(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 632 559**

(51) Int. CI.:

H04L 9/08 (2006.01)
H04W 12/02 (2009.01)
H04W 12/08 (2009.01)
G06F 21/60 (2013.01)
G06F 21/62 (2013.01)
H04W 12/12 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **19.03.2013 PCT/CN2013/072878**

(87) Fecha y número de publicación internacional: **10.10.2013 WO13149548**

(96) Fecha de presentación y número de la solicitud europea: **19.03.2013 E 13772153 (6)**

(97) Fecha y número de publicación de la concesión europea: **21.06.2017 EP 2835997**

(54) Título: **Método de cifrado de teléfono celular y método de descifrado**

(30) Prioridad:

06.04.2012 CN 201210100946

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
14.09.2017

(73) Titular/es:

HUIZHOU TCL MOBILE COMMUNICATION CO., LTD. (100.0%)
70 Huifeng 4th Road Zhongkai Hi-Tech Development District
Huizhou, Guangdong 516006, CN

(72) Inventor/es:

WANG, YAHUI

(74) Agente/Representante:

SÁEZ MAESO, Ana

DESCRIPCIÓN

Método de cifrado de teléfono celular y método de descifrado

Campo de la invención

La presente divulgación se refiere al campo de dispositivos de teléfonos móviles y más particularmente con un método de cifrado de datos y un método de descifrado de datos para un teléfono móvil, de acuerdo con el preámbulo de la reivindicación 1 y reivindicación 6, respectivamente.

Antecedentes de la invención

Para usuarios de teléfonos móviles convencionales, la pérdida de los teléfonos móviles puede provocar el uso malicioso de fotografías, información de vídeos o información financiera almacenada en teléfonos móviles y la fuga de información privada personal, que puede generar una gran influencia en el propietario del teléfono móvil.

Adicionalmente, se han desplegado ampliamente redes WIFI en lugares públicos tal como cafeterías, restaurantes y librerías, etcétera. Cuando los teléfonos móviles se utilizan para navegar en páginas web o ejecutar aplicaciones de red a través de redes WIFI, existe el riesgo de que los documentos almacenados en los teléfonos móviles sean robados por hackers.

En el caso de los documentos almacenados en teléfonos móviles se obtengan por personas malintencionadas, las personas malintencionadas pueden cargar los documentos a internet para navegar porque el público que navega provoque la fuga de información privada del propietario del teléfono móvil, e incluso peor, pueda hacer estragos a los propietarios de los teléfonos móviles provocando sustanciales pérdidas económicas a los propietarios.

Una Solicitud de Patente China CN102368850A (D1) divulga un método de cifrado y descifrado para un documento de video sobre un teléfono móvil. El método de cifrado comprende: ingresar un primer código sobre un primer teléfono móvil por un usuario; combinar el primer código con un número de identificación del primer teléfono móvil para formar una cadena de caracteres cifrados; y cifrar el documento de video médiate la cadena de caracteres cifrados para generar un documento de vídeo cifrado. En forma correspondiente, el método de cifrado comprende: ingresar un segundo código en un segundo teléfono móvil por un usuario; comparar el segundo código con el primer código; Si el segundo código es igual que el primer código, combinar el segundo código con un número de identificación del segundo teléfono móvil para formar una cadena de caracteres descifrados; y comparar el número de identificación del segundo teléfono móvil con aquel del primer teléfono móvil y descifrar el documento de video cifrado por la cadena de caracteres descifrados en el que si el número de identificación del segundo teléfono móvil es igual que aquel del primer teléfono móvil (es decir, el segundo teléfono móvil y el primer teléfono móvil son un mismo teléfono móvil) , el documento de video se descifra exitosamente y el documento de video descifrado se puede leer o utilizar normalmente; en contraste, si el número de identificación del segundo teléfono móvil es diferente de aquel del primer teléfono móvil (es decir, el segundo teléfono móvil y el primer teléfono móvil son teléfonos móviles diferentes), el documento de video descifrado se daña y no se puede leer o utilizar.

Por lo tanto, el método de cifrado y descifrado del documento D1 utiliza el número de identificación del teléfono móvil, para asegurar que los documentos solo se lean o sean utilizados por el mismo teléfono móvil y no se puede leer o utilizar por cualquier otro teléfono móvil, para proteger la seguridad de los documentos.

Sin embargo, el método de cifrado y descifrado del documento D1 sólo puede proteger los documentos cifrados almacenados en el teléfono móvil de que sean leídos por otros dispositivos, pero si el teléfono que almacena los documentos cifrados es robado, el documento D1 no puede proporcionar una protección adicional para los documentos almacenados en el teléfono móvil robado, y los documentos almacenados en el teléfono móvil robado se pueden leer o utilizar pueden ser utilizados por otros usuarios.

De acuerdo con lo anterior, lo que se necesita es proporcionar un método de cifrado de datos y un método de descifrado de datos para un teléfono móvil con el fin de proteger la seguridad de los datos del teléfono móvil.

Resumen de la invención

Un problema técnico principal que va a resolver la presente divulgación es proporcionar un método de cifrado de datos y un método de descifrado de datos para un teléfono móvil con el fin de proteger la seguridad de los datos del teléfono móvil.

Para resolver el problema técnico mencionado anteriormente, una solución técnica adoptada por la presente divulgación es proporcionar un método de cifrado de datos para un teléfono móvil de acuerdo con la reivindicación 1.

El método de cifrado de datos para un teléfono móvil comprende: obtener una entrada de código PIN por un usuario y obtener un código de tarjeta SIM de una tarjeta SIM de acuerdo con el código PIN, y combinar el código PIN y el

código de la tarjeta SIM en una cadena de contraseña; utilizar la cadena de contraseña para cifrar los datos fuente con el fin de obtener datos cifrados; y configurar un código de identificación (ID) de datos cifrados al utilizar número IMEI del teléfono móvil, y colocar el código ID de datos cifrados antes de los datos cifrados.

La etapa de utilizar la cadena de contraseña para cifrar datos fuente con el fin de obtener datos cifrados puede comprender: con respecto a los datos fuente en unidades del número de bytes de la cadena de contraseña; realizar una operación lógica en la cadena de contraseña y los datos fuente que se leen; y almacenar los datos fuente, que se obtienen de la operación lógica, como los datos cifrados.

La operación lógica puede ser una operación XOR.

Para resolver el problema técnico mencionado anteriormente, otra solución técnica adoptada por la presente divulgación es proporcionar un método de descifrado de datos para un teléfono móvil de acuerdo con la reivindicación 6.

El método de descifrado de datos para un teléfono móvil puede comprender: obtener una entrada de código PIN para un usuario y obtener un código de tarjeta SIM de una tarjeta SIM de acuerdo con el código PIN, y combinar el código PIN y el código de la tarjeta SIM en una cadena de contraseña; y utilizar la cadena de contraseña para descifrar los datos cifrados con el fin de obtener datos fuente.

La etapa de utilizar la cadena de contraseña para descifrar datos cifrados con el fin de obtener datos fuente puede comprender: leer los datos cifrados en unidades del número de bytes de la cadena de contraseña; realizar una operación lógica de la cadena de contraseña y los datos cifrados que se leen; y almacenar los datos cifrados, que se obtienen de la operación lógica, como los datos fuente.

La operación lógica es una operación XOR.

El método de cifrado de datos para un teléfono móvil comprende: obtener una entrada de código PIN por un usuario y obtener un código de tarjeta SIM de una tarjeta SIM de acuerdo con el código PIN y combinar el código PIN y el código de tarjeta SIM en la cadena de contraseña; y utilizar la cadena de contraseña para cifrar datos fuente con el fin de obtener datos cifrados.

Preferiblemente, la etapa de utilizar la cadena de contraseña para cifrar datos fuente con el fin de obtener datos cifrados comprende: leer los datos fuente en unidades del número de bytes de la cadena de contraseña; realizando una operación lógica en la cadena de contraseña y los datos fuente que se leen; y almacenar los datos fuente, que se obtienen de la operación lógica, como los datos cifrados.

Preferiblemente, la etapa de realizar una operación lógica en la cadena de contraseña y los datos fuente que se leen comprende: realizar una operación lógica directamente sobre la cadena de contraseña y los datos fuente que se leen cuando el número de bytes de los datos fuente que se leen es igual al número de bytes de la cadena de contraseña; y extraer parte de la cadena de contraseña, de la cual el número de bytes es igual al número de bytes de los datos fuente que se leen de la cadena de contraseña, y luego realizar una operación lógica de la parte de la cadena de contraseña y los datos fuente que se leen cuando el número de bytes de los datos fuente que se leen es menor que el número de bytes de la cadena de contraseña.

Preferiblemente, después de la etapa de utilizar de la cadena de contraseña para cifrar datos fuente con el fin de obtener datos cifrados, se fija un código de identificación (ID) de datos cifrados al utilizar un número IMEI del teléfono móvil, y el código ID de datos cifrados se coloca antes de los datos cifrados.

Preferiblemente, la operación lógica es una operación XOR.

Para resolver el problema técnico mencionado anteriormente, otra solución técnica adoptada por la presente divulgación es proporcionar un método de descifrado de datos para un teléfono móvil. El método de descifrado de datos para un teléfono móvil comprende: obtener una entrada de código PIN por un usuario y obtener un código de tarjeta SIM de una tarjeta SIM de acuerdo con el código PIN y combinar el código PIN y el código de tarjeta SIM en una cadena de contraseña; y utilizar la cadena de contraseña para descifrar datos cifrados con el fin de obtener datos fuente.

Preferiblemente, la etapa de utilizar la cadena de contraseña para descifrar datos cifrados con el fin de obtener datos fuente comprende: leer los datos cifrados en unidades del número de bytes de la cadena de contraseña; realizar una operación lógica de la cadena de contraseña y los datos cifrados que se leen; y almacenar los datos cifrados, que se obtienen de la operación lógica, como los datos fuente.

Preferiblemente, la etapa de realizar una operación lógica en la cadena de contraseña y los datos cifrados que se leen comprende: realizar una operación lógica directamente sobre la cadena de contraseña y los datos cifrados que se leen cuando el número de bytes en los datos cifrados que se leen es igual al número de bytes de la cadena de

contraseña; y extraer parte de la cadena de contraseña, de cual el número de bytes es igual al número de bytes de los datos cifrados que se leen de la cadena de contraseña, y luego realizar una operación lógica sobre la parte de la cadena de contraseña y los datos cifrados que se leen cuando el número de bytes de datos cifrados que se leen es menor que el número de bytes de la cadena de contraseña.

Preferiblemente, después de la etapa de utilizar la cadena de contraseña para descifrar datos cifrados con el fin de obtener datos fuente, se elimina un código de identificación (ID) de datos cifrados puesto antes de los datos cifrados de acuerdo con un número IMEI del teléfono móvil.

Preferiblemente, la operación lógica es una operación XOR.

Como se compara con la técnica anterior, los beneficios de la presente divulgación son como sigue: el método de cifrado de datos y el método de descifrado de datos para un teléfono móvil de la presente divulgación cifra o descifra documentos almacenados en el teléfono móvil al combinar el código de tarjeta SIM y el código PIN en una cadena de contraseña y de esta forma, los datos del teléfono móvil no serán robados y se puede proteger la seguridad de los datos.

Breve descripción de los dibujos

La figura 1 es un diagrama de bloques funcional de un teléfono móvil basado en un método de cifrado/descifrado para un teléfono móvil de la presente divulgación;

La figura 2 es un diagrama de flujo de una primera realización de un método de cifrado de datos para un teléfono móvil de acuerdo con la presente divulgación;

La figura 3 es una vista esquemática que ilustra cómo se leen los datos fuente en la primera realización del método de cifrado de datos para un teléfono móvil de acuerdo con la presente divulgación;

La figura 4 es un diagrama de flujo de una primera realización de un método de descifrado de datos para un teléfono móvil de acuerdo con la presente divulgación;

La figura 5 es una esquemática que ilustra cómo se leen datos cifrados en la primera realización del método de descifrado de datos para un teléfono móvil de acuerdo con la presente divulgación;

La figura 6 es un diagrama de flujo de un método que detecta códigos PIN encendidos basado en el método de cifrado/descifrado de datos para un teléfono móvil divulgado por la presente divulgación;

La figura 7 es un diagrama de diagrama de flujo de un método de borrado remoto de información basado en el método de cifrado/descifrado de datos para un teléfono móvil divulgado por la presente divulgación;

La figura 8 es un diagrama de flujo de un método de entrada de datos basado en el método de cifrado/descifrado de datos para un teléfono móvil divulgado por la presente divulgación; y

La figura 9 es un diagrama de flujo de un método para configurar datos cifrados en datos n cifrados basados en el método de cifrado/descifrado de datos para un teléfono móvil divulgado por la presente divulgación.

Descripción detallada de la invención

Con referencia a la figura 1 en primer lugar, la figura 1 es un diagrama de bloques funcional de un teléfono móvil basado en el método de cifrado/descifrado de datos para un teléfono móvil de la presente divulgación. Como se muestra en la figura 1, el teléfono móvil basado en el método de cifrado/descifrado de datos para el teléfono móvil de la presente divulgación comprende principalmente: un teclado 101, una cámara 102, una pantalla 103 LCD (pantalla de cristal líquido), una memoria 104, un chip 105 de procesamiento de señal de banda base, un módulo 106 de gestión de energía, una batería 107, un módulo 108 RF (Radio frecuencia), una tarjeta 109 SIM y una ranura 110 de tarjeta SD (Tarjeta de Memoria Digital Segura). Las funciones de los anteriores módulos son como sigue:

el teclado 101: comprende un teclado físico o un teclado virtual ubicado en una pantalla táctil y se configura para controlar el sistema de un teléfono móvil;

la cámara 102: se configura para tomar una fotografía o registrar un vídeo, en donde los datos de vídeo o las fotografías capturadas por la cámara pueden ser cifrados mediante la presente divulgación.

la pantalla 103 LCD: se configura para visualizar una interfaz de control;

la memoria 104: se configura para almacenar sistemas y programas para implementar el método de la presente divulgación y también almacenar datos personales (por ejemplo, fotografías, videos, grabaciones, mensajes y libros

de direcciones del teléfono móvil) del usuario, en donde los datos personales en la memoria pueden estar cifrados o descifrados.

el chip 105 de procesamiento de señal de base de banda: se utilizar como una unidad de procesamiento central, y se configura para controlar módulos periféricos del sistema;

el módulo 106 de gestión de energía: se configurado para convertir energía de la batería en un voltaje necesario para la operación de los módulos funcionales;

la batería 107: se configura para proporcionar la energía para el sistema;

el módulo 108 RF: se configura para alcanzar comunicación entre el sistema de teléfono móvil y la red externa y en la presente divulgación, más se configuran adicionalmente para recibir información de control transmitida desde el exterior por el usuario del teléfono móvil;

la tarjeta 109 SIM (módulo de identidad del suscriptor): se configura para almacenar un código de tarjeta SIM y un código de identificación de red del usuario, en donde la tarjeta 109 SIM se puede activar para detección de código PIN. Sólo si la autenticación de código PIN de la tarjeta SIM pasa, los datos de la red en la tarjeta SIM pueden ser accesados por el teléfono móvil.

la ranura 110 de tarjeta SD: se configura para conectar con la tarjeta SD y permite al usuario expandir un espacio para almacenar documentos de datos fácilmente, en donde los datos personales en la tarjeta SD también se pueden cifrar o descifrar, y el que un mensaje para borrar información personal es recibido por el sistema de teléfono móvil, el sistema borrará todos los datos de la tarjeta SD automáticamente. En la presente divulgación, los datos en la ranura de tarjeta SD pueden estar cifrados.

De esta manera, en términos de hardware, el teléfono móvil basado en el método de cifrado/descifrado de datos para el teléfono móvil de la presente divulgación es exactamente igual que el teléfono móvil convencional. Al escribir el método de cifrado/descifrado para el teléfono móvil de la presente divulgación en el chip 105 de procesamiento de señal de base de banda, el chip 105 de procesamiento de señal de base de banda puede cifrar o descifrar los datos del teléfono móvil de acuerdo con el método. Específicamente, el método de cifrado/descifrado de datos para el teléfono móvil se puede implementar mediante códigos de software.

El método de cifrado/descifrado de datos para el teléfono móvil de la presente divulgación se describirá en detalle con referencia a la figura 2 a figura 5.

Con referencia a la figura 2, la figura 2 es un diagrama de flujo de una primera realización de un método de cifrado de datos para un teléfono móvil de acuerdo con la presente divulgación. Como se muestra en la figura 2, el método de cifrado de datos para el teléfono móvil de la presente divulgación comprende las siguientes etapas de:

Etapa 201: obtener una entrada de código PIN (número de identificación personal) por un usuario y obtener un código de tarjeta SIM de la tarjeta 109 SIM de acuerdo con el código PIN y combinar el código PIN y el código de la tarjeta SIM en una cadena de contraseña; y

Etapa 202: utilizar la cadena de contraseña para cifrar datos de fuente con el fin de obtener datos cifrados.

En la etapa 201, el usuario puede pedir el código PIN del operador de red una entrada del código PIN a través del teclado 101. El chip 105 de procesamiento de señal banda base obtiene el código PIN, obtiene el código de tarjeta SIM de la tarjeta 109 SIM de acuerdo con el código PIN y combina el código PIN y el código de tarjeta SIM en una cadena de contraseña. El código PIN y el código de tarjeta SIM se pueden combinar con el código PIN que precede al código de tarjeta SIM o el código de tarjeta SIM que precede al código PIN o al insertar caracteres del código PIN en el código de tarjeta SIM para formar la cadena de contraseña. Preferiblemente, el código PIN y el código de tarjeta SIM se combinan con el código PIN que precede al código de tarjeta SIM para formar la cadena de contraseña en la presente divulgación.

Adicionalmente, después de obtener el código PIN, el chip 105 de procesamiento de señal de base de banda puede adicionalmente almacenar el código PIN en la memoria 104 para posterior uso en el método de descifrado de datos para un teléfono móvil.

Específicamente, en la etapa 202, los datos fuente se pueden leer en unidades de un número de bytes de la cadena de contraseña, se realiza una operación lógica sobre la cadena de contraseña y los datos fuente que se leen y los datos fuente que han realizado la operación lógica se almacenan como datos cifrados, obteniendo así datos cifrados.

En la etapa de realizar la operación lógica en la cadena de contraseña y los datos fuente que se leen, la operación lógica se realiza directamente sobre la cadena de contraseña y los datos fuente que se leen cuando el número de

bytes en los datos fuente que se leen es igual a un número de bytes de la cadena de contraseña; y cuando el número de bytes de los datos fuente que se leen es menor que el número de bytes de la cadena de contraseña, una parte de la cadena de contraseña, de la que el número de bytes es igual al número de bytes de los datos fuente que se leen, se extrae de la cadena de contraseña, y luego se realiza la operación lógica sobre la parte de la cadena de contraseña y los datos fuente que se leen.

Específicamente, con referencia a la figura 3, la figura 3 es una vista esquemática que ilustra cómo se leen los datos fuente en la primera realización del método de cifrado de datos para un teléfono móvil de acuerdo con la presente divulgación. Como se muestra en la figura 3, una cadena 40 de contraseña consiste de un código PIN (de 4 bytes) y un código de tarjeta SIM (de 16 bytes), de tal manera que el número de bytes de la cadena 40 de contraseña es 20 bytes. Asumiendo que el número de bytes de los datos 30 de tarjeta son 132 bytes, los datos 30 de fuente se pueden dividir en 7 bloques de datos (es decir, los bloques 301-307 de datos como se muestra en la figura 3) de tal manera que se lee en unidades de 20 bytes de la cadena 40 de contraseña.

Cuando los datos 30 de fuente se leen en unidades del número de bytes (20 bytes) de la cadena 40 de contraseña, que divide el número 132 de bytes de los datos 30 de fuente por el número 20 de los bytes de la cadena 40 de contraseña resulta en un restante de 12. Por lo tanto, el número de bytes de los bloques 301-306 de datos que se leen es 20 bytes, y el número de bytes del bloque 307 de datos que se lee al final es de solo 12 bytes. Cuando el bloque 307 de datos se lee en unidades de 20 bytes, se leerá un exceso de 8 bytes, y se necesita eliminar el exceso de 8 bytes. Específicamente, los 12 restantes se restan del número 20 de bytes de la cadena de contraseña para obtener un valor de diferencia de 8, que es solo el número de bytes excesivos que se leerían cuando se lee el último bloque 307 de datos en unidades del número de bytes de la cadena 40 de contraseña. Entonces, los 8 bytes de exceso de datos se eliminan de tal manera que se puede leer correctamente el último bloque 307 de datos.

En razón a que el número de bytes en los bloques 301-306 de datos es igual que el número de bytes de la cadena 40 de contraseña, se puede realizar directamente la operación lógica sobre la cadena de contraseña y cada uno de los bloques 301-306 de datos respectivamente. En razón a que el número de bytes del bloque 307 de datos es 12, que es menos que el número 20 de bytes de la cadena 40 de contraseña, parte de la cadena de contraseña, de la cual el número de bytes es igual al número de bytes del bloque 307 de datos, se puede extraer de la cadena 40 de contraseña, y luego se realiza la operación lógica sobre la parte de la cadena de contraseña y el bloque 307 de datos.

Específicamente, los datos de 12 bytes se pueden extraer desde el inicio de la cadena 40 de contraseña de 20 bytes, y luego se realiza la operación lógica sobre los datos de 12 bytes y el bloque 307 de datos. Por supuesto, los datos de 12 bytes también se pueden extraer inversamente desde el final de la cadena 40 de contraseña de 20 bytes, y luego se realiza la operación lógica sobre los datos de 12 bytes y el bloque 307 de datos, y no se hace limitación a esto mediante la presente divulgación.

De acuerdo con lo anterior, después que los datos 30 de fuente se cifran al utilizar la cadena 40 de contraseña, se pueden obtener los datos 50 cifrados. El número de bytes de los datos 50 cifrados es igual que aquel de los datos 30 de fuente (es decir, 132 bytes).

En realizaciones alternas de la presente divulgación, después que se obtienen los datos cifrados, se puede fijar adicionalmente un código de identificación (ID) de datos cifrados al utilizar un número IMEI (identidad de equipo móvil internacional) del teléfono móvil, y el código ID de datos cifrados se coloca antes de los datos 50 cifrados. Específicamente, el número IMEI se puede duplicar de tal manera que se combinas dos números IMEI idénticos para formar el código ID de datos cifrados. El número IMEI tiene 15 bytes, de tal manera que el número de bytes de los dos números IMEI idénticos es 30 bytes. Después que se fija el código ID de datos cifrados, se puede determinar si los datos que se leen son datos cifrados al detectar el código ID de datos cifrados de 30 bytes que coloca antes de los datos 50 cifrados.

Adicionalmente, en el método de cifrado de datos para el teléfono móvil de la presente divulgación, la operación lógica mencionada anteriormente en preferiblemente una operación XOR. Por supuesto, otras operaciones lógicas tal como la operación AND, la operación OR, o la operación NOT también pueden estar cubiertas dentro del alcance de la presente invención, y no se hace limitación específica a esta mediante la presente divulgación.

Un método de descifrado de datos para un teléfono móvil para descifrar los datos cifrados generados por el método de cifrado de datos mencionado anteriormente para un teléfono móvil se describirá en detalle con referencia a la figura 4 en lo sucesivo. La figura 4 es un diagrama de flujo de la primera realización del método de descifrado de datos para un teléfono móvil de acuerdo con la presente divulgación. Como se muestra en la figura 4, el método de descifrado de datos para el teléfono móvil de la presente divulgación comprende las siguientes etapas de:

Etapa 401: obtener una entrada de código PIN por un usuario y obtener un código de tarjeta SIM de la tarjeta 109 SIM de acuerdo con el código PIN y combinar el código PIN y el código de tarjeta SIM en una cadena de contraseña; y

Etapa 402: utilizar la cadena de contraseña para descifrar datos cifrados con el fin de obtener datos fuente.

En la etapa 401, el usuario pide el código PIN del operador de red, e ingresa el código PIN a través del teclado 101. El chip 105 de procesamiento de señal de base de banda obtiene el código PIN guardado en la etapa de cifrado de la memoria 104 y compara el código PIN guardado con el código PIN de entrada. Si los dos códigos PIN son iguales, el código de tarjeta SIM se obtiene de la tarjeta 109 SIM al utilizar el código PIN, y el código PIN y el código de la tarjeta SIM se combinan en una cadena de contraseña. Si los dos códigos PIN son diferentes entre si, se le dirá al usuario que el código PIN es incorrecto y el usuario necesita reingresar el código PIN. La forma en que la cadena de contraseña se combina no se limita mientras que la cadena de contraseña es igual que aquella utilizada en la etapa de cifrado.

Específicamente, en la etapa 402, puede ser que un dato cifrado se lea en unidades del número de bytes de la cadena de contraseña, se realiza una operación lógica sobre la cadena de contraseña y los datos cifrados que se leen, y los datos cifrados, que han realizado la operación lógica, se almacenan como datos fuente, obteniendo así los datos fuente.

En la etapa de realizar una operación lógica en la cadena de contraseña y los datos cifrados que se leen, se realiza la operación lógica directamente sobre la cadena de contraseña y los datos cifrados que se leen cuando el número de bytes de los datos cifrados que se leen es igual al número de bytes de la cadena de contraseña. Cuando el número de bytes de los datos cifrados que se leen es menor que el número de bytes de la cadena de contraseña, parte de la cadena de contraseña, de la que el número de bytes es igual al número de bytes de datos cifrados que se leen, se extrae de la cadena de contraseña, y luego se realiza la operación lógica sobre la parte de la cadena de contraseña y los datos cifrados que se leen.

Específicamente, con referencia a la figura 5, la figura 5 es una vista esquemática que ilustra cómo se leen los datos cifrados en la primera realización del método de descifrado de datos para un teléfono móvil de acuerdo con la presente divulgación. Como se muestra en la figura 5, la cadena 40 de contraseña consiste de un código PIN (de 4 bytes) y un código de tarjeta SIM (de 16 bytes), de tal manera que el número de bytes de la cadena 40 de contraseña es 20 bytes. Si el número de bytes de los datos 50 cifrados es 132 bytes, los datos 50 cifrados se pueden dividir en 7 bloques de datos (es decir, los bloques 501-507 de datos como se muestra en la figura 5) cuando se lee en unidades del número de bytes (20 bytes) de la cadena 40 de contraseña.

Cuando los datos 50 cifrados se leen en unidades del número de bytes (20 bytes) de la cadena 40 de contraseña, que dividen el número 132 de bytes de los datos 50 cifrados por el número 20 de los bytes de la cadena 40 de contraseña resulta en un restante de 12. Por lo tanto, el número de bytes de los bloques 501-506 de datos que se leen es 20 bytes, y el número de bytes del bloque 507 de datos que se lee es por lo menos de solo 12 bytes. Cuando el bloque 507 de datos se lee en unidades de 20 bytes, se leerá un exceso de 8 bytes, y es necesario eliminar el exceso de 8 bytes. Específicamente, los 12 restantes se restan del número 20 bytes de la cadena de contraseña para obtener una diferencia de 8, que es sólo el número exceso de bytes cuando se lee el último bloque 507 de datos en unidades del número de bytes de la cadena 40 de contraseña. El exceso de 8 bytes se elimina de tal manera que el último bloque 507 de datos se pueda leer correctamente.

En razón a que el número de bytes de los bloques 501-506 de datos es el mismo que el número de bytes de la cadena 40 de contraseña, se puede realizar la operación lógica directamente sobre la cadena de contraseña y cada uno de los bloques 501-506 de datos respectivamente. En razón a que el número de bytes de cada bloque 507 de datos es 12, que es menor que el número 20 de bytes de la cadena 40 de contraseña, una parte de la cadena de contraseña, de cual el número de bytes es igual al número de bytes del bloque 507 de datos, se puede extraer de la cadena 40 de contraseña, y luego se realiza la operación lógica sobre la parte de la cadena de contraseña y el bloque 507 de datos.

Específicamente, los datos de 12 bytes se pueden extraer del inicio de la cadena 40 de contraseña de 20 bytes, y luego se realiza la operación lógica sobre los datos de 12 bytes y el bloque 507 de datos. Por supuesto, los datos de 12 bytes también se pueden extraer en forma inversa desde el extremo de la cadena 40 de contraseña de 20 bytes, y luego se realiza la operación lógica sobre los datos de 12 bytes y el bloque 507 de datos, y no se hace limitación a esto mediante la presente divulgación.

De acuerdo con lo anterior, después de que ese realiza la operación lógica sobre los datos 50 cifrados al utilizar la cadena 40 de contraseña, se puede obtener los datos 30 fuente. El número de bytes de los datos 30 de fuente es igual que aquel de los datos 50 cifrados (es decir, 132 bytes).

Durante el proceso de cifrado realizado sobre los datos fuente, la cadena de contraseña que consiste del código de tarjeta SIM y el código PIN se utiliza para realizar la operación lógica sobre los datos fuente con el fin de cifrar los datos fuente; y durante el proceso de descifrado realizado en los datos cifrados, se utiliza la cadena de contraseña para realizar la operación lógica correspondiente sobre los datos cifrados. Sólo cuando el usuario ingresa el código PIN correcto, se puede generar la cadena de contraseña para restaurar correctamente los datos fuente, y un usuario no autorizado es incapaz de obtener el código PIN correcto e incluso si el sabe el código PIN correcto, es imposible

obtener el código de la tarjeta SIM correcto de la tarjeta SIM antes que la tarjeta SIM se inserta en el teléfono móvil. Por lo tanto, el método de cifrado de datos y el método de descifrado de datos para el teléfono móvil de la presente divulgación cifra o descifra documentos almacenados en el teléfono móvil al combinar el código de la tarjeta SIM y el código PIN en la cadena de contraseña de tal manera que los datos de los teléfonos móviles no serán robados y se puede proteger la seguridad de los datos.

En el método de descifrado de datos, si la operación lógica utilizada en el método de cifrado de datos es una operación XOR, entonces la operación lógica utilizada en el método de descifrado de datos también debe ser en forma correspondiente la operación XOR. Por supuesto, otras operaciones lógicas tal como la operación AND, la operación OX, la no operación NOT, etcétera, también están cubiertos dentro del alcance de la presente invención, y no se hace limitación específica a esto mediante la presente divulgación. Por ejemplo, si la operación lógica en el método de cifrado de datos es la operación NOT, entonces la operación lógica en el método de descifrado de datos también debe ser la operación NOT correspondientemente. La operación XOR es la preferida para la presente divulgación.

Si se selecciona colocar el código ID de datos cifrados antes de los datos 50 cifrados en el método de cifrado de datos, entonces el código ID de datos cifrados antes de los datos 50 cifrados necesita eliminarse de forma correspondiente de acuerdo con el número IMEI del teléfono móvil en el método de descifrado. Específicamente, puede ser que el número IMEI se obtenga del teléfono móvil, el número 30 de los bytes del código ID de datos cifrados se obtiene de acuerdo con el número IMEI, y luego los datos de 30 bytes se retiran ante que los datos cifrados eliminen el código ID de datos cifrados.

Cabe entender que, el método de cifrado/descifrado descrito en las realizaciones anteriores se puede implementar al programar en el diseño práctico, por ejemplo, se puede implementar al utilizar herramientas de programación tal como C, C++ y Java de acuerdo con los conceptos de la invención descritos anteriormente. Los códigos correspondientes se pueden guardar en la memoria 104 y correr mediante el chip 105 de procesamiento de señal de banda base para alcanzar el cifrado/descifrado de los datos del teléfono móvil. El chip 105 de procesamiento de señal de banda base puede controlar o accesar los dispositivos periféricos tal como la tarjeta 109 SIM, la ranura 110 de tarjetas SD, el teclado 101, la pantalla LCD y el módulo 108 RF de acuerdo con códigos de programa de tal manera que se puede lograr operaciones tal como la interacción entre usuarios, adquisición de datos y guardado los datos.

Adicionalmente con el fin de describir las soluciones técnicas de la presente divulgación, se describirán específicamente en adelante ejemplos de aplicaciones específicas basados en el método de cifrado/descifrado de datos para un teléfono móvil divulgados por la presente divulgación con referencia a la figura 6, a figura 9.

Con referencia a la figura 6, la figura 6 es un diagrama de flujo de un método de detección de código PIN encendido basado en el método de cifrado/descifrado de datos para un teléfono móvil divulgado por la presente divulgación. Como se muestra en la figura 6, el método de detección de código PIN encendido comprende:

Etapa 601: encender el teléfono móvil.

Etapa 602: pedir al usuario ingresar el código PIN, específicamente, con subtítulos en la pantalla 103 LCD.

Etapa 603: detectar si el código PIN es incorrecto. Específicamente, la entrada del código PIN por el usuario se transmite a la tarjeta SIM para detección, y la etapa 604 se ejecuta si se detecta que el código PIN es correcto; y de otra parte, se ejecuta la etapa 605.

Etapa 604: activar una aplicación de cifrado/descifrado de datos del teléfono móvil.

Etapa 605: desactivar la aplicación de cifrado/descifrado de datos del teléfono móvil.

En esta realización, la aplicación de cifrado/descifrado de datos del teléfono móvil mencionado en la etapa 604 y la etapa 605 es una aplicación que corresponde al método de cifrado/descifrado de datos para el teléfono móvil de la presente divulgación. Cuando falla la autenticación del código PIN, se cierra la aplicación de cifrado/descifrado de datos del teléfono móvil. En este caso, el usuario del teléfono móvil será incapaz de cifrar datos o descifrar los datos cifrados.

Con referencia a la figura 7, la figura 7 es un diagrama de flujo de un método remoto de borrado de información basado en el método de cifrado/descifrado de datos para el teléfono móvil divulgado por la presente divulgación. El método remoto de borrado de información comprende:

Etapa 701: recibir un mensaje corto. Esta Etapa se ejecuta principalmente por el módulo 108 RF.

Etapa 702: Juzgar si el contenido del mensaje corto es un comando de borrado. Si el contenido de los mensajes cortos es un comando de borrado, se ejecuta la etapa 704; y de otra forma, se ejecuta la etapa 703. El comando de

borrado se relaciona con el número IMEI local (es decir, el número IMEI del teléfono móvil que recibe el mensaje corto). En un teléfono móvil que transmite el mensaje corto, dos cadenas idénticas de números IMEI locales se combinan en un código de identificación (ID) de comando de borrado (por ejemplo, si el número IMEI local es 123456789012345, entonces el código ID de comando de borrado es 123456789012345123456789012345). El código PIN del teléfono móvil que transmite el mensaje corto se pone detrás de un comando ID pide borrado para formar el comando de borrado. Si el contenido de un mensaje corto es un comando de borrado se puede determinar al extraer los primeros 30 bytes del contenido del mensaje corto y luego determinar si los datos en este segmento de bytes es el código ID del comando de borrado.

Etapa 703: detectar si se activa la aplicación de cifrado/descifrado. Si se activa la aplicación cifrado/descifrado, se ejecuta la etapa 707; y de otra forma, se ejecuta directamente la etapa 708.

Etapa 704: determinar si existe el código de PIN local en el comando de borrado. Específicamente, una cadena de caracteres que consiste de 4 bytes, es decir, los 31 primeros bytes al byte 34, del contenido del mensaje corto se extrae y se detecta si esta cadena de caracteres es igual que el código PIN en este teléfono móvil. Si esta cadena de caracteres es igual que el código PIN almacenado en este teléfono móvil, se ejecuta la etapa 706; y de otra forma, se ejecuta la etapa 705.

Etapa 705: borrar todo el contenido en la tarjeta SD (si la tarjeta SD no se inserta en el teléfono móvil, no se ejecutará esta etapa) y restaurar el sistema del teléfono móvil a la configuración de fábrica de tal manera que todos los datos (por ejemplo, fotografías, videos, grabaciones, contactos, mensajes o similares) en la memoria 104 también se borran.

Etapa 706: ignorar el mensaje corto. Es decir, el mensaje corto ni se ejecuta ni guarda en una bandeja de entrada.

Etapa 707: realizar la operación de cifrado de teléfono móvil de datos sobre el contenido del mensaje corto.

Etapa 708: guardar el contenido del mensaje corto.

De acuerdo con lo anterior, si el usuario pierde su teléfono móvil, el método de borrado de información remota basado en el método de cifrado/descifrado de datos para el teléfono móvil divulgado por la presente divulgación puede enviar un mensaje corto preeditado que comprende el comando de borrado al teléfono móvil que se ha perdido. Como resultado, el teléfono móvil que se ha perdido puede eliminar los datos de la tarjeta SD y ser restaurado a la configuración de fábrica. Por lo tanto, se puede proteger la seguridad de los datos del teléfono móvil del usuario.

Con referencia a la figura 8, la figura 8 es un diagrama de flujo de un método de entrada de datos basado en el método de cifrado/descifrado de datos para el teléfono móvil divulgado por la presente divulgación. El método de entrada de datos se utiliza principalmente para datos ingresado a través de dispositivos periféricos tal como un micrófono o una cámara y comprende las siguientes etapas:

Etapa 801: ingresar datos, en donde los datos ingresados se refieren a los datos ingresados a través de dispositivos periféricos tal como un micrófono (no mostrado en la figura 1) o una cámara 102.

Etapa 802: detectar si la aplicación de cifrado/descifrado de datos del teléfono móvil esta activa. Si los datos de la aplicación de cifrado/descifrado de datos del teléfono móvil está activa, se ejecuta la etapa 803; y de otra parte, se ejecuta la etapa 804.

Etapa 803: cifrar los datos.

Etapa 804: guardar los datos.

El método de entrada de datos puede asegurar efectivamente la seguridad de los datos ingresados a través de los dispositivos periféricos tal como el micrófono o la cámara 102.

Con referencia a la figura 9, la figura 9 es un diagrama de flujos de un método para convertir datos no cifrados en datos cifrados basados en el método de cifrado/descifrado de datos para el teléfono móvil divulgado por la presente divulgación. El método para convertir datos no cifrados en datos cifrados se utiliza principalmente para datos almacenados en la tarjeta SD debido a la siguiente razón: es probable que los datos se copian de un equipo y necesiten ser cifrados, de esta manera este método se proporciona para evitar la fuga de información. El método comprende las siguientes etapas:

Etapa 901: leer datos desde la tarjeta SD.

Etapa 902: cifrar los datos.

Etapa 903: guardar los datos cifrados en la tarjeta SD para reemplazar los datos originales.

A través de la operación de cifrado mencionada anteriormente, incluso si se pierde la tarjeta SD, los datos cifrados en la tarjeta SD no serán leídos fácilmente por terceros. De esta manera, el método para convertir datos no cifrados en datos cifrados puede proteger efectivamente la seguridad de los datos de la tarjeta SD.

Como se puede saber a partir de las anteriores descripciones, el método de cifrado de datos y el método de descifrado de datos para el teléfono móvil divulgado por la presente divulgación cifra o descifra documentos almacenados en el teléfono móvil mediante al combinar el código de la tarjeta SIM y el código PIN en una cadena de contraseña de tal manera que los datos del teléfono móvil no serán robados y se protege la seguridad de los datos.

Lo que se describió anteriormente son sólo realizaciones de la presente divulgación, pero no pretende limitar el alcance de la presente divulgación. Cualesquier estructuras equivalentes o modificaciones de flujo de procesos equivalentes que se hagan de acuerdo con la especificación y los dibujos adjuntos de la presente divulgación, o cualquier aplicación directa o indirecta de la presente divulgación en otros campos técnicos relacionados estarán cubiertos dentro del alcance de la presente divulgación.

REIVINDICACIONES

1. Un método de cifrado de datos para un teléfono móvil, el método de cifrado de datos comprende:

obtener una entrada de código PIN por un usuario y obtener un código de tarjeta SIM de una tarjeta SIM de acuerdo con el código PIN y combinar el código PIN y el código de la tarjeta SIM en una cadena (40) de contraseña; y

utilizar la cadena (40) de contraseña para cifrar datos (30) fuente con el fin de obtener datos (50) cifrados;

caracterizado porque los datos cifrados se borran del teléfono móvil con la tarjeta SIM de acuerdo con un mensaje corto de un comando de borrado recibido por el teléfono móvil, en el que el comando de borrado comprende un código ID de comando de borrado y el código PIN y el código ID de comando de borrado se fija mediante un número IMEI local del teléfono móvil.

2. El método de cifrado de datos para un teléfono móvil de la reivindicación 1, en el que la etapa de utilizar la cadena (40) de contraseña para cifrar datos (30) fuente con el fin de obtener datos (50) cifrados:

leer los datos (30) fuente en unidades (301~307) de un número de bytes de la cadena (40) de contraseña;

realizar una operación lógica en la cadena (40) de contraseña y los datos (30) de fuente que se leen; y

almacenar los datos fuente, que han realizado la operación lógica, como datos (50) cifrados.

3. El método de cifrado de datos para un teléfono móvil de la reivindicación 2, en el que la etapa de realizar una operación lógica en la cadena (40) de contraseña y los datos (30) de fuente que se leen, comprende:

realizar la operación lógica directamente sobre la cadena (40) de contraseña y los datos (30) fuente que se leen cuando el número de bytes de los datos (30) de fuente que se leen es igual a un número de bytes de la cadena (40) de contraseña; y

extraer una parte de la cadena (40) de contraseña, de la cual el número de bytes es igual al número de bytes de los datos (30) fuente que se leen, de la cadena (40) de contraseña, y luego realizar la operación lógica sobre la parte de la cadena (40) de contraseña y los datos (30) fuente que se leen cuando el número de bytes de los datos (30) fuente que se leen es menor que el número de bytes de la cadena (40) de contraseña.

4. El método de cifrado de datos para un teléfono móvil de la reivindicación 1, en el que después de la etapa de utilizar de la cadena (40) de contraseña para cifrar datos de la fuente (30) con el fin de obtener datos (50) cifrados, se fija un código de identificación (ID) de datos cifrados al utilizar el número IMEI del teléfono móvil, y el código ID de datos cifrados se coloca antes de los datos (50) cifrados.

5. El método de cifrado de datos para un teléfono móvil de la reivindicación 1, en el que la operación lógica es una operación XOR.

6. Un método de descifrado de datos para un teléfono móvil, en el que el método descifrado de datos comprende:

obtener una entrada de código PIN por un usuario y obtener un código de tarjeta SIM de una tarjeta SIM de acuerdo con el código PIN, y combinar el código PIN y la tarjeta SIM en una cadena (40) de contraseña; y

utilizar la cadena (40) de contraseña para descifrar los datos (50) cifrados con el fin de obtener datos (30) fuente;

caracterizado porque los datos cifrados se borran del teléfono móvil con la tarjeta SIM de acuerdo con un mensaje corto de un comando de borrado recibido por el teléfono móvil, en el que el comando de borrado comprende un código ID de comando de borrado y el código PIN y el código ID de comando de borrado se fija mediante un número IMEI local del teléfono móvil.

7. El método de descifrado de datos para un teléfono móvil de la reivindicación 6, en el que la etapa de utilizar de la cadena (40) de contraseña para descifrar datos (50) cifrados con el fin de obtener datos (30) de fuente comprende:

Leer los datos (50) cifrados en unidades (501~507) de un número de bytes de la cadena (40) de contraseña;

realizar una operación lógica en la cadena (40) de contraseña y los datos (50) cifrados que se leen; y

almacenar los datos cifrados, que han realizado la operación lógica, como los datos (30) fuente.

8. El método de descifrado de datos para un teléfono móvil de la reivindicación 7, en el que la etapa de realizar una operación lógica en la cadena (40) de contraseña y los datos (50) de cifrados que se leen, comprende:

realizar la operación lógica directamente sobre la cadena (40) de contraseña y los datos (50) cifrados que se leen cuando el número de bytes de los datos (50) cifrados que se leen es igual a un número de bytes de la cadena (40) de contraseña; y

extraer una parte de la cadena (40) de contraseña, de la cual el número de bytes es igual al número de bytes de los datos (50) cifrados que se leen, de la cadena (40) de contraseña, y luego realizar la operación lógica sobre la parte de la cadena (40) de contraseña, y los datos (50) cifrados que se leen cuando el número de bytes de los datos (50) cifrados que se leen es menor que el número de bytes de la cadena (40) de contraseña.

9. El método de descifrado de datos para un teléfono móvil de la reivindicación 6, en el que en la etapa de utilizar de la cadena (40) de contraseña para descifrar datos (50) cifrados con el fin de obtener datos (30) fuente, se elimina una entrada de código de identificación (ID) de datos cifrados antes de los datos (50) cifrados de acuerdo con el número IMEI del teléfono móvil.

10. El método de descifrado de datos para un teléfono móvil de la reivindicación 6, en el que la operación lógica es una operación XOR.

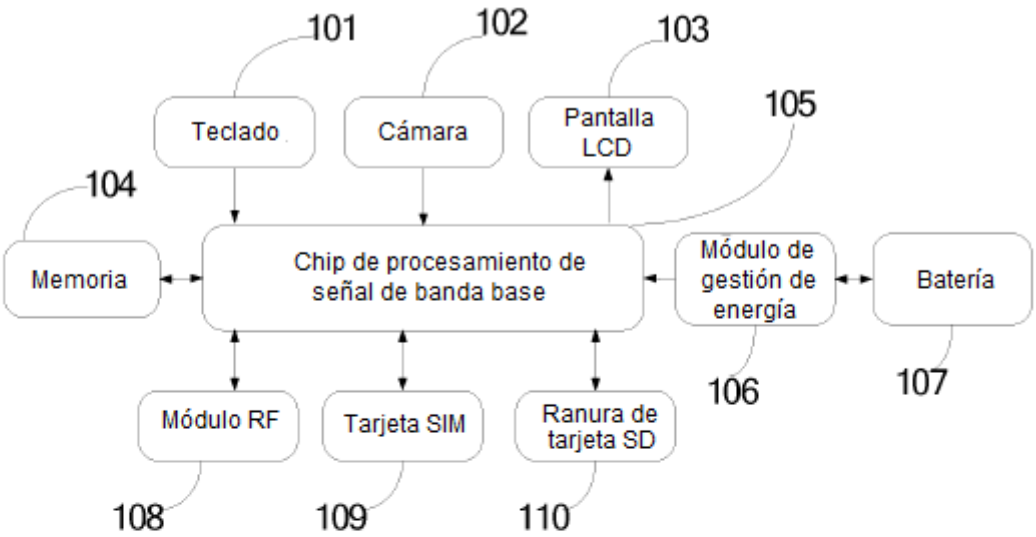
101
102
103
Teclado
Cámara
Pantalla LCD
105
104
Memoria
Chip de procesamiento de señal de banda base
Módulo de gestión de energía
Batería
106
107
Módulo RF
Tarjeta SIM
Ranura de tarjeta SD
108
109
110

FIG. 1

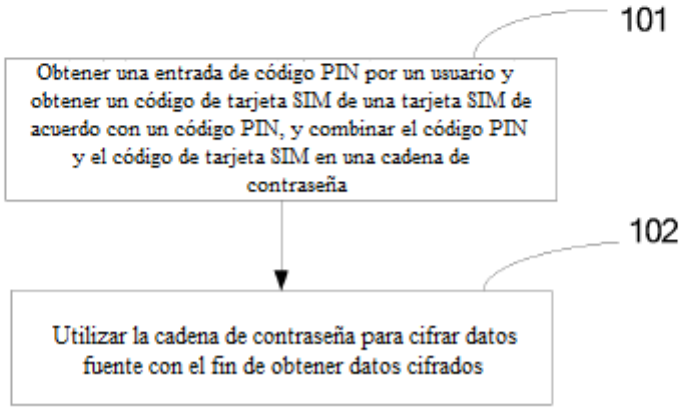
101
Obtener una entrada de código PIN por un usuario y obtener un código de tarjeta SIM de una tarjeta SIM de acuerdo con un código PIN, y combinar el código PIN y el código de tarjeta SIM en una cadena de contraseña
102
Utilizar la cadena de contraseña para cifrar datos fuente con el fin de obtener datos cifrados

FIG. 2

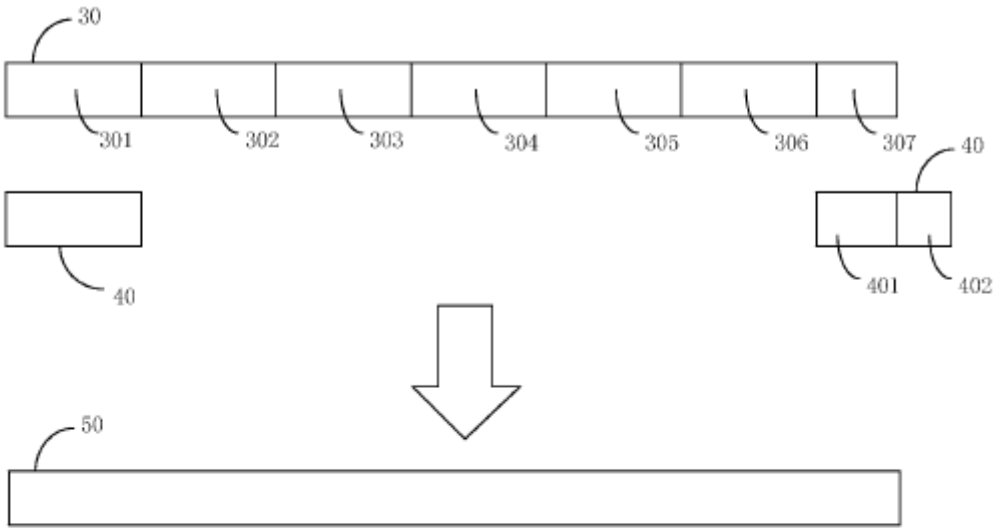
30
301
302
303
304
305
306
307
40
40
401
402
50

FIG. 3

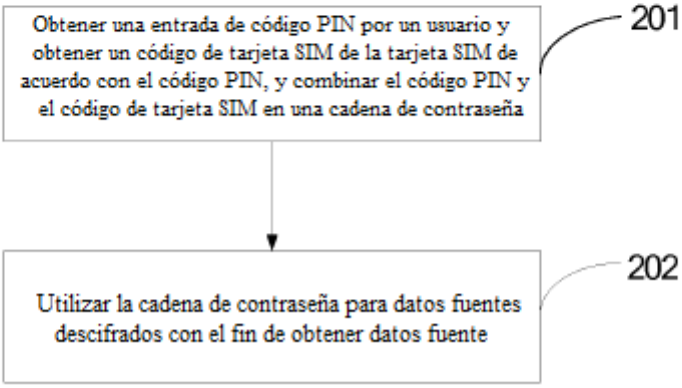
Obtener una entrada de código PIN por un usuario y obtener un código de tarjeta SIM de la tarjeta SIM de acuerdo con el código PIN, y combinar el código PIN y el código de tarjeta SIM en una cadena de contraseña
201
Utilizar la cadena de contraseña para datos fuentes descifrados con el fin de obtener datos fuente
202

FIG. 4

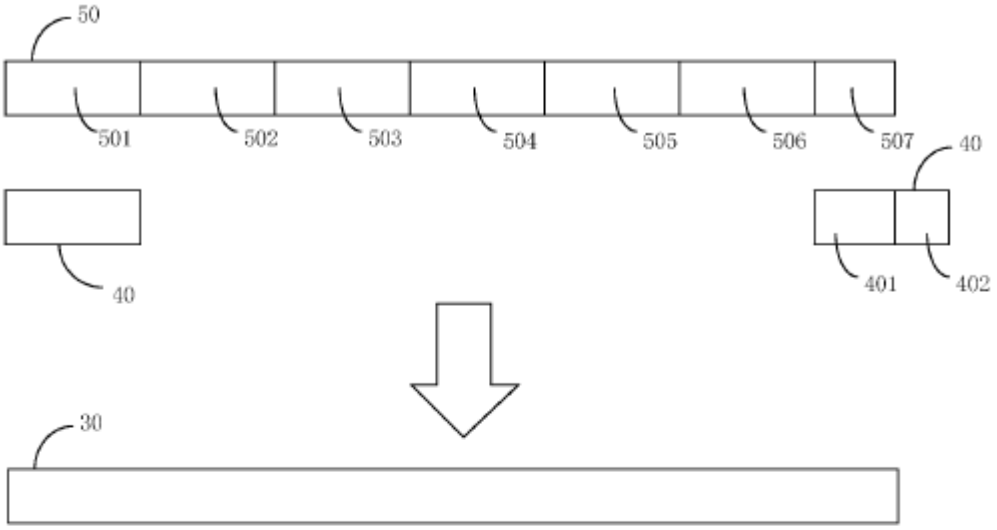
50
501
502
503
504
505
506
507
40
40
401
402
30

FIG. 5

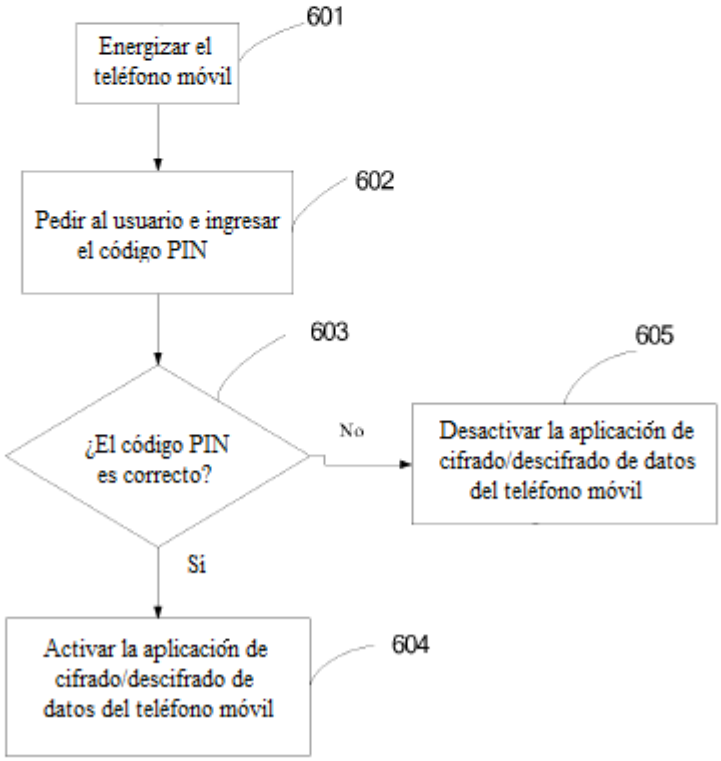
601
Energizar el teléfono móvil
602
Pedir al usuario e ingresar el código PIN
603
¿El código PIN es correcto?
No
605
Desactivar la aplicación de cifrado/descifrado de datos del teléfono móvil
Si
Activar la aplicación de cifrado/descifrado de datos del teléfono móvil
604

FIG. 6

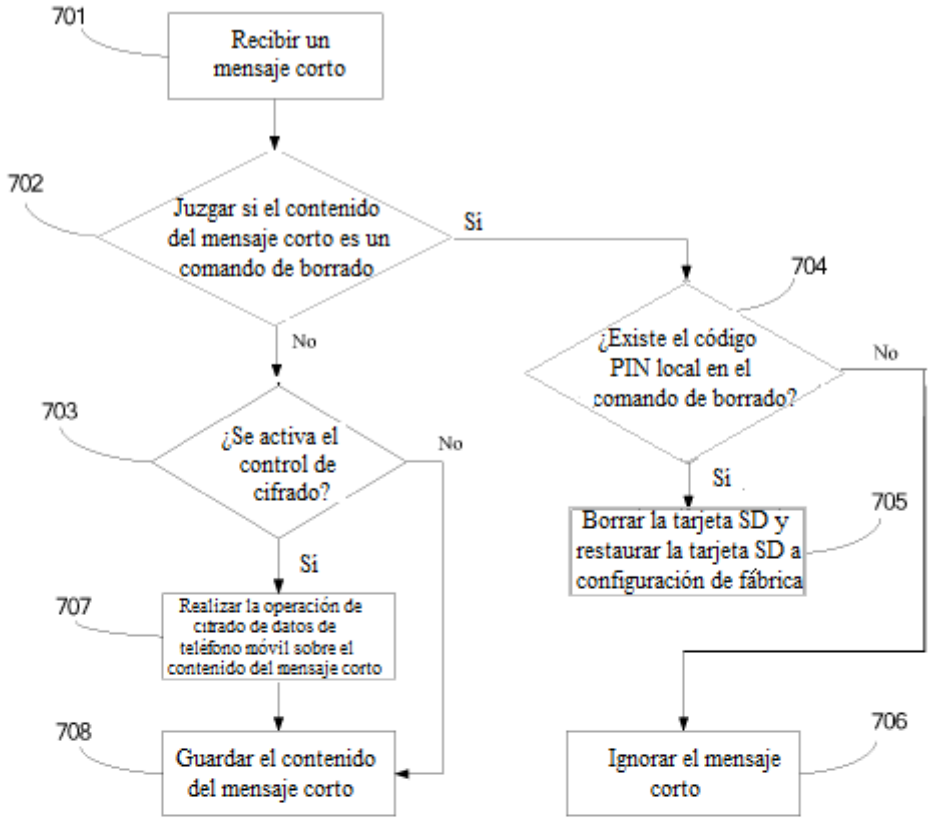
701
Recibir un mensaje corto
702
Juzgar si el contenido del mensaje corto es un comando de borrado
Si
No
704
¿Existe el código PIN local en el comando de borrado?
No
Si
705
Borrar la tarjeta SD y restaurar la tarjeta SD a configuración de fábrica
703
¿Se activa el control de cifrado?
No
Si
707
Realizar la operación de cifrado de datos de teléfono móvil sobre el contenido del mensaje corto
708
Guardar el contenido del mensaje corto
706
Ignorar el mensaje corto

FIG. 7

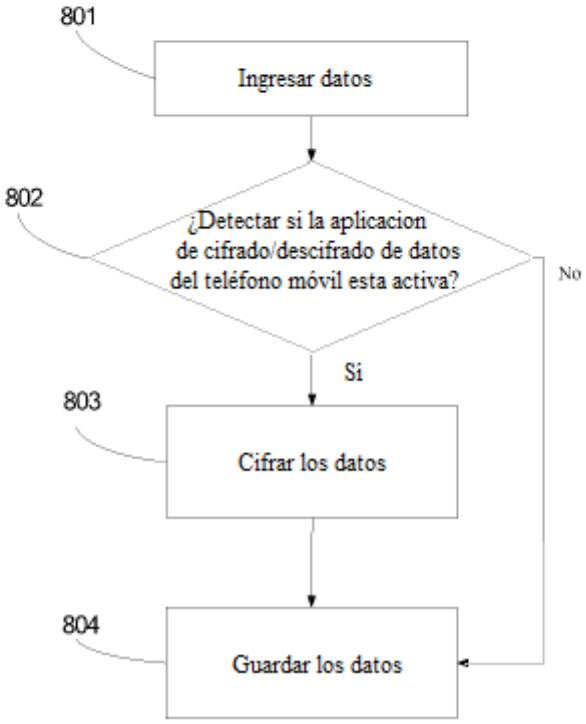
801
Ingresar datos
802
¿Detectar si la aplicacion de cifrado/descifrado de datos del teléfono móvil esta activa?
No
Si
803
Cifrar los datos
804
Guardar los datos

FIG. 8

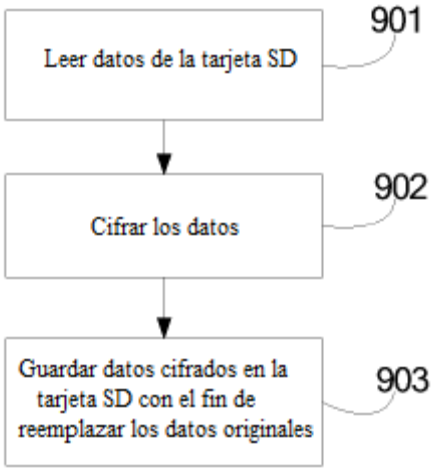
Leer datos de la tarjeta SD
901
Cifrar los datos
902
Guardar datos cifrados en la tarjeta SD con el fin de reemplazar los datos originales
903

FIG. 9