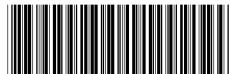


(19) 中华人民共和国国家知识产权局



(12) 发明专利申请

(10) 申请公布号 CN 103366102 A

(43) 申请公布日 2013. 10. 23

(21) 申请号 201310123521. 1

H04L 9/14 (2006. 01)

(22) 申请日 2013. 04. 10

(30) 优先权数据

61/622, 312 2012. 04. 10 US

61/636, 460 2012. 04. 20 US

13/460, 805 2012. 04. 30 US

(71) 申请人 西部数据技术公司

地址 美国加利福尼亚州

(72) 发明人 D · L · 必兰肯比克尔 D · 伊巴拉

L · 和森林克

(74) 专利代理机构 北京纪凯知识产权代理有限

公司 11245

代理人 赵蓉民 李英

(51) Int. Cl.

G06F 21/10 (2013. 01)

权利要求书2页 说明书18页 附图14页

(54) 发明名称

用于内容传输和分配的数字版权管理系统

(57) 摘要

本发明涉及一种针对可下载并从一个存储器安全传输到另一个存储器的内容的数字版权管理(DRM)。存储器可为磁盘驱动器，或网络连接式存储器。存储器执行加密操作并提供信任根。DRM系统使得内容能够安全拷贝或内容从一个存储装置到另一个存储装置的传输。在这个实施例中，由两个存储装置认证和信任的受信任服务器代理内容的传输。受信任的服务器可为DRM系统的单独实体，或DRM系统的现有服务器的组件或功能。在另一个实施例中，存储装置可以以对等的方式传输内容。可基于关联内容的数字证书授权和控制内容的传输。

1. 一种第一存储装置，其配置用于提供内容至表现所述内容的播放器系统，其中所述内容已由受信任的服务器从第二存储装置传输，所述第一存储装置包括：

存储介质，其包括所述播放器系统可访问的用户区域和所述播放器系统无法访问的非用户区域；以及

控制器，其包括提供硬件信任根和受保护存储器的加密模块，其中所述控制器配置用于认证所述播放器系统，基于所述认证建立与所述播放器系统的受保护通信信道，向所述播放器系统提供第一加密密钥，其中所述第一加密密钥是所述第二存储装置特有的并且基于由所述第二存储装置隐藏的密钥，向所述播放器系统提供关联所述内容的第二加密密钥，和从所述存储介质的用户区域向所述播放器系统提供加密形式的所述内容，其中基于所述第一加密密钥和所述第二加密密钥的加密组合，所述内容是可访问的。

2. 根据权利要求 1 所述的第一存储装置，其中所述控制器经配置基于公钥基础设施认证所述播放器系统。

3. 根据权利要求 1 所述的第一存储装置，其中所述加密模块经配置加密所述第一加密密钥，所述第一加密密钥基于由所述加密模块隐藏的密钥，是所述第二存储装置特有的。

4. 根据权利要求 1 所述的第一存储装置，其中所述加密模块经配置加密所述第一加密密钥，所述第一加密密钥基于由所述加密模块隐藏的密钥，是所述第二存储装置特有的。

5. 一种播放器系统，其经配置播放受信任服务器传输的已加密内容，所述系统包括：

第一接口，其经配置与存储已加密内容的第一存储装置通信，其中所述内容由所述受信任服务器从第二存储装置传输至所述第一存储装置；以及

处理器，其经配置认证所述第一存储装置，通过所述第一接口与所述第一存储装置建立受保护通信信道，从所述第一存储装置接收绑定加密密钥，从所述第一存储装置接收关联所述内容的第二加密密钥，基于所述绑定加密密钥和所述第二加密密钥的加密组合，确定所述内容的访问密钥，从所述第一存储装置接收所述已加密内容，并基于所述访问密钥解密所述内容，其中所述绑定密钥是所述第二存储装置特有的并且基于所述第二存储装置中隐藏的密钥。

6. 根据权利要求 5 所述的播放器系统，其中所述处理器经配置而基于公钥基础设施与所述第一存储装置互相认证。

7. 根据权利要求 5 所述的播放器系统，其中所述处理器经配置而基于数字证书确定对来自所述第一存储的内容的重放的授权。

8. 根据权利要求 5 所述的播放器系统，其中所述处理器经配置表现所述内容成音频格式。

9. 根据权利要求 5 所述的播放器系统，其中所述处理器经配置表现所述内容成视频格式。

10. 根据权利要求 5 所述的播放器系统，其进一步包括用于向显示器输出所述内容的输出接口。

11. 使得能够通过受信任的服务器从第一存储器将内容授权传输至第二存储器的方法，所述方法包括：

接收对于所述第一存储器独特的绑定密钥，并绑定所述内容至所述第一存储器；

基于隐藏在所述第二存储器上的第二隐藏密钥，通过所述第二存储器加密所述绑定密

钥；

将所加密的绑定密钥存储在所述第二存储器的安全区域中；

从所述第一存储器接收第一加密密钥；

基于隐藏在所述第二存储器上的第二隐藏密钥，通过所述第二存储器加密所述第一加密密钥。

将所述第一加密密钥存储在所述第二装置的安全区域中。

12. 根据权利要求 11 所述的方法，其进一步包括从所述第一存储器复制所述加密内容至所述第二存储器。

13. 根据权利要求 11 所述的方法，其进一步包括基于接收的至少一个数字证书授权所述内容的传输。

14. 根据权利要求 11 所述的方法，其进一步包括通过所述受信任服务器与所述第一存储器建立受保护通信信道。

15. 根据权利要求 11 所述的方法，其进一步包括从受信任站点接收指示所述内容已被复制的数字证书。

16. 根据权利要求 11 所述的方法，其进一步包括加密所述数字证书，并将所加密的数字证书存储在所述第二存储器的安全区域中。

17. 根据权利要求 11 所述的方法，其中建立所述受保护通信信道包括通过主机装置认证所述第一存储器。

18. 根据权利要求 11 所述的方法，其中接收对于所述第一存储器独特的绑定密钥包括，接收基于所述第二存储器的要求而产生的临时绑定密钥。

19. 根据权利要求 11 所述的方法，其中所述绑定密钥基于隐藏在所述第一存储器上的第一隐藏密钥。

20. 根据权利要求 11 所述的方法，进一步包括基于所述内容的安全元数据中指定的数字证书或许可中的至少一个授权所述内容的复制。

用于内容传输和分配的数字版权管理系统

[0001] 相关申请的交叉引用

[0002] 本专利申请要求 2012 年 4 月 10 日提交的标题为“DIGITAL RIGHTS MANAGEMENT SYSTEM, DEVICES, AND METHODS FOR DIGITAL CONTENT”, 申请号为 61/622,312 (档案号码 T5453.P) 的美国临时专利申请的优先权, 和 2012 年 4 月 20 号提交的, 标题为“DIGITAL RIGHTS MANAGEMENT SYSTEM TRANSFER OF CONTENT AND DISTRIBUTION”, 申请号为 61/636, 460 (档案号码 T5921.P) 的美国临时专利申请的优先权, 其全部内容通过引用并入此处。

背景技术

[0003] 已经提出许多不同的数字版权管理(“DRM”)系统并在各种平台上实施它们。通常, DRM 指用于控制数字内容和装置的使用的技术。例如, DRM 常用于防止数字内容的未授权复制。

[0004] 如今, 存在多种多样的能够使用户复制和分配数字内容, 特别是已经下载或存储在存储装置如硬盘上的内容的计算装置。而且, 迄今为止大多数 DRM 系统都存在安全漏洞并已经被规避。遗憾的是, 由于当前的 DRM 系统的这些漏洞, 内容公司限制了它们的出售物或使用了难以使用的 DRM 系统。

附图说明

[0005] 现在将参考以下附图对体现本发明各种特征的系统和方法进行描述, 其中:

[0006] 图 1 示出根据一个实施例的示范系统;

[0007] 图 1A 根据另一个实施例示出示范对等系统;

[0008] 图 1B 根据另一个实施例示出示范的受信任服务器系统;

[0009] 图 1C 根据一个实施例示出具有用于分配内容至存储装置的信息站的示例;

[0010] 图 2 根据一个实施例示出示范审计系统;

[0011] 图 3 根据一个实施例示出示范下载系统;

[0012] 图 4 根据一个实施例示出示范客户端系统;

[0013] 图 5 根据一个实施例示出示范存储装置;

[0014] 图 6 根据一个实施例示出产生绑定内容至存储装置的绑定密钥的示范过程流程;

[0015] 图 7 根据一个实施例示出向存储装置提供内容的示范过程流程;

[0016] 图 7A 根据一个实施例示出从主存储装置至次存储装置对等复制或传输内容的示范过程流程;

[0017] 图 7B 根据一个实施例示出通过受信任服务器从主存储装置至次存储装置复制或传输内容的示范过程流程;

[0018] 图 7C 根据一个实施例示出从信息站提供内容至存储装置的示范过程流程;

[0019] 图 8 根据一个实施例示出播放来自次存储装置的内容的示范过程流程。

具体实施方式

[0020] 在一个实施例中，数字内容可通过受信任服务器从一个存储装置安全地传输至另一个装置。具体地，数字内容可基于安全元数据，如密钥、版权等的传输从一个装置传输至另一个。一旦安全元数据的传输已经完成，内容也可被复制或传输。提供数字版权管理(“DRM”)方法和系统用于数字内容的受控分配、传输和重放。例如，提供数字版权管理(“DRM”)方法和系统用于数字内容的受控分配，例如通过信息站，和数字内容的重放。数字内容可包括内容本身和元数据。内容可为任何已知格式的文本、文件、音频、视频、多媒体、视频游戏等。内容元数据可为用于处理内容的与该内容相关的任何数据或信息。可使用内容元数据以提供安全的数字内容处理，且提供 DRM 保护。内容元数据也可包括一个或更多数字证书。

[0021] 在一个实施例中，DRM 系统使内容能够安全复制或传输，例如，从一个存储装置到另一个存储装置。在这个实施例中，内容的传输是基于存储装置间受信任对等的传输执行的。例如，存储装置可使用通透地遂穿一个或更多个主机装置的安全信道从一个存储装置直接传输内容至另一个。在另一个实施例中，DRM 系统使内容和 / 或内容元数据能够安全复制或传输，例如，以对等的方式从一个存储装置到另一个存储装置。

[0022] 在另一个实施例中，DRM 系统使内容和 / 或内容元数据能够安全复制或传输，例如，通过受信任服务器从一个存储装置到另一个存储装置。在这个实施例中，内容和内容元数据的传输由两组存储装置认证和信任的受信任服务器代理。受信任服务器可为 DRM 系统的单独实体或 DRM 系统的现有服务器的组件或功能。

[0023] 在另一个实施例中，用户可获取内容的一个或更多个复件，但不拥有内容元数据，如必要的加密密钥。因此，在这个实施例中，用户可和系统联系以获取安全的元数据并获得访问内容的权利。在一个实施例中，加密的内容可仅为文本、文件、音频、视频、多媒体、视频游戏等的一部分或多于一个部分。

[0024] 提供内容的服务器可加密内容的每个复件，该加密是基于对内容的该复件独特的访问密钥。因此，如果访问密钥泄露，则仅内容的一个复件的保护受损。在另一个实施例中，为保护内容可使用非对称加密。

[0025] 另外，基于访问密钥的配置，内容可独特地绑定至具体装置，如智能存储装置。例如，从至少两个组件生成内容的访问密钥。第一组件为绑定密钥，其对上面存储内容的存储装置是独特 / 特有的。在一个实施例中，利用随机数或输入该随机数到密钥生成器中，存储装置可生成绑定密钥。第二组件是内容特有的内容密钥。在一个实施例中，用于生成访问密钥的算法可实现为可许可或可更新的函数。

[0026] 在一个实施例中，只向某些实体提供基于两个组件生成访问密钥的算法。例如，存储内容的存储装置不保留其绑定密钥的任何复件，也不具有生成访问密钥的算法。生成绑定密钥的算法可为可许可或可更新的。

[0027] 在一个实施例中，使用了双向认证，例如，利用公钥基础设施(“PKI”)和基于公钥证书的认证来确保系统中的实体是受信任的。系统的各种组件，如存储装置，可为智能的，并从而能够彼此双向认证，这在现有技术中是不可能的。例如，存储装置和播放器或下载服务器可彼此互相认证。这种形式的认证确保存储装置确认和播放器的信任关系，反之亦然。常规的 DVD 和蓝光光盘不包含认证或和播放器或下载服务器建立信任关系的这种部件。PKI 因此提供一个环境，其中 DRM 系统的实体可注册其身份并彼此建立信任。

[0028] 在一个实施例中,DRM 系统的实体使用公钥证书,也就是,证明其身份的数字证书,并确定其内容的各种使用的授权。在另一个实施例中,受信任方管理证书颁发机构(“CA”)以监督 PKI 和数字证书。此外,在任何实施例中可供给 CA 的多个级别。

[0029] 可从 CA 的一个或更多个向 DRM 系统的所有装置颁发证书。如果需要,一个实施例可规定实体的证书的全部撤销。如上所述,可在实体间使用双向互相认证,以建立用于交换和分配内容的安全通信信道。也可向每项内容颁发数字证书。这允许内容在确定装置是否可信任时发挥作用。

[0030] 现在将对本发明的某些实施例进行描述。这些实施例仅以例子的形式示出,且不意欲限制本发明的范围。确实,这里描述的新方法和系统可以各种其它形式体现。此外,可对这里描述的方法和系统的形式作出各种省略、替换和改变,而不偏离本发明的精神。为说明一些实施例,现在将参考附图。

[0031] 图 1 示出一个实施例的示范系统 100。如所示的,系统 100 可包括,除了别的之外,审计系统 102、下载系统 104、客户端系统 106 和网络 108。现在将对这些组件和其操作的某些方面做出进一步描述。

[0032] 审计系统 102 作为系统 100 的受信任方。此外,审计系统 102 可提供与在系统 100 中内容的分配和重放相关的各种管理功能。在一个实施例中,审计系统 102 验证并证明加密密钥为系统 100 中使用的 PKI 的一部分。参考图 2 对审计系统 102 做出进一步的描述。

[0033] 下载系统 104 包括用于在系统 100 中分配内容的硬件和软件组件。在一个实施例中,下载系统 104 包括网站,其包括至内容的链接。下载系统 104 也可提供链接以允许与审计系统 102 的事务,如至密钥服务器和证书颁发机构的链接。参考图 3 对下载系统 104 进行进一步描述。

[0034] 客户端系统 106 可为用于访问系统 100 所提供内容的任何装置。例如,客户端系统 106 可包括计算机、电视机、便携式或移动装置、视频游戏控制台、便携式视频游戏控制台和关联的存储器。任何能够下载、存储或播放内容的装置可实施作为客户端系统 106 的部分。例如,客户端系统 106 可包括台式计算机、膝上型计算机、平板计算机、智能电话、电视机、数字视频录像机、机顶盒、视频游戏控制台或便携式视频游戏控制台,或其它形式的电子装置。客户端系统 106 也可包括有线和 / 或无线网络和存储器,如网络连接式存储(“NAS”)或外部驱动器。实施例可对任何形式的存储装置有效,如固态和闪存存储器。参考图 4 对客户端系统 106 进一步描述。

[0035] 客户端系统 106 可包括多种存储装置,用户可利用其存储并访问客户端。例如,如所示的,客户端系统 106 可包括主存储装置 110 和次存储装置 112。主存储装置 110,例如,可为硬盘驱动器、闪存驱动器、混合驱动器等。这种存储装置对本领域技术人员是已知的。在另一个实施例中,存储装置可为网络连接式存储器。

[0036] 次存储装置 112 代表客户端系统 106 可使用的任何额外存储器。例如,次存储装置 112 可为客户端系统 106 的附加硬盘驱动器、外置驱动器等。替代地,次存储装置 112 可为主存储装置 110 的备份存储器。在另一个实施例中,存储装置可为网络连接式存储器。

[0037] 网络 108 提供通信基础设施,系统 100 的各种组件通过其进行通信。网络 108 可包括网络和网络元件的任何集合。例如,可于互联网上实施网络 108。然而,网络 108 可包括任何局域网、城域网或广域网,并可作为专用网络、公共网络等实施。因此,网络 108 可包

括有线或无线通信链接。

[0038] 受信任服务器 114 用作控制局, 允许内容从一个存储装置移至另一个存储装置。在一个实施例中, 受信任服务器 114 可用已知硬件和软件实施。例如, 受信任服务器 114 可为耦合到与系统的其它服务器分离的网络 108 的服务器。替代地, 受信任服务器 114 可在同一硬件上实施, 或可集成为另一个组件如下载系统 104 或审计系统 102 的组件。受信任服务器 114 可经配置基于利用内容的数字证书或例如, 存储在下载系统 104 中的安全内容元数据, 控制内容的复制和传输。参考图 7A 对传输或复制内容的示范过程做出进一步描述。

[0039] 系统 100 可支持下载和播放内容的几种情况。例如, 内容可通过网络 108 从客户端系统 106 下载到便携式存储装置中。然后, 通过从存储装置流式传输内容, 内容可在重放装置上播放, 如蓝光播放器、游戏控制台、电视机。作为另一个例子, 重放装置可包括集成的存储装置, 其用于内容的下载和重放。作为另一个使用情况, 内容可下载到在客户端系统 106 中的 NAS 系统。

[0040] 然而另一个实施可包括客户端系统 106, 其具有绑定内容的连接网络的存储装置或媒体播放器。然后, 客户端系统 106 的用户可远程访问内容并在移动装置上播放, 如 iPad、iPod、iPhone、便携式视频游戏控制台, 如便携式 PlayStation® 或 Nintendo DS 等, 其通过 WiFi、3G、4G 或其它通信信道上的安全连接, 如无线连接, 连接至存储装置或媒体播放器。在系统 100 的另一个实施中, 客户端系统 106 包括如通过蓝牙或 WiFi 或类似的通信系统可无线访问的便携式存储装置或媒体播放器。客户端系统 106 中的便携式存储装置或媒体播放器因此可作为客户端系统 106 中用于在便携式和启用网络的查看装置上重放的内容的来源。

[0041] 图 1A 示出实施例的另一个示范对等系统 100。如所示的, 系统 100 可包括, 除了别的之外, 审计系统 102、下载系统 104、客户端系统 106 和网络 108。在这个实施例中, 次存储器 112 远离客户端系统 106, 如网络备份存储系统、网络连接式存储器或云存储系统。

[0042] 次存储系统 112 可以是为客户端系统 106 提供文件备份和存储的任何系统和服务, 该文件包括由系统 100 的 DRM 保护的内容。可基于已知硬件和软件实施存储系统 112。例如, 次存储系统 112 可为服务器、文件托管服务、内容柜(content locker)等。在一个实施例中, 次存储系统 112 可使用 HTTP 和 FTP 访问来访问文件。此外, 次存储系统 112 可提供主存储 110 的自动或定期备份、加密、逐文件恢复、文件同步、数据压缩、版本控制等。

[0043] 图 1B 示出实施例的另一个示范受信任服务器系统 100。如所示的, 系统 100 可包括, 除了别的之外, 审计系统 102、下载系统 104、客户端系统 106、网络 108 和受信任服务器 114。在这个实施例中, 次存储器 112 作为远程备份存储系统 116 的部分实施。替换地, 次存储器 112 可为网络连接式存储器。

[0044] 备份存储系统 116 可为任何为客户端系统 106 提供文件备份和存储的系统和服务, 这些文件包括由系统 100 的 DRM 保护的内容。备份存储系统 116 可基于已知硬件和软件实施。例如, 备份存储系统 116 可为服务器、文件托管服务、内容柜等。在一个实施例中, 备份存储系统 116 可使用 HTTP 和 FTP 访问来访问文件。

[0045] 备份存储系统 116 也可提供各种功能, 以保护次存储 112。例如, 备份存储系统 116 可提供主存储 110 的自动或定期备份、加密、逐文件恢复、文件同步、数据压缩、版本控制等。如所示的, 虚线示出功能关系。在一个实施例中, 安全的连接通过客户端系统代理,

作为对客户端系统透明的安全隧道 / 通道。

[0046] 图 1C 示出实施例的示范系统 100，其具有用于分配内容至存储装置的信息站。如所示的，系统 100 可包括，除了别的之外，审计系统 102、下载系统 104、信息站 106' 和网络 108。现在将对这些组件和其操作的某些方面进行进一步描述。

[0047] 审计系统 102 用作系统 100 的受信任方。此外，审计系统 102 可提供和系统 100 中内容的分配和重放相关的各种管理功能。在一个实施例中，审计系统 102 验证并证实加密密钥为系统 100 中使用的 PKI 的部分。参考图 2 对审计系统 102 做出进一步描述。

[0048] 下载系统 104 包括用于在系统 100 中分配内容的硬件和软件组件。在一个实施例中，下载系统 104 包括网站，其包括至内容的链接。下载系统 104 也可提供链接以允许与审计系统 102 的事务，如至密钥服务器和证书颁发机构的链接。参考图 3 对下载系统 104 做出进一步描述。

[0049] 信息站 106' 可为用于访问和分配系统 100 提供的内容的任何装置。例如，信息站 106' 可作为自助服务的计算机终端实施。在一个实施例中，信息站 106' 可包括专用硬件和软件，其经设计使得信息站 106' 放置在公共环境中。信息站 106' 可包括各种用户接口设备，如键盘、显示器等，以允许使用信息站 106'。

[0050] 如所示的，信息站 106' 可直接或间接耦合至本地内容数据库 110。本地内容数据库 110 用作为例如从下载系统 104 下载的多个内容的本地存储基础设施。因此，如所示的，用户可连接存储装置 112 至信息站 106'，并从本地内容数据库 110 或下载系统 104 下载内容。参考图 4 对信息站 106' 做出进一步描述。

[0051] 网络 108 提供通信基础设施，系统 100 的各种组件通过其进行通信。网络 108 可包括网络和网络元件的任何集合。例如，网络 108 可于互联网上实施。然而，网络 108 可包括任何局域网、城域网或广域网，并可实施为专用网络、公共网络等。因此，网络 108 可包括有线或无线通信链接。

[0052] 系统 100 可支持下载和播放内容的几种情况。例如，内容可通过网络 108 从信息站 106' 下载到便携式存储装置 112。然后，通过从存储装置流式传输内容，内容可在重放装置如蓝光播放器、游戏控制台、电视机上播放。作为另一个例子，重放装置可包括集成的存储装置，其用于内容的下载和重放。

[0053] 然而另一个实施可包括具有高速接口如 USB (通用串行总线)3.0 接口等的信息站 106'，存储装置或媒体播放器可与高速接口相连。然后，信息站 106' 的用户可访问本地数据库 110 中的内容，或从下载系统 104 下载内容用于以后在移动装置如 iPad、iPod、iPhone 等上播放。在一个实施例中，信息站 106' 通过借助 WiFi、3G、4G 或其它通信信道，如 USB3.0，的安全连接，如无线连接，连接至存储装置或媒体播放器。

[0054] 图 2 示出实施例的示范审计系统。如所示的，审计系统 102 可包括密钥服务器 200、密钥数据库 202 和证书颁发机构 204。

[0055] 密钥服务器 200 是接收并提供一个实施例中利用的各种加密密钥的服务器。密钥服务器 200 可利用已知硬件和软件实施。在一个实施例中，密钥服务器 200 分配密钥作为部分数字证书。数字证书可包含密钥和有关密钥所有人的信息。密钥服务器 200 可提供已知格式的证书，如 X.509、PKCS、OpenPGP 等。

[0056] 密钥数据库 202 存储密钥和密钥服务器 200 使用的其它相关信息。密钥数据库

202 可利用已知数据库管理系统如 Oracle、DB2、MicrosoftSQL、PostgreSQL 和 MySQL 实施。

[0057] 证书颁发机构(或 CA)204 为系统 100 颁发数字证书。可为系统 100 中每个受信任方定制证书格式和内容。此外,在一个实施例中,每项内容可具有受信任方证书作为其部分元数据。证书允许和内容关联的软件独立确定客户端系统 106 中的播放器是否正在尝试访问可信任的内容。例如,如果客户端系统 106 中的播放器不被信任,关联内容的软件可限制播放器访问高清晰内容或其它部分内容。在系统 100 中,任何受信任方都可撤销所有证书,撤销某些证书或已颁发证书的某些部分。

[0058] 在一个实施例中,公钥基础设施(PKI)用于证书签名。例如,在系统 100 中,PKI 在装置认证过程中用在客户端系统 106 中,并用于在存储装置、下载系统 104 或重放装置间建立安全通信信道。在一个实施例中,系统 100 中各种实体间使用双向认证。例如,存储装置可为智能装置,其经配置进行有效认证,并基于完全双向认证建立和重放装置或下载服务器 104 的信任关系。

[0059] 在系统 100 的实体间,每次安全会话可利用独特的安全参数。例如,会话密钥、会话 ID、初始化向量(“IV”)、基于散列的消息认证码(“HMAC”)密钥可以是对每次会话特有的。在一个实施例中,系统 100 利用基于对称加密受保护的安全通信信道。在另一个实施例中,系统 100 可利用 PKI 建立安全信道。

[0060] 图 3 示出实施例的示范下载系统。如所示的,下载系统 104 可包括下载服务器 300 和内容数据库 302。

[0061] 下载服务器 300 为系统 100 交付内容,例如,至客户端系统 106。在一个实施例中,下载服务器 300 用可源自绑定密钥和内容密钥的访问密钥加密内容。下面对绑定密钥和内容密钥做出进一步描述。

[0062] 如所示的,下载服务器 300 可包括网络服务器,其提供各种网页 306 至客户端系统 106,从而使得内容数据库 302 中的内容可访问。在一个实施例中,为了提供内容,下载服务器 200 提供具有很多网页 306 的一个或更多个网站。

[0063] 在一个实施例中,内容的每份复印件都是独特加密的。可独特加密内容整体,或可独特加密内容的某些部分。因此,如果一项内容或其访问加密曾经受损,则损害只限于该项内容。如以下将进一步描述,只有下载服务器 300 和播放器具有生成访问密钥的算法。此外,如上所述,生成访问密钥的算法可为可获许可或可更新函数。

[0064] 内容数据库 302 存储内容、内容元数据和下载服务器提供的有关信息。提供存储和访问基础设施以提供内容项。这种数据库管理系统对本领域技术人员是已知的。

[0065] 内容提供商 304 概念上代表内容源。例如,内容提供商 304 可代表其它数据库或内容存储库、内容交付网络等。任意内容源可包括在任意实施例中。

[0066] 图 4 示出实施例的示范客户端系统 106。许多内容提供商的顾虑为,客户端系统中基于软件的播放器被认为具有高安全风险,因为其易于修改和受黑客攻击。实施例的一个好处是,客户端系统 106 包括具有硬件信任根的装置。装置中的硬件信任根包括安全的加密硬件,其使内容能够重放,重放不只是基于软件,而是利用硬件信任根中提供的加密硬件。

[0067] 例如,在一个实施例中,媒体播放器可包括专用硬件加密处理电路和执行安全计算和关键加密参数的安全存储的加密边界。作为另一个例子,网络连接式存储(“NAS”)控

制器可包括可作为信任根的专用硬件。因此,一个实施例可提供能够实现内容的安全下载,内容的安全存储和内容的安全重放的安全 DRM 系统。

[0068] 如将进一步描述的,客户端系统 106 包括智能存储装置,如具有存储介质 402 的主存储装置 110 和包括硬件信任根作为加密处理模块 409 的部分的控制器 408。在一个实施例中,加密处理模块 409 与其它控制器功能是分离的。明文非对称和对称密钥访问限于加密模块。在这个实施例中,非对称和对称密钥可在加密模块中生成。系统 100 的 DRM 使用公 / 私密钥对。任何存储在加密模块外部的密钥是受密码保护的。因为非对称和对称密钥在加密模块 409 内,所以攻击者难以获得私钥。这允许安全的 PKI 实施作为系统 100 的 DRM 的部分。在另一个实施例中,各种密钥或加密数据可注入或安全地存储在存储装置 110 上。例如,在安全的制造环境中,一个或更多个密钥可注入到存储装置 110 上。

[0069] 在一个实施例中,加密模块 409 用于生成安全地在其边界内的额外密钥。例如,加密模块 409 可经配置生成用于绑定内容至存储装置 110 的绑定密钥。加密模块 409 也可包括对安全信息数字签名并将其存储在非安全存储器中的能力,和对安全信息数字签名并加密及将其存储在非安全存储器中的能力。

[0070] 在一个实施例中,客户端系统 106 中的重放装置也可被从证书颁发机构 204 颁发证书。在一个实施例中该证书可存储在播放器的处理器无法访问的安全区域。在另一个实施例中,例如,在主机装置上运行的播放器可在任意地方存储证书,如,在存储介质 402 的用户区或其它非安全区域中。重放装置可以以加密形式或受保护形式存储证书,如带有数字签名。当播放器和存储装置 110 执行认证时,两个装置中的加密模块将会是能够访问安全数据以执行认证并建立安全通信信道的唯一实体。

[0071] 在一个实施例中,内容和内容元数据不提供访问内容的入口。相反地,一旦建立安全的通信信道,重放装置将请求绑定和内容密钥。回应该请求,存储装置然后可发送绑定和内容密钥至播放器,使得其可生成访问密钥。访问密钥用于解密并表现内容。本领域技术人员将意识到,通过利用这些安全加密模块用于安全相关的通信和安全参数、内容元数据(如绑定和内容密钥)和密钥的处理,系统 100 的 DRM 比现有系统更加难以攻击和损坏。

[0072] 如图所示,客户端系统 106 可包括主机装置 400 和存储装置 110。主机装置 400 可包括,除其它以外,处理器 404、主机加密模块 405 和输出装置 406。现在将对主机装置 404 的这些组件做出进一步描述。

[0073] 处理器 404 包括硬件,用于执行指导主机装置 400 的操作的指令。这种处理器对本领域技术人员是已知的。

[0074] 主机加密模块 405 包括用于为主机装置执行加密操作的硬件。此外,主机加密模块 405 可利用各种安全措施被封装或嵌入以抵抗篡改。

[0075] 输出装置 406 代表打算输出内容的任何装置。例如,输出装置 406 可包括显示器、音频扬声器等。这种输出装置对本领域技术人员是众所周知的。

[0076] 存储装置 110 可包括,除其它以外,存储介质 402、控制器 408 和加密模块 409。现在对存储装置 110 的这些组件做出进一步描述。

[0077] 控制器 408 包括控制存储装置 110 的操作并能够实现与主机装置 400 的通信的硬件和固件。控制器 408 可利用已知的硬件和组件实施。

[0078] 加密模块 409 可为存储装置 110 提供信任基础,如硬件信任根。在一个实施例中,

加密模块 409 为安全加密处理器,其经配置执行各种加密操作。在一个实施例中,加密模块 409 可实施为外部片上系统,其利用各种安全措施被封装以检测篡改,并使其抵抗篡改。在另一个实施例中,加密模块 409 可实施为另一个片上系统内的部分或嵌入其中,或实施为利用各种安全措施封装以检测或抵抗篡改的其它硬件。加密模块可以与其它片上系统(“SoC”)功能隔离或不隔离。

[0079] 存储介质 402 是指存储装置 110 用于存储信息的物理介质。在一个实施例中,存储介质 402 可包括磁性介质、光学介质、半导体介质,如闪存等。在一个实施例中存储介质 402 可包括这些介质的任意组合。

[0080] 图 5 进一步示出实施例的示范存储装置 110。如图所示,加密模块 409 可包括受保护存储器 502。此外,存储介质 410 可包括用户区域 504 和非用户区域 506。

[0081] 受保护存储器 502 提供安全区域以存储有关系统 100 提供的 DRM 的敏感信息,如内容元数据。在一个实施例中,受保护存储器 502 实施为一次性可编程非易失性存储器(“OTP NVM”)。作为 OTP NVM,受保护存储器 502 只可被编程一次并难以改变。此外,受保护存储器 502 也可包括一个或更多个存储器,如 ROM (只读存储器)、静态 RAM (随机存取存储器)和动态 RAM。

[0082] 至于用户区域 504,存储介质 410 的这个区域被提供作为主机装置 400 可访问的存储空间。例如,用户区域 504 可为根据由主机装置 400 使用的逻辑块地址(LBA)可寻址的。

[0083] 存储装置 110 可经配置包括受保护的用户空间 504 中的分区。也就是,可利用加密模块 409 生成的单独密钥加密这个分区中的数据。只许可认证的下载客户端或播放器访问该分区。在一个实施例中,来自用户空间 504 中这个分区的所有或某些数据可只通过安全的认证信道发送。

[0084] 用户空间 504 的这个分区可用于,例如,额外内容元数据文件和有关系统 100 的 DRM 的信息。实际内容本身可只以加密的形式从下载服务器 300 发送或发送至客户端系统 106 中的播放器,因此内容可存储在用户空间 504 中。

[0085] 如图所示,存储装置 110 也可包括非用户区域 506。非用户区域 506 为主机无法直接访问的存储介质 410 的保留区。例如,非用户区域 506 可指主机系统无法寻址的区域。在一个实施例中,非用户区域 506 而保留用于由控制器 408 和加密模块使用,例如,以存储有关系统 100 的 DRM 的各种敏感信息,如内容元数据信息。

[0086] 在一个实施例中,加密模块 409 可产生新安全密钥,并允许存储装置 110 为介质的特别分区区域产生安全的独特磁盘加密密钥,该特别分区区域在用户 LBA 空间如非用户区域 506 中不可见。利用该密钥,加密模块 409 因此可加密所有数据至该非用户区域 506。

[0087] 非用户区域 506 可用于存储有关系统 100 的 DRM 的安全元数据。该元数据可包括,例如,证书、密钥文件、许可文件等。例如,存储装置 110 将具有从证书颁发机构 204 颁发给它的证书。该证书可存储在这个非用户区域 506 中,并将为该区域利用密钥加密。这将绑定证书至存储装置 110。因此,如果驱动器的克隆复件以某种方式被制造,则克隆体将不包括用于非用户区域 506 的加密密钥,并且因此,存储在该区域中的数据无法被正确解密。

[0088] 替换地,关键安全参数,如密钥、证书或其它物体,可分别被加密保护并存储到存储介质。

[0089] 因此,在一个实施例中,为了访问内容,控制器 408 和记录介质 410 无法彼此分开

起作用。也就是，控制器 408 或介质 410 的完整复件单独将不足以访问内容。

[0090] 图 6 示出生成绑定内容至存储装置的绑定密钥的示范过程流程。在一个实施例中，利用随机数并输入该随机数到密钥生成器中，存储装置可生成绑定密钥。密钥生成器可在存储装置或存储装置的硬件组件中运行的软件。在一个实施例中，绑定密钥由两部分组成。在一个实施例中，第一部分基于存储装置的缺陷列表。第二部分基于存储装置上加密模块隐藏的密钥。为保护绑定密钥，绑定密钥不和内容或内容元数据一起存储在存储装置 110 中。相反地，绑定密钥的部分是分别存储的。此外，在一个实施例中，绑定密钥作为临时密钥生成，并且因此，只有当需要时才被存储装置计算。本方法还包括针对可更新函数的能力。如上所述，绑定密钥可以是各个存储装置特有或一类装置特有的，如同一类型的装置等。

[0091] 如图所示，第一，存储装置 110 被提示以确定或识别关于其自身的独特特征。例如，存储装置 110 可确定或识别缺陷列表 600。在一个实施例中，缺陷列表 600 对应制造时存在于存储介质 410 上的缺陷的 P- 列表或零时列表 (time-zero list)。当然，在其它实施例中，独特特征可源自或来源于存储装置 110 的其它部分。

[0092] 第二，加密模块 409 加密处理缺陷列表 600 并生成独特的标识符 602。例如，加密模块 409 可计算来自缺陷列表 600 的信息的散列。此外，加密模块 409 可对独特标识符 602 数字签名。替代地，可通过利用随机数生成器生成存储装置特有的随机数，生成独特标识符 602。例如，加密模块 409 可包括随机数生成器，其为加密模块 409 中的物理装置或组件或是在加密模块 409 中运行的软件。替代地，随机数生成器可为单独的软件或在存储装置上运行的硬件装置。

[0093] 第三，加密模块 409 可在安全区域中存储独特标识符 602。例如，如图所示，加密模块 409 也可在非用户区域 506 中存储加密保护的独特标识符 602。

[0094] 第四，加密模块 409 可生成隐藏的密钥 604。在一个实施例中，密钥 604 是隐藏的，因为其不和其他内容元数据一起存储，而是存储在受保护的存储器 502 中。加密模块 409 可生成一个或一组多个隐藏密钥 604。因此，如果这些密钥中的一个泄露，加密模块 409 可切换至组中的下一个密钥。如果使用了所有密钥，或如果不希望产生或存储密钥组，那么加密模块 409 可根据请求生成新的隐藏密钥 604。值得注意，控制器 408 可经配置跟踪哪个内容被绑定到哪个密钥。

[0095] 基于独特标识符 602 和隐藏密钥 604，存储装置 110 可生成绑定密钥 606，其源自控制器 408 提供的信息和存储介质 410 的独特特征。在一个实施例中，加密模块 409 临时生成绑定密钥 606。

[0096] 绑定密钥 606 将内容加密绑定到存储装置 110。例如，绑定密钥 606 可作为内容的元数据的部分通过安全通信信道被发送至下载系统 104 中的下载服务器 300。然后，下载服务器 300 可利用绑定密钥作为用于加密内容的访问密钥的一个组件。

[0097] 在合适的时间，也可通过安全信道使得认证的播放器可获得绑定密钥 606，以在内容的重放期间使用。例如，存放装置 110 可配置有专用命令，其只有当发送装置已经被认证并通过安全信道通信时才被接受。

[0098] 基于绑定密钥 606，因为存储装置中的隐藏密钥是独特的且安全地存储在加密模块 409 的受保护存储器 502 中且无法复制或克隆到另一个驱动器，所以即使完成了整体介

质 410 的精确逐位复制, 克隆的介质也将无法用于表现内容。

[0099] 图 7 示出向存储装置供应内容的示范过程流程。在这个实施例中, 可撤销性和可再生性是 DRM 系统的属性。作为额外的安全系统组件, 示出的过程流程可包括各种可再生性特征。例如, 密钥可被淘汰或预先生成的随机密钥可与安全分配算法一起使用, 该安全分配算法随时间的变化而变化或针对向存储装置 110 提供的每项内容以随机方式利用多个密钥。例如, 实施例可利用可适用于所有播放器的更新文件的令牌化。

[0100] 在一个实施例中, 过程涉及内容和内容元数据的提供, 如绑定密钥和内容密钥。其它元数据, 如数字证书等也可被提供作为实施例的部分。

[0101] 如图所示, 第一, 存储装置 110 和下载服务器 300 彼此间建立安全的通信信道。例如, 下载服务器 300 和存储装置 110 可使用 PKI 建立安全通信信道。具体地, 主机 400 可向存储装置 110 请求证书。存储装置 110 可收回其证书, 例如, 从其在介质 510 中的非用户区域 506。然后, 存储装置 110 可发送装置会话 ID 和其证书。证书包括其公钥 $\text{Public}_{\text{Device}}$ 。

[0102] 在一个实施例中, 主机 400 核实证书。例如, 主机 400 可检查证书上的签名。主机 400 也可检查其撤销列表以确保来自存储装置 110 的证书没有被撤销。替代地, 主机 400 可通过网络 108 与审计系统 102 和证书颁发机构 204 进行通信, 以核实证书并检查证书的撤销状态。

[0103] 然后, 主机 400 通过发送主机会话 ID 和其证书至存储装置 110 来做出回应, 其证书包括其公钥 $\text{Public}_{\text{Host}}$ 。存储装置 110 核实主机证书并检查签名。存储装置 110 也可检查其自身撤销列表以确保主机 400 没有被撤销。

[0104] 然后, 主机 400 可从存储装置 110 请求会话密钥。作为回应, 在一个实施例中, 存储装置 110 用 $\text{Public}_{\text{Host}}$ 加密随机会话密钥、随机装置初始化向量 (“IV”) 和随机装置基于散列的消息认证码 (“HMAC”) 密钥, 并发送其至主机 400。

[0105] 主机 400 用 $\text{Private}_{\text{Host}}$ 解密信息, 以恢复装置会话密钥、装置 IV 和装置 HMAC 密钥。主机 400 用 $\text{Public}_{\text{Device}}$ 加密随机主机会话密钥、随机主机 IV 和随机主机 HMAC, 并发送这条信息至存储装置 110。然后, 存储装置 110 用 $\text{Private}_{\text{Device}}$ 解密这条信息, 以恢复主机 400 的会话密钥、主机 IV 和主机 HMAC 密钥。

[0106] 主机 400 也可用装置会话密钥加密随机盘问, 并发送其至存储装置 110。存储装置 110 用装置会话密钥解密主机随机盘问, 并然后用主机会话密钥加密主机随机盘问, 并将这条信息发送回主机 400。主机 400 用主机会话密钥解密主机随机盘问, 并确认其与原来发送到存储装置 110 的内容相匹配。这证明存储装置 110 知道对应于用其装置证书发送的公钥的私钥。

[0107] 为进一步确认, 主机 400 可向存储装置 110 请求随机盘问。存储装置 110 用主机会话密钥加密装置随机盘问, 并发送这条信息至主机 400。然后, 主机 400 用主机会话密钥解密装置随机盘问, 并用装置会话密钥加密装置随机盘问, 并将这条信息发送回存储装置 110。存储装置用装置会话密钥解密装置随机盘问, 并确认其与原来发送到主机 400 的内容相匹配。这证明主机 400 因此知道对应于用主机 400 的证书发送的公钥的私钥。

[0108] 在一个实施例中, 存储装置 110 可使用 AES 加密与主机会话密钥和主机 IV, 用于到主机 400 的安全消息。主机 400 也可使用 AES 加密与装置会话密钥和装置 IV, 用于到存储装置 110 的安全消息。

[0109] 一旦已经建立安全会话,会话通信可利用非对称或对称算法实施。在一个实施例中,每个安全信息可包括具有序列号和消息长度的头部,用合适的会话密钥和 IV 加密的主体消息 AES,和具有消息主体的 SHA-256HMAC 的脚部。在一个实施例中,会话通信基于非对称加密建立,并然后基于对称加密受到保护。例如,一旦已经建立安全会话,会话通信可基于对称加密实施,如具有会话密钥和建立 IV 的 AES 加密和 AES 解密。每个安全消息可包括具有序列号和消息长度的头部,用合适的会话密钥和 IV 加密的主体消息 AES,和具有消息主体的 SHA-256HMAC 的脚部。在另一个实施例中,也可使用非对称加密以在会话期间保护通信量。

[0110] 第二,由于建立了安全信道,下载服务器 300 向存储装置 110 请求绑定密钥。具体地,下载服务器 300 可通过安全信道发送消息至存储装置 110。如上所述,在一个实施例中,绑定密钥 606 最初是不在内容的元数据中的,且当需要时生成。

[0111] 第三,存储装置 110 生成绑定密钥 606。具体地,加密模块 409 基于独特密钥 602 和隐藏密钥 604 生成绑定密钥 606。

[0112] 在一个实施例中,加密模块 409 使用单向散列算法或高级加密标准(AES)算法来生成绑定密钥, Kb, 其中:

[0113] $K_b = F(K_{root}, ID_m)$

[0114] 其中, F 是单向函数,

[0115] K_{root} 是加密模块 409 生成的密钥,也就是,隐藏密钥 604,

[0116] ID_m 是在存储装置 110 的制造过程中分配的独特介质标识符号码,如独特标识符 602。

[0117] 替代地,加密模块 409 可利用随机数,如来自随机数生成器的随机数,并输入该随机数到密钥生成器中生成绑定密钥。密钥生成器可为在加密模块 409 中的软件或硬件组件。

[0118] 第四,下载服务器 300 向密钥服务器 200 请求用于保护内容的内容密钥。可通过各种方法分配内容密钥至内容。例如,密钥服务器 200 可分配每项内容特有的内容密钥。在一个实施例中,内容密钥 700 作为内容的部分元数据提供,并存储在存储装置 110 上。当发送至主机 400 时,内容密钥 700 可受加密保护。

[0119] 第五,密钥服务器 200 向下载服务器 300 提供内容密钥 700。具体地,密钥服务器 200 可与下载服务器 300 建立安全信道,例如,基于 PKI。

[0120] 第六,下载服务器 300 基于绑定密钥 606 和内容密钥 700 生成访问密钥 706。具体地,下载服务器 300 可使用独特算法来加密结合绑定密钥 606 和内容密钥 700,并生成访问密钥 706,例如,基于单向散列算法。独特算法可仅对系统 100 的某些实体是已知的,如下载服务器 300 和客户端系统 106 中受信任的重放装置。算法可为可获许可或可更新的函数。此外,一个或更多个算法可通过内容的安全元数据的字段或部分从下载服务器 300 传递至客户端系统 106 中的受信任组件。例如,一组多个算法可最初配置或建立在客户端系统 106 的受信任组件中。然后,下载服务器 300 可在内容的安全元数据中提供指针或指示器,指示当生成访问密钥时要使用的算法组。

[0121] 在一个实施例中,访问密钥 706 不包括在内容元数据中,也不存储在下载服务器 300 上。例如,取而代之地,下载服务器 300 可经配置临时生成访问密钥 706。替代地,用于

生成访问密钥 706 的信息可由下载服务器 300 存档到安全远程存储器。例如，审计系统 102 可作为用于安全存储绑定密钥 606 和 / 或内容密钥 700 的安全存储库。

[0122] 第七，下载服务器 300 向存储装置 110 提供内容密钥 700。然后，存储装置 110 安全地存储内容密钥 700。例如，存储装置 110 可存储内容密钥 700 在非用户区域 506 中。

[0123] 第八，下载服务器 300 将内容 702 的全部或部分加密成已加密内容 704。例如，下载服务器 300 可使用 AES 加密，以基于访问密钥 706 加密内容 702。

[0124] 第九，下载服务器 300 向存储装置 110 提供已加密内容 704。存储装置 110 然后可存储已加密内容 704，例如，在其用户区域中。

[0125] 图 7A 示出根据一个实施例从主存储装置复制或传输内容至次存储装置的示范过程流程。如图所示，首先，存储装置 110 和次存储装置 112 彼此间建立安全的通信信道。例如，这些实体可使用 PKI 来建立彼此的安全通信信道，其通透地遂穿过一个或更多个主机系统 400。

[0126] 一旦已建立安全会话，可基于对称加密，如具有会话密钥和建立的 IV 的 AES 加密和 AES 解密实施会话通信。每个安全消息可包括具有序列号和消息长度的头部，用合适的会话密钥和 IV 加密的主体消息 AES，和具有消息主体的 SHA-256HMAC 的脚部。在另一个实施例中，也可使用非对称加密以在会话期间保护通信量。

[0127] 在一个实施例中，存储装置 110 可利用主机装置 400 代理安全信道，安全信道通透地遂穿过主机装置。例如，存储装置 110 可为连接主机的直接附加 USB。在这个实施例中，主机提供在安全信道的建立中用于辅助的代理，但安全信道实施为通过主机的安全隧道。为说明的目的，为了附图的清晰，省略了通过主机的遂穿。

[0128] 第二，既然已建立了安全信道，主存储装置 110 和次存储器 112 每个都请求传输或复制内容的许可。例如，主存储装置 110 和次存储装置 112 每个都可从彼此请求传输内容的许可。次存储器 112 和主存储器 110 可基于各种标准单个确定许可。在一个实施例中，存储装置 110 和 112 可分析一个或更多个数字证书，以确定传输内容和 / 或内容源数据的授权和访问限制。

[0129] 第三，存储装置 110 生成绑定密钥 606。具体地，加密模块 409 基于独特密钥 602 和隐藏密钥 604 生成绑定密钥 606。值得注意的是，绑定密钥 606 绑定至存储装置 110 的特征产生了内容的所有权链和鉴识溯源性。

[0130] 此外，次存储器 112 也可从存储装置 110 获取内容密钥 700。在一个实施例中，主存储装置 110 向次存储装置 112 提供绑定密钥 606 和内容密钥 700。在一个实施例中，内容密钥源自主存储器 110。

[0131] 在另一个实施例中，次存储器 112 从其它来源如受信任服务器 114、下载系统 104 或审计系统 102 获取内容密钥 700。例如，次存储器 112 可经配置与这些实体之一建立安全通信信道并请求内容密钥 700。次存储器 112 做出的这个请求也可由受信任系统 114 确认或授权。在一个实施例中，存储装置不需要第三方或受信任系统，并且取而代之地，建立对等的安全连接。对等连接可以以多种方式建立，包括，例如，存储装置 110 或 112 的一个或更多个数字证书中规定的策略限制，内容等。

[0132] 第四，主存储装置 110 可通过受信任服务器 114 传输已加密内容 704，并传输至次存储器 112。该传输可利用已知的文件传输协议、流传输等执行。在一个实施例中，主存储

装置 110 通过受信任服务器 114 传输内容 704 的安全元数据至次存储器 112。然后,内容 704 可通过受信任服务器 114 或主存储装置 110 和次存储装置 112 间的对等连接,从主存储装置 110 传输至次存储器 112。

[0133] 图 7B 示出根据一个实施例通过受信任服务器从主存储装置复制或传输内容至次存储装置的示范过程流程。如图所示,第一,存储装置 110 和次存储装置 112 建立与受信任服务器 114 的安全通信信道。例如,这些实体可使用 PKI 建立彼此间和与受信任服务器 114 的安全通信信道。然后,受信任服务器 114 可控制和监督内容从存储装置 110 到次存储装置 112 的传输,下面将对其进行描述。

[0134] 一旦已建立安全会话,会话通信可基于对称加密如具有会话密钥和建立的 IV 的 AES 加密和 AES 解密实施。每个安全消息可包括具有序列号和消息长度的头部,用合适的会话密钥和 IV 加密的主体消息 AES,和具有消息主体的 SHA-256HMAC 的脚部。在另一个实施例中,也可使用非对称加密以在会话期间保护通信量。

[0135] 在一个实施例中,存储装置 110 可利用主机装置 400 代理安全信道,安全信道通透地遂穿过主机装置 400。例如,存储装置 110 可为连接主机的直接附加 USB。在这个实施例中,主机提供在安全信道的建立中用于辅助的代理,但安全信道实施为通过主机的安全隧道。为说明的目的,为了附图的清晰,省略了通过主机的遂穿。

[0136] 第二,由于已建立了安全信道,所以主存储装置 110 和次存储器 112 每个都请求传输或复制内容的许可。例如,主存储装置 110 和次存储装置 112 可从受信任服务器 114 请求传输内容的许可。受信任服务器 114 可基于各种标准确定许可。在一个实施例中,受信任服务器 114 可分析一个或更多个数字证书,如存储装置 110 和 112 和内容的数字证书。

[0137] 第三,存储装置 110 生成绑定密钥 606。具体地,加密模块 409 基于独特密钥 602 和隐藏密钥 604 生成绑定密钥 606。值得注意的是,绑定密钥 606 绑定至存储装置 110 的这个特征产生了内容的所有权链和鉴识溯源性。例如,在一个实施例中,来自存储装置 110 的绑定密钥 606 可通过安全信道发送至次存储装置 112。然后,次存储装置 112 可用其自身的隐藏密钥加密绑定密钥 606,且因此,主存储装置 110 的绑定密钥 606 也加密地绑定至次存储装置 112。

[0138] 此外,次存储器 112 也可从存储装置 110 获取内容密钥 700。在一个实施例中,主存储装置 110 向次存储装置 112 提供绑定密钥 606 和内容密钥 700。

[0139] 在另一个实施例中,次存储器 112 从另一来源,如受信任服务器 114、下载系统 104 或审计系统 102 获取内容密钥 700。例如,次存储器 112 可经配置与这些实体之一建立安全通信信道并请求内容密钥 700。次存储器 112 做出的这个请求也可由受信任系统 114 确认或授权。

[0140] 第四,主存储装置 110 可传输已加密内容 704 至次存储器 112。该传输可利用已知的文件传输、流传输等的协议执行。在一个实施例中,内容的传输直接发生在主存储装置 110 和次存储器 112 之间。在另一个实施例中,传输通过受信任服务器 114 发生。在另一个实施例中,第一存储器 110 证明内容的所有权。然后,通过生成新绑定密钥并传输元数据,重新绑定内容至次存储器 112。也就是,受信任服务器重新提供内容至次存储装置。

[0141] 图 8 示出根据一个实施例的播放来自次存储装置 112 的内容的示范过程流程。如图所示,第一,主机系统 400 和次存储装置 112 可彼此间建立安全通信信道。为简洁,上面

参考图 7 提供了基于 PKI 的建立安全信道的例子。在一个实施例中，存储装置 110 将评估内容的数字证书和播放器证书，以确定播放器适合接收内容和 / 或内容元数据。

[0142] 第二，主机系统 400 向次存储装置 112 请求绑定密钥 606。值得注意的是，在一个实施例中，存储装置 112 安全地保留主存储装置 110 的绑定密钥 606，内容起初是向该主存储装置 110 提供的。如上所述，如果需要，例如为了恢复，盗窃侦查等，这个特征提供了内容的鉴识信息和所有权溯源性。

[0143] 相应地，第三，存储装置 112 提供主存储装置 110 的绑定密钥 606。在一个实施例中，次存储装置 112 在其安全存储区域 506 中以加密的形式存储绑定密钥 606，并使用来自其加密模块 409 的隐藏密钥 605。如上所述，主存储装置 110 的这个绑定密钥 606 加密地绑定到次存储装置 112。

[0144] 第四，主机系统 400 向存储装置 110 请求内容密钥 700。在一个实施例中，内容密钥 700 可从存储在存储装置的非用户区域中的内容元数据取回。具体地，主机系统 400 可基于各种参数，如内容标识符等，请求或指定内容密钥 700。

[0145] 第五，存储装置 110 向主机系统 400 提供内容密钥 700。例如，存储装置 110 可访问非用户区域 506 并传输内容密钥 700 至主机系统 400。当取回内容密钥 700 时，加密模块 409 可需要执行各种密码功能，如解密，检查数字签名等。

[0146] 第六，为了解密内容，主机系统 400 生成访问密钥 706。具体地，主机的加密模块 405 基于绑定密钥 606 和内容密钥 700 的加密组合生成访问密钥 706。用仅在加密模块 405 中已知的独特算法编程加密模块 405。例如，主机系统 400 的加密模块可包含用产生访问密钥 706 的算法编程的 OTP NVM。

[0147] 第七，存储装置 110 向主机系统 400 提供已加密内容 704。在一个实施例中，存储装置 110 使已加密内容 704 流传输到主机系统 400。

[0148] 第八，主机系统 400 加密地处理已加密内容 704，从而以非加密方式恢复内容 702。如上所述，在一个实施例中，内容利用访问密钥 706 基于对称加密如 AES128 进行加密。一旦处于解码或非加密的形式，然后主机系统 400 可输出内容 702 至输出 406。值得注意的是，主机系统 400 可重新加密用于递送至输出 406 的内容。例如，如果输出 406 为高清晰度多媒体接口 (“HDMI”) 装置，那么主机 400 可利用目前为 HDMI 装置指定的高带宽数字内容保护 (“HDCP”) 加密重新加密内容，并以这个安全的形式传输内容。在一个实施例中，主机 400 可解密内容，并接着利用安全的传输加密协议，如高带宽数字内容保护 (HDCP)，重新加密内容，并输出重新加密的内容至显示装置，如电视机、监视器等。在另一个实施例中，主机 400 解密内容，然后利用例如数字传输内容保护 (DTCP) 重新加密内容，并发送重新加密的内容至重放装置，如电视机、监视器等。相应地，在一个实施例中，当在系统 100 的实体间传输时，内容总是处于安全的形式。

[0149] 图 7C 示出从信息站提供内容至存储装置的示范过程流程。在这个实施例中，可撤销性和可再生性是 DRM 系统的属性。作为额外的安全系统组件，示出的过程流程可包括各种可再生性特征。例如，密钥可被淘汰或预先生成的随机密钥可与安全分配算法一起使用，该安全分配算法可随时间的变化而变化或为待向存储装置 112 提供的每项内容以随机方式利用多个密钥。例如，实施例可利用可适用于所有播放器的更新文件的令牌化 (tokenizing)。

[0150] 如图所示,第一,存储装置 112 和信息站 106 彼此间建立安全的通信信道。如上所述,通信可通过有线接口进行,如 USB3.0 接口,或无线接口,如 WiFi、3G、4G 等。例如,信息站 106 和存储装置 112 可使用 PKI 建立安全通信信道。具体地,信息站 106 可向存储装置 112 请求证书。存储装置 112 可例如,从介质 510 中其非用户区域 506,取回其证书。然后,存储装置 112 可发送装置会话 ID 和其证书。该证书包括其公钥 : $\text{Public}_{\text{Device}}$ 。

[0151] 信息站 106 核实证书。例如,信息站 106 可检查证书上的签名。信息站 106 也可检查其撤销列表以确保来自存储装置 112 的证书没有被撤销。替代地,信息站 106 可通过网络 108 与审计系统 102 和证书颁发机构 204 进行通信,以核实证书并检查证书的撤销状态。

[0152] 然后,信息站 106 通过发送主机会话 ID 和其证书,包括其公钥 $\text{Public}_{\text{Host}}$ 至存储装置 112 来做出回应。存储装置 112 核实主机证书并检查签名。存储装置 112 也可检查其撤销列表以确保信息站 106 没有被撤销。

[0153] 然后,信息站 106 可向存储装置 112 请求会话密钥。作为回应,在一个实施例中,存储装置 112 用 $\text{Public}_{\text{Host}}$ 加密随机会话密钥,随机装置初始化向量(“IV”)和随机装置基于散列的消息认证码(“HMAC”)密钥,并发送其至信息站 106。

[0154] 信息站 106 用 $\text{Private}_{\text{Host}}$ 解密信息,以恢复装置会话密钥、装置 IV 和装置 HMAC 密钥。信息站 106 用 $\text{Public}_{\text{Device}}$ 加密随机主机会话密钥、随机主机 IV 和随机主机 HMAC 密钥,并发送这条信息至存储装置 112。然后,存储装置 112 用 $\text{Private}_{\text{Device}}$ 解密这条信息,以恢复信息站的会话密钥、主机 IV 和主机 HMAC 密钥。

[0155] 信息站 106 也可用装置会话密钥加密随机盘问,并发送其至存储装置 112。存储装置 112 用装置会话密钥解密主机随机盘问,并然后用主机会话密钥加密主机随机盘问,并将这条信息发送回信息站 106。信息站 106 用主机会话密钥解密主机随机盘问,并确认其与原来发送到存储装置 112 的内容相匹配。这证明存储装置 112 知道对应于用其装置证书发送的公钥的私钥。

[0156] 为进一步确认,信息站 106 可向存储装置 112 请求随机盘问。存储装置 112 用主机会话密钥加密装置随机盘问,并发送这条信息至信息站 106。然后,信息站 106 用主机会话密钥解密装置随机盘问,并用装置会话密钥加密装置随机盘问,并将这条信息发送回存储装置 112。存储装置用装置会话密钥解密装置随机盘问,并确认其与原来发送到信息站 106 的内容相匹配。这证明了信息站 106 因此知道对应于用信息站的证书发送的公钥的私钥。

[0157] 在一个实施例中,存储装置 112 可使用 AES 加密与信息站会话密钥和主机 IV 用于至信息站 106 的安全消息。信息站 106 也使用 AES 加密与装置会话密钥和装置 IV 用于至存储装置 112 的安全消息。

[0158] 一旦已建立安全会话,可利用对称算法实施会话通信。在一个实施例中,每个安全信息可包括具有序列号和消息长度的头部,用合适的会话密钥和 IV 加密的主体消息 AES,和具有消息主体的 SHA-256HMAC 的脚部。在另一个实施例中,会话通信基于非对称加密建立,并然后基于对称加密受到保护。例如,一旦建立了安全会话,会话通信可基于对称加密如具有会话密钥和建立的 IV 的 AES 加密和 AES 解密实施。每个安全消息可包括具有序列号和消息长度的头部,用合适的会话密钥和 IV 加密的主体消息 AES,和具有消息主体的

SHA-256HMAC 的脚部。在另一个实施例中，也可使用非对称加密以在会话期间保护通信量。

[0159] 第二，由于建立了安全信道，下载信息站 106 向存储装置 112 请求绑定密钥。具体地，信息站 106 可通过安全信道发送消息至存储装置 112。如上所述，在一个实施例中，绑定密钥 606 最初是不在信息站 106 提供的内容的元数据中，而是当需要时被生成。

[0160] 第三，存储装置 112 生成绑定密钥 606。具体地，加密模块 409 基于独特密钥 602 和隐藏密钥 604 生成绑定密钥 606。

[0161] 在一个实施例中，加密模块 409 使用单向散列算法或高级加密标准(AES) 算法来生成绑定密钥， K_b ，其中：

[0162] $K_b = F(K_{root}, ID_m)$

[0163] 其中， F 是单向函数，

[0164] K_{root} 是加密模块 409 生成的密钥，也就是，隐藏密钥 604，

[0165] ID_m 是在存储装置 112 的制造过程中分配的独特介质标识符号码，如独特标识符 602。

[0166] 第四，信息站 106 向密钥服务器 200 请求用于保护内容的内容密钥。内容密钥可通过各种方法分配至内容。例如，密钥服务器 200 可分配每项内容特有的内容密钥。在一个实施例中，内容密钥作为内容的部分元数据提供，并存储在存储装置上。

[0167] 第五，密钥服务器 200 向信息站 106 提供内容密钥 700。具体地，信息站 106 可与下载服务器 300 建立安全信道，例如，基于 PKI。

[0168] 第六，信息站 106 基于绑定密钥 606 和内容密钥 700 生成访问密钥 706。具体地，下载服务器 300 可使用独特算法来加密结合绑定密钥 606 和内容密钥 700，并生成访问密钥 706，例如，基于单向散列算法。独特算法可仅对系统 100 的某些实体是已知的，如信息站 106 和主机 400 中受信任的重放装置。

[0169] 在一个实施例中，信息站 106 可经配置临时生成访问密钥 706，以致其不存储在信息站 106 上。替代地，用于生成访问密钥 706 的信息可由信息站 106 存档到安全远程存储器。例如，审计系统 102 可作为安全存储绑定密钥 606 和 / 或内容密钥 700 的安全存储库。

[0170] 第七，信息站 106 向存储装置 112 提供内容密钥 700。然后，存储装置 112 安全地存储内容密钥 700。例如，存储装置 112 可存储内容密钥 700 在非用户区域 506 中。

[0171] 第八，信息站 106 将内容 702 的全部或部分加密成已加密内容 704。例如，信息站 106 可使用 AES 加密，以基于访问密钥 706 加密内容 702。

[0172] 第九，信息站 106 向存储装置 112 提供已加密内容 704。存储装置 112 然后可存储已加密内容 704。

[0173] 图 8 示出播放内容的示范过程流程。如图所示，第一，主机系统 400 和存储装置 112 建立彼此间安全的通信信道。为简洁起见，上面参考图 7 提供基于 PKI 的建立安全信道的例子。

[0174] 第二，主机系统 400 向存储装置 112 请求绑定密钥 606，因为其不在内容元数据中。值得注意的是，在一个实施例中，存储装置 112 不保留绑定密钥 606。在另一个实施例中，主机系统 400 请求对于要播放的内容特定的绑定密钥 606。这允许，例如，存储装置 112 使用用于生成绑定密钥 606 的不同算法。使用的算法可取决于各种标准，如内容的具体项、内容类型、内容源、内容的复印件数目等。

[0175] 相应地,第三,存储装置 112 临时生成绑定密钥 606。具体地,如上所述,加密模块 409 基于隐藏密钥 604 和独特标识符 602 的加密结合生成绑定密钥 606。一旦生成,存储装置 112 可传输绑定密钥 606 至主机系统 400。

[0176] 第四,主机系统 400 向存储装置 112 请求内容密钥 700。在一个实施例中,内容密钥 700 可从存储在存储装置 402 上非用户区域 506 中的内容元数据取回。主机系统 400 可基于各种参数,如内容标识符等,指定内容密钥 700。

[0177] 第五,存储装置 112 向主机系统 400 提供内容密钥 700。例如,存储装置 112 可访问非用户区域 506 并传输内容密钥 700 至主机系统 400。当取回内容密钥 700 时,加密模块 409 可需要执行各种加密功能,如解密,检查数字签名等。

[0178] 第六,为解密内容,主机系统 400 生成访问密钥 706。具体地,主机的加密模块 405 基于绑定密钥 606 和内容密钥 700 的加密结合生成访问密钥 706。用仅在加密模块 405 中是已知的独特算法编程加密模块 405。例如,加密模块 405 可包括包含 OTP NVM,其用产生访问密钥 706 的算法编程。这种特征允许,除了其它以外,访问密钥 706 实质上不在内容元数据中。

[0179] 第七,存储装置 112 向主机系统 400 提供已加密内容 704。在一个实施例中,存储装置 112 使已加密内容 704 流传输到主机系统 400。

[0180] 第八,主机系统 400 加密地处理已加密内容 704,从而以非加密方式恢复内容 702。如上所述,在一个实施例中,内容利用访问密钥 706 基于对称加密如 AES128 进行加密。一旦处于解码或非加密的形式,然后主机系统 400 可输出内容 702 至输出 406。值得注意的是,主机系统 400 可重新加密用于递送至输出 406 的内容。例如,如果输出 406 为高清晰度多媒体接口(“HDMI”)装置,那么主机 400 可利用目前为 HDMI 装置指定的高带宽数字内容保护(“HDCP”)加密重新加密内容,并以这个安全的形式传输内容。在一个实施例中,主机 400 可解密内容,并接着利用安全的传输加密协议,如高带宽数字内容保护协议(HDCP),重新加密内容,并输出重新加密的内容至显示装置,如电视机、监视器等。在另一个实施例中,主机 400 解密内容,然后利用,例如数字传输内容保护(DTCP)重新加密内容,并发送重新加密的内容至重放装置,如电视机、监视器等。相应地,在一个实施例中,当在系统 100 的实体间传输时,内容总是处于被保护的形式。

[0181] 以上公开的具体实施例的特征和属性可以不同方式结合,以形成另外的实施例,其全部都在本发明公开的范围内。例如,在网络连接式存储(NSA)的情况下,NSA 存储可包含一个或更多个存储装置,并实施各种技术(如 RAID),其导致内容可传遍多个存储装置。在包括单个驱动器的 NAS 的情况下,NAS 控制器可经配置,以类似以上描述的方式绑定内容至单驱动器的存储装置。在包括多个驱动器的 NAS 的情况下,内容可绑定至 NAS 子系统,而不是具体存储装置或存储介质或除具体存储装置或存储介质之外。相应地,NAS 子系统可包含安全的加密模块。在实施例的这个变体中,对于 NAS 存储,独特密钥组可由 NAS 控制器生成,并安全地存储在 NAS 的安全存储中。然后,绑定至 NAS 的内容可以类似以上描述的方式执行。因此,即使完成了驱动器的克隆复件,该驱动器也将无法使用,除非其安装在完全一样的 NAS 系统中。本方法可用于替换 NAS RAID 系统中损坏的驱动器,同时确保克隆的驱动器是没有用的。

[0182] 尽管本公开提供了某些实施例和应用,但是对本领域一般技术人员显而易见的其

他实施例，包括不提供这里阐述的全部特征和优点的实施例，也在本公开的范围内。相应地，本公开的范围打算只参考所附权利要求来限定。

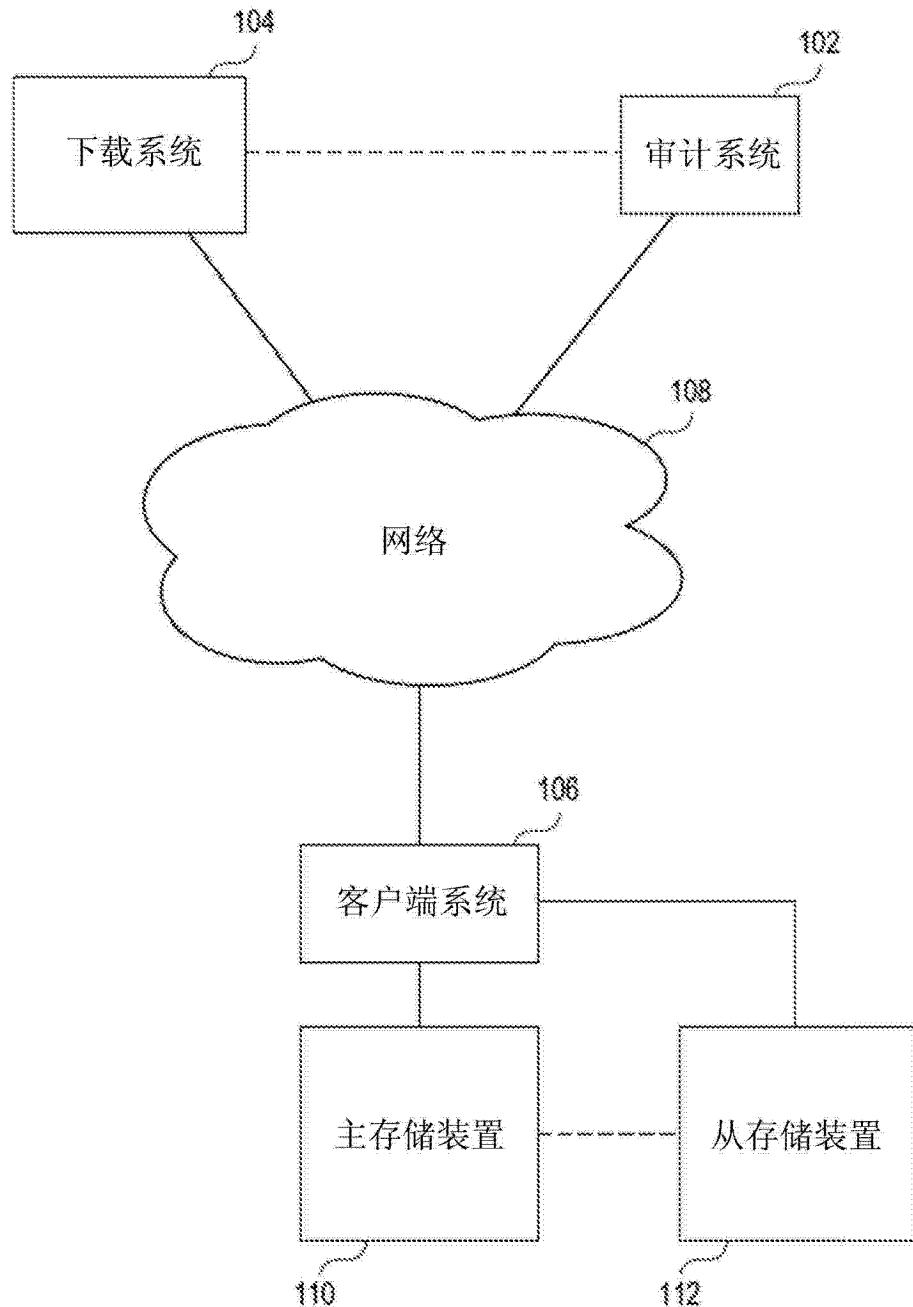


图 1

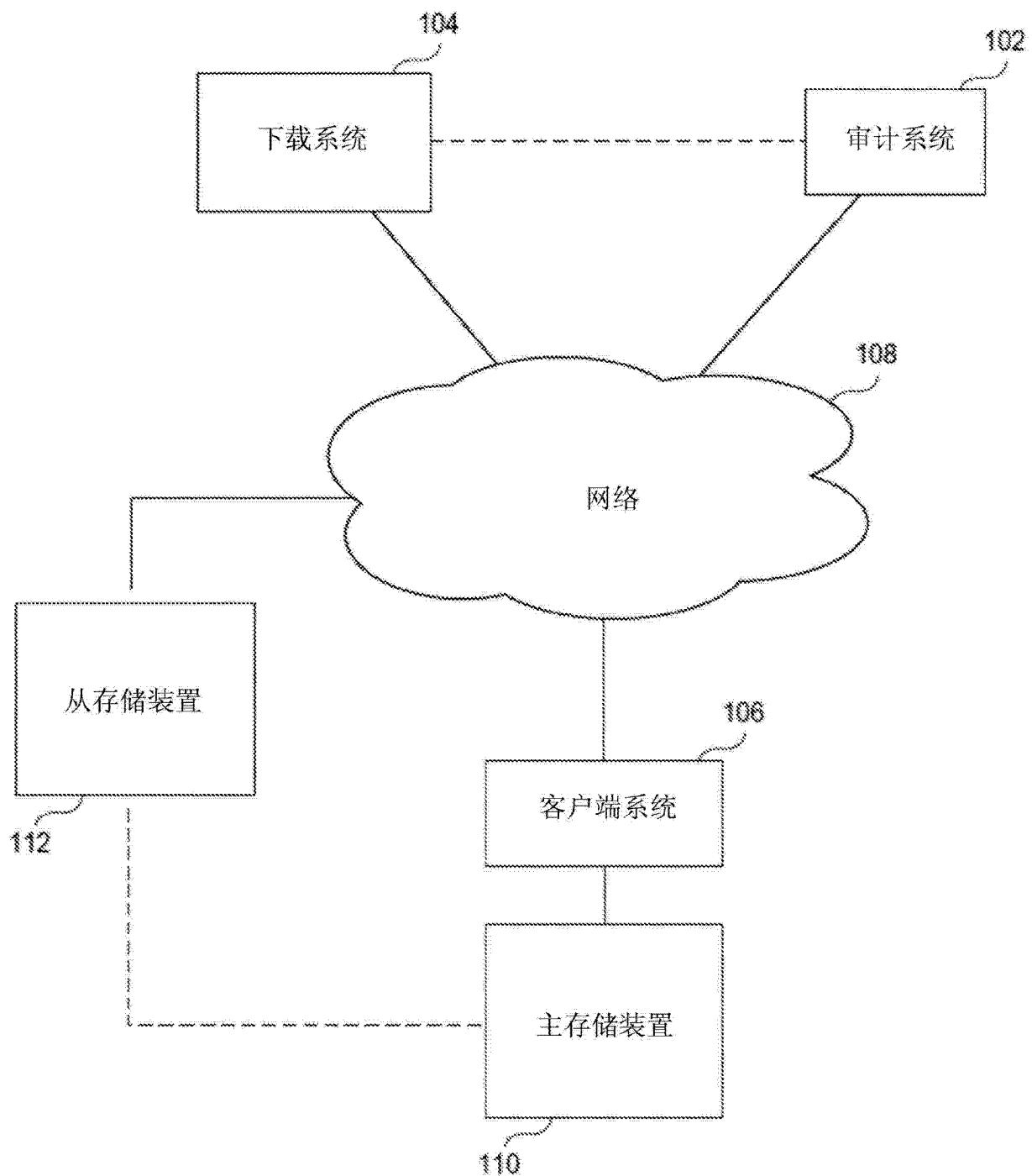


图 1A

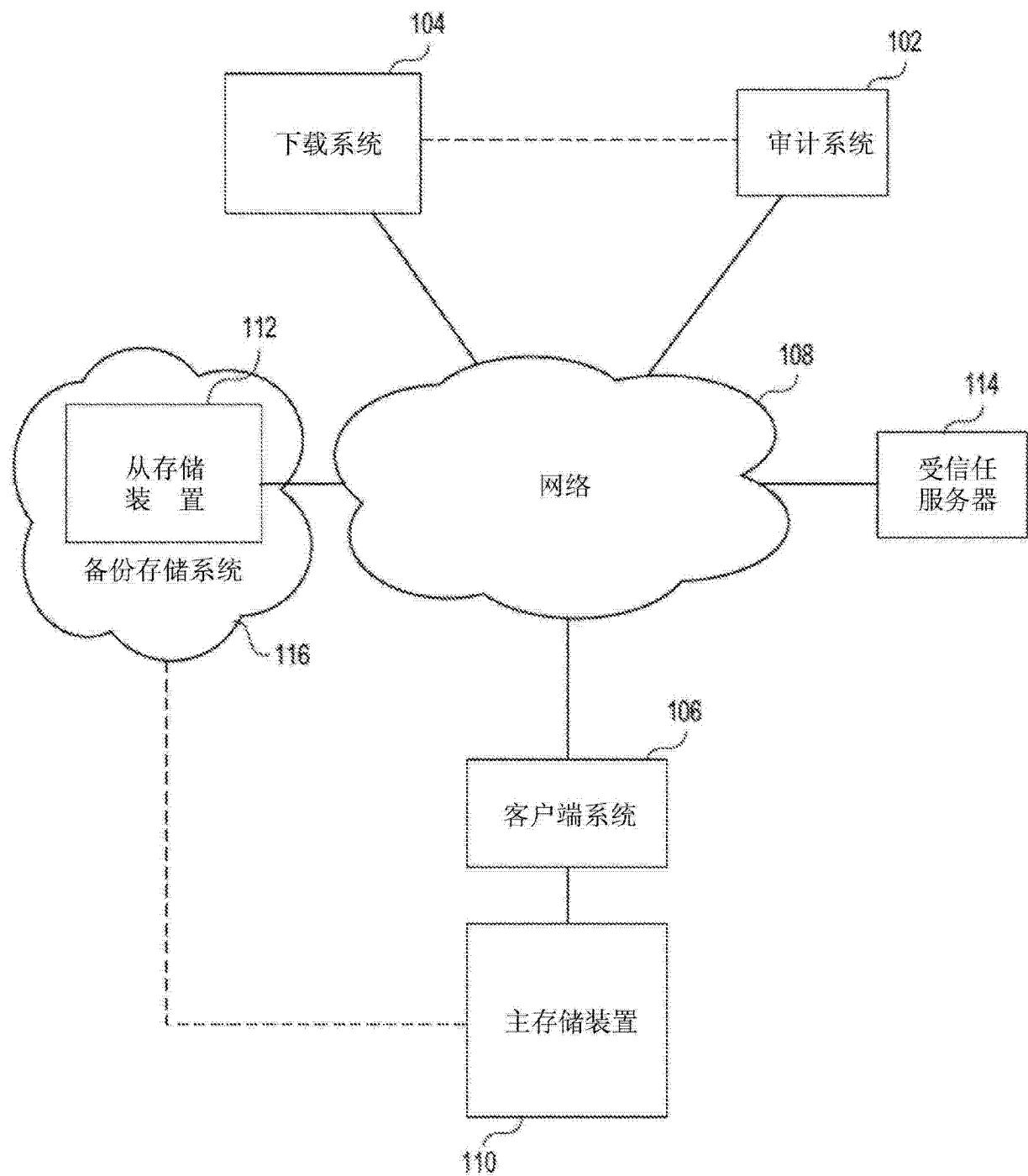


图 1B

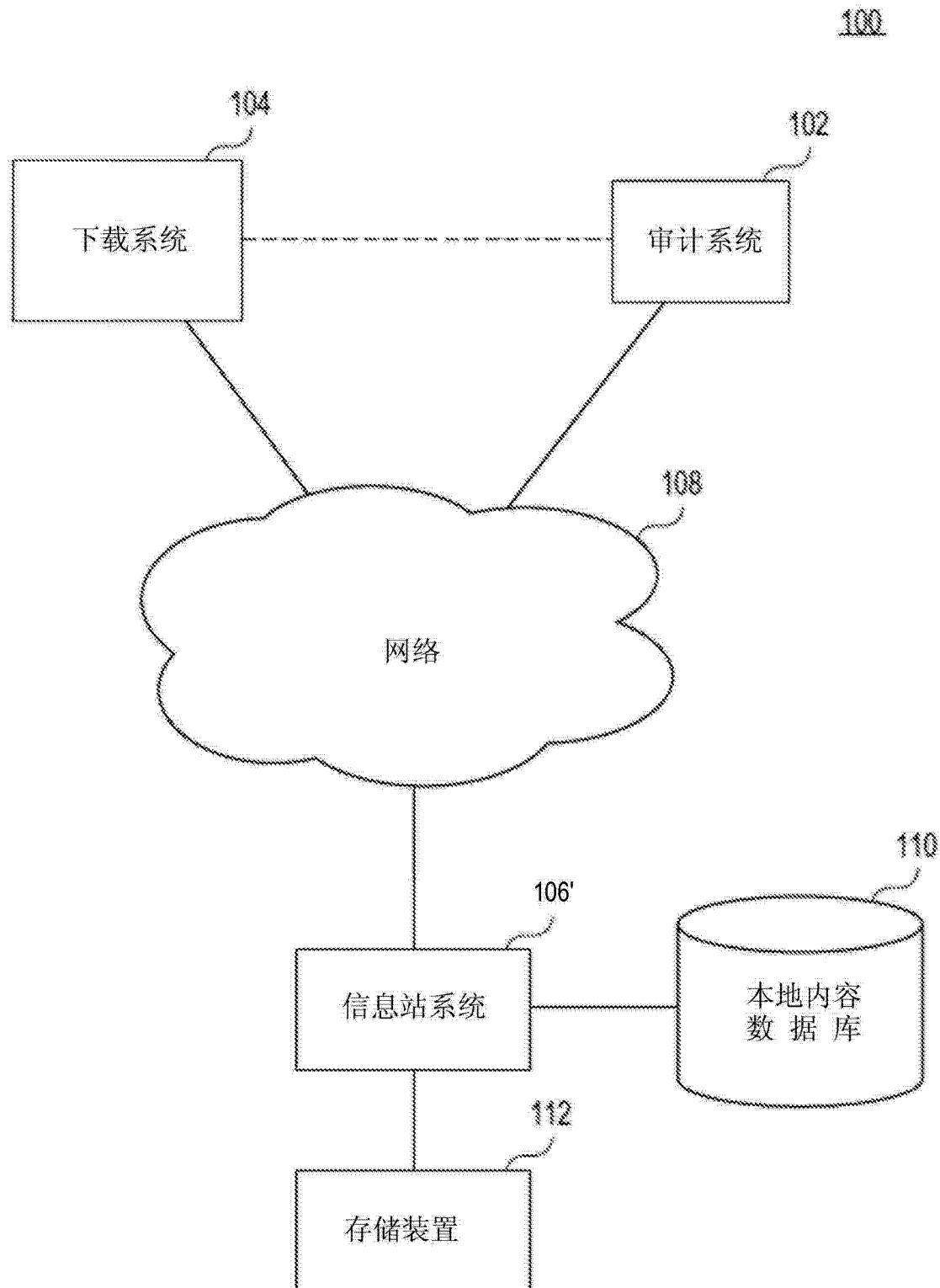


图 1C

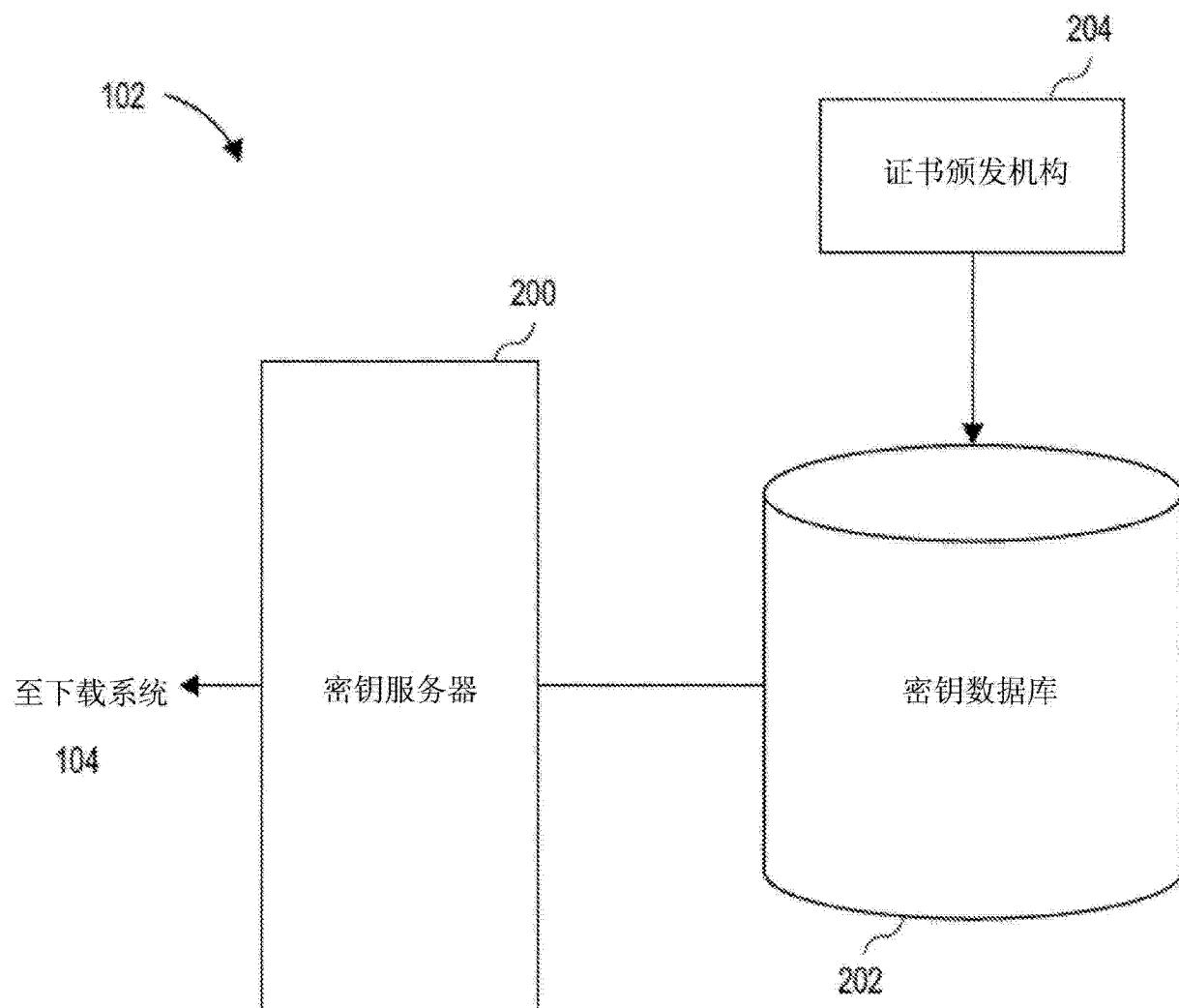


图 2

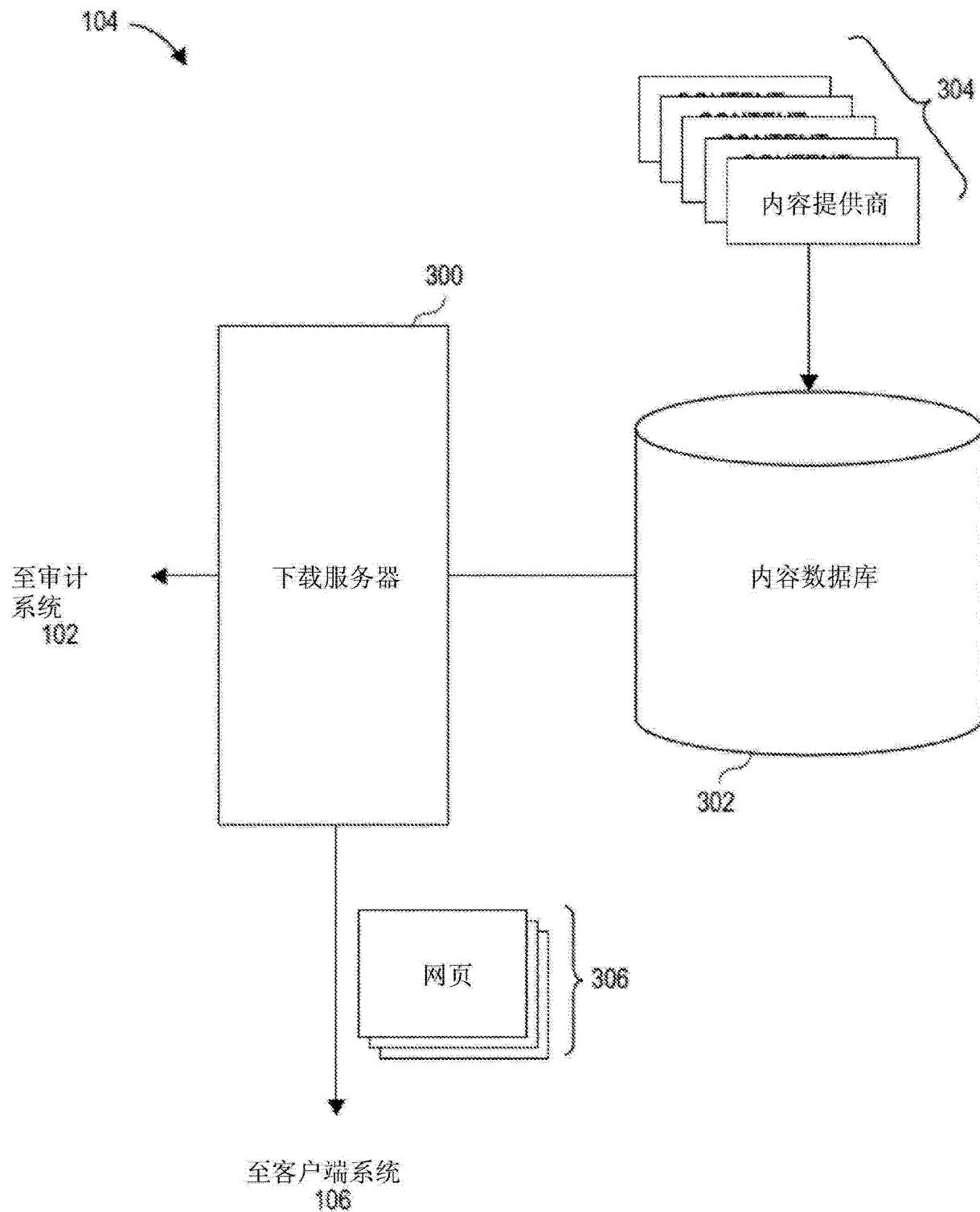


图 3

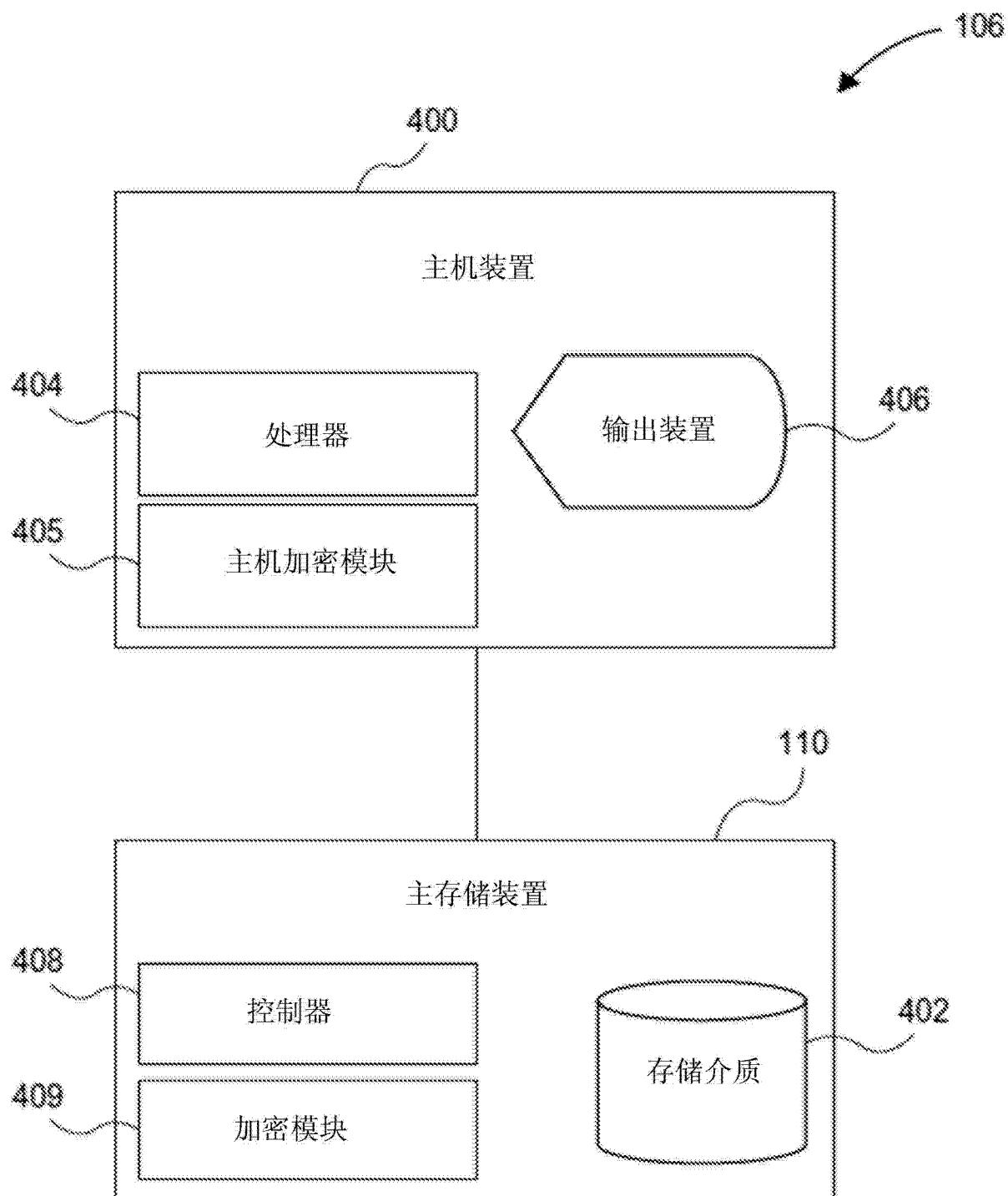


图 4

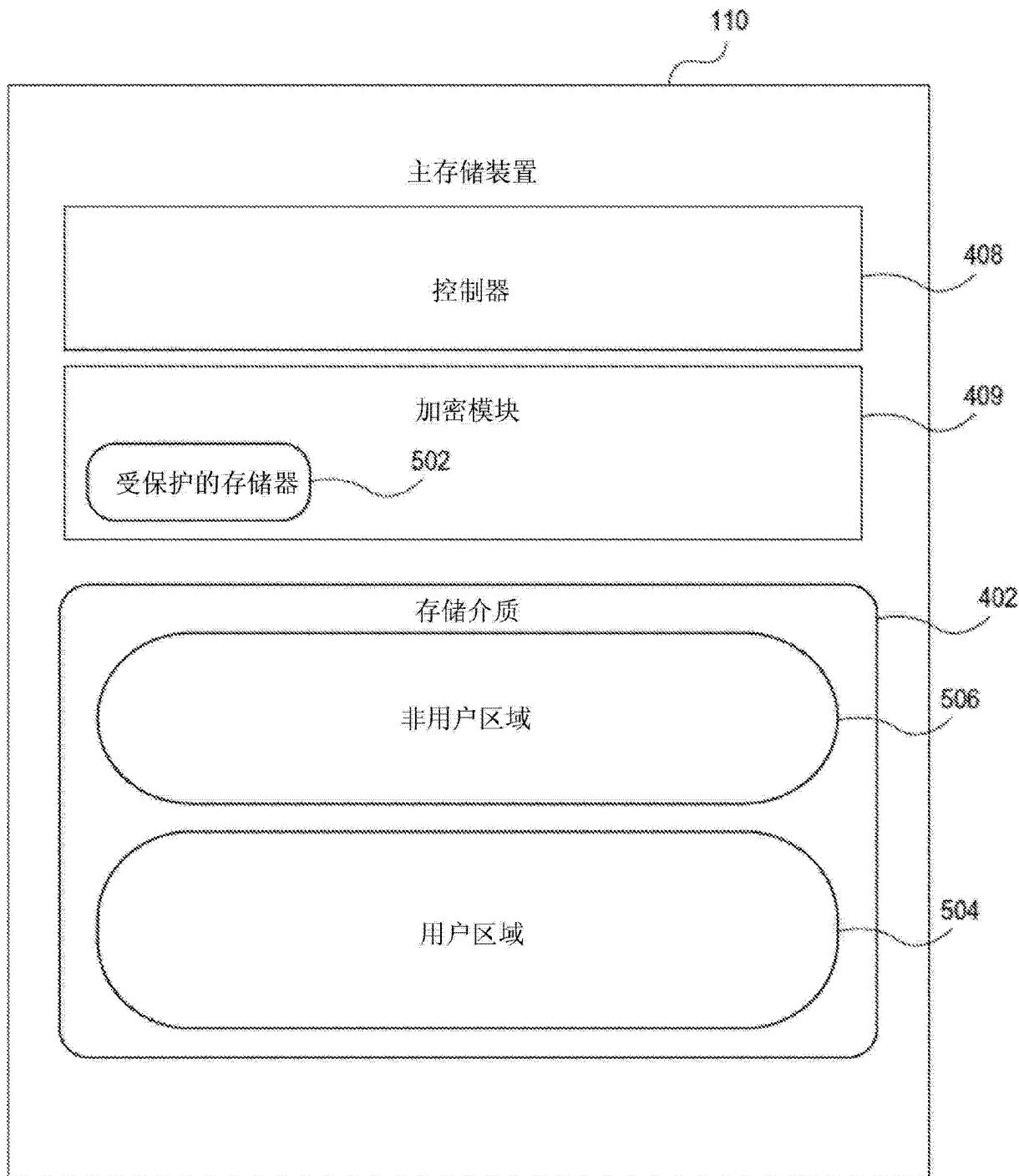


图 5

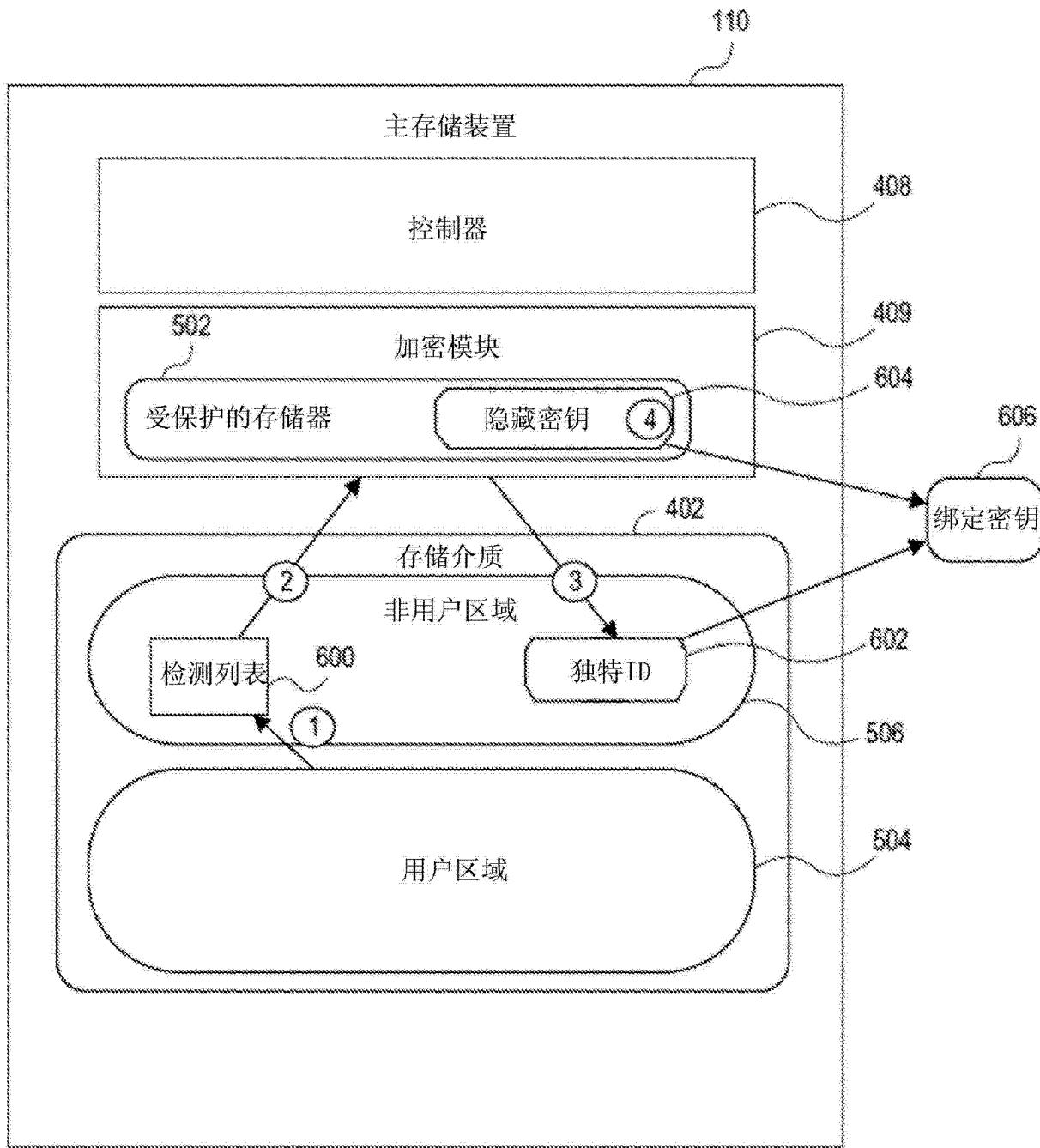


图 6

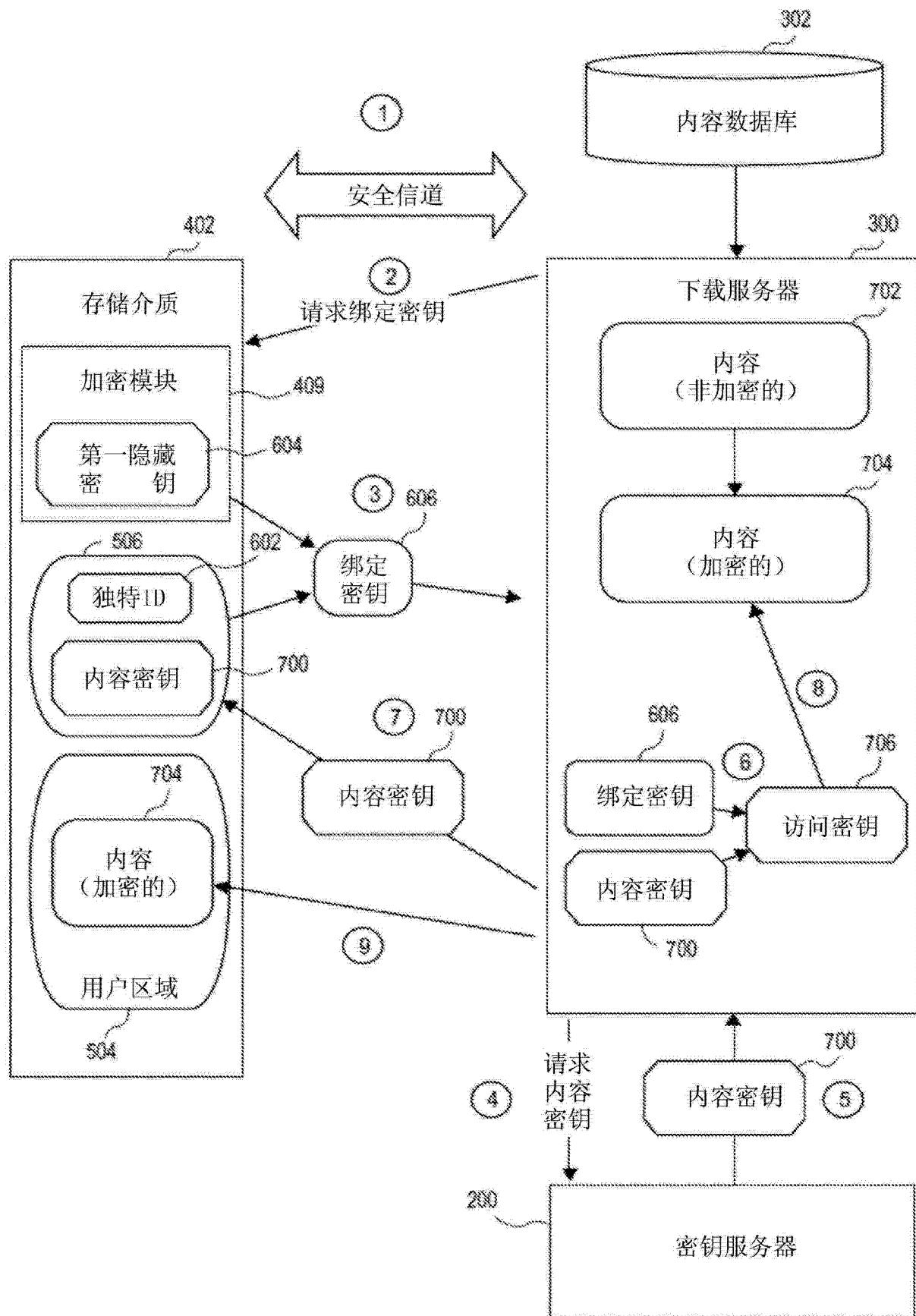


图 7

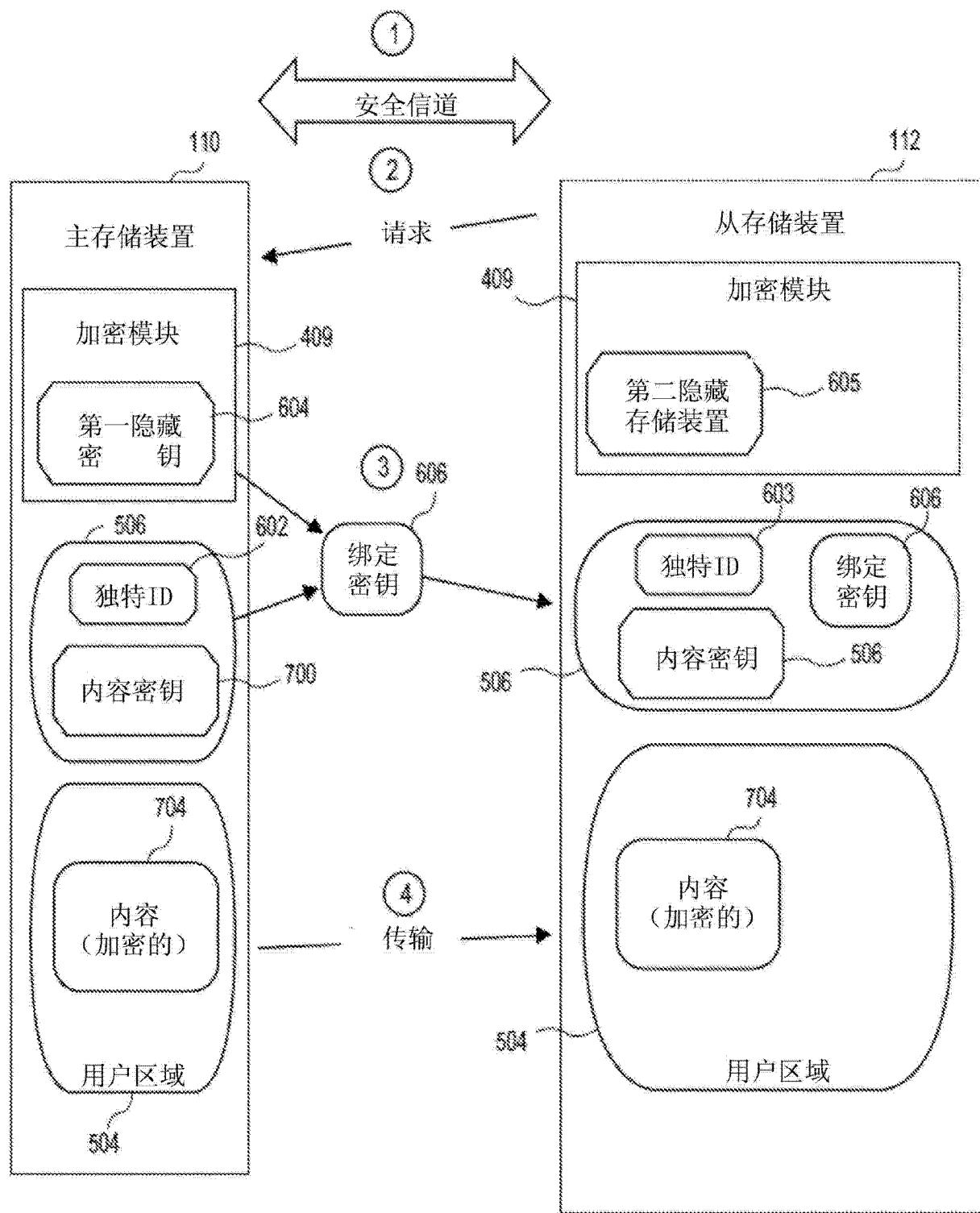


图 7A

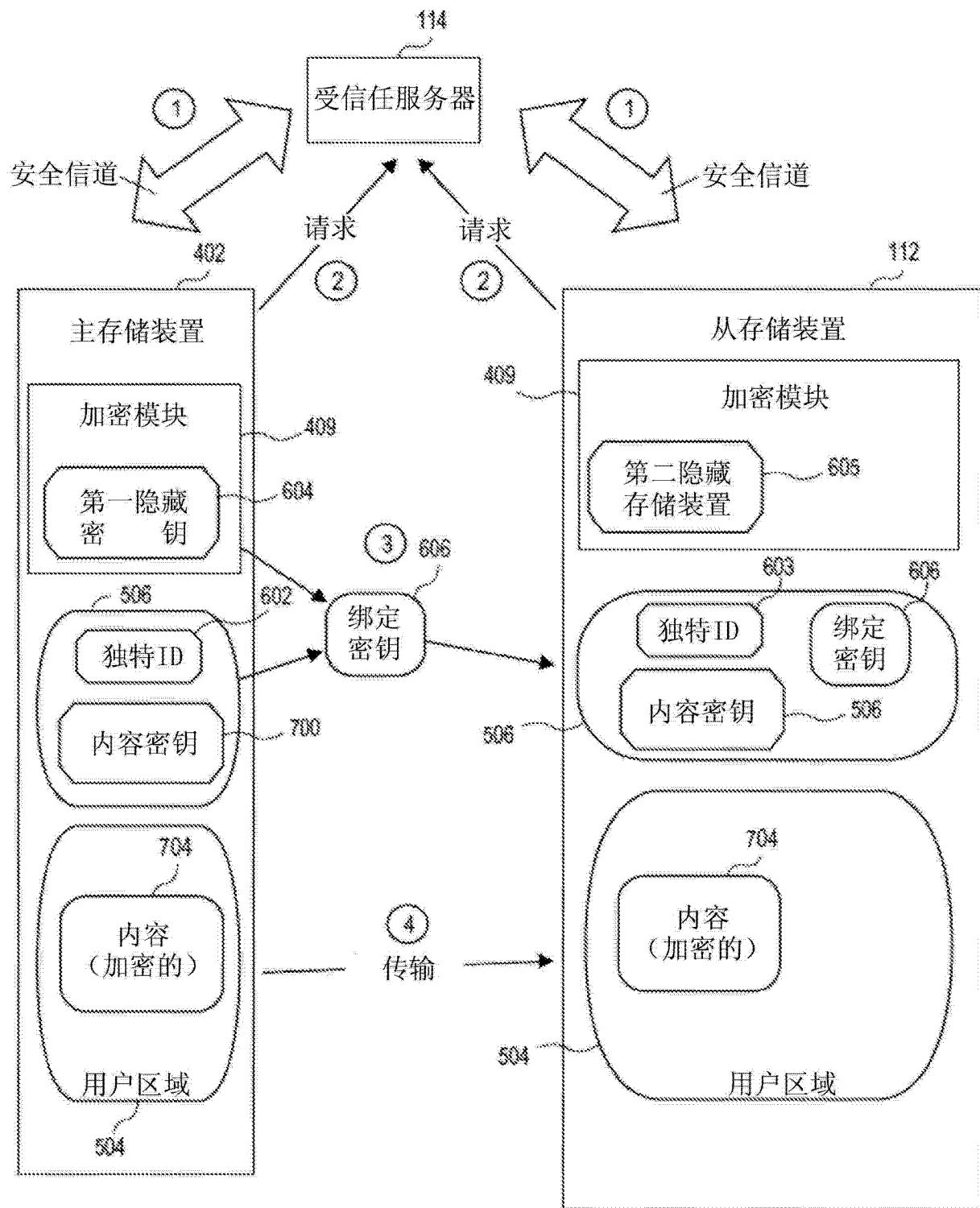


图 7B

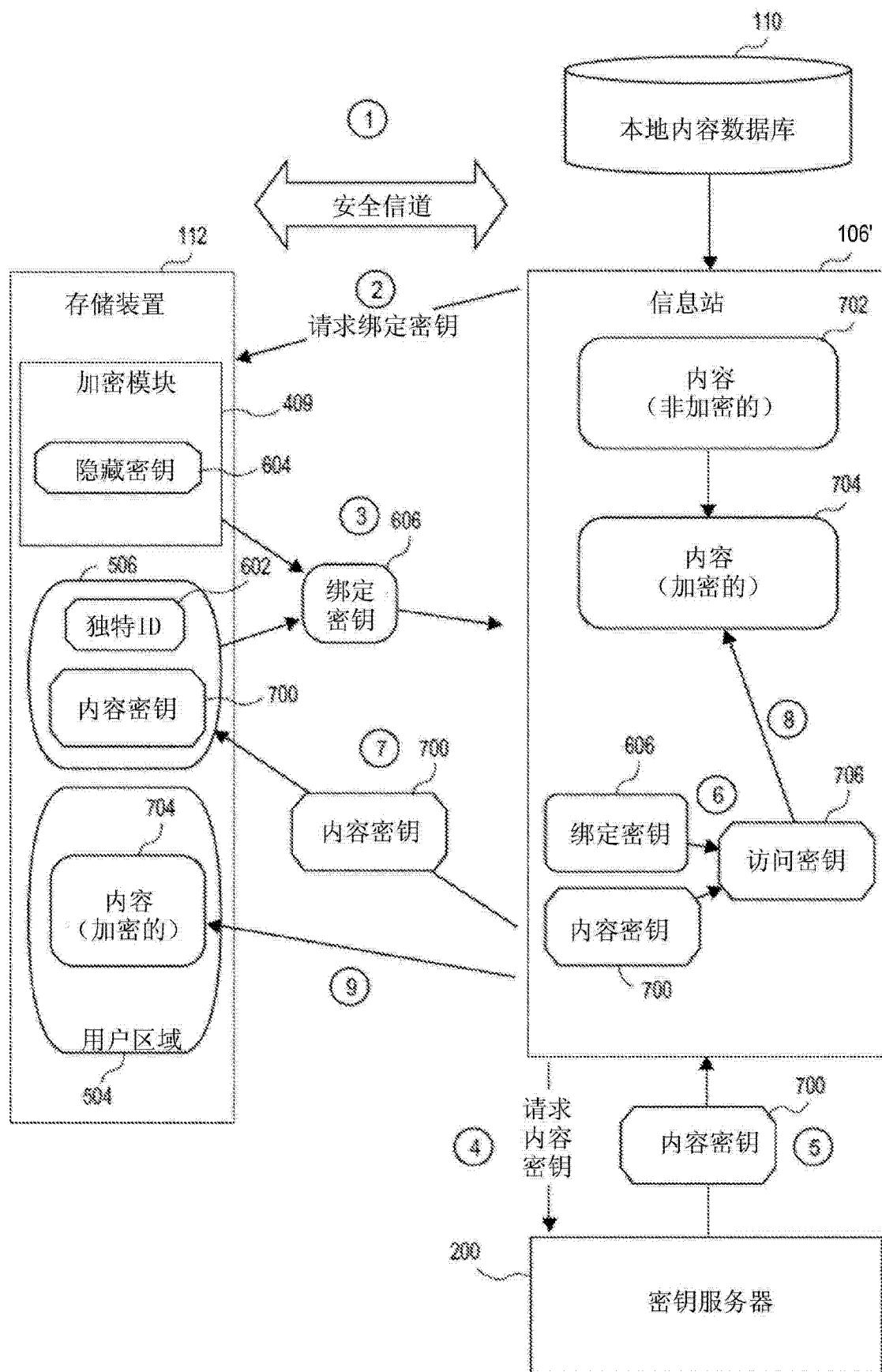


图 7C

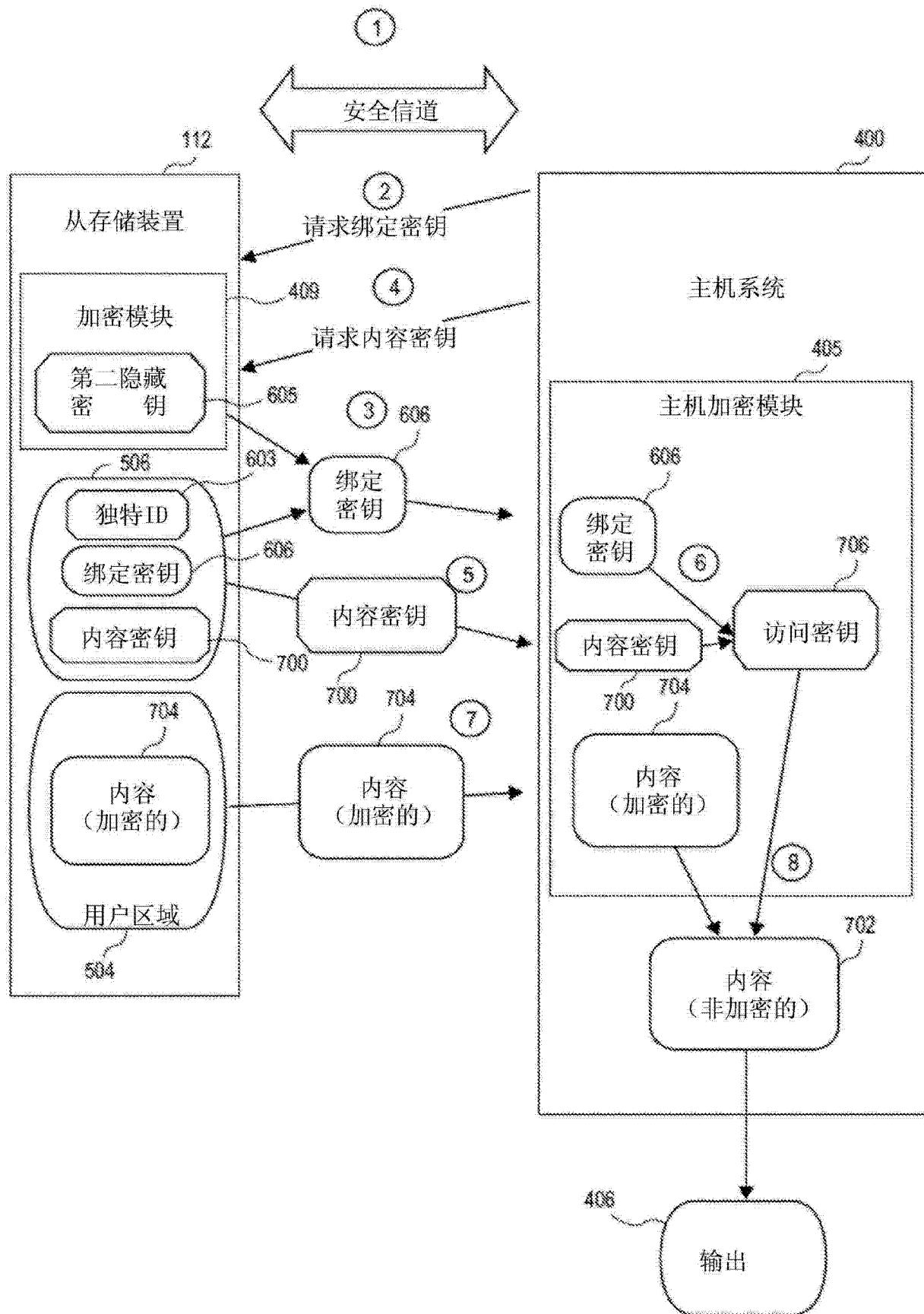


图 8