(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 550 377**

(51) Int. CI.:

H04W 12/04 (2009.01)
H04W 12/02 (2009.01)
H04L 9/08 (2006.01)
H04L 9/32 (2006.01)
H04L 29/06 (2006.01)
G06K 19/07 (2006.01)
H04B 5/00 (2006.01)
H04W 12/12 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **28.08.2012 E 12827379 (4)**

(97) Fecha y número de publicación de la concesión europea: **22.07.2015 EP 2725736**

(54) Título: **Métodos y terminales para comunicación segura por radio frecuencia**

(30) Prioridad:

29.08.2011 CN 201110250429

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
06.11.2015

(73) Titular/es:

NATIONZ TECHNOLOGIES INC. (100.0%)
2F-8F, Building A, IER of Huazhong University of Science and Technology No. 9, Yuexing Ave 3 Nanshan District
Shenzhen, Guangdong 518057, CN

(72) Inventor/es:

LI, MEIXIANG

(74) Agente/Representante:

IZQUIERDO BLANCO, María Alicia

Métodos y terminales para comunicación segura por radio frecuencia

Descripción

CAMPO DE LA INVENCIÓN

[0001] Esta invención se relaciona con el campo de las comunicaciones, y más particularmente con un método de comunicación segura por radiofrecuencia (RF), un terminal y sistema de comunicación segura por RF.

ANTECEDENTES

[0002] Con la popularización de los terminales móviles, la demanda de pagos electrónicos efectuados mediante los terminales móviles se ha convertido en un aspecto de gran urgencia. En la actualidad, la tecnología de pagos electrónicos tiene una variedad de aplicaciones. Una de las aplicaciones se realiza mediante la integración de un módulo de comunicación de RF de 2,4 GHz, una bobina de acoplamiento magnético y un módulo de procesamiento por inducción magnética en una tarjeta de modelo de identificación de suscriptor (SIM, por sus siglas en inglés) o tarjeta digital segura (SD, por sus siglas en inglés). En este tipo de aplicación, por medio de la detección de la intensidad de una señal de acoplamiento magnético y la recepción de la información de canal magnético mediante la tarjeta SIM o tarjeta SD instalada en el teléfono móvil, se activa el módulo de comunicación de radiofrecuencia de 2,4 GHz integrado en la tarjeta SIM o la tarjeta SD y se realiza la comunicación de la transacción de datos. Debido a que la energía de la señal de acoplamiento magnético en el espacio disminuye con la distancia en una relación de tercera potencia y tiene una muy adecuada coherencia para diferentes teléfonos móviles, esta aplicación realiza el intercambio de datos al alta velocidad por RF y controla la distancia de la comunicación de datos de RF de la tarjeta SIM o la tarjeta SD en una variedad de terminales móviles, por lo tanto, se convierte en una solución de pago electrónico por terminal móvil fiable. Además, todo el sistema completo de recepción y procesamiento se integra en la tarjeta SIM o la tarjeta SD y no se necesita hacer ninguna modificación al terminal del teléfono móvil, por lo tanto, tiene un excelente valor de promoción de aplicación. Sin embargo, debido a la falta de medidas de protección adecuadas, cuando se realizan transacciones de datos, un atacante puede obtener los parámetros del canal por RF actual mediante un análisis, hasta establecer una conexión con la tarjeta de RF activada, con lo cual aumentan los riesgos para la seguridad.
La EP1024626 A1 revela un método, un aparato y un sistema de comunicación para el intercambio de información en un entorno generalizado en red. De esta manera se puede obtener una sesión segura y autenticada. En consecuencia, se utilizan un primer dispositivo y por lo menos un segundo dispositivo remoto. Se inicia un canal unidireccional de comunicación inalámbrica entre el primer dispositivo y el segundo dispositivo remoto, con esto se envía una secuencia mediante el canal unidireccional de comunicación inalámbrica desde el primer dispositivo hasta el segundo dispositivo remoto para suministrar al segundo dispositivo remoto información de cifrado. Una respuesta cifrada se envía mediante un medio de transmisión inalámbrica al primer dispositivo por medio de uso de dicha información de cifrado para el cifrado;
La US 20030093663 A1 revela una técnica para la transmisión de las instrucciones iniciales a un canal de comunicación seguro entre dispositivos mediante una clave de clave criptográfica. La clave se genera mediante un primer dispositivo y una copia de la clave se envía a un segundo dispositivo por medio de un canal de comunicación inalámbrica de corto alcance a fin de que proporcione a cada dispositivo con una clave compartida. En una realización, el canal de corto alcance comprende un par de transpondedor/lector de transpondedor en el cual el transpondedor se coloca próximo al lector de transpondedor para activar la comunicación entre los dispositivos. Al recibir la clave compartida, se ejecutan algoritmos simétricos de conformidad de clave autenticada, uno para cada dispositivo, para generar de manera cooperativa una clave criptográfica que se utiliza para proporcionar un canal de comunicación seguro con el uso de un protocolo de comunicación cifrada basado en la clave criptográfica.

BREVE RESUMEN DE LA REVELACIÓN

[0003] Los principales problemas técnicos que debe solucionar la presente invención incluyen proporcionar un método de comunicación segura por radiofrecuencia (RF), un terminal y un sistema de comunicación segura por RF, que mejoren la seguridad del proceso de transacción de datos por enlaces de RF.

[0004] La invención se define en las Reivindicaciones independientes 1,4, 7 y 11. Para resolver los problemas técnicos anteriores, la presente invención incluye las siguientes soluciones técnicas:

[0005] Un método para la comunicación segura por radiofrecuencia, que comprende:

[0006] la generación de datos de canal magnético y la transmisión de datos de canal magnético a través de un canal magnético;

[0007] el establecimiento de un enlace de radiofrecuencia con un dispositivo semejante que envía de regreso la información de respuesta de los datos de canal magnético y en donde:
el cálculo de los parámetros del canal de radiofrecuencia, basado en los datos de canal magnético; y en donde la recepción de la información de respuesta de los datos de canal magnético proveniente del dispositivo semejante en

un canal de radiofrecuencia correspondiente, basada en los parámetros del canal de radiofrecuencia.

[0008] la generación de primeros datos de radiofrecuencia, el cifrado de los primeros datos de radiofrecuencia con el uso de los datos del canal magnético y la transmisión de los primeros datos de radiofrecuencia cifrados al dispositivo semejante por medio del enlace de radiofrecuencia; y

[0009] la recepción de segundos datos de radiofrecuencia cifrados transmitidos por el dispositivo semejante por medio del enlace de radiofrecuencia y el descifrado de los segundos datos de radiofrecuencia cifrados mediante el uso de los datos de canal magnético.

[0010] En una realización, los parámetros del canal de radiofrecuencia incluyen un punto de frecuencia de RF y una dirección de radiofrecuencia.

[0011] En una realización, los primeros datos de radiofrecuencia son datos de la aplicación, y los segundos datos de radiofrecuencia son datos de respuesta de los datos de la aplicación.

[0012] En una realización, los datos de canal magnético se generan de manera aleatoria.

[0013] Un método para la comunicación segura por radiofrecuencia, que comprende:
la recepción de datos de canal magnético a través de un canal magnético;
el establecimiento de un enlace de radiofrecuencia con un dispositivo semejante que envía los datos de canal magnético;
y en donde:
basado en los datos de canal magnético recibidos,
el cálculo de los parámetros (S803) del canal de radiofrecuencia; y
el envío de la información de respuesta (S804) de los datos de canal magnético al dispositivo semejante en un canal de radiofrecuencia correspondiente, basada en los parámetros del canal de radiofrecuencia.
la generación de terceros datos de radiofrecuencia, el cifrado de los terceros datos de radiofrecuencia con el uso de los datos del canal magnético y la transmisión de los terceros datos de radiofrecuencia cifrados al dispositivo semejante por medio del enlace de radiofrecuencia; y
la recepción de cuartos datos de radiofrecuencia cifrados transmitidos por el dispositivo semejante por medio del enlace de radiofrecuencia y el descifrado de los cuartos datos de radiofrecuencia cifrados mediante el uso de los datos de canal magnético.

[0014] En una realización, antes del cálculo de los parámetros del canal de radiofrecuencia basado en los datos de canal magnético, el proceso además incluye:

[0015] la detección de la intensidad de la señal magnética de los datos de canal magnético;
la determinación de si la intensidad de señal magnética detectada es mayor que un valor predeterminado; y si la intensidad de señal magnética detectada es mayor que el valor predeterminado, basado en los datos de canal magnético recibidos, el cálculo de los parámetros del canal de radiofrecuencia.

[0016] En una realización, los parámetros del canal de radiofrecuencia incluyen un punto de frecuencia de RF y una dirección de radiofrecuencia.

[0017] En una realización, los cuartos datos de radiofrecuencia son datos de la aplicación, y los terceros datos de radiofrecuencia son datos de respuesta de los datos de la aplicación.

[0018] Un terminal, que comprende:
un módulo generador de señales magnéticas configurado para generar los datos de canal magnético y transmitir los datos de canal magnético por medio de un canal magnético;
un módulo transceptor de radiofrecuencia configurado para establecer un enlace de radiofrecuencia con un dispositivo semejante, el cual envía de regreso la información de respuesta de los datos de canal magnético, transmitir los primeros datos de radiofrecuencia cifrados al dispositivo semejante por medio del enlace de radiofrecuencia y recibir los segundos datos de radiofrecuencia cifrados, transmitidos por el dispositivo semejante mediante el enlace de radiofrecuencia;
y un módulo de control configurado para generar los primeros datos de radiofrecuencia, cifrar los primeros datos de radiofrecuencia con el uso de los datos de canal magnético, transmitir los primeros datos de radiofrecuencia cifrados al módulo transceptor de radiofrecuencia y descifrar los segundos datos de radiofrecuencia cifrados mediante el uso de los datos de canal magnético y en donde el módulo de control incluye: un submódulo de transformación (131) configurado para calcular los parámetros del canal de radiofrecuencia, basado en los datos de canal magnético.

[0019] En una realización, el módulo generador de señales magnéticas incluye un submódulo generador de datos de canal magnético y un submódulo generador de señales magnéticas. El submódulo generador de datos de canal magnético se configura para generar los datos de canal magnético. El submódulo generador de señales magnéticas se configura para transmitir los datos de canal magnético a través del canal magnético.

[0020] En una realización, el módulo transceptor de radiofrecuencia se configura para recibir la información de respuesta de los datos de canal magnético proveniente del dispositivo semejante en un canal de radiofrecuencia correspondiente, basado en los parámetros del canal de radiofrecuencia.

[0021] En una realización, el módulo de control incluye un módulo de aplicación y un módulo de cifrado y descifrado. El módulo de aplicación se configura para generar los primeros datos de radiofrecuencia, transmitir los primeros datos de radiofrecuencia al módulo de cifrado y descifrado, y realizar un proceso aplicado correspondiente a los segundos datos de radiofrecuencia descifrados por el módulo de cifrado y descifrado. El módulo de cifrado y descifrado se configura para cifrar los primeros datos de radiofrecuencia con el uso de los datos de canal magnético, transmitir los primeros datos de radiofrecuencia cifrados al módulo transceptor de radiofrecuencia, descifrar los segundos datos de radiofrecuencia cifrados, transmitidos por el dispositivo semejante con el uso de los datos de canal magnético, y transmitir los segundos datos de radiofrecuencia descifrados al módulo de aplicación.

[0022] Un terminal, que comprende:
un módulo de inducción magnética configurado para recibir los datos de canal magnético enviados desde afuera por medio de un canal magnético;
un módulo transceptor de radiofrecuencia configurado para establecer un enlace de radiofrecuencia con un dispositivo semejante, el cual transmite los datos de canal magnético, transmitir los terceros datos de radiofrecuencia cifrados al dispositivo semejante por medio del enlace de radiofrecuencia y recibir los cuartos datos de radiofrecuencia cifrados, transmitidos por el dispositivo semejante mediante el enlace de radiofrecuencia;
y un módulo de control configurado para generar los terceros datos de radiofrecuencia, cifrar los terceros datos de radiofrecuencia con el uso de los datos de canal magnético, transmitir los terceros datos de radiofrecuencia cifrados al módulo transceptor de radiofrecuencia y descifrar los cuartos datos de radiofrecuencia cifrados mediante el uso de los datos de canal magnético y en donde el módulo de control incluye: un submódulo de transformación configurado para calcular los parámetros del canal de radiofrecuencia, basado en los datos de canal magnético recibidos por el módulo de inducción magnética.

[0023] En una realización, el módulo transceptor de radiofrecuencia se configura para enviar la información de respuesta de los datos de canal magnético al dispositivo semejante en un canal de radiofrecuencia correspondiente, basado en los parámetros del canal de radiofrecuencia.

[0024] En una realización, el módulo de control también incluye un submódulo de detección y un submódulo de determinación. El submódulo de detección se configura para detectar la intensidad de señal magnética de los datos de canal magnético recibidos por el módulo de inducción magnética. El submódulo de determinación se configura para determinar si la intensidad de señal magnética detectada es mayor que un valor predeterminado. El submódulo de transformación se configura para calcular los parámetros del canal de radiofrecuencia, basado en los datos de canal magnético recibidos por el módulo de inducción magnética, cuando el submódulo de determinación determina que la intensidad de señal magnética es mayor que el valor predeterminado.

[0025] En una realización, el módulo de control incluye un módulo de aplicación y un módulo de cifrado y descifrado, donde:
el módulo de aplicación se configura para generar los terceros datos de radiofrecuencia, transmitir los terceros datos de radiofrecuencia al módulo de cifrado y descifrado, y realizar un proceso aplicado correspondiente a los cuartos datos de radiofrecuencia descifrados por el módulo de cifrado y descifrado; y
el módulo de cifrado y descifrado, después del cifrado de los terceros datos de radiofrecuencia con el uso de los datos de canal magnético, se configura para transmitir los terceros datos de radiofrecuencia cifrados al módulo transceptor de radiofrecuencia y descifrar los cuartos datos de radiofrecuencia cifrados, transmitidos por el dispositivo semejante con el uso de los datos de canal magnético, y transmitir los datos descifrados al módulo de aplicación.

[0026] Un sistema de comunicación segura por RF comprende un primer terminal de acuerdo con cualquiera de las opciones anteriores y al menos un segundo terminal de acuerdo con cualquiera de las opciones anteriores. El primer terminal y el segundo terminal transmiten los datos de canal magnético por medio de un canal magnético, y descifran y cifran los datos de radiofrecuencia transmitidos en el enlace de radiofrecuencia entre el primer terminal y el segundo terminal mediante el uso de los datos de canal magnético.

[0027] En una realización, el primer terminal es un lector de tarjetas y el segundo terminal es un terminal con una tarjeta de radiofrecuencia incorporada.

[0028] En una realización, la tarjeta de RF es una tarjeta SIM de radiofrecuencia o una tarjeta SD de radiofrecuencia.

[0029] Efectos ventajosos de la presente invención: los datos de RF transmitidos en el enlace de RF se cifran con el uso de los datos de canal magnético transmitidos por el canal magnético. Es decir, los datos transmitidos en el enlace de RF se cifran con el uso de la información de control de seguridad transmitida por el canal magnético. Debido a que la distancia de transmisión del canal magnético es corta y este no es fácil de interceptarse, incluso si

un atacante falsifica un dispositivo semejante mediante una especificación de protocolo público, y establece una conexión con el segundo terminal activado desde una distancia, puesto que los datos de canal magnético como una clave de seguridad para el cifrado de datos no pueden ser robados, el proceso de cifrado o descifrado de los datos de RF no puede completarse, evitando el riesgo de que la clave predeterminada sea interceptada o descifrada. Por lo tanto, no puede implementarse un ataque sustancial a la transacción, mejorando la seguridad del proceso de intercambio de los datos a través del enlace de radiofrecuencia. Al mismo tiempo, los datos de RF transmitidos por el enlace de RF se cifran directamente mediante el uso de los datos de canal magnético y no requieren un sistema de gestión de distribución de claves específico, con lo cual se reducen la dificultad y los costos del mantenimiento de la seguridad.

[0030] Además, los dispositivos en ambos extremos calculan los parámetros del canal de radiofrecuencia, basados en los datos de canal magnético, y establecen un enlace de radiofrecuencia correspondiente, simplificando aún más el proceso de establecimiento del enlace de RF.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

[0031] La figura 1 ilustra un diagrama de esquema estructural de un ejemplo de un primer terminal coherente con las realizaciones reveladas;
La figura 2 ilustra un diagrama de esquema estructural de otro ejemplo de un primer terminal coherente con las realizaciones reveladas;
La figura 3 ilustra un diagrama de esquema estructural de un ejemplo de un lector de tarjetas por radiofrecuencia (RF) coherente con las realizaciones reveladas;
La figura 4 ilustra un diagrama de esquema estructural de un ejemplo de un segundo terminal coherente con las realizaciones reveladas;
La figura 5 ilustra un diagrama de esquema estructural de otro ejemplo de un segundo terminal coherente con las realizaciones reveladas;
La figura 6 ilustra un diagrama de esquema estructural de un ejemplo de una tarjeta SIM de RF coherente con las realizaciones reveladas;
La figura 7 ilustra un diagrama esquemático de un ejemplo de sistema de comunicación segura por RF coherente con las realizaciones reveladas; y
La figura 8 ilustra un diagrama de flujo de un ejemplo de un método para la comunicación segura por radiofrecuencia de un sistema de comunicación por RF mostrado en la figura 7 coherente con las realizaciones reveladas.

DESCRIPCIÓN DETALLADA

[0032] La presente invención además se ilustra a través de algunas realizaciones específicas en combinación con los dibujos que se proporcionan más adelante.

[0033] La idea principal de la invención es que, entre un primer terminal y un segundo terminal, al comienzo, los datos de canal magnético se transmitan por medio de un canal magnético; después, los datos de radiofrecuencia (RF) transmitidos en un enlace de radiofrecuencia entre el primer terminal y el segundo terminal se cifran y descifran mediante el uso de los datos de canal magnético, mejorando la seguridad del proceso de intercambio de datos en el enlace de radiofrecuencia. El primer terminal incluye un dispositivo lector de tarjetas, como un lector de tarjetas, aunque no se limita a este. El segundo terminal incluye un terminal de tarjetas de RF incorporado, como un terminal móvil, aunque no se limita a este. La tarjeta de RF puede incluir una tarjeta de módulo de identificación de suscriptor (SIM) de RF y una tarjeta digital segura (SD) de RF, aunque no se limita a estas. Los datos de radiofrecuencia transmitidos en el enlace de radiofrecuencia incluyen datos de aplicación y datos de respuesta de los datos de aplicación, aunque no se limitan a estos.

[0034] En referencia a la figura 1, esta figura 1 es un diagrama de esquema estructural de un primer terminal proporcionado por una realización de la presente invención. El primer terminal incluye un módulo generador de señales magnéticas 11, un módulo transceptor de RF 12 y un módulo de control 13. El módulo generador de señales magnéticas 11 se configura para generar datos de canal magnético y transmitir los datos de canal magnético por medio de un canal magnético. El módulo transceptor de RF 12 se configura para establecer un enlace de radiofrecuencia con un segundo terminal que envía de regreso una información de respuesta de los datos de canal magnético, para transmitir los primeros datos de radiofrecuencia cifrados al dispositivo semejante a través de un enlace de radiofrecuencia o para recibir los segundos datos de radiofrecuencia cifrados, transmitidos por el dispositivo semejante mediante el enlace de radiofrecuencia. El módulo de control 13, después de que los primeros datos de radiofrecuencia se cifran usando los datos de canal magnético, se configura para generar los primeros datos de radiofrecuencia para transmitir los primeros datos de radiofrecuencia cifrados al módulo transceptor de RF y descifrar los segundos datos de radiofrecuencia cifrados usando los datos de canal magnético.

[0035] Específicamente, los primeros datos de radiofrecuencia pueden ser datos de aplicación enviados desde el primer terminal al segundo terminal; y los segundos datos de radiofrecuencia pueden ser datos de respuesta de los datos de aplicación enviados de regreso desde el segundo terminal al primer terminal.

[0036] En referencia a la figura 2, esta figura 2 es un diagrama de esquema estructural de un primer terminal proporcionado por otra realización de la presente invención. El primer terminal incluye un módulo generador de señales magnéticas 11, un módulo transceptor de RF 12 y un módulo de control 13. El módulo generador de señales magnéticas 11 incluye un submódulo generador de datos de canal magnético 111 y un submódulo generador de señales magnéticas 112. El módulo de control 13 incluye un submódulo de transformación 131, un módulo de aplicación 132 y un módulo de cifrado y descifrado 133. El submódulo de transformación 131 se conecta con el submódulo generador de datos de canal magnético 111 y el módulo transceptor de RF 12, respectivamente. El módulo de cifrado y descifrado 133 se conecta con el módulo de aplicación 132, el submódulo generador de datos de canal magnético 111 y el módulo de transceptor de RF 12, respectivamente. El submódulo generador de datos de canal magnético 111 también se conecta con el submódulo generador de señales magnéticas 112.

[0037] El submódulo generador de datos de canal magnético 111 se configura para generar los datos de canal magnético de manera aleatoria. El submódulo generador de señales magnéticas 112 se configura para transmitir los datos de canal magnético a través de un canal magnético. El submódulo de transformación 131 se configuró para calcular los parámetros del canal de radiofrecuencia, basado en los datos de canal magnético generados por el submódulo generador de datos de canal magnético 111. El módulo transceptor de RF 12 se configura para recibir la información de respuesta de los datos de canal magnético enviados de regreso del segundo terminal en un canal de radiofrecuencia correspondiente, basada en los parámetros del canal de radiofrecuencia obtenidos por el submódulo de transformación 131, y establecer un enlace de radiofrecuencia con el segundo terminal. El módulo de aplicación 132 se configura para generar los primeros datos de radiofrecuencia y transmitir los primeros datos de radiofrecuencia al módulo de cifrado y descifrado 133. El módulo de cifrado y descifrado 133, después del cifrado de los primeros datos de radiofrecuencia con el uso de los datos de canal magnético generado por el submódulo generador de datos de canal magnético 111, se configura para transmitir los primeros datos de radiofrecuencia cifrados al módulo transceptor de RF 12. El módulo transceptor de RF 12 se configura para transmitir los primeros datos de radiofrecuencia cifrados al segundo terminal mediante el enlace de radiofrecuencia. El módulo transceptor de RF 12 también se configura para recibir los segundos datos de radiofrecuencia cifrados transmitidos por el segundo terminal por el enlace de radiofrecuencia y transmitir los segundos datos de radiofrecuencia cifrados al módulo de cifrado y descifrado 133. El módulo de cifrado y descifrado 133 también se configura para descifrar los segundos datos de radiofrecuencia cifrados transmitidos por el segundo terminal usando los datos de canal magnético generados por el submódulo generador de datos de canal magnético 111 y transmitir los datos descifrados al módulo de aplicación 132. El módulo de aplicación 132 también se configura para realizar un procesamiento aplicado correspondiente a los segundos datos de radiofrecuencia descifrados por el módulo de cifrado y descifrado 133.

[0038] En la presente realización, el método para el cálculo de los parámetros del canal de radiofrecuencia por el submódulo de transformación 131, basado en los datos de canal magnético generados por el submódulo generador de datos de canal magnético 111, puede incluir la realización de una transformación irreversible a los datos de canal magnético generados por el submódulo generador de datos de canal magnético 111 y la generación de los parámetros correspondientes del canal de radiofrecuencia, basado en el resultado de la transformación. En función de los parámetros del canal de radiofrecuencia, el módulo transceptor de RF 12 recibe y transmite la información de RF por el canal de radiofrecuencia correspondiente. En la presente realización, el módulo de cifrado y descifrado 133 también puede integrarse en el módulo generador de señales magnéticas 11. Es decir, el módulo generador de señales magnéticas 11 cifra y descifra los datos de radiofrecuencia. En la presente realización, los parámetros del canal de radiofrecuencia incluyen un punto de frecuencia de RF y una dirección. En función del punto de frecuencia de RF y la dirección, se obtiene el canal de radiofrecuencia correspondiente. Los primeros datos de radiofrecuencia pueden ser datos de aplicación a enviarse desde el primer terminal al segundo terminal; los segundos datos de radiofrecuencia pueden ser datos de respuesta de los datos de aplicación enviados de regreso desde el segundo terminal al primer terminal.

[0039] En la presente realización, el primer terminal genera los datos de canal magnético de manera aleatoria por medio del módulo generador de señales magnéticas. En función de los datos de canal magnético, el submódulo de transformación calcula los parámetros del canal de radiofrecuencia. En función de los parámetros del canal de radiofrecuencia, el módulo transceptor de RF establece un enlace de radiofrecuencia con el segundo terminal. El módulo de cifrado y descifrado continúa cifrando los primeros datos de radiofrecuencia a transmitirse al segundo terminal con el uso de los datos de canal magnético. El módulo transceptor de RF transmite los primeros datos de radiofrecuencia cifrados por medio del módulo de cifrado y descifrado al segundo terminal mediante el enlace de radiofrecuencia. Debido a que los datos de canal magnético generados son aleatorios y es lo único válido en la transacción actual, puede evitarse el riesgo de que los datos de canal magnético sean interceptados o dañados. Al mismo tiempo, los datos de canal magnético son objeto de una transformación irreversible. En función del resultado irreversible, se generan los parámetros del canal de radiofrecuencia. Por lo tanto, incluso si un atacante obtiene los parámetros del canal de radiofrecuencia actual mediante un análisis, el atacante no puede obtener los datos de canal magnético generados actualmente, mejorando la seguridad de los datos de canal magnético como una clave secreta para el cifrado de datos. Es decir, con el uso del primer terminal de la realización, incluso si el atacante falsifica una estación base de comunicación magnética de RF usando una especificación de protocolo público y establece una conexión con el segundo terminal activado por el primer terminal desde una ubicación distante, debido a que no pueden obtenerse los datos de canal magnético que se generan cuando el primer terminal activa el

segundo terminal, no puede completarse el proceso para el cifrado o descifrado de los datos de RF. En consecuencia, no puede implementarse un ataque sustancial a la transacción, además mejora la seguridad del proceso de intercambio de los datos a través del enlace de radiofrecuencia. Además, esta implementación no requiere de un sistema exclusivo de gestión de distribución de claves, con lo cual se reducen la dificultad y los costos de mantenimiento de la seguridad.

[0040] En referencia a la figura 3, esta figura 3 es un diagrama de esquema estructural de un lector de tarjetas por RF proporcionado por una realización de la presente invención. El lector de tarjetas por RF incluye al menos un microcontrolador 301, al menos un módulo transceptor de RF 302 con una antena de RF, y al menos un módulo generador de señales magnéticas 303. La antena de RF se configura para detectar y emitir una señal de RF. El módulo transceptor de RF 302 y al menos un microcontrolador 301 se configuran para transmitir y recibir los datos de RF entre un lector de tarjetas por RF y una tarjeta de RF. El módulo generador de señales magnéticas 303 se conecta con el microcontrolador 301. El módulo generador de señales magnéticas 303 se configura para generar datos de canal magnético de manera aleatoria y transmitir los datos de canal magnético por medio de un canal magnético. El microcontrolador 301 basado en los datos de canal magnético generados por el módulo generador de señales magnéticas 303, se configura para calcular los parámetros del canal de radiofrecuencia, para generar los primeros datos de radiofrecuencia, después de que los primeros datos de radiofrecuencia se cifran usando los datos de canal magnético generados por el módulo generador de señales magnéticas 303, para transmitir los primeros datos de radiofrecuencia cifrados al módulo transceptor de RF 302. El módulo transceptor de RF 302, basado en los parámetros del canal de radiofrecuencia obtenidos por el microcontrolador 301, se configura para recibir la información de respuesta de los datos de canal magnético enviados de regreso por la tarjeta de RF por un canal de radiofrecuencia correspondiente para establecer un enlace de radiofrecuencia con la tarjeta de RF y transmitir los primeros datos de radiofrecuencia cifrados a la tarjeta de RF por el enlace de radiofrecuencia. El módulo transceptor de RF 302 también se configura para recibir los segundos datos de radiofrecuencia cifrados transmitidos por la tarjeta de RF por medio del enlace de radiofrecuencia y transmitir los segundos datos de radiofrecuencia cifrados al microcontrolador 301. El microcontrolador 301 también se configura para descifrar los segundos datos de radiofrecuencia cifrados usando los datos de canal magnético generados por el módulo generador de señales magnéticas 303 y realizar un proceso aplicado correspondiente a los datos descifrados.

[0041] Específicamente, los primeros datos de radiofrecuencia pueden ser datos de aplicación a enviarse desde el lector de tarjetas por radiofrecuencia a la tarjeta de radiofrecuencia; y los segundos datos de radiofrecuencia pueden ser datos de respuesta de los datos de aplicación enviados de regreso desde la tarjeta de radiofrecuencia al lector de tarjetas por radiofrecuencia.

[0042] En referencia a la figura 4, esta figura 4 es un diagrama de esquema estructural de un segundo terminal proporcionado por una realización de la presente invención. El segundo terminal incluye un módulo de inducción magnética 41, un módulo transceptor de RF 42 y un módulo de control 43. El módulo de inducción magnética 41 se configura para recibir los datos de canal magnético transmitidos por medio de un canal magnético. El módulo transceptor de RF 42 se configura para establecer un enlace de radiofrecuencia con un dispositivo semejante, el cual transmite los datos de canal magnético, para transmitir los terceros datos de radiofrecuencia cifrados al dispositivo semejante a través de un enlace de radiofrecuencia y para recibir los cuartos datos de radiofrecuencia cifrados, transmitidos por el dispositivo semejante mediante el enlace de radiofrecuencia. El módulo de control 43 se configura para generar los terceros datos de radiofrecuencia, para cifrar los terceros datos de radiofrecuencia usando los datos de canal magnético, para transmitir los terceros datos de radiofrecuencia cifrados al módulo transceptor de RF y descifrar los cuartos datos de radiofrecuencia cifrados usando los datos de canal magnético.

[0043] Específicamente, los cuartos datos de radiofrecuencia pueden ser datos de aplicación enviados desde al primer terminal al segundo terminal; y los terceros datos de radiofrecuencia pueden ser datos de respuesta de los datos de aplicación enviados de regreso desde el segundo terminal al primer terminal.

[0044] En referencia a la figura 5, esta figura 5 es un diagrama de esquema estructural de un segundo terminal proporcionado por otra realización de la presente invención. El segundo terminal incluye un módulo de inducción magnética 41, un módulo transceptor de RF 42 y un módulo de control 43. El módulo de control 43 incluye un submódulo de transformación 431, un submódulo de detección 432, un submódulo de determinación 433, un módulo de aplicación 434, y un módulo de cifrado y descifrado 435. El módulo de inducción magnética 41 se configura para recibir los datos de canal magnético enviados desde un dispositivo externo por medio de un canal magnético. El submódulo de detección 432 se configura para detectar la intensidad de señal magnética de los datos de canal magnético recibidos por el módulo de inducción magnética 41. El submódulo de determinación 433 se configura para determinar si la intensidad de señal magnética es mayor que un valor predeterminado. Cuando el submódulo de determinación 433 determina que la intensidad de señal magnética es mayor que el valor predeterminado, el submódulo de transformación 431 se configura para calcular los parámetros del canal de radiofrecuencia, basado en los datos de canal magnético recibidos por el módulo de inducción magnética 41. El módulo transceptor de RF 42 se configura para enviar la información de respuesta de los datos de canal magnético por un canal de radiofrecuencia correspondiente al primer terminal para establecer un enlace de radiofrecuencia con el primer terminal, basado en los parámetros del canal de radiofrecuencia. El módulo de aplicación 434 se configura para generar los terceros datos de radiofrecuencia y para transmitir los terceros datos de radiofrecuencia al módulo de cifrado y descifrado

435. El módulo de cifrado y descifrado 435 se configura para cifrar los terceros datos de radiofrecuencia con el uso de los datos de canal magnético recibidos por el módulo de inducción magnética 41, y para transmitir los terceros datos de radiofrecuencia cifrados al módulo transceptor de RF 42. El módulo transceptor de RF 42 se configura, después de que se transmiten los terceros datos de radiofrecuencia cifrados por el primer terminal, para cifrar los cuartos datos de radiofrecuencia y transmitir los datos de radiofrecuencia cifrados al módulo de cifrado y descifrado 435. El módulo de cifrado y descifrado 435 se configura para descifrar los cuartos datos de radiofrecuencia cifrados con el uso de los datos de canal magnético recibidos por el módulo de inducción magnética 41 y transmitir los cuartos datos de radiofrecuencia descifrados al módulo de aplicación 434. El módulo de aplicación 434 se configura para realizar un proceso aplicado correspondiente para los cuartos datos de radiofrecuencia descifrados por el módulo de cifrado y descifrado 435.

[0045] En la realización, el método de cálculo de los parámetros del canal de radiofrecuencia por el submódulo de transformación 431, basado en los datos de canal magnético recibidos por el módulo de inducción magnética 41, puede incluir la realización de una transformación irreversible a los datos de canal magnético recibidos por el módulo de inducción magnética 41 y la generación de los parámetros correspondientes del canal de radiofrecuencia, basado en el resultado de la transformación. En función de los parámetros del canal de radiofrecuencia, el módulo transceptor de RF 42 recibe y transmite la información de RF por el canal de radiofrecuencia correspondiente. En la realización, los parámetros del canal de radiofrecuencia incluyen un punto de frecuencia de RF y una dirección. En función del punto de frecuencia de RF y la dirección, puede obtenerse el canal de radiofrecuencia correspondiente. Los cuartos datos de radiofrecuencia pueden ser datos de aplicación enviados desde al primer terminal al segundo terminal; y los terceros datos de radiofrecuencia pueden ser datos de respuesta de los datos de aplicación enviados de regreso desde el segundo terminal al primer terminal. En la presente realización, el módulo de cifrado y descifrado 435 también puede integrarse en el módulo de inducción magnética 41 o en el módulo de aplicación 434. Es decir, el módulo de inducción magnética 41 o el módulo de aplicación 434 cifran y descifran los datos de radiofrecuencia.

[0046] En la realización, un segundo terminal recibe los datos de canal magnético generados de manera aleatoria enviados desde el primer terminal por medio de un módulo de inducción magnética. Un submódulo de transformación realiza una transformación irreversible a los datos de canal magnético generados y genera los parámetros del canal de radiofrecuencia basado en el resultado de la transformación. Un submódulo de transformación envía de regreso la información de respuesta de los datos de canal magnético al primer terminal, por tanto, se establece un enlace de radiofrecuencia. El módulo transceptor de RF recibe los datos de radiofrecuencia cifrados enviados desde el primer terminal en el enlace de radiofrecuencia, evitando el riesgo de que la clave predeterminada de seguridad sea interceptada o descifrada. Incluso si un atacante obtiene los parámetros del canal de radiofrecuencia actual mediante análisis, el atacante no puede obtener la información de los datos originales del canal magnético, mejorando la seguridad de los datos de canal magnético como una clave secreta para el cifrado de datos. Es decir, con el uso del primer terminal de la realización, incluso si el atacante falsifica una estación base de comunicación magnética de RF usando una especificación de protocolo público y establece una conexión con el segundo terminal activado por el primer terminal desde una ubicación distante, debido a que no pueden obtenerse los datos de canal magnético generados cuando el primer terminal activa el segundo terminal, no puede completarse el proceso de cifrado o descifrado de los datos de RF. No puede implementarse un ataque sustancial a la transacción, además mejora la seguridad del proceso de intercambio de los datos a través del enlace de radiofrecuencia. Al mismo tiempo, esta implementación no requiere de un sistema exclusivo de gestión de distribución de claves, con lo cual se reducen la dificultad y los costos de mantenimiento de la seguridad.

[0047] En la realización, el segundo terminal puede ser un terminal con una tarjeta SIM de RF o tarjeta SD. Por supuesto, se comprende que otros dispositivos de RF también pueden utilizarse, basándose en los principios y funciones de la realización.

[0048] En referencia a la figura 6, esta figura 6 es un diagrama de esquema estructural de una tarjeta SIM de RF proporcionada por una realización de la presente invención. La tarjeta SIM incluye al menos un módulo transceptor de RF 601, un microcontrolador 602, un módulo de inducción magnética 603, y un módulo de aplicación de tarjeta SIM 604. El módulo transceptor de RF 601 incluye una antena de RF. La antena de RF se configura para detectar y emitir una señal de RF. El módulo de inducción magnética 603 se configura para inducir una intensidad de señal magnética de los datos de canal magnético enviados desde un dispositivo lector de tarjetas por RF y recibir los datos de canal magnético. El módulo transceptor de RF 601 conectado al microcontrolador 602 se configura para transmitir o recibir las señales de RF por medio de la antena de RF. El microcontrolador 602 se configura para procesar la información de RF recibida y transmitida, y la información del canal magnético. El proceso incluye la detección de la intensidad de señal magnética de los datos de canal magnético generados por el lector de tarjetas y recibidos por el módulo de inducción magnética 603, y determina si la intensidad de señal magnética detectada es mayor que un valor predeterminado. Cuando el resultado de una evaluación es que la intensidad de señal magnética detectada es mayor que el valor predeterminado, basado en los datos de canal magnético, se calculan los parámetros del canal de radiofrecuencia. Específicamente, los datos de canal magnético pueden realizar una transformación irreversible para obtener una dirección y punto de frecuencia correspondientes. En función del punto de frecuencia de RF y la dirección, se envía de regreso una información de respuesta de los datos de canal magnético al dispositivo lector de tarjetas por medio del módulo transceptor de RF 601 para establecer un enlace de RF con el dispositivo lector de

tarjetas. El módulo de aplicación de la tarjeta SIM 604 se configura para realizar una aplicación de tarjeta SIM correspondiente, que incluye la generación de los terceros datos de radiofrecuencia. El microcontrolador 602 se configura para cifrar los terceros datos de radiofrecuencia con el uso de los datos de canal magnético y transmitir los terceros datos de radiofrecuencia cifrados al módulo transceptor de RF 601. El módulo transceptor de RF 601 se configura para transmitir los cuartos datos de radiofrecuencia cifrados al dispositivo lector de tarjetas por medio del enlace de RF. El módulo transceptor de RF 601 también se configura para recibir los cuartos datos de radiofrecuencia cifrados transmitidos mediante el dispositivo lector de tarjetas por el enlace de RF. El microcontrolador 602 también se configura para descifrar los cuartos datos de radiofrecuencia cifrados recibidos con el uso de los datos de canal magnético. El módulo de aplicación de la tarjeta SIM 604 también se configura para realizar una un proceso aplicado correspondiente para los datos de radiofrecuencia descifrados.

[0049] Específicamente, los cuartos datos de radiofrecuencia pueden ser datos de aplicación enviados desde el lector de tarjetas a la tarjeta SIM de radiofrecuencia; y los terceros datos de radiofrecuencia pueden ser datos de respuesta de los datos de aplicación enviados de regreso desde la tarjeta SIM de radiofrecuencia al lector de tarjetas.

[0050] En la realización, también se proporciona un sistema de comunicación segura por RF. En referencia a la figura 7, esta figura 7 es un diagrama esquemático de un ejemplo de sistema de comunicación segura por RF coherente con las realizaciones reveladas. El sistema de comunicación segura por RF incluye al menos un primer terminal 701 y al menos un segundo terminal 702. El primer terminal 701 se configura para generar datos de canal magnético de manera aleatoria y establecer un enlace de radiofrecuencia con el segundo terminal 702 mediante el uso de los datos de comunicación magnética generados. El primer terminal 701 se configura para cifrar los datos de radiofrecuencia mediante el uso de los datos de canal magnético generados, y a continuación transmitir los datos de radiofrecuencia cifrados al segundo terminal 702 por medio del enlace de radiofrecuencia establecido. El primer terminal 701 también se configura para descifrar los datos de respuesta de radiofrecuencia enviados de regreso desde el segundo terminal 702 con el uso de los datos de canal magnético generados.

[0051] En función del sistema de comunicación segura por RF anterior, en la realización también se proporciona un método para una comunicación segura por radiofrecuencia. El método para una comunicación segura por radiofrecuencia de la presente realización además se ilustra a través de algunas realizaciones específicas en combinación con los dibujos que se proporcionan más adelante. En referencia a lo que se muestra en la figura 8, el método para una comunicación segura por radiofrecuencia de la realización incluye los siguientes pasos:

[0052] S801: Un primer terminal genera datos de canal magnético de manera aleatoria y transmite los datos de canal magnético generados por un canal magnético

[0053] S802: un segundo terminal detecta la intensidad de señal magnética de los datos de canal magnético y determina si la intensidad de señal magnética es mayor que un valor predeterminado. Si es así, el proceso va al paso S803; si no, el proceso continúa detectando la intensidad de señal magnética de los datos de canal magnético.

[0054] S803: el segundo terminal realiza una transformación irreversible a los datos de canal magnético actuales recibidos y genera parámetros del canal de radiofrecuencia basado en el resultado de la transformación.

[0055] S804: en función de los parámetros del canal de radiofrecuencia, el segundo terminal transmite la información de respuesta de los datos de canal magnético por un canal de radiofrecuencia correspondiente.

[0056] S805: el primer terminal realiza una transformación irreversible a los datos de canal magnético y genera los parámetros del canal de radiofrecuencia basado en el resultado de la transformación. En función de los parámetros del canal de radiofrecuencia, el primer terminal recibe la información de respuesta de los datos de canal magnético enviados desde el segundo terminal de la comunicación magnética en el canal de radiofrecuencia correspondiente y completa el establecimiento de un enlace de radiofrecuencia.

[0057] En la realización, los parámetros del canal de radiofrecuencia incluyen un punto de frecuencia de RF y una dirección. El canal de radiofrecuencia correspondiente puede obtenerse por medio del punto de frecuencia de RF y la dirección. La transformación irreversible implementada por el segundo terminal y la transformación irreversible implementada por el primer terminal son la misma y puede obtenerse el mismo resultado de transformación. En función del resultado de la transformación y el mismo algoritmo (por ejemplo, un algoritmo de cifrado), el segundo terminal genera el mismo punto de frecuencia de la radiofrecuencia y dirección.

[0058] S806: el primer terminal cifra los datos de aplicación mediante el uso de la información de los datos de canal magnético y transmite los datos de aplicación cifrados al segundo terminal por medio del enlace de radiofrecuencia establecido.

[0059] S807: el segundo terminal recibe los datos de aplicación cifrados transmitidos por el primer terminal mediante el enlace de radiofrecuencia establecido.

[0060] S808: el segundo terminal descifra los datos de aplicación cifrados con el uso de los datos de canal magnético recibidos.

[0061] S809: El segundo terminal ejecuta las instrucciones de la aplicación correspondiente en los datos de aplicación descifrados, cifra el resultado de la ejecución con el uso de los datos de canal magnético recibidos y transmite el resultado de ejecución cifrado al primer terminal por medio del enlace de radiofrecuencia establecido

[0062] S810: el primer terminal recibe el resultado de ejecución cifrado devuelto por el segundo terminal mediante el enlace de radiofrecuencia establecido.

[0063] S811: El primer terminal descifra el resultado de ejecución cifrado con el uso de los datos de canal magnético y realiza un proceso de aplicación correspondiente a los datos descifrados Entonces, el primer terminal puede continuar cifrando el resultado del procesamiento por medio de los datos de canal magnético y regresa el resultado de procesamiento cifrado al segundo terminal.

[0064] En la realización, los datos de RF transmitidos en el enlace de RF se cifran con el uso de los datos de canal magnético transmitidos por el canal magnético. Es decir, los datos transmitidos en el enlace de RF se cifran con el uso de la información de control de seguridad transmitida por el canal magnético. Debido a que la distancia de transmisión del canal magnético es corta y este no es fácil de interceptarse, incluso si el atacante falsifica un primer terminal mediante una especificación de protocolo público, y establece una conexión con el segundo terminal activado desde una ubicación distante, puesto que los datos de canal magnético como una clave de seguridad para el cifrado de datos no pueden ser robados, el proceso de cifrado o descifrado de los datos de RF no puede completarse, evitando el riesgo de que la clave predeterminada de seguridad sea interceptada o descifrada. No puede implementarse un ataque sustancial a la transacción, con lo que se mejora la seguridad del proceso de intercambio de los datos a través del enlace de radiofrecuencia. Al mismo tiempo, los datos de RF transmitidos por el enlace de RF se cifran directamente mediante el uso de los datos de canal magnético y no se requiere de un sistema exclusivo de gestión de distribución de claves, con lo cual se reducen la dificultad y los costos del mantenimiento de la seguridad. El primer terminal y el segundo terminal calculan los parámetros del canal de radiofrecuencia, basados en los datos de canal magnético, y establecen un enlace de radiofrecuencia correspondiente, simplificando aún más el proceso de establecimiento del enlace de RF.

[0065] El contenido anterior representa las descripciones con mayor detalle de la presente invención en conjunto con las realizaciones particulares y no puede afirmarse que las implementaciones específicas de la presente invención solamente se limiten a estas descripciones. En cuanto a los versados en la técnica de la presente invención, algunas deducciones sencillas o reemplazos hechos, bajo la condición de no apartarse de los conceptos de la presente invención, deben considerarse protegidos por el alcance de la presente invención.

Reivindicaciones

1. Un método para la comunicación segura por radiofrecuencia realizada por un terminal (701), que comprende:
la generación de datos de canal magnético (S801) y la transmisión de los datos de canal magnético (S801) por medio de un canal magnético;
el establecimiento (S803) de un enlace de radiofrecuencia con un dispositivo semejante que envía de regreso la información de respuesta (S804) de los datos de canal magnético; y en donde:
el cálculo de los parámetros (S803) del canal de radiofrecuencia, basado en los datos de canal magnético; y en donde la recepción de la información de respuesta de los datos de canal magnético proveniente del dispositivo semejante en un canal de radiofrecuencia correspondiente, basada en los parámetros del canal de radiofrecuencia;
la generación (S805) de primeros datos de radiofrecuencia, el cifrado (S806) de los primeros datos de radiofrecuencia con el uso de los datos del canal magnético y la transmisión (S806) de los primeros datos de radiofrecuencia cifrados al dispositivo semejante por medio del enlace de radiofrecuencia; y
la recepción (S807) de segundos datos de radiofrecuencia cifrados transmitidos por el dispositivo semejante por medio del enlace de radiofrecuencia y el descifrado (S808) de los segundos datos de radiofrecuencia cifrados mediante el uso de los datos de canal magnético.

2. El método de acuerdo con la Reivindicación 1, en donde:
los parámetros del canal de radiofrecuencia incluye un punto de frecuencia de RF y una dirección de radiofrecuencia.

3. El método de acuerdo con cualquiera de las Reivindicaciones 1 y 2, en donde:
los datos de canal magnético se generan (S801) de manera aleatoria.

4. Un método para la comunicación segura por radiofrecuencia realizada por un terminal (702), que comprende:
la recepción (S802) de datos de canal magnético a través de un canal magnético;
el establecimiento (S803) de un enlace de radiofrecuencia con un dispositivo semejante que envía (S804) los datos de canal magnético y en donde:
el cálculo de los parámetros (S803) del canal de radiofrecuencia, basado en los datos de canal magnético recibidos; y el envío (S804) de la información de respuesta de los datos de canal magnético al dispositivo semejante en un canal de radiofrecuencia correspondiente, basada en los parámetros del canal de radiofrecuencia.
la generación de terceros datos de radiofrecuencia, el cifrado (S809) de los terceros datos de radiofrecuencia con el uso de los datos del canal magnético y la transmisión (S809) de los terceros datos de radiofrecuencia cifrados al dispositivo semejante por medio del enlace de radiofrecuencia; y
la recepción (S810) de cuartos datos de radiofrecuencia cifrados transmitidos por el dispositivo semejante por medio del enlace de radiofrecuencia y el descifrado (S811) de los cuartos datos de radiofrecuencia cifrados mediante el uso de los datos de canal magnético.

5. El método de acuerdo con la Reivindicación 4, antes del cálculo de los parámetros del canal de radiofrecuencia basado en los datos de canal magnético, que además incluye:
la detección (S802) de la intensidad de la señal magnética de los datos de canal magnético; la determinación (S802) de si la intensidad de señal magnética detectada es mayor que un valor predeterminado; y
si la intensidad de señal magnética detectada es mayor que el valor predeterminado, basado en los datos de canal magnético recibidos, el cálculo de los parámetros (S803) del canal de radiofrecuencia.

6. El método de acuerdo con cualquiera de las Reivindicaciones 4 y 5, en donde:
los cuartos datos de radiofrecuencia son datos de aplicación; y
los terceros datos de radiofrecuencia son datos de respuesta de los datos de aplicación.

7. Un terminal (701), que comprende:
un módulo generador de señales magnéticas (11,303) configurado para generar datos de canal magnético y transmitir los datos de canal magnético a través de un canal magnético;
un módulo transceptor de radiofrecuencia (12,302) configurado para establecer un enlace de radiofrecuencia con un dispositivo semejante que envía de regreso una información de respuesta de los datos de canal magnético, para transmitir primeros datos de radiofrecuencia cifrados al dispositivo semejante a través de un enlace de radiofrecuencia y para recibir segundos datos de radiofrecuencia cifrados, transmitidos por el dispositivo semejante mediante el enlace de radiofrecuencia; y
un módulo de control (13,301) configurado para generar los primeros datos de radiofrecuencia, para cifrar los primeros datos de radiofrecuencia usando los datos de canal magnético, para transmitir los primeros datos de radiofrecuencia cifrados al módulo transceptor de radiofrecuencia (12,302) y descifrar los segundos datos de radiofrecuencia cifrados usando los datos de canal magnético y en donde el módulo de control incluye:
Un submódulo de transformación (131) configurado para calcular los parámetros del canal de radiofrecuencia,
basado en los datos de canal magnético.

8. El terminal (701) de acuerdo con la Reivindicación 7, en donde:
el módulo generador de señales magnéticas (11) incluye un submódulo generador de datos de canal magnético (111) y un submódulo generador de señales magnéticas (112);
el submódulo generador de datos de canal magnético (111) se configura para generar los datos de canal magnético; y
el submódulo generador de señales magnéticas (112) se configura para transmitir los datos de canal magnético a través del canal magnético.

9. El terminal (701) de acuerdo con la Reivindicación 8, en donde:
el módulo transceptor de radiofrecuencia (12) se configura para recibir la información de respuesta de los datos de canal magnético proveniente del dispositivo semejante en un canal de radiofrecuencia correspondiente, basado en los parámetros del canal de radiofrecuencia.

10. El terminal (701) de acuerdo con cualquiera de las Reivindicaciones 7 a 9, en donde:
el módulo de control (13) incluye un módulo de aplicación (132) y un módulo de cifrado y descifrado (133);
el módulo de aplicación (132) se configura para generar los primeros datos de radiofrecuencia, transmitir los primeros datos de radiofrecuencia al módulo de cifrado y descifrado (133), y realizar un proceso aplicado correspondiente a los segundos datos de radiofrecuencia descifrados por el módulo de cifrado y descifrado; y el módulo de cifrado y descifrado (133) se configura para cifrar los primeros datos de radiofrecuencia con el uso de los datos de canal magnético, para transmitir los primeros datos de radiofrecuencia cifrados al módulo transceptor de radiofrecuencia (12), para descifrar los segundos datos de radiofrecuencia cifrados, transmitidos por el dispositivo semejante con el uso de los datos de canal magnético, y para transmitir los segundos datos de radiofrecuencia descifrados al módulo de aplicación (132).

11. Un terminal (702), que comprende:
un módulo de inducción magnética (41,603) configurado para recibir los datos de canal magnético enviados desde afuera por medio de un canal magnético; un módulo transceptor de radiofrecuencia (42,601) configurado para establecer un enlace de radiofrecuencia con un dispositivo semejante, el cual transmite los datos de canal magnético, transmitir los terceros datos de radiofrecuencia cifrados al dispositivo semejante por medio del enlace de radiofrecuencia y recibir los cuartos datos de radiofrecuencia cifrados, transmitidos por el dispositivo semejante mediante el enlace de radiofrecuencia; y un módulo de control (43,602) configurado para generar los terceros datos de radiofrecuencia, cifrar los terceros datos de radiofrecuencia con el uso de los datos de canal magnético, transmitir los terceros datos de radiofrecuencia cifrados al módulo transceptor de radiofrecuencia y descifrar los cuartos datos de radiofrecuencia cifrados mediante el uso de los datos de canal magnético y en donde el módulo de control incluye:
un submódulo de transformación (431) configurado para calcular los parámetros del canal de radiofrecuencia, basado en los datos de canal magnético recibidos por el módulo de inducción magnética (41).

12. El terminal (702) de acuerdo con la Reivindicación 11, en donde:
el módulo transceptor de radiofrecuencia (42) se configura para enviar la información de respuesta de los datos de canal magnético al dispositivo semejante en un canal de radiofrecuencia correspondiente, basado en los parámetros del canal de radiofrecuencia.

13. El terminal (702) de acuerdo con la Reivindicación 11, en donde:
el módulo de control (43) también incluye un módulo de detección (432) y un submódulo de determinación (433);
el submódulo de detección (432) se configura para detectar la intensidad de señal magnética de los datos de canal magnético recibidos por el módulo de inducción magnética (41);
el submódulo de determinación (433) se configura para determinar si la intensidad de señal magnética detectada es mayor que un valor predeterminado; y
un submódulo de transformación (431) se configura para calcular los parámetros del canal de radiofrecuencia, basado en los datos de canal magnético recibidos por el módulo de inducción magnética (41), cuando el submódulo de determinación (433) determina que la intensidad de señal magnética es mayor que el valor predeterminado.

14. El terminal (702) de acuerdo con cualquiera de las Reivindicaciones 11 a 13, en donde:
el módulo de control (43,602) incluye un módulo de aplicación (434,604) y un módulo de cifrado y descifrado (435);
el módulo de aplicación (434) se configura para generar los terceros datos de radiofrecuencia y para transmitir los terceros datos de radiofrecuencia al módulo de cifrado y descifrado (435), y realizar un proceso aplicado correspondiente a los cuartos datos de radiofrecuencia descifrados por el módulo de cifrado y descifrado (435);
y el módulo de cifrado y descifrado (435), después del cifrado de los terceros datos de radiofrecuencia con el uso de los datos de canal magnético, se configura para transmitir los terceros datos de radiofrecuencia cifrados al módulo transceptor de radiofrecuencia (42), para descifrar los cuartos datos de radiofrecuencia cifrados transmitidos por el dispositivo semejante con el uso de los datos de canal magnético, y para transmitir los datos descifrados al módulo de aplicación (434).

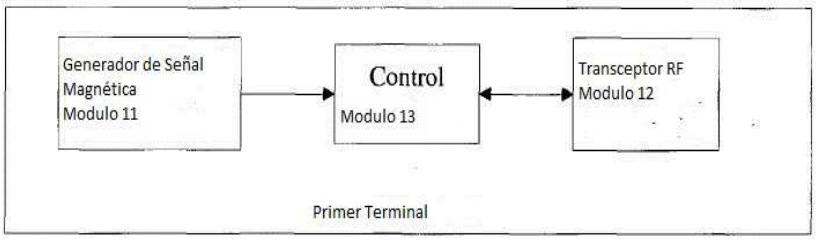
Generador de Señal
Magnética
Modulo 11
Control
Modulo 13
Transceptor RF
Modulo 12
Primer Terminal

FIG. 1

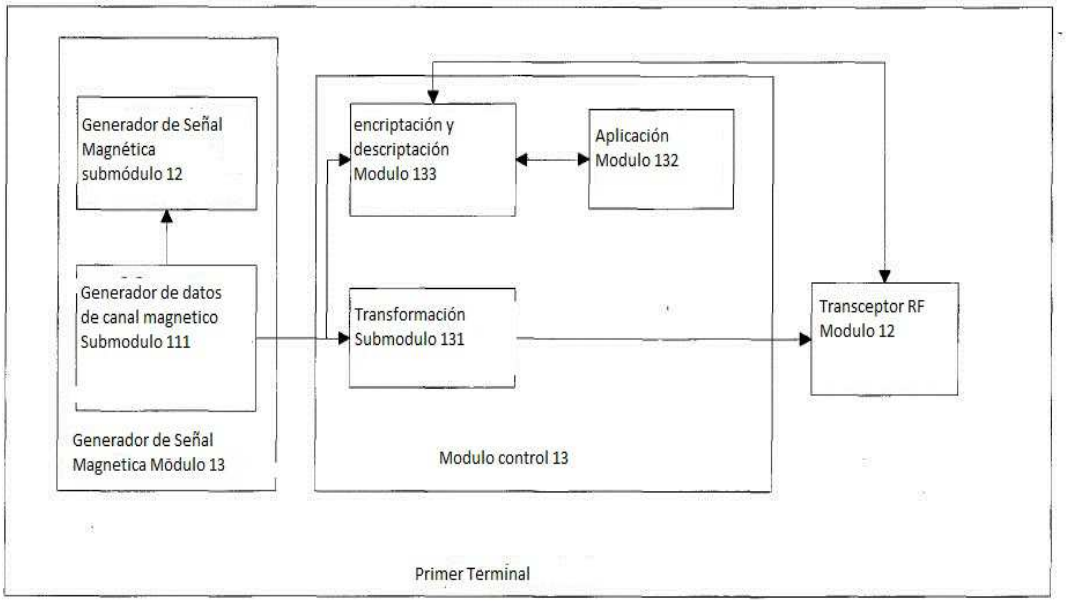
Generador de Señal
Magnética
submódulo 12
Generador de datos
de canal magnetico
Submodulo 111
Generador de Señal
Magnetica Módulo 13
encriptación y
descriptación
Modulo 133
Aplicación
Modulo 132
Transformación
Submodulo 131
Modulo control 13
Transceptor RF
Modulo 12
Primer Terminal

FIG. 2

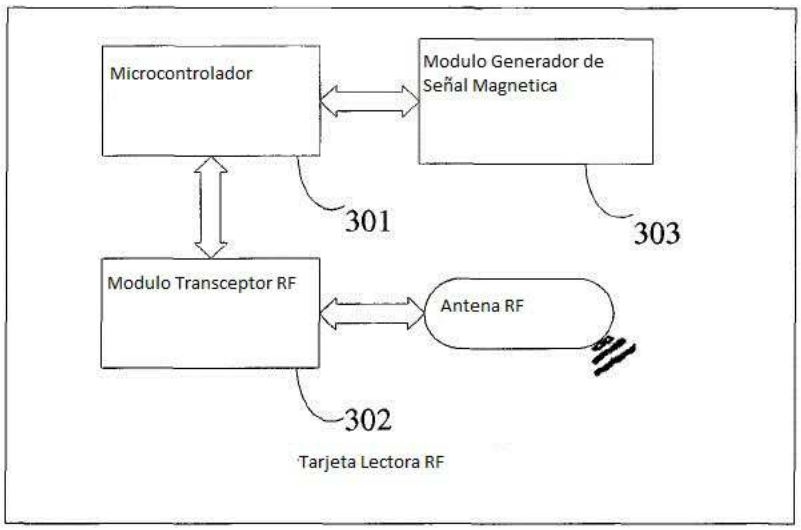
Microcontrolador
Modulo Generador de Señal Magnetica
301
303
Modulo Transceptor RF
Antena RF
302
Tarjeta Lectora RF

FIG. 3

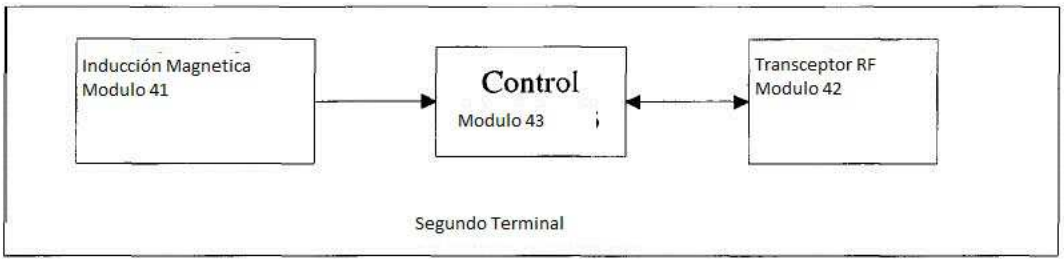
Inducción Magnetica Modulo 41
Control
Modulo 43
Transceptor RF Modulo 42
Segundo Terminal

FIG. 4

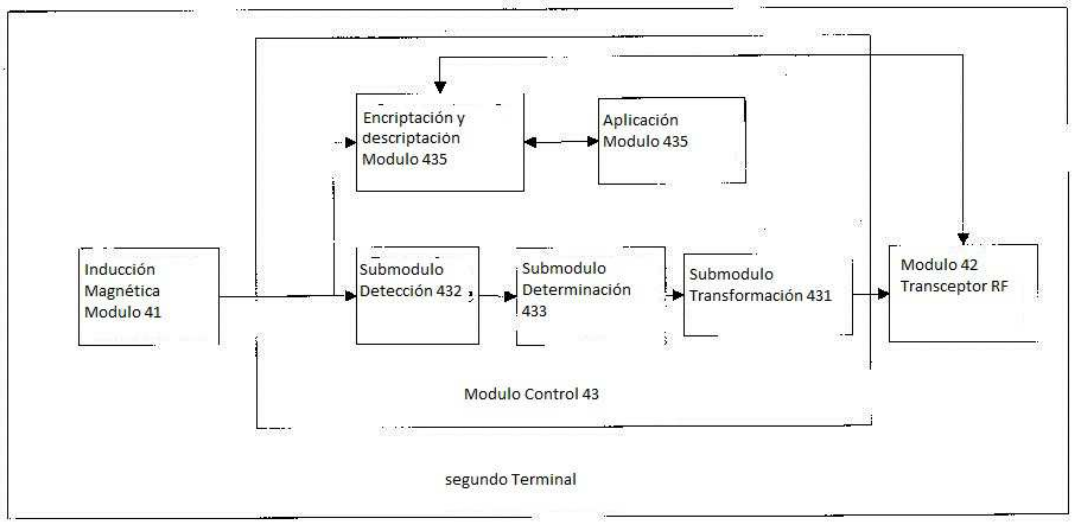

FIG. 5

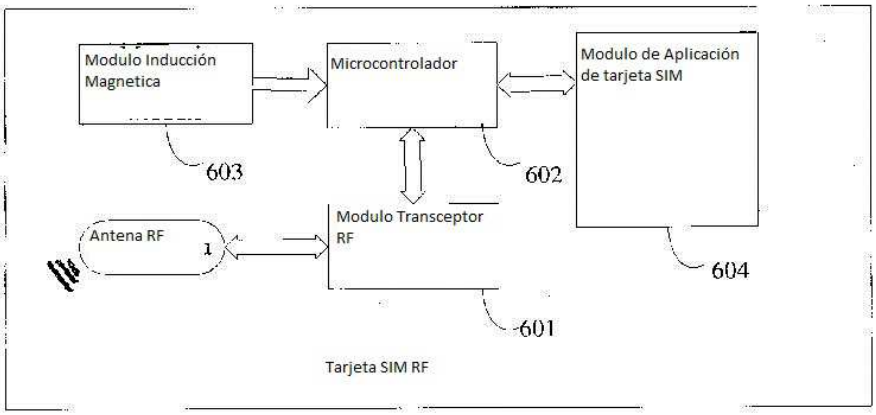

FIG. 6

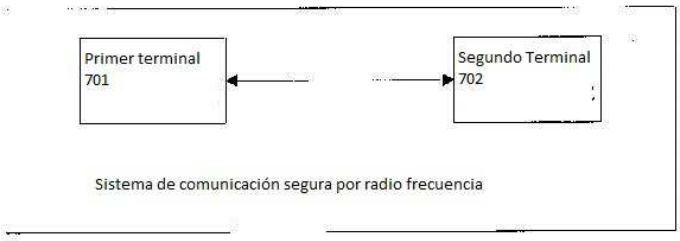

FIG. 7

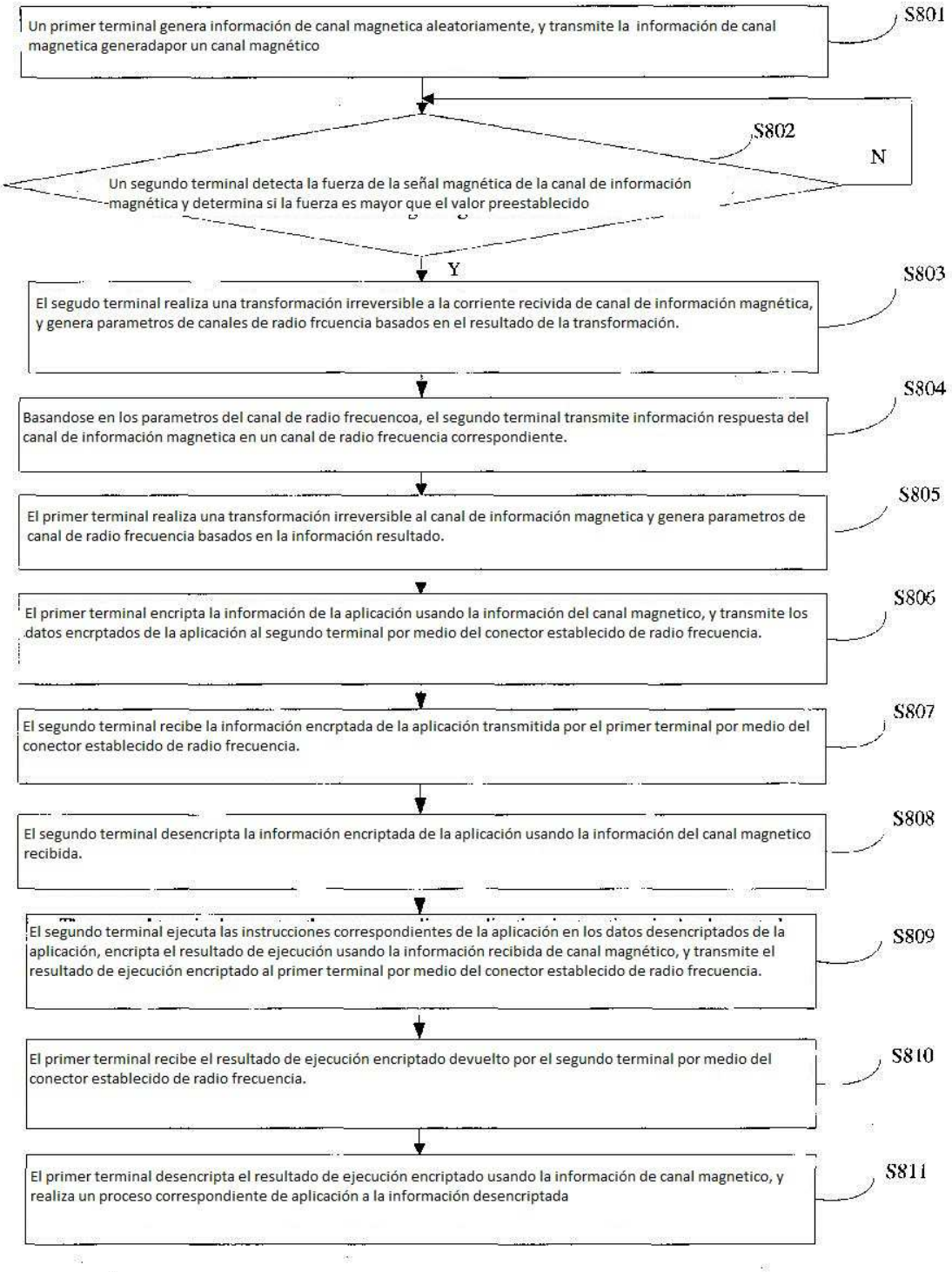
Un primer terminal genera información de canal magnetica aleatoriamente, y transmite la información de canal magnetica generadapor un canal magnético
S801
Un segundo terminal detecta la fuerza de la señal magnética de la canal de información magnética y determina si la fuerza es mayor que el valor preestablecido
S802
N
Y
El segudo terminal realiza una transformación irreversible a la corriente recivida de canal de información magnética, y genera parametros de canales de radio frcuencia basados en el resultado de la transformación.
S803
Basandose en los parametros del canal de radio frecuencoa, el segundo terminal transmite información respuesta del canal de información magnetica en un canal de radio frecuencia correspondiente.
S804
El primer terminal realiza una transformación irreversible al canal de información magnetica y genera parametros de canal de radio frecuencia basados en la información resultado.
S805
El primer terminal encripta la información de la aplicación usando la información del canal magnetico, y transmite los datos encrptados de la aplicación al segundo terminal por medio del conector establecido de radio frecuencia.
S806
El segundo terminal recibe la información encrptada de la aplicación transmitida por el primer terminal por medio del conector establecido de radio frecuencia.
S807
El segundo terminal desencripta la información encriptada de la aplicación usando la información del canal magnetico recibida.
S808
El segundo terminal ejecuta las instrucciones correspondientes de la aplicación en los datos desencriptados de la aplicación, encripta el resultado de ejecución usando la información recibida de canal magnético, y transmite el resultado de ejecución encriptado al primer terminal por medio del conector establecido de radio frecuencia.
S809
El primer terminal recibe el resultado de ejecución encriptado devuelto por el segundo terminal por medio del conector establecido de radio frecuencia.
S810
El primer terminal desencripta el resultado de ejecución encriptado usando la información de canal magnetico, y realiza un proceso correspondiente de aplicación a la información desencriptada
S811

FIG. 8