(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 382 778**

(51) Int. CI.:
G08C 19/28 (2006.01)
G07C 9/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **00650129 .0**
(96) Fecha de presentación: **13.09.2000**
(97) Número de publicación de la solicitud: **1085481**
(97) Fecha de publicación de la solicitud: **21.03.2001**

(54) Título: **Un transmisor para control remoto**

(30) Prioridad:
13.09.1999 IE 990766

(45) Fecha de publicación de la mención BOPI:
13.06.2012

(45) Fecha de la publicación del folleto de la patente:
13.06.2012

(73) Titular/es:
FAAC Electronics Limited
4055 Kingswood Avenue, Citywest
Dublin 24, IE

(72) Inventor/es:
Moriarty, Donal y
O'Connell, Thomas

(74) Agente/Representante:
Ungría López, Javier

DESCRIPCIÓN

Un transmisor para control remoto

La invención se refiere a un transmisor para un grupo de control remoto para una función compartida tal como la apertura de una puerta de garaje. Se refiere también a un receptor para tal grupo y a un grupo de un receptor y una pluralidad de transmisores.

Nuestra Patente Europea previa Nº EP0651119B1 describe un transmisor que tiene una capacidad de aprender un código de modo que se pueda usar en un grupo de control remoto. Una instrucción embebida permite una versatilidad acerca de cómo tiene lugar el aprendizaje. También, hay una “escucha” automática cada vez que se presiona el botón de transmisión.

Tales características en un transmisor son muy útiles para el aprendizaje. Sin embargo, se mantiene la necesidad de la mejora de la seguridad en el enlace transmisor-receptor. Un enfoque para conseguir una seguridad mejorada es cifrarla usando una clave de cifrado. Sin embargo, esto significa que el ingeniero de instalación necesita acceder al receptor para programarlo para permitir la presentación de cada nuevo transmisor en el grupo. Esto es costoso en tiempo y caro.

Por lo tanto es un objetivo de la invención proporcionar:

(a) una seguridad mejorada en el enlace transmisor-receptor, con

(b) la presentación automática de un nuevo transmisor al receptor sin necesidad de involucrar al ingeniero de instalación.

El documento US5661804 describe un transceptor que se puede entrenar para el aprendizaje y la transmisión de una señal de activación que incluye un código variable de modo rotativo.

De acuerdo con la invención, se proporciona un grupo de control remoto como se expone en la reivindicación 1.

En una realización, el código válido es variable de acuerdo con un criterio prestablecido.

En una realización, el código válido comprende un índice de saltos.

En otra realización, el código válido comprende una combinación de un valor de discriminación fijo conocido para el receptor y un índice de saltos.

En una realización, el transmisor esclavo comprende medios para la generación de la clave de cifrado mediante el procesamiento de una clave establecida por el fabricante con un código del emplazamiento que es único para el grupo.

En una realización, el transmisor esclavo comprende medios para la recepción del código del emplazamiento en una señal de radiación de enseñanza cifrada y para el descifrado de esa señal para determinar el código del emplazamiento usando una clave de descifrado de enseñanza.

En una realización, el transmisor esclavo comprende medios para el almacenamiento de un número de serie específico del transmisor y para la transmisión del número de serie junto con el código cifrado.

De acuerdo con otro aspecto, el procesador del transmisor maestro comprende:

medios para el almacenamiento de un código del emplazamiento que es único para el grupo de control remoto,

medios para el cifrado del código del emplazamiento con una clave de cifrado de enseñanza para la enseñanza y

medios para dirigir la transmisión del código del emplazamiento cifrado en una señal de radiación de enseñanza.

En una realización, el procesador del receptor comprende medios para:

la identificación de un número de serie del transmisor en una transmisión recibida y la determinación de si es válido,

la identificación de un índice de saltos y un valor de discriminación en el código descifrado y

la determinación de si el valor de discriminación y el índice de saltos son válidos.

En otra realización, el procesador del receptor comprende medios para la determinación de si el número de serie es válido mediante:

la comparación del número de serie con una lista almacenada de números de serie válidos,

la determinación de que el número de serie es válido si es el mismo que un número de serie válido almacenado o si se recibe posteriormente un código cifrado nuevo que contenga el mismo número de serie y un índice de saltos válido.

La invención se comprenderá más claramente a partir de la siguiente descripción de algunas realizaciones de la misma, dadas a modo de ejemplo solamente con referencia a los dibujos adjuntos en los que la Fig. 1 es un diagrama esquemático de un transmisor de un grupo de control remoto de la invención.

Con referencia a la Fig. 1, el transmisor 1 del grupo de control remoto comprende:

2: un microprocesador,
3: una memoria que tiene una capacidad para cuatro códigos del emplazamiento (grupo), cuatro números de serie, cuatro índices de saltos, cuatro claves de cifrado y cuatro valores de discriminación,
4. un receptor de la radiación conectado al microprocesador 2,
5: una antena transmisora, conectada a un circuito oscilador 6,
7: cuatro interruptores,
8: un paquete de baterías y
9: un regulador que proporciona +Vreg para la totalidad del circuito.

La capacidad de la memoria es adecuada para cuatro conjuntos de datos, como se ha descrito anteriormente. Esto permite que se use el transmisor 1 para hasta cuatro grupos de control remoto diferentes. Sin embargo, por claridad, se describe a continuación solamente el funcionamiento para un grupo.

El microprocesador 2 se programa para reconocer la pulsación de un interruptor 7 como una instrucción de transmisión. La pulsación simultánea de dos o más interruptores en varias configuraciones prestablecidas se interpretan como instrucciones del usuario para funciones auxiliares tales como un modo de enseñanza o aleatorización de los códigos. La programación del microprocesador 2 durante la fabricación determina si el transmisor es un maestro o un esclavo. Los esclavos no tienen un modo de enseñanza. El transmisor 1 es un esclavo.

El transmisor 1 es parte de un grupo de control remoto que comprende también un receptor y un transmisor maestro. Éste último se usa para la enseñanza tanto del receptor como de los transmisores 1. Tiene la misma configuración de hardware que el transmisor 1, pero se programa adicionalmente con un modo de enseñanza.

Se da al grupo de control remoto un código del emplazamiento único por parte del instalador y el transmisor maestro enseña el código del emplazamiento al receptor y a los transmisores 1. Esto da poder al instalador para fijar la manera en la que el grupo de control remoto funciona desde un punto de vista de seguridad. Cada transmisor maestro está programado previamente en fábrica con un código del emplazamiento único (para él). Por lo tanto el instalador puede usar el código del emplazamiento programado previamente de un transmisor maestro como el del grupo. Alternativamente, puede cambiarlo mediante la aleatorización del valor prestablecido.

Cada nuevo transmisor almacena lo siguiente después de la fabricación:

un número de serie de 24 bits (programado previamente durante la fabricación) que es único para el nuevo transmisor,

un índice de saltos de 20 bits inicial que se incrementará posteriormente cada vez que se use el nuevo transmisor,

una clave de cifrado fijada por el fabricante y

una clave de descifrado para el descifrado de un código del emplazamiento en una sesión de enseñanza.

El transmisor maestro enseña el código del emplazamiento a un transmisor (esclavo) 1 usando una clave de cifrado de enseñanza. El transmisor 1 la descifra usando una clave de descifrado de enseñanza. Después del descifrado, el transmisor 1 usa el código del emplazamiento para generar la clave de cifrado para su uso en el envío de señales al receptor para el control de la función del grupo compartido. Después de que se use para generar la clave de cifrado, no se almacena necesariamente dado que ya no se requiere de nuevo. La clave de cifrado tiene 64 bits de largo. El transmisor maestro también enseña un valor de discriminación al transmisor 1. Éste es un valor acordado que

permite al receptor determinar que ha descifrado correctamente la transmisión. Podría, por ejemplo, ser parte del código del emplazamiento o del número de serie o de cualquier otro número acordado.

La clave de cifrado podría alternativamente ser generada solamente por el transmisor maestro y enseñada al receptor y los transmisores 1. Sin embargo esto conlleva la desventaja de involucrar la transmisión de la clave de cifrado.

Cuando se da el nuevo transmisor al usuario, él o ella pueden usarlo inmediatamente sin necesidad de que un ingeniero de instalación acceda al receptor. Hay dos etapas en la presentación del nuevo transmisor al receptor por parte del usuario como sigue:

(a) Aceptación inicial

El usuario pulsa el botón de “transmisión”. El microcontrolador cifra el índice de saltos inicial y el valor de discriminación con la clave de cifrado para proporcionar un código de cifrado válido. El número de serie (sin cifrar) y el código cifrado se transmiten y se reciben por parte del receptor. El receptor descifra el código usando su clave de descifrado almacenada para determinar el valor de discriminación y el índice de saltos inicial. El receptor comprueba entonces el valor de discriminación (descifrado) y, si es válido, almacena el número de serie y el índice de saltos inicial.

(b) Aceptación de activación

El usuario pulsa de nuevo el botón de “transmisión” y el transmisor incrementa el índice de saltos y cifra a continuación el valor de discriminación y el índice de saltos incrementado para proporcionar un nuevo código cifrado. Aunque pueda haber solamente un dígito de diferencia entre este índice de saltos incrementado y el índice de saltos inicial, el código cifrado es muy diferente debido a la compleja naturaleza del cifrado. El receptor descifra el nuevo código cifrado para determinar el valor de discriminación y el índice de saltos incrementado y lee el número de serie. Si se satisfacen los siguientes criterios el receptor activa la función del grupo compartido (por ejemplo abrir una puerta) y almacena el índice de saltos incrementado:

el número de serie es el mismo que el primero,
el índice de saltos incrementado descifrado coincide con el criterio de saltos (mayor que el primero) y el valor de discriminación es correcto.

Posteriormente, el usuario sólo necesita pulsar el botón de transmisión una vez para activar la función del grupo compartido. Este proceso de aceptación en dos etapas impide que una señal de ruido espurio “aceptable” sea capaz de activar la función del grupo.

Se apreciará que no hay necesidad de que el ingeniero de instalación programe el receptor para presentar (validar) un nuevo transmisor. Sin embargo, esto no se consigue a expensas de una seguridad reducida dado que hay un cifrado integral. Así, por ejemplo, una organización del instalador puede enseñar un nuevo transmisor y enviarlo al usuario por correo, con ahorros considerables de tiempo y dinero. Otro aspecto que contribuye a la seguridad es el hecho de que la “rotura” del cifrado en un grupo no tendrá efectos sobre la seguridad en otro grupo que tenga el mismo u otro equipo del fabricante. Esto es debido a que la clave de cifrado es única para cada grupo. También, la copia no autorizada del código cifrado transmitido no supone un beneficio para un ladrón ya que cambia desde una transmisión a la siguiente de una manera impredecible debido al cifrado del valor de discriminación combinado y al incremento del índice de saltos. Se concibe que donde se requiere particularmente una fuerte seguridad (tal como en un banco) el usuario puede almacenar con seguridad el transmisor maestro (único) impidiendo de ese modo cualquier enseñanza no autorizada de nuevos transmisores.

La invención no se limita a las realizaciones descritas sino que puede variar en construcción y en detalles.

REIVINDICACIONES

1. Un grupo de control remoto para un emplazamiento, comprendiendo el grupo:

al menos un transmisor esclavo que comprende un dispositivo de transmisión, un botón de transmisión, un procesador, un receptor de la radiación y una memoria,
un transmisor maestro para la enseñanza del transmisor esclavo, comprendiendo el transmisor maestro una memoria, un procesador y un dispositivo de transmisión y
un receptor que comprende una memoria, una interfaz para una función compartida y un procesador que comprende medios para el control de la función compartida a través de dicha interfaz,
en el que cada procesador del transmisor esclavo comprende medios para el cifrado de un código válido con una clave de cifrado para generar un código cifrado y la dirección de la transmisión del código cifrado y
en el que el procesador del receptor comprende medios para el descifrado de un código cifrado recibido para generar un código descifrado y para determinar si el código descifrado es válido,
caracterizado por que,
la clave de cifrado usada por cada procesador del transmisor esclavo para cifrar el código válido está únicamente asociada con el grupo de control remoto y cada transmisor esclavo comprende medios para el aprendizaje de la clave de cifrado en respuesta a una señal de radiación de enseñanza transmitida por el transmisor maestro;
el procesador del transmisor maestro comprende medios para la enseñanza de la clave de cifrado al transmisor esclavo y al receptor y
el procesador del receptor comprende medios para el almacenamiento de una clave de cifrado asociada únicamente con el grupo de control remoto y el uso de dicha clave de cifrado para descifrar un código cifrado recibido.

2. Un grupo de control remoto como se reivindica en la reivindicación 1, en el que el código válido es variable de acuerdo con criterios prestablecidos.

3. Un grupo de control remoto como se reivindica en la reivindicación 2, en el que el código válido comprende un índice de saltos.

4. Un grupo de control remoto como se reivindica en la reivindicación 2 ó 3, en el que el código válido comprende una combinación de un valor de discriminación fijo conocido para el receptor y un índice de saltos.

5. Un grupo de control remoto como se reivindica en la reivindicación 1, en el que el transmisor esclavo comprende medios para la generación de la clave de cifrado mediante el procesamiento de una clave fijada por el fabricante con un código del emplazamiento que es único para el grupo.

6. Un grupo de control remoto como se reivindica en la reivindicación 5, en el que el transmisor esclavo comprende medios para la recepción del código del emplazamiento en una señal de radiación de enseñanza cifrada y para el descifrado de dicha señal para determinar el código del emplazamiento usando una clave de descifrado de enseñanza.

7. Un grupo de control remoto como se reivindica en cualquier reivindicación precedente, en el que el transmisor esclavo comprende medios para el almacenamiento de un número de serie específico del transmisor y para la transmisión del número de serie junto con el código cifrado.

8. Un grupo de control remoto como se reivindica en cualquier reivindicación precedente, en el que el transmisor maestro comprende:

medios para el almacenamiento de un código del emplazamiento que es único para el grupo de control remoto,
medios para el cifrado del código del emplazamiento con una clave de cifrado de enseñanza para la enseñanza y
medios para dirigir la transmisión del código del emplazamiento cifrado en una señal de radiación de enseñanza.

9. Un grupo de control remoto como se reivindica en cualquiera de las reivindicaciones 4 a 8, en el que el procesador del receptor comprende medios para:

la identificación de un número de serie del transmisor en una transmisión recibida y la determinación de si es válido,
la identificación de un índice de saltos y un valor de discriminación en el código descifrado y
la determinación de si el valor de discriminación y el índice de saltos son válidos.

10. Un grupo de control remoto como se reivindica en la reivindicación 9, en el que el procesador del receptor comprende medios para la determinación de si el número de serie es válido mediante:

la comparación del número de serie con una lista almacenada de números de serie válidos,
la determinación de que el número de serie es válido si es el mismo que un número de serie válido almacenado o si posteriormente recibe un código cifrado nuevo que contiene el mismo número de serie y un índice de saltos válido.

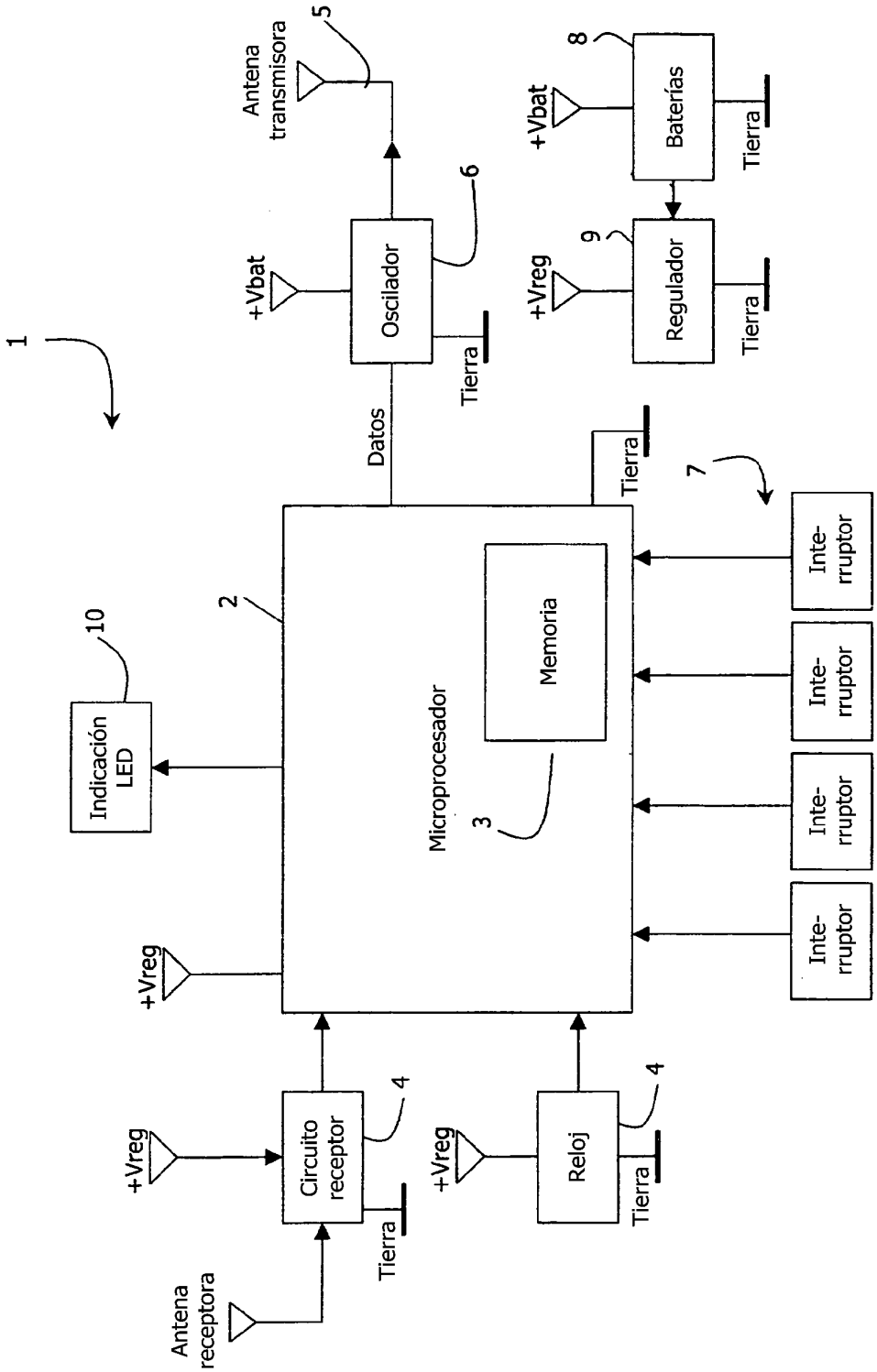
1
Antena transmisora
5
+Vbat
Oscilador
6
Tierra
Datos
+Vbat
8
Baterías
Tierra
+Vreg
9
Regulador
Tierra
Tierra
7
Inte-rruptor
Inte-rruptor
Inte-rruptor
Inte-rruptor
2
10
Indicación LED
Memoria
Microprocesador
3
+Vreg
+Vreg
Circuito receptor
4
Tierra
Antena receptora
+Vreg
Reloj
4
Tierra

Fig. 1