(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 367 692**

(51) Int. Cl.:
H04W 12/04 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **04775405 .6**
(96) Fecha de presentación : **10.09.2004**
(97) Número de publicación de la solicitud: **1671511**
(97) Fecha de publicación de la solicitud: **21.06.2006**

(54) Título: **Diseño de seguridad mejorado para criptografía en sistemas de comunicación de móviles.**

(30) Prioridad: **26.09.2003 US 505748 P**

(45) Fecha de publicación de la mención BOPI:
07.11.2011

(45) Fecha de la publicación del folleto de la patente:
07.11.2011

(73) Titular/es: **Telefonaktiebolaget LM Ericsson (publ)**
Svardvagen 2
S-175 68 Jarfalla, SE

(72) Inventor/es: **Blom, Rolf;**
Näslund, Mats y
Arkko, Jari

(74) Agente: **De Elzaburu Márquez, Alberto**

DESCRIPCIÓN

Diseño de seguridad mejorado para criptografía en sistemas de comunicaciones de móviles

Campo técnico

La presente invención se refiere en general a aspectos criptográficos en sistemas de comunicación, y, más particularmente, a mejoras de seguridad para el GSM (Sistema Global para Comunicación de Móviles), el UMTS (Sistema Universal de Telecomunicaciones de Móviles) y sistemas de comunicación similares.

Antecedentes

En las comunicaciones de móviles, por ejemplo, según la normativa GSM o UMTS, la seguridad es de suma importancia. Esto está muy relacionado con el aumento del uso de las comunicaciones de móviles en relaciones comerciales y para comunicaciones privadas. En este momento se sabe que, por ejemplo, el GSM padece problemas de seguridad. Tal como se ha descrito recientemente en la referencia [1], es posible recuperar la clave de cifrado vulnerando el algoritmo criptográfico A5/2. Existen tres elecciones básicas de algoritmo para datos por conmutación de circuitos, A5/1, A5/2, A5/3, y tres algoritmos básicos para datos por paquetes, GEA1, GEA2 y GEA3. No obstante, debe observarse que existen también algoritmos de 128 bits más resistentes indicados como A5/4 y GEA4. El terminal señaliza sus capacidades, en particular el conjunto de algoritmos criptográficos que soporta, a la red. A continuación, la red selecciona qué algoritmo criptográfico usar. Obsérvese que esta señalización no está protegida. De este modo, el terminal no tiene la opción de detectar si un atacante está señalizando que debería usar el A5/2, y cuándo lo está haciendo, y que esta información se origina en un operador legítimo.

En general, existen por lo menos tres tipos de ataques. El primer tipo implica que un atacante intercepte y descifre el tráfico cuando el sistema está usando el algoritmo A5/2 vulnerado.

El segundo tipo de ataque comprende la interceptación de tráfico asociado al procedimiento de AKA para registrar datos de tráfico y el valor RAND que se usa. Posteriormente, una estación base falsa puede hacer que el terminal móvil ejecute un procedimiento de AKA usando el RAND registrado previamente y que, a continuación, cifre el tráfico usando el algoritmo A5/2, lo cual permite que el atacante recupere la clave criptográfica Kc. Debido a la simple dependencia con respecto al RAND, esta clave, Kc, será la misma clave que se usó para proteger el tráfico registrado.

El tercer tipo de ataque implica que un hombre-en-el-medio activo obligue al terminal a usar el algoritmo A5/2, permitiendo de este modo el cálculo de la clave criptográfica.

La normativa UMTS recomienda métodos que superan la mayoría de estos problemas. No obstante, se prevé un escenario en el que los terminales GSM se usarán durante un periodo de tiempo considerable hasta que la gran mayoría de usuarios se hayan convertido en propietarios de terminales UMTS. De hecho, muchos servicios avanzados estarán disponibles en teléfonos GSM y los usuarios pueden ser reacios a cambiar sus teléfonos hasta que pase un cierto tiempo.

Adicionalmente, aunque el UMTS dispone de contramedidas que lo hacen resistente a estos ataques, existe evidentemente una preocupación de que avances futuros en el cripto-análisis descubran que también existen problemas similares en el mismo y/o en otros sistemas de comunicación. Por otra parte, podría haber una implicación de problemas de seguridad cuando se produzcan desplazamientos itinerantes entre tipos diferentes de redes, tales como redes GSM y UMTS.

Sumario de la invención

La presente invención supera estos y otros inconvenientes de las disposiciones de la técnica anterior.

Es un objetivo general de la presente invención proporcionar un diseño de seguridad mejorada para sistemas de comunicación.

En particular, es un objetivo de la invención proporcionar mejoras de seguridad para una comunicación cifrada que se basa en acuerdos de claves en sistemas de comunicación de móviles tales como el GSM y el UMTS.

Un objetivo especial consiste en mejorar la gestión de claves para el GSM y el UMTS con el fin de limitar el impacto de la vulneración del A5/2 y ataques futuros sobre otros algoritmos.

Se ha reconocido que un defecto importante en los diseños de seguridad de la técnica anterior es que, aunque la clave de seguridad criptográfica dependa de cierto desafío aleatorio, se usa la misma clave con independencia del algoritmo de seguridad concreto. Una idea básica según la invención consiste en mejorar o actualizar los algoritmos básicos de seguridad criptográfica por medio de una modificación, específica del algoritmo, de la clave de seguridad generada en el procedimiento normal de acuerdo de clave del sistema de comunicación de móviles.

Para la comunicación entre el terminal móvil y el lado de la red, se selecciona normalmente, o bien por parte del lado de la red o bien basándose en un acuerdo mutuo entre el móvil y el lado de la red, una versión mejorada de uno de los algoritmos básicos de seguridad criptográfica soportados por el móvil. A continuación, la clave de seguridad básica resultante del procedimiento de acuerdo de clave entre el terminal móvil y la red se modifica dependiendo de información representativa del algoritmo seleccionado para generar una clave de seguridad específica del algoritmo. Finalmente, el algoritmo de seguridad básico se aplica con la clave de seguridad específica del algoritmo, como entrada de clave para mejorar la seguridad para una comunicación protegida en la red de comunicación de móviles.

Tal como se ha mencionado, la selección del algoritmo se puede realizar en el lado de la red, en cuyo caso el lado de la red transmite información representativa del algoritmo seleccionado al terminal móvil. Esta solución es consistente, por ejemplo, con el GSM actual, donde la red selecciona los algoritmos A5/1 a A5/3.

No obstante, de manera alternativa, especialmente para otros sistemas de comunicación, la selección del algoritmo de seguridad mejorada según la invención se puede basar, si se desea, en un acuerdo entre el terminal móvil y el lado de la red, por ejemplo, ejecutado por medio de un procedimiento de señalización de entrada en contacto, un protocolo de oferta-respuesta o un protocolo de negociación similar.

Preferentemente, los algoritmos originales implementados en hardware se mantienen iguales (por lo menos en el terminal móvil), y, para cada algoritmo original que necesita una mejora de seguridad, se define un algoritmo de seguridad actualizado (virtual), tal como un algoritmo de cifrado/criptográfico mejorado, basándose en el algoritmo original junto con la modificación de la clave específica del algoritmo. La modificación de la clave se realiza típicamente por medio de una función de modificación de clave, que procesa la clave de entrada basándose en un identificador de algoritmo o información similar representativa del algoritmo seleccionado y, posiblemente, en algunos datos adicionales para generar una clave modificada, la cual se reenvía al algoritmo de seguridad original.

Si es deseable soportar, no solamente las versiones mejoradas de los algoritmos de seguridad, sino también mantener un soporte para los algoritmos básicos, por ejemplo, con fines relacionados con la interoperabilidad, el identificador de algoritmo debe poder distinguir entre los algoritmos de seguridad básicos originales y los algoritmos de seguridad mejorada.

En la práctica, la solución básica únicamente requiere actualizaciones de software en los terminales y/o en el sistema de red. En una realización preferida de la invención, el problema se resuelve básicamente modificando los terminales y dejándolos señalizar que ellos (solamente) soportan versiones mejoradas actualizadas de los algoritmos básicos originales. Los esfuerzos de normalización se pueden mantener a un nivel mínimo, puesto que solamente es necesario normalizar la función de modificación y los identificadores de algoritmo.

En el lado de la red, el procesado de selección del algoritmo, de modificación de la clave y de seguridad criptográfica, tal como el cifrado, se puede implementar en un único nodo, o se puede distribuir en varios nodos. Frecuentemente, la selección del algoritmo y la modificación de la clave se implementan en el mismo nodo. No obstante, alternativamente, la selección del algoritmo y la modificación de la clave se pueden distribuir, si se desea, en más de un nodo de la red. Por ejemplo, un nodo puede calcular claves específicas de algoritmo para un conjunto completo de algoritmos de seguridad, y transferir las claves a otro nodo, el cual, a continuación, selecciona una versión mejorada de un algoritmo de seguridad y extrae o deriva la clave apropiada a partir del conjunto recibido de claves. Dependiendo de la implementación del sistema, se puede realizar el cifrado real u otro procesado de seguridad en el mismo nodo en el que se derivó la clave o en un nodo aparte.

La invención proporciona también soporte para la protección contra repeticiones, la autenticación básica de la red y/o la selección de un algoritmo seguro, preferentemente basándose en la codificación o inserción de información en información de AKA existente tal como el desafío aleatorio usado en el procedimiento de AKA con el terminal móvil. La autenticación de la red se logra preferentemente insertando información de autenticación dependiente de la clave, tal como un MAC (Código de Autenticación de Mensaje) que puede ser verificado por el terminal móvil. Calculando el MAC con respecto a la información de protección contra repeticiones y/o información sobre los algoritmos permitidos por la red doméstica, esta información recibirá cierta protección de integridad, dando como resultado una protección contra repeticiones segura y/o una selección de algoritmos segura.

Aunque el problema actualmente más urgente se refiere a algoritmos GSM vulnerados, es evidente que la modificación de clave es útil no solamente en el GSM, sino también en el UMTS, el CDMA o sistemas de futuras generaciones, para garantizar de manera preventiva que posteriormente no aparezcan problemas similares (tal vez todavía no descubiertos), puesto que la derivación de clave en el mismo es actualmente también independiente del algoritmo. En efecto, la invención es aplicable en varios sistemas de comunicaciones, que incluyen, por ejemplo, sistemas GSM/GPRS, W-LAN (Red de Área Local Inalámbrica), UMTS e IMS (Subsistema Multimedia IP).

De este modo, la invención proporciona un remedio para un defecto de un diseño de seguridad básico en, por ejemplo, los procedimientos de AKA del GSM/UMTS. La solución propuesta encaja bien en la estructura de protocolos existente y presenta consecuencias de implementación limitadas, lo cual hace posible un rápido despliegue.

La invención ofrece las siguientes ventajas:

- Una solución eficaz a un defecto de un diseño de seguridad básico;
- Es suficiente con modificar la clave, al mismo tiempo que se permite que los algoritmos originales implementados en hardware permanezcan invariables;
- Esfuerzo mínimo de normalización;
- Encaja bien en la estructura de protocolos existente; y
- Consecuencias de implementación limitadas, lo cual hace posible un despliegue rápido.

Se apreciarán otras ventajas ofrecidas por la presente invención al leer la siguiente descripción de las realizaciones de la invención.

Breve descripción de los dibujos

La invención, junto con objetivos y ventajas adicionales de la misma, se entenderá mejor en referencia a la siguiente descripción considerada conjuntamente con los dibujos adjuntos, en los cuales:

la Fig. 1 es un diagrama de bloques esquemático que ilustra una solución básica según una realización preferida, ejemplificativa, de la invención con un algoritmo global definido mediante una modificación de clave específica del algoritmo en combinación con un algoritmo criptográfico básico original;

la Fig. 2 es un diagrama de flujo esquemático de un método para mejorar la seguridad para una comunicación protegida en un sistema de comunicaciones de móviles según una realización preferida de la invención;

la Fig. 3 es un diagrama de señales básico, esquemático, según una realización preferida, ejemplificativa, de la invención;

la Fig. 4 es un diagrama de bloques esquemático que ilustra partes relevantes de un terminal móvil según una realización ejemplificativa de la invención, que implementa una modificación de clave específica del algoritmo;

la Fig. 5 ilustra una arquitectura de red ejemplificativa, que ilustra los nodos implicados para tipos diferentes de sistemas de comunicación;

la Fig. 6 es un diagrama esquemático que ilustra una vista general del procedimiento de establecimiento de modo de cifrado mejorado y de modificación de clave según una realización ejemplificativa, específica, de la invención; y

la Fig. 7 es un diagrama de señales básico, esquemático, según otra realización preferida, ejemplificativa, de la invención, que incluye mejoras de algoritmos de seguridad con protección contra repeticiones y autenticación de red integradas.

Descripción detallada de realizaciones de la invención

Puede resultar útil comenzar con un breve análisis de los defectos de seguridad básica en el GSM. Un defecto en el diseño actual es que la clave usada para todos los algoritmos se obtiene de la misma manera con independencia del algoritmo del cifrado que se vaya a usar. Si no fuera así, la vulneración del A5/2 habría significado simplemente eso, y los ataques de tipo 2 y 3 mencionados en la sección de antecedentes no se podrían haber usado para interceptar tráfico protegido con otros algoritmos.

Además, la importancia del error de diseño se incrementa por el hecho de que la señalización no está protegida (no existe autenticación de red y, consecuentemente, ni integridad ni protección contra repeticiones). Tal como se ha mencionado, esto se corrige en el UMTS. Podría parecer que la mejora de la seguridad del GSM en la del UMTS arreglaría los problemas. No obstante, esto requiere modificaciones en el AuC (Centro de Autenticación), en estaciones base, en terminales y en tarjetas SIM (Módulo de Identidad de Abonado), y constituiría una manera muy costosa de resolver los problemas.

Por otro lado, la invención proporciona un remedio a este tipo de defectos de seguridad, basándose principalmente en una modificación, específica del algoritmo, del material de aplicación de claves de AKA. En referencia a la Fig. 1, puede observarse que el material de aplicación de claves proporcionado por el procedimiento 10 de AKA convencional se usa como entrada a un algoritmo 20 de seguridad mejorada, el cual se forma mediante una modificación 22 de clave en combinación con un algoritmo 24 de seguridad original. Para garantizar un material de aplicación de claves dependiente del algoritmo como salida de la unidad de modificación, como entrada a la unidad de modificación se aplica información que representa o, identifica de otro modo, un algoritmo seleccionado. Aunque

la invención no incrementa la seguridad de algoritmos básicos subyacentes como tal, el material de claves no resulta tan útil para ataques sobre cualquiera de los otros algoritmos. La modificación de la clave se realiza normalmente mediante una función de modificación criptográfica, la cual por lo menos debería ser una función unidireccional y preferentemente una función seudo-aleatoria. Por ejemplo, la función de modificación criptográfica se puede implementar como una función *hash* criptográfica. Opcionalmente se puede introducir otra información relacionada con la AKA, tal como RAND y RES del procedimiento de AKA, para conseguir que los ataques de pre-cálculo resulten inviables, y también se puede introducir información de contexto opcional si se pueden identificar otros tipos de ataques de licitación a la baja (*bidding-down*).

El procesado de seguridad de los algoritmos de seguridad está relacionado típicamente con la confidencialidad y el cifrado de datos, aunque alternativamente se puede referir a la integridad y/o autenticación de datos.

La modificación de la clave se puede considerar como un pre-procesado del algoritmo, aunque también puede verse como un post-procesado del AKA, en el que la clave de salida del procedimiento de AKA convencional se procesa a posteriori para producir una clave dependiente del algoritmo. Es simplemente una cuestión de definiciones.

La Fig. 2 es un diagrama de flujo esquemático de un método para mejorar la seguridad para una comunicación protegida en un sistema de comunicaciones de móviles según una realización preferida de la invención. En la etapa S1, se realiza un procedimiento de acuerdo de clave, habitualmente como parte de un procedimiento de AKA completo que implica también la autenticación del terminal móvil. En la etapa S2, se selecciona una versión mejorada o modernización de uno de los algoritmos de seguridad básicos, en el lado de la red o basándose en un acuerdo mutuo entre el terminal móvil y el lado de la red. Como se ha indicado previamente, los algoritmos de seguridad mejorada son frecuentemente algoritmos de cifrado/criptográficos mejorados en cuanto a seguridad, aunque pueden resultar interesantes otros tipos de proceso de seguridad. Si el algoritmo se selecciona en el lado de la red, se transmite desde el lado de la red al terminal móvil información representativa del algoritmo seleccionado. En este caso, si el móvil está en la red doméstica, la selección del algoritmo la realiza habitualmente la red doméstica. Si el móvil se desplaza de forma itinerante en una red visitada, la red visitada habitualmente realiza la selección del algoritmo según alguna política predeterminada. La selección realizada por la red visitada se puede comprobar finalmente con respecto a una política de seguridad de la red doméstica, de tal manera que el algoritmo seleccionado sea aceptado por la red doméstica. Alternativamente, se realiza una negociación entre el terminal móvil y el lado de la red para decidir qué algoritmo de seguridad usar, por ejemplo, por medio de un procedimiento de señalización de entrada en contacto.

De todos modos, al final se produce algún acuerdo sobre qué algoritmo de seguridad usar para una comunicación protegida con el terminal móvil. El orden particular en el que se realizan el acuerdo del algoritmo y el acuerdo de la clave no es habitualmente crítico, aunque puede que resulte ventajoso realizar el acuerdo del algoritmo después de una autenticación satisfactoria del terminal móvil. En la etapa S3, se modifica información de clave, típicamente una clave de seguridad básica, del procedimiento de acuerdo de clave de la etapa S1 para generar información de clave específica del algoritmo. En la etapa S4, se aplica a continuación el algoritmo de seguridad básico correspondiente con la información de clave modificada y específica del algoritmo como entrada de clave. Consiguiendo que la información de clave de seguridad sea específica del algoritmo o dependiente del algoritmo, se mejora la seguridad para la comunicación protegida entre la red y el terminal móvil.

La modificación de la clave específica del algoritmo y el uso de la información de clave modificada se implementa preferentemente en el terminal móvil así como en el lado de la red, pero por lo menos en el lado del terminal. Considerando el número elevado de terminales móviles que se pueden ver afectados por un algoritmo de seguridad vulnerado, puede que resulte muy ventajoso implementar la modificación de la clave en software, y simplemente realizar una modernización de software de los terminales. Esto significa que los algoritmos originales implementados en hardware pueden permanecer invariables, limitando significativamente las consecuencias de la implementación. La modificación de la clave se realiza típicamente mediante una función de modificación de clave, implementada en software, tal como una función *hash* criptográfica unidireccional, la cual procesa la clave de entrada basándose en un identificador de algoritmo y, posiblemente, algunos datos adicionales, para generar una clave modificada, que posteriormente se reenvía al algoritmo de seguridad original. De modo similar, el nodo o nodos de red relevantes se pueden actualizar por medio de modernizaciones de software.

Básicamente, la invención sugiere una modificación del material de aplicación de claves producido en procedimientos de AKA convencionales, tales como el AKA del GSM y el AKA del UMTS, para generar claves dependientes del algoritmo. Aunque la invención es en general aplicable en varios sistemas de comunicación incluyendo GSM, GPRS, W-LAN, CDMA, UMTS, IMS o sistemas de generaciones futuras, la invención se describirá a continuación principalmente en el contexto de procedimientos de AKA del GSM/GPRS y del UMTS.

Un ejemplo específico para el AKA del GSM:

Kc'=Modificar_GSM (Kc, Id_Algoritmo, [RAND, RES, Otra_info_contexto])

y para el UMTS:

Ck', Ik' = Modificar_UMTS (Ck, Ik, Id_Algoritmo, [RAND, RES, Otra_info_contexto])

donde las funciones Modificar_GSM ( ) y Modificar_UMTS ( ) son funciones criptográficas, por ejemplo, basadas en MD5, SHA1 o alguna variante de los mismos, que realizan un truncamiento respectivamente a los 64/128 bits de más a la izquierda. En el caso del UMTS, es también posible usar como entrada para producir una salida de 256 bits alguna función que tome tanto Ck como Ik. El RAND se puede introducir para conseguir que los ataques de pre-cálculo resulten inviables. Para traspasos entre MSC y traspasos similares en otros sistemas, el RAND se transfiere entonces, típicamente, junto con la información de traspaso convencional desde el MSC antiguo al MSC nuevo.

A continuación se describirá principalmente la invención en referencia al escenario en el que la selección del algoritmo se realiza en el lado de la red. No obstante, debe entenderse que la misma también es viable para implementar un procedimiento básico de señalización de entrada en contacto o un mecanismo de negociación similar en el que el terminal móvil y el lado de la red llegan a un acuerdo sobre qué algoritmo de seguridad usar para la comunicación protegida.

Puede resultar útil describir la señalización general entre el terminal y el lado de la red según una realización preferida, ejemplificativa, de la invención, en referencia a la Fig. 3.

1. El terminal señaliza qué algoritmos actualizados soporta, así como una ID de usuario o abonado.

El lado de la red (que implica la red doméstica y/o la red visitada en la forma y en el momento requeridos por un procedimiento de AKA convencional) inicia la autenticación y el acuerdo de clave creando un RAND, calculando una respuesta esperada y una o más claves. Sobre la base de la ID de abonado, en el lado de la red se puede recuperar la clave relevante de abonado secreta y compartida para permitir los cálculos de AKA.

2. La red envía el RAND al terminal.

3. El terminal introduce el RAND en el SIM GSM, el SIM UMTS, el ISIM o una funcionalidad similar y, basándose en una clave de abonado compartida, obtiene una respuesta RES y una o más claves.

4. El terminal envía la RES al lado de la red.

5. El lado de la red comprueba la RES para autenticar el terminal. Cuando el móvil está en la red doméstica, la red doméstica comprueba la RES con respecto a una respuesta esperada XRES. Cuando el terminal móvil está en una red visitada, la red visitada normalmente comprueba la RES por comparación con una XRES recibida desde la red doméstica. En la terminología GSM, tanto a la RES como a la XRES se les hace referencia normalmente como SRES.

6. En este ejemplo, el lado de la red (red doméstica o red visitada dependiendo de en dónde esté situado el móvil) selecciona preferentemente uno de los algoritmos actualizados soportados por el terminal e inicia el cifrado. Naturalmente, el lado de la red debe soportar también el algoritmo seleccionado de seguridad mejorada.

7. El lado de la red envía la ID de algoritmo al terminal.

8. El terminal inicia el cifrado basándose en el algoritmo actualizado seleccionado que incluye una modificación de clave dependiente del algoritmo.

Si resulta deseable soportar, no solamente las versiones mejoradas de los algoritmos de seguridad, sino también mantener un soporte para los algoritmos básicos, por ejemplo, por razones relacionadas con la interoperabilidad, el identificador de algoritmo debe poder distinguir entre los algoritmos de seguridad básicos originales y los algoritmos de seguridad mejorados.

La siguiente Tabla I ilustra un posible ejemplo de identificadores de algoritmo para los algoritmos criptográficos GSM/GPRS básicos y un conjunto correspondiente de algoritmos criptográficos mejorados:

Algoritmos de seguridad básicos:	ID de algoritmo
A5/1	1
A5/2	2
...	...
A5/*k*	*k*
GEA1	*k*+1
GEA2	*k*+2

...	...
GEA*m*	*k*+*m*
Algoritmos de seguridad mejorados:	ID de algoritmo
A5/1’	(*k*+*m*)+1
A5/2’	(*k*+*m*)+2
...	...
A5/*k*’	(*k*+*m*)+*k*
GEA1’	(*k*+*m*+*k*)+1
GEA2’	(*k*+*m*+*k*)+2
...	...
GEA*m*’	(*k*+*m*+*k*)+*m*

De este modo se han definido nuevo algoritmos criptográficos mejorados, representados en este caso por As/1’, As/2’,..., A5/*k*’,..., GEA1’, GEA2’,..., GEA*m*’ para el caso particular del cifrado GSM y GPRS. Generalizando, se supone que hay un número, *k*, de algoritmos A5 y un número, *m*, de algoritmos GEA, donde normalmente *k* = *m* = 4. Tal como se ha descrito previamente, cada uno de los algoritmos mejorados se forma mediante modificación de clave específica del algoritmo en combinación con el algoritmo básico correspondiente. Si, por alguna razón, la red selecciona un algoritmo de seguridad básico, la clave de AKA se trasladará de manera transparente sin modificación, al algoritmo básico.

Naturalmente, se pueden usar otras formas de diferenciar los identificadores de algoritmo, por ejemplo, basándose en representaciones binarias o hexadecimales.

Por ejemplo, puesto que el GSM se ha especificado en la actualidad de manera que soporta hasta ocho algoritmos, una manera sencilla consistiría en dejar que A5/j, donde j=5, 6, 7 y 8 indica respectivamente AS/1’, AS/2’, AS/3’ y A5/4’. En relación con los algoritmos de 128 bits A5/4 y también GEA4, puede que no resulte necesario proporcionar variantes mejoradas, puesto que los mismos se consideran, por lo menos en la actualidad, muy resistentes.

Si se desea soportar únicamente los algoritmos mejorados actualizados, en la siguiente Tabla II se ofrece un posible ejemplo de identificadores de algoritmo para los algoritmos criptográficos de GSM/GPRS mejorados propuestos.

Algoritmos de seguridad mejorados:	ID de algoritmo:
A5/1’	1
A5/2’	2
...	...
A5/*k*’	*k*
GEA1’	*k*+1
GEA2’	*k*+2
...	...
GEA*m*’	*k*+*m*

Una solución ejemplificativa consiste en modernizar los terminales y dejarles señalizar que únicamente soportan la versión actualizada de los algoritmos básicos (actuales). Esto se puede realizar definiendo nuevos algoritmos criptográficos, por ejemplo, AS/1’, A5/2’,..., A5/*k*’, GEA1’, GEA2’,..., GEA*m*’ para el caso particular de GSM y GPRS, o mediante una indicación en la señalización de capacidades generales del terminal.

Un ejemplo de un procedimiento completo se puede describir como:

1. El terminal señaliza el soporte de A5/x’, A5/y’,..., y también envía la ID de usuario o abonado.
2. La red envía el RAND al terminal.
3. El terminal introduce el RAND en el SIM y obtiene RES y Kc.
4. El terminal envía la RES a la red.
5. La red comprueba la RES.

6. Después de una autenticación satisfactoria, la red selecciona un algoritmo soportado, por ejemplo, A5/y', e inicia el cifrado con el uso de A5/y'.

7. La red envía el identificador de algoritmo de A5/y' al terminal.

8. El terminal inicia el cifrado con el uso del algoritmo actualizado A5/y'=(modificación de clave y A5/y). En la práctica, esto significa típicamente que el terminal calcula la clave modificada a usar realizando Kc'=Modificar (Kc, identificador_A5/y', [RES], [RAND]) y aplica la clave modificada Kc' al algoritmo de hardware original A5/y.

Tal como se ha mencionado anteriormente, la función de modificación debería ser por lo menos una función unidireccional, preferentemente una función seudo-aleatoria. Se puede usar una función *hash* criptográfica convencional con clave, MD5, SHA-1, o alguna variante de las mismas, por ejemplo, HMAC. Si se desea, incluso es posible cambiar (aumentar/reducir) el tamaño de la clave AKA básica por medio de la función de modificación. Por ejemplo, se puede utilizar un procesado de claves y/o una concatenación de material de claves para aumentar el tamaño de la clave final. Por ejemplo, la unidad de modificación puede invocar el SIM una segunda vez usando el RAND más una constante predeterminada como nuevo desafío aleatorio y concatenar la primera clave de AKA con la segunda clave de AKA para generar una nueva clave de tamaño doble, la cual posteriormente se puede hacer específica del algoritmo por medio de una función unidireccional criptográfica. Otro ejemplo implica el procesado de la clave de AKA, por ejemplo, desplazando bits, para generar una clave de AKA procesada, la cual a continuación se puede concatenar con la clave de AKA original para aumentar el tamaño de la clave. Naturalmente, la unidad de modificación puede incluir otras funciones de mejora de la seguridad que se pueden combinar con la modificación de clave específica del algoritmo propuesta por la invención.

La Fig. 4 es un diagrama de bloques esquemático de las partes relevantes de un terminal móvil según una realización ejemplificativa de la invención, que implementa una modificación de clave específica del algoritmo. Normalmente, la funcionalidad 10 de AKA se implementa en un módulo de identidad (IM) convencional 15 tal como la tarjeta SIM del GSM, aunque alternativamente se puede proporcionar en cualquier otro lugar del terminal móvil 100. A continuación la(s) clave(s) de salida del AKA se reenvía, opcionalmente junto con el RAND, la RES y/o información de contexto, al módulo 22 de modificación de clave de la invención. El módulo 22 de modificación de clave procesa la(s) clave(s) de salida del AKA en respuesta a un identificador de algoritmo representativo del algoritmo de seguridad seleccionado para generar una clave de seguridad específica del algoritmo. A continuación, esta clave modificada se transfiere al algoritmo 24 de seguridad básico, ejemplificado en este caso mediante un algoritmo criptográfico, tal como, por ejemplo, cualquiera de los algoritmos originales A5/1, A5/2, A5/3, GEA1, GEA2 y GEA3. Evidentemente, el algoritmo 24 de seguridad básico recibe también la información a proteger por el algoritmo de seguridad. En el caso del cifrado, los datos denominados de "texto limpio" son cifrados por el algoritmo de seguridad basándose en la clave de seguridad específica de algoritmo para generar datos de salida cifrados. El módulo 22 de modificación de clave se implementa normalmente como software/hardware del terminal, preferentemente usando las capacidades generales de terminal correspondientes al móvil 100. Tal como se ha mencionado, resulta ventajoso implementar la modificación de la clave como una modernización de software basándose en una función de modificación criptográfica adecuada para su ejecución por parte del hardware de procesado del terminal. No obstante, si algún diseñador/fabricante de móviles desea que todas las funciones criptográficas estén en hardware, no hay nada que evite una implementación en hardware de la modificación de la clave. Por ejemplo, los teléfonos GSM nuevos pueden estar provistos de un módulo de hardware adicional de modificación de la clave que esté dispuesto para cooperar con el módulo de AKA y el algoritmo de cifrado criptográfico, básico, común. El algoritmo criptográfico 24 se realiza típicamente en hardware del terminal, preferentemente cerca de la cadena 30 de RX/TX. El módulo 15 de identidad puede ser cualquier módulo de identidad resistente a manipulaciones indebidas conocido en la técnica, incluyendo tarjetas SIM convencionales usadas en teléfonos móviles GSM (Sistema Global para Comunicaciones de Móviles), SIM UMTS (Sistema Universal de Telecomunicaciones de Móviles) (USIM), SIM WAP (Protocolo de Aplicaciones Inalámbricas), conocido también como WIM, ISIM (Módulo de Identidad de Subsistema Multimedia IP) y, de manera más general, módulos UICC (Tarjeta de Circuito Integrado Universal). La funcionalidad de AKA no se debe implementar necesariamente en un módulo de identidad, o por lo menos no en un módulo de hardware tal como el SIM común. Incluso es posible emular un módulo de identidad completo que incluya funcionalidad de AKA en software.

Como se ha mencionado, la invención se puede aplicar tanto cuando el terminal móvil está en su red doméstica como cuando se desplaza de manera itinerante en una red visitada, siempre que la red doméstica y la red visitada, respectivamente, soporten unos algoritmos de seguridad mejorados (es suficiente con que la red doméstica tenga conocimiento de la existencia de los algoritmos). Debido a que este último caso, cuando el móvil se desplaza de manera itinerante en una red visitada, es algo más complejo, se describirá brevemente una arquitectura de red ejemplificativa que incluye tanto una red doméstica como una red visitada en referencia a la Fig. 5. Además de una arquitectura de red general, la Fig. 5 ilustra también los nodos implicados para cada uno de una serie de sistemas de comunicación ejemplificativos.

La arquitectura de red global incluye un terminal móvil 100, un punto 200 de acceso a red, uno o más nodos 300 denominados habilitadores de seguridad en la red visitada y uno o más nodos 400 de red de gestión de abonados

en la red doméstica. El punto de acceso a red puede ser, por ejemplo, un nodo BTS (Estación Transceptora Base), un nodo B o un punto de acceso de W-LAN, dependiendo del sistema de comunicación considerado. Básicamente, los nodos habilitadores 300 de seguridad en la red visitada deben proporcionar soporte para la autenticación del usuario, en los cuales los terminales móviles se autentican con respecto a la red con el fin de obtener acceso a los servicios de red. Esta autenticación puede servir también como base para facturación de los usuarios. Los protocolos de seguridad básicos de los sistemas de comunicación actuales implican normalmente un procedimiento de autenticación con desafío-respuesta y de acuerdo de clave (AKA). El procedimiento de AKA se basa de la manera más frecuente en una criptografía simétrica que usa una clave secreta compartida entre el terminal móvil y la red doméstica, tal como se ha descrito previamente. En el terminal móvil 100, la clave secreta compartida se almacena normalmente en un módulo de identidad de abonado, tal como el SIM GSM, el USIM, el ISIM, el WIM, o, de forma más general, en una UICC. En la red doméstica, uno o más nodos 400 de red gestionan los abonados e información de seguridad relacionada. El(los) nodo(s) 400 de gestión de abonados de la red doméstica se comunica con el(los) nodo(s) habilitador(es) 300 de seguridad en la red visitada, habitualmente transfiriendo información relacionada con el AKA y opcionalmente también información de política de seguridad desde la red doméstica a la red visitada. De acuerdo con una realización ejemplificativa de la invención, el(los) nodo(s) habilitador(es) de seguridad incluye también una funcionalidad para seleccionar un algoritmo de seguridad adecuado para una comunicación protegida con el terminal móvil. Preferentemente, el(los) nodo(s) habilitador(es) 300 de seguridad se implementa con una función de modificación de clave para modificar la(s) clave(s) de salida del AKA normal(es) dependiendo del algoritmo seleccionado con el fin de proporcionar soporte para los algoritmos de seguridad mejorados, de acuerdo con la invención. Estos nodos habilitadores de seguridad pueden incluir también los motores criptográficos reales para el procesado de seguridad, tal como el cifrado. No obstante, en algunos sistemas tal como el GSM, el cifrado se implementa en la estación transceptora base real que actúa como punto de acceso a la red.

La selección del algoritmo, la modificación de la clave, y el cifrado real se pueden implementar en un único nodo, o se pueden distribuir en varios nodos. Frecuentemente, la selección del algoritmo y la modificación de la clave se implementan en el mismo nodo. No obstante, de manera alternativa, la selección del algoritmo y la modificación de la clave se pueden distribuir, si se desea, en múltiples nodos de red. Dependiendo de la implementación del sistema, el cifrado real u otro procesado de seguridad puede estar ubicado conjuntamente o no con la funcionalidad de generación de clave. En este último caso, la clave específica de algoritmo, modificada, a usar en el algoritmo de cifrado puede que se tenga que transferir a un nodo independiente, en el cual se realiza el cifrado.

Para un sistema GSM, los nodos habilitadores de seguridad se corresponden típicamente con el BSC (Controlador de Estaciones Base) y el MSC/VLR (Centro de Conmutación de Móviles/Registro de Posiciones Visitadas). En el lado de la red doméstica, el HLR/AuC (Registro de Posiciones Domésticas/Centro de Autenticación) de la red GSM gestionará normalmente abonados e información relacionada con la seguridad. Naturalmente, el(los) nodo(s) 300 de red habilitador(es) de abonados puede(n) ser un HLR/AuC de un operador doméstico, que implique posiblemente un servidor de AAA (Autorización, Autenticación y Contabilidad) que puede estar ubicado conjuntamente o no con el centro de autenticación. No obstante, también puede ser un intermediario que actúe como un centro de autenticación general, o centro de identidad, para una serie de operadores de red diferentes. Básicamente, en el lado de la red, la solución propuesta únicamente requiere la extensión de los identificadores de algoritmo y la implementación de una modificación de clave específica de algoritmo en un lugar adecuado en el BSC o en el MSC/VLR. En el GSM, el cifrado real se ejecuta en la estación base BTS. Esto significa que la clave modificada se debe reenviar desde el BSC a la estación base para el cifrado real. Por tanto, la BTS se puede considerar también como parte del(de los) nodo(s) habilitador(es) de seguridad. Los parámetros convencionales de autenticación y de acuerdo de clave se obtienen típicamente del HLR/AuC.

Para un sistema GPRS/GSM, tanto la modificación de clave como el cifrado se implementan típicamente en el nodo SGSN (Nodo de Soporte de Servicio GPRS), el cual gestiona también la autenticación de abonados en la red visitada. El BSS (Sistema de Estaciones Base) GSM con su estación base BTS tiene por lo tanto un papel más pasivo en este contexto, en comparación con el caso del GSM puro.

Para un sistema W-LAN del 3GPP, los nodos habilitadores de seguridad se corresponden típicamente con el nodo AAA proxy y el WSN/FA (Nodo de Servicio de W-LAN), que interacciona con el Punto de Acceso (AP) de W-LAN. Los parámetros convencionales de autenticación y de acuerdo de clave se obtienen del HLR/AuC y un servidor AAA.

Para un sistema UMTS, el punto de acceso es el NodoB, y los nodos habilitadores de seguridad se corresponden con el RNC (Controlador de Red de Radiocomunicaciones) y los nodos MSC. En la red doméstica, el HLR/AuC se ocupa de la interacción necesaria con los nodos MSC y RNC.

Para un sub-sistema Multimedia IP, el nodo CSCF (Función de Control del Estado de las Llamadas) Proxy se corresponde con el nodo habilitador de seguridad, y puede incluir una modificación de clave específica del algoritmo para mejorar la seguridad para una señalización de control a nivel de aplicación. En las generaciones futuras del sistema IMS, los datos de usuario se pueden proteger también utilizando una modificación de clave según la invención. En la red doméstica, un nodo HSS (Sistema de Abonados Domésticos) proporciona los parámetros requeridos de autenticación y de acuerdo de clave, y el CSCF de Servicio normalmente autentica abonados IMS.

La Fig. 6 es un diagrama esquemático que ilustra una vista general del establecimiento del modo de cifrado mejorado y el procedimiento de modificación de clave según una realización ejemplificativa de la invención, en relación con el caso específico del GSM. En una marca de clase de MS similar a la normalizada en la TS24.008, se transfiere una lista de algoritmos soportados por el móvil desde el terminal móvil 100 al BSS (Sistema de Estaciones Base), preferentemente al BSC 310 a través de la estación base BTS 200, suponiendo que la decisión o negociación del algoritmo tiene lugar en el BSC. La lista de algoritmos soportados incluye preferentemente por lo menos los algoritmos de seguridad mejorados A5/1', A5/2', A5/3', aunque posiblemente también los algoritmos básicos A5/1, A5/2 y A5/3. El MSC 320 transfiere una lista de algoritmos permitidos por la política de seguridad de la red visitada al sistema BSS y, más particularmente, al BSC 310 en una orden CMC (Orden de Modo de Cifrado) similar a la normalizada en la TS48.008. A continuación, el sistema BSS, y especialmente el BSC 310, selecciona normalmente un algoritmo para la comunicación protegida con el terminal móvil basándose en la lista de algoritmos soportados y la lista de algoritmos permitidos y, si se selecciona un algoritmo de seguridad mejorado, preferentemente obtiene una clave de seguridad específica del algoritmo. El sistema BSS transmite también un identificador de algoritmo correspondiente al algoritmo seleccionado hacia el terminal móvil en una orden CMC de interfaz de radiocomunicaciones similar a la normalizada en la TS 44.018. Por ejemplo, la obtención de la clave se puede lograr calculando la clave modificada en el BSC 310 dependiendo del algoritmo seleccionado. Alternativamente, el MSC 320 calcula claves modificadas específicas del algoritmo para todos los algoritmos permitidos por la red visitada y las transfiere, preferentemente en relación con la orden CMC, al BSC, el cual a su vez selecciona el algoritmo y extrae la clave apropiada de entre el conjunto calculado de claves. En el GSM, el cifrado real se realiza por medio de la estación base BTS 200 del sistema BSS. En este caso, el terminal móvil 100 está provisto de una funcionalidad de modificación de clave según la invención y aplica el identificador de algoritmo, posiblemente junto con información adicional, en la función de modificación de clave para generar una clave específica de algoritmo, correspondiente, que se usará para el cifrado.

Tal como se ha mencionado previamente, la selección del algoritmo realizada por la red visitada se puede comprobar con respecto a una política de seguridad de la red doméstica, de tal manera que se pueda garantizar que el algoritmo seleccionado es aceptado por la red doméstica. Normalmente, esto significa que se transfiere una lista de algoritmos permitidos por la red doméstica hacia el terminal móvil. Esta información preferentemente está protegida en cuanto a integridad de manera que el móvil pueda estar seguro de que la información no ha sido manipulada indebidamente, tal como se describirá posteriormente.

La invención también proporciona preferentemente soporte para protección contra repeticiones, autenticación de red básica y/o selección segura de algoritmos, preferentemente basándose en la codificación o inserción de información en información de AKA existente tal como el RAND de desafío aleatorio usado en el procedimiento de AKA con el terminal móvil. Si también se pueden aceptar modificaciones en el AuC o el nodo correspondiente en el lado de la red doméstica, se pueden lograr una protección contra repeticiones, una autenticación de red así como otras mejoras en la seguridad tal como se describirá posteriormente.

Se supone que el valor de RAND es aleatorio, pero es posible usar unos pocos bits de RAND para señalizar alguna información adicional desde la red doméstica (AuC) al terminal con el fin de mejorar adicionalmente la seguridad. Las realizaciones anteriores arreglan los problemas con la exclusividad de clave por algoritmo, pero en general no eliminan los problemas con la repetición o falta de autenticación de red. La solución ejemplificativa a continuación logra esto con cambios adicionales mínimos (solamente en el AuC y el terminal) y sin señalización nueva.

La Fig. 7 es un diagrama de señales básico y esquemático según otra realización preferida, ejemplificativa, de la invención, que incluye mejoras del algoritmo de seguridad con protección contra repeticiones y autenticación de red integradas. Para simplificar, el siguiente ejemplo está relacionado con el caso del GSM, aunque los mecanismos descritos no se limitan al mismo, tal como entenderán fácilmente los expertos.

1. El terminal señaliza qué algoritmos actualizados soporta, preferentemente junto con su ID de abonado, a la red visitada y el nodo MSC/VLR.

2. La red visitada reenvía la ID de abonado a la red doméstica, y, más particularmente, al HLR/AuC o el nodo correspondiente.

3. En esta realización particular, el AuC forma valores de RAND de la manera siguiente. (Suponiendo que RAND tiene normalmente un tamaño de 128).

A. El AuC mantiene para cada móvil (SIM) un contador, c, del número de autenticaciones realizadas para dicho móvil. Este contador puede tener, por ejemplo, un tamaño de t = 16 bits, que se permite que se reinicialice en módulo 2^16. El contador c es un ejemplo representativo de información de protección contra repeticiones.

B. Se genera un valor aleatorio R de (128-t-m) bits, en el AuC, donde posteriormente se determina m.

C. El valor r = R ‖c‖00...0 (tantos ceros como sea necesario para conseguir que el tamaño de r sea 128 bits, es decir, m bits) se hace pasar a través de la función de generación de clave del GSM, obteniendo una

clave k. Alternativamente, se puede usar algún otro esquema de relleno. De manera más general, r es una función f de R y c y posiblemente también otra información opcional.

D. Se forma el valor RAND = r‖MAC(k, r) y el mismo se usa para generar la clave de cifrado Kc y la respuesta esperada XRES. En este caso, MAC (Código de Autenticación de Mensaje) es una función de autenticación de mensajes, por ejemplo, HMAC, truncada a m bits, por ejemplo, m = 32. El MAC es un ejemplo representativo de información de autenticación de red.

4-5. El RAND se envía al móvil de la manera habitual (y Kc, XRES se envía a la red visitada).

6. El AuC incrementa c en uno. En el lado del terminal, se realizan preferentemente las siguientes acciones:

A. El móvil mantiene también un contador c', del número de autenticaciones que ha realizado.

B. Cuando el móvil recibe RAND, extrae r y c del mismo.

C. El móvil comprueba que c está "delante" (véase posteriormente) de su valor de c' local. En caso negativo, aborta el protocolo.

D. Si no, el móvil envía a continuación r al SIM, y obtiene k (reutilizando el SIM).

E. El móvil comprueba si MAC es correcto calculando XMAC(k, r) y comparando MAC y XMAC. Si MAC no es correcto, el móvil aborta el protocolo.

F. Por otro lado, si el MAC es correcto, se ha verificado la autenticidad de la red. El móvil actualiza también su contador fijando c' = c.

7. El móvil invoca nuevamente el SIM, pero ahora con el RAND completo como entrada para obtener RES y Kc.

8. El terminal envía RES al lado de la red.

9. La red visitada normalmente comprueba RES por comparación con la XRES recibida desde la red doméstica, para autenticar el terminal.

10. La red visitada selecciona uno de los algoritmos mejorados actualizados soportados por el terminal e inicia el cifrado.

11. La red visitada envía la ID de algoritmo al terminal.

12. El terminal inicia el cifrado basándose en el algoritmo actualizado seleccionado que incluye una modificación de clave dependiente del algoritmo.

El móvil ahora se puede comunicar con la red visitada. Obsérvese que, debido a las propiedades seudo-aleatorias de la función MAC, la reducción de la entropía relativa de RAND es pequeña, básicamente se pierden solo los bits correspondientes al contador.

Para comprobar si c está "delante" se usa una aritmética normal de números secuenciales. Dos valores de t bits, a y b, se comparan de la manera siguiente. Si

$$a > b \text{ y } a-b < 2^{(t-1)},$$

o

$$a < b \text{ pero } b-a > 2^{(t-1)}$$

entonces se dice que a está "delante" de b, en cualquier otro caso no lo está. Una solución alternativa podría ser usar una indicación de tiempo como información de protección contra repeticiones en lugar de un contador.

Como el MAC se calcula sobre r el cual incluye el valor c, se producirá cierta protección de integridad también para estos datos. Se observa que si un atacante modifica la información de protección contra repeticiones, el MAC no se puede verificar y el protocolo será abortado. De todos modos, con independencia de si se usa o no un MAC, el valor de RAND ya no será el mismo, dando como resultado una RES incorrecta que no coincide con la respuesta esperada XRES en el lado de la red. Por tanto, no existe ninguna posibilidad de autenticación satisfactoria del usuario si alguien ha manipulado indebidamente el valor de RAND.

Alternativamente, los aspectos de protección contra repeticiones y de autenticación de red se pueden separar y ejecutar de manera independiente entre sí. Para la protección contra repeticiones, se puede codificar un valor de contador o una indicación de tiempo, o el mismo se puede insertar de otra manera en el valor de RAND. Para una

autenticación de red básica, se calcula, en el lado de la red, información de autenticación dependiente de la clave, tal como un código MAC o similar, y la misma se transmite al terminal móvil para su verificación.

También son posibles otras mejoras combinando los fundamentos anteriores con algunas ideas adicionales que ya han sido propuestas, por ejemplo, en la contribución [2]. Por ejemplo, se pueden asignar unos pocos bits adicionales de RAND para señalizar una política de seguridad desde la red doméstica al móvil.

En la invención, por ejemplo, el bit j:ésimo de RAND se puede fijar a 1 si y solo si se permite usar el número de algoritmo j (según cierta numeración acordada de algoritmos) por parte del móvil. De este modo, se puede comunicar, insertada en el RAND, una lista completa de algoritmos permitidos por la red doméstica. A continuación, el terminal móvil puede comprobar si el algoritmo seleccionado por la red visitada es aceptado por la red doméstica. En caso negativo, el terminal móvil abortará el protocolo. También es posible y deseable proporcionar protección de integridad calculando un MAC sobre la información sobre algoritmos de seguridad permitidos por la red doméstica.

Por lo tanto, si se desea, la protección contra repeticiones, la autenticación de red y la selección segura de algoritmos se pueden integrar todas ellas, por ejemplo, dejando el valor r = R ‖c‖algoritmos permitidos‖00...0 (tantos ceros como se requiera para hacer que r tenga, por ejemplo, un tamaño de 128 bits). El valor RAND = r ‖ MAC(k, r) se forma y se usa para generar la clave de cifrado Kc, y la respuesta esperada XRES. El valor r, el valor de contador c así como la información sobre algoritmos permitidos por la red doméstica son extraídos por el móvil, y se comprueba el MAC.

Una ventaja de la invención es que la solución puede coexistir con otras propuestas, incluyendo aquellas que se exponen en líneas generales en las referencias [2, 3]. Aunque las propuestas [2, 3] sí mejoran varios aspectos de seguridad, ninguna de ella proporciona la separación de claves deseada. Esto significa que si los algoritmos X e Y están ambos permitidos y son soportados, entonces el móvil potencialmente puede acabar ejecutando tanto X como Y con la misma clave, Kc.

En comparación con las realizaciones básicas de modificación de clave, en la protección contra repeticiones, la autenticación de red y/o la selección segura de algoritmos, el único nodo adicional que necesita modificaciones es el HLR/AuC en el lado de la red. En redes de tercera generación, el nodo CSCF (Función de Control de Estados de Llamada) en el sub-sistema Multimedia IP necesita actualizarse en las realizaciones básicas de modificación de clave, y con la protección contra repeticiones, la autenticación de red y/o la selección segura de algoritmos, el nodo HSS (Sistema de Abonados Domésticos) también requiere modificación.

Las realizaciones descritas anteriormente se ofrecen simplemente como ejemplos.

Referencias

[1] "Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication" de Barkan, Biham, y Keller, Proceedings of Crypto 2003, Lecture Notes in Computer Science vol. 2729, Springer-Verlag.

[2] "Cipher key separation for A/Gb security enhancements", S3-030463, 3GPP S3#29, 15 a 18 de julio de 2003, San Francisco, USA.

[3] "Enhanced Security for A/Gb", S3-030361, 3GPP S3#29, 15 a 18 de julio de 2003, San Francisco, USA.

REIVINDICACIONES

1. Método de mejora de la seguridad para una comunicación protegida basada en un procedimiento de acuerdo de clave (S 1) en una red de comunicaciones de móviles que presta servicio a un terminal móvil (100) que tiene por lo menos un algoritmo de seguridad criptográfico básico, comprendiendo dicho método las etapas de:

   - seleccionar una versión mejorada de un algoritmo de seguridad criptográfico básico para la comunicación entre el terminal móvil y el lado de la red (S2);

   - modificar una clave de seguridad básica resultante del procedimiento de acuerdo de clave en función de información representativa del algoritmo seleccionado para generar una clave de seguridad específica de algoritmo (S3);

   - aplicar el algoritmo de seguridad criptográfico básico con la clave de seguridad específica del algoritmo como entrada de clave para mejorar la seguridad para la comunicación protegida en dicha red de comunicaciones de móviles (S4).

2. Método de la reivindicación 1, en el que dicha etapa de seleccionar una versión mejorada de un algoritmo de seguridad criptográfico básico se realiza en el lado de la red, y dicho método comprende además la etapa de transmitir información representativa del algoritmo seleccionado al terminal móvil.

3. Método de la reivindicación 1, en el que dicha etapa de seleccionar una versión mejorada de un algoritmo de seguridad criptográfico básico se basa en un acuerdo entre dicho terminal móvil y dicha red.

4. Método de la reivindicación 1, en el que dichas etapas de modificar una clave de seguridad básica y aplicar el algoritmo de seguridad criptográfico básico con la clave específica del algoritmo como entrada de clave se realizan tanto en el lado de la red como en el terminal móvil.

5. Método de la reivindicación 1, en el que el algoritmo de seguridad básico junto con la modificación, específica del algoritmo, de dicha clave de seguridad básica se corresponden con la versión mejorada del algoritmo de seguridad.

6. Método de la reivindicación 1, en el que dicho terminal móvil modifica la clave de seguridad básica resultante del procedimiento de acuerdo de clave en función de dicha información representativa del algoritmo seleccionado, y reenvía la clave de seguridad modificada a un motor criptográfico para el algoritmo de seguridad básico en dicho terminal móvil.

7. Método de la reivindicación 1, en el que dicha información representativa del algoritmo seleccionado es un identificador de algoritmo que identifica la versión mejorada seleccionada del algoritmo de seguridad.

8. Método de la reivindicación 1, en el que dicha etapa de seleccionar una versión mejorada del algoritmo de seguridad se basa en una lista de algoritmos soportados del terminal móvil y una lista de algoritmos permitidos por la red.

9. Método de la reivindicación 1, en el que dichos algoritmos de seguridad se configuran para por lo menos una de confidencialidad de datos, integridad de datos y autenticación.

10. Método de la reivindicación 9, en el que dichos algoritmos de seguridad se configuran para una comunicación cifrada en dicha red de comunicaciones de móviles.

11. Método de la reivindicación 1, que comprende además las etapas de:

   - insertar, por parte de dicho lado de la red, información de protección contra repeticiones, en un desafío aleatorio, RAND, usado para la autenticación y el acuerdo de clave con el terminal móvil;

   - extraer de dicho desafío aleatorio, por parte de dicho terminal móvil, dicha información de protección contra repeticiones; y

   - realizar, por parte de dicho terminal móvil, una comprobación de la protección contra repeticiones basándose en la información extraída de protección contra repeticiones.

12. Método de la reivindicación 11, en el que dicha información de protección contra repeticiones se basa en un contador o se basa en el tiempo.

13. Método de la reivindicación 1, que comprende además las etapas de:

   - generar, por parte de dicho lado de la red, información de autenticación dependiente de la clave, por lo menos parcialmente basándose en una clave secreta compartida entre el terminal móvil y el lado de la red;

- insertar, por parte de dicho lado de la red, dicha información de autenticación dependiente de la clave en el desafío aleatorio, RAND, usado para la autenticación y el acuerdo de clave con el terminal móvil;

- extraer de dicho desafío aleatorio, por parte de dicho terminal móvil, dicha información de autenticación dependiente de la clave; y

- comprobar, por parte de dicho terminal móvil, dicha información de autenticación dependiente de la clave por lo menos parcialmente basándose en dicha clave secreta compartida, para verificar la autenticidad de la red.

14. Método de la reivindicación 13, en el que dichas etapas de generar información de autenticación dependiente de la clave y comprobar dicha información de autenticación dependiente de la clave se realizan basándose por lo menos parcialmente en un valor aleatorio iniciado desde el lado de la red y una clave derivada localmente a partir de dicha clave secreta compartida, insertándose dicho valor aleatorio en dicho desafío aleatorio, RAND, junto con dicha información de autenticación dependiente de la clave.

15. Método de la reivindicación 13, en el que dichas etapas de generar información de autenticación dependiente de la clave y comprobar dicha información de autenticación dependiente de la clave se realizan basándose por lo menos parcialmente en dicha clave secreta compartida y por lo menos un elemento de información, insertándose dicho por lo menos un elemento de información en dicho desafío aleatorio, RAND, junto con dicha información de autenticación dependiente de la clave, protegiendo así, en cuanto a integridad, dicho por lo menos un elemento de información.

16. Método de la reivindicación 15, en el que dicho por lo menos un elemento de información incluye información de protección contra repeticiones.

17. Método de la reivindicación 15, en el que dicha etapa de seleccionar una versión mejorada del algoritmo de seguridad es realizada por una red visitada, dicho por lo menos un elemento de información incluye información sobre algoritmos de seguridad permitidos por una red doméstica del terminal móvil, y dicho terminal móvil comprueba si el algoritmo de seguridad seleccionado por la red visitada está permitido por la red doméstica.

18. Método de la reivindicación 1, en el que dicha etapa de modificar una clave de seguridad básica se realiza basándose en una función de modificación criptográfica implementada por software, sensible a la clave de seguridad básica, e información representativa del algoritmo seleccionado.

19. Disposición para mejorar la seguridad para una comunicación protegida basada en un procedimiento de acuerdo de clave en una red de comunicaciones de móviles que presta servicio a un terminal móvil (100) que tiene por lo menos un algoritmo de seguridad básico, comprendiendo dicha disposición:

- medios para seleccionar una versión mejorada de un algoritmo (24) de seguridad criptográfico básico para la comunicación entre el terminal móvil y el lado de la red;

- medios para modificar una clave de seguridad básica resultante del procedimiento de acuerdo de clave en función de información representativa del algoritmo seleccionado, para generar una clave de seguridad específica del algoritmo;

- medios para aplicar el algoritmo (24) de seguridad criptográfico básico con la clave de seguridad específica del algoritmo como entrada de clave para mejorar la seguridad para la comunicación protegida en dicha red de comunicaciones de móviles.

20. Disposición de la reivindicación 19, en la que dichos medios de selección comprenden medios para seleccionar, en el lado de la red, dicha versión mejorada de un algoritmo de seguridad criptográfico básico para la comunicación con el terminal móvil, y dicha disposición comprende además medios para transmitir información representativa del algoritmo seleccionado al terminal móvil.

21. Disposición de la reivindicación 19, en la que dichos medios de selección comprenden medios para negociar entre dicho terminal móvil y dicha red con el fin de seleccionar una versión mejorada de un algoritmo de seguridad criptográfico básico.

22. Disposición de la reivindicación 19, en la que dichos medios para modificar una clave de seguridad básica y dichos medios para aplicar el algoritmo de seguridad criptográfico básico con la clave de seguridad específica del algoritmo como entrada de clave están implementados tanto en el lado de la red como en el terminal móvil.

23. Disposición de la reivindicación 19, en la que el algoritmo de seguridad básico junto con la modificación, específica del algoritmo, de dicha clave de seguridad básica se corresponden con la versión mejorada del algoritmo de seguridad.

24. Disposición de la reivindicación 19, en la que dicho terminal móvil se puede hacer funcionar para modificar la clave de seguridad básica resultante del procedimiento de acuerdo de clave en función de la información representativa del algoritmo seleccionado, y para reenviar la clave de seguridad modificada a un motor criptográfico para el algoritmo de seguridad básico.

25. Disposición de la reivindicación 19, en la que dichos medios para seleccionar una versión mejorada del algoritmo de seguridad funcionan basándose en una lista de algoritmos soportados del terminal móvil y una lista de algoritmos permitidos por la red.

26. Disposición de la reivindicación 20, en la que un nodo de red se puede hacer funcionar para seleccionar una versión mejorada de un algoritmo de seguridad básico y modificar la clave de seguridad en el lado de la red, y para comunicar información representativa del algoritmo seleccionado al terminal móvil.

27. Disposición de la reivindicación 20, en la que un primer nodo de red se puede hacer funcionar para calcular, para cada uno de una pluralidad de algoritmos de seguridad criptográficos, una clave de seguridad específica del algoritmo y para transferir el conjunto calculado de claves de seguridad específicas del algoritmo a un segundo nodo de red, pudiéndose hacer funcionar dicho segundo nodo de red para seleccionar una versión mejorada de un algoritmo de seguridad básico y para extraer una clave de seguridad a partir de dicho conjunto de claves de seguridad específicas de algoritmo.

28. Disposición de la reivindicación 19, en la que dichos algoritmos de seguridad están configurados para una comunicación cifrada en dicha red de comunicaciones de móviles.

29. Disposición de la reivindicación 19, que comprende además:

- medios para insertar, en el lado de la red, información de protección contra repeticiones, en un desafío aleatorio, RAND, usado para la autenticación y el acuerdo de clave con el terminal móvil;

- medios para extraer de dicho desafío aleatorio, en dicho terminal móvil, dicha información de protección contra repeticiones; y

- medios para realizar, en dicho terminal móvil, una comprobación de la protección contra repeticiones basándose en la información extraída de protección contra repeticiones.

30. Disposición de la reivindicación 19, que comprende además:

- medios para generar, en el lado de la red, información de autenticación dependiente de la clave, por lo menos parcialmente basándose en una clave secreta compartida entre el terminal móvil y el lado de la red;

- medios para insertar, en el lado de la red, dicha información de autenticación dependiente de la clave en el desafío aleatorio, RAND, usado para la autenticación y el acuerdo de clave con el terminal móvil;

- medios para extraer de dicho desafío aleatorio, en dicho terminal móvil, dicha información de autenticación dependiente de la clave; y

- medios para comprobar, en dicho terminal móvil, dicha información de autenticación dependiente de la clave por lo menos parcialmente basándose en dicha clave secreta compartida, para verificar la autenticidad de la red.

31. Disposición de la reivindicación 19, en la que dichos medios para modificar una clave de seguridad básica se proporcionan como una actualización de software.

32. Terminal móvil (100) para su funcionamiento en una red de comunicaciones de móviles, comprendiendo dicho terminal:

- una funcionalidad (10) de autenticación y acuerdo de clave, AKA;

- un motor para un algoritmo (24) de seguridad criptográfico básico;

- medios para modificar una clave de seguridad básica a partir de dicha funcionalidad AKA en respuesta a información representativa de un algoritmo de seguridad criptográfico seleccionado, con el fin de generar una clave de seguridad específica del algoritmo para introducirla en dicho motor de algoritmo de seguridad criptográfico básico con el fin de mejorar la seguridad para una comunicación protegida en dicha red de comunicaciones de móviles.

33. Terminal móvil de la reivindicación 32, en el que el algoritmo de seguridad seleccionado es una versión mejorada del algoritmo de seguridad criptográfico básico, y la versión mejorada del algoritmo de seguridad básico se selecciona desde el lado de la red, y dicho terminal móvil se puede hacer funcionar para recibir información representativa del algoritmo seleccionado desde el lado de la red.

34. Terminal móvil de la reivindicación 32, en el que el algoritmo de seguridad criptográfico básico junto con la modificación de dicha clave de seguridad básica en una clave de seguridad específica del algoritmo se corresponden con un algoritmo de seguridad criptográfico mejorado.

35. Terminal móvil de la reivindicación 32, en el que dichos medios para modificar una clave de seguridad básica se proporcionan como una actualización de software en el terminal móvil.

36. Nodo (300) de red para su funcionamiento en una red de comunicaciones de móviles que presta servicio a un terminal móvil (100) que soporta por lo menos un algoritmo (24) de seguridad criptográfico básico, comprendiendo dicho nodo de red:

- medios para obtener, a partir de una clave de seguridad básica resultante de un procedimiento de acuerdo de clave, una clave de seguridad específica del algoritmo, correspondiente a una versión mejorada del algoritmo de seguridad criptográfico básico para su introducción en el algoritmo (24) de seguridad criptográfico básico con el fin de mejorar la seguridad para una comunicación protegida en dicha red de comunicaciones de móviles.

37. Nodo de red de la reivindicación 36, que comprende además medios para seleccionar dicha versión mejorada de un algoritmo de seguridad criptográfico básico para una comunicación protegida con un terminal móvil.

38. Nodo de red de la reivindicación 37, en el que dichos medios para obtener una clave de seguridad específica del algoritmo comprenden medios para modificar una clave de seguridad básica resultante de un procedimiento de acuerdo de clave en dicha red de comunicaciones de móviles en función de información representativa del algoritmo seleccionado.

39. Nodo de red de la reivindicación 38, en el que dichos medios para modificar una clave de seguridad básica se proporcionan como una actualización de software en el nodo de red.

40. Nodo de red de la reivindicación 36, en el que dichos medios para obtener una clave de seguridad específica del algoritmo comprenden medios para seleccionar una clave de seguridad a partir de un conjunto pre-calculado de claves de seguridad específicas de algoritmo correspondientes a una pluralidad de algoritmos de seguridad.

41. Nodo de red de la reivindicación 37, que comprende además medios para comunicar, al terminal móvil, información específica del algoritmo, correspondiente al algoritmo seleccionado.

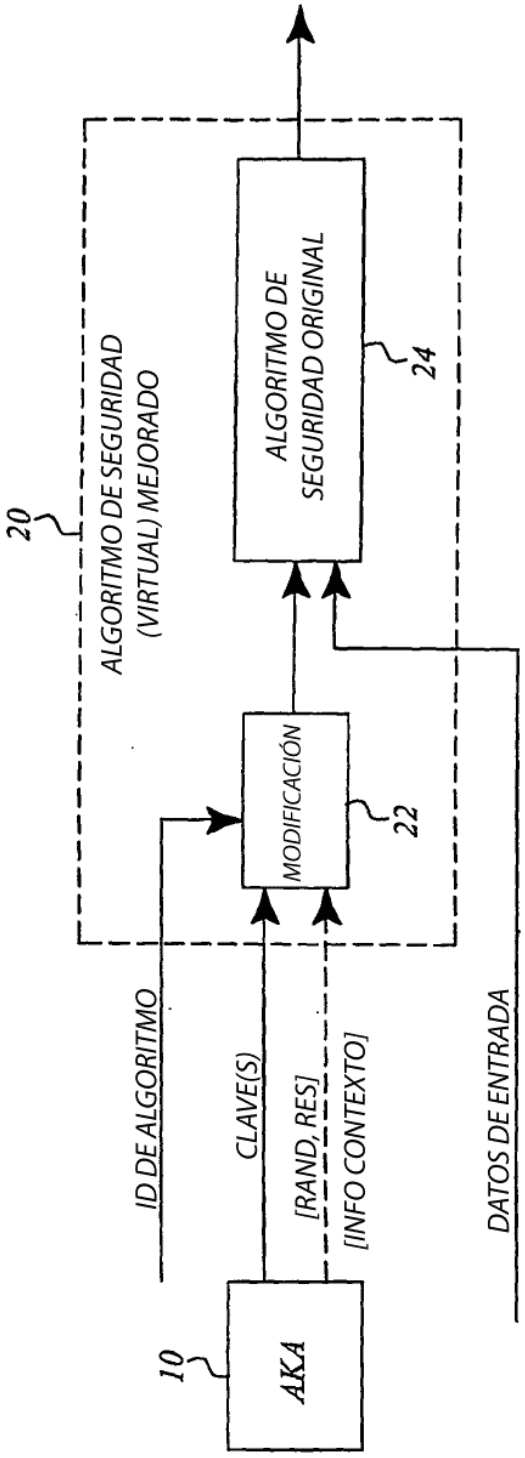
20
ALGORITMO DE SEGURIDAD (VIRTUAL) MEJORADO
ALGORITMO DE SEGURIDAD ORIGINAL
24
MODIFICACIÓN
22
ID DE ALGORITMO
CLAVE(S)
[RAND, RES]
[INFO CONTEXTO]
DATOS DE ENTRADA
10
AKA

Fig. 1

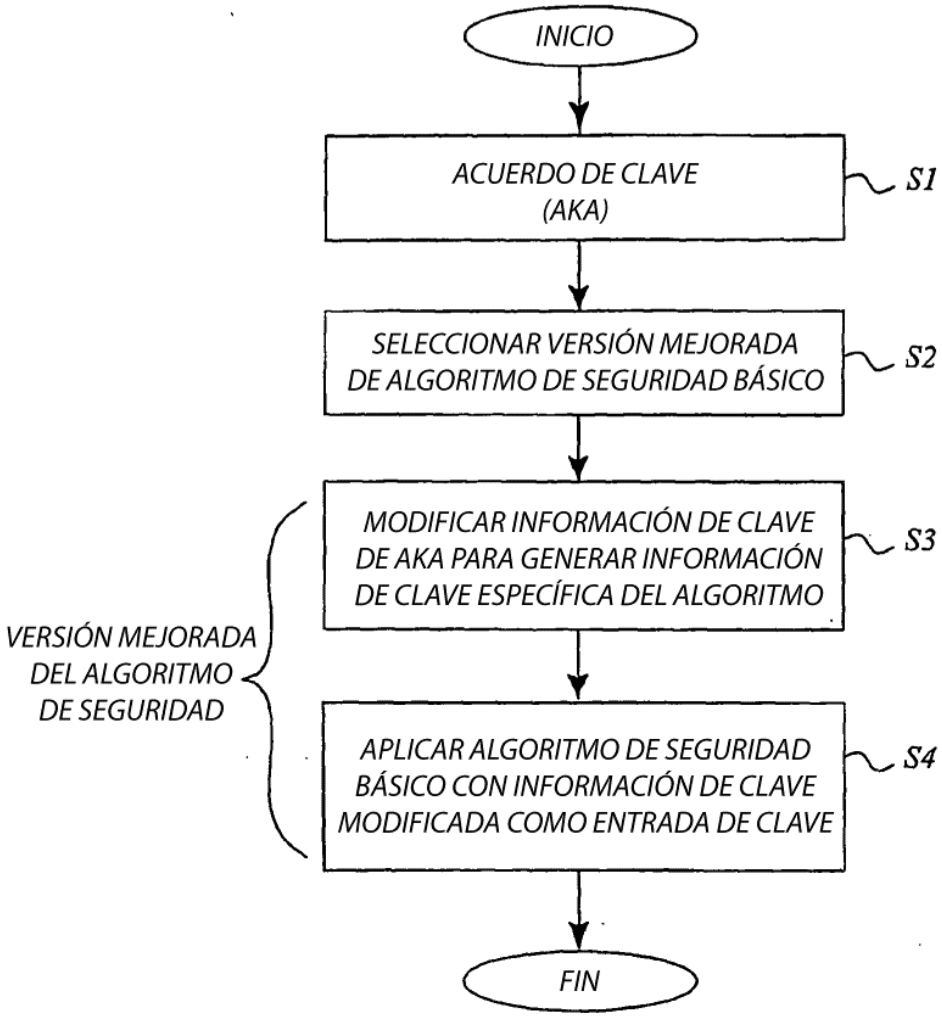
INICIO
ACUERDO DE CLAVE (AKA)
S1
SELECCIONAR VERSIÓN MEJORADA DE ALGORITMO DE SEGURIDAD BÁSICO
S2
MODIFICAR INFORMACIÓN DE CLAVE DE AKA PARA GENERAR INFORMACIÓN DE CLAVE ESPECÍFICA DEL ALGORITMO
S3
VERSIÓN MEJORADA DEL ALGORITMO DE SEGURIDAD
APLICAR ALGORITMO DE SEGURIDAD BÁSICO CON INFORMACIÓN DE CLAVE MODIFICADA COMO ENTRADA DE CLAVE
S4
FIN

Fig. 2

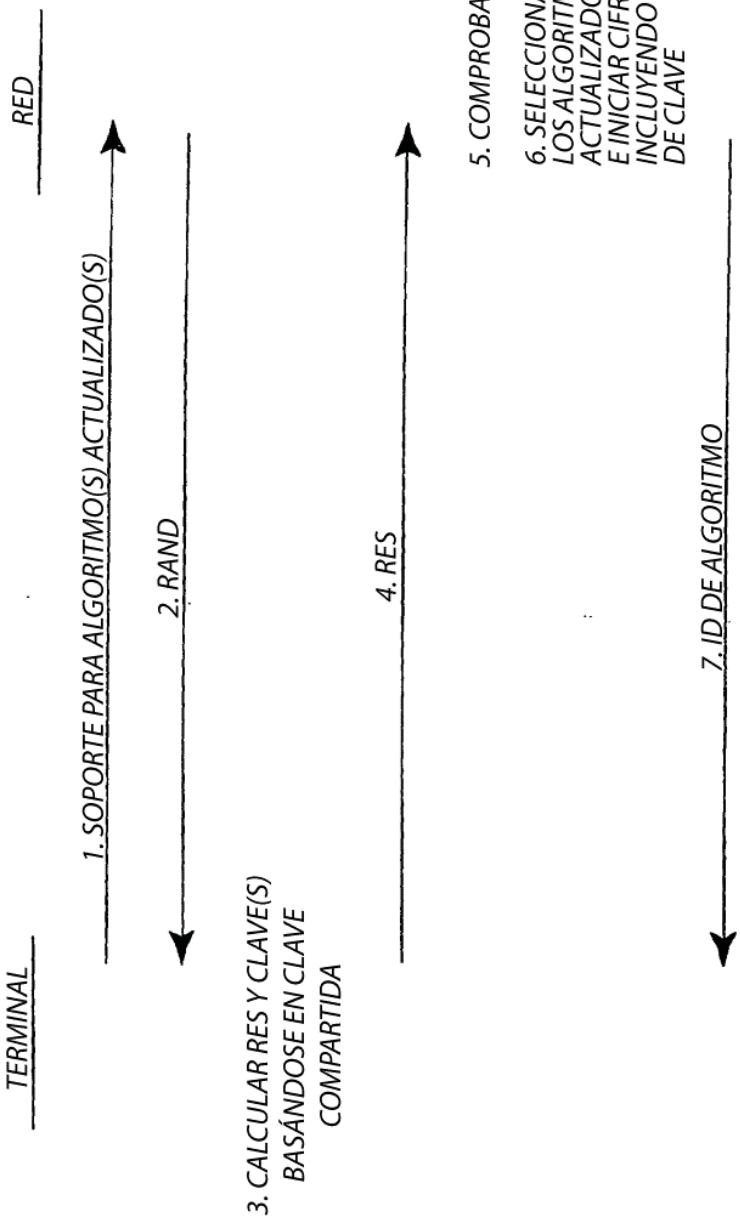
TERMINAL
RED
1. SOPORTE PARA ALGORITMO(S) ACTUALIZADO(S)
2. RAND
3. CALCULAR RES Y CLAVE(S) BASÁNDOSE EN CLAVE COMPARTIDA
4. RES
5. COMPROBAR RES
6. SELECCIONAR UNO DE LOS ALGORITMOS ACTUALIZADOS SOPORTADOS E INICIAR CIFRADO INCLUYENDO MODIFICACIÓN DE CLAVE
7. ID DE ALGORITMO
8. INICIAR CIFRADO BASÁNDOSE EN ALGORITMO ACTUALIZADO SELECCIONADO INCLUYENDO MODIFICACIÓN DE CLAVE

Fig. 3

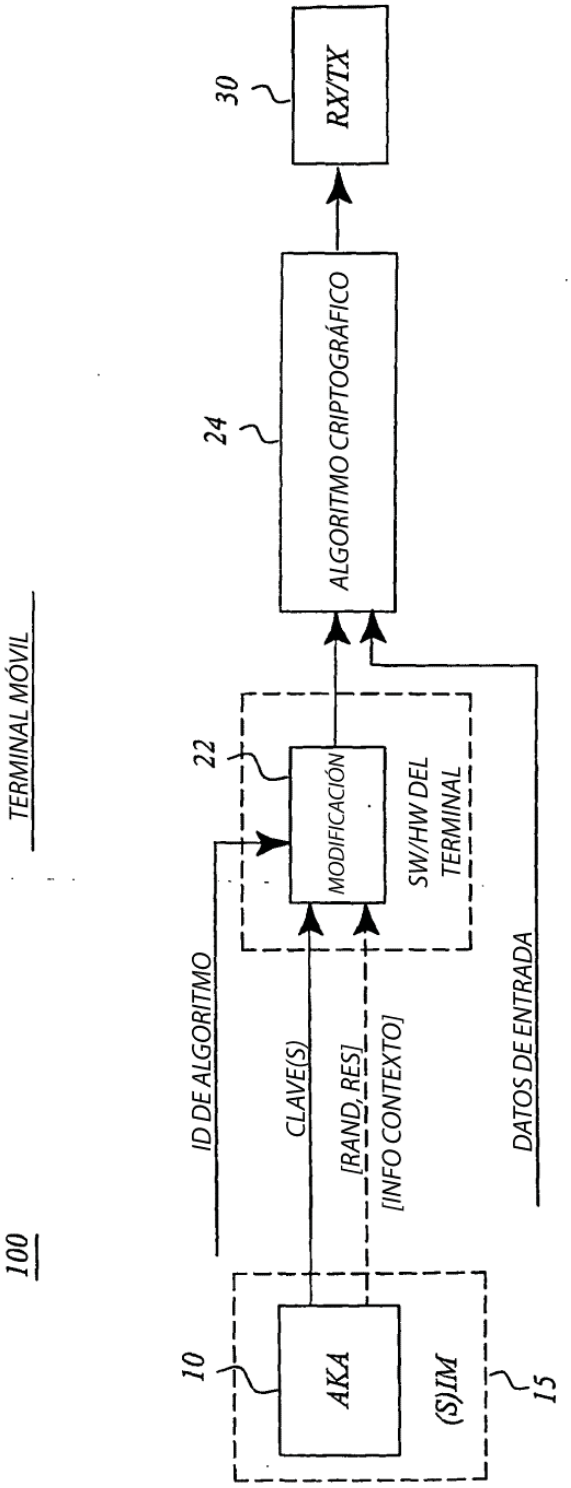
100
TERMINAL MÓVIL
10
AKA
(S)IM
15
ID DE ALGORITMO
CLAVE(S)
[RAND, RES]
[INFO CONTEXTO]
22
MODIFICACIÓN
SW/HW DEL TERMINAL
24
ALGORITMO CRIPTOGRÁFICO
DATOS DE ENTRADA
30
RX/TX

Fig. 4

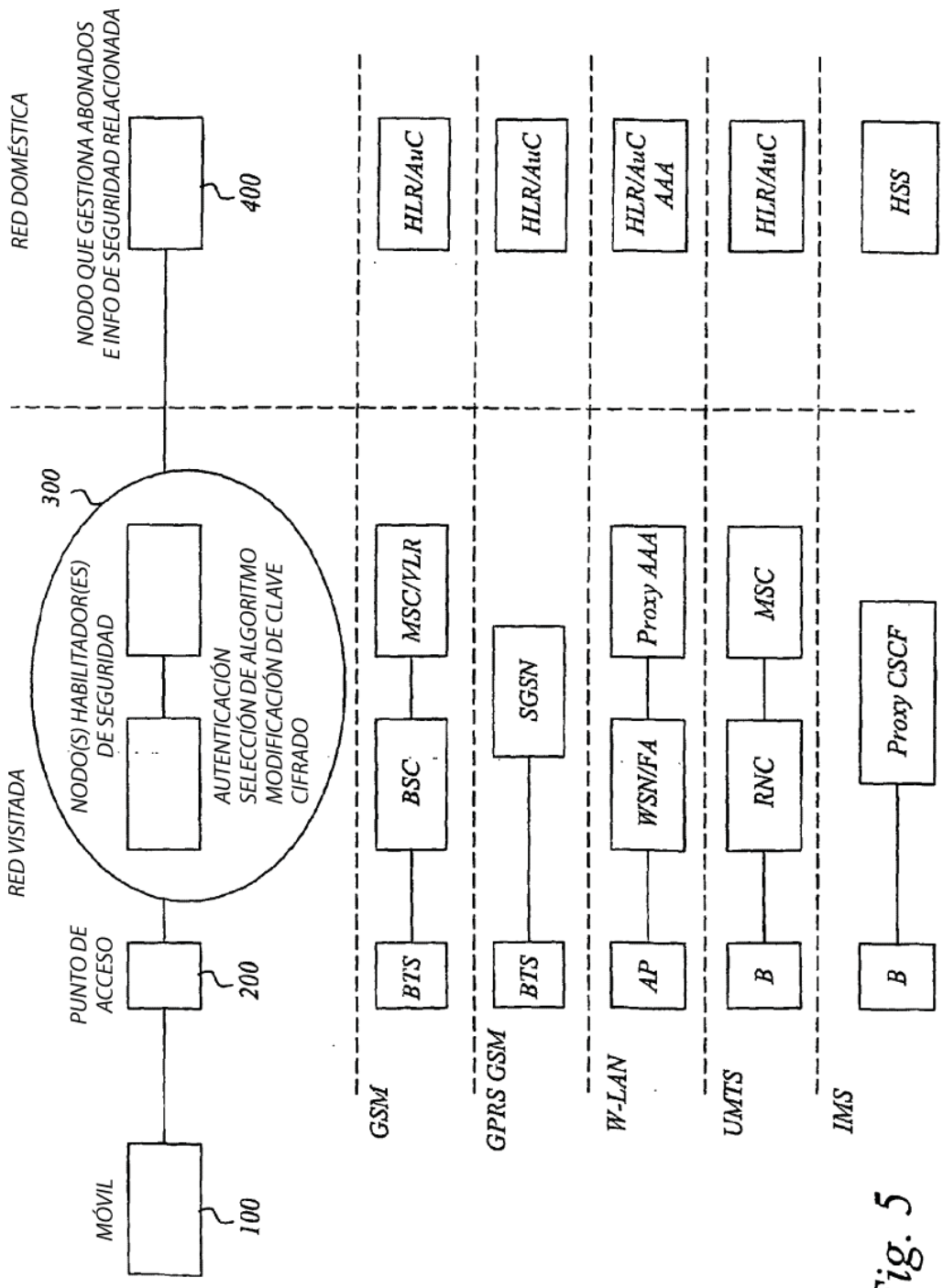
RED DOMÉSTICA
NODO QUE GESTIONA ABONADOS E INFO DE SEGURIDAD RELACIONADA
400
300
RED VISITADA
NODO(S) HABILITADOR(ES) DE SEGURIDAD
AUTENTICACIÓN
SELECCIÓN DE ALGORITMO
MODIFICACIÓN DE CLAVE
CIFRADO
PUNTO DE ACCESO
200
MÓVIL
100
GSM
BTS
BSC
MSC/VLR
HLR/AuC
GPRS GSM
BTS
SGSN
HLR/AuC
W-LAN
AP
WSN/FA
Proxy AAA
HLR/AuC AAA
UMTS
B
RNC
MSC
HLR/AuC
IMS
B
Proxy CSCF
HSS

Fig. 5

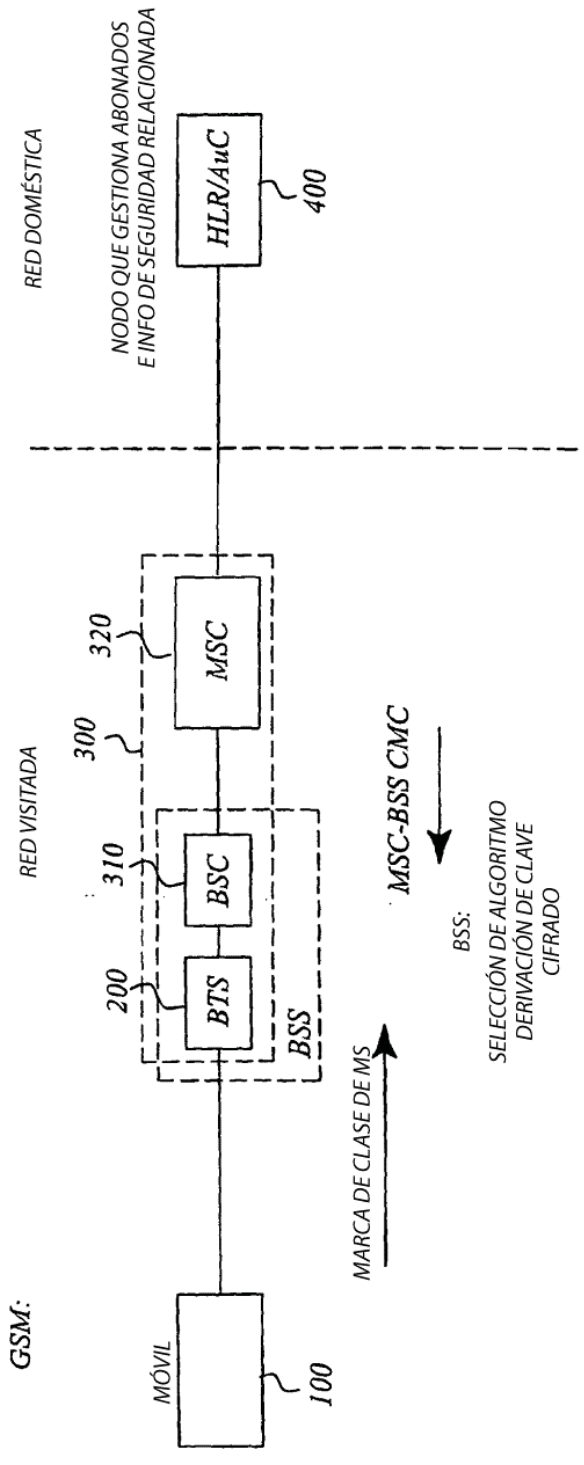
GSM:
MÓVIL
100
BTS
BSC
BSS
200
310
RED VISITADA
300
MSC
320
RED DOMÉSTICA
NODO QUE GESTIONA ABONADOS E INFO DE SEGURIDAD RELACIONADA
HLR/AuC
400
MARCA DE CLASE DE MS
MSC-BSS CMC
BSS:
SELECCIÓN DE ALGORITMO
DERIVACIÓN DE CLAVE
CIFRADO
INTERFAZ DE RADIOCOMUNICACIONES
CMC
MODIFICACIÓN DE CLAVE
CIFRADO

Fig. 6

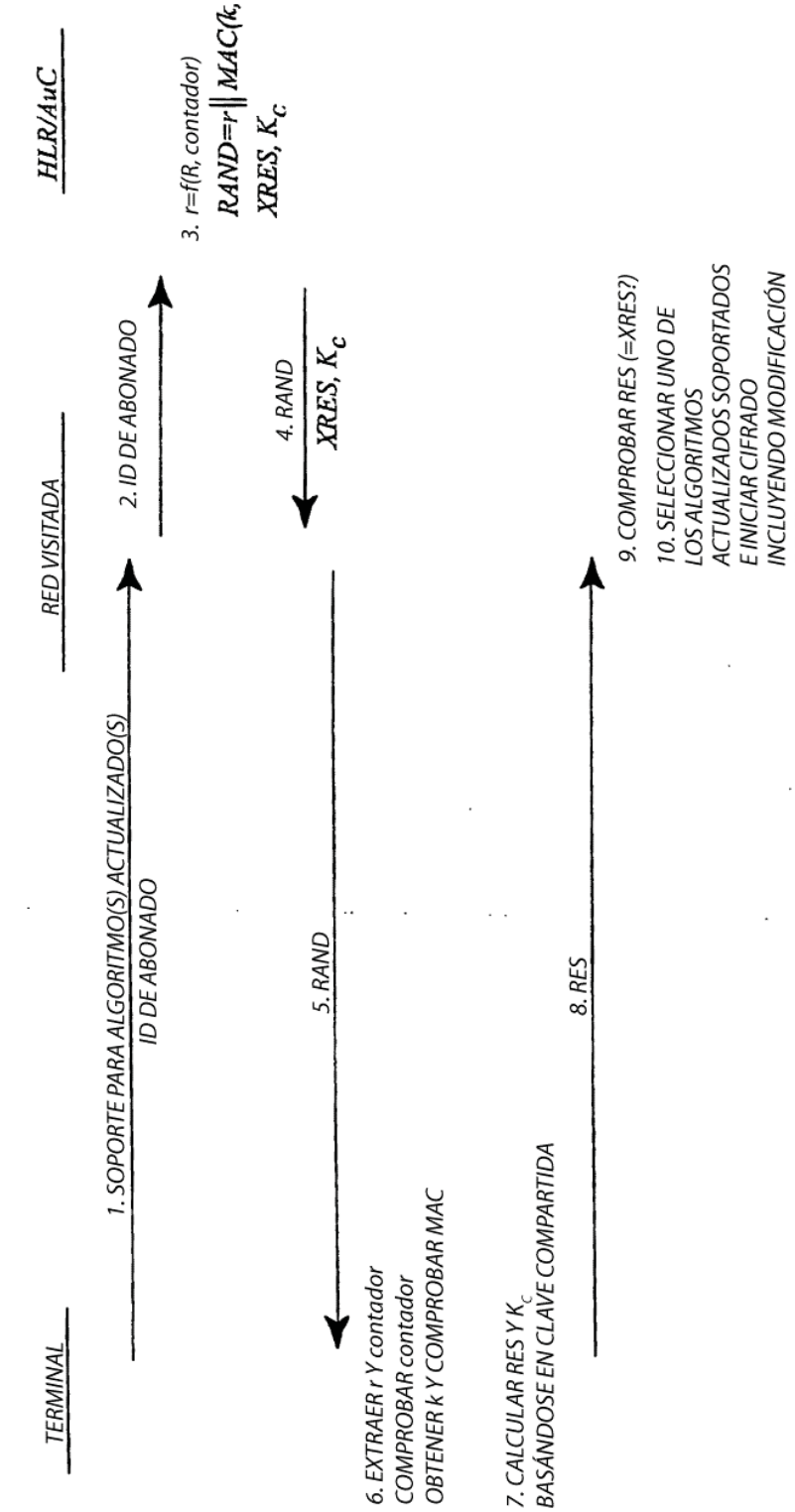
TERMINAL
RED VISITADA
HLR/AuC
1. SOPORTE PARA ALGORITMO(S) ACTUALIZADO(S)
ID DE ABONADO
2. ID DE ABONADO
3. r=f(R, contador)
RAND=r||MAC(k, r)
XRES, Kc
4. RAND
XRES, Kc
5. RAND
6. EXTRAER r Y contador
COMPROBAR contador
OBTENER k Y COMPROBAR MAC
7. CALCULAR RES Y Kc
BASÁNDOSE EN CLAVE COMPARTIDA
8. RES
9. COMPROBAR RES (=XRES?)
10. SELECCIONAR UNO DE
LOS ALGORITMOS
ACTUALIZADOS SOPORTADOS
E INICIAR CIFRADO
INCLUYENDO MODIFICACIÓN
DE CLAVE
11. ID DE ALGORITMO
12. INICIAR CIFRADO BASÁNDOSE EN
ALGORITMO ACTUALIZADO SELECCIONADO
INCLUYENDO MODIFICACIÓN DE CLAVE

Fig. 7