimiento de RLC, configurado para mantener las configuraciones de RLC de todas las RB establecidas entre el UE y la segunda estación base;

un módulo de mantenimiento de MAC, configurado para mantener las configuraciones de MAC de todas las RB establecidas entre el UE y la segunda estación base;

un módulo de mantenimiento de activación, configurado para mantener un estado activo de una SCell activada entre el UE y la segunda estación base;

un módulo de mantenimiento de C-RNTI, configurado para mantener un C-RNTI utilizado para la comunicación entre el UE y la segunda estación base; y

un módulo de mantenimiento de transmisión, configurado para mantener la transmisión de datos entre el UE y la segunda estación base.

En algunas realizaciones de la presente invención, si el mensaje de comando de cambio de clave porta información de indicación que indica que el UE suspende la transmisión de datos entre el UE y la primera estación base, luego de que el módulo de determinación determina, según el mensaje de comando de cambio de clave, si mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o el eNodoB secundario y/o si mantener la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario, el UE incluye además al menos uno de los siguientes módulos:

un módulo de mantenimiento de PDCP, configurado para mantener las configuraciones de PDCP de todas las RB establecidas entre el UE y la primera estación base;

un módulo de mantenimiento de RLC, configurado para mantener las configuraciones de RLC de todas las RB establecidas entre el UE y la primera estación base;

un módulo de mantenimiento de MAC, configurado para mantener las configuraciones de MAC de todas las RB establecidas entre el UE y la primera estación base;

un módulo de mantenimiento de activación, configurado para mantener un estado activo de una SCell activada entre el UE y la primera estación base;

un módulo de mantenimiento de C-RNTI, configurado para mantener un C-RNTI utilizado para la comunicación entre el UE y la primera estación base; y

un módulo de suspensión de transmisión, configurado para suspender la transmisión de datos entre el UE y la primera estación base.

En algunas realizaciones de la presente invención, si el mensaje de comando de cambio de clave porta información de indicación que indica que el UE detiene la transmisión de datos entre el UE y la primera estación base, luego de que el módulo de determinación determina, según el mensaje de comando de cambio de clave, si mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o el eNodoB secundario y/o si mantener la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario, el UE incluye además al menos uno de los siguientes módulos:

un módulo de reconfiguración de PDCP, configurado para reconfigurar las configuraciones de PDCP de todas las RB

establecidas entre el UE y la primera estación base;

un módulo de reconfiguración de RLC, configurado para reconfigurar las configuraciones de RLC de todas las RB establecidas entre el UE y la primera estación base;

un módulo de reconfiguración de MAC, configurado para reconfigurar las configuraciones de MAC de todas las RB establecidas entre el UE y la primera estación base; y

un módulo de detención de transmisión, configurado para detener la transmisión de datos entre el UE y la primera estación base.

Se puede aprender de las descripciones anteriores en esta realización de la presente invención que: un eNodoB maestro envía un mensaje de comando de cambio de clave a un UE, un módulo de cambio de clave realiza, según el mensaje de comando de cambio de clave, un cambio de clave de seguridad entre el UE y una primera estación base, y un módulo de determinación determina, según el mensaje de comando de cambio de clave, si mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o un eNodoB secundario y/o si mantener la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario; luego de que el UE completa el cambio de clave de seguridad, un módulo de envío de mensajes envía un mensaje de cambio de clave completado al eNodoB maestro, el eNodoB maestro puede recibir el mensaje de cambio de clave completado enviado por el UE, la primera estación base puede determinar, al utilizar el eNodoB maestro, que se complete el cambio de clave de seguridad entre el UE y la primera estación base, y la primera estación base y el UE pueden utilizar una nueva clave de seguridad para realizar la transmisión de datos. Por lo tanto, según esta realización de la presente invención, puede implementarse un cambio de clave de seguridad cuando un UE lleva a cabo la comunicación de conectividad dual con un MeNB y un SeNB.

Una realización de la presente invención proporciona además un medio de almacenamiento por computadora, donde el medio de almacenamiento por computadora almacena un programa y el programa realiza algunas o todas las etapas registradas en las realizaciones del método anterior.

Lo siguiente describe otra estación base proporcionada en una realización de la presente invención, y la estación base específicamente se refiere a un eNodoB maestro. Como se muestra en la Figura 6, la estación base 600 incluye:

un aparato de entrada 601, un aparato de salida 602, un procesador 603 y una memoria 604 (puede haber uno o más procesadores 603 en la estación base 600 y un procesador se utiliza como ejemplo en la Figura 6). En algunas realizaciones de la presente invención, el aparato de entrada 601, el aparato de salida 602, el procesador 603 y la memoria 604 pueden conectarse al utilizar un bus o de otro modo; en la Figura 6, la conexión mediante el uso de un bus se utiliza como ejemplo.

El procesador 603 está configurado para realizar las siguientes etapas:

determinar que se debe realizar un cambio de clave de seguridad entre una primera estación base y el equipo de usuario UE, donde la primera estación base incluye al menos uno del eNodoB maestro y un eNodoB secundario;

enviar un mensaje de comando de cambio de clave al UE de manera que el UE realiza, según el mensaje de comando de cambio de clave, el cambio de clave de seguridad entre el UE y la primera estación base, y determina, según el mensaje de comando de cambio de clave, si mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o el eNodoB secundario y/o si mantener la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario; y

recibir un mensaje de cambio de clave completado enviado por el UE de manera que la primera estación base determina que se completa el cambio de clave de seguridad entre el UE y la primera estación base.

En algunas realizaciones de la presente invención, el procesador 603 está configurado además para realizar la siguiente etapa: si la primera estación base determinada por el eNodoB maestro incluye el eNodoB secundario, luego de recibir el mensaje de cambio de clave completado enviado por el UE, reenvía el mensaje de cambio de clave completado al eNodoB secundario, de manera que el eNodoB secundario determina que se complete el cambio de clave de seguridad entre el UE y el eNodoB secundario.

En otras realizaciones de la presente invención, el mensaje de comando de cambio de clave almacenado en la memoria 604 porta información de indicación que indica si el UE realiza acceso aleatorio a la primera estación base.

En algunas realizaciones de la presente invención, si el mensaje de comando de cambio de clave indica que el UE realiza acceso aleatorio a la primera estación base, el procesador 603 está configurado además para realizar la siguiente etapa: enviar al UE el mensaje de comando de cambio de clave que incluye información sobre un recurso de acceso aleatorio de manera que el UE realiza acceso aleatorio a la primera estación base según la información sobre el recurso de acceso aleatorio.

En algunas realizaciones de la presente invención, el procesador 603 está configurado para realizar las siguientes etapas: determinar que un cambio de clave de seguridad debe realizarse entre una primera estación base y el equipo

de usuario UE puede incluir:

recibir un comando de indicación de clave enviado por una entidad de gestión de movilidad MME, donde el comando de indicación de clave se utiliza para ordenar que se realice la regeneración de clave (Key Re-key) entre el eNodoB maestro y el UE y/u ordenar que se realice la regeneración de clave entre el eNodoB secundario y el UE; y

determinar, según el comando de indicación de clave, que debe realizarse la regeneración de clave entre la primera estación base y el UE.

En otras realizaciones de la presente invención, si el eNodoB maestro determina que la regeneración de clave debe realizarse entre la primera estación base y el UE, el mensaje de comando de cambio de clave almacenado en la memoria 604 porta la información de célula, asociada con el cambio de clave de seguridad, del eNodoB secundario o información de estación base, asociada con el cambio de clave de seguridad, del eNodoB secundario.

En algunas realizaciones de la presente invención, el procesador 603 está específicamente configurado para realizar la siguiente etapa: si la primera estación base determinada por el eNodoB maestro incluye el eNodoB secundario, luego de determinar que debe realizarse el cambio de clave de seguridad entre la primera estación base y el equipo de usuario UE, enviar un mensaje de indicación de cambio de clave al eNodoB secundario, donde el mensaje de indicación de cambio de clave se utiliza para ordenar al eNodoB secundario a que realice el cambio de clave de seguridad y el mensaje de indicación de cambio de clave incluye una clave intermedia del lado del eNodoB secundario generada por el eNodoB maestro según una clave intermedia del lado del eNodoB maestro actualizada e información de célula, asociado con el cambio de clave de seguridad del eNodoB secundario o información de estación base, asociado con el cambio de clave de seguridad del eNodoB secundario, o el mensaje de indicación de cambio de clave incluye una clave intermedia del lado del eNodoB secundario generada por la MME para el eNodoB secundario.

En algunas realizaciones de la presente invención, el procesador 603 está configurado para realizar las siguientes etapas:

determinar si un conteo del protocolo de convergencia de datos por paquete, conteo PDCP, actual del UE en un eNodoB maestro se ajusta automáticamente dentro de los tiempos preestablecidos, y si el conteo PDCP del UE en el eNodoB maestro se ajusta automáticamente dentro de los tiempos preestablecidos, determinar que el cambio de clave de seguridad debe realizarse entre la primera estación base y el UE, y determinar que se utilizará un modo actualización de clave (Key Refresh), donde la primera estación base es el eNodoB maestro;

y/o

cuando el eNodoB maestro recibe información de indicación que es enviada por el eNodoB secundario y que indica que un conteo PDCP en un eNodoB secundario se ajusta automáticamente dentro de los tiempos preestablecidos, o el eNodoB maestro recibe información de indicación que es enviada por el eNodoB secundario y que indica que el eNodoB secundario debe realizar la actualización de clave, o el eNodoB maestro recibe información de indicación que es informada por el UE y que indica que un conteo PDCP actual en un lado del eNodoB secundario se ajusta automáticamente dentro de los tiempos preestablecidos, determinar que debe realizarse el cambio de clave de seguridad entre la primera estación base y el UE y determinar que se va a utilizar un modo de actualización de clave, donde la primera estación base es el eNodoB secundario.

En algunas realizaciones de la presente invención, el mensaje de comando de cambio de clave almacenado en la memoria 604 incluye una primera información de indicación y segunda información de indicación, la primera información de indicación se utiliza para indicar que el cambio de clave de seguridad debe realizarse entre el eNodoB maestro y el UE y la segunda información de indicación se utiliza para indicar que el cambio de clave de seguridad debe realizarse entre el eNodoB secundario y el UE.

En algunas realizaciones de la presente invención, la primera información de indicación almacenada en la memoria 604 se utiliza además para indicar que un modo para realizar el cambio de clave de seguridad entre el eNodoB maestro y el UE es la regeneración de clave o la actualización de clave.

La segunda información de indicación se utiliza además para indicar que un modo para realizar el cambio de clave de seguridad entre el eNodoB secundario y el UE es la regeneración de clave o la actualización de clave.

En algunas realizaciones de la presente invención, el mensaje de comando de cambio de clave almacenado en la memoria 604 incluye una primera información de contexto de clave de seguridad y segunda información de contexto de clave de seguridad, la primera información de contexto de clave de seguridad se utiliza para indicar que el cambio de clave de seguridad debe realizarse entre el eNodoB maestro y el UE y la segunda información de contexto de clave de seguridad se utiliza para indicar que el cambio de clave de seguridad debe realizarse entre el eNodoB secundario y el UE.

En algunas realizaciones de la presente invención, la primera información de contexto de clave de seguridad almacenada en la memoria 604 se utiliza además para indicar que un modo para realizar el cambio de clave de seguridad entre el eNodoB maestro y el UE es la regeneración de clave o la actualización de clave; la segunda

información de contexto de clave de seguridad se utiliza además para indicar que un modo para realizar el cambio de clave de seguridad entre el eNodoB secundario y el UE es la regeneración de clave o la actualización de clave.

En algunas realizaciones de la presente invención, el mensaje de comando de cambio de clave almacenado en la memoria 604 indica, al utilizar un valor de un campo del indicador de cambio de clave Key Change Indicator, que un modo para realizar el cambio de clave de seguridad entre la primera estación base y el UE es la regeneración de clave o la actualización de clave.

En algunas realizaciones de la presente invención, el mensaje de comando de cambio de clave almacenado en la memoria 604 porta información de indicación que indica que el UE mantiene la transmisión de datos entre el UE y una segunda estación base o indica que el UE suspende la transmisión de datos entre el UE y la primera estación base o indica que el UE detiene la transmisión de datos entre el UE y la primera estación base, donde cuando la segunda estación base es el eNodoB maestro, la primera estación base es el eNodoB secundario o cuando la segunda estación base es el eNodoB secundario, la segunda estación base es el eNodoB maestro.

En algunas realizaciones de la presente invención, el mensaje de comando de cambio de clave almacenado en la memoria 604 es específicamente un mensaje de comando de traspaso HO intracelular.

Puede aprenderse de las descripciones anteriores en esta realización de la presente invención que: un eNodoB maestro determina que debe realizarse un cambio de clave de seguridad entre una primera estación base y un UE, donde la primera estación base incluye al menos uno del eNodoB maestro y un eNodoB secundario; luego de que el eNodoB maestro determina que el cambio de clave de seguridad debe realizarse entre la primera estación base y el UE, el eNodoB maestro envía un mensaje de comando de cambio de clave al UE de manera que el UE realiza, según el mensaje de comando de cambio de clave, el cambio de clave de seguridad entre el UE y la primera estación base, y determina, según el mensaje de comando de cambio de clave, si mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o el eNodoB secundario y/o si mantener la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario; y luego de que el UE completa el cambio de clave de seguridad, el UE envía un mensaje de cambio de clave completado al eNodoB maestro, el eNodoB maestro puede recibir el mensaje de cambio de clave completado enviado por el UE de manera que la primera estación base pueda determinar, al utilizar el eNodoB maestro, que se complete el cambio de clave de seguridad entre el UE y la primera estación base, y la primera estación base y el UE pueden usar una nueva clave de seguridad para llevar a cabo la transmisión de datos. Por lo tanto, según esta realización de la presente invención, puede implementarse un cambio de clave de seguridad cuando un UE lleva a cabo la comunicación de conectividad dual con un MeNB y un SeNB.

Lo siguiente describe otro UE proporcionado en una realización de la presente invención y como se muestra en la Figura 7, el UE 700 incluye:

un aparato de entrada 701, un aparato de salida 702, un procesador 703 y una memoria 704 (puede haber uno o más procesadores 703 en el UE 700 y un procesador se utiliza como un ejemplo en la Figura 7). En algunas realizaciones de la presente invención, el aparato de entrada 701, el aparato de salida 702, el procesador 703 y la memoria 704 pueden conectarse al utilizar un bus o de otro modo; en la Figura 7, la conexión mediante el uso de un bus se utiliza como ejemplo.

El procesador 703 está configurado para realizar las siguientes etapas:

recibir un mensaje de comando de cambio de clave enviado por un eNodoB maestro, donde el mensaje de comando de cambio de clave incluye información de indicación de que el eNodoB maestro ordena que se realice un cambio de clave de seguridad entre el UE y una primera estación base, donde la primera estación base incluye al menos uno del eNodoB maestro y un eNodoB secundario;

realizar, según el mensaje de comando de cambio de clave, el cambio de clave de seguridad entre el UE y la primera estación base;

determinar, según el mensaje de comando de cambio de clave, si mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o el eNodoB secundario y/o si mantener la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario; y

enviar un mensaje de cambio de clave completado al eNodoB maestro de manera que la primera estación base determina que se complete el cambio de clave de seguridad entre el UE y la primera estación base.

En algunas realizaciones de la presente invención, el mensaje de comando de cambio de clave porta información de indicación que indica si el UE realiza acceso aleatorio a la primera estación base y el procesador 703 está configurado además para realizar la siguiente etapa: luego de recibir el mensaje de comando de cambio de clave enviado por el eNodoB maestro, determinar, según la información de indicación que es transmitida en el mensaje de comando de cambio de clave y que indica si el UE realiza acceso aleatorio a la primera estación base, si realizar acceso aleatorio a la primera estación base.

En algunas realizaciones de la presente invención, si el mensaje de comando de cambio de clave indica que el UE

realiza acceso aleatorio a la primera estación base, el procesador 703 está configurado para realizar la siguiente etapa: recibir un mensaje de comando de cambio de clave que es enviado por el eNodoB maestro y que incluye información sobre un recurso de acceso aleatorio y realiza acceso aleatorio a la primera estación base según la información sobre el recurso de acceso aleatorio.

En algunas realizaciones de la presente invención, el procesador 703 está configurado para realizar la siguiente etapa: si la información de indicación incluida en el mensaje de comando de cambio de clave recibido por el UE incluye una primera información de indicación y segunda información de indicación, donde la primera información de indicación se utiliza para indicar que el cambio de clave de seguridad debe realizarse entre el eNodoB maestro y el UE y la segunda información de indicación se utiliza para indicar que el cambio de clave de seguridad debe realizarse entre el eNodoB secundario y el UE, determinar, según la primera información de indicación y/o la segunda información de indicación, que la primera estación base se encuentra en una de las siguientes tres condiciones: la primera estación base es el eNodoB maestro, la primera estación base es el eNodoB secundario y la primera estación base es el eNodoB maestro y el eNodoB secundario.

En algunas realizaciones de la presente invención, la primera información de indicación se utiliza además para indicar que un modo para realizar el cambio de clave de seguridad entre el eNodoB maestro y el UE es la regeneración de clave o la actualización de clave y el procesador 703 está configurado para realizar la siguiente etapa: realizar, según la primera información de indicación, el cambio de clave de seguridad entre el UE y el eNodoB maestro en el modo de regeneración de clave o actualización de clave.

En algunas realizaciones de la presente invención, la segunda información de indicación se utiliza además para indicar que un modo para realizar el cambio de clave de seguridad entre el eNodoB secundario y el UE es la regeneración de clave o la actualización de clave y el procesador 703 está configurado para realizar la siguiente etapa: la realización, mediante el UE según el mensaje de comando de cambio de clave, del cambio de clave de seguridad entre el UE y la primera estación base es específicamente: realizar, según la segunda información de indicación, el cambio de clave de seguridad entre el UE y el eNodoB secundario en el modo de regeneración de clave o actualización de clave.

En otras realizaciones de la presente invención, el procesador 703 está configurado para realizar la siguiente etapa: si la información de indicación incluida en el mensaje de comando de cambio de clave recibido por el UE incluye una primera información de contexto de clave de seguridad y segunda información de contexto de clave de seguridad, donde la primera información de contexto de clave de seguridad se utiliza para indicar que el cambio de clave de seguridad debe realizarse entre el eNodoB maestro y el UE y la segunda información de contexto de clave de seguridad se utiliza para indicar que el cambio de clave de seguridad debe realizarse entre el eNodoB secundario y el UE, determinar, según la primera información de contexto de clave de seguridad y/o la segunda información de contexto de clave de seguridad, que la primera estación base se encuentra en una de las siguientes tres condiciones: la primera estación base es el eNodoB maestro, la primera estación base es el eNodoB secundario y la primera estación base es el eNodoB maestro y el eNodoB secundario.

En algunas realizaciones de la presente invención, la primera información de contexto de clave de seguridad se utiliza además para indicar que un modo para realizar el cambio de clave de seguridad entre el eNodoB maestro y el UE es la regeneración de clave o la actualización de clave, y el procesador 703 está configurado para realizar la siguiente etapa: realizar, mediante el UE según el mensaje de comando de cambio de clave, el cambio de clave de seguridad entre el UE y la primera estación base es específicamente: realizar, según la primera información de contexto de clave de seguridad, el cambio de clave de seguridad entre el UE y el eNodoB maestro en el modo de regeneración de clave o actualización de clave.

En algunas realizaciones de la presente invención, la segunda información de contexto de clave de seguridad se utiliza además para indicar que un modo para realizar el cambio de clave de seguridad entre el eNodoB secundario y el UE es la regeneración de clave o la actualización de clave y el procesador 703 está configurado para realizar la siguiente etapa: la realización, mediante el UE según el mensaje de comando de cambio de clave, del cambio de clave de seguridad entre el UE y la primera estación base es específicamente: realizar, según la segunda información de contexto de clave de seguridad, el cambio de clave de seguridad entre el UE y el eNodoB secundario en el modo de regeneración de clave o actualización de clave.

En algunas realizaciones de la presente invención, si la información de indicación incluida en el mensaje de comando de cambio de clave es un campo del indicador de cambio de clave Key Change Indicator, el procesador 703 está configurado para realizar la siguiente etapa: la realización, mediante el UE según el mensaje de comando de cambio de clave, del cambio de clave de seguridad entre el UE y la primera estación base es específicamente: determinar, al utilizar el valor del campo del indicador de cambio de clave, la realización del cambio de clave de seguridad entre el UE y la primera estación base en un modo de regeneración de clave o actualización de clave.

En algunas realizaciones de la presente invención, el procesador 703 está configurado para realizar la siguiente etapa:

determinar, según la primera información de indicación y la segunda información de indicación que están incluidas

en el mensaje de comando de cambio de clave, si mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o el eNodoB secundario, donde la primera información de indicación se utiliza para indicar que el cambio de clave de seguridad debe realizarse entre el eNodoB maestro y el UE y la segunda información de indicación se utiliza para indicar que el cambio de clave de seguridad debe realizarse entre el eNodoB secundario y el UE;

o

determinar, según la primera información de contexto de clave de seguridad y segunda información de contexto de clave de seguridad que están incluidas en el mensaje de comando de cambio de clave, si mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o el eNodoB secundario, donde la primera información de contexto de clave de seguridad se utiliza para indicar que el cambio de clave de seguridad debe realizarse entre el eNodoB maestro y el UE y la segunda información de contexto de clave de seguridad se utiliza para indicar que el cambio de clave de seguridad debe realizarse entre el eNodoB secundario y el UE;

o

determinar, según un campo del indicador de cambio de clave Key Change Indicator incluida en el mensaje de comando de cambio de clave, si mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o el eNodoB secundario;

o

determinar, según la información de indicación que está incluida en el mensaje de comando de cambio de clave y que indica que el UE mantiene la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario, si mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o el eNodoB secundario.

En algunas realizaciones de la presente invención, el procesador 703 está configurado para realizar la siguiente etapa:

al determinar, según el campo del indicador de cambio de clave, que se debe realizar la regeneración de clave, determinar no mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o el eNodoB secundario;

o

al determinar, según el campo del indicador de cambio de clave, que se debe realizar la actualización de clave en función de una clave intermedia del lado de UE que corresponde al eNodoB maestro, determinar mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o el eNodoB secundario;

o

al determinar, según el campo del indicador de cambio de clave, que se debe realizar la actualización de clave en función de un siguiente salto NH, determinar mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o el eNodoB secundario.

En algunas realizaciones de la presente invención, el procesador 703 está configurado para realizar la siguiente etapa:

determinar, según la primera información de indicación y la segunda información de indicación que están incluidas en el mensaje de comando de cambio de clave, si mantener la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario, donde la primera información de indicación se utiliza para indicar que el cambio de clave de seguridad debe realizarse entre el eNodoB maestro y el UE y la segunda información de indicación se utiliza para indicar que el cambio de clave de seguridad debe realizarse entre el eNodoB secundario y el UE;

o

determinar, según la primera información de contexto de clave de seguridad y la segunda información de contexto de clave de seguridad que están incluidas en el mensaje de comando de cambio de clave, si mantener la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario, donde la primera información de contexto de clave de seguridad se utiliza para indicar que el cambio de clave de seguridad debe realizarse entre el eNodoB maestro y el UE y la segunda información de contexto de clave de seguridad se utiliza para indicar que el cambio de clave de seguridad debe realizarse entre el eNodoB secundario y el UE;

o

determinar, según el campo del indicador de cambio de clave incluida en el mensaje de comando de cambio de clave, si mantener la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario;

o

determinar, según la información de indicación que está incluida en el mensaje de comando de cambio de clave y que indica que el UE mantiene la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario, si mantener la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario.

En algunas realizaciones de la presente invención, el procesador 703 está configurado para realizar la siguiente etapa:

al determinar, según el campo del indicador de cambio de clave, que debe realizarse la regeneración de clave, determinar no mantener la transmisión de datos entre el UE y el eNodoB maestro o entre el UE y el eNodoB secundario; o

al determinar, según el campo del indicador de cambio de clave, que se debe realizar la actualización de clave en función de una clave intermedia del lado de UE que corresponde al eNodoB maestro, determinar mantener la transmisión de datos entre el UE y el eNodoB secundario;

o

al determinar, según el campo del indicador de cambio de clave, que se debe realizar la actualización de clave en función de un NH, determinar mantener la información de configuración de estrato de acceso entre el UE y el eNodoB secundario.

En algunas realizaciones de la presente invención, cuando el UE determina, según la información de comando de cambio de clave, que la información de configuración de estrato de acceso entre el UE y el eNodoB maestro debe mantenerse, y/o que la transmisión de datos entre el UE y el eNodoB maestro debe mantenerse, el procesador 703 está configurado para realizar las siguientes etapas:

mantener las configuraciones del protocolo de convergencia de datos por paquetes PDCP de todas las portadoras de radio RB establecidas entre el UE y el eNodoB maestro;

mantener las configuraciones de Control de Enlace de Radio RLC de todas las RB establecidas entre el UE y el eNodoB maestro;

mantener las configuraciones de Control de Acceso al Medio MAC de todas las RB establecidas entre el UE y el eNodoB maestro;

mantener un estado activo de una célula secundaria, SCell, activada entre el UE y el eNodoB maestro;

mantener un identificador temporal de red de radio celular C-RNTI, utilizado para la comunicación entre el UE y el eNodoB maestro; y

mantener o suspender la transmisión de datos entre el UE y el eNodoB maestro.

En algunas realizaciones de la presente invención, cuando el UE determina, según la información de comando de cambio de clave, que la información de configuración de estrato de acceso entre el UE y el eNodoB secundario debe mantenerse, y/o que la transmisión de datos entre el UE y el eNodoB secundario debe mantenerse, el procesador 703 está configurado para realizar las siguientes etapas: mantener la información de configuración de estrato de acceso entre el UE y el eNodoB secundario y/o mantener la transmisión de datos entre el UE y el eNodoB secundario incluye al menos una de las siguientes etapas:

mantener las configuraciones de PDCP de todas las RB establecidas entre el UE y el eNodoB secundario;

mantener las configuraciones de RLC de todas las RB establecidas entre el UE y el eNodoB secundario;

mantener las configuraciones de MAC de todas las RB establecidas entre el UE y el eNodoB secundario;

mantener un estado activo de una SCell activada entre el UE y el eNodoB secundario;

mantener un C-RNTI utilizado para la comunicación entre el UE y el eNodoB secundario; y mantener o suspender la transmisión de datos entre el UE y el eNodoB secundario.

En algunas realizaciones de la presente invención, el procesador 703 está configurado para realizar la siguiente etapa: la realización, mediante el UE según el mensaje de comando de cambio de clave, del cambio de clave de seguridad entre el UE y la primera estación base específicamente incluye:

cuando la primera estación base es el eNodoB maestro, si el UE determina, según el mensaje de comando de cambio de clave, que un modo para realizar el cambio de clave de seguridad entre el eNodoB maestro y el UE es la actualización de clave, se realiza el cambio de clave de seguridad entre el UE y el eNodoB maestro en el modo de actualización de clave.

Luego de determinar, según el mensaje de comando de cambio de clave, si mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o el eNodoB secundario y/o si mantener la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario, el procesador 703 está configurado para realizar al menos una de las siguientes etapas:

mantener las configuraciones del protocolo de convergencia de datos por paquetes PDCP de todas las portadoras de radio RB establecidas entre el UE y el eNodoB secundario;

mantener las configuraciones de Control de Enlace de Radio RLC de todas las RB establecidas entre el UE y el eNodoB secundario;

mantener las configuraciones de Control de Acceso al Medio MAC de todas las RB establecidas entre el UE y el eNodoB secundario;

mantener el estado activo de la célula secundaria, SCell, activada entre el UE y el eNodoB secundario;

mantener un identificador temporal de red de radio celular C-RNTI, utilizado para la comunicación entre el UE y el eNodoB secundario; y

mantener o suspender la transmisión de datos entre el UE y el eNodoB secundario.

En algunas realizaciones de la presente invención, el procesador 703 está configurado para realizar las siguientes etapas:

actualizar, en función de un valor de un conteo de encadenamiento de siguiente salto (Next Hop Chaining Count) indicado por el mensaje de comando de cambio de clave y mediante el uso de una clave intermedia del lado del UE actual que corresponde al eNodoB maestro o un siguiente salto NH, la clave intermedia del lado del UE que corresponde al eNodoB maestro; y

generar, al utilizar una clave intermedia del lado del UE actualizada que corresponde al eNodoB maestro y un algoritmo de seguridad del eNodoB maestro, una nueva clave de seguridad que corresponde al eNodoB maestro, donde la nueva clave de seguridad que corresponde al eNodoB maestro incluye: una clave de cifrado y una clave de protección de integridad que se utilizan para la comunicación entre el UE y el eNodoB maestro.

En algunas realizaciones de la presente invención, el procesador 703 está configurado para realizar la siguiente etapa: antes de que el UE determine, según el mensaje de comando de cambio de clave, si mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o el eNodoB secundario y/o si mantener la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario, determinar que la realización del cambio de clave de seguridad entre el UE y el eNodoB maestro en el modo de actualización de clave está basada en la clave intermedia del lado del UE actual que corresponde al eNodoB maestro.

En algunas realizaciones de la presente invención, el procesador 703 está configurado para realizar la siguiente etapa:

determinar, según la primera información de indicación o la primera información de contexto de clave de seguridad o información de contexto de seguridad que es transmitida en el mensaje de comando de cambio de clave, que el modo para realizar el cambio de clave de seguridad entre el eNodoB maestro y el UE es la actualización de clave.

En algunas realizaciones de la presente invención, el procesador 703 está configurado para realizar la siguiente etapa: cuando la primera estación base es el eNodoB maestro, si el UE determina, según el mensaje de comando de cambio de clave, que el modo para realizar el cambio de seguridad entre el eNodoB maestro y el UE es la regeneración de clave, realizar el cambio de clave de seguridad entre el UE y el eNodoB maestro en el modo de regeneración de clave.

Luego de determinar, según el mensaje de comando de cambio de clave, si mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o el eNodoB secundario y/o si mantener la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario, el procesador 703 está configurado además para realizar al menos una de las siguientes etapas:

reconfigurar las configuraciones de PDCP de todas las RB establecidas entre el UE y el eNodoB maestro;

reconfigurar las configuraciones de PDCP de todas las RB establecidas entre el UE y el eNodoB secundario;

reconfigurar las configuraciones de RLC de todas las RB establecidas entre el UE y el eNodoB maestro;

reconfigurar las configuraciones de RLC de todas las RB establecidas entre el UE y el eNodoB secundario;

reconfigurar las configuraciones de MAC de todas las RB establecidas entre el UE y el eNodoB maestro;

reconfigurar las configuraciones de MAC de todas las RB establecidas entre el UE y el eNodoB secundario;

detener la transmisión de datos entre el UE y el eNodoB maestro; y detener la transmisión de datos entre el UE y el

eNodoB secundario.

En algunas realizaciones de la presente invención, el procesador 703 está configurado para realizar las siguientes etapas: la realización, mediante el UE, del cambio de clave de seguridad entre el UE y el eNodoB maestro en el modo de regeneración de clave específicamente incluye:

actualizar una clave intermedia del lado del UE entre el UE y el eNodoB maestro en función de una clave intermedia de entidad de gestión de seguridad de acceso actualizada ASME; y

generar, según una clave intermedia del lado del UE actualizada que corresponde al eNodoB maestro y un algoritmo de seguridad del eNodoB maestro, una nueva clave de seguridad que corresponde al eNodoB maestro, donde la nueva clave de seguridad que corresponde al eNodoB maestro incluye: una clave de cifrado y una clave de protección de integridad que se utilizan para la comunicación entre el UE y el eNodoB maestro.

En algunas realizaciones de la presente invención, el procesador 703 está configurado además para realizar las siguientes etapas: luego de que el UE actualiza la clave intermedia del lado del UE que corresponde al eNodoB maestro en función de una clave intermedia de entidad de gestión de seguridad de acceso ASME, actualiza, según la clave intermedia del lado del eNodoB maestro actualizada e información de célula, asociado con el cambio de clave de seguridad, del eNodoB secundario o información de estación base, asociado con el cambio de clave de seguridad del eNodoB secundario, una clave intermedia del lado del UE que corresponde al eNodoB secundario; y

genera, según una clave intermedia del lado del UE actualizada que corresponde al eNodoB secundario y un algoritmo de seguridad del eNodoB secundario, una nueva clave de seguridad que corresponde al eNodoB secundario, donde la nueva clave de seguridad que corresponde al eNodoB secundario incluye una clave de cifrado utilizada para la comunicación entre el UE y el eNodoB secundario.

En algunas realizaciones de la presente invención, el procesador 703 está configurado para realizar la siguiente etapa: que el UE determine, según la información de indicación incluida en el mensaje de comando de cambio de clave, que el modo para realizar el cambio de clave de seguridad entre el eNodoB maestro y el UE es la regeneración de clave es específicamente:

determinar, según la primera información de indicación o la primera información de contexto de clave de seguridad o información de contexto de seguridad que es transmitida en el mensaje de comando de cambio de clave, que el modo para realizar el cambio de clave de seguridad entre el eNodoB maestro y el UE es la regeneración de clave.

En algunas realizaciones de la presente invención, si la información de indicación transmitida en el mensaje de comando de cambio de clave indica que el UE mantiene la transmisión de datos entre el UE y una segunda estación base, luego de que el UE determina, según el mensaje de comando de cambio de clave, si mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o el eNodoB secundario y/o si mantener la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario, el procesador 703 está configurado además para realizar al menos una de las siguientes etapas:

mantener las configuraciones de PDCP de todas las RB establecidas entre el UE y la segunda estación base, donde cuando la segunda estación base es el eNodoB maestro, la primera estación base es el eNodoB secundario; o cuando la segunda estación base es el eNodoB secundario, la segunda estación base es el eNodoB maestro;

mantener las configuraciones de RLC de todas las RB establecidas entre el UE y la segunda estación base;

mantener las configuraciones de MAC de todas las RB establecidas entre el UE y la segunda estación base;

mantener un estado activo de una SCell activada entre el UE y la segunda estación base;

mantener un C-RNTI utilizado para la comunicación entre el UE y la segunda estación base; y

mantener la transmisión de datos entre el UE y la segunda estación base.

En algunas realizaciones de la presente invención, si el mensaje de comando de cambio de clave porta información de indicación que indica que el UE suspende la transmisión de datos entre el UE y la primera estación base, luego de que el UE determina, según el mensaje de comando de cambio de clave, si mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o el eNodoB secundario y/o si mantener la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario, el procesador 703 está configurado además para realizar al menos una de las siguientes etapas:

mantener las configuraciones de PDCP de todas las RB establecidas entre el UE y la primera estación base;

mantener las configuraciones de RLC de todas las RB establecidas entre el UE y la primera estación base;

mantener las configuraciones de MAC de todas las RB establecidas entre el UE y la primera estación base;

mantener un estado activo de una SCell activada entre el UE y la primera estación base;

mantener un C-RNTI utilizado para la comunicación entre el UE y la primera estación base; y

suspender la transmisión de datos entre el UE y la primera estación base.

En algunas realizaciones de la presente invención, si el mensaje de comando de cambio de clave porta información de indicación que indica que el UE detiene la transmisión de datos entre el UE y la primera estación base, luego de que el UE determina, según el mensaje de comando de cambio de clave, si mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o el eNodoB secundario y/o si mantener la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario, el procesador 703 está configurado para realizar al menos una de las siguientes etapas:

reconfigurar las configuraciones de PDCP de todas las RB establecidas entre el UE y la primera estación base;

reconfigurar las configuraciones de RLC de todas las RB establecidas entre el UE y la primera estación base;

reconfigurar las configuraciones de MAC de todas las RB establecidas entre el UE y la primera estación base;

detener la transmisión de datos entre el UE y la primera estación base.

Se puede aprender de las descripciones anteriores en esta realización de la presente invención que: un eNodoB maestro envía un mensaje de comando de cambio de clave a un UE, y el UE realiza, según el mensaje de comando de cambio de clave, un cambio de clave de seguridad entre el UE y una primera estación base, y determina, según el mensaje de comando de cambio de clave, si mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o un eNodoB secundario y/o si mantener la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario; luego de que el UE completa el cambio de clave de seguridad, el UE envía un mensaje de cambio de clave completado al eNodoB maestro, el eNodoB maestro puede recibir el mensaje de cambio de clave completado enviado por el UE, la primera estación base puede determinar, al utilizar el eNodoB maestro, que se complete el cambio de clave de seguridad entre el UE y la primera estación base, y la primera estación base y el UE pueden utilizar una nueva clave de seguridad para realizar la transmisión de datos. Por lo tanto, según esta realización de la presente invención, puede implementarse un cambio de clave de seguridad cuando un UE lleva a cabo la comunicación de conectividad dual con un MeNB y un SeNB.

Además, debería observarse que la realización del aparato descrito es meramente ilustrativa. Las unidades descritas como partes separadas pueden o no estar físicamente separadas, y partes visualizadas como unidades pueden o no ser unidades físicas, pueden ubicarse en una posición, o pueden distribuirse en una pluralidad de unidades de redes. Algunos o todos los módulos pueden seleccionarse según los requisitos actuales para lograr los objetivos de las soluciones de las realizaciones. Además, en los dibujos adjuntos de las realizaciones del aparato proporcionadas por la presente invención, las relaciones de conexión entre módulos indican que los módulos tienen conexiones de comunicación entre sí, que pueden implementarse específicamente como uno o más buses de comunicaciones o cables de señal. Los expertos en la técnica pueden comprender e implementar las realizaciones de la presente invención sin esfuerzos creativos.

Los expertos en la técnica pueden comprender claramente, en función de la descripción de los modos de implementación anteriores, que la presente invención puede implementarse mediante software además de hardware universal necesario o mediante hardware dedicado, que incluye un circuito integrado específico de la aplicación, un CPU dedicado, una memoria dedicada, un componente dedicado y similares. Generalmente, cualquier función que pueda realizarse por un programa informático puede implementarse fácilmente al utilizar hardware correspondiente. Además, una estructura de hardware específica utilizada para lograr una misma función puede tener varias formas, por ejemplo, en una forma de un circuito análogo, un circuito digital, un circuito dedicado o similares. Sin embargo, en lo que respecta a la presente invención, la implementación de un programa de software es un mejor modo de implementación en la mayoría de los casos. Con base en tal entendimiento, las soluciones técnicas de la presente invención esencialmente, o la parte que contribuye a la técnica anterior pueden implementarse en forma de un producto de software. El producto de software informático se almacena en un medio de almacenamiento legible por computadora, tal como un disco flexible, una memoria USB, un disco duro extraíble, una memoria de solo lectura (en inglés, Read-Only Memory - ROM), una memoria de acceso aleatorio (en inglés, Random Access Memory - RAM), un disco magnético o un disco óptico de una computadora e incluye varias instrucciones para ordenar a un dispositivo informático (que puede ser una computadora personal, un servidor, un dispositivo de red o similar) a que realice los métodos descritos en las realizaciones de la presente invención.

Se pretende que las realizaciones anteriores sean meramente para describir las soluciones técnicas de la presente invención, pero no para limitar la presente invención. Aunque la presente invención se describe en detalle con referencia a las realizaciones anteriores, los expertos en la técnica deberán comprender que aún pueden realizar modificaciones a las soluciones técnicas descritas en las realizaciones anteriores o realizar reemplazos equivalentes a algunas características técnicas de los mismos, sin alejarse del alcance de las soluciones técnicas de las realizaciones de la presente invención.

REIVINDICACIONES

1. Un método de cambio de clave de seguridad, que comprende:

recibir (201), mediante el equipo de usuario UE, un mensaje de comando de cambio de clave desde un eNodoB maestro, MeNB, en donde el mensaje de comando de cambio de clave comprende información de indicación de que un cambio de clave de seguridad puede realizar entre el UE y un eNodoB secundario, SeNB, en donde el UE está configurado con una conectividad dual entre el MeNB y el SeNB;
realizar (202), mediante el UE según el mensaje de comando de cambio de clave, el cambio de clave de seguridad entre el UE y el SeNB;
determinar (203), mediante el UE según el mensaje de comando de cambio de clave, si mantener la información de configuración de estrato de acceso entre el UE y el SeNB; y
enviar (204), mediante el UE, un mensaje de cambio de clave completado al MeNB;
en donde la información de configuración de estrato de acceso entre UE y el SeNB comprende al menos uno de los siguientes:

información de configuración del protocolo de convergencia de datos por paquetes, PDCP, entre el UE y el SeNB;
información de configuración del Control de Radio Enlace, RLC, entre el UE y el SeNB;
información de configuración del Control de Acceso al Medio, MAC, entre el UE y el SeNB;
un estado activo de una célula secundaria, SCell, activada entre el UE y el SeNB;
un identificador temporal de red de radio celular, C-RNTI, utilizado para la comunicación entre el UE y el SeNB.

2. El método según la reivindicación 1, en donde el mensaje de comando de cambio de clave porta información de indicación que indica si el UE realiza acceso aleatorio al SeNB, y luego de recibir, mediante el UE, un mensaje de comando de cambio de clave desde el MeNB, el método comprende, además:

determinar, mediante el UE según el mensaje de comando de cambio de clave, si realizar acceso aleatorio al SeNB.

3. El método según la reivindicación 1 o 2, en donde el mensaje de comando de cambio de clave comprende además información sobre un recurso de acceso aleatorio y el método comprende, además:

realizar, mediante el UE, acceso aleatorio al SeNB según la información sobre el recurso de acceso aleatorio.

4. El método según una cualquiera de las reivindicaciones 1 a 3, en donde el mensaje de comando de cambio de clave comprende la primera información de indicación y la segunda información de indicación, en donde la primera información de indicación se utiliza para indicar que debe realizarse un cambio de clave de seguridad entre el MeNB y el UE y la segunda información de indicación se utiliza para indicar que un cambio de clave de seguridad debe realizarse entre el SeNB; y el método comprende además:

realizar, mediante el UE según el mensaje de comando de cambio de clave, el cambio de clave de seguridad entre el UE y el MeNB.

5. El método según la reivindicación 4, en donde la primera información de indicación se utiliza además para indicar que un modo de realizar el cambio de clave de seguridad entre el MeNB y el UE es la regeneración de clave o la actualización de clave y
el cambio de clave de seguridad entre el UE y el MeNB comprende:

realizar, mediante el UE según la primera información de indicación, el cambio de clave de seguridad entre el UE y el MeNB en un modo de regeneración de clave o actualización de clave; y
la segunda información de indicación se utiliza además para indicar que un modo para realizar el cambio de clave de seguridad entre el SeNB y el UE es la actualización de clave, y
el cambio de clave de seguridad entre el UE y el SeNB comprende:
realizar, mediante el UE según la segunda información de indicación, el cambio de clave de seguridad entre el UE y el SeNB en el modo de actualización de clave.

6. El método según una cualquiera de las reivindicaciones 1 a 5, en donde la determinación, mediante el UE según la información de comando de cambio de clave, de si mantener la información de configuración de estrato de acceso entre el UE y el SeNB comprende:

determinar, mediante el UE según el campo del indicador de cambio de clave comprendida en el mensaje de comando de cambio de clave, si mantener la información de configuración de estrato de acceso entre el UE y el SeNB.

7. El método según la reivindicación 6, en donde la determinación, mediante el UE según un campo del indicador de cambio de clave comprendida en el mensaje de comando de cambio de clave, de si mantener la información de configuración de estrato de acceso entre el UE y el SeNB comprende:

al determinar, según el campo del indicador de cambio de clave, que debe realizarse la regeneración de clave, determinar, mediante el UE, no mantener la información de configuración de estrato de acceso entre el UE y el SeNB;

o
al determinar, según el campo del indicador de cambio de clave, que debe realizarse la actualización de clave en función de una clave intermedia del lado de UE que corresponde al MeNB, determinar, mediante el UE, mantener la información de configuración de estrato de acceso entre el UE y el SeNB; o
al determinar, según el campo del indicador de cambio de clave, que debe realizarse la actualización de clave en función de un siguiente salto, NH, determinar, mediante el UE, mantener la información de configuración de estrato de acceso entre el UE y el SeNB.

8. Equipo de usuario, UE, que comprende:

un módulo de recepción de mensajes (501), configurado para recibir un mensaje de comando de cambio de clave desde un eNodoB maestro, MeNB, en donde el mensaje de comando de cambio de clave comprende información de indicación de que debe realizarse un cambio de clave de seguridad entre el UE y un eNodoB secundario, SeNB, en donde el UE está configurado con una conectividad dual entre el MeNB y el SeNB;
un módulo de cambio de clave (502), configurado para realizar, según el mensaje de comando de cambio de clave, el cambio de clave de seguridad entre el UE y el SeNB;
un módulo de determinación (503), configurado para determinar, según el mensaje de comando de cambio de clave, si mantener la información de configuración de estrato de acceso entre el UE y el SeNB; y
un módulo de envío de mensajes (504), configurado para enviar un mensaje de cambio de clave completado al MeNB; en donde la información de configuración de estrato de acceso entre el UE y el SeNB comprende al menos uno de los siguientes:

Información de configuración del protocolo de convergencia de datos por paquetes, PDCP, entre el UE y el SeNB;
información de configuración del Control de Radio Enlace, RLC, entre el UE y el SeNB;
información de configuración del Control de Acceso al Medio, MAC, entre el UE y el SeNB;
un estado activo de una célula secundaria, SCell, activada entre el UE y el SeNB;
un identificador temporal de red de radio celular, C-RNTI, utilizado para la comunicación entre el UE y el SeNB.

9. El UE según la reivindicación 8, en donde el mensaje de comando de cambio de clave porta información de indicación que indica si el UE realiza acceso aleatorio al SeNB y el módulo de determinación está configurado además para: luego de que el módulo de recepción de mensajes recibe el mensaje de comando de cambio de clave desde el MeNB, determinar, según el mensaje de comando de cambio de clave, si realizar acceso aleatorio al SeNB.

10. El UE según la reivindicación 8 o 9, en donde el mensaje de comando de cambio de clave comprende además información sobre un recurso de acceso aleatorio, y el UE comprende además un módulo de acceso aleatorio, configurado para realizar acceso aleatorio al SeNB según la información sobre el recurso de acceso aleatorio.

11. El UE según una cualquiera de las reivindicaciones 8 a 10, en donde el mensaje de comando de cambio de clave comprende la primera información de indicación y la segunda información de indicación, en donde la primera información de indicación se utiliza para indicar que debe realizarse un cambio de clave de seguridad entre el eNodoB maestro y el UE y la segunda información de indicación se utiliza para indicar que un cambio de clave de seguridad debe realizarse entre el eNodoB secundario y el UE, y
el módulo de cambio de clave está configurado además para realizar, según el mensaje de comando de cambio de clave, el cambio de clave de seguridad entre el UE y el MeNB.

12. El UE según la reivindicación 11, en donde la primera información de indicación se utiliza además para indicar que un modo para realizar el cambio de clave de seguridad entre el MeNB y el UE es la regeneración de clave o la actualización de clave, y
el módulo de cambio de clave está configurado para realizar, según la primera información de indicación, el cambio de clave de seguridad entre el UE y el MeNB en un modo de regeneración de clave o actualización de clave; y
la segunda información de indicación se utiliza además para indicar que un modo para realizar el cambio de clave de seguridad entre el SeNB y el UE es la actualización de clave y
el módulo de cambio de clave está configurado para realizar, según la segunda información de indicación, el cambio de clave de seguridad entre el UE y el SeNB en el modo de actualización de clave.

13. El UE según una cualquiera de las reivindicaciones 8 a 12, en donde el módulo de determinación está configurado para:

al determinar, según el campo del indicador de cambio de clave, que debe realizarse la regeneración de clave, determinar no mantener la información de configuración de estrato de acceso entre el UE y el SeNB; o
al determinar, según el campo del indicador de cambio de clave, que debe realizarse la actualización de clave en función de una clave intermedia del lado de UE que corresponde al MeNB, determinar mantener la información de configuración de estrato de acceso entre el UE y el SeNB; o
al determinar, según el campo del indicador de cambio de clave, que debe realizarse la actualización de clave en función de un siguiente salto, NH, determinar mantener la información de configuración de estrato de acceso entre el UE y el SeNB.

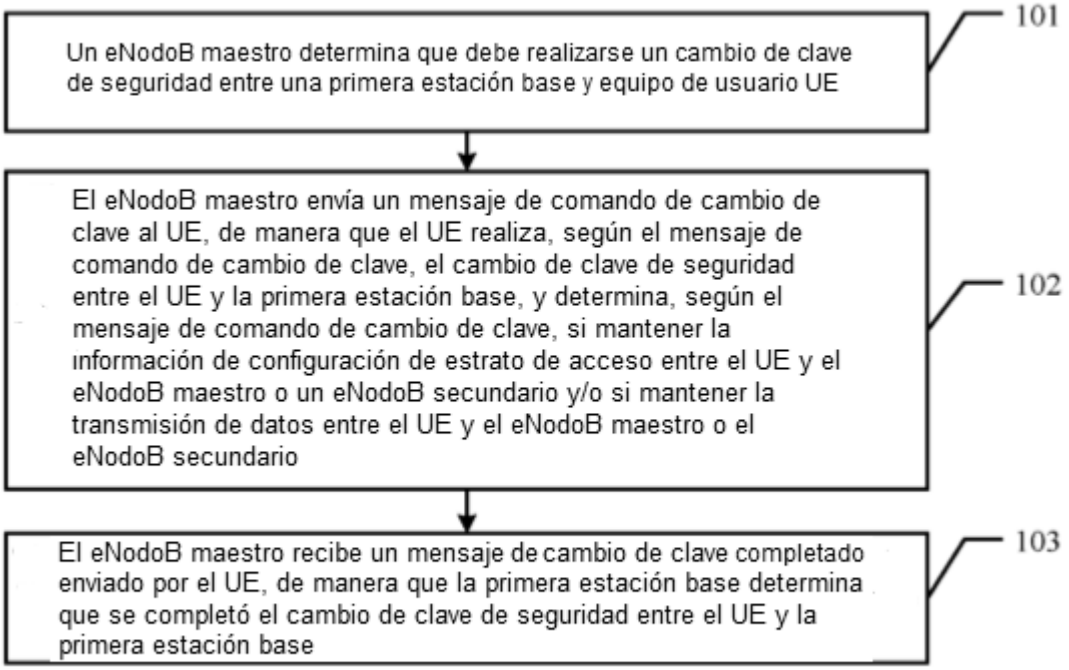
Un eNodoB maestro determina que debe realizarse un cambio de clave de seguridad entre una primera estación base y equipo de usuario UE
101
El eNodoB maestro envía un mensaje de comando de cambio de clave al UE, de manera que el UE realiza, según el mensaje de comando de cambio de clave, el cambio de clave de seguridad entre el UE y la primera estación base, y determina, según el mensaje de comando de cambio de clave, si mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o un eNodoB secundario y/o si mantener la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario
102
El eNodoB maestro recibe un mensaje de cambio de clave completado enviado por el UE, de manera que la primera estación base determina que se completó el cambio de clave de seguridad entre el UE y la primera estación base
103

FIG. 1

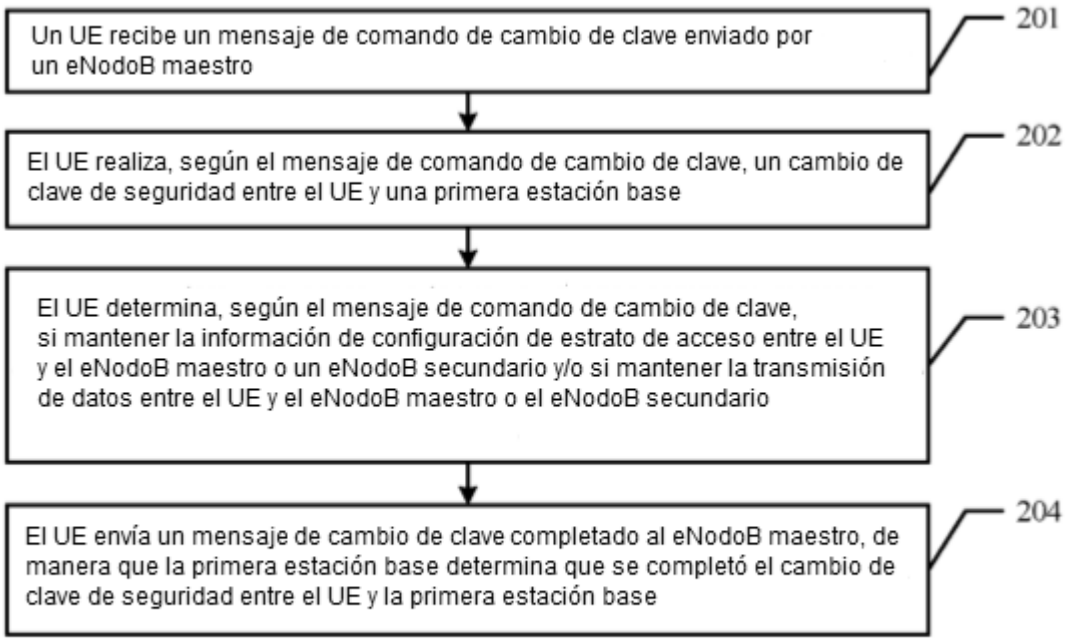
Un UE recibe un mensaje de comando de cambio de clave enviado por un eNodoB maestro
201
El UE realiza, según el mensaje de comando de cambio de clave, un cambio de clave de seguridad entre el UE y una primera estación base
202
El UE determina, según el mensaje de comando de cambio de clave, si mantener la información de configuración de estrato de acceso entre el UE y el eNodoB maestro o un eNodoB secundario y/o si mantener la transmisión de datos entre el UE y el eNodoB maestro o el eNodoB secundario
203
El UE envía un mensaje de cambio de clave completado al eNodoB maestro, de manera que la primera estación base determina que se completó el cambio de clave de seguridad entre el UE y la primera estación base
204

FIG. 2

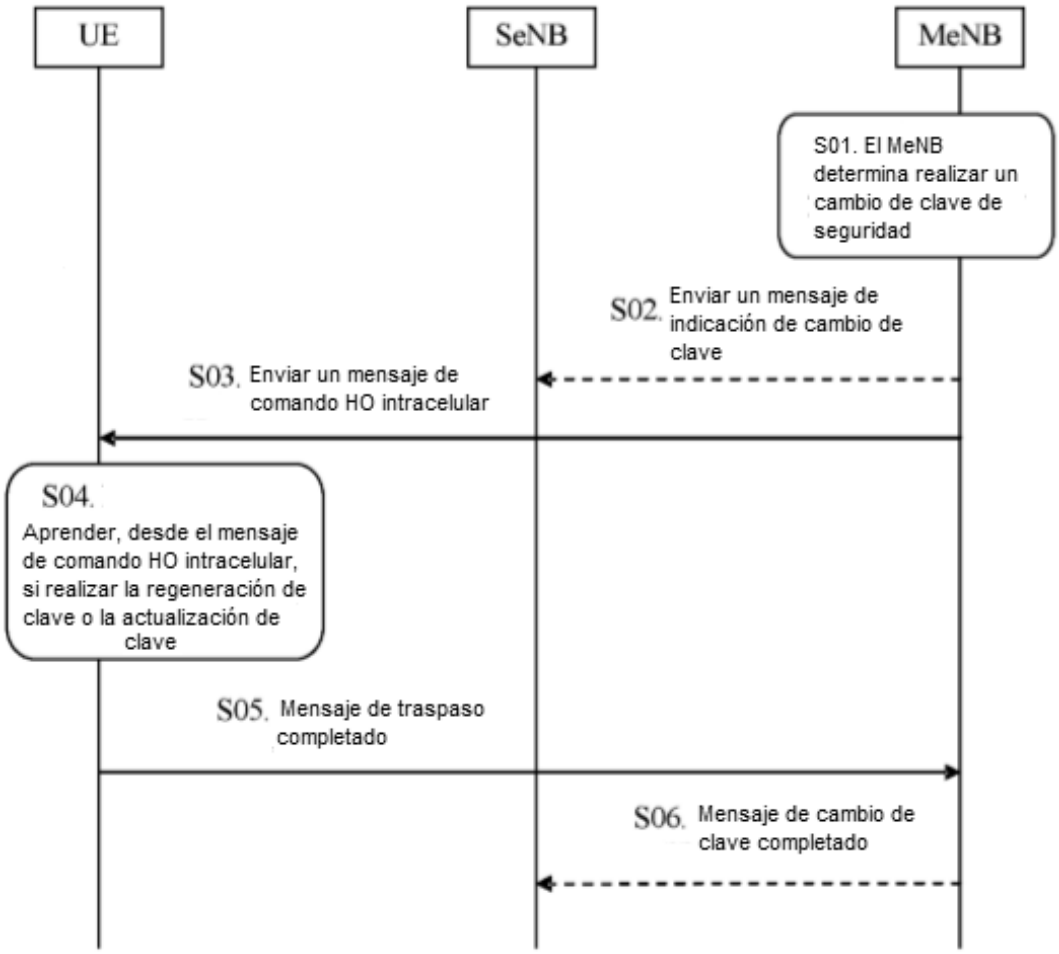
UE
SeNB
MeNB
S01. El MeNB determina realizar un cambio de clave de seguridad
S02. Enviar un mensaje de indicación de cambio de clave
S03. Enviar un mensaje de comando HO intracelular
S04. Aprender, desde el mensaje de comando HO intracelular, si realizar la regeneración de clave o la actualización de clave
S05. Mensaje de traspaso completado
S06. Mensaje de cambio de clave completado

FIG. 3-a

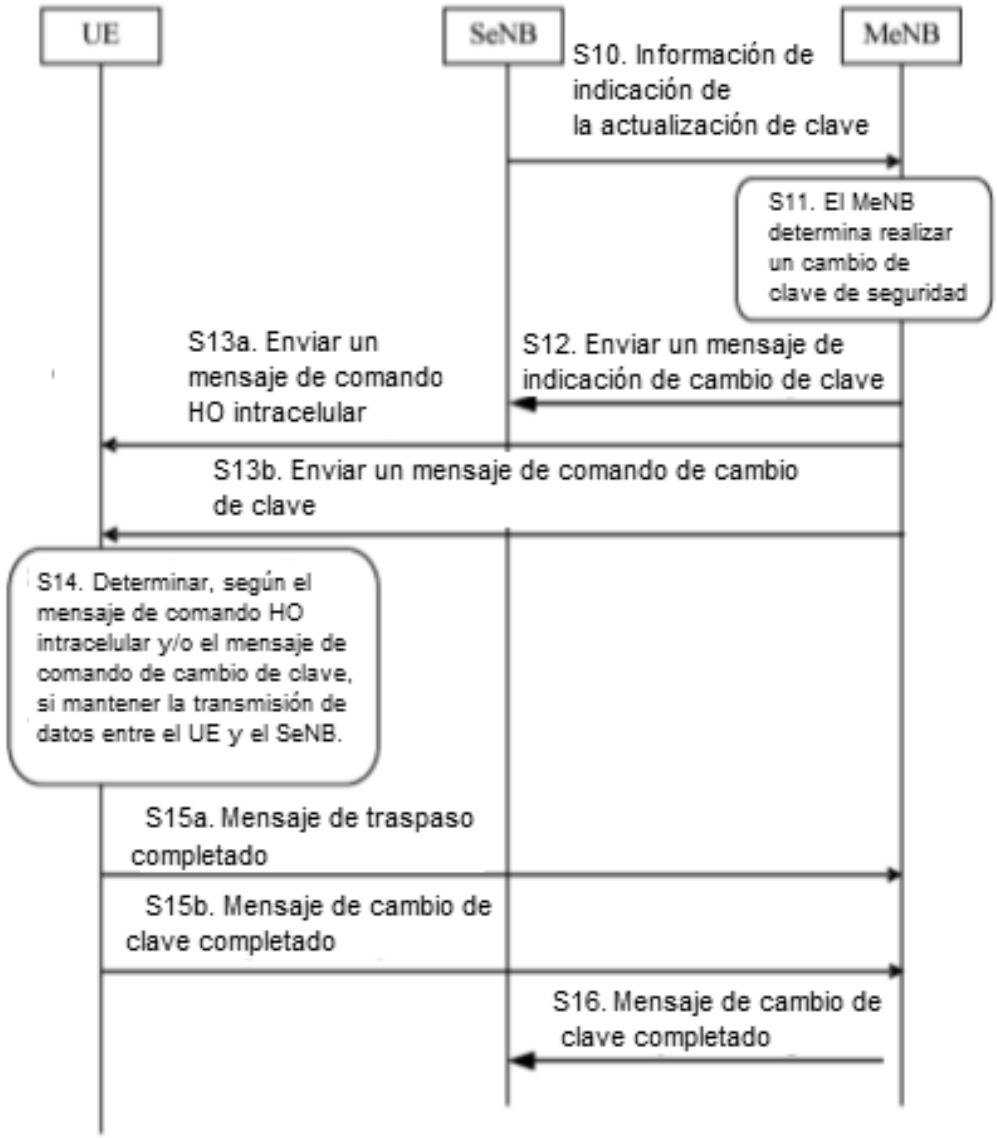
UE
SeNB
MeNB
S10. Información de indicación de la actualización de clave
S11. El MeNB determina realizar un cambio de clave de seguridad
S13a. Enviar un mensaje de comando HO intracelular
S12. Enviar un mensaje de indicación de cambio de clave
S13b. Enviar un mensaje de comando de cambio de clave
S14. Determinar, según el mensaje de comando HO intracelular y/o el mensaje de comando de cambio de clave, si mantener la transmisión de datos entre el UE y el SeNB.
S15a. Mensaje de traspaso completado
S15b. Mensaje de cambio de clave completado
S16. Mensaje de cambio de clave completado

FIG. 3-b

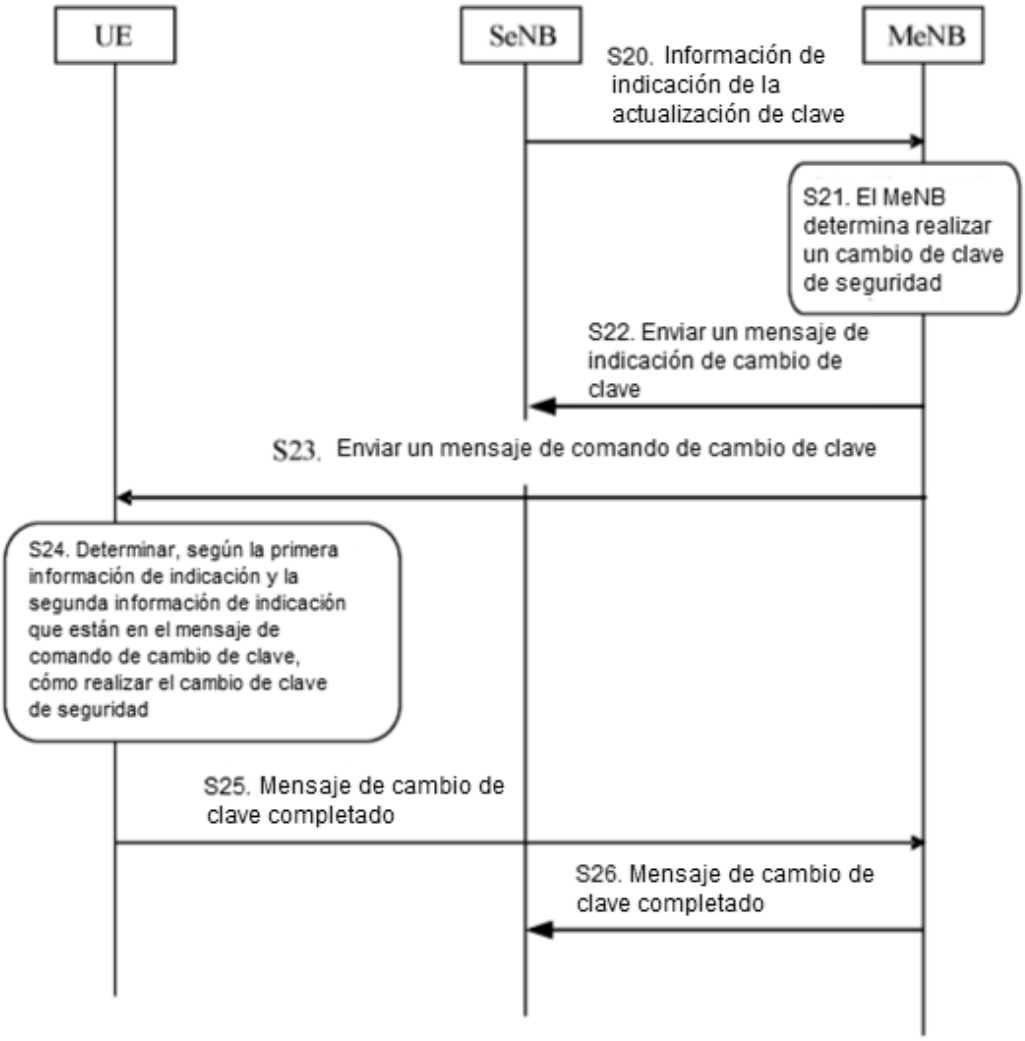
UE
SeNB
MeNB
S20. Información de indicación de la actualización de clave
S21. El MeNB determina realizar un cambio de clave de seguridad
S22. Enviar un mensaje de indicación de cambio de clave
S23. Enviar un mensaje de comando de cambio de clave
S24. Determinar, según la primera información de indicación y la segunda información de indicación que están en el mensaje de comando de cambio de clave, cómo realizar el cambio de clave de seguridad
S25. Mensaje de cambio de clave completado
S26. Mensaje de cambio de clave completado

FIG. 3-c

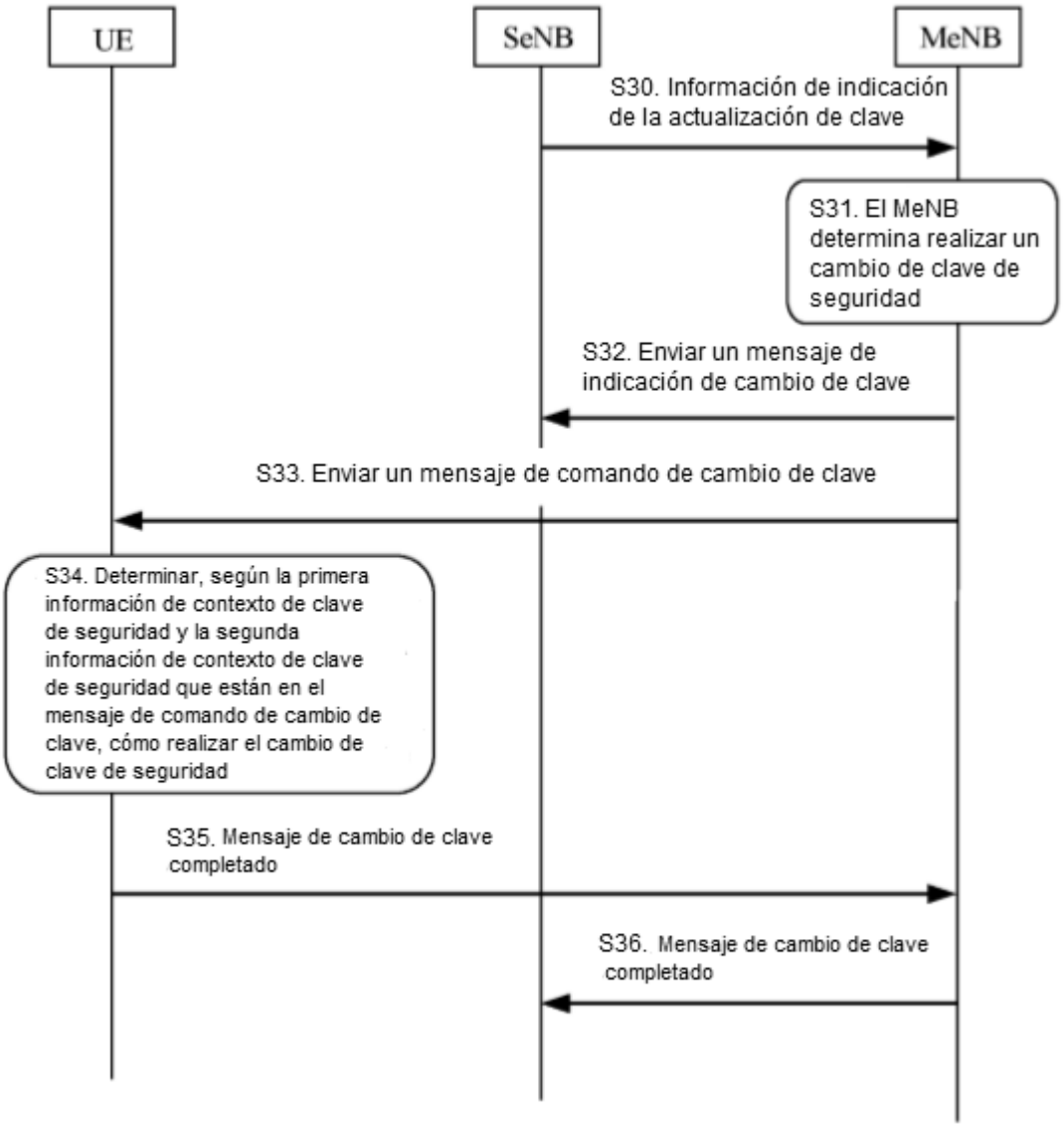
UE
SeNB
MeNB
S30. Información de indicación de la actualización de clave
S31. El MeNB determina realizar un cambio de clave de seguridad
S32. Enviar un mensaje de indicación de cambio de clave
S33. Enviar un mensaje de comando de cambio de clave
S34. Determinar, según la primera información de contexto de clave de seguridad y la segunda información de contexto de clave de seguridad que están en el mensaje de comando de cambio de clave, cómo realizar el cambio de clave de seguridad
S35. Mensaje de cambio de clave completado
S36. Mensaje de cambio de clave completado

FIG. 3-d

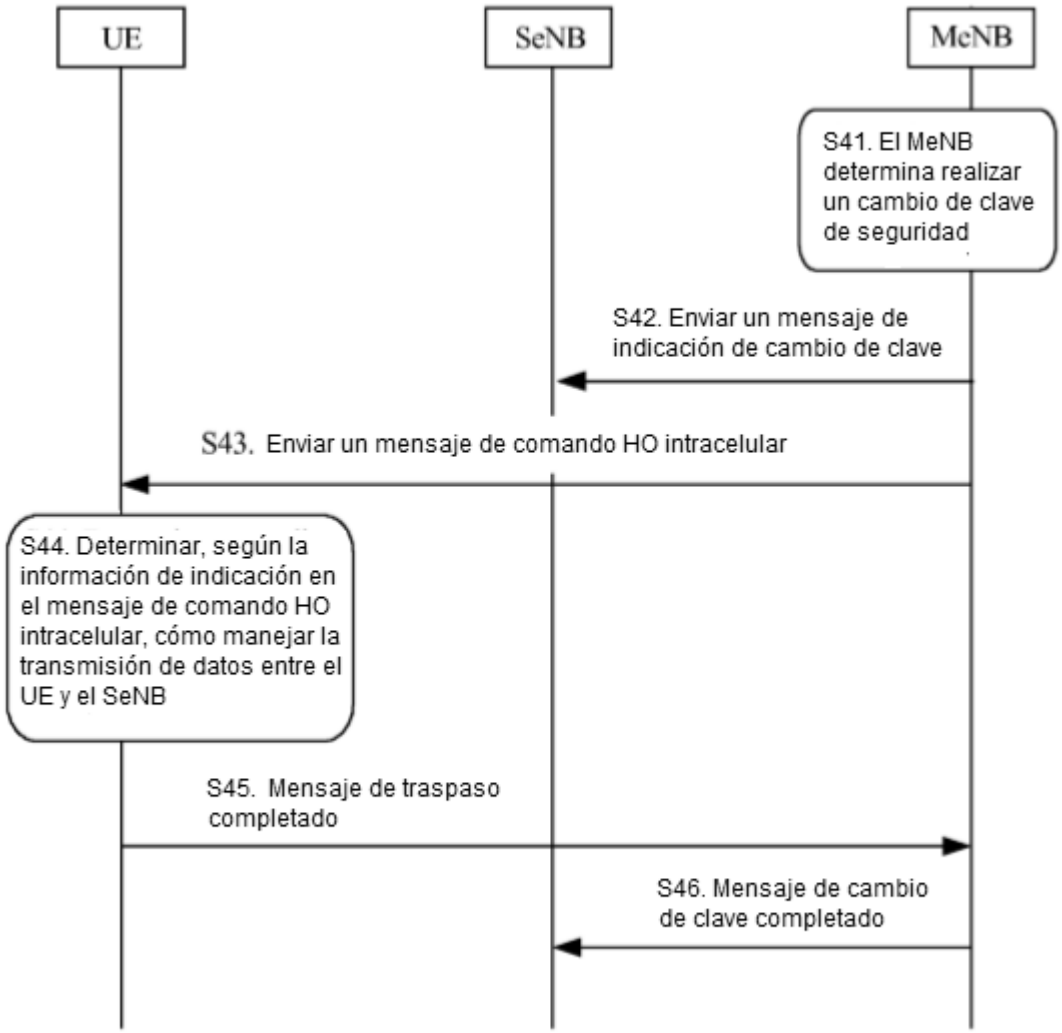
UE
SeNB
MeNB
S41. El MeNB determina realizar un cambio de clave de seguridad
S42. Enviar un mensaje de indicación de cambio de clave
S43. Enviar un mensaje de comando HO intracelular
S44. Determinar, según la información de indicación en el mensaje de comando HO intracelular, cómo manejar la transmisión de datos entre el UE y el SeNB
S45. Mensaje de traspaso completado
S46. Mensaje de cambio de clave completado

FIG. 3-e

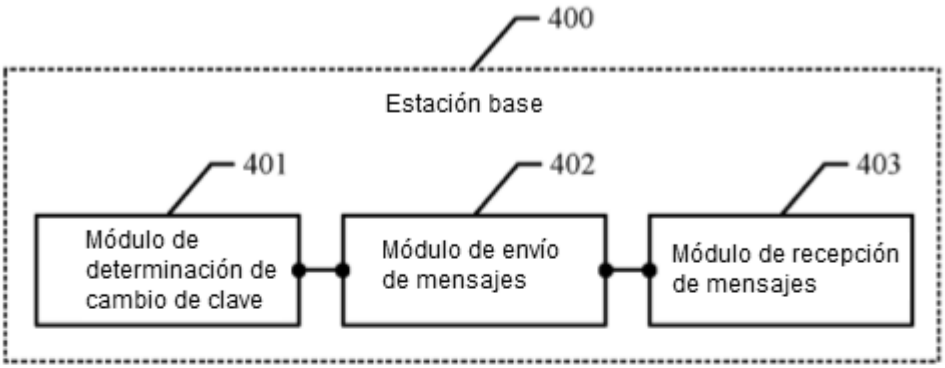

FIG. 4-a

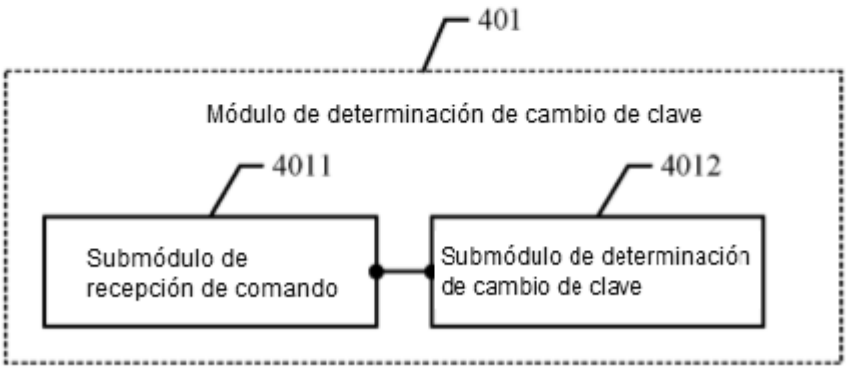

FIG. 4-b

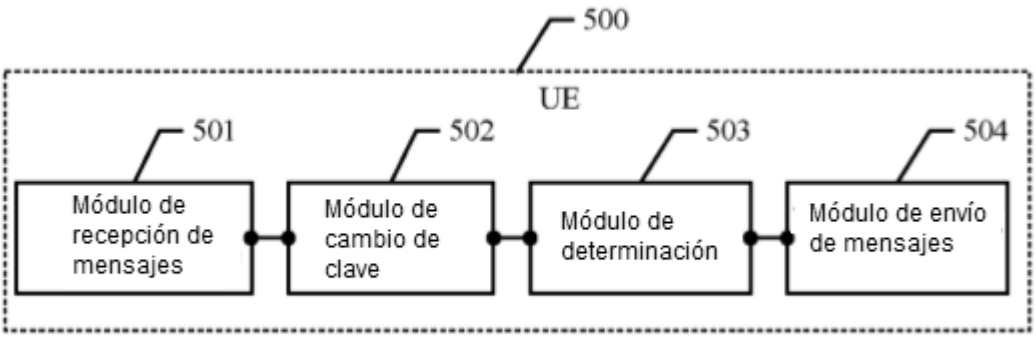

FIG. 5-a

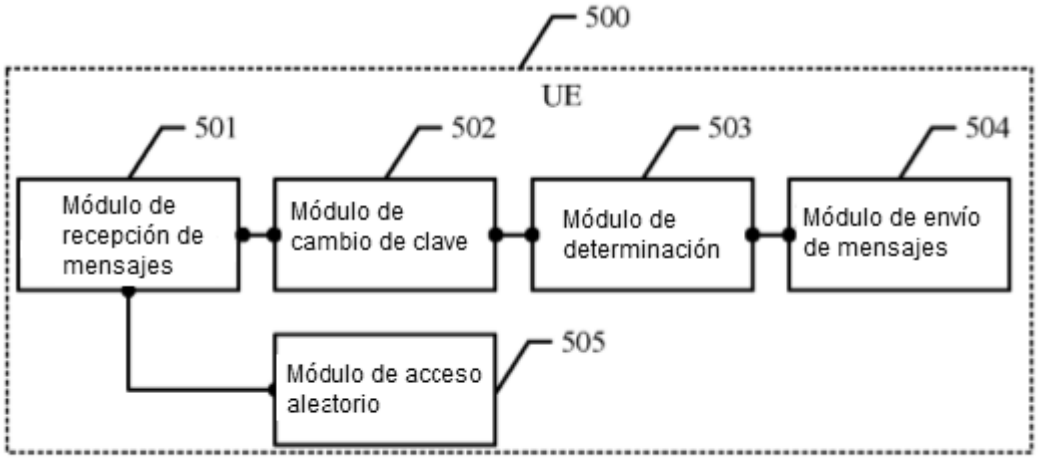
500
UE
501
Módulo de recepción de mensajes
502
Módulo de cambio de clave
503
Módulo de determinación
504
Módulo de envío de mensajes
505
Módulo de acceso aleatorio

FIG. 5-b

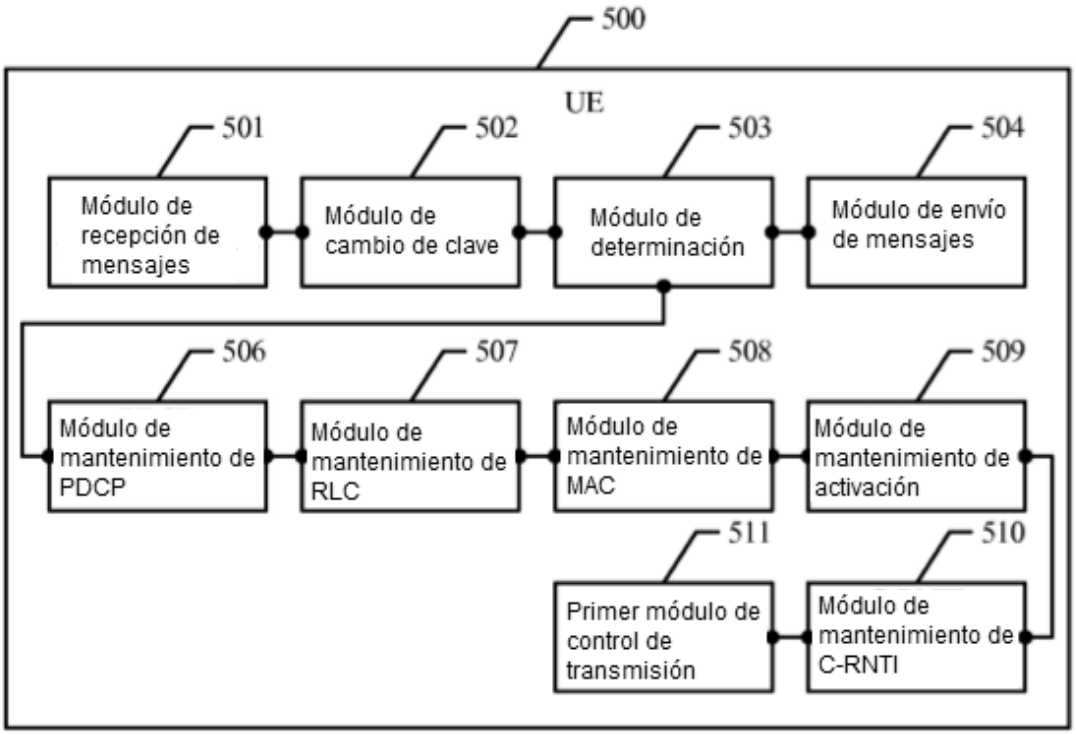
500
UE
501
Módulo de recepción de mensajes
502
Módulo de cambio de clave
503
Módulo de determinación
504
Módulo de envío de mensajes
506
Módulo de mantenimiento de PDCP
507
Módulo de mantenimiento de RLC
508
Módulo de mantenimiento de MAC
509
Módulo de mantenimiento de activación
511
Primer módulo de control de transmisión
510
Módulo de mantenimiento de C-RNTI

FIG. 5-c

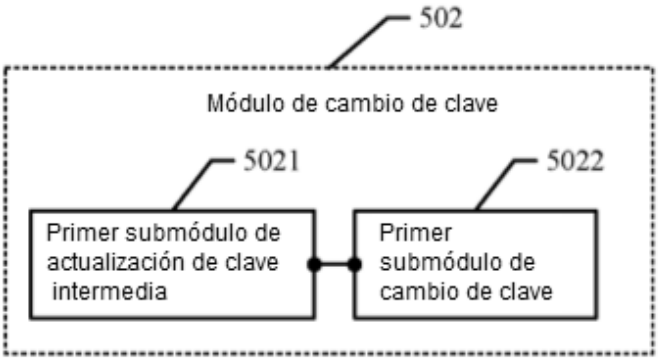
502
Módulo de cambio de clave
5021
5022
Primer submódulo de actualización de clave intermedia
Primer submódulo de cambio de clave

FIG. 5-d

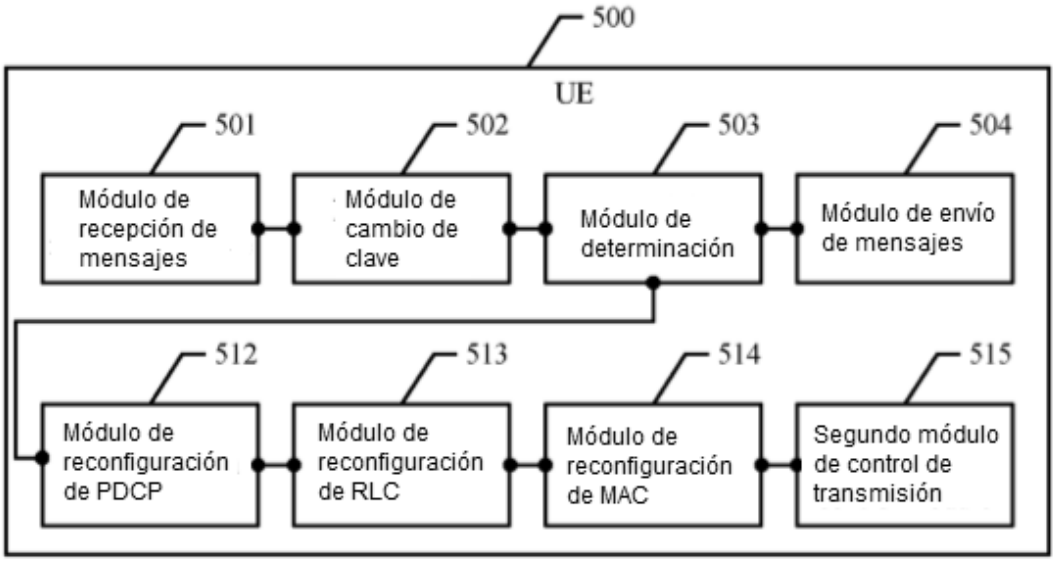
500
UE
501
502
503
504
Módulo de recepción de mensajes
Módulo de cambio de clave
Módulo de determinación
Módulo de envío de mensajes
512
513
514
515
Módulo de reconfiguración de PDCP
Módulo de reconfiguración de RLC
Módulo de reconfiguración de MAC
Segundo módulo de control de transmisión

FIG. 5-e

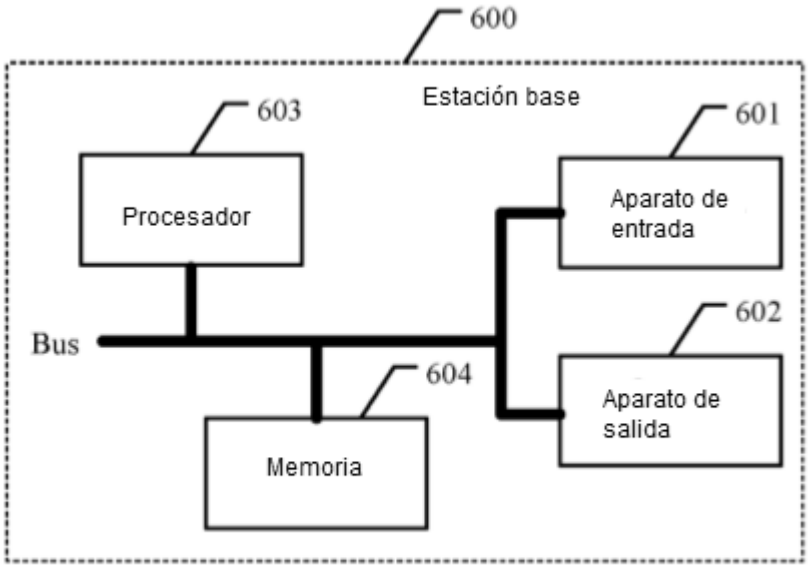
600
Estación base
603
Procesador
601
Aparato de entrada
602
Aparato de salida
Bus
604
Memoria

FIG. 6

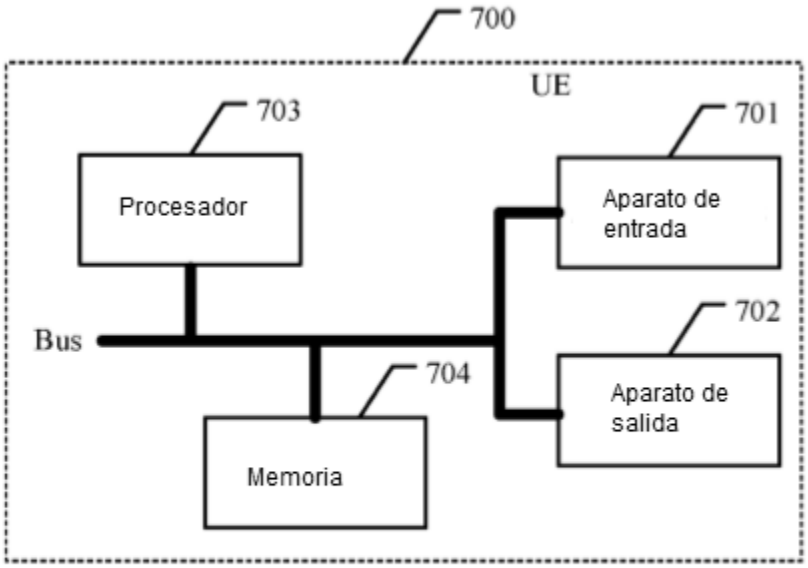
700
UE
703
Procesador
701
Aparato de entrada
702
Aparato de salida
Bus
704
Memoria

FIG. 7