(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 103597488 B
(45)授权公告日 2016.08.24

(21)申请号 201280028593.1

(22)申请日 2012.04.11

(30)优先权数据
61/474212 2011.04.11 US

(85)PCT国际申请进入国家阶段日
2013.12.11

(86)PCT国际申请的申请数据
PCT/US2012/033150 2012.04.11

(87)PCT国际申请的公布数据
WO2012/142178 EN 2012.10.18

(73)专利权人 英特托拉斯技术公司
地址 美国加利福尼亚州

(72)发明人 W.K.凯里 J.尼尔森

(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 蒋骏 马永利

(51)Int.Cl.
G06F 21/10(2013.01)

(56)对比文件
CN 100536559 C,2009.09.02,
CN 1607762 A,2005.04.20,
CN 101216871 A,2008.07.09,
CN 1613255 A,2005.05.04,
CN 1116803 A,1996.02.14,
US 2000/3182235 A1,2003.09.25,
US 2006/0174194 A1,2006.08.03,
US 2002/0010679 A1,2002.01.24,
EP 1724699 A1,2006.11.22,
US 2009/0112867 A1,2009.04.30,
US 2009/0031038 A1,2009.01.29,

审查员 王慧敏

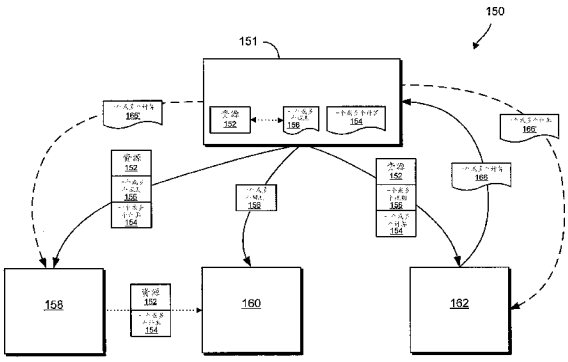
权利要求书2页 说明书18页 附图5页

(54)发明名称

信息安全系统和方法

(57)摘要

提供了用于管理派生的电子资源的系统和方法。在一个实施例中，数字资源与一个或多个规则和一个或多个计算的组相关联，其中所述规则对应于用于访问所述数字资源的一个或多个条件，以及所述计算对所述数字资源进行操作以便提供与所述数字资源不同的数字资源的特定视图。



CN 103597488 B

1.一种用于管理数字资源的使用的系统，所述系统包括：

打包引擎，其被设置成打包所述数字资源，其中所述打包引擎被设置成将一个或多个规则与所述数字资源相关联，以及将一个或多个计算的组与所述数字资源相关联，所述规则对应于用于访问数字资源的一个或多个条件，所述计算包括计算机可读指令，所述计算机可读指令对所述数字资源进行操作以便提供与所述数字资源不同的数字资源的特定视图；

最终用户装置，其可操作来检索和渲染所述数字资源，其中所述用户装置包括数字版权管理引擎，其被设置为评估与所述数字资源相关联的规则并且实施其中的条款，以及利用所述计算机可读指令来对所述数字资源进行操作以便提供对所述数字资源的派生物的访问，

其中所述计算当被应用于所述数字资源时，产生所述数字资源的有限视图，不可能从所述数字资源的有限视图重新创建所述数字资源。

2.权利要求1的系统，其中与所述数字资源相关联的至少一个计算与给定用户相关联，以便通过要求在将所述数字资源中所包含的信息展现给所述用户之前对所述数字资源应用计算，来限制所述用户对所述信息的访问。

3.权利要求2的系统，其中至少一个计算与用户组而非个别用户相关联。

4.权利要求2的系统，其中其视图被计算所限制的实体是非人主体。

5.权利要求3的系统，其中通过明确列出计算所适用于的用户来指定所述用户组。

6.权利要求3的系统，其中通过提供为所述用户组所共有的属性来指定所述用户组，使得所述计算对于所述属性所适用于的任何用户是必需的。

7.权利要求1的系统，其中所计算的有限视图取决于用户、用户组或计算所适用于的其他主体。

8.权利要求1的系统，其中至少一个计算结合了随机或伪随机信息以便隐藏初始资源。

9.权利要求8的系统，其中用于隐藏数字资源的所述伪随机信息是基于一组确定性的种子信息。

10.权利要求9的系统，其中用于生成所述伪随机信息的确定性种子信息与给定的主体相关联，使得相同主体总是接收所述数字资源的相同隐藏视图。

11.权利要求1的系统，进一步包括：

用于接收用于将新的计算组与所述数字资源相关联的请求的装置。

12.权利要求11的系统，进一步包括：

用于批准用于将所述新的计算组与所述数字资源相关联的请求的装置。

13.权利要求1的系统，进一步包括：

用于使用密码技术来将计算与所述数字资源相关联的装置。

14.权利要求13的系统，其中通过创建数字签名的文档来做出关联，所述文档由数字资源的唯一表示和要与所述数字资源相关联的计算的唯一表示的配对构成。

15.权利要求14的系统，其中所述数字资源的唯一表示是应用单向函数的结果。

16.权利要求15的系统，其中所述单向函数包括SHA-1散列函数。

17.权利要求14的系统，其中所述数字资源的唯一表示是与所述数字资源相关联的唯一标识符。

18.权利要求17的系统，其中与所述数字资源相关联的唯一标识符由信任的第三方所分配。

19.权利要求18的系统，其中，通过对包含所述标识符和所述数字资源两者，或所述数字资源的表示的文档进行数字签名，信任的第三方已经做出所述唯一标识符与所述数字资源之间的关联。

20.权利要求14的系统，其中要与所述数字资源相关联的计算的表示是以机器可读格式表达的计算本身。

21.权利要求14的系统，其中要与所述数字资源相关联的计算的表示是对所述计算的机器可读表示应用单向函数的结果。

22.权利要求14的系统，其中要与所述数字资源相关联的计算的表示是与所述计算相关联的唯一标识符。

23.权利要求22的系统，其中与所述计算相关联的所述唯一标识符由信任的第三方所分配。

24.权利要求23的系统，其中，通过对包含所述标识符和所述计算两者，或所述计算的表示的文档进行数字签名，所述信任的第三方已经做出所述唯一标识符与所述计算之间的关联。

25.权利要求13的系统，其中，通过将计算的机器可读表示在被用于将规则与数字资源相关联的相同安全包中进行打包，所述计算与所述数字资源以密码方式相关联。

信息安全系统和方法

[0001] 对相关申请的交叉引用

[0002] 本申请要求2011年4月11日提交的临时申请号61/474,212的优先权的权益,其通过引用整体地结合于本文中。

[0003] 提出用于促进信息内容的安全、持久的管理的系统和方法。将理解的是,如其中采用的许多部件、系统和方法那样,这些系统和方法是新的。

附图说明

[0004] 通过连同附图一起参考下列详细描述,将容易地理解本发明的主题,其中:

[0005] 图1A示出了用于分配派生资源的说明性系统。

[0006] 图1B示出了用于提供对派生资源的访问的说明性系统。

[0007] 图2示出了根据一个实施例的对资源运行的计算的示例。

[0008] 图3示出了用于管理电子资源的说明性系统。

[0009] 图4示出了可被用来实践本发明的主题的实施例的系统的更详细示例。

具体实施方式

[0010] 本发明的主题的详细描述被提供如下。虽然描述了若干个实施例,但应理解的是,本发明的主题并不局限于任何一个实施例,而是涵盖了大量的替代、修改和等同方式。此外,虽然下列描述中阐述了许多具体细节以便提供对本发明的主题的透彻理解,但在没有一些或所有这些细节的情况下,可以实践一些实施例。此外,为了清楚起见,现有技术中已知的某些技术材料尚未被详细描述,以便避免不必要地模糊本发明的主题。

[0011] 提出用于促进信息内容的安全、持续的管理的系统和方法。将理解的是,如其中采用的许多元件、系统和方法那样,这些系统和方法是新的。

[0012] 数字版权管理("DRM")系统通常使用加密来将资源与用于管理对该资源的访问的一组规则持久关联。在很多情况下,要被保护的资源为一块数字内容,例如电子书、视听流或视频游戏。为了访问资源,用户可能需要指示将要执行的动作,这随后触发了为该特定动作管理资源的规则的评估。如果在规则下允许该动作,则DRM系统提供对资源的访问,如其被初始打包的那样。此类型的资源可以被认为是"静态"的,因为它以其中将其初始打包的形式被呈现给用户(虽然可能首先需要应用资源使用中实际上隐含的解码、解压缩或其他计算)。

[0013] 一些DRM系统能够选择用于访问的一部分资源。例如,有DRM功能的视频播放器可提供对单个视频轨道的访问,即使多个轨道被编码在一个文件中。规则评估引擎通常允许用户指定资源的哪个子集将要被访问。也已经存在一些努力来根据商业模式提供打包资源的不同视图。例如,有可能利用MPEG-4 SVC编码方案集成DRM系统,以允许根据为对视频的访问所支付的价格来对视频进行更低或更高分辨率的访问。然而,在这两种情况下,资源及其所有可能的变体是被预先计算和数字签名的,使得它们不能被修改。

[0014] 静态资源(或其中的部分)如它们被打包器所编码的那样被精确地呈现给用户。与

此相反，派生的资源是在呈现给用户之前通过计算（通常但不必然，在消费点处执行）而从初始资源所计算的资源。

[0015] 在一个优选的实施例中，产生派生资源的计算被表达为用于在初始资源上操作以产生初始资源的特定视图的计算机可读指令。在一些实施例中，虽然计算可涉及数学计算的使用，但如这里所使用的术语“计算”并不被如此限制，而是涵盖用于产生初始资源的特定呈现（例如不公开初始资源中所有信息的呈现）的指令、程序、方法或其他机制的任何集合。例如，如果初始资源是“姓名-出生日期-身高”三联体（triplet）的列表，则计算的示例将是命令渲染应用来仅显示“出生日期-身高”对的列表的任何合适方式（即从显示中省略“姓名”数据）。计算的另一示例将是一组指令，这些指令将对被设置成生成用于显示的中间身高和平均身高的初始数据进行操作。

[0016] 可以按照各种方式来指定计算，其示例包括但不限于下列中的一些或全部：

[0017] ●它们可在由初始打包器（首先加密资源的实体）打包的时刻被关联。

[0018] ●它们可在打包后被产生，且与资源安全地关联。这些事后计算可由数据的打包器所创建，或者，在一些实施例中，由希望在受保护资源上运行的计算的第三方所创建。

[0019] 在一些实施例中，资源可以在无任何相关联计算的情况下被保护。在一些实施例中，DRM系统可被设计为仅根据它们相关联的计算来访问派生资源（例如，打包的或以其他方式同样标识的资源）。在这样的实施例中，如果不存在与资源相关联的计算，将有效地防止访问。在其他实施例中，资源可在默认情况下为可访问的，除非被相关联的规则所禁止。在这样的实施例中，如果不存在与资源相关联的计算，资源将是可访问的（根据任何相关联的规则），除非为了授权对资源的访问，与资源相关联的规则需要拥有一个或多个计算。

[0020] 派生资源在其中对资源的访问应当依赖例如下列的因素的情况下尤其有用：将执行动作的原则、规则评估点处的环境考虑（例如计算能力）、由DRM系统所管理的状态变量（例如支付状态）、已经揭示的关于资源的信息量，等等。在这些情况下，目标通常是可能基于评估点处的情境来提供对初始资源的派生物的访问。

[0021] 派生资源可具有使它们相比于静态资源尤其有用的若干个属性。这样的属性可包括下列中的一些或全部：

[0022] 后期绑定

[0023] 需要原始资源的精确视图无需被提前计算；打包器可关联产生派生资源的计算。如果新类型的计算资源变得重要，数据的打包器可仅提供一组新的规则和计算，而不是重新计算、重新打包以及重新发送整个初始资源（其可能是大的数据集）。

[0024] 例如，假设初始资源是人类基因组序列。可利用揭示关于基因组的某些有限信息——主体是男性还是女性？主体在BRCA2基因中是否有一定的突变？等等的若干计算，来加密和打包资源。在稍后的日期，数据的拥有者确定提供对序列的新方面的访问是重要的，数据的新方面例如是与HIV风险有关的CCL3基因的副本的数目。打包器创建新计算，将其与初始资源相关联，并将其分配到感兴趣的各方。对于打包器来说，提前了解此计算或提供对数据的无限制的访问是没有必要的。

[0025] 第三方计算

[0026] 计算可由打包的信息的用户所提出，并随后与资源安全地相关联，例如通过初始打包器和/或有权这样做的另一实体。

[0027] 继续人类基因组序列的示例，假设序列被加密并发送到希望将关于序列的信息并入其研究中的研究员。作为初始打包的部分，研究员接收提供数据的各个视图的一组计算。研究员已发现一种新算法，该算法从若干基因组合信息以便估计特定疾病的风险，但是使用由数据所有者已提供的计算不能得到他所需要的所有信息。研究员创建一个计算，该计算当对序列运行时，将产生他的估计。他将此计算发送给所有者。假设所有者同意，新计算与资源安全关联，并以允许他对序列运行计算的形式被发送回给研究员。

[0028] 类似示例将是由制药公司所创建以通过分析基因组序列估计特定药物的适当剂量的计算。此类型的剂量敏感性分析经常被执行用于为抗凝血剂、华法林(warfarin)进行开方。CYP2C9和VKORC1基因中具有特定变体的患者可能或多或少对此药敏感。利用派生资源，在没有额外湿性实验室工作的情况下，对已被预先存储和保护(例如出生时)的基因组序列运行此敏感性测试是可能的。

[0029] 计算的组成

[0030] 当确定第三方计算应该被绑定到资源时，打包器可能希望允许计算继续进行，但是将其前置或后置条件添加到产生派生资源的计算流程。

[0031] 例如，假设管理的资源是连同地址信息的给定(大)区域的地图。第三方提出了一种计算，该计算给定地址、返回与地址相关联的空间坐标。一般而言，打包器可能愿意接受此计算，但他不希望公开确切坐标。而是，他将偏好的是计算仅返回城市或邻近地区等。所有者/打包器随后创建第二计算，其消耗由第三方所提出的计算的输出，并将其修改以隐藏更详细的信息。当他将第三方计算绑定到资源时，他请求在输出可被返回到请求者之前应用他自己的第二计算。

[0032] 在一些实施例中，计算可与制订并发送包含关于何时、由谁以及在什么情况下派生资源的信息的审核记录的资源相关联。

[0033] 图1A示出了根据一些实施例的用于管理数字资源152的示例系统150。如图1A中所示，由第一实体151(例如数字资源152的所有者或分配者或代表其行动的实体)将数字资源152(例如，科研数据、医疗记录、遗传信息、媒体内容，等等)与一个或多个计算154和一个或多个规则156的组一起打包。例如，资源152可被加密、数字签名，和/或以其他方式被保护，并与一个或多个计算154和一个或多个规则156安全地关联。经由任何合适的通信介质(例如，计算机网络，诸如互联网、移动通信网络等)，资源152可与一个或多个计算154和/或一个或多个规则156一起被分配到远程实体158。替代地或另外，资源152可独立于一个或多个计算154和/或一个或多个规则156而被分配到远程实体160。另一实体162可对第一实体151提出关于资源152的额外计算166。第一实体可将计算166与资源152安全地关联(例如以实体162所提出的形式、或以修改的形式，或者利用被要求与计算166一起执行的额外的前置或后置计算，等等)，并且分配(或使得可用于分配)这样的计算166′，用于结合资源152一起使用。

[0034] 隐私保存计算

[0035] 如上述示例中那样，派生资源可被用来帮助保存初始数据的隐私。在一些实施例中，若干因素可帮助确定可被绑定到资源的计算的类型。例如，可分析已被绑定到资源的计算的已知历史来确保仅发生期望数量的公开。例如，打包器可能已发行计算，当一起使用时，该计算可能以其他方式揭示比所预期的更多的信息。因此，例如，打包器可决定逐渐减

小由连续计算所揭示的数据的分辨率。为此目的，打包器还可能希望考虑在对资源的各种计算的执行时所需的审核记录。

[0036] 在一些实施例中，计算可以被至少部分随机化来保护数据的隐私/保密性。例如通过在输出前添加随机噪声到资源，计算可被匿名。虽然对手可多次执行计算并评估所返回的派生资源的统计信息(例如平均值)，但在一些实施例中，打包器可以对此攻击进行减轻，例如，通过限制这种请求的数目、随着做出越来越多的请求而改变统计信息、记住状态变量(例如随机数种子)，使得相同主体在计算的每个应用上得到相同的随机化数据(从而防止统计攻击)等等。

[0037] 对于不同主体的不同视图

[0038] 在一些实施例中，计算可取决于例如访问信息的主体的条件。在这样的实施例中，打包资源中的不同利益相关者可获得不同的视图；不同计算可与不同主体相关联。这种能力与指定规则中的特定主体来选通对资源的整体访问的能力进行交互；规则组可规定给定主体究竟是否有机会访问资源，并且其因此确定是否曾经计算了派生资源。然而，如果其的确运行，则计算可决定根据做出请求的主体或主体的属性(例如给定级别中的会员)而产生不同的派生物。

[0039] 例如，使用这种技术，人们可以构建受保护的健康记录，该记录可被医院中的所有医生访问，但当被患者的主治医生访问时其包括额外的细节。派生资源方法允许管理的资源保留单个包，与针对不同主体需要多个包相反。

[0040] 不同情境中的不同视图

[0041] 正如，在一些实施例中，资源的视图可取决于请求对资源访问的主体，因此该视图可取决于执行计算的点处存在的其他情境信息。

[0042] 例如，管理一块内容的一组规则可能允许对被注册到给定用户的任意装置的访问，但是计算可能以用于特定类型装置的给定分辨率输出资源。或者，特定类型的装置上可能只示出具体的摘录，而在其他装置类型上全分辨率是可用的。

[0043] 保存数据精确度

[0044] 虽然已给出多个示例，其中例如为了保存隐私、呈现给用户的数据的准确度或精确度被降低，将被理解的是，在一些实施例中，产生派生资源的计算不一定是有损的；也就是说，它们在产生派生资源的过程中不需要去除任何初始信息。使用派生资源，初始数据无需被重复过滤或重新打包，因而没有丢失将来或许有用的信息。

[0045] 例如，假设该资源是用于给定患者的一系列活动水平(如通过加速度计所记录的)。一般而言，物理治疗师可能仅对每日平均的活动水平感兴趣，因而资源可能与产生这些平均值的一组计算一起供给。提供那些平均值的一种方法将是取得初始资源、执行平均、以及然后将平均值序列作为单独资源保护。然而，这种方法不提供返回到高分辨率数据中来确定例如给定锻炼期的强度的能力。而是，如果根据派生资源方法的优选实施例执行平均，新计算可提供尚且不能从被过滤、重新打包的活动数据中获得的信息，因为初始的原始数据将仍然是可用于由这样的新计算使用的。

[0046] 可审核性

[0047] 在一些实施例中，作为用于渲染的条件执行的计算可被表达用于标准化机器，使得资源的初始打包器可验证并依赖指定计算的结果，或者其可使用先前议定的语义来被声

明地表达。

[0048] 在一些实施例中，当打包器将计算与资源相关联时，计算首先被验证（尤其是如果其通过第三方生成）。一般而言，计算功能的自动验证是困难的，且计算框架越具表达性，就越困难。因此，打包器可依靠各种启发式方法，诸如检查描述计算的元数据，在测试环境中在批准计算之前运行计算，验证所提出的计算由可信的第三方所签名，认证提议者的身份，等等。统一的计算框架——例如以其表达计算的具体语言——帮助打包器来验证所提出的计算。

[0049] 管理多个子资源的计算

[0050] 可利用派生资源方法管理的一种类型的资源，可以是整个数据库的子资源，其中由一个或多个密钥来保护数据库。在这个规划中，对资源运行计算类似于查询数据库。打包器可通过约束计算来限制可对资源执行的查询的种类。

[0051] 例如，假设管理的资源是特定人口的一组完整基因序列和健康记录。相关联的计算允许用户查询资源以确定，例如，人口中多少女性表达了BRCA1基因。或者有多少在年龄18到45岁之间的女性针对该基因进行编码。在此示例中，数据资源和对其操作的计算的组合允许用户探索数据。在此示例中，可对数据集执行的计算的类型可由初始打包器所定义；打包器将来必要时可添加进一步的计算。例如，如果假定某种相关，打包器可提供允许其他用户在初始数据集中探索该相关的一组计算。利用静态资源，数据在打包之前将已经被减少，且信息将丢失。利用派生资源，全数据集可被保存，具有将来需要时给定的额外访问。

[0052] 计算绑定的委派

[0053] 在一些实施例中，不一定要求资源的发起者或创建者执行资源和计算之间的全部绑定。例如，发起者可将计算的绑定委派给第三方，例如被设计来将一组资源作为单个的逻辑资源进行管理的数据库。

[0054] 例如，基因测序仪可以建立与在线服务器的信任通道，并对其上载序列信息，将确定将来可能对序列运行哪些种类的计算的能力委派给服务。

[0055] 返回派生资源

[0056] 在一些实施例中，可将派生资源返回作为对另一派生资源运行计算的结果。

[0057] 例如，初始资源可能包括一组管理的子资源。当对资源执行相关联的计算来提取有关特定子资源的信息时，该计算可导致产生第二派生资源，该第二派生资源包括子资源和用于询问该子资源的一组计算。

[0058] 计算的位置

[0059] 在一个优选实施例中，在受保护的处理环境中执行与管理的资源相关联的计算。在一些实施例中，该受保护的处理环境的位置上没有逻辑限制。在一些实施例中，资源的所有者/打包器发出虚拟安全包到用于各种消费实体来处理的世界中；计算（以及规则评估）发生在消费者地点处受保护的处理环境中。图1B中示出了这种情况的示例，其示出了根据本发明的主题的一个实施例的管理派生资源的说明性系统。如图1B中所示，虚拟安全包102包括规则104、计算106、密钥108和初始资源110。由安全计算环境112，根据其规则来处理虚拟安全包102以产生派生资源114。图1B中所示围绕虚拟安全包102的虚线意在指示所示四个子组件（104、106、108和110）可以一起或单独进行分配，但使用例如密码技术与彼此持久相关联。图1B中所示的情境信息116，可以包括例如来自其中正在执行资源派生的环境的信

息，其可以包括例如从系统的用户所收集的信息。图1B中所示出的意图信息118可例如指定用户希望对数据的利用，且可被用来至少部分地确定应当评估哪些规则104和计算106。

[0060] 应当理解的是，图1B被呈现用于说明的目的，且存在许多其他可行的可能性。例如，该资源的所有者/打包器在其自身受保护的处理环境中可执行一些或全部计算，并将结果返回到请求者，例如基于请求者的某些属性，诸如认证的身份。替代地(或另外)，资源发起者已向其委派授权来附属或执行这些计算的委派人可执行对资源的计算。

[0061] 针对远程资源进行计算

[0062] 通过将以上描述的第三方计算技术与关于计算位置所描述的技术相组合，提出一种计算以针对远程资源而运行变得可能。在这样的一个实施例中，资源的所有者可确定用于认证和验证所提出的计算的必要步骤，并然后针对其自己的资源执行计算，返回结果给请求者。图2中图示了这种配置的一个示例。

[0063] 在一些实施例中，计算和资源之间的逻辑绑定可按照一种或多种方式发生，包括例如：

[0064] 按名称——计算与指定其将运行于的一个或多个资源的元数据一起出现。

[0065] 按属性——将资源连同必须对于要操作于的资源是真实的一组属性一起发送。例如，请求者可发送查询串，接收方可使用该查询串来确定其上应运行计算的资源组。

[0066] 图2 示出了计算可如何被提出以针对资源进行运行的示例。用户202做出涉及资源的请求，并由认证者A 204所认证。包括计算208的安全包206被发送到评估器系统210，在那里其被评估器210所检验和认证，并利用策略P 214针对资源R 212运行。结果216被返回到用户202，可能通过一系列的中间环节。

[0067] 将理解的是，本文所述的系统和方法可被应用到几乎任何类型的内容，下文包括其中的一些非限制性示例。

[0068] 派生资源的示例

[0069] 可缩放视频——在一些实施例中，是上文所述的SVC(“可缩放视频编码”)媒体示例——其中基于所支付的金额，授予对不同级别的预先计算的分辨率的访问——可以由单个、高分辨率视频资源和一组计算的组合所代替，其中的每一个由其自身的规则所管理。例如，假如某些条件得到满足，并且首先由指定计算过滤资源，用户也许可以访问低分辨率版本的视频。每个级别的分辨率可与产生用于渲染的适当信号的指定计算相关联。

[0070] 过滤的健康数据——在一些实施例中，在给定由健康相关的测量序列(例如，上几个月内每一秒所测量的脉搏)所构成的数据系列的情况下，不同主体可被准许访问不同的数据分辨率。患者自己也许可以访问以全分辨率的整个数据系列，而他的医生也许可以访问较粗糙的视图——后面两星期内的平均休息和活动脉搏。在这种情况下，医生可能仍然可访问个人可识别信息，而完全不相关的第三方(诸如流行病学家或研究员)也许只可以访问全部或部分匿名数据。执行数据去分辨率的计算可与初始数据资源一起被打包。在这种情况下，管理对数据系列访问的规则，可以与不同的主体或角色相关联。

[0071] 虚拟世界——在一些实施例中，初始资源可以是游戏，其由以足够细节所编码的虚拟空间的描述所构成，其中足够强大的渲染引擎可产生三维、交互的空间模型。例如，虚拟空间的一个区域可能仅对已在游戏中达到特定等级的用户可用。管理资源的规则执行视图的计算，或者对于产生视图所必要的计算。

[0072] 通用解码——在一些实施例中，该初始资源可由以特定专有格式所编码的交互式视听呈现所构成。与渲染资源相关联的计算可包含用于数据的完整解码器，该解码器以允许其在目标平台上被渲染的方式解码初始资源。

[0073] 基因信息的管理——在一些实施例中，管理的资源可以是，例如，一组完整的基因序列和特定人口的健康度量，例如如上所述的。

[0074] 科学研究——在科学研究中，常常重要的是，使数据是最大程度可用且可验证的，同时仍然确保其受保护。信誉良好的科学出版物通常将希望确保所公布的研究中驱动结论的数据对其他科学家可用，以便其可以被检验。被用来处理该数据的算法也应该可用于同行评审。同时，数据应不易受篡改影响。因此，在一些实施例中，数据可以受保护的形式被公布，具有指定可对数据集执行的特定计算的规则。这样的安排同时满足开放性/公布和完整性保护的需求。

[0075] 协商广告负担——在另一个示例中，媒体(例如，视频或音频)流可由广告所部分地资助。在该示例中，资源可包括主节目和可以在某些位置处被插入到主节目流中的一组广告。当资源被访问时，返回的派生资源可以例如包括一定数量的基于例如请求内容资源的主体、该主体的属性、和/或渲染点处的情境的这些广告。例如，如果主体已经查看过给定节目中的一组给定的广告，则计算可在另一组中进行替代。如果观众已经为订阅进行支付，则计算可完全地消除广告。

[0076] 协商优惠券价值——另一个示例是对上述广告示例的变体；然而，该示例中返回的资源不是媒体流，而是数字优惠券。可以通过计算和用户之间的交互来确定优惠券的面值。如果用户愿意收看被包括为初始资源的部分的广告，则用户得到优惠券上更好的赎回价值。

[0077] 如前面结合图1B所指示的，在一些实施例中，虚拟安全包102的元素被绑定在一起。如图1B中所示，这些元素可能包括初始资源110、被用于加密和/或解密资源的一个或多个密钥108、基于初始产生派生资源的一个或多个计算106的组、管理对初始和/或派生资源访问的一个或多个规则104的组。

[0078] 在一些实施例中，绑定可以包括将这些元件一起打包在单个包中，但是其还可以包括应用密码(或其他计算)技术来关联这些元素，即使当它们被单独分配时。打包器可使用多个因素来确定计算是否应当被绑定到资源。这些可能包括，例如，计算创建方的认证、该方的属性(例如受信任组中的成员)、与计算相关联的元数据检查、在测试环境中运行计算的结果，等等。

[0079] 在一些实施例中，如下所述，可利用不同力度来绑定计算。

[0080] 强绑定

[0081] 在强绑定示例中，计算、规则、资源和密钥被一起密码绑定到虚拟安全包中。可以被用于将计算绑定到资源的一种机制，是要在与选通对资源的整体访问的规则相同的包中包括计算。用户可选择这些规则中的哪些来评估，且如果条件满足，相关联的计算在其被返回时被应用于资源。将被理解的是，任何合适机制可被用来将规则绑定到资源。例如，在一些实施例中，可以使用2006年10月18日所提交，共同转让、共同未决的编号11/583,693(公开号2007/0180519A1)美国专利申请(“'693'申请”)中所描述的绑定技术。

[0082] 在一些实施例中，可以使用安全地将计算与资源相关联的单独绑定对象来完成绑

定。该绑定对象可包含唯一标识被绑定资源的一些信息，例如，资源的散列(hash)、资源ID、对加密资源的密钥的参考，等等。绑定对象还可包含计算本身或者对计算的参考二者之一，诸如计算程序的散列、唯一标识符等。绑定对象可以自身被签名，以提供绑定的完整性保护，以及认证在评估点处的绑定创建方。

[0083] 使用这种方法，计算可从规则、资源和密钥单独地行进，但逻辑上保持在安全虚拟包内。在一些实施例中，计算可通过使用指向其他绑定对象的绑定对象来连锁(组成)，以被用作为前置或后置计算。而且，利用绑定对象方法，没有必要创建资源和计算之间的先验相关——可以在以后的时间绑定计算，且在一些实施例中其可由其他方所提出。

[0084] 弱绑定

[0085] 在一些实施例中，替代地可以使用相对弱的绑定，例如基于由名称或属性而不是使用密码学来标识计算。

[0086] 如图1B中所示，在优选的实施例中，安全计算环境被用来评估规则和对初始资源应用计算。在一些实施例中，安全计算环境具有以下属性中的一些或全部：

[0087] ●它将安全包中的元素的源验证为值得信任——在一些实施例中，它具有在来自或不来自已知或可信源的虚拟安全包之间进行区分的能力，并在后者情况下，安全计算环境能够避免评估规则或执行资源派生。

[0088] ●它防止篡改在对内容访问的点处与规则评估或资源派生计算或与其相干扰。

[0089] ●它保护被用来加密来自未授权访问的内容的密钥。

[0090] 在一些实施例中，明确定义的计算引擎被用来产生派生资源。可根据表达计算的方式设计此计算引擎的实施例。例如：

[0091] 声明性计算——计算可以被声明地表达，使用以专用语言所编写的文档，其指示需要对初始资源执行的计算，但是没有给出关于如何实现这些计算的指导。在这种情况下，计算引擎应该理解利用其来指定计算的专用语言的语义，使得虚拟安全包的初始创造者可确保以预计的方式执行计算。打包器和用户通常将提前对声明性语言达成一致。

[0092] 程序性计算——计算还可被表达为针对标准化机器所编写的程序。特别地，系统设计可指定表达这些计算的虚拟机器语言。由于计算的初始创造者知晓用于标准化机器的规范，其可创建具有对其操作的充分理解的程序性计算，而无需预先指定正被执行的计算的高级语义。

[0093] 在一些实施例中，例如在规则评估点处，还可使用可选的受保护的数据库，来存储被用作对计算的输入或用来以其他方式影响计算的状态变量。

[0094] 示例

[0095] 根据本发明的主题的实施例的派生资源的实现和使用的一些附加示例在以下被呈现。虽然许多示例与生物学和流行病学相关，将理解的是，本发明的主题并不限于这些领域。

[0096] 在大型调查中保存隐私

[0097] 该示例中，全国调查正试图确定某种类型疾病、职业、家庭住址之间的联系。调查的目的是产生具有用于不同类型疾病的高中低风险的地图。在缩放系统中结合该地图，因此使地图观众可从全局视图缩放到局部视图。查询界面允许观众要求不同类型条件和职业的显示。

[0098] 调查在安全环境中组合来自多个不同数据库的结果，并将结果打包为管理的派生资源。

[0099] 在此例中，用于在管理的派生资源内部查询结果的规则可能如下：

[0100] ●当查询的结果在大区域内，其结果将是具体的，例如，如果返回多于100个结果，则具有处于特定状态中的疾病的教师数量将被报告为以量级10的准确度。如果返回少于100个结果，则所报告的值将是具有50左右的常态和10的偏差的随机值。

[0101] ●对于逐渐变小的区域，结果的准确度将劣化，使得你永远无法得到比30个结果的量级更好的准确度。

[0102] ●随机结果将被插入到返回值中，以确定无法通过调查中缩小选择所识别的个人，然而，如果在请求数据视图的状态下，请求者可提供将他或她识别为执业医生的证书，则所有结果精确到低至约两个。

[0103] 可从调查中心下载所得到的管理派生资源，并在具有安全计算环境的任何计算机上对其进行查看。

[0104] 在不能识别具有该条件的实际个人的情况下，这允许偶然观察者查看位置和诊断的病例之间的效果(如果有的话)。该状态下的执业医生可得到准确得多的视图。

[0105] 为了实现此示例，执行调查的人可针对相关数据查询多个数据库，并从这些结果中创建新的数据库。该数据库可被实现为文件。针对数据库的两组不同的存取函数可被实现为计算机程序。该程序可驻留于计算机系统的存储器中所存储的程序文件中。

[0106] 与执业医生有关的程序可利用认可的国家认证管理委员会的公钥来加密。做到这一点的一种方法是创建对称密钥、利用该密钥加密该程序，然后利用国家认证管理委员会的公钥来加密对称密钥。

[0107] 数据库文件、与公众有关的存取程序文件以及与执业医生有关的加密的程序可全部被打包成传输文件。该文件可利用公共安全计算环境提供者的公钥来加密，且可被分配到想要查看调查的任何人。

[0108] 当用户想要经由查看器来查看调查时，他或她首先呈现证书。证书可以是与安全计算环境一起出现的标准证书，或来自例如可断言用户是合格执业医生的权威人士的证书二者之一。

[0109] 在以后的时间，调查已被公布之后，医生注意到特定基因ABC1、环境因素和特定疾病诊断之间的联系。他写给调查的作者，并请求执行高分辨率研究的许可，使用他的国家管理委员会颁发的全科医师证书来执行他的数据和调查数据之间的高分辨率相关性。他提供他想要执行的计算作为文件中的计算机程序。连同计算机程序一起，他还发送他自身的证书。

[0110] 调查中的利益相关者检查计算机程序和医生的证书。他们发回连同管理的派生资源一起被加载的指令包，以及允许医生查看高分辨率数据的签名的声明。

[0111] 然后医生连同新指令包一起加载初始管理的派生资源，以及其签名的证书。在安全环境中，新指令被识别为来自调查的利益相关者。签名的证书也被识别。管理的派生资源现在将新指令结合到自身中。这产生了管理的派生资源，其除了当其在医生证书的情境中操作从而针对他的特殊计算而运行时，在所有情况下都充当旧的管理的派生资源。

[0112] 个性化医疗

[0113] Susan使用在线服务来追踪她的运动养生。该服务维护个人健康记录，并存储从Susan用来追踪她的健康的各种生物统计传感器收集的信息，该生物统计传感器包括体重秤和记录了(每秒一次)Susan的活动等级、位置、心率、脉搏血氧测定和皮电反应(GSR)的多功能健身手表。

[0114] Susan将数据从她的手表上载到她的PC(例如使用蓝牙、BluetoothLE、ANT+、6LoWPAN、USB连接、附着到她的计算机的小型低功率无线电基站等等)，其通过互联网自动将数据上载到服务中。使用诸如HTTPS协议的标准技术通过安全信道发生上载。

[0115] 通过服务，Susan定位私人教练来帮助她微调她的日常生活。在通过服务与教练建立关系之后，教练生成用于访问Susan的数据的请求——每个星期日晚上，教练希望收到该星期期间Susan每个锻炼的列表，并且对于每个锻炼，接收如以下的统计信息：(a)锻炼的开始和结束时间，(b)锻炼期间行进的距离，(c)起始心率、峰值心率、以及Susan处于5％的峰值心率内的时间长度，以及(d)峰值心率下的皮电反应(GSR)。

[0116] 服务为教练提供用户界面，通过该用户界面做出此请求并将请求发送给Susan。用于数据的请求包含每星期要被收集的数据的人可读描述。Susan接收并批准请求，但附有附加条件，即仅可查看早7点到晚7点之间收集的数据。

[0117] 每个星期日晚上，服务收集Susan前一星期期间已生成的所有数据，并将其打包为被发送到她的私人教练以供审查的单个资源。

[0118] 服务将针对本星期的所有数据——以其原始格式——收集到单束中，并利用由服务生成的唯一对称密钥来加密该束。

[0119] 该服务生成允许教练访问此数据的规则。当数据包被教练访问时，此规则可基于例如评估的Susan与教练之间关系的某些数字表示。

[0120] 此外，服务生成一组计算来与数据包相关联，该数据包计算对于每个锻炼而言，教练所已经要求的元素。编写这些计算以在教练用来审查数据的嵌入客户端软件中的虚拟机上运行。

[0121] 该服务创建将数据包、规则和计算以密码形式链接在一起的许可对象。为提供一个示例的实例化，许可对象可以包含以下子组件中的一些或全部：

[0122] ●数据结构，其将数据包绑定到标识符，该标识符包含标识符和数据本身的密码散列，

[0123] ●数据结构，其将用来加密数据包的对称加密密钥绑定到密钥标识符，该密钥标识符包含密钥标识符和实际密钥，

[0124] ●一系列数据结构，每个用于一个规则，其通过将规则标识符与可执行规则的字节代码的密码散列一起打包，来将规则绑定到其相应的标识符，

[0125] ●一系列数据结构，每个用于一个计算，其通过将计算标识符与可执行计算的字节代码的密码散列一起打包，来将计算绑定到其相应的标识符，

[0126] ●数据结构，其包含数据包的标识符，以及用来加密数据的密钥的标识符，

[0127] ●数据结构，其包含数据包的标识符，以及用来管理对数据包访问的规则集的标识符，

[0128] ●数据结构，其包含数据包的标识符，以及将在数据包中产生信息的视图的相关联计算的标识符，

[0129] ●规则集，以字节码格式，其将由接收器通过虚拟机执行，

[0130] ●计算集，以字节码格式，其将由接收器通过虚拟机执行，和/或

[0131] ●元数据，其被用来建立包中的数据表示什么（例如，这是Susan的数据、其被收集的星期，等等）。

[0132] 私人教练使用允许他探索针对他的所有客户的数据的软件包。使用实现用于访问数据的安全执行环境的软件开发工具包（SDK）来建立此软件。在星期一早上，教练打开并启动软件包，该软件包连接到该服务，并下载他可能已经从他的客户接收的任何新信息。

[0133] 为了审查Susan的数据，教练在由软件呈现的用户界面中点击Susan的名字。软件可在其安全处理环境中做若干事情，包括例如下列中的一些或全部：

[0134] ●使用它了解的各个许可对象中的元数据来识别Susan的数据包（此信息可能在一些本地数据库中被索引），

[0135] ●打开最近一星期的许可对象，并使用将数据包链接到规则集的数据结构来查找和加载与数据包相关联的规则，

[0136] ●基于规则中所表达的条件是否得到满足，执行实例化规则的字节码，并做出关于是否继续进行处理的决定，

[0137] ●假设规则已成功被评估，使用将数据包绑定到加密密钥的数据结构来获得密钥并解密数据，

[0138] ●使用将数据包绑定到其计算的数据结构来加载和执行计算，其产生数据包的若干视图，每个用于一个计算，

[0139] ●使这些计算的结果对用于显示的软件包的用户界面部分可用，

[0140] ●将审核记录发回到在线服务，Susan可以定期检查该在线服务以确定她的数据正如何被使用。

[0141] 教练在他的用户界面中看到这些计算的结果。注意，从其中派生这些结果的基础数据并不暴露给教练，使得例如，教练不能得知锻炼发生在哪来，即使该信息被包含在数据包中由Susan上载并被发送给教练的原始数据中。

[0142] 在几个星期内对Susan数据进行评估之后，私人教练想要鼓励Susan通过在更多样化的地形上进行其锻炼来增加她的耐力。为了评定该养生法的有效性，教练希望具有关于Susan正在哪儿锻炼的信息，使得他可把该信息标绘在区域的地图上，并确定她是否在上坡、在相对平坦区域上前行等。他希望连同详细心率数据一起收到此数据，使得他可以将心率针对位置相关联。教练使用由在线服务所提供的界面来请求来自Susan的该附加信息。

[0143] Susan接收请求，但给予教练访问详细位置信息不会感觉舒服。毕竟，她从未见亲自过教练，且关于给出这样的信息有点持谨慎态度。然而，她确实理解教练要求此数据的原因，并且希望支持他的分析，因此，与其接受教练的请求，Susan自己使用在线服务处的界面来创建允许访问海拔高度数据而非纬度和经度的计算。

[0144] 服务界面呈现用于模板库中可用的不同计算的结构化浏览器。浏览器呈现关于不同类型数据的计算，例如“位置”、“健身”等。

[0145] Susan浏览到“位置”区域，并注意到若干计算对她是可用的：“完整的位置信息”、“纬度/经度”、“ 海拔高度”。

[0146] Susan选择“海拔高度”，且界面随后允许她选择用于在时间上和空间上二者的计

算的数据分辨率。例如，Susan可选择用于时间分辨率的“每30秒”或“5分钟往绩平均(trailing average)”和用于空间分辨率的“全分辨率”或“+/-10米内随机化”。

[0147] 使用类似过程，Susan选择在30秒间隔上提供心率数据的计算。

[0148] 一旦Susan已选择她想要应用的计算，她使用附加界面来授权私人教练以获得此计算。从那以后(或直到Susan撤回授权)，此计算将被包括为发送给教练的每星期报告的一部分。

[0149] 教练开始接收海拔高度和详细的心率数据，他使用这些数据来评定Susan锻炼的有效性，并提供反馈。在评估有一星期效用的数据之后，他发现该新信息是有用的，并对Susan过去的数据请求Susan授权的类似信息。结果，教练从在线服务接收新的许可对象，该新的许可对象对他已接收和存储的数据包提供海拔高度/心率计算；该服务无需重新传送数据包自身，仅重新传送新的许可对象。

[0150] 在进行新养生法几个月后，Susan的心血管效率似乎没有一直以预期方式改善。她的锻炼断断续续地进行，经常在中间休息。为具有专长于关于员工的运动医学的医生的组织工作的教练，希望得到来自从不同位置工作的主治医生的一些输入。通过服务，教练问Susan这是否将是可接受的，并且她同意了。教练直接向医生转发有上个月效用的Susan的数据。包括数据包和许可。

[0151] 医生试图打开数据来运行计算，并且(因为他根本尚未被授权来访问数据)被提示通过由他的软件来请求来自Susan的授权。他这样做，且授权请求被发送给Susan，Susan批准该请求。

[0152] 在分析数据之后，医生开始怀疑具有不良氧合的问题，并且，通过在线服务，请求对Susan的脉搏血氧测定数据进行附加访问，Susan同意医生的请求。请注意，教练不可以访问相同的数据；该服务已创建用于医生的脉搏血氧测定数据的单独计算，并仅对医生发送包含那些计算的许可。

[0153] 医生从数据中得出一些结论，并且将他的建议提供回到教练，该教练修改Susan的养生法以反映医生的输入。她的心血管性能开始改善。

[0154] 在以后的一些时间，在服务和有效授权中审查她的数据的使用时，Susan认识到医生仍然可访问她的信息，并选择禁用此访问，因为咨询已经完成。颁发给该医生的许可被标记为无效，医生的软件被通知此事实，并没有未来的许可在此授权下被创建或发送到医生。在其他实施例中，该许可在指定的时间段之后自动到期。

[0155] 视频下载服务

[0156] Ian订阅了在线电影服务，这给予他无限制访问用于他的所有各种渲染装置的各种各样的电影。

[0157] 该服务被设计用于节目的下载和持久存储，与更多的面向流送的模型相反。通过视频的渐进式下载可效仿流送，但即使在此模型中，首先获得许可，且在渲染该渐进式下载流之前评估规则。

[0158] 该服务提供了多个的订阅等级，包括由广告支持的标准清晰度免费等级。这最初是Ian的选项。其他选项(收费表上的)包括没有广告的标准清晰度提供和高清晰度提供。

[0159] 该服务被设计为通过对等分布网络提供高清晰度视频文件给所有客户。分配多版本的逻辑和每个电影的分辨率被认为过于复杂，因此每个客户无论其订阅等级如何，均收

到完全相同的高清晰度视频文件。

[0160] 从许可单独分配该视频文件。当客户请求许可时，许可包含得出特定客户的数据视图的计算，将客户有权查看的视频流确切地提供给渲染系统。

[0161] 在免费的、广告支持的标准清晰度等级的情况下，每个许可中包含三个计算。(i)从打包的视频中提取标准清晰度流的计算，(ii)定期从广告服务器下载广告文件，并将它们插入到输出流中的计算，如果广告服务器不可达，则回落到一些默认广告，(iii)将广告印象的审核记录发回到广告服务器的计算。

[0162] 如先前示例中所述的那样，这些计算被绑定到视频文件。

[0163] 在客户端软件中由安全计算环境执行这些计算，该环境评估许可、解密内容并在将其返回到客户端的本地渲染引擎之前将输出的计算应用到内容。

[0164] 当客户订阅高级等级时——其花费金钱——在渲染之前应用这些输出计算之一或二者的要求被移除。

[0165] 该服务被设计为通过允许客户免费地分配受保护的内容来使广告收益最大化。如果受保护内容的接收方是付费订户，他可以透明地获得许可来以他已经支付的分辨率渲染内容。如果接收方不是订户，他根本不能渲染视频直到他安装了客户端软件。直接分布式视频与让接收方查看带有广告的标准清晰度视频的默认许可捆绑在一起。

[0166] Ian在去出差前将电影下载到他的平板电脑上。他非常喜欢该电影，使得他想把副本给他的朋友Jim。他简单地拷贝电影文件(其包含打包的视频内容和默认许可)到Jim的系统上，于是Jim能够观看该电影。

[0167] 欣赏电影之后，Jim决定支付对该服务的订阅。一旦他这样做，他获得用于他所具有的内容的允许在没有广告的情况下进行渲染的许可。这些许可被非常快地下载，且升级立即生效，而无需重新下载相对较大的视频文件。

[0168] 在更加家庭友好的尝试中，电影服务进入到与被称为“Movies4Families”的组织的合作关系中。此组织审查由服务所提供的所有电影，并确定哪些场景可能不适合年轻观众，按类型(例如轻微暴力、脏话、裸露、讽刺等)将它们分类。

[0169] 对于每个这样的场景，组织创建修改输出流的计算，以消除令人反感的场景、白屏两秒钟、发出哔哔声、替代故事情节中的叠接，或采取使电影更加家庭友好所需的任何其他措施。

[0170] 这些计算取决于用户设置。例如，如果父母将他们小孩的客户端配置为针对10岁，那么可应用与将应用于15岁的计算不同的某些默认计算。

[0171] 父母控制也可包含微调过滤的能力。

[0172] Ian报名参加Movies4Families服务。结果，对于他从主视频服务下载的每一部电影，他的客户端也将从应用适当过滤的Movies4Families服务提取计算。当在他年幼儿子的装置上渲染视频时，过滤器确保他没有正看到不适当部分。

[0173] 从技术上讲，由Movies4Families创建的计算被绑定到他们以与视频服务绑定他们同样的方式来管理的电影——通过创建一个对象，该对象将用于视频的标识符与用于计算的标识符绑定在一起。

[0174] 在这个示例中，假设电影服务中使用的视频客户端将仅信任由持有认证密钥的实体所数字签名的许可和计算，其中认证密钥由电影服务本身发行。在这种情况下，电影服务

已向Movies4Families发行认证密钥，该认证密钥允许他们对将电影和过滤计算进行关联的对象进行数字签名。

[0175] Movies4Families发送计算本身和计算和电影之间的绑定给客户端，该计算和电影均利用得自于视频服务的密钥来数字签名。同样地，视频客户端识别签名，并将在渲染时应用所请求的计算。

[0176] 过滤功能取决于客户端中的设置。例如，Ian和他年幼的儿子可能均使用他们各自的客户端来观看同一电影，但是由于儿子的客户端已被配置为针对10岁，他的流可能被重过滤，而Ian看到初始未过滤的电影。该示例示出了客户端侧处维护的状态变量可如何影响所执行的计算。

[0177] 数字重混音和混搭

[0178] John是已经创建了影响深远的芬克音轨(funk track)，并利用不允许复制的许可对其进行数字分配的音乐家。

[0179] Malcom是一位DJ，他希望制作(或出售)结合了与若干其他音轨混音的John的初始音轨的4秒样本的数字混搭。

[0180] 使用数字混音软件，Malcom创建从John的音轨中提取相关4秒的计算，通过镶边器(flanger)将其过滤，并在适当点处将其输入到他的混音中。

[0181] Malcom将此计算发送给John，只要每次播放John被支付半美分，John就批准该特定使用。他签名该计算，将其绑定到他的初始音轨，并添加每次播放摘录向他发送审核记录的后置条件，允许他追踪用于计费的使用。

[0182] Malcolm打包他自己的混搭，包括John的初始音轨和提取并过滤4秒样本的计算。在渲染的时候，在适当点处应用John的计算，且John最终得到使用其初始样本的报酬。

[0183] 遗传学

[0184] Elizabeth加入一项临床试验，该试验需要她将她的基因组测序。该试验是要调查某些基因类型和用于抗癌医药的最佳剂量之间的关系。

[0185] Elizabeth首先需要在存储和管理对她的基因组的访问的基因信息服务处建立账户。一旦她已经注册了此账户，服务生成随机样本号(和条码)，她将其打印出来并带到测序实验室。

[0186] Elizabeth提供她的样本，且实验室技术人员扫描该条码，将Elizabeth的基因组序列与随机样本号相关联。

[0187] 基因组被安全上载到信息服务，且随机样本号被用来查找Elizabeth的账户并创建她的基因组和她的其他账户信息之间的绑定。

[0188] 以这样的方式创建基因信息服务，使得基因序列本身可在多个研究设施间以受保护的形式被自由地复制，但是解密或访问该序列的许可必须由Elizabeth本人所给予，如由服务所认证的那样。这种架构允许Elizabeth的基因序列(其是几千兆字节的相当大的文件)被分配给可能在研究中对使用它感兴趣的研究人员，但是其中所有此类使用由Elizabeth所审核和控制。

[0189] 当Elizabeth注册用于临床试验时，她被要求批准科学家设计研究曾要求过的针对她的基因组的某些查询。例如，假设研究与乳腺癌有关，且研究人员正要求访问与BRCA1、BRCA2和TP53基因有关的信息。

[0190] 由于Elizabeth批准她的基因组的这些用途，对于这些特定研究人员，遗传学服务创建了若干个计算来针对Elizabeth的基因组运行，这些计算提取所需信息并将其提供给授权方。这些计算也具有审核要求，这使每次执行计算时审核报告被发送到遗传学服务。从而Elizabeth可以追踪她的信息正在如何被使用，以及被谁使用。例如，如本文别处所述，通过对将基因组和计算以密码方式绑定在一起的数据结构进行数字签名，服务将这些计算绑定到基因组。

[0191] 在以后的某个日期，参加这项研究的研究人员之一发现了他认为是抗癌药物性能和迄今未知遗传机制之间的新联系的内容。

[0192] 使用该遗传学服务，研究人员执行查询来从服务中具有账户的所有人当中识别可能的研究人群。此查询识别已参加过关于乳腺癌的先前研究的人，而无需向研究人员透露他们的身份。

[0193] 研究人员揭开130名候选人用于他的新研究，但他不知道他们是谁。系统中可能有其他候选人，但他们已预兆他们没有兴趣参加未来的研究，所以他们不会作为候选人而对研究人员露面。

[0194] 使用由遗传学服务所提供的界面，研究人员将计算上载到系统中，该系统将询问基因组以对假设模式进行测试。

[0195] 研究人员在其实验室中使用软件来创建此计算，并通过针对他已经完全访问的基因组运行该计算来验证该计算。

[0196] 他通过界面将计算上载到服务，其允许他指定关于计算的元数据(其将被用于什么，等等)，并使用他控制的密钥来对计算进行数字签名。

[0197] 使用遗传学服务，研究人员问130个候选人中的每个人他们是否愿意参加。对于那些同意的人，服务将新计算绑定到他们各自的基因组序列，条件是仅计算的发起者可运行它——与被用来对计算进行签名的公钥相对应的私钥的持有者。

[0198] 当他们到达时，这些计算被转发给研究人员，且研究人员将这些计算应用于他的实验室中已有的基因组序列，或如果他不再有副本，则下载相关基因组序列的副本。

[0199] 研究人员发现关于Elizabeth的特定序列的一些奇特的事情，并使用该服务来将请求她与他联系的匿名消息发送给她。通过电话，研究人员解释他发现了什么，并向Elizabeth请求对她整个序列访问的许可，使得他可进一步调查。

[0200] 使用该服务，Elizabeth创建计算，将其绑定到她的基因组，并将其发送给研究人员。计算允许指定研究人员来针对她的基因组运行任何附加计算，只要他在信任环境中将其运行，并要求审核每个这样的访问。

[0201] 实际上，Elizabeth已委派给研究人员将任何新计算绑定到她的基因组的能力，只要他被认证，且使用信任环境来执行计算。这允许Elizabeth对她的基因组进行一定程度的控制，如果她仅仅给予研究人员未受保护的文件，她将不具有这种控制。

[0202] 技术上，这可能采取由Elizabeth所要求的前置计算的形式，其根据Elizabeth已设置的条件，认证链中的下一个计算(由研究人员所提出的一个计算)。它也可能被实现为后置条件，其首先运行研究人员所提出的计算，并然后根据条件允许或不允许输出。

[0203] 研究人员可以请求绑定其他类型计算的能力(例如，允许合作者询问Elizabeth的基因组的能力)，但他必须首先获得Elizabeth的许可来绑定和分配这些计算。

[0204] 科学研究

[0205] Josh是社会科学研究人员，他正在带有政治色彩的领域中发表论文。他事先知道他的发现在某些政治团体当中将存在争议，并且他将被指控过滤数据来满足自己的政治议程。他需要能够证明他没有，例如省略不方便的样本，但他需要在不展现原始数据本身的情况下能够证明这一点，该初始数据可能被用来识别他的研究课题。

[0206] Josh以良好定义的格式收集他的数据，仔细地文档化他的数据源（且理想地收集可用于以后验证的签名或生物测定）。他创建了处理数据和提取统计信息的一系列节目，作为其研究的一部分。一旦他已经做出有关数据的一些结论，他将数据打包到容器中，并利用他生成的对称密钥将其加密。

[0207] Josh打包他已用来计算他的最后结果的计算，该计算包括例如：产生某些统计表来出现在他的论文中的一系列计算，产生用于他的论文的各种图/图表的计算，等等。

[0208] Josh使用本文中别的地方所公开的技术，将这些计算绑定到他的原始数据，并将打包的数据和计算一起放在公众可访问的网站上。

[0209] Josh发表他的论文。当评论员指责他有选择性的数据操纵时，Josh将评论员引导到该网站，在那里，他可以下载Josh的初始数据包和计算来自己执行实验。

[0210] 评论员下载数据集，并验证该数据由于被打包而尚未被篡改，计算产生Josh的论文中所示出的结果，以及以人可读格式的计算本身并不试图消除不支持该结论的数据。

[0211] 在验证这些事情之后，评论员仍不接受Josh的结论。评论员认为Josh已忽略特定因素的偏见影响。评论员创建考虑偏见因素的Josh的计算之一的修改版本，并提出该计算给Josh。

[0212] Josh接受批评为有效，签名计算来将其绑定到他的数据集，并将绑定发回给评论员，评论员针对数据运行新计算。如其结果表明，Josh的结论仍然有效，且Josh现在将批评员提出的计算包括为用于验证他的结果的他的公众包的部分。

[0213] 将理解的是，存在多种方式来实现本文所述的系统和方法。例如，在一些实施例中，可连同'693申请中所述的数字版权管理技术，和/或共同转让的编号10/863,551（公开号2005/0027871）的美国专利申请（"'551申请"）中所述的数字版权管理或服务编排技术一起使用本文所述的系统和方法（'693申请和'551申请两者的内容均通过引用整体地结合到本文中），虽然任何其他合适的DRM和/或服务技术可被代替使用。

[0214] 图3示出了用于管理电子内容的说明性系统300，该电子内容包括派生资源，例如本文中所述的那些。如图3中所示的，持有电子内容303中版权的实体302，对内容进行打包以便由最终用户308a-e（统称为"最终用户308"，其中参考数字308可互换地指的是最终用户或最终用户的计算系统，如将根据上下文清楚的）进行分配和消费。例如，实体302可以包括内容所有者、创建者或提供者，例如个人、研究人员、音乐家、电影工作室、出版社、软件公司、作者、移动服务提供商、互联网内容下载或订阅服务、有线或卫星电视提供商、公司的雇员，等等，或代表其行动的实体，而内容303可以包括任何电子内容，例如个人医疗数据、遗传信息、研究结果、数字视频、音频或文本内容、电影、歌曲、视频游戏、一件软件、电子邮件消息、文本消息、文字处理文档、报告、或任何其他娱乐、企业或其他内容。

[0215] 图3中所示出的示例中，实体302使用打包引擎309来将许可306和一个或多个计算307与打包内容304相关联。许可306基于策略305或实体302的其他意愿，并指定内容的准许

和/或禁止的用途和/或一个或多个条件，该一个或多个条件必须被满足，以便利用该内容，或必须被满足为使用的条件或后果。根据由许可306所指定的策略，计算307提供内容的各种视图。内容也可以通过一个或多个密码机制（例如加密或数字签名技术）来保护，为此信任权限310可以被用于获得适当的密码密钥、证书，等等。

[0216] 如图3中所示的，可以由任何合适手段，例如经由如互联网的网络312、局域网311、无线网络、虚拟私有网络315、广域网等，经由电缆、卫星、广播或蜂窝通信314，和/或经由可记录介质316，例如光盘（CD）、数字多功能盘（DVD）、闪存卡（例如，安全数字（SD）卡）等，来将打包内容304、许可306和计算307提供给最终用户308。打包内容304可连同单包或传输313中或从相同或不同资源接收的单独的包或传输中的许可306和/或计算307一起被输送到用户。

[0217] 最终用户的系统（例如，个人电脑308e、移动电话308a、电视和/或电视机顶盒308c、平板装置308d、便携式音频和/或视频播放器、电子书阅读器，等等）包含可操作来检索和渲染内容的应用软件317、硬件和/或专用逻辑。用户的系统还包括软件和/或硬件，这里被称作数字版权管理引擎318，用于评估与打包内容304相关联的许可306和计算307，并实施其中的条款（和/或使应用317能够实施这样的条款），例如仅在由许可证306准许并根据计算307的情况下，通过选择性地授予用户对内容的访问。数字版权管理引擎318可与应用317在结构或功能上集成，或可包括单独的一件软件和/或硬件。替代地，或附加地，用户的系统，例如系统308c，可以与远程系统，例如系统308b（例如，服务器，用户的装置网络中的另一个装置，例如个人电脑或电视机顶盒，等等）进行通信，该远程系统使用数字版权管理引擎来做出关于是否授予用户对先前所获得的或由用户所请求的内容的访问的确定320。

[0218] 数字版权管理引擎和/或用户的系统上或与其远程通信的其他软件，也可记录关于用户对受保护内容的访问或者受保护内容的其他用途的信息。在一些实施例中，该信息的一些或全部可能被传送到远程方（例如交换所（clearinghouse）322，内容创建者、所有者或提供者302，用户的经理，代表其行动的实体，等等），例如以供在追踪所有者的个人信息的使用、分配收入（例如特许费，基于广告的收入等）、确定用户偏好、实施系统策略（例如，监测如何以及何时使用机密信息）等方面使用。将理解的是，尽管图3示出了说明性结构和一组说明性关系，但可在任何合适情境中实践本文中所述的系统和方法，且因此将理解的是，图3是出于说明和解释的目的而非限制的目的被提供的。

[0219] 图4示出了可被用来实践本发明主题的实施例的系统400的更详细示例。例如，系统400可以包括最终用户装置308、内容提供者的装置302等等的实施例。例如，系统400可包括通用计算装置，诸如个人计算机308e或网络服务器315，或专门的计算装置，诸如蜂窝电话308a、个人数字助理、便携式音频或视频播放器、电视机顶盒、电话亭（kiosk）、游戏系统，等等。系统400通常将包括处理器402、存储器404、用户界面406、用于接纳可移除存储器408的端口407、网络接口410以及用于连接前述元件的一个或多个总线412。系统400的操作通常将由在存储器404中所存储的程序的指导下操作的处理器402所控制。存储器404一般将包括高速随机存取存储器（RAM）和例如磁盘和/或闪速EEPROM的非易失性存储器两者。存储器404的某些部分可被限制，使得它们不能从系统400的其他组件读出或向该其他组件写入。端口407可包括磁盘驱动器或存储器插槽，其用于接纳计算机可读介质408，例如软盘、

CD-ROM、DVD、存储卡、SD卡、其他磁性或光学介质，等等。网络接口410通常可操作来提供系统400和其他计算装置(和/或计算装置的网络)之间经由网络420(例如互联网或内联网(例如LAN、WAN、VPN等))的连接，且可采用一种或多种通信技术来物理地产生这样的连接(例如无线、以太网，等等)。在一些实施例中，系统400可能还包括处理单元403，该处理单元403被保护免受由系统400的用户或其他实体的篡改。这样的安全处理单元可帮助增强敏感操作的安全性，例如密钥管理、签名验证以及其他方面的数字版权管理过程的安全性。

[0220] 如图4中所示，计算装置400的存储器404可包括用于控制计算装置400的操作的各种程序或模块。例如，存储器404通常将包括操作系统420，用于管理应用、外围设备等的执行；主机应用430，用于渲染受保护的电子内容；以及DRM引擎432，用于实现本文中所述的一些或全部版权管理功能。如本文中别处所述，DRM引擎432可以包括与各种其他模块互操作和/或控制各种其他模块，例如用于执行控制程序的虚拟机422，以及用于存储敏感信息的受保护数据库424，和/或一个或多个密码模块426，用于执行密码操作，例如加密和/或解密内容、计算散列函数和消息认证码、评估数字签名，等等。存储器404通常还将包括受保护内容428和相关联的许可和计算429，以及密码密钥、证书，等等(未示出)。

[0221] 在本领域的普通技术人员将理解，可利用与图4中所图示的类似或相同的计算装置，或利用实质上任何其他合适计算装置，包括不拥有图4中所示某些组件的计算装置和/或拥有未示出的其他组件的计算装置，来实践本文所述的系统和方法。因而应当理解的是，图4是出于说明而非限制的目的被提供的。

[0222] 虽然出于清楚的目的，前述内容已经以一些细节被描述，但将显而易见的是，在所附权利要求的范围之内可做出某些改变和修改。例如，虽然已经描述了利用例如'693申请中所述的DRM引擎的若干示例，但将理解的是，使用用于根据规则或策略来管理内容的任何合适软件和/或硬件可以实现本文中所述的系统和方法的实施例。应当注意的是，存在实现本文所述的过程和设备的许多替代方式。因此，当前实施例将被认为是说明性的而非限制性的，并且本发明的主题不被限制于在本文中给出的细节，而是可以在所附权利要求的范围和等同方式内被修改。

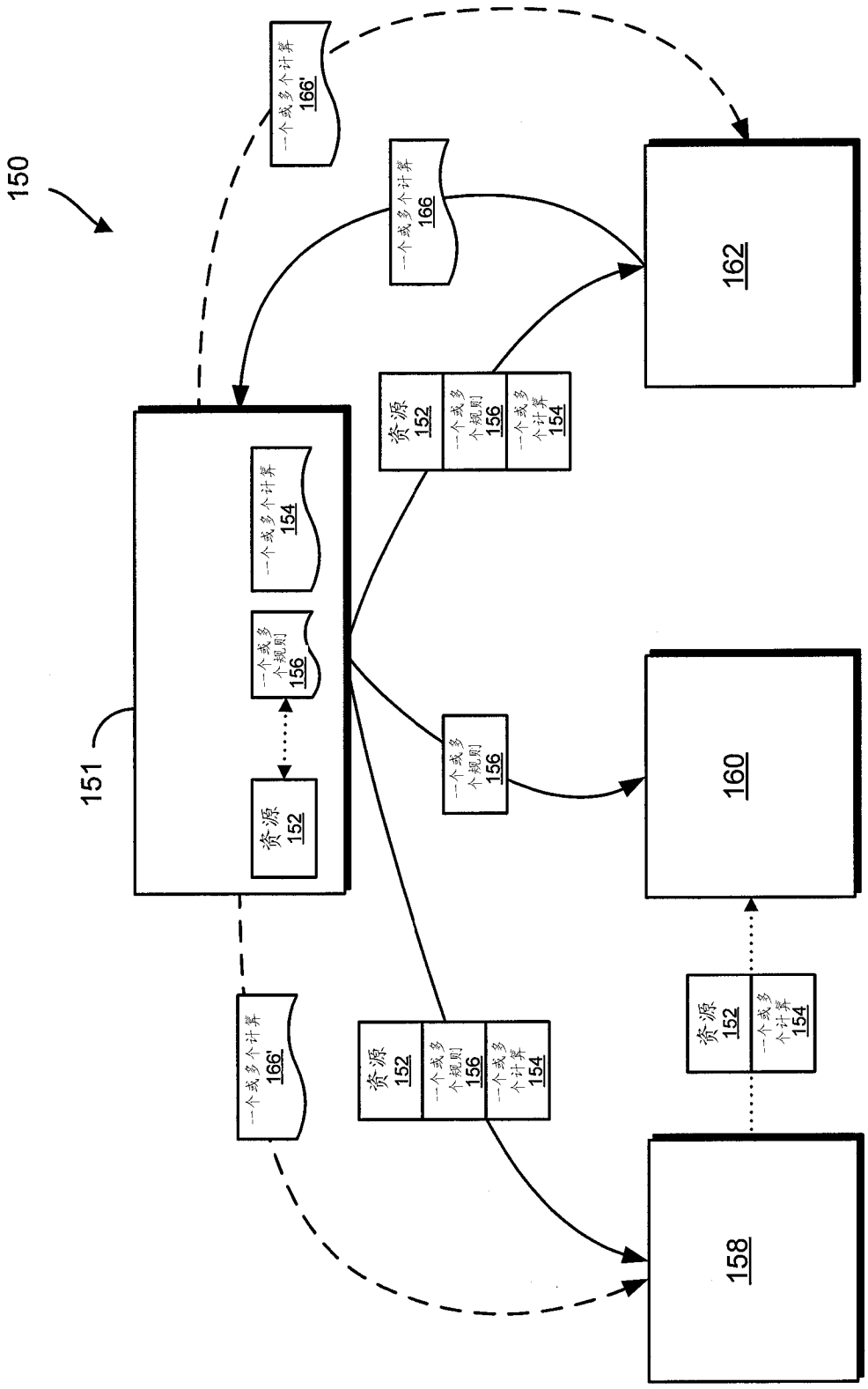

150
151
一个或多个计算 166'
一个或多个计算 166
162
资源 152
一个或多个规则 156
一个或多个计算 154
一个或多个计算 154
一个或多个规则 156
资源 152
一个或多个规则 156
160
一个或多个计算 166'
资源 152
一个或多个规则 156
一个或多个计算 154
资源 152
一个或多个计算 154
158

图 1A

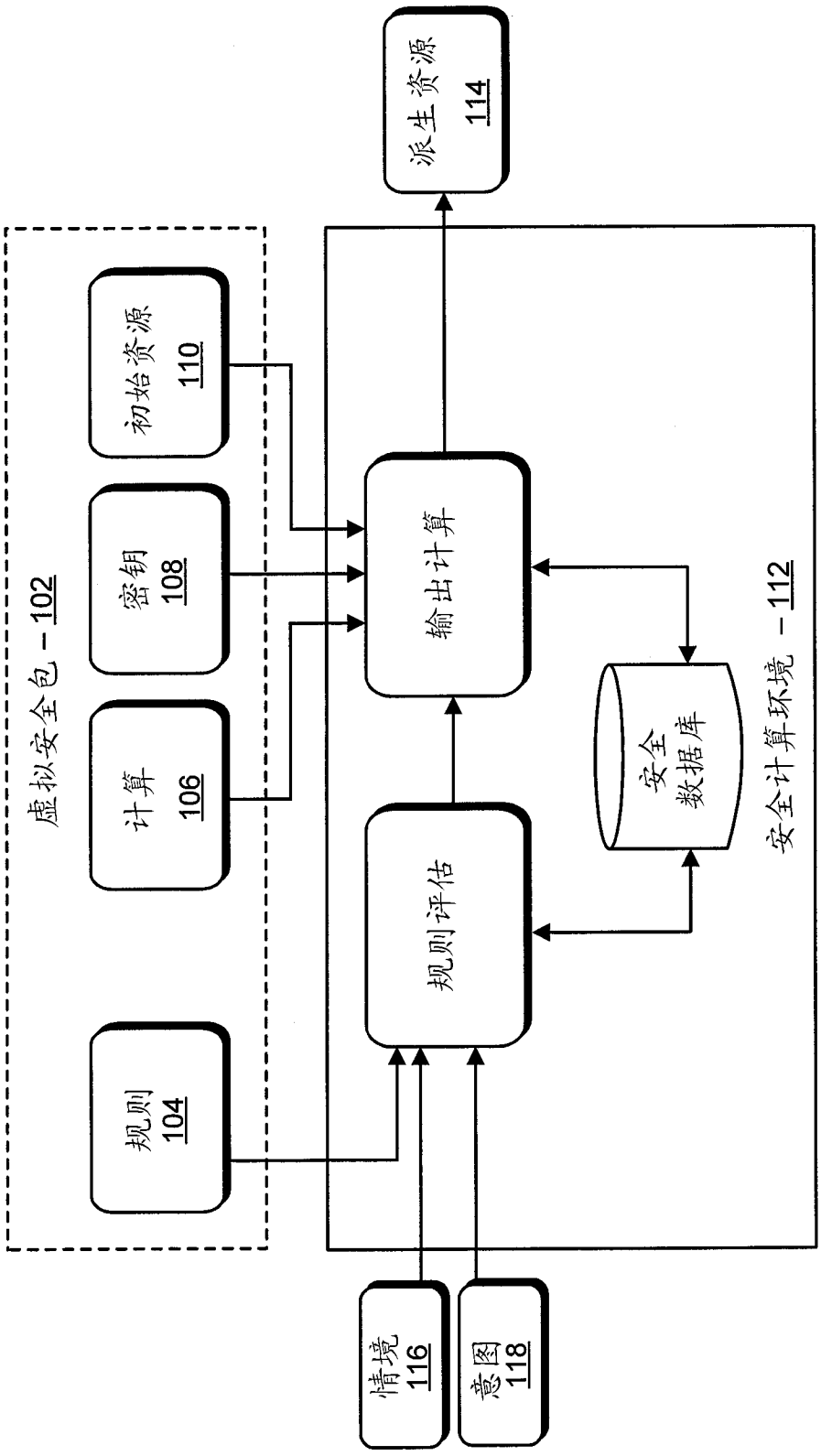

派生资源
114
虚拟安全包 – 102
初始资源
110
密钥
108
计算
106
规则
104
输出计算
规则评估
安全
数据库
安全计算环境 – 112
情境
116
意图
118

图 1B

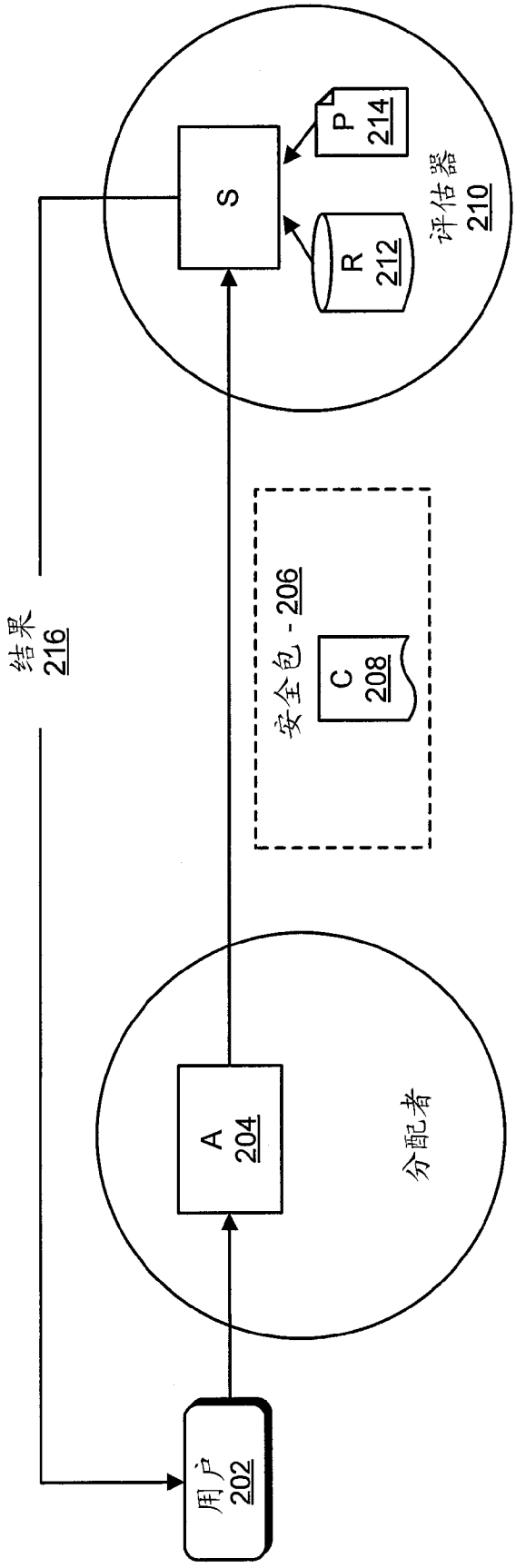


图 2

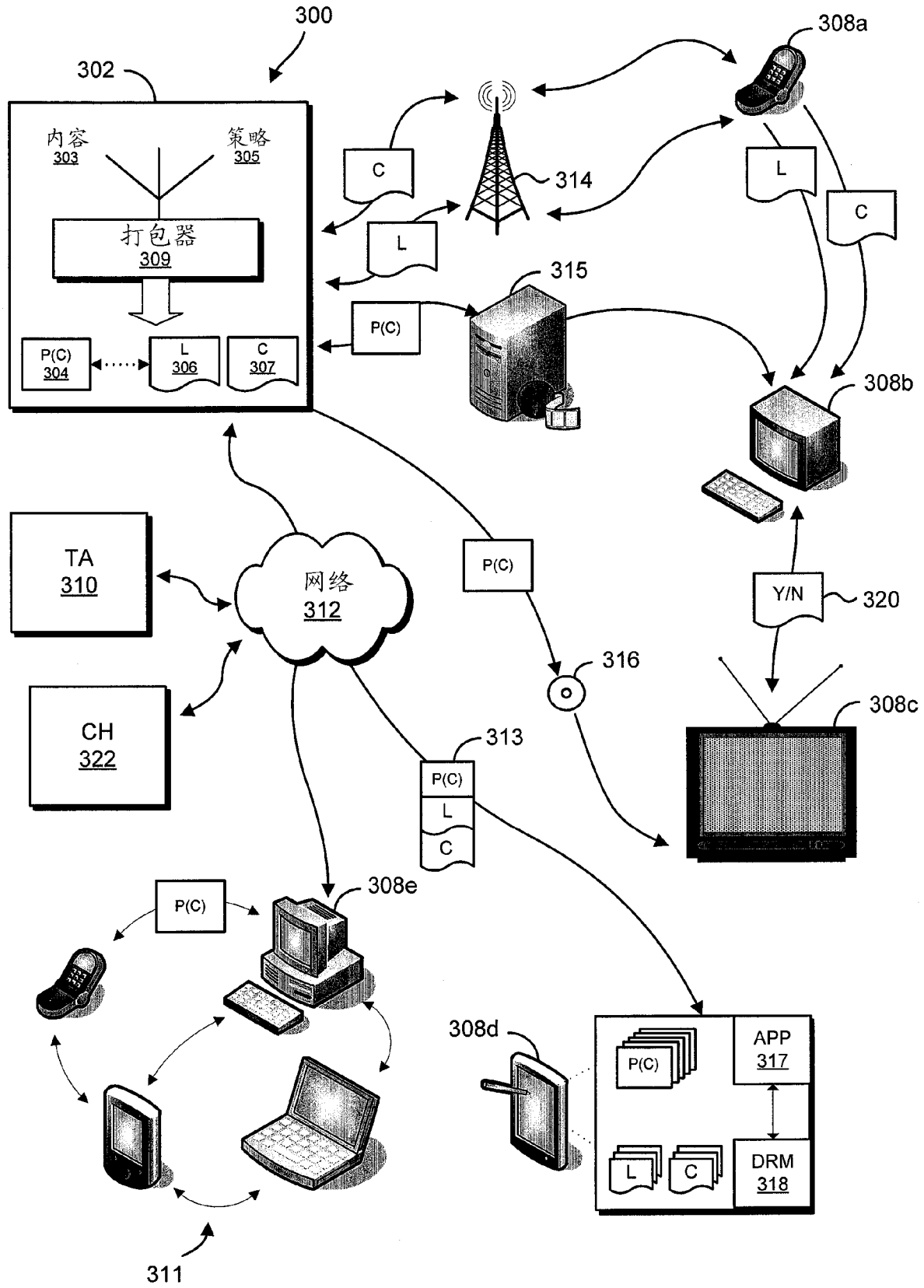

300
302
内容
303
策略
305
打包器
309
P(C)
304
L
306
C
307
C
L
314
308a
L
C
315
P(C)
308b
TA
310
网络
312
P(C)
Y/N
320
316
CH
322
313
P(C)
L
C
308c
P(C)
308e
308d
APP
317
P(C)
L
C
DRM
318
311

图 3

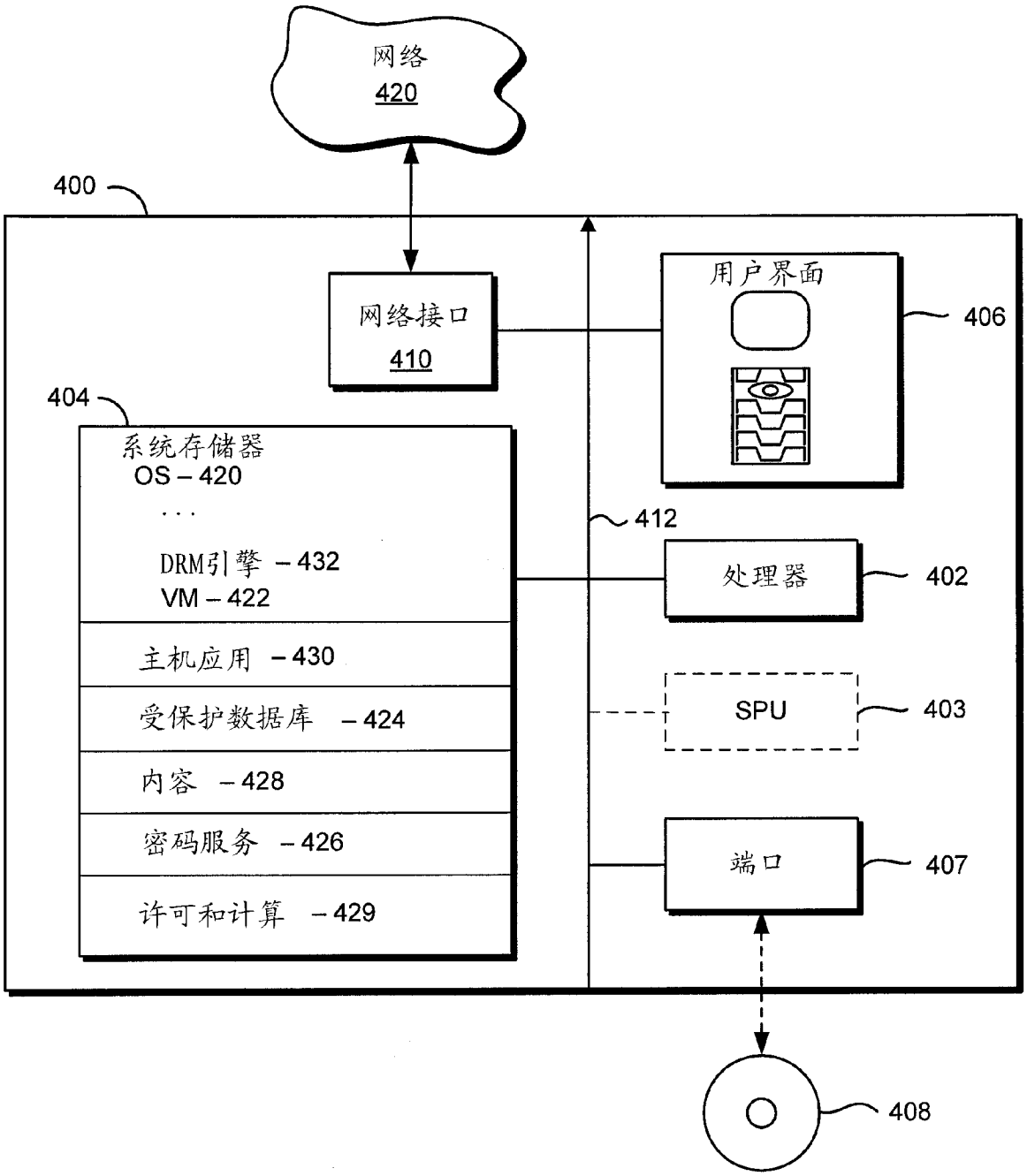

网络
420
400
网络接口
410
用户界面
406
404
系统存储器
OS – 420
...
DRM引擎 – 432
VM – 422
主机应用 – 430
受保护数据库 – 424
内容 – 428
密码服务 – 426
许可和计算 – 429
412
处理器
402
SPU
403
端口
407
408

图 4