(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 929 464**

(51) Int. CI.:

H04L 9/32 (2006.01)
H04W 12/04 (2011.01)
H04W 12/02 (2009.01)
H04W 12/00 (2011.01)
H04W 4/70 (2008.01)
H04W 84/12 (2009.01)
H04W 12/50 (2011.01)
H04W 12/30 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **30.03.2017 PCT/CN2017/078852**

(87) Fecha y número de publicación internacional: **31.05.2018 WO18094938**

(96) Fecha de presentación y número de la solicitud europea: **30.03.2017 E 17874242 (5)**

(97) Fecha y número de publicación de la concesión europea: **31.08.2022 EP 3537652**

(54) Título: **Método para controlar de forma segura un aparato doméstico inteligente y dispositivo terminal**

(30) Prioridad:

26.11.2016 CN 201611057266

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
29.11.2022

(73) Titular/es:

HUAWEI TECHNOLOGIES CO., LTD. (100.0%)
Huawei Administration Building, Bantian, Longgang District
Shenzhen, Guangdong 518129, CN

(72) Inventor/es:

XU, JIANFENG

(74) Agente/Representante:

ELZABURU, S.L.P

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Método para controlar de forma segura un aparato doméstico inteligente y dispositivo terminal

Campo técnico

Esta solicitud se relaciona con el campo de las tecnologías de la comunicación y, en particular, con un método para controlar de forma segura un hogar inteligente y un dispositivo terminal.

Antecedentes

Como una red Fidelidad Inalámbrica (en inglés Wireless Fidelity, Wi-Fi) es muy utilizada, cada vez son más los dispositivos inteligentes que realizan la comunicación basada en la red Wi-Fi. En el campo del hogar inteligente, una gran cantidad de dispositivos domésticos inteligentes necesitan acceder a una red Wi-Fi generada por un enrutador. Sin embargo, limitados por un formulario, los dispositivos domésticos inteligentes, como una lámpara de mesa inteligente y un enchufe inteligente, generalmente no tienen pantalla ni teclado. No se puede seleccionar un identificador de conjunto de servicios (en inglés, Service Set Identifier, SSID) de la red Wi-Fi y no se puede ingresar una contraseña de la red Wi-Fi. Además, cuando el dispositivo doméstico inteligente está conectado a la red Wi-Fi mediante el uso de algunos métodos para configurar una red mediante una APP en un teléfono inteligente, el estado del enrutador conectado no se puede ver en el dispositivo.

En la técnica anterior, la configuración de red para un dispositivo doméstico inteligente y una red Wi-Fi se implementa de las dos maneras siguientes.

Manera 1: en una tecnología de configuración de red Soft-AP, un dispositivo doméstico inteligente que va a acceder a una red está en un modo Soft-AP y publica un nombre del dispositivo doméstico inteligente que va a acceder a una red. Un usuario selecciona, en una interfaz de programa de aplicación (en inglés Application, APP) de un dispositivo inteligente, el dispositivo doméstico inteligente que va a acceder a una red y que necesita ser configurado; ingresa, en la interfaz de la APP, un nombre y una contraseña de Wi-Fi generados por un enrutador; y toca un botón de configuración para completar la configuración. Al escanear el nombre del dispositivo doméstico inteligente, una APP del dispositivo inteligente se desconecta de un enrutador actual, se conecta a un Soft-AP del dispositivo doméstico inteligente que va a acceder a una red y luego envía información de configuración de red preestablecida al dispositivo doméstico inteligente. La información de configuración de la red incluye el nombre y la contraseña de la Wi-Fi generada por el enrutador. Después de obtener, desde la APP, el nombre y la contraseña de la Wi-Fi generada por el enrutador, el dispositivo doméstico inteligente que va a acceder a una red sale del modo Soft-AP y se conecta al enrutador. La APP vuelve a estar conectada al enrutador y recibe una notificación de que el dispositivo doméstico inteligente que va a acceder a una red está en línea.

Manera 2: en una tecnología de configuración de red de difusión, un dispositivo inteligente envía información de configuración de red a un dispositivo doméstico inteligente agregando la información de configuración de red a un paquete de multidifusión de Wi-Fi, un paquete de difusión de Wi-Fi, un paquete de unidifusión de Wi-Fi, o cualquier combinación de los mismos. Después de recibir la información de configuración de la red, el dispositivo doméstico inteligente se conecta automáticamente a una red Wi-Fi especificada por la información de configuración de la red. El dispositivo inteligente incluye dispositivos domésticos inteligentes como un teléfono inteligente, un decodificador (en ingles Set Top Box, STB) y un decodificador de televisión inteligente.

En conclusión, en el estado de la técnica, el usuario utiliza una manera de configuración de red sin contacto y sin proximidad. Existen los siguientes problemas: Se agrega por error otro dispositivo doméstico inteligente a una red Wi-Fi de un enrutador en un hogar del usuario, o se configura un dispositivo doméstico inteligente del usuario en otra red Wi-Fi de un enrutador en un hogar de otro usuario, o un terminal inteligente de otro usuario falsifica un dispositivo terminal inteligente en un hogar del usuario, o la información de configuración es interceptada por un dispositivo de interceptación inalámbrico malicioso circundante, o similar. Cómo proporcionar una solución segura y de confianza de configuración de red para un dispositivo doméstico inteligente y una red Wi-Fi para evitar la fuga de información de configuración de red es un problema que debe resolverse actualmente.

El documento EP 3 007 480 A1 se refiere a un método para realizar un proceso de emparejamiento en un dispositivo inalámbrico en un sistema de comunicación inalámbrica, comprendiendo el método: transmitir una señal que incluye una clave de cifrado a un terminal; recibir un mensaje de éxito de autenticación que está cifrado en base a la clave de cifrado del terminal; y realizar el proceso de emparejamiento con un coordinador en función de la clave de cifrado, en el que el mensaje de éxito de la autenticación se recibe si la autenticación del dispositivo inalámbrico tiene éxito en función de la intensidad de la señal recibida de la señal que incluye la clave de cifrado que se mide en el terminal, y en el que la clave de cifrado se transmite desde el terminal al coordinador si la autenticación del dispositivo inalámbrico tiene éxito.

El documento US 2016/174146 A1 se refiere a un método para conectar un aparato inteligente no conectado a una red inalámbrica, que comprende: recibir, por un terminal, información del aparato difundida por el aparato inteligente desconectado, la información del aparato contiene al menos una identificación del aparato inteligente desconectado; mostrar, por parte del terminal, una notificación para conectar el aparato inteligente no conectado a la red inalámbrica;

recibir, por parte del terminal, una instrucción de conexión activada por un usuario según la notificación; y conectar el aparato inteligente no conectado a la red inalámbrica según las instrucciones de conexión.

El documento US 2014/226817 A1 se refiere a un método para distribuir información de configuración de red a través de una red inalámbrica a un dispositivo no cliente, que comprende: determinar, mediante un dispositivo cliente de red, la información de configuración de red; y generar, por parte del dispositivo cliente de la red, un paquete de datos que tiene la información de configuración de la red; transmitir el paquete de datos que tiene la información de configuración de la red a través de la red inalámbrica de manera multidifusión.

El documento WO 2011/139962 A1 se refiere a un sistema para unir un dispositivo electrónico a una red inalámbrica segura, comprendiendo dicho sistema: un módulo de activación para activar dicho dispositivo electrónico para que entre en un modo de configuración, permitiendo dicho modo de configuración que dicho dispositivo electrónico se conecte y sea configurado por un dispositivo informático; un módulo de a para recopilar ajustes de conexión que comprende configuraciones de seguridad para dicha red inalámbrica desde dicho dispositivo informático, siendo dicho dispositivo informático un miembro de dicha red inalámbrica; un módulo de red para crear un enlace de red entre dicho dispositivo informático y dicho dispositivo electrónico, habilitando la creación de dicho enlace de red al menos en parte mediante dicha activación de dicho dispositivo electrónico para entrar en el modo de configuración; y un módulo de configuración para comunicarse a través de dicho enlace de red con dicho dispositivo electrónico para configurar dicho dispositivo electrónico con dichos ajustes de conexión.

El Documento Sarikaya Huawei M Sethi Ericsson B: "Secure IoT Bootstrapping: A Survey; draft-sarikaya-t2trg-sbootstrapping-01.txt", Grupo de Trabajo de Ingeniería de Internet, IETF; StandardWorkingDraft, Internet Society (ISOC) 4, rue des Falaises CH- 1205 Ginebra, Suiza presenta un estudio de los mecanismos de arranque seguros disponibles para objetos inteligentes que forman parte de una red de Internet de las cosas (IoT). Su objetivo es proporcionar una clasificación estructurada de los mecanismos disponibles. A los desarrolladores de IoT se les presentan diferentes opciones para elegir, según su caso de uso, los requisitos de seguridad y la interfaz de usuario disponible en sus objetos inteligentes.

El documento CN 105 933 904 A se refiere a un método de conexión a la red que comprende los pasos: obtener la identificación del equipo inteligente; obtener una clave secreta del equipo inteligente en base a la identificación del equipo inteligente, en donde la clave secreta del equipo inteligente es diferente de la identificación del equipo inteligente; llevar a cabo el cifrado de la información de configuración de una red inalámbrica de destino a través de la clave secreta del equipo inteligente, y obtener la información de configuración cifrada, donde la red inalámbrica de destino es una red inalámbrica a la que está conectado actualmente un terminal; transmitir la información de configuración cifrada y permitir que el equipo inteligente acceda a la red inalámbrica de destino basándose en la información de configuración cifrada.

Resumen

La invención está definida por las reivindicaciones adjuntas.

Breve descripción de los dibujos

La FIG. 1 es un diagrama de flujo de un método para controlar de forma segura un dispositivo doméstico inteligente según una realización de esta solicitud;

La FIG. 2 es un diagrama de flujo de otro método para controlar de forma segura un dispositivo doméstico inteligente según una realización de esta solicitud;

La FIG. 3 es un diagrama de flujo de otro método más para controlar de forma segura un dispositivo doméstico inteligente según una realización de esta solicitud;

La FIG. 4A y la FIG. 4B son un diagrama de flujo de otro método más para controlar de forma segura un dispositivo doméstico inteligente según una realización de esta solicitud;

La FIG. 5 es un diagrama esquemático de un dispositivo terminal inteligente según una realización de esta solicitud;

La FIG. 6 es un diagrama esquemático de un dispositivo doméstico inteligente según una realización de esta solicitud;

La FIG. 7 es un diagrama estructural del hardware de un dispositivo terminal inteligente según una realización de esta solicitud; y

La FIG. 8 es un diagrama estructural del hardware de un dispositivo doméstico inteligente según una realización de esta solicitud.

Descripción de realizaciones

Para hacer más claros los objetivos, las soluciones técnicas y las ventajas de esta solicitud, a continuación se describe más detalladamente esta solicitud con referencia a los dibujos adjuntos.

Las realizaciones de esta solicitud proporcionan un método para controlar de forma segura un dispositivo doméstico inteligente y un dispositivo terminal, para resolver un problema de la técnica anterior de que la información de configuración de un dispositivo doméstico inteligente y una red Wi-Fi es interceptada por un dispositivo de interceptación inalámbrico malicioso circundante, se falsifica un dispositivo doméstico inteligente o se falsifica un terminal inteligente. El método y el aparato están concebidos en base a una misma invención. El método y el aparato tienen principios similares para resolver los problemas. Por lo tanto, para la implementación del aparato y el método, se refieren entre sí y no se describen los detalles de las partes repetidas. Además, en la descripción de esta solicitud, las palabras como "primero" y "segundo" se utilizan meramente para descripción de distinción, y no deben entenderse como una indicación o implicación de importancia relativa o una indicación o implicación de un orden.

Con referencia a los dibujos adjuntos, lo siguiente describe en detalle el método para controlar de forma segura un dispositivo doméstico inteligente según esta solicitud.

Haciendo referencia a la FIG. 1, la FIG. 1 es un diagrama de flujo de un método para controlar de forma segura un dispositivo doméstico inteligente según esta solicitud. Cuando es necesario configurar una red para un dispositivo doméstico inteligente, un usuario agrega, en una interfaz de APP en un dispositivo inteligente, el dispositivo doméstico inteligente que debe acceder a una red y que debe configurarse. El método incluye los siguientes pasos.

S101. Un dispositivo terminal inteligente muestra al menos una indicación de operación para un dispositivo doméstico inteligente cuando el dispositivo terminal inteligente recibe una instrucción de operación ingresada por un usuario para agregar el dispositivo doméstico inteligente, donde la indicación de operación se usa para indicar al usuario que realice el control de funciones en el dispositivo doméstico inteligente.

Por ejemplo, el dispositivo terminal inteligente puede ser un teléfono inteligente, un STB, OTT o similar, y el dispositivo doméstico inteligente puede ser una lámpara de mesa inteligente, un acondicionador de aire inteligente, una caja de sonido inteligente o similar. Cuando el dispositivo terminal inteligente es un teléfono inteligente, el dispositivo doméstico inteligente es una lámpara de mesa inteligente, y cuando el teléfono inteligente necesita configurar la lámpara de mesa inteligente, una indicación de operación mostrada por un programa de aplicación (en inglés Application, APP) en el teléfono inteligente indica una combinación de control de función que se puede realizar en el hogar inteligente, y la combinación puede ser cualquier control de función que se realice repetidamente cualquier cantidad de veces. Por ejemplo, el control de funciones de la lámpara de mesa inteligente es: {encender, apagar, iluminar, atenuar}. En este caso, la indicación de operación puede ser encender la lámpara de mesa inteligente dos veces consecutivas, tres veces consecutivas o cuatro veces consecutivas, o atenuar la lámpara de mesa inteligente después de encender la lámpara de mesa inteligente. Cuando el dispositivo doméstico inteligente es un acondicionador de aire inteligente, la indicación de operación que muestra la aplicación puede ser presionar secuencialmente una o más teclas de un control remoto del acondicionador de aire inteligente, o presionar una tecla compuesta del control remoto. La aplicación en el teléfono inteligente muestra aleatoriamente una o más indicaciones de operación. La indicación de operación se determina en función del tipo de dispositivo doméstico inteligente.

S102. El dispositivo terminal inteligente genera, al determinar una indicación de operación seleccionada por el usuario a partir de la al menos una indicación de operación, una primera clave basada en la indicación de operación seleccionada, donde la primera clave es utilizada por el dispositivo terminal inteligente para cifrar la información que se va a enviar al dispositivo doméstico inteligente.

Opcionalmente, el dispositivo terminal inteligente utiliza además la primera clave para autenticar la información que se va a enviar al dispositivo doméstico inteligente.

Específicamente, la indicación de operación seleccionada se procesa utilizando un algoritmo específico para generar la primera clave. La indicación de operación determinada puede hacerse corresponder a una combinación de números aleatorios usando el algoritmo especificado. Los números aleatorios pueden cifrarse aún más mediante el uso de un cifrado de cuarto cuadrado, un cifrado de sustitución, un cifrado de transposición, un cifrado de rotor, un cifrado polialfabético y un cifrado de transposición. Esto no está limitado en la presente invención.

En esta realización de la presente invención, se proporciona el método para controlar de forma segura un dispositivo doméstico inteligente. El dispositivo terminal inteligente selecciona la indicación de operación correspondiente en función del tipo de dispositivo doméstico inteligente y genera, en función de la indicación de operación, la primera clave utilizada para cifrar la información que se enviará al dispositivo doméstico inteligente. El usuario gestiona y controla la configuración de la red a corta distancia. De esta manera, se proporciona una solución segura y de confianza de configuración de red para el dispositivo doméstico inteligente y una red Wi-Fi, para evitar la fuga de información de configuración de red.

En una posible implementación, después del paso S101, el método incluye además: recibir, por parte del dispositivo terminal inteligente, la indicación de operación seleccionada por el usuario de la al menos una indicación de operación.

En una posible implementación, después del paso S102, el método incluye además: generar, por parte del dispositivo terminal inteligente, una segunda clave basada en la primera clave, donde la segunda clave es utilizada por el dispositivo terminal inteligente para cifrar la información que se enviará a el dispositivo doméstico inteligente. Específicamente, el dispositivo terminal inteligente genera la segunda clave combinando la primera clave y otra forma

de encriptación. La otra forma de encriptación incluye un algoritmo de encriptación AES.

Opcionalmente, la segunda clave puede ser utilizada además por el dispositivo terminal inteligente para autenticar la información que se va a enviar al dispositivo doméstico inteligente.

En esta realización de la presente invención, la información enviada por el dispositivo terminal inteligente al dispositivo doméstico inteligente se cifra mediante el uso de la segunda clave, para mejorar aún más la seguridad de la información de configuración de la red.

En una posible implementación, después del paso S102, el método incluye además: cifrar, por parte del dispositivo terminal inteligente usando la primera clave, información de autenticación para controlar el dispositivo terminal inteligente para acceder a una red Wi-Fi, y enviar información de autenticación cifrada de la red Wi-Fi al dispositivo doméstico inteligente, donde la información de autenticación incluye al menos un nombre, una contraseña o un certificado de la red Wi-Fi.

En una posible implementación, después de que el dispositivo terminal inteligente almacene la segunda clave, el método incluye además: cifrar, por parte del dispositivo terminal inteligente mediante el uso de la segunda clave, la información de autenticación para controlar el dispositivo terminal inteligente para acceder a la red Wi-Fi, y enviar información de autenticación cifrada de la red Wi-Fi al dispositivo doméstico inteligente, donde la información de autenticación incluye al menos uno de los siguientes: el nombre, la contraseña o el certificado de la red Wi-Fi.

Haciendo referencia a la FIG. 2, la FIG. 2 es un diagrama de flujo de otro método para controlar de forma segura un dispositivo doméstico inteligente según esta solicitud. El método incluye los siguientes pasos:

S201. Un dispositivo terminal inteligente muestra al menos una indicación de operación para un dispositivo doméstico inteligente cuando el dispositivo terminal inteligente recibe una instrucción ingresada por un usuario para realizar una operación de configuración de red en el dispositivo doméstico inteligente, donde la indicación de operación se usa para instruir al usuario a realizar el control de funciones en el dispositivo doméstico inteligente.

S202. El dispositivo terminal inteligente genera, cuando determina una indicación de operación seleccionada por el usuario, una primera clave basada en la indicación de operación seleccionada, donde la primera clave es utilizada por el dispositivo terminal inteligente para cifrar información que se enviará al dispositivo doméstico inteligente.

Haciendo referencia a la FIG. 3, la FIG. 3 es un diagrama de flujo de otro método más para controlar de forma segura un dispositivo doméstico inteligente según esta solicitud. El método incluye los siguientes pasos:

S301. Un dispositivo doméstico inteligente recibe una instrucción de control de función activada por un usuario, donde el usuario ingresa la instrucción de control de función en función de al menos una indicación de operación que se muestra en un dispositivo terminal inteligente, y la indicación de operación se usa para instruir al usuario a realizar un control de función en el dispositivo doméstico inteligente.

Opcionalmente, la instrucción de control de función recibida por el dispositivo doméstico inteligente es activada por el usuario a través del contacto o es una operación a una distancia extremadamente cercana.

S302. El dispositivo doméstico inteligente genera una primera clave basada en la instrucción de control de función, donde la primera clave se usa para descifrar la información cifrada enviada por el dispositivo terminal inteligente al dispositivo doméstico inteligente.

Opcionalmente, la primera clave se usa además para autenticar la información enviada por el dispositivo terminal inteligente al dispositivo doméstico inteligente.

En una posible implementación, después del paso S302, el método incluye además: generar, por parte del dispositivo terminal inteligente, una segunda clave basada en la primera clave, donde la segunda clave se usa para descifrar la información cifrada enviada por el dispositivo terminal inteligente al dispositivo doméstico inteligente, o autenticar la información enviada por el dispositivo terminal inteligente al dispositivo doméstico inteligente.

Específicamente, el dispositivo terminal inteligente genera la segunda clave combinando la primera clave y otra forma de descifrado.

En una posible implementación, después del paso S302, el método incluye además: recibir, por parte del dispositivo doméstico inteligente, información de autenticación cifrada que es de una red Wi-Fi y enviada por el dispositivo terminal inteligente, y descifrar la información de autenticación cifrada de la red Wi-Fi mediante el uso de la primera clave almacenada, para obtener información de autenticación descifrada de la red Wi-Fi, donde la información de autenticación incluye al menos uno de un nombre, una contraseña o un certificado de la red Wi-Fi; y acceder, mediante el dispositivo doméstico inteligente, a la red Wi-Fi correspondiente utilizando la información de autenticación descifrada de la red Wi-Fi.

En una posible implementación, después de que el dispositivo doméstico inteligente almacene la segunda clave, el método incluye además: recibir, por parte del dispositivo doméstico inteligente, la información de autenticación cifrada

que es de la red Wi-Fi y enviada por el dispositivo terminal inteligente, y descifrar la información de autenticación cifrada de la red Wi-Fi mediante el uso de la segunda clave almacenada, para obtener información de autenticación descifrada de la red Wi-Fi, donde la información de autenticación incluye al menos uno de los siguientes: el nombre, la contraseña o el certificado de la red Wi-Fi -Fi red; y acceder, mediante el dispositivo doméstico inteligente, a la red Wi-Fi correspondiente utilizando la información de autenticación descifrada de la red Wi-Fi.

Haciendo referencia a la FIG. 4A y la FIG. 4B, la FIG. 4A y la FIG. 4B son un diagrama de flujo de otro método más para controlar de forma segura un dispositivo doméstico inteligente según una realización de esta solicitud. Se supone que un dispositivo terminal inteligente es un teléfono inteligente y un dispositivo doméstico inteligente es una lámpara de mesa inteligente. El método incluye los siguientes pasos:

S401. Cuando se enciende y se inicia, la lámpara de mesa inteligente que no ha accedido a una red crea un punto de acceso (en inglés Access Point, AP) habilitado por software para el exterior, o notifica a un dispositivo circundante sobre un identificador de conjunto de servicio Wi-Fi (en inglés Service Set Identifier, SSID) especial de la lámpara de mesa inteligente en forma de difusión/multidifusión, donde el SSID incluye un modelo y similar de la lámpara de mesa inteligente.

S402. El teléfono inteligente encuentra la lámpara de mesa inteligente que lo rodea mediante el uso de una función de escaneo de dispositivos Wi-Fi, el teléfono inteligente envía activamente información rápida de que se encuentra la lámpara de mesa inteligente, o un usuario ingresa activamente en un proceso de configuración de la lámpara de mesa inteligente, y luego el usuario activa, en el teléfono inteligente, un proceso de agregar la lámpara de mesa inteligente.

S403. Una APP en el teléfono inteligente muestra, en una interfaz basada en un tipo de lámpara de mesa inteligente escaneada, una indicación de operación seleccionada aleatoriamente de una serie de indicaciones de operación predefinidas, donde, por ejemplo, la indicación de operación es encender/apagar la lámpara de mesa inteligente tres veces.

S404. La APP en el teléfono inteligente codifica la indicación de operación seleccionada mediante el uso de un algoritmo específico para formar una clave de cifrado y cifra la información de autenticación mediante la combinación de la clave de cifrado y otra forma de cifrado.

S405. La lámpara de mesa inteligente recibe una instrucción de control de función ingresada por el usuario, donde la instrucción de control de función se ingresa en función de la indicación de operación seleccionada que se muestra en la interfaz por la APP en el teléfono inteligente, por ejemplo, encender/apagar la lámpara de mesa inteligente tres veces.

S406. La lámpara de mesa inteligente registra la instrucción de control de función y genera y almacena una clave de descifrado basada en la instrucción de control de función.

S407. La aplicación en el teléfono inteligente envía información de autenticación encriptada a la lámpara de mesa inteligente utilizando una configuración de red de transmisión/multidifusión existente o tecnología de configuración de red Soft-AP.

S408. Después de recibir la información de autenticación, la lámpara de mesa inteligente obtiene información de autenticación de texto sin cifrar a través del descifrado mediante el uso de la clave de descifrado previamente almacenada y en combinación con otra forma de descifrado o autenticación, como un algoritmo de cifrado AES.

S409. La lámpara de mesa inteligente se conecta a un enrutador utilizando la información de autenticación de texto sin cifrar obtenida a través del descifrado y notifica al teléfono inteligente mediante una red del enrutador para completar la configuración de la red.

Basada en un mismo concepto de invención que las realizaciones del método, esta solicitud proporciona además un diagrama esquemático de un dispositivo terminal inteligente. Como se muestra en la FIG. 5, el dispositivo terminal inteligente incluye:

un módulo 501 de pantalla, configurado para mostrar al menos una indicación de operación para un dispositivo doméstico inteligente cuando el dispositivo terminal inteligente recibe una instrucción de operación ingresada por un usuario para agregar el dispositivo doméstico inteligente, donde la indicación de operación se usa para instruir al usuario a realizar control de función en el dispositivo doméstico inteligente; y

un módulo 502 de procesamiento, configurado para generar, cuando se determina una indicación de operación seleccionada por el usuario de al menos una indicación de operación, una primera clave basada en la indicación de operación seleccionada, donde la primera clave es utilizada por el dispositivo terminal inteligente para cifrar información que se enviará al dispositivo doméstico inteligente.

En esta realización de la presente invención, se proporciona el dispositivo terminal inteligente. El dispositivo terminal inteligente selecciona la indicación de operación correspondiente en base a un tipo de dispositivo doméstico inteligente y genera, en base a la indicación de operación, la primera clave utilizada para cifrar la información que se va a enviar

al dispositivo doméstico inteligente. El usuario gestiona y controla la configuración de la red a corta distancia. De esta manera, se proporciona una solución segura y de confianza de configuración de red para el dispositivo doméstico inteligente y una red Wi-Fi, para evitar la fuga de información de configuración de red.

En una posible implementación, el módulo 502 de procesamiento está configurado además para recibir la indicación de operación seleccionada por el usuario de la al menos una indicación de operación.

En una posible implementación, el módulo 502 de procesamiento está además configurado para generar una segunda clave basada en la primera clave. La segunda clave es utilizada por el dispositivo terminal inteligente para cifrar la información que se va a enviar al dispositivo doméstico inteligente.

En una posible implementación, el dispositivo terminal inteligente incluye además: un módulo de envío, configurado para: cifrar, utilizando la clave de cifrado, información de autenticación para controlar el dispositivo terminal inteligente para acceder a una red Wi-Fi, y enviar información de autenticación cifrada de la red Wi-Fi al dispositivo doméstico inteligente, donde la información de autenticación incluye al menos un nombre, una contraseña o un certificado de la red Wi-Fi.

En una posible implementación, la indicación de operación se determina en base a un tipo de dispositivo doméstico inteligente.

Basada en el mismo concepto de invención que las realizaciones del método, esta solicitud proporciona además un diagrama esquemático de un dispositivo doméstico inteligente. Como se muestra en la FIG. 6, el dispositivo doméstico inteligente incluye:

un módulo 601 de recepción, configurado para recibir una instrucción de control de función activada por un usuario, donde el usuario ingresa la instrucción de control de función en base a al menos una indicación de operación mostrada en un dispositivo terminal inteligente, y la indicación de operación se usa para instruir al usuario para realizar el control de función en el dispositivo doméstico inteligente; y

un módulo 602 de generación, configurado para generar una primera clave basada en la instrucción de control de función, donde la primera clave se usa para descifrar información cifrada enviada por el dispositivo terminal inteligente al dispositivo doméstico inteligente.

En una posible implementación, el módulo de procesamiento está además configurado para generar una segunda clave basada en la primera clave. La segunda clave se utiliza para descifrar la información cifrada enviada por el dispositivo terminal inteligente al dispositivo doméstico inteligente.

En una posible implementación, el dispositivo doméstico inteligente incluye además: un módulo de procesamiento, configurado para: recibir información de autenticación cifrada que es de una red Wi-Fi y enviada por el dispositivo terminal inteligente, y descifrar la información de autenticación cifrada de la red Wi-Fi red mediante el uso de la clave de descifrado almacenada, para obtener información de autenticación descifrada de la red Wi-Fi, donde la información de autenticación incluye al menos un nombre, una contraseña o un certificado de la red Wi-Fi. El módulo de procesamiento se configura además para acceder a la red Wi-Fi correspondiente mediante el uso de la información de autenticación descifrada de la red Wi-Fi.

La división de módulos en las realizaciones de esta solicitud es un ejemplo, es simplemente una división de función lógica y puede haber otra división durante la implementación real. Además, los módulos funcionales en las realizaciones de esta aplicación pueden estar integrados en un procesador, o pueden existir solos físicamente, o dos o más módulos están integrados en un módulo. El módulo integrado puede implementarse en forma de hardware, o puede implementarse en forma de un módulo funcional de software.

Cuando el módulo integrado se implementa en forma de hardware, como se muestra en la FIG. 7, un dispositivo terminal inteligente puede incluir un procesador 701. El hardware de una entidad correspondiente al módulo puede ser el procesador 701. El procesador 701 puede ser una unidad central de procesamiento (en inglés central processing unit, CPU para abreviar), un módulo de procesamiento digital, o similar. El procesador 701 recibe una instrucción de operación enviada por un usuario para agregar un dispositivo doméstico inteligente. El aparato incluye además una memoria 702, configurada para almacenar un programa ejecutado por el procesador 701. La memoria 702 puede ser una memoria no volátil como un disco duro o un disco de estado sólido, o puede ser una memoria volátil (en inglés volatile memory) como una memoria de acceso aleatorio (inglés: memoria de acceso aleatorio, RAM para abreviar). La memoria 702 es cualquier otro medio que puede configurarse para transportar o almacenar el código de programa deseado en forma de una instrucción o una estructura de datos y al que puede acceder un ordenador, pero no se limita a ello.

El procesador 701 está configurado para ejecutar el código de programa almacenado en la memoria 702, para invocar específicamente una instrucción de programa almacenada en la primera memoria para: controlar, cuando se recibe la instrucción de operación ingresada por el usuario para agregar el dispositivo doméstico inteligente, una pantalla 703 para mostrar al menos una indicación de operación para el dispositivo doméstico inteligente, donde la indicación de operación se usa para indicar al usuario que realice el control de función en el dispositivo doméstico inteligente; y

generar, cuando se determina una indicación de operación seleccionada por el usuario de al menos una indicación de operación, una primera clave basada en la indicación de operación seleccionada, donde la primera clave es utilizada por el dispositivo terminal inteligente para cifrar la información que se enviará al dispositivo doméstico inteligente.

Un medio de conexión específico entre el procesador 701, la memoria 702 y la pantalla 703 no está limitado en esta realización de esta solicitud. En esta realización de esta solicitud, la memoria 702, el procesador 701 y la pantalla 703 están conectados usando un bus 704 en la FIG. 7. El bus se indica con una línea en negrita en la FIG. 7. Una forma de conexión entre otros componentes es simplemente un ejemplo para la descripción y no impone ninguna limitación. El bus puede clasificarse en un bus de direcciones, un bus de datos, un bus de control y similares. Para facilitar la indicación, el bus se indica usando solo una línea en negrita en la FIG. 7. Sin embargo, no indica que haya un solo bus o un solo tipo de bus.

Una realización de la presente invención proporciona además un dispositivo doméstico inteligente. El dispositivo doméstico inteligente incluye: una memoria 802, configurada para almacenar una instrucción de programa; y un procesador 801, configurado para invocar la instrucción de programa almacenada en la memoria 802 para: recibir una instrucción de control de función activada por un usuario, donde el usuario ingresa la instrucción de control de función en base a al menos una indicación de operación mostrada en un terminal inteligente dispositivo, y la indicación de operación se utiliza para indicar al usuario que realice el control de funciones en el dispositivo doméstico inteligente; y generar una primera clave basada en la instrucción de control de función, donde la primera clave se usa para descifrar información cifrada enviada por el dispositivo terminal inteligente al dispositivo doméstico inteligente. Un medio de conexión específico entre el procesador 801 y la memoria 802 no está limitado en esta realización de esta solicitud. En esta realización de esta aplicación, la memoria 802 y el procesador 801 están conectados usando un bus 803 en la FIG. 8. El bus se indica con una línea en negrita en la FIG. 8. Una forma de conexión entre otros componentes es simplemente un ejemplo para la descripción y no impone ninguna limitación. El bus puede clasificarse en un bus de direcciones, un bus de datos, un bus de control y similares. Para facilitar la indicación, el bus se indica usando solo una línea en negrita en la FIG. 8. Sin embargo, no indica que haya un solo bus o un solo tipo de bus.

Una realización de la presente invención proporciona además un medio de almacenamiento legible por ordenador, configurado para almacenar una instrucción de software informática utilizada para ejecutar operaciones que necesitan ser ejecutadas por el procesador. La instrucción de software informática incluye un programa utilizado para ejecutar las operaciones que debe ejecutar el procesador.

Los expertos en la materia deben comprender que las realizaciones de esta solicitud pueden proporcionarse como un método, un sistema o un producto de programa informático. Por lo tanto, esta aplicación puede usar una forma de realizaciones de solo hardware, realizaciones de solo software o realizaciones con una combinación de software y hardware. Además, esta solicitud puede usar una forma de producto de programa informático que se implementa en uno o más medios de almacenamiento utilizables por ordenador (incluidos, entre otros, una memoria de disco magnético, un CD-ROM, una memoria óptica y similares) que incluyen código de programa utilizable por ordenador.

Esta solicitud se describe con referencia a los diagramas de flujo y/o diagramas de bloques del método, el dispositivo (sistema) y el producto de programa informático según las realizaciones de esta solicitud. Debe entenderse que las instrucciones del programa informático pueden usarse para implementar cada proceso y/o cada bloque en los diagramas de flujo y/o los diagramas de bloques, y una combinación de un proceso y/o un bloque en los diagramas de flujo y/o los diagramas de bloques. Estas instrucciones de programas informáticos pueden proporcionarse para un ordenador de propósito general, un ordenador dedicada, un procesador integrado o un procesador de cualquier otro dispositivo programable de procesamiento de datos para generar una máquina, de modo que las instrucciones ejecutadas por un ordenador o un procesador de cualquier otro dispositivo de procesamiento de datos programable genera un aparato para implementar una función específica en uno o más procesos en los diagramas de flujo y/o en uno o más bloques en los diagramas de bloques.

Estas instrucciones de programas informáticos pueden almacenarse en una memoria legible por ordenador que puede instruir al ordenador o cualquier otro dispositivo de procesamiento de datos programable para que funcione de una manera específica, de modo que las instrucciones almacenadas en la memoria legible por ordenador generen un artefacto que incluye un aparato de instrucción. El aparato de instrucción implementa una función específica en uno o más procesos en los diagramas de flujo y/o en uno o más bloques en los diagramas de bloques. Estas instrucciones de programas informáticos también pueden cargarse en un ordenador u otro dispositivo de procesamiento de datos programable, de modo que se realice una serie de operaciones y pasos en el ordenador o en el otro dispositivo programable, generando así un procesamiento implementado por ordenador . Por lo tanto, las instrucciones ejecutadas en el ordenador u otro dispositivo programable proporcionan pasos para implementar una función específica en uno o más procesos en los diagramas de flujo y/o en uno o más bloques en los diagramas de bloques.

REIVINDICACIONES

1. Un método para controlar de forma segura un dispositivo doméstico inteligente, en el que el método comprende:

mostrar (S101), mediante un dispositivo terminal inteligente, al menos una indicación de operación para un dispositivo doméstico inteligente cuando el dispositivo terminal inteligente recibe una instrucción de operación ingresada por un usuario para agregar el dispositivo doméstico inteligente a una red o para realizar una configuración de red en el dispositivo doméstico inteligente, en el que la indicación de operación se usa para indicar al usuario que realice el control de funciones en el dispositivo doméstico inteligente, en el que realizar el control de funciones en el dispositivo doméstico inteligente comprende o consiste en introducir una instrucción de control de funciones en el dispositivo doméstico inteligente; y

generar (S102), por parte del dispositivo terminal inteligente al determinar una indicación de operación seleccionada por el usuario de al menos una indicación de operación, una primera clave basada en la indicación de operación seleccionada, donde la primera clave es utilizada por el dispositivo terminal inteligente para cifrar información que se enviará al dispositivo doméstico inteligente.

2. El método según la reivindicación 1, en el que después de haberse mostrado (S101), por parte de un dispositivo terminal inteligente, al menos una indicación de operación para un dispositivo doméstico inteligente cuando el dispositivo terminal inteligente recibe una instrucción de operación ingresada por un usuario para agregar el dispositivo doméstico inteligente a una red o para realizar una configuración de red en el dispositivo doméstico inteligente, el método comprende además:

recibir, por el dispositivo terminal inteligente, la indicación de operación seleccionada por el usuario de la al menos una indicación de operación.

3. El método según la reivindicación 1, en el que después de la generación (S102), por parte del dispositivo terminal inteligente al determinar una indicación de operación seleccionada por el usuario de al menos una indicación de operación, una primera clave basada en la indicación de operación seleccionada, el método además comprende:

generar, por parte del dispositivo terminal inteligente, una segunda clave basada en la primera clave, en donde la segunda clave es utilizada por el dispositivo terminal inteligente para cifrar la información que se va a enviar al dispositivo doméstico inteligente.

4. El método según la reivindicación 1, en el que después de la generación (S102), por parte del dispositivo terminal inteligente al determinar una indicación de operación seleccionada por el usuario de al menos una indicación de operación, una primera clave basada en la indicación de operación seleccionada, el método además comprende:

cifrar, mediante el dispositivo terminal inteligente mediante el uso de la primera clave, información de autenticación para controlar el dispositivo terminal inteligente para acceder a una red Wi-Fi, y enviar información de autenticación cifrada de la red Wi-Fi al dispositivo doméstico inteligente, en el que la información de autenticación comprende al menos uno de un nombre, una contraseña o un certificado de la red Wi-Fi.

5. El método según cualquiera de las reivindicaciones 1-4, en el que la indicación de operación se determina en base a un tipo de dispositivo doméstico inteligente.

6. Un método para controlar de forma segura un dispositivo doméstico inteligente, en el que el método comprende:

recibir (S301), mediante un dispositivo doméstico inteligente, una instrucción de control de función activada por un usuario, en el que el usuario ingresa la instrucción de control de función en base a al menos una indicación de operación mostrada en un dispositivo terminal inteligente, y se usa la indicación de operación para indicar al usuario que realice el control de funciones en el dispositivo doméstico inteligente; y

generar (S302), por parte del dispositivo doméstico inteligente, una primera clave basada en la instrucción de control de función, donde la primera clave se utiliza para descifrar información cifrada enviada por el dispositivo terminal inteligente al dispositivo doméstico inteligente.

7. El método según la reivindicación 6, en el que después de generar (S302), por parte del dispositivo doméstico inteligente, una primera clave basada en la instrucción de control de función, el método comprende además:

generar, por parte del dispositivo terminal inteligente, una segunda clave basada en la primera clave, donde la segunda clave se usa para descifrar la información cifrada enviada por el dispositivo terminal inteligente al dispositivo doméstico inteligente.

8. El método según la reivindicación 6, en el que después de generar (S302), por parte del dispositivo doméstico inteligente, una primera clave basada en la instrucción de control de funciones, el método comprende además:

recibir, por parte del dispositivo doméstico inteligente, información de autenticación cifrada que es de una red Wi-Fi y enviada por el dispositivo terminal inteligente, y descifrar la información de autenticación cifrada de la red

Wi-Fi usando la primera clave, para obtener información de autenticación descifrada de la red Wi-Fi, en el que la información de autenticación comprende al menos uno de un nombre, una contraseña o un certificado de la red Wi-Fi; y

acceder, mediante el dispositivo doméstico inteligente, a la red Wi-Fi correspondiente utilizando la información de autenticación descifrada de la red Wi-Fi.

9. Un dispositivo terminal inteligente, en el que el dispositivo terminal inteligente comprende:

un módulo (501) de pantalla, configurado para mostrar al menos una indicación de operación para un dispositivo doméstico inteligente cuando el dispositivo terminal inteligente recibe una instrucción de operación ingresada por un usuario para agregar el dispositivo doméstico inteligente a una red o para realizar una configuración de red en el dispositivo doméstico inteligente, en el que la indicación de operación se utiliza para instruir al usuario para que realice el control de funciones en el dispositivo doméstico inteligente, en el que realizar el control de función en el dispositivo doméstico inteligente comprende o consiste en introducir una instrucción de control de función en el dispositivo doméstico inteligente; y

un módulo (502) de procesamiento, configurado para generar, cuando se determina una indicación de operación seleccionada por el usuario de al menos una indicación de operación, una primera clave basada en la indicación de operación seleccionada, donde la primera clave es utilizada por el dispositivo terminal inteligente para cifrar la información que se enviará al dispositivo doméstico inteligente.

10. El dispositivo terminal inteligente según la reivindicación 9, en el que el módulo (502) de procesamiento está configurado además para:

recibir la indicación de operación seleccionada por el usuario de la al menos una indicación de operación.

11. El dispositivo terminal inteligente según la reivindicación 9 o 10, en el que el módulo (502) de procesamiento está configurado además para:

generar una segunda clave basada en la primera clave, en el que la segunda clave es utilizada por el dispositivo terminal inteligente para cifrar la información que se va a enviar al dispositivo doméstico inteligente.

12. Dispositivo terminal inteligente según cualquiera de las reivindicaciones 9 a 11, en el que el dispositivo terminal inteligente comprende además:

un módulo de envío, configurado para: cifrar, utilizando la primera clave, información de autenticación para controlar el dispositivo terminal inteligente para acceder a una red Wi-Fi, y enviar información de autenticación cifrada de la red Wi-Fi al dispositivo doméstico inteligente, en el que la información de autenticación comprende al menos uno de un nombre, una contraseña o un certificado de la red Wi-Fi.

13. Un dispositivo doméstico inteligente, en el que el dispositivo doméstico inteligente comprende:

un módulo (601) receptor, configurado para recibir una instrucción de control de función activada por un usuario, en el que el usuario ingresa la instrucción de control de función en función de al menos una indicación de operación que se muestra en un dispositivo terminal inteligente, y la indicación de operación se usa para instruir al usuario para que realice el control de funciones en el dispositivo doméstico inteligente; y

un módulo (602) de generación, configurado para generar una primera clave basada en la instrucción de control de funciones, donde la primera clave se usa para descifrar información cifrada enviada por el dispositivo terminal inteligente al dispositivo doméstico inteligente.

14. El dispositivo doméstico inteligente según la reivindicación 13, en el que el módulo de procesamiento está configurado además para:

generar una segunda clave basada en la primera clave, en el que la segunda clave se utiliza para descifrar la información cifrada enviada por el dispositivo terminal inteligente al dispositivo doméstico inteligente.

15. El dispositivo doméstico inteligente según la reivindicación 13 o 14, en el que el dispositivo doméstico inteligente comprende además:

un módulo de procesamiento, configurado para: recibir información de autenticación cifrada que es de una red Wi-Fi y enviada por el dispositivo terminal inteligente, y descifrar la información de autenticación cifrada de la red Wi-Fi usando la primera clave, para obtener información de autenticación descifrada de la red Wi-Fi, donde la información de autenticación comprende al menos uno de un nombre, una contraseña o un certificado de la red Wi-Fi, donde

el módulo de procesamiento se configura además para acceder a la red Wi-Fi correspondiente utilizando la información de autenticación descifrada de la red Wi-Fi.

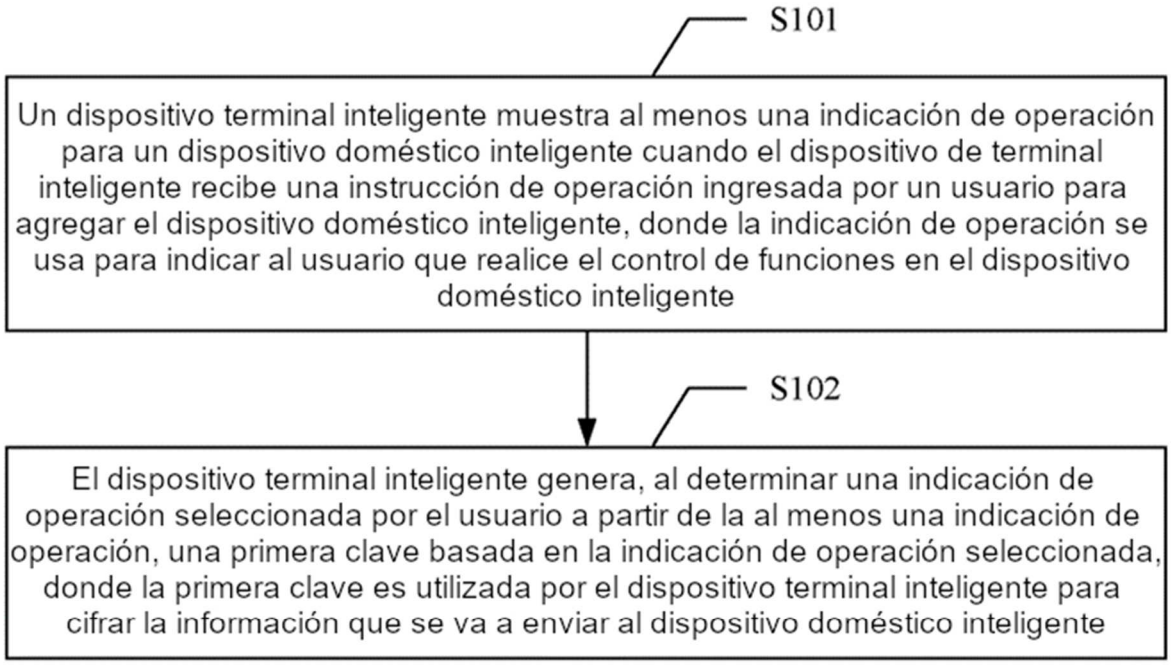
S101
Un dispositivo terminal inteligente muestra al menos una indicación de operación para un dispositivo doméstico inteligente cuando el dispositivo de terminal inteligente recibe una instrucción de operación ingresada por un usuario para agregar el dispositivo doméstico inteligente, donde la indicación de operación se usa para indicar al usuario que realice el control de funciones en el dispositivo doméstico inteligente
S102
El dispositivo terminal inteligente genera, al determinar una indicación de operación seleccionada por el usuario a partir de la al menos una indicación de operación, una primera clave basada en la indicación de operación seleccionada, donde la primera clave es utilizada por el dispositivo terminal inteligente para cifrar la información que se va a enviar al dispositivo doméstico inteligente

FIG. 1

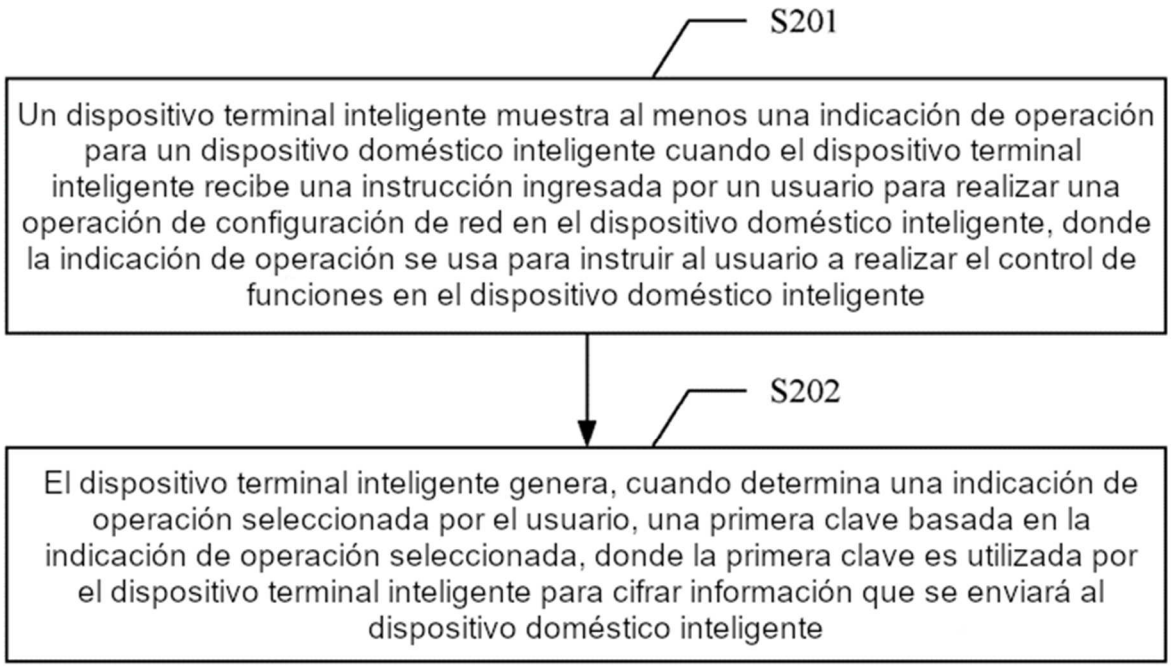
S201
Un dispositivo terminal inteligente muestra al menos una indicación de operación para un dispositivo doméstico inteligente cuando el dispositivo terminal inteligente recibe una instrucción ingresada por un usuario para realizar una operación de configuración de red en el dispositivo doméstico inteligente, donde la indicación de operación se usa para instruir al usuario a realizar el control de funciones en el dispositivo doméstico inteligente
S202
El dispositivo terminal inteligente genera, cuando determina una indicación de operación seleccionada por el usuario, una primera clave basada en la indicación de operación seleccionada, donde la primera clave es utilizada por el dispositivo terminal inteligente para cifrar información que se enviará al dispositivo doméstico inteligente

FIG. 2

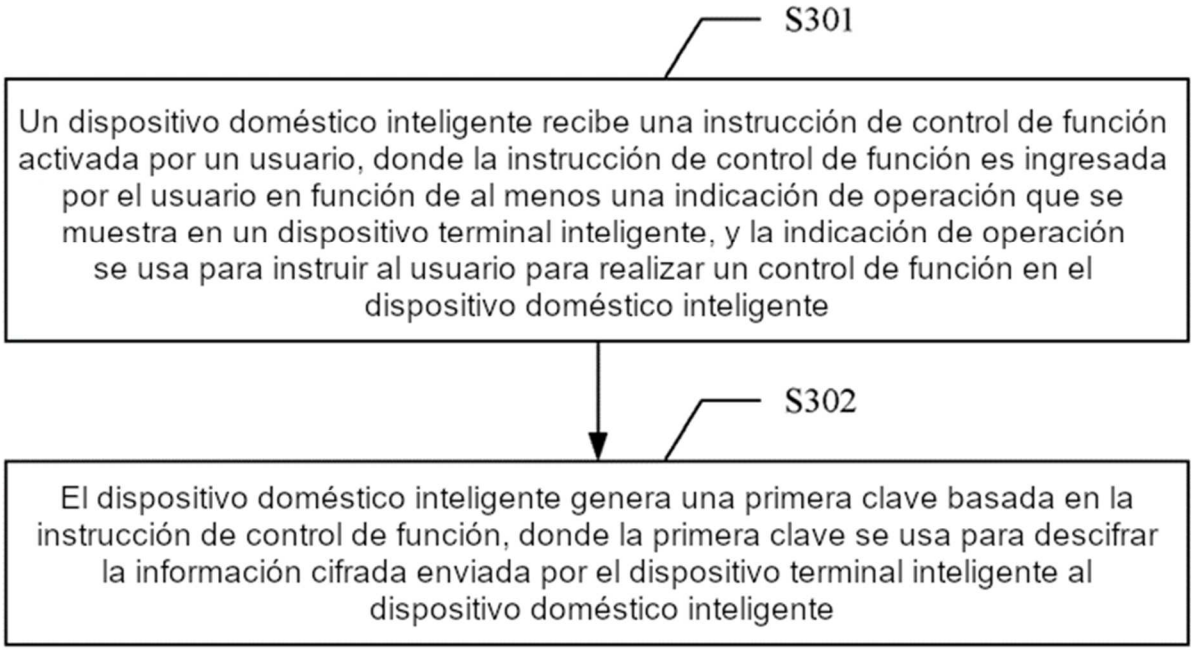
S301
Un dispositivo doméstico inteligente recibe una instrucción de control de función activada por un usuario, donde la instrucción de control de función es ingresada por el usuario en función de al menos una indicación de operación que se muestra en un dispositivo terminal inteligente, y la indicación de operación se usa para instruir al usuario para realizar un control de función en el dispositivo doméstico inteligente
S302
El dispositivo doméstico inteligente genera una primera clave basada en la instrucción de control de función, donde la primera clave se usa para descifrar la información cifrada enviada por el dispositivo terminal inteligente al dispositivo doméstico inteligente

FIG. 3

SIGUE EN
FIG. 4B

FIG. 4A

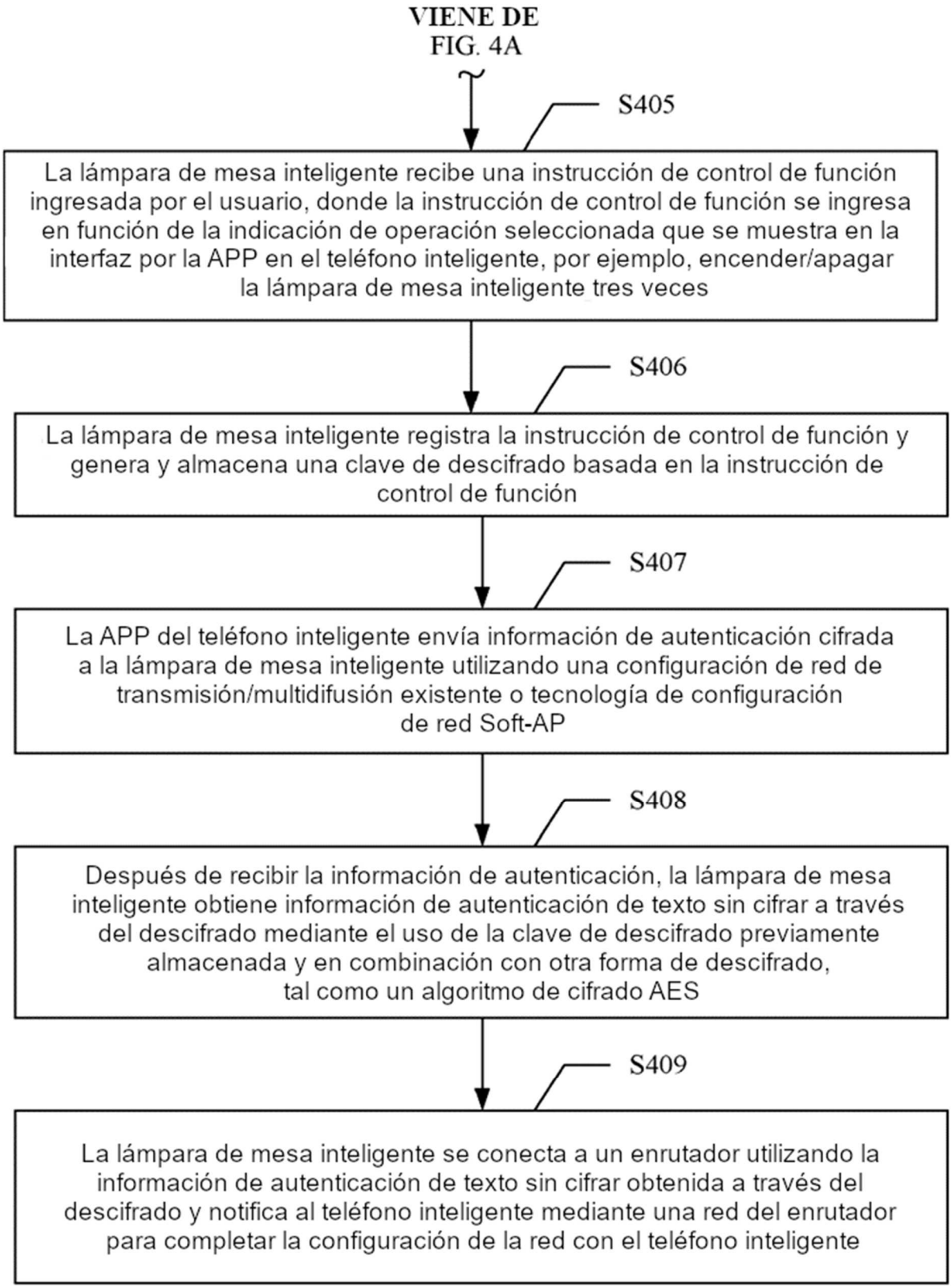
VIENE DE
FIG. 4A
S405
La lámpara de mesa inteligente recibe una instrucción de control de función ingresada por el usuario, donde la instrucción de control de función se ingresa en función de la indicación de operación seleccionada que se muestra en la interfaz por la APP en el teléfono inteligente, por ejemplo, encender/apagar la lámpara de mesa inteligente tres veces
S406
La lámpara de mesa inteligente registra la instrucción de control de función y genera y almacena una clave de descifrado basada en la instrucción de control de función
S407
La APP del teléfono inteligente envía información de autenticación cifrada a la lámpara de mesa inteligente utilizando una configuración de red de transmisión/multidifusión existente o tecnología de configuración de red Soft-AP
S408
Después de recibir la información de autenticación, la lámpara de mesa inteligente obtiene información de autenticación de texto sin cifrar a través del descifrado mediante el uso de la clave de descifrado previamente almacenada y en combinación con otra forma de descifrado, tal como un algoritmo de cifrado AES
S409
La lámpara de mesa inteligente se conecta a un enrutador utilizando la información de autenticación de texto sin cifrar obtenida a través del descifrado y notifica al teléfono inteligente mediante una red del enrutador para completar la configuración de la red con el teléfono inteligente

FIG. 4B

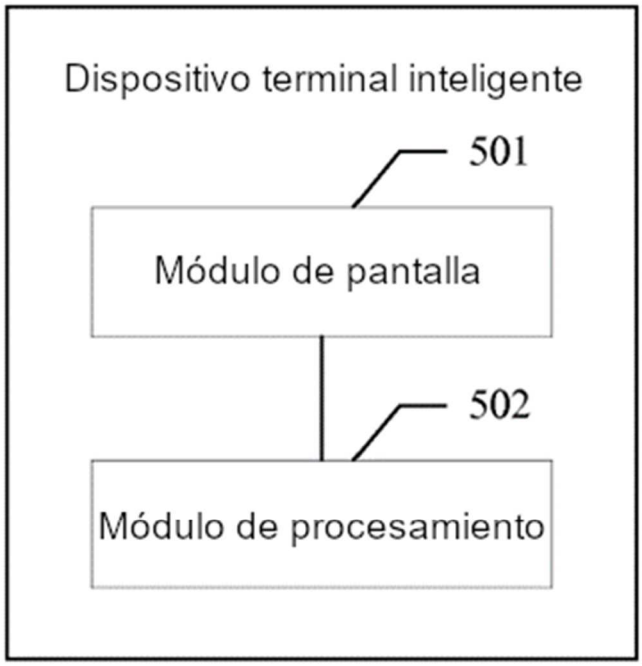
Dispositivo terminal inteligente
501
Módulo de pantalla
502
Módulo de procesamiento

FIG. 5

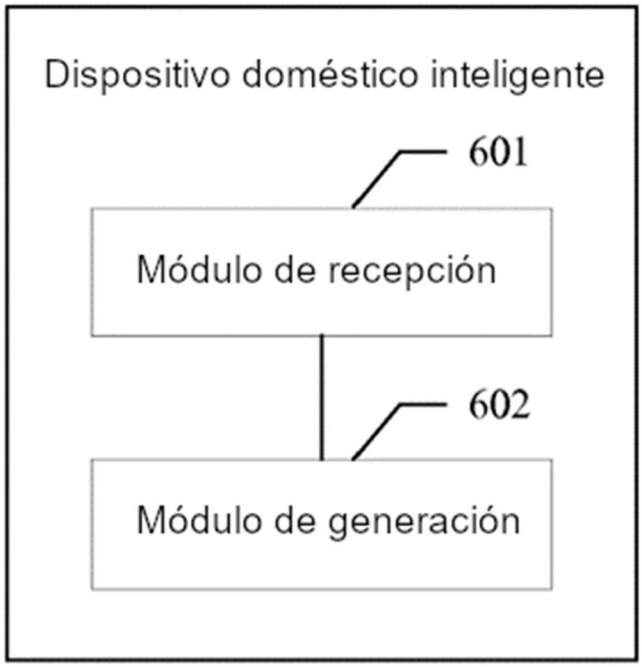
Dispositivo doméstico inteligente
601
Módulo de recepción
602
Módulo de generación

FIG. 6

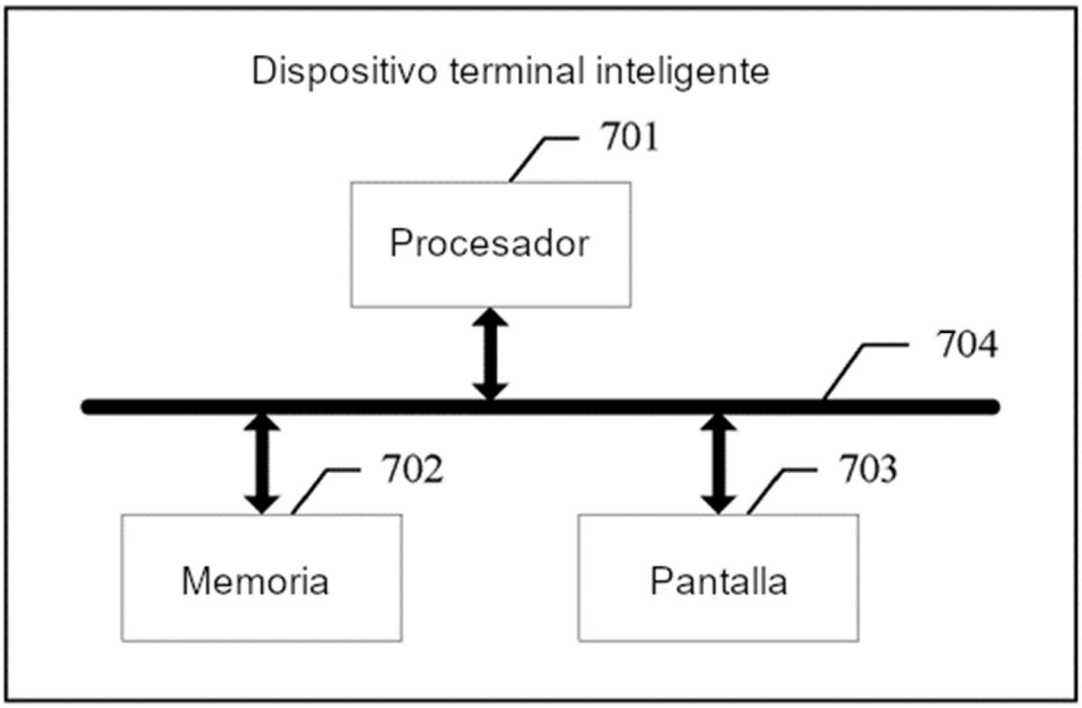
Dispositivo terminal inteligente
701
Procesador
704
702
703
Memoria
Pantalla

FIG. 7

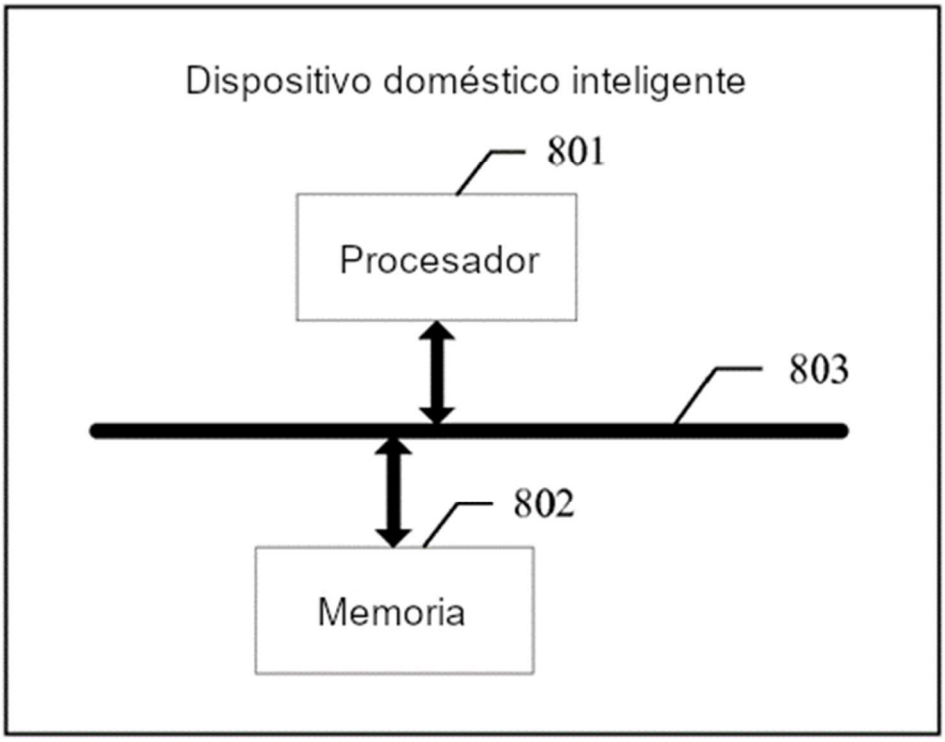
Dispositivo doméstico inteligente
801
Procesador
803
802
Memoria

FIG. 8