



(12) 发明专利

(10) 授权公告号 CN 101243431 B

(45) 授权公告日 2011. 03. 09

(21) 申请号 200680029348. 7

(51) Int. Cl.

(22) 申请日 2006. 08. 10

G06F 17/00 (2006. 01)

H04L 9/32 (2006. 01)

(30) 优先权数据

11/201, 751 2005. 08. 11 US

(56) 对比文件

CN 1498479 A, 2004. 05. 19,

(85) PCT申请进入国家阶段日

2008. 02. 13

审查员 姜玲玲

(86) PCT申请的申请数据

PCT/US2006/031185 2006. 08. 10

(87) PCT申请的公布数据

W02007/021830 EN 2007. 02. 22

(73) 专利权人 微软公司

地址 美国华盛顿州

(72) 发明人 A·E·克莱门次 J·M·阿尔科夫

S·巴哈特 E·P·奥莉维拉

A·帕卡

(74) 专利代理机构 上海专利商标事务所有限公

司 31100

代理人 陈斌

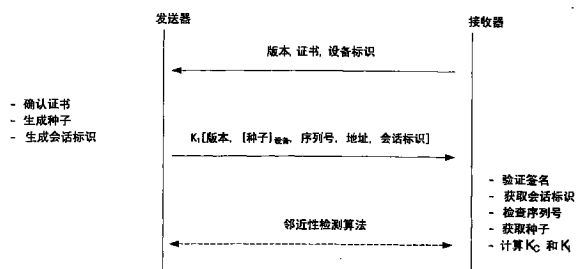
权利要求书 1 页 说明书 13 页 附图 11 页

(54) 发明名称

保护各种内容类型的数字媒体

(57) 摘要

描述了允许将数字权限管理策略与具有任意内容类型或传输控制协议的数字媒体相关联的系统 and / 或方法 (“工具”)。在某些实施例中,该工具解密媒体文件的数据段并向这些段中的每一段添加一描述符。这些描述符可允许加密的媒体文件的接收器解密该文件并根据正确的数字权限管理策略来消费该文件。



1. 一种用于客户机 - 服务器系统中的计算机实现的方法, 其中客户机具有公钥 / 私钥对, 服务器具有所述客户机的公钥, 所述方法包括:

所述服务器使用所述客户机的公钥来加密根内容密钥;

所述服务器将加密的根内容密钥发送到所述客户机;

所述服务器加密具有任意内容类型的媒体文件的各数据段以提供加密的数据段, 其中每个数据段是用由所述根内容密钥加密的相应的叶内容密钥加密的;

所述服务器向经加密的数据段添加描述符, 每一加密的数据段的描述符包括指示用于该加密的数据段的相关联数字权限管理策略的密钥 ID 以及用于确定用于解密该加密的数据段的叶内容密钥的初始化向量; 以及

所述服务器将加密的叶内容密钥发送到所述客户机。

2. 如权利要求 1 所述的方法, 其特征在于, 所述加密各数据段的动作使用计数器模式的 AES 来加密数据段, 其中每个数据段包括多个数据块, 所述 AES 基于数据段 ID 与相关联的数据段内的块数的 128 位串接以及叶内容密钥来为每个数据段生成密钥流。

3. 如权利要求 1 所述的方法, 其特征在于, 每一描述符具有同样在其相关联的数字权限管理策略内的密钥 ID。

4. 如权利要求 1 所述的方法, 其特征在于, 每一加密的数据段的描述符包括允许在该加密的数据段与其描述符之间进行区分的长度指示符。

5. 如权利要求 1 所述的方法, 其特征在于, 所述媒体文件包括第一部分和第二部分, 所述第一部分与第一数字权限管理策略相关联, 而所述第二部分与第二数字权限管理策略相关联, 并且其中, 所述添加动作将指示所述第一数字权限管理策略的第一描述符添加到所述第一部分中的加密的数据段, 并将指示所述第二数字权限管理策略的第二描述符添加到所述第二部分中的加密的数据段。

6. 如权利要求 1 所述的方法, 其特征在于, 所述加密的数据段包括符合 RTP 数据协议的分组或符合 HTTP 协议的帧。

7. 如权利要求 6 所述的方法, 其特征在于, 所述添加动作在所述加密的数据段包括符合 RTP 协议的分组时将所述描述符串接到所述加密的数据段的末尾, 或者在所述加密的数据段包括符合 HTTP 协议的帧时将所述描述符串接到所述加密的数据段的开头。

8. 一种用于客户机 - 服务器系统中的计算机实现的方法, 其中客户机具有公钥 / 私钥对, 服务器具有所述客户机的公钥, 所述方法包括:

在所述客户机, 接收加密的根内容密钥;

在所述客户机, 使用所述客户机的私钥来解密根内容密钥; 以及

在所述客户机, 使用所述根内容密钥来解密多个加密的叶内容密钥, 其中每个加密的叶内容密钥对应于具有任意内容类型的媒体文件的多个加密的数据段中的一个, 每一加密的数据段包括一描述符, 该描述符包括指示用于该加密的数据段的相关联数字权限管理策略的密钥 ID 以及用于确定用于解密该加密的数据段的叶内容密钥的初始化向量。

保护各种内容类型的数字媒体

[0001] 背景

[0002] 数字权限管理 (DRM) 指的是用于诸如通过控制或限制电子设备上对数字媒体内容的使用来保护内容的技术。DRM 的一个特征是它可将媒体内容绑定到给定机器或设备。由此, 涉及特定一段内容并定义了与该段内容相关联的权限和限制的许可证通常被绑定到给定的机器或设备。结果, 用户可能无法取得该段内容并将其移至另一机器来回放该内容。

[0003] 当前的 DRM 技术是有限制的。它们通常仅与用于传输数字媒体的两种类型的协议兼容 - HTTP 和 RTSP。但是其它协议现在或将来可能更适用于传输数字媒体。并且, 受 DRM 保护的内容可能限于一特定内容类型。一种特定内容类型 - ASF 文件 - 仅允许一组权限和限制, 即“策略”应用于整个 ASF 文件。例如, 当呈现视频文件时, 或者需要在对整个文件的模拟视频输出上启用宏视觉 (Macrovision), 或者完全不需要宏视觉。

[0004] 概述

[0005] 描述了允许数字权限管理策略与具有任意内容类型或传输控制协议的数字媒体相关联的系统和 / 或方法 (“工具”)。在某些实施例中, 该工具加密媒体文件的各数据段并将一描述符添加到这些段中的每一段。这些描述符可允许所加密的媒体文件的接收器解密该文件并根据正确的数字权限管理策略来消费该文件。

[0006] 提供本概述以用简化的形式介绍将在以下详细描述中进一步描述的一些概念。本概述并不旨在标识出所要求保护的主题的关键或必要特征, 也不旨在用于协助确定所要求保护的主题的范围。

[0007] 附图简述

[0008] 图 1 示出了在一个实施例中可使用本发明实施例的协议的示例性注册过程。

[0009] 图 2 示出了在一个实施例中可使用本发明实施例的协议的示例性邻近性检测过程。

[0010] 图 3 是在一个实施例中可使用本发明实施例的协议的示例性会话建立过程。

[0011] 图 4 示出了在一个实施例中可使用本发明实施例的协议的示例性数据传输过程。

[0012] 图 5 示出了根据一个实施例的可使用本发明实施例的流传送协议的各方面。

[0013] 图 6 示出了根据一个实施例的与根许可证和叶许可证相关联的各方面。

[0014] 图 7 示出了根据一个实施例的与根许可证和叶许可证相关联的各方面。

[0015] 图 8 示出了具有与五个不同示例性数字权限管理策略相关联的七个部分的示例性单个媒体文件。

[0016] 图 9 示出了具有与密钥 ID (KID) 相关联的示例性数据段的图 8 的单个媒体文件。

[0017] 图 10 示出了对于图 9 所示的数据段的根据一个实施例的分组。

[0018] 图 11 是示出该工具允许内容无关加密和解密的一种方式的流程图。

[0019] 图 12 示出了根据一个实施例的示例加密。

[0020] 图 13 是示出根据一个实施例的根和叶许可证的通信的流程图。

[0021] 详细描述

[0022] 概述

[0023] 描述了允许数字权限管理策略与具有任意内容类型或传输控制协议的数字媒体相关联的工具。在某些实施例中,该工具加密媒体文件的各数据段并将一描述符添加到这些段中的每一段。这些描述符可允许所加密的媒体文件的接收器解密该文件并根据正确的数字权限管理策略来消费该文件。

[0024] 在以下讨论中,提供了题为“内容安全和许可证传输协议”的小节,该节描述了其中可采用本发明技术的一个特定系统。在此之后,提供了题为“RTSP”和“HTTP”的小节,以向不熟悉这些协议的读者给出对这些空间中的本发明技术的理解。

[0025] 在该节之后,提供了题为“根和叶许可证”的小节,该节描述了对一媒体文件启用多个其它许可证的初始的根许可证的概念。在该节之后,提供了题为“具有多个叶许可证的单个加密的媒体文件”的小节,该节描述了如何可使用与一媒体文件的各部分相关联的叶许可证来将该媒体文件与一个以上数字权限管理策略相关联。

[0026] 在这些小节之后,两小节,即题为“描述符”的第一节和题为“内容无关数据加密”的第二节描述了用于媒体文件的各数据段的描述符以及该工具可使用这些描述符来允许与媒体文件的数字内容类型无关地加密媒体文件的方式。最后一节“使用根和叶许可证”描述了该工具可使用根和叶许可证的一种方式。

[0027] 内容安全和许可证传输协议

[0028] 以下提供了为在数字链路上流动的内容提供安全和传输许可证的示例性协议的讨论。该协议仅构成了可使用各种发明技术的一个示例性协议。可以理解和明白,可利用其它协议而不脱离所要求保护的的主题的精神和范围。

[0029] 在此描述中使用以下密码表示法:

[0030] $K\{\text{数据}\}$ 用机密密钥 K 加密的数据

[0031] $K[\text{数据}]$ 用机密密钥 K 签署的数据

[0032] $\{\text{数据}\}_{\text{设备}}$ 用设备的公钥加密的数据

[0033] $[\text{数据}]_{\text{设备}}$ 用设备的私钥签署的数据

[0034] 在该特定协议中,有五个主要过程:注册、重新确认、邻近性检测、会话建立和数据传输。

[0035] 在注册过程中,发送器(即,具有要发送到另一设备的内容的设备)可唯一并安全地标识-预期接收器(即,要向其发送内容的设备)。在该特定协议中,发送器维护具有注册的接收器的数据库,并且确保不会同时使用多于一较小的预定数目的接收器。在注册过程期间,发送器还采用了邻近性检测过程来确保接收器在网络中位于发送器“附近”,以防止受保护内容的大范围分发。

[0036] 重新确认过程用于确保接收器持续地在发送器的“附近”。除非接收器已在过去的一段预定时间内注册或重新确认,否则不向其传送内容。

[0037] 会话建立过程在接收器向发送器请求内容的任何时候使用。发送器强制设备必须在完成会话建立之前注册并最近被确认。

[0038] 一旦建立了会话,所请求内容的数据传输可用一安全的方式来进行。接收器可重复使用该会话来检索内容的特定部分(寻找),但是必须建立新的会话来检索不同的内容。

[0039] 现在结合图 1 以及下表来考虑注册过程,下表描述了在注册期间在发送器和接收器之间传递的各种消息。

[0040]

消息	值	描述
注册请求消息	版本	8 位协议版本
	证书	接收器的 XML 数字证书。
	设备标识	128 位序列号。
注册响应消息	版本	8 位协议版本
	{种子}设备	用于导出内容加密密钥和内容完整性密钥的 128 位种子。
	序列号	128 位序列号
	地址	发送器传入和传出的邻近分组套接字的地址。
	会话标识	128 位随机会话标识。
邻近性检测算法		在带外执行邻近性检测算法。

[0041] 此处,接收器发送除其它信息外还包含接收器的数字证书的注册请求消息。响应于接收该注册请求消息,发送器确认接收器的证书,生成种子和随机会话标识,在注册响应消息中按上述格式向接收器返回同样的内容。接收器然后确认发送器的签名,获取会话标识并执行附图中所示的其它动作。接收器和发送器然后可经历以下描述的邻近性检测过程。

[0042] 对于重新确认,执行与上述相同的过程,区别在于,在重新确认期间,接收器已在数据库中注册。

[0043] 对于邻近性检测,结合图 2 考虑以下。

[0044] 在邻近性检测过程期间,接收器向发送器发送包含邻近性检测初始化消息中指示的会话标识的消息。发送器然后向接收器发送包含现时值 (Nonce) (128 位随机值) 的消息,并测量接收器以使用内容加密密钥加密的现时值来答复所花的时间。最后,发送器向接收器发送指示邻近性检测成功与否的消息。

[0045] 接收器可重复该过程,直到它确认邻近性检测成功。当该特定协议在基于 IP 的网络上使用时,通过 UDP 来交换邻近性检测消息。接收器经由注册响应消息知道发送器的地址。接收器的地址不需要单独传送,因为可通过检查承载邻近性检测初始化消息的 UDP 分组的传入 IP 报头来确定。

[0046] 下表描述了在邻近性检测期间交换的消息:

[0047]

消息	值	描述
邻近性开始消息	会话标识	由发送器发送的同一 128 位会话标识值。
邻近性质询消息	序号	8 位递增序号。
	会话标识	同一 128 位会话标识。
	现时值	128 位随机值。
邻近性响应消息	序号	由发送器确定的同一序号。
	会话标识	同一 128 位会话标识。
	KC{现时值}	使用内容加密密钥加密的 128 位现时值。
邻近性结果消息	会话标识	同一 128 位会话标识。
	结果	指示注册过程成功还是失败的状态码。

[0048] 对于会话建立,结合图 3 和描述在会话建立期间交换的消息的下表考虑以下。

[0049]

消息	值	描述	
许可证请求消息	版本	8 位协议版本	
	证书	接收器的 XML 数字证书。	
	序列号	128 位序列号。	
	动作	请求的内容使用。例如：“播放”、“复制”或“刻录”。	
	权限标识	128 位随机权限标识。	
	CRL 版本	接收器 CRL 的版本。	
许可证响应消息	版本	8 位协议版本	
	CRL	发送器的 CRL。仅在发送器具有高于接收器的 CRL 的版本号且接收器组件也具有发送能力时才发送。	
	许可证	KC (用接收器的公钥加密)	128 位随机内容加密密钥。
		KI (用接收器的公钥加密)	128 位随机内容完整性密钥。
		CRL 版本	发送器的 CRL 版本
		权限标识	由接收器发送的同一 128 位随机权限标识。
	序列号		128 位序列号。

[0050] 在此示例中，从接收器向发送器发送许可证请求消息，它包含上述信息。作为响应，发送器可发送包含上述信息的许可证响应消息。

[0051] 在该特定示例中，用 XMR 格式表示许可证，许可证包括内容加密密钥、内容完整性密钥、发送器 CRL 的版本、128 位权限标识和 128 位序列号。许可证还包含使用 OMAC 用内容完整性密钥计算的 OMAC。

[0052] 对于数据传输过程，结合图 4 考虑以下。一旦会话建立完成，即以控制协议专用的方式执行数据传输。数据传输请求和响应两者必须为控制协议和内容类型特别定义。这概念性地表示在图 4 中。

[0053] 在提供了可用于本发明实施例的示例性协议的简要概述之后，现在考虑 RTSP 的一些背景信息。

[0054] RTSP

[0055] 如本领域的技术人员所理解的，实时流传送协议，即 RTSP 是用于对连续媒体（例如，具有如流传送等实时特性的数据）的传送进行控制的应用层协议。RTSP 提供允许对诸如音频和视频等实时数据进行受控的、按需的传送的可扩展框架。数据源可包括实况数据馈送和已存储的剪辑两者。该协议旨在控制多个数据传送会话，提供用于选择诸如 UDP、组播 UDP 和 TCP 等传送信道的手段，并提供用于基于 RTP 选择传送机制的手段。

[0056] RTSP 建立并控制单个或多个时间同步的连续媒体流,诸如音频和视频。它自己一般不传送连续流,然而连续媒体流与控制流的交织是可能的。换言之,RTSP 用作多媒体服务器的“网络遥控器”。

[0057] 要被控制的流的集合由演示描述来定义。在 RTSP 中,不存在 RTSP 连接的概念;相反,服务器维护由标识符标记的会话。RTSP 会话决不绑定至传输层连接,诸如 TCP 连接。在 RTSP 会话期间,RTSP 客户机可打开或关闭至服务器的众多可靠的传输连接以发出 RTSP 请求。或者,如本领域的技术人员可以理解的,可使用诸如 UDP 等无连接传输协议。

[0058] 由 RTSP 控制的流可使用 RTP,但 RTSP 的操作不依赖于用于承载连续媒体的传输机制。

[0059] 现在结合图 5 考虑客户机 / 接收器 500 与服务器 / 发送器 502 之间的典型的 RTSP 请求 / 响应交换。

[0060] 初步地,RTSP 请求 / 响应具有为简洁起见未作描述的报头。在 RTSP 中,客户机 / 接收器 500 一般发出被称为描述 (DESCRIBE) 的请求,它针对从服务器 502 检索由请求 URL 标识的演示或媒体对象的描述。服务器 502 用以会话描述协议 (SESSION DESCRIPTION PROTOCOL) (SDP) 表示的被请求资源的描述作出响应。描述响应 (SDP) 包含其所描述的资源的所有媒体初始化信息。

[0061] 接着,客户机 500 发送对指定要用于流传送媒体的传输机制的 URI 的设置 (SETUP) 请求。在图 5 的示例中,为音频和视频两者发送设置请求。客户机 500 还在设置请求中指示它将利用的传输参数。设置请求中的传输报头指定客户机可接受用于数据传输的传输参数。来自服务器 502 的响应 (RESPONSE) 包含由服务器所选的传输参数。服务器还响应于该设置请求生成会话标识符。

[0062] 此时,客户机可发出播放 (PLAY) 请求,它告知服务器以经由设置中指定的机制来开始发送数据。响应于接收播放请求,服务器可开始流传送内容,在此示例中,该内容为音频 / 视频内容。如本领域的技术人员可以理解的,在此示例中,流传送的内容使用 RTP 分组封装并通过 UDP 发送。

[0063] RTSP 协议具有感兴趣的其它方法,包括暂停 (PAUSE)、拆卸 (TEARDOWN)、获取参数 (GET_PARAMETER)、设置参数 (SET_PARAMETER)、重定向 (REDIRECT) 和记录 (RECORD)。关于 RTSP 的其它背景,读者应查询 1998 年 4 月的 RTSP RFC 中 Schulzrinne, H., Rao, A. 和 R. Lanphier 的“Real TimeStreaming Protocol (实时流传送协议) (RTSP)”, RFC 2326,可在 <http://www.ietf.org/rfc/rfc2326.txt> 获得。

[0064] 根和叶许可证

[0065] 在所示和描述的实施例中,采用了根许可证和叶许可证的概念。此处,根许可证用于设置内容密钥 (根内容密钥) 并将其安全地传送到客户机 / 接收器,使得客户机 / 接收器可解密随后传送的叶许可证。一旦根内容密钥被安全地传送到客户机 / 接收器,服务器 / 发送器可使用发送给客户机 / 接收器的根内容密钥来加密用于各叶许可证的内容密钥 (叶内容密钥)。使用根内容密钥,客户机可解密叶内容密钥和叶许可证中的相关联策略。每一叶许可证还具有能够将叶许可证与媒体内容的一部分相关联的唯一标识符。此处,该唯一标识符被称为密钥 ID 或 KID,并且对每一叶许可证被编号为 1 到 n (叶₁, 叶₂, ..., 叶 _{n}), KID_{叶 n} 。

[0066] 为提供关于可如何实现该特定方案的一个示例,结合图 6 考虑以下。在该特定示例中,图 6 的系统被配置成对公钥密码操作使用 1024 位 RSA 密钥,而对对称密码操作使用 128 位 AES 密钥。当然,这仅作为一个示例来提供,并不旨在限制所要求保护的主题的应用。

[0067] 在此示例中,客户机 / 接收器 600 具有公钥 / 私钥对 650,而服务器 / 发送器 602 具有客户机 / 接收器的公钥。在此示例中,客户机 / 接收器的公钥和私钥中的每一个都是 1024 位 RSA 密钥。使用客户机 / 接收器的公钥,服务器 / 发送器构建一包含用客户机 / 接收器的公钥加密的根内容密钥的根许可证。该根内容密钥是 128 位 AES 内容密钥。该根许可证然后被发送到客户机 / 接收器。在图 6 中,这被示为在客户机 / 接收器和服务器 - 发送器之间发生的第一通信,其中加密的根内容密钥被表示为 { 内容密钥_根 }_{客户机}。然而,可以理解,在所示的通信之前可发生其它通信。

[0068] 从服务器 / 发送器接收到加密的根内容密钥之后,客户机 / 接收器现在可使用其私钥来解密该内容密钥,并且可安全地储存解密的根内容密钥以供将来使用。

[0069] 此时,考虑发生了什么事情。服务器 / 发送器已向客户机 / 接收器安全地传送了现在可用作后续密码操作的基础的密钥。更具体地,现在考虑多个特定的策略可能涉及单个媒体文件中的多个特定的受 DRM 保护的内容段。在这一情况下,服务器 / 发送器可准备各自包含数字权限管理策略和特定的叶内容密钥的加密形式的多个叶许可证。在此示例中,每一叶内容密钥是使用根内容密钥来加密的 128 位 AES 内容密钥。由此,客户机 / 接收器所经历并导致的、与解密新的以及附加的叶内容密钥相关联的计算复杂度和开销相对于与 1024 位 RSA 密钥操作相关联的计算复杂度开销被降低,因为现在客户机 / 接收器只需使用 128 位的 AES 内容密钥 (即,根内容密钥) 来解密。

[0070] HTTP

[0071] 讨论了根和叶许可证的概念以及其各自可如何在上述上下文中采用之后,现在考虑可如何使用 HTTP 来传送根和叶许可证。

[0072] 当利用 HTTP 来承载受 DRM 保护的内容时,客户机向服务器 / 发送器发出两个请求。首先,客户机发出检索根许可证的提出 (POST) 请求。其次,客户机发出检索受 DRM 保护的内容的获取 (GET) 请求。在此示例中客户机发出请求,因为在 HTTP 中,服务器通常不能启动与客户机的通信。

[0073] 具体地,结合以下讨论考虑图 7。当客户机希望接收根许可证时,它向服务器发出提出请求。提出请求如上所述包含许可证请求消息。响应于接收到此通信,服务器用包含根许可证的许可证响应消息来响应,在至少一个实施例中,该根许可证用 XMR 来表达。接收到根许可证并相应地处理它之后,客户机向服务器发出要求受 DRM 保护的内容的获取请求。响应于获取请求,服务器用与一个或多个许可证响应消息交错的所请求内容的各段来回复。许可证响应消息各自包含涉及该受 DRM 保护的内容的一特定部分的叶许可证。可使用任何适当的机制或交错技术来形成服务器的回复。

[0074] 仅作为一个实现示例,在一个特定上下文中,考虑以下。

[0075] 在仅一个示例中,使用四字节的成帧报头来封装数据和控制块。成帧报头包含一字节的 ASCII 美元符号 (0×24),之后是一字节的块类型标识符,之后是两字节的封装数据的长度,以网络字节顺序来表示。

[0076]	部分	字段
	报头	8 位 ASCII 美元符号(0x24)
		8 位块类型
	数据长度	16 位封装数据长度

[0077] 控制块使用 ASCII ‘c’ 字符 (0×63) 作为其类型标识符。该块包含消息,通常是许可证响应消息。

[0078] 数据块使用 ASCII ‘d’ 字符 (0×63) 作为其类型标识符。该块包含数据段描述符,后面直接跟有媒体数据。

[0079] 数据段描述符可与加密的或明文的内容相关联。描述符中的已加密标志传达此信息。数据段描述符与所发送的文件的一部分相关联,对该部分,如果其被加密,则向其应用单个策略和内容加密密钥。换言之,内容加密密钥和策略不能在段内改变。

[0080] 根据一个实施例,一典型的具有链接加密的 HTTP 响应由以下块组成:

[0081] 1. 承载具有链许可证的许可证响应消息的控制块 [\$c]。

[0082] 2. 一个或多个数据块 [\$d]。

[0083] 在文件传输期间存在密钥或策略改变的情况下,则增加以下步骤:

[0084] 3. 承载具有新的链许可证的许可证响应消息的新控制块 [\$c]。

[0085] 4. 一个或多个数据块 [\$d]。

[0086] 注意,在多次密钥或策略改变的情况下,步骤 3 和 4 可发生多次。

[0087] 具有多个叶许可证的单个加密的媒体文件

[0088] 该工具允许单个加密的媒体文件具有与不同策略相关联的各部分。该单个加密的媒体文件可以是任意的内容类型(例如,ASF、MPEG、WAV 或其它文件),并且可使用各种控制协议来传输。

[0089] 在以下所示并描述的图 8 的实施例中,单个加密的媒体文件 800 具有七个部分 802、804、806、808、810、812 和 814。假定该媒体文件是关于音乐视频历史的媒体节目。第一部分是对音乐视频的介绍,第二部分是音乐视频,第三部分是广告,第四部分是另一音乐视频,第五部分是另一音乐视频,第六部分是另一广告,第七部分是该节目的结束。

[0090] 此处,媒体节目的创建者希望对各部分具有不同的权限。该创建者可能希望允许媒体节目的用户播放介绍和结束部分,并对其复制特定次数。该创建者可能不愿意将同一权限授予音乐视频;此处假定该节目的创建者不拥有这些音乐视频,因此它们服从不同的使用策略。该创建者也可能愿意使广告被免费使用—且因此它们可按用户喜欢的方式来复制、使用和播放。

[0091] 为支配对这些部分中的每一个的使用,每一部分与一策略相关联。此处,该策略在具有 KID 和内容密钥的叶许可证中。假定对该媒体节目接收一个根许可证和五个叶许可证。叶许可证在图 8 中的 816、818、820、822 和 824 处示出。每一叶许可证具有唯一 KID (KID₁、KID₂、KID₃、KID₄ 和 KID₅) 和唯一叶内容密钥(叶内容密钥₁、叶内容密钥₂、叶内容密钥₃、叶内容密钥₄ 和叶内容密钥₅)。每一叶许可证还包含允许或排除使用每一相关联部分的媒体的某些权限的策略(策略₁、策略₂、策略₃、策略₄ 和策略₅)。这些叶许可证用 XMR(可扩展媒体权限)来表达,然而也可使用其它语言。

[0092] 第一策略（叶许可证 #1 的策略）允许与其相关联的媒体被播放最多 10 次并被复制最多三次。因此，该策略允许该节目的介绍和结束部分被播放和复制特定的次数。

[0093] 第二策略允许与其相关联的媒体仅被播放一次并且不被复制。由此，该节目的第一音乐视频只能被播放一次。如果用户试图第二次播放整个节目，则将不播放该视频。

[0094] 第三策略允许与其相关联的媒体以所需的任何方式来使用。该策略本身可对此进行宣告 – 对相关媒体播放、复制或其它使用没有任何限制。然而，在某些实施例中，该媒体的各部分可改为明文（而非加密）的。此一示例在以下描述。在任一情况下，第一和第二广告两者都可用任何所需的方式来使用。

[0095] 第四策略允许与其相关联的媒体被播放用户想要播放的次数，但是不能被复制。由此，第二音乐视频可被播放但不可被复制。

[0096] 第五策略允许与其相关联的媒体被播放用户想要播放的次数并被复制，但是仅作为模拟文件。由此，第三音乐视频可被播放，并且仅以特定方式被复制。

[0097] 每一部分与许可证之间的关联在图 8 中用虚线示出。该工具可建立该关联的方式将在以下更详细描述。

[0098] 描述符

[0099] 该工具可将各策略与单个媒体文件的各部分相关联。继续所示并描述的图 8 的实施例，每一部分通过叶许可证与一策略相关联。为更好地解释如何建立该关联，更详细地示出了单个媒体文件 800 的一部分。

[0100] 图 9 示出了第四部分 808 被展开以示出该部分可与一策略相关联的方式的媒体文件 800。此处，媒体文件在各部分一般有序的情况下接收。在此示例中，接收根许可证，之后是第一叶许可证，之后是媒体文件的第一部分，之后是第二叶许可证，之后是第二部分，依此类推。此处，如上所述，在接收媒体文件的开头之前完全不接收叶许可证。因此，第一和第三叶许可证可在与其相关联的部分之前被再次发送（因此，第一叶许可证可在第一部分之前发送并在七部分之前被再次发送）。

[0101] 当对媒体文件的一部分要遵循一新的策略时，在与第四叶许可证相关联的该媒体部分之前发送一新的叶许可证（此处为第四叶许可证 822）。

[0102] 此处，该叶许可证作为控制块 902 的一部分来发送，之后是第四部分 808 的数据段 904-914。然而，在 RTSP 中，许可证在 SDP 描述符或通知（ANNOUNCE）消息中传送。该特定实施例着眼于对 HTTP 的使用，然而叶许可证和数据的使用及通信也可使用 RTSP，诸如在以上关于图 7 的描述中所阐明的。控制块包括图 8 和 9 的叶许可证 822。叶许可证具有叶内容密钥₄、策略₄和 KID₄。一旦接收到，可使用根内容密钥来解密第四叶许可证。KID 可用明文来发送，或加密地发送但能够被解密。

[0103] 每一数据段与一策略相关联，此处数据段 904-914 与相应的第四策略相关联。该关联是用第四叶许可证的 KID 来建立的。KID 或与该 KID 相关联的标识符被储存在每一数据段中。KID 可以是相对较短的一段信息，甚至是占少于一字节的存储器的整数。因此，接收器可基于指示适当策略的 KID 将数据段与适当的策略相关联。

[0104] 描述符可与现在存在或将来创建的各种控制和数据协议以及分组结构一起使用。一个这样的示例性数据协议是 RTP。此处，描述符定向地追加到每一分组的末尾。在另一实施例中，使用 HTTP 控制协议。此处描述符定向地追加到每一帧的开头。

[0105] 图 10 示出了根据 RTSP 将数据段与叶许可证相关联的描述符。

[0106] 在该示例中,数据段 1000 可包括 RTP 有效载荷格式报头 1008 和有效载荷数据 1010。此处,有效载荷数据和有效载荷格式报头被加密,其一个示例作为以下图 11 的一部分来描述。

[0107] 此处,该描述符根据 RTP 协议被追加到有效载荷数据的末尾,然而它可被放置在数据协议所允许的任何适当的位置。如本领域的技术人员所理解的,将描述符放在有效载荷数据的末尾可减轻后向兼容性问题。

[0108] 在本实施例中,RTP 分组 -RTP 报头除外 - 与描述符 1012 相关联。描述符 1012 又随其承载了可在允许解密有效载荷数据 1010 和 RTP 有效载荷格式报头 1008 的解密过程中使用的加密参数(例如,与第四叶内容密钥相关联的初始化向量(IV))。在此特定示例中,单个策略和内容加密密钥应用于有效载荷数据 1010。根据一个实施例,描述符 1012 包括如下数据结构:

[0109]	部分		字段
	标志		8 位标志
	扩展		8 位数字的扩展
			多个可变长度扩展
	长度		数据段描述符长度

[0110] 在此示例中,标志部分是指示数据段的属性的位字段。当前定义了以下位:位 0(加密的数据)。当该位被设为 1 时,它指示该数据段是加密形式的。否则,该数据段是明文。

[0111] 扩展部分包括 KID 和 IV;此处 KID 是 KID₄,而 IV 与叶内容密钥₄相关联。

[0112] 关于扩展部分,扩展字段的数字指示包括在该描述符中的可变长度扩展的数目。关于可变长度扩展字段,每一扩展具有以下格式:

[0113]	字段	
		8 位扩展类型
		16 位扩展长度
		可变长度扩展

[0114] 根据一个实施例,KID 和 IV 被定义如下:

[0115] KID

[0116] 扩展类型:对密钥 ID 扩展必须被设为 1。

[0117] 扩展长度:必须被设为 16,表示 128 位(16 字节)。

[0118] 扩展:必须包含用于结合该描述符传送的加密媒体的密钥 ID 值。该扩展仅在加密数据标志被设为 1 时使用。

[0119] 初始化向量(IV)

[0120] 扩展类型:对初始化向量扩展必须被设为 2。

[0121] 扩展长度:必须被设为 8,表示 64 位(8 字节)。

[0122] 扩展:必须包含用于结合该描述符传送的加密媒体的初始化向量。该扩展仅在加密数据标志被设为 1 时使用。

[0123] 关于长度部分,在此实施例中,该部分必须包含以字节表示的描述符的总长度。该长度不包括结合该描述符传送的媒体数据的大小。

[0124] 内容无关数据加密

[0125] 图 11 是描述根据一个实施例的方法中的各步骤的流程图。该方法可结合任何适当的硬件、软件、固件或其组合来执行。在一个实施例中,该方法和结合诸如以上示出并描述的系统来实现。另外,在以下讨论中,所执行的动作中的某一些被描述为由服务器/发送器执行,而其它动作被描述为由客户机/接收器执行。服务器/发送器和客户机/接收器的示例在上文中提供。

[0126] 步骤 1102 接收媒体文件。该媒体文件可具有允许该媒体文件被分成数据段、加密、发送、接收和解密的任何内容类型。例如,它可以是 ASF、MPEG2 TS、MPEG2 ES 或 WAV 文件。

[0127] 步骤 1104 将该媒体文件划分成数据段。这些数据段可包括符合诸如 RTP 或 HTTP 等各种控制协议的分组、其它数据片段或帧。

[0128] 步骤 1106 加密每一数据段。步骤 1106 可根据此处所描述的任一实施例来完成该加密。由此,它可用叶内容密钥来加密有效载荷数据,并用根内容密钥来加密该叶内容密钥。采用根内容密钥,接收器稍后可解密该叶内容密钥并使用该叶内容密钥来解密有效载荷数据。

[0129] 在一个实施例中,步骤 1106 使用计数器(Counter)模式的 AES 来加密每一数据段或其部分。图 12 示出了用于使用该技术来加密单个数据段的过程。在此实施例中,计数器模式创建一字节流,该字节流然后与数据段的明文字节进行异或以创建加密的数据段。密钥流生成器使用 AES 轮(round)来一次生成 16 字节的密钥流块。对 AES 轮的输入是内容加密密钥(K_c) (例如,叶内容密钥)和数据段 ID 与该数据段内的块数的 128 位串接。

[0130] 密钥流生成器的输出应是来自数据段的相应块(i)的数据的逐字节异或。在数据段不能被 16 字节平均划分的情况下,仅来自最后一个块的媒体数据的有效字节应与该密钥流异或并为加密的数据段保留。

[0131] 步骤 1108 向每一加密的数据段添加描述符。描述符可包括 KID、IV 或此处所述的其它元素。每一描述符指示可用于支配数据段的有效载荷数据的相关联数字权限管理策略。根据上述一个实施例,该数字全选管理策略被包含在先前接收的叶许可证中。每一描述符还可指示可用于解密数据段的内容密钥(例如,特定叶内容密钥)。

[0132] 注意,这些步骤的结果可以是被划分成数据段的任意内容类型的媒体文件,每一数据段被加密并具有可用于稍后将加密的数据与数字权限管理策略相关联的描述符。

[0133] 在一个实施例中,该描述符包含长度指示符。有了该长度指示符,加密的数据段的接收器可确定描述符何时结束或开始。该长度指示符允许在数据段或其分组内的各个位置将描述符添加到加密的数据段。对于 RTP 协议,例如,该描述符被添加到具有数据段的 RTP 分组的末尾。对于 HTTP 协议,例如,该描述符被添加到具有数据段的帧的开头。注意,通过

具有可辨别的长度,描述符可被添加到数据段的各个部分并且因此允许将描述符用于各种传输协议。

[0134] 步骤 1110 将具有描述符的加密的数据段(以及明文数据段,如果有的话)发送到接收器。允许接收器以本领域中已知的方式来定向(例如,以正确的顺序放置)数据段。接收器可使用与数据段相关联的内容密钥来解密数据段。此外,接收器使用该描述符可确定对媒体文件或其一部分应使用什么权限策略。如果媒体文件具有应受不同权限策略支配的部分,则该方法还可在步骤 1104 中基于媒体文件的部分来划分数据段并向不同部分的数据段分配不同的描述符。

[0135] 步骤 1112 接收并解密加密的数据段。接收器(诸如客户机/接收器 500 或 600)解密数据段并基于其描述符向其分配适当的权限策略。在一个实施例中,接收器使用描述符中的初始化向量来解密数据段。接收器基于 KID 来确定适当的叶内容密钥,然后在用根内容密钥解密了叶内容密钥之后用其来解密数据段。

[0136] 步骤 1114 将每一数据段与一权限策略相关联。在一个实施例中,接收器使用描述符以及具有权限策略的叶许可证中找到的密钥 ID(KID)来完成这一关联。

[0137] 使用根和叶许可证

[0138] 图 13 是描述根据一个实施例的方法中的各步骤的流程图。该方法可结合任何适当的硬件、软件、固件或其组合来执行。在一个实施例中,该方法可结合诸如以上示出并描述的那些系统来实现。另外,在以下讨论中,所执行的动作中的某一些被描述为由服务器/发送器来执行,而其它动作被描述为由客户机/接收器来执行。服务器/发送器和客户机/接收器的示例在上文中提供。

[0139] 步骤 1300 使用客户机/接收器的公钥来加密根内容密钥。可利用任何适当的内容密钥,以上仅给出了其一个示例。步骤 1302 将包含加密的根内容密钥的根许可证发送给客户机/接收器。可利用任何适当的方法来实现此步骤。在以下讨论中,提供了利用两种不同协议的两个具体示例。可以理解和明白,这些仅构成示例,且并不旨在将所要求保护的主题的应用仅限于所描述的特定协议。

[0140] 步骤 1304 接收服务器/发送器发送的根许可证,且步骤 1306 解密该加密的根内容密钥。在此示例中,该步骤通过使用客户机/接收器的私钥解密该加密的根内容密钥来执行。

[0141] 步骤 1308 准备叶许可证,并用根内容密钥来加密叶内容密钥。步骤 1310 将叶许可证发送给客户机/接收器。可以回想,叶许可证可以且通常的确包含用于受 DRM 保护的内容的策略。应当理解和明白,步骤 1308 和 1310 可以对给定的一段受 DRM 保护的内容执行多次。即,对于具有不同策略的每一部分,可准备相应的叶许可证并将其发送给客户机/接收器。

[0142] 步骤 1312 接收叶许可证,且步骤 1314 使用先前接收到的根内容密钥来解密叶内容密钥。步骤 1316 然后使用解密的叶内容密钥来解密内容。它还使用上述描述符将适当的叶许可证与媒体文件的一部分(如果该媒体文件具有多个部分)相关联。

[0143] 可以理解和明白,步骤 1312、1314 和 1316 可对客户机/接收器接收到的每一新的叶许可证执行。

[0144] 结论

[0145] 本文描述了可用于将数字权限管理策略与具有任意内容类型或传输控制协议的数字媒体相关联的技术。在某些情况下,这允许加密的媒体文件的接收器解密该文件并根据不同的数字权限管理策略来消费该文件的各部分。在某些情况下,这还允许发送器用一组技术来加密许多不同类型的媒体文件。尽管用结构特征和 / 或方法步骤专用的语言描述了本发明,但可以理解,所附权利要求书中定义的本发明不必限于所述的特定特征或步骤。相反,这些特定特征和步骤是作为实现所要求保护的本发明的优选形式而公开的。

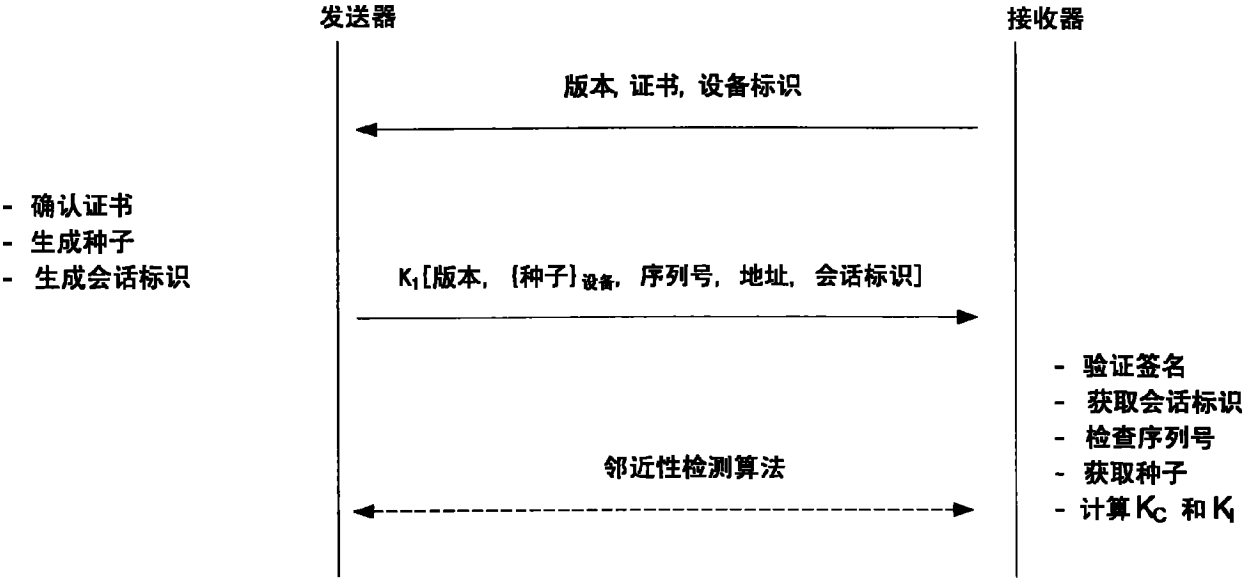


图 1

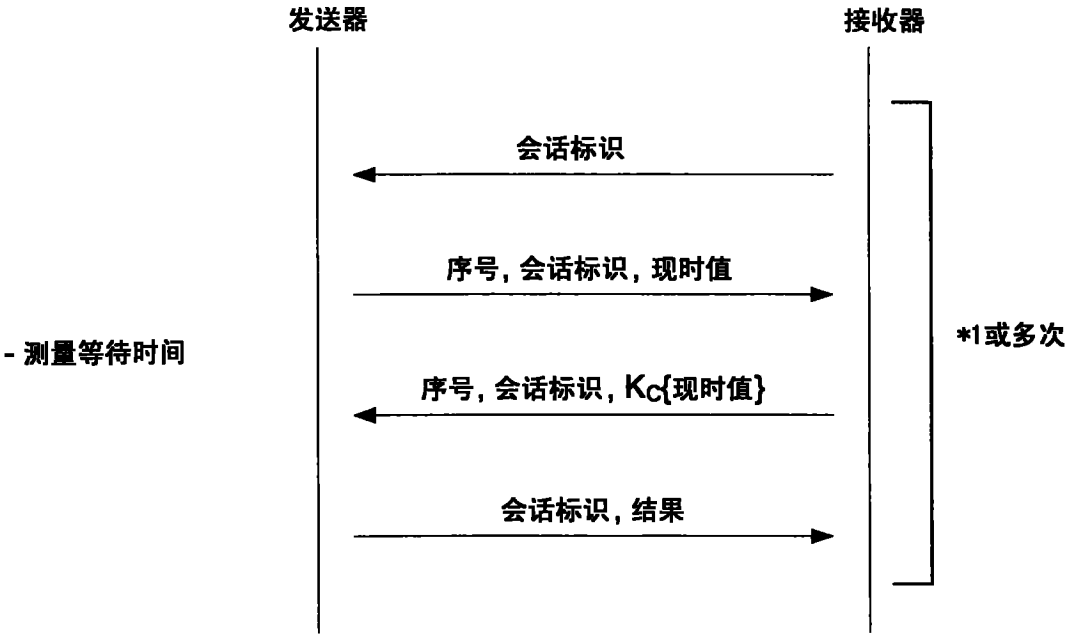


图 2

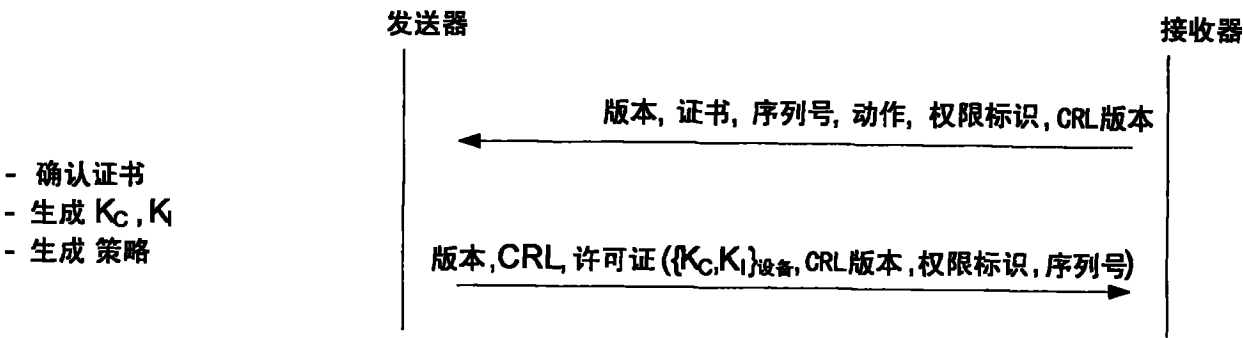


图 3

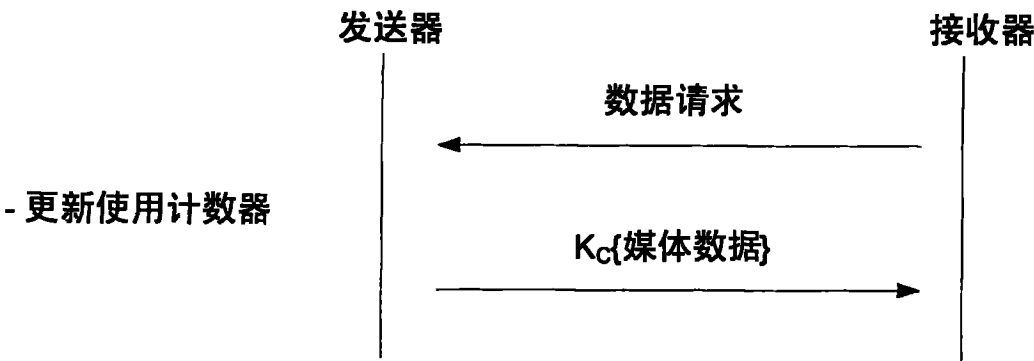


图 4

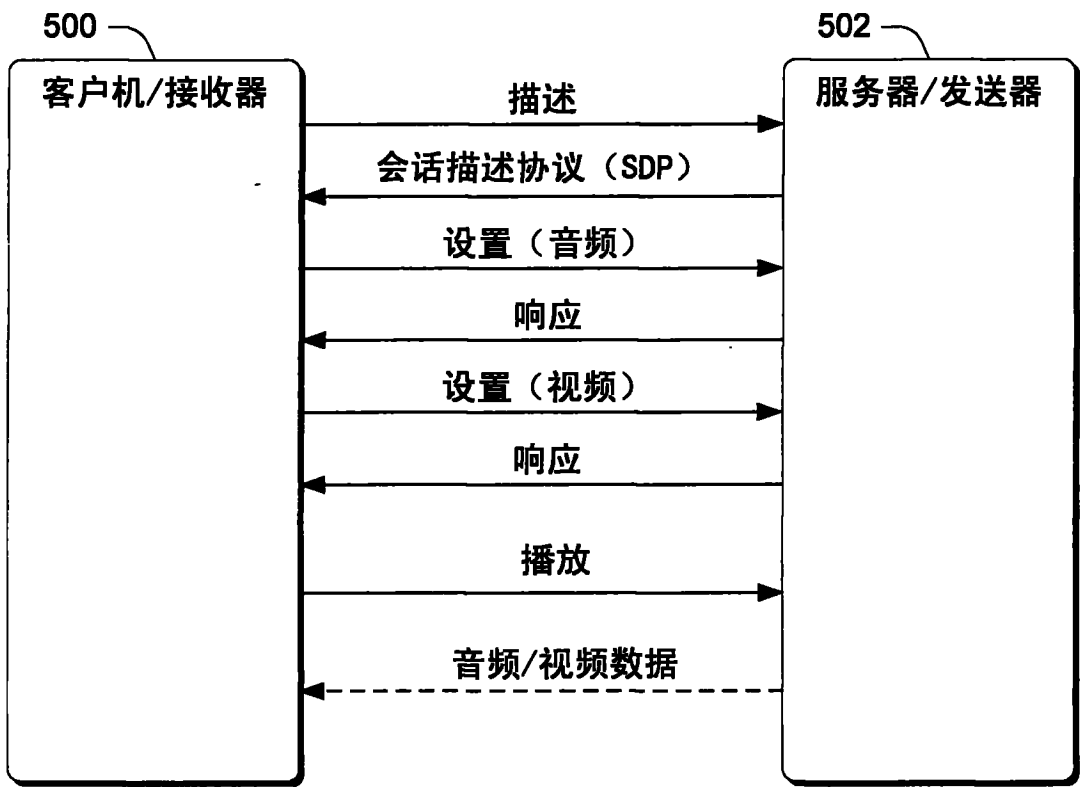


图 5

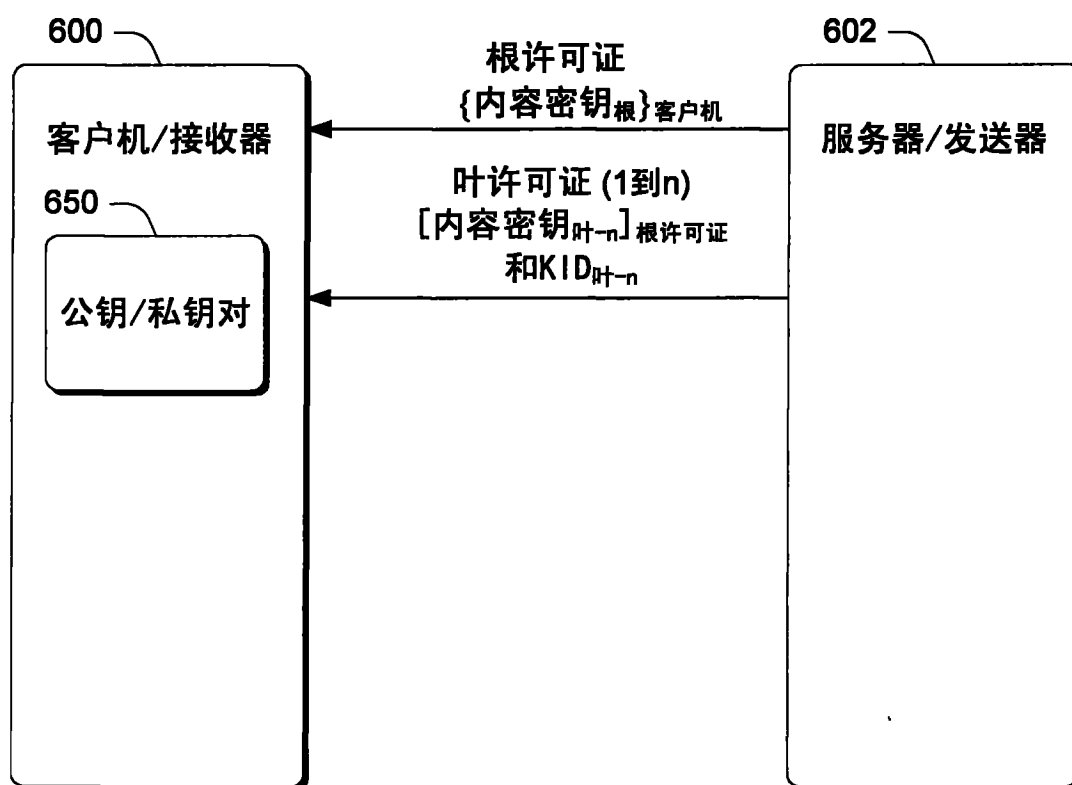


图 6

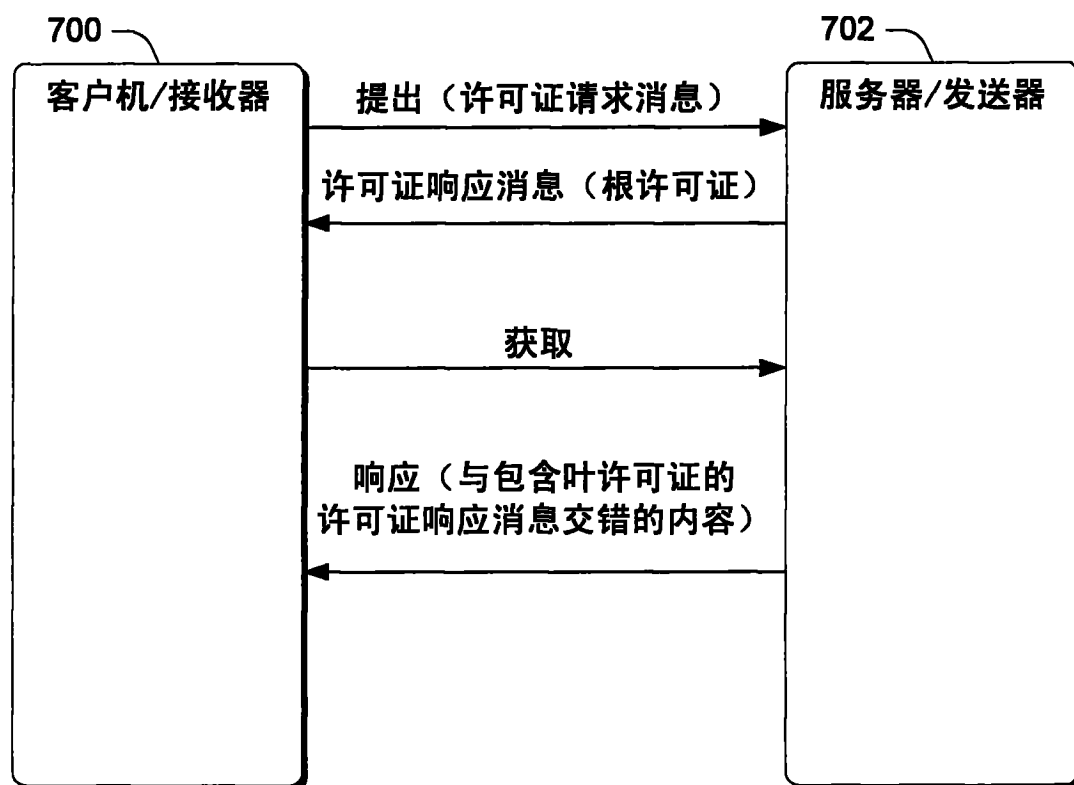


图 7

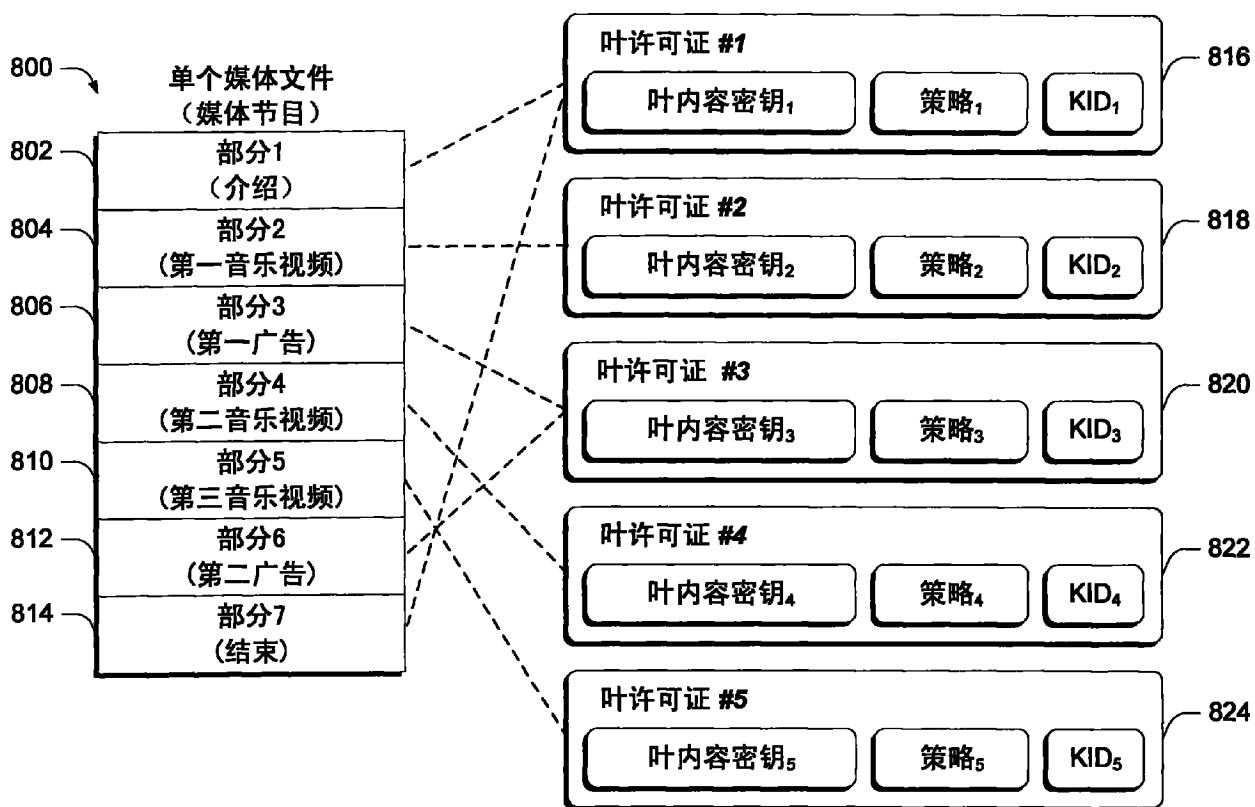


图 8

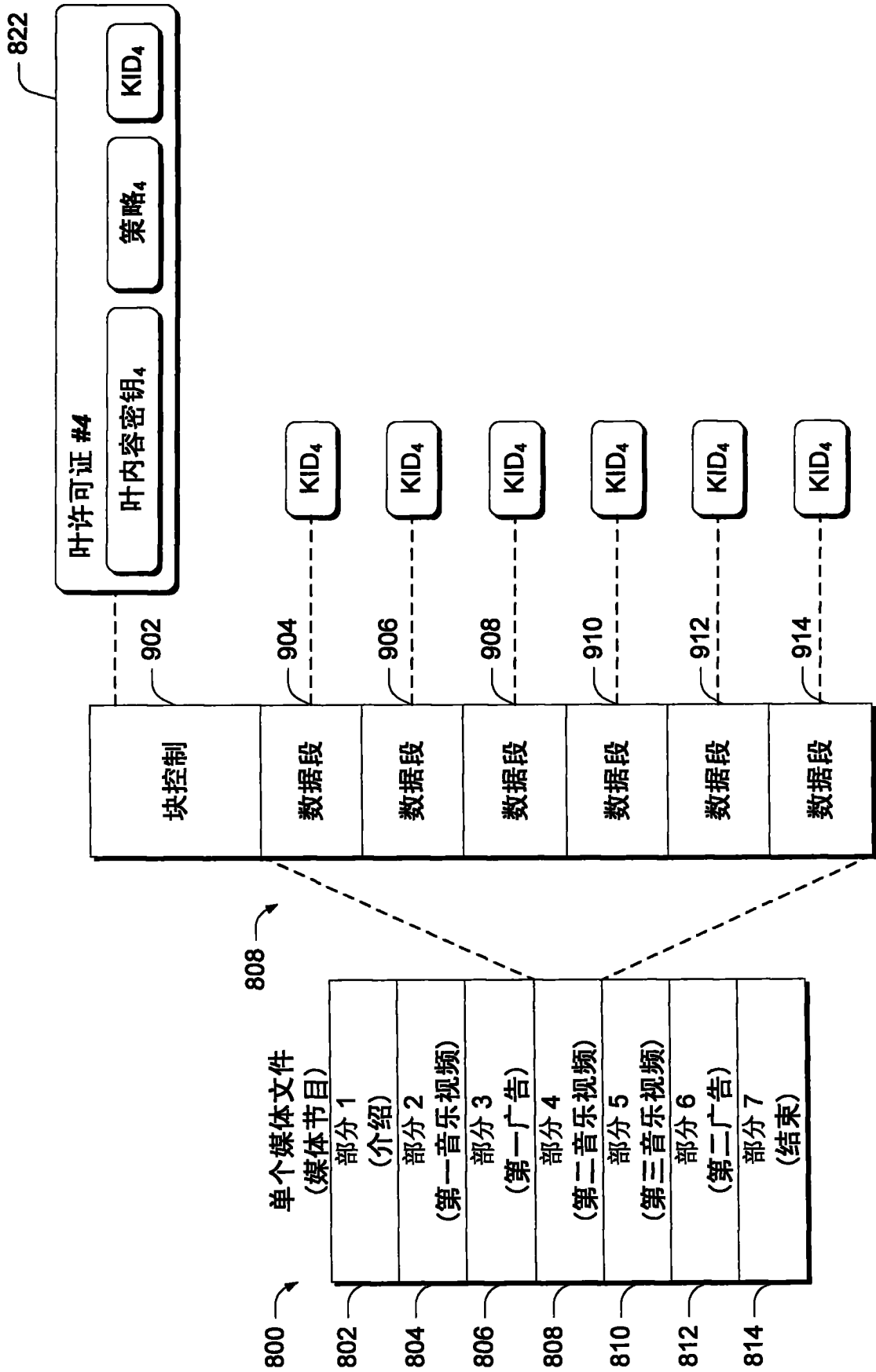


图 9

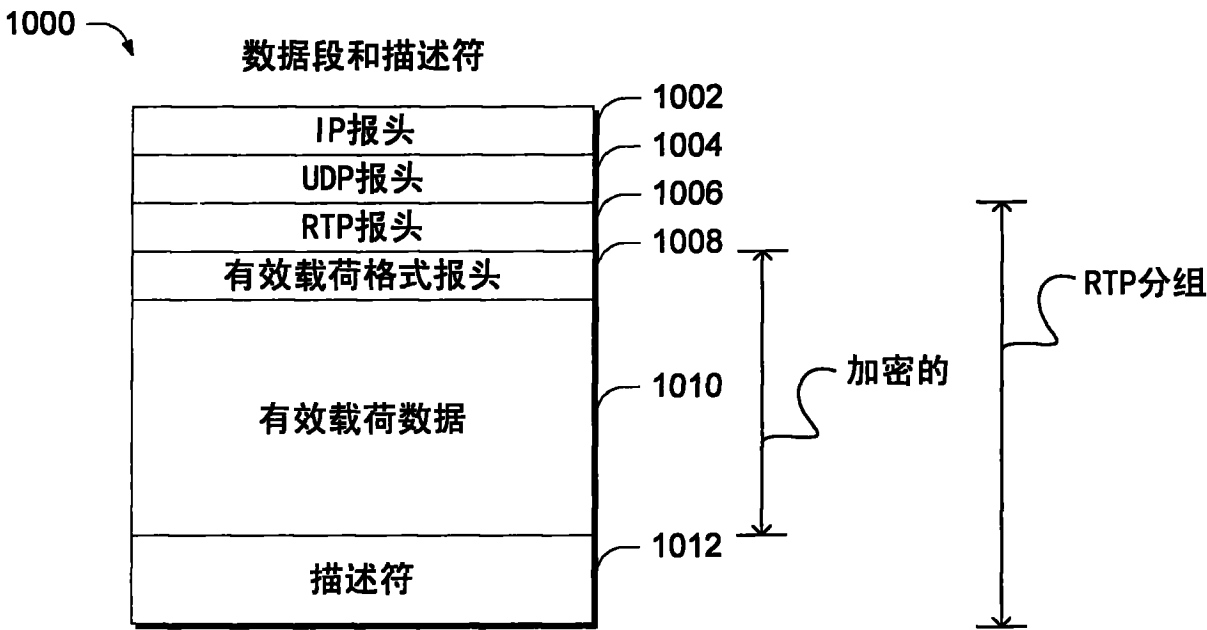


图 10

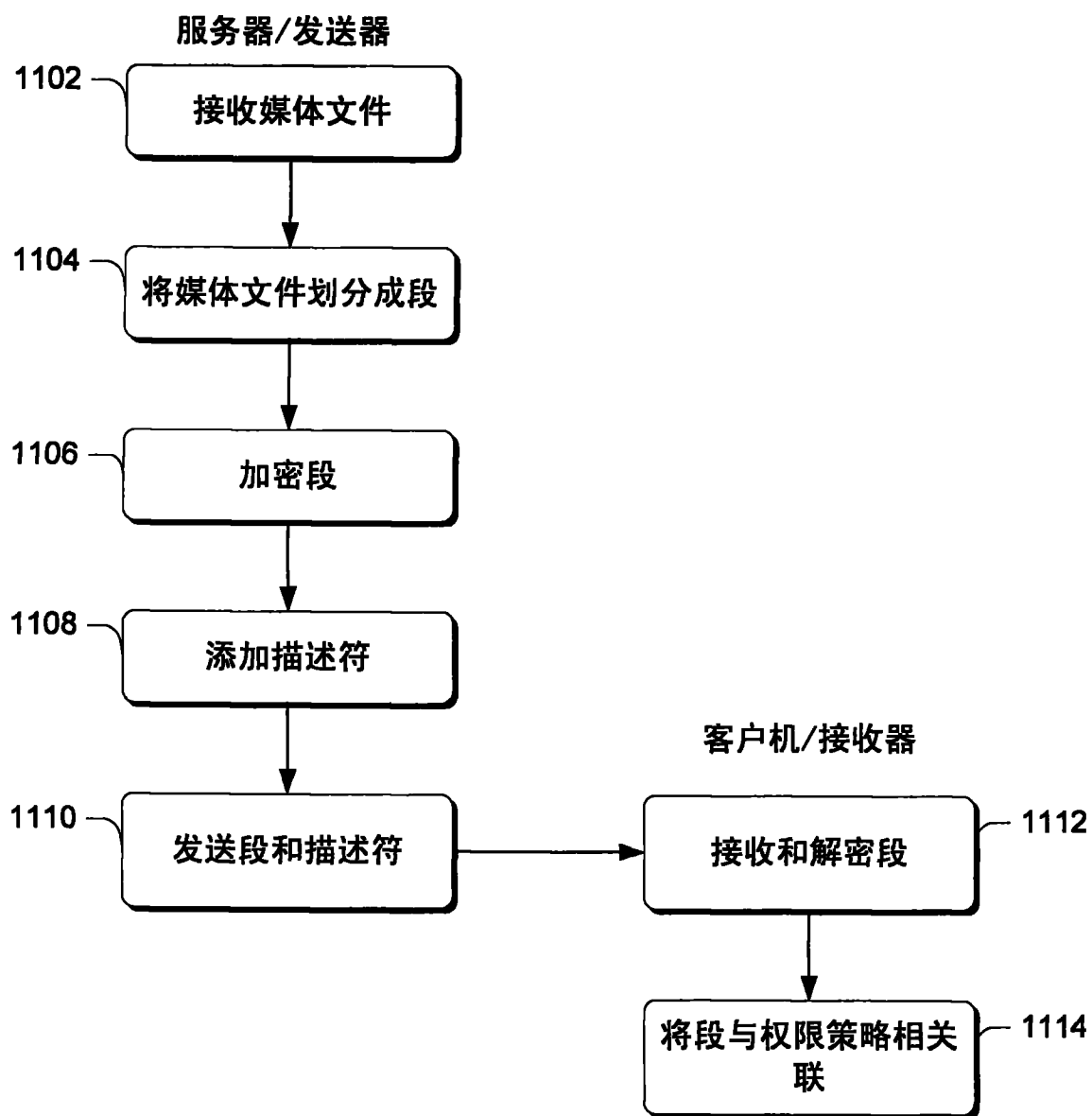


图 11

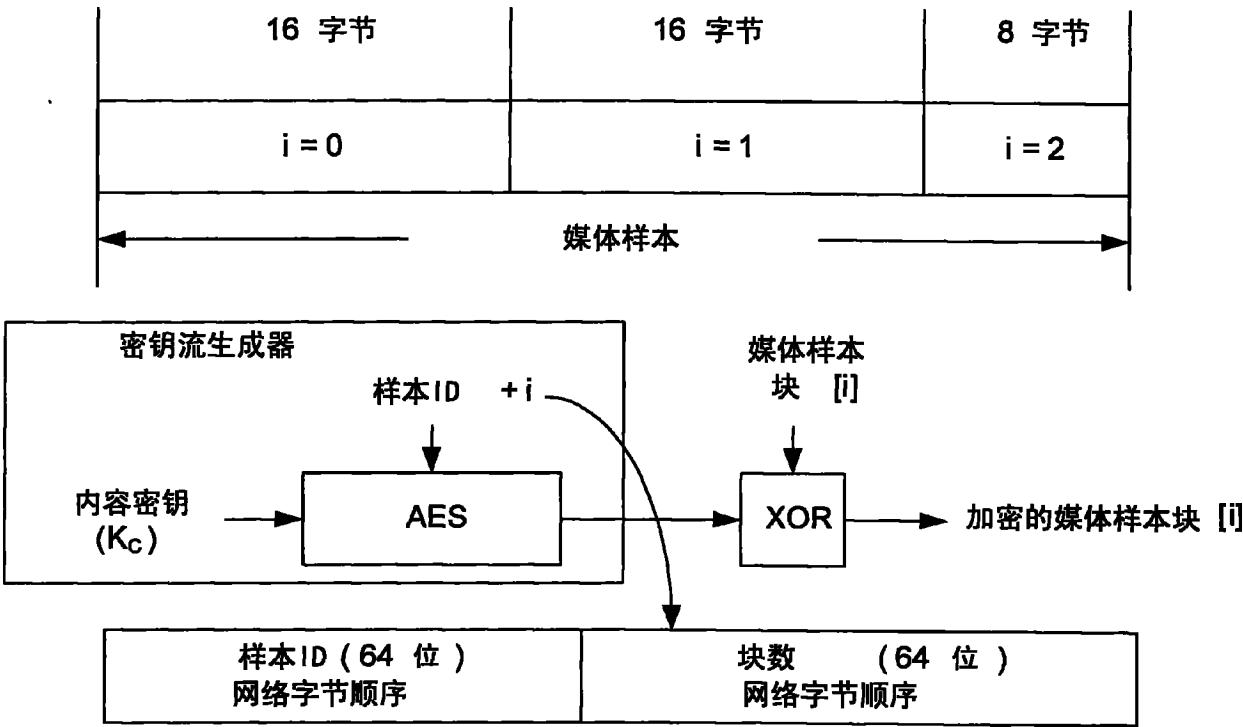


图 12

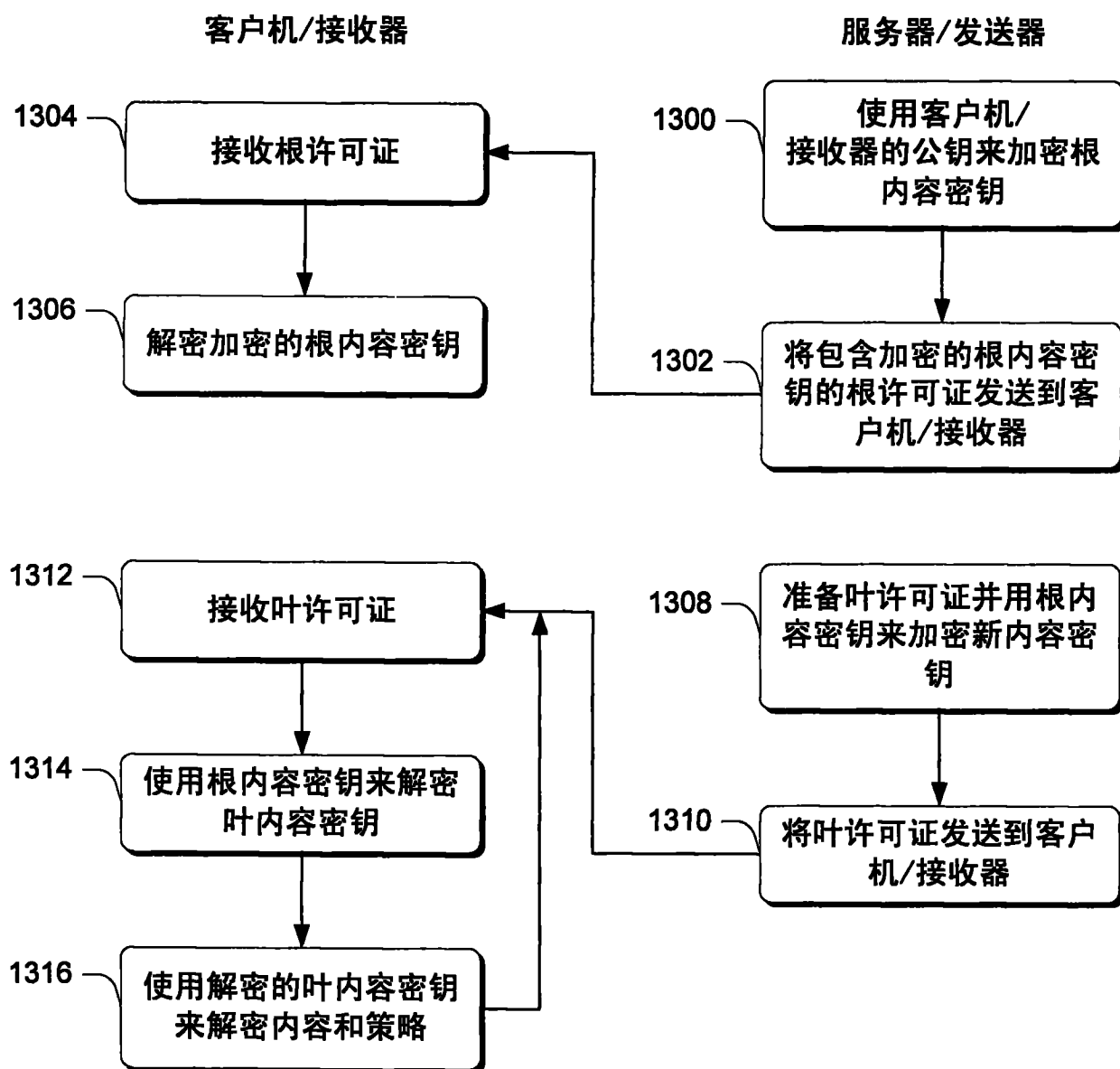


图 13