



(12) 发明专利申请

(10) 申请公布号 CN 103098482 A

(43) 申请公布日 2013.05.08

(21) 申请号 201180036416.3

(74) 专利代理机构 中国国际贸易促进委员会专

(22) 申请日 2011.07.22

利商标事务所 11038

(30) 优先权数据

代理人 王莉莉

10193145.9 2010.11.30 EP

(51) Int. Cl.

61/367,470 2010.07.26 US

H04N 21/422(2011.01)

(85) PCT申请进入国家阶段日

H04N 21/266(2011.01)

2013.01.25

H04N 21/4623(2011.01)

(86) PCT申请的申请数据

G06F 21/10(2013.01)

PCT/EP2011/062684 2011.07.22

G08C 17/02(2006.01)

(87) PCT申请的公布数据

H04N 5/44(2006.01)

WO2012/013608 EN 2012.02.02

(71) 申请人 纳格拉影像股份有限公司

权利要求书2页 说明书5页 附图3页

地址 瑞士舍索 - 苏尔 - 洛桑

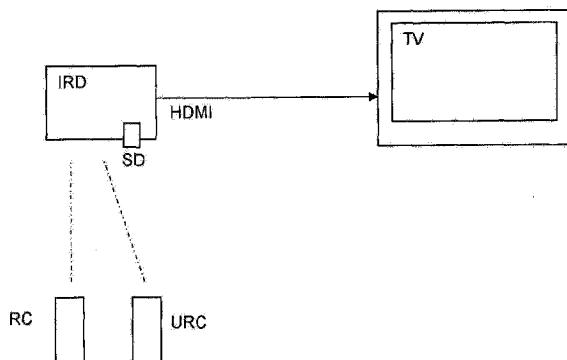
(72) 发明人 A·库德尔斯基 C·尼科拉斯

(54) 发明名称

用于音频 / 视频接收器 / 解码器的安全遥控器

(57) 摘要

为了限制通用远程控制设备的使用,本发明涉及包括远程控制设备和安全设备的系统,所述远程控制设备和所述安全设备共享由所述远程控制设备和所述安全设备形成的对所特有的公共密钥、算法或协议。所述远程控制设备包括以无线的方式发送数据至包括所述安全设备的接收器的装置。与所述安全设备配对的所述远程控制设备的特征在于:由所述远程控制设备向所述接收器发送的数据是所述远程设备和所述安全设备形成的对所特有的,所述远程控制设备包括加密装置和保存特定密钥的存储器,所述数据由所述加密装置利用所述特定密钥加密,所述安全设备包括解密装置和对应于所述特定密钥的密钥,以对接收的数据进行解密。



1. 一种包括远程控制设备和安全设备的系统，所述远程控制设备和所述安全设备共享由所述远程控制设备和所述安全设备形成的对所特有的公共密钥、算法或协议，所述远程控制设备包括以无线的方式发送数据至包括所述安全设备的接收器的装置，与所述安全设备配对的所述远程控制设备的特征在于：由所述远程控制设备向所述接收器发送的数据是所述远程设备和所述安全设备形成的对所特有的，所述远程控制设备包括加密装置和保存特定密钥的存储器，所述数据由所述加密装置利用所述特定密钥加密，所述安全设备包括解密装置和对应于所述特定密钥的密钥，以对接收的数据进行解密。

2. 根据权利要求 1 的系统，特征在于，所述远程控制设备由配备有用户命令装置的专用的便携式单元构成，所述用户命令装置被配置成激活红外发射器 / 接收器，在所述远程控制设备和所述安全设备之间交换加密的数据。

3. 根据权利要求 1 的系统，特征在于，所述远程控制设备由配备有至少一个用户命令应用程序的便携式计算机单元构成，所述至少一个用户命令应用程序被配置成激活射频发射器 / 接收器，在所述便携式计算机单元和所述安全设备之间交换加密的数据。

4. 根据权利要求 3 的系统，特征在于，所述便携式计算机单元由便携式计算机、便携式平板计算机、或智能手机中的任何一个组成。

5. 根据权利要求 3 或 4 的系统，特征在于，所述远程控制设备的所述用户命令应用程序进一步被配置成在用户请求时从管理中心下载至少包括密钥、算法或协议的配对数据，所述配对数据由所述远程控制设备重新传输至所述安全设备 IRD。

6. 根据权利要求 1 至 4 的任何一个的系统，特征在于，所述远程控制设备还包括用于传输配对数据下载请求至所述安全设备的装置，所述安全设备具有将所述请求转发给管理中心的装置，所述配对数据经由所述安全设备由所述管理中心传输至所述远程控制设备。

7. 根据权利要求 1 至 6 的任何一个的系统，特征在于，所述特定密钥是在设备初始化阶段至少基于所述远程控制设备的标识符、或所述安全设备的标识符、或所述远程设备的标识符和所述安全设备的标识符产生的。

8. 根据权利要求 1 至 7 的任何一个的系统，特征在于，所述远程控制设备包括根据特定算法或协议参数化的消息生成器，所述消息生成器将用户命令数据概述成根据特定协议或算法配置的消息，所述安全设备 IRD 包括由所述特定协议或算法参数化的消息解释器使得所述用户命令数据被取回。

9. 根据权利要求 1 至 8 中的任何一个的系统，特征在于，所述安全设备被集成在所述接收器中。

10. 根据权利要求 1 至 9 的任何一个的系统，特征在于，所述安全设备由可移除地连接至所述接收器的安全模块构成，所述安全模块被配置成至少保存使所述安全模块和所述远程控制设备配对所需的密钥、算法和协议，所述接收器包括将从所述远程控制设备接收的数据转发至所述安全模块的装置和从所述安全模块收回要被所述接收器处理的明文形式的所述接收数据的装置。

11. 一种包括应用程序的便携式计算机单元，所述应用程序被配置成共享由平板计算机和安全设备形成的对所特有的公共密钥、算法、或协议，所述安全设备远离所述便携式计算机单元，所述便携式计算机单元具有以无线的方式发送数据至所述安全设备的装置，特征在于：由所述便携式计算机单元向所述安全设备发送的数据是所述便携式计算机单元和

所述安全设备形成的对所特有的，所述便携式计算机单元包括加密装置和保存特定密钥的存储器，所述数据在发送至所述安全设备之前由所述加密装置利用所述特定密钥加密。

12. 根据权利要求 11 的便携式计算机单元，特征在于，所述便携式计算机单元由便携式计算机、便携式平板计算机、或智能手机中的任何一个组成。

用于音频 / 视频接收器 / 解码器的安全遥控器

技术领域

[0001] 本发明涉及用于电视接收的接收器 / 解码器的领域, 更具体地, 关注于所述接收器 / 解码器的遥控器。

背景技术

[0002] 接收器 / 解码器, 也称为 IRD (集成接收机装置) 或机顶盒, 是一种连接至输入信号用于接收电视频道的家用电器。该输入信号可以具有不同的类型, 并且可以由诸如卫星、陆地接收天线、电缆或 IP 连接之类的各种源来提供。

[0003] 然后, 该输入信号由 IRD 处理, 以对用户请求的频道进行调谐或过滤。IRD 通常连接至电视机, 从而允许用户观看所选择的电视频道的显示内容。

[0004] IRD 还可以包括通常位于硬盘上的记录能力并且执行与对内容的有条件的访问相关的各种任务。出于此目的, IRD 可以连接至安全模块, 该安全模块负责处理访问权限消息、检查访问条件、以及发行授权访问内容的密钥。

[0005] IRD 可以是被直接插入至电视机的连接槽中的模块的形式, 输入信号首先被电视机接收并且过滤(或调谐)然后被传递至对访问条件和安全层的解密进行处理的模块。

[0006] IRD 由允许传输诸多用户命令的遥控器驱动, 该诸多用户命令例如是 : 选择频道 ; 例如在来源控制的情况下, 输入密码 ; 激活电子节目指南(EPG) ; 管理用户参数和简介 ; 调度内容记录 ; 选择各种操作模式 ; 等等。

[0007] IRD 与遥控器之间的通信协议是已知的, 某些生产商提出了具有增强特征(如, 驱动多个装置)的可兼容遥控器。

[0008] IRD 不仅用于单向消费设备中, 还用于交互式设备中, 以输入定购货物的命令, 参与调查, 或者仅仅证实用户的存在。在该具体的情况下, 文献 WO2009/109583 提出了一种对用户观看广告进行奖励的机制。该文献描述了显示伪随机人物以查明真实用户坐在电视机旁而不是连接至网站的改良的遥控器, 该网站在无需任何用户存在的情况下自动地向所有连接的遥控器发送正确答案。

发明内容

[0009] 本发明的一个主要目的是提供对遥控器和 IRD 之间的通信的保护, 使得仅指定的遥控器可以传输命令至指定的 IRD。

[0010] 此目的由以下系统来实现, 该系统包括远程控制设备和安全设备, 所述远程控制设备和所述安全设备共享由所述远程控制设备和所述安全设备形成的对所特有的公共密钥、算法或协议, 所述远程控制设备包括以无线的方式发送数据至包括所述安全设备的接收器的装置, 与所述安全设备配对的所述远程控制设备的特征在于 : 由所述远程控制设备向所述接收器发送的数据是所述远程设备和所述安全设备形成的对所特有的, 所述远程控制设备包括加密装置和保存特定密钥的存储器, 所述数据由所述加密装置利用所述特定密钥加密, 所述安全设备包括解密装置和对应于所述特定密钥的密钥, 以对接收的数据进行

解密。

[0011] 本发明的另一对象是包括应用程序的便携式计算机单元，所述应用程序被配置成共享由平板计算机和安全设备形成的对所特有的公共密钥、算法、或协议，所述安全设备远离所述便携式计算机单元，所述便携式计算机单元具有以无线的方式发送数据至所述安全设备的装置，特征在于：由所述便携式计算机单元向所述安全设备发送的数据是所述便携式计算机单元和所述安全设备形成的对所特有的，所述便携式计算机单元包括加密装置和保存特定密钥的存储器，所述数据在发送至所述安全设备之前由所述加密装置利用所述特定密钥加密。

[0012] 可以通过下述方法之一确保所述保护：

[0013] 一使用配对协议按照安全设备仅能接收来自已经与所述安全设备配对的授权的远程控制设备的命令的方式来使所述远程控制设备和所述安全设备配对。所述配对可以是一对一，或者是类配对，即，一个远程控制设备与属于相同用户和 / 或位于相同住所 (accommodation) 的一组安全设备的配对。这种配对不等同于被设计为避免不同的远程控制设备之间的干扰的标准配对(例如，蓝牙协议)。这意味着仅具有授权的算法和 / 或密钥的授权的设备能被配对。

[0014] 在初始化阶段执行登记(enroll)远程控制设备的步骤，在该初始化阶段，在远程控制设备和安全设备中定义了包括合适的密钥和算法的配对数据。该初始化可以在远程控制设备和安全设备的制造过程中完成，或者通过从安全设备发送合适的密钥和算法至远程控制设备来完成。

[0015] 一该配对协议可以是来自“主”远程控制设备的学习处理和一类安全设备所特有的(或指定的安全设备所特有的)密钥和 / 或特定算法的组合。从远程控制设备的登记处理按照在安全设备处登记主远程控制设备的方法相同的方法来进行。

[0016] 一通过利用密码术或等同物以明文的或加密的和 / 或签名的形式传输数据来使用安全设备和远程控制设备之间的双向数据交换。这种动态数据交换可以在安全设备开启或启动时执行，并且可选地在安全设备和远程控制设备之间定期地执行这种动态数据交换。

[0017] 一通过同步(如，时间)和加密的和 / 或签名的命令使用远程控制设备和安全设备之间的单向(或双向)数据传输，该加密的和 / 或签名的命令对于外部观察者是不可预知的。

[0018] 一使用远程控制设备和安全设备之间的单向(或双向)数据传输，该数据传输是可变的。重复先前发送的命令不会导致预期动作。

[0019] 根据本发明，包含诸如密钥、算法或协议之类的配对数据的设备被称为安全设备并且可以是IRD设备自身或与IRD关联的安全模块，这取决于不同的实施例。

[0020] 远程控制设备可以由配备有用户命令装置的专用的便携式单元构成，该用户命令装置例如是小键盘并且被配置成激活红外发射器 / 接收器，在远程控制设备和安全设备之间交换加密的数据。

[0021] 根据一个实施例，远程控制设备由便携式计算机单元构成，该便携式计算机单元具有与外部网络通信的装置并且配备有至少一个用户命令应用程序，该用户命令应用程序被配置成激活射频发射器 / 接收器，在便携式计算机单元和安全设备之间交换加密的数据。

[0022] 便携式计算机单元可以由便携式计算机、便携式平板计算机或智能手机中的任何一个组成。

[0023] 射频发射器 / 接收器可以是蓝牙、WiFi 类型,或者是使用无线电波的无线接收器的其它类型。

附图说明

[0024] 根据以下涉及作为非限制性示例给出的附图的详细说明可以更好地理解本发明。

[0025] 图 1 示出了驱动远程集线器的远程控制设备,一个或多个其它设备连接至该远程集线器。

[0026] 图 2 示出了驱动安全设备的私有的和通用的远程控制设备。

[0027] 图 3 示出了与连接在安全设备和电视机之间的中间设备相连的远程控制设备。

[0028] 图 4 图示了在通信协议中使用的加密层。

[0029] 图 5 图示了其中多个远程控制设备通过使用加密层进行通信的情况。

具体实施方式

[0030] 图 1 示出了使用通用远程控制设备 RC 的一个具体方式。由于 RF 接收器的 IR,远程集线器 HUB 接收来自通用远程控制设备 RC 的命令。该远程控制设备 RC 进一步包括 IR 发射器(或 RF 发射器),将命令传递至安全设备 IRD 或诸如电视机 TV 之类的其他设备。远程集线器 HUB 的角色是过滤并且引导远程控制设备 RC 发送的命令至合适的设备。通过将远程控制设备 RC 与安全设备 IRD 配对,系统将因为远程集线器 HUB 不知道用于与安全设备 IRD 通信所需的密钥、算法或协议不再运行。

[0031] 按照类似的方式,根据图 2 的系统将禁止使用通用远程控制设备 URC,尤其是当其连接至因特网以从管理中心接收命令时。当使用针对观看广告的奖励政策来执行调查时,这将尤其有用。利用个人化或配对的远程控制设备 RC,只有真实的人才能传递命令并且回答显示在屏幕上的问题。

[0032] 如上所述,真实的远程控制设备 RC 包含一个密钥或多个密钥以对与 IRD 的通信进行加密。等同于一个远程控制设备的一个密钥或多个密钥被保存在 IRD 中以解密命令。当用于加密或解密该通信的密钥(或多个密钥)为设定的远程控制设备 IRD 所特有时,实现了这两个设备之间的配对。替代加密,IRD 与远程控制设备之间的协议可以为该设备对所特有。由于查找表,可以获得 IRD 所接收的数据的含义,在该查找表中,所接收的数据是该表的输入,并且该输入所指的数据形成表的输出数据以及正确的命令。

[0033] 图 3 示出了中间设备 MM 将覆盖图添加至由 IRD 在电视机 TV 的显示器上产生的图像之上的情况。该覆盖图可以添加与当前显示的节目相关的信息和 / 或广告。中间设备 MM 可以连接至因特网并且将来自 IRD 的广告替代为中间设备 MM 的供应商生成的广告。按照相同的方式,所配对的远程控制设备将禁止在这种情况下使用标准的通用远程控制设备。

[0034] 安全设备优选地由可移除地连接至接收器的安全模块构成,该安全模块被配置成至少保存配对所述安全模块和所述远程控制设备所需的密钥 Ka、算法 ALG、以及协议信息。由此,该接收器包括将从远程控制设备接收的数据转发至安全模块的装置和从所述安全模块取回要被所述接收器处理的明文形式的所述接收数据的装置。然后,远程控制设备和安

全模块也被配对,即,相同的密钥 Ka、算法 ALG、或协议被保存在安全模块和远程控制设备 RC 中。

[0035] IRD 接收来自远程控制设备 RC 的命令并且将这些命令传递至安全模块。作为回报,安全设备将这些私有命令转化成所有 IRD 共有的并由 IRD 执行的通用命令。

[0036] 远程控制设备可以具有 IR (红外) 发射器、射频发射器或这两者。可以利用两个或多个 IRD 来激活该配对。根据第一实施例,所有 IRD 共享相同的秘密(secret)。因此,所有接收器均能理解远程控制设备发送的命令。在另一个实施例中,远程控制设备包括选择器,该选择器允许选择目标设备并且从保存多个目标设备数据的存储器加载合适的数据。因此,每个目标设备可以利用其自己的安全层(密钥或协议)来被记录,该安全层顺序地被加载至目标设备。按照与以上针对单个设备进行初始化的方式相同的方式来针对每个设备执行初始化。

[0037] 如图 5 所示,安全设备可以与不只一个的远程控制设备配对。在这种情况下,安全模块在其存储器中针对每个远程控制设备保存特定密钥 KM、KS1、KS2…KSn,算法 ALG0、ALG1、ALG2…ALGn,或协议。主远程控制设备 RCM 和多个从远程控制设备 KS1、KS2…KSn 可以被记录在安全模块中并且被配对,从远程控制设备 KS1、KS2…KSn 的密钥是基于主密钥 KM 生成的。

[0038] 在优选的实施例中,由每个远程控制设备发送的包含命令数据的消息包括具有指示哪个远程控制设备当前正在发送该消息的指示符的标题。然后,安全设备可以加载正确的密钥 KM、KS1、KS2…KSn,算法 ALG0、ALG1、ALG2…ALGn,或协议,以取回相关用户的命令。

[0039] 在本发明中,远程控制设备包括保存各种参数(密钥、算法或协议)的存储器,这些参数关于与接收器 IRD 的私有通信。在特定密钥的情况下,远程控制设备包括加密装置和保存特定密钥的存储器。在特定协议或算法的情况下,远程控制设备包括根据该特定协议或算法参数化的消息生成器。该消息生成器接收来自小键盘的用户命令数据并且将该用户命令数据概述成根据特定协议或算法配置的消息。安全设备 IRD 在接收消息时通过使用消息解释器来处理该消息,通过特定协议或算法来使该消息解释器参数化,使得取回用户发送的命令数据。

[0040] 在初始化阶段,远程控制设备可以生成特定密钥(或特定协议或算法的参数)并且将其发送至安全设备。该密钥可以是对称的也可以是不对称的。假如是不对称密钥,则远程控制设备优先地保留专用密钥并且公开密钥被发送至安全设备。在该初始化步骤之后,远程控制设备和安全设备被配对。

[0041] 在一个实施例中,可以在初始化阶段至少基于远程控制设备的标识符、安全设备的标识符、或者远程控制设备的标识符和安全设备的标识符来生成该特定密钥。

[0042] 根据又一个实施例,通过特定密钥、协议或算法将远程控制设备预初始化。该远程控制设备进一步包括标识符。然后,用户连同 IRD 接收器、安全设备(或安全模块)的标识符一起发送其远程控制设备的标识符至管理中心。管理中心为 IRD 接收器预备包含特定密钥、协议或算法的诸如 EMM (授权管理信息) 的消息,该 IRD 接收器读取该消息并且将密钥、协议或算法数据加载至安全设备。由此,远程控制设备和安全设备(接收器、安全模块)被配对。

[0043] 根据与由诸如便携式计算机、便携式平板计算机或智能手机之类的便携式计算

机单元构成的远程控制设备相关的又一个实施例,响应于用户请求,可以直接从管理中心下载至少包括密钥、算法和协议的配对数据。由于便携式计算机单元经由无线移动网络(WiFi, 3G, GPRS, EDGE, 等等)配备有因特网连接,用户可以通过使用先前安装在便携式计算机单元中的远程控制应用程序注册要配对的安全设备IRD。响应于该注册或请求,管理中心发送必要的配对数据至便携式计算机单元,便携式计算机单元将这些必要的配对数据重新传输至安全设备IRD。然后,当远程控制应用程序与IRD通信以保存并且与远程控制设备和安全设备共享配对数据时,该配对处理结束。

[0044] 根据具体地与由专用于远程控制并且没有任何至外部网络的通信装置的便携式单元构成的远程控制设备相关的又一个实施例,配对数据是由具有至管理中心的通信装置的IRD提供的。可以利用远程控制设备将下载请求发送至安全设备IRD,安全设备IRD将该请求转发至管理中心。连接至IRD的电视机的屏幕上的合适的用户界面通过允许输入针对请求和IRD注册的参数以及通过显示与配对数据下载相关的消息来引导用户。然后,管理中心发送的数据按照相反的顺序遵循相同的路径。该处理也可以可选地由具有便携式计算机、便携式平板计算机、或智能手机的形式的远程控制设备来应用。

[0045] 该下载护理不仅仅在远程设备和IRD的第一次使用或初始化阶段执行,还在配对数据的任何更新或恢复时执行,例如,当IRD软件变化时。

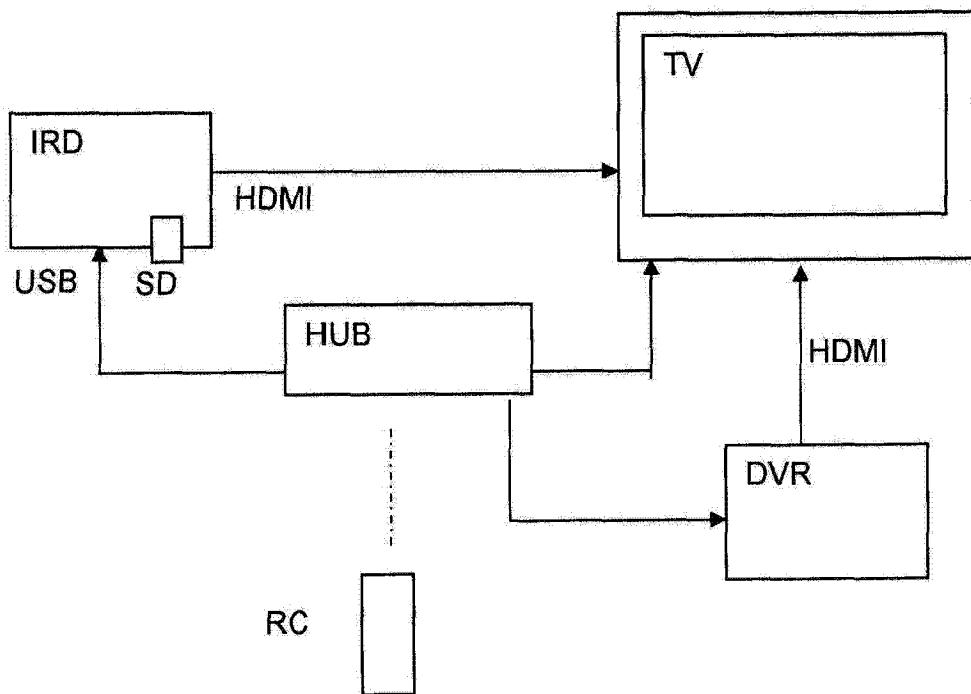


图 1

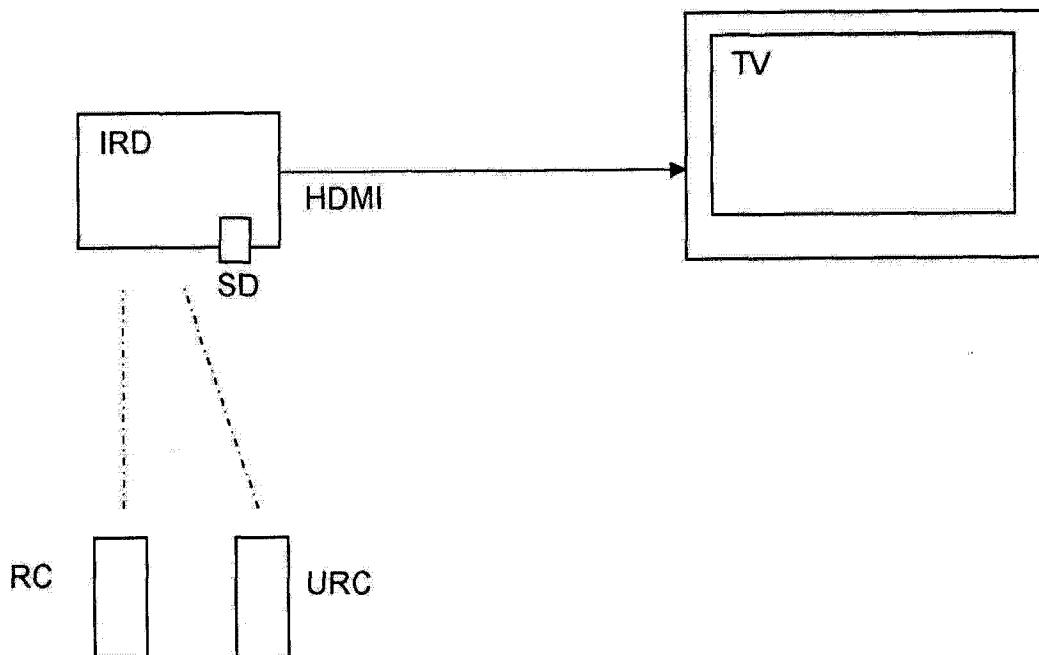


图 2

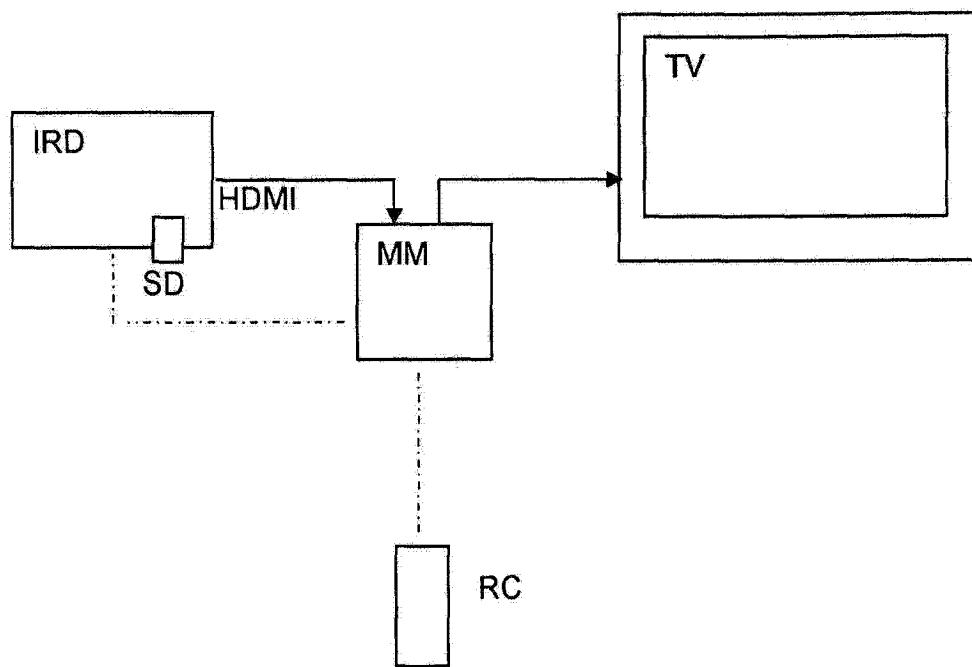


图 3

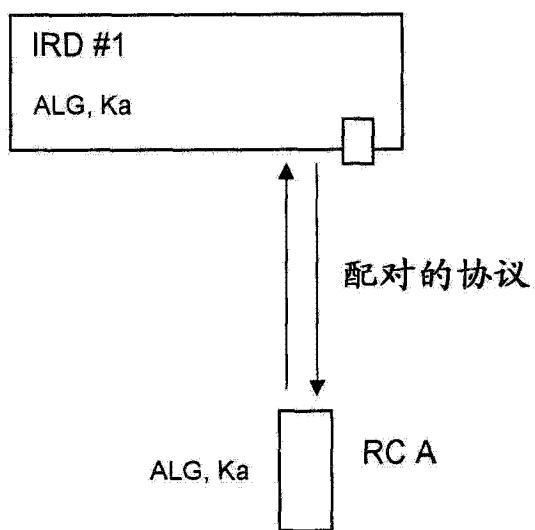


图 4

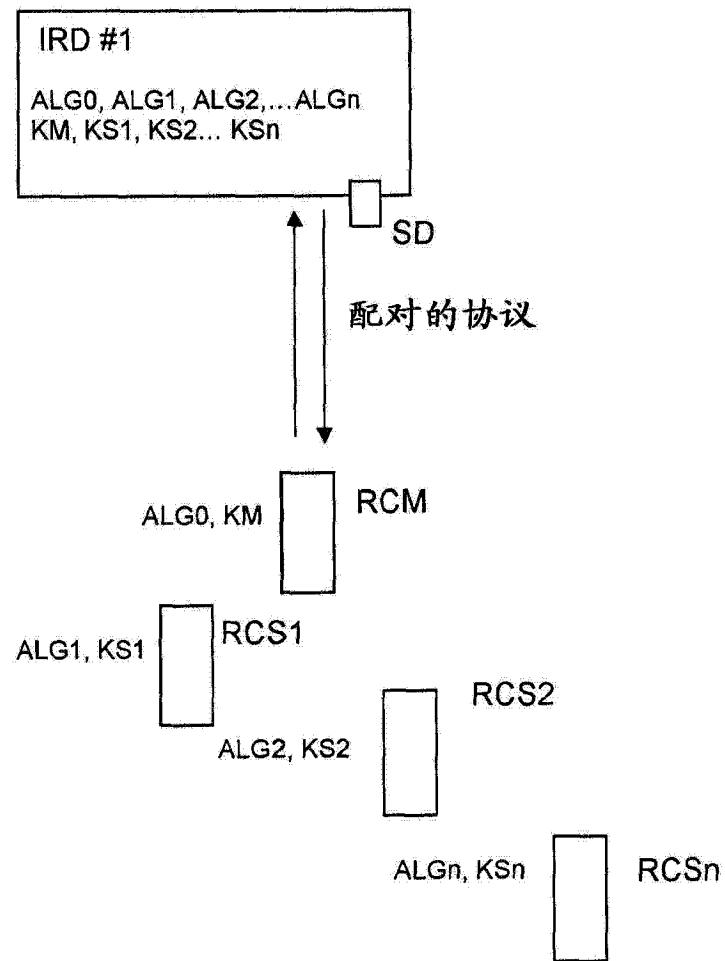


图 5