(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 1868187 B
(45)授权公告日 2010.06.16

(21)申请号 200480029614.7
(22)申请日 2004.01.27
(30)优先权数据
60/494,836 2003.08.13 US
(85)PCT申请进入国家阶段日
2006.04.10
(86)PCT申请的申请数据
PCT/US2004/002407 2004.01.27
(87)PCT申请的公布数据
WO2005/020541 EN 2005.03.03
(73)专利权人 汤姆森许可公司
地址 法国布洛涅-比扬古
(72)发明人 J·张 J·李 K·拉马斯瓦米
(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 杨凯 刘杰
(51)Int.Cl.
H04L 29/06(2006.01)
G06F 1/00(2006.01)
(56)对比文件
WO 03/061189 A1,2003.07.24, 说明书第2页第28行至第5页第7行,第12页第7-19行,第18页第6行至第22页第3行,第29页第12行至第31页第11行,图1、3.
US 2002/0131594 A1,2002.09.19, 说明书第0023、0024、0068、0070、0073、0085、0087、0089、0107、0229、0230段.
审查员 郑剑文

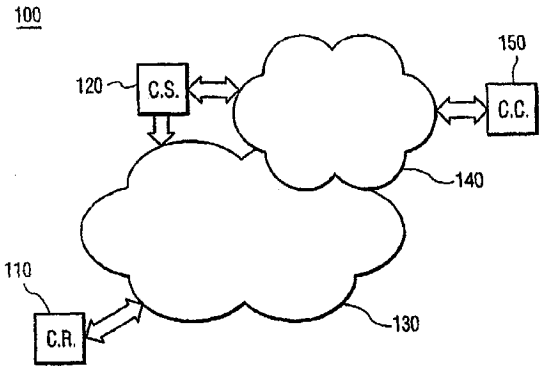
权利要求书 2 页 说明书 5 页 附图 6 页

(54)发明名称

通过内容密钥使通信网络上内容传递安全的方法及装置

(57)摘要

公开了一种将在网络上接收的安全内容解扰的方法。所述方法可用在位于与网络(140)通信的远程地点的接收装置(150)中,用以接收用远程地点所知的加密密钥(P_u)加扰的第一信息项,并用对应的解密密钥解扰所述第一信息项,其中第一信息项包括访问代码(CAC)和内容密钥(K_c),在管理第二信息项的服务器(120)验证所述访问代码(CAC)以后,接收用内容密钥加扰的第二信息项并用所述内容密钥(K_c)解扰所述第二信息项。



CN 1868187 B

1. 一种与具有至少一个服务器的网络通信的位于远程地点的装置，其中包括：

用于接收用所述远程地点所知的密钥加扰的包含访问代码和内容密钥的第一信息项的装置，所述访问代码响应内容请求器对第二信息项的请求而生成；

用于用对应的解密密钥解扰所述第一信息项的装置；

用于将所述访问代码传送到管理所述第二信息项的服务器的装置；以及

用于在管理第二信息项的所述服务器验证所述访问代码后，接收用所述内容密钥加扰的所述第二信息项的装置。

2. 按照权利要求 1 所述的装置，其中，所述用于解扰的装置还包括用所述内容密钥解扰所述第二信息项的装置。

3. 按照权利要求 1 所述的装置，其中，所述第一信息项包含使用限制指示。

4. 按照权利要求 1 所述的装置，其中，还包括用于自动地、在预定时间、偏离该预定时间地或者响应手动输入地传送未加密的访问代码的装置。

5. 按照权利要求 1 所述的装置，其中，所述内容密钥选自公开密钥或共享密钥。

6. 按照权利要求 3 所述的装置，其中，所述使用限制指示选自使用次数或时间周期。

7. 按照权利要求 1 所述的装置，其中，所述第一信息项还包含内容存储位置。

8. 按照权利要求 7 所述的装置，还包括用于传送所述内容存储位置的装置。

9. 按照权利要求 7 所述的装置，其中，所述内容存储位置是已知的。

10. 一种在与具有至少一个服务器的网络通信的位于远程地点的接收装置中使用的、解扰在所述网络上接收的安全内容的方法，所述方法包括如下步骤：

接收用所述远程地点所知的密钥加扰的包含访问代码和内容密钥的第一信息项，所述访问代码响应内容请求器对第二信息项的请求而生成；

用对应的解密密钥解扰所述第一信息项；

将所述访问代码传送到管理所述第二信息项的服务器 1；

在管理第二信息项的所述服务器验证所述访问代码后，接收用所述内容密钥加扰的所述第二信息项；以及

用所述内容密钥解扰所述第二信息项。

11. 按照权利要求 10 所述的方法，其中，所述第一信息项包含使用限制指示。

12. 按照权利要求 10 所述的方法，其中，所述内容密钥选自如下所列的各项：公开密钥、共享密钥。

13. 按照权利要求 11 所述的方法，其中，所述使用限制指示选自如下所列的各项：使用次数、时间周期。

14. 按照权利要求 10 所述的方法，其中，所述第一信息项还包含内容存储位置。

15. 按照权利要求 14 所述的方法，其中，所述内容存储位置是已知的。

16. 一种在网络上传送安全内容的方法，包括如下步骤：

在第一网络的第一服务器上接收来自文件请求装置的内容请求，所述请求包含为指定的远程地点所知的加密密钥；

响应所述文件请求装置对内容的所述请求在所述服务器上生成包含访问代码和内容密钥的第一信息项；以及

传送所述第一信息项至具有文件接收装置的所述指定的远程地点，其中所述访问代码

和所述内容密钥用所述加密密钥加扰；

从具有所述文件接收装置的所述指定的远程地点接收所述访问代码；

在验证所述访问代码后在第二网络上传送所述安全内容，其中所述安全内容用所述内容密钥加密。

17. 按照权利要求 16 所述的方法，其中，所述第一网络和所述第二网络是相同的网络。

18. 按照权利要求 16 所述的方法，其中，所述文件请求装置是掌上电脑、蜂窝电话、笔记本电脑或个人电脑。

19. 按照权利要求 17 所述的方法，其中，所述文件请求装置是掌上电脑、蜂窝电话、笔记本电脑或个人电脑。

20. 按照权利要求 16 所述的方法，其中，所述第一网络是无线网络。

21. 按照权利要求 16 所述的方法，其中，所述第一信息项包含所述内容的存储位置。

22. 按照权利要求 16 所述的方法，还包括以下步骤：向与所述第一服务器通信的至少一个其他服务器传送所述内容，其中所述内容用所述内容密钥加扰。

23. 按照权利要求 22 所述的方法，还包括以下步骤：在验证所述访问代码后在第二网络上传送所述安全内容，其中所述安全内容用所述内容密钥加扰。

24. 按照权利要求 16 所述的方法，其中，传送所述访问代码和所述内容密钥的步骤在所述第一网络上进行。

25. 按照权利要求 16 所述的方法，其中，传送所述访问代码和所述内容密钥的步骤在所述第二网络上进行。

26. 按照权利要求 16 所述的方法，其中，所述第二网络是高速网络。

27. 按照权利要求 26 所述的方法，其中，所述第二网络是内容传递网络。

28. 按照权利要求 16 所述的方法，还包括如下步骤：向所述指定的远程地点传送所述内容的存储位置。

通过内容密钥使通信网络上内容传递安全的方法及装置

[0001] 优先权主张

[0002] 本申请是 2002 年 10 月 12 日提交的标题为“延迟的网络信息传送的装置与方法 (Apparatus and Methods for Delayed NetworkInformation Transfer)”的共有的同时待审的美国专利申请号 PCT/US/39474 的部分继续申请，该申请通过引用而纳入本文。相关专利申请

[0003] 本申请与 2002 年 10 月 12 日提交的标题为“用代理下载数据的系统与方法 (System and Method for Downloading Data Using AProxy)”的共同受让的同时待审的美国专利申请号 PCT/US/02/39475 相关，该申请通过引用而纳入本文。

技术领域

[0004] 本发明一般地涉及电子数据传输，更具体地说，涉及在网络环境中使电子信息安全的方法。

背景技术

[0005] 在通过网络运营传递多介质内容时，用户或内容请求器 (CR) 可以操作例如蜂窝电话或掌上电脑 (PDA) 的装置，向内容服务器 (CS) 发出请求，授权内容服务器马上下载所请求的数据、信息项或内容。另一方面，CR 可以请求 CS 按安排的时间下载所请求的数据、信息项或内容。而且，CR 可立即或按照安排的时间请求数据、信息项或内容被下载或者传递到第二装置，即内容接收机或消费装置 (CC)。后面这种运行方式更适用于当 CR 装置运行在带宽窄的网络上而缺乏足够的带宽下载所需要的信息时。例如，用户可以使用运行在低速网络上的蜂窝装置请求将音频和 / 或视频 (多介质) 信息传递到例如家用电脑或手提电脑等接收装置上。

[0006] 然而，在 CS 提供所请求的信息之前，CR 和 / 或 CC 必须分别被授权请求和 / 或接收所要求的信息。

[0007] 因此，要求这些装置更好地保护多介质内容，防止未经授权的获得以及未经授权方的进入。

发明内容

[0008] 公开了一种解扰在网络上接收的安全内容的方法。在一实施例中，所述方法可用在位于与网络通信的远程地点的接收装置上，用以接收经远程地点已知的加密密钥加扰的第一信息项，使用对应的解密密钥解扰所述第一信息项，其中第一信息项包括访问代码和内容密钥，在管理第二信息项的服务器验证所述访问代码以后，接收经内容密钥加扰的第二信息项以及用所述内容密钥解扰所述第二信息项。在本发明另一方面，第一信息项包括所要求的内容的存储位置。该存储位置也可用密钥加密。

附图说明

[0009] 图 1 表示示范性内容传递的框架；

[0010] 图 2 表示在图 1 所示的传递框架内实现安全内容传递的示范性过程；

[0011] 图 3 表示另一示范性内容传递框架；

[0012] 图 4 表示在图 3 所示的传递框架内实现安全内容传递的示范性过程；

[0013] 图 5 表示按照本发明一方面的安全内容信息加扰过程的流程图；

[0014] 图 6 表示按照本发明一方面的安全内容信息解扰过程的流程图；以及

[0015] 图 7 表示执行本发明所示过程的装置。

[0016] 应当理解这些附图仅用于说明本发明概念，并不作为限制本发明的定义。图 1-7 所示的并结合附图详细说明的实施例仅用作示例性实施例，并不构成实现本发明的唯一方式。而且，相同的标记（在适当的地方可能还附加字符）用于标注相同的部件。

具体实施方式

[0017] 图 1 表示内容传递框架 100 的通信，内容传递框架 100 包含通过网络 130 与内容服务器 (CS) 120 通信的内容请求器 (CR) 110。CS120 还通过网络 140 与内容消费装置 150 通信。在一个示范结构中，网络 130 可以是低速网络，而网络 140 可以是高速网络。在另一结构中，网络 130 和 140 可以是速度相差不大的相同网络或者不同网络。在一实施例中，CR110 可以是蜂窝电话，网络 130 可以是较低速的无线网络。网络 140 可以是例如互联网或专用内容传递网络 (CDN) 等的高速网络。在另一实施例中，CR110 可以是手提电脑，网络 130 可以是与互联网（可以表示为网络 140）连接的局域网。

[0018] 图 2 表示在图 1 所示的网络结构上提供安全内容传递的示范性运行过程 200。在这示范运行过程中，CR110 经由网络 130 向 CS120 发出如箭头 210 所示的对信息内容的请求。在一示范实施例中，请求 210 可包含与内容消费装置 (CC) 150 关联的加密密钥。例如，假如 CC150 使用公开密钥 / 私有密钥加密，那未 CC150 的公开密钥（标为 P_u）可提供给 CS120。数字证书也可用来核实内容请求器 110 之经授权访问 CS120。在另一方面，密钥 P_u 可以是为 CS120 和 CC150 所知的或共享的密钥值。

[0019] 所提供的加密密钥本身可以用为 CR110 和 CS120 所知或共享的密钥加密或者加扰。共享密钥（标为 S_0）用箭头 210 表示，向 CS120 确保 CR110 是获准做出请求的。在一方面，CR110 可以在为 CS120 提供的服务而注册时获得共享密钥 S_0。另一方面，CR110 可以使用通过向 CS120 发送常规用户名称和密码而建立的经防护的链路与 CS120 通信。CS120 可以做出响应，向用户 CR110 提供共享密钥 S_0。例如互联网协议地址或存储位置等对指定的 CC150 的参照数据也可以包含在请求中。

[0020] CS120 在鉴别 CR110 是获准做出请求 210 以后，为指定的内容消费装置建立内容访问证书 (CAC) 或者访问代码。CAC 由指定的 CC150 用于在以后时间访问请求的内容。由箭头 220 表示的通知发送给 CC150。在此场合，通知 220 包含 CAC 和内容密钥（标为 K_c）。密钥 K_c 用于加扰或者加密请求的内容。使用与 CC150 有关的密钥 P_u 加扰或者加密 CAC 和 K_c，在此图的示例中 P_u 由 CR110 给予的。由 LIC 表示的使用限制或执照可以与内容密钥 K_c 有关的。在此场合执照 LIC 可以限制 K_c 为有效的次数或者时间周期。对密钥 K_c 的这种使用限制提供了限制内容的后续分配的手段。

[0021] CC150 用与密钥 P_u 有关的解密密钥来解密或解扰通知消息，以获得 CAC 和密钥 K_c。然后，如箭头 225 所示，向 CS120 发送 CAC 以授权对所请求信息项的传递或下载。在图示的

顺序中，内容下载由箭头 230 表示。一旦收到信息项，如箭头 240 所示，用所给的密钥 K_c 解扰或者解密信息项。现在 CC150 可以看到由 CC110 请求的已解扰的内容。本领域技术人员当知，密钥 K_c 用于加密或者解密所提供的内容，因此密钥 K_c 可以被称为加密密钥、解密密钥或者内容传递密钥。

[0022] 尽管在此叙述的顺序提供比较及时的请求内容的传递，本领域技术人员应知，来自 CS120 的 CAC 的传递可以按预定时间发生，或者按从做出初次请求的时间算起的预定延迟发生。从 CC150 至 CS120 的 CAC 传递可以自动或手动地执行。在手动执行时用户可以在 CC150 上做启动操作，使 CAC 被发送。同样地，CS120 可以延迟 CAC 和内容密钥 Kc 的发送，直至已知的时间或者在经过已知的时间偏移后。

[0023] 图 3 表示按照本发明一方面的内容传递框架 300。在该图示例中，CR110 和 CS120 如上所述通过网络 130 通信。CS120 也通过网络 140 与 CDN 中介器 310 通信，而 CDN 中介器 310 还可以通过网络 330 与一个或多个边缘服务器（由 ES320 表示）通信。而且，在此图示例中，CC150 已经进入至少一个网络 330。如上所述，网络 130、140 和 330 可以是具有不同、相同或者相差不大的数据传输速度的网络。例如，网络 130 可以是低速、窄带网络，而网络 140 和 330 可以是高速、宽带网络。网络 330 还可代表专用内容传递网络 (CDN)。本领域技术人员当会理解，网络 130、140 和 330 也可以是相同网络。所示的 CDN 结构和 CDN 中介器 310 的使用使系统能将请求的内容分发给当地可能有多个用户请求相同内容的不同的边缘服务器。

[0024] 图 4 表示在图 3 所示的网络结构上提供安全内容传递的示范性时序序列 400。如上所述，在此序列中，CR110 请求（如箭头 210 所示）CS120 提供指定的内容给 CC150。内容服务器 120 从 CDN 中介器 310 获得与 CC150 关联的指定的 ES 的信息。CS120 还生成 CAC 并创建高速缓存内容访问证书 (CCAC)。在本发明的一方面，CAC 包含指定的 CC150 的地址以及口令。同样地，CCAC 包含指定的边缘服务器 (ES)320 的地址以及第二口令。CAC 和 CCAC 被加密，并被送至 CDN 中介器 310，如箭头 410 所示。在此例中，使用为 CS120 和 CDN 中介器 310 所知或共享的密钥（标为 S_1）加密 CAC 和 CCAC。CDN 中介器 310 解密所发送的信息，并且此例中用密钥（称为 S_2）再加密 CAC 和 CCAC。密钥 S_2 由 CDN 中介器 310 和 ES320 共有或共享。如箭头 430 所示，ES320 用 CAC 从 CS 120 访问请求的内容，请求的内容通过来自 CS120 的内容密钥 K_c 加扰。CS120 还向 CC150 发出通知，如箭头 220 所示。该通知 220 与图 2 所示的相似，包含有关所请求信息或内容的存储位置（即 ES320 地址）的信息和加密或加扰的 CCAC 以及内容密钥 K_c。如上所述，使用与 CC150 关联的或 CC150 已知的密钥 P_u 加密 CCAC 和密钥 K_c。而且，内容的存储位置也可被加密。另一方面，内容的存储位置可以不加扰地提供。

[0025] 然后 CC150 可以解密信息，并将所接收的 CCAC 发送给 ES320，如箭头 340 所示。CC150 然后可以下载所请求的或所要求的使用密钥 K_c 加密的内容，如箭头 230’所示。如上所述，CC150 就可以解密所接收的内容。在本发明另一方面，密钥 K_c 可以与使用限制执照关联，使用限制执照限制密钥 K_c 的有效期。

[0026] 图 5 表示按照本发明原理解密请求内容的示范性过程 500 的流程图。在此示范性过程中，在步骤 510 确定是否收到消息。假如答案为否，那未过程继续等待消息接收。然而，假如答案为是，在步骤 520 使用私有密钥解密或者解扰该消息。从被解密的消息得到内

容访问代码和密钥 K_c。例如，对于图 2 所示的顺序而言，内容访问密钥或代码就是所生成的 CAC，对于图 3 而言，内容访问密钥或代码就是所生成的 CCAC。

[0027] 在本发明的一方面，所要求的内容的存储位置也可包含在消息中。存储位置可以清楚地提供或者可加扰。在本发明的一方面，内容的存储位置可以由 CC150 得知，因此，不再需要包含在发送的消息中。

[0028] 在步骤 540，确定所请求的内容是否要下载。假如答案为否，那未在步骤 540 过程继续等待直至接收到某个要求下载的指示。例如，要求下载的指示可以发生在已知的时刻、与请求的时间偏离已知时间的时刻或者由用户手动输入的时刻。已知时刻或已知的时间偏离可以由用户在初次请求时给定。

[0029] 在步骤 550，当接收到指示时，内容访问密钥 (CAC 或者 CCAC) 被发送到已知的或者特定的内容存储位置。在步骤 560 接收内容，并在步骤 570 确定是否所有内容已经收到。假如答案为否，那未在步骤 560 过程继续接收所要求的内容。然而，假如答案为是，则使用提供的内容密钥即 K_c 将内容解密。

[0030] 图 6 表示按照本发明原理生成内容传递密钥或者代码的示范性过程 600 的流程图。在此图示过程中，在步骤 610 确定是否收到消息。假如答案为否，那未过程继续等待消息接收。

[0031] 然而，假如答案为是，那未在步骤 620 确定发送方是否被授权请求内容传递。假如答案为否，那未在步骤 610 继续等待消息接收。然而，假如答案为是，那未在步骤 625，用双方共有的密钥解密所请求的消息。消息包含所要求内容的信息并可包含所要求的消费装置位置的信息，假如所要求的消费装置位置不是已知的、预设或预定的地址，例如预先指定的地址。这个信息可以不加密地发送。消费装置的公开密钥或者其它加密信息被加密地发送。

[0032] 在步骤 630，内容访问密钥和内容密钥 K_c 被生成，并用由请求器或用户提供的公开密钥或其它加密信息加密。在步骤 640，经加密的信息通过通知消息传递给消费装置。

[0033] 在步骤 650，确定所要求的内容是否存储或保持在为消费装置所知的存储位置，即内容存储位置是否预设或预定的。假如答案为是，过程结束。然而，假如答案为否，那未在步骤 660 使用提供的公开密钥或者其它加密信息将内容存储位置加密，并在步骤 665 传递给消费装置。

[0034] 在步骤 670，使用内容服务器和含有或将含有所要求内容的边缘服务器之间已知的加密密钥将内容访问密钥或者代码加密或加扰。在步骤 680，用内容传递密钥 K_c 将内容加密。使用密钥 K_c 加扰内容的好处在于，服务器不需要附加的保密等级来防止对内容的未经授权的访问。而且，用密钥 K_c 来存储介质还有一个好处，就是它以对消费装置透明的方式存储内容，而不论是内容服务器还者边缘服务器传递内容。在步骤 685，内容被发送到消费装置或用户的位置。本领域技术人员当知，图 5 表示的过程更专门地与图 4 表示的顺序相关，图 4 的顺序在图 1 所示的顺序上增加了一些过程步骤。然而，也会认识到，当内容存储位置为消费装置已知时，过程 600 也能用于图 1 表示的顺序。

[0035] 图 7 表示实现在图 2-4 所示的示范性过程中描述的实施本发明原理的系统 700。在此示范性系统实施例 700 中，输入数据在网络 750 上从源 705 接收，并由处理系统 710 执行一个或多个程序（软件或者固件）加以处理。处理系统 710 的处理结果可以再通过网络 770 发送，以在显示器 780、报告设备 790 和 / 或第二处理系统 795 上观看。

[0036] 特别地，处理系统 710 包括通过网络 750 从所示出的源装置 705 接收数据的一个或多个输入 / 输出装置 740。然后，所接收的数据加到与输入 / 输出装置 740 和存储器 730 通信的处理器 720 上。输入 / 输出装置 740、处理器 720 和存储器 730 可以通过通信介质 725 通信。通信介质 725 可代表例如 ISA、PCI、PCMCIA 总线的通信网络，电路的一个或多个内部连线，电路板卡或者其它装置，以及这些或其它通信介质的若干部分和若干组合。处理系统 710 和 / 或处理器 720 可以表示手持的计算器、专用或通用处理系统、桌面电脑、手提电脑或者掌上电脑 (PDA) 装置等，以及可以执行所说明的运行过程的这些或者其它装置的若干部分或若干组合。

[0037] 处理器 720 可以是用来执行电脑指令代码或代码和逻辑运算组合的中央处理单元 (CPU) 或者例如 PAL、ASIC、FGPA 的专用硬件 / 软件。在一实施例中，处理器 720 可包含被执行时实现本文所述的运行过程的代码。该代码可包含在存储器 730 中，可以从例如 CD-ROM 或软盘等存储介质 (标记为 783) 中读出或下载，可以由手动输入装置 785(例如键盘或者小键盘) 输入或者可以在需要时从磁或光介质 (未图示) 读出。如图所示，处理器 720 可通过输入 / 输出装置 740 得到由输入装置 783、785 和 / 或磁介质提供的信息项。而且，由输入 / 输出装置 740 接收的数据可立即由处理器 720 访问或者可存储在存储器 730 中。处理器 720 还可提供处理结果给显示器 780、报告设备 790 或者第二处理单元 795。

[0038] 本领域技术人员应知，处理器、处理系统、电脑或电脑系统的术语可以表示与一个或多个存储单元和与至少一个处理单元电连接并且通信的其它装置 (例如外围设备) 通信的一个或多个处理单元。而且，所示的装置可以通过例如串行、并行、ISA 总线、微沟道总线、PCI 总线、PCMCIA 总线、USB 等内部总线或者电路、电路板卡或其它装置的内部连线，以及这些和其它通信介质的部分和组合或者例如互联网和内联网的外部网络与一个或多个处理单元电连接。在其他实施例中，硬件电路可代替软件指令或者与软件指令结合来实现本发明。例如，本文所述的部件也可为分离的硬件部件，或者集成为一个单独的单元。

[0039] 应当理解，所述的运行过程可以使用不同处理器顺序地或者并行地实现，以确定特定值。处理系统 710 也可以与各个源 705 双向通信。处理系统 710 还可越过一个或多个网络连接从一个或多个服务器在例如互联网、内联网的全球电脑通信网络、广域网 (WAN)、城域网 (MAN)、局域网 (LAN)、地面广播系统、有线电视网络、无线网络或者电话网络 (POTS) 以及这些和其它类型网络的部分和组合上接收或发送数据。应该理解，网络 750 和 770 也可以是内部网络或者电路、电路板卡或其它装置的一个或多个内部连线，以及这些和其它通信介质的若干部分和若干组合或者例如互联网和内联网等外部网络。

[0040] 尽管已经图示、叙述并指出适用于本发明优选实施例的本发明的基本创新特征，但是应该理解，本领域技术人员可以在所述的装置、公开装置的形式和细节以及它们的运行过程方面做出各种省略、替代和变化，而并不脱离本发明的精神。尽管对本发明的公开涉及多介质内容的安全，本领域技术人员应当认识到本文所述的方法和装置可以适用于需要安全的传递和授权访问的任何信息。显然，以基本相同的方式基本执行相同功能来达到相同结果的这些部件的所有组合均在本发明的范围内。从一个到另一个所述实施例的部件替代也完全在本文的考虑之中。

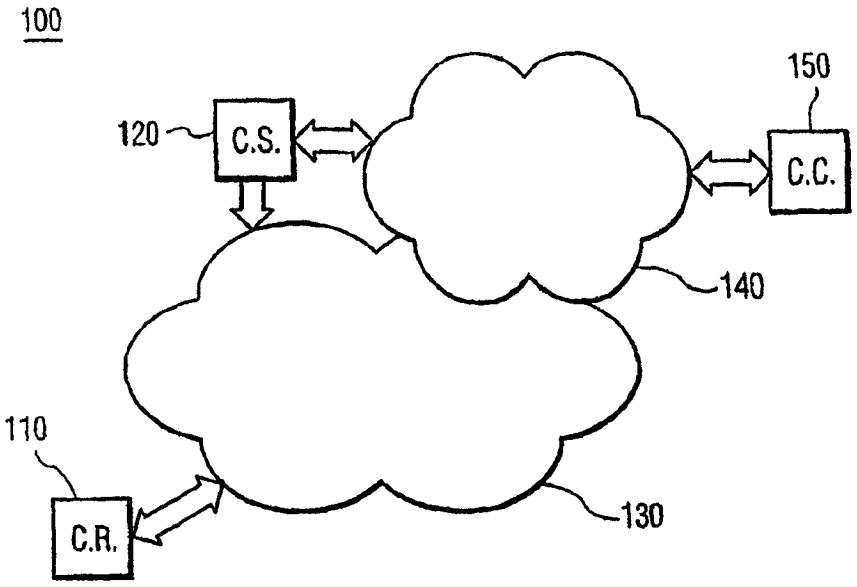

100
150
120
C.S.
C.C.
140
110
C.R.
130

图 1

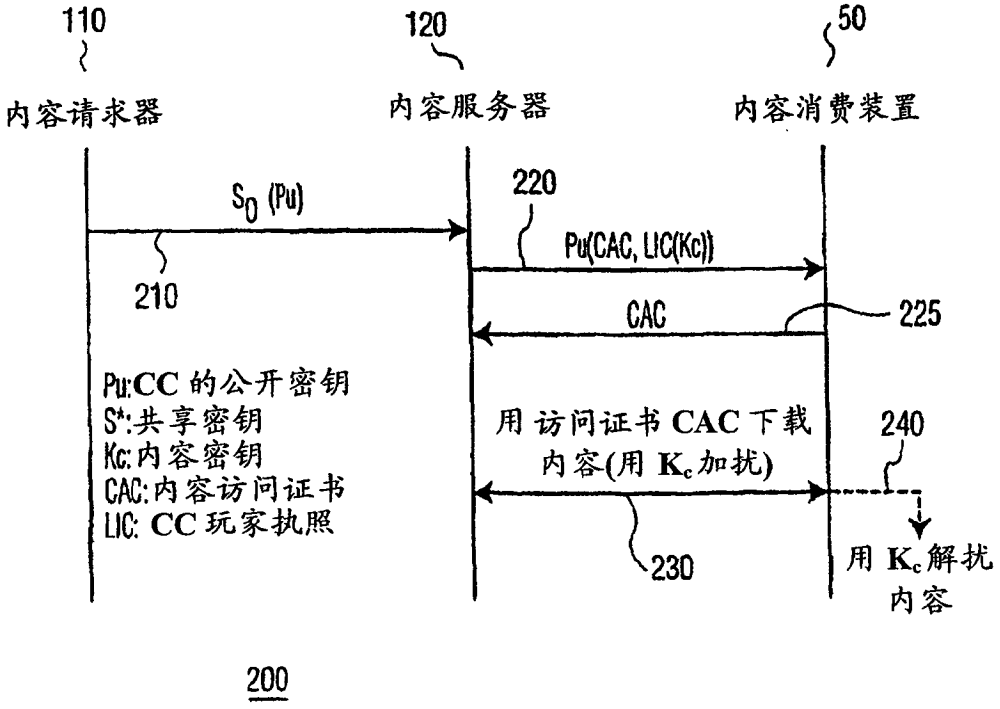

110
120
50
内容请求器
内容服务器
内容消费装置
S_0 (Pu)
220
Pu(CAC, LIC(Kc))
210
CAC
225
Pu:CC 的公开密钥
S*:共享密钥
Kc:内容密钥
CAC:内容访问证书
LIC: CC 玩家执照
用访问证书 CAC 下载
内容(用 K_c 加扰)
240
230
用 K_c 解扰
内容
200

图 2

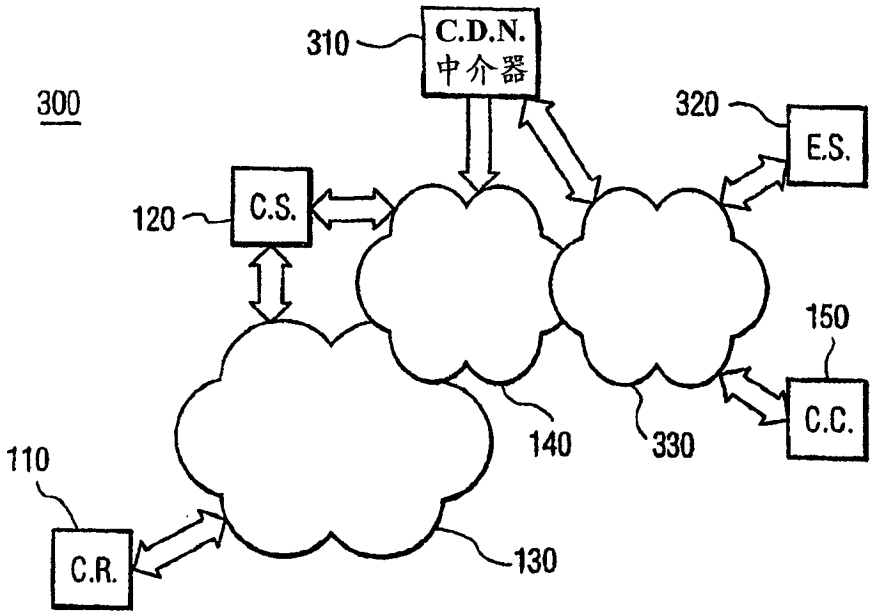


图 3

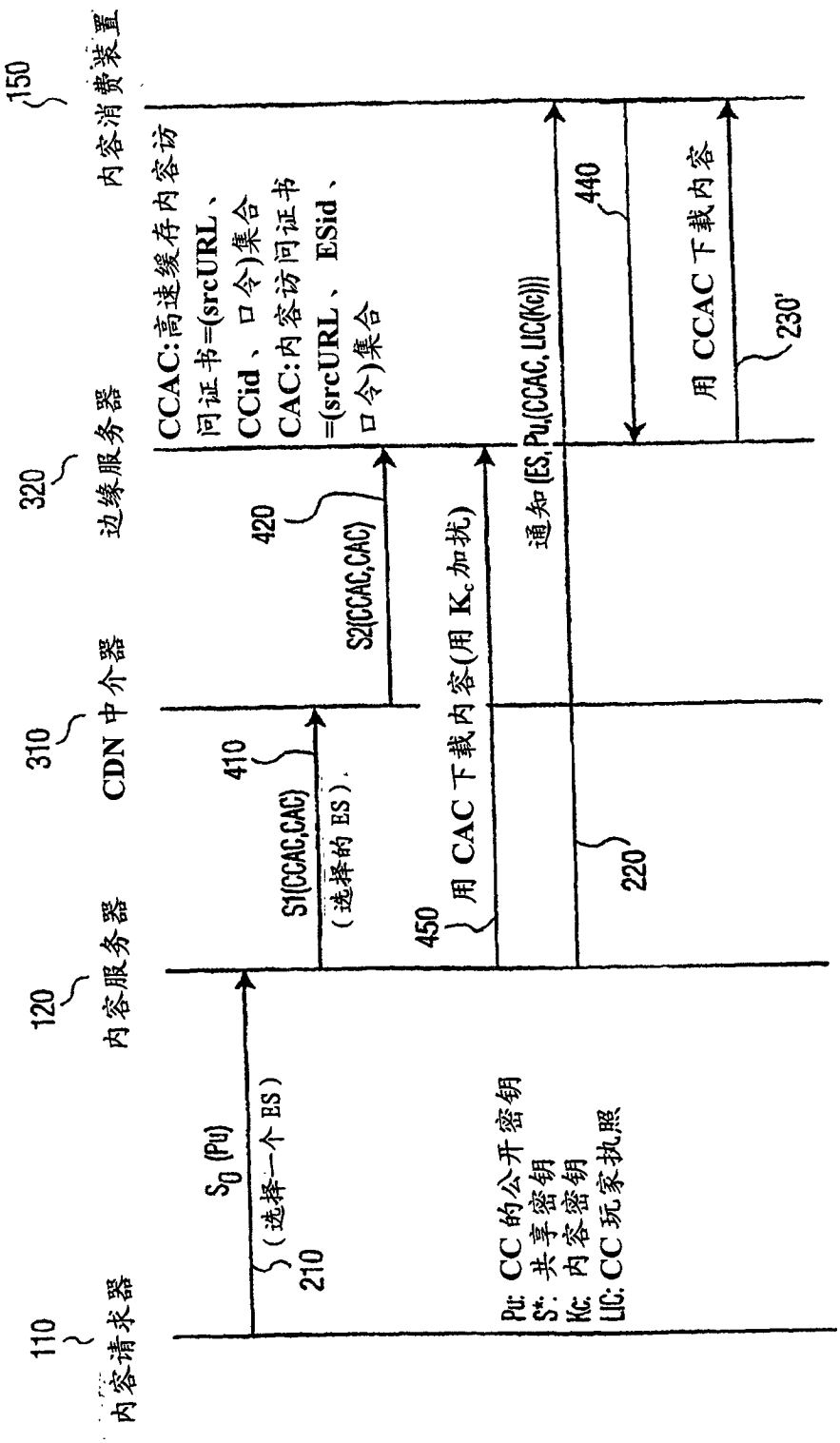

110
内容请求器
120
内容服务器
310
CDN 中介器
320
边缘服务器
150
内容消费装置
S_0 (Pu)
(选择一个 ES)
210
S1(CCAC,CAC)
(选择的 ES)
410
S2(CCAC,CAC)
420
CCAC:高速缓存内容访问证书=(srcURL、CCid、口令)集合
CAC:内容访问证书=(srcURL、ESid、口令)集合
450
用 CAC 下载内容(用 K_c 加扰)
通知 (ES, Pu_i(CCAC, LIC(K_c)))
220
440
用 CCAC 下载内容
230'
Pu: CC 的公开密钥
S*: 共享密钥
Kc: 内容密钥
LIC: CC 玩家执照

图 4

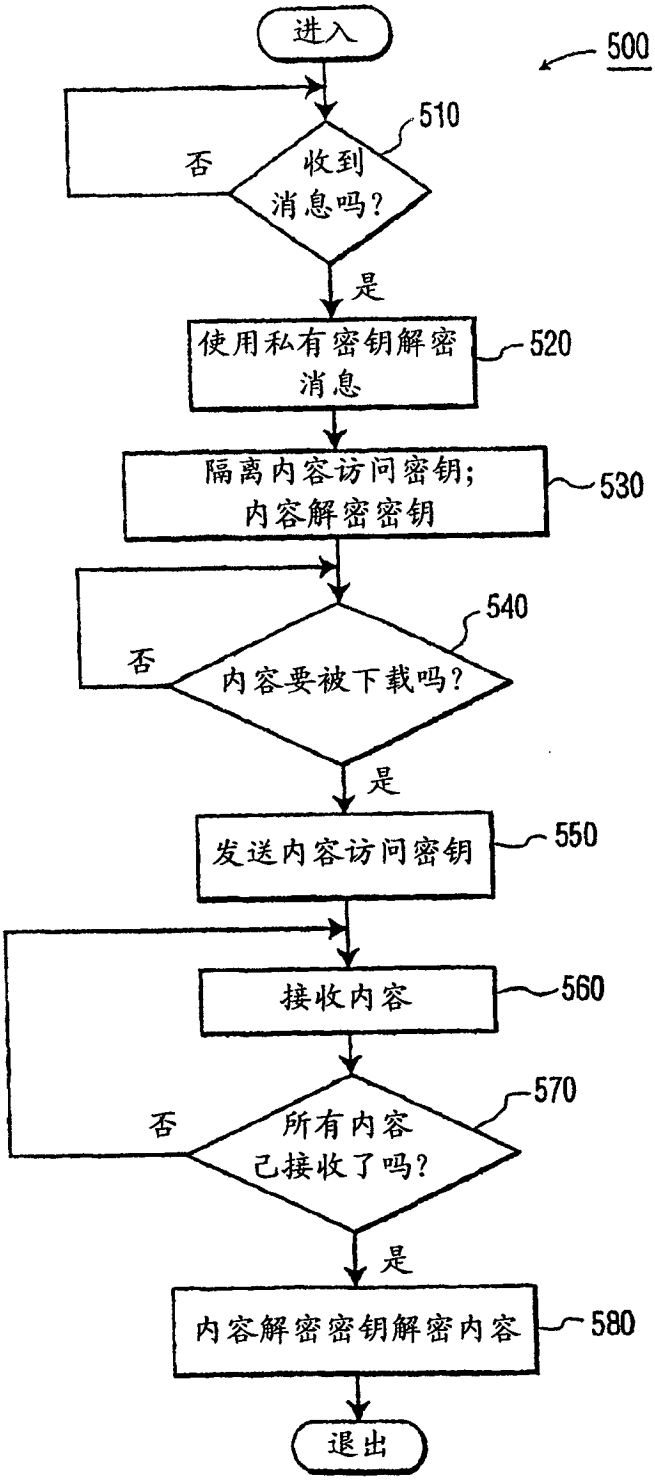

进入
500
510
否
收到
消息吗?
是
使用私有密钥解密
消息
520
隔离内容访问密钥;
内容解密密钥
530
540
否
内容要被下载吗?
是
发送内容访问密钥
550
接收内容
560
570
否
所有内容
已接收了吗?
是
内容解密密钥解密内容
580
退出

图 5

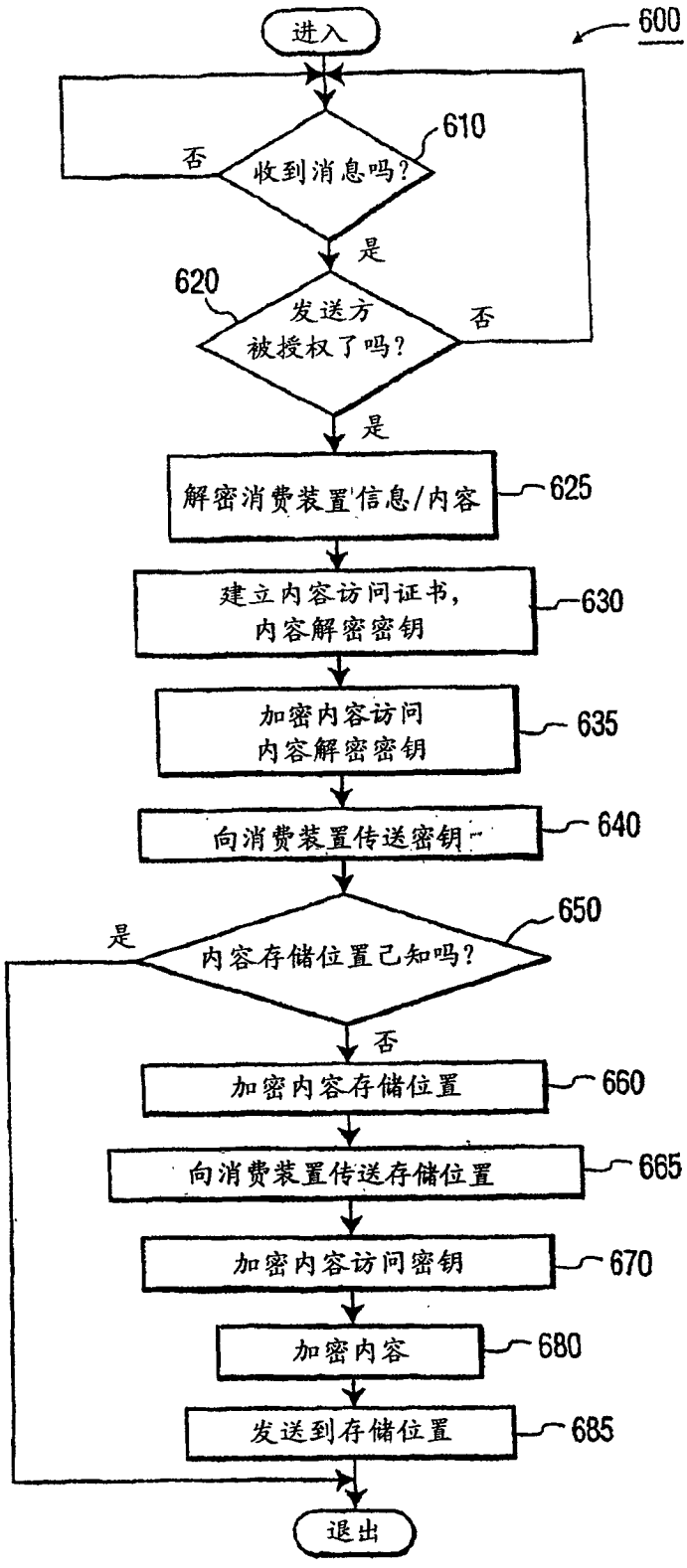

进入
600
610
收到消息吗?
否
是
620
发送方
被授权了吗?
否
是
解密消费装置信息/内容
625
建立内容访问证书,
内容解密密钥
630
加密内容访问
内容解密密钥
635
向消费装置传送密钥
640
650
内容存储位置已知吗?
是
否
加密内容存储位置
660
向消费装置传送存储位置
665
加密内容访问密钥
670
加密内容
680
发送到存储位置
685
退出

图 6

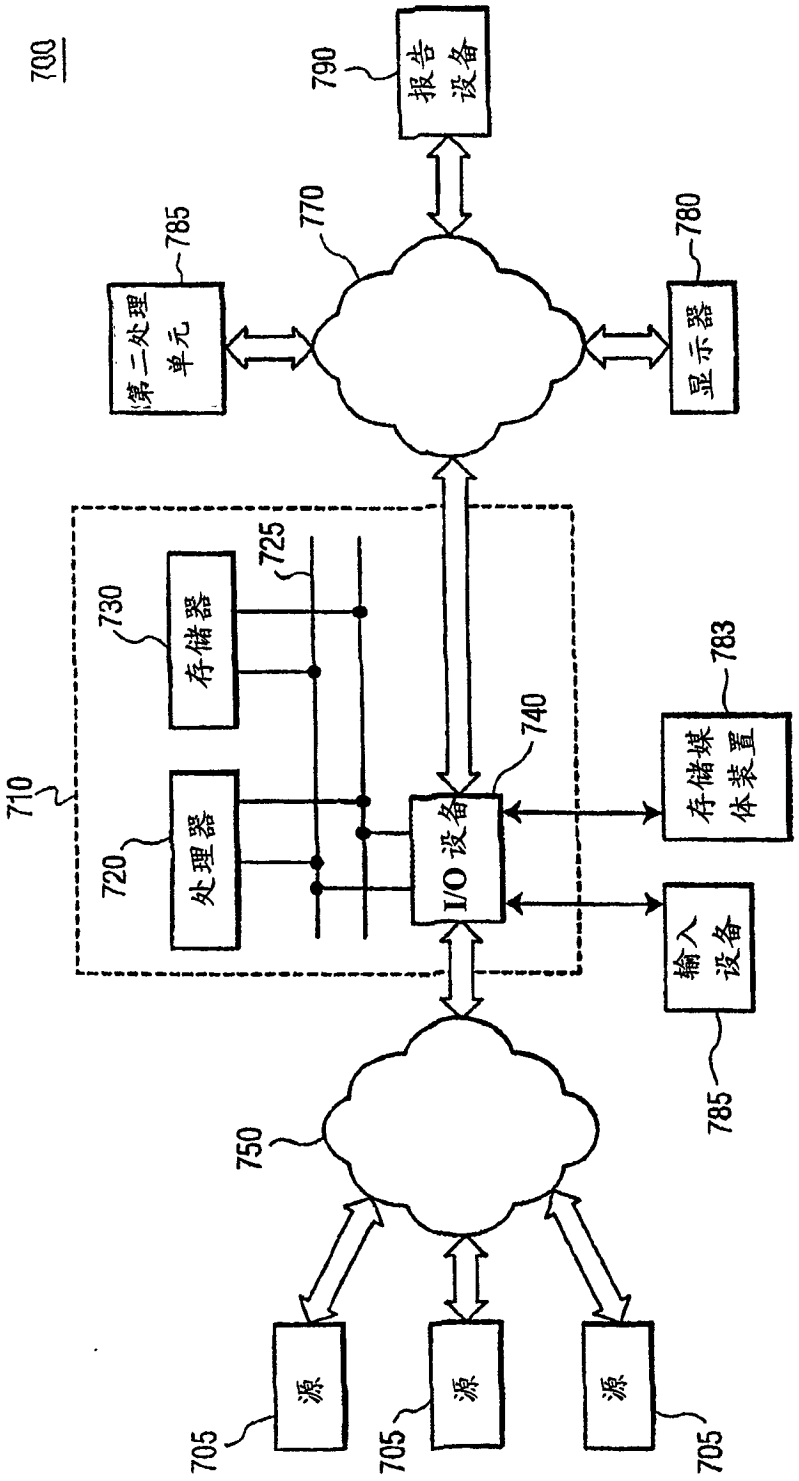

700
790
报告设备
770
785
第二处理单元
780
显示器
710
730
存储器
725
720
处理器
I/O 设备
740
783
存储媒体装置
输入设备
785
750
705
源
705
源
705
源

图 7