(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 539 706**

(51) Int. CI.:

H05B 37/02 (2006.01)
H04W 12/06 (2009.01)
H04L 29/06 (2006.01)
H04L 12/28 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **20.12.2011 E 11810680 (6)**

(97) Fecha y número de publicación de la concesión europea: **06.05.2015 EP 2659740**

(54) Título: **Un sistema de iluminación, una fuente luminosa, un dispositivo y un procedimiento de autorización del dispositivo por la fuente luminosa**

(30) Prioridad:

30.12.2010 EP 10197344

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
03.07.2015

(73) Titular/es:

KONINKLIJKE PHILIPS N.V. (100.0%)
High Tech Campus 5
5656 AE Eindhoven, NL

(72) Inventor/es:

GARCIA MORCHON, OSCAR y
DENTENEER, THEODORUS JACOBUS JOHANNES

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Un sistema de iluminación, una fuente luminosa, un dispositivo y un procedimiento de autorización del dispositivo por la fuente luminosa

CAMPO DE LA INVENCIÓN

La invención se refiere al campo de los sistemas de luz codificada. En tales sistemas la fuente luminosa transmite, en uso, información por medio de la luz que se emite por la fuente luminosa, de tal modo que los humanos no pueden percibir la codificación de la información en la luz, mientras que otros dispositivos, tales como un controlador remoto, son capaces de extraer la información de la luz emitida. La información es, por ejemplo, un identificador de la fuente luminosa. El otro dispositivo puede apuntar a la fuente luminosa en funcionamiento, recibe la luz emitida sobre un sensor fotosensible y es capaz de extraer la información de la señal generada por el sensor. La información extraída puede comprender el identificador de la fuente luminosa, que se puede utilizar para dirigir la fuente luminosa cuando se envían de vuelta mensajes de control a la fuente luminosa para controlar el funcionamiento de la fuente luminosa. Los mensajes de control se envían frecuentemente por medio de otro canal de comunicación, por ejemplo, por medio de luz infrarroja o por medio de señales de radio. La fuente luminosa puede recibir los mensajes de control y utiliza el identificador que es parte del mensaje de control para determinar si el mensaje de control está dirigido a la fuente luminosa. Si es así, se ejecuta el comando de control del mensaje de control por la fuente luminosa. Mediante el uso de este mecanismo, un usuario puede controlar simplemente una fuente luminosa apuntando un controlador remoto a una fuente luminosa y requiriendo un efecto de luz específico. Se debe apreciar que el otro dispositivo puede ser otra fuente luminosa que recibe luz de la primera fuente luminosa, y por medio de este mecanismo la otra fuente luminosa puede controlar la fuente luminosa.

ANTECEDENTES DE LA INVENCIÓN

La solicitud de patente publicada WO2008/139360A1 da a conocer un procedimiento y un sistema para controlar un sistema de iluminación. Un controlador remoto se utiliza para medir la influencia de una o más fuentes luminosas en diferentes posiciones, por ejemplo, en una oficina. Estas mediciones se almacenan en un controlador central y se utilizan para controlar, posteriormente, la emisión de luz de las fuentes luminosas del sistema de iluminación para obtener un patrón de iluminación específico en la oficina. En un modo de realización, las fuentes luminosas del sistema de iluminación pueden transmitir su identificador (ID) de fuente luminosa codificado en la luz que se emite por la fuente luminosa. El controlador remoto es capaz de extraer el ID de la fuente luminosa a partir de la luz recibida, y el controlador remoto caracteriza otros elementos de la luz recibida. La información obtenida se transmite al controlador central para su almacenamiento en el controlador central y para su uso posterior cuando el controlador central tiene que controlar el sistema de iluminación para obtener el patrón de iluminación específico.

El controlador remoto puede enviar una petición de usuario al controlador central para tener un patrón de luz específico en una ubicación específica. El controlador central puede controlar subsiguientemente las fuentes luminosas del sistema de iluminación y el control se basa en las mediciones obtenidas previamente.

En un modo de realización, el controlador remoto es capaz de comunicarse directamente con las fuentes luminosas del sistema de iluminación para controlar directamente las fuentes luminosas. Así pues, además de controlar las fuentes luminosas por medio del controlador central, el sistema de iluminación de la solicitud de patente citada comprende asimismo un subsistema tradicional de luz codificada en el que el controlador remoto es capaz de controlar directamente una o más de las fuentes luminosas.

En el subsistema de luz codificada discutido, y en los sistemas de luz codificada tradicionales, existe un elevado riesgo de que se confundan controladores remotos. Si están presentes diferentes controladores remotos en la misma habitación, cada uno de los controladores remotos puede recibir la información de la fuente luminosa y puede proporcionar comandos de control a la fuente luminosa de la cual se recibe el identificador de fuente luminosa. Por ejemplo, si el sistema de la solicitud de patente citada se utiliza en una oficina, puede estar presente un controlador remoto en cada una de las mesas para controlar la luz en las mesas respectivas. Estos controladores remotos pueden utilizarse asimismo para recibir información de cada una de las fuentes luminosas del sistema de iluminación y como tal los controladores remotos se pueden utilizar para controlar cada una de las fuentes luminosas. Sin embargo, esto no es deseable, por ejemplo, en la oficina ya que cada empleado puede desear un ajuste distinto en su mesa.

La publicación de patente WO2009/031112 (Philips) da a conocer un controlador inalámbrico en una red de luces, en el que el controlador se autentica utilizando una función criptográfica.

RESUMEN DE LA INVENCIÓN

Es un objeto de la invención proporcionar un sistema de iluminación codificada que evita la confusión de distintos controladores remotos.

Un primer aspecto de la invención proporciona un sistema de iluminación como se reivindica en la reivindicación 1. Un segundo aspecto de la invención proporciona una fuente luminosa como se reivindica en la reivindicación 13. Un tercer aspecto de la invención proporciona un dispositivo como se reivindica en la reivindicación 14. Un cuarto aspecto de la invención proporciona un procedimiento como se reivindica en la reivindicación 15. Modos de realización ventajosos se definen en las reivindicaciones dependientes.

Un sistema de iluminación de acuerdo con el primer aspecto de la invención comprende una fuente luminosa para emitir luz, un dispositivo para controlar la fuente luminosa, un primer canal de comunicación de la fuente luminosa al dispositivo, y un segundo canal de comunicación del dispositivo a la fuente luminosa. El primer canal de comunicación se forma modulando información en la luz emitida de la fuente luminosa. La fuente luminosa comprende un generador de señales de identificación, un transmisor de la fuente luminosa, un receptor de la fuente luminosa y unos medios de autorización. El generador de señales de identificación genera una señal de identificación con una función criptográfica que recibe un argumento que comprende una primera llave criptográfica. El transmisor de la fuente luminosa transmite la señal de identificación por medio del primer canal de comunicación. El receptor de la fuente luminosa recibe una respuesta del dispositivo a través del segundo canal de comunicación. Los medios de autorización autorizan que el dispositivo controle la fuente luminosa comparando la respuesta recibida con una referencia, y si la respuesta recibida concuerda con la referencia, el dispositivo es autorizado. El dispositivo comprende un receptor del dispositivo, un generador de respuestas y un transmisor del dispositivo. El receptor del dispositivo recibe la señal de identificación a través del primer canal de comunicación. El generador de respuestas genera la respuesta con la función criptográfica que recibe argumentos que comprenden la señal de identificación recibida y una segunda llave criptográfica. El transmisor del dispositivo transmite la respuesta a la fuente luminosa a través del segundo canal de comunicación.

La solución de la invención para resolver el problema de la confusión de dispositivos es proporcionar llaves criptográficas y una función criptográfica en la fuente luminosa y en los dispositivos tales que la señal de identificación que se genera por la fuente luminosa depende de la primera llave criptográfica, y tal que la respuesta que se genera por el dispositivo depende de la señal de identificación recibida y de la segunda llave criptográfica. La fuente luminosa espera una respuesta específica, que es la referencia, y esta expectativa se basa en el uso de una combinación correcta de la primera llave criptográfica y de la segunda llave criptográfica. Por ejemplo, en un sistema criptográfico simétrico, la primera llave criptográfica y la segunda llave criptográfica tienen que ser la misma para permitir que el dispositivo genere una respuesta que se espera por la fuente luminosa. Así pues, el uso de llaves criptográficas proporciona un mecanismo que se puede utilizar para acoplar un dispositivo específico a fuentes luminosas específicas. La fuente luminosa solo permitirá que el dispositivo controle la fuente luminosa si el dispositivo puede generar la respuesta correcta, dicho de otro modo, si el dispositivo tiene la segunda llave criptográfica correcta. Por ejemplo, programando combinaciones específicas de llaves criptográficas en las fuentes luminosas y en los dispositivos de un sistema de iluminación, se evita la confusión de dispositivos.

Tradicionalmente, en el campo de los sistemas de iluminación, solo había disponible por habitación una, o unas pocas, luminaria(s) y no se reconocía el problema de la confusión de dispositivos. Tradicionalmente solo los dispositivos de una marca se podían comunicar con la fuente luminosa de la misma marca basándose en protocolos de comunicación específicos de las marcas. En el campo de sistemas de iluminación codificada se está elaborando una norma y como tal, dispositivos de una marca específica pueden controlar fuentes luminosas de otras marcas. Así pues, el riesgo de confusión de dispositivos se vuelve un problema más relevante. Además, en la actualidad muchos sistemas de iluminación utilizan emisores de luz en miniatura y como tales el número de fuentes luminosas en un sistema de iluminación aumenta, lo que puede dar como resultado, de nuevo, un problema de confusión mayor. Basándose en el reconocimiento de que el uso de la señal de identificación y la respuesta, que se generan con una función criptográfica que tiene una llave criptográfica como uno de los argumentos, puede resolver el problema de confusión, los inventores han llegado a la conclusión que tal mecanismo se puede implementar en la fuente luminosa y en el dispositivo de un sistema de iluminación codificado. Se debe apreciar que la señal de identificación debe tener un número suficiente de dígitos para evitar el conflicto entre diferentes señales de identificación generadas por diferentes fuentes luminosas. La función criptográfica debe ser una función que genere tales señales de identificación distintivas. Además, la función criptográfica puede ser una función de codificación, una función hash o una función basada en cifrado.

La respuesta y la referencia son concordantes si la semejanza entre la referencia y la respuesta es lo suficientemente alta. En un modo de realización, ser concordante significa que la respuesta y la referencia son iguales. En otro modo de realización la respuesta y la referencia son concordantes si son iguales más de un número predefinido de dígitos de los dos números. En aún otro modo de realización adicional, la referencia y la respuesta son concordantes si la diferencia entre los dos valores se encuentra por debajo de un valor máximo predefinido.

Autorizar significa, en el contexto de la invención, que el dispositivo autorizado tiene una llave criptográfica correcta y que el dispositivo puede controlar la fuente luminosa. No significa que el dispositivo esté autenticado. Dicho de otro modo, como resultado de la autorización la fuente luminosa sabe que un comando de control que se envía junto con la respuesta tiene que ser ejecutado, o que comandos de control, que se enviarán a la fuente luminosa en un intervalo de tiempo tras el momento de autorización, tienen que ser ejecutados para controlar la emisión de luz por el

emisor de luz de la fuente luminosa. Sin embargo, la fuente luminosa no sabe exactamente qué dispositivo específico es el dispositivo autorizado.

El dispositivo del sistema de iluminación puede ser cualquier dispositivo que se configura para recibir la luz de la fuente luminosa, deducir información de la luz, y que se configura para transmitir esa información de nuevo a la fuente luminosa a través de un segundo canal de comunicación. Así pues, todo dispositivo que se configura para controlar la fuente luminosa puede ser el dispositivo del sistema de iluminación. Opcionalmente, el dispositivo puede ser otra fuente luminosa que es un maestro en el sistema de iluminación, lo que significa que esta otra fuente luminosa controla el funcionamiento de la fuente luminosa del sistema de iluminación. En un modo de realización, el dispositivo es un controlador remoto para controlar la fuente luminosa.

Se debe apreciar que la solicitud de patente WO2008/139360A1 citada discute la posibilidad de un mal uso del sistema de iluminación descrito en la misma, y discute una posible solución. Se ha propuesto proporcionar un mecanismo de control de acceso para el dispositivo por el controlador central del sistema de iluminación con criptografía de llave pública o criptografía de llave simétrica. Así pues, la solicitud de patente citada apunta a una solución que comprende la introducción de un controlador central. Tal solución es diferente de la solución de la invención y es relativamente costosa.

En un modo de realización, la fuente luminosa comprende un identificador de fuente luminosa único pre-programado y el generador de señales de identificación se configura para utilizar el identificador de fuente luminosa único como un argumento adicional para la función criptográfica. Así pues, la señal de identificación generada depende igualmente de un número único y por tanto la señal de identificación generada es única y no entra en conflicto con señales de identificación de otras fuentes luminosas. Esto es especialmente ventajoso cuando se utilizan varias fuentes luminosas en la misma área y cuando el dispositivo tiene que recibir una señal de identificación única para evitar que señales de identificación de distintas fuentes luminosas sean confundidas por el dispositivo. Si el experto en la técnica desea tener una señal de identificación única parece lógico generar un número aleatorio con un número suficiente de dígitos de tal modo que la probabilidad de generar la misma señal de identificación por distintas fuentes luminosas sea baja. Sin embargo, para generar un número aleatorio, relativamente grande, y por tanto costoso, hay que incluir bloques de elementos físicos en las fuentes luminosas, lo que da como resultado fuentes luminosas relativamente costosas. Utilizando un identificador único, que por ejemplo se pre-programa en la fuente luminosa en el momento de producción de la fuente luminosa, o que por ejemplo se programa en la fuente luminosa cuando se instala la fuente luminosa, se evita el uso de tal generador de números aleatorios costoso en cada una de las fuentes luminosas. Así pues, la solución del modo de realización es una solución relativamente barata para evitar la generación de señales de identificación en conflicto. Se debe indicar que el identificador de fuente luminosa es un número con una cantidad suficiente de dígitos para tener suficientes identificadores de fuente luminosa únicos disponibles.

En un modo de realización adicional, el primer canal de comunicación es un canal de transmisión unidireccional. Dicho de otro modo, la información que se transmite a través del primer canal de comunicación se transmite desde la fuente luminosa y puede ser recibida por una pluralidad de receptores que son capaces de recibir la información de transmisión. Se debe apreciar que la transmisión no es por definición en todas direcciones, sino que puede estar dirigida asimismo a un área específica: la luz que se emite por la fuente luminosa se emite hacia un área específica y todos los dispositivos presentes en el haz de luz pueden recibir información a través de la luz emitida. Nótese que los dispositivos pueden recibir la información tras una reflexión de la luz por un objeto, tal como una pared o suelo.

En un modo de realización adicional, el transmisor de la fuente luminosa se configura para transmitir regularmente un identificador a través del primer canal de comunicación y en el que el transmisor de la fuente luminosa se configura además para transmitir regularmente la señal de identificación generada como el identificador. Así pues, dicho de otro modo, no se transmite ningún identificador de fuente luminosa, sino que se transmite la señal de identificación generada. Esto proporciona una ventaja de privacidad, ya que, si otro dispositivo intenta infiltrarse en el sistema de iluminación, ese dispositivo no puede detectar basándose en la información en la luz emitida desde qué fuente luminosa específica se origina la información.

En otro modo de realización, el transmisor de la fuente luminosa se configura para transmitir regularmente la respuesta en lugar de la señal de identificación y el dispositivo está autorizado por la fuente luminosa. Al comenzar a transmitir la respuesta en lugar de la señal de identificación, el dispositivo puede detectar en la luz recibida que la información comprendida en la luz emitida es igual a la respuesta que se envió previamente. Esto es una forma de realimentación y por tanto el dispositivo sabe que está autorizado por la fuente luminosa y por tanto el dispositivo conoce que puede controlar la fuente luminosa.

En un modo de realización, el transmisor del dispositivo transmite un mensaje a través del segundo canal de comunicación. El mensaje comprende un identificador de la fuente luminosa. El transmisor del dispositivo se configura para utilizar la respuesta generada como el identificador en el mensaje. Dicho de otro modo, no se utiliza ningún identificador de fuente luminosa para dirigir la fuente luminosa, sino que se utiliza la respuesta como el identificador. Esto da como resultado un beneficio adicional desde el punto de vista de protección de la privacidad: dispositivos capaces de recibir los mensajes del segundo canal de comunicación no son capaces de detectar qué

fuentes luminosas están controladas por el dispositivo. Especialmente, si esto se utiliza en combinación con el modo de realización anterior, en el que el transmisor de la fuente luminosa transmite la señal de identificación en lugar del identificador, la fuente luminosa transmite un primer pseudo identificador, y el dispositivo transmite un segundo pseudo identificador. Así pues, es imposible para otros dispositivos, que intentan atacar el sistema, detectar qué fuente luminosa específica emitió el primer pseudo identificador y es imposible para los otros dispositivos detectar a qué fuente luminosa específica se dirige el mensaje. Se debe apreciar que, cuando se utilizan pseudo identificadores, puede ser más difícil que la fuente luminosa identifique los mensajes recibidos a través del segundo canal de comunicación como un mensaje dirigido a la fuente luminosa. La fuente luminosa puede procesar todos los mensajes y comprobar las respuestas de cada mensaje con la referencia con el fin de superar este problema. Si hay una concordancia lo más probable es que el mensaje estuviera dirigido a la fuente luminosa. Alternativamente, la fuente luminosa puede calcular igualmente la respuesta esperada y filtrar mensajes basándose en la respuesta calculada.

En otro modo de realización, el generador de señales de identificación utiliza una señal de identificación generada anteriormente o una respuesta recibida anteriormente asimismo como un argumento para la función criptográfica. La señal de identificación generada anteriormente y la respuesta recibida anteriormente son números generados anteriormente. Esto significa que, tan pronto como tal número generado anteriormente se utiliza como un argumento, la señal de identificación cambia a otro valor. Así pues, visto en el tiempo, las señales de identificación sucesivas cambian. El cambio de las señales de identificación convierte al sistema de iluminación en más seguro con respecto a ataques al sistema. Aunque los dispositivos atacantes pueden registrar la señal de identificación que se ha emitido por la fuente luminosa y la respuesta del dispositivo subsecuentemente transmitida, los dispositivos atacantes no tienen pistas de qué respuestas se deben enviar tan pronto como cambia la señal de identificación. La fuente luminosa puede tener una memoria para almacenar señales de identificación anteriormente generadas o respuestas anteriormente recibidas, tal que esté disponible un número anterior cuando la fuente luminosa comienza a funcionar tras un periodo de inactividad. Se debe apreciar que, cuando la fuente luminosa se utiliza por primera vez, no se encuentra disponible un número anteriormente generado. Así pues, la fuente luminosa no puede utilizar un número anteriormente generado en su primer uso, pero puede utilizar un número que ha sido pre-almacenado en la memoria durante la fabricación de la fuente luminosa. Tal número pre-almacenado puede ser un número fijo que es el mismo número para toda fuente luminosa, por ejemplo, 0, o puede ser un número aleatorio, que es diferente para diferentes fuentes luminosas.

En un modo de realización, la fuente luminosa puede generar (y transmitir) la misma señal de identificación basándose en un número específico anteriormente generado durante un intervalo de tiempo predefinido. Tras el intervalo predefinido el generador de señales de identificación puede conmutar para utilizar otro número anteriormente generado como un argumento para la función criptográfica. Así pues, en instantes regulares en el tiempo, la fuente luminosa comienza a transmitir otra señal de identificación. En otro modo de realización, la fuente luminosa solo conmuta al uso de otro número anteriormente generado tras el instante en el tiempo en el que el dispositivo fue autorizado.

En un modo de realización, el generador de señales de identificación genera asimismo la referencia con la función criptográfica que recibe argumentos que comprenden la señal de identificación generada y la primera llave criptográfica. Es ventajoso generar la referencia de acuerdo con este modo de realización cuando la fuente luminosa tiene que comprobar si la segunda llave criptográfica es la misma que la primera llave criptográfica: en ese caso la referencia generada es la misma que la respuesta generada.

En un modo de realización adicional, la fuente luminosa comprende un identificador de fuente luminosa único pre-programado, y la fuente luminosa comprende además unos medios de concatenación de la fuente luminosa que concatenan la señal de identificación con el identificador de fuente luminosa. La concatenación del identificador de fuente luminosa y de la señal de identificación es transmitida por el transmisor de la fuente luminosa en lugar de transmitir tan solo la señal de identificación. Así pues, la información que se transmite a través del primer canal de comunicación comprende igualmente el identificador de fuente luminosa, lo que puede ser ventajoso cuando el dispositivo tiene que saber de qué fuente luminosa específica se origina la señal de identificación. Sin embargo, el efecto de privacidad discutido en otro modo de realización no está presente en este modo de realización.

En otro modo de realización, el dispositivo comprende además unos medios de concatenación del dispositivo para concatenar la respuesta generada con la señal de identificación recibida. La concatenación de la señal de identificación y la respuesta es transmitida por el transmisor del dispositivo en lugar de transmitir tan solo la respuesta. Así pues, la fuente luminosa puede detectar en la concatenación recibida que está incluida la señal de identificación que se envió previamente a través del primer canal de comunicación, y, consecuentemente, la fuente luminosa entiende inmediatamente que la información recibida (que comprende la respuesta) se dirige a la fuente luminosa y como tal que tiene que comparar la respuesta con la referencia. Esto evita que la fuente luminosa tenga que comparar cada respuesta del receptor con la referencia ya que queda claro inmediatamente qué concatenaciones recibidas están dirigidas a la frente luminosa.

Si, de acuerdo con el modo de realización anteriormente descrito, el identificador de fuente luminosa se concatena con la señal de identificación, los medios de concatenación del dispositivo pueden concatenar igualmente el

identificador de fuente luminosa con la respuesta generada y/o con la señal de identificación recibida. Si el identificador de fuente luminosa se concatena, es todavía mucho más claro para la fuente luminosa que el mensaje que comprende la concatenación está dirigido a la fuente luminosa. Se debe apreciar que el efecto de privacidad, que ha sido discutido en otro modo de realización, no está presente en este modo de realización.

En un modo de realización, el dispositivo comprende además unos medios de recepción de comandos de control que reciben un comando de control de un usuario para controlar la fuente luminosa. El transmisor del dispositivo transmite el comando de control junto con la respuesta, por ejemplo, en un único mensaje. La fuente luminosa comprende además un controlador de la fuente luminosa que es capaz de ejecutar el comando de control que se recibe junto con la respuesta. El controlador de la fuente luminosa solo ejecuta el comando de control si el dispositivo está autorizado por la fuente luminosa.

El control de la fuente luminosa depende de la autorización del dispositivo por la fuente luminosa. Así pues, se ha proporcionado un mecanismo de acceso seguro que solo permite que dispositivos específicos, que tienen la segunda llave criptográfica correcta, controlen la fuente luminosa. En este modo de realización, el mensaje de control ya se manda con la respuesta a la fuente luminosa y como tal no se tienen que enviar mensajes de control adicionales del dispositivo a la fuente luminosa. Como consecuencia, el modo de realización es relativamente eficiente con respecto al ancho de banda de transmisión.

En otro modo de realización, la fuente luminosa permite la recepción de un comando de control de la fuente luminosa a través del segundo canal de comunicación durante un intervalo de tiempo predefinido tras el instante en el tiempo en el que el dispositivo es autorizado por la fuente luminosa. La fuente luminosa comprende además un controlador de la fuente luminosa para ejecutar el comando de control de la fuente luminosa recibido. Así pues, el controlador de la fuente luminosa controla el funcionamiento de un emisor de luz de la fuente luminosa si se ejecuta el comando de control de la fuente luminosa recibido.

De acuerdo con el modo de realización, la comunicación señal de identificación-respuesta se utiliza para autorizar el dispositivo, y en una comunicación subsiguiente el dispositivo puede enviar comandos de control de la fuente luminosa a la fuente luminosa durante un intervalo de tiempo predefinido. Así pues, tras la autorización hay un intervalo de tiempo durante el cual el dispositivo está autorizado transmitir un comando de control de la fuente luminosa sin ser autorizado de nuevo. Esto no requiere que el dispositivo tenga que recibir la señal de identificación (posiblemente cambiada) de nuevo (al extraer la señal de identificación a partir de la luz emitida por la fuente luminosa) y no tiene que devolver una respuesta, y por tanto el usuario puede mover el dispositivo a otra posición donde la luz emitida por el emisor de luz no caiga en el sensor fotosensible del dispositivo.

El modo de realización puede combinarse con otro modo de realización discutido anteriormente. El dispositivo puede ser informado acerca de la autorización basándose en un modo de realización descrito anteriormente. En el modo de realización descrito anteriormente el emisor de luz comienza a transmitir la respuesta a través del primer canal de comunicación tras la autorización, que es una indicación para el dispositivo de que ha comenzado el intervalo predefinido.

De acuerdo con un segundo aspecto de la invención, se proporciona una fuente luminosa para su uso en el sistema de acuerdo con el primer aspecto de la invención. La fuente luminosa comprende los mismos medios que la fuente luminosa del sistema de acuerdo con la invención.

De acuerdo con un tercer aspecto de la invención, se proporciona un dispositivo para su uso en el sistema de acuerdo con el primer aspecto de la invención. El dispositivo comprende los mismos medios que la fuente luminosa del sistema de acuerdo con la invención.

La fuente luminosa de acuerdo con el segundo aspecto de la invención y el dispositivo de acuerdo con el tercer aspecto de la invención proporcionan las mismas ventajas que el sistema de iluminación de acuerdo con el primer aspecto de la invención y tienen modos de realización similares con efectos similares a los de los modos de realización correspondientes del sistema de iluminación.

En otro modo de realización se proporciona una luminaria que comprende la fuente luminosa de acuerdo con el segundo aspecto de la invención.

De acuerdo con un cuarto aspecto de la invención, un procedimiento de autorización de un dispositivo por una fuente luminosa para permitir al dispositivo controlar la fuente luminosa. El procedimiento comprende las etapas de: i) generar una señal de identificación con una función criptográfica que recibe un argumento que comprende una primera llave criptográfica, ii) transmitir la señal de identificación de la fuente luminosa al dispositivo a través de un primer canal de comunicación que se forma modulando información en la luz emitida de la fuente luminosa, iii) recibir la señal de identificación del primer canal de comunicación, iv) generar una respuesta con la función criptográfica que recibe la señal de identificación recibida y una segunda llave criptográfica como argumentos, v) transmitir la respuesta del dispositivo a la fuente luminosa a través de un segundo canal de comunicación, vi) recibir la respuesta del segundo canal de comunicación, y vii) autorizar el dispositivo comparando el segundo pseudo identificador

recibido con una referencia, y, si el segundo pseudo identificador recibido concuerda con la referencia, el dispositivo es autorizado por la fuente luminosa.

El procedimiento de acuerdo con el cuarto aspecto de la invención proporciona las mismas ventajas del sistema de iluminación de acuerdo con el primer aspecto de la invención y tiene modos de realización similares con efectos similares a los modos de realización correspondientes del sistema de iluminación.

La etapas i), ii), vi) y vii) se realizan mediante la fuente luminosa. Las etapas iii), iv) y v) se realizan mediante el dispositivo.

En un modo de realización se proporciona un producto de programa de ordenador que comprende instrucciones para hacer que un procesador de una fuente luminosa realice las etapas de generar una señal de identificación con una función criptográfica que recibe un argumento que comprende una primera llave criptográfica y autorizar un dispositivo mediante la comparación de un segundo pseudo identificador recibido con una referencia.

En otro modo de realización, se proporciona un producto de programa de ordenador que comprende instrucciones para hacer que un procesador de un dispositivo realice la etapa de generar una respuesta con la función criptográfica que recibe una señal de identificación recibida y una segunda llave criptográfica como argumentos.

Se debe apreciar que la invención no se limita a fuentes luminosas o dispositivos que comprenden tan solo equipo físico de propósito especial, tal como el generador de señales de identificación, el transmisor de la fuente luminosa, el receptor de la fuente luminosa, los medios de autorización, el receptor del dispositivo, el generador de respuestas y/o el transmisor del dispositivo. En un modo de realización, la fuente luminosa y/o el dispositivo pueden tener un procesador de propósito general que se programa para realizar por lo menos una de las tareas de, o al menos parte de las tareas del generador de señales de identificación, el transmisor de la fuente luminosa, el receptor de la fuente luminosa, los medios de autorización, el receptor del dispositivo, el generador de respuestas y/o el transmisor del dispositivo.

Estos y otros aspectos de la invención son aparentes y serán dilucidados con referencia a los modos de realización descritos en lo que sigue.

Se apreciara por parte de los expertos en la técnica que se pueden combinar dos o más de los modos de realización, implementaciones, y/o aspectos de la invención anteriormente mencionados en cualquier forma considerada útil.

Modificaciones y variaciones del sistema, los dispositivos, el procedimiento, y/o el producto de programa de ordenador, que corresponden a las modificaciones y variaciones del sistema descritas, se pueden llevar a cabo por un experto en la técnica basándose en la presente descripción.

BREVE DESCRIPCIÓN DE LAS FIGURAS

En las figuras:

la fig. 1 muestra esquemáticamente un modo de realización del sistema de iluminación de acuerdo con el primer modo de realización de la invención,

la fig. 2 muestra esquemáticamente otro modo de realización del sistema de iluminación,

la fig. 3 muestra esquemáticamente un primer modo de realización de un protocolo que es implementado por el sistema de iluminación o que se realiza mediante el procedimiento de acuerdo con el cuarto aspecto de la invención,

la fig. 4 muestra esquemáticamente un segundo modo de realización del protocolo,

la fig. 5 muestra esquemáticamente un tercer modo de realización del protocolo,

la fig. 6 muestra esquemáticamente un cuarto modo de realización del protocolo, y

la fig. 7 muestra esquemáticamente un modo de realización del procedimiento de acuerdo con el cuarto aspecto de la invención.

Se debe apreciar que elementos denotados mediante los mismos números de referencia en diferentes figuras tienen los mismos elementos estructurales y las mismas funciones, o son las mismas señales. Donde la función y/o estructura de tal elemento se ha explicado, no hay necesidad de una explicación repetida del mismo en la descripción detallada.

Las figuras son meramente esquemáticas y no están dibujadas a escala. Concretamente por claridad algunas dimensiones están fuertemente exageradas.

DESCRIPCIÓN DETALLADA DE LA INVENCIÓN

Un primer modo de realización de un sistema 100 de acuerdo con el primer aspecto de la invención se muestra en la fig. 1. El sistema 100 comprende una fuente luminosa 110 y un controlador remoto 150. El sistema comprende un primer canal de comunicación que se forma mediante información modulada en la luz 116 emitida por la fuente luminosa 110. El sistema 100 comprende además un segundo canal de comunicación que se forma por ondas de radio 160 transmitidas por el controlador remoto 150.

La fuente luminosa 110 comprende un emisor de luz 114 que puede emitir luz 116. Se puede modular información en la luz emitida 116 de tal modo que un humano no pueda percibir la información en la luz emitida 116, mientras que el controlador remoto 150 es capaz de extraer la información de la luz 116. Alternativamente, la información modulada puede ser visible cuando se desea una inspección visual por un humano, por ejemplo, cuando la fuente luminosa y el controlador remoto tienen que realizar un procedimiento de emparejamiento. La fuente luminosa 110 comprende un generador de señales de identificación 118 que genera una señal de identificación con una función criptográfica. La función criptográfica recibe por lo menos una primera llave criptográfica como argumento. La señal de identificación se proporciona al transmisor 112 de la fuente luminosa que transmite la señal de identificación a través del primer canal de comunicación. Dicho de otro modo, el transmisor 112 de la fuente luminosa genera una señal de excitación para el emisor de luz 114. Dependiendo de la señal de excitación, el emisor de luz 114 está en un estado de emisión o de no emisión. La señal de excitación se genera en el transmisor de la fuente luminosa de tal modo que la señal de identificación se codifica en la luz 116.

El controlador remoto 150 comprende un receptor 152 del controlador remoto que comprende un sensor fotosensible para convertir la luz recibida en una señal eléctrica, y que comprende medios para extraer información codificada en la luz. Así pues, el receptor 152 del controlador remoto recibe la señal de identificación codificada en la luz 116. La señal de identificación recibida se suministra a un generador de respuestas 154 del controlador remoto 150. El generador de respuestas genera una respuesta con la función criptográfica que recibe un número de argumento que incluye por lo menos la señal de identificación y una segunda llave criptográfica. La función criptográfica puede ser la misma función criptográfica que la función criptográfica del generador de señales de identificación 118 de la fuente luminosa 110. La respuesta que se genera por el generador de respuestas 154 se suministra a un transmisor 156 del controlador remoto. En un sistema inalámbrico, como el sistema de la fig. 1, el transmisor 156 del controlador remoto impulsa una señal de transmisión a una antena 162 tal que la respuesta se transmite a través del segundo canal de comunicación, utilizando ondas de radio 160, a la fuente luminosa 110. Se debe apreciar que los modos de realización de la invención no se limitan a un segundo canal de comunicación a través de ondas de radio. Se pueden utilizar igualmente otros medios de comunicación, tales como, por ejemplo, luz infrarroja.

La fuente luminosa 110 comprende una antena 124 para recibir las ondas de radio 160 que son emitidas por el controlador remoto 150. Si se utiliza otro medio de comunicación, puede no ser necesaria la antena, pero se tienen que proporcionar otros medios que reciban las señales a través del otro medio de comunicación. La antena 124 está acoplada a un receptor 122 de la fuente luminosa para recibir la respuesta que se transmite a través del segundo canal de comunicación por el controlador remoto 150. La respuesta recibida se suministra a los medios de autorización 120 que pueden autorizar el controlador remoto 150 para que controle la fuente luminosa 110. Los medios de autorización 120 comparan la respuesta recibida con una referencia y si se encuentra una concordancia, el controlador remoto 150 es autorizado por la fuente luminosa 110.

La respuesta y la referencia son concordantes si la semejanza entre la referencia y la respuesta es lo suficientemente alta. En un modo de realización, concordante puede significar que la respuesta y la referencia son iguales. En otro modo de realización, la respuesta y la referencia son concordantes si son iguales más de un número predefinido de dígitos de los dos números. En aún un modo de realización adicional, la referencia y la respuesta son concordantes si la diferencia entre los dos valores se encuentra por debajo de un valor máximo predefinido. La comprobación que se ejecuta para identificar si la respuesta y la referencia son concordantes tiene que estar adaptada al sistema criptográfico que se ha usado. Se puede utilizar, por ejemplo, una función criptográfica que genera señales de identificación y respuestas de las cuales, por ejemplo, los primeros dos dígitos difieren de otras señales de identificación y respuestas generadas cuando las llaves utilizadas difieren en al menos un dígito. En tal sistema se pueden distribuir diferentes llaves a diferentes dispositivos para permitir que los dispositivos con las llaves diferentes controlen una fuente luminosa específica.

En un modo de realización, el generador de señales de identificación genera asimismo la referencia *ref.* La referencia se utiliza cuando se recibe una respuesta y si la respuesta recibida concuerda con la referencia generada, el controlador remoto 150, 250 puede ser autorizado por la fuente luminosa 110, 210.

En un modo de realización, como se muestra en la fig. 1, los medios de autorización se pueden acoplar al generador de señales de identificación 118. Si el controlador remoto 150 es autorizado por los medios de autorización, la

respuesta recibida es suministrada al generador de señales de identificación 118 de tal modo que la respuesta recibida se puede utilizar como uno de los argumentos de la función criptográfica para generar otra señal de identificación. En otro modo de realización, los medios de autorización 120 pueden acoplarse al transmisor de la fuente luminosa para transmitir la respuesta recibida si el controlador remoto 150 es autorizado por la fuente luminosa 110.

En un modo de realización, el controlador remoto 150 puede comprender además unos medios de recepción de comandos de control 158 que se pueden utilizar por un usuario para proporcionar un comando de control para controlar la fuente luminosa 110. El comando de control recibido es suministrado al transmisor del controlador remoto que transmite el comando de control a través del segundo canal de comunicación hacia la fuente luminosa. El controlador remoto 150 puede enviar el comando de control junto con la respuesta en un único mensaje a la fuente luminosa 110, o el comando de control puede ser enviado en un mensaje distinto a la fuente luminosa 110 con la inclusión de la respuesta en el mensaje.

En la fig. 2 se proporciona otro modo de realización de un sistema de iluminación 200. El sistema de iluminación 200 comprende una fuente luminosa 210 y un controlador remoto 250. El sistema comprende además dos canales de comunicación que son similares a los canales de comunicación de sistema 100 de la fig. 1. Así pues, la luz 116 emitida por el emisor de luz 114 de la fuente luminosa 210 comprende información que se codifica de modo invisible en la luz 116, formando así el primer canal de comunicación. El segundo canal de comunicación se forma mediante ondas de radio 116 que se transmiten por el controlador remoto 250 y que se reciben por la fuente luminosa 210. La fuente luminosa 210 comprende un procesador 212 que realiza las tareas del generador de señales de identificación 118, transmisor 112 de la fuente luminosa, el receptor 122 de la fuente luminosa y/o los medios de autorización 120 de la fuente luminosa 110 de la fig. 1. El controlador remoto 250 comprende un procesador 254 que realiza las tareas del generador de respuestas 154 y/o el transmisor 154 del controlador remoto del controlador remoto 150 de la fig. 1. Se debe apreciar que la fuente luminosa 110, 210 y/o el controlador remoto 150, 250 pueden tener ambos un procesador que se programa para realizar todas o tan solo algunas de las tareas de los bloques de elementos físicos de propósito especial 118, 112, 120, 122, 152, 154, 156 y pueden tener todavía algunos de los bloques de elementos físicos de propósito especial 118, 112, 120, 122, 152, 154, 156. Además, los procesadores 212, 254 pueden tener memoria volátil y/o no volátil en la que se almacena información. En la memoria no volátil del procesador 212 de la fuente luminosa 210 se puede almacenar un identificador de la fuente luminosa único (ID) que se puede utilizar igualmente como un argumento de la función criptográfica al generar la señal de identificación. Además, los procesadores 212, 254 se puede configurar para realizar otras tareas como concatenar la señal de identificación (o la respuesta) con el ID de la fuente luminosa. La fuente luminosa 110, 210 y/o el controlador remoto 150, 250 pueden tener asimismo elementos físicos de propósito especial para realizar la concatenación de distintos tipos de información. Además, el procesador 212 de la fuente luminosa 210 se puede utilizar para controlar el funcionamiento como la fuente luminosa de acuerdo con comandos de control que son recibidos del controlador remoto.

El sistema 100 de la fig. 1 y el sistema 200 de la fig. 2 proporcionan medios para ejecutar un protocolo para autorizar el controlador remoto 150, 250 por la fuente luminosa 110, 210. En las figs. 3, 4, 5 y 6 se discuten modos de realización del protocolo.

En la fig. 3 se muestra un protocolo de autorización 300. Las acciones realizadas por la fuente luminosa 110, 210 se presentan en el extremo izquierdo 312 de la figura. El intercambio de información a través de los canales de transmisión se presenta en la parte intermedia 314 de la figura. Si se dibuja una línea de puntos (como la línea 302) en la parte intermedia 314, se utiliza un primer canal de comunicación que utiliza luz que es transmitida por la fuente luminosa 110, 210 como un portador de transmisión. Si se dibuja una línea discontinua (como la línea 304) en la parte intermedia 314, se utiliza un segundo canal de comunicación que utiliza, por ejemplo, ondas de radio o luz infrarroja como un portador de transmisión. Las acciones realizadas en el controlador remoto 150, 250 se presentan en el extremo derecho 316 de la figura. La dirección vertical es la dimensión temporal. Una acción mostrada en la parte superior de la figura se realiza antes que una acción realizada en la parte inferior de la figura.

Como se observa en la fig. 3, la primera acción, que se realizan el instante de tiempo *t1*, es la generación de una señal de identificación ch_{t1}. La señal de identificación ch_{t1} se genera con una función criptográfica *f(...)* y uno de los argumentos de la función criptográfica *f(...)* es la primera llave criptográfica *llave1*. En otros modos de realización, la función criptográfica *f(...)* puede recibir más argumentos. La señal de identificación ch_{t1} generada se transmite de la fuente luminosa 110, 210 al controlador remoto 150, 250 a través del primer canal de comunicación 302. Subsiguientemente, el controlador remoto 150, 250 genera, en un segundo instante de tiempo *t2*, una respuesta rp_{t2} con la función criptográfica *f(...)*. Los argumentos para la función criptográfica son por lo menos la señal de identificación ch_{t1} recibida y una segunda llave criptográfica *llave2*. La respuesta rp_{t2} generada se transmite del controlador remoto 150, 250 a la fuente luminosa 110, 210 a través del segundo canal de comunicación 304. En un tercer instante de tiempo, la fuente luminosa 110, 210 compara la respuesta rp_{t2} recibida con una referencia. Si hay una concordancia, dicho de otro modo, si la semejanza entre la referencia y la respuesta rp_{t2} recibida es lo suficientemente alta, el controlador remoto 150, 250, es autorizado a controlar la fuente luminosa 110, 210.

La señal de identificación ch_{t1} debe ser un número lo suficientemente largo para evitar el conflicto entre diferentes

señales de identificación generadas por diferentes fuentes luminosas. En un modo de realización, la señal de identificación tiene por lo menos 80 bits de largo. En otro modo de realización, la señal de identificación tiene por lo menos 128 bits de largo. Además, la función criptográfica *f(...)* debe ser una función que genere señales de identificación ch_{t1} distintivas si los valores de los argumentos difieren. Dicho de otro modo, la función criptográfica debe tener un carácter distintivo.

En los modos de realización de la fig. 1 y la fig. 2, la fuente luminosa autoriza a un controlador remoto a controlar la fuente luminosa. Sin embargo, el controlador remoto 150, 250 puede ser igualmente otro tipo de dispositivo, por ejemplo, otra fuente luminosa que sea un maestro del sistema de iluminación y que tenga que controlar otras fuentes luminosas en el sistema de iluminación. Aunque en los modos de realización de la fig. 1 y la fig. 2 los dos canales de comunicación son canales diferentes debido a que un canal utiliza luz visible como portador de información y el otro canal utiliza ondas de radio o luz infrarroja como portador de información. Sin embargo, cuando se utilizan dos fuentes luminosas y una fuente luminosa tiene que controlar a la otra fuente luminosa, el primer canal de comunicación y el segundo canal de comunicación se pueden formar mediante información modulada en luz visible. En tal configuración, la distinción entre el primer canal de comunicación y el segundo canal de comunicación se forma principalmente por la fuente luminosa que modula la información en la luz.

Como se muestra en la fig. 3, el controlador remoto 150, 250 puede transmitir un comando de control a la fuente luminosa 110, 210 junto con la respuesta rp_{t2} generada. Si la respuesta rp_{t2} recibida concuerda con la referencia, el comando de control recibido *comando* se ejecuta por la fuente luminosa en un cuarto instante de tiempo, controlando así el funcionamiento de la fuente luminosa de acuerdo con el comando de control *comando*. En algunos ajustes, especialmente cuando la respuesta no tiene que concordar exactamente con la referencia, algunos bits o dígitos de la respuesta pueden ser redundantes y en tales casos los bits o dígitos redundantes se pueden utilizar para comunicar el *comando* a la fuente luminosa.

En la fig. 4, se muestra otro modo de realización de un protocolo de autorización 400. En un primer instante de tiempo *t1* la fuente luminosa 110, 210 genera una señal de identificación ch_{t1} con una función criptográfica *f(...)* que recibe un identificador de fuente luminosa único ID_{ls} y una primera llave criptográfica como argumentos. Así pues, la señal de identificación ch_{t1} generada es diferente de otras señales de identificación generadas en otra fuente luminosa, debido a que en las otras fuentes luminosas el identificador de fuente luminosa es diferente. La fuente luminosa 110, 210 transmite la señal de identificación ch_{t1} generada en instantes regulares de tiempo a través del primer canal de comunicación 302. En un instante de tiempo concreto, el controlador remoto 150, 250 recibe la señal de identificación ch_{t1} transmitida y genera una respuesta rp_{t2} del mismo modo que se discutió en el protocolo de autorización 300 de la fig. 3. La respuesta rp_{t2} generada se transmite a la fuente luminosa 110, 210 a través del segundo canal de comunicación 304. La fuente luminosa 110, 210 recibe la respuesta rp_{t2} transmitida y compara la respuesta recibida con una referencia *ref.* Si hay una concordancia, la respuesta rp_{t2} se transmite de nuevo al controlador remoto 150, 250 a través del primer canal de comunicación 302. En el mismo instante de tiempo que el instante de tiempo en el que el controlador remoto 150, 250 fue autorizado a controlar la fuente luminosa 110, 210 se inicia un intervalo de tiempo 406 durante el cual es autorizado a controlar la fuente luminosa mediante el envío de comandos de control a través del segundo canal de comunicación 304 a la fuente luminosa 110, 210. En la fig. 4 se muestra que durante el intervalo de tiempo 406 el controlador remoto 150, 250 transmite dos comandos de control *comando1*, *comando2* a la fuente luminosa 110, 210, y que la fuente luminosa 110, 210 ejecuta los comandos de control de tal modo que el funcionamiento de la fuente luminosa 110, 210 es controlado de acuerdo con los comandos recibidos.

En la fig. 5 se muestra otro modo de realización de un protocolo de autorización 500. Se debe apreciar que en la fig. 5 no se presentan actividades en el lado del controlador remoto 150, 250, sin embargo, el controlador remoto 150, 250 puede responder a las señales de identificación ch_{tn} recibidas del mismo modo que se ha presentado en otros modos de realización de los protocolos de autorización 300, 400, 600 de las figs. 3, 4 y 6.

La fig. 5 muestra un modo de realización de la fuente luminosa 110, 210 en el que la fuente luminosa 110, 210 utiliza la señal de identificación ch_{tn-1} anteriormente generada para generar la señal de identificación ch_{tn}. Como se muestra, en un segundo instante de tiempo *t2*, se genera la señal de identificación ch_{t2} generada con la función criptográfica *f(...)*, que recibe la señal de identificación ch_{t1} generada en un primer instante de tiempo *t1*, como uno de los argumentos. Lo mismo se aplica al tercer instante de tiempo *t3*, instante de tiempo en el que la señal de identificación ch_{t2} generada en el segundo instante de tiempo *t2* se utiliza como uno de los argumentos de la función criptográfica *f(...)*. En el modo de realización de la fig. 5, cada señal de identificación ch_{tn} generada se transmite repetidamente durante un intervalo de tiempo. En otro modo de realización, una señal de identificación ch_{tn} generada no se cambia hasta que el controlador remoto 150, 250 es autorizado por la fuente luminosa 110, 210. Tras la autorización, en un primer modo de realización, la respuesta rp_{tn-1} recibida se puede utilizar como un argumento de la función criptográfica *f(...)*, y en un segundo modo de realización se puede utilizar la señal de identificación ch_{tn-1} anteriormente generada.

En la fig. 6, se presenta un modo de realización adicional de un protocolo de autorización 600. El protocolo de autorización 600 es similar al protocolo de autorización 300 de la fig. 3, sin embargo, se transmite más información a través de los canales de comunicación y se utiliza más información para generar la respuesta rp_{t2}. En lugar de

transmitir tan solo la señal de identificación ch_{t1} generada, se concatena un identificador de la fuente luminosa único ID_{ls} de la fuente luminosa con la señal de identificación ch_{t1} generada. Se debe apreciar que el símbolo ○ se utiliza para indicar una concatenación de dos valores. La concatenación ID_{ls}○ch_{t1} del identificador único ID_{ls} y la señal de identificación ch_{t1} generada se transmite a través del primer canal de comunicación de la fuente luminosa 110, 210 al controlador remoto 150, 250. Inmediatamente después de transmitir la concatenación ID_{ls}○ch_{t1}, la fuente luminosa 110, 210 genera una referencia *ref* que se utiliza en un instante posterior de tiempo para comparar con una respuesta rp_{t2} recibida. La referencia *ref* representa la respuesta esperada. La referencia *ref* se genera con la función criptográfica que recibe la primera llave criptográfica y la concatenación ID_{ls}○ch_{t1} transmitida como argumentos.

Si el identificador de la fuente luminosa ID_{ls} siempre tiene el mismo número de dígitos, el controlador remoto puede deducir el identificador de la fuente luminosa ID_{ls} de la concatenación ID_{ls}○ch_{t1} recibida. En el modo de realización mostrado en la fig. 6, la respuesta rp_{t2} generada se basa no solo en la señal de identificación ch_{t1} recibida, sino asimismo en el identificador de la fuente luminosa ID_{ls}, ya que la concatenación ID_{ls}○ch_{t1} es un argumento de la función criptográfica *f(...)*. Sin embargo, el modo de realización no se limita a utilizar la concatenación ID_{ls}○ch_{t1} al generar la respuesta rp_{t2}: en lugar de utilizar la concatenación ID_{ls}○ch_{t1} como argumento, se puede utilizar solo la señal de identificación ch_{t1}. Subsiguientemente, la respuesta rp_{t2} generada se concatena con la señal de identificación ch_{t1} recibida, o con el identificador de la fuente luminosa ID_{ls} recibido, o se concatena con la concatenación ID_{ls}○ch_{t1} recibida del identificador de la fuente luminosa ID_{ls} y la señal de identificación ch_{t1}. En el modo de realización específico de la fig. 6, la respuesta rp_{t2} generada se concatena con la concatenación ID_{ls}○ch_{t1} recibida y como tal la concatenación ID_{ls}○ch_{t1}○rp_{t2} se transmite del controlador remoto 150, 250 a la fuente luminosa 110, 210 a través del segundo canal de comunicación 304.

La fuente luminosa 110, 210 puede detectar simplemente inspeccionando los primeros dígitos de la concatenación ID_{ls}○ch_{t1}○rp_{t2} el valor del identificador ID_{ls} de la fuente luminosa, y por tanto, la fuente luminosa 110, 220 puede detectar fácilmente si la información transmitida se dirige a la fuente luminosa 110, 210. Además, en la fuente luminosa 110, 210, la respuesta rp_{t2} se extrae de la concatenación recibida y se compara con la referencia *ref.* Si hay una concordancia, dicho de otro modo, si la referencia *ref* es igual a la respuesta rp_{t2}, el controlador remoto 150, 250 es autorizado por la fuente luminosa 110, 210 a controlar la fuente luminosa 110, 210.

El controlador remoto 150, 250 puede enviar, junto con la concatenación ID_{ls}○ch_{t1}○rp_{t2}, un comando de control *comando*, y si el controlador remoto 150, 250 es autorizado por la fuente luminosa 110, 210, el comando de control *comando* recibido es ejecutado por la fuente luminosa 110, 210, de tal modo que la emisión de luz por la fuente luminosa 110, 210 varía de acuerdo con el comando de control *comando*.

En la fig. 7 se proporciona un procedimiento 700 de acuerdo con el cuarto aspecto de la invención. El procedimiento 700 comprende las etapas de i) generar 702 una señal de identificación con una función criptográfica que recibe una primera llave criptográfica como argumento, ii) transmitir 704 la señal de identificación de la fuente luminosa al dispositivo a través de un primer canal de comunicación que se forma modulando información en la luz emitida de la fuente luminosa, iii) recibir 706 la señal de identificación del primer canal de comunicación, iv) generar 708 una respuesta con la función criptográfica que recibe la señal de identificación recibida y una segunda llave criptográfica como argumentos, v) transmitir 710 la respuesta del dispositivo a la fuente luminosa a través de un segundo canal de comunicación, vi) recibir 712 la respuesta del segundo canal de comunicación, y vii) autorizar 714 el dispositivo comparando el segundo pseudo identificador recibido con una referencia, y, si el segundo pseudo identificador recibido concuerda con la referencia, el dispositivo es autorizado por la fuente luminosa.

En un modo de realización, se proporciona un producto de programa de ordenador que comprende instrucciones para hacer que un procesador de una fuente luminosa realice las etapas de generar una señal de identificación con una función criptográfica que recibe un argumento que comprende una primera llave criptográfica y autorizar un dispositivo comparando un segundo pseudo identificador recibido con una referencia. El producto de programa de ordenador puede comprender además instrucciones para realizar al menos parcialmente la etapa de transmitir la señal de identificación de la fuente luminosa al dispositivo a través de un primer canal de comunicación que se forma modulando información en la luz emitida de la fuente luminosa y para realizar al menos parcialmente las etapas de recibir la respuesta del segundo canal de comunicación.

En otro modo de realización, se proporciona un producto de programa de ordenador que comprende instrucciones para hacer que un procesador de un dispositivo realice la etapa de generar una respuesta con la función criptográfica que recibe una señal de identificación recibida y una segunda llave criptográfica como argumentos. El producto de programa de ordenador puede comprender además instrucciones para realizar al menos parcialmente la etapa de recibir la señal de identificación a través del primer canal de comunicación y para realizar al menos parcialmente la etapa de transmitir 710 la respuesta del dispositivo a la fuente luminosa a través de un segundo canal de comunicación.

Se apreciará que la invención se extiende igualmente a programas de ordenador, concretamente programas de ordenador sobre o en un portador, adaptados para llevar a la práctica la invención. El programa puede tener la forma de código fuente, código objeto, un código intermedio entre código fuente y objeto tal como una forma parcialmente

compilada, o en cualquier otra forma adecuada para su uso en la implementación del procedimiento de acuerdo con la invención. Asimismo se apreciará que tal programa puede tener muchos diseños arquitectónicos distintos. Por ejemplo, un código de programa que implementa la funcionalidad del procedimiento o sistema de acuerdo con la invención se puede subdividir en una o más subrutinas. Muchas formas diferentes de distribuir la funcionalidad entre estas subrutinas serán aparentes para el experto en la técnica. Las subrutinas se pueden almacenar conjuntamente en un fichero ejecutable para formar un programa autocontenido. Tal fichero ejecutable puede comprender instrucciones ejecutables por un ordenador, por ejemplo, instrucciones de procesador y/o instrucciones de intérprete (por ejemplo, instrucciones de intérprete de Java). Alternativamente, una o más o todas las subrutinas se pueden almacenar en al menos una librería externa y vincularlas con un programa principal ya sea estática o dinámicamente, por ejemplo en tiempo de ejecución. El programa principal contiene por lo menos una llamada a por lo menos una de las subrutinas. Asimismo, las subrutinas pueden comprender llamadas de función una a otra. Un modo de realización relacionado con un producto de programa de ordenador comprende instrucciones ejecutables en un ordenador que corresponden a cada una de las etapas de procesamiento de al menos uno de los procedimientos establecidos. Estas instrucciones se pueden subdividir en subrutinas y/o almacenar en uno o más ficheros que se pueden vincular estática o dinámicamente. Otro modo de realización relacionado con un producto de programa de ordenador comprende instrucciones ejecutables que corresponden a cada uno de los medios de al menos uno de los sistemas y/o productos establecidos. Estas instrucciones se pueden subdividir en subrutinas y/o almacenarse en uno o más ficheros que se pueden vincular estática o dinámicamente.

El portador de un programa de ordenador puede ser cualquier entidad o dispositivo capaz de transportar el programa. Por ejemplo, el portador puede incluir un medio de almacenamiento, tal como una ROM, por ejemplo un CD ROM o una ROM de semiconductor, o un medio de registro magnético, por ejemplo un disco flexible o un disco duro. Además, el portador puede ser un portador transmisible tal como una señal eléctrica u óptica, que se puede transportar por medio de un cable eléctrico u óptico o por radio u otros medios. Cuando el programa se materializa en tal señal, el portador puede estar constituido por tal cable u otro dispositivo o medios. Alternativamente, el portador puede ser un circuito integrado en el que está embebido el programa, estando adaptado el circuito integrado para realizar, o para ser usado en la realización de, el procedimiento relevante.

Se debe apreciar que los modos de realización anteriormente mencionados antes que limitar la invención la ilustran, y que los expertos en la técnica serán capaces de diseñar muchos modos de realización alternativos sin alejarse del ámbito de las reivindicaciones adjuntas.

En las reivindicaciones, cualesquiera signos de referencia situados entre paréntesis no se deben considerar como limitativos de la reivindicación. El uso del verbo “comprender” y su conjugación no excluye la presencia de elementos o etapas además de los establecidos en una reivindicación. El artículo “un” precediendo a un elemento no excluye la presencia de una pluralidad de tales elementos. La invención se puede implementar por medio de elementos físicos que comprenden diversos elementos distintos, y por medio de un ordenador adecuadamente programado. En la reivindicación de dispositivo que enumera diversos medios, algunos de estos medios se pueden materializar mediante el mismo elemento físico. La mera circunstancia de que ciertas medidas se reciten en reivindicaciones dependientes mutuamente diferentes no indica que una combinación de estas medidas no se pueda utilizar de modo ventajoso.

REIVINDICACIONES

1. Sistema de iluminación (100, 200) que comprende una fuente luminosa (110, 210) para emitir luz (116), un dispositivo (150, 250) para controlar la fuente luminosa (110, 210) un primer canal de comunicación de la fuente luminosa (110, 210) al dispositivo (150, 250), formándose el primer canal de comunicación por modulación de información en la luz emitida (116) de la fuente luminosa (110, 210), y un segundo canal de comunicación del dispositivo (150, 250) a la fuente luminosa (110, 210), comprendiendo la fuente luminosa (110, 210):

- un generador de señales de identificación (118, 212) para generar una señal de identificación (ch_{t1}, ch_{t2}, ch_{t3}, ch_{tn}) con una función criptográfica (f) que recibe un argumento que comprende una primera llave criptográfica (llave1),

- un transmisor (112, 212) de la fuente luminosa para transmitir la señal de identificación (ch_{t1}, ch_{t2}, ch_{t3}, ch_{tn}) a través del primer canal de comunicación,

- un receptor (122, 212) de la fuente luminosa para recibir una respuesta (rp_{t2}) del dispositivo (150, 250) a través del segundo canal de comunicación, y

- unos medios de autorización (120, 212) para autorizar el dispositivo (150, 250) para que controle la fuente luminosa (110, 210) comparando la respuesta (rp_{t2}) recibida con una referencia (ref), y si la respuesta (rp_{t2}) recibida concuerda con la referencia (ref) se autoriza el dispositivo (150, 250),

comprendiendo el dispositivo (150, 250):

- un receptor (152) del dispositivo para recibir la señal de identificación (ch_{t1}, ch_{t2}, ch_{t3}, ch_{tn}) a través del primer canal de comunicación,

- un generador de respuestas (154, 254) para generar la respuesta (rp_{t2}) con la función criptográfica (f) que recibe argumentos que comprenden la señal de identificación (ch_{t1}, ch_{t2}, ch_{t3}, ch_{tn}) recibida y una segunda llave criptográfica (llave2), y

- un transmisor (156, 254) del dispositivo para transmitir la respuesta (rp_{t2}) a la fuente luminosa (110, 210) a través del segundo canal de comunicación.

2. Un sistema de iluminación (100, 200) según la reivindicación 1, en el que la fuente luminosa (110, 210) comprende un identificador de la fuente luminosa único (ID_{ls}) en el que el generador de señales de identificación (118, 212) se configura para comprender el identificador de la fuente luminosa único (ID_{ls}) como un argumento adicional de la función criptográfica (f).

3. Un sistema de iluminación (100, 200) según la reivindicación 2, en el que el primer canal de comunicación es un canal de transmisión unidireccional.

4. Un sistema de iluminación (100, 200) según la reivindicación 3, en el que el transmisor (112, 212) de la fuente luminosa se configura para transmitir regularmente un identificador a través del primer canal de comunicación y en el que el transmisor de la fuente luminosa se configura además para transmitir regularmente la señal de identificación (ch_{t1}, ch_{t2}, ch_{t3}, ch_{tn}) generada como el identificador.

5. Un sistema de iluminación (100, 200) según la reivindicación 4, en el que el transmisor (112, 212) de la fuente luminosa se configura para emitir regularmente la respuesta (rp_{t2}) en lugar de la señal de identificación (ch_{t1}, ch_{t2}, ch_{t3}, ch_{tn}) si el dispositivo (150, 250) es autorizado por la fuente luminosa (110, 210).

6. Un sistema de iluminación (100, 200) según la reivindicación 1, en el que el transmisor (156, 254) del dispositivo se configura para transmitir un mensaje a través del segundo canal de comunicación, comprendiendo el mensaje un identificador (ID_{ls}) de la fuente luminosa (110, 210), y en el que el transmisor (156, 254) del dispositivo se configura para utilizar la respuesta (rp_{t2}) generada como el identificador en el mensaje.

7. Un sistema de iluminación (100, 200) según la reivindicación 1, en el que el generador de señales de identificación (118, 212) se configura para comprender una señal de identificación (ch_{tn-1}) previamente generada o una respuesta (rp_{t2}) previamente recibida en los argumentos de la función criptográfica (f).

8. Un sistema de iluminación (100, 200) según la reivindicación 1, en el que el generador de señales de identificación (118, 212) se configura asimismo para generar la referencia (ref) con la función criptográfica (f) que recibe argumentos que comprenden la señal de identificación (ch_{t1}, ch_{t2}, ch_{t3}, ch_{tn}) generada y la primera llave criptográfica (*llave1*).

9. Un sistema de iluminación (100, 200) según la reivindicación 1, en el que la fuente luminosa (110, 210) comprende un identificador de la fuente luminosa único (ID_{ls}) pre-programado, en el que la fuente luminosa (110, 210) comprende además unos medios de concatenación de la fuente luminosa para concatenar la señal de identificación (ch_{t1}, ch_{t2}, ch_{t3}, ch_{tn}) con el identificador de la fuente luminosa (ID_{ls}) y en el que el transmisor (112, 212) de la fuente luminosa se configura para transmitir la concatenación ($ID_{ls} \circ ch_{t1}$).

10. Un sistema de iluminación (100, 200) según la reivindicación 1, en el que el dispositivo (150, 250) comprende además unos medios de concatenación del dispositivo para concatenar la respuesta (rp_{t2}) generada con la señal de identificación (ch_{t1}, ch_{t2}, ch_{t3}, ch_{tn}) recibida, y en el que el transmisor (156, 254) del dispositivo se configura para transmitir la concatenación ($ID_{ls} \circ ch_{t1} \circ rp_{t2}$).

11. Un sistema de iluminación (100, 200) según la reivindicación 1,

- en el que el dispositivo (150, 250) comprende además unos medios de recepción de comandos de control () para recibir un comando de control () de un usuario para controlar la fuente luminosa,

- en el que el transmisor (156, 254) del dispositivo se configura para transmitir el comando de control () junto con la respuesta (rp_{t2}), y

la fuente luminosa (110, 210) comprende además un controlador de la fuente luminosa para ejecutar el comando de control que se recibe junto con la respuesta (rp_{t2}), el controlador de la fuente luminosa se configura para ejecutar el comando solo si el dispositivo (150, 250) es autorizado por la fuente luminosa (110, 210).

12. Un sistema de iluminación (100, 200) según la reivindicación 1, en el que la fuente luminosa (110, 210) se configura para permitir la recepción de un comando de control () de la fuente luminosa a través del segundo canal de comunicación durante un intervalo de tiempo () predefinido que sigue al instante de tiempo en el que el dispositivo (150, 250) es autorizado por la fuente luminosa (110, 210),

la fuente luminosa (110, 210) comprende además un controlador de la fuente luminosa para ejecutar el comando de control () de la fuente luminosa recibido.

13. Una fuente luminosa (110, 210) para su uso en el sistema (100, 200) de acuerdo con la reivindicación 1, comprendiendo la fuente luminosa (110, 210):

- un generador de señales de identificación (118, 212) para generar una señal de identificación (ch_{t1}, ch_{t2}, ch_{t3}, ch_{tn}) con una función criptográfica (f) que recibe un argumento que comprende una primera llave criptográfica (llave1),

- un transmisor (112, 212) de la fuente luminosa para transmitir la señal de identificación (ch_{t1}, ch_{t2}, ch_{t3}, ch_{tn}) a través del primer canal de comunicación de la fuente luminosa (110, 210) a un dispositivo (150, 250),

- un receptor (122, 212) de la fuente luminosa para recibir una respuesta (rp_{t2}) del dispositivo (150, 250) un segundo canal de comunicación, y

- unos medios de autorización (120, 212) para autorizar el dispositivo (150, 250) para que controle la fuente luminosa (110, 210) comparando la respuesta (rp_{t2}) recibida con una referencia (ref), y si la respuesta (rp_{t2}) recibida concuerda con la referencia (ref) se autoriza el dispositivo (150, 250),

14. Un dispositivo (150, 250)para su uso en el sistema (100, 200) según la reivindicación 1, comprendiendo el dispositivo:

- un receptor (152) del dispositivo para recibir la señal de identificación (ch_{t1}, ch_{t2}, ch_{t3}, ch_{tn}) a través de un primer canal de comunicación que es un canal de comunicación de una fuente luminosa al dispositivo (150, 250),

- un generador de respuestas (154, 254) para generar una respuesta (rp_{t2}) con la función criptográfica (f) que recibe argumentos que comprenden la señal de identificación (ch_{t1}, ch_{t2}, ch_{t3}, ch_{tn}) recibida y una segunda llave criptográfica (), y

- un transmisor (156, 254) del dispositivo para transmitir la respuesta (rp_{t2}) a la fuente luminosa (110, 210) a través del segundo canal de comunicación.

15. Un procedimiento (700) de autorización de un dispositivo por una fuente luminosa para permitir al dispositivo controlar la fuente luminosa, procedimiento que comprende las etapas de:

- generar (702) una señal de identificación con una función criptográfica que recibe un argumento que comprende una primera llave criptográfica,

- transmitir (704) la señal de identificación de la fuente luminosa al dispositivo a través de un primer canal de comunicación que se forma modulando información en la luz emitida de la fuente luminosa,

- recibir (706) la señal de identificación del primer canal de comunicación,

- generar (708) una respuesta con la función criptográfica que recibe argumentos que comprenden la señal de identificación recibida y una segunda llave criptográfica,

- transmitir (710) la respuesta del dispositivo a la fuente luminosa a través de un segundo canal de comunicación,

- recibir (712) la respuesta del segundo canal de comunicación, y

- autorizar (714) el dispositivo comparando el segundo pseudo identificador recibido con una referencia, y, si el segundo pseudo identificador recibido concuerda con la referencia, el dispositivo es autorizado por la fuente luminosa.

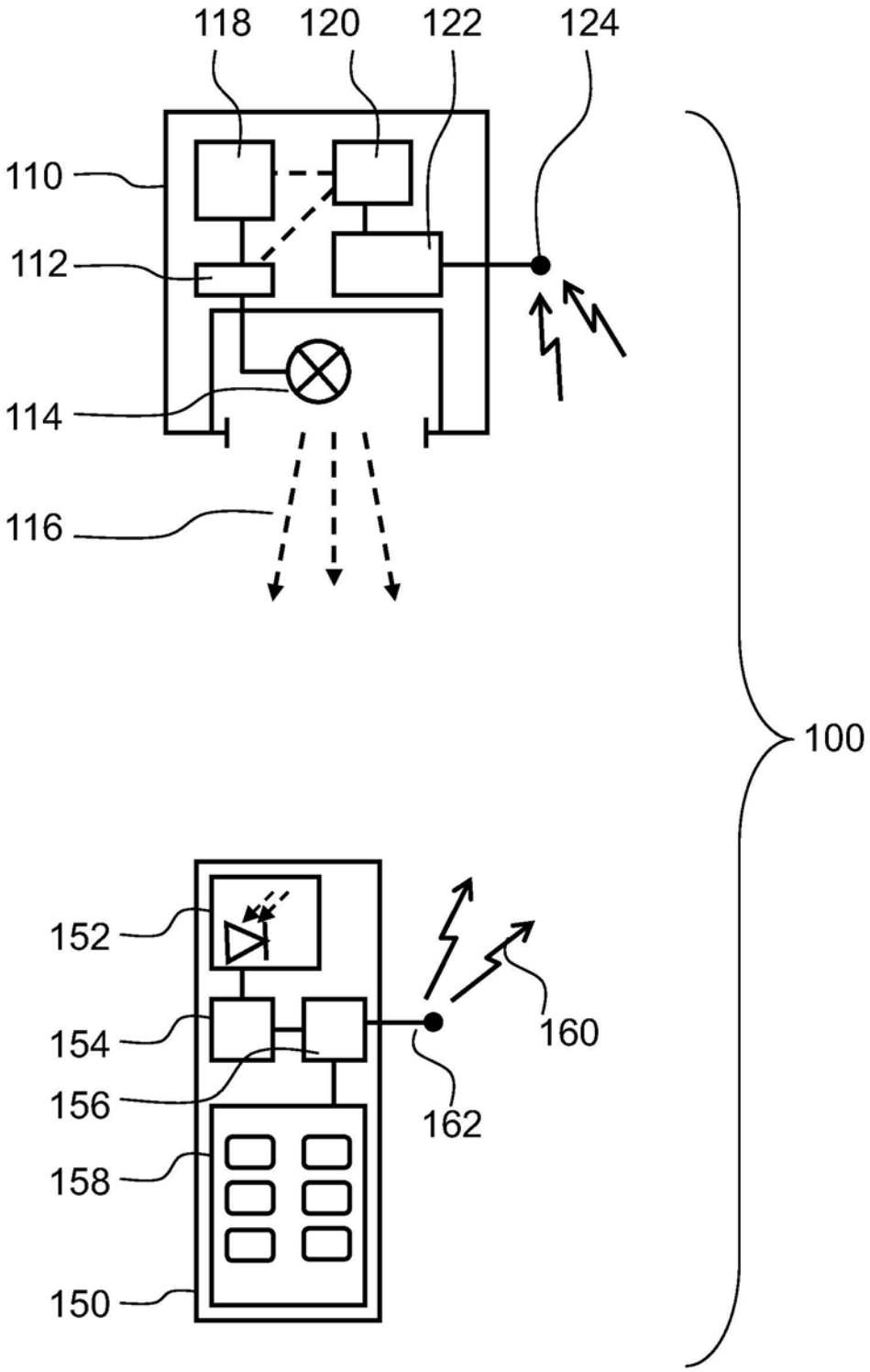

Fig. 1

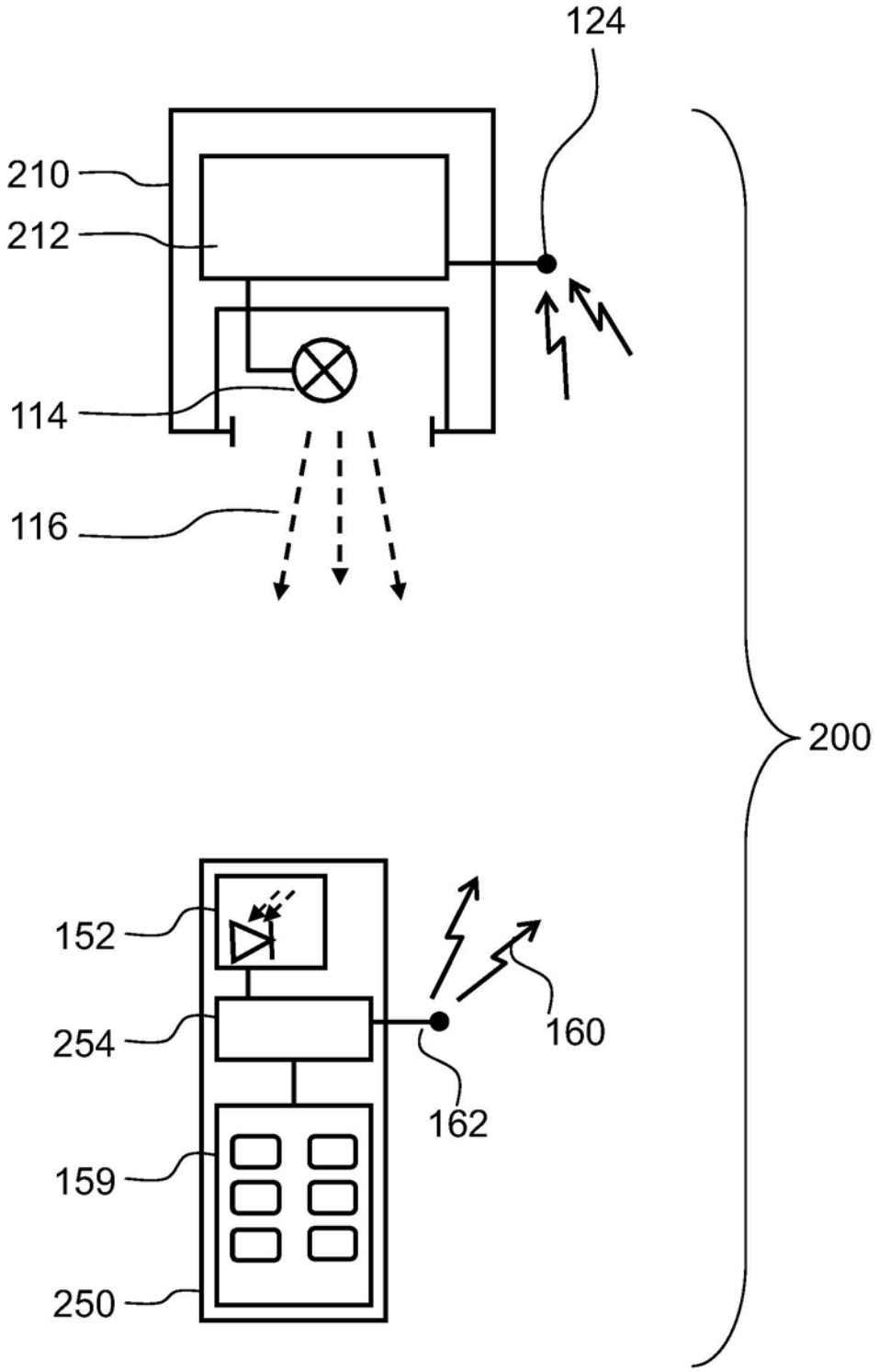

Fig. 2

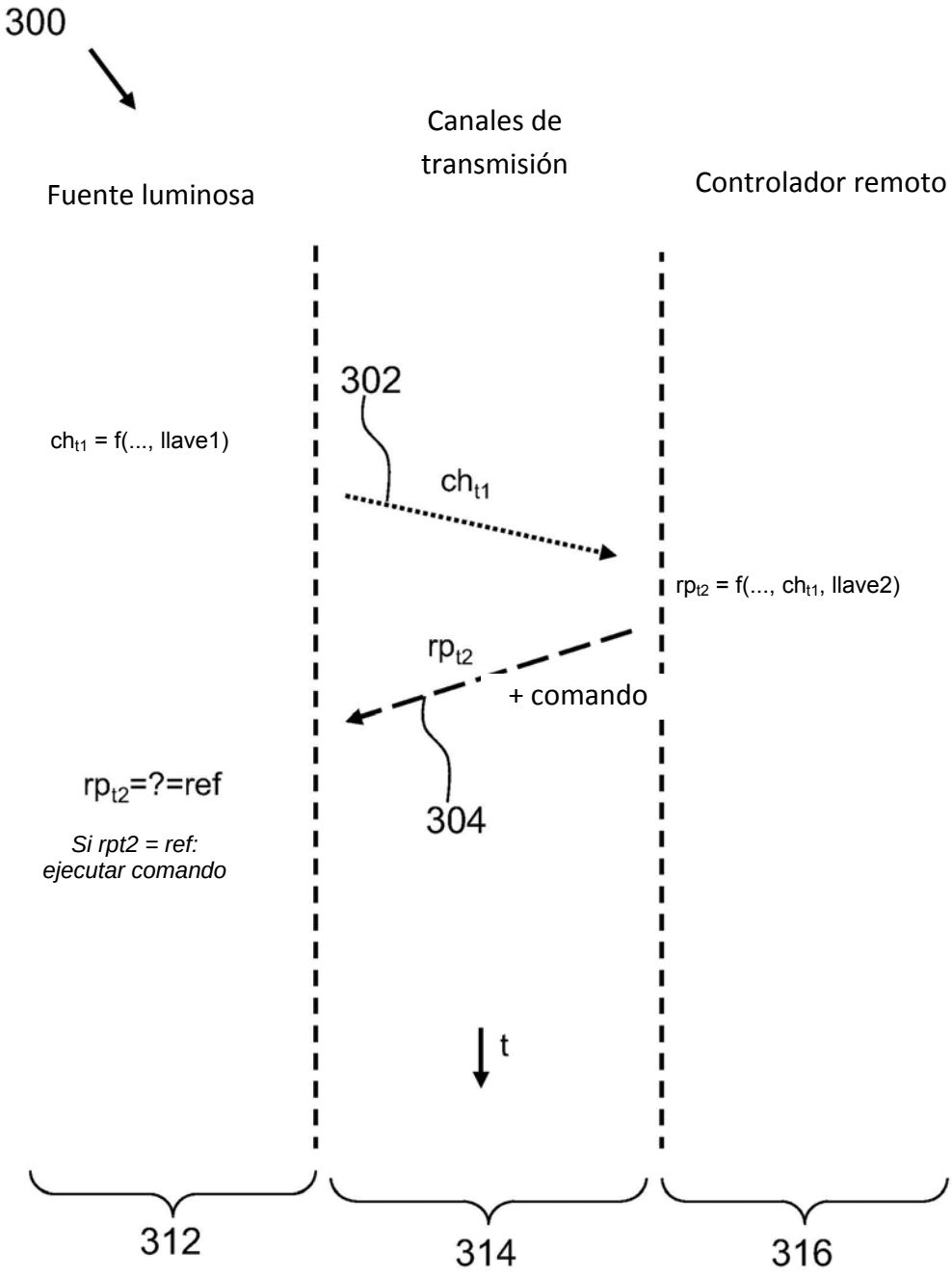
300
Canales de transmisión
Fuente luminosa
Controlador remoto
302
ch_{t1} = f(..., llave1)
ch_{t1}
rp_{t2} = f(..., ch_{t1}, llave2)
rp_{t2}
+ comando
rp_{t2}=?=ref
304
Si rpt2 = ref:
ejecutar comando
t
312
314
316

Fig. 3

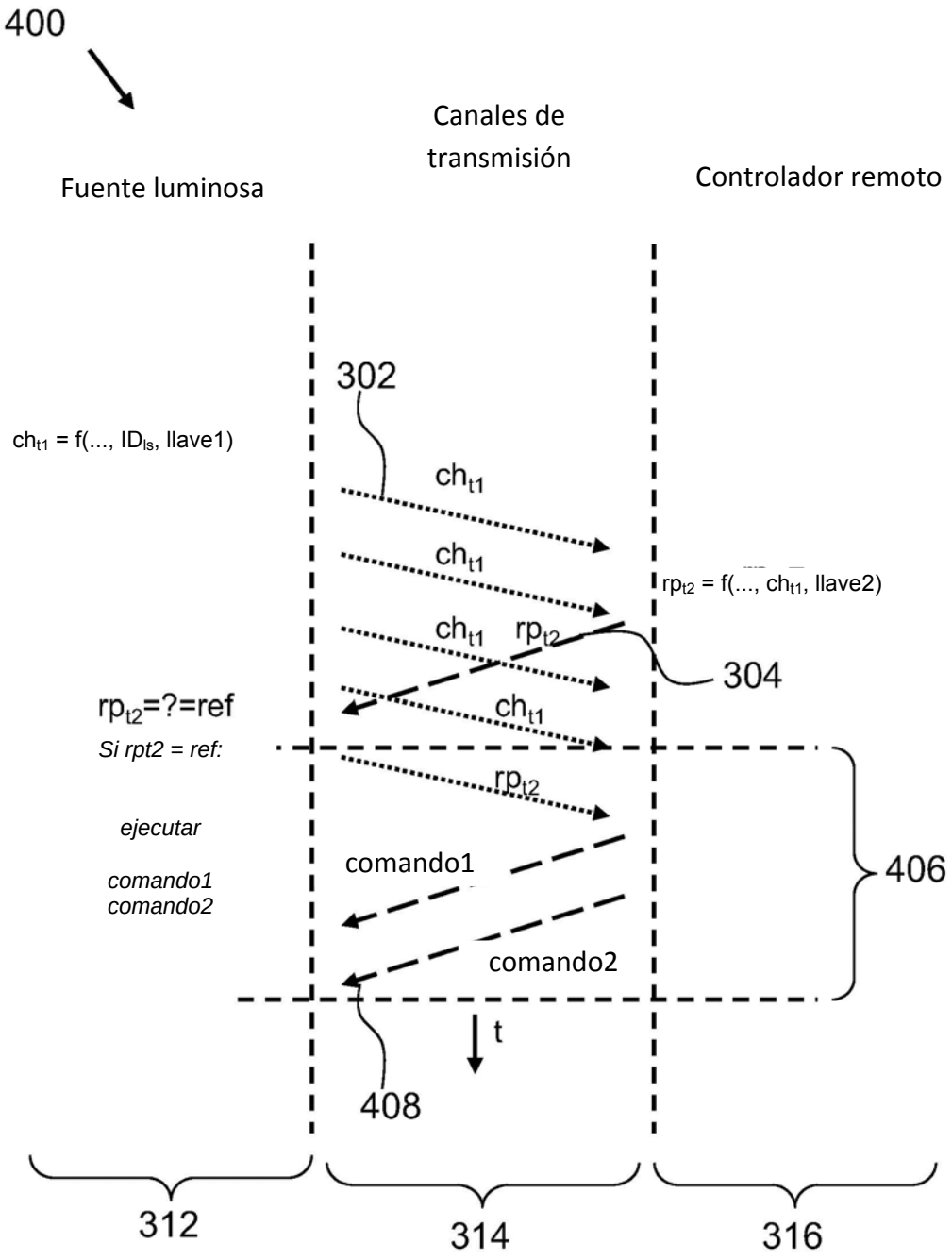
400
Canales de transmisión
Fuente luminosa
Controlador remoto
302
ch_{t1} = f(..., ID_{ls}, llave1)
ch_{t1}
ch_{t1}
rp_{t2} = f(..., ch_{t1}, llave2)
ch_{t1} rp_{t2}
304
rp_{t2}=?=ref
ch_{t1}
Si rpt2 = ref:
rp_{t2}
ejecutar
comando1
comando2
comando1
406
comando2
t
408
312
314
316

Fig. 4

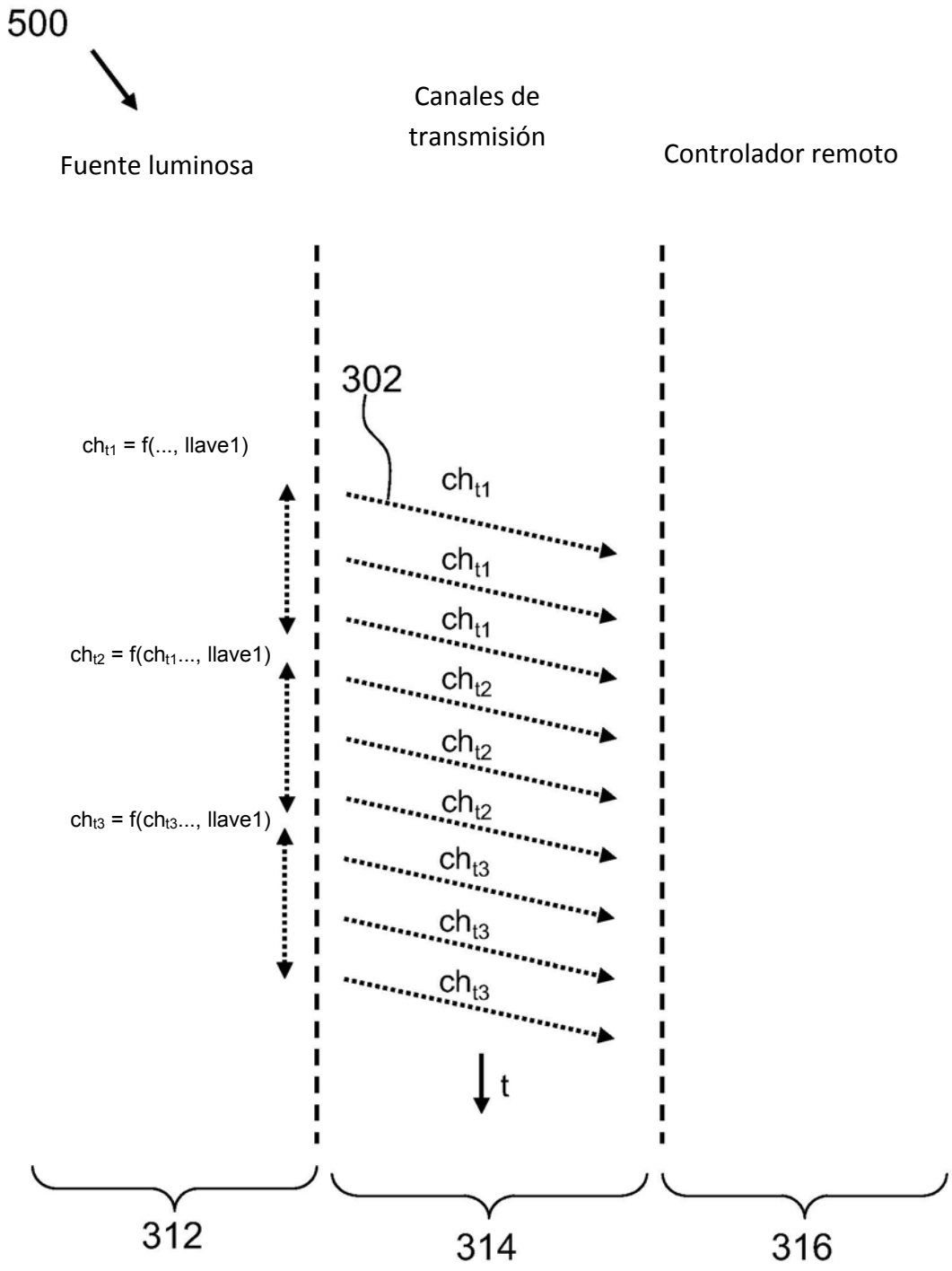
500
Fuente luminosa
Canales de transmisión
Controlador remoto
302
ch_{t1} = f(..., llave1)
ch_{t2} = f(ch_{t1}..., llave1)
ch_{t3} = f(ch_{t3}..., llave1)
ch_{t1}
ch_{t1}
ch_{t1}
ch_{t2}
ch_{t2}
ch_{t2}
ch_{t3}
ch_{t3}
ch_{t3}
t
312
314
316

Fig. 5

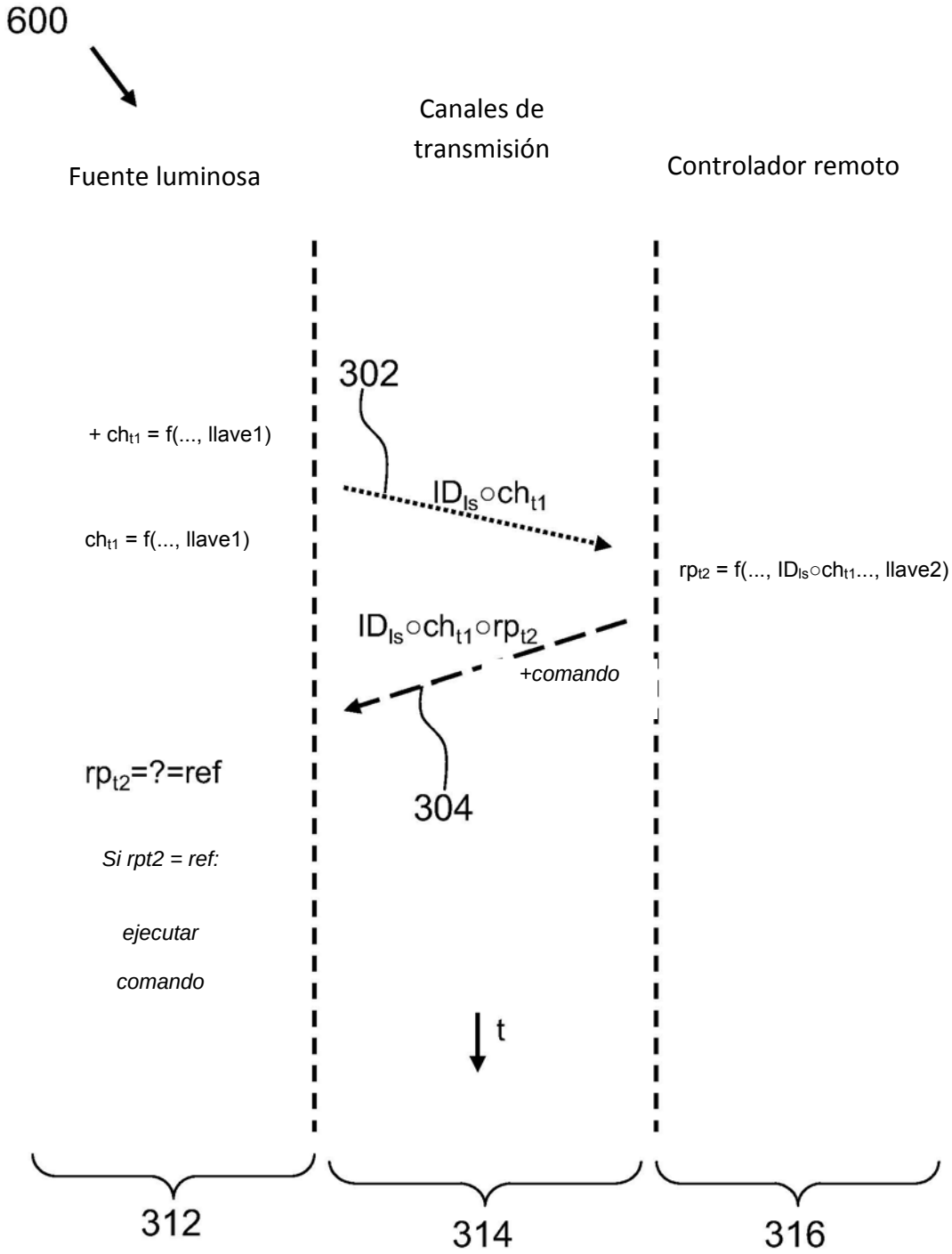
600
Fuente luminosa
Canales de transmisión
Controlador remoto
302
+ ch_{t1} = f(..., llave1)
ch_{t1} = f(..., llave1)
$ID_{ls} \circ ch_{t1}$
rp_{t2} = f(..., $ID_{ls} \circ ch_{t1}$..., llave2)
$ID_{ls} \circ ch_{t1} \circ rp_{t2}$
+comando
304
rp_{t2}=?=ref
Si rpt2 = ref:
ejecutar
comando
t
312
314
316

Fig. 6

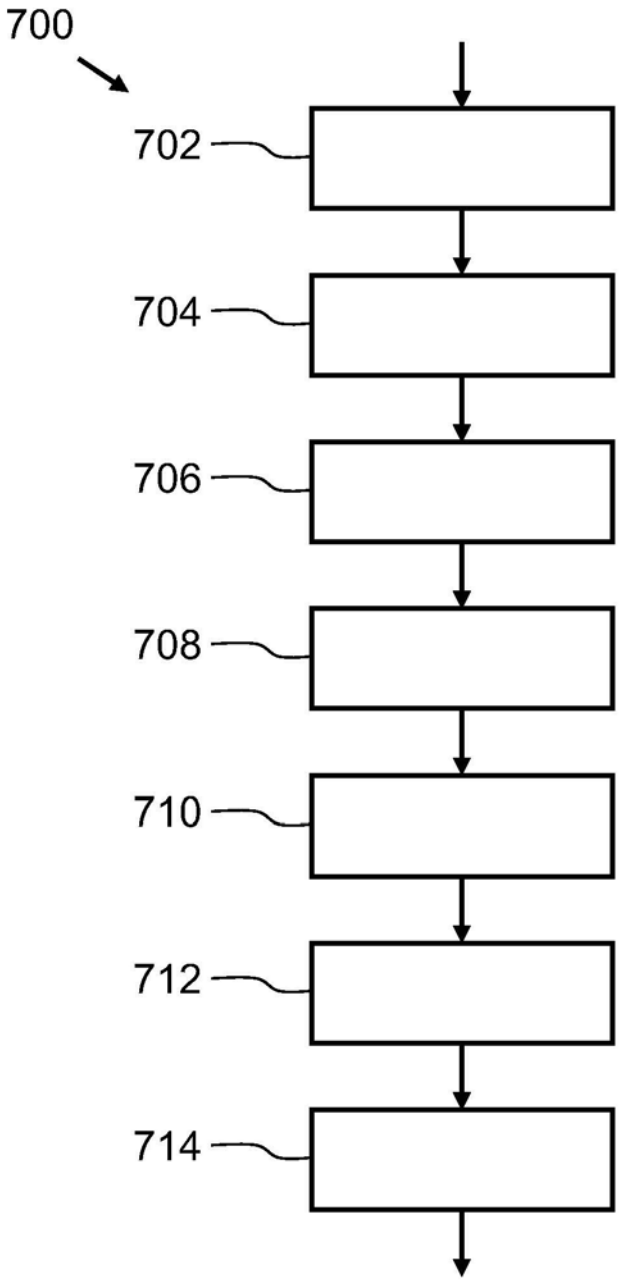

Fig. 7