(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 595 384**

(51) Int. CI.:

H04N 21/422 (2011.01)
H04N 7/167 (2006.01)
G06F 21/10 (2013.01)
H04W 12/06 (2009.01)
G08C 17/02 (2006.01)
H04N 5/44 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **22.07.2011 PCT/EP2011/062684**

(87) Fecha y número de publicación internacional: **02.02.2012 WO12013608**

(96) Fecha de presentación y número de la solicitud europea: **22.07.2011 E 11741552 (1)**

(97) Fecha y número de publicación de la concesión europea: **13.07.2016 EP 2599322**

(54) Título: **Control remoto seguro para receptor/descodificador de audio/video**

(30) Prioridad:

30.11.2010 EP 10193145
26.07.2010 US 367470 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
29.12.2016

(73) Titular/es:

NAGRAVISION S.A. (100.0%)
Route de Genève 22-24
1033 Cheseaux-sur-Lausanne, CH

(72) Inventor/es:

KUDELSKI, ANDRÉ y
NICOLAS, CHRISTOPHE

(74) Agente/Representante:

TOMAS GIL, Tesifonte Enrique

DESCRIPCIÓN

Control remoto seguro para receptor/descodificador de audio/video

Introducción

[0001] La presente invención se refiere al campo de receptor/descodificador para recepción de televisión y en particular focalizado en el control remoto de dicho receptor/descodificador.

Antecedentes técnicos

[0002] Un receptor/decodificador también llamado IRD (dispositivo receptor integrado) o descodificador de señales digitales es un aparato interno conectado a una señal de entrada para recibir canales de televisión.
La señal de entrada puede ser de diferentes tipos y proporcionada por varias fuentes tal como satélite, antena de recepción terrestre, cable o conexiones IP.

[0003] La señal de entrada es luego procesada por el IRD para sintonizar o filtrar un canal solicitado por el usuario.
El IRD es generalmente conectado a una televisión que permite a un usuario observar el contenido visualizado de un canal de televisión seleccionado.

[0004] El IRD también puede comprender capacidades de grabación generalmente en un disco duro y ejecuta varias tareas relacionadas con el acceso condicional al contenido.
Para tal fin, el IRD se puede conectar a un módulo de seguridad encargado del tratamiento de mensajes de derechos de acceso, control de las condiciones de acceso y liberación de claves de autorización de acceso al contenido.

[0005] El IRD puede estar en la forma de un módulo directamente conectado en una ranura de conexión de la televisión, la señal de entrada siendo primero recibida y filtrada (o sintonizada) por la televisión y pasada al módulo que procesa las condiciones de acceso y la desencriptación de la capa de seguridad.

[0006] El IRD es dirigido por un control remoto que permite la transmisión de numerosas órdenes de usuario tales como: selección de un canal, introducción de una contraseña en caso de control parental por ejemplo, activación de una guía electrónica de programas (EPG), gestión de parámetros y perfiles de usuario, programación de grabación de contenidos, selección de varios modos de operaciones, etc.

[0007] El protocolo de comunicación entre el IRD y el control remoto siendo conocido, algunos fabricantes proponen controles remotos compatibles teniendo características mejoradas tal como la transmisión de una pluralidad de dispositivos.

[0008] Un IRD no es solo usado en un dispositivo de consumo de sentido único, sino que también se usa en un dispositivo interactivo para introducir órdenes para pedir productos, para participar en una encuesta o sencillamente para confirmar la presencia del usuario.
En este caso particular, el documento WO2009/109583 propone un mecanismo para recompensar a un usuario por observar publicidades.
Este documento describe la presentación de un carácter pseudo-aleatorio para averiguar que un usuario real está junto a la televisión antes que un control remoto modificado conectado a un sitio web que transmite automáticamente la respuesta adecuada a todos los controles remotos conectados sin requerir la presencia de ningún usuario.

[0009] El documento "Research of New Wireless Sensor Network Protocol: ZigBee RF4CE" Su Dong-Feng et al. divulga una especificación estandarizada para controles remotos basados en RF que proporcionan una solución para el sistema electrónico del consumidor que presenta una simple red de comunicaciones de bajo coste y robusta para conectividad inalámbrica en dos direcciones.
El protocolo ZigBee RF4CE sostiene un servicio de emparejamiento habilitado estableciendo un enlace de emparejamiento bajo petición a partir de una aplicación intercambiando un conjunto similar de información entre un originador y un nodo de red objetivo.
La aplicación en el nodo objetivo puede elegir si aceptar el par y confirmar la solicitud de nuevo al nodo del originador.
Si la solicitud de emparejamiento tuvo éxito, ambos nodos almacenan un enlace de emparejamiento en sus tablas de emparejamiento respectivas que permiten a un originador comunicarse con un objetivo y luego el objetivo comunica de nuevo al originador.
Cada entrada en la tabla de emparejamiento contiene toda la información necesaria para la capa de red para transmitir un marco al nodo objetivo.
Un emparejamiento dinámico de dispositivos por la creación de un canal seguro entre éstos es descrito.
La clave almacenada en los dispositivos es la misma para todos los dispositivos genuinos, por ejemplo un descodificador de señales digitales puede comunicar con todos los controles remotos genuinos ya que la clave es común para todos los controles remotos genuinos.

Para evitar exponer la clave a piratas informáticos, cambia en cada establecimiento de una comunicación y generalmente se basa o deriva de la clave común.

[0010] El documento "A Secure and Robust Connectivity Architecture for Smart Devices and Applications", Taeshik Shon et al. divulga una arquitectura de conectividad que usa RF4CE (radiofrecuencia para electrónica de consumo) basada en configuración cero inalámbrica y enfoque mejorado de acuerdo de clave.
El método de configuración cero se requiere para proporcionar conexión simple y fácil entre varios dispositivos soportados por Wi-Fi.
En particular para complementar las vulnerabilidades del esquema existente de acuerdo de claves de RF4CE un esquema de emparejamiento puede ser una buena alternativa.
Antes de que el proceso de emparejamiento inicie un terminal móvil y dispositivo objetivo tal como un aparato de TV o un ordenador personal el hecho de que cada uno proporcione un certificado realizará un proceso de autentificación mutuo.
Después de terminar el proceso de autentificación mutuo, la arquitectura de conectividad ejecuta la distribución de semillas de claves bifásicas llamada de modo rápido y modo principal.
Primero, durante el modo rápido el dispositivo objetivo entrega N semillas generadas de forma aleatoria al terminal móvil.
En cada lado, el terminal móvil y dispositivo objetivo pueden seleccionar el mismo número n de semillas entre las N semillas, y luego se usan para generar la misma clave de encriptación de enlace.
Para seleccionar n semillas, cada nodo utiliza la función de máscara de selección aleatoria que genera un número aleatorio con el tamaño de 255 bits usando la dirección y el identificador del dispositivo único previamente compartido en el procedimiento de autentificación.
En segundo lugar, durante el modo principal, todas las semillas de claves hasta 255 se transmiten al terminal móvil cada una encriptada usando claves de encriptación de semillas diferentes.
Las claves de encriptación de semillas son calculadas aplicando una función de derivación en los parámetros (dirección, identificador único, número aleatorio, semillas) del procedimiento de autentificación mutuo.
Este procedimiento mejorado de emparejamiento usa claves múltiples determinadas por N semillas transmitidas por el dispositivo objetivo al dispositivo móvil.

Breve descripción de la invención

[0011] Un objetivo principal de la presente invención es proporcionar una protección de la comunicación entre el control remoto y el IRD de modo que solo un control remoto dado pueda transmitir órdenes a un IRD dado.

[0012] Este objetivo se consigue por un sistema que comprende un dispositivo de control remoto y un dispositivo de seguridad, ambos compartiendo una clave común, algoritmos o protocolo específico para un par formado por el dispositivo de control remoto y el dispositivo de seguridad, el dispositivo de control remoto que comprende medios para enviar datos de forma inalámbrica a un receptor que comprende el dispositivo de seguridad, el dispositivo de control remoto que está emparejado con el dispositivo de seguridad se caracteriza por el hecho de que los datos enviados por el dispositivo de control remoto hacia el receptor es específico para el par formado por el dispositivo de control remoto y el dispositivo de seguridad, dicho dispositivo de control remoto comprendiendo medios de encriptación y una memoria para memorizar una clave específica, dichos datos siendo encriptados por los medios de encriptación con la clave específica, el dispositivo de seguridad comprendiendo medios de desencriptación y una clave que corresponde con la clave específica para desencriptar los datos recibidos.

[0013] Otro objeto de la invención es una unidad de ordenador portátil que incluye una aplicación configurada para compartir una clave común, algoritmos o protocolo específico para un par formado por el ordenador tableta y un dispositivo de seguridad distante de la unidad de ordenador portátil teniendo medios para enviar datos de forma inalámbrica al dispositivo de seguridad, caracterizado por el hecho de que los datos enviados por la unidad de ordenador portátil hacia el dispositivo de seguridad son específicos del par formado por la unidad de ordenador portátil y el dispositivo de seguridad, la unidad de ordenador portátil comprende medios de encriptación y una memoria para memorizar una clave específica, dichos datos siendo encriptados por los medios de encriptación con la clave específica antes del envío al dispositivo de seguridad.

[0014] La protección se puede conceder por uno de los siguientes métodos:
- utilizar un protocolo de emparejamiento para emparejar el dispositivo de control remoto con el dispositivo de seguridad de manera que la seguridad pueda solo recibir órdenes de un dispositivo de control remoto autorizado que ha sido emparejado con el dispositivo de seguridad.
Este emparejamiento puede ser uno a uno o un emparejamiento por clases es decir un emparejamiento de un dispositivo de control remoto con un grupo de dispositivos de seguridad de un mismo usuario y/o situado en una misma acomodación.
Este emparejamiento no es equivalente al emparejamiento estándar que se diseña para evitar interferencias entre dispositivos de control remoto diferentes (por ejemplo protocolo de bluetooth).
Esto significa que solo equipo autorizado, con un algoritmo y/o clave autorizados puede ser emparejado.

[0015] Un proceso de inscripción del dispositivo de control remoto se realiza durante una fase de inicialización donde

datos de emparejamiento que incluyen una clave apropiada y algoritmo se definen en el dispositivo de control remoto al igual que en el dispositivo de seguridad.
Esta inicialización puede realizarse en el proceso de fabricación de ambos dispositivos o a través del envío de la clave apropiada y algoritmo desde el dispositivo de seguridad al dispositivo de control remoto.
• el protocolo de emparejamiento puede ser una combinación de un proceso de aprendizaje de un dispositivo de control remoto "maestro" y una clave y/o un algoritmo específico que es específico de la clase de dispositivos de seguridad (o específico de un dispositivo de seguridad dado).
El proceso de inscripción del dispositivo de control remoto esclavo sigue el mismo método que la inscripción del dispositivo de control remoto maestro con el dispositivo de seguridad.
• utilización de un intercambio de datos bidireccional entre el dispositivo de seguridad y el dispositivo de control remoto transmitiendo los datos en la forma clara o encriptada y/o firmada usando criptografía o equivalente.
Este intercambio de datos dinámico se puede realizar al inicio o arranque del dispositivo de seguridad, y opcionalmente en una base regular entre el dispositivo de seguridad y el dispositivo de control remoto.
• utilización de una transmisión de datos de sentido único (o bidireccional) entre el dispositivo de control remoto y el dispositivo de seguridad con sincronización (por ejemplo temporal) y órdenes encriptadas y/o firmadas que no son previsibles para un observador externo.
• utilización de una transmisión de datos de sentido único (o bidireccional) entre el dispositivo de control remoto y el dispositivo de seguridad que es variable.
Una repetición de un comando previamente enviado no resultará en la acción prevista.

[0016] Según la presente invención, el dispositivo que contiene datos emparejados tal como una clave, algoritmos o protocolo se llama dispositivo de seguridad y puede ser el dispositivo IRD mismo o un módulo de seguridad asociado al IRD, dependiendo de las distintas formas de realización.

[0017] El dispositivo de control remoto se puede completar por una unidad portátil dedicada provista de medios de comando de usuario tal como un teclado configurado para la activación de un transmisor / receptor infrarrojo que intercambia datos encriptados entre el dispositivo de control remoto y el dispositivo de seguridad.

[0018] Según una forma de realización, el dispositivo de control remoto se compone de una unidad de ordenador portátil que tiene medios para comunicar con redes externas y provisto de al menos una aplicación de comando de usuario configurada para la activación de un transmisor / receptor de radiofrecuencia que intercambia datos encriptados entre la unidad de ordenador portátil y el dispositivo de seguridad.

[0019] La unidad de ordenador portátil puede consistir en un ordenador portátil, un ordenador tableta portátil o un teléfono inteligente.

[0020] El transmisor / receptor de radiofrecuencia puede ser de tipo Bluetooth, WiFi, o cualquier otro tipo de transmisor-receptor inalámbrico que usa ondas de radio.

Breve descripción de las figuras

[0021] La invención será mejor entendida con la siguiente descripción detallada, que se refiere a las figuras anexas dadas como ejemplos no limitativos.
La Figura 1 muestra un dispositivo de control remoto que dirige un concentrador remoto al que se conecta bien uno o una pluralidad de otros dispositivos.
La Figura 2 muestra un dispositivo de control remoto universal y de propietario que dirige un dispositivo de seguridad.
La Figura 3 muestra un dispositivo de control remoto en relación con un dispositivo intermedio conectado entre un dispositivo de seguridad y una televisión.
La Figura 4 ilustra una capa de encriptación usada en el protocolo de comunicación
La Figura 5 ilustra una caja donde dispositivos de control remoto múltiples comunican usando una capa de encriptación.

Descripción detallada de la invención

[0022] La figura 1 muestra una vía particular de uso de un dispositivo de control remoto RC universal.
Un concentrador remoto HUB recibe órdenes del dispositivo remoto RC universal gracias a un receptor IR o RF.
Comprende además un emisor IR (o emisor RF) que pasa las órdenes al dispositivo de seguridad IRD o a otro dispositivo tal como una televisión TV.
El papel del concentrador remoto HUB es filtrar y dirigir las órdenes directas enviadas por el dispositivo de control remoto RC al dispositivo apropiado.
Con un emparejamiento del dispositivo de control remoto RC con el dispositivo de seguridad IRD, este sistema ya no funcionará ya que el concentrador remoto HUB no conocerá las claves necesarias, algoritmo o protocolo usado para comunicar con el dispositivo de seguridad IRD.

[0023] De una manera similar un sistema según la figura 2 prohibirá el uso de un dispositivo de control remoto

universal URC en particular cuando se conecta a Internet para recibir órdenes de un centro de gestión.
Este podría ser particularmente útil cuando las encuestas son realizadas utilizando una política de recompensa por la observación de publicidades.
Con un dispositivo de control remoto RC personalizado o emparejado, solo una persona real puede pasar las órdenes y responder a las preguntas visualizadas en la pantalla.

[0024] Como se indica anteriormente, el dispositivo de control remoto RC genuino contiene una clave o una pluralidad de claves para encriptar la comunicación con el IRD.
Una clave o una pluralidad de claves equivalente a una del dispositivo de control remoto se almacena en el IRD para desencriptar las órdenes.
El emparejamiento entre estos dos dispositivos se consigue cuando la clave (o claves) usadas para encriptar o desencriptar esta comunicación es específica del dispositivo de control remoto IRD establecido.
En vez de encriptación, el protocolo entre el IRD y el dispositivo de control remoto puede ser específico de este par de dispositivo.
El significado de unos datos recibidos por el IRD se obtiene gracias a una tabla de consulta donde los datos recibidos son la entrada de la tabla y los datos señalados por la entrada de los datos de salida de la tabla al igual que la orden correcta.

[0025] La figura 3 muestra un caso donde un recubrimiento se añade por un dispositivo intermedio MM encima de la imagen producida por el IRD en la pantalla de la televisión TV.
Este recubrimiento puede añadir información y/o publicidad relacionada con el programa visualizado corriente.
Este dispositivo intermedio MM se puede conectar a Internet y sustituir las publicidades que vienen del IRD por publicidades generadas por el proveedor del dispositivo intermedio MM.
De la misma manera, el dispositivo de control remoto emparejado prohibirá el uso de un dispositivo de control remoto universal estándar en este caso.

[0026] El dispositivo de seguridad está preferiblemente compuesto por un módulo de seguridad conectado de manera extraíble, al receptor y configurado para el almacenamiento de al menos claves Ka, algoritmos ALG e información de protocolo requerida para el emparejamiento de dicho módulo de seguridad con el dispositivo de control remoto.
El receptor comprende así medios para enviar datos recibidos del dispositivo de control remoto al módulo de seguridad y medios para recuperar del módulo de seguridad dichos datos recibidos en forma clara para ser procesados por el receptor.
El dispositivo de control remoto y el módulo de seguridad son luego también emparejados, es decir la misma clave Ka, algoritmos ALG o protocolo se almacenan en el módulo de seguridad y el dispositivo de control remoto RC.

[0027] El IRD recibe las órdenes del dispositivo de control remoto RC y las pasa al módulo de seguridad.
En cambio, el módulo de seguridad convierte estas órdenes del propietario en un comando genérico común para todos los IRD y ejecutable por el IRD.

[0028] El dispositivo de control remoto puede tener un transmisor IR (infrarrojo), un transmisor de radiofrecuencia o ambos.
El emparejamiento se puede activar con dos o más IRD.
Según una primera forma de realización, todos los IRD comparten el mismo secreto.
Las órdenes enviadas por el dispositivo de control remoto son por lo tanto comprensibles por todos los receptores.
En otra forma de realización, el dispositivo de control remoto comprende un selector que permite la selección de un dispositivo objetivo y la carga de los datos apropiados desde una memoria que almacena diferentes datos del dispositivo objetivo.
Cada dispositivo objetivo puede así ser registrado con su propia capa de seguridad (claves o protocolo) que pueden ser consecutivamente cargados en el dispositivo objetivo.
Una inicialización se realiza para cada dispositivo de la misma manera que para un dispositivo único como se ha descrito anteriormente.

[0029] Como se ha ilustrado en la figura 5, el dispositivo de seguridad se puede emparejar con más de un dispositivo de control remoto.
En este caso, el módulo de seguridad almacena en su memoria las claves específicas KM, KS1, KS2,...KSn, algoritmos ALG0, ALG1, ALG2,..., ALGn o protocolo para cada dispositivo de control remoto.
Un dispositivo de control remoto RCM maestro y una pluralidad de dispositivos de control remoto esclavos KS1, KS2,...KSn se pueden registrar en el módulo de seguridad y emparejar, las claves de los esclavos KS1, KS2,... KSn son generadas basándose en la llave maestra KM.

[0030] En una forma de realización preferida, el mensaje enviado por cada dispositivo de control remoto que contiene los datos de comando, comprende una cabecera con un identificador para indicar qué dispositivo de control remoto está enviando actualmente este mensaje.
El dispositivo de seguridad puede luego cargar la clave correcta KM, KS1, KS2,...KSn, algoritmo ALG0, ALG1, ALG2,..., ALGn o protocolo para recuperar la orden del usuario relacionada.

[0031] En la presente invención, el dispositivo de control remoto comprende una memoria para almacenar los distintos parámetros (clave, algoritmos o protocolo) que pertenecen a la comunicación del propietario con el receptor IRD.
En el caso de una clave específica, el dispositivo de control remoto comprende medios de encriptación y una memoria para almacenar la clave específica.
En el caso de un protocolo o algoritmo específico, el dispositivo de control remoto comprende un constructor de mensaje que se parametriza según el protocolo o algoritmo específico.
Este constructor de mensajes recibe los datos de comando del usuario desde el teclado y encapsula los datos de comando del usuario en un mensaje configurado según un protocolo o algoritmo específico.
El dispositivo de seguridad IRD, cuando recibe el mensaje lo procesa usando un intérprete de mensajes que se parametriza por el protocolo o algoritmo específico de modo que los datos de comando enviados por el usuario son recuperados.

[0032] Durante una fase de inicialización el dispositivo de control remoto puede generar la clave específica (o el parámetro del protocolo o algoritmo específico) y enviarla al dispositivo de seguridad.
Esta clave puede ser bien simétrica o asimétrica.
En caso de una clave asimétrica, el dispositivo de control remoto mantiene preferiblemente la clave privada y la clave pública se envía al dispositivo de seguridad.
Después de este paso de inicialización, el dispositivo de control remoto y el dispositivo de seguridad son emparejados.

[0033] En una forma de realización, la clave específica puede ser generada, durante la fase de inicialización, basándose en al menos un identificador del dispositivo de control remoto o un identificador del dispositivo de seguridad o el identificador del dispositivo de control remoto y el identificador del dispositivo de seguridad.

[0034] Según una otra forma de realización, el dispositivo de control remoto se preinicializa por la clave, protocolo o algoritmo específico.
Este dispositivo de control remoto comprende además un identificador.
El usuario luego envía el identificador de su dispositivo de control remoto a un centro de gestión junto con un identificador del receptor IRD, dispositivo de seguridad (o módulo de seguridad).
El centro de gestión prepara un mensaje tal como un EMM (mensaje de gestión de derechos) que contiene la clave, protocolo o algoritmo específico hacia el receptor IRD que lee este mensaje y carga la clave, protocolo o datos de algoritmo en el dispositivo de seguridad.
El dispositivo de control remoto y el dispositivo de seguridad (receptor, módulo de seguridad) son así emparejados.

[0035] Según otra forma de realización relacionada con un dispositivo de control remoto compuesto por una unidad de ordenador portátil tal como un ordenador portátil, un ordenador portátil o un teléfono inteligente, los datos de emparejamiento incluyendo al menos una clave, un algoritmo y protocolo pueden ser directamente descargados de un centro de gestión bajo solicitud del usuario.
Como la unidad de ordenador portátil dispone de una conexión a Internet por medio de una red móvil inalámbrica (WiFi, 3G, GPRS, EDGE, etc.), el usuario puede registrar el dispositivo de seguridad IRD que tiene que ser emparejado usando la aplicación de control remoto previamente instalada en la unidad de ordenador portátil.
En respuesta al registro o solicitud, el centro de gestión envía los datos de emparejamiento necesarios a la unidad de ordenador portátil que los transmite al dispositivo de seguridad IRD.
El proceso de emparejamiento es luego completado cuando la aplicación de control remoto comunica con el IRD para el almacenar y compartir los datos de emparejamiento con ambos dispositivos.

[0036] Según otra forma de realización relacionada en particular con un dispositivo de control remoto compuesto por una unidad portátil dedicada para el control remoto solo sin ningún medio de comunicación a redes externas, los datos de emparejamiento se proporcionan por el IRD que tiene medios de comunicación al centro de gestión.
Una solicitud de descarga se puede enviar con el dispositivo de control remoto al dispositivo de seguridad IRD que transmite la solicitud al centro de gestión.
Una interfaz de usuario apropiada en la pantalla de la televisión conectada al IRD guía al usuario permitiéndole introducir parámetros para la solicitud y registro de IRD al igual que mensajes de visualización relacionados con la descarga de datos de emparejamiento.
Los datos de emparejamiento enviados por el centro de gestión luego seguirán el mismo camino en el orden inverso.
Este procedimiento también se puede aplicar opcionalmente por un dispositivo de control remoto en la forma de un ordenador portátil, un ordenador tableta portátil o un teléfono inteligente.

[0037] Los procedimientos de descarga son realizados no solo en el primer uso o fase de inicialización del dispositivo de control remoto y el IRD sino también en cualquier actualización o renovación de los datos de emparejamiento por ejemplo cuando el software de IRD cambia.

REIVINDICACIONES

1. Sistema que comprende un dispositivo de control remoto (RC) y un dispositivo de seguridad (IRD), ambos dispositivos que comparten una clave común (Ka), algoritmos (ALG) o protocolo específico de un par formado por el dispositivo de control remoto (RC) y el dispositivo de seguridad (IRD), la clave común (Ka) siendo generada, durante una fase de inicialización del dispositivo, basándose en al menos un identificador del dispositivo de control remoto (RC) o un identificador del dispositivo de seguridad (IRD) o el identificador del dispositivo de control remoto y el identificador del dispositivo de seguridad, el dispositivo de control remoto (RC) se configura para transmitir datos de forma inalámbrica a un receptor que comprende el dispositivo de seguridad, el dispositivo de control remoto (RC) estando emparejado con el dispositivo de seguridad (IRD) **se caracteriza por el hecho de que** éste comprende medios de encriptación y una memoria para memorizar la clave común (Ka), algoritmos (ALG) o protocolo, los datos enviados por el dispositivo de control remoto (RC) siendo encriptados por los medios de encriptación con la clave común (Ka), el dispositivo de seguridad (IRD) comprendiendo medios de desencriptación, una clave que corresponde con la clave común (Ka) y algoritmos (ALG) o protocolo, para desencriptar los datos recibidos, el dispositivo de control remoto (RC) comprende además un transmisor configurado para transmitir una solicitud de descarga de datos de emparejamiento al dispositivo de seguridad (IRD), dicho dispositivo de seguridad (IRD) estando configurado para enviar la solicitud a un centro de gestión, los datos de emparejamiento siendo transmitidos por el centro de gestión al dispositivo de control remoto (RC) por medio del dispositivo de seguridad (IRD).

2. Sistema según la reivindicación 1, **caracterizado por el hecho de que** el dispositivo de control remoto (RC) incluye una unidad portátil dedicada provista de medios de comando de usuario configurados para la activación de un transmisor / receptor infrarrojo que intercambia datos encriptados entre el dispositivo de control remoto (RC) y el dispositivo de seguridad (IRD).

3. Sistema según la reivindicación 1, **caracterizado por el hecho de que** el dispositivo de control remoto (RC) incluye una unidad de ordenador portátil provista de al menos una aplicación de comando de usuario configurada para la activación de un transmisor / receptor de radiofrecuencia que intercambia datos encriptados entre la unidad de ordenador portátil y el dispositivo de seguridad (IRD).

4. Sistema según la reivindicación 3, **caracterizado por el hecho de que** la unidad de ordenador portátil es uno de entre un ordenador portátil, un ordenador tableta portátil o un teléfono inteligente.

5. Sistema según la reivindicación 3 o 4, **caracterizado por el hecho de que** la aplicación de comando del usuario del dispositivo de control remoto (RC) es posteriormente configurada para la descarga de los datos de emparejamiento incluyendo al menos una clave, algoritmo o protocolo de un centro de gestión bajo solicitud del usuario, dichos datos de emparejamiento siendo retransmitidos al dispositivo de seguridad (IRD) por el dispositivo de control remoto (RC).

6. Sistema según alguna de las reivindicaciones 1 a 5, **caracterizado por el hecho de que** el dispositivo de control remoto (RC) comprende un constructor de mensajes parametrizado según un algoritmo (ALG) o protocolo específico, dicho constructor de mensajes encapsulando datos de comando del usuario en un mensaje configurado según el algoritmo (ALG) o protocolo específico, el dispositivo de seguridad (IRD), que comprende un intérprete de mensajes que se parametriza por el algoritmo específico (ALG) o protocolo de modo que los datos de comando del usuario son recuperados.

7. Sistema según cualquiera de las reivindicaciones 1 a 6, **caracterizado por el hecho de que** el dispositivo de seguridad (IRD) se integra en el receptor.

8. Sistema según cualquiera de las reivindicaciones 1 a 7, **caracterizado por el hecho de que** el dispositivo de seguridad (IRD) incluye un módulo de seguridad conectado de manera extraíble al receptor, el módulo de seguridad siendo configurado para el almacenamiento de al menos claves, algoritmos e información de protocolo requeridos para el emparejamiento de dicho módulo de seguridad con el dispositivo de control remoto (RC), dicho receptor siendo configurado para transmitir datos recibidos del dispositivo de control remoto (RC) al módulo de seguridad y para recuperar del módulo de seguridad dichos datos recibidos en forma clara para ser procesados por el receptor.

9. Unidad de ordenador portátil que incluye una aplicación configurada para compartir una clave común (Ka), algoritmos (ALG) o protocolo específicos para un par formado por el ordenador portátil y un dispositivo de seguridad (IRD) distante de la unidad de ordenador portátil, la clave común (Ka) siendo generada, durante una fase de inicialización del dispositivo, basándose en al menos un identificador del dispositivo de control remoto (RC) o un identificador del dispositivo de seguridad (IRD) o el identificador del dispositivo de control remoto y el identificador del dispositivo de seguridad, la unidad de ordenador portátil se configura para transmitir datos de forma inalámbrica al dispositivo de seguridad (IRD), **caracterizada por el hecho de que** éste comprende medios de encriptación y una memoria para memorizar la clave común (Ka), algoritmos (ALG) o protocolo, dichos datos siendo encriptados por los medios de encriptación con la clave común (Ka) antes de su envío al dispositivo de seguridad (IRD), la unidad de ordenador portátil comprende además un transmisor configurado para transmitir una solicitud de descarga de datos

de emparejamiento al dispositivo de seguridad (IRD), dicho dispositivo de seguridad (IRD siendo configurado para enviar la solicitud a un centro de gestión, los datos de emparejamiento siendo transmitidos por el centro de gestión a la unidad de ordenador portátil por medio del dispositivo de seguridad (IRD).

10. Unidad de ordenador portátil según la reivindicación 9, **caracterizada por el hecho de que** es uno de entre un ordenador portátil, un ordenador tableta portátil o un teléfono inteligente.

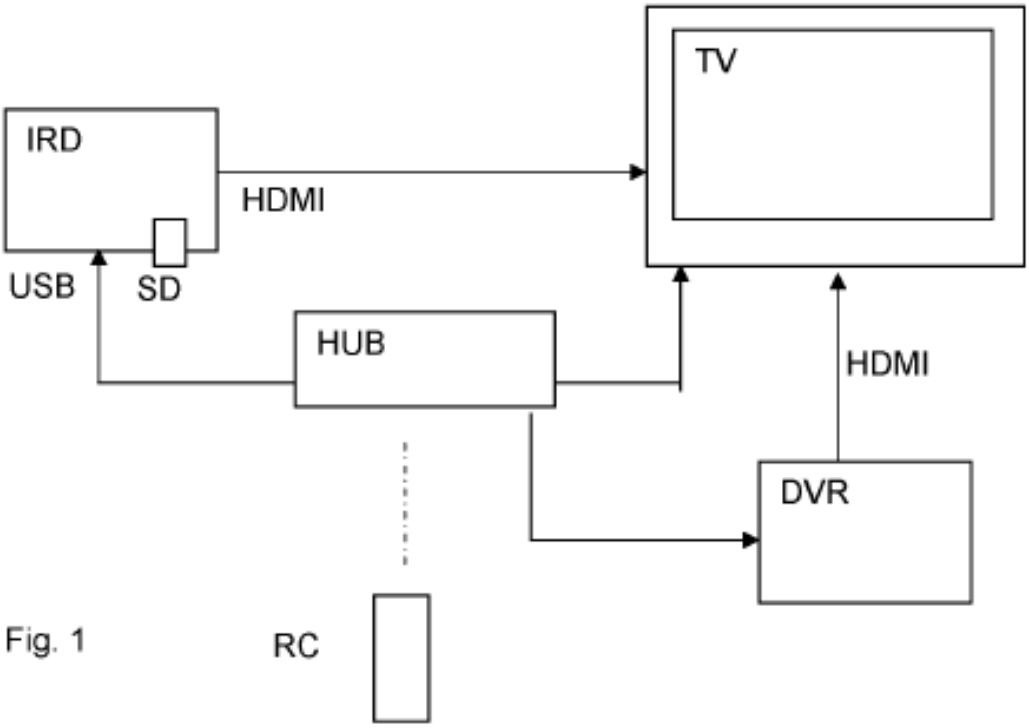

Fig. 1

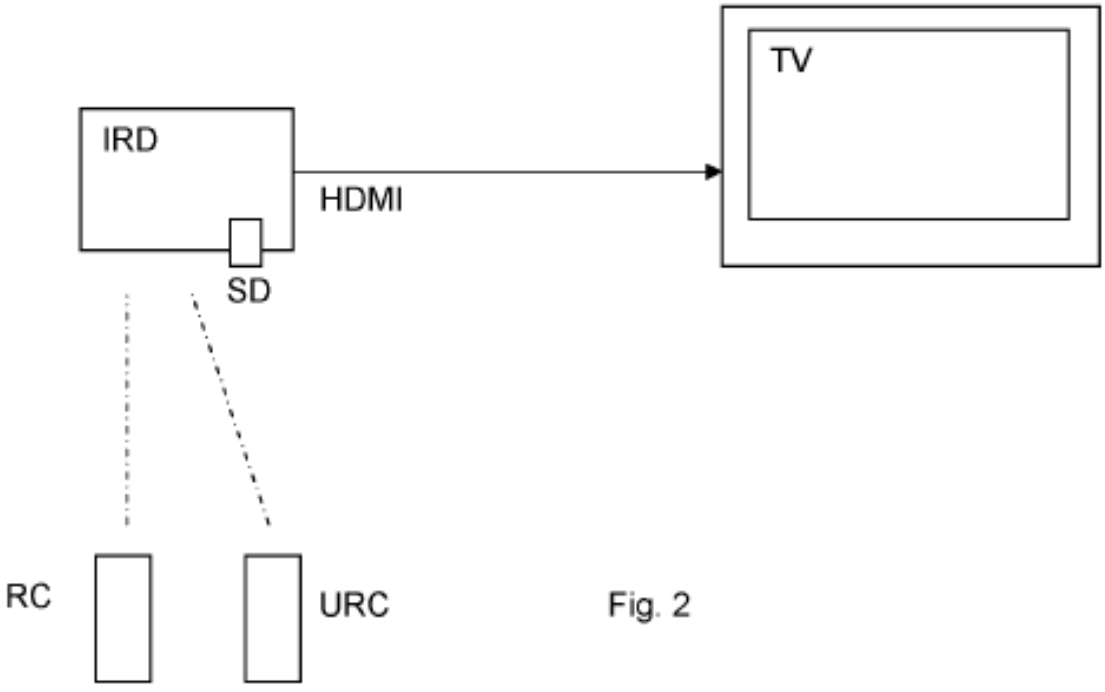

Fig. 2

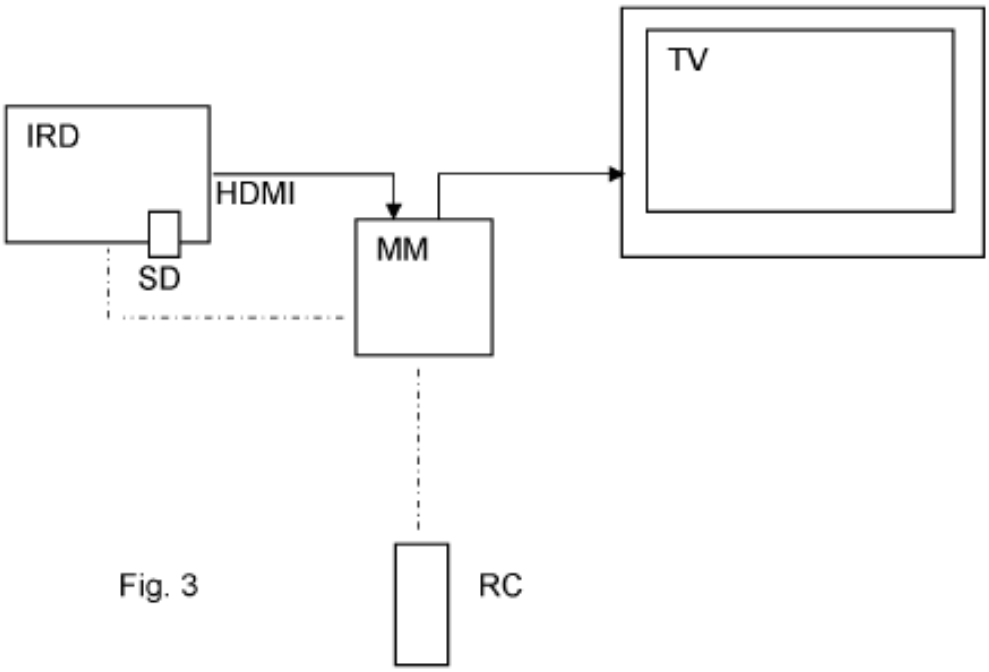
TV
IRD
HDMI
SD
MM
RC

Fig. 3

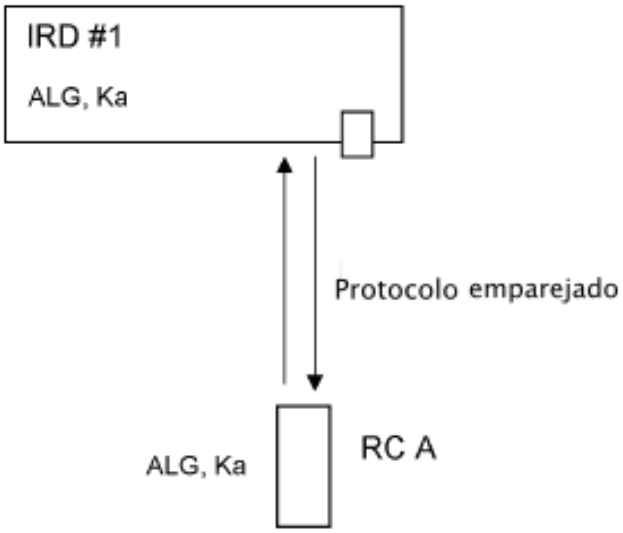
IRD #1
ALG, Ka
Protocolo emparejado
ALG, Ka
RC A

Fig. 4

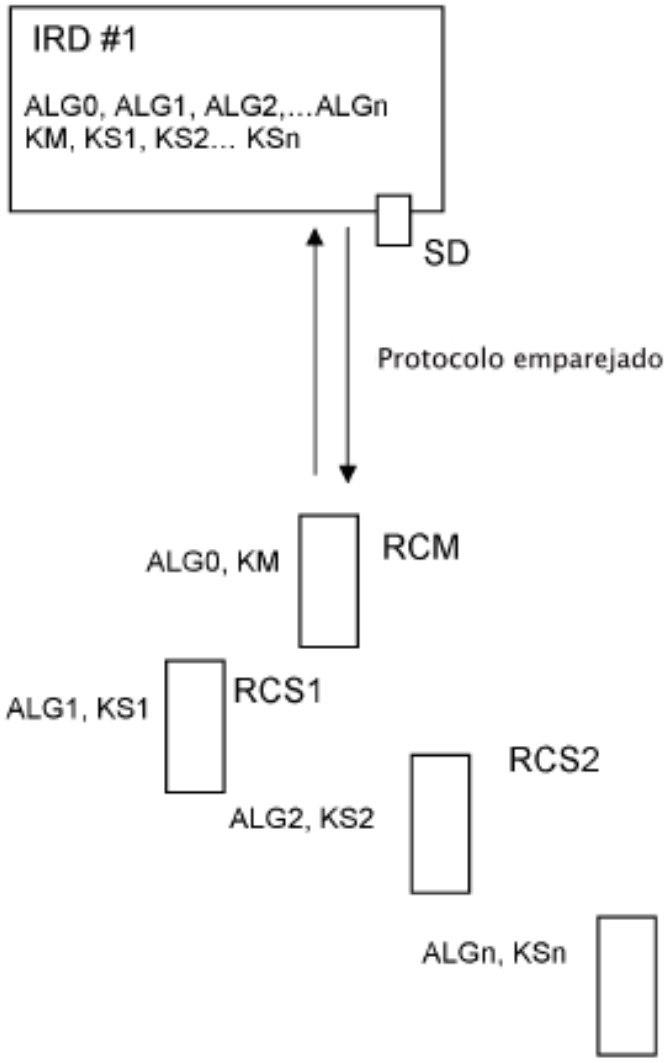
IRD #1
ALG0, ALG1, ALG2,...ALGn
KM, KS1, KS2... KSn
SD
Protocolo emparejado
ALG0, KM
RCM
ALG1, KS1
RCS1
RCS2
ALG2, KS2
ALGn, KSn
RCSn

Fig. 5