(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 104967514 A
(43)申请公布日 2015.10.07

(21)申请号 201510346154.0
(22)申请日 2010.08.30
(30)优先权数据
2009-208687 2009.09.09 JP
2010-117832 2010.05.21 JP
(62)分案原申请数据
201080039101.X 2010.08.30
(71)申请人 索尼公司
地址 日本东京都
(72)发明人 中野雄彦
(74)专利代理机构 北京市柳沈律师事务所 11105
代理人 郭定辉
(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/08(2006.01)
H04N 21/258(2011.01)
H04N 21/6334(2011.01)

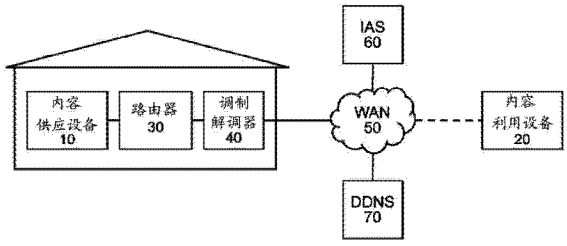
权利要求书2页 说明书21页 附图18页

(54)发明名称

信源设备及其产生解密已加密内容的信号的方法

(57)摘要

公开了信源设备。所述信源设备包括：第一授权部分，配置为将命令发送到所述条件访问设备，并从所述条件访问设备接收对所述命令的响应；登记部分，配置为当所述命令的发送和所述响应的接收之间经过的时间不超过预定时间时，登记所述条件访问设备；以及第二授权部分，配置为不用确认往返时间(RTT)地产生允许条件访问的信号，其中，所述登记部分登记多个条件访问设备，并且已加密内容可从所述多个条件访问设备中的一个或一些中远程地进行访问。



CN 104967514 A

1. 一种用于选择性地产生允许条件访问设备解密已加密内容的信号的信源设备，所述信源设备包括：

第一授权部分，配置为将命令发送到所述条件访问设备，并从所述条件访问设备接收对所述命令的响应；

登记部分，配置为当所述命令的发送和所述响应的接收之间经过的时间不超过预定时间时，登记所述条件访问设备；以及

第二授权部分，配置为不用确认往返时间（RTT）地产生允许条件访问的信号，

其中，所述登记部分登记多个条件访问设备，并且已加密内容可从所述多个条件访问设备中的一个或一些中远程地进行访问。

2. 如权利要求 1 所述的信源设备，其中，当已经向所述信源设备登记所述条件访问设备时满足非 RTT 条件。

3. 如权利要求 2 所述的信源设备，其中，当以下情况时满足非 RTT 条件：

已经向所述信源设备登记所述条件访问设备；和

所述内容已经

指定为可远程访问；或者

未指定为远程不可访问。

4. 如权利要求 3 所述的信源设备，其中，仅当下列情况时满足所述非 RTT 条件：

已经向所述信源设备登记所述条件访问设备；和

所述内容已经指定为可远程访问。

5. 如权利要求 1 所述的信源设备，其中，所述登记部分配置为：

发送第二命令到所述条件访问设备；和

从所述条件访问设备接收对所述第二命令的第二响应。

6. 如权利要求 5 所述的信源设备，其中，当在所述第二命令的传输和所述第二响应的接收之间经过的第二时间不超过第二预定时间时，向所述信源设备登记所述条件访问设备。

7. 如权利要求 1 所述的信源设备，其中，在任意一个时间仅可以向信源设备登记阈值以下的数目的条件访问设备。

8. 如权利要求 1 所述的信源设备，其中，所述允许条件访问的信号包括用于产生用于解密内容的内容密钥的交换密钥。

9. 如权利要求 8 所述的信源设备，其中，所述允许条件访问的信号包括用于产生内容密钥的随机数。

10. 如权利要求 1 所述的信源设备，其中，预定时间是 7 毫秒。

11. 一种用于通过信源设备选择性地产生允许条件访问设备解密已加密内容的信号的方法，所述方法包括：

发送命令到所述条件访问设备；

从所述条件访问设备接收对所述命令的响应；

当在所述命令的发送和所述响应的接收之间经过的时间不超过预定时间时，登记多个条件访问设备；并且

产生允许条件访问而不用确认往返时间（RTT）的信号，

其中，内容信息可从多个条件访问设备中的一个或一些中远程地进行访问。

信源设备及其产生解密已加密内容的信号的方法

[0001] 交叉参考

[0002] 本申请是申请日为2010年8月30日、于2012年3月2日提交到中国专利局、发明名称为“通信系统、通信设备、通信方法和计算机程序”、申请号为201080039101.X的PCT发明申请的分案申请。

技术领域

[0003] 本发明涉及用于防止内容传输中的非法使用的通信系统、通信设备和通信方法，更具体地，涉及用于根据预定相互验证和密钥交换(AKE:验证和密钥交换)算法来交换用于加密内容的解密密钥以及发送加密内容的通信系统、通信设备和通信方法。

[0004] 更具体地，本发明涉及用于经由使用比如WAN之类的外部网络的远程访问(RA)来安全地发送内容的通信系统，和用于当超过关于往返时间(RTT)、IP(因特网协议)路由器的跳数等的限制时经由远程访问安全地发送内容的通信设备和通信方法，更具体地，涉及通信系统、通信设备和通信方法。

背景技术

[0005] 在过去，广播内容和在封装介质中的内容已经基本上用在安装接收设备或者再现设备的位置或者用在经由家庭网络连接到那些设备的设备中(在下文中，也称为“本地访问(LA)”)。例如，从通信路径、编解码器等的技术观点来看，已经难以使用便携式设备从外部连接接收设备或者再现设备并使用经由比如WAN(广域网)之类的外部网络发送的内容(在下文中，也称为“远程访问(RA)”)。但是，在将来预期比如LTE(长期演化)和WiMAX(微波访问的世界互用性)之类的数据通信技术和比如H.264之类的高压缩编解码器将流行。因此，存在将通过使用那些技术来实现远程访问的可能性。例如，用户可以从外部远程访问家庭服务器并再现内容。

[0006] 另一方面，在复制、伪造等时数字化内容相对容易操作。首先，在远程访问时，需要用于防止在内容传输中发生的非法使用的机制，即，需要在允许内容的个体或者局部使用时的版权保护。

[0007] 作为关于数字内容的传输保护的工业标准技术，存在由DTLA(数字传输许可管理者)开发的DTCP(数字传输内容保护)。在DTCP中，布置用于内容传输的设备间验证协议和加密内容的传输协议。简而言之，规定符合DTCP的设备不以未加密状态发送容易处理的压缩内容到外部设备，根据预定相互验证和密钥交换(AKE)算法产生解密加密内容所需的交换密钥，限制基于AKE命令交换密钥的设备的范围，等等。作为内容供应商(信源)的服务器和作为内容供应目的地(信宿)的客户端通过交换AKE命令来经由验证处理而共享密钥，因此通过使用密钥加密传输路径来执行内容传输。因此，由于未授权的客户端除非与服务器验证成功，否则不能获得加密密钥，所以未授权的客户端不能欣赏内容。

[0008] DTCP最初规定例如使用IEEE1394作为传输路径的家庭网络中的内容传输。近年来，也全力进行尝试如由DLNA(数字生活网络联盟)表示的、经由IP网络局部地循环数字

化 AV 内容的活动。在这点上，对于经由 IP 网络局部地循环数字内容的尝试，正在开发支持 IP 网络的 DTCP 技术，即，DTCP-IP(DTCP 映射到 IP)。

[0009] DTCP-IP 是其中将 DTCP 技术移植到 IP 网络的类似技术。DTCP-IP 使用 IP 网络作为传输路径并使用在 IP 网络上实现的内容传输协议，比如 HTTP(超文本传送协议)和 RTP(实时传送协议)，以发送加密内容。当根据 HTTP 处理发送内容时，例如，通过创建用于 HTTP 的 TCP/IP 连接来执行加密内容的下载传输，其中信源是 HTTP 服务器且信宿是 HTTP 客户端(假设在执行上载传输时，信源变为 HTTP 客户端且信宿变为 HTTP 服务器)。

[0010] 当前 DTCP-IP(DTCP 卷 1 规范补充 E 修订版 1.2) 主要意在保证仅内容的局部使用。因此，往返时间 (RTT :往返时间) 关于 AKE 命令最大限于 7 毫秒，且 IP 路由器的跳数的上限 (TTL :生存周期) 设置为 3。

[0011] 例如，提出了如下的信息通信系统，其从开始 DTCP-IP 验证起持续监控每一接收到的 AKE 命令并持续更新 TTL 值的最大值直到正好在信源结束 DTCP-IP 验证之前为止，检查正好在验证处理结束之前 TTL 值的最大值，当最大值是 3 或者更少时交换密钥并结束验证处理，并且当最大值超过 3 时结束验证处理而不执行最后阶段的处理(参见，例如，日本专利申请特开 No.2007-36351)。

[0012] 但是，当施加关于 RTT 和 TTL 的限制时，难以从家庭外的远程位置访问在局部家庭网络的服务器中的版权保护的内容。

[0013] 尽管考虑到用户友好性，期望允许关于内容的远程访问，但是它与希望保护版权的内容所有者的利益矛盾。

[0014] [引文列表]

[0015] [专利文献]

[0016] [PTL1] 日本专利申请特开 No.2007-36351

发明内容

[0017] 技术问题

[0018] 考虑如上所述的情况，存在能够通过根据预定相互验证和密钥交换 (AKE) 算法来交换用于加密内容的解密密钥来有利地防止内容传输中的非法使用的优良的通信系统、通信设备、通信方法和计算机程序的需要。

[0019] 还存在能够在超过往返时间 (RTT)、IP 路由器的跳数 (TTL) 等的限制时，经由使用比如 WAN 之类的外部网络的远程访问来安全地发送内容的优良的通信系统、通信设备、通信方法和计算机程序。

[0020] 技术方案

[0021] 因此，公开了用于选择性地产生信号以允许解密已加密内容的条件访问设备。该条件访问设备可以包括第一和第二授权部分。第一授权部分可以配置为接收由信源设备发送的命令，并将对该命令的响应发送到信源设备。第一授权部分也可以配置为一旦接收到指示在信源设备的命令发送和信源设备的响应接收之间经过的时间不超过预定往返时间 (RTT) 的指示信号，就产生允许内容的解密的第一授权信号。第二授权部分可以配置为无论何时满足非 RTT 条件，都产生允许内容的解密的第二授权信号。

[0022] 还公开了用于选择性地产生允许条件访问设备解密加密内容的信号的信源设备。

信源设备可以包括第一和第二授权部分。第一授权部分可以配置为发送命令到条件访问设备，并从条件访问设备接收对该命令的响应。第一授权部分还可以配置为当在命令的发送和响应的接收之间经过的时间不超过预定往返时间 (RTT) 时，产生允许条件访问设备解密内容的第一授权信号。第二授权部分可以配置为无论何时满足非 RTT 条件，都产生允许条件访问设备解密内容的第二授权信号。

[0023] 另外，公开了用于通过条件访问设备选择性地产生信号以允许解密已加密内容的方法。处理器可以执行程序以使得条件访问设备执行该方法。该程序可以存储在条件访问设备的存储器上或存储在另一计算机可读存储介质上。该方法可以包括接收由信源设备发送的命令，并将对该命令的响应发送到信源设备。该方法还可以包括，一旦接收到指示在信源设备的命令的发送和信源设备的响应的接收之间经过的时间不超过预定往返时间 (RTT) 的指示信号，就产生允许内容的解密的第一授权信号。另外，该方法可以包括，无论何时满足非 RTT 条件，都产生允许内容的解密的第二授权信号。

[0024] 还公开了用于通过信源设备选择性地产生信号以允许条件访问设备解密加密内容的方法。处理器可以执行程序以使得信源设备执行该方法。该程序可以存储在信源设备的存储器上或存储在另一计算机可读存储介质上。该方法可以包括发送命令到条件访问设备，和从条件访问设备接收对该命令的响应。该方法还可以包括，当在命令的发送和响应的接收之间经过的时间不超过预定往返时间 (RTT) 时，产生允许条件访问设备解密内容的第一授权信号。另外，该方法可以包括，无论何时满足非 RTT 条件，都产生允许条件访问设备解密内容的第二授权信号。

[0025] 还公开了用于选择性地产生允许条件访问设备解密已加密内容的信号的信源设备，所述信源设备包括：第一授权部分，配置为将命令发送到所述条件访问设备，并从所述条件访问设备接收对所述命令的响应；登记部分，配置为当所述命令的发送和所述响应的接收之间经过的时间不超过预定时间时，登记所述条件访问设备；以及第二授权部分，配置为不用确认往返时间 (RTT) 地产生允许条件访问的信号，其中，所述登记部分登记多个条件访问设备，并且已加密内容可从所述多个条件访问设备中的一个或一些中远程地进行访问。

[0026] 还公开了用于通过信源设备选择性地产生允许条件访问设备解密已加密内容的信号的方法，所述方法包括：发送命令到所述条件访问设备；从所述条件访问设备接收对所述命令的响应；当在所述命令的发送和所述响应的接收之间经过的时间不超过预定时间时，登记多个条件访问设备；并且产生允许条件访问而不用确认往返时间 (RTT) 的信号，其中，内容信息可从多个条件访问设备中的一个或一些中远程地进行访问。

[0027] 应当注意，在这里使用的“系统”指的是其中逻辑地组装多个设备（或实现特定功能的功能模块）的系统，且设备或功能模块是否存在于单个外壳内并不特别相关。

[0028] 本发明的这些和其它目的、特征和优点将通过以下如附图图示的其具体实施方式的详细说明而变得更加明显。

附图说明

[0029] 图 1 是示意性地示出了根据本发明的实施例的通信系统的结构实例的图；

[0030] 图 2 是示意性地示出了根据本发明实施例的通信系统的另一结构实例的图；

[0031] 图 3 是示意性地示出了内容供应设备的功能结构的图；

[0032] 图 4 是示意性地示出了内容利用设备的功能结构的图；

[0033] 图 5 是用于解释通过 DTCP-IP 在信源和信宿之间执行加密内容传输的机制的图；

[0034] 图 6 是示出了根据当前 DTCP-IP 在信源和信宿之间执行的、使用 AKE 命令的相互验证和密钥交换的操作序列的图；

[0035] 图 7 是示出了在 RA- 信源中登记 RA- 信宿时的验证序列的实例的图；

[0036] 图 8 是示出了用于 RA- 信源登记 RA- 信宿的“RA- 信宿登记”处理的过程的流程图；

[0037] 图 9 是示出了在 RA- 信源向 RA- 信宿提供远程访问交换密钥时的验证序列的实例的图；

[0038] 图 10 是示出了用于 RA- 信源确认 RA- 信宿的登记和要提供的远程访问交换密钥的数目的“RA- 信宿 ID 确认”处理的过程的流程图。

[0039] 图 11 是示意性地示出了其中 RA- 信源和 RA- 信宿以菊花链模式另外连接到另一设备且可以另外输出接收到的内容的系统结构的实例的图；

[0040] 图 12 是示意性地示出了其中 RA- 信源和 RA- 信宿以菊花链模式另外连接到另该设备且可以另外输出接收到的内容的系统结构的实例的图；

[0041] 图 13 是示意性地示出了其中 RA- 信源和 RA- 信宿以菊花链模式另外连接到另该设备且可以另外输出接收到的内容的系统结构的实例的图；

[0042] 图 14 是示出了在 Source#0 通过执行 DEP-RA-AKE 仅与 Sink#1 共享密钥时的验证序列的实例的图；

[0043] 图 15 是示出了用于信源对于远程访问输出的替换验证信宿的“DEP_RA- 信宿确认”处理的过程的流程图；

[0044] 图 16 是示出了在 RA- 信宿同时发送相同内容的数目受限的情况下 RA- 信宿从 RA- 信源请求内容时的操作序列的图；

[0045] 图 17 是示出了用于管理相同内容的输出数目的、由 RA- 信源响应于内容数据的请求而执行的处理过程的流程图。

[0046] 图 18 是示出了用于作为 RA- 信源操作的设备通过 MOVE 功能来记录内容或者接受内容的处理过程的流程图；

[0047] 图 19 是示出了 RA- 信宿从 RA- 信源请求内容的操作序列的图；

[0048] 图 20 是示出了内容远程访问 (RA) 输出计数管理 1 的处理过程的流程图；

[0049] 图 21 是示出了信宿从信源请求内容以代替远程访问的操作序列的图；

[0050] 图 22 是示出了内容远程访问输出替换管理的处理过程的流程图；

[0051] 图 23 是用于解释防止 RA- 标记的伪造的方法的实例的图，更具体地，示出了将 RA- 标记的值输入到用于计算加密密钥的函数并在加密密钥 Kc 的值上反映其的方法的图；

[0052] 图 24 是用于解释防止 RA- 标记的伪造的方法的实例的图，更具体地，示出了处理要通过散列函数以纯文本发送的加密密钥和包含 RA- 标记的信息并获得签名数据的方法；

[0053] 图 25 是用于解释防止 RA- 标记的伪造的方法的实例的图，更具体地，示出了与内容数据一起加密 RA- 标记时的存储目的地的图；

[0054] 图 26 是用于解释防止 RA- 标记的伪造的方法的实例的图，更具体地，示出了与内

容数据一起加密 RA- 标记时的存储目的地的图；

[0055] 图 27 是示出了 RA- 信源更新对于内容设置的 RA- 标记和 T 的处理过程的流程图；

[0056] 图 28 是示出了用于远程访问的 AKE 控制命令的结构实例的图；

[0057] 图 29 是示出了要应用于内容供应设备的个人计算机的结构实例的图；

[0058] 图 30 是示出了要应用于内容供应设备的记录器的结构实例的图。

具体实施方式

[0059] 本发明涉及用于经由使用比如 WAN 之类的外部网络的远程访问 (RA) 安全地发送内容的通信系统。该通信系统基本上由通过远程访问提供内容的服务器 (RA- 信源) 和通过远程访问请求内容的客户端 (RA- 信宿) 构成。在说明书中，在远程访问时执行的 AKE 处理将被称为“RA-AKE”。在下文中，将参考附图具体地描述本发明的实施例。

[0060] 图 1 示意性地示出了根据本发明的实施例的通信系统的结构实例。在如图所示的通信系统中，与 RA- 信源对应的信源设备 (例如，内容供应设备 10) 在家庭内提供，且与 RA- 信宿对应的条件访问设备 (例如，内容利用设备 20) 在外部提供。内容利用设备 20 使用类似蜂窝电话的通信功能来远程访问内容供应设备 10。

[0061] 内容供应设备 10 经由通用的路由器 30 和调制解调器 40 连接到比如 WAN 50 的外部网络。WAN 50 例如是因特网。在 WAN 50 侧上的 IP 地址被从用户签约的因特网访问服务 (IAS) 提供商 60 分配给路由器 30。内容利用设备 20 原则上也访问该 IP 地址。路由器 30 将私人 IP 地址分配给内容供应设备 10，并通过关于经由 WAN 50 的访问转发的端口中继通信。应当注意，可以由 IAS 提供商 60 更新分配给路由器 30 的 IP 地址。在这种情况下，可以使用 DDNS 服务 70 来使用路由器 30 或者内容供应设备 10 的 DDNS(动态 DNS(域名系统)) 功能。

[0062] 图 2 示意性地示出了根据本发明实施例的通信系统的另一结构实例。在如图所示的通信系统中，对应于 RA- 信宿的内容利用设备 20 也在家庭内提供并经由路由器 31 和调制解调器 41 连接到 WAN 50。从内容利用设备 20 发出的 TCP/IP(传输控制协议 / 因特网协议) 通信由路由器 31 的 NAT(网络地址翻译) 功能地址转换，但是除此之外与图 1 的情况下的相同。

[0063] 图 3 示意性地示出了内容供应设备 10 的功能结构。内容供应设备 10 包括 CPU(中央处理单元)11、内容接收 / 再现部分 12、通信部分 13、存储部分 14 和计时器 15，并用作通过远程访问发送内容的 RA- 信源。

[0064] 内容接收 / 再现部分 12 具有广播接收功能和封装介质再现功能。CPU 11 恰当地保护由内容接收 / 再现部分 12 获得的可远程访问的内容，并此后经由通信部分 13 将其发送到已经经历通过 RA-AKE 的相互验证和密钥交换的 RA- 信宿 (内容利用设备 20)。

[0065] 存储部分 14 存储已经变得需要由将在后面描述的登记处理存储的 RA- 信宿的识别信息、经由 RA-AKE 与 RA- 信宿共享的远程访问交换密钥、关于交换密钥的识别信息等等。此外，存储部分 14 还可以用于存储由内容接收 / 再现部分 12 获得的内容。

[0066] 当在处理可远程访问的内容时要求时间管理时 (例如，当管理如将在之后描述的从在基准时间点的时间到远程访问不可用时间限制的时段时) 使用计时器 15。

[0067] 图 4 示意性地示出了内容利用设备 20 的功能结构。内容利用设备 20 包括 CPU 21、

通信部分 22、内容输出部分 23 和存储部分 24，并用作通过远程访问接收内容的 RA- 信宿。

[0068] 除经由通信部分 22 关于 RA- 信源（内容供应设备 10）的、将在后面描述的设备登记处理之外，作为 RA- 信宿的内容利用设备 20 通过执行 RA-AKE 从 RA- 信源获得交换密钥，并将其存储在存储部分 24 中，使用基于获得的密钥计算的加密密钥解密从 RA- 信源获得的加密内容，并从内容输出部分 23 输出内容。存储部分 24 用于存储从 RA- 信源接收到的交换密钥和内容。

[0069] 在以下描述中，从交换密钥计算加密密钥的方法基于 DTCP-IP（假设本发明的要点不需要限于该方法）。

[0070] 这里，将参考图 5 描述用于通过 DTCP-IP 在信源和信宿之间执行加密内容传输的机制。作为内容传输方法，存在将信源中的内容复制到信宿的方法和将内容从信源完整地移动到信宿而在信源中不留下内容的方法（公知的）。将基于复制内容的前一方法用作内容传输方法的前提给出关于图 5 的描述。

[0071] 信源和信宿首先建立一个 TCP/IP 连接并执行设备间验证 (AKE 处理)。由 DTLA（如上所述）发布的设备证书嵌入在符合 DTCP 的设备中。在 AKE 处理中，信源和信宿可以在互相确认它们是合格的符合 DTCP 的设备之后共享认证密钥 Kauth。

[0072] 一旦 AKE 处理成功，信源（例如，信源的授权部分）产生授权信号。例如，信源产生作为内容密钥 Kc 的基础的交换密钥 Kx，并在以认证密钥 Kauth 将其加密之后将其发送到信宿。通过在信源和信宿中的每一个中将预定操作处理应用于交换密钥 Kx，可以产生要用于在内容传输时加密内容的内容密钥 K_c。

[0073] 然后，在符合 DTCP 的设备之间通过 AKE 的验证和密钥交换处理之后，使用比如 HTTP 和 RTP 的协议开始内容传输。在图 5 所示的实例中，根据 HTTP 处理执行内容传输。此时，除用于 AKE 处理的 TCT/IP 连接之外创建用于 HTTP 的 TCT/IP 连接（即，信源和信宿中的每一个具有用于 AKE 处理和内容传输的单独的套接信息 (IP 地址和端口编号的组合））。

[0074] 对于基于 HTTP 协议执行内容传输，存在两种方法，包括其中信宿从信源请求内容的下载方法和其中信源侧将内容推送到信宿的上载方法。在前一方法中，作为信宿的 HTTP 客户端基于例如使用 HTTP GET 方法的 HTTP 请求从作为信源的 HTTP 服务器请求内容，且信源发送所请求的内容作为 HTTP 响应。在后一方法中，作为信源的 HTTP 客户端响应于例如使用 HTTP POST 方法的 HTTP 请求，开始与作为信宿的 HTTP 服务器的传输。

[0075] 从信源发送的数据是由信源在执行 AKE 验证之后使用共享密钥加密内容而获得的数据。具体地说，信源使用随机数字 (random number) 产生随机数 (nonce)Nc，并产生与交换密钥 Kx、随机数 Nc 和加密方式对应的内容密钥 Kc。然后，信源使用内容密钥 Kc 加密由信宿请求的内容，并通过 TCP 流发送包括加密内容的有效载荷和包括关于随机数 Nc 和加密方式的信息的报头构成的分组。在 IP 协议中，TCP 流被划分为作为预定单元的分组大小，且通过划分获得的每一分组附加有报头部分以变为发送给指定 IP 地址的 IP 分组。

[0076] 在从信源接收到每一 IP 分组时，信宿侧将它们集合为 TCP 流。然后，信宿（例如，信宿的授权部分）产生允许解密已加密内容的授权信号。例如，信宿从流中提取随机数 Nc 和 E-EMI，并使用随机数 Nc、E-EMI 和交换密钥 Kx 计算内容密钥 Kc。然后可以使用内容密钥 Kc 解密加密内容。另外，可以关于解密的纯文本内容执行再现处理。替代地，信宿在存储部分 24 中存储内容而不解密加密内容或者发送其到另一设备。在结束如上所述使用 HTTP

协议的内容传输时，例如，从信宿侧按照需要切断内容传输中使用的 TCP 连接（在 DTCP-IP 中，由分组的报头部分中描述的 E-EMI（扩展加密方式指示符）和嵌入 CCI（复制控制信息）这两个机制实现伴随内容的复制控制信息的传输）。

[0077] 应当注意，在 DTCP-IP 中限定在连续未使用时间超过预定时间段（例如，2 小时）之前要丢弃交换密钥。对于信宿不可能使用加密内容除非从信源获得最新的交换密钥 Kx。此外，作为交换密钥 Kx 的操作方法，存在对于每一信宿准备一个密钥的方法和使用一个密钥而无论信宿的数目如何的方法。

[0078] 图 6 示出了根据当前 DTCP-IP 在信源和信宿之间执行的、使用 AKE 命令 (RTT-AKE) 的相互验证和密钥交换的操作序列。例如，在信源的第一授权部分和信宿的第一授权部分之间执行相互验证和密钥交换。

[0079] 在 AKE 处理的挑战响应 (challenge-response) 部分中 (AKE 的挑战响应部分)，首先从请求内容的信宿发送命令（例如，包括 Rx 随机数字和 Rx 证书的 Rx 挑战）。响应于 Rx 挑战，从信源发送回另一命令（例如，包括 Tx 随机数字和 Tx 证书的 Tx 挑战）。此后，普通挑战响应验证处理继续，其中从信源发送包括 Rx 随机数字、Tx 消息和 Tx 签名的 Rx 响应，而从信宿发送包括 Tx 随机数字、Rx 消息和 Rx 签名的 Tx 响应。在挑战响应部分中发送的每一挑战命令包括装置 ID 作为对设备唯一的识别信息。

[0080] 在如上所述的挑战响应验证处理中，施加关于 TTL（IP 路由器的跳数）的限制。具体地说，在当前 DTCP-IP 中，在发送 AKE 中使用的命令的 TCP/IP 通信中，传输设备的 TTL 被设置为 3 或者更少，且当 TTL 大于 3 时接收设备需要使接收数据无效。

[0081] 此后，经由保护的 RTT 协议从信源向信宿发送 EXCHANGE_KEY 命令，且响应于该命令从信宿发送回响应（未示出）。

[0082] 在图 6 所示的根据当前 DTCP-IP 的 RTT-AKE 中，关于 AKE 命令限制往返时间 (RTT) 和 IP 路由器的跳数 (TTL)，且 RTT-AKE 不能按照原样地应用于远程访问（如上所述）。但是，考虑用户的友好性，用户期望从外部远程访问家庭服务器并再现内容。当然需要保证希望保护版权的内容所有者的利益。因此，远程访问需要限于内容所有者允许的内容范围内，且也需要保护要远程访问的内容。

[0083] 另一方面，在远程访问时的 AKE 处理中，即，本发明提出的 RA-AKE 中，不执行在图 6 所示的 RTT-AKE 处理中执行的“保护的 RTT 协议”。具体地说，即使信源和信宿之间的 RTT 超过 7 毫秒时，也不取消例如在信源的第二授权部分和信宿的第二授权部分之间执行的 AKE 处理。此外，在 RA-AKE 中，不设置 TTL 的上限。具体地说，通过在 RA-AKE 中不施加对于 RTT 和 TTL 的限制，即使支持远程访问的信源（内容供应设备 10）和支持远程访问的信宿（内容利用设备 20）隔开响应延迟时间超过 7 毫秒且跳数超过 3 的距离时，也可以在各设备之间成功地执行 AKE 处理，且因此可以共享远程访问交换密钥。

[0084] 应当注意，因为在其中不施加对于 RTT 和 TTL 的限制的通信系统中任意设备之间的内容传输变得可能，所以从内容的版权保护的观点看需要用于防止非法使用的机制。

[0085] 作为由于在 RA-AKE 处理中不施加对于 RTT 和 TTL 的限制的事实而发生的非法使用之一，可能未指定数目的用户（即，超过版权法允许的私人使用的范围的范围）将它们的 RA- 信宿连接到特定用户的 RA- 信源并远程使用在该 RA- 信源中的内容。因此，需要限制来自未指定数目的用户的连接。

[0086] 对于限制来自未指定数目的用户的连接，存在其中 RA- 信源仅与预先登记的 RA- 信宿执行 RA-AKE 处理的方法以及限制在 RA-AKE 处理中提供密钥的 RA- 信宿的数目的方法。关于前一方法中的预先登记，通过仅当如在当前 DTCP-IP 的 RTT-AKE 中，其中 RTT 和 TTL 受限的 AKE 处理成功结束时，RA- 信源才存储 RA- 信宿的设备特定 ID，可以防止发生其中未指定数目的用户在 RA-AKE 处理中成功的情况。

[0087] 此外，通过限制要在 RA- 信源中登记的 RA- 信宿的数目，可以限制非法使用的规模。在以下描述中，假定 RA- 信源包括用于登记预定数目的 RA- 信宿的 ID 的“RA 登记处”（在存储部分 14 内）。这里，通过即使在已经在 RA- 信源中登记了 RA- 信宿的设备特定 ID 的情况下，也如将在之后描述的那样，限制在内容传输中提供远程访问交换密钥的 RA- 信宿的数目，可以限制非法使用的规模。

[0088] 例如，在其中 RTT 和 TTL 落入限制中的家庭预先执行 RA- 信宿的登记处理。在这种情况下，RA- 信源的登记部分可以登记 10 个 RA- 信宿那么多。即使关于 RA- 信源预先登记 10 个 RA- 信宿，RA- 信源也仅向 5 个 RA- 信宿提供远程访问交换密钥。

[0089] 图 7 示出了在 RA- 信源中登记 RA- 信宿时的验证序列的实例。

[0090] 验证序列以 RA- 信宿的登记部分发送登记请求命令“RA_REGI_INIT”到 RA- 信源而开始。在 RA-AKE 处理的挑战响应部分（AKE 的挑战响应部分）中，首先从 RA- 信宿发送命令（例如，包括 Rx 随机数字和 Rx 证书的 Rx 挑战）。响应于该挑战，从 RA- 信源发送回另一命令（例如，包括 Tx 随机数字和 Tx 证书的 Tx 挑战）。此后，从 RA- 信源发送包括 Rx 随机数字、Tx 消息和 Tx 签名的 Rx 响应，而从 RA- 信宿发送包括 Tx 随机数字、Rx 消息和 Rx 签名的 Tx 响应。

[0091] 应当注意，与“RA_REGI_INIT”的传输对应的信息，比如“RA_REGI_INIT 标记”可以并入要作为 Rx 挑战发送的信息来代替发送“RA_REGI_INIT”。

[0092] 每一挑战命令包括作为对设备唯一的识别信息的装置 ID。应当注意在挑战响应部分中，可以从信宿向信源发送“RESPONSE2”作为响应。在这种情况下，由于在设备中实现的公共装置密钥和公共装置证书，对于设备来说，装置 ID 变得不特定。当发送 RESPONSE2 时，作为 RESPONSE2 中包括的设备特定信息的 IDu 代替装置 ID 用作设备特定识别信息。

[0093] 在登记处理中的 RA-AKE 处理的挑战响应部分是与在当前 DTCP-IP 中的 RTT-AKE 处理中相同的处理，这指的是施加对于 TTL 的限制。此后，遵循保护的 RTT 协议，且当在 RA- 信源和 RA- 信宿之间的 RTT 超过 7 毫秒时取消 RA-AKE 处理。

[0094] RA- 信源执行用于登记直到该时间点处理已经成功的 RA- 信宿的“RA- 信宿登记”处理。然后，如果存在空间，则 RA- 信源在存储部分 14 中的 RA 登记处中另外登记 RA- 信宿的 ID，并使用用于发送结果代码的命令“RA_REGI_END”向 RA- 信宿通知该结果。

[0095] 应当注意，将图 7 中的“RA_REGI_INIT”和“RA_REGI_END”添加到 DTCP-IP 的 AKE 控制命令作为远程访问命令。图 28 示出了用于远程访问的 AKE 控制命令的结构实例。在图 28 所示的实例中，将新的值分配给子函数字段，且可以在 AKE_Info 中携带信息。

[0096] 图 8 示出了用于 RA- 信源登记 RA- 信宿的“RA- 信宿登记”处理的过程的流程图。

[0097] RA- 信源首先检查是否已经中止了在处理例程之前已经执行的前一处理（AKE 的挑战响应部分和保护的 RTT 协议）（步骤 S1）。

[0098] 这里，在已经中止前一处理的情况下（在步骤 S1 的“是”），RA- 信源向作为请求源

的 RA- 信宿通知结果代码，该结果代码通知登记处理已经以“失败”结束（步骤 S9），并结束处理例程。

[0099] 在已经正常地结束前一处理的情况下（在步骤 S1 的“否”），RA- 信源检查是否已经接收到 RESPONSE2（如上所述）（步骤 S2）。然后，当接收到 RESPONSE2 时（在步骤 S2 的“是”），RA- 信源将 IDu 设置为作为请求源的 RA- 信宿的 ID（步骤 S3）。另一方面，当未接收到 RESPONSE2 时（在步骤 S2 的“否”），RA- 信源将 ID 设置为作为请求源的 RA- 信宿的 ID（步骤 S4）。

[0100] 随后，RA- 信源检查作为请求源的 RA- 信宿的 ID 是否已经登记在 RA 登记处中（步骤 S5）。

[0101] 这里，当作为请求源的 RA- 信宿的 ID 已经登记在 RA 登记处中时（在步骤 S5 的“是”），RA- 信源向作为请求源的 RA- 信宿通知结果代码，该结果代码通知登记处理已经以“成功”结束（步骤 S8），并结束该处理例程。

[0102] 另一方面，当作为请求源的 RA- 信宿的 ID 还未登记在 RA 登记处中时（在步骤 S5 的“否”），RA- 信源然后检查在存储部分 14 内的 RA 登记处中是否存在空间（步骤 S6）。

[0103] 这里，当在 RA 登记处中没有空间时（在步骤 S6 的“否”），RA- 信源向作为请求源的 RA- 信宿通知结果代码，该结果代码通知登记处理已经以“失败”结束（步骤 S9），并结束该处理例程。

[0104] 另外，当在 RA 登记处中存在空间时（在步骤 S6 的“是”），RA- 信源另外在 RA 登记处中登记 RA- 信宿的 ID（步骤 S7）。然后，RA- 信源向作为请求源的 RA- 信宿通知结果代码，该结果代码通知登记处理具有以“成功”结束（步骤 S8），并结束该处理例程。

[0105] 如上参考图 7 和图 8 所述的，当类似于 RTT-AKE 验证处理成功时，如果存在空间，则 RA- 信源另外在 RA 登记处中登记 RA- 信宿的 ID。RA- 信宿需要经由用于远程访问 RA- 信源的验证处理，在 RA- 信源的 RA 登记处中登记它自己的 ID。因此，RA- 信源可以基于 RA 登记处的可登记数目来限制可以使用 RA- 信源的 RA- 信宿的数目，且因此限制内容的非法使用的规模。

[0106] 图 9 示出了在 RA- 信源向 RA- 信宿提供远程访问交换密钥时的验证序列的实例。图 9 所示的序列包括限制提供远程访问交换密钥的 RA- 信宿的数目的机制。

[0107] 该验证序列以 RA- 信宿发送密钥提供请求命令“RA_AKE_INIT”到 RA- 信源而开始。在 RA-AKE 处理的挑战响应部分（AKE 的挑战响应部分）中，首先从 RA- 信宿发送包括 Rx 随机数字和 Rx 证书的 Rx 挑战。响应于该挑战，从 RA- 信源发送回包括 Tx 随机数字和 Tx 证书的 Tx 挑战。此后，从 RA- 信源发送包括 Rx 随机数字、Tx 消息和 Tx 签名的 Rx 响应，而从 RA- 信宿发送包括 Tx 随机数字、Rx 消息和 Rx 签名的 Tx 响应。

[0108] 应当注意，与“RA_AKE_INIT”的传输对应的信息，比如“RA_AKE_INIT 标记”可以并入要作为 Rx 挑战发送的信息来代替发送“RA_AKE_INIT”。

[0109] 每一挑战命令包括作为对设备唯一的识别信息。应当注意在挑战响应部分中，可以从信宿向信源发送“RESPONSE2”作为响应。在这种情况下，RESPONSE2 中包括的 IDu 用作设备特定识别信息代替装置 ID（如上所述）。

[0110] 在 RA- 信源中的登记需要对于 TTL 的限制，但是在用于提供远程访问交换密钥的 RA-AKE 处理中省略。此外，在用于提供密钥的 RA-AKE 处理中也省略保护的 RTT 协议。因

此，RA- 信宿即使在远程环境下也可以请求远程访问交换密钥，即，通过远程访问使用内容。

[0111] 在验证处理成功时，RA- 信源执行“RA- 信宿 ID 确认”处理。在该处理中，RA- 信源确认作为请求源的 RA- 信宿的 ID 是否已经登记在 RA 登记处中，且还确认提供的远程访问交换密钥 (KC) 的数目是否已经超过上限。然后，当做出那些确认时，RA- 信源使用命令“RA_EXCHANGE_KEY”发送远程访问交换密钥 (RA_Kx)、交换密钥的 ID(RA_Kx_label) 和结果代码到 RA- 信宿。

[0112] 应当注意，提供的远程访问交换密钥的数目的上限与可以在存储部分 14 内的 RA 登记处中登记的 ID 的数目相同或更小。换句话说，除通过限制预先登记的数目来限制内容的非法使用的规模的方法之外，可以另外通过限制基于 KC 的上限限制可使用的 RA- 信宿的数目来限制非法使用的规模。此外，除关于 RA 登记处中登记的数目的限制之外，可以通过设置 KC 的上限来将可以在 RA- 信源中登记的 RA- 信宿的数目设置得大于可以使用内容的 RA- 信宿的数目，结果是可以省略当登记新的 RA- 信宿时删除旧的登记内容的时间和努力。

[0113] 提供的远程访问交换密钥 KC 的数目是在从 RA- 信源提供到 RA- 信宿的交换密钥以外的有效交换密钥的数目。因此，在其中交换密钥不提供到任何 RA- 信宿的初始状态下 KC 是 0，且 KC 可以减小与由 RA- 信源丢弃的所提供的交换密钥的数目那么多。

[0114] 这里，当 KC 的上限是 2 或更大时，作为远程访问交换密钥的操作方法，存在对于每一 RA- 信宿使用一个密钥的方法和使用一个密钥而无论 RA- 信宿的数目如何的方法。在前一方法中，当丢弃一个交换密钥时 KC 递减 1，且在后一方法中，当丢弃交换密钥时 KC 复位为 0。

[0115] 对于远程访问交换密钥 (RA_Kx) 的丢弃，如在 DTCP-IP 中那样，基于在连续未使用时间超过预定时间段之前丢弃交换密钥的规则的操作是可想象的。此外，其中在结束远程访问时 RA- 信宿与交换密钥的 ID(RA_Kx_label) 一起发送请求丢弃交换密钥的命令 (RA_FINISH) 的操作形式也是可想象的。将丢弃请求命令 RA_FINISH 与图 9 的“RA_AKE_INIT”和“RA_EXCHANGE_KEY”一起添加到用于 DTCP-IP 的 AKE 控制命令，作为远程访问命令。

[0116] 图 10 示出了用于 RA- 信源确认 RA- 信宿的登记和提供的远程访问交换密钥的数目的“RA- 信宿 ID 确认”处理的过程的流程图。

[0117] RA- 信源首先检查是否已经中止了在处理例程之前已经执行的前一处理 (AKE 的挑战响应部分和保护的 RTT 协议) (步骤 S11)。

[0118] 这里，在已经中止前一处理的情况下 (在步骤 S11 的“是”)，RA- 信源取消关于作为请求源的 RA- 信宿的 RA-AKE 处理 (步骤 S20) 并结束该处理例程。

[0119] 在已经正常地结束前一处理的情况下 (在步骤 S11 的“否”)，RA- 信源检查是否已经接收到了 RESPONSE2(步骤 S12)。然后，当接收到 RESPONSE2 时 (在步骤 S12 的“是”)，RA- 信源将 IDu 设置为作为请求源的 RA- 信宿的 ID(步骤 S13)。另一方面，当未接收到 RESPONSE2 时 (在步骤 S12 的“否”)，RA- 信源将装置 ID 设置为作为请求源的 RA- 信宿的 ID(步骤 S14)。

[0120] 随后，RA- 信源检查作为请求源的 RA- 信宿的 ID 是否已经登记在存储部分 14 内的 RA 登记处中 (步骤 S15)。

[0121] 这里，当不能确认作为请求源的 RA- 信宿的 ID 登记在 RA 登记处中时 (在步骤 S15 的“否”)，RA- 信源取消关于作为请求源的 RA- 信宿的 RA-AKE 处理 (步骤 S20) 并结束该处

理例程。

[0122] 另一方面，当确认作为请求源的 RA- 信宿的 ID 已经登记在 RA 登记处中时（在步骤 S15 的“是”），RA- 信源然后检查提供的远程访问交换密钥的数目是否小于上限值（步骤 S16）。

[0123] 当确认提供的远程访问交换密钥 KC 的数目小于上限值时（在步骤 S16 的“是”），RA- 信源仅将 KC 递增 1（步骤 S17），与远程访问交换密钥 (RA_Kx) 及其 ID(RA_Kx_label) 一起向作为请求源的 RA- 信宿通知结果代码，该结果代码通知确认处理已经“成功”结束（步骤 S19），并结束该处理例程。

[0124] 另一方面，当确认提供的远程访问交换密钥 KC 的数目已经达到上限（在步骤 S16 的“否”）时，RA- 信源向作为请求源的 RA- 信宿通知结果代码，该结果代码通知“忙碌”状态（步骤 S18），并结束该处理例程。

[0125] 当由 RA- 信源和 RA- 信宿共享远程访问交换密钥时，通过远程访问的内容传输变得可能。图 19 示出了 RA- 信宿从 RA- 信源请求内容的操作序列。应当注意在图 19 中，RA- 信宿基于 HTTP 协议从 RA- 信源请求内容，且通过下载方法发送内容。

[0126] 在通过图 9 所示的 RA-AKE 处理获得远程访问交换密钥 (RA_Kx) 及其 ID(RA_Kx_label) 之后，RA- 信宿通过使用 HTTP GET 方法的 HTTP 请求 (HTTP GET 请求）从 RA- 信源请求内容数据。在请求内容数据时，与内容 URL 一起发送远程访问交换密钥的 ID(RA_Kx_label)。这里，将定义用于从 RA- 信宿向 RA- 信源发送交换密钥 ID(RA_Kx_label) 的报头字段。

[0127] 在接收内容数据请求时，RA- 信源执行用于检测所请求的内容的远程访问输出数目的“内容远程访问 (RA) 输出管理 1”处理。然后，在确认在请求中指定的 URL 的内容可以通过远程访问输出之后，RA- 信源使用由交换密钥 ID 指定的远程访问交换密钥来计算加密密钥，并发送回由加密密钥加密的内容作为 HTTP 响应 (HTTP GET 响应）。

[0128] 图 20 示出了由 RA- 信源执行的“内容远程访问 (RA) 输出管理 1”的处理过程的流程图。

[0129] 首先，RA- 信源检查由 HTTP 请求中包括的交换密钥 ID 指示的交换密钥是否用于 DTCP-IP（步骤 S51）。

[0130] 这里，当由 HTTP 请求中包括的交换密钥 ID 指示的交换密钥不用于 DTCP-IP 时（在步骤 S51 的“否”），RA- 信源然后检查交换密钥是否用于远程访问（步骤 S52）。

[0131] 当交换密钥用于远程访问时（在步骤 S52 的“是”），RA- 信源检查由 HTTP 请求中包括的 URL 指定的内容是否可远程访问（步骤 S53）。例如，可以使用 RA- 标记（将在后面描述的）管理内容是否可远程访问。

[0132] 当由 HTTP 请求中包括的交换密钥 ID 指示的交换密钥用于 DTCP-IP 时（在步骤 S51 的“是”）或者当由 HTTP 请求指定的内容可远程访问时（在步骤 S53 的“是”），RA- 信源将 OK（确定）设置为对来自 RA- 信宿的 HTTP 请求 (HTTP GET 请求）的响应（步骤 S54），并结束该处理例程。

[0133] 另一方面，当由 HTTP 请求中包括的交换密钥 ID 指示的交换密钥不用于远程访问时（在步骤 S52 的“否”）或者当 HTTP 请求指定的内容不可远程访问时（在步骤 S53 的“否”），RA- 信源将 ERROR（错误）设置为对来自 RA- 信宿的 HTTP 请求 (HTTP GET 请求）的

响应（步骤 S55），并结束该处理例程。

[0134] 在迄今为止的描述中，已经假定通信系统仅由一对 RA- 信源和 RA- 信宿构成。但是，每一 RA- 信源和 RA- 信宿可以以菊花链模式另外连接到另一设备并在该状态下发送内容。版权保护的内容的传输范围最初应该在家庭内，且内容的重复接收和传输是不适宜的。因此，存在技术上防止重复地接收和发送内容的需要。在本实施例中，为了对于登记时 RTT 和 TTL 和提供的密钥数目更严格的限制，添加几个规则。

[0135] 在图 11 所示的系统结构的实例中，与 RA-Source#0 连接的 RA-Sink#1 另外包括作为 RA-Source#1 的功能，且连接到另一设备 RA-Sink#2。在这种情况下，通过禁止通过远程访问作为 RA-Sink#1 的 RA- 信源而接收的内容通过作为 RA-Source#1 的远程访问另外输出到 RA-Sink#2，防止从作为内容供应商的 RA-Source#0 的管理不能达到的位置远程访问内容。

[0136] 此外，在图 12 所示的系统结构的实例中，由于作为 Source#1 的功能，RA-Sink#1 通过远程访问与 RA-Source#0 连接，且还通过 DTCP-IP 连接到另一设备 Sink#2。此外，Sink#2 也包括作为 RA-Source#2 的功能，且因此连接到另一设备 RA-Sink#3。RA-Sink#1 能够通过 DTCP-IP 将通过远程访问接收到的内容本地地发送到另一设备 Sink#2。通过 DTCP-IP 的本地传输基于用于版权保护的机制，且没有问题。另外，通过禁止由 Sink#2 接收到的内容通过作为 RA-Source#2 的远程访问另外输出到 RA-Sink#3，防止从作为内容供应商的 RA-Source#0 的管理不能达到的位置远程访问内容。

[0137] 简而言之，参考图 11 和图 12 描述的系统操作禁止设备通过远程访问输出通过经由 DTCP-IP 的远程访问或者本地传输接收的内容，由此防止内容供应商非故意的远程访问。作为实现这种操作的方法，存在在内容的远程访问和本地传输时设置以下规则 (1) 和 (2) 的方法。

[0138] (1)RA- 信源不执行远程访问输出，除非内容伴随有“远程访问输出可用”的信息。

[0139] (2)RA- 信源和信源在通过 DTCP-IP 的远程访问或者本地传输时不发送指示远程访问输出的可用性的信息。

[0140] 在图 13 所示的系统结构的实例中，通过 DTCP-IP 与 Source#0 连接的 Sink#1 也具有作为 RA-Source#1 的功能，且因此连接到另一设备 RA-Sink#2。Source#0 可以仅通过 DTCP-IP 本地地发送内容到 Sink#1。通过 DTCP-IP 的本地传输基于用于版权保护的机制，且没有问题。这里，当施加限制规则 (1) 和 (2) 时，Sink#1 不能作为 RA-Source#1，通过远程访问另外输出接收到的内容到 RA-Sink#2。

[0141] 在这种情况下，虽然可以防止在内容供应商的管理不能达到的位置的远程访问输出，但是即使伴随有“远程访问输出可用”的信息的内容也不通过远程访问输出。在这点上，本发明的发明人认为不必禁止其中 RA-Source#1 作为 Sink#1 通过远程访问将通过经由 DTCP-IP 本地传输接收到的内容另外输出到取代 Source#0 的另一设备 RA-Sink#2 的操作（即，代替远程访问输出）。可以通过 Source#0 通过执行 DEP RA-AKE 而仅与 Sink#1 共享密钥、Sink#1 使用该密钥加密内容并发送其并且 RA-Source#1 通过远程访问输出内容，来实现代替远程访问输出的操作。

[0142] 图 14 示出了在 Source#0 通过执行 DEP-RA-AKE 仅与 Sink#1 共享密钥时的验证序列的实例。

[0143] 该验证序列以 Sink#1 发送密钥提供请求命令“DEP_RA_INIT”到 Source#0 开始。在 AKE 处理的挑战响应部分 (AKE 的挑战响应部分) 中，首先从 Sink#1 发送包括 Rx 随机数字和 Rx 证书的 Rx 挑战。响应于该挑战，从 Source#0 发送回包括 Tx 随机数字和 Tx 证书的 Tx 挑战。此后，从 Source#0 发送包括 Rx 随机数字、Tx 消息和 Tx 签名的 Rx 响应，而从 Sink#1 发送包括 Tx 随机数字、Rx 消息和 Rx 签名的 Tx 响应。

[0144] 应当注意，与“DEP_RA_AKE”的传输对应的信息，比如“DEP_RA_AKE 标记”可以并入要作为 Rx 挑战发送的信息来代替发送“DEP_RA_AKE”。

[0145] 每一挑战命令包括作为对设备唯一的识别信息。应当注意在挑战响应部分中，可以从信宿向信源发送“RESPONSE2”作为响应。在这种情况下，RESPONSE2 中包括的 IDu 用作设备特定识别信息代替装置 ID(如上所述)。

[0146] 因为经由 DTCP-IP 执行 AKE 处理，所以施加对于 TTL 的限制。另外，遵循保护的 RTT 协议。用于代替远程访问输出的 DEP-RA-AKE 处理只应当本地地执行，且如在当前 DTCP-IP 中的 RTT-AKE 中那样，施加关于 RTT 和 TTL 的限制。

[0147] 在验证处理成功时，Source#0 执行“DEP_RA- 信宿确认”处理。在该处理中，Source#0 仅与 Sink#1 共享密钥，且禁止与其他设备的 DEP-RA-AKE。然后，当确认可以仅与 Sink#1 共享密钥时，Source#0 使用命令“DEP-RA_EXCHANGE_KEY”，将用于远程访问输出替换的交换密钥 (D-RA_Kx)、其 ID(D-RA_Kx_label) 和结果代码发送到 Sink#1。

[0148] 此后，Source#0 禁止与其他设备的 DEP-RA-AKE 直到丢弃由 AKE 共享的密钥为止。此外，在 Sink#1 侧，使用经由处理过程共享的用于远程访问输出替换的交换密钥，加密并发送内容，同时伴随有“远程访问输出可用”的信息。因此，Sink#1 可以通过远程访问输出内容到作为 RA-Source#1 的 RA-Sink#2。

[0149] 图 15 示出了用于信源对于远程访问输出的替换验证信宿的“DEP_RA- 信宿确认”处理的过程的流程图。

[0150] 信源首先检查是否已经中止了在处理例程之前已经执行的前一处理 (AKE 的挑战响应部分和保护的 RTT 协议)(步骤 S21)。

[0151] 这里，在已经中止前一处理的情况下 (在步骤 S21 的“是”)，信源取消关于作为请求源的信宿的 DEP_RA- 信宿处理 (步骤 S30)，并结束该处理例程。

[0152] 在已经正常地结束前一处理的情况下 (在步骤 S21 的“否”)，信源检查是否已经接收到了 RESPONSE2(步骤 S22)。然后，当接收到了 RESPONSE2 时 (在步骤 S22 的“是”)，信源将 IDu 设置为作为请求源的信宿的 ID(步骤 S23)。另一方面，当未接收到 RESPONSE2 时 (在步骤 S22 的“否”)，信源将装置 ID 设置为作为请求源的信宿的 ID(步骤 S24)。

[0153] 随后，信源检查它自己的 DEP_RA 登记处是否为空 (步骤 S25)。DEP_RA 登记处是在存储部分 14 内准备的、用于存储允许内容通过远程访问输出到的单个设备的 ID 的登记处。

[0154] 这里，当确认 DEP_RA 登记处为空时 (在步骤 S25 的“是”)，信源在 DEP_RA 登记处中替换作为请求源的信宿的 ID(步骤 S26)。然后，信源使用命令“DEP-RA_EXCHANGE_KEY”发送用于远程访问输出替换的交换密钥 (D-RA_Kx)、其 ID(D-RA_Kx_label) 和结果代码到 Sink#1(步骤 S29)，并结束该处理例程。

[0155] 另一方面，当确认 DEP_RA 登记处不为空时 (在步骤 S25 的“否”)，信源另外检查

DEP_RA 登记处中存储的 ID 是否匹配作为请求源的信宿的 ID（步骤 S27）。

[0156] 当存储在 DEP_RA 登记处中的 ID 匹配作为请求源的信宿的 ID 时，即，当作为请求源的信宿已经登记为用于代替内容的远程访问输出的设备时（在步骤 S27 的“是”），信源使用命令“DEP-RA_EXCHANGE_KEY”发送用于远程访问输出替换的交换密钥 (D-RA_Kx)、其 ID(D-RA_Kx_label) 和结果代码到 Sink#1（步骤 S29），并结束该处理例程。

[0157] 另一方面，当存储在 DEP_RA 登记处中的 ID 不匹配作为请求源的信宿的 ID 时（在步骤 S27 的“否”），信源向作为请求源的信宿通知结果代码，该结果代码通知“忙碌”状态（步骤 S28），并结束该处理例程。

[0158] 在执行图 15 所示的处理过程之后，信源不能冗余地执行与其他设备的 DEP-RA-AKE。此外，通过在丢弃由 DEP-RA-AKE 共享的用于远程访问输出替换的交换密钥 (D-RA_Kx) 时清空 DEP_RA 登记处，变得可以执行与其他设备的 DEP-RA-AKE。

[0159] 对于用于远程访问输出替换的交换密钥 (D-RA_Kx) 的丢弃，其中信宿在结束远程访问输出替换时与交换密钥的 ID(D-RA_Kx_label) 一起发送请求交换密钥的丢弃的命令 (DEP_RA_FINISH) 的操作形式是可想象的。将丢弃的请求命令 DEP_RA_FINISH 与图 14 的“DEP_RA_INIT”和“DEP_RA_EXCHANGE_KEY”一起添加到 DTCP-IP 的 AKE 控制命令作为远程访问命令。

[0160] 图 21 示出了用于信宿（具有作为 RA- 信源的功能）从信源请求对于其要代替远程访问的内容的操作序列。应当注意在图 21 中，信宿根据 HTTP 协议从信源请求内容，且通过下载方法发送内容。

[0161] 在通过图 14 所示的 DEP-RA-AKE 处理获得用于远程访问输出替换的交换密钥 (D-RA_Kx) 及其 ID(D-RA_Kx_label) 之后，信宿通过使用 HTTP GET 方法的 HTTP 请求 (HTTP GET 请求）从信源请求内容数据。在请求内容数据时，与内容 URL 一起发送用于远程访问输出替换的交换密钥的 ID(D-RA_Kx_label)。这里，将定义用于从信宿向信源发送交换密钥 ID 的报头字段 (D-RA_Kx_label)。

[0162] 在接收内容的远程访问输出替换的请求时，信源执行用于检查所请求的内容的远程访问输出是否可以代替的“内容远程访问替换 (DEP-RA) 输出管理 1”的处理。然后，在确认可以代替请求中指定的 URL 的内容的远程访问输出之后，信源使用由交换密钥 ID 指定的、用于远程访问输出替换的交换密钥来计算加密密钥，并发送回由加密密钥加密的内容作为 HTTP 响应 (HTTP GET 响应），同时内容伴随有“远程访问输出可用”的信息。

[0163] 图 22 示出了由请求代替远程访问输出的信源执行的内容远程访问输出替换管理的处理过程的流程图。

[0164] 首先，信源检查由 HTTP 请求中包括的交换密钥 ID 指示的交换密钥是否用于 DTCP-IP（步骤 S61）。

[0165] 这里，当由 HTTP 请求中包括的交换密钥 ID 指示的交换密钥不用于 DTCP-IP 时（在步骤 S61 的“否”），信源然后检查交换密钥是否用于远程访问输出替换（步骤 S62）。

[0166] 当交换密钥用于远程访问输出替换时（在步骤 S62 的“是”），信源检查由 HTTP 请求中包括的 URL 指定的内容是否可远程访问（步骤 S63）。例如，可以使用 RA- 标记（将在后面描述的）管理内容是否可远程访问。

[0167] 当由 HTTP 请求中包括的交换密钥 ID 指示的交换密钥用于 DTCP-IP 时（在步骤

S61 的“是”）或者当由 HTTP 请求指定的内容可远程访问时（在步骤 S63 的“是”），信源将 OK（确定）设置为对来自信宿的 HTTP 请求 (HTTP GET 请求）的响应（步骤 S64）。

[0168] 另一方面，当由 HTTP 请求中包括的交换密钥 ID 指示的交换密钥不用于远程访问输出替换时（在步骤 S62 的“否”）或者当由 HTTP 请求指定的内容不可远程访问时（在步骤 S63 的“否”），信源将 ERROR（错误）设置为对来自信宿的 HTTP 请求 (HTTP GET 请求）的响应（步骤 S65）。

[0169] 应当注意，在图 13 所示的系统结构中，虽然当要从 Source#0 发送不能远程访问的内容到 Sink#1 时基于当前 DTCP-IP 执行内容传输，但是通过以下结构，可以在使用用于远程访问输出替换的交换密钥 (D-RA_Kx) 的传输中处理可远程访问的内容和不可远程访问的内容两者。

[0170] 在使用由 DEP-RA-AKE 共享的交换密钥的内容传输中，Source#0 添加远程访问可用性信息 (RA- 标记）到内容，以使得 RA-Source#1 可以判断是否可以通过远程访问输出接收到的内容。

[0171] 应当注意，通过与内容数据一起加密 RA- 标记或者将 RA- 标记的值输入到用于计算加密密钥的函数并将其反映在加密密钥 Kc 的值上的方法（参见图 23）或者与通过以散列函数处理信息和加密密钥而获得的签名数据（签名）一起发送包括 RA- 标记的纯文本信息的方法（参见图 24），可以防止发生伪造。

[0172] 此外，当加密 RA- 标记与内容数据时，可以提供由 DTCP-IP 操作的 DTCP_descriptor、PCP-UR 的保留位（参见图 25 和图 26）或者关于新的内容的信息的容器作为存储目的地，并将 RA- 标记存储在其中。

[0173] 应当注意，在图 13 所示的如上所述的系统结构中，假定 Sink#1 经由 RA-Source#1 通过远程访问从 Source#0 输出内容而不记录该内容。作为修改的实例，也在从 Source#0 到 Sink#1 的内容的 MOVE（移动）的情况下，RA-Source#1 可以判断是否可以通过使用由 DEP-RA-AKE 共享的密钥、在内容传输时附加远程访问可用性信息 (RA- 标记）、而经由远程访问输出接收到的内容。这里，用于 DTCP-IP 的 MOVE 功能指的是在信宿编码和记录接收到的内容作为仅有副本以及在信源侧删除发送的内容或者使得不可用的情况下，加密内容从信源到信宿的传输。

[0174] 迄今为止已经描述了限制可以使用 RA- 信源的 RA- 信宿的数目的方法。但是，一些内容所有者可能要求通过限制可以同时使用所有者自己通过远程访问提供的内容的设备的数目，来抑制伪造的威胁，如在经由远程访问由接收器立即输出记录禁止付费节目的情况下那样。

[0175] 作为限制内容的远程访问的数目的方法，存在管理通过哪个 RA- 信宿正在远程访问哪个内容以及对于每一 RA- 信宿改变要在 RA-AKE 中共享的密钥的方法。此外，仅需要 RA- 信源不同时发送相同内容到预定数目或更多的 RA- 信宿。

[0176] 例如，RA- 信源使用如下所示的用于限制可以同时远程访问内容的 RA- 信宿的数目的管理表。

[0177] 【表 1】

[0178]

URL	RA_Kx_label
(用于内容 X 的 URL)	80
(用于内容 Y 的 URL)	81

[0179] 在管理表中,在每一项中管理正发送到 RA- 信宿的内容的 URL 和与 RA- 信宿具有一对一对应关系的交换密钥 ID(RA_Kx_label) 的组合。在管理表中其中 URL 匹配但是交换密钥 ID 不同的项意味着正在由不同 RA- 信宿使用单个内容。

[0180] RA- 信源在新开始内容传输之前参考管理表,并执行控制以使得不将相同内容发送到多于预定数目的 RA- 信宿。当允许开始内容传输时,RA- 信源在管理表中添加由 URL 和交换密钥 ID 的组合构成的项。

[0181] 图 16 示出了在同时发送相同内容到其的 RA- 信宿的数目受限的情况下在 RA- 信宿从 RA- 信源请求内容时的操作序列。

[0182] 在通过图 9 所示的 RA-AKE 处理获得远程访问交换密钥 (RA_Kx) 及其 ID(RA_Kx_label) 之后,RA- 信宿通过使用 HTTP GET 方法的 HTTP 请求 (HTTP GET 请求) 从 RA- 信源请求内容数据。在请求内容数据时,与内容 URL 一起发送远程访问交换密钥的 ID(RA_Kx_label)。这里,将定义用于从 RA- 信宿向 RA- 信源发送交换密钥 ID(RA_Kx_label) 的报头字段。

[0183] 在接收到内容数据请求时,RA- 信源执行用于检查同时通过远程访问输出请求的内容的 RA- 信宿的数目的“单个内容远程访问 (RA) 输出管理 2”的处理。当同时发送指定 URL 的内容的 RA- 信宿的数目低于限制时,RA- 信源使用由交换密钥 ID 指定的远程访问交换密钥计算加密密钥,并发送回由加密密钥加密的内容作为 HTTP 响应 (HTTP GET 响应)。另外,RA- 信源在管理表中添加项。

[0184] 应当注意,当 RA- 信源丢弃远程访问交换密钥时,从表中删除与丢弃的密钥对应的项。此外,也可以与远程访问交换密钥 ID(RA_Kx_label) 一起发送在 RA- 信宿结束远程访问 (RA_FINISH) 时请求从管理表删除项的命令 (如上所述)。

[0185] 图 17 示出了由 RA- 信源响应于内容数据请求执行的、用于管理相同内容的输出数目的处理过程的流程图。

[0186] 首先,RA- 信源检查由 HTTP 请求中包括的交换密钥 ID 指示的交换密钥是否用于 DTCP-IP(步骤 S31)。

[0187] 这里,当由 HTTP 请求中包括的交换密钥 ID 指示的交换密钥用于 DTCP-IP 时 (在步骤 S31 的“是”),RA- 信源将 OK(确定) 设置为对来自 RA- 信宿的 HTTP 请求 (HTTP GET 请求) 的响应 (步骤 S38),并结束该处理例程。

[0188] 这里,当由 HTTP 请求中包括的交换密钥 ID 指示的交换密钥不用于 DTCP-IP 时 (在步骤 S31 的“否”),RA- 信源然后检查交换密钥是否用于远程访问 (步骤 S32)。

[0189] 当交换密钥用于远程访问时 (在步骤 S32 的“是”),RA- 信源检查由 HTTP 请求中包括的 URL 指定的内容是否可远程访问 (步骤 S33)。例如,可以使用 RA- 标记 (将在后面描述的) 管理内容是否可远程访问。

[0190] 当由 HTTP 请求中包括的交换密钥 ID 指示的交换密钥不用于远程访问时 (在步骤

S32 的“否”）或者当 HTTP 请求指定的内容不可远程访问时（在步骤 S33 的“否”），RA- 信源将 ERROR（错误）设置为对来自 RA- 信宿的 HTTP 请求 (HTTP GET 请求）的响应（步骤 S39），并结束该处理例程。

[0191] 另外，当确认由 HTTP 请求指定的内容可远程访问时（在步骤 S33 的“是”），RA- 信源检查是否存在其 URL 和交换密钥 ID 与管理表中的内容数据请求中包括的 URL 和交换密钥 ID(RA_Kx_label) 相同的项（步骤 S34）。

[0192] 这里，当存在其 URL 和交换密钥 ID 与管理表中的内容数据请求中包括的 URL 和交换密钥 ID(RA_Kx_label) 相同的项时（在步骤 S34 的“是”），即使当由作为请求源的 RA- 信宿使用内容时也不超过使用限制。在这点上，RA- 信源将“OK”（确定）设置为对来自作为请求源的 RA- 信宿的 HTTP GET 请求的响应（步骤 S38），并结束该处理例程。

[0193] 另一方面，当没有其 URL 和交换密钥 ID 与管理表中的内容数据请求中包括的 URL 和交换密钥 ID(RA_Kx_label) 相同的项时（在步骤 S34 的“否”），RA- 信源然后检查是否存在在管理表中具有相同 URL 的项（步骤 S35）。

[0194] 当没有其 URL 与管理表中的内容数据请求中包括的 URL 相同的项时（在步骤 S35 的“否”），即使当由作为请求源的 RA- 信宿使用内容时也不超过使用限制。在这点上，RA- 信源在管理表中添加由内容数据请求指定的 URL 和交换密钥 ID(RA_Kx_label) 的组合构成的项（步骤 S37）。然后，RA- 信源将“OK”（确定）设置为对来自作为请求源的 RA- 信宿的 HTTP GET 请求的响应（步骤 S38），并结束该处理例程。

[0195] 另一方面，当存在其 URL 与管理表中的内容数据请求中包括的 URL 相同的项时（在步骤 S35 的“是”），存在如果 RA- 信源响应于请求提供内容到作为请求源的 RA- 信宿则可能超过使用限制的担心。在这点上，RA- 信源进一步检查管理表中其 URL 与内容数据请求中包括的 URL 相同的项的数目是否小于上限值（步骤 S36）。

[0196] 当在管理表中其 URL 与内容数据请求中包括的 URL 相同的项的数目小于上限值时（在步骤 S36 的“是”），即使当由作为请求源的 RA- 信宿使用内容时也不超过使用限制。在这点上，RA- 信源在管理表中添加由内容数据请求指定的 URL 和交换密钥 ID(RA_Kx_label) 的组合构成的项（步骤 S37），将“OK”（确定）设置为对来自作为请求源的 RA- 信宿的 HTTP GET 请求的响应（步骤 S38），并结束该处理例程。

[0197] 如果在管理表中其 URL 与内容数据请求中包括的 URL 相同的项的数目已经达到上限值（在步骤 S36 的“否”），则当由作为请求源的 RA- 信宿使用内容时超过使用限制。因此，RA- 信源将“ERROR”（错误）设置为对来自作为请求源的 RA- 信宿的 HTTP GET 请求的响应（步骤 S39），并结束该处理例程。

[0198] 已经基于不能远程访问未伴随有“远程访问输出可用”的信息的内容的前提进行了上述描述。但是，实际上，如果内容是可记录内容，则通过在比如 DVD 和存储卡之类的可拆卸记录介质中写入内容，可以在家庭外部携带内容并用于不同设备。因此，使得即使当内容未伴随有“远程访问输出可用”的信息时，在记录内容之后也能够远程访问可记录内容的操作也是可能的。

[0199] 应当注意，由于可以在内容的写入目的地是可拆卸记录介质的情况下在完全写入之后取出由 RA- 信宿接收到的内容，因此也可以在内容的记录期间或者直到从记录开始经过预定时间段为止要求远程访问的抑制。

[0200] 图 18 示出了用于作为 RA- 信源操作的设备通过 MOVE 功能来记录内容或者接受内容的处理过程的流程图。

[0201] RA- 信源首先检查接收到的内容是否伴随有关于“远程访问输出可用性”的信息（步骤 S41）。

[0202] 这里，当接收到的内容伴随有关于“远程访问输出可用性”的信息时（在步骤 S45 的“是”），RA- 信源进一步检查信息的指定内容是否为“远程访问输出可用”（步骤 S42）。

[0203] 这里，当关于“远程访问输出可用性”的信息的指定内容不是“远程访问输出可用”时（在步骤 S42 的“否”），RA- 信源基于该信息设置“无限”作为远程访问不可用时间限制（步骤 S43）。

[0204] 随后，RA- 信源设置指示接收到的内容的远程访问输出的可用性的 RA- 标记（步骤 S44），并结束该处理例程。

[0205] 另一方面，当内容未伴随有关于“远程访问输出可用性”的信息时（在步骤 S45 的“否”），作为将预定时间段与在基准时间点的时间相加的结果，RA- 信源获得值 T（步骤 S46），将 T 设置为内容的远程访问不可用时间限制（步骤 S47），在设置中将 RA- 标记初始化为“不可用”以禁止内容的远程访问输出直到该时间限制为止（步骤 S48），并结束该处理例程。

[0206] 这里，基准时间点指的是广播节目的开头的定时处的时间（如果内容例如是广播内容），且与作为节目信息等的内容一起发送的节目的时间长度用作要与其相加的预定时间段。对于在记录日期不清楚的记录介质中的内容，通过将内容再现长度与已经进行由 MOVE 功能尝试接受内容的时间相加而获得的值可以用作 T。

[0207] 应当注意，虽然在图 18 中未示出，但是当内容伴随有“远程访问输出不可用”的信息时（在步骤 S42），RA- 信源设置“不可用”作为 RA- 标记并设置“无限”作为 T。

[0208] 通过图 18 所示的处理过程，RA- 标记设置为“不可用”且其 T 不能设置为“无限”的内容可以被处理为指定定时之后的可远程访问的内容。

[0209] 图 27 示出了 RA- 信源更新对于内容设置的 RA- 标记和 T 的处理过程的流程图。

[0210] RA- 信源首先检查内容的 RA- 标记是否被设置为“可用”（步骤 S71）。这里，当内容的 RA- 标记已经设置为“可用”时（在步骤 S71 的“是”），全部跳过随后的处理，且该处理例程结束。

[0211] 当内容的 RA- 标记未被设置为“可用”时（在步骤 S71 的“否”），RA- 信源然后检查内容的远程访问不可用时间限制是否被设置为“无限”（步骤 S72）。这里，当内容的远程访问不可用时间限制被设置为“无限”时（在步骤 S72 的“是”），全部跳过随后的处理，且该处理例程结束。

[0212] 当内容的远程访问不可用时间限制未被设置为“无限”时（在步骤 S72 的“否”），RA- 信源然后检查是否已经经过内容的远程访问不可用时间限制（步骤 S73）。

[0213] 当还未经过内容的远程访问不可用时间限制时（在步骤 S73 的“是”），该处理例程立即结束。另一方面，当内容的远程访问不可用时间限制不在将来时，即，当已经经过了远程访问不可用时间限制时（在步骤 S73 的“否”），RA- 信源将内容的 RA- 标记更新为“可用”（步骤 S74），并结束该处理例程。

[0214] 通过 RA- 信源周期性地执行图 27 中所示的处理过程，可以将内容的 RA- 标记更新

为“可用”。例如向外呈现内容列表（未示出）的定时可以例示为处理过程的特定执行定时。

[0215] 在 DTCP-IP 中仅在家庭网络内使用内容。但是，通过缩窄该实施例的通信系统中非法使用的可能性，可以从家庭外部，即，通过远程访问使用内容。

[0216] 此外，在该实施例的通信系统中，通过调整用于限制远程访问的多个限制值，比如 RTT、TTL、使用内容的 RA- 信宿的数目和提供的交换密钥的数目的限制值，可以灵活地构造系统。

[0217] 另外，根据该实施例的通信系统，可以实现内容的远程访问而不施加对于 RTT 和 TTL 的限制，同时基于 DTCP-IP 通信协议构造系统。

[0218] 已经参考图 3 描述了与根据本发明的通信系统中的 RA- 信源对应的内容供应设备的功能结构。例如，个人计算机、记录器或者各种其他信息设备可以用作内容供应设备。

[0219] 图 29 示出了要应用于内容供应设备的个人计算机 80 的结构实例。如图所示的个人计算机 80 包括比如经由总线 88 相互连接的 CPU 81、RAM（随机存取存储器）82、EEPROM（电可擦可编程只读存储器）83、显示器 84、扬声器 85、包括 HDD（硬盘驱动器）和 SDD（超密磁盘）的大容量信息存储设备 86 和 I/O 接口 87 之类的电路组件。

[0220] CPU 81 读出并执行加载到作为主存储器的 RAM 82 的程序。

[0221] 将与内容的加密和解密相关的功能加载到 RAM 82。例如，将用于执行 DTCP-IP 功能的程序和用于执行 RA-AKE 处理的程序加载到 RAM 82。此外，将用于在 RA- 信源中登记 RA- 信宿时执行验证序列（参见图 7）的程序加载到 RAM 82，作为用于执行 RA-AKE 处理并由 CPU 81 执行的程序的一部分。

[0222] EEPROM 83 是可重写的非易失性存储设备，并存储设置信息等。当个人计算机 80 作为 RA- 信源，即，内容供应设备操作时，在 EEPROM 83 中存储要作为 RA- 信宿的终端 ID。

[0223] 在个人计算机 80 上，在接收到登记 RA- 信宿（例如，移动终端）作为可以从 RA- 信宿与其执行 RA-AKE 过程的终端的请求时，CPU 81 从 RAM 82 读出其中描述 DTCP-IP 的 AKE 处理的程序，并与 RA- 信宿执行 AKE 过程。

[0224] 在该过程成功时，CPU 81 根据存储在 RAM 82 中的程序在 EEPROM 83 中存储 RA- 信宿的终端 ID。

[0225] 此后，在个人计算机 80 上，CPU 81 在接收 RA-AKE 处理的请求时，执行比较已经发出请求的终端的 ID 与存储在 EEPROM 83 中的 RA- 信宿的终端 ID 的处理，并确定是否完成 RA-AKE 处理。

[0226] 然后，在完成 RA-AKE 处理时，产生要在个人计算机 80 与已经发出 RA-AKE 处理请求的终端之间共享的内容密钥。将产生的内容密钥临时存储在个人计算机 80 一侧上，且通过在从大容量信息存储设备 86 读出内容时临时存储的内容密钥来加密内容。经由 I/O 接口 87 外部地输出加密内容。当 I/O 接口 87 具有无线 LAN 功能时，加密内容经由无线 LAN 发送到已经发出 RA-AKE 处理请求的终端。

[0227] 图 30 示出了要应用于内容供应设备的记录器 90 的结构实例。如图所示的记录器 90 包括系统芯片 91、大容量存储设备 92、RAM 93、EEPROM 94 和无线 LAN 芯片 95。

[0228] 系统芯片 91 包括由芯片内的总线 91d 相互连接的、比如 CPU 91a、协处理器 91b 和接口功能部分 91c 之类的电路组件。

[0229] CPU 91a 能够执行在经由接口功能部分 91c 与其连接的存储设备中存储的程序。

[0230] 协处理器 91b 是辅助操作设备，且主要执行运动图像的压缩和解码处理，比如 H264、VC1、MPEG2 和 JPEG 算法。

[0231] 大容量存储设备 92 例如是 HDD 或者 SDD，并存储要提供到内容利用设备的内容。

[0232] 要由 CPU 91a 执行的程序被加载到作为主存储器的 RAM 93。加载到 RAM 93 的程序主要是实现与内容的加密和解密相关的功能的程序，比如用于执行 DTCP-IP 功能的程序和用于执行 RA-AKE 处理的程序。

[0233] EEPROM 94 是可重写的非易失性存储设备，并存储设置信息等。当记录器 90 作为 RA- 信源，即，内容供应设备操作时，在 EEPROM 94 中存储要作为 RA- 信宿的终端 ID。

[0234] 在记录器 90 上，在从 RA- 信宿接收登记 RA- 信宿（例如，移动终端）作为可以与其执行 RA-AKE 过程的终端的请求时，CPU 91a 从 RAM 93 读出其中描述 DTCP-IP 的 AKE 处理的程序，并与 RA- 信宿执行 AKE 过程。

[0235] 在该过程成功时，CPU 91a 根据存储在 RAM 93 中的程序在 EEPROM 94 中存储 RA- 信宿的终端 ID。

[0236] 此后，在记录器 90 上，CPU 91a 在接收到 RA-AKE 处理的请求时，执行比较已经发出请求的终端的 ID 与存储在 EEPROM 94 中的 RA- 信宿的终端 ID，并确定是否完成 RA-AKE 处理的处理。

[0237] 然后，在完成 RA-AKE 处理时，产生要在记录器 90 与已经发出 RA-AKE 处理请求的终端之间共享的内容密钥。产生的内容密钥临时存储在记录器 90 一侧上，且在从大容量存储设备 92 读出内容时通过临时存储的内容密钥来加密内容。加密内容经由接口功能部分 91c 和无线 LAN 芯片 95 发送到已经发出 RA-AKE 处理请求的终端。

[0238] [工业实用性]

[0239] 迄今为止，已经参考特定实施例具体地描述了本发明。本领域技术人员应该理解，取决于设计要求及其他因数，可以进行各种修改、组合、部分组合和变更，只要它们在所附权利要求或其等效物的范围内即可。

[0240] 作为本发明的应用实例，存在其中家庭外的客户端远程访问应用了 DTCP-IP 的家庭网络上的服务器以使用内容的通信系统，尽管不限于此。本发明类似地可应用于用于在超过往返时间 (RTT)、IP 路由器的跳数 (TTL) 等的限制时，经由使用比如 WAN 之类的外部网络的远程访问发送需要版权保护或者为其它目的保护的内容的任何其他内容传输系统。

[0241] 简而言之，已经以范例的形式公开了本发明，且说明书的描述性内容不以限制的方式解释。为了判断本发明的实质，应该考虑权利要求的范围。

[0242] 本申请包含与于 2009 年 9 月 9 日在日本专利局提交的日本优先权专利申请 JP 2009-208687 和于 2010 年 5 月 21 日在日本专利局提交的日本优先权专利申请 JP 2010-117832 中公开的主题相关的主题，将其全部内容通过引用包括于此。

[0243] [附图标记列表]

[0244] 10 内容供应设备 (RA- 信源)

[0245] 11 CPU

[0246] 12 内容接收 / 再现部分

[0247] 13 通信部分

[0248] 14 存储部分

[0249] 15 计时器

[0250] 20 内容利用设备(RA-信宿)

[0251] 21 CPU

[0252] 22 通信部分

[0253] 23 内容输出部分

[0254] 24 存储部分

[0255] 30,31 路由器

[0256] 40,41 调制解调器

[0257] 50 WAN

[0258] 60 IAS 提供者

[0259] 70 DDNS 服务

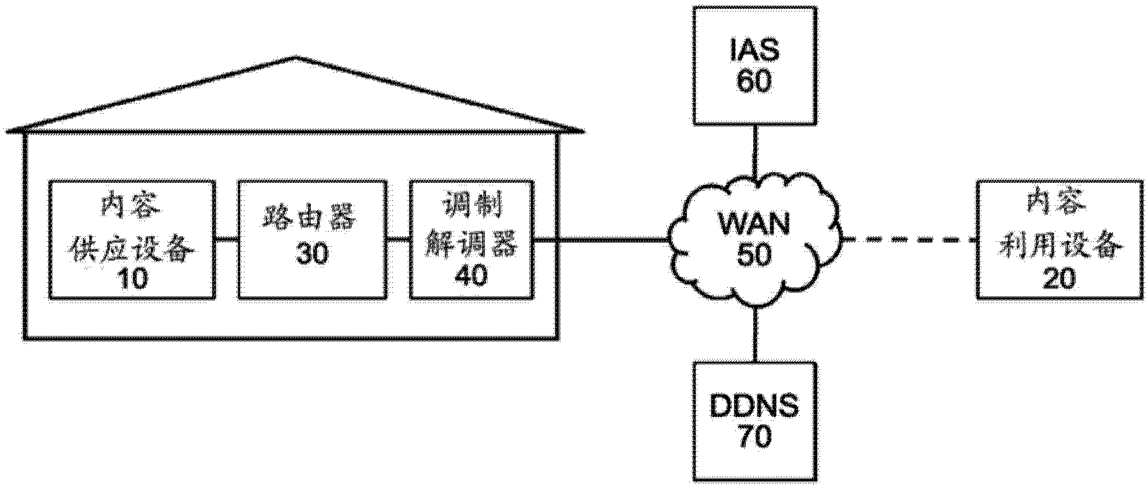

IAS
60
内容
供应设备
10
路由器
30
调制
解调器
40
WAN
50
内容
利用设备
20
DDNS
70

图 1

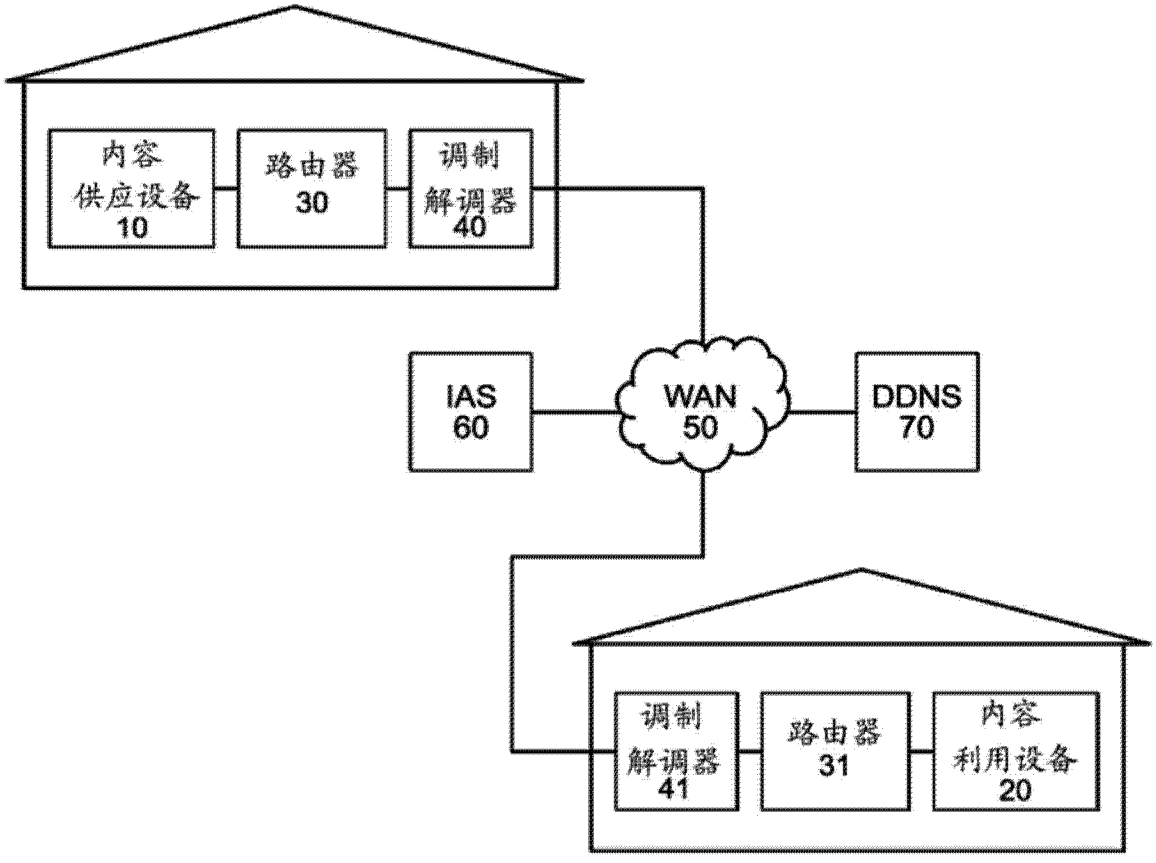

内容
供应设备
10
路由器
30
调制
解调器
40
IAS
60
WAN
50
DDNS
70
调制
解调器
41
路由器
31
内容
利用设备
20

图 2

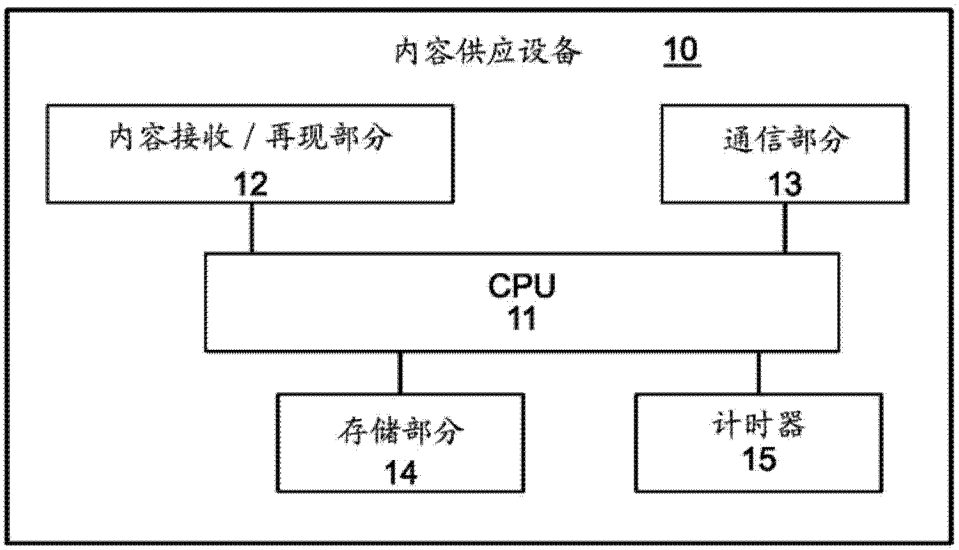

内容供应设备
10
内容接收 / 再现部分
12
通信部分
13
CPU
11
存储部分
14
计时器
15

图 3

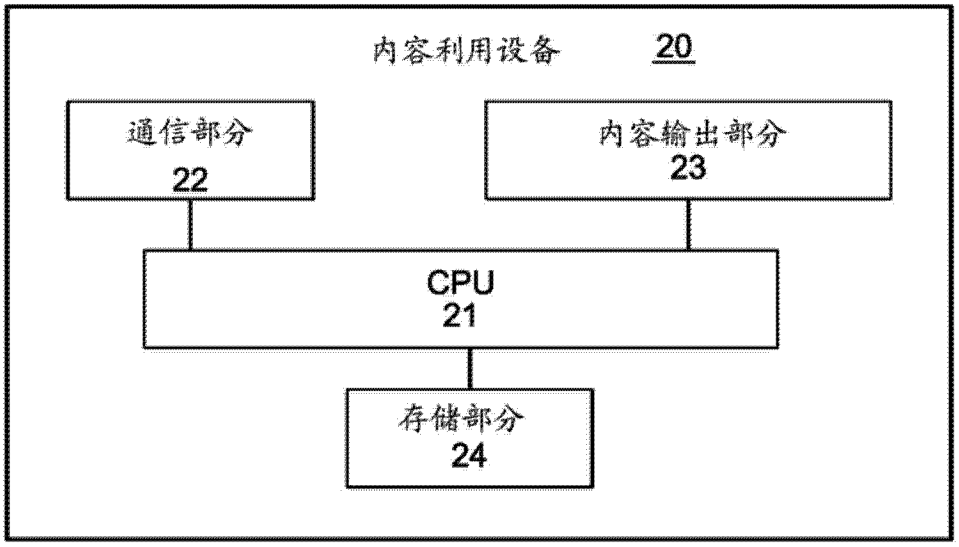

内容利用设备
20
通信部分
22
内容输出部分
23
CPU
21
存储部分
24

图 4

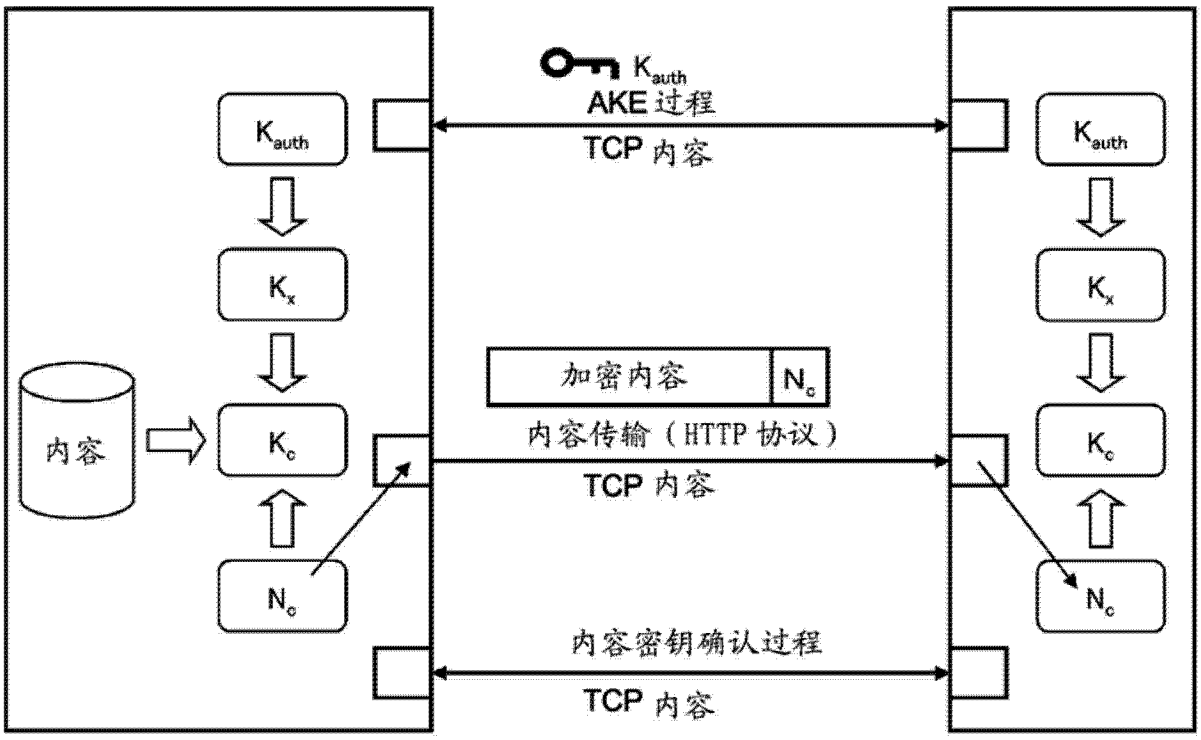

K_{auth}
AKE 过程
TCP 内容
K_{auth}
K_x
K_c
N_c
内容
加密内容
N_c
内容传输（HTTP 协议）
TCP 内容
内容密钥确认过程
TCP 内容

图 5

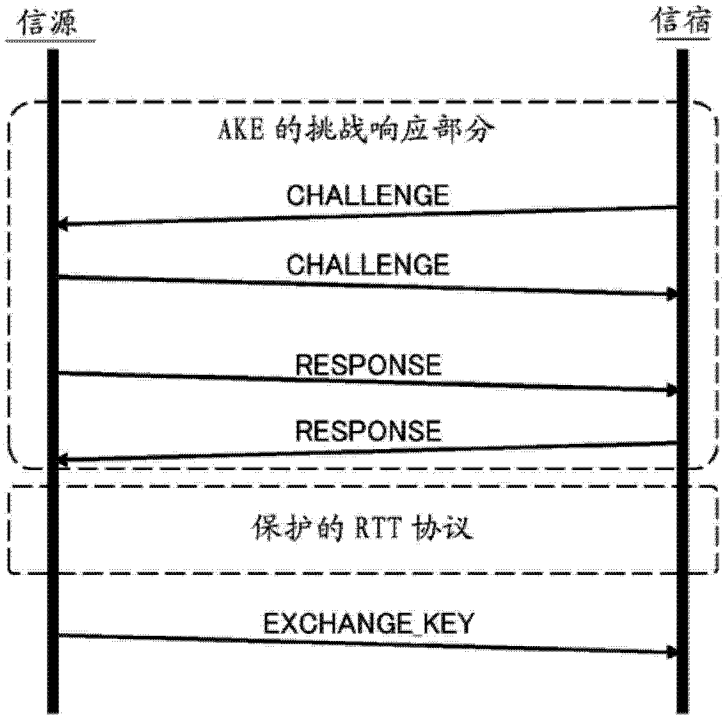

信源
信宿
AKE 的挑战响应部分
CHALLENGE
CHALLENGE
RESPONSE
RESPONSE
保护的 RTT 协议
EXCHANGE_KEY

图 6

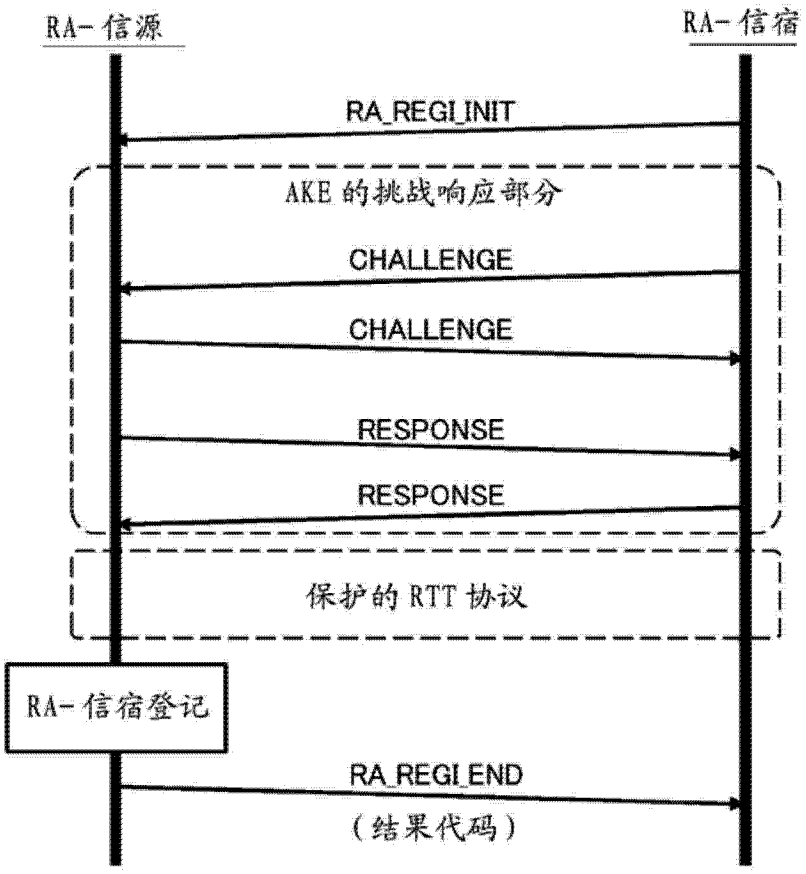

RA-信源
RA-信宿
RA_REGI_INIT
AKE 的挑战响应部分
CHALLENGE
CHALLENGE
RESPONSE
RESPONSE
保护的 RTT 协议
RA-信宿登记
RA_REGI_END
（结果代码）

图 7

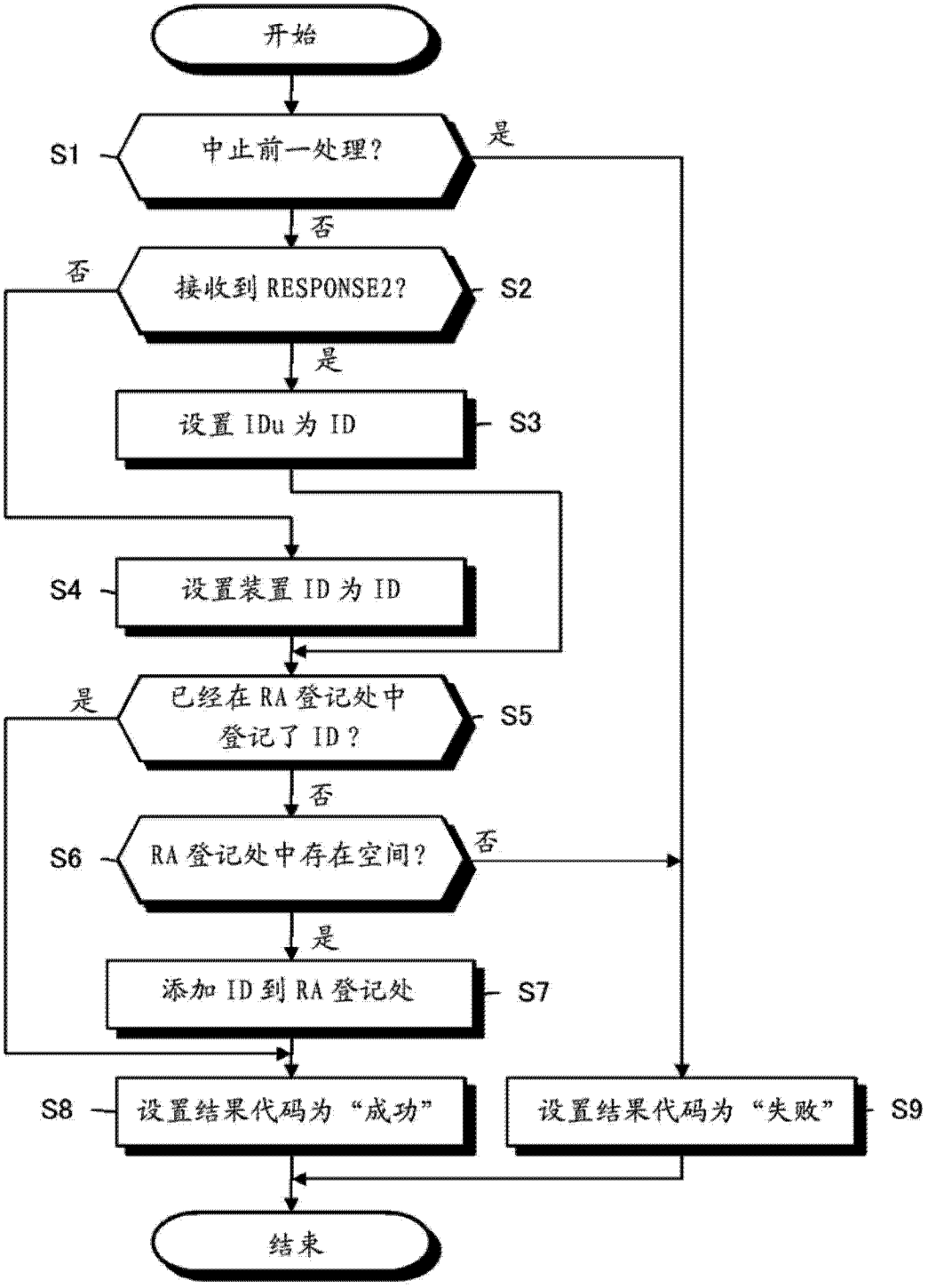

开始
S1
中止前一处理?
是
否
否
接收到 RESPONSE2?
S2
是
设置 IDu 为 ID
S3
S4
设置装置 ID 为 ID
是
已经在 RA 登记处中
登记了 ID ?
S5
否
S6
RA 登记处中存在空间?
否
是
添加 ID 到 RA 登记处
S7
S8
设置结果代码为“成功”
设置结果代码为“失败”
S9
结束

图 8

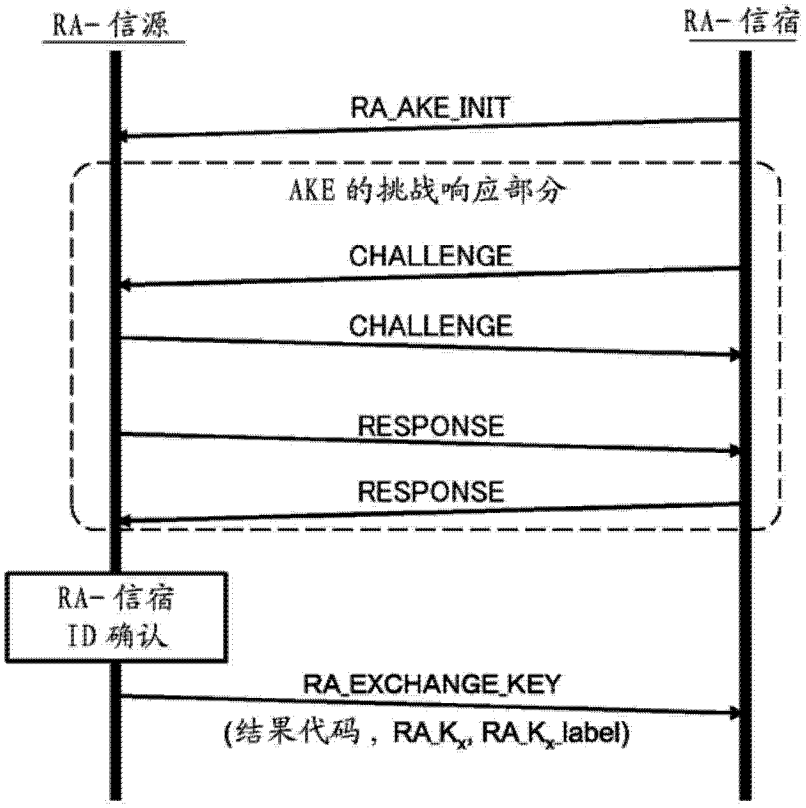

RA-信源
RA-信宿
RA_AKE_INIT
AKE 的挑战响应部分
CHALLENGE
CHALLENGE
RESPONSE
RESPONSE
RA-信宿
ID 确认
RA_EXCHANGE_KEY
(结果代码，RA_Kx, RA_Kx_label)

图 9

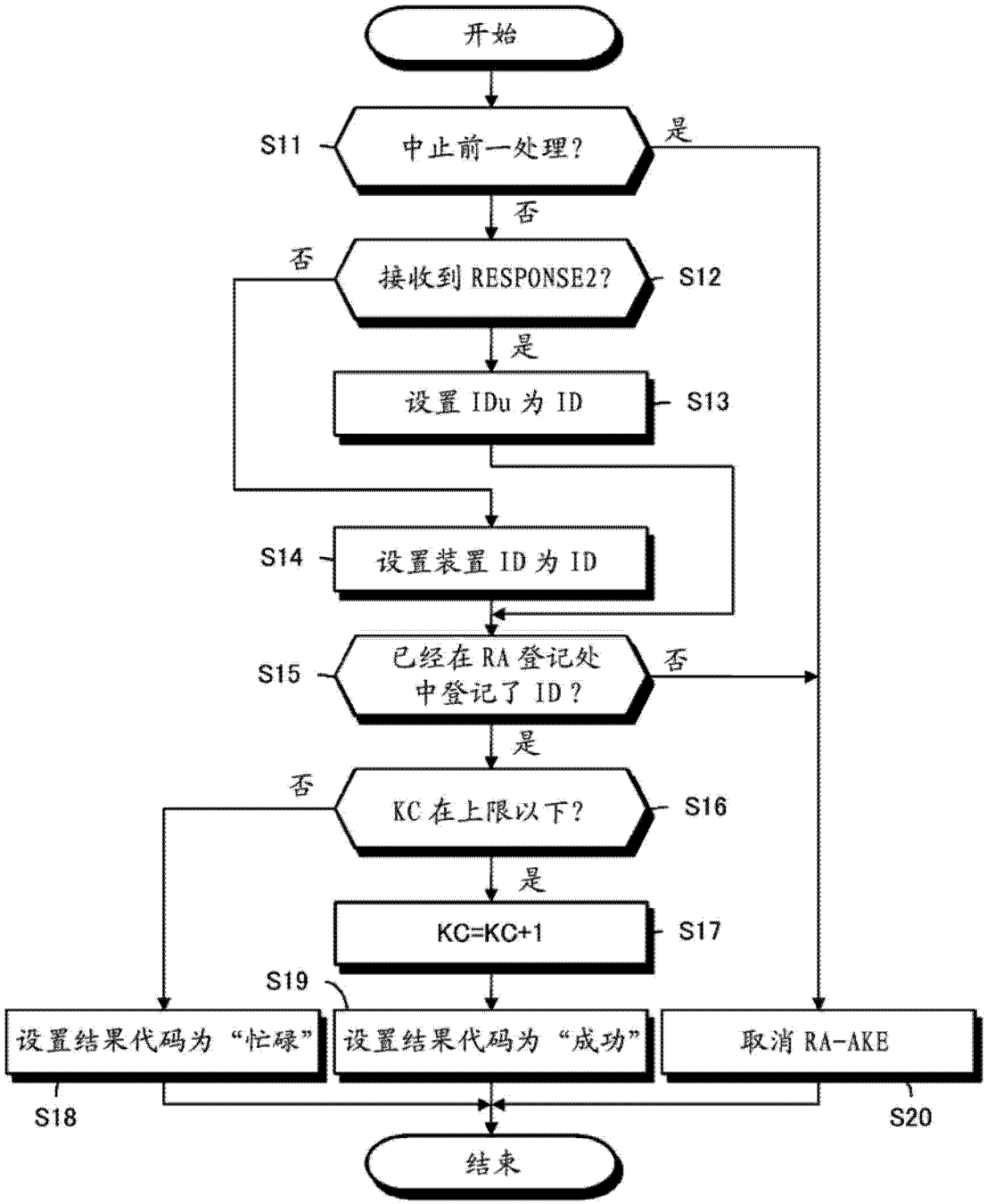

开始
S11
中止前一处理?
是
否
否
接收到 RESPONSE2?
S12
是
设置 IDu 为 ID
S13
S14
设置装置 ID 为 ID
S15
已经在 RA 登记处
中登记了 ID?
否
是
否
KC 在上限以下?
S16
是
KC=KC+1
S17
S19
设置结果代码为“忙碌”
设置结果代码为“成功”
取消 RA-AKE
S18
S20
结束

图 10

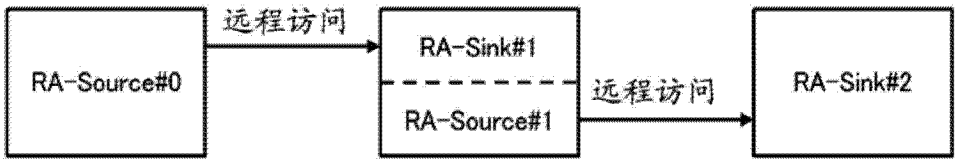

RA-Source#0
远程访问
RA-Sink#1
RA-Source#1
远程访问
RA-Sink#2

图 11

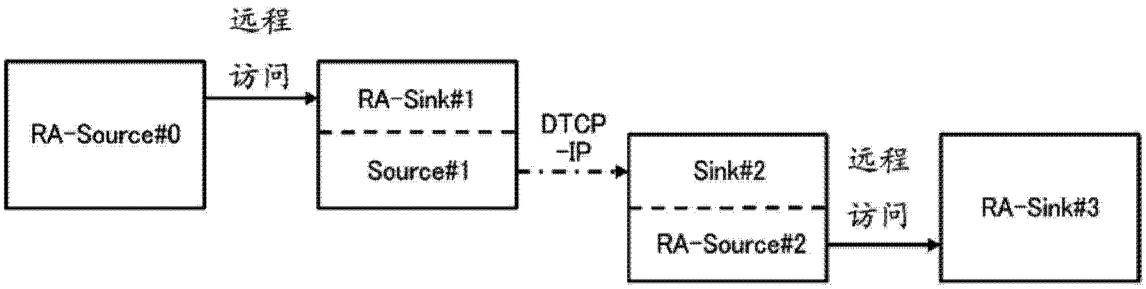

远程
访问
RA-Source#0
RA-Sink#1
Source#1
DTCP
-IP
Sink#2
RA-Source#2
远程
访问
RA-Sink#3

图 12

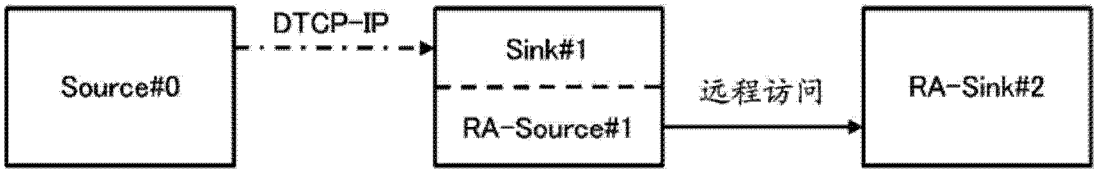

Source#0
DTCP-IP
Sink#1
RA-Source#1
远程访问
RA-Sink#2

图 13

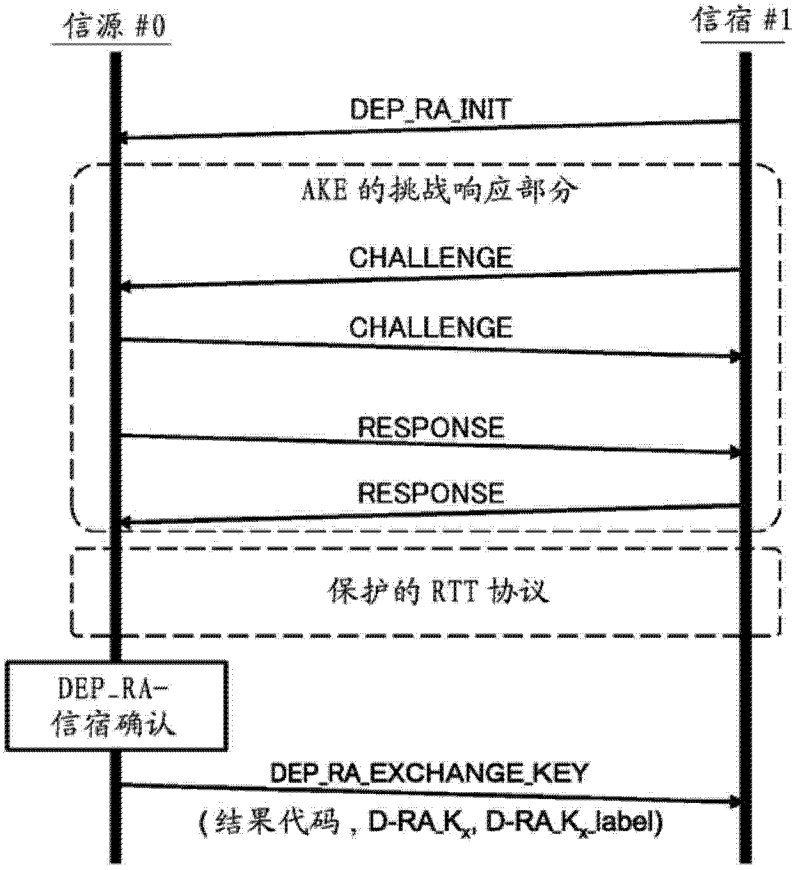

信源 #0
信宿 #1
DEP_RA_INIT
AKE 的挑战响应部分
CHALLENGE
CHALLENGE
RESPONSE
RESPONSE
保护的 RTT 协议
DEP_RA-
信宿确认
DEP_RA_EXCHANGE_KEY
(结果代码，D-RA_K$_x$, D-RA_K$_x$_label)

图 14

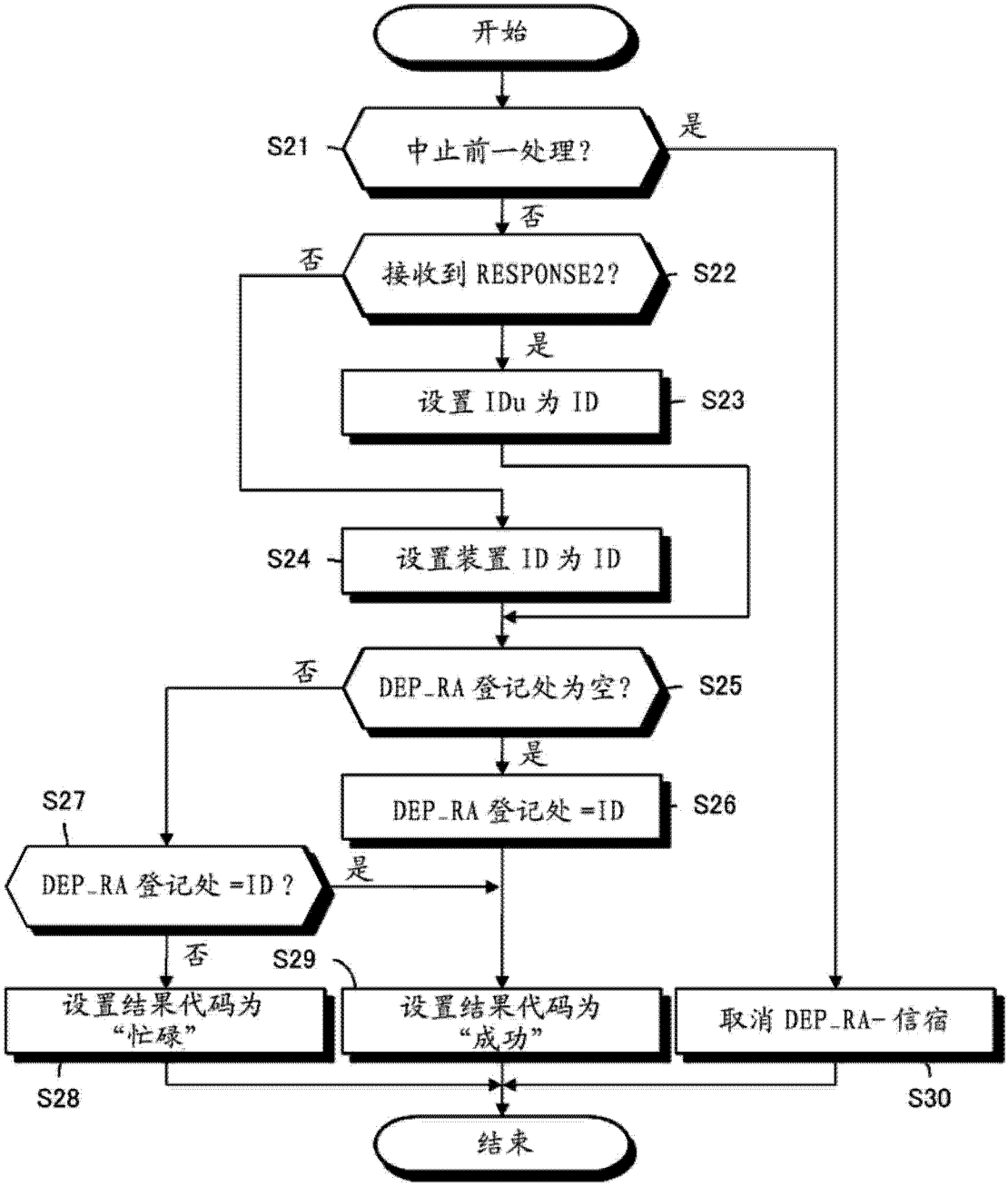

开始
S21
中止前一处理?
是
否
否
接收到 RESPONSE2?
S22
是
设置 IDu 为 ID
S23
S24
设置装置 ID 为 ID
否
DEP_RA 登记处为空?
S25
是
S27
DEP_RA 登记处 =ID
S26
DEP_RA 登记处 =ID ?
是
否
S29
设置结果代码为
“忙碌”
设置结果代码为
“成功”
取消 DEP_RA- 信宿
S28
S30
结束

图 15

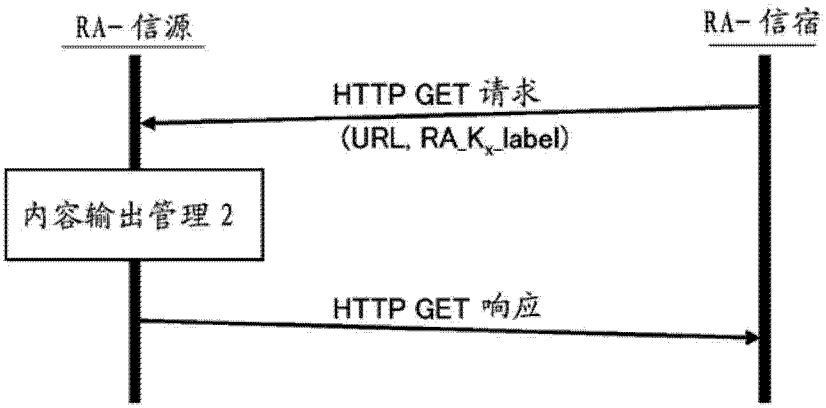


图 16

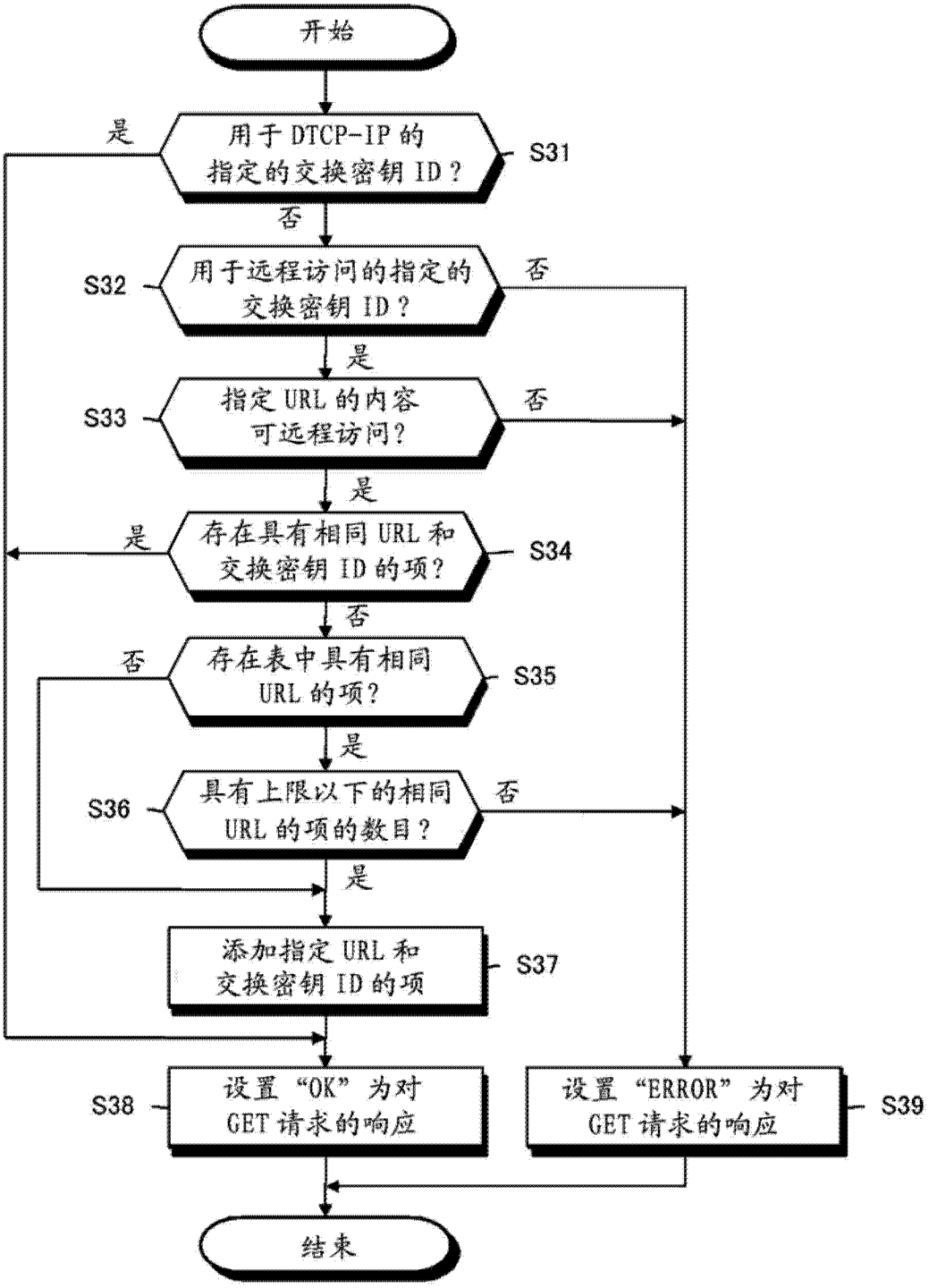

开始
用于 DTCP-IP 的指定的交换密钥 ID？
S31
是
否
用于远程访问的指定的交换密钥 ID？
S32
否
是
指定 URL 的内容可远程访问？
S33
否
是
存在具有相同 URL 和交换密钥 ID 的项？
S34
是
否
存在表中具有相同 URL 的项？
S35
否
是
具有上限以下的相同 URL 的项的数目？
S36
否
是
添加指定 URL 和交换密钥 ID 的项
S37
设置“OK”为对 GET 请求的响应
S38
设置“ERROR”为对 GET 请求的响应
S39
结束

图 17

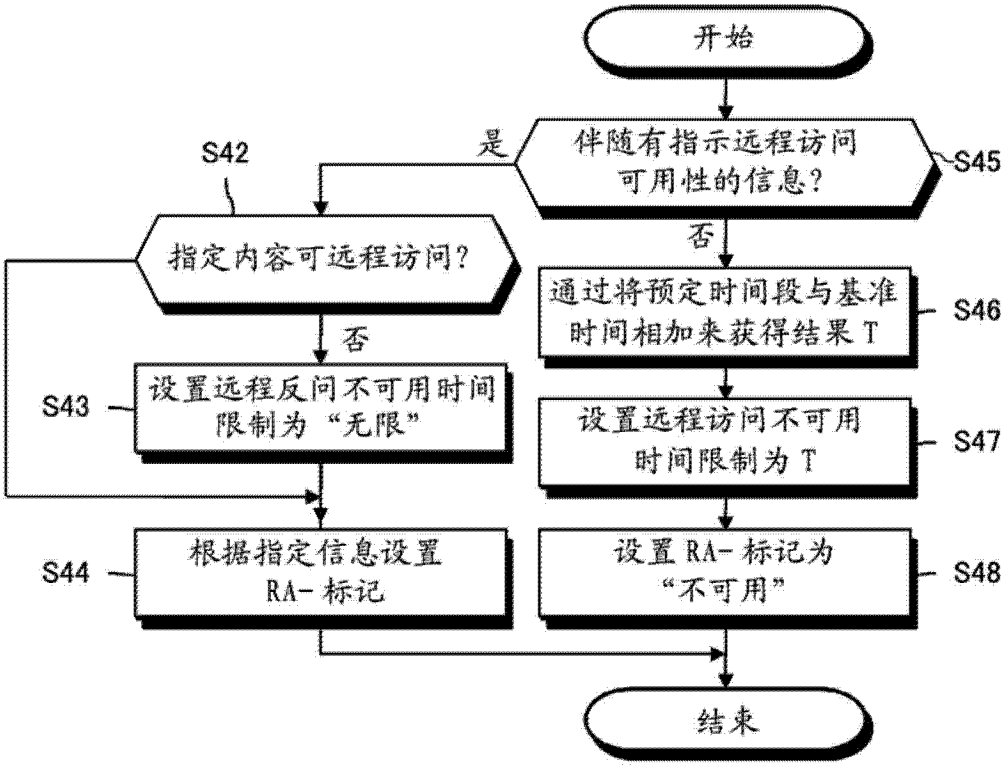

开始
伴随有指示远程访问可用性的信息?
是
否
S45
S42
指定内容可远程访问?
否
通过将预定时间段与基准时间相加来获得结果 T
S46
S43
设置远程反问不可用时间限制为“无限”
设置远程访问不可用时间限制为 T
S47
S44
根据指定信息设置 RA- 标记
设置 RA- 标记为“不可用”
S48
结束

图 18

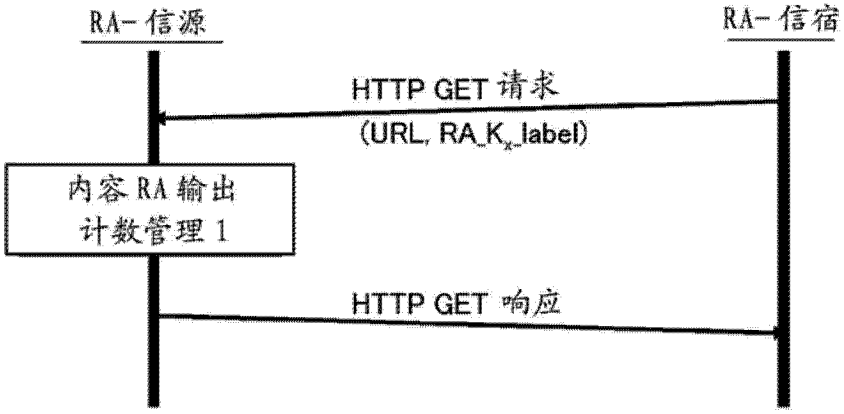

RA- 信源
RA- 信宿
HTTP GET 请求
(URL, RA_K_x_label)
内容 RA 输出
计数管理 1
HTTP GET 响应

图 19

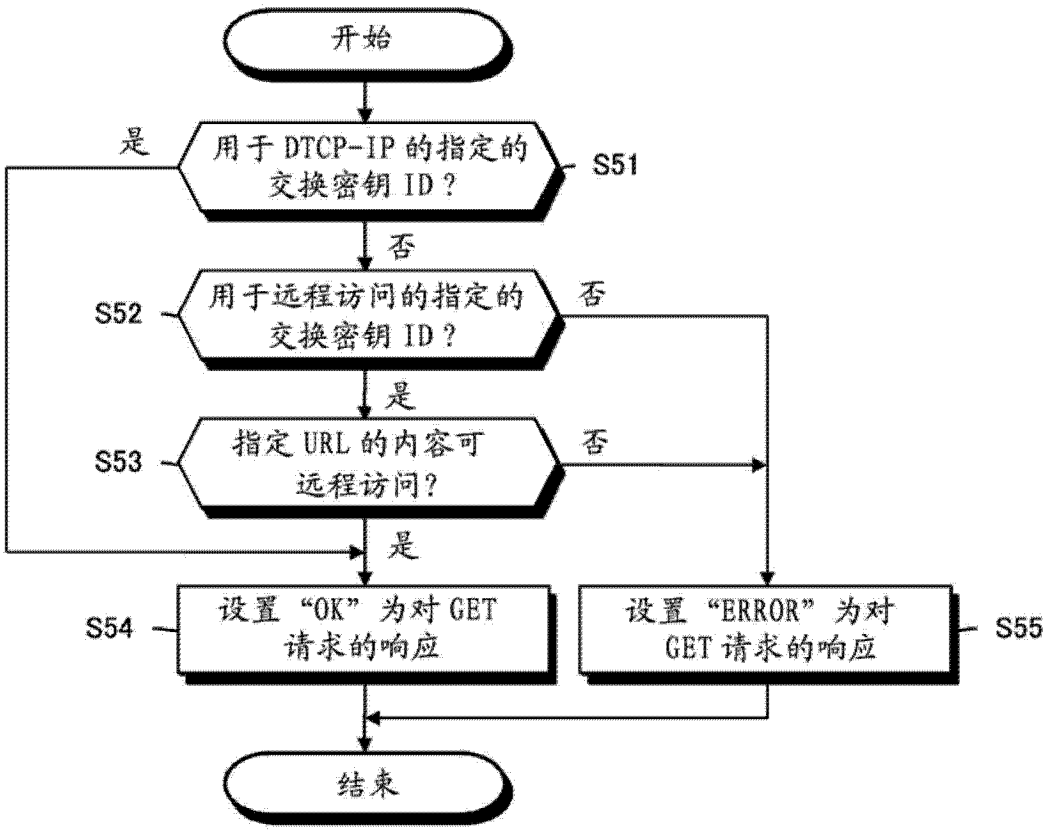

开始
是
用于 DTCP-IP 的指定的交换密钥 ID？
S51
否
S52
用于远程访问的指定的交换密钥 ID？
否
是
S53
指定 URL 的内容可远程访问？
否
是
S54
设置“OK”为对 GET 请求的响应
设置“ERROR”为对 GET 请求的响应
S55
结束

图 20

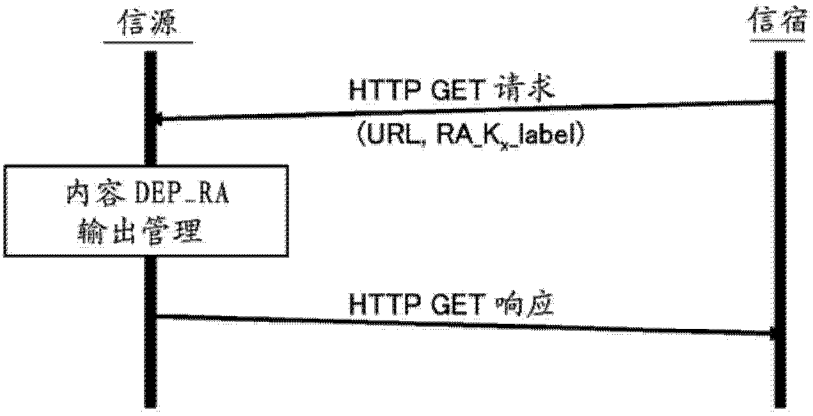

信源
信宿
HTTP GET 请求
(URL, RA_Kx_label)
内容 DEP_RA 输出管理
HTTP GET 响应

图 21

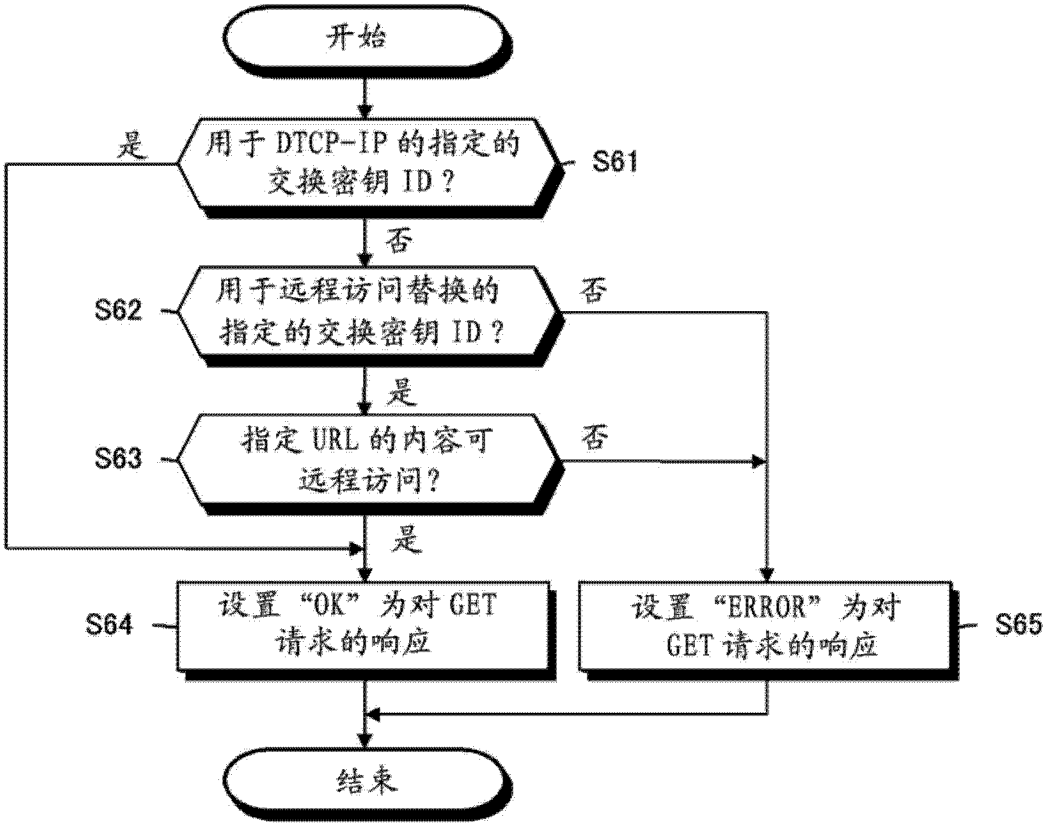

开始
用于 DTCP-IP 的指定的交换密钥 ID？
是
S61
否
用于远程访问替换的指定的交换密钥 ID？
S62
否
是
指定 URL 的内容可远程访问？
S63
否
是
设置“OK”为对 GET 请求的响应
S64
设置“ERROR”为对 GET 请求的响应
S65
结束

图 22

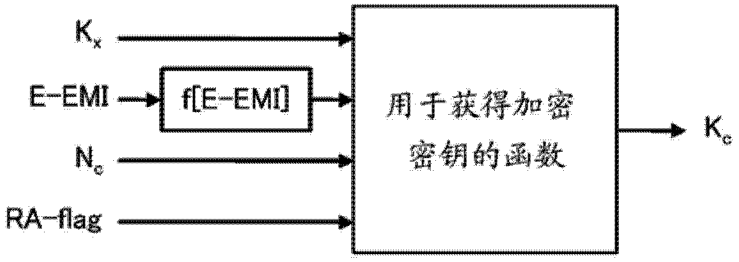

Kx
E-EMI
f[E-EMI]
Nc
RA-flag
用于获得加密密钥的函数
Kc

图 23

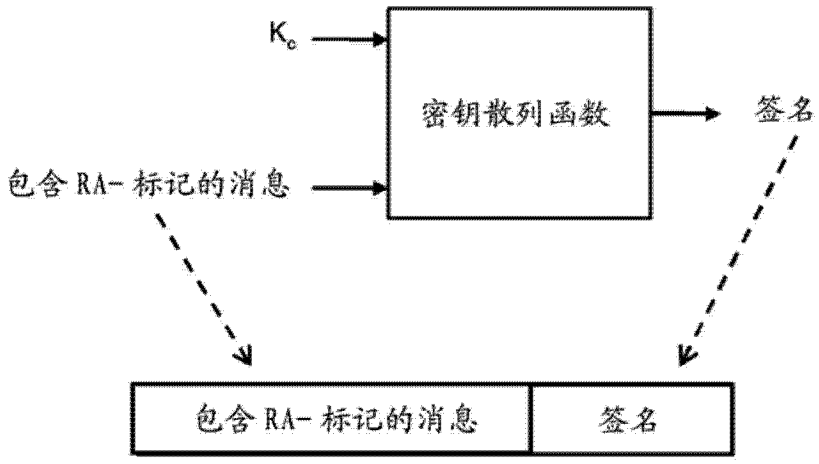


图 24

语法	大小（位）	格式	值
DTCP_descriptor (){			
descriptor_tag	8	uimsbf	0x88
descriptor_length	8	uimsbf	
CA_System_ID	16	uimsbf	0x0fff
for(i=0; i<descriptor_length-2; i++){			
private_data_byte	8	bslbf	
}			
}			

语法	大小（位）	格式
Private_data_type{		
Reserved	1	bslbf
Retention_Move_mode	1	bslbf
Retention_State	3	bslbf
EPN	1	bslbf
DTCP_CCI	2	bslbf
Reserved	5	bslbf
Image_Constraint_Token	1	bslbf
APS	2	bslbf
}		

图 25

	msb							lsb
PCP-UR[0]	UR 模式		内容类型		APS		ICT	
PCP-UR[1]	保留的							

图 26

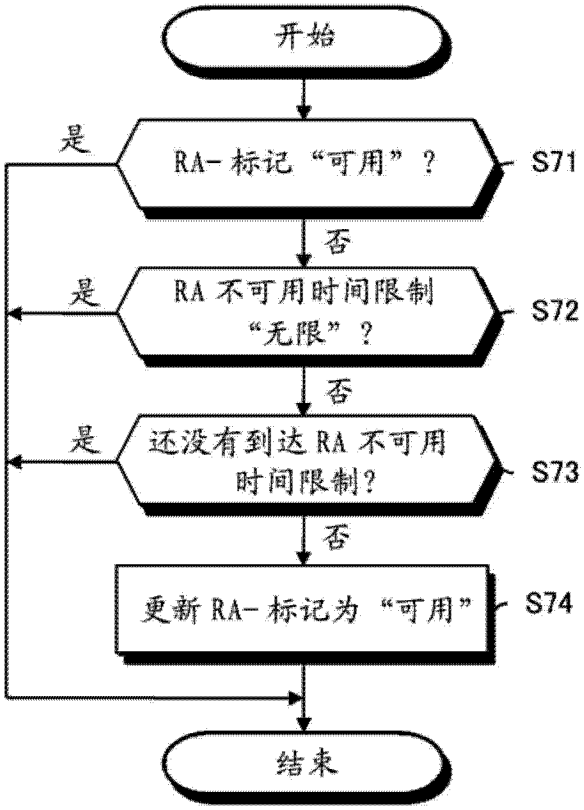


图 27

	msb							lsb
Type[0]	0	0	0	0	0	0	0	1
Length[0]	(msb) 控制和 AKE_Info 字段（N+8）的字节长度 (lsb)							
Length[1]								
Control[0]	保留的（零）				ctype/response			
Control[1]	Category = 0000_2 (AKE)				AKE_ID = 0000_2			
Control[2]	子函数							
Control[3]	AKE_procedure							
Control[4]	exchange_key							
Control[5]	subfunction_dependent							
Control[6]	AKE_label							
Control[7]	数目（可选）				状态			
AKE_Info[0..N-1]	AKE_Info							

图 28

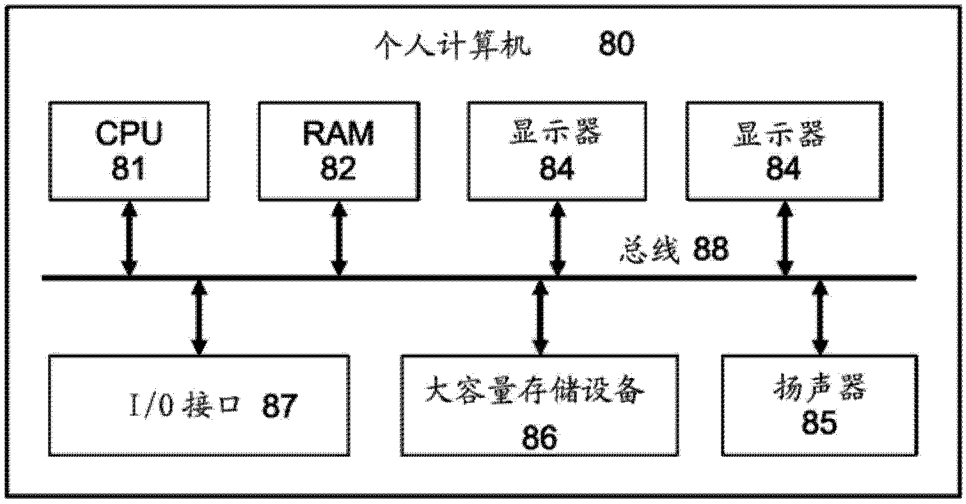


图 29

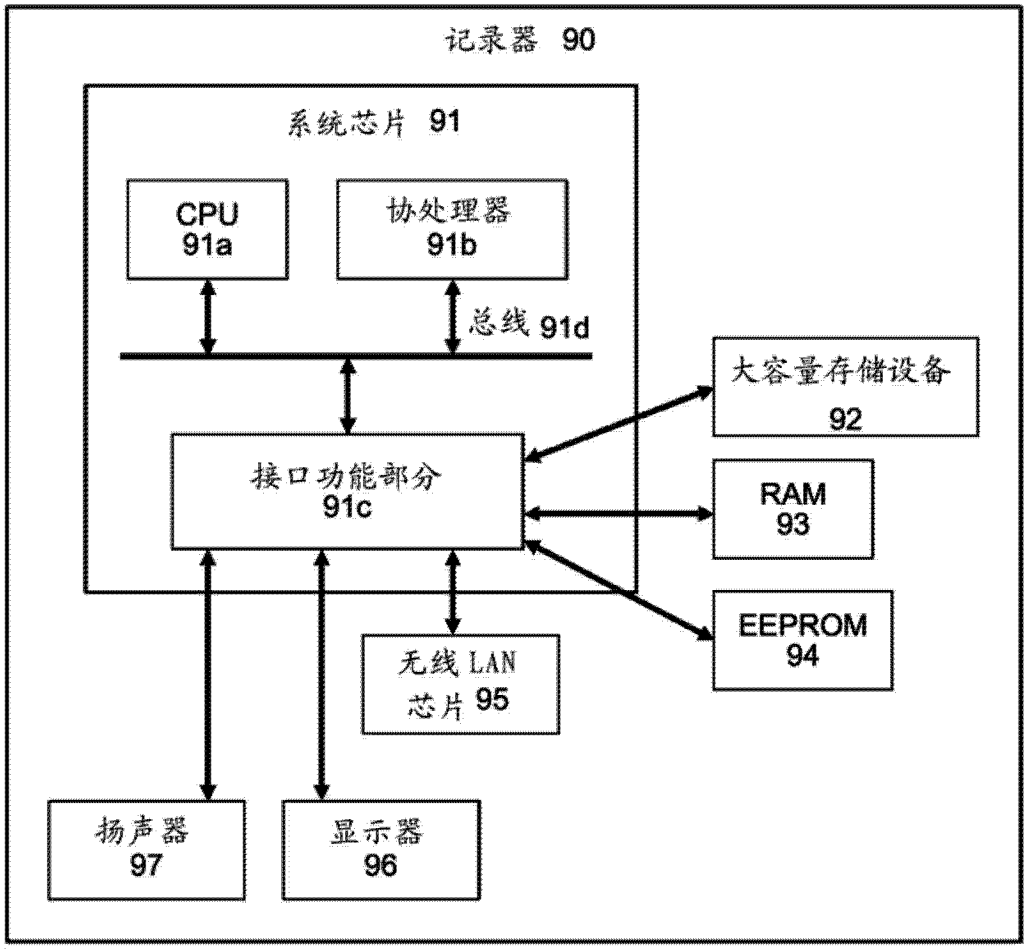

记录器 90
系统芯片 91
CPU
91a
协处理器
91b
总线 91d
大容量存储设备
92
接口功能部分
91c
RAM
93
EEPROM
94
无线 LAN
芯片 95
扬声器
97
显示器
96

图 30