(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 414 616**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04W 12/04 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **08.10.2008 E 08836867 (5)**

(97) Fecha y número de publicación de la concesión europea: **03.04.2013 EP 2210437**

(54) Título: **Comunicación inalámbrica segura**

(30) Prioridad:

09.10.2007 US 998125 P
02.10.2008 US 285336

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
22.07.2013

(73) Titular/es:

ALCATEL LUCENT (100.0%)
3, avenue Octave Gréard
75007 Paris , FR

(72) Inventor/es:

PATEL, SARVAR

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Comunicación inalámbrica segura

Antecedentes

1. Campo de la de la invención

La presente invención se refiere a un procedimiento y a un sistema para comunicaciones inalámbricas seguras. En particular, la presente invención se refiere a un procedimiento para establecer claves de autenticación en el equipo de red y en el móvil para establecer un canal de comunicación autenticado mutuamente.

2. Descripción de la técnica relacionada

Los procedimientos y procesos de seguridad relacionados con las comunicaciones inalámbricas han evolucionado en los últimos años. En particular, la seguridad CDMA 2G evolucionó a la seguridad CDMA 3G.

Como es bien conocido en la técnica, la seguridad CDMA 2G implica autenticación celular y encriptación de voz (CAVE). En particular, la seguridad CDMA 2G usa al menos una clave raíz comúnmente conocida como claves Akey y de datos secretos compartidos (SSD). Las claves de SSD se generan a través de un procedimiento de actualización de SSD bien conocido. Las claves son claves SSD de semi-largo plazo y son tratadas como claves raíz en este documento. Las claves de SSD pueden ser compartidas con un Registro de Ubicación de Visitante (VLR) de una red si el VLR es el sistema servidor local por un equipo móvil, por ejemplo. Además, protocolos de seguridad, convencionales CDMA 2G pueden implicar un procedimiento de impugnación y de respuesta global y un único procedimiento de impugnación y de respuesta.

Para el procedimiento de impugnación global, la red transmite un RAND de forma aleatoria al equipo móvil. Un equipo móvil que realiza un acceso del sistema (por ejemplo, registro, origen de la llamada y terminación de la llamada) en una red que requiere autenticación, crea y envía un AUTHR de respuesta de autenticación mediante una clave de largo plazo. El par RAND/AUTHR se reenvía al Registro de Ubicación Local/Centro de Autenticación (HLR/AC) para la verificación. Además para las llamadas de tipo de origen de la llamada, los últimos 6 dígitos se utilizan para calcular la AUTHR. Tanto para el origen de la llamada y la terminación de llamadas el móvil genera claves que son útiles para la llamada (es decir, SMEKEY y PLCM). El HLR/AC también genera y devuelve al VLR el SMEKEY y PLCM si se verifica el par RAND/AUTHR.

Un procedimiento de impugnación único puede ser realizado por la red que intenta comunicarse con un equipo móvil en cualquier momento ya sea en el canal de control o canal de tráfico. Por ejemplo, el VLR solicita un par de impugnación único y respuesta esperada, RANDU y AUTHU desde el HLR/AC. La red envía el RANDU al equipo móvil y el equipo móvil calcula un AUTHU de respuesta utilizando una clave de largo plazo y envía una AUTHU de respuesta a la red. La red verifica el par RANDU/AUTHU.

Los protocolos convencionales CDMA 3G de seguridad se basan en un protocolo de autenticación y acuerdo de claves (AKA) y proporcionan autenticación mutua significando que (i) el equipo móvil autentica la red y (ii) la red autentica el equipo móvil antes de que se realicen las comunicaciones. Los protocolos de seguridad AKA bien conocidos usados en CDMA 3G se basan en quíntuples. Los quíntuples incluyen un número aleatorio RAND, XRES respuesta esperada, clave de cifrado CK, clave de integridad IK y señal de autenticación de red AUTN. Una señal de autenticación de red AUTN convencional se basa en un número de secuencia SQN, una clave de anonimato AK, un campo de gestión de autenticación AMF y un código de autenticación de mensajes (MAC).

Por ejemplo, el equipo móvil genera su propio MAC sobre la base de un número de secuencia SQN almacenado en el equipo móvil, una clave secreta K almacenada en el equipo móvil, la AMF, y el número aleatorio RAND. Entonces, el MAC generado en el equipo móvil se compara con el MAC extraído de la señal de autenticación de la red AUTN recibida del sistema de servicio. Aún más, el equipo móvil puede determinar si el número de secuencia SQN extraído de la señal de autenticación de red es un valor aceptable. Si el equipo móvil autentica correctamente la red, el equipo móvil prepara una respuesta RES y transmite la respuesta RES de retorno al sistema de servicio de la red. El sistema de servicio de la red compara a continuación la respuesta XRES esperada con la respuesta RES para autenticar el equipo móvil, completando de este modo la autenticación mutua de acuerdo con el protocolo de seguridad AKA convencional.

Si el equipo móvil durante el proceso de autenticación determina el MAC, que se extrajo de la señal de autenticación de red AUTN, no coincide con el MAC generado en el equipo móvil, el equipo móvil transmite un mensaje de fallo al sistema de servicio de la red. Además, si el equipo móvil, durante el proceso de autenticación, determina que el valor de MAC, que se extrajo de la señal de autenticación de la red AUTN, coincide con el valor MAC generado por el equipo móvil, pero que el número de secuencia SQN está fuera del rango admisible, el equipo móvil transmite un mensaje de resincronización a la red. El protocolo de seguridad AKA como se ha descrito brevemente más arriba y que se usa en CDMA 3G es bien conocido en la técnica y por lo tanto, no se proporciona más información en este documento en aras de la brevedad.

Mientras que los protocolos de seguridad han evolucionado por la transición de protocolos de seguridad CDMA de 2G a protocolos de seguridad CDMA 3G, que también se aplican en algunos protocolos de seguridad IMS convencionales, algunos de los equipos de hardware que se utilizan para las comunicaciones inalámbricas no se han actualizado y/o no son capaces de procesar los protocolos más evolucionados. Por ejemplo, algunas empresas que hayan invertido importantes cantidades de tiempo, investigación y dinero en el hardware usado para procesar los protocolos de seguridad CDMA 2G han optado por no actualizar el hardware, por diversas razones asociadas al coste. Por lo tanto, algunos dispositivos de hardware CDMA 2G convencionales no son actualmente capaces de proporcionar un canal de comunicación mutuamente autenticado utilizando los protocolos de seguridad AKA de CDMA 3G convencional.

En consecuencia, se han hecho propuestas que tratan de establecer un canal de comunicación mutuamente autenticado sin necesidad de utilizar protocolo de seguridad AKA basado en quíntuples como base descrito anteriormente con respecto a CDMA3G. Dicho de otra manera, estas propuestas están tratando de utilizar procedimientos de autenticación IS-41 utilizados anteriormente en los protocolos de seguridad CDMA 2G. Sin embargo, todas estas propuestas sufren de, al menos, la siguiente deficiencia. En particular, un compromiso de una clave de sesión IS-41 pasada (por ejemplo, SMEKEY y PLCM) permitiría a un atacante volver a reproducir un número aleatorio y completar con éxito el protocolo de acuerdo de claves y comunicarse con un equipo móvil o una red. Por lo tanto, estas propuestas no son seguras cuando se revela una clave de sesión IS-41 utilizada anteriormente.

El documento WO 2006/029051 divulga un procedimiento según el preámbulo de la reivindicación 1.

Sumario

Realizaciones ejemplares proporcionan procedimientos y aparatos relacionados con el establecimiento de comunicaciones entre el equipo móvil y una red que aprovecha los protocolos de seguridad ANSI-41.

En una realización, el procedimiento realizado por un equipo móvil para autenticar la comunicación con una red incluye las etapas de la reivindicación 1.

En otra realización, un procedimiento realizado por una red para establecer la red con un equipo móvil incluye la generación de una impugnación. La impugnación incluye un campo de número de secuencia, un campo de gestión de autenticación, y un campo de número al azar. El campo de número de secuencia incluye un número de secuencia y una parte de un primer número aleatorio de la red asociados con el equipo móvil. El campo de la gestión de autenticación incluye otra porción del primer número aleatorio, y el campo de número aleatorio incluye un segundo número aleatorio y una porción adicional del primer número aleatorio. La realización incluye además obtener al menos una clave de equipo móvil usando el primer número aleatorio, obtener al menos una clave de red utilizando un segundo número aleatorio, y la generación de una clave de autenticación basada en la clave de equipo móvil y la clave de red. Un primer código de autenticación de mensaje se genera en base a la clave de autenticación de acuerdo con el protocolo de autenticación y el acuerdo de clave de seguridad, y se genera una señal de autenticación en función del número de secuencia en el campo de número de secuencia, el campo de la gestión de autenticación y el primer código de autenticación de mensaje. El reto y la señal de autenticación se envían a los equipos móviles.

Breve descripción de los dibujos

La presente invención se comprenderá más completamente a partir de la descripción detallada dada a continuación en este documento y en los dibujos que acompañan, en los que los elementos están representados por los mismos números de referencia, que se dan a modo de ilustración solamente y por lo tanto no son limitativos de la presente invención y en el que:

La figura 1 ilustra un sistema de comunicación de acuerdo con una realización ejemplar.

La figura 2 ilustra una realización ejemplar de un equipo móvil.

La figura 3 ilustra una realización ejemplar de un número aleatorio RANDM que tiene una longitud mayor que los números aleatorios usados convencionalmente en el establecimiento de canales de comunicación.

La figura 4 ilustra una realización ejemplar de una impugnación AKA, que puede ser generada por un servidor de abonado de origen (HSS) y utilizado tanto por un HSS y un equipo móvil para establecer un canal de comunicación autenticado mutuamente entre el HSS 400 y el equipo móvil.

La figura 5 es un híbrido de un diagrama de flujo y un diagrama de señalización que ilustra una realización ejemplar de las operaciones realizadas y las comunicaciones entre el HSS, HLR/AC y el equipo móvil para formar un canal de comunicación mutuamente autenticado.

La figura 6 es un diagrama de flujo que ilustra un ejemplo el funcionamiento del equipo móvil en la autenticación del HSS.

Descripción detallada de las realizaciones ejemplares

La figura 1 ilustra un sistema de comunicación 10 que incluye al menos un equipo móvil (ME) 100, un registro de localizaciones base (HLR) 300 y un servidor de suscripción local (HSS) 400. Un experto en la materia apreciará que el sistema de comunicación 10 que se ilustra en la figura 1 se simplifica y que incluiría varios componentes intermedios utilizados para la comunicación entre el ME 100, el HLR/AC 300 y el HSS 400. La ubicación del ME 100, el tipo de servicio solicitado por el ME 100, etc., pueden determinar si el HLR 300 o el HSS 400 proporcionan un servicio solicitado al ME 100.

De acuerdo con el realización ejemplar como se describe con respecto a la figura 1, el HLR 300 incluye un centro de autenticación (AC) 310. Un experto en la materia apreciará el HLR 300 y el AC 310 pueden ser componentes separados y distintos del sistema de comunicación en lugar de que el AC 310 se incluya con el HLR 300 como se muestra en la figura 1. En el resto de esta aplicación, el HLR 300 y el centro de autentificación 310 serán referidos colectivamente como un Registro de Ubicación/Centro de autenticación (HLR/AC). El HLR/AC 300 incluye una funcionalidad para realizar procedimientos de seguridad CDMA 2G bien conocidos tales como la autenticación celular y el cifrado de voz (CAVE).

De acuerdo con el realización ejemplar, el HSS 400 puede comportarse como un registro de ubicación visitante (VLR) con respecto al HLR/AC 300, y aprovechar la funcionalidad de seguridad CMDA 2G del HLR/AC 300 para establecer un canal de comunicación mutuamente autenticado sin tener ninguna clave criptográfica AKA acordada a priori con el ME 100.

La figura 2 ilustra una realización ejemplar de ME 100. Como se muestra en la figura 2, el ME 100 incluye un módulo de identidad de usuario (UIM), una memoria 120, un procesador 130 y un transceptor 140. El UIM puede ser un módulo de identidad de usuario convencional. Alternativamente, un experto en la materia apreciarán que el UIM de ME 100 podría ser un módulo de identidad de usuario extraíble convencional (RUIM). Por ejemplo, el UIM puede ser un módulo que fue desarrollado para funcionar de acuerdo con los protocolos de seguridad CDMA 2G. Como tal, el UIM puede almacenar un MIN/IMSI/TMSI como es bien conocido en la técnica y no se discutirá aquí con más detalle en aras de la brevedad.

La memoria 120, el procesador 130 y el transceptor 140 pueden ser usados en conjunción con el UIM para llevar a cabo realizaciones ejemplares de los procedimientos descritos a continuación con respecto a las figuras 3 y 4. Para facilitar la explicación, la memoria 120, el procesador 130 y el transceptor 140 se denominan colectivamente como ME en las realizaciones ejemplares descritas a continuación.

La figura 3 ilustra una realización ejemplar de un número aleatorio RANDM que tiene una longitud mayor que los números aleatorios usados convencionalmente en el establecimiento de canales de comunicación. El ME 100 genera el número aleatorio RANDM. Por ejemplo, la generación del número aleatorio RANDM se activa después de la inserción de un UIM en el ME 100 y/o en respuesta a una señal recibida desde el HSS 400. El número aleatorio RANDM que se muestra en la figura 3 incluye 72 bits. En particular, el número aleatorio RANDM incluye 20 bits aleatorios, 32 bits que se utilizan en la autenticación celular y encriptación de voz (CAVE), y 20 bits que representan 6 dígitos de llamadas, por ejemplo. En lo sucesivo, el número aleatorio RANDM generado por el ME 100 y que se almacena en el ME se conoce como $RANDM_{ME}$, y el subíndice ME indica que el número aleatorio se almacena en el ME 100. Este número aleatorio $RANDM_{ME}$ se comunica al HSS 400, y se almacena en el HSS 400 como $RANDM_{HSS}$.

La figura 4 ilustra una realización ejemplar de una impugnación AKA, que puede ser generada por el HSS 400 y utilizada tanto por un HSS 400 como por un ME 100 para establecer un canal de comunicación mutuamente autenticado entre el HSS 400 y el ME 100. Como se muestra en la figura 4, la impugnación de AKA incluye el número aleatorio RANDM del formato mostrado en la figura 3. Sin embargo, debido a que el número aleatorio RANDM incluido en la impugnación AKA es un número aleatorio RANDM almacenado en el HSS 400, el número aleatorio se conoce como $RANDM_{HSS}$. Del mismo modo, el número aleatorio RANDM almacenado en el ME se conoce como $RANDM_{ME}$. La impugnación de AKA proporciona mayor seguridad, al menos en parte, sobre la base de un número aleatorio RANDM que tiene una longitud mayor que los números aleatorios usados convencionalmente en el establecimiento de canales de comunicación.

Como se muestra en la figura 4, la impugnación AKA incluye un campo de número de secuencia (SQN), un campo de gestión de autenticación (AMF) y un campo de acuerdo de claves de números aleatorios de autenticación (AKA_RAND). Al menos una porción de cada uno del campo SQN, AMF, y del campo AKA_RAND incluye un número de bits del $RANDM_{HSS}$ previamente almacenado en el HSS 400 y se utiliza para generar la impugnación de AKA.

Haciendo referencia a la figura 4, el campo SQN incluye al menos una parte de un número de secuencia almacenado en el HSS 400 (SQN_{HSS}), un indicador o bandera (R), y una porción del número aleatorio $RANDM_{HSS}$. En particular, el campo SQN tiene un total de 48 bits incluyendo 16 bits del SQN_{HSS}, 1 bit para el indicador, y 31 bits del $RANDM_{HSS}$. El campo SQN es una de las entradas a una función que se utiliza para generar un código de autenticación de mensajes (MAC).

El indicador de R del campo SQN es utilizado por el HSS 400 para activar el ME 100 para generar y almacenar un

nuevo número aleatorio $RANDM_{ME}$. Como se ha indicado anteriormente, el número aleatorio $RANDM_{ME}$ puede ser de 72 bits. Por ejemplo, si el indicador R es un "1", el ME 100 genera y almacena un nuevo número aleatorio $RANDM_{ME}$, mientras que si el indicador es un "0", el ME 100 no genera ni almacena un nuevo número aleatorio $RANDM_{ME}$.

Todavía con referencia a la figura 4, el AMF incluye 16 bits del número aleatorio almacenados en el HSS 400 $RANDM_{HSS}$. El AMF es otra de las entradas a una función que se utiliza para calcular un MAC.

El campo AKA_RAND incluye una porción del número aleatorio $RANDM_{HSS}$ almacenado en el HSS 400, y los bits aleatorios generados por el HSS 400. En particular, el campo AKA_RAND incluye 128 bits. Los 128 bits del campo de AKA_RAND incluyen 25 bits del número aleatorio $RANDM_{HSS}$, una única impugnación RANDU incluyendo 24 bits y otros 79 bits generados por el HSS 400.

Las operaciones realizadas y las comunicaciones que involucran la impugnación conocida como se muestra en la figura 4 y/o la información extraída de la impugnación conocida se describen ahora con respecto a la figura 5.

La figura 5 es un híbrido de un diagrama de flujo y un de diagrama señalización que ilustra realizaciones ejemplares de las operaciones realizadas y las comunicaciones entre el HSS 400, el HLR/AC 300 y el ME 100.

Como se muestra, el As es bien conocido, el HSS 400 obtiene el par de números aleatorios conocidos RANDU/AUTHU en cooperación con el HLR/AC 300. El HSS 400 envía el par RANDU/AUTHU como el RANDU/AUTHR bien conocido al HLR/AC 300 para obtener las claves de red $KEYSN_{HSS}$ tales como SMEKEY y PLCM. A saber, el HSS 400 aprovecha la funcionalidad de seguridad CDMA 2G del HLR/AC 300. El HLR/AC 300 genera las claves de red $KEYSN_{HSS}$ según la CAVE, y devuelve las claves de red $KEYSN_{HSS}$ al HSS 400.

Del mismo modo, el HSS 400 envía el número aleatorio móvil $RANDM_{HSS}$ al HLR/AC 300. Como se discutió anteriormente, el número aleatorio móvil $RANDM_{HSS}$ puede haber sido recibido antes desde el ME como $RANDM_{ME}$ y almacenado en el HSS 400 como el número aleatorio móvil $RANDM_{HSS}$. A saber, el número aleatorio móvil $RANDM_{HSS}$ es un número aleatorio que la red asocia con el equipo móvil. El HLR/AC 300 realiza la operación en la CAVE en el $RANDM_{HSS}$ para generar claves de equipos móviles $KEYSM_{HSS}$ tales como SMEKEY y PLCM.

Puede ser que un número aleatorio móvil $RANDM_{HSS}$ no esté disponible en el HSS 400, por ejemplo, el número aleatorio móvil $RANDM_{ME}$ no se recibió con anterioridad o se ha eliminado del HSS 400. En este caso, la red creará el número aleatorio $RANDM_{HSS}$. Por ejemplo, el HSS 400 puede crear un segundo número aleatorio RANDN y utilizar este segundo número aleatorio RANDN como la porción de CAVE RAND (ver la figura 3) del número aleatorio móvil $RANDN_{HSS}$ almacenado en el HSS 400. Además, el HSS 400 puede generar bits aleatorios para ser incluidos en la sección aleatoria del número aleatorio móvil $RANDM_{HSS}$ almacenado en el HSS 400, así como establecer los bits de la sección de dígitos de la llamada del número aleatorio móvil $RANDM_{HSS}$ todos en "1". Se observa que incluir todos unos en la sección de dígitos de la llamada del número aleatorio móvil $RANDM_{HSS}$ enviada en una impugnación podría indicar al ME la información sobre el RANDN.

Volviendo a la figura 5, en la etapa S550, el HSS 400 genera una clave de autenticación AKA_key. Por ejemplo, la clave de autenticación AKA_key puede ser un hash de las claves $KEYSN_{HSS}$ de red y $KEYSM_{HSS}$ móvil como se muestra mediante la siguiente ecuación: AKA_key = H_1 ($KEYSM_{HSS}$, $KEYSN_{HSS}$). En la etapa S560, el HSS 400 utiliza la AKA_KEY de acuerdo con la autenticación CMDA 3G y con los protocolos de acuerdo de claves, junto con el RANDU, los valores de AMF y el número de secuencia SQN_{HSS} para generar un código de autenticación de mensaje MAC_{HSS} que se almacena en el HSS 400.

El HSS genera entonces la impugnación de la figura 4 y la señal de autorización AUTN en la etapa S570. La señal de autorización AUTN está formada para incluir una clave de anonimato AK, el número de secuencia SQN_{HSS}, el campo de gestión de autenticación AMF y el código de autenticación de mensaje MAC_{HSS}. La impugnación y la señal de autorización AUTN se envían al ME 100.

La figura 6 es un diagrama de flujo que ilustra el funcionamiento ejemplar del equipo móvil en la autenticación del HSS a la recepción de la impugnación y de la señal de autorización AUTN. En particular, el transceptor 140 del ME 100 recibe la impugnación y la señal desde el HSS 400 y proporciona la información al procesador 130 para su procesamiento y/o la memoria 120 para el almacenamiento.

Como se muestra en la figura 6, en la etapa S610, el ME 100 extrae el RANDU del campo AKA_RAND de la impugnación recibida y el ME 100 puede utilizar el número aleatorio extraído RANDU para generar las claves de red $KEYSN_{ME}$ tales como la PLCM y la SMEKEY. Como se mencionó anteriormente, la generación de claves sobre la base de un número aleatorio es bien conocida en la técnica y puede ser fácilmente realizada por un UIM del ME 100 usando la CAVE. Se apreciará que el ME 100 y el HLR/AC 300 generan las claves de red KEYSN de la misma manera.

Además, el procesador 130 del ME extrae en la etapa S620 el número aleatorio $RANDM_{HSS}$ desde la impugnación recibida, y el procesador 130 genera las claves móviles $KEYSM_{ME}$. Una vez más, el ME 100 utiliza la CAVE en la $RANDM_{HSS}$ para generar las claves móviles $KEYSM_{ME}$. Como alternativa, las claves móviles $KEYSM_{ME}$ pueden

haberse generado ya en base a $RANDM_{ME}$ y se almacenan en la memoria 140 del ME 100. Por ejemplo, el procesador 130 establece los 20 bits menos significativos como seis dígitos marcados, los siguientes 32 bits menos significativos como una CAVE RAND y proporciona esta información al UIM para obtener una respuesta de autenticación móvil AUTHM y las claves móviles $KEYSM_{ME}$.

Una vez que se obtienen tanto las claves de red $KEYSN_{ME}$ como las claves de móvil $KEYSM_{ME}$ mediante el ME 100, el ME 100 genera la clave de autenticación AKA_key en la etapa S630. Por ejemplo, la clave de autenticación AKA_key puede ser un hash de las claves de red $KEYSN_{ME}$ y $KEYSM_{ME}$ móvil como se muestra por la siguiente ecuación: AKA_key = H1 ($KEYSN_{ME}$, $KEYSN_{ME}$).

En la etapa S640, el ME 100 genera entonces el código de autenticación del mensaje esperado XMAC. El código de autenticación de mensaje esperado XMAC se genera mediante el ME 100 usando el número aleatorio móvil $RANDM_{HSS}$ desde la parte de SQN de la impugnación AKA y la clave de autenticación AKA_key generada y almacenada en el ME 100 de acuerdo con la autenticación CDMA 3G y los protocolos de seguridad de acuerdo de clave.

El ME 100 compara entonces el código de autenticación de mensaje esperado XMAC con el $MACM_{HSS}$ obtenido de la señal de autenticación AUTN en la etapa S650. Si el código de autenticación de mensaje esperado XMAC y el $MACM_{HSS}$ asociado con el HSS 400 no coincide, el ME 100 envía un fallo de autenticación al HSS 400 como se muestra en la figura 6, y el protocolo de seguridad es abortado. Alternativamente, si el código de autenticación de mensaje esperado XMAC y el $MACM_{HSS}$ asociado con el HSS 400 coinciden, el procedimiento que se muestra en la figura 6 pasa a la etapa S660.

En la etapa S660, el ME 100 determina si el número aleatorio móvil $RANDM_{HSS}$ recibido del HSS 400 en la impugnación AKA coincide con el número aleatorio móvil $RANDM_{ME}$ almacenado en el ME 100. Si el número aleatorio móvil $RANDM_{HSS}$ recibido del HSS 400 no coincide con el número aleatorio móvil $RANDM_{ME}$ almacenado en la memoria 140 del ME 100, el ME 100 genera y envía un mensaje de resincronización en la etapa S670. Como se muestra en la figura 6, el mensaje de resincronización incluye un campo de número de secuencia SQN_{RESYNC} y un campo MACS.

De acuerdo con una realización ejemplar, el mensaje de resincronización incluye el número aleatorio móvil $RANDM_{ME}$ almacenado en el ME 100. Por ejemplo, en la figura 6, el campo de número de secuencia incluye 48 bits del $RANDM_{ME}$ y el campo MACS incluye 24 bits del número aleatorio móvil $RANDM_{ME}$. Además, el campo MACS incluye 18 bits de una respuesta de autenticación móvil AUTHRM que se hace un XOR con 18 bits de MACS, así como 22 bits de MACS. Generación de una respuesta de autenticación móvil AUTHRM es bien conocida en la técnica y por lo tanto no se discute en este documento en aras de la brevedad.

En respuesta a la recepción del mensaje de resincronización, el HSS 400 genera un $MACS_{HSS}$ utilizando la clave de autenticación AKA_key para verificar el ME 100. En particular, el HSS 400 realiza una función pseudo aleatoria usando la clave de autenticación previamente generada AKA_key, el número aleatorio móvil $RANDM_{HSS}$ almacenado en el HSS 400, y el número aleatorio AKA_RAND almacenado en el HSS 400.

El HSS 400 compara entonces el $MACS_{HSS}$ con el MACS recibido en el mensaje de resincronización proporcionado por el ME 100. Por ejemplo, el HSS 400 puede extraer los 22 bits menos significativos del MACS recibido en el mensaje de resincronización y comparar los 22 bits extraídos con los 22 bits menos significativos del $MACS_{HSS}$.

Además, el HSS 400 extrae la respuesta de autenticación móvil AUTHRM recibida del ME 100 aplicándole una operación XOR a los siguientes 18 bits de MACS. De acuerdo con una realización de ejemplo, el HSS 400 envía entonces el AUTHRM junto con la información adicional para el HLR/AC 300 para verificar el ME 100 y obtener nuevas claves móviles $KEYSM_{HSS}$. La información adicional incluye una CAVE $RANDM_{ME}$ y los dígitos de llamada, por ejemplo. Si la respuesta de autenticación móvil es verificada por el HLR/AC 300, 18 bits del MACS también son verificados y por lo tanto, se verifican un total de 40 bits.

Alternativamente, si en la etapa S660, el $RANDM_{HSS}$ es igual al $RANDM_{ME}$, el procedimiento que se muestra en la figura 6 pasa a la etapa S680. En la etapa S680, el ME 100 determina si el número de secuencia SQN es aceptable. El número de secuencia SQN asociado con el proceso de autenticación actual se compara con un número de secuencia SQN_{ME} previamente almacenado en el ME 100. Por ejemplo, el número de secuencia SQN asociado con el proceso de autenticación actual debe ser mayor que el número de secuencia SQN_{ME} almacenado previamente en el ME 100, pero dentro de un cierto rango. Dicho de otra manera, el número de secuencia SQN asociado con el proceso de autenticación actual debe ser mayor que el número de secuencia SQN_{ME} previamente almacenado en el ME 100 y menos de un límite superior de un número de secuencia admisible $SQN_{ME} + \Delta$, es decir, SQNMD < SQN < SQNME + Δ, donde Δ es un valor de número entero.

Si en la etapa S680, el número de secuencia SQN se determinó estuviera fuera de un rango permisible, el ME 100 envía un mensaje de resincronización en la etapa S690. Como se muestra en la figura 6, el mensaje de resincronización incluye un campo de número de secuencia SQN_{RESYNC} y un campo de MACS. Por ejemplo, el campo SQN_{RESYNC} del mensaje de resincronización puede incluir ceros para los 32 bits más significativos de un número de secuencia de 48 bits y los 16 bits menos significativos del número de secuencia de 48 bits pueden

establecerse en un número de secuencia SQN_{ME} previamente almacenado en el ME 100. Como se discutió previamente, el ME 100 genera una AKA_KEY basada en la impugnación recibida. La AKA_key generada se utiliza para calcular un MAC, que está incluido en el campo de MACS del mensaje de resincronización.

El HSS 400 recibe el mensaje de resincronización generado debido a que el número de secuencia SQN se determinó que estaba fuera de un rango permisible. El HSS 400 procesa el mensaje de resincronización recibido. Por ejemplo, el HSS 400 puede estar configurado para reconocer que si los 32 bits más significativos del número de secuencia de 48 bits que se incluye en el campo de resincronización de secuencia SQN_{RESYNC} se establecen en ceros, indica que el mensaje de resincronización incluye un número de secuencia SQN_{ME} almacenado en el ME 100. En consecuencia, el HSS 400 almacena el número de secuencia SQN_{ME} para su futuro uso. Sin embargo, el HSS 400 también verifica el ME 100 utilizando los 64 bits de MACS que se incluyen en el campo MACS como se discutió anteriormente.

Si, en la etapa S680, el ME 100 determina que el número de secuencia SQN asociado con la operación de autenticación actual está dentro de un rango permisible, el ME 100 genera un mensaje de respuesta RES en la etapa S700. La generación de un mensaje de respuesta RES basado en un número aleatorio y una clave secreta almacenada en el ME es bien conocida en la técnica y por lo tanto, no se discute en este documento en aras de la brevedad. El ME 100 también calcula una clave de cifrado CK y de la clave de integridad IK basadas en el número aleatorio y la clave secreta. El cálculo de una clave de cifrado CK y de la clave de integridad IK también es bien conocido en la técnica.

Volviendo a la figura 5, el ME 100 envía el mensaje de respuesta RES al HSS 400. El HSS 400 ya se habrá generado un mensaje de respuesta esperado XRES en la etapa S580 en la manera bien conocida. En la etapa S590, el HSS o una entidad de red en nombre del HSS 400 compara el mensaje de respuesta al mensaje de respuesta XRES esperado. Si no existe ninguna coincidencia, la autenticación falla. Sin embargo, si existe una coincidencia, el HSS 400 y el ME 100 establecen un canal de comunicación mutuamente autenticado.

Los procedimientos y aparatos y sistemas descritos anteriormente proporcionan al menos garantías de seguridad de 64 bits. Además, durante la formación de la impugnación, los procedimientos implican enviar tanto el número aleatorio desde el equipo móvil y la red. Una clave de acuerdo de clave de autenticación (AKA) se basa en claves CDMA a partir de impugnaciones. Aún más, el equipo móvil regenera un número aleatorio de 72 bits asociado con el equipo móvil sólo en la inserción UIM y no durante la resincronización. Durante la resincronización, se envía ya sea el número aleatorio de 72 bits generado o almacenado en el equipo móvil o se envía un número de secuencia de 16 bits. La red verifica y acepta el mensaje de resincronización y almacena el número aleatorio de 72 bits proporcionado por el equipo móvil. Aún más, cuando se envía una impugnación, la red utiliza un número aleatorio de 72 bits que la red asocia con el equipo móvil y un número aleatorio de nueva creación para crear claves de CDMA que a su vez generan una clave de AKA. La clave AKA se utiliza con funciones AKA estándar para crear un MAC, RES, CK e IK.

Siendo la invención así descrita, será obvio que la misma puede ser variada de muchas maneras. Tales variaciones no deben ser consideradas como una desviación del alcance de la invención, y se pretende que todas las modificaciones que serán obvias para un experto en la materia estén incluidas dentro del alcance de la presente invención.

REIVINDICACIONES

1. Procedimiento realizado por el equipo móvil (100) para autenticar una red (400), comprendiendo el procedimiento:

recibir información de autenticación a partir de dicha red, incluyendo dicha información de autenticación un primer número aleatorio, RANDU, generado por un servidor de suscripción local, HSS (400), de dicha red;
extraer dicho primer número aleatorio, RANDU, de la información de autenticación recibida;
generar (S610) al menos una clave de red, $KEYSN_{ME}$, a partir del primer número aleatorio, RANDU, utilizando la autenticación celular y la encriptación de voz;
generar (S630) una clave de autenticación basada en la clave de red, $KEYSN_{ME}$, y un segundo valor;
generar (S640) un mensaje de código de autenticación de red esperado, XMAC, sobre la base de la clave de autenticación y al menos una parte de la información de autenticación recibida de acuerdo con el protocolo de autenticación y de acuerdo con la clave de seguridad; y
autenticar (S650, S660, S680) la red (400) basado en el mensaje de código de autenticación de red esperado, XMAC, **caracterizado porque** dicho procedimiento comprende además:

obtener un segundo número aleatorio, $RANDM_{HSS}$, siendo el segundo número aleatorio un número aleatorio que el equipo móvil (100) había generado y había enviado a la red (400) para ser incorporado en la información de autenticación;
generar (S620) al menos una clave de equipos móviles, $KEYSM_{ME}$, basada en el segundo número aleatorio, $RANDM_{HSS}$, mediante la autenticación celular y la encriptación de voz, constituyendo dicha clave de equipo móvil, $KEYSM_{ME}$, dicho segundo valor.

2. Procedimiento de acuerdo con la reivindicación 1, en el que la etapa de autenticación comprende:

obtener un código de autenticación de mensaje, MAC_{HSS}, a partir de la información de autenticación recibida, y
comparar (S650) el código de autenticación de mensaje esperado, XMAC, con el código de autenticación de mensaje obtenido, MAC_{HSS}.

3. Procedimiento de acuerdo con la reivindicación 2, en el que la etapa de autenticación comprende además:

comparar (S660) el segundo número al azar, $RANDM_{HSS}$, con un tercer número al azar, $RANDM_{ME}$, almacenado en el equipo móvil (100); y
enviar (S670) un mensaje de resincronización a la red (400) si el segundo número aleatorio, $RANDM_{HSS}$, no coincide con el tercer número al azar, $RANDM_{ME}$, incluyendo el mensaje de resincronización al menos una porción del tercer de número aleatorio.

4. Procedimiento de acuerdo con la reivindicación 2, en el que la información de autenticación recibida incluye un campo de número de secuencia, SQN, un campo de gestión de autenticación, AMF, y una clave de campo de número aleatorio de acuerdo de autenticación, AKA_RAND, y
que comprende además:

determinar (S680) si un número de secuencia en el campo de número de secuencia, SQN, está dentro de un rango permisible; y
enviar (S690) un mensaje de resincronización si se determinó que el número de secuencia no está dentro del rango permitido.

5. Procedimiento de acuerdo con la reivindicación 4, en el que el mensaje de resincronización incluye un número de secuencia almacenado en el equipo móvil.

6. Procedimiento de acuerdo con la reivindicación 1, en el que la información de autenticación recibida incluye un campo de número de secuencia, SQN, un campo de gestión de autenticación, AMF, y una clave de campo de número aleatorio acuerdo autenticación, AKA_RAND, y

que comprende además:

obtener un código de autenticación de mensajes, MAC_{HSS}, a partir de la información recibida;
comparar (S650) el código de autenticación de mensaje esperado, XMAC, con el código de autenticación de mensaje obtenido, MAC_{HSS},
comparar (S660) el segundo número al azar, RANDM, con un tercer número al azar, $RANDM_{ME}$, Almacenado en el equipo móvil; y
determinar (S680) si un número de secuencia en el campo de número de secuencia, SQN, está dentro de un rango permisible; y
enviar (S700) una respuesta de autenticación a la red si el código de autenticación de mensaje esperado coincide con el código de autenticación de mensaje obtenido, el segundo número aleatorio coincide con el tercer número aleatorio, y el campo de número de secuencia está dentro del rango permisible.

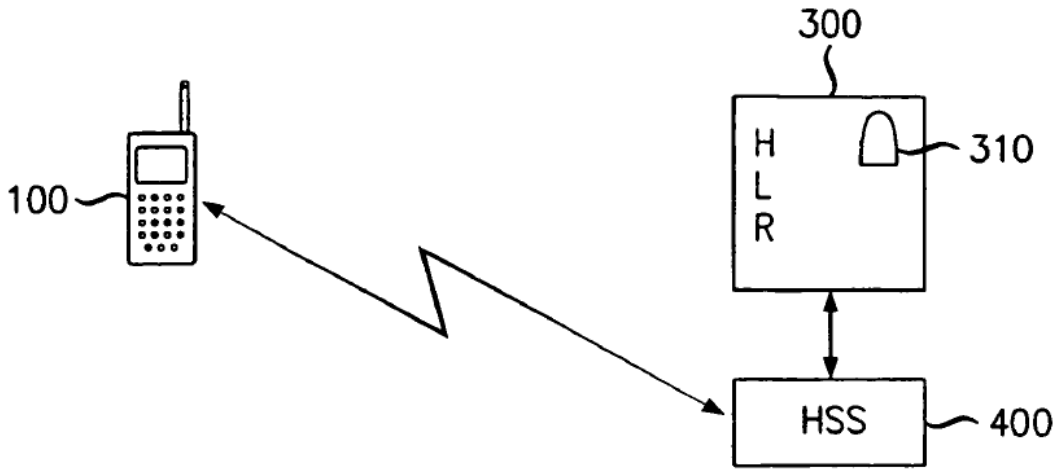


FIG. 1

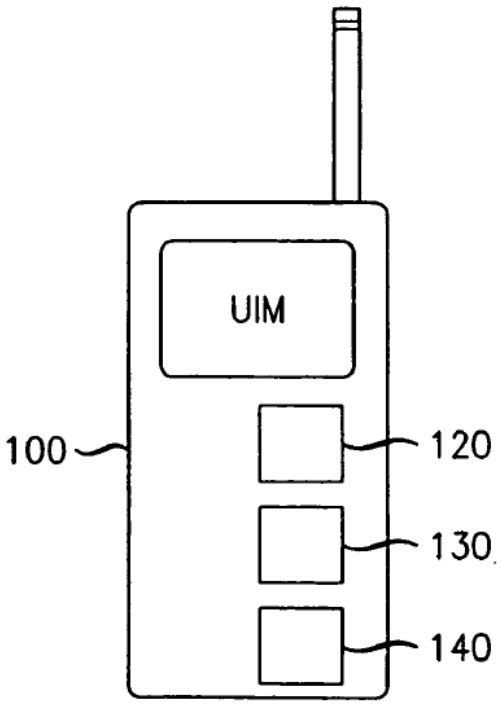


FIG. 2


RANDM (72 bits)
aleatorio
(20 bits)
CAVE RAND
(32 bits)
6 dígitos de llamadas
(20 bits)

FIG. 3

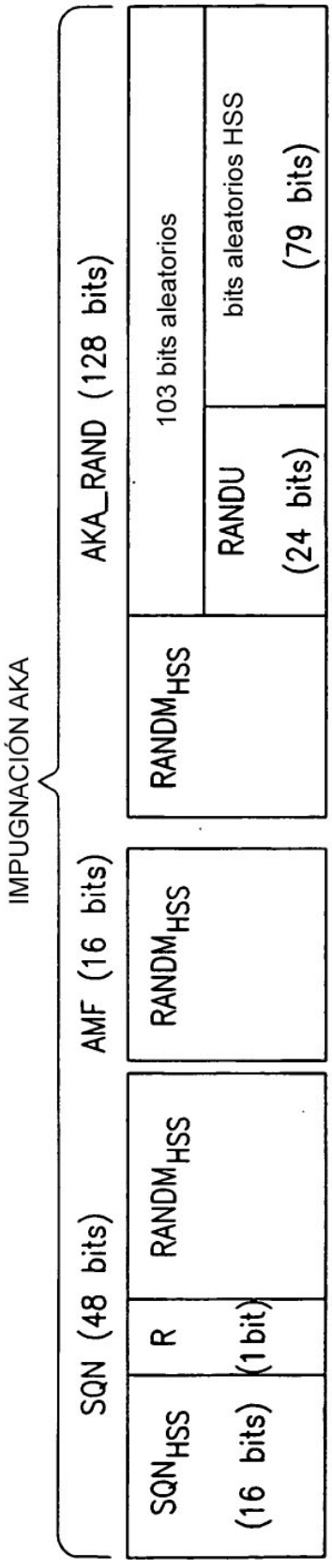
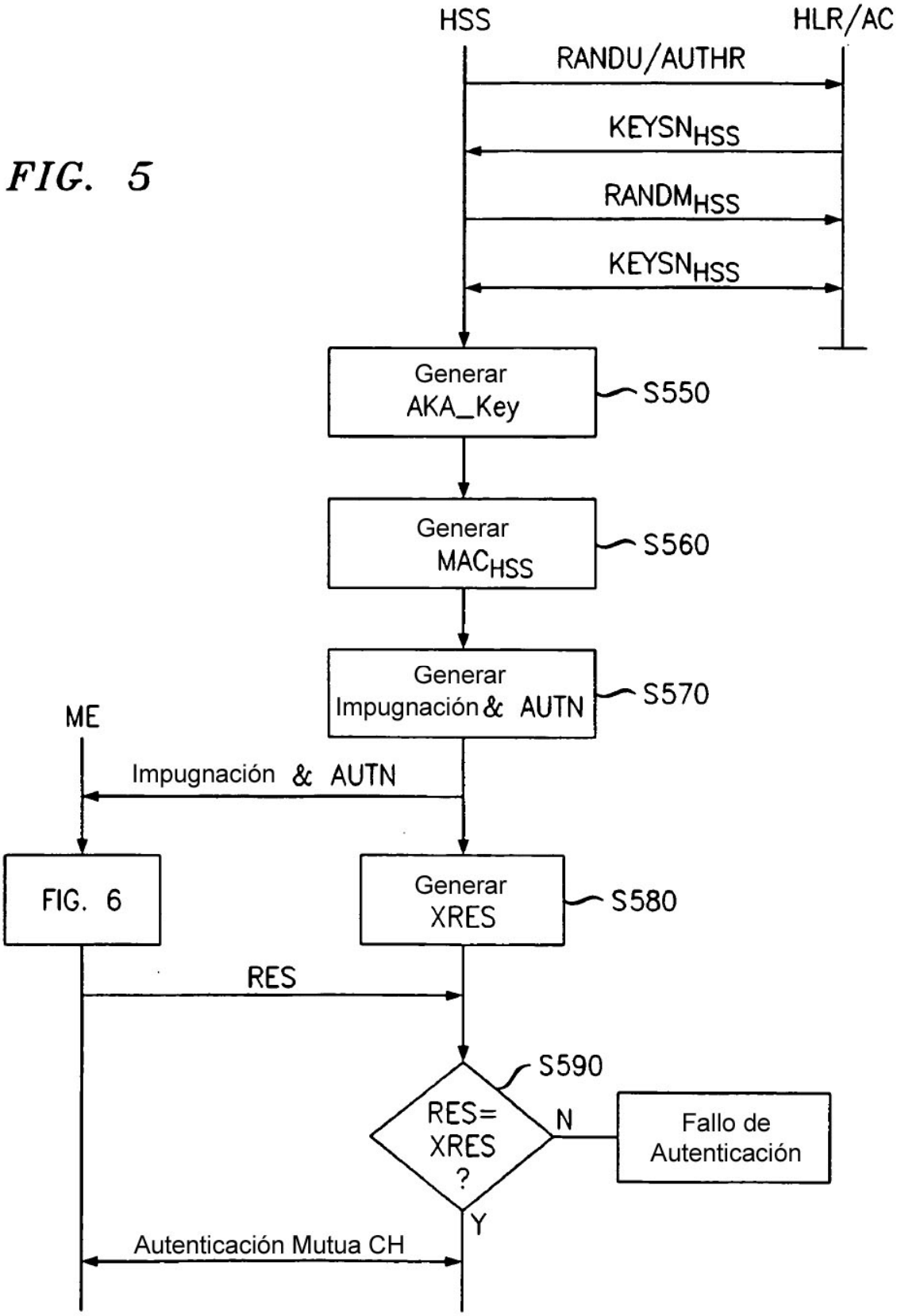

IMPUGNACIÓN AKA
AKA_RAND (128 bits)
SQN (48 bits)
AMF (16 bits)
RANDM_HSS
SQN_HSS
(16 bits)
R
(1 bit)
RANDM_HSS
RANDM_HSS
RANDU
(24 bits)
103 bits aleatorios
bits aleatorios HSS
(79 bits)
(72 bits)

FIG. 4

FIG. 5


HSS
HLR/AC
RANDU/AUTHR
KEYSN$_{HSS}$
RANDM$_{HSS}$
KEYSN$_{HSS}$
Generar AKA_Key
S550
Generar MAC$_{HSS}$
S560
Generar Impugnación & AUTN
S570
ME
Impugnación & AUTN
FIG. 6
Generar XRES
S580
RES
S590
RES= XRES ?
N
Fallo de Autenticación
Y
Autenticación Mutua CH

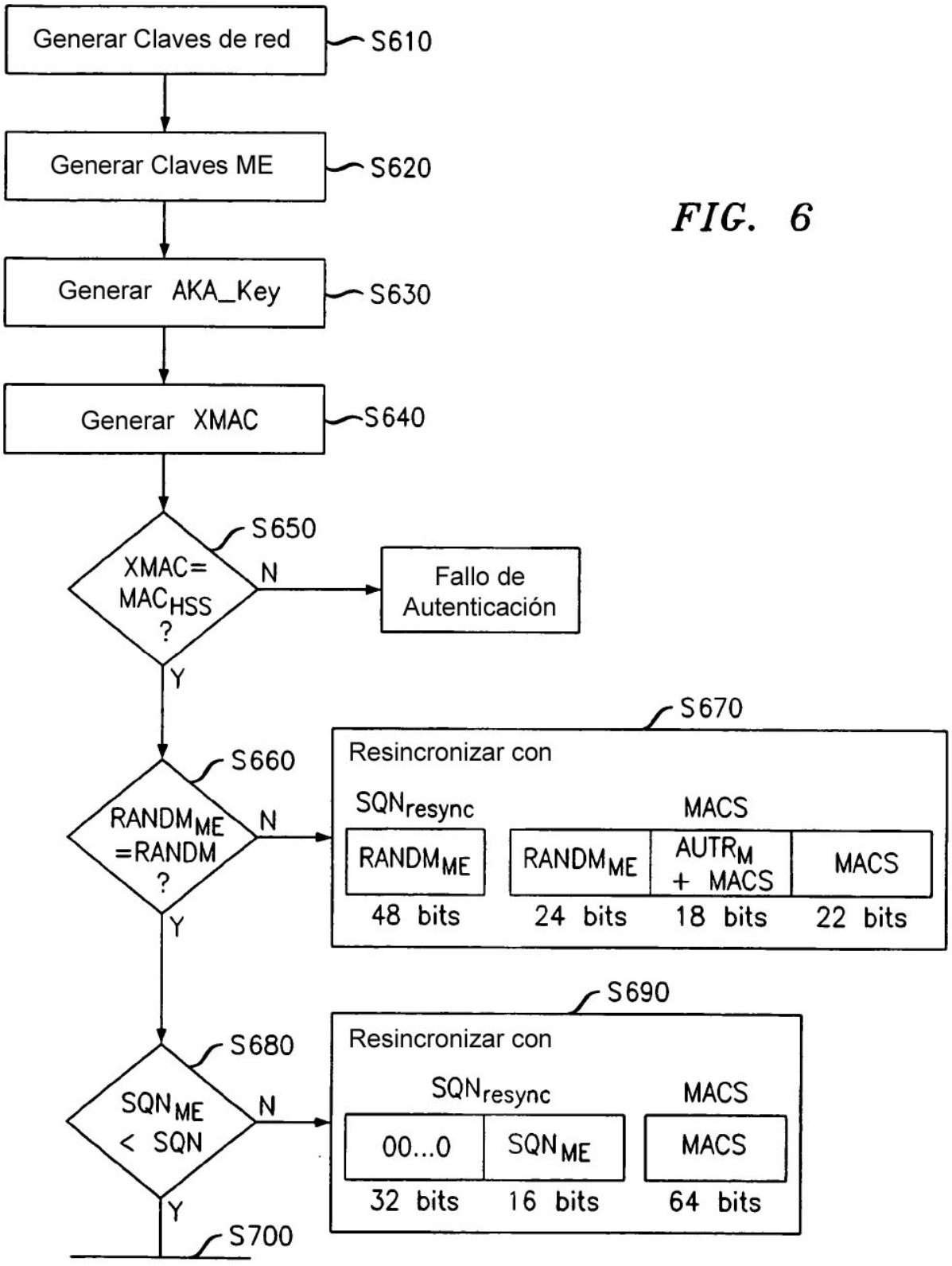

Generar Claves de red
S610
Generar Claves ME
S620
Generar AKA_Key
S630
Generar XMAC
S640
S650
XMAC= MAC HSS ?
N
Fallo de Autenticación
Y
S660
RANDM ME =RANDM ?
N
Y
S670
Resincronizar con
SQN resync
MACS
RANDM ME
RANDM ME
AUTR M + MACS
MACS
48 bits
24 bits
18 bits
22 bits
S680
SQN ME < SQN
N
Y
S690
Resincronizar con
SQN resync
MACS
00...0
SQN ME
MACS
32 bits
16 bits
64 bits
S700

FIG. 6