(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 617 067**

(51) Int. CI.:

***H04L 9/08*** (2006.01)
***H04L 9/32*** (2006.01)
***H04L 9/06*** (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **21.07.2008 E 13003646 (0)**

(97) Fecha y número de publicación de la concesión europea: **14.12.2016 EP 2658163**

(54) Título: **Generación de claves criptográficas**

(30) Prioridad:

**06.06.2008 US 59386 P**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**15.06.2017**

(73) Titular/es:

**TELEFONAKTIEBOLAGET LM ERICSSON (PUBL) (100.0%)**
**164 83 Stockholm, SE**

(72) Inventor/es:

**NÄSLUND, MATS y**
**NORRMAN, KARL**

(74) Agente/Representante:

**DE ELZABURU MÁRQUEZ, Alberto**

## DESCRIPCIÓN

Generación de claves criptográficas

### Campo técnico

La presente invención de manera general se refiere a una técnica para generar claves criptográficas. Particularmente, la invención se refiere a una técnica de generación de claves criptográficas que proporciona un alto nivel de seguridad.

### Antecedentes

El protocolo de Autentificación y Acuerdo de Claves (AKA) es un protocolo basado en desafío-respuesta que usa criptografía simétrica. Las metas principales de AKA incluyen autentificación mutua mediante dos entidades que comunican una con otra y el establecimiento de claves criptográficas para proteger la comunicación intercambiada entre medias. Una variante de AKA es la AKA de UMTS, incluida en la arquitectura de seguridad estandarizada por el 3GPP para redes de comunicación móvil de 3G en la Especificación Técnica TS 33.102 de 3G.

El concepto básico de AKA de UMTS se muestra en la Fig. 1. Con referencia a esta figura, el protocolo de AKA de UMTS se ejecuta entre un equipo de usuario (UE) y una entidad de red (NE). La entidad de red inicia la AKA enviando una petición de autentificación de usuario al UE. Junto con la petición, un desafío aleatorio, o código aleatorio (RAND), y un Testigo de Autentificación (AUTN) se envían al UE. Tras la recepción del RAND y el AUTN, el UE, entre otras cosas, calcula una Clave de Cifrado (CK) y una Clave de Integridad (IK) y entonces las usa para funciones de cifrado e integridad.

El 3GPP también está emprendiendo la estandarización de las denominadas redes de comunicación “más allá de 3G”. La Evolución de Arquitectura de Sistema (SAE) y la Evolución de Largo Plazo (LTE) son dos aspectos estrechamente relacionados de la red más allá de 3G. Comparado con las redes 3G convencionales, una red basada en SAE/LTE puede imponer mayores requisitos o/ de más seguridad. Por ejemplo, se pueden necesitar más claves criptográficas para asegurar la comunicación a diferentes niveles. El 3GPP ha recomendado, en otro documento relacionado con el estándar, el TR 33.821 del 3GPP, una jerarquía de claves para derivar más claves criptográficas para uso en SAE/LTE.

La Fig. 2 muestra esta jerarquía de claves. En lo más alto de la jerarquía está una clave K, una clave criptográfica de largo plazo compartida entre el Módulo Universal de Identidad de Abonado (USIM) del UE y el Centro de Autentificación (AuC) que reside en la red. Un nivel más abajo está un par de claves criptográficas CK e IK que se derivan por el UE, particularmente por el USIM del mismo, de una misma manera o similar que la operación de AKA del UMTS mencionada anteriormente. Más abajo en la jerarquía está una clave $K_{ASME}$ que se deriva por el UE de la CK, IK, y, si es necesario, algunos otros parámetros. Una vez derivada, la $K_{ASME}$ se transfiere desde el AuC a la red de acceso, particularmente a la Entidad de Gestión de Seguridad de Acceso (ASME) de la red SAE/LTE, y entonces se comparte entre el UE y la red. Cuando la red de acceso está basada en tecnología LTE, las funcionalidades de la ASME se manejan por una Entidad de Gestión de Movilidad (MME).

La clave $K_{ASME}$, y las claves “por debajo” de ella en la jerarquía, se pueden derivar aplicando una cierta función criptográfica. Por ejemplo,

$$K_{ASME} = KDF(CK \,||\, IK, 0x02 \,||\, PLMN\_ID \,||\, < otro\_parámetro > )$$

donde KDF se basa en una función de derivación de clave (KDF) de Arquitectura de Inicialización Genérica (GBA). Una KDF de GBA se especifica en la TS 33.220 de 3G.

La KDF de GBA puede hacer uso de funciones para generar claves criptográficas tales como las funciones para generar claves de Algoritmo de Generación de Claves Seguras (SHA). Entre las muchas funciones de generación de claves SHA, SHA-256 es una variante altamente segura dado que se considera resistente a colisión y actúa como una función pseudoaleatoria. Como sugiere su nombre, SHA-256 es una función de generación de claves de Algoritmo de Generación de Claves Seguras con una longitud de resumen (salida) de 256 bits. El PLMN_ID es un identificador de la red que sirve al UE.

Se ha comprobado que, para lograr un alto nivel de seguridad, no es suficiente basar la función KDF de GBA principalmente en CK e IK solamente. La razón fundamental para esto es el riesgo de que un UE dado pudiera obtener la misma CK dos veces, o dos UE diferentes puedan obtener la misma CK. En tales casos, la “unicidad” de las entradas a la KDF es baja, y puede ocurrir una colisión entre diferentes UE (que usan la misma $K_{ASME}$).

Como observación general, mientras que es cierto que KDF(x) produce la misma clave que KDF(y) si x = y, lo inverso puede no mantenerse siempre. Es decir, incluso si $x \neq y$, puede ocurrir todavía que KDF(x) = KDF(y). No obstante, este es un suceso improbable dado que la KDF se recomienda que esté basada en SHA-256 que, como se mencionó, se ha diseñado para ser resistente a colisiones. De esta manera, para la técnica descrita en la presente memoria, se puede suponer de manera segura que KDF(x) = KDF(y) sí y solo sí x = y. Esta suposición

permite que la técnica descrita en la presente memoria esté centrada en asegurar la “unicidad” de las entradas a la KDF.

El órgano de estandarización de la especificación de la KDF de GBA (ETSI/SAGE, el Grupo de Expertos de Algoritmo Especial) ha señalado el problema anterior y recomendado incluir la Identidad de Usuario Privado del UE (IMPI) en <otro_parámetro> para evitar colisiones entre diferentes UE. Como recomendación adicional, un código aleatorio tal como el RAND también se puede incluir en <otro_parámetro>. Esto se describe en una declaración de coordinación desde ETSI/SAGE a SA3 del 3GPP (en el número de documento S3 – 030219 del 3GPP).

No obstante, se ha encontrado que las recomendaciones anteriores aún pueden no garantizar la “unicidad” de las entradas a la KDF. Esto se puede ver a partir del análisis de más delante de la propiedad de seguridad de la función KDF de GBA y su uso en SAE/LTE para uno y el mismo UE (por ejemplo una y la misma IMPI).

En primer lugar, se considera la siguiente construcción básica:

**KDF(CK, IMPI).**

Dado que se ha supuesto que IMPI = IMPI’ (cuando el UE está fijo), esta construcción básica conducirá a colisión para dos entradas (CK, IMPI), (CK’, IMPI’) si y solo sí CK = CK’.

En segundo lugar, se considera otra construcción, la cual es más cercana a la KDF de GBA real:

**KDF(CK || IK, IMPI).**

No obstante, incluir IK dentro de las entradas no cambia la propiedad de colisión anterior como uno pudiera creer al principio. Es decir, KDF(CK || IK, IMPI) será igual a KDF(CK’ || IK’, IMPI) sí y solo sí CK = CK’. Para comprender por qué incluir IK no ayudaría, es necesario considerar cómo se producen CK e IK por el algoritmo criptográfico ejecutado en el UE.

El algoritmo criptográfico del lado de UE típico es el algoritmo Milenage el cual se muestra en la Fig. 9. En la Fig. 9, Ek indica el algoritmo Estándar de Cifrado Avanzado (AES), también conocido como el algoritmo Rijndael, que usa la clave K (almacenada en el AuC y el USIM del UE). Consideremos ahora qué ocurre si CK = CK’. Dado que el AES es una permutación (una asignación uno a uno), esto implica que el valor intermedio (que ocurre en la flecha gruesa) se determina únicamente por la salida de f3 que pasa a ser CK. Pero esto implica que el valor de la fecha gruesa cuando se produce la CK debe ser el mismo que el valor que ocurre en el mismo lugar cuando CK’ fue producido. Esto a su vez significa que los valores que ocurren como entrada a f4 deben ser los mismos y consecuentemente, los mismos valores de f4 deben ocurrir. Como suele suceder, f4 *es* IK. De esta manera se ha mostrado que CK = CK’ sí y solo sí IK = IK’.

A continuación, una construcción “mejorada” según la recomendación del órgano de estandarización (SAGE), es decir, que incluye el RAND en las entradas, se considera:

**KDF(CK || IK, RAND || IMPI).**

Suponemos que CK = CK’ (y de esta manera IK = IK’). Se espera que el uso de RAND garantizará la unicidad. No obstante, esto no es cierto. Consideremos de nuevo la parte “relevante” del algoritmo Milenage que produjo la CK e IK a partir del RAND: Como se muestra en la Fig. 9, hay una situación en la que el valor en la flecha gruesa que corresponde al RAND es el mismo que el que corresponde al RAND’. Pero de nuevo, AES (Ek) es una permutación de manera que las *entradas* deben ser iguales, es decir RAND = RAND’. (El hecho de que AES es dependiente de K no ayuda dado que se supone un UE fijo y de esta manera el mismo K ocurrirá en ambos casos.)

En otras palabras, se ha mostrado que (CK || IK, RAND || IMPI) = (CK’ || IK’, RAND’|| IMPI) si y sólo sí RAND = RAND’. En el caso de SAE/LTE, el PLMN_ID también puede incluir las entradas, pero dado que es altamente probable que el UE permanezca en la misma red varias veces, no se puede confiar en este parámetro PLMN_ID para el propósito de garantizar la unicidad.

Un planteamiento alternativo para intentar evitar una colisión podría ser usar otro algoritmo distinto del AES para el procesamiento criptográfico de los algoritmos f3 y f4. Específicamente, el análisis anterior estaba basado en el hecho de que el AES es una permutación. Por lo tanto sería posible usar una no permutación (asignación de muchos a uno) en lugar de AES. Esto es problemático por dos razones. Primero de todo, se deben adaptar los USIM existentes para ser adecuados para la arquitectura SAE del 3GPP. En segundo lugar, eligiendo una función de no permutación, uno realmente aumenta la probabilidad de que dos salidas de por ejemplo f3 colisionen.

La carencia de unicidad de las entradas puede ser un problema de seguridad serio. Dado que la colisión ocurrirá si y sólo sí RAND = RAND’, y dado que RAND es de 128 bits, la colisión se espera que ocurra después de cerca de 2^(128/2) = 2^64 autenticaciones (esta es la denominada “paradoja del cumpleaños”). Claramente, este es menor que el nivel de seguridad objetivo de GBA (que es de 128 bits). Para LTE el caso es incluso peor, dado que LTE se requiere que proporcione un nivel de seguridad de 256 bits. De esta manera, la alta probabilidad de colisión es un obstáculo significativo para proporcionar el nivel de seguridad requerido en SAE/LTE.

**Compendio**

Por consiguiente, hay una necesidad de una solución que evite las colisiones mencionadas anteriormente. La solución también debería trabajar idealmente con USIM ya desplegados y no requerir la sustitución de todos los USIM.

Según un primer aspecto, se proporciona un método para generar una clave criptográfica. La clave criptográfica se usa para, entre otras cosas, proteger una comunicación entre dos entidades. El método se lleva a cabo por la primera entidad. El método forma parte de una operación de seguridad distribuida tal como un procedimiento de Autenticación y Acuerdo de Claves (AKA) en base a un protocolo AKA que se inicia por la segunda entidad. El método comprende proporcionar al menos dos parámetros, que como un todo se pueden ver como una entrada que va a ser proporcionada a una función de derivación de clave, en la que el primer parámetro o bien comprende o bien se deriva de un conjunto de claves criptográficas que se han calculado por la primera entidad ejecutando la operación de seguridad y en la que el segundo parámetro o bien comprende o bien se deriva de un testigo calculado por una segunda entidad ejecutando la operación de seguridad para la primera entidad. El método además comprende aplicar o realizar, la función de derivación de clave para generar la clave criptográfica en base a la entrada proporcionada. El testigo o bien comprende o bien se deriva de un Número de Secuencia (SQN) que indica el número de veces que la operación de seguridad se ha iniciado por la segundo entidad para la primera entidad. Además, la entrada, que comprende los dos parámetros como un todo, es única cada vez que la operación de seguridad se inicia por la segunda entidad para la primera entidad.

La expresión “un parámetro comprende X” puede significar que la variable X, en su formato de cadena, forma el parámetro o parte del mismo. La expresión “un parámetro se deriva de X” puede significar que el parámetro es el resultado de aplicar ciertas funciones, tales como funciones matemáticas, a al menos una variable X. Ejemplos de las funciones incluyen, pero no se limitan a, operaciones aritméticas, operaciones lógicas, operaciones de cadena y cualquier combinación de las mismas. La operación aritmética puede ser suma, resta, multiplicación, etc. y cualquier combinación significativa de las mismas. La operación lógica puede ser AND, OR, OR Exclusiva (xOR), NOT, etc. y cualquier combinación significativa de las mismas. La operación de cadena puede ser Concatenación, Invertir, Sustituir, etc. y cualquier combinación significativa de las mismas. Además, la operación aritmética, la operación lógica y la operación de cadena se pueden combinar.

El testigo puede tomar muchas formas. En un caso, el SQN en sí mismo puede ser el testigo. Alternativamente, el testigo se puede derivar del SQN usando un algoritmo que implica ciertas operaciones matemáticas, tales como al menos una de una operación matemática, una operación lógica y una operación de cadena. Por ejemplo, el testigo puede comprender o se puede derivar de un Testigo de Autenticación (AUTN) construido por la segunda entidad en base al SQN y entregado a la primera entidad. Esta construcción y entrega puede ser parte de la operación de seguridad. Específicamente, el testigo puede comprender una OR exclusiva del SQN y una Clave de Anonimato (AK). La Clave de Anonimato puede ser una clave criptográfica producida por una función de generación de claves, tal como la función f5 que usa un desafío aleatorio conforme al protocolo AKA.

Más específicamente, el testigo puede ser una concatenación de la OR exclusiva del SQN y la Clave de Anonimato, un Campo de Autenticación y Gestión de Claves (AMF) y un Código de Autenticación de Mensajes (MAC). Esta concatenación se puede expresar como

**testigo = AUTN = (SQN xOR AK) || AMF || MAC**

o

**testigo = función (AUTN) = función ((SQN xOR AK) || AMF || MAC).**

El segundo parámetro puede comprender además o se puede derivar del desafío aleatorio o código aleatorio (RAND). El RAND se puede generar por la segunda entidad y entregar a la primera entidad como parte de la operación de seguridad. El segundo parámetro aún puede comprender además o se puede derivar de un identificador asociado con la primera entidad. Por lo tanto, el segundo parámetro puede ser una concatenación de la OR exclusiva de un desafío aleatorio (RAND), un identificador asociado con la primera entidad y el testigo.

El identificador asociado con la primera entidad puede comprender o se puede derivar de un identificador de la primera entidad. Ejemplos del identificador de la primera entidad incluyen la Identidad de Usuario Privado (IMPI) o la Identidad de Abonado Móvil Internacional (IMSI) de la primera entidad. Alternativamente, el identificador asociado con la primera entidad puede comprender o se puede derivar de un identificador de una red de comunicaciones asociada con la primera entidad. Un ejemplo de tal red de comunicaciones es una red de servicio de la primera entidad. El identificador de la red de comunicaciones puede ser un Identificador de Red Pública Móvil Terrestre (PLMN_ID).

Específicamente, el segundo parámetro puede comprender o se puede derivar de una concatenación de 0x02, un PLMN_ID, un RAND, una IMPI o IMSI y el testigo. Esto se podría expresar como

**0x02 || PLMN_ID || RAND || IMPI || testigo.**

Cuando el testigo es el SQN en sí mismo, lo anterior llega a ser

**0x02 || PLMN_ID || RAND || IMPI || SQN;**

y cuando el testigo es el AUTN, lo anterior llega a ser

**0x02 || PLMN_ID || RAND || IMPI || AUTN.**

Con respecto al primer parámetro usado en el método, este parámetro puede comprender o se puede derivar de un conjunto de claves criptográficas que se han obtenido por la primera entidad ejecutando la operación de seguridad. El conjunto de claves criptográficas puede comprender o se puede derivar de una Clave de Cifrado (CK) y una Clave de Integridad (IK).

La CK y la IK pueden ser la clave de cifrado y la clave de integridad calculadas por la primera entidad en base a un AUTN y un RAND. El AUTN y el RAND se pueden entregar desde la segunda entidad. Este cálculo, así como la entrega del AUTN y del RAND puede formar partes de la operación de seguridad.

En una implementación, el primer parámetro puede comprender o se puede derivar de una concatenación de la CK y la IK. Esto se puede expresar matemáticamente como

**CK || IK.**

El método descrito en la presente memoria genera una clave criptográfica. Esta clave se puede compartir al menos por la primera entidad y la segunda entidad, en cualquier comunicación posterior entre las mismas. En ciertas implementaciones, esta clave puede ser una $K_{ASME}$ a la que se refiere en la "jerarquía de claves" de la Fig. 2, la cual se puede compartir por la primera entidad y una Entidad de Gestión de Seguridad de Acceso (ASME) de la segunda entidad.

El método se puede extender para comprender la aplicación de una o más funciones de derivación de claves adicionales; por ello, se pueden generar claves más criptográficas. Tal generación se basa en o hace uso de, la clave criptográfica generada en el método básico, no extendido descrito anteriormente, por ejemplo, la $K_{ASME}$.

Las claves criptográficas generadas por el método extendido pueden incluir al menos una de un conjunto de claves criptográficas para proteger el tráfico de Estrato de No Acceso (NAS); un conjunto de claves criptográficas para la protección del tráfico de Control de Recursos Radio (RRC); un conjunto de claves criptográficas para la protección del tráfico de Plano de Usuario (UP); y una clave criptográfica intermedia, tal como una $K_{eNB}$, para derivar las claves criptográficas para proteger el tráfico RRC y/o las claves criptográficas para proteger el tráfico UP. Para una comprensión más fácil de estas claves, se hace referencia a la Fig. 2 que ilustra la jerarquía de claves usada en SAE/LTE.

Específicamente, el conjunto de claves criptográficas para proteger el tráfico NAS puede comprender una clave para proteger el tráfico NAS con un algoritmo de cifrado ($K_{NASenc}$) y/u otra clave para proteger el tráfico NAS con un algoritmo de integridad ($K_{NASint}$). De manera similar, el conjunto de claves criptográficas para la protección del tráfico RRC puede comprender una clave para proteger el tráfico RRC con un algoritmo de cifrado ($K_{RRCenc}$) y/u otra clave para proteger el tráfico RRC con un algoritmo de integridad ($K_{RRCint}$). Además, el conjunto de claves criptográficas para la protección del tráfico UP puede comprender una clave para proteger el tráfico UP con un algoritmo de cifrado ($K_{UPenc}$).

Para la técnica descrita en la presente memoria, la "primera entidad" puede ser un equipo de usuario, tal como una estación móvil. La "segunda entidad" puede ser una entidad situada dentro de una red de comunicaciones, por lo tanto, una "entidad de red". Particularmente, la segunda entidad se puede situar en una red SAE/LTE.

La segunda entidad puede comprender un Centro de Autentificación (AuC)/Servidor Local de Abonado (HSS) y una Entidad de Gestión de Movilidad (MME). La MME puede ser responsable de la iniciación de la operación de seguridad para la primera entidad. Las claves criptográficas generadas se pueden generar por el AuC/HSS y se pueden compartir por la primera entidad y la MME. El AuC/HSS puede aumentar el SQN, particularmente cada vez que se inicia la operación de seguridad para la primera entidad. Además, el AuC/HSS también puede construir el AUTN en base al SQN.

La operación de seguridad referida en la presente memoria se puede realizar por la primera y segunda entidades de una manera cooperativa. Por ejemplo, la operación de seguridad se puede basar en un procedimiento AKA, tal como el protocolo de AKA.

La función de derivación de claves referida por el método puede ser una función de derivación de claves de Arquitectura de Inicialización Genérica (GBA). Una función de derivación de claves de Arquitectura de Inicialización Genérica puede emplear una función de generación de claves de Algoritmo de Generación de Claves Seguras (SHA). En particular, se puede emplear una función de generación de claves de Algoritmo de Generación de Claves Seguras con un resumen de una longitud de 256 bits (SHA-256).

Según otro aspecto, se proporciona un producto de programa de ordenador. El producto de programa de ordenador comprende partes de código de programa para realizar los pasos del método descritos en la presente memoria cuando el producto de programa de ordenador se ejecuta en un sistema informático para un dispositivo informático. El producto de programa de ordenador se puede almacenar en un medio de notificación legible por ordenador.

Según otro aspecto, se proporciona un producto de programa de ordenador. El producto de programa de ordenador comprende partes de código de programa para realizar los pasos del método descritos en la presente memoria cuando el producto de programa de ordenador se ejecuta en un sistema informático para un dispositivo informático. El producto de programa de ordenador se puede almacenar en un medio de notificación legible por ordenador.

En general, la solución se puede poner en práctica por medio de un planteamiento hardware, software o hardware/software combinado.

En cuanto a una realización hardware, se proporciona un dispositivo adaptado para generar una clave criptográfica para una entidad de comunicaciones. El dispositivo se adapta para realizar una operación de seguridad, de la cual la generación de clave criptográfica puede ser una parte de la misma. Un ejemplo de la operación de seguridad es el procedimiento AKA basado en el protocolo AKA. El dispositivo comprende un primer componente adaptado para proporcionar una entrada a una función de derivación de clave, la entrada que comprende al menos dos parámetros. El primer parámetro o bien comprende o bien se deriva de un conjunto de claves criptográficas que se han calculado por la entidad de comunicaciones ejecutando la operación de seguridad y el segundo parámetro o bien comprende o se deriva de un testigo para uso por la entidad de comunicaciones, en la que el testigo comprende o se deriva de un número de secuencia (SQN) que indica el número de veces que la operación de seguridad se ha iniciado para la entidad de comunicaciones. El dispositivo además comprende un segundo componente adaptado para ejecutar la función de derivación de clave para generar la clave criptográfica en base a la entrada proporcionada. La entrada es única cada vez que la operación de seguridad se inicializa para la entidad de comunicación.

El testigo puede tomar muchas formas. En un caso, el SQN en sí mismo puede ser un testigo. Alternativamente, el testigo se puede derivar del SQN usando un algoritmo que implica ciertas operaciones matemáticas, tales como al menos una operación aritmética, una operación lógica y una operación de cadena. Por ejemplo, el testigo puede comprender o se puede derivar de un Testigo de Autenticación (AUTN) en base al SQN y proporcionado a la entidad de comunicaciones. Esta formación y entrega de testigo puede ser parte de la operación de seguridad. Específicamente, el testigo puede comprender una OR exclusiva del SQN y una Clave de Anonimato (AK). La Clave de Anonimato puede ser una clave criptográfica producida por una función de generación de clave, tal como la función f5 que usa un desafío aleatorio conforme al protocolo AKA.

Por ejemplo, el testigo puede ser una concatenación de la OR exclusiva del SQN y una Clave de Anonimato (AK), un Campo de Autentificación y Gestión de Claves (AMF) y un Código de Autentificación de Mensajes (MAC). Específicamente, esto se puede expresar como

**testigo = AUTN = (SQN xOR AK) || AMF || MAC.**

El segundo parámetro además puede comprender o se puede derivar del desafío aleatorio o código aleatorio (RAND). El RAND se puede proporcionar a la entidad de comunicaciones como parte de la operación de seguridad. El segundo parámetro aún además puede comprender o se puede derivar de un identificador asociado con la entidad de comunicaciones. En este caso, el identificador puede comprender o se puede derivar de un identificador de la entidad de comunicaciones tal como una Identidad de Usuario Privado (IMPI) o una Identidad de Abonado Móvil Internacional (IMSI) de la otra entidad de comunicaciones. Alternativamente, el segundo parámetro aún además puede comprender o se puede derivar de un identificador de una red de comunicaciones asociada con la entidad de comunicaciones, particularmente una red de servicio de la entidad de comunicaciones. Este identificador de la red de comunicaciones puede ser un Identificador de Red Pública Móvil Terrestre (PLMN_ID).

Un ejemplo particular del segundo parámetro puede comprender o se puede derivar de una concatenación de 0x02, un PLMN_ID, un RAND, una IMPI o una IMSI y el testigo. Por ejemplo, el segundo parámetro se puede expresar como

**0x02 || PLMN_ID || RAND || IMPI || testigo.**

Cuando el testigo es el SQN, lo anterior llega a ser

**0x02 || PLMN_ID || RAND || IMPI || SQN;**

y cuando el testigo es el AUTN, lo anterior llega a ser

**0x02 || PLMN_ID || RAND || IMPI || AUTN.**

Como se mencionó anteriormente, el primer parámetro puede comprender o se puede derivar de un conjunto de claves criptográficas. Particularmente, este conjunto de claves criptográficas puede comprender una Clave de Cifrado (CK) y una Clave de Integridad (IK) que han sido calculadas por la entidad de comunicaciones como parte

de la operación de seguridad. Alternativamente, el conjunto de claves criptográficas se puede derivar de la Clave de Cifrado y la Clave de Integridad.

Como una implementación particular, el primer parámetro puede comprender o se puede derivar de una concatenación de la CK y la IK, que se puede expresar como

**CK || IK.**

El dispositivo puede generar no solamente la clave criptográfica en base al primer y segundo parámetros proporcionados, sino también más claves criptográficas en base a la clave criptográfica generada. Al hacerlo así, el dispositivo se puede adaptar para aplicar una o más funciones de derivación de claves adicionales para generar las más claves criptográficas en base a la clave criptográfica que se ha generado.

Estas “más claves criptográficas” pueden comprender al menos una de un conjunto de claves criptográficas para la protección de tráfico de Estrato de No Acceso (NAS), un conjunto de claves criptográficas para la protección de tráfico de Control de Recursos Radio (RRC), un conjunto de claves criptográficas para la protección de tráfico del Plano de Usuario (UP) y una clave criptográfica intermedia $K_{eNB}$ para derivar las claves criptográficas para la protección del tráfico de RRC y/o las claves criptográficas para la protección del tráfico UP.

La entidad de comunicaciones referida anteriormente puede ser un equipo de usuario, tal como una estación móvil (por ejemplo, un teléfono móvil o una tarjeta de red).

Según un aspecto adicional, se proporciona un equipo de usuario que comprende el dispositivo presentado anteriormente. El equipo de usuario puede ser una estación móvil.

Según aún un aspecto adicional, se proporciona un sistema que comprende el equipo de usuario mencionado anteriormente. El sistema también comprende una entidad de red. La entidad de red se puede usar dentro de una red SAE/LTE. La entidad de red puede comprender un AuC/HSS y una MME. La MME puede ser responsable de inicializar la operación de seguridad para el equipo de usuario. El AuC/HSS puede generar la clave criptográfica. Las claves criptográficas generadas se pueden compartir por el equipo de usuario y la MME. El AuC/HSS puede aumentar el SQN, particularmente cada vez que la operación de seguridad se inicializa para el equipo de usuario. Además, el AuC/HSS también puede construir el AUTN en base al SQN.

Según un aspecto adicional, se proporciona un método para generar una clave criptográfica. La clave criptográfica se usa para, entre otros, proteger la comunicación entre dos entidades. El método se lleva a cabo por la primera entidad. El método forma parte de una operación de seguridad distribuida que se inicia por la segunda entidad. El método comprende proporcionar al menos dos parámetros, en donde el primer parámetro o bien comprende o bien se deriva de un conjunto de claves criptográficas que se han calculado por la primera entidad ejecutando la operación de seguridad; y el segundo parámetro o bien comprende o bien se deriva de un testigo que tiene un valor diferente cada vez que se inicia la operación de seguridad por la segunda entidad para la primera entidad (en otras palabras, el valor del testigo nunca es el mismo para cualesquiera dos operaciones de seguridad); y aplicando una función de derivación de claves para generar una clave criptográfica basada en los parámetros proporcionados.

La expresión “un parámetro comprende X” puede significar que la variable X, en su formato de cadena, forma el parámetro o parte del mismo. La expresión “un parámetro se deriva de X” puede significar que el parámetro es el resultado de aplicar ciertas funciones, tales como funciones matemáticas, a al menos la variable X. Ejemplos de funciones incluyen, pero no se limitan a, operaciones aritméticas, operaciones lógicas, operaciones de cadena, y cualquier combinación de las mismas. La operación aritmética puede ser suma, resta, multiplicación, et., y cualesquiera combinaciones significativas de las mismas. La operación lógica puede ser Y, O, O Exclusiva (xOR), NO, etc., y cualesquiera combinaciones significativas de las mismas. La operación de cadena puede ser Concatenación, Inversión, Sustitución, etc., y cualesquiera combinaciones significativas de las mismas. Además, se pueden combinar la operación aritmética, la operación lógica y la operación de cadena.

Particularmente, el testigo mencionado anteriormente puede comprender o ser derivado de un número de secuencia (SQN) que indica el número de veces que la operación de seguridad se ha iniciado por la segunda entidad para la primera entidad. Con cada iniciación, se puede aumentar el SQN por la segunda entidad. Este mecanismo asegura que el testigo tiene un valor diferente para cada operación de seguridad iniciada.

El testigo puede tomar muchas formas. En un caso, el SQN en sí mismo puede ser el testigo. Alternativamente, el testigo se puede derivar del SQN usando un algoritmo que implica ciertas operaciones matemáticas, tales como al menos una de una operación aritmética, una operación lógica y una operación de cadena. Por ejemplo, el testigo puede comprender o ser derivado de un Testigo de Autentificación (AUTN) construido por la segunda entidad en base al SQN y entregado a la primera entidad. Esta construcción y entrega puede ser parte de la operación de seguridad.

Específicamente, el testigo puede comprender una O exclusiva del SQN y una Clave de Anonimato (AK). Más específicamente, el testigo puede ser una concatenación de la O exclusiva del SQN y la Clave de Anonimato (AK),

un Campo de Autentificación y Gestión de Claves (AMF), y un Código de Autentificación de Mensajes (MAC). Esta concatenación se puede expresar como

**testigo = AUTN = (SQN xOR AK) || AMF || MAC**

o

**testigo = función (AUTN) = función ((SQN xOR AK) || AMF || MAC)**

El segundo parámetro puede comprender además o ser derivado de un desafío aleatorio, o código aleatorio (RAND). El RAND se puede generar por la segunda entidad y entregar a la primera entidad como parte de la operación de seguridad. El segundo parámetro puede además comprender aún o ser derivado de un identificador de la primera entidad. Este identificador puede ser una Identidad de Usuario Privado (IMPI) o una Identidad Internacional de Abonado Móvil (IMSI). Incluso además, el segundo parámetro puede comprender o ser derivado de un identificador de red de comunicaciones y particularmente la red de servicio de la primera entidad. Por ejemplo, este identificador podría ser un Identificador Publico de Red Móvil Terrestre (PLMN_ID).

Específicamente, el segundo parámetro puede comprender o ser derivado de una concatenación de 0x02, un PLMN_ID, un RAND, un IMPI o IMSI, y el testigo. Esto se podría expresar como

**0x02 || PLMN_ID || RAND || IMPI || testigo.**

Cuando el testigo es el SQN en sí mismo, lo anterior llega a ser

**0x02 || PLMN_ID || RAND || IMPI || SQN;**

y cuando el testigo es el AUTN, lo anterior llega a ser

**0x02 || PLMN_ID || RAND || IMPI || AUTN.**

Con respecto al primer parámetro usado en el método, este parámetro comprende o se deriva de un conjunto de claves criptográficas que se han obtenido por la primera entidad ejecutando la operación de seguridad. El conjunto de claves criptográficas puede comprender o ser derivado de una Clave de Cifrado (CK) y una Clave de Integridad (IK).

La CK e IK pueden ser la clave de cifrado y la clave de integridad calculada por la primera entidad en base a un AUTN y un RAND. El AUTN y el RAND se pueden entregar desde la segunda entidad. Este cálculo así como la entrega del AUTN y del RAND puede formar parte de la operación de seguridad.

En una implementación, el primer parámetro puede comprender o ser derivado de una concatenación del CK e IK. Esto se puede expresar matemáticamente como

**CK || IK.**

El método descrito en la presente memoria genera una clave criptográfica. Esta clave puede ser compartida al menos por la primera entidad y la segunda entidad, en cualquier comunicación posterior entre los dos. En ciertas implementaciones, esta clave puede ser una $K_{ASME}$ a la que se refiere en la “jerarquía de claves” de la Fig. 2, la cual puede ser compartida por la primera entidad y una Entidad de Gestión de Seguridad de Acceso (ASME) de la segunda entidad.

El método se puede extender para comprender la aplicación de una o más funciones de derivación de claves adicionales para generar claves más criptográficas. Tal generación se basa en, o hace uso de, la clave criptográfica generada en el método básico, no extendido descrito anteriormente, por ejemplo la $K_{ASME}$.

Las claves criptográficas generadas por el método extendido pueden incluir al menos una de un conjunto de claves criptográficas para proteger el tráfico de Estrato de No Acceso (NAS); un conjunto de claves criptográficas para la protección del tráfico de Control de Recursos Radio (RRC); un conjunto de claves criptográficas para la protección del tráfico de Plano de Usuario (UP); y una clave criptográfica intermedia, tal como una $K_{eNB}$, para derivar las claves criptográficas para proteger el tráfico RRC y/o las claves criptográficas para proteger el tráfico UP. Para una comprensión más fácil de estas claves, se hace referencia a la Fig. 2 que ilustra la jerarquía de claves usada en SAE/LTE.

Específicamente, el conjunto de claves criptográficas para proteger el tráfico NAS puede comprender una clave para proteger el tráfico NAS con un algoritmo de cifrado ($K_{NASenc}$) y/u otra clave para proteger el tráfico NAS con un algoritmo de integridad ($K_{NASint}$). De manera similar, el conjunto de claves criptográficas para la protección del tráfico RRC puede comprender una clave para proteger el tráfico RRC con un algoritmo de cifrado ($K_{RRCenc}$) y/u otra clave para proteger el tráfico RRC con un algoritmo de integridad ($K_{RRCint}$). Además, el conjunto de claves criptográficas para la protección del tráfico UP puede comprender una clave para proteger el tráfico UP con un algoritmo de cifrado ($K_{UPenc}$).

Para la técnica descrita en la presente memoria, la “primera entidad” puede ser un equipo de usuario, tal como una estación móvil. La “segunda entidad” puede ser una entidad situada dentro de una red de comunicaciones, por lo tanto una “entidad de red”. Particularmente, la segunda entidad se puede situar en una red SAE/LTE.

La segunda entidad puede comprender un Centro de Autentificación (AuC)/Servidor de Abonado Residencial (HSS) y una Entidad de Gestión de Movilidad (MME). La MME puede ser responsable de la iniciación de la operación de seguridad. Las claves criptográficas generadas se pueden generar por el AuC/HSS y ser compartidas por la primera entidad y la MME. El AuC/HSS puede aumentar el SQN, particularmente cada vez que se inicia la operación de seguridad para la primera entidad. Además, el AuC/HSS también puede construir la AUTN en base al SQN.

La operación de seguridad referida en la presente memoria se puede realizar por la primera y segunda entidades de una manera cooperativa. Por ejemplo, la operación de seguridad se puede basar en un procedimiento de AKA, tal como el protocolo de AKA de UMTS.

La función de derivación de claves referida por el método puede ser una función de derivación de claves de Arquitectura de Inicialización Genérica (GBA). Una función de derivación de claves de Arquitectura de Inicialización Genérica puede emplear una función de generación de claves de Algoritmo de Generación de Claves Seguras (SHA). En particular, se puede emplear una función de generación de claves de Algoritmo de Generación de Claves Seguras con un resumen de una longitud de 256 bits (SHA-256).

Según un aspecto adicional, se proporciona un producto de programa de ordenador. El producto de programa de ordenador comprende partes de código de programa para realizar los pasos del método descritos en la presente memoria cuando el producto de programa de ordenador se ejecuta en un sistema informático para un dispositivo informático. El producto de programa de ordenador se puede almacenar en un medio de notificación legible por ordenador.

En general, la solución se puede poner en práctica por medio de un planteamiento de componentes físicos, soporte lógico, o componentes físicos/soporte lógico combinados.

Como para una realización de componentes físicos adicional, se proporciona un dispositivo adaptado para generar una clave criptográfica para una entidad de comunicaciones. El dispositivo puede realizar una operación de seguridad, de la cual la generación de clave criptográfica puede ser parte de la misma. El dispositivo comprende un primer componente adaptado para proporcionar al menos dos parámetros, en donde el primer parámetro puede comprender o ser derivado de un conjunto de claves criptográficas que se han calculado por la entidad de comunicaciones mediante la ejecución de la operación de seguridad, y el segundo parámetro puede comprender o ser derivado de un testigo que tiene un valor diferente cada vez que la operación de seguridad se inicializa para la entidad de comunicaciones. El dispositivo además comprende un segundo componente adaptado para ejecutar una función de derivación de claves para generar una clave criptográfica en base a los parámetros proporcionados.

Como se dijo anteriormente, el testigo puede tomar muchas formas posibles. El testigo puede comprender o ser derivado de un SQN que indica el número de veces que la operación de seguridad se ha iniciado para la entidad de comunicaciones. En una implementación, el SQN en sí mismo es el testigo. Alternativamente, el testigo se puede derivar del SQN usando un algoritmo que implica al menos una de una operación aritmética, una operación lógica y una operación de cadena. Por ejemplo, el testigo puede comprender o ser derivado de un AUTN que se construye en base al SQN y entrega a la entidad de comunicaciones, en donde esta construcción y entrega forma parte de la operación de seguridad. Por ejemplo, el testigo puede ser una concatenación de O exclusiva del SQN y una Clave de Anonimato (AK), un Campo de Autentificación y Gestión de Claves (AMF), y un Código de Autentificación de Mensajes (MAC). Específicamente, esto se puede expresar como

**testigo = AUTN = (SQN xOR AK) || AMF || MAC.**

Además del testigo, el segundo parámetro también puede comprender o ser derivado de un RAND. El RAND se puede entregar a la entidad de comunicaciones como parte de la operación de seguridad. Además, el segundo parámetro puede comprender o ser derivado de un identificador de la entidad de comunicaciones. Un ejemplo del identificador es una Identidad de Usuario Privado (IMPI) de la entidad de comunicaciones. Incluso además, el segundo parámetro puede comprender o ser derivado de un identificador de la red de servicio de la entidad de comunicaciones. Este identificador podría ser un Identificador Público de Red Móvil Terrestre (PLMN_ID).

Un ejemplo particular del segundo parámetro puede comprender o ser derivado de una concatenación de 0x02, un PLMN_ID, un RAND, un IMPI o un IMSI, y el testigo. Por ejemplo, el segundo parámetro se puede expresar como

**0x02 || PLMN_ID || RAND || IMPI || testigo.**

Cuando el testigo es el SQN, lo anterior llega a ser

**0x02 || PLMN_ID || RAND || IMPI || SQN;**

y cuando el testigo es el AUTN, lo anterior llega a ser

**0x02 || PLMN_ID || RAND || IMPI || AUTN.**

Como se mencionó anteriormente, el primer parámetro puede comprender o ser derivado de un conjunto de claves criptográficas. Particularmente, este conjunto de claves criptográficas puede comprender una Clave de Cifrado (CK) y una Clave de Integridad (IK) que ha sido calculada por la entidad de comunicaciones como parte de la operación de seguridad. Alternativamente, el conjunto de claves criptográficas se puede derivar de la Clave de Cifrado y la Clave de Integridad.

Como una implementación particular, el primer parámetro puede comprender o ser derivado de una concatenación de la CK e IK, que se puede expresar como

**CK || IK.**

El dispositivo puede generar no solamente la clave criptográfica en base al primer y segundo parámetros proporcionados, sino también claves más criptográficas en base a la clave criptográfica generada. Al hacerlo así, el dispositivo se puede adaptar para aplicar una o más funciones de derivación de claves adicionales para generar las claves más criptográficas en base a la clave criptográfica que se ha generado.

Estas “claves más criptográficas” pueden comprender al menos una de un conjunto de claves criptográficas para la protección de tráfico de Estrato de No Acceso (NAS), un conjunto de claves criptográficas para la protección del tráfico de Control de Recursos Radio (RRC), un conjunto de claves criptográficas para la protección del tráfico del Plano de Usuario (UP), y una clave criptográfica intermedia $K_{eNB}$ para derivar las claves criptográficas para la protección del tráfico de RRC y/o las claves criptográficas para la protección del tráfico UP.

La entidad de comunicaciones referido anteriormente puede ser un equipo de usuario, tal como una estación móvil (por ejemplo, un teléfono móvil o una tarjeta de red).

Según un aspecto adicional, se proporciona un equipo de usuario que comprende el dispositivo presentado anteriormente. El equipo de usuario puede ser una estación móvil.

Según aún un aspecto adicional, se proporciona un sistema que comprende el equipo de usuario mencionado anteriormente. El sistema también comprende una entidad de red. La entidad de red se puede usar para una red SAE/LTE. La entidad de red puede comprender un AuC/HSS y una MME. La MME puede ser responsable de iniciar la operación de seguridad para el equipo de usuario. El AuC/HSS puede generar la clave criptográfica. Las claves criptográficas generadas se pueden compartir por el equipo de usuario y la MME. El AuC/HSS puede aumentar el SQN, particularmente cada vez que la operación de seguridad se inicia para el equipo de usuario. Además, el AuC/HSS también puede construir el AUTN en base al SQN.

**Breve descripción de los dibujos**

A continuación, la técnica de generación de claves criptográficas se describirá con referencia a las realizaciones ejemplares ilustradas en los dibujos, en donde:

La Fig. 1 es un diagrama que muestra el concepto básico del protocolo AKA de UMTS;

La Fig. 2 es un diagrama de bloques que ilustra una jerarquía de claves propuesta para el sistema SAE/LTE;

La Fig. 3 es un diagrama de bloques que muestra una realización del dispositivo;

La Fig. 4 es un diagrama de bloques que muestra una realización del sistema;

La Fig. 5 es un diagrama de bloques que muestra una realización del método;

La Fig. 6 es un diagrama de bloques que muestra un procedimiento de la operación de AKA de UMTS, Generación de un Vector de Autentificación por una entidad de red;

La Fig. 7 es un diagrama de bloques que muestra otro procedimiento de la operación de AKA de UMTS, Autentificación y Establecimiento de Claves;

La Fig. 8 es un diagrama de bloques que muestra la función de autentificación general realizada por el UE como parte de la operación de AKA de UMTS;

La Fig. 9 es un diagrama de bloques que muestra un algoritmo criptográfico particular para realizar la función de autentificación anterior en el UE; y

La Fig. 10 es un diagrama de bloques que muestra un detalle particular del algoritmo criptográfico anterior.

**Descripción detallada**

En la siguiente descripción, para propósitos de explicación y no de limitación, se fijan en adelante detalles específicos, tales como secuencias particulares de pasos, interfaces y configuraciones, para proporcionar una minuciosa comprensión de la técnica de generación de claves criptográficas. Será evidente a aquellos expertos en la técnica que la técnica se puede poner en práctica en otras realizaciones que se salen de estos detalles específicos. Por ejemplo, mientras que la técnica se describirá en primer lugar en contexto con el protocolo de AKA de UMTS y en el entorno de red SAE/LTE, será evidente para las personas expertas que la técnica también se puede poner en práctica en conexión con otros protocolos, arquitecturas, o entornos de seguridad.

Además, aquellos expertos en la técnica apreciarán que las funciones explicadas en la presente memoria más adelante se pueden implementar usando soporte lógico que funciona en conjunto con un microprocesador u ordenador de propósito general programado. También se apreciará que mientras que la técnica se describe en primer lugar en forma de métodos y dispositivos, la técnica también se puede realizar en un producto de programa de ordenador así como en un sistema que comprende un procesador de ordenador y una memoria acoplada al procesador, en donde la memoria se codifica con uno o más programas que pueden realizar la función descrita en la presente memoria.

La Fig. 3 muestra una realización de un dispositivo 100 adaptado para generar una clave criptográfica para una entidad de comunicaciones (no mostrada en la Fig. 3). La entidad de comunicaciones está adaptada para ejecutar una operación de seguridad. El dispositivo 100 comprende un primer componente 102 y un segundo componente 104. El primer componente 102 está adaptado para proporcionar al menos dos parámetros, figuradamente mostrados en las fechas 106 y 108.

El primer parámetro 106 comprende o se deriva de un conjunto de claves criptográficas 110 y 112. (Aunque se muestran dos claves en la figura, el conjunto de claves criptográficas puede incluir cualquier número de claves.) El conjunto de claves criptográficas se ha calculado por la entidad de comunicaciones ejecutando la operación de seguridad. La derivación del conjunto de claves criptográficas 110 y 112 en el primer parámetro 106 se muestra figuradamente como un bloque 114. El segundo parámetro 108 comprende o se deriva de un testigo 116. El testigo 116 tiene un valor diferente cada vez que se inicia la operación de seguridad para la entidad de comunicaciones. La derivación del testigo 116 en el segundo parámetro 108 se muestra figuradamente como un bloque 118. El segundo componente 104 del dispositivo 100 está adaptado para ejecutar una función de derivación de clave para generar una clave criptográfica 120 en base a los parámetros 106 y 108 proporcionados.

Con referencia a la Fig. 4, se muestra una realización de un sistema 200 que comprende el dispositivo 100 mencionado anteriormente. El dispositivo 100 puede estar comprendido en una entidad de comunicaciones 202, que puede ser un UE, tal como una estación móvil. Por supuesto, la entidad de comunicaciones 202 puede ser cualquier tipo adecuado de entidad de comunicaciones capaz de acoger el dispositivo 100. Además, el sistema comprende una entidad de red 204, que puede residir en una red SAE/LTE. La entidad de red 204 puede comprender un AuC o HSS y una MME. También puede ser otra entidad de comunicaciones en una red SAE/LTE.

Correspondiente al dispositivo de generación de claves criptográficas 100 mostrado en las Fig. 3 y 4, un diagrama 300 que ilustra una realización de un método para generar una clave criptográfica se muestra en la Fig. 5. La clave generada se usa para proteger la comunicación entre dos entidades. La primera entidad 302 puede corresponder a la entidad de comunicaciones 202 como se muestra en la Fig. 4, y la segunda entidad 304 puede corresponder a la entidad de red 204 de la Fig. 4. La primera entidad puede ser un UE. No obstante, la realización no está limitada a un escenario de UE-entidad de red. En su lugar, se puede aplicar a cualesquiera dos entidades de comunicaciones en general.

La MME puede ser responsable de iniciar la operación de seguridad para la entidad de comunicaciones 202. Las claves criptográficas generadas se pueden compartir por la MME y la entidad de comunicaciones 202.

Particularmente, la realización del método se lleva a cabo por la primera entidad 302 como parte de una operación de seguridad ilustrada figuradamente en la fecha 300', que se inicia por la segunda entidad 304 (particularmente por la MME de la misma) para la primera entidad 302. La realización en sí misma comprende dos pasos, 306 y 308. El paso 306 proporciona al menos dos parámetros (106 y 108 de la Fig. 3). El primer parámetro comprende o se deriva de un conjunto de claves criptográficas (110 y 112 como se muestra en la Fig. 3) que se ha calculado por la primera entidad 302 ejecutando la operación de seguridad 300'. El segundo parámetro comprende o se deriva de un testigo (116 como se muestra en la Fig. 3) que tiene un valor diferente cada vez que se inicia la operación de seguridad 300' por la segunda entidad 304 para la primera entidad 302. En el segundo paso 308, una función de derivación de clave se aplica para generar una clave criptográfica (120 como se muestra en la Fig.3) en base a los parámetros proporcionados (106 y 108 como se muestra en la Fig. 3).

Más adelante, se dan detalles considerables para explicar la técnica de generación de claves criptográficas con un énfasis particular sobre cómo la técnica puede evitar con éxito la colisión de claves entre dos UE, o de manera más importante, entre dos ejecuciones distintas de la operación de seguridad para uno y el mismo UE.

La generación de claves criptográficas puede ser parte de la operación de AKA de UMTS. La AKA de UMTS está basada en la implementación que el UE, particularmente el USIM del mismo, y el AuC/HSS en el Entorno

Residencial (HE) del UE comparten una clave secreta específica de usuario K, ciertas funciones de autentificación de mensajes f1, f2 y ciertas funciones de generación de claves criptográficas f3, f4, f5. Además el USIM y el AuC/HSS hacen el seguimiento de los contadores, o números de secuencia $SQN_{UE}$ y $SQN_{HE}$ respectivamente para soportar la autentificación de red. Por ejemplo, el AuC/HSS puede aumentar el $SQN_{HE,}$ particularmente cada vez que se inicia la operación de seguridad para la primera entidad. La operación de AKA de UMTS comprende un número de procedimientos, incluyendo la Generación de Vectores de Autentificación (AV), y Autentificación y Establecimiento de Claves.

El propósito del procedimiento de AV es proporcionar el SN/VLR (o MME) con un grupo de AV nuevos del HE del UE para realizar un número de autentificaciones de usuario. La Generación de Vectores de Autentificación por el HE se ilustra en la Fig. 6. Con referencia a esta figura, tras la recepción de una petición desde el SN/VLR, el AuC/HSS envía un grupo ordenado de n Vectores de Autentificación AV (1…n) al SN/VLR. Cada AV comprende un número aleatorio (o desafío aleatorio) RAND, una respuesta esperada XRES, una clave de cifrado CK, una clave de integridad IK y un testigo de autentificación AUNT.

El AuC/HSS comienza con la generación de un número de secuencia nuevo SQN y un desafío impredecible RAND. Posteriormente se calculan los siguientes valores:

- un código de autentificación de mensajes MAC = f1(SQN || RAND || AMF) donde f1 es una función de autentificación de mensajes;

- una respuesta esperada XRES = f2 (RAND) donde f2 es una función de autentificación de mensajes (posiblemente truncada);

- una clave de cifrado CK = f3 (RAND) donde f3 es una función de generación de claves;

- una clave de integridad IK = f4 (RAND) donde f4 es una función de generación de claves; y

- una clave de anonimato AK = f5 (RAND) donde f5 es una función de generación de claves.

Finalmente se construye el testigo de autentificación AUTN = (SQN xOR AK) || AMF || MAC. Se puede construir por el AuC/HSS. Aquí, la AK es una clave de anonimato usada para ocultar el SQN ya que este último puede exponer la identidad y ubicación del UE. El ocultamiento del SQN es para proteger contra ataques pasivos. El uso de la AK puede ser opcional. Cuando la AK no se usa, se puede usar figuradamente en su lugar el valor AK = 000…0.

El grupo de los AV se envía de vuelta al SN/VLR solicitante en una respuesta de autentificación. Cada AV es válido para una (y sólo una) autentificación y acuerdo de claves entre el SN/VLR y el USIM.

El siguiente procedimiento de la operación de AKA de UMTS, Autentificación y Establecimiento de Claves, es autentificar y establecer mutuamente las claves de cifrado y de integridad entre el SN/VLR y el UE. Este proceso se ilustra en la Fig. 7. Con referencia a esta figura, cuando el SN/VLR inicia una autentificación y acuerdo de claves, selecciona el siguiente AV del grupo y envía los parámetros RAND y AUTN al UE. El USIM comprueba si se puede aceptar el AUTN y, en su caso, produce una respuesta RES que se envía de vuelta al SN/VLR. Particularmente, los procedimientos del UE se muestran en la Fig. 8.

Con referencia a la Fig. 8, tras la recepción del RAND y AUTN el UE primero calcula la clave de anonimato AK = f5 (RAND) (o usa AK = 000…0) y recupera el número de secuencia SQN = (SQN xOR AK) xOR AK. A continuación el UE calcula XMAC = f1 (SQN || RAND || AMF) y compara éste con el MAC que se incluye en el AUTN. Si son diferentes, el UE envía un *rechazo de autentificación de usuario* de vuelta al SN/VLR con una indicación de la causa y el UE abandona el procedimiento. De otro modo, el UE verifica que el SQN recibido está en el intervalo correcto.

Si el SQN se considera que está en el intervalo correcto, el UE calcula RES = f2 (RAND) e incluye este parámetro en una *respuesta de autentificación de usuario* de vuelta al SN/VLR. Finalmente el UE calcula la clave de cifrado CK = f3 (RAND) y la clave de integridad IK = f4 (RAND). Para mejorar la eficiencia, RES, CK e IK también se podrían calcular anteriores en cualquier momento después de recibir el RAND. El UE puede almacenar el RAND para propósitos de resincronización.

Tras la recepción de la respuesta de autentificación de usuario el SN/VLR compara la RES con la respuesta esperada XRES desde el vector de autentificación seleccionado. Si XRES es igual a RES entonces la autentificación del usuario se ha aceptado. Las claves nuevamente calculadas CK e IK entonces se transferirán por el USIM y el SN/VLR a las entidades que realizan las funciones de cifrado e integridad.

De lo anterior, se puede ver que la operación de AKA de UMTS está basada en un par (RAND, AUTN) y el AUTN comprende o se deriva de un número de secuencia, SQN, según

**AUTN = (SQN xOR AK) || AMF || MAC**

donde AK es una clave de anonimato, que se puede producir por Milenage (ver la Fig. 9) desde la salida “f5” anterior.

La función de más adelante es una primera solución al problema de colisión expuesto anteriormente:

**KDF(CK || IK, RAND || IMPI || SQN)**

donde SQN se han incluido de esta manera en las entradas. Ahora, incluso si dos RAND son el mismo, es decir, RAND = RAND', el hecho de que el SQN siempre aumente (por ejemplo, por uno) asegurará que las entradas son diferentes, únicas, o distintas.

Una solución alternativa es usar

**KDF(CK || IK, RAND || IMPI || AUTN).**

Esta solución puede ser más simple de implementar dado que el AUTN se puede usar "como está" a partir de la señalización de la AKA. No obstante, la "unicidad" de las entradas en este caso puede no ser obvia dado que

**AUTN = (SQN xOR AK) || AMF || MAC**

e incluso si SQN $\neq$ SQN', si no se puede ver inmediatamente que (SQN xOR AK), (SQN' xOR AK') serán distintos ya que la AK podría "cancelar" potencialmente las diferencias. No obstante, más adelante, la distinción de (SQN xOR AK) se puede demostrar.

Supongamos que

**(CK || IK, RAND || IMPI || AUTN) = (CK' || IK', RAND' || IMPI || AUTN').**

Ya se ha mostrado que esto implica que CK = CK', IK = IK', y RAND = RAND'. De esta manera queda por ser comprobado si podría ser que AUTN = AUTN'. Esta comprobación se puede traducir en comprobar si

**(SQN xOR AK) || AMF || MAC = (SQN' xOR AK') || AMF' || MAC'.**

Supongamos sin pérdida de generalidad que AMF = AMF' y MAC = MAC'. Entonces solamente es necesario comprobar si lo siguiente podría mantener:

**SQN xOR AK = SQN' xOR AK'.**

Recordar que se espera que RAND = RAND'. Con referencia al algoritmo Milenage mostrado en la Fig. 9, esto implica que AK = AK' (ya que se produjeron a partir de los mismos RAND). De esta manera, tenía que ser que

**SQN = SQN',**

que es una contradicción dado que, como ya se señaló, SQN siempre "intensifica" y de esta manera SQN $\neq$ SQN'.

De esta manera, se demuestra que la segunda solución también garantiza la unicidad de las entradas a la función KDF.

Como solución general, en lugar de usar SQN o AUTN para lograr la unicidad, es factible cualquier testigo que tiene un valor diferente cada vez que la operación de AKA de UMTS se inicia por la red para el UE. Por ejemplo, SQN xOR AK (que forma parte del AUTN) se puede usar dado que tiene (mediante el análisis anterior) la propiedad de unicidad requerida.

La técnica de generación de claves criptográficas descrita aquí anteriormente presenta numerosas ventajas. Por ejemplo, garantiza la unicidad de las entradas de KDF. Por lo tanto, evita con éxito los encargos provocados por posibles entradas idénticas. Con esta técnica, la clave criptográfica generada será capaz de cumplir, por ejemplo, los requisitos de alto nivel de seguridad en los sistemas SAE/LTE. Como una ventaja adicional, la técnica se puede implementar en base a los USIM ya desplegados sin requerir alguna sustitución del USIM. Otra ventaja específica con el uso del AUTN más que el SQN es que la invención se puede implementar en el terminal móvil (fuera del USIM).

Aunque las realizaciones de la técnica de generación de claves criptográficas se ha ilustrado en los dibujos adjuntos y descrito en una descripción anteriormente mencionada, se entenderá que la técnica no está limitada a las realizaciones descritas en la presente memoria. La técnica es capaz de numerosas readaptaciones, modificaciones y sustituciones sin salirse del alcance de la invención.

**Símbolos y abreviaturas**

Para los propósitos del presente documento, aplican los siguientes símbolos y abreviaturas:

|| Concatenación

xOR OR Exclusiva

| | |
|---|---|
| f1 | Función de autenticación de mensajes usada para calcular MAC |
| f2 | Función de autenticación de mensajes usada para calcular RES y XRES |
| f3 | Función de generación de claves usada para calcular CK |
| f4 | Función de generación de claves usada para calcular IK |
| f5 | Función de generación de claves usada para calcular AK |
| K | Clave secreta a largo plazo compartida entre el USIM y el AuC |
| 3GPP | Proyecto de Cooperación de Tercera Generación |
| AES | Estándar de Cifrado Avanzado |
| AK | Clave de Anonimato |
| AKA | Protocolo de Autenticación y Acuerdo de Claves |
| AMF | Campo de Autenticación y Gestión de Claves |
| ASME | Entidad de Gestión de Seguridad de Acceso |
| AUTN | Testigo de Autenticación |
| AV | Vector de Autenticación |
| CK | Clave de Cifrado |
| eNB | Nodo B mejorado |
| HE | Entorno Local |
| HLR | Registro de Posición Base |
| HSS | Servidor Local de Abonado |
| IK | Clave de Integridad |
| IMPI | Identidad de Usuario Privado |
| IMSI | Identidad de Abonado Móvil Internacional |
| KDF | Función de Derivación de Clave |
| LTE | Evolución a Largo Plazo |
| MAC | Código de Autenticación de Mensaje |
| MME | Entidad de Gestión de Movilidad |
| MS | Estación Base |
| MSC | Centro de Conmutación de Servicios Móviles |
| NAS | Estrato de No Acceso |
| PLMN | Red Pública Móvil Terrestre |
| RAND | Desafío aleatorio |
| RRC | Control de Recursos Radio |
| SAE | Evolución de Arquitectura de Sistema |
| SN | Red de Servicio |
| SQN | Número de secuencia |
| UE | Equipo de Usuario |
| UMTS | Sistema de Telecomunicación Móvil Universal |

| | |
|---|---|
| UP | Plano de Usuario |
| USIM | Módulo de Identidad de Abonado Universal |
| VLR | Registro de Posición Visitado |
| XRES | Respuesta Esperada |

**REIVINDICACIONES**

1. Un método para generar una clave criptográfica (120) para proteger una comunicación entre dos entidades (202, 204), en donde el método se lleva a cabo por la primera entidad (202, 302) como parte de un procedimiento de Autentificación y Acuerdo de Claves <AKA> en base a un protocolo de AKA iniciado por la segunda entidad (204, 304), en el que la primera entidad es un equipo de usuario, tal como una estación móvil, y la segunda entidad es una entidad de red de Evolución de Largo Plazo (LTE), en donde el método comprende los pasos de:

- proporcionar (306) una entrada a una función de derivación de clave, comprendiendo la entrada al menos dos parámetros (106, 108), en donde el primer parámetro (106) comprende o se deriva de un conjunto de claves criptográficas (110, 112) que se han calculado por la primera entidad (202) ejecutando el procedimiento de AKA, y el segundo parámetro se deriva de un testigo (116) calculado por la segunda entidad (204, 304) ejecutando el procedimiento de AKA para la primera entidad (202, 302); y

- aplicar (308) la función de derivación de clave para generar la clave criptográfica (120) en base a la entrada proporcionada;

en donde el testigo (116) comprende un O exclusivo de un número de secuencia <SQN> y una clave de anonimato <AK>, en donde la entrada es única cada vez que se inicia el procedimiento de AKA por la segunda entidad (204, 304) para la primera entidad (202, 302).

2. El método de la reivindicación 1, en donde la AK es una clave criptográfica producida por una función de generación de claves f5 que usa un desafío aleatorio conforme al protocolo de AKA.

3. El método de la reivindicación 2, en donde el testigo (116) es una concatenación de O exclusiva del SQN y la AK, un Campo de Autentificación y Gestión de Claves <AMF>, y un Código de Autentificación de Mensajes <MAC>.

4. El método de cualquiera de las reivindicaciones 1 a 3, en donde el segundo parámetro (108) es una concatenación de O exclusiva o un desafío aleatorio (RAND), un identificador asociado con la primera entidad (202, 302), y el testigo (116).

5. El método de la reivindicación 4, en donde el identificador asociado con la primera entidad (202, 302) comprende o se deriva de un identificador de la primera entidad, tal como una Identidad de Usuario Privado <IMPI> o una Identidad de Abonado Móvil Internacional <IMSI> de la primera entidad o el identificador asociado con la primera entidad (202, 302) comprende o se deriva de un identificador de una red de comunicaciones asociado con la primera entidad, particularmente una red de servicio de la primera entidad (202, 302).

6. El método de cualquiera de las reivindicaciones precedentes, en donde el conjunto de claves criptográficas (110, 112) comprendidas en el primer parámetro (106) o desde el que se deriva el primer parámetro (106) comprende o se deriva de una Clave de Cifrado <CK> (110) y una Clave de Integridad <IK> (112).

7. El método de cualquiera de las reivindicaciones precedentes, que además comprende el paso de:

- aplicar una o más funciones de derivación de clave adicionales para generar claves más criptográficas en base a la clave criptográfica (120) generada.

8. El método de la reivindicación 7, en donde las claves más criptográficas comprenden al menos uno de los siguientes:

- un conjunto de claves criptográficas para la protección de tráfico de Estrato de No Acceso <NAS>;

- un conjunto de claves criptográficas para la protección de tráfico de Control de Recursos Radio <RRC>;

- un conjunto de claves criptográficas para la protección de tráfico de Plano de Usuario <UP>; y

- una clave criptográfica intermedia <$K_{eNB}$> para derivar las claves criptográficas para la protección de tráfico RRC y/o las claves criptográficas para la protección de tráfico de UP.

9. El método de cualquiera de las reivindicaciones precedentes, la segunda entidad (204, 304) reside en una red de Evolución de Arquitectura de Sistema <SAE>/Evolución de Largo Plazo <LTE>.

10. El método de la reivindicación 9, en donde la segunda entidad (204, 304) comprende un Centro de Autentificación <AuC>/Servidor de Abonado Residencial <HSS> y una Entidad de Gestión de Movilidad <MME>.

11. El método de cualquiera de las reivindicaciones precedentes, en donde el procedimiento de Autentificación y acuerdo de Claves se realiza de manera cooperativa por la primera (202, 302) y segunda (204, 304) entidades.

12. El método de cualquiera de las reivindicaciones precedentes, en donde la operación de seguridad se basa en el protocolo de AKA de UMTS.

13. Un producto de programa de ordenador que comprende las partes de código de programa de ordenador para ejecutar los pasos del método según cualquiera de las reivindicaciones precedentes cuando el producto de programa de ordenador se ejecuta en un sistema informático.

14. El producto de programa de ordenador de la reivindicación 13, en donde el producto de programa de ordenador se almacena en un medio de grabación legible por ordenador.

15. Un dispositivo (100) adaptado para generar una clave criptográfica (120) para una entidad de comunicaciones móvil (202, 302) adaptada para ejecutar un procedimiento de Autentificación y Acuerdo de Claves <AKA>, siendo la entidad de comunicaciones (202, 302) un equipo de usuario, tal como una estación móvil, adaptada para cooperar con una entidad de red LTE para realizar el procedimiento de AKA, en donde el dispositivo (100) comprende:

- un primer componente (102) adaptado para proporcionar una entrada a una función de derivación de clave, comprendiendo la entrada al menos dos parámetros (106, 108), en donde el primer parámetro (106) comprende o se deriva de un conjunto de claves criptográficas (110, 112) que se han calculado por la entidad de comunicaciones (202, 302) ejecutando el procedimiento de AKA, y el segundo parámetro (108) se deriva de un testigo (116) a usar por la entidad de comunicaciones (202, 302); y

- un segundo componente (104) adaptado para ejecutar la función de derivación de clave para generar la clave criptográfica (120) en base a la entrada proporcionada;

en donde el testigo (116) comprende un O exclusivo de un número de secuencia <SQN> y una clave de anonimato <AK>; y

en donde la entrada es única cada vez que se inicia el procedimiento de AKA para la entidad de comunicaciones (202, 302).

16. El dispositivo (100) de la reivindicación 15, en donde la AK es una clave criptográfica producida por una función de generación de claves f5 que usa un desafío aleatorio conforme al protocolo de AKA.

17. El dispositivo de la reivindicación 15 o 16, en donde el testigo (116) es una concatenación de O exclusiva del SQN y la AK, un Campo de Autentificación y Gestión de Claves <AMF>, y un Código de Autentificación de Mensajes <MAC>.

18. El dispositivo de cualquiera de las reivindicaciones 15 a 17, en donde el segundo parámetro (108) es una concatenación de O exclusiva o un desafío aleatorio (RAND), un identificador asociado con la primera entidad, y el testigo (116).

19. El dispositivo de la reivindicación 18, en donde el identificador asociado con la primera entidad (202, 302) comprende o se deriva de un identificador de la primera entidad, tal como una Identidad de Usuario Privado <IMPI> o una Identidad de Abonado Móvil Internacional <IMSI> de la primera entidad o el identificador asociado con la primera entidad (202, 302) comprende o se deriva de un identificador de una red de comunicaciones asociado con la primera entidad, particularmente una red de servicio de la primera entidad (202, 302).

20. El dispositivo (100) de cualquiera de las reivindicaciones 15 a 19, en donde el conjunto de claves criptográficas (110, 112) comprendido en el primer parámetro (106) o del que se deriva el primer parámetro (106) comprende o se deriva de una Clave Cifrada <CK> (110) y una Clave de Integridad <IK> (112) calculadas por la entidad de comunicaciones (202, 302) como parte del procedimiento de AKA.

21. El dispositivo (100) de cualquiera de las reivindicaciones 15 a 20, adaptado además para aplicar una o más funciones de derivación de clave adicionales para generar claves más criptográficas en base a la clave criptográfica (120) generada.

22. Un equipo de usuario (202) que comprende el dispositivo (100) según cualquiera de las reivindicaciones 15 a 21.

23. Un sistema que comprende el equipo de usuario (202, 302) de la reivindicación 22 y una entidad de red (304) para una red de Evolución de Arquitectura de Sistema <SAE>/Evolución de Largo Plazo <LTE>.

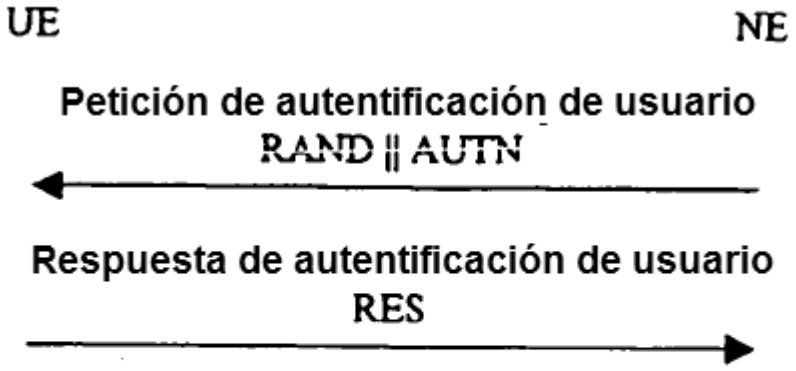
UE
NE
Petición de autentificación de usuario
RAND || AUTN
Respuesta de autentificación de usuario
RES

Fig. 1

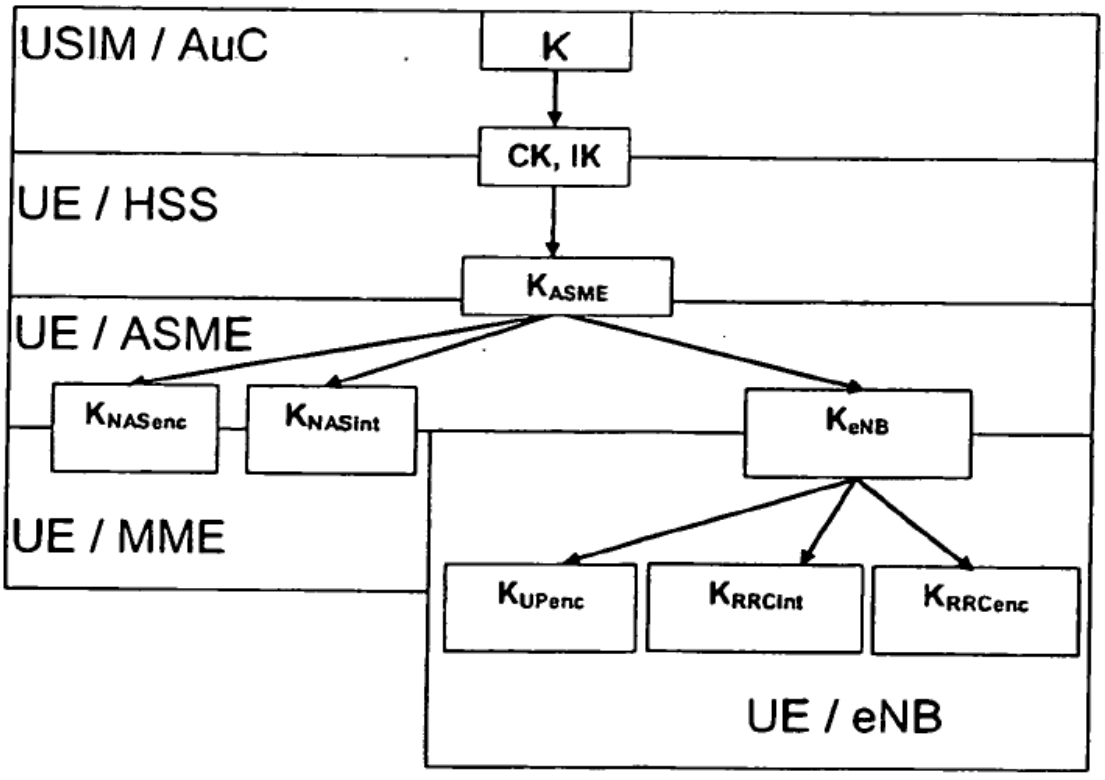
USIM / AuC
K
CK, IK
UE / HSS
KASME
UE / ASME
KNASenc
KNASint
KeNB
UE / MME
KUPenc
KRRCint
KRRCenc
UE / eNB

Fig. 2

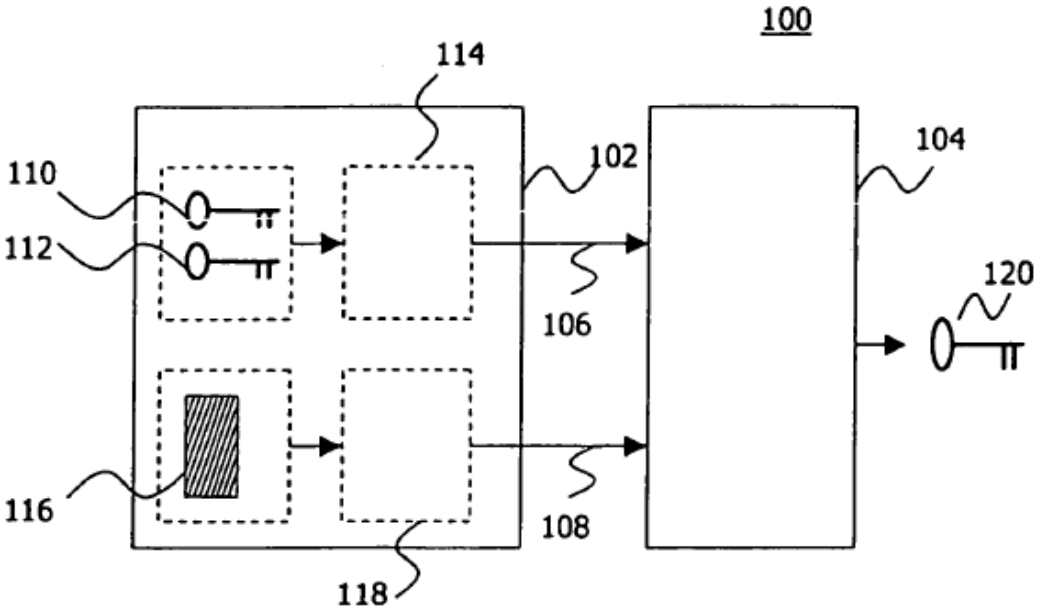


Fig. 3

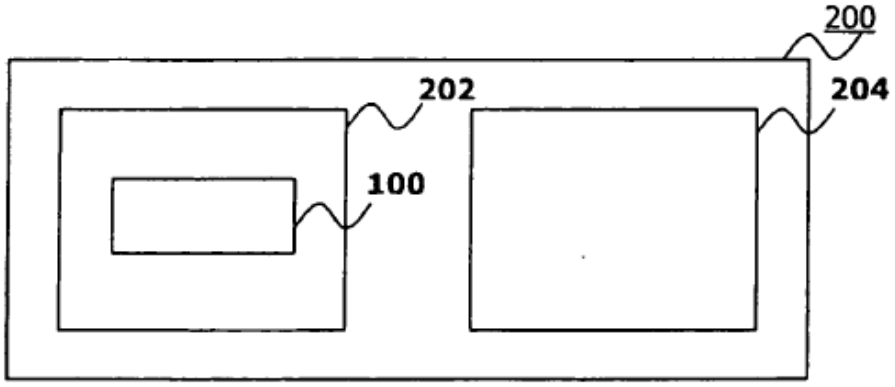


Fig. 4

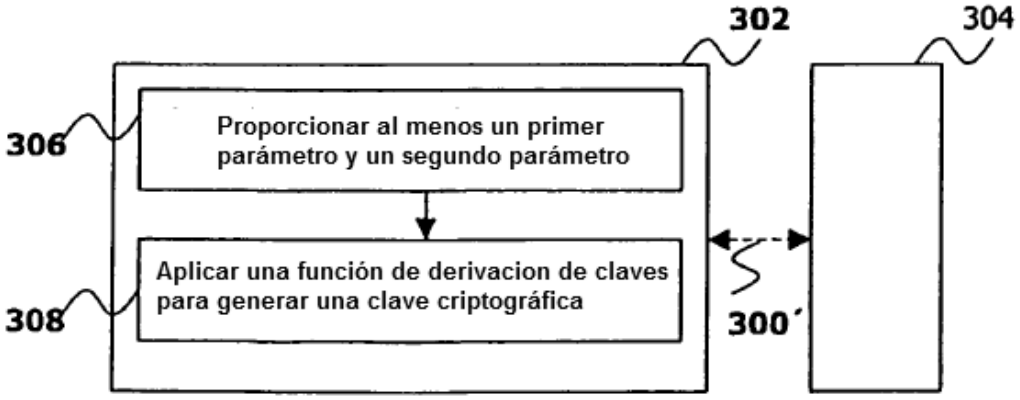


Fig. 5

300

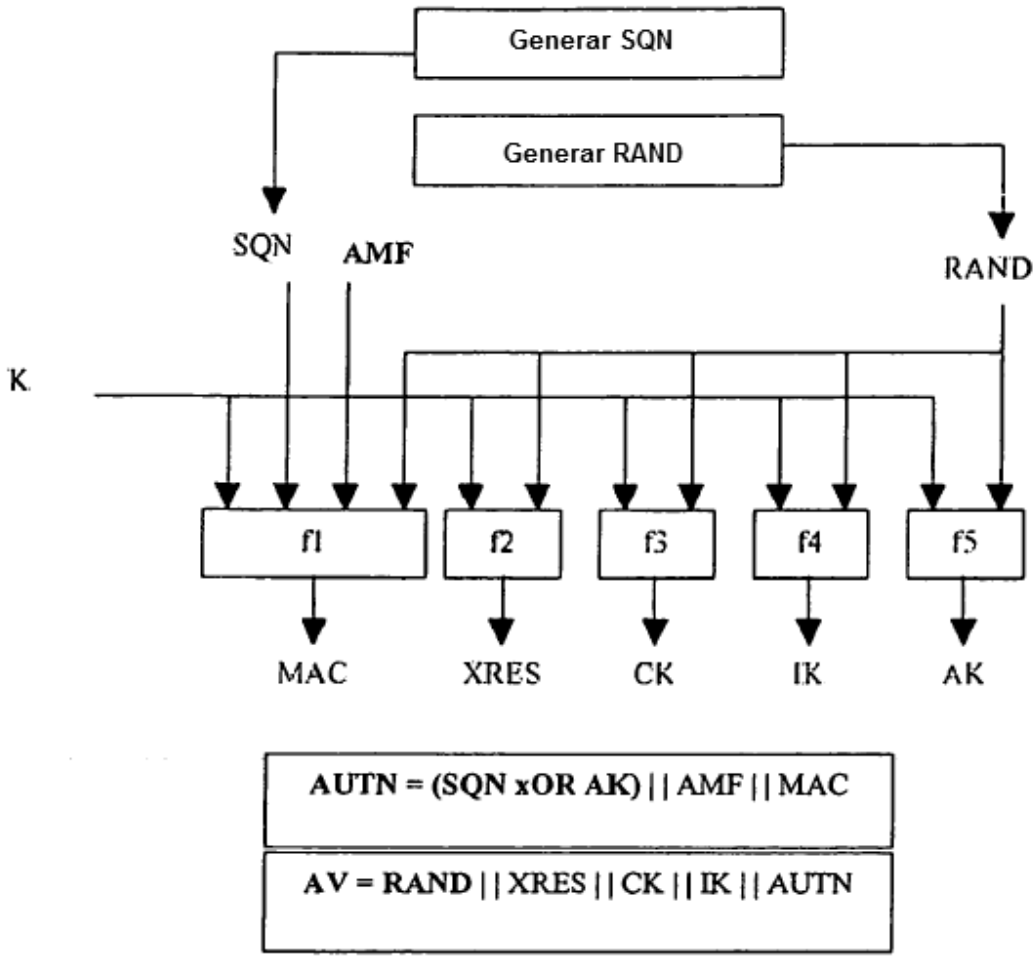
Generar SQN
Generar RAND
SQN
AMF
RAND
K
f1
f2
f3
f4
f5
MAC
XRES
CK
IK
AK
AUTN = (SQN xOR AK) || AMF || MAC
AV = RAND || XRES || CK || IK || AUTN

Fig. 6

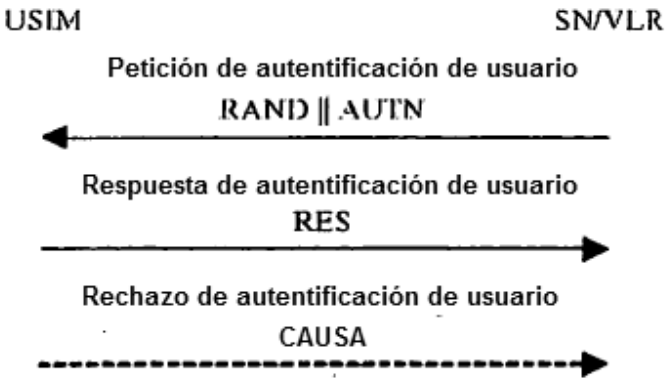
USIM
SN/VLR
Petición de autentificación de usuario
RAND || AUTN
Respuesta de autentificación de usuario
RES
Rechazo de autentificación de usuario
CAUSA

Fig. 7

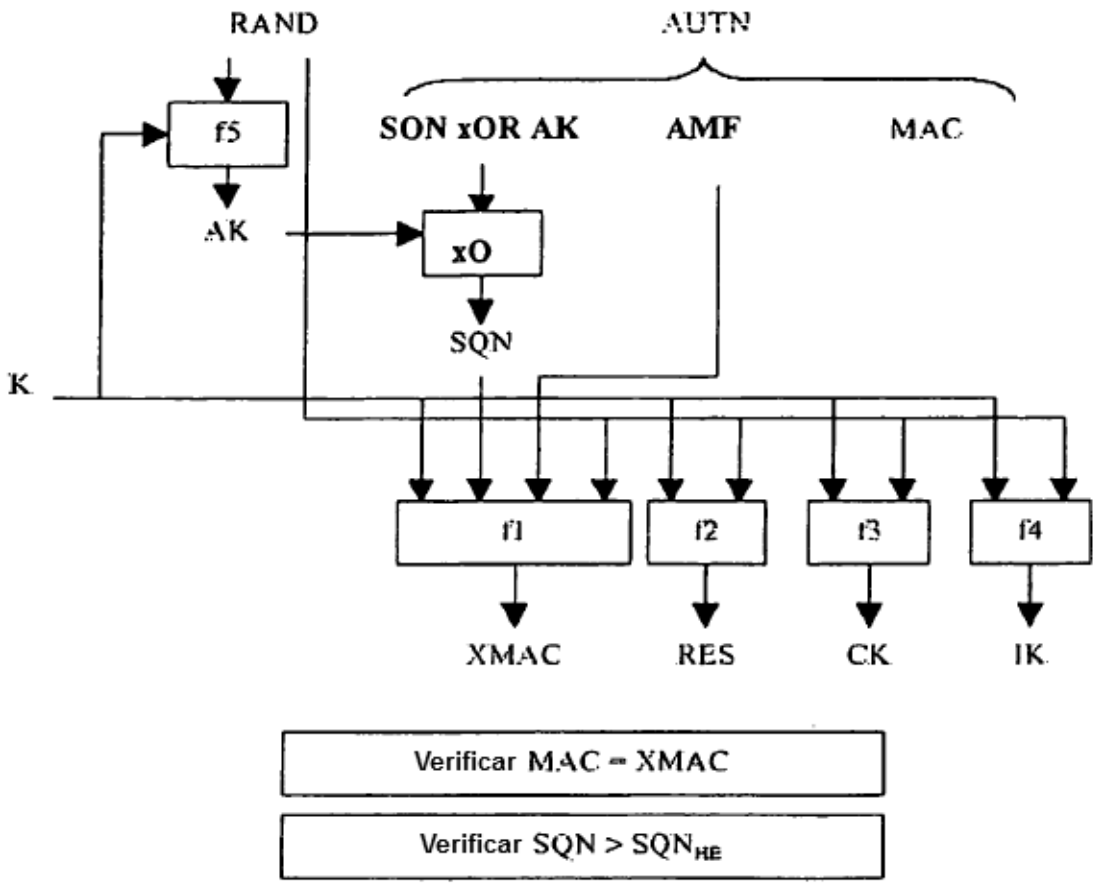
RAND
AUTN
f5
SON xOR AK
AMF
MAC
AK
xO
SQN
K
f1
f2
f3
f4
XMAC
RES
CK
IK
Verificar MAC = XMAC
Verificar SQN > SQN$_{HE}$

Fig. 8

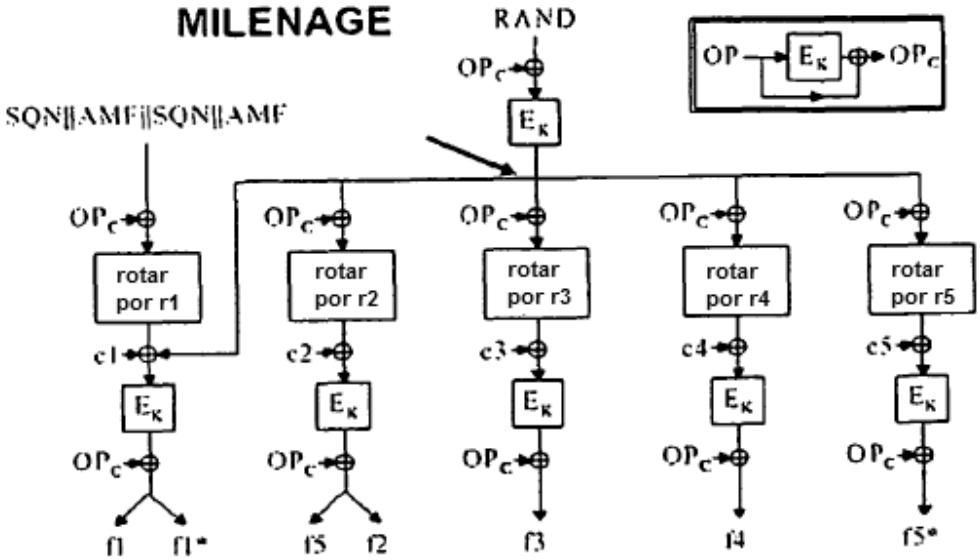
MILENAGE
RAND
OP
$E_K$
$OP_C$
SQN‖AMF‖SQN‖AMF
rotar por r1
rotar por r2
rotar por r3
rotar por r4
rotar por r5
c1
c2
c3
c4
c5
f1
f1*
f5
f2
f3
f4
f5*

Fig. 9

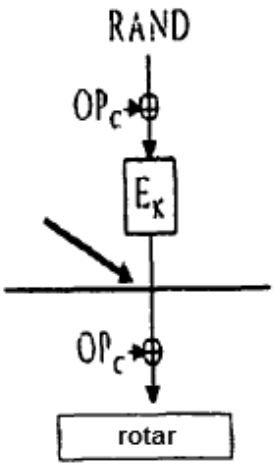
RAND
$OP_C$
$E_K$
rotar

Fig. 10