(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 589 681**

(51) Int. CI.:

H04W 4/14 (2009.01)
H04W 12/02 (2009.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **22.04.2011 PCT/CN2011/073192**

(87) Fecha y número de publicación internacional: **07.06.2012 WO12071846**

(96) Fecha de presentación y número de la solicitud europea: **22.04.2011 E 11844921 (4)**

(97) Fecha y número de publicación de la concesión europea: **15.06.2016 EP 2549778**

(54) Título: **Procedimiento y sistema para cifrar mensajes cortos**

(30) Prioridad:

01.12.2010 CN 201010568985

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
15.11.2016

(73) Titular/es:

ZTE CORPORATION (100.0%)
ZTE Plaza, Keji Road South, Hi-Tech Industrial Park, Nanshan District
Shenzhen, Guangdong 518057, CN

(72) Inventor/es:

SUN, JUNSHENG;
ZHANG, PENGBO;
CAO, YAOBIN;
DENG, FANGMIN;
XUE, TAO;
YU, SONG y
YANG, YULIN

(74) Agente/Representante:

DURÁN MOYA, Luis Alfonso

DESCRIPCIÓN

Procedimiento y sistema para cifrar mensajes cortos

Sector técnico

La presente invención se refiere al sector de las comunicaciones móviles y, más concretamente, a un procedimiento y un sistema para implementar el cifrado de mensajes cortos.

Antecedentes técnicos

Con el aumento de la popularización de los terminales de telefonía móvil, los SMS (servicios de mensajes cortos) han jugado un papel cada vez más significativo en la vida diaria de la gente y se han convertido en una forma de comunicación importante para las personas. Debido a la popularización de los SMS, el problema de la seguridad de los SMS se ha hecho cada vez más importante. Esto se debe a que en muchos casos el mensaje corto transmitirá información importante, y si se intercepta la información, se causarán importantes pérdidas al individuo. Debido al mecanismo fijo actual de los SMS, el contenido del mensaje de almacena en la estructura de la PDU (unidad de datos de protocolo) como texto simple. Cómo garantizar la transmisión segura de los mensajes cortos se convierte en un problema importante.

Los modos existentes de cifrado de mensajes cortos incluyen principalmente los siguientes tipos:

(1) el mensaje corto que ha sido transmitido y recibido se protege contra un acceso ilegal añadiendo permisos de acceso al módulo de mensajes cortos del teléfono móvil;

(2) el acceso legal al mensaje corto se protege llevando a cabo una configuración especial de permisos para un mensaje corto individual;

(3) el mensaje corto se protege cifrando el contenido del mensaje corto y con un acceso mediante clave o contraseña;

(4) la transmisión segura de un mensaje corto se consigue en el modo de texto cifrado añadiendo un campo de seguridad y contenido de seguridad mediante una PDU de mensajes cortos extendida, y la parte de recepción analiza el campo de seguridad para descifrar el mensaje corto final;

(5) la información de cifrado se determina en primer lugar de manera negociada, y después se transmite el mensaje corto.

En los que, (1), (2) y (3) son procedimientos de protección basados en el lado del teléfono móvil, y (4) y (5) son procedimientos de protección basados en el lado de la red inalámbrica.

Hablando en términos generales, los procedimientos de protección basados en el lado de la red inalámbrica son más importantes que los procedimientos de protección basados en el lado del teléfono móvil ya que el teléfono móvil normalmente está en nuestras manos, así que prestaremos más atención a la seguridad de los SMS en la transmisión por la red inalámbrica.

Los procedimientos de protección existentes del lado inalámbrico y del lado de red necesitan generalmente una extensión o una modificación del formato de la PDU de mensajes cortos, y además, también debe implementarse la negociación del algoritmo de cifrado y la transmisión de la clave. En los que, la transmisión de la clave y el algoritmo de cifrado no son seguros de por sí.

Las tecnologías relacionadas se conocen a partir de los documentos WO 99/35784A1, US 2009/265552A1 y US 2009/325543A1.

Características de la invención

El problema técnico a solucionar es conseguir un procedimiento y un sistema para implementar el cifrado de los mensajes cortos de tal manera que se garantice la transmisión segura de los servicios de mensajes cortos (SMS).

Las características del procedimiento según la presente invención se definen en las reivindicaciones independientes. Las mejoras y realizaciones adicionales están previstas en las reivindicaciones dependientes.

Está previsto un procedimiento para implementar el cifrado de mensajes cortos, que incluye los siguientes pasos:

una estación móvil (MS) de la parte de transmisión cifra el mensaje corto a transmitir utilizando una clave de cifrado (CK) de la parte de transmisión como identificador de cifrado y a continuación envía el mensaje corto;

un centro de conmutación móvil (MSC) al que pertenece la MS de la parte de transmisión descifra el mensaje corto utilizando la CK de la parte de transmisión como factor de descifrado tras recibir el mensaje corto, y a continuación envía el mensaje corto a un centro de servicios de mensajes cortos (SC) a través de un centro de servicios de mensajes de funcionamiento conjunto (IWMSC);

tras recibir el mensaje corto transmitido por el SC a través de una puerta del centro de conmutación móvil (GM-SC), el MSC al que pertenece la MS de la parte de recepción cifra el mensaje corto utilizando la CK de la parte de recepción como identificador de cifrado, y después envía el mensaje corto a la MS de la parte de recepción;

tras recibir el mensaje corto, la MS de la parte de recepción descifra el mensaje corto utilizando la CK de la parte de recepción como factor de descifrado, recuperando de este modo el contenido del mensaje corto.

El procedimiento anterior tiene además la siguiente característica:

el paso de que la MS de la parte de transmisión cifra el mensaje corto a transmitir utilizando la CK de la parte de transmisión como identificador de cifrado y a continuación envía el mensaje corto comprende: la MS de la parte de transmisión cifra los datos de usuario (UD) de una unidad de datos de protocolo (PDU) del mensaje corto a transmitir utilizando la CK de la parte de transmisión como identificador de cifrado mediante un módulo propio de cifrado-descifrado, estableciendo un identificador de cifrado en la PDU del mensaje corto a transmitir, y a continuación envía el mensaje corto;

el paso de que el MSC al que pertenece la MS de la parte de transmisión descifra el mensaje corto utilizando la CK de la parte de transmisión como factor de descifrado tras recibir el mensaje corto comprende: tras recibir el mensaje corto, si se decide conforme al identificador de cifrado que el mensaje corto es un mensaje corto cifrado, el MSC al que pertenece la MS de la parte de transmisión descifra los UD de la PDU del mensaje corto utilizando la CK de la parte de transmisión como factor de descifrado mediante un módulo propio de cifrado-descifrado;

el paso de que el MSC al que pertenece la MS de la parte de recepción cifra el mensaje corto utilizando la CK de la parte de recepción como identificador de cifrado tras recibir el mensaje corto comprende: tras recibir el mensaje corto, si se decide conforme al identificador de cifrado en el mismo que es necesario cifrar el mensaje corto, el MSC al que pertenece la MS de la parte de recepción cifra los UD de la PDU del mensaje corto utilizando la CK de la parte de recepción como identificador de cifrado mediante un módulo propio de cifrado-descifrado;

el paso de que la MS de la parte de recepción descifra el mensaje corto utilizando la CK de la parte de recepción como factor de descifrado tras recibir el mensaje corto comprende: tras recibir el mensaje corto, si se decide conforme al identificador de cifrado en el mismo que el mensaje corto es un mensaje corto cifrado, la MS de la parte de recepción descifra los UD de la PDU del mensaje corto utilizando la CK de la parte de recepción como factor de descifrado mediante un módulo propio de cifrado-descifrado.

El procedimiento anterior tiene además la siguiente característica:

tras descifrar los UD de la PDU del mensaje corto, el MSC al que pertenece la MS de la parte de transmisión cifra los UD de la PDU del mensaje corto utilizando un identificador de usuario de la parte de recepción como identificador de cifrado mediante el módulo propio de cifrado-descifrado, y después transmite el mensaje corto al SC a través del IWMSC;

tras recibir el mensaje corto transmitido por el SC a través del GMSC, si se decide conforme al identificador de cifrado en el mismo que es necesario cifrar el mensaje corto, el MSC al que pertenece la MS de la parte de recepción descifra en primer lugar los UD de la PDU del mensaje corto utilizando el identificador de usuario de la parte de recepción como factor de descifrado mediante el módulo propio de cifrado-descifrado, y a continuación cifra los UD de la PDU del mensaje corto utilizando la CK de la parte de recepción como identificador de cifrado.

Preferentemente, el procedimiento anterior tiene además la siguiente característica:

la CK se calcula con un algoritmo particular a partir de un valor aleatorio (RAND) generado en el proceso de autentificación de la MS y el MSC de la parte a la que pertenece la CK y una clave raíz (Ki) del usuario.

Preferentemente, el procedimiento anterior tiene además la siguiente característica:

el identificador del usuario de la parte de recepción es el número ISDN internacional del suscriptor móvil (MSISDN) o el número de identificación del suscriptor móvil internacional (IMSI) de la parte de recepción.

Preferentemente, el procedimiento anterior tiene además la siguiente característica:

antes de que la MS de la parte de transmisión cifre el mensaje corto a transmitir, la MS proporciona una intercomunicación del usuario de la parte de transmisión para seleccionar si se debe cifrar el mensaje corto a transmitir, y si el usuario de la parte de transmisión selecciona el cifrado, la MS de la parte de transmisión cifra el mensaje corto a transmitir.

Asimismo se proporciona un procedimiento para transmitir un mensaje corto cifrado, que comprende los siguientes pasos:

una estación móvil (MS) de la parte de transmisión cifra un mensaje corto a transmitir utilizando una clave de cifrado (CK) de la parte de transmisión como identificador de cifrado y a continuación envía el mensaje corto;

un centro de conmutación móvil (MSC) al que pertenece la MS de la parte de transmisión descifra el mensaje corto utilizando la CK de la parte de transmisión como factor de descifrado tras recibir el mensaje corto, y a continuación envía el mensaje corto a un centro de servicio de mensajes cortos (SC) a través de un centro de servicios de mensajes de funcionamiento conjunto (IWMSC).

El procedimiento anterior tiene además la siguiente característica:

el paso de que la MS de la parte de transmisión cifra el mensaje corto a transmitir utilizando la CK de la parte de transmisión como identificador de cifrado y a continuación envía el mensaje corto comprende: la MS de la parte de transmisión cifra los datos de usuario (UD) de la unidad de datos de protocolo (PDU) del mensaje corto a transmitir utilizando la CK de la parte de transmisión como identificador de cifrado mediante un módulo propio de cifrado-descifrado, estableciendo un identificador de cifrado en la PDU del mensaje corto a transmitir, y a continuación envía el mensaje corto;

el paso de que el MSC al que pertenece la MS de la parte de transmisión descifra el mensaje corto utilizando la CK de la parte de transmisión como factor de descifrado tras recibir el mensaje corto comprende: tras recibir el mensaje corto, si se decide conforme al identificador de cifrado que el mensaje corto es un mensaje corto cifrado, el MSC al que pertenece la MS de la parte de transmisión descifra los UD de la PDU del mensaje corto utilizando la CK de la parte de transmisión como factor de descifrado mediante un módulo propio de cifrado-descifrado;

El procedimiento anterior tiene además la siguiente característica:

tras descifrar los UD de la PDU del mensaje corto, el MSC al que pertenece la MS de la parte de transmisión cifra los UD de la PDU del mensaje corto utilizando un identificador de usuario de la parte de recepción como identificador de cifrado mediante el módulo propio de cifrado-descifrado, y a continuación transmite el mensaje corto al SC a través del IWMSC.

Asimismo se proporciona un procedimiento para recibir un mensaje corto cifrado, que comprende los siguientes pasos:

tras recibir el mensaje corto transmitido por el centro de servicios de mensajes cortos (SC) a través de una puerta del centro de conmutación móvil (GMSC), el centro de conmutación móvil (MSC) al que pertenece la estación móvil (MS) de la parte de recepción cifra el mensaje corto utilizando una clave de cifrado (CK) de la parte de recepción como identificador de cifrado y a continuación envía el mensaje corto a la MS de la parte de recepción;

tras recibir el mensaje corto, la MS de la parte de recepción descifra el mensaje corto utilizando la CK de la parte de recepción como factor de descifrado, recuperando así el contenido del mensaje corto.

El procedimiento anterior tiene además la siguiente característica:

el paso de que el MSC al que pertenece la MS de la parte de recepción cifra el mensaje corto utilizando la CK de la parte de recepción como identificador de cifrado tras recibir el mensaje corto comprende: tras recibir el mensaje corto, si se decide conforme al identificador de cifrado en el mismo que es necesario cifrar el mensaje corto, el MSC al que pertenece la MS de la parte de recepción cifra los UD de la PDU del mensaje corto utilizando la CK de la parte de recepción como identificador de cifrado mediante un módulo propio de cifrado-descifrado;

el paso de que la MS de la parte de recepción descifra el mensaje corto utilizando la CK de la parte de recepción como factor de descifrado tras recibir el mensaje corto comprende: tras recibir el mensaje corto, si se decide conforme al identificador de cifrado en el mismo que el mensaje corto es un mensaje corto cifrado, la MS de la parte de recepción descifra los UD de la PDU del mensaje corto utilizando la CK de la parte de recepción como factor de descifrado mediante un módulo propio de cifrado-descifrado.

El procedimiento anterior tiene además la siguiente característica:

tras recibir el mensaje corto transmitido por el SC a través del GMSC, si se decide conforme al identificador de cifrado en el mismo que es necesario cifrar el mensaje corto, el MSC al que pertenece la MS de la parte de recepción descifra en primer lugar los UD de la PDU del mensaje corto utilizando el identificador de usuario de la parte de recepción como factor de descifrado mediante el módulo propio de cifrado-descifrado, y a continuación cifra los UD de la PDU del mensaje corto utilizando la CK de la parte de recepción como identificador de cifrado.

Asimismo se proporciona un sistema para implementar el cifrado de un mensaje corto, que comprende una MS de la parte de transmisión, un MSC al que pertenece la MS de la parte de transmisión, un MSC al que pertenece la MS de la parte de recepción, la MS de la parte de recepción, y la MS y el MSC de la parte de transmisión y la MS y el MSC de la parte de recepción están todos ellos configurados con módulos de cifrado-descifrado,

la MS de la parte de transmisión se configura para cifrar el mensaje corto a transmitir utilizando una clave de cifrado (CK) de la parte de transmisión como identificador de cifrado mediante el módulo propio de cifrado-descifrado y a continuación envía el mensaje corto;

el MSC al que pertenece la MS de la parte de transmisión está configurado para descifrar el mensaje corto utilizando la CK de la parte de transmisión como factor de descifrado tras recibir el mensaje corto, y a continuación envía el mensaje corto a un centro de servicios de mensajes cortos (SC) mediante un centro de servicios de mensajes de funcionamiento conjunto (IWMSC);

el MSC al que pertenece la MS de la parte de recepción está configurado para cifrar el mensaje corto utilizando la CK de la parte de recepción como identificador de cifrado mediante el módulo propio de cifrado-descifrado tras recibir el mensaje corto transmitido por el SC a través del GMSC y a continuación envía el mensaje corto a la MS de la parte de recepción;

la MS de la parte de recepción está configurada para descifrar el mensaje corto utilizando la CK de la parte de recepción como factor de descifrado mediante el módulo propio de cifrado-descifrado tras recibir el mensaje corto, recuperando así el contenido del mensaje corto.

Asimismo está dispuesto una estación móvil (MS), que comprende un módulo de transmisión y un módulo de recepción, así como un módulo de cifrado-descifrado, comprendiendo el módulo de cifrado-descifrado un módulo secundario de cifrado y un módulo secundario de descifrado, en los que,

el módulo secundario de cifrado está configurado para cifrar el mensaje corto a transmitir utilizando la CK actual como identificador de cifrado, y envía el mensaje corto a través del módulo de transmisión;

el módulo secundario de descifrado está configurado para descifrar el mensaje corto recibido por el módulo de recepción utilizando la CK actual como factor de descifrado, recuperando así el contenido del mensaje corto.

Preferentemente, la MS anterior también presenta la siguiente característica:

la MS comprende también un módulo de intercomunicación,

el módulo de intercomunicación se configura para proporcionar la intercomunicación de usuario para seleccionar si se debe cifrar el mensaje corto a transmitir, y si el usuario selecciona el cifrado, informa al módulo de cifrado para que el módulo de cifrado cifre el mensaje corto a transmitir.

Asimismo está dispuesto un centro de conmutación móvil (MSC), que comprende un módulo de transmisión y un módulo de recepción, así como un módulo de cifrado-descifrado, comprendiendo el módulo de cifrado-descifrado un módulo secundario de cifrado y un módulo secundario de descifrado, en los que,
el módulo secundario de descifrado está configurado para descifrar el mensaje corto utilizando la CK de la parte de transmisión como factor de descifrado una vez que el módulo de recepción recibe el mensaje corto de la MS de la parte de transmisión, y a continuación envía el mensaje corto a un centro de servicios de mensajes cortos (SC) mediante el módulo de transmisión;

el módulo secundario de cifrado está configurado para cifrar el mensaje corto utilizando la CK de la parte de recepción como identificador de cifrado una vez que el módulo de recepción recibe el mensaje corto del SC y a continuación envía el mensaje corto a la MS de la parte de recepción.

Preferentemente, el MSC anterior presenta asimismo la siguiente característica:

el módulo secundario de cifrado está configurado también para que, después de que el módulo secundario de descifrado descifra el mensaje corto utilizando la CK de la parte de transmisión, cifrar el mensaje corto utilizando el identificador de usuario de la parte de recepción como identificador de cifrado, y a continuación transmite el mensaje corto al SC a través del módulo de transmisión;

el módulo secundario de descifrado está configurado también para que, una vez que el módulo de recepción recibe el mensaje corto del SC, en primer lugar descifra el mensaje corto utilizando el identificador de usuario de la parte de recepción como factor de descifrado, y después cifra el mensaje corto utilizando la CK de la parte de recepción como identificador de cifrado mediante el módulo secundario de cifrado.

En comparación con la técnica anterior, en el documento de la patente, añadiendo el módulo de cifrado-descifrado correspondiente a la MS (estación móvil) y al MSC (centro de conmutación móvil), el mensaje corto se cifra y se descifra utilizando la CK (clave de cifrado) que varía con el RAND (valor aleatorio) como identificador de cifrado-descifrado, y la clave está altamente protegida durante todo el proceso, y no es compartida por los extremos de recepción y transmisión, de modo que el mensaje corto cifrado tiene una alta confidencialidad. Además, el módulo de cifrado-descifrado puede ser proporcionado por la tercera parte e integrado en el terminal y en el dispositivo de red, y está configurado para cambiar el algoritmo según sea necesario y es responsable de llevar a cabo la operación de cifrado-descifrado de los datos del mensaje corto. De este modo, incluso la red, el dispositivo terminal de suministro y el operador no pueden fracturar el mensaje corto cifrado. Además, en el esquema del documento de la patente, el identificador de cifrado es distinto cada vez, lo que aumenta la dificultad de fracturar en el entorno de la transmisión inalámbrica. Además, se puede conseguir la seguridad de todo el entorno de transmisión mediante configuraciones opcionales.

Breve descripción de los dibujos

La figura 1 muestra la estructura del sistema para cifrar un mensaje corto según un ejemplo de la presente invención;

La figura 2 es un diagrama de flujo del envío por la MS de un mensaje corto cifrado;

La figura 3 es un diagrama de flujo de la recepción en la MS de un mensaje corto cifrado;

La figura 4 es un diagrama de flujo del envío de un mensaje corto cifrado al centro de servicios de mensajes cortos (SC);

La figura 5 es un diagrama de flujo del envío por el SC de un mensaje corto cifrado a la parte de recepción.

Realizaciones preferentes de la invención

El concepto básico de la presente invención es que el módulo de cifrado-descifrado está configurado en la MS y en el MSC, y el módulo de cifrado-descifrado cifra y descifra los datos de usuario (UD) del mensaje corto utilizando la CK (clave de cifrado) como identificador de cifrado-descifrado, aumentando así la seguridad del entorno de transmisión inalámbrica del mensaje corto. Opcionalmente, también se puede implementar una configuración apropiada para conseguir la seguridad del mensaje corto en el entorno de red posterior, consiguiendo así la seguridad de todo el entorno de transmisión.

El procedimiento para implementar el cifrado del mensaje corto según el ejemplo de la presente invención comprende los siguientes pasos:

Paso 1, la MS (también denominada MS A) de la parte de transmisión cifra los UD de la PDU del mensaje corto a transmitir utilizando la CK de la parte de transmisión como identificador de cifrado mediante el módulo propio de cifrado-descifrado, establece un identificador de cifrado en la PDU del mensaje corto a transmitir, y a continuación envía el mensaje corto;

Paso 2, después de que el mensaje corto llega al MSC al que pertenece la MS A mediante el BSS (sistema secundario de estaciones base, que comprende una BTS (estación base transceptora) y un BSC (controlador de estaciones base)) y el MSC recibe el mensaje corto, si se decide conforme al identificador de cifrado en el mismo que el mensaje corto es un mensaje corto cifrado, el MSC descifra los UD de la PDU del mensaje corto utilizando la CK de la parte de transmisión como factor de descifrado mediante de un

módulo propio de cifrado-descifrado, y después envía el mensaje corto al SC (centro de servicios) a través de un IWMSC (centro de servicios de mensajes de funcionamiento conjunto);

Paso 3, después de que el MSC al que pertenece la MS de la parte de recepción recibe el mensaje corto transmitido por el SC a través del GMSC (centro de conmutación de puerta móvil), si se decide conforme al identificador de cifrado en el mismo que es necesario cifrar el mensaje corto, el MSC al que pertenece la MS de la parte de recepción cifra los UD de la PDU del mensaje corto utilizando la CK de la parte de recepción como identificador de cifrado mediante su módulo de cifrado-descifrado y a continuación envía el mensaje corto a la MS (que se puede denominar MS B) de la parte de recepción a través de la BTS y el BSC a los que pertenece la MS de la parte de recepción;

Paso 4, tras recibir el mensaje corto, si se decide conforme al identificador de cifrado en el mismo que el mensaje corto es un mensaje corto cifrado, la MS B descifra los UD de la PDU del mensaje corto utilizando la CK de la parte de recepción como factor de descifrado mediante un módulo propio de cifrado-descifrado, recuperando así el contenido del mensaje corto.

En que, los pasos anteriores 1 y 2 son flujos de transmisión de un mensaje corto cifrado, mientras que los pasos 3 y 4 son flujos de recepción de un mensaje corto cifrado.

Los pasos anteriores pueden garantizar la transmisión segura del mensaje corto en el enlace inalámbrico y entre la MS y el MSC. Para garantizar la transmisión segura en el enlace MSC-IWMSCSC-GMSC-MS, opcionalmente, en el paso 2, después de que el MSC al que pertenece la MS de la parte de transmisión descifra los UD de la PDU del mensaje corto, cifra los UD de la PDU del mensaje corto utilizando el identificador de usuario de la parte de recepción como identificador de cifrado mediante un módulo propio de cifrado-descifrado, y a continuación envía el mensaje corto al SC a través del IWMSC;

igualmente, en el paso 3, tras recibir el mensaje corto transmitido por el SC a través del GMSC, si se decide conforme al identificador de cifrado en el mismo que es necesario cifrar el mensaje corto, el MSC al que pertenece la MS de la parte de recepción descifra en primer lugar los UD de la PDU del mensaje corto utilizando el identificador de usuario de la parte de recepción como factor de descifrado mediante el módulo propio de cifrado-descifrado, y a continuación cifra los UD de la PDU del mensaje corto utilizando la CK de la parte de recepción como identificador de cifrado.

Los pasos opcionales (cifrado o descifrado utilizando el identificador de usuario de la parte de recepción como identificador de cifrado) de los pasos 2 y 3 anteriores deben estar presentes o ausentes simultáneamente en el sistema completo para garantizar la estabilidad de todo el sistema.

El identificador anterior del usuario de la parte de recepción es el MSISDN (número ISDN/PSTN internacional de suscriptor móvil) o el IMSI (número de identificación de suscriptor móvil internacional) de la parte de recepción.

El módulo anterior de cifrado-descifrado no está limitado a un módulo de cifrado-descifrado del software, y puede ser un módulo de cifrado-descifrado del hardware, e incluso puede ser un módulo de cifrado-descifrado del hardware capaz de actualizar el algoritmo de cifrado-descifrado.

La CK se calcula con un algoritmo particular (por ejemplo, en el sistema GSM se utiliza el algoritmo A8) a partir de un valor aleatorio (RAND) generado en el proceso de autentificación de la MS y el MSC y una clave raíz (Ki) del usuario. RAND es un número aleatorio distribuido a la MS durante el proceso de autentificación de la red para el usuario cuando se establece el enlace de señalización. Ki es una clave segura (128 bits) compartida por el USIM (módulo de identidad de suscriptor universal) y el HLR/AUC (registro de ubicación local/centro de autentificación) de la red local.

El identificador de cifrado puede ser implementado utilizando los bits restantes de la PDU o mediante un campo ampliado.

Además, en el paso 1, opcionalmente, la MS puede proporcionar una intercomunicación para el usuario de la parte de transmisión para que seleccione si se debe cifrar el mensaje corto a transmitir, y si el usuario de la parte de transmisión selecciona el cifrado, la MS de la parte de transmisión cifra los UD de la PDU del mensaje corto a transmitir.

El sistema del ejemplo de la presente invención comprende la MS de la parte de transmisión, el MSC al que pertenece la MS de la parte de transmisión, el MSC al que pertenece la MS de la parte de recepción, y la MS de la parte de recepción, tal como se ha descrito anteriormente.

En la presente invención, para transmitir el mensaje corto cifrado con mayor seguridad, la modificación consiste únicamente en configurar el módulo de cifrado-descifrado en la MS y el MSC, y los otros flujos fijos del mensaje corto no varían.

La figura 2 es el flujo del envío por la MS del mensaje corto cifrado, y esta figura describe el proceso de cifrado de un mensaje corto.

Cuando el usuario edita completamente el mensaje corto y organiza los datos de la PDU del mensaje corto y los prepara para enviarlos, si el usuario selecciona el cifrado del mensaje corto, la MS cifra la parte de datos del usuario de la PDU del mensaje corto utilizando su propia CK (la CK de la parte de transmisión) como identificador de cifrado del módulo de cifrado-descifrado, y a continuación establece con el mensaje corto un identificador de cifrado de dicho mensaje corto, y finalmente transmite el mensaje corto a través de la intecomunicación aire. Como implementación específica, los bits restantes Bit3 y Bit2 del estándar de codificación de datos DSC de la PDU pueden ser utilizados opcionalmente como 11 para el identificador de cifrado (actualmente la combinación 11 no se utiliza todavía). Este paso puede garantizar una alta seguridad de la transmisión inalámbrica. Si el usuario selecciona que el mensaje corto no se debe cifrar, el mensaje corto se transmite directamente mediante la intercomunicación aire según el flujo normal. Para simplificar la descripción, la descripción que sigue sólo incluye el flujo de procesamiento de la descifrado del mensaje corto, ya que un mensaje corto sin cifrar utiliza el flujo normal.

La figura 3 es el flujo de recepción en la MS de un mensaje corto cifrado, y esta figura describe cómo la MS recibe el mensaje corto cifrado.

Después de que la MS reciba el mensaje corto, decide si el identificador de cifrado es el modo de cifrado; en caso afirmativo, descifra la parte de datos de usuario de la PDU del mensaje corto utilizando su propia CK (la CK de la parte de recepción) como factor de descifrado del módulo de cifrado-descifrado, recuperando así el contenido del mensaje corto.

La figura 4 es el flujo de envío de un mensaje corto cifrado al SC de mensajes cortos, y esta figura describe cómo el mensaje corto cifrado enviado desde la MS es enviado al SC. En el que, el bloque de líneas punteadas es un paso opcional.

El mensaje corto cifrado enviado desde la MS se envía al MSC para reenviarlo tras ser recibido por el BSS, y el MSC necesita decidir si el mensaje corto es un mensaje corto cifrado cuando recibe la PDU del mensaje corto, y en caso afirmativo, necesita descifrar el mensaje corto utilizando la misma CK compartida por la parte de transmisión como factor de descifrado del algoritmo de descifrado del módulo de cifrado-descifrado. En este caso se debe observar que el motivo de que deba realizarse la descifrado es que el mensaje corto es transmitido conforme al mecanismo de almacenamiento-y-envío, y la CK obtenida mediante la autentificación de la parte de transmisión no puede ser obtenida por la parte de recepción. Incluso si el mensaje corto se descifra aquí, la práctica en el proceso anterior ha garantizado la alta seguridad del enlace completo desde la MS hasta el MSC. Para garantizar la alta seguridad del enlace completo desde el MSC hasta el SC, se puede implementar opcionalmente una operación de cifrado adicional, y para garantizar que la operación de cifrado se puede descifrar correctamente, se selecciona el identificador de la parte de recepción (puede seleccionarse el MSISDN como ejemplo) como identificador de cifrado para cifrar el mensaje corto que se acaba de descifrar. A continuación, el mensaje corto cifrado se guarda siempre con cifrado cuando se entrega al IWM-SC y finalmente al SC, garantizando así la seguridad del enlace entre el MSC y el SC. La seguridad del enlace completo se puede garantizar siempre que se garantice la seguridad del algoritmo de cifrado-descifrado. Por supuesto, la parte opcional de la figura puede no utilizarse, y de este modo el mensaje corto transmitido a continuación es un mensaje corto de texto simple que sólo tiene el identificador de cifrado, y la seguridad del enlace desde el MSC hasta el SC tendrá unas ciertas pérdidas.

La figura 5 es el flujo de envío por el SC de un mensaje corto cifrado a la parte de recepción, y esta figura describe cómo el SC transmite el mensaje corto recibido a la MS de la parte de recepción con seguridad. En el que, el bloque de líneas punteadas es un paso opcional, y está presente simultáneamente con el bloque de líneas punteadas de la figura 4.

La función del SC tras recibir el mensaje corto es volver a guardar y enviar el mensaje corto a la parte de recepción. El SC en primer lugar entrega el mensaje completo al GMSC, el GMSC busca a continuación el MSC al que pertenecen varias partes receptoras y vuelve a enviar el mensaje corto al MSC, y el MSC envía el mensaje corto a la MS de la parte de recepción a través del BSS tras la búsqueda de la MS de la parte de recepción y autentificarse correctamente. Antes de enviar el mensaje corto, el MSC debe decidir si el mensaje corto tiene un identificador del mensaje corto cifrado. Si no existe ningún identificador del mensaje corto, el MSC transmite el mensaje corto como un mensaje corto normal; de lo contrario, los datos de usuario de la PDU se descifran en primer lugar utilizando el identificador de la parte de recepción como factor de descifrado del módulo de cifrado-descifrado cuando el sistema completo dispone del módulo opcional, y cuando no existe módulo opcional, el mensaje corto en sí es el contenido descifrado y por lo tanto no necesita ser descifrado; a continuación, en cuanto al contenido descifrado, los datos de usuario de la PDU se cifran utilizando la CK de la parte de recepción como identificador de cifrado del módulo de cifrado-descifrado, y a continuación el mensaje corto cifrado se envía a la parte de recepción a través del sistema BSS. En este caso se debe tener en cuenta que el módulo opcional debe configurarse colectivamente por completo con el fin de evitar la transmisión de la clave y por la comodidad de la posterior actualización del algoritmo del módulo de cifrado-descifrado.

En consecuencia, la MS en el ejemplo de la presente invención comprende un módulo de transmisión, un módulo de recepción y un módulo de cifrado-descifrado, comprendiendo el módulo de cifrado-descifrado un módulo secundario de cifrado y un módulo secundario de descifrado, en que, el módulo secundario de cifrado está configurado para cifrar el mensaje corto a transmitir utilizando la CK actual como identificador de cifrado, y envía el mensaje corto a través del módulo de transmisión;

el módulo secundario de descifrado está configurado para descifrar el mensaje corto recibido por el módulo de recepción utilizando la CK actual como factor de descifrado, recuperando así el contenido del mensaje corto.

Opcionalmente, la MS también incluye un módulo de intercomunicación,

el módulo de intercomunicación se configura para proporcionar una intercomunicación para que el usuario seleccione si se debe cifrar el mensaje corto a transmitir, y si el usuario selecciona el cifrado, informa al módulo de cifrado para que el módulo de cifrado cifre el mensaje corto a transmitir.

En consecuencia, el MSC en el ejemplo de la presente invención comprende un módulo de transmisión y un módulo de recepción, así como un módulo de cifrado-descifrado, comprendiendo el módulo de cifrado-descifrado un módulo secundario de cifrado y un módulo secundario de descifrado, en que,

el módulo secundario de descifrado se configura para descifrar el mensaje corto utilizando la CK de la parte de transmisión como factor de descifrado una vez que el módulo de recepción recibe el mensaje corto de la MS de la parte de transmisión, y a continuación envía el mensaje corto al centro de servicios (SC) mediante el módulo de transmisión;

el módulo secundario de cifrado está configurado para cifrar el mensaje corto utilizando la CK de la parte de recepción como identificador de cifrado una vez que el módulo de recepción recibe el mensaje corto del SC y a continuación envía el mensaje corto a la MS de la parte de recepción.

Opcionalmente, el módulo secundario de cifrado está configurado además para que, después que el módulo secundario de descifrado descifra el mensaje corto utilizando la CK de la parte de transmisión, cifrar el mensaje corto utilizando el identificador de usuario de la parte de recepción como identificador de cifrado, y a continuación transmite el mensaje corto al SC a través del módulo de transmisión; el módulo secundario de descifrado está configurado además para que, después de que el módulo de recepción reciba el mensaje corto del SC, descifra en primer lugar el mensaje corto utilizando el identificador de usuario de la parte de recepción como factor de descifrado, y a continuación cifra el mensaje corto utilizando la CK de la parte de recepción como identificador de cifrado a través del módulo secundario de cifrado.

Un experto con habilidad normal en la técnica puede comprender que todos o parte de los pasos del procedimiento anterior pueden implementarse dotando al hardware correspondiente de un programa, que puede ser almacenado en un medio legible por ordenador, como por ejemplo una memoria de sólo lectura, un disco magnético o un disco óptico. Opcionalmente, todos o parte de los pasos de los ejemplos anteriores también pueden implementarse utilizando uno o varios circuitos integrados. Igualmente, cada módulo/unidad de los ejemplos anteriores puede implementarse en forma de hardware, o en la forma de módulos funcionales de software. La presente invención no está limitada a una forma determinada de combinación de hardware y software.

Los ejemplos anteriores son sólo ejemplos preferentes de la presente invención, y no se utilizan para limitar la presente invención. Para un experto con habilidad normal en la técnica, la presente invención puede tener diversas modificaciones y cambios que caigan dentro del alcance de las reivindicaciones.

Aplicabilidad industrial

En la presente invención, mediante la adición del módulo de cifrado-descifrado correspondiente en la MS y el MSC, el mensaje corto se cifra y se descifra utilizando la CK que varía con el RAND (valor aleatorio) como identificador de cifrado-descifrado, para garantizar así que la red, el proveedor del dispositivo terminal y el operador no puedan fracturar el mensaje corto cifrado, y para garantizar la transmisión segura del SMS. Además, en el esquema de la presente invención, el identificador de cifrado es distinto cada vez, lo que aumenta la dificultad de fracturar el entorno de la transmisión inalámbrica. Además, la seguridad de todo el entorno de transmisión se puede conseguir con configuraciones opcionales.

REIVINDICACIONES

1. Procedimiento para implementar el cifrado de un mensaje corto, que comprende los siguientes pasos:

una estación móvil MS de la parte de transmisión cifra un mensaje corto a transmitir utilizando una clave de cifrado CK de la parte de transmisión como identificador de cifrado y después envía el mensaje corto;

un centro de conmutación móvil MSC al que pertenece la MS de la parte de transmisión descifra el mensaje corto utilizando la CK de la parte de transmisión como factor de descifrado tras recibir el mensaje corto, y a continuación envía el mensaje corto a un centro de servicios de mensajes cortos SC a través de un centro de servicios de mensajes de funcionamiento conjunto IWMSC;

tras recibir el mensaje corto transmitido por el SC a través de una puerta de un centro de conmutación móvil GMSC, el MSC al que pertenece la MS de la parte de recepción cifra el mensaje corto utilizando la CK de la parte de recepción como identificador de cifrado y a continuación envía el mensaje corto a la MS de la parte de recepción;

tras recibir el mensaje corto, la MS de la parte de recepción descifra el mensaje corto utilizando la CK de la parte de recepción como factor de descifrado, recuperando así el contenido del mensaje corto,

en el que la CK se calcula con un algoritmo determinado a partir de un valor aleatorio RAND generado en el proceso de autentificación de la MS y el MSC de la parte a la que pertenece la CK y una clave raíz Ki del usuario;

en el que el paso de que la MS de la parte de transmisión cifra el mensaje corto a transmitir utilizando la CK de la parte de transmisión como identificador de cifrado y a continuación envía el mensaje corto, comprende: la MS de la parte de transmisión cifra los datos de usuario UD de una unidad de datos de protocolo PDU del mensaje corto a transmitir utilizando la CK de la parte de transmisión como identificador de cifrado a través de un módulo propio de cifrado-descifrado, estableciendo un identificador de cifrado en la PDU del mensaje corto a transmitir, y a continuación envía el mensaje corto;

el paso en el que el MSC al que pertenece la MS de la parte de transmisión descifra el mensaje corto utilizando la CK de la parte de transmisión como factor de descifrado tras recibir el mensaje corto comprende: tras recibir el mensaje corto, si se decide conforme al identificador de cifrado en el que, dado que el mensaje corto es un mensaje corto cifrado, el MSC al que pertenece la MS de la parte de transmisión descifra los UD de la PDU del mensaje corto utilizando la CK de la parte de transmisión como factor de descifrado a través de un módulo propio de cifrado-descifrado;

el paso en el que el MSC al que pertenece la parte de recepción cifra el mensaje corto utilizando la CK de la parte de recepción como identificador de cifrado tras recibir el mensaje corto comprende: tras recibir el mensaje corto, si se decide conforme al identificador de cifrado en el que, dado que se debe cifrar el mensaje corto, el MSC al que pertenece la MS de la parte de recepción cifra los UD de la PDU del mensaje corto utilizando la CK de la parte de recepción como identificador de cifrado a través de un módulo propio de cifrado-descifrado;

el paso en que la MS de la parte de recepción descifra el mensaje corto utilizando la CK de la parte de recepción como factor de descifrado tras recibir el mensaje corto comprende: tras recibir el mensaje corto, si se decide conforme al identificador de cifrado en el mismo que el mensaje corto es un mensaje corto cifrado, la MS de la parte de recepción descifra los UD de la PDU del mensaje corto utilizando la CK de la parte de recepción como factor de descifrado a través de un módulo propio de cifrado-descifrado;

caracterizado porque tras descifrar los UD de la PDU del mensaje corto, el MSC al que pertenece la MS de la parte de transmisión cifra los UD de la PDU del mensaje corto utilizando un identificador de usuario de la parte de recepción como identificador de cifrado a través del módulo propio de cifrado-descifrado, y a continuación transmite el mensaje corto al SC a través del IWMSC; tras recibir el mensaje corto transmitido por el SC a través del GMSC, si se decide conforme al identificador de cifrado en el mismo que es necesario cifrar el mensaje corto, el MSC al que pertenece la MS de la parte de recepción descifra en primer lugar los UD de la PDU del mensaje corto utilizando el identificador del usuario de la parte de recepción como factor de descifrado a través del módulo propio de cifrado-descifrado, y a continuación cifra los UD de la PDU del mensaje corto utilizando la CK de la parte de recepción como identificador de cifrado.

2. Procedimiento, según la reivindicación 1, en que, el identificador de usuario de la parte de recepción es el número ISDN internacional del suscriptor móvil, MSISDN, o el número de identificación del suscriptor móvil internacional, IMSI, de la parte de recepción.

3. Procedimiento, según las reivindicaciones 1 o 2, en que, antes de que la MS de la parte de transmisión cifre el mensaje corto a transmitir, la MS proporciona una intercomunicación al usuario de la parte de transmisión para que seleccione si desea cifrar el mensaje corto a enviar, y si el usuario de la parte de transmisión selecciona el cifrado, la MS de la parte de transmisión cifra el mensaje corto a transmitir.

4. Procedimiento para transmitir un mensaje corto cifrado, que comprende los siguientes pasos:

una estación móvil MS de la parte de transmisión cifra el mensaje corto a transmitir utilizando la clave de cifrado CK de la parte de transmisión como identificador de cifrado y a continuación envía el mensaje corto;

el centro de conmutación móvil MSC al que pertenece la MS de la parte de transmisión descifra el mensaje corto utilizando la CK de la parte de transmisión como factor de descifrado tras recibir el mensaje corto, y a continuación envía el mensaje corto a un centro de servicios de mensajes cortos SC a través del centro de servicios de mensajes de funcionamiento conjunto IWMSC,

en el que la CK se calcula con un algoritmo determinado a partir de un valor aleatorio (RAND) generado en el proceso de autentificación de la MS y el MSC de la parte a la que pertenece la CK y una clave raíz Ki del usuario;

en el que el paso de que la MS de la parte de transmisión cifra el mensaje corto a transmitir utilizando la CK de la parte de transmisión como identificador de cifrado y a continuación envía el mensaje corto comprende: la MS de la parte de transmisión cifra los datos de usuario (UD) de la unidad de datos de protocolo (PDU) del mensaje corto a transmitir utilizando la CK de la parte de transmisión como identificador de cifrado a través del módulo propio de cifrado-descifrado, estableciendo un identificador de cifrado en la PDU del mensaje corto a transmitir, y enviando a continuación el mensaje corto;

el paso de que el MSC al que pertenece la MS de la parte de transmisión descifra el mensaje corto utilizando la CK de la parte de transmisión como factor de descifrado tras recibir el mensaje corto comprende: tras recibir el mensaje corto, si se determina conforme al identificador de cifrado en el mismo que el mensaje corto es un mensaje corto cifrado, el MSC al que pertenece la MS de la parte de transmisión descifra los UD de la PDU del mensaje corto utilizando la CK de la parte de transmisión como factor de descifrado a través del módulo propio de cifrado-descifrado;

caracterizado porque tras descifrar los UD de la PDU del mensaje corto, el MSC al que pertenece la MS de la parte de transmisión cifra los UD de la PDU del mensaje corto utilizando el identificador de usuario de la parte de recepción como identificador de cifrado mediante el módulo propio de cifrado-descifrado, y a continuación transmite el mensaje corto al SC a través del IWMSC.

5. Procedimiento para recibir un mensaje corto cifrado, que comprende los siguientes pasos:

tras recibir el mensaje corto transmitido por el centro de servicios de mensajes cortos SC a través de la puerta del centro de conmutación móvil GMSC, el centro de conmutación móvil MSC al que pertenece la estación móvil (MS) de la parte de recepción cifra el mensaje corto utilizando la clave de cifrado CK de la parte de recepción como identificador de cifrado y a continuación envía el mensaje corto a la MS de la parte de recepción;

tras recibir el mensaje corto, la MS de la parte de recepción descifra el mensaje corto utilizando la CK de la parte de recepción como factor de descifrado, recuperando de este modo el contenido del mensaje corto,

en que la CK se calcula con un algoritmo determinado a partir de un valor aleatorio RAND generado en el proceso de autentificación de la MS y el MSC de la parte a la que pertenece la CK y una clave raíz Ki del usuario;

en que el paso de que el MSC al que pertenece la MS de la parte de recepción cifra el mensaje corto utilizando la CK de la parte de recepción como identificador de cifrado tras recibir el mensaje corto comprende: tras recibir el mensaje corto, si se decide conforme al identificador de cifrado en el mismo que el mensaje corto se debe cifrar, el MSC al que pertenece la MS de la parte de recepción cifra los UD de la PDU del mensaje corto utilizando la CK de la parte de recepción como identificador de cifrado mediante el módulo propio de cifrado-descifrado;

el paso de que la MS de la parte de recepción descifra el mensaje corto utilizando la CK de la parte de recepción como factor de descifrado tras recibir el mensaje corto comprende: tras recibir el mensaje corto, si se decide conforme al identificador de cifrado en el mismo que el mensaje corto es un mensaje corto cifrado, la MS de la parte de recepción descifra los UD de la PDU del mensaje corto utilizando la CK de la parte de recepción como factor de descifrado mediante el módulo propio de cifrado-descifrado;

caracterizado porque tras recibir el mensaje corto transmitido por el SC a través del GMSC, si se decide conforme al identificador de cifrado en el mismo que es necesario cifrar el mensaje corto, el MSC al que pertenece la MS de la parte de recepción descifra en primer lugar los UD de la PSU del mensaje corto utilizando el identificador de usuario de la parte de recepción como factor de descifrado mediante el módulo propio de cifrado-descifrado, y a continuación cifra los UD de la PDU del mensaje corto utilizando la CK de la parte de recepción como identificador de cifrado.

6. Sistema para implementar el cifrado de un mensaje corto, que comprende una estación móvil MS de la parte de transmisión, un centro de conmutación móvil MSC al que pertenece la MS de la parte de transmisión, un MSC al que pertenece la MS de la parte de recepción, la MS de la parte de recepción, y la MS y el MSC de la parte de transmisión y la MS y el MSC de la parte de recepción se configuran con módulos de cifrado-descifrado, en los que,

la MS de la parte de transmisión se configura para cifrar el mensaje corto a transmitir utilizando una clave de cifrado CK de la parte de transmisión como identificador de cifrado mediante el módulo propio de cifrado-descifrado y a continuación envía el mensaje corto;

el MSC al que pertenece la MS de la parte de transmisión se configura para descifrar el mensaje corto utilizando la CK de la parte de transmisión como factor de descifrado mediante el módulo propio de cifrado-descifrado tras recibir el mensaje corto, y a continuación envía el mensaje corto a un centro de servicios de mensajes cortos SC a través de un centro de servicios de mensajes de funcionamiento conjunto IWMSC;

el MSC al que pertenece la MS de la parte de recepción se configura para cifrar el mensaje corto utilizando la CK de la parte de recepción como identificador de cifrado mediante el módulo propio de cifrado-descifrado tras recibir el mensaje corto transmitido por el SC a través del GMSC y a continuación envía el mensaje corto a la MS de la parte de recepción;

la MS de la parte de recepción está configurada para descifrar el mensaje corto utilizando la CK de la parte de recepción como factor de descifrado mediante el módulo propio de cifrado-descifrado tras recibir el mensaje corto, recuperando así el contenido del mensaje corto,

en que la CK se calcula con un algoritmo determinado a partir de un valor aleatorio RAND generado en el proceso de autentificación de la MS y el MSC de la parte a la que pertenece la CK y una clave raíz Ki del usuario; en que el paso de que la MS de la parte de transmisión cifra el mensaje corto a transmitir utilizando la CK de la parte de transmisión como identificador de cifrado mediante el módulo propio de cifrado-descifrado y a continuación envía el mensaje corto comprende: la MS de la parte de transmisión cifra los datos de usuario UD de la unidad de datos de protocolo PDU del mensaje corto a transmitir utilizando la CK de la parte de transmisión como identificador de cifrado a través del módulo propio de cifrado-descifrado, estableciendo un identificador de cifrado en la PDU del mensaje corto a transmitir, y a continuación envía el mensaje corto;

el paso de que el MSC al que pertenece la MS de la parte de transmisión descifra el mensaje corto utilizando la CK de la parte de transmisión como factor de descifrado mediante el módulo propio de cifrado-descifrado tras recibir el mensaje corto comprende: tras recibir el mensaje corto, si se decide conforme al identificador de cifrado en el mismo que el mensaje corto es un mensaje corto cifrado, el MSC al que pertenece la MS de la parte de transmisión descifra los UD de la PDU del mensaje corto utilizando la CK de la parte de transmisión como factor de descifrado mediante el módulo propio de cifrado-descifrado;

el paso de que el MSC al que pertenece la MS de la parte de recepción cifra el mensaje corto utilizando la CK de la parte de recepción como identificador de cifrado mediante el módulo propio de cifrado-descifrado tras recibir el mensaje corto comprende: tras recibir el mensaje corto, si se decide conforme al identificador de cifrado en el mismo que es necesario cifrar el mensaje corto, el MSC al que pertenece la MS de la parte de recepción cifra los UD de la PDU del mensaje corto utilizando la CK de la parte de recepción como identificador de cifrado mediante un módulo propio de cifrado-descifrado;

el paso de que la MS de la parte de recepción descifra el mensaje corto utilizando la CK de la parte de recepción como factor de descifrado mediante el módulo propio de cifrado-descifrado tras recibir el mensaje corto comprende: tras recibir el mensaje corto, si se decide conforme al identificador de cifrado en el mismo que el mensaje corto es un mensaje corto cifrado, la MS de la parte de recepción descifra los UD de la PDU del mensaje corto utilizando la CK de la parte de recepción como factor de descifrado mediante el módulo propio de cifrado-descifrado;

caracterizado porque tras descifrar los UD de la PDU del mensaje corto, el MSC al que pertenece la MS de la parte de transmisión cifra los UD de la PDU del mensaje corto utilizando el identificador de usuario de la parte de recepción como identificador de cifrado mediante el módulo propio de cifrado-descifrado, y a continuación transmite el mensaje corto al SC a través del IWMSC;

tras recibir el mensaje corto transmitido por el SC a través del GMSC, si se decide conforme al identificador de cifrado en el mismo que es necesario cifrar el mensaje corto, el MSC al que pertenece la MS de la parte de

recepción descifra en primer lugar los UD de la PDU del mensaje corto utilizando el identificador de usuario de la parte de recepción como factor de descifrado mediante el módulo propio de cifrado-descifrado, y a continuación cifra los UD de la PDU del mensaje corto utilizando la CK de la parte de recepción como identificador de cifrado.

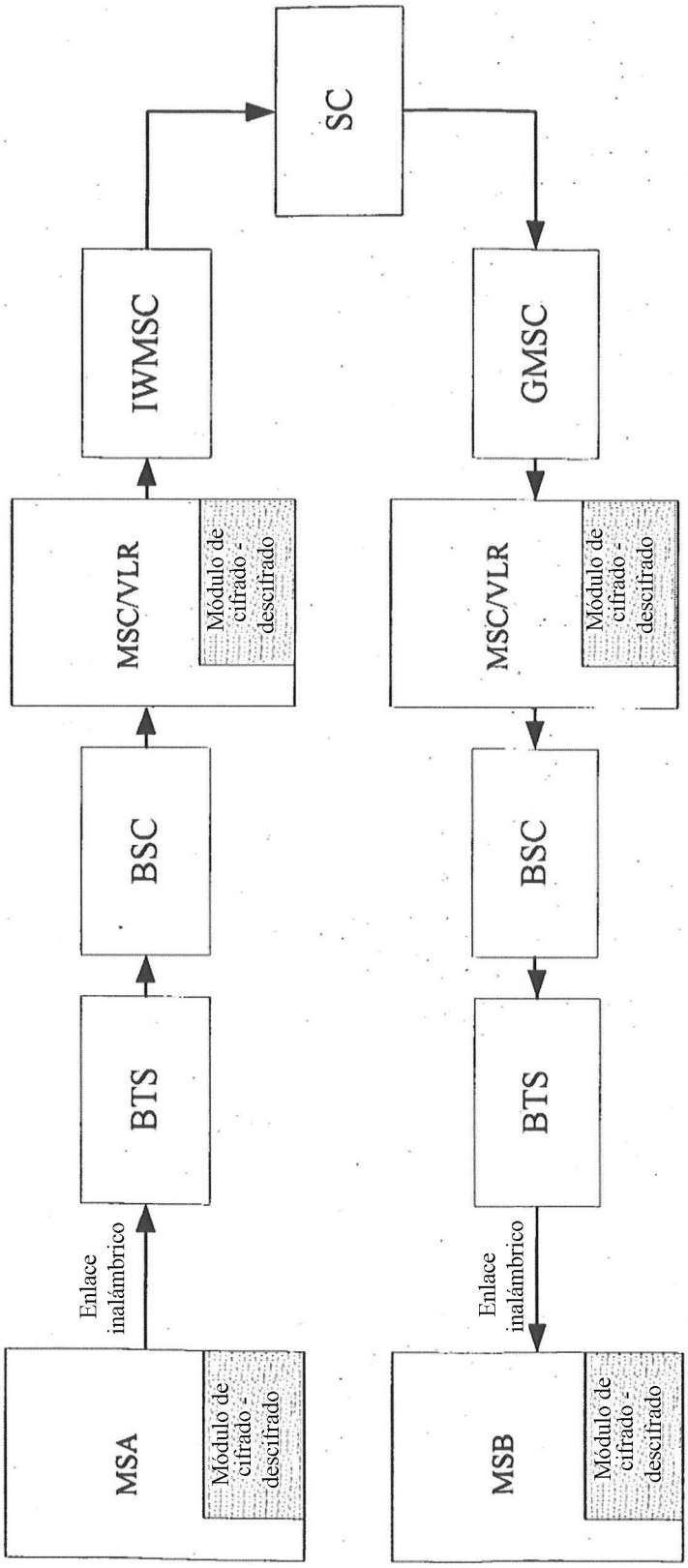
SC
IWMSC
GMSC
MSC/VLR
Módulo de cifrado - descifrado
MSC/VLR
Módulo de cifrado - descifrado
BSC
BSC
BTS
BTS
Enlace inalámbrico
Enlace inalámbrico
MSA
Módulo de cifrado - descifrado
MSB
Módulo de cifrado - descifrado

FIG. 1

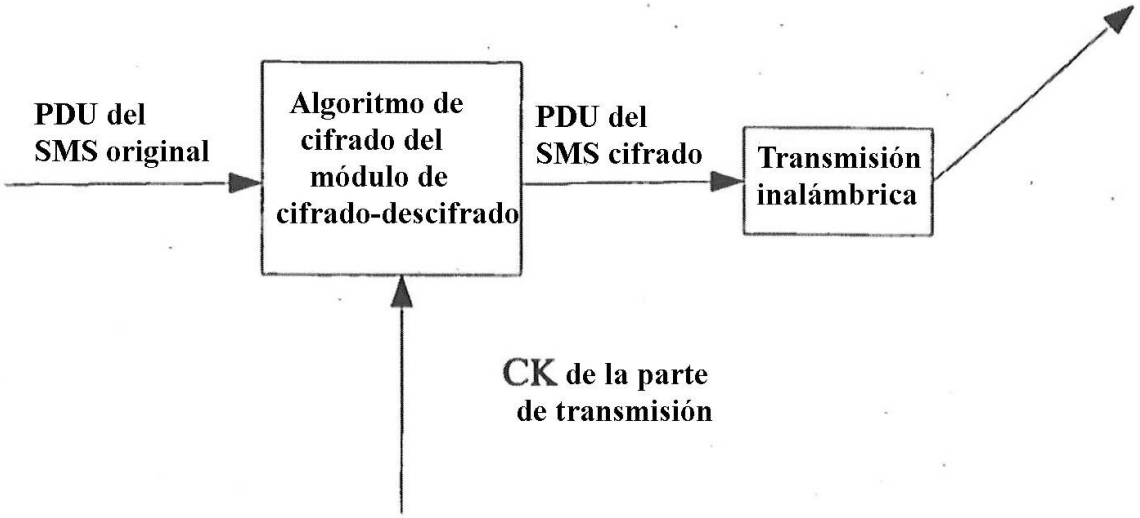
PDU del
SMS original
Algoritmo de
cifrado del
módulo de
cifrado-descifrado
PDU del
SMS cifrado
Transmisión
inalámbrica
CK de la parte
de transmisión

FIG. 2

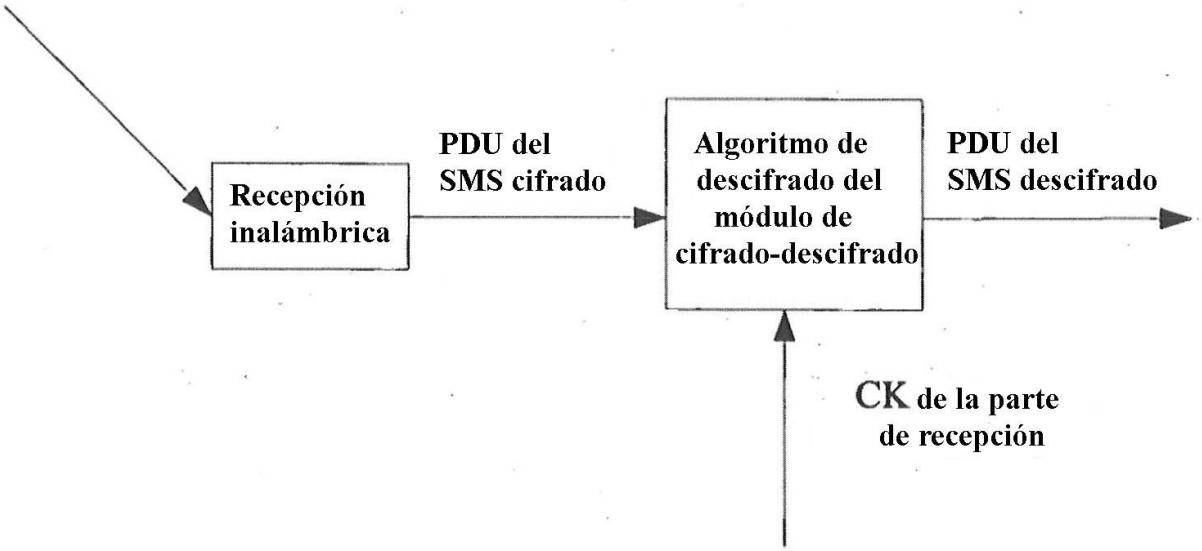
Recepción
inalámbrica
PDU del
SMS cifrado
Algoritmo de
descifrado del
módulo de
cifrado-descifrado
PDU del
SMS descifrado
CK de la parte
de recepción

FIG. 3

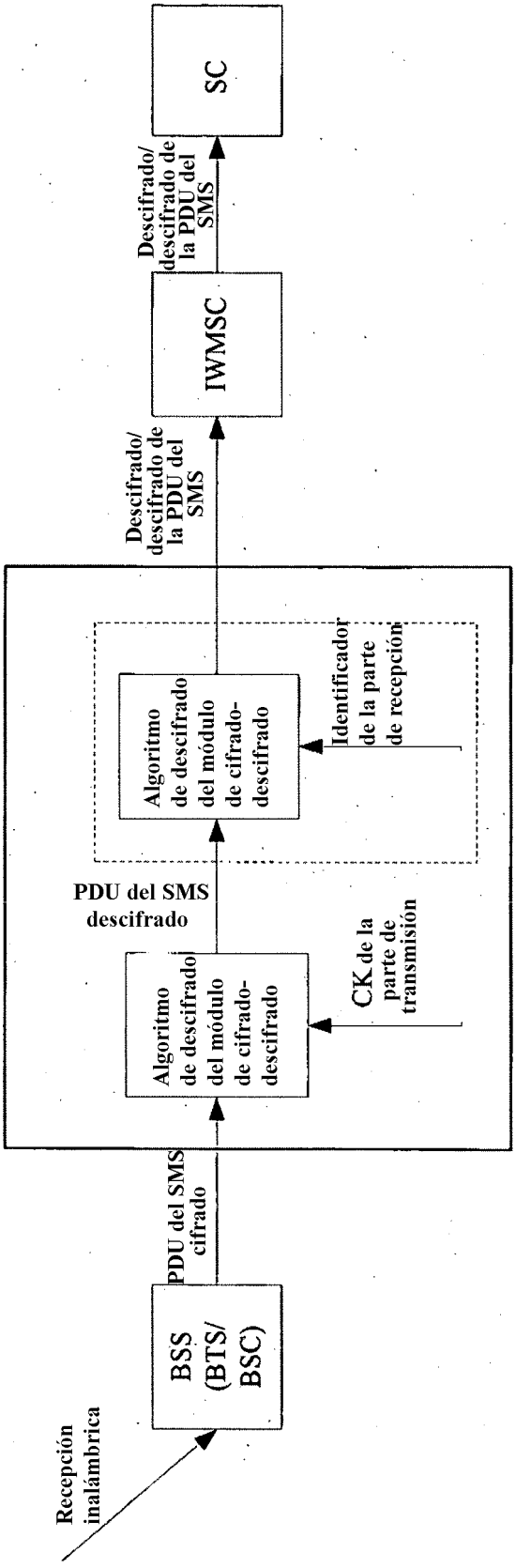
Recepción inalámbrica
BSS (BTS/ BSC)
PDU del SMS cifrado
Algoritmo de descifrado del módulo de cifrado-descifrado
CK de la parte de transmisión
PDU del SMS descifrado
Algoritmo de descifrado del módulo de cifrado-descifrado
Identificador de la parte de recepción
Descifrado/ descifrado de la PDU del SMS
IWMSC
Descifrado/ descifrado de la PDU del SMS
SC

FIG. 4

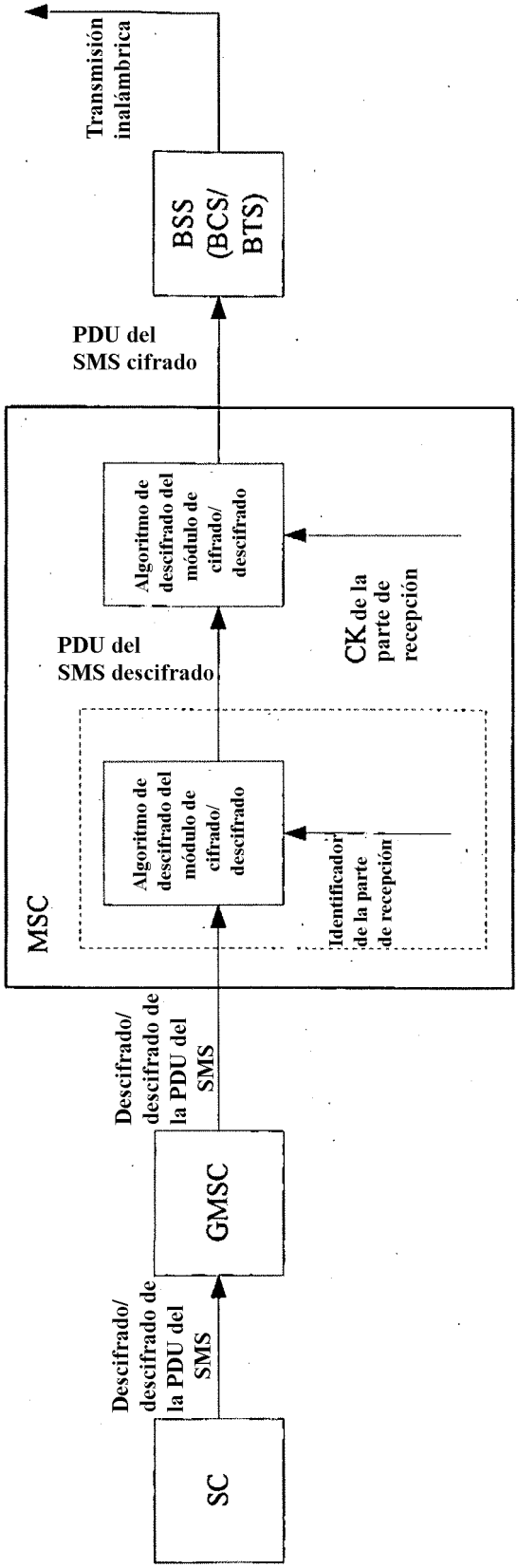
Transmisión inalámbrica
BSS (BCS/ BTS)
PDU del SMS cifrado
MSC
Algoritmo de descifrado del módulo de cifrado/ descifrado
CK de la parte de recepción
PDU del SMS descifrado
Algoritmo de descifrado del módulo de cifrado/ descifrado
Identificador de la parte de recepción
Descifrado/ descifrado de la PDU del SMS
GMSC
Descifrado/ descifrado de la PDU del SMS
SC

FIG. 5