(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 101390104 B
(45)授权公告日 2012.08.22

(21)申请号 200780006214.8
(22)申请日 2007.02.26
(30)优先权数据
11/361,154 2006.02.24 US
(85)PCT申请进入国家阶段日
2008.08.21
(86)PCT申请的申请数据
PCT/US2007/062826 2007.02.26
(87)PCT申请的公布数据
WO2007/101166 EN 2007.09.07
(73)专利权人 高通股份有限公司
地址 美国加利福尼亚州
(72)发明人 朱利安·杜兰德 贾森·B·克纳吉
佩尔·尼尔森 克里斯托夫·伯纳德
埃米·麦加雷根
布赖恩·L·坎贝尔
(74)专利代理机构 北京律盟知识产权代理有限责任公司 11287
代理人 刘国伟
(51)Int.Cl.
G06F 21/00(2006.01)
(56)对比文件
US 5774651 A,1998.06.30, 全文.
US 6832318 B1,2004.12.14, 全文.
US 20020120722 A1,2002.08.29, 全文.
审查员 董鑫

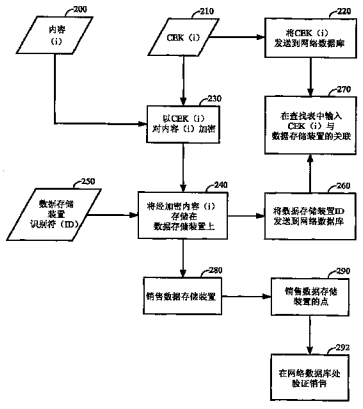
权利要求书 2 页 说明书 15 页 附图 12 页

(54)发明名称

用于应用程序和媒体内容的受保护分布的方法和设备

(57)摘要

本发明提供保护媒体内容的分布的方法、装置、设备、计算机可读媒体和处理器。对媒体内容进行加密，且相关联密码机制被存储并可远程地在联网数据库处存取或可内部地在数据存储装置存储器内存取。通过使所述密码机制与数据存储装置标识以及视需要计算装置标识相关联来准予对所述密码机制的存取。



CN 101390104 B

1. 一种在受保护环境中分布内容的方法，所述方法包括：

获得第一存储装置识别符与密码机制之间的关联；

获得所述密码机制的至少一密钥；

从计算装置接收对存取受保护内容的至少一部分的请求，所述请求包括受保护内容部分识别符；以及

基于所述受保护内容部分识别符与所述第一存储装置识别符之间的对应而将所述密码机制的至少所述密钥转发到所述计算装置。

2. 根据权利要求 1 所述的方法，其进一步包括：

获得所述第一存储装置识别符、所述受保护内容的至少一个其它部分与至少一个其它密码机制之间的关联；

获得所述其它密码机制的至少一密钥；

从所述计算装置接收对存取所述受保护内容的至少所述一个其它部分的请求，所述请求包括所述受保护内容部分识别符；以及

基于所述受保护内容部分识别符与所述第一存储装置识别符之间的对应而将所述一个其它密码机制的至少所述密钥转发到所述计算装置。

3. 根据权利要求 1 所述的方法，其进一步包括：

获得计算装置识别符、所述第一存储装置识别符与所述密码机制之间的关联，所述计算装置识别符与所述计算装置相关联；

其中从所述计算装置接收所述请求进一步包括一个其它计算装置识别符；且

其中将所述密码机制的至少所述密钥转发到所述计算装置进一步包括基于所述计算装置识别符与所述一个其它计算装置识别符之间的对应而进行转发。

4. 根据权利要求 1 所述的方法，其进一步包括：

获得采购交易、所述第一存储装置识别符与所述密码机制之间的关联，所述采购交易与所述计算装置相关联；且

其中将所述密码机制的至少所述密钥转发到所述计算装置进一步包括基于所述受保护内容部分识别符、所述第一存储装置识别符与所述采购交易之间的对应而进行转发，

其中，所述采购交易涉及与存储装置的转移相关的信息。

5. 根据权利要求 1 所述的方法，其进一步包括：

从至少一个其它计算装置接收对存取所述受保护内容的至少一部分的请求，所述请求包括第三存储装置识别符；以及

基于所述第三存储装置识别符与所述第一存储装置识别符之间的不对应而将购买选项消息转发到所述一个其它计算装置。

6. 根据权利要求 5 所述的方法，其进一步包括响应于所述购买选项消息从所述一个其它计算装置接收付款信息，以及基于接收的所述付款信息而将所述密码机制的至少所述密钥转发到所述计算装置。

7. 根据权利要求 1 所述的方法，其中转发所述密码机制的至少所述密钥进一步包括转发所述密码机制。

8. 根据权利要求 1 所述的方法，其中获得第一存储装置识别符与密码机制之间的关联进一步包括获得所述受保护内容的多个部分与相应的多个密码机制之间的关联，其中受保

护内容的所述多个部分的每一者对应于所述多个密码机制中的至少一者。

9. 根据权利要求 1 所述的方法，其进一步包括：

在具有所述第一存储装置识别符的存储装置上载入未受保护内容；

利用所述密码机制加密所述未受保护内容的至少一部分，借此定义所述受保护内容的所述至少一部分；以及

定义所述第一存储装置识别符与所述密码机制之间的关联。

10. 根据权利要求 1 所述的方法，其进一步包括：

存储一个或一个以上采购交易数据，其中每一采购交易与所述受保护内容的相应部分相关联；以及

基于所述存储的采购交易数据辨别计算装置存取受保护内容部分的授权，

其中，所述采购交易涉及与存储装置的转移相关的信息。

11. 根据权利要求 10 所述的方法，其进一步包括基于对存取受保护内容部分的所述授权的识别而将与受保护内容部分相关的数据传送到所述计算装置。

12. 根据权利要求 1 所述的方法，其进一步包括：

监视所述计算装置的内容存取活动；以及

基于对内容存取活动的所述监视而将内容购买建议传送到所述计算装置。

13. 根据权利要求 12 所述的方法，其进一步包括：

监视所述计算装置的环境属性；以及

基于对环境属性的所述监视而将内容购买建议传送到所述计算装置。

14. 一种在受保护环境中分布内容的装置，其包括：

用于获得第一存储装置识别符与密码机制之间的关联的装置；

用于获得所述密码机制的至少一密钥的装置；

用于从计算装置接收对存取受保护内容的至少一部分的请求的装置，所述请求包括受保护内容部分识别符；以及

用于基于所述受保护内容部分识别符与所述第一存储装置识别符之间的对应而将所述密码机制的至少所述密钥转发到所述计算装置的装置。

用于应用程序和媒体内容的受保护分布的方法和设备

技术领域

[0001] 所描述的方面大体涉及网络环境中媒体内容的受保护分布。更明确地说，所描述的方面涉及在可移除数据存储装置上媒体内容和应用程序的受保护分布。

背景技术

[0002] 例如紧密光盘 (CD)、数字视频光盘 (DVD)、快闪媒体卡等可移除数据存储装置已在例如音乐文件、视频文件、多媒体文件、电视游戏应用程序、商业应用程序、文本文件等数字媒体内容的分布中变得日益流行。这些类型的数据存储装置为媒体经销商提供相对便宜的用于物理数据存储的媒体，同时为可移除数据存储装置的用户提供用于使存储装置与例如台式计算机、膝上型计算机、电视游戏机、手提式计算装置等多种计算装置介接的装置。

[0003] 媒体内容提供商的一个当前关注是保护与媒体内容相关联的知识产权。如果可轻易地在计算装置之间且因此在用户之间移动内容，那么与媒体内容和 / 或应用程序相关联的版权和专利保护（即，数字权利）可能受到危害。用于在确保强有力的知识产权保护的受保护环境中分布数据的当前装置成本过高和 / 或技术上不容许。由于可移除数据存储装置通常是便宜的装置，内容提供商不愿意实施可能增加装置成本的知识产权保护方法。

[0004] 除了内容提供商对于知识产权保护的关注外，内容的用户还需要一种不会另外对其对于媒体内容的存取造成负担的保护装置。对于内容的用户友好存取从装置可销售性的观点来看很重要，从而确保用户继续购买此类型的数据存储装置。因此，需要开发出可无缝地操作且因而对存储装置的用户造成最小负担的知识产权保护装置。

[0005] 其它保护关注还可依据装置上存储的内容的类型和形式而与可移除数据存储装置有关。在此方面，存储较大媒体文件和 / 或对象的数据存储装置可引起额外关注。举例来说，内容提供商可在单一数据存储装置中提供大量媒体内容、应用程序或文件。一些内容（例如，可执行文件等）可能需要保护，而其它内容（例如，资源文件等）可能不需要保护。能够将保护限于所关注内容会提供许多益处。举例来说，通过将保护仅限于相关内容（例如，音乐文件、视频文件、电视游戏应用程序），剩余内容可由多个用户存取且剩余内容可促使额外用户购买受保护的内容。另外，通过将受保护内容仅限于相关内容，将内容从受保护内容转换为未受保护内容的整个过程极为顺畅，因此增加过程的效率并使用户获得更为友好的体验。

[0006] 另外，较大媒体文件和 / 或应用程序可能要求对于内容的指定部分的个别保护。通过开发出允许对内容的各个部分的个别保护的方法和过程，可设计出新的且具创新性的商业模式以向用户提供对于此类内容的存取。举例来说，在如今的电视游戏市场中，希望购买电视游戏应用程序的额外特征或升级的用户通常被要求购买额外数据存储装置，这要求对电视游戏零售商的回访。因此，需要提供一种允许用户对于额外特征、升级等的按需存取的数据存储装置，因此消除用户再访问零售分店或另外找到对额外特征的购买途径的需要。

[0007] 因此，需要开发出一种用于在可移除数据存储装置中实施数据保护的装置，其从

成本角度来看为内容提供商提供合理的解决方案，且为装置用户提供一种用户友好的存取受保护内容的装置。另外，需要提供一种包含大量内容 / 应用程序的存储的数据存储装置，所述内容 / 应用程序中的一些要求保护而一些不要求保护。并且，需要开发出用于提供对与存储在数据存储装置上的主要内容有关的额外特征或内容的按需受保护存取的方法和设备。

发明内容

[0008] 因此，呈现在例如 CD、DVD、快闪媒体卡等可移除数据存储装置中提供数据保护的装置、方法、设备、计算机可读媒体和处理器。所提供的数据保护在技术设计上较简单且从成本实施的观点来看也是合理的。所述装置、方法、设备、计算机可读媒体和处理器可经配置以仅向存储在装置上的内容的要求保护的那些部分提供此类保护，借此允许未受保护的内容保持可由所有用户存取。另外，所述方法、设备、计算机可读媒体和处理器可经配置以基于存储装置与一个或一个以上计算装置的关联而限制对受保护内容的存取。并且，所述方法、设备、计算机可读媒体和处理器可经配置以向存储在装置上的内容的若干部分提供个别保护，因此基于用户的特许权将用户存取限于内容的个别部分。

[0009] 在一些方面，一种在受保护环境中获得内容的方法包括接收包括存储装置识别符和受保护内容的存储装置。所述方法进一步包含将存储装置识别符转发到网络装置。此外，所述方法包含基于与存储装置识别符的关联从网络装置接收对于密码机制的至少一参考。另外，所述方法包含利用所述密码机制存取受保护内容的至少一部分。在相关方面，计算机可读媒体确实地存储指令序列，所述指令当执行时促使计算机装置执行上文描述的动作。在另一相关方面，至少一个处理器可经配置以执行上文描述的操作。

[0010] 在其它方面，一种无线装置包括用于接收包括存储装置识别符和受保护内容的存储装置的装置。所述无线装置进一步包括用于将存储装置识别符转发到网络装置的装置，和用于基于与存储装置识别符的关联从网络装置接收对于密码机制的至少一参考的装置。另外，所述无线装置包含用于利用所述密码机制存取受保护内容的至少一部分的装置。

[0011] 在另外其它方面，例如无线装置、台式计算机、膝上型装置、游戏机等计算装置包括处理引擎和可由处理引擎执行的内容存取起始器模块。可操作以辨别存储在存储装置上的受保护内容的内容存取起始器将存储装置识别符传送到网络装置，从网络装置接收对与存储装置识别符相关联的第一密码机制的至少一参考，并将第一密码机制应用于受保护内容的至少一部分以将受保护内容的所述部分转换为未受保护内容的一部分。

[0012] 在另外其它方面，一种在受保护环境中分布内容的方法包括获得第一存储装置识别符与密码机制之间的关联，以及获得对密码机制的至少一参考。所述方法进一步包含从计算装置接收对存取受保护内容的至少一部分的请求，其中所述请求包括第二存储装置识别符。另外，所述方法包含基于第二存储装置识别符的至少一部分与第一存储装置识别符之间的对应而至少将对密码机制的所述参考转发到计算装置。

[0013] 所述方法获得所述第一存储装置识别符、所述受保护内容的至少一个其它部分与至少一个其它密码机制之间的关联；获得对所述其它密码机制的至少一密钥；从所述计算装置接收对存取所述受保护内容的至少所述一个其它部分的请求，所述请求包括所述第二存储装置识别符；以及基于所述第二存储装置识别符与所述第一存储装置识别符之间的对

应而将对所述一个其它密码机制的至少所述密钥转发到所述计算装置。

[0014] 所述方法进一步包括获得计算装置识别符、所述第一存储装置识别符与所述密码机制之间的关联，所述计算装置识别符与所述计算装置相关联；其中从所述计算装置接收所述请求进一步包括一个其它计算装置识别符；且其中将对所述密码机制的至少所述密钥转发到所述计算装置进一步包括基于所述计算装置识别符与所述一个其它计算装置识别符之间的对应而进行转发。

[0015] 所述方法进一步包括获得采购交易、所述第一存储装置识别符与所述密码机制之间的关联，所述采购交易与所述计算装置相关联；且其中将对所述密码机制的至少所述密钥转发到所述计算装置进一步包括基于所述第二存储装置识别符、所述第一存储装置识别符与所述采购交易之间的对应而进行转发。

[0016] 所述方法进一步包括从至少一个其它计算装置接收对存取所述受保护内容的至少一部分的请求，所述请求包括第三存储装置识别符；以及基于所述第三存储装置识别符的至少一部分与所述第一存储装置识别符之间的不对应而将购买选项消息转发到所述一个其它计算装置。

[0017] 所述方法进一步包括响应于所述购买选项消息从所述一个其它计算装置接收付款信息，以及基于接收的所述付款信息而将对所述密码机制的至少所述密钥转发到所述计算装置。

[0018] 优选的，转发对所述密码机制的至少所述密钥进一步包括转发所述密码机制。

[0019] 优选的，获得第一存储装置识别符与密码机制之间的关联进一步包括获得所述受保护内容的多个部分与相应的多个密码机制之间的关联，其中受保护内容的所述多个部分的每一者对应于所述多个密码机制中的至少一者。

[0020] 所述方法进一步包括在具有所述第一存储装置识别符的存储装置上载入未受保护内容；利用所述密码机制遮掩所述未受保护内容的至少一部分，借此定义所述受保护内容的所述至少一部分；以及定义所述第一存储装置识别符与所述密码机制之间的关联。

[0021] 所述方法进一步包括存储一个或一个以上采购交易数据，其中每一采购交易与所述受保护内容的相应部分相关联；以及基于所述存储的采购交易数据辨别计算装置存取受保护内容部分的授权。

[0022] 所述方法进一步包括基于对存取受保护内容部分的所述授权的识别而将与受保护内容部分相关的数据传送到所述计算装置。

[0023] 所述方法进一步包括监视所述计算装置的内容存取活动；以及基于对内容存取活动的所述监视而将内容购买建议传送到所述计算装置。

[0024] 所述方法进一步包括监视所述计算装置的环境属性；以及基于对环境属性的所述监视而将内容购买建议传送到所述计算装置。

[0025] 在相关方面，计算机可读媒体确实地存储指令序列，所述指令当执行时促使计算机装置执行上文描述的动作。在另一相关方面，至少一个处理器可经配置以执行上文描述的操作。

[0026] 在另外的方面，定义能够与计算装置联网的网络装置，例如网络服务器或任何其它装置。网络装置包括用于获得第一存储装置识别符与密码机制之间的关联的装置，以及用于获得对密码机制的至少一参考的装置。所述网络装置进一步包含用于从计算装置接收

对存取受保护内容的至少一部分的请求的装置，所述请求包括第二存储装置识别符。另外，所述网络装置包含用于基于第二存储装置识别符的至少一部分与第一存储装置识别符之间的对应而至少将对密码机制的所述参考转发到计算装置的装置。

[0027] 在其它方面，一种网络装置包括处理引擎和可由处理引擎执行的个人化模块。可操作以从联网计算装置接收存储装置识别符的个人化模块确定与存储装置识别符相关联的密码机制，并将对密码机制的至少一参考传送到计算装置。

[0028] 在另外其它方面，一种分布内容的方法包括在具有存储装置识别符的存储装置上载入未受保护内容，所述存储装置经配置用于与计算装置进行可移除通信。所述方法进一步包含利用密码机制遮掩未受保护内容的至少一部分，借此定义受保护内容的至少一部分。并且，所述方法包含定义存储装置识别符与密码机制之间的关联。另外，所述方法包含将所定义的关联转发到网络装置，所述网络装置可操作以向具有存储装置识别符的联网计算装置提供对受保护内容的至少所述部分的存取。

[0029] 在某一方面，例如媒体卡、CD、DVD、游戏卡盘等数据存储装置包含包括数据存储装置识别符和受保护内容（例如，加密内容）的存储器。所述数据存储装置识别符可以是序列号或与装置相关联的任何其它识别符。可通过将识别符传送到利用与识别符相关联的密码机制进行响应的网络装置而将受保护内容转换为未受保护内容。

[0030] 因此，所描述的方面提供一种用于保护存储在可移除数据存储装置上的内容的具成本效益且有效的装置。

附图说明

[0031] 下文将结合附图描述所揭示的方面，提供附图是为了说明而不限制所揭示的方面，其中相同标志表示相同元件，且其中：

[0032] 图 1 说明用于提供受保护环境中的内容分布的一般系统的一个方面；

[0033] 图 2 是用于提供受保护环境中的内容分布的系统的一个方面的框图；

[0034] 图 3 说明与图 2 的计算装置相关联的无线网络（明确地说，蜂窝式装置网络）的一个方面；

[0035] 图 4 是用于提供可移除数据存储装置的一个方面的流程图；

[0036] 图 5 是用于个人化通信网络中的可移除数据存储装置、计算装置和受保护内容的方面的流程图；

[0037] 图 6 和 7 是用于提供受保护环境中的内容分布的一个方面的过程流程图；

[0038] 图 8 和 9 是用于提供受保护环境中的内容分布的替代方面的过程流程图；以及

[0039] 图 10-12 是用于提供受保护环境中的内容分布的另一替代方面的过程流程图。

具体实施方式

[0040] 参看附图描述本发明装置、设备、方法、计算机可读媒体和处理器，附图中展示本发明的各方面。然而，所述装置、设备、方法、计算机可读媒体和处理器可以许多不同形式实施，且不应解释为限于本文陈述的方面；事实上，提供这些方面使得本揭示内容将是详尽且完整的，且将把本发明的范围完全传达给所属领域的技术人员。此外，在本描述中，相同标号始终表示相同元件。

[0041] 本发明装置、设备、方法、计算机可读媒体和处理器提供存储在可移除数据存储装置中的内容的受保护分布，所述可移除数据存储装置例如磁性媒体、光学媒体、磁带、软盘、硬盘等。举例来说，可移除数据存储装置可采取 CD、DVD、快闪媒体卡等形式。内容（如本文所引用）涵盖可存储在数据存储装置上的可执行或不可执行的任何数字媒体文件、应用程序、例行程序、数据或其它信息。此外，受保护内容（如本文所引用）包括内容的安全和 / 或被遮掩形式，例如可通过对内容加密、散列内容、将内容译成密码等而获得。另外，密钥（如本文所引用）涵盖用以将未受保护内容变换成受保护内容和 / 或将受保护内容变换成未受保护内容的密码机制，例如应用于内容的加密算法、散列、密码、公共密钥、私人密钥、对称密钥等。

[0042] 参看图 1，在一个方面，示意说明一种用于提供内容的受保护分布的系统。所述系统包含可移除数据存储装置 10，例如 CD 10A、DVD 10B、快闪媒体卡 10C 和智能卡 10D。图 1 所示的可移除数据存储装置仅为举例说明，还预期其它可移除数据存储装置且在当前方面的范围内。可移除数据存储装置包含存储器 12，其存储受保护内容 14 和数据存储装置识别符 16。受保护内容是本文中用于表示被保护而免于用户存取的所有内容，通常受保护内容可采取经编码或经译成密码的内容（即，经加密内容）的形式。数据存储装置识别符 16 通常是将所述数据存储装置与其它数据存储装置唯一地区分的数据存储装置序列号或某一其它识别符。

[0043] 可移除数据存储装置 10 正与计算装置 20 进行数据通信。计算装置可包含无线通信装置 20A、无线游戏装置 20B、膝上型计算机 20C 或台式计算机 20D。图 1 所示的计算装置仅为举例说明，还预期其它计算装置且在当前方面的范围内。在许多方面，数据存储装置与计算装置之间的数据通信需要将存储装置可移除地固定在计算装置内。然而，在其它方面，也可能系统经配置使得在存储装置远离计算装置时存储装置与计算装置进行有线或无线数据通信。举例来说，数据存储装置可经配置以经由短程通信，例如经由红外 (IR) 波、Bluetooth® 协议消息、Wi-Fi 技术、Wi-Max 技术等与计算装置通信。

[0044] 计算装置 20 包含计算机平台 22，其提供内容存取起始器模块 24 的执行。内容存取起始器模块包含用于以下操作的可执行指令 ：辨别与计算装置通信的数据存储装置 10 上的受保护内容 14 ；响应于受保护内容的辨别而将数据存储装置识别符 16 传送到网络装置 40 ；响应于识别符 16 的传送从网络装置接收一个或一个以上内容密钥 42 ；以及出于存取内容的目的将所述一个或一个以上密钥应用于受保护内容 14。

[0045] 所述系统还可包含与计算装置 20 进行网络通信的网络装置 40，例如网络服务器。网络装置执行个人化模块 44，其确定数据存储装置识别符 16 与内容密钥 42 之间的关联。一旦个人化模块确定数据存储装置识别符 16 与内容密钥 42 之间的关联，个人化模块就可从网络数据库 46 中检索所述一个或一个以上内容密钥。进而，网络装置 40 可将所述一个或一个以上内容密钥 42 传送到计算装置，计算装置出于将受保护内容转换为用户可存取的未受保护内容的目的将所述一个或一个以上密钥应用于受保护内容 14。图 1 所示的网络装置仅为举例说明，还预期能够联网到计算装置 20 且能够执行个人化模块 44 的任何装置且在当前方面的范围内。如计算装置的功能性所指示，网络装置可与计算装置进行有线通信、无线通信或有线通信与无线通信两者。

[0046] 根据系统方面，图 2 提供用于提供内容的受保护分布的系统的更详细框图。可移

除数据存储装置 10 可包含存储器 12，例如快闪、只读和 / 或随机存取存储器 (RAM 和 ROM)、EPROM、EEPROM 等，其存储受保护内容 14 和数据存储装置识别符 16。如所说明，数据存储装置 10 可存储受保护内容的单一实体，例如第一受保护内容 14A，或数据存储装置可视需要存储多个受保护内容，例如第二受保护内容 14B 和第 n 受保护内容 14C。在其中数据存储装置存储多个受保护内容的方面中，每一受保护内容部分或实体可视需要具有相关联受保护内容部分识别符 18A、18B 和 18C。受保护内容部分识别符可与应用于受保护内容部分以将所述内容转换为未受保护内容的一个或一个以上内容密钥 42 相关联。

[0047] 在一些方面，存储在数据存储装置上的所有内容均可为受保护内容，而在其它方面，数据存储装置可存储额外未受保护内容 15。未受保护内容 15 可以是所有用户在任何时间容易存取的内容。举例来说，未受保护内容可以是媒体播放器应用程序，且受保护内容可以是一个或一个以上媒体文件（例如，音乐文件、视频文件等）。或者，一旦受保护内容已转换为内容，未受保护内容可以是与受保护内容结合使用的文件、应用程序、例行程序等。举例来说，数据存储装置可存储大量应用程序和 / 或媒体资源，其中核心应用程序可受到保护且资源文件可不受保护。一旦已准予对受保护核心应用程序的存取，就认为核心应用程序是可执行的，且可在执行期间利用未受保护的资源文件。

[0048] 在一些方面，未受保护内容 15 可包含存储在存储装置 10 上的受保护内容 14 的预览和 / 或存储和保护于存储装置上或远程存储在网络装置处的额外相关内容的预览，所述额外相关内容例如游戏应用、额外相关音乐或视频文件等的额外版本。在这些方面，未受保护内容可包含出于购买受保护内容和 / 或额外相关内容的目的向用户提供对网络服务器或网站的存取的嵌入式链接。在其中未受保护内容 15 包含受保护内容 14 的预览的方面，数据存储装置可被免费分配给潜在内容买主，未受保护预览内容充当对购买受保护内容的引诱物 (enticement)。在其中未受保护内容是额外相关内容（即，原本不由数据存储装置的买主购买的内容）的预览的其他方面，额外内容可以是存储在数据存储装置上的额外受保护内容，或额外内容可以是在购买后下载到计算装置 20 的远程存储的内容。

[0049] 另外，在一些方面，未受保护内容 15 可包含存储在存储装置 10 上的受保护内容 14 的限制使用，和 / 或存储和保护于存储装置上或远程存储在网络装置处的额外相关内容的限制使用。举例来说，未受保护内容 15 可包含限制使用游戏应用程序、音乐文件、视频文件等。在这些方面，数据存储装置 10 可经配置使得未受保护内容 15 具有限制使用，例如 ：预定有限数目的使用或播放 ；其中未受保护内容可能可用的预定有限的时间周期 ；少于受保护内容的完全功能性的一组预定功能性 ；以及对于完整量的内容的预定有限部分的可存取性。或者，在其它方面，数据存储装置 10 可经配置使得未受保护内容的限制使用与计算装置相关联。举例来说，未受保护音乐文件可限于每计算装置播放两次，因此允许未受保护音乐文件在任何适应的计算装置上至多播放两次。在这些方面，网络装置 40 可通过要求计算装置在初始激活未受保护限制使用内容时将装置识别符传送到网络装置而提供对计算装置的限制使用的跟踪。

[0050] 系统额外包含具有计算机平台 22 的计算装置 20，所述计算机平台 22 可在网络 68 上传输和接收数据，并执行存储在计算装置数据储存库 26 或数据存储装置存储器 12 中的例行程序和应用程序。数据储存库 26 存储内容存取起始器模块 24，其提供由内容存取起始器逻辑 27 执行以进行以下动作的指令 ：辨别由计算装置读取的数据存储装置上的受保护

内容；响应于受保护内容的辨别而将数据存储装置识别符传送到网络装置；响应于识别符的传送从网络装置接收一个或一个以上内容密钥；以及出于存取内容的目的将所述一个或一个以上密钥应用于受保护内容。在其它方面，内容存取起始器模块 24 可作为未受保护内容 15 存储在数据存储装置上。

[0051] 数据储存库 26 通常还可存储计算装置识别符 29。在一些方面，计算装置识别符可经实施以将计算装置与数据存储装置和 / 或内容密钥相关联。

[0052] 数据储存库 26 可包括易失性和非易失性存储器，例如只读和 / 或随机存取存储器 (RAM 和 ROM)、EPROM、EEPROM、快闪卡，或为计算机平台所共有的任何存储器。此外，数据储存库 26 可包含一个或一个以上快闪存储器单元或可以是任何次级或三级存储装置，例如磁性媒体、光学媒体、磁带或软盘或硬盘。

[0053] 此外，计算机平台 22 还包含至少一个处理引擎 28，其可以是专用集成电路 (“ASIC”) 或其它芯片集、处理器、逻辑电路，或其它数据处理装置。处理引擎 28 或其它处理器 (例如，ASIC) 可执行应用程序编程接口 (“API”) 层 30，其与存储在计算装置 20 的数据储存库 26 中或数据存储装置 10 的存储器 12 中的任何常驻或非常驻程序 (例如，内容存取起始器模块 24) 介接。在其中计算装置为无线计算装置的方面，API 30 通常是在计算装置上执行的运行时环境接口。一个此类运行时环境是由美国加州圣地亚哥市 (San Diego，California) 的高通公司 (Qualcomm，Inc.) 开发的 Binary Runtime Environment for Wireless®(BREW®)软件。可利用 (例如) 操作以控制无线计算装置上的应用程序的执行的其它运行时环境。

[0054] 处理引擎 28 通常包含各种处理子系统 32，其实现于硬件、固件、软件及其组合中，并实现计算装置 20 的功能性和计算装置在网络 68 上的可操作性。举例来说，处理子系统 32 允许起始和维持网络通信，并与其它联网装置交换数据。在其中计算装置由无线通信装置实施的一个方面，通信处理引擎 28 可包含处理子系统 32 中的一者或一组合，例如 :例如 : 声音、非易失性存储器、文件系统、传输、接收、搜索器、层 1、层 2、层 3、主控制、远程过程、手持机、功率管理、诊断、数字信号处理器、声码器、消息收发、呼叫管理器、Bluetooth®系统、Bluetooth® LPOS、位置确定、定位引擎、用户接口、休眠、数据服务、安全、验证、USIM/SIM、语音服务、图形、USB、例如 MPEG 的多媒体、GPRS 等。对于所揭示的方面，处理引擎 28 的处理子系统 32 可包含与在计算机平台 22 上执行的应用程序交互的任何子系统组件。举例来说，处理子系统 32 可包含代表内容存取起始器模块 24 从 API 30 接收数据读取和数据写入的任何子系统组件。

[0055] 计算机平台 22 可进一步包含通信模块 34，其实现于硬件、固件、软件及其组合中，并实现计算装置 20 的各个组件之间以及装置 20 与网络 68 之间的通信。通信模块可包含用于建立无线通信连接的必需的硬件、固件、软件和 / 或其组合。

[0056] 另外，计算装置 20 可包含用于产生到无线装置中的输入的输入机制 36 和用于产生供计算装置的用户消耗的信息的输出机制 38。举例来说，输入机制 36 可包含例如键或键盘、鼠标、触摸屏显示器、与语音识别模块相关联的麦克风等机制。此外，举例来说，输出机制 38 可包含显示器、音频扬声器、触觉反馈机制等。

[0057] 所述系统额外包含具有计算平台 48 的网络装置 40，所述计算平台 48 可在网络 68 上传输和接收数据。计算机平台 48 包含处理引擎 50，其能够执行存储在网络装置数据储存

库 52 中或网络数据库 46 中的模块、例行程序和 / 或应用程序。处理引擎 50 可以是专用集成电路 (“ASIC”) 或其它芯片集、处理器、逻辑电路，或其它数据处理装置。网络数据库 46 可驻留在远离网络装置 40 的装置中，或数据库可驻留在网络装置内部。在其中数据库 46 驻留在网络装置 40 内部的方面，数据库可包含在数据储存库 52 内。

[0058] 数据储存库 52 可包括易失性和非易失性存储器，例如只读和 / 或随机存取存储器 (RAM 和 ROM)、EPROM、EEPROM、快闪卡，或计算机平台常见的任何存储器。此外，数据储存库 26 可包含一个或一个以上快闪存储器单元或可以是任何次级或三级存储装置，例如磁性媒体、光学媒体、磁带或软盘或硬盘。数据储存库 52 可包含个人化模块 44，其包含由个人化逻辑 54 利用以进行以下动作的指令 :确定数据存储装置 10 与内容密钥 42 之间的关联。在替代方面，个人化模块 44 还可确定计算装置 20 与数据存储装置 10 之间的关联和 / 或受保护内容部分 18 与内容密钥 42 之间的关联。个人化模块 44 通过评估网络数据库 48 并定位在特定查找表内的关联或某一其它形式的关联元素来确定关联。如此，网络数据库可包含数据存储装置识别符和内容密钥查找表 56，以用于确定数据存储装置 10 与内容密钥 42 之间的关联。在替代方面，网络数据库可包含数据存储装置识别符和计算装置识别符查找表 58，以用于确定数据存储装置 10 与计算装置 20 之间的关联。在另外其它方面，网络数据库可包含受保护内容部分识别符和内容密钥查找表 60，以用于确定受保护内容部分 18 与内容密钥 42 之间的关联。

[0059] 在一些方面，网络数据库还可出于初始将受保护内容下载到数据存储装置和 / 或更新 / 替代数据存储装置上的受保护内容的目的而存储受保护内容 14。举例来说，如果数据存储装置 10 的用户错放、丢失或另外不再拥有数据存储装置，那么用户可能够联系网络装置并基于将计算装置或用户与受保护内容相关联的计算装置识别符或用户识别符来检索受保护内容。

[0060] 另外，网络数据库还可存储个别数据存储装置文件 63，其提供关于受保护内容的参数、设置和其它信息的远程存储。举例来说，如果受保护内容 14 是游戏应用程序，那么数据存储装置文件可存储游戏设置、所达到的游戏级别、中断的游戏等。通过提供文件 63 的远程存储，网络装置可限制计算装置 20 的存储能力，且 / 或充当后备存储装置。举例来说，如果用户不再拥有数据存储装置并要求替代装置或购买初始数据存储装置的更新或新版本，那么网络装置可初始地辨别用户或计算装置并将数据存储装置文件 63 中的设置应用于替代装置、更新装置或新版本 / 后续装置中所发现的内容。

[0061] 网络装置可额外包含监视模块 65，其包含由监视逻辑 67 利用以进行以下动作的指令 :监视计算装置 20 上内容的使用。在此方面，监视模块确认存储在数据存储装置 10 上的内容和由计算装置存取或另外执行的任何其它内容。另外，监视模块可监视计算装置的环境属性，例如无线装置的地理位置、装置的移动、装置的时间点等。对由计算装置存取或使用的内容的监视可通过从计算装置上传日志或另外与计算装置通信来实现。基于存储在数据存储装置上的内容和由计算装置存取或另外执行的任何其它内容，建议逻辑 69 将把对其它类似内容的建议推送到装置，例如类似音乐文件、音频文件、游戏应用程序等。另外，监视模块 65 可使用环境数据来使建议基于计算装置的环境属性，例如装置的位置、时刻等。

[0062] 数据储存库 52 可额外包含通信模块 64，其包含由通信逻辑 66 利用以进行以下动

作的指令：从计算装置接收识别符通信，以及将内容密钥通信传输到计算装置。通信模块64可实现于硬件、固件、软件及其组合中，并且使网络装置40的各个组件之间以及装置40与网络68之间的通信成为可能。通信模块可包含用于建立无线和/或有线通信连接的必需的硬件、固件、软件和/或其组合。

[0063] 在一个方面，提供一种无线网络环境中内容的受保护分布的方法。图3提供说明性无线系统（明确地说，蜂窝式电话系统）的框图。如先前所述，本文揭示的方面不限于无线网络环境且还可实施在有线网络环境中。根据当前方面的网络通信包含（但不限于）将识别符（即，数据存储装置识别符、计算装置识别符和/或受保护内容部分识别符）传送到网络装置，以及将控制密钥从网络装置传送到计算装置。

[0064] 参看图3，在一个方面，计算装置20包括无线通信装置，例如蜂窝式电话。蜂窝式电话系统70可包含经由载波网络76连接到有线网络74的无线网络72。无线通信装置20被制造成具有增加的计算能力，且常可在无线网络72上传送包含语音和数据的包。如之前所描述，这些“智能”无线装置20具有常驻在其本地计算机平台22上的API 30，所述API 30允许软件开发商创建在无线通信装置20上操作并控制装置上的某一功能性的软件应用程序。图3是较充分地说明无线通信网络的组件以及本发明的一个方面的元件的相互关系的代表图。无线网络72仅是示范性的且可包含远程模块（例如无线通信装置20）在空中相互之间通信和/或在无线网络72的组件（包括但不限于无线网络载波和/或服务器）之间通信所凭借的任何系统。

[0065] 在系统70中，网络装置40可在有线网络74（例如，局域网，LAN）上与用于存储内容密钥42和相关联查找表的单独的网络数据库46通信。此外，数据管理服务器78可与网络装置40通信以提供后处理能力、数据流控制等。网络装置40、网络数据库46和数据管理服务器78可与提供蜂窝式电信服务所需的任何其它网络组件一起存在于蜂窝式电话系统70上。网络装置40和/或数据管理服务器78通过数据链路80和82与载波网络76通信，所述数据链路80和82可以是例如因特网、安全LAN、WAN或其它网络等的数据链路。载波网络76控制发送到移动交换中心（“MSC”）84的消息（一般为数据包）。此外，载波网络76通过网络82（例如因特网和/或POTS（“普通老式电话服务”））与MSC 84通信。通常，在网络82中，网络或因特网部分传递数据，而POTS部分传递语音信息。MSC 84可通过另一网络88（例如用于数据传递的数据网络和/或因特网部分以及用于语音信息的POTS部分）而连接到多个基站（“BTS”）86。BTS 86最终通过短消息收发服务（“SMS”）或其它空中方法以无线方式将消息广播到无线通信装置20。

[0066] 图4提供用于向数据存储装置提供受保护内容和数据存储装置与受保护内容密钥的关联的一方面的流程图。主要参看图4，且其次参看图1和2，数据元素200是内容提供商希望保护的内容(i)。如先前所论述，数据可以是提供商存储在数据存储装置上的所有内容，或存储在装置上的内容的任何部分。示范性内容包含（但不限于）音乐文件、视频文件、多媒体文件、可执行文件等。数据元素210是内容加密密钥(CEK)(42)。在所说明的方面，常规加密算法（例如，XOR加密算法）产生导致随机密钥的CEK。可基于所需安全性程度来确定密钥长度，在一些方面，128位的密钥长度可提供必需的安全性。应注意，可用多个密钥对内容进行加密以实现额外安全性。

[0067] 在替代方面，可使用数据存储装置或计算装置的识别符来产生内容加密密钥。在

这些方面，识别符用作加密算法中的“种子”以产生加密密钥。在这些替代方面，可在过程中的另外的阶段，例如在将内容存储在数据存储装置上的时点或在使数据存储装置与计算装置通信的时点，产生加密密钥。在这些替代方面，有可能通过将密钥存储在数据存储装置上或计算装置上而避免对“存储－转发”方法的需要。在其中将密钥存储在数据存储装置上或计算装置上并从数据存储装置或计算装置检索密钥的这些方面，避免了需要后端网络存储和内容密钥的检索，且因此不是过程或系统的必需元素。

[0068] 在事件 220 处，将内容加密密钥传送到网络数据库 (46) 以用于与数据存储装置识别符的后续关联。内容加密密钥可在通信网络上以电子方式传送到网络数据库，或可通过数据输入功能手动地传送密钥。

[0069] 在事件 230 处，将加密密钥 (一或多个)(42) 应用于内容从而产生受保护内容 (14)，即加密内容，且在事件 240 处，将受保护内容 (14) 存储在数据存储装置上。数据元素 250 表示与每一数据存储装置相关联的唯一识别符 (16)，通常是与数据存储装置相关联的序列号等。在装置存储器内将唯一识别符存储为元数据。另外，应注意，事件 240 可视需要包含将未受保护内容 (15) 存储在数据存储装置上。如先前所述，未受保护数据可包含所述受保护内容和 / 或存储在数据存储装置上或远程服务器上的额外受保护内容的预览。另外，在其中未受保护内容包含预览的方面，可为完全内容的存取和 / 或购买提供嵌入式链接。未受保护内容可额外提供存储装置的用户可存取有限使用次数的限制使用内容。

[0070] 在事件 260 处，将数据存储装置识别符连同 CEK 或适当的 CEK 识别符一起传送到网络数据库 (46)，且在事件 270 处，将 CEK(i) 与数据存储装置之间的关联输入到相应的 CEK 和数据存储装置查找表 (56) 中。CEK(i) 与数据存储装置之间的关联由在网络装置处执行且正与网络数据库 (46) 进行网络通信的个人化模块 (44) 实现。

[0071] 在任选事件 280 处，在存储器 (12) 中包含受保护内容 (14) 的数据存储装置 (10) 通过常规销售途径销售或以另外方式投放于商业市场上。在其它方面，数据存储装置可由用户在不发生商业交易的情况下获得，例如在其中数据存储装置不用于商业收益或在无补偿的情况下另外提供给用户的那些情况中。在任选事件 290 处，数据存储装置由用户购买或由用户另外合法获得。举例来说，具有受保护内容的数据存储装置可在商业销售中被购买或被转移给企业的职员。在任选事件 292 处，可通过将销售、获得、转移和 / 或交换交易以及装置识别符传送到网络数据库 (46) 来验证数据存储装置的购买、合法获得、转移和 / 或交换。

[0072] 主要参看图 5，且其次参看图 1 和 2，根据一个方面，一过程包含存储在数据存储装置 (10) 上的受保护内容 (14) 的个人化和内容的后续存取。在事件 400 处，通过使存储装置与计算装置 (20) 通信来激活数据存储装置。在许多方面，计算装置可包含用于接纳和固定例如 CD、DVD、快闪媒体卡等的可移除数据存储装置的插座。然而，在替代方面，计算装置可包含例如 IR 或 Bluetooth® 通信等的短程通信功能性，其允许计算装置在不与存储装置形成物理接触的情况下读取数据。一旦，初始读取数据存储装置，就在计算装置上执行驻留在计算装置上、存储装置上或相关联网络上的受保护存取起始器模块 (24) 以辨别受保护内容。

[0073] 一旦已在计算装置处辨别受保护内容，在事件 410 处，计算装置就将存储装置识别符 (16) 和或者与各个计算装置 (20) 相关联的计算装置识别符 (29) 传送到网络装置 (40)。举例来说，网络装置 (40) 可存在于有线或无线网络中，视需要超出适当防火墙 (90)。

网络装置对存储装置识别符和（任选）计算装置识别符的接收可引起网络装置内个人化模块 (44) 的执行。个人化模块确定数据存储装置识别符、计算装置识别符（如果有的话）与内容密钥之间的关联。如此，在事件 420 处，数据存储装置识别符 (16) 和或者计算装置识别符 (29) 被从网络装置转发到网络数据库 (46)。在不包含计算装置识别符的一些方面，过程可直接进行到事件 440，如下文所论述。然而，在包含计算装置识别符的替代方面，在事件 430 处，个人化模块确定数据存储装置先前是否已与计算装置相关联。（见图 8 和 9，以及将数据存储装置与计算装置相关联和确定关联的详细流程的相关论述）。如果数据存储装置先前未与任何计算装置相关联，或如果其已与和当前计算装置识别符相关联的计算装置相关联，那么过程进行到事件 440。在事件 440 处，利用 CEK 和数据存储装置识别符查找表 (56) 来检索与数据存储装置识别符相关联的内容密钥 (42)。在事件 450 处，从网络数据库检索内容加密密钥并将其传送到网络装置，且在事件 460 处，网络装置将内容加密密钥传送到计算装置。

[0074] 一旦计算装置 (20) 已接收内容加密密钥 (42)，在事件 470 处，计算装置就将加密密钥应用于受保护内容以将内容解密或另外从受保护 / 安全形式转换为未受保护 / 畅行无阻 (in-the-clear) 形式。如此，在事件 470 之后，计算装置能够存取内容的至少选定部分。在事件 480 处，计算装置可将内容加密密钥存储在计算装置存储器的安全部分中。通过将内容密钥存储在计算装置存储器中，计算装置内的数据存储装置的个人化仅需要发生一次。计算装置每次后续使用数据存储装置时可依赖于存储在计算装置存储器中的密钥来进行解密。

[0075] 图 6 和 7 提供根据一个方面用于具有受保护内容的数据存储装置的个人化的过程流程图。主要参看图 6 和 7，且其次参看图 1 和 2，在事件 600 处，将一个或一个以上内容加密密钥 (42) 应用于内容，且在事件 610 处，将内容加密密钥存储在网络数据库 (46) 中。如先前所论述，内容加密密钥可使用常规随机数产生算法而随机产生，或所述密钥可通过使用数据存储装置识别符或计算装置识别符作为随机数产生器 (RNG) 算法中的“种子”而产生。在事件 620 处，将受保护内容（即，加密内容）存储在包含唯一识别符的数据存储装置上。在事件 630 处，将数据存储装置识别符与内容加密密钥相关联，且将识别符与密钥之间的关联存储在网络数据库处。

[0076] 在事件 640 处，希望存取存储在装置上的内容的用户获得数据存储装置。在一些方面，举例来说，数据存储装置可在商业交易中出售。在其它方面，例如在企业中，可将数据存储装置颁发给用户，例如职员或代理商。在将装置转移给用户的购买或其它交易后，可通过将购买确认或转移确认作为获得数据存储在网络数据库处来实现对购买或转移的验证。视需要，在事件 650 处，将获得数据传送到网络数据库并存储在其中。举例来说，在商业销售中，获得数据包括关于销售的信息，例如购买确认或转移确认，其可在销售 / 转移的时点通过自动化手段（例如，经由通信网络）传送到数据库。

[0077] 在事件 660 处，使数据存储装置与计算装置通信，且计算装置试图存取存储在存储装置上的数据。在决策 670 处，作出关于存储装置是否存储未受保护内容的确定。如果数据存储装置存储未受保护内容，那么在事件 680 处，可在计算装置上存取未受保护内容。如果数据存储装置不包含未受保护内容，或在存取未受保护内容之后，那么在事件 690 处，计算装置可辨别受保护内容，并在事件 700 处，建立与网络装置的网络通信。可“无缝地”，

即在装置用户不了解的情况下建立网络通信连接，或计算装置可与要求对于建立网络通信的许可的用户介接，作为提供对受保护内容的存取的手段。

[0078] 一旦已建立连接，在事件 710 处，就将数据存储装置识别符传送到网络装置。在任选决策 720 处，网络装置可确定使用数据存储装置 / 内容的权利是否可通过检验和 / 或验证。举例来说，网络装置可试图确定数据存储装置识别符是否已被置于使用状态，即装置是否已被适当出售或转移给用户，相反情况为（例如）装置被偷窃并正被非法使用或脱离控制与内容相关联的使用权的实体的控制。如果采购无法通过验证，那么在任选事件 730 处，网络装置将购买选项消息发送到计算装置，或将错误 / 拒绝存取消息发送到用户。购买选项消息可通过允许以下操作而允许数据存储装置上内容的超级分布 :第一用户将存储装置递送给第二用户，第二用户接着可通过对权利的专门购买而合法地获得对受保护内容的存取。如果权利可通过验证，那么在决策 740 处，网络装置确定存储装置识别符是否与一个或一个以上密钥相关联。如果确定数据存储装置不与加密密钥相关联，那么在事件 750 处，网络装置将错误 / 拒绝存取消息发送到计算装置。

[0079] 如果确定数据存储装置与一个或一个以上密钥相关联，那么在事件 760 处（参看图 7），从网络数据库中检索密钥，且在事件 770 处，将密钥传送到计算装置。在事件 780 处，将密钥应用于受保护内容以对内容解密（将受保护内容转换为未受保护内容），且在事件 790 处，计算装置准予对内容的存取。在事件 800 处，将密钥存储在计算装置存储器中以用于受保护内容的后续解码。

[0080] 图 8 和 9 提供根据一个方面用于具有受保护内容的数据存储装置的个人化以及所述存储装置到计算装置的个人化的过程流程图。主要参看图 8 和 9，且其次参看图 1 和 2，在事件 900 处，将一个或一个以上内容加密密钥 (42) 应用于内容，且在事件 910 处，将内容加密密钥存储在网络数据库 (46) 中。在事件 920 处，将受保护内容（即，加密内容）存储在包含唯一识别符的数据存储装置上。在事件 930 处，将数据存储装置识别符与内容加密密钥相关联，且将识别符与密钥之间的关联存储在网络数据库处。

[0081] 在事件 940 处，希望存取存储在装置上的内容的用户获得数据存储装置，如上文详细论述（见图 6，事件 640）。视需要，在事件 950 处，将关于数据存储装置的采购的信息传送到网络数据库并存储在其中。

[0082] 在事件 960 处，使数据存储装置与计算装置通信，且计算装置试图存取存储在存储装置上的数据。在决策 970 处，作出关于存储装置是否存储未受保护内容的确定。如果数据存储装置存储未受保护内容，那么在事件 980 处，可在计算装置上存取未受保护内容。如果数据存储装置不包含未受保护内容，或在存取未受保护内容之后，那么在事件 990 处，计算装置可辨别受保护内容，并在事件 1000 处，建立与网络装置的网络通信。可“无缝地”，即在装置用户不了解的情况下建立网络通信连接，或计算装置可与要求对于建立网络通信的许可的用户介接，作为提供对受保护内容的存取的手段。

[0083] 一旦已建立连接，在事件 1010 处，就将数据存储装置识别符和计算装置识别符传送到网络装置。在任选决策 1020 处，网络装置确定用户对于数据存储装置 / 内容的权利是否可通过验证，如上文详细论述（见图 6，事件 720）。如果权利无法通过验证，那么在任选事件 1030 处，网络装置将购买选项消息发送到计算装置，或将错误 / 拒绝存取消息发送到用户。如果权利可通过验证，那么在决策 1040 处，网络装置确定数据存储装置是否与任何

计算装置或预定最大数目的计算装置相关联。如果确定数据存储装置未与计算装置相关联或仍未达到预定最大数目的计算装置，那么在事件 1050 处，网络装置存储计算装置与数据存储装置之间的关联。

[0084] 如果确定数据存储装置与任何计算装置相关联或已达到预定最大数目的计算装置关联，那么在决策 1060 处（参看图 9），网络装置确定数据存储装置是否与当前通信的计算装置相关联。如果确定数据存储装置不与当前通信的计算装置相关联，那么在事件 1070 处，网络装置将购买选项消息或错误 / 拒绝存取消息发送到计算装置。如果确定存储装置与当前通信的计算装置相关联，那么在决策 1080 处，网络装置确定存储装置识别符是否与一个或一个以上密钥相关联。如果确定数据存储装置不与加密密钥相关联，那么在事件 1090 处，网络装置将错误 / 拒绝存取消息发送到计算装置。

[0085] 如果确定数据存储装置与一个或一个以上密钥相关联，那么在事件 1100 处，从网络数据库中检索密钥，且在事件 1110 处，将密钥传送到计算装置。在事件 1120 处，将密钥应用于受保护内容以对内容解密（将受保护内容转换为未受保护内容），且在事件 1130 处，计算装置准予对内容的存取。在事件 1140 处，可将所述一个或一个以上密钥存储在计算装置存储器的安全部分中以用于受保护内容的后续解码。

[0086] 图 10-12 提供根据替代方面用于具有受保护内容的数据存储装置的个人化的过程流程图。在所描述的流程中，数据存储装置包含多个受保护内容部分，每一部分可被个别存取。主要参看图 10-12，且其次参看图 1 和 2，在事件 1200 处，将一个或一个以上内容加密密钥 (42) 应用于每一内容部分，且在事件 1210 处，将内容加密密钥与相应内容部分识别符相关联并将关联存储在网络数据库 (46) 中。在事件 1220 处，将受保护内容部分存储在包含唯一识别符的数据存储装置上。在事件 1230 处，将数据存储装置识别符与内容加密密钥相关联，且将存储装置识别符与内容密钥之间的关联存储在网络数据库处。

[0087] 在事件 1240 处，希望存取存储在装置上的内容的用户获得数据存储装置，如上文详细论述。视需要，在事件 1250 处，将购买确认或转移确认传送到网络数据库并存储在其中。通常在销售 / 转移的时点将关于用户获得数据存储装置的信息通过自动化手段（例如，经由通信网络）传送到数据库。

[0088] 在事件 1260 处，使数据存储装置与计算装置通信，且计算装置试图存取存储在存储装置上的数据。在决策 1270 处，作出关于存储装置是否存储未受保护内容的确定。如果数据存储装置存储未受保护内容，那么在事件 1280 处，可在计算装置上存取未受保护内容。如果数据存储装置不包含未受保护内容，或在存取未受保护内容之后，那么在事件 1290 处，计算装置可辨别受保护内容，并在事件 1300 处，建立与网络装置的网络通信。可“无缝地”，即在装置用户不了解的情况下建立网络通信连接，或计算装置可与要求对于建立网络通信的许可的用户介接，作为提供对受保护内容的存取的手段。

[0089] 一旦已建立连接，在事件 1310 处，就将数据存储装置识别符和第一受保护内容部分识别符传送到网络装置。在任选决策 1320 处，网络装置确定用户对于数据存储装置 / 内容的权利是否可通过验证，如上文详细论述。如果权利无法通过验证，那么在任选事件 1330 处，网络装置将购买选项消息发送到计算装置，或将错误 / 拒绝存取消息发送到用户。如果权利可通过验证，那么在决策 1340 处（参看图 11），网络装置确定存储装置识别符和第一受保护内容部分识别符是否与一个或一个以上密钥相关联。如果确定数据存储装置或内容部

分不与加密密钥相关联，那么在事件 1350 处，网络装置将错误 / 拒绝存取消息发送到计算装置。

[0090] 如果确定数据存储装置和第一受保护内容部分与一个或一个以上预定密钥相关联，那么在事件 1360 处，从网络数据库中检索密钥，且在事件 1370 处，将密钥传送到计算装置。在事件 1380 处，将密钥应用于第一受保护内容部分以对内容的第一部分解密（将受保护内容转换为未受保护内容），且在事件 1390 处，计算装置准予对第一内容部分的存取。在事件 1400 处，可将密钥存储在计算装置存储器的安全部分中以用于第一受保护内容部分的后续解码。

[0091] 在事件 1410 处，计算装置向用户提供询问用户是否希望存取额外受保护内容部分的提示。对额外受保护内容部分的存取可要求用户购买受保护内容部分或另外获得存取额外内容部分的许可。举例来说，额外内容部分可以是与初始音频或视频文件（即，第一受保护内容部分）相关联的额外音频或视频文件、与初始游戏应用程序相关联的额外游戏等级、初始游戏应用程序的额外增强 / 特征等。计算装置可经配置以周期性地或在用户已完成或执行全部初始内容之后提示用户。

[0092] 在事件 1420 处，用户选择存取额外受保护内容部分中的一者或一者以上（本文中稍后称为“第 n”部分），且在一些方面，此选择可要求额外付款。在替代方面，额外受保护部分可经配置以被自动存取而无需提示或选择（即，自动检索并应用密钥）。此类自动存取可以预定间隔或在发生预定事件时发生。

[0093] 在事件 1430 处（参看图 12），在计算装置与网络装置之间建立网络连接。一旦已建立连接，在事件 1440 处，就将数据存储装置识别符和“第 n”受保护内容部分识别符传送到网络装置。在决策 1450 处，网络装置确定存储装置识别符和“第 n”受保护内容部分识别符是否与一个或一个以上密钥相关联。如果确定数据存储装置或内容部分不与加密密钥相关联，那么在事件 1460 处，网络装置将错误 / 拒绝存取消息发送到计算装置。

[0094] 如果确定数据存储装置和“第 n”受保护内容部分与一个或一个以上预定密钥相关联，那么在事件 1470 处，从网络数据库中检索密钥，且在事件 1480 处，将密钥传送到计算装置。在事件 1490 处，将密钥应用于“第 n”受保护内容部分以对内容的“第 n”部分解密（将受保护内容转换为未受保护内容），且在事件 1500 处，计算装置准予对“第 n”内容部分的存取。在事件 1510 处，可将密钥存储在计算装置存储器的安全部分中以用于“第 n”受保护内容部分的后续解码。

[0095] 因此，所描述的方面提供保护媒体内容的分布的方法、装置、设备、计算机可读媒体和处理器。当前方面的简单方法允许对媒体内容加密并存储相关联内容加密密钥，且可在联网数据库处远程地或在数据存储装置存储器内部存取所述内容加密密钥。一旦加密，就通过确定内容加密密钥与数据存储装置标识和（视需要）计算装置标识之间的关联来准予对内容加密密钥的存取。当前方面提供一种通过保护或加密内容的主要或重要部分（例如，可执行程序或音频 / 视频文件）同时允许内容的次要或较不重要部分保持不受保护来保护数据存储装置上的大量媒体内容的方法。

[0096] 结合本文所揭示的实施例而描述的各种说明性逻辑、逻辑区块、模块和电路可用通用处理器、数字信号处理器 (DSP)、专用集成电路 (ASIC)、现场可编程门阵列 (FPGA) 或其它可编程逻辑组件、离散门或晶体管逻辑、离散硬件组件或经设计以执行本文所描述的功

能的其任何组合来实施或执行。通用处理器可以是微处理器，但在替代实施例中，处理器可以是任何常规处理器、控制器、微控制器或状态机。处理器也可实施为计算装置的组合，例如 DSP 与微处理器的组合、多个微处理器、结合 DSP 核心的一个或一个以上微处理器，或任何其它此类配置。

[0097] 此外，结合本文所揭示的实施例而描述的方法或算法的步骤可直接在硬件中、由处理器执行的软件模块中或所述两者的组合中实施。软件模块可常驻在 RAM 存储器、快闪存储器、ROM 存储器、EPROM 存储器、EEPROM 存储器、寄存器、硬盘、活动磁盘、CD-ROM 或此项技术中已知的任何其它形式的存储媒体中。示范性存储媒体耦合到处理器，使得处理器可从存储媒体读取信息并向存储媒体写入信息。在替代实施例中，存储媒体可与处理器形成一体。处理器和存储媒体可驻留在 ASIC 中。ASIC 可驻留在用户终端中。在替代实施例中，处理器和存储媒体可作为离散组件而驻留在用户终端中。

[0098] 虽然以上揭示内容展示说明性方面和 / 或实施例，但应注意，可在不脱离所附权利要求书所界定的所描述方面和 / 或实施例的范围的情况下在本文中作出各种变化和修改。此外，尽管可能以单数形式描述或主张所描述的实施例的元件，但除非明确规定限于单数形式，否则也预期复数形式。另外，除非另外规定，否则任何方面和 / 或实施例的全部或一部分可与任何其它方面和 / 或实施例的全部或一部分一起利用。

[0099] 因此，得到以上描述和相关联图式中呈现的教示的益处的本发明所属领域的技术人员可了解本发明的许多修改和其它实施例。因此，应了解，本发明不限于所揭示的特定实施例，且希望修改和其它实施例包含在所附权利要求书的范围内。尽管本文中使用特定术语，但其仅在一般和描述性意义上使用而不用于限制的目的。

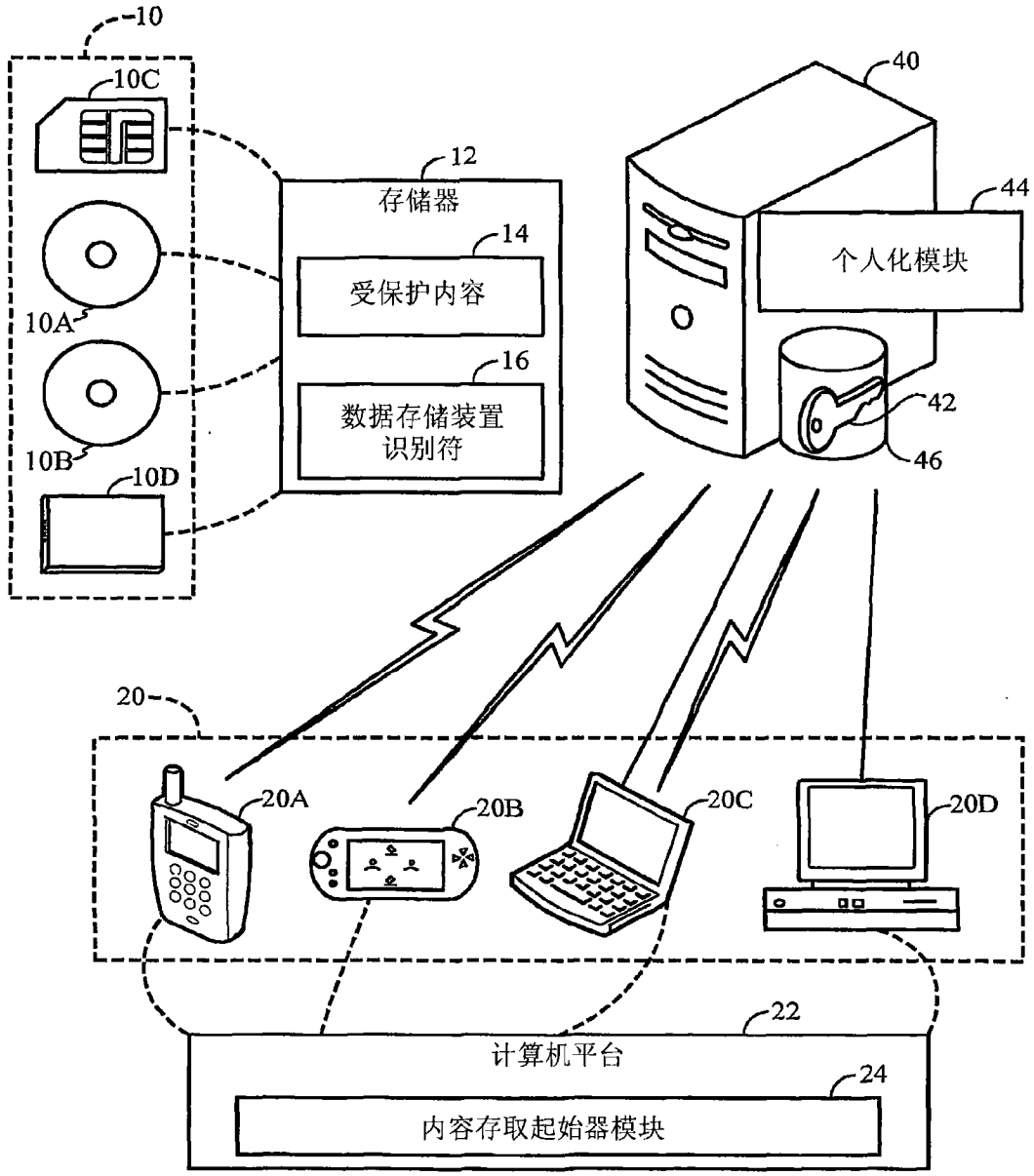

10
10C
10A
10B
10D
12
存储器
14
受保护内容
16
数据存储装置
识别符
40
44
个人化模块
42
46
20
20A
20B
20C
20D
22
计算机平台
24
内容存取起始器模块

图 1

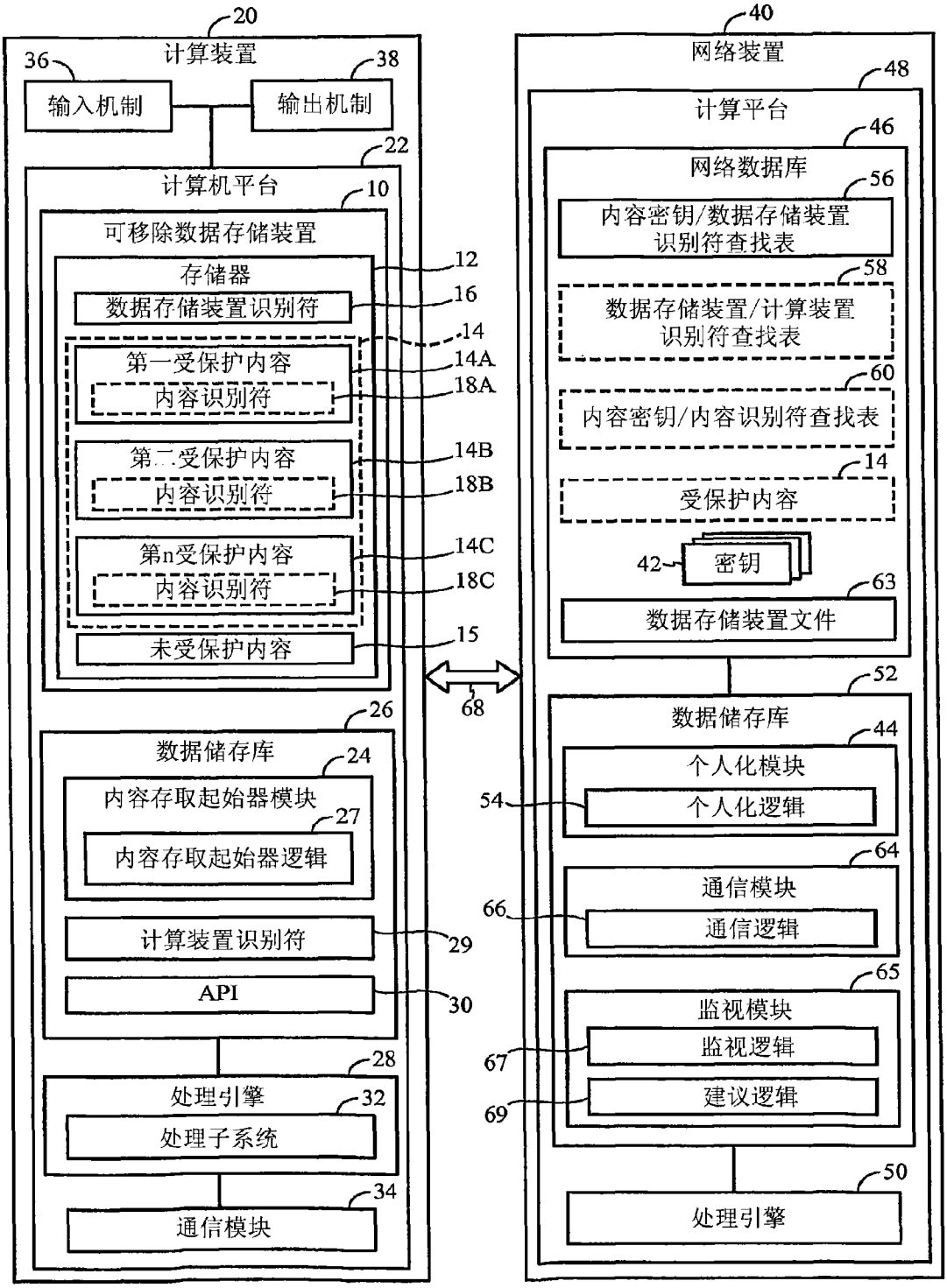

20
计算装置
36
输入机制
38
输出机制
22
计算机平台
10
可移除数据存储装置
存储器
12
数据存储装置识别符
16
14
第一受保护内容
14A
内容识别符
18A
第二受保护内容
14B
内容识别符
18B
第n受保护内容
14C
内容识别符
18C
未受保护内容
15
68
26
数据储存库
24
内容存取起始器模块
27
内容存取起始器逻辑
计算装置识别符
29
API
30
28
处理引擎
32
处理子系统
34
通信模块
40
网络装置
48
计算平台
46
网络数据库
56
内容密钥/数据存储装置识别符查找表
58
数据存储装置/计算装置识别符查找表
60
内容密钥/内容识别符查找表
14
受保护内容
42
密钥
63
数据存储装置文件
52
数据储存库
44
个人化模块
54
个人化逻辑
64
通信模块
66
通信逻辑
65
监视模块
67
监视逻辑
69
建议逻辑
50
处理引擎

图 2

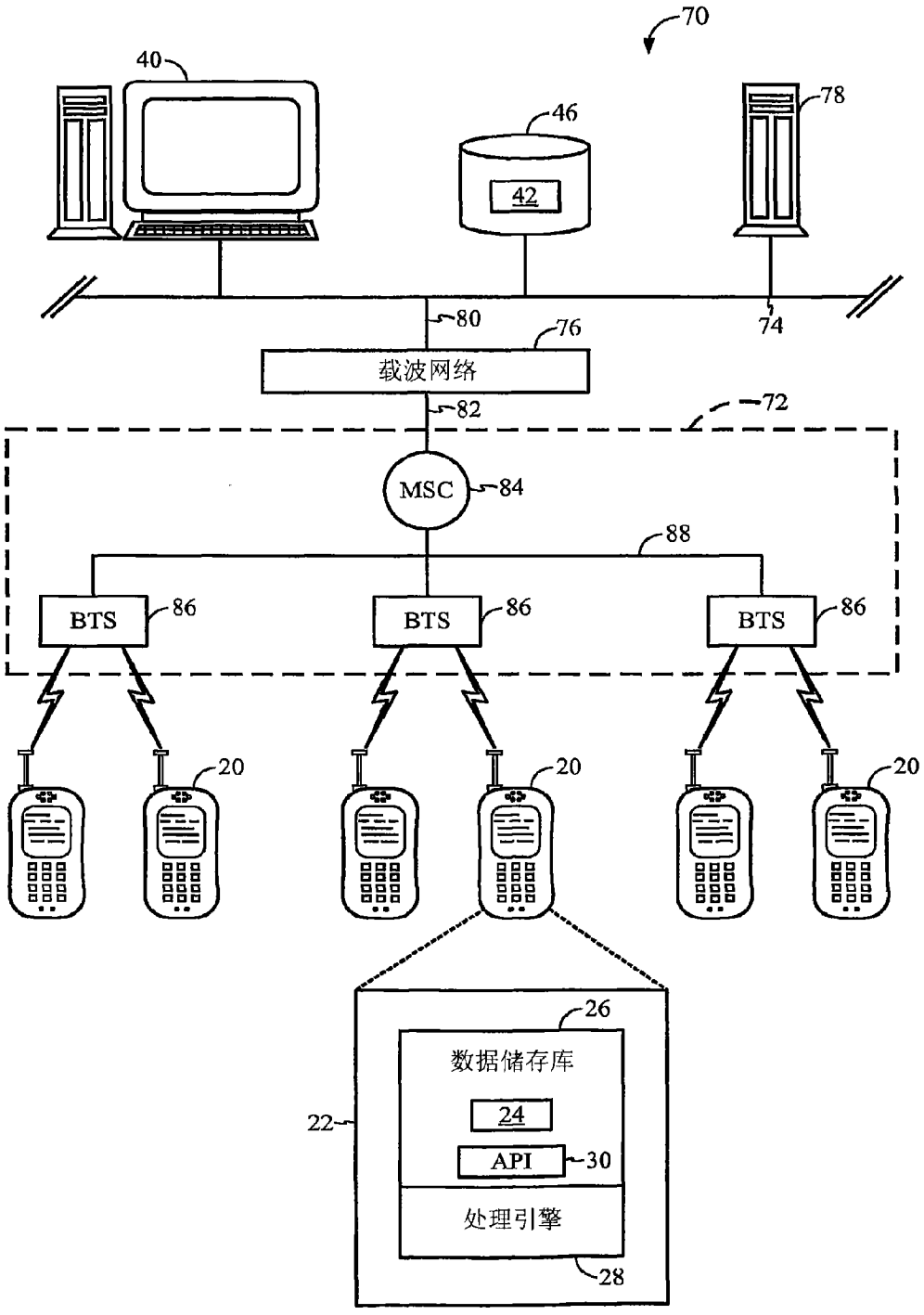

70
40
46
42
78
80
76
74
载波网络
82
72
MSC
84
88
BTS
86
BTS
86
BTS
86
20
20
20
26
数据储存库
24
22
API
30
处理引擎
28

图 3

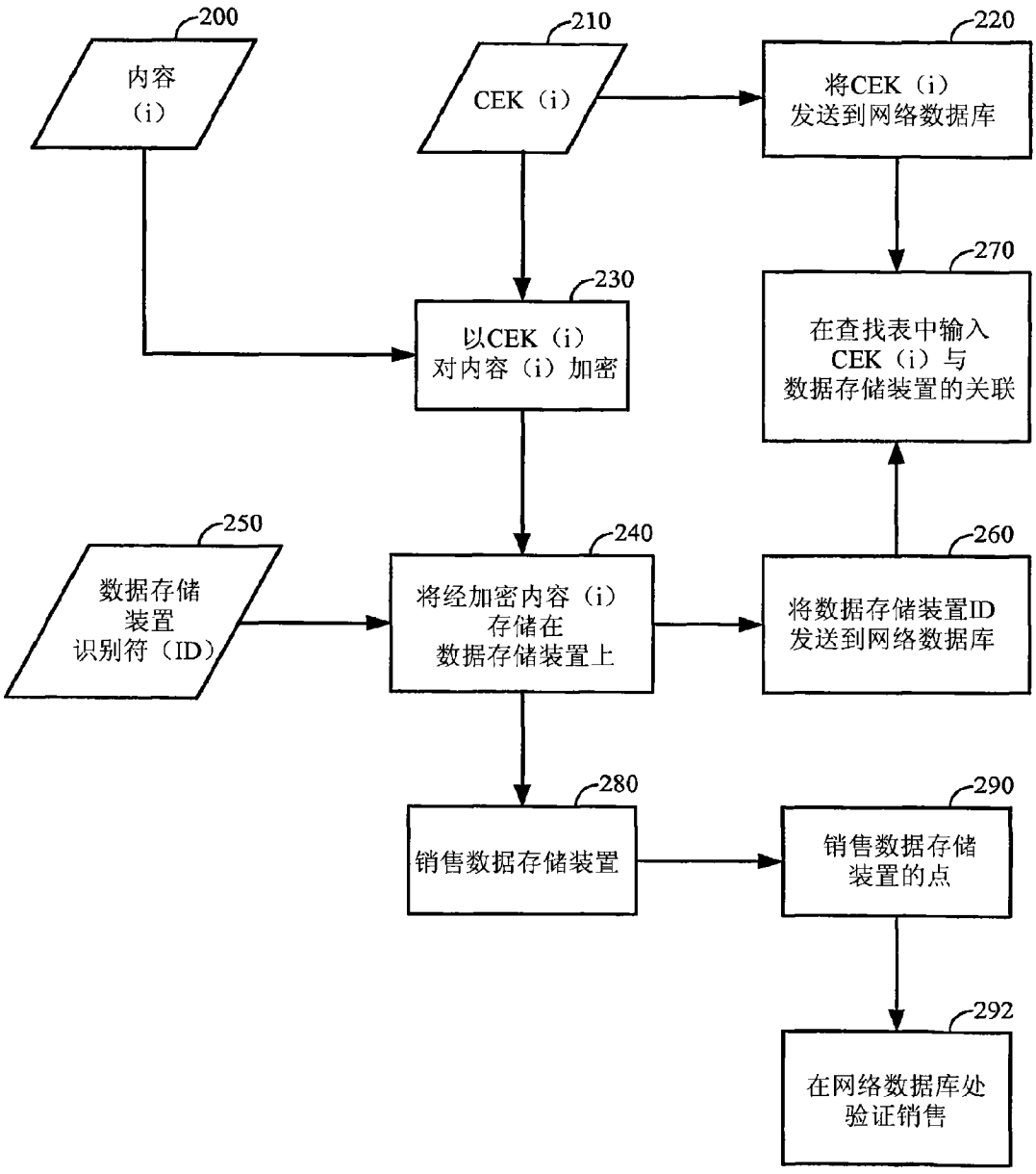

200
内容
(i)
210
CEK (i)
220
将CEK (i)
发送到网络数据库
270
在查找表中输入
CEK (i) 与
数据存储装置的关联
230
以CEK (i)
对内容 (i) 加密
250
数据存储
装置
识别符 (ID)
240
将经加密内容 (i)
存储在
数据存储装置上
260
将数据存储装置ID
发送到网络数据库
280
销售数据存储装置
290
销售数据存储
装置的点
292
在网络数据库处
验证销售

图 4

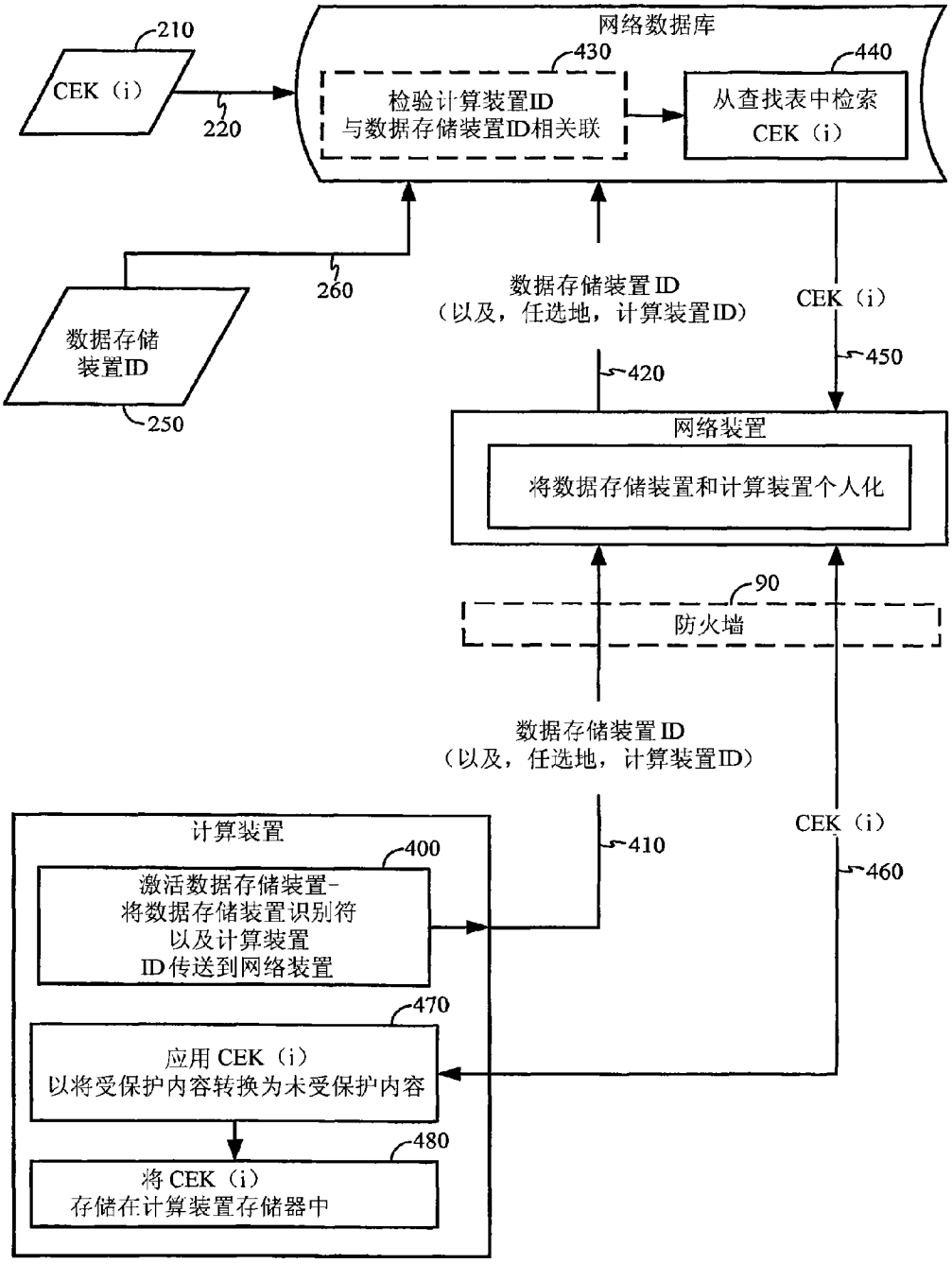

网络数据库
210
CEK（i）
220
430
检验计算装置ID
与数据存储装置ID相关联
440
从查找表中检索
CEK（i）
260
数据存储
装置ID
250
数据存储装置ID
（以及，任选地，计算装置ID）
CEK（i）
450
420
网络装置
将数据存储装置和计算装置个人化
90
防火墙
数据存储装置ID
（以及，任选地，计算装置ID）
CEK（i）
460
410
计算装置
400
激活数据存储装置-
将数据存储装置识别符
以及计算装置
ID传送到网络装置
470
应用 CEK（i）
以将受保护内容转换为未受保护内容
480
将 CEK（i）
存储在计算装置存储器中

图 5

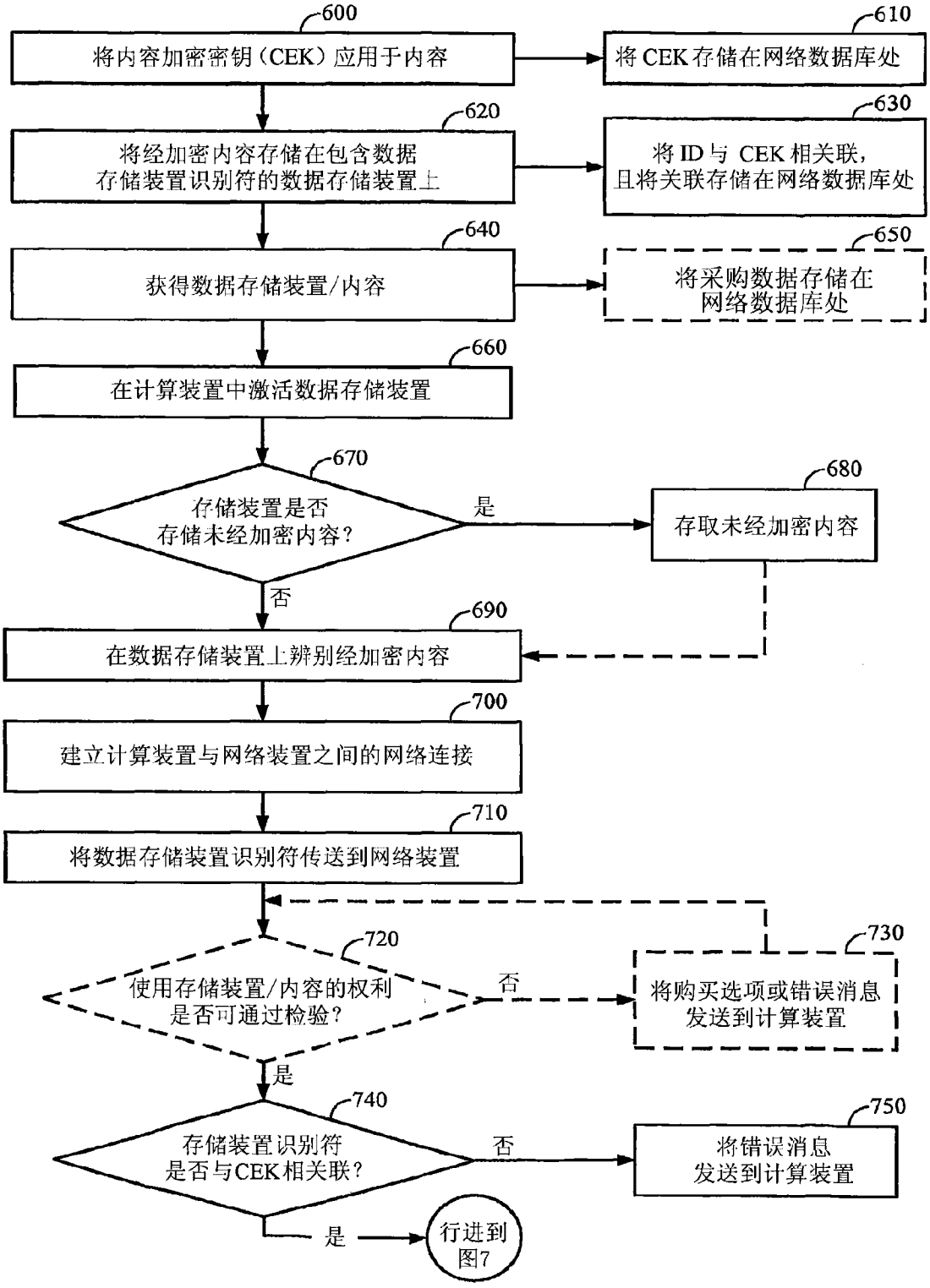

600
将内容加密密钥（CEK）应用于内容
610
将CEK存储在网络数据库处
620
将经加密内容存储在包含数据存储装置识别符的数据存储装置上
630
将ID与CEK相关联，且将关联存储在网络数据库处
640
获得数据存储装置/内容
650
将采购数据存储在网络数据库处
660
在计算装置中激活数据存储装置
670
存储装置是否存储未经加密内容？
是
680
存取未经加密内容
否
690
在数据存储装置上辨别经加密内容
700
建立计算装置与网络装置之间的网络连接
710
将数据存储装置识别符传送到网络装置
720
使用存储装置/内容的权利是否可通过检验？
否
730
将购买选项或错误消息发送到计算装置
是
740
存储装置识别符是否与CEK相关联？
否
750
将错误消息发送到计算装置
是
行进到图7

图 6

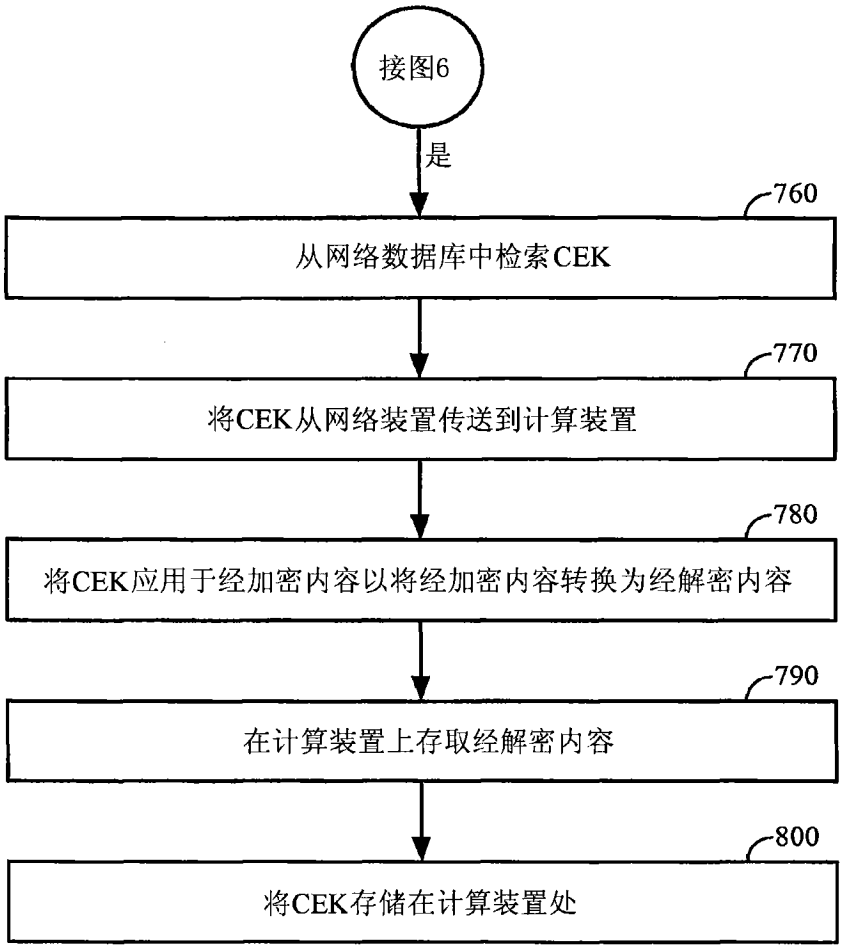

接图6
是
760
从网络数据库中检索CEK
770
将CEK从网络装置传送到计算装置
780
将CEK应用于经加密内容以将经加密内容转换为经解密内容
790
在计算装置上存取经解密内容
800
将CEK存储在计算装置处

图 7

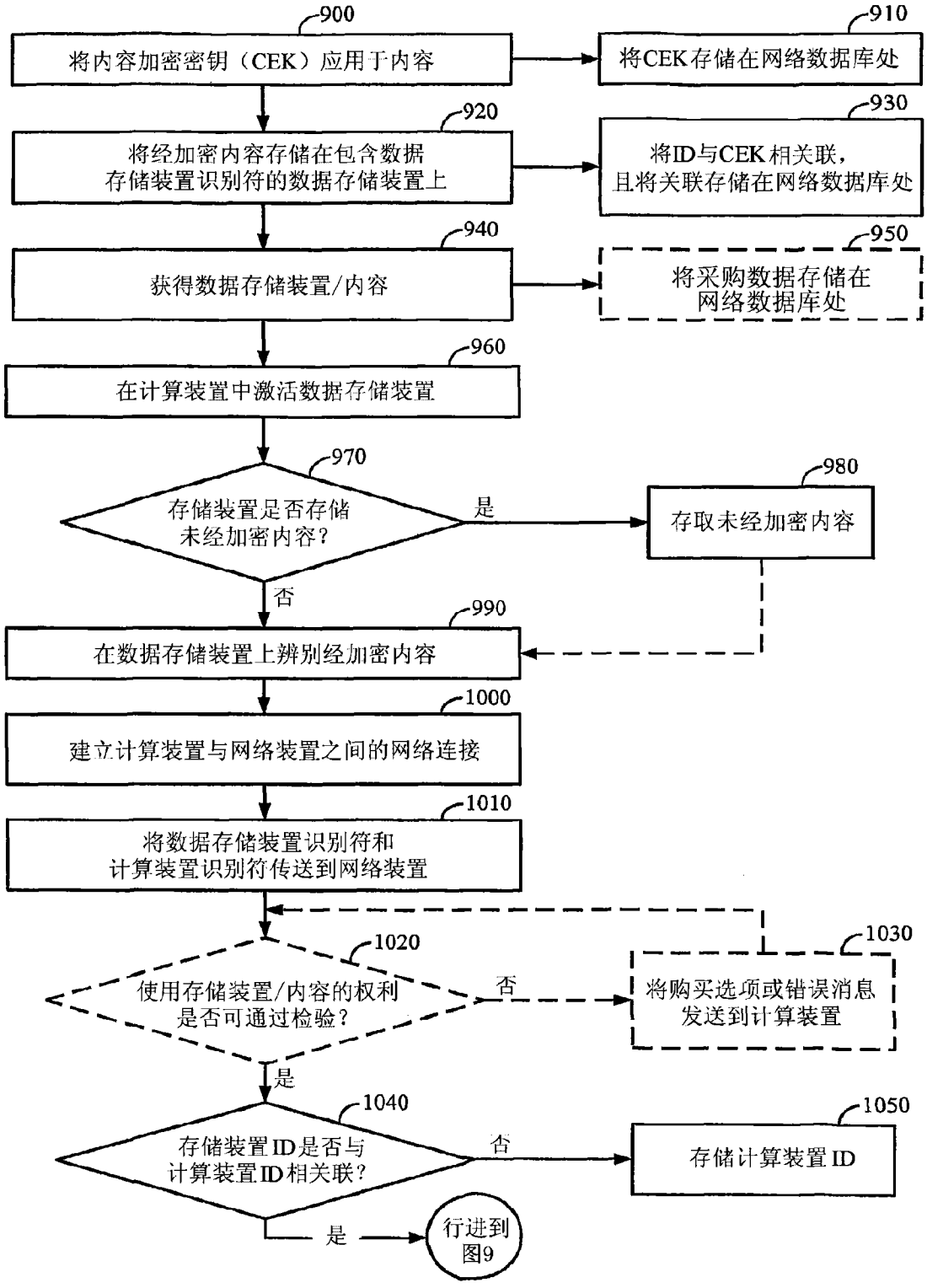

900
将内容加密密钥（CEK）应用于内容
910
将CEK存储在网络数据库处
920
将经加密内容存储在包含数据存储装置识别符的数据存储装置上
930
将ID与CEK相关联，且将关联存储在网络数据库处
940
获得数据存储装置/内容
950
将采购数据存储在网络数据库处
960
在计算装置中激活数据存储装置
970
存储装置是否存储未经加密内容？
是
980
存取未经加密内容
否
990
在数据存储装置上辨别经加密内容
1000
建立计算装置与网络装置之间的网络连接
1010
将数据存储装置识别符和计算装置识别符传送到网络装置
1020
使用存储装置/内容的权利是否可通过检验？
否
1030
将购买选项或错误消息发送到计算装置
是
1040
存储装置ID是否与计算装置ID相关联？
否
1050
存储计算装置ID
是
行进到图9

图 8

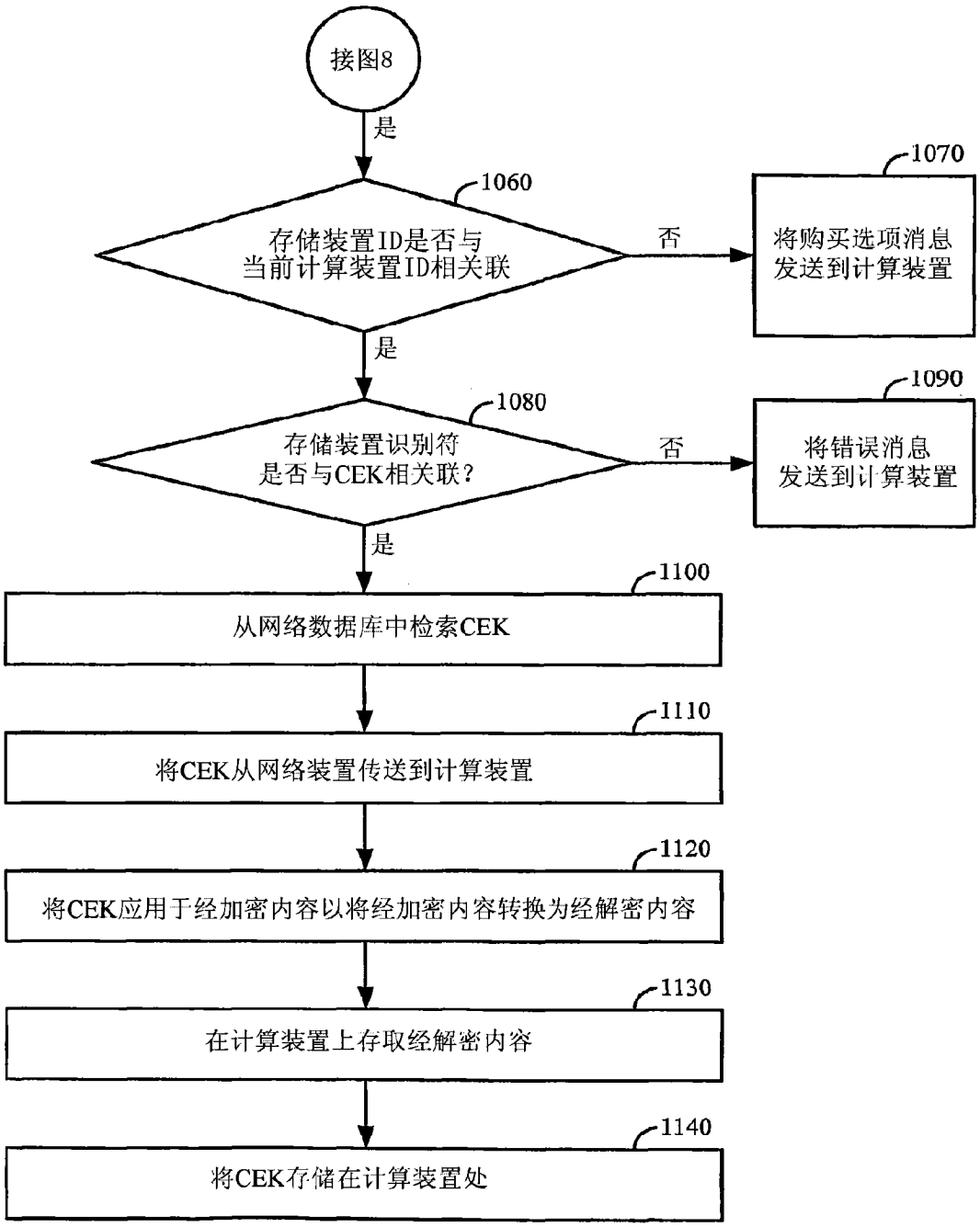

接图8
是
1060
存储装置ID是否与
当前计算装置ID相关联
否
1070
将购买选项消息
发送到计算装置
是
1080
存储装置识别符
是否与CEK相关联?
否
1090
将错误消息
发送到计算装置
是
1100
从网络数据库中检索CEK
1110
将CEK从网络装置传送到计算装置
1120
将CEK应用于经加密内容以将经加密内容转换为经解密内容
1130
在计算装置上存取经解密内容
1140
将CEK存储在计算装置处

图 9

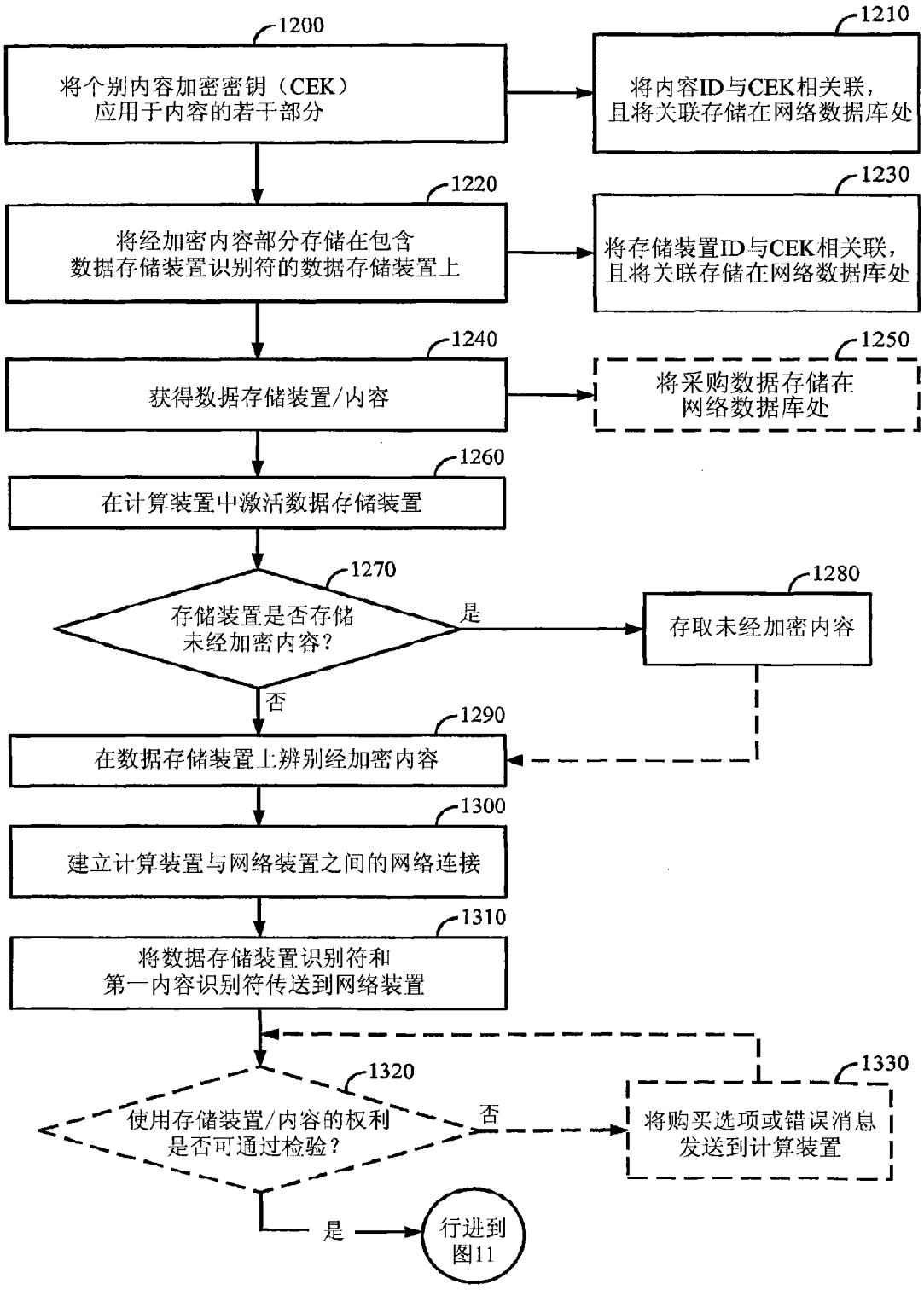

1200
将个别内容加密密钥（CEK）应用于内容的若干部分
1210
将内容ID与CEK相关联，且将关联存储在网络数据库处
1220
将经加密内容部分存储在包含数据存储装置识别符的数据存储装置上
1230
将存储装置ID与CEK相关联，且将关联存储在网络数据库处
1240
获得数据存储装置/内容
1250
将采购数据存储在网络数据库处
1260
在计算装置中激活数据存储装置
1270
存储装置是否存储未经加密内容？
是
1280
存取未经加密内容
否
1290
在数据存储装置上辨别经加密内容
1300
建立计算装置与网络装置之间的网络连接
1310
将数据存储装置识别符和第一内容识别符传送到网络装置
1320
使用存储装置/内容的权利是否可通过检验？
否
1330
将购买选项或错误消息发送到计算装置
是
行进到图11

图 10

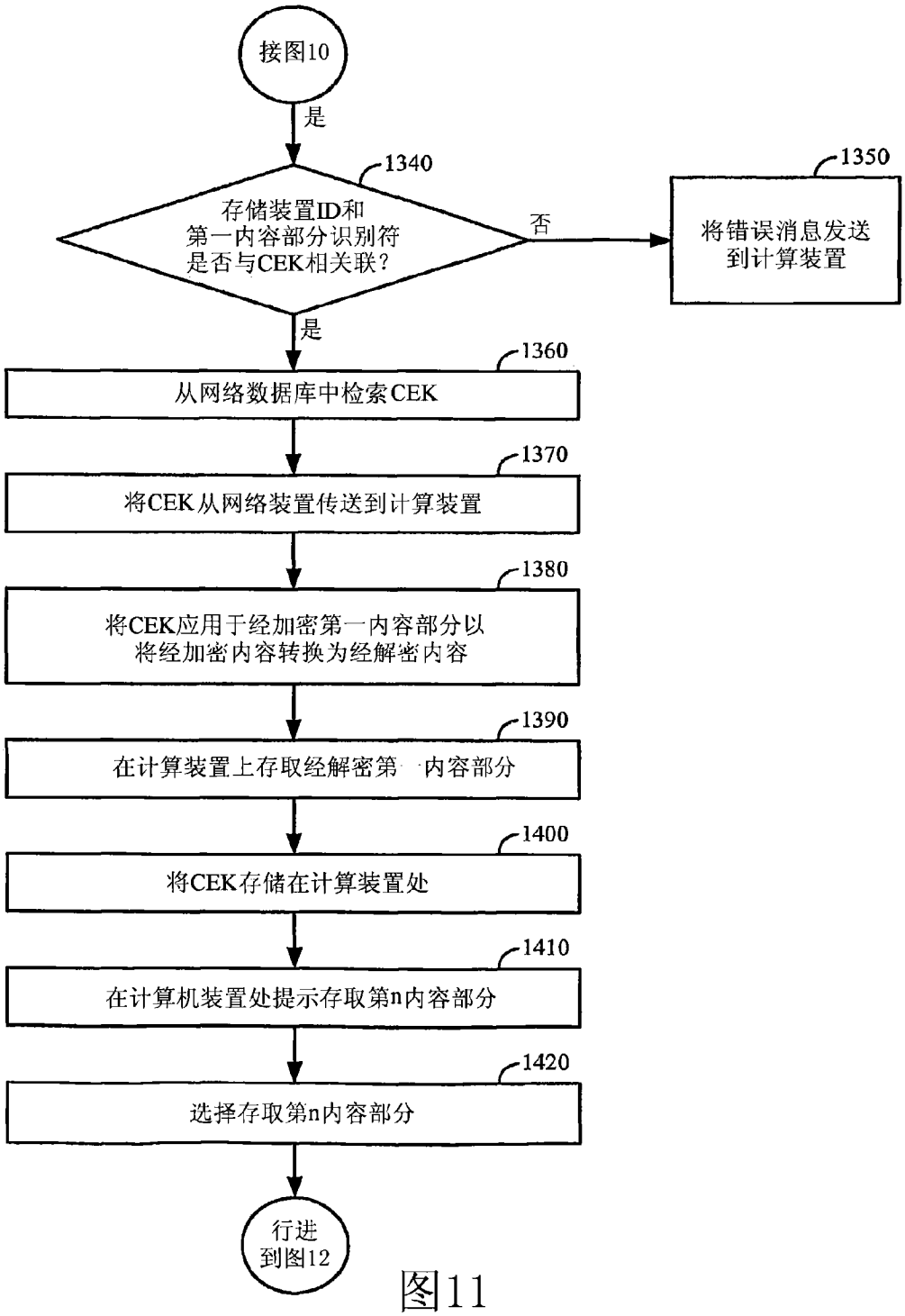

接图10
是
1340
存储装置ID和
第一内容部分识别符
是否与CEK相关联?
否
1350
将错误消息发送
到计算装置
是
1360
从网络数据库中检索CEK
1370
将CEK从网络装置传送到计算装置
1380
将CEK应用于经加密第一内容部分以
将经加密内容转换为经解密内容
1390
在计算装置上存取经解密第 内容部分
1400
将CEK存储在计算装置处
1410
在计算机装置处提示存取第n内容部分
1420
选择存取第n内容部分
行进
到图12

图11

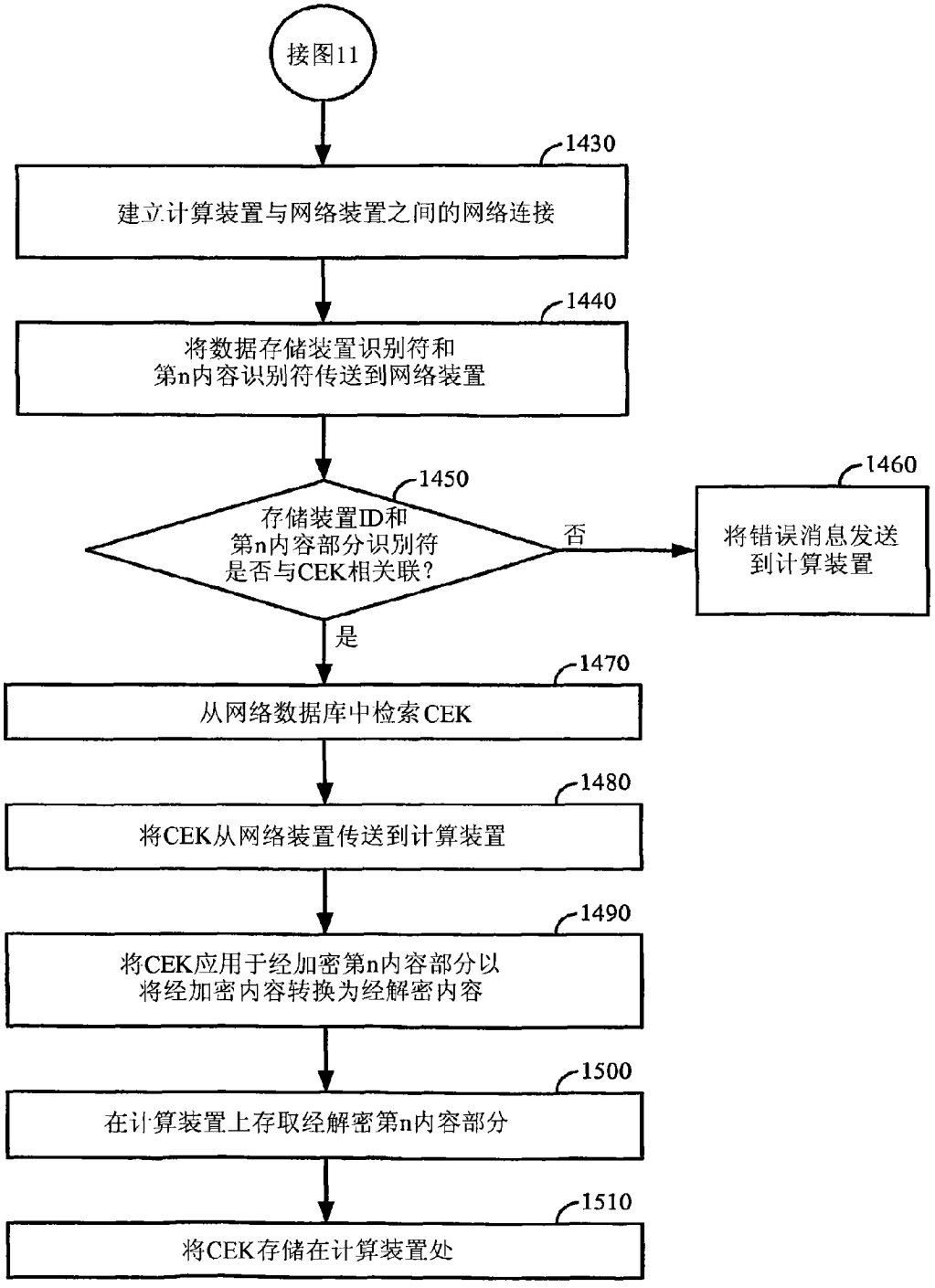

接图11
1430
建立计算装置与网络装置之间的网络连接
1440
将数据存储装置识别符和
第n内容识别符传送到网络装置
1450
存储装置ID和
第n内容部分识别符
是否与CEK相关联?
否
1460
将错误消息发送
到计算装置
是
1470
从网络数据库中检索CEK
1480
将CEK从网络装置传送到计算装置
1490
将CEK应用于经加密第n内容部分以
将经加密内容转换为经解密内容
1500
在计算装置上存取经解密第n内容部分
1510
将CEK存储在计算装置处

图 12