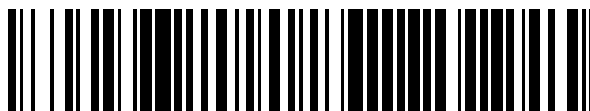


19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



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

51 Int. Cl.:

H04L 9/08 (2006.01)

H04L 9/32 (2006.01)

H04L 9/06 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA LIMITADA

T7

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 modificada tras limitación: **29.12.2021 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 limitada:

28.04.2022

73 Titular/es:

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

72 Inventor/es:

**NÄSLUND, MATS y
NORRMAN, KARL**

74 Agente/Representante:

ELZABURU, S.L.P

ES 2 617 067 T7

DESCRIPCIÓN

Generación de claves criptográficas

Campo técnico

- 5 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

- 10 El protocolo de Autenticación y Acuerdo de Claves (AKA) es un protocolo basado en desafío-respuesta que usa criptografía simétrica. Las metas principales de AKA incluyen autenticación 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.

- 15 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 autenticación de usuario al UE. Junto con la petición, un desafío aleatorio, o código aleatorio (RAND), y un Testigo de Autenticación (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.

- 20 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 requisitos mayores y/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.

- 25 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 Autenticación (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).

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

$$K_{ASME} = \text{KDF}(\text{CK} \parallel \text{IK}, 0x02 \parallel \text{PLMN_ID} \parallel \text{< otro_parámetro >})$$

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.

- 40 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 pseudo-aleatoria. 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.

- 45 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}).

- 50 Como observación general, mientras que es cierto que $\text{KDF}(x)$ produce la misma clave que $\text{KDF}(y)$ si $x = y$, lo inverso puede no mantenerse siempre. Es decir, incluso si $x \neq y$, puede ocurrir todavía que $\text{KDF}(x) = \text{KDF}(y)$. 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 $\text{KDF}(x) = \text{KDF}(y)$ 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 adelante 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 si $CK = CK'$.

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 $KDF(CK' || IK', IMPI)$ si y solo si $CK = CK'$. 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 flecha 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 $CK = CK'$ si y solo si $IK = IK'$.

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 si $RAND = RAND'$. 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 si $RAND = RAND'$, 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.

- 5 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, en el que la primera entidad es un equipo de usuario, tal como una estación móvil. El método forma parte de una operación de seguridad distribuida. La operación de seguridad es un procedimiento de Autenticación y Acuerdo de Claves (AKA) en base a un protocolo AKA que se inicia por la segunda entidad, en el que la segunda entidad es una entidad de red de Evolución de Largo Plazo (LTE). 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 se deriva de un testigo calculado por la segunda entidad ejecutando la operación de seguridad para la primera entidad. El método además comprende aplicar la función de derivación de clave para generar la clave criptográfica en base a la entrada proporcionada. El testigo es una concatenación de una OR exclusiva de un Número de Secuencia (SQN) y una clave de anonimato (AK), un Campo de Autenticación y Gestión de Claves (AMF), y un Código de Autenticación de Mensajes (MAC). 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.

- 30 El testigo se deriva 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.

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.

- 35 El testigo es 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

$$\text{testigo} = \text{AUTN} = (\text{SQN xOR AK}) \parallel \text{AMF} \parallel \text{MAC}$$

El segundo parámetro puede ser una concatenación de la OR exclusiva de un desafío aleatorio (RAND) y un identificador asociado con la primera entidad y el testigo.

- 40 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 segundo parámetro puede ser una concatenación de la OR exclusiva de un desafío aleatorio (RAND) y un identificador asociado con la primera entidad, y el testigo.

Esto se podría expresar como

$$\text{RAND xOR } \langle \text{identificador asociado con la primera entidad} \rangle \parallel \text{testigo}.$$

- 50 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).

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.

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.

Para la técnica descrita en la presente memoria, la segunda entidad se puede situar en una red SAE/LTE.

La segunda entidad puede comprender un Centro de Autenticación (AuC)/Servidor Local de Abonado (HSS) y una Entidad de Gestión de Movilidad (MME).

La operación de seguridad referida en la presente memoria se puede realizar por la primera y segunda entidades de una manera cooperativa.

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, siendo la entidad de comunicaciones un equipo de usuario, tal como una estación móvil, adaptada para cooperar con una entidad de red LTE. El dispositivo está adaptado para realizar una operación de seguridad, de la cual la generación de clave criptográfica puede ser una parte de la misma, en el que 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, comprendiendo la entrada 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 se deriva de un testigo para uso por la entidad de comunicaciones, en la que el testigo es una concatenación de una OR exclusiva de un número de secuencia (SQN) y una clave de anonimato (AK), un Campo de Autenticación y Gestión de Claves (AMF), y un Código de Autenticación de Mensajes (MAC). 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.

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.

El testigo es una concatenación de la OR exclusiva del SQN y una Clave de Anonimato (AK), un Campo de Autenticación y Gestión de Claves (AMF) y un Código de Autenticación de Mensajes (MAC). Esto se puede expresar como

$$\text{testigo} = \text{AUTN} = (\text{SQN} \text{ XOR } \text{AK}) \parallel \text{AMF} \parallel \text{MAC}.$$

El segundo parámetro puede ser una concatenación de la OR exclusiva de un desafío aleatorio (RAND) y un identificador asociado con la primera entidad y el testigo. En este caso, el identificador asociado con la primera entidad puede comprender o se puede derivar 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. Alternativamente, el identificador asociado con la primera entidad aún más puede comprender o se puede derivar de un identificador de una red de comunicaciones asociada con la primera entidad, particularmente una red de servicio de la primera entidad.

El segundo parámetro puede ser una concatenación de la OR exclusiva de un desafío aleatorio (RAND) y un identificador asociado con la primera entidad y el testigo. Por ejemplo, el segundo parámetro se puede expresar como

$$\text{RAND XOR } \langle \text{identificador asociado con la primera entidad} \rangle \parallel \text{testigo}.$$

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.

5 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.

10 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.

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.

15 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 operación de seguridad se puede basar en el protocolo AKA de UMTS.

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:

- 20 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;
- 25 La Fig. 6 es un diagrama de bloques que muestra un procedimiento de la operación de AKA de UMTS, Generación de un Vector de Autenticación por una entidad de red;
- La Fig. 7 es un diagrama de bloques que muestra otro procedimiento de la operación de AKA de UMTS, Autenticación y Establecimiento de Claves;
- 30 La Fig. 8 es un diagrama de bloques que muestra la función de autenticación 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 autenticación anterior en el UE; y
- La Fig. 10 es un diagrama de bloques que muestra un detalle particular del algoritmo criptográfico anterior.

Descripción detallada

35 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
40 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
45 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 autenticación 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 autenticación 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 Autenticación (AV), y Autenticación 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 autenticaciones de usuario. La Generación de Vectores de Autenticación 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 Autenticación 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 autenticación 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 autenticación de mensajes $MAC = f_1(SQN \parallel RAND \parallel AMF)$ donde f_1 es una función de autenticación de mensajes;

5 - una respuesta esperada $XRES = f_2(RAND)$ donde f_2 es una función de autenticación de mensajes (posiblemente trunca);

- una clave de cifrado $CK = f_3(RAND)$ donde f_3 es una función de generación de claves;

- una clave de integridad $IK = f_4(RAND)$ donde f_4 es una función de generación de claves; y

- una clave de anonimato $AK = f_5(RAND)$ donde f_5 es una función de generación de claves.

10 Finalmente se construye el testigo de autenticación $AUTN = (SQN \text{ XOR } AK) \parallel AMF \parallel MAC$. 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 $AK = 000...0$.

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

El siguiente procedimiento de la operación de AKA de UMTS, Autenticación y Establecimiento de Claves, es autenticar 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 autenticación 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.

20 Con referencia a la Fig. 8, tras la recepción del RAND y AUTN el UE primero calcula la clave de anonimato $AK = f_5(RAND)$ (o usa $AK = 000...0$) y recupera el número de secuencia $SQN = (SQN \text{ XOR } AK) \text{ XOR } AK$. A continuación el UE calcula $XMAC = f_1(SQN \parallel RAND \parallel AMF)$ y compara éste con el MAC que se incluye en el AUTN. Si son diferentes, el UE envía un *rechazo de autenticación 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.

25 Si el SQN se considera que está en el intervalo correcto, el UE calcula $RES = f_2(RAND)$ e incluye este parámetro en una *respuesta de autenticación de usuario* de vuelta al SN/VLR. Finalmente el UE calcula la clave de cifrado $CK = f_3(RAND)$ y la clave de integridad $IK = f_4(RAND)$. 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.

30 Tras la recepción de la respuesta de autenticación de usuario el SN/VLR compara la RES con la respuesta esperada XRES desde el vector de autenticación seleccionado. Si XRES es igual a RES entonces la autenticación 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.

35 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

$$AUTN = (SQN \text{ XOR } AK) \parallel AMF \parallel MAC$$

40 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:

$$KDF(CK \parallel IK, RAND \parallel IMPI \parallel SQN)$$

45 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

$$KDF(CK \parallel IK, RAND \parallel IMPI \parallel AUTN).$$

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

$$\text{AUTN} = (\text{SQN} \text{ XOR } \text{AK}) \parallel \text{AMF} \parallel \text{MAC}$$

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

5 Supongamos que

$$(\text{CK} \parallel \text{IK}, \text{RAND} \parallel \text{IMPI} \parallel \text{AUTN}) = (\text{CK}' \parallel \text{IK}', \text{RAND}' \parallel \text{IMPI} \parallel \text{AUTN}').$$

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

$$(\text{SQN} \text{ XOR } \text{AK}) \parallel \text{AMF} \parallel \text{MAC} = (\text{SQN}' \text{ XOR } \text{AK}') \parallel \text{AMF}' \parallel \text{MAC}'.$$

10 Supongamos sin pérdida de generalidad que $\text{AMF} = \text{AMF}'$ y $\text{MAC} = \text{MAC}'$. Entonces solamente es necesario comprobar si lo siguiente podría mantener:

$$\text{SQN} \text{ XOR } \text{AK} = \text{SQN}' \text{ XOR } \text{AK}'.$$

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

15
$$\text{SQN} = \text{SQN}',$$

que es una contradicción dado que, como ya se señaló, SQN siempre “intensifica” y de esta manera $\text{SQN} \neq \text{SQN}'$.

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

20 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, $\text{SQN} \text{ XOR } \text{AK}$ (que forma parte del AUTN) se puede usar dado que tiene (mediante el análisis anterior) la propiedad de unicidad requerida.

25 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).

30 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

35 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

40 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

45 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
5	AUTN	Testigo de Autenticación
	AV	Vector de Autenticación
	CK	Clave de Cifrado
	eNB	Nodo B mejorado
	HE	Entorno Local
10	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
15	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
20	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
25	SAE	Evolución de Arquitectura de Sistema
	SN	Red de Servicio
	SQN	Número de secuencia
	UE	Equipo de Usuario
	UMTS	Sistema de Telecomunicación Móvil Universal
30	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 Autenticación 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) es una concatenación de una OR exclusiva de un número de secuencia <SQN> y una clave de anonimato <AK>, un Campo de Autenticación y Gestión de Claves <AMF>, y un Código de Autenticación de Mensajes <MAC>;

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 1 o 2, 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).
4. El método de la reivindicación 3, 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).
5. 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).
6. 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.
7. El método de la reivindicación 6, 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.
8. 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>.
9. El método de la reivindicación 8, en donde la segunda entidad (204, 304) comprende un Centro de Autenticación <AuC>/Servidor de Abonado Residencial <HSS> y una Entidad de Gestión de Movilidad <MME>.
10. El método de cualquiera de las reivindicaciones precedentes, en donde el procedimiento de Autenticación y acuerdo de Claves se realiza de manera cooperativa por la primera (202, 302) y segunda (204, 304) entidades.
11. El método de cualquiera de las reivindicaciones precedentes, en donde la operación de seguridad se basa en el protocolo de AKA de UMTS.

12. 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.
- 5 13. El producto de programa de ordenador de la reivindicación 12, en donde el producto de programa de ordenador se almacena en un medio de grabación legible por ordenador.
14. Un dispositivo (100) adaptado para generar una clave criptográfica (120) para una entidad de comunicaciones móvil (202, 302) adaptada para ejecutar un procedimiento de Autenticación 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:
- 10 - 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
- 15 - 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) es una concatenación de una OR exclusiva de un número de secuencia <SQN> y una clave de anonimato <AK>, un Campo de Autenticación y Gestión de Claves <AMF>, y un Código de Autenticación de Mensajes <MAC>; y
- 20 en donde la entrada es única cada vez que se inicia el procedimiento de AKA para la entidad de comunicaciones (202, 302).
15. El dispositivo (100) de la reivindicación 14, 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.
- 25 16. El dispositivo de la reivindicación 14 o 15, 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).
17. El dispositivo de la reivindicación 16, 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).
- 30 18. El dispositivo (100) de cualquiera de las reivindicaciones 14 a 17, 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.
- 35 19. El dispositivo (100) de cualquiera de las reivindicaciones 14 a 18, 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.
20. Un equipo de usuario (202) que comprende el dispositivo (100) según cualquiera de las reivindicaciones 14 a 19.
- 40 21. Un sistema que comprende el equipo de usuario (202, 302) de la reivindicación 20 y una entidad de red (304) para una red de Evolución de Arquitectura de Sistema <SAE>/Evolución de Largo Plazo <LTE>.

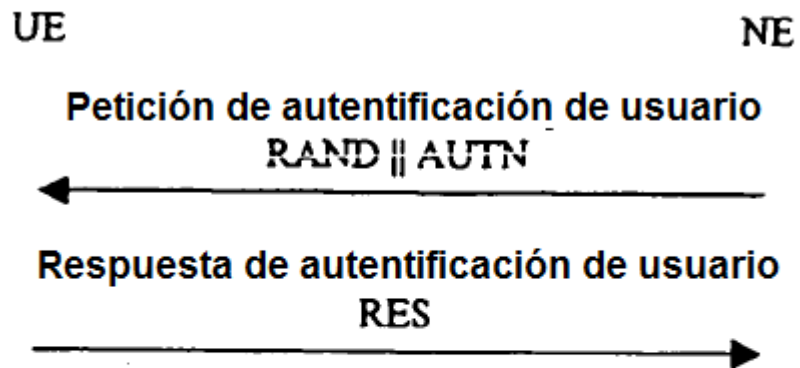


Fig. 1

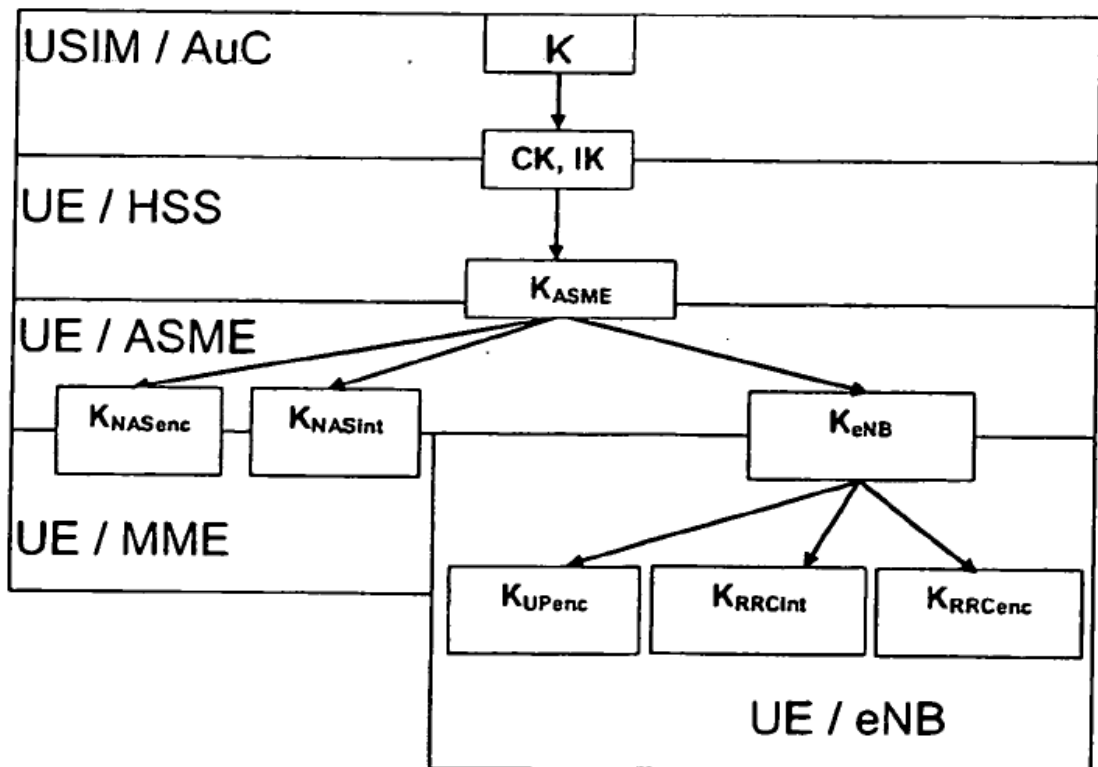


Fig. 2

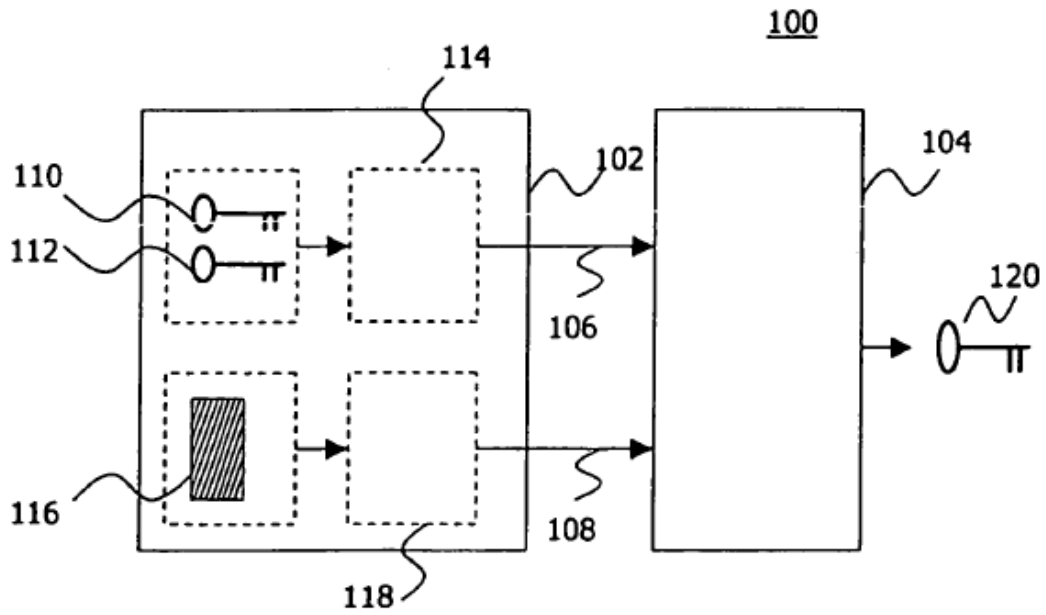


Fig. 3

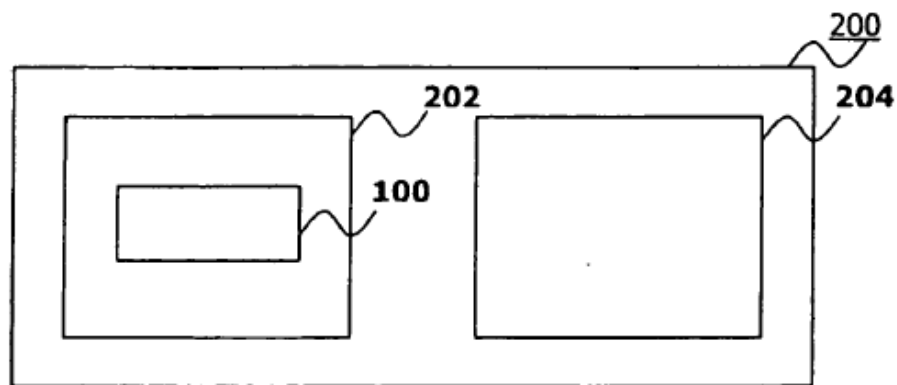


Fig. 4

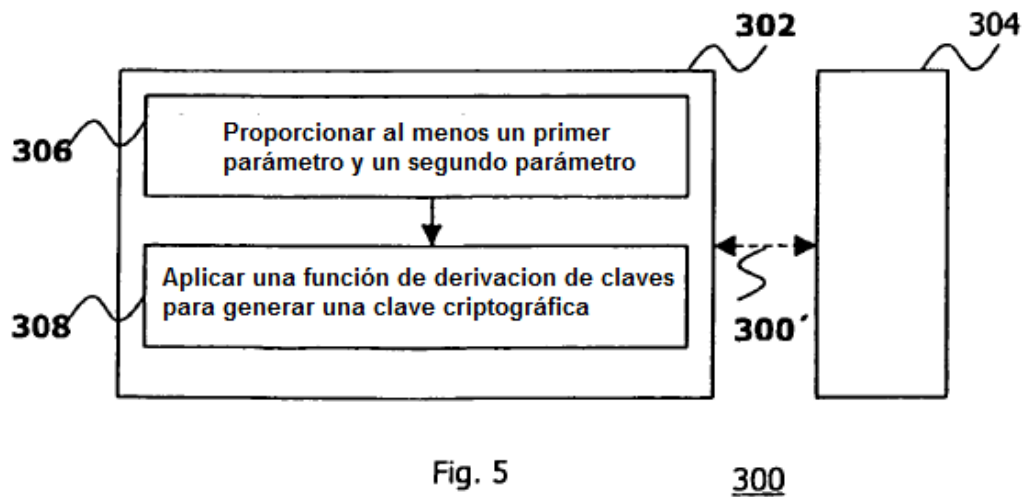


Fig. 5

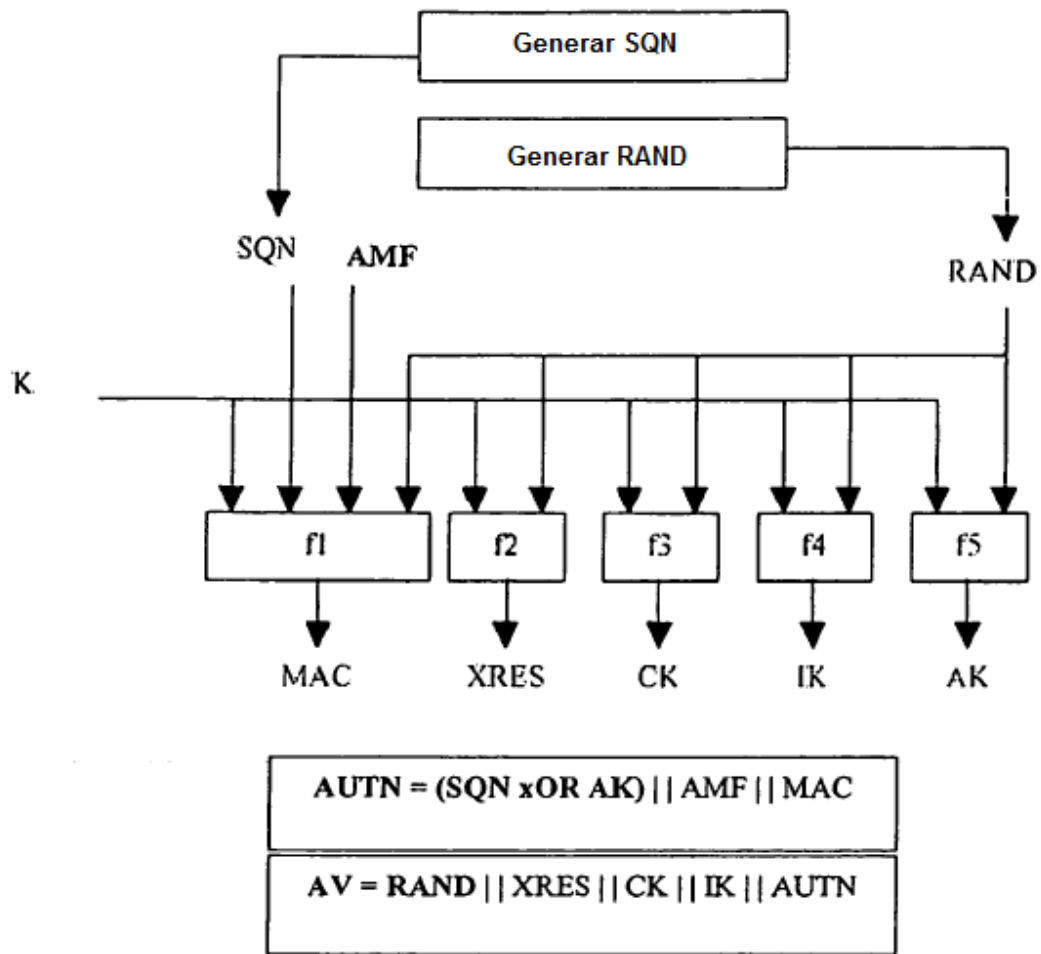


Fig. 6

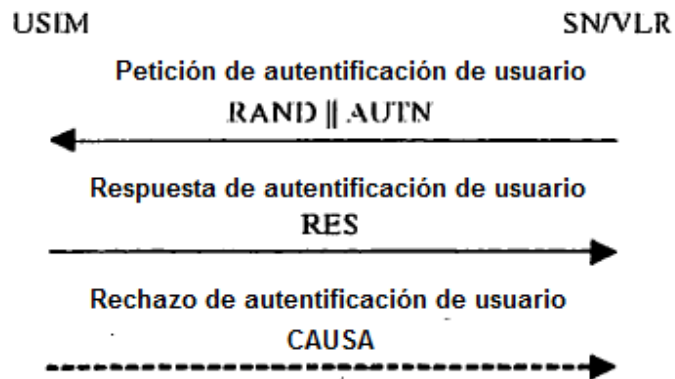


Fig. 7

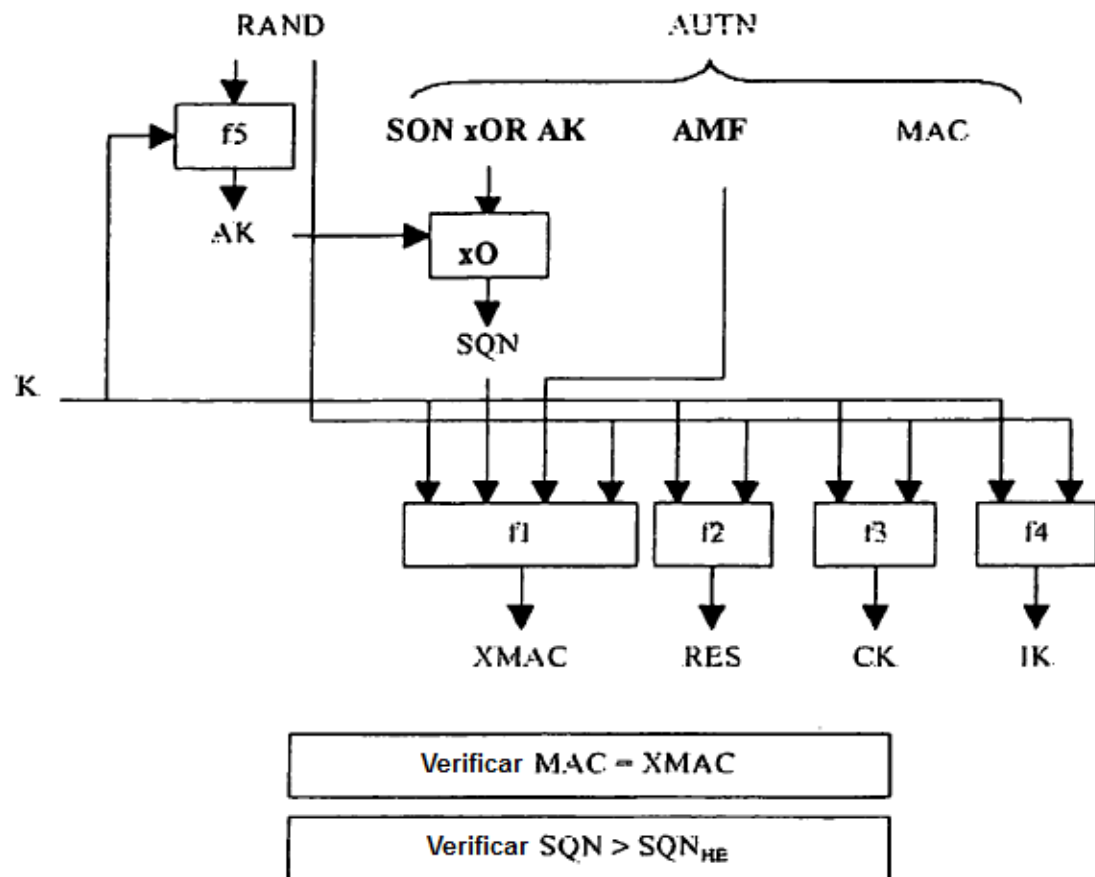


Fig. 8

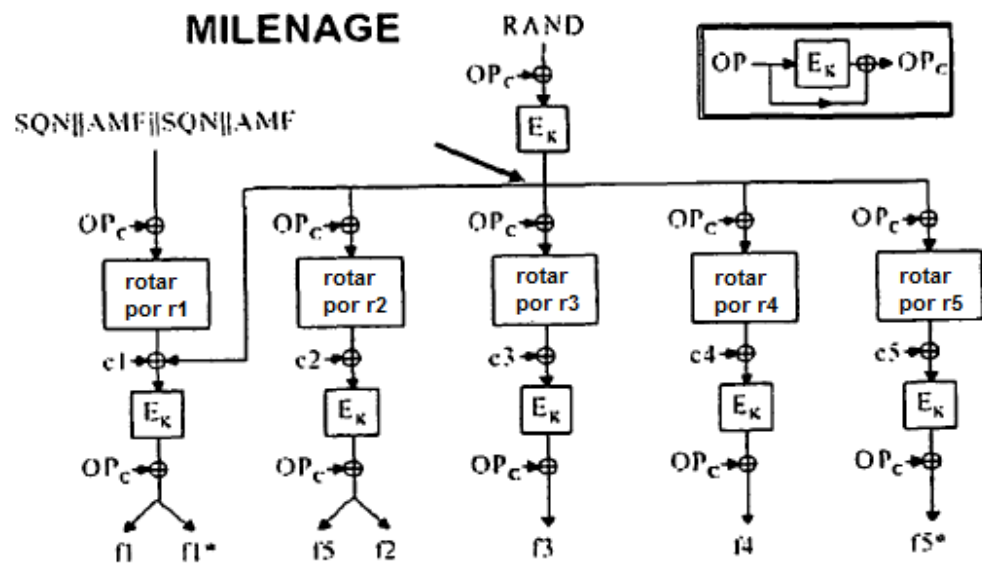


Fig. 9

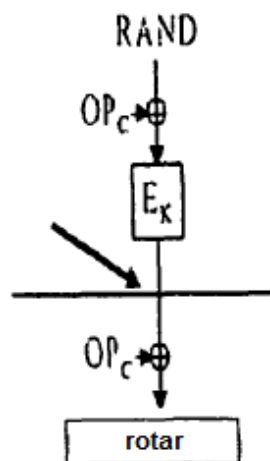


Fig. 10