[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04L 9/00
H04L 12/24

[12] 发明专利申请公开说明书

[21] 申请号 200410011928.6

[43] 公开日 2005 年 4 月 20 日

[11] 公开号 CN 1607762A

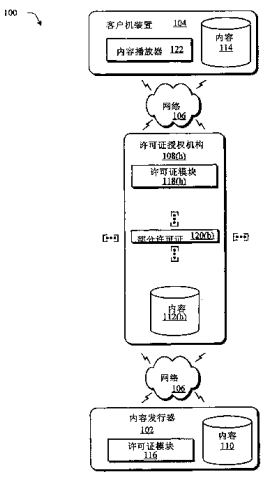
[22] 申请日 2004.9.21
[21] 申请号 200410011928.6
[30] 优先权
[32] 2003.10.14 [33] US [31] 10/685,234
[71] 申请人 微软公司
地址 美国华盛顿州
[72] 发明人 B·朱 G·顾 S·李
[74] 专利代理机构 上海专利商标事务所有限公司
代理人 谢喜堂

权利要求书 11 页 说明书 17 页 附图 9 页

[54] 发明名称 数字权限管理系统

[57] 摘要

描述了一种用于数字权限管理(DRM)系统的公共许可基础结构(PLI)。在一个实现中，一种方法包括生成一用于内容的正式许可证。该正式许可证包括用于解密该内容的解密密钥和用于访问该内容的访问规则。多个许可证授权机构被配置成提供多个部分许可证。多个部分许可证可组合来形成该正式许可证。每一许可证授权机构提供一相应的部分许可证。



ISSN1008-4274

1．一种方法，其特征在于，它包括：

生成一用于内容的正式许可证，其包括：

用于解密所述内容的解密密钥；和

用于访问所述内容的访问规则；以及

配置多个许可证授权机构来提供多个部分许可证，其中：

每一所述许可证授权机构提供一相应的所述部分许可证；以及

所述多个部分许可证可组合来形成所述正式许可证。

2．如权利要求 1 所述的方法，其特征在于，所述多个部分许可证依照一(*k*, *m*)阈值机密共享模式来提供，其中：

k 个所述部分许可证可组合来形成所述正式许可证；以及

任意 *k*-1 个或更少的所述部分许可证的知识不可以用来形成包括在所述正式许可证内的信息。

3．如权利要求 1 所述的方法，其特征在于，所述配置包括：

通过加密所述正式许可证从所述正式许可证生成一预许可证；

将一加密密钥划分成多个部分机密共享，其中，所述加密密钥用于解密所述预许可证；以及

向每一所述许可证授权机构发送所述预许可证和一相应的所述部分机密共享，使得每一所述许可证授权机构被配置成从相应的所述部分机密共享和所述预许可证生成相应的所述部分许可证。

4．如权利要求 3 所述的方法，其特征在于，每一所述许可证授权机构通过使用一可核实机密共享（VSS）模式核实所述预许可证和相应的所述部分机密共享。

5．如权利要求 1 所述的方法，其特征在于，所述配置包括：

通过加密所述正式许可证，使用一具有一公钥和一私钥的非对称加密算法从所述正式许可证生成一预许可证，其中，所述正式许可证、所述预许可证和所述公钥分别被如下表示为“*license*”、“*prel*”和“*PK*”：

$$prel = (license)^{pk};$$

依照一(*k*, *m*)阈值机密共享模式通过以下行动将所述私钥 *SK* 划分成 *m* 个部分机密共享：

生成一共享多项式*f(x)*，它被表示如下：

$f(x)=a_0+a_1x+\ldots+a_{k-1}x^{k-1}$，其中$a_0=SK$；以及

对相应的所述许可证授权机构，由id_i表示，其中$i=1,\ldots,m$，计算每一所述部分机密共享，被表示为S_i，如下：

$S_i=f(id_i)\bmod\phi(N)$，其中N是RSA模数，$\phi(N)$是欧拉ϕ函数；以及

向相应的所述许可证授权机构发送所述预许可证和一相应的所述部分机密共享，其中，每一所述许可证授权机构被配置成从相应的所述部分机密共享和所述预许可证生成相应的所述部分许可证。

6．如权利要求5所述的方法，其特征在于，每一所述许可证授权机构通过使用一可核实机密共享（VSS）模式核实所述预许可证和相应的所述部分机密共享，其中，将所述共享多项式的*f(x)*系数的k个公共证据（表示为$\{g^{a_0},\cdots,g^{a_{k-1}}\}$，其中$g\in Z_N^*$）传递到每一所述许可证授权机构$id_i$，以通过确定以下公式是否成立来核实相应的所述部分机密共享S_i的有效性：

$$g^{S_i}=g^{a_0}\cdot(g^{a_1})^{id_i}\cdot\ldots\cdot(g^{a_{k-1}})^{id_i^{k-1}}\bmod N。$$

7．如权利要求1所述的方法，其特征在于，它还包括包装所述内容以包括适合查找每一所述许可证授权机构的一个或多个网络地址。

8．如权利要求1所述的方法，其特征在于，每一所述许可证授权机构通信上耦合至一对等网络。

9．如权利要求1所述的方法，其特征在于，基于一考虑配置所述多个许可证授权机构，使得至少一个所述许可证授权机构提供两个或多个所述部分许可证，其中，所述考虑选自以下组：

至少一个所述许可证授权机构对非授权访问的安全性；

所述多个许可证授权机构的负载共享；

每一所述许可证授权机构的可用性；

每一所述许可证授权机构的网络可用性；

每一所述许可证授权机构的硬件资源；

每一所述许可证授权机构的软件资源；以及

其任一组合。

10．如权利要求1所述的方法，其特征在于，所述配置包括向所述多个许可证授权机构发送所述多个部分许可证，使得每一所述许可证授权机构储存相应的所

述部分许可证。

11．一个或多个包括计算机可执行指令的计算机可读媒质，其特征在于，当执行所述指令时，执行权利要求 1 所述的方法。

12．一种包括计算机可执行指令的计算机可读媒质，其特征在于，当由计算机执行所述指令时，指示所述计算机：

配置多个许可证授权机构来提供多个部分许可证，其中：

每一所述许可证授权机构提供一相应的所述部分许可证；

每一所述许可证授权机构具有一网络地址；

所述多个部分许可证可组合来形成一正式许可证；以及

所述正式许可证提供对内容的访问；以及

包装所述内容以包括适合查找每一所述许可证授权机构的一个或多个网络地址。

13．如权利要求 12 所述的计算机可读媒质，其特征在于，所述一个或多个网络地址包括用于查找每一所述许可证授权机构的网络地址的一个或多个代理地址。

14．如权利要求 12 所述的计算机可读媒质，其特征在于，所述一个或多个网络地址包括每一所述许可证授权机构的网络地址。

15．如权利要求 12 所述的计算机可读媒质，其特征在于，所述多个许可证授权机构被配置成依照一(k, m)阈值机密共享模式提供所述多个部分许可证，其中：

k 个所述部分许可证可组合来形成所述正式许可证；以及

任意 k-1 个或更少的所述部分许可证的知识不可以用来形成包括在所述正式许可证内的信息。

16．如权利要求 12 所述的计算机可读媒质，其特征在于，当由所述计算机执行时，所述计算机可执行指令指示所述计算机通过以下行动配置多个许可证授权机构：

通过加密所述正式许可证从所述正式许可证生成一预许可证；

将一加密密钥划分成多个部分机密共享，其中，所述加密密钥用于解密所述预许可证；以及

向每一所述许可证授权机构发送所述预许可证和一相应的所述部分机密共享，使得每一所述许可证授权机构被配置成从相应的所述部分机密共享和所述预许可证生成相应的所述部分许可证。

17. 如权利要求 16 所述的计算机可读媒质，其特征在于，每一所述许可证授权机构通过使用一可核实机密共享（VSS）模式核实所述预许可证和相应的所述部分机密共享。

18. 如权利要求 12 所述的计算机可读媒质，其特征在于，当由所述计算机执行时，所述计算机可执行指令指示所述计算机通过向所述多个许可证授权机构发送所述多个部分许可证来配置所述多个许可证授权机构，使得每一所述许可证授权机构储存相应的所述部分许可证。

19. 一种包括计算机可执行指令的计算机可读媒质，其特征在于，当由计算机执行所述指令时，指示所述计算机：

加密内容；

为所述加密内容生成一正式许可证，它包括访问规则和一用于解密所述加密内容的解密密钥；

加密所述正式许可证来生成一预许可证；

将一适合解密所述预许可证的加密密钥划分成多个部分机密共享；

向多个许可证授权机构上传所述预许可证和所述多个部分机密共享，使得每一所述许可证授权机构接收一相应的所述部分机密共享和所述预许可证；

包装所述加密内容以包括适合查找每一所述许可证授权机构的一个或多个网络地址；以及

分发所包装的内容。

20. 如权利要求 19 所述的计算机可读媒质，其特征在于，所述多个许可证授权机构被配置成依照一(k, m)阈值机密共享模式提供所述多个部分许可证，其中：

k 个所述部分许可证可组合来形成所述正式许可证；以及

任意 k-1 个或更少的所述部分许可证的知识不可以用来形成包括在所述正式许可证内的信息。

21. 如权利要求 19 所述的计算机可读媒质，其特征在于，每一所述许可证授权机构通过使用一可核实机密共享（VSS）模式核实所述预许可证和相应的所述部分机密共享。

22. 一种方法，其特征在于，它包括：

通过网络从多个许可证授权机构获取多个部分许可证，其中，每一所述部分许可证分别由一不同的所述许可证授权机构提供；以及

从所述多个部分许可证形成一正式许可证，其中，所述正式许可证包括用于访问内容的访问规则和解密密钥。

23．如权利要求 22 所述的方法，其特征在于，所述获取包括：

检查所述内容以找出多个许可证授权机构的多个网络地址；

从所述多个许可证授权机构请求所述多个部分许可证；以及

接收具有由每一所述许可证授权机构提供的一个或多个所述部分许可证的一个或多个通信。

24．如权利要求 22 所述的方法，其特征在于，所述形成包括组合所述多个部分许可证来形成所述正式许可证。

25．如权利要求 22 所述的方法，其特征在于，所述多个部分许可证依照一(*k*, *m*)阈值机密共享模式来提供，其中：

k 个所述部分许可证可组合来形成所述正式许可证；以及

任意 *k*-1 个或更少的所述部分许可证的知识不能用来形成包括在所述正式许可证内的信息。

26．如权利要求 25 所述的方法，其特征在于，它还包括确定是否接收了 *k* 个正确的部分许可证。

27．如权利要求 22 所述的方法，其特征在于：

通过以下行动从所述多个许可证授权机构获取所述多个部分许可证：

依照以下公式，由每一所述许可证授权机构 id_i 从一部分机密共享 S_i 和一预许可证 *prel* 计算所述部分许可证 $prel_i$：

$$prel_i = (prel)^{S_i} \bmod N ;$$

生成一随机数 *u* 来计算 $A_1 = g^u$， $A_2 = prel^u$， $r = u - c * S_i$，以及

$$c = hash(g^{S_i}, prel, A_1, A_2)；以及$$

由每一所述许可证授权机构传递所述部分许可证 $prel_i$、A_1、A_2 和 *r*；以及

所述正式许可证通过以下行动从所述多个部分许可证形成：

通过以下步骤，通过确认每一所述部分许可证 $prel_i$ 确定是否接收了 *k* 个正确的部分许可证：

从一共享多项式的系数的公共证据计算

$$g^{S_i} = g^{a_0} \cdot (g^{a_1})^{id_i} \cdot \ldots \cdot (g^{a_{k-1}})^{id_i^{k-1}} \bmod N$$

所述公共证据被表示为$\{g^{a_0},\cdots,g^{a_{k-1}}\}$，它用于生成所述部分机密共享$S_i$，其中$g \in Z_N^*$；

应用$c = hash(g^{S_i}, prel_i, A_1, A_2)$来计算$c$；以及

对每一所述部分许可证$prel_i$检查$g^r \cdot (g^{S_i})^c = A_1$和$prel^r \cdot (prel_i)^c = A_2$是否成立，并且如果成立，每一所述部分许可证$prel_i$是有效的；并当获取$k$个有效的所述部分许可证时，组合所述多个部分许可证来形成所述正式许可证，被表示为*license*，其中：

$$license = \prod_i (prel_i)^{l_{id_i}(0)} = (prel)^{\sum_i S_i \cdot l_{id_i}(0)}$$

$$= (prel)^{SK} = ((license)^{PK})^{SK} \bmod N,$$

其中，$l_{id_i}(x) = \prod_{j=1, j\neq i}^{k} \frac{x - id_j}{id_i - id_j}$。

28．一个或多个包括计算机可执行指令的计算机可读媒质，其特征在于，当执行所述指令时，执行权利要求22所述的方法。

29．一种包括计算机可执行指令的计算机可读媒质，其特征在于，当由计算机执行所述指令时，指示所述计算机：

检查包装的内容以找出多个许可证授权机构的多个网络地址；

从所述多个许可证授权机构请求多个部分许可证；

从所述多个许可证授权机构接收所述多个部分许可证，其中每一所述许可证授权机构提供至少一个所述部分许可证；

组合所述多个部分许可证来形成一正式许可证，其中，所述正式许可证包括访问规则和用于解密所述包装的内容的解密密钥；以及

通过使用所述加密密钥解密所述包装内容并检查所述正式许可证的访问规则输出所述内容。

30．如权利要求29所述的计算机可读媒质，其特征在于，所述多个部分许可证依照一(*k*, *m*)阈值机密共享模式来提供，其中：

*k*个所述部分许可证可组合来形成所述正式许可证；

任意*k*-1个或更少的所述部分许可证的知识不能用来形成包括在所述正式许可证内的信息。

31．一种方法，其特征在于，它包括：

以第一排列配置多个许可证授权机构来提供多个部分许可证，其中：

每一所述许可证授权机构提供至少一个所述部分许可证；以及

所述多个部分许可证可组合来形成一包括访问规则和用于内容的解密密钥的正式许可证；以及，更新所述第一排列来形成一第二排列，使得：

所述第二排列中的每一所述许可证授权机构提供可组合来形成所述正式许可证的多个更新的部分许可证的至少一个；以及

所述第一排列中提供的所述部分许可证不能与所述更新的部分许可证组合来形成所述正式许可证。

32．如权利要求 31 所述的方法，其特征在于，所述更新周期性地执行。

33．如权利要求 31 所述的方法，其特征在于，所述更新通过以下步骤执行：

由每一许可证授权机构 i 使用一随机更新多项式 $f_{i,update}(x)$ 生成一随机 (k, m) 共享，其中：

$$f_{i,update}(x) = b_{i,1}x + \ldots b_{i,k-1}x^{k-1}$$；以及

由每一所述许可证授权机构 i 分发一子共享 S_{ij}，使得每一所述许可证授权机构 i 具有一来自另一所述许可证授权机构的相应的所述子共享 S_{ij}，其中：

所述子共享 $S_{i,j} = f_{i,update}(j), j = 1,\cdots,m$ 由每一所述许可证授权机构 i 计算；

所述子共享 S_{ij} 被添加到每一所述许可证授权机构的所述原始共享 S_i 来形成一新的更新的共享

$$S_i' = S_i + \sum_{j=1}^{m} S_{j,i}$$；以及

形成一新的机密共享多项式 $f_{new}(x)$，它是用于生成所述第一排列中的所述多个部分许可证的原始多项式 $f(x)$ 与所述随机生成的多项式 $f_{i,update}(x)$ 的每一个的总和。

34．一种内容发行器，其特征在于，它包括：

处理器；以及

存储器，它被配置成维护：

一正式许可证，它包括访问规则和用于内容的解密密钥；以及

一许可证模块，它可在所述处理器上执行来形成包括用于配置多个许可证授权机构的数据的一个或多个传输，使得：

每一所述许可证授权机构提供多个部分许可证之一；以及

所述多个部分许可证可组合来形成所述正式许可证。

35．如权利要求 34 所述的内容发行器，其特征在于，所述多个许可证授权机

构依照一(*k*, *m*)阈值机密共享模式被配置成提供所述多个部分许可证，其中：

k 个所述部分许可证可组合来形成所述正式许可证；以及

任意 *k*-1 个或更少的所述部分许可证的知识不能用来形成包括在所述正式许可证内的信息。

36. 如权利要求 34 所述的内容发行器，其特征在于：

所述配置包括：

通过加密所述正式许可证从所述正式许可证生成一预许可证；以及

将一加密密钥划分成多个部分机密共享，其中所述加密密钥用于解密所述预许可证；以及

所述一个或多个传输包括所述预许可证和所述多个部分机密共享，使得每一所述许可证授权机构被配置成从一相应的所述部分机密共享和所述预许可证生成一相应的所述部分许可证。

37. 如权利要求 34 所述的内容发行器，其特征在于，所述配置包括向所述多个许可证授权机构发送所述多个部分许可证，使得每一所述许可证授权机构储存相应的所述部分许可证。

38. 一种包括具有多个节点的对等网络的数字权限管理系统，其特征在于：

一个所述节点包括一可执行来形成一个或多个传输的许可证模块，其中，每一所述传输包括一预许可证和一用于加密所述预许可证的加密密钥的部分机密共享；

至少两个所述节点被配置成从相应的所述传输中接收的一相应的所述部分机密共享和所述预许可证生成多个部分许可证的相应的一个；以及

k 个所述部分许可证可组合来形成一包括加密密钥和用于访问内容的访问规则的正式许可证。

39. 如权利要求 38 所述的数字权限管理系统，其特征在于，一个或多个所述节点提供所述内容。

40. 如权利要求 38 所述的数字权限管理系统，其特征在于，任意 *k*-1 个或更少的所述部分许可证的知识不能用来形成包括在所述正式许可证内的信息。

41. 一种包括具有多个节点的对等网络的数字权限管理系统，其特征在于：

至少两个所述节点的每一个被配置成提供多个部分许可证的至少一个；以及

一个所述节点包括：

一用于从所述多个部分许可证形成一正式许可证的数字权限管理模块，其中，所述正式许可证包括访问规则和用于解密加密内容的解密密钥；以及

一用于输出使用所述正式许可证访问的内容的内容播放器。

42．如权利要求41所述的数字权限管理系统，其特征在于，所述多个部分许可证依照一(*k*, *m*)阈值机密共享模式来提供，其中：

*k*个所述部分许可证可组合来形成所述正式许可证；以及

任意*k*-1个或更少的所述部分许可证的知识不能用来形成包括在所述正式许可证内的信息。

43．一种客户机装置，其特征在于，它包括：

处理器；以及

存储器，它被配置成维护：

一包括适合查找多个许可证授权机构的一个或多个网络地址的包装内容，其中，每一所述许可证授权机构储存一个或多个部分许可证；

一可在所述处理器上执行来输出内容的内容播放器；以及

一数字权限管理模块，它可在所述处理器上执行的来：

使用所述一个或多个网络地址从所述多个许可证授权机构获取所述部分许可证；以及

从所获取的部分许可证形成一正式许可证，其中，所述正式许可证提供对由所述内容播放器输出的所述包装内容的访问。

44．如权利要求43所述的客户机装置，其特征在于，可在所述处理器上执行的所述数字权限管理模块通过以下步骤获取所述部分许可证：

检查所包装的内容以找出所述多个许可证授权机构的所述一个或多个网络地址；

从每一所述许可证授权机构请求一个或多个所述部分许可证；以及

接收具有由每一所述许可证授权机构提供的所述一个或多个部分许可证的一个或多个通信。

45．如权利要求43所述的客户机装置，其特征在于，所述多个部分许可证依照一(*k*, *m*)阈值机密共享模式来提供，其中：

*k*个所述部分许可证可组合来形成所述正式许可证；以及

任意*k*-1个或更少的所述部分许可证的知识不能用来形成包括在所述正式许

可证内的信息。

46. 如权利要求 43 所述的客户机装置，其特征在于，所述一个或多个网络地址包括一用于查找每一所述许可证授权机构的网络地址的代理地址。

47. 如权利要求 43 所述的客户机装置，其特征在于，所述一个或多个网络地址包括每一所述许可证授权机构的网络地址。

48. 如权利要求 43 所述的客户机装置，其特征在于，可在所述处理器上执行的所述数字权限管理模块：

从所述多个许可证授权机构获取所述部分许可证，其中，每一所述许可证授权机构通过执行以下步骤提供一相应的所述部分许可证：

由每一所述许可证授权机构依照以下公式从一部分机密共享 S_i 和一预许可证 *prel* 计算所述部分许可证 $prel_i$：

$$prel_i = (prel)^{S_i} \bmod N ;$$

生成一随机数 u 来计算 $A_1 = g^u$， $A_2 = prel^u$， $r = u - c * S_i$，以及

$$c = hash(g^{S_i}, prel_i, A_1, A_2)；以及$$

由每一所述许可证授权机构传递所述部分许可证 $prel_i$、A_1、A_2 和 r；以及

所述正式许可证通过以下步骤从所述多个部分许可证形成：

通过以下步骤验证每一所述部分许可证 $prel_i$ 确定是否接收了 k 个正确的部分许可证：

从一共享多项式系数的公共证据计算

$$g^{S_i} = g^{a_0} \cdot (g^{a_1})^{id_i} \cdot \ldots \cdot (g^{a_{k-1}})^{id_i^{k-1}} \bmod N$$

所述证据被表示为 $\{g^{a_0}, \cdots, g^{a_{k-1}}\}$，它们用于生成所述部分机密共享 S_i，其中 $g \in Z_N^*$；

应用 $c = hash(g^{S_i}, prel_i, A_1, A_2)$ 来计算 c；以及

对每一所述部分许可证 $prel_i$ 检查 $g^r \cdot (g^{S_i})^c = A_1$ 和 $prel^r \cdot (prel_i)^c = A_2$ 是否成立，如果成立，则每一所述部分许可证 $prel_i$ 是有效的；以及

当获取了 k 个有效的所述部分许可证时，组合所述多个部分许可证来形成所述正式许可证，它被表示为 *license*，其中：

$$license = \prod_i (prel_i)^{l_{id_i}(0)} = (prel)^{\sum_i S_i \cdot l_{id_i}(0)}$$

$$= (prel)^{SK} = ((license)^{PK})^{SK} \bmod N ,$$

其中，$l_{id_i}(x)=\prod_{j=1,j\neq i}^{k}\frac{x-id_j}{id_i-id_j}$。

数字权限管理系统

技术领域

本发明一般涉及数字权限管理领域，尤其涉及分布式数字权限管理系统。

背景技术

用户能够以日益增长的各种方式访问很大范围的内容。如软件和数字媒体等内容的广泛可用性，以及通过因特网对内容的简易访问导致了内容的无意识和非授权使用。可以采用数字权限管理（DRM）来管理内容从创建到消费的权限，并可保护数字内容不被非法访问或复制。大多数 DRM 系统基于加密，即对内容进行加密和分发。传统地，想要输出加密内容的消费者首先必需获取访问该内容的许可并获得该加密内容的解密密钥，解密密钥可以加密许可证的形式提供。DRM 系统通过使用加密许可证强制了数字内容的正确使用。

在常规 DRM 系统中，由集中式许可证服务器处理许可证获取请求。这令集中式许可证服务器的运行和维护变得负载重、复杂且昂贵，并令其成为 DRM 系统中的薄弱环节。例如，集中式许可证服务器的故障可破坏正常的 DRM 服务。此外，小的内容提供者，如对等网络中的对等体，可能无法负担提供和/或使用集中式许可证服务器的服务的费用。

对等网络最近在学术界和商业中吸引了日益增加的注意力。对等网络提供了许多合乎需要的特征，如自适应、自组织、负载平衡、故障容许、低成本、高可用性、可量测性，并可被配置成提供大量的资源。对等网络显现为一种共享大量数据的普及方式，如由对等体下载被认为可用于通过对等 web 站点下载的歌曲。然而，大多数对等网络不具备数字权限管理或访问控制。因此，对等网络可能会侵犯被认为可用于由对等网络下载的作品中的版权。

因此，始终需要一种用于数字权限管理系统的分布式公共许可基础结构。

发明内容

描述了一种用于数字权限管理（DRM）的公共许可基础结构（PLI）。DRM

系统提供了诸如歌曲、图像、文档、数字媒体、软件等内容的保护。可通过一分布式 PLI 提供 DRM 系统，其中，由多个许可证授权机构提供多个部分许可证。许可证授权机构通过网络通信来耦合。部分许可证可组合以形成可用于输入内容的正式许可证。

可以采用一(*k*, *m*)阈值机密共享模式，使得可以使用 *m* 个部分许可证的任意 *k* 个来形成正式许可证。通过实现(*k*, *m*)阈值机密共享模式，DRM 系统可以是故障容许的，使得如果一个许可证授权机构无法提供部分许可证，其它许可证授权机构可提供部分许可证来形成正式许可证。也可以通过密码算法，如先进加密标准（AES）以及 Rivest、Shamir 和 Adleman（RSA）来增强描述的 DRM 系统的可靠性和入侵容许，以提供健壮的内容保护并确保仅授权用户可访问该内容。因此，DRM 系统可以在对等网络中使用，并由此调节了对等网络的复制和高速缓存机制，而保护了内容不受非授权访问。

在一个实现中，一种方法包括为内容生成一正式许可证。该正式许可证包括一用于解密该内容的解密密钥，还包括用于访问该内容的访问规则。多个许可证授权机构被配置成提供多个部分许可证。部分许可证可组合来形成正式许可证。每一许可证授权机构提供部分许可证的相应的一个或多个。

在另一实现中，一种方法包括通过网络从多个许可证授权机构获取多个部分许可证。由不同的许可证授权机构分别提供每一部分许可证。从包括用于访问内容的访问规则和解密密钥的多个部分许可证形成正式许可证。

附图说明

图 1 所示是在其中示出了在对等网络中采用公共许可基础结构的数字权限管理（DRM）系统的一个示例性实现。

图 2 所示是在其中更详细地示出了图 1 的 DRM 系统的客户机装置、内容发行器和许可证授权机构的一个示例性实现。

图 3 是所示是一个示例性实现的过程的流程图，其中 DRM 系统中的多个许可证授权机构被配置成提供可用于形成正式许可证的部分许可证。

图 4 是描述一个示例性实现的过程的流程图，其中从图 3 的部分许可证形成正式许可证以输出内容。

图 5 所示是一个示例性实现的过程的流程图，其中 DRM 系统采用一(*k*, *m*)阈

值机密共享模式使得多个许可证授权机构被配置成提供可用于形成正式许可证的部分许可证。

图 6 是一个示例性实现中的过程的流程图，其中由客户机装置形成图 5 的正式许可证以播放内容。

图 7 所示是一个示例性实现的过程流，它示出了使用一(*k*, *m*)阈值机密共享模式来提供用于形成正式许可证的部分许可证的 DRM 系统中的冗余。

图 8 所示是一个示例性实现的过程的流程图，其中在采用(*k*, *m*)阈值机密共享模式的 DRM 系统中使用更新模式。

图 9 所示描述了在其中生成部分机密共享的子共享的示例性更新模式。

在该讨论的实例中，使用相同的标号标识相同的结构和组件。

具体实施方式

综述

描述了一种用于数字权限管理（DRM）系统的公共许可基础结构（PLI）。本发明描述的 PLI 可以在分散型系统中实现来为 DRM 系统中的消费者提供公共许可证服务。PLI 可担当不昂贵的许可证服务提供者来保护内容，并因此可以由各种各样的内容发行器使用。例如，作者可以保护内容不受非许可使用的方式向消费者提供书的副本、音乐组可以同样的方式提供歌曲等等。由此 DRM 系统可对无法负担常规的基于服务器/客户机的 DRM 系统和传统分发通道的小内容提供者，如对等网络中的对等体有用。

该 PLI 可包括共同为消费者提供分布式 DRM 许可证服务的多个许可证授权机构。例如，每一许可证授权机构可提供多个部分许可证的一个或多个。多个部分许可证可用于形成由消费者的内容播放器使用的正式许可证以输出内容。多个部分许可证可由许可证授权机构使用一阈值机密共享模式提供，使得该正式许可证可从若干个指定的部分许可证形成，如参考图 5-8 将详细描述的。基于 PLI 和许可证授权机构，DRM 系统可为对等网络中的消费者提供内容的保护和数字权限管理。由此，PLI 可调节对等网络的功能，如分发、访问和搜索内容，而仍保护在对等网络中提供的内容。

环境

图1所示是在其中示出了在对等网络中采用PLI的DRM系统100的一个示例性实现。DRM系统100包括通过网络106通信上耦合至客户机装置104的内容发行器102。多个许可证授权机构108(h)也通信上耦合至网络106。客户机装置104、内容发行器102和多个许可证授权机构108(h)的每一个表示网络106中的一个节点。节点可以被认为是一种发送数据的连接点，如向其它节点提供数据的再分发点和/或作为数据的目的地和/或源的端点。

网络106被配置成对等网络。对等网络允许网络106的节点访问位于每一节点，即客户机装置104、内容发行器102和多个许可证授权机构108(h)上的共享资源。过去已知且使用的对等网络的示例包括以下网络：

• Freenet（免费网），由I.Clarke、B.Wiley、O.Sanberg和T.Hong在“Freenet: A Distributed Anonymous Information Storage and Retrieval System（免费网：一种分布式匿名信息存储和检索系统）”，国际会刊 *Workshop on Design Issues in Anonymity and Unobservability*, Springer Verlag, LNCS 2009, 2001中描述；

•Chord（图形树），由I.Stoica、R.Morris、D.Karger、M.F.Kaashoek、H.Balakrishnan在“Chord A Scalable Peer-to-peer Lookup Service for Internet Applications（图形树，一种用于因特网应用的可伸缩对等查找服务）”，会刊ACM SIGCOMM'01，圣地亚哥，加利福尼亚州，美国2001中描述；

• CAN（内容可寻址网络），由S.Ratnasamy、P.Francis、M.Handley、R.Karp和S.Shenker在“A Scalable Content-Addressable Network（一种可伸缩内容可寻址网络）”，会刊ACM SIGCOMM'01，圣地亚哥，加利福尼亚州，美国，2001中描述；

•Pastry，由A.Rowstron和P.Druschel在“Pastry: Scalable, Decentralized Object Location and Routing for Large-Scale Peer-to-Peer Systems（Pastry：用于大规模对等系统的可伸缩、分散型对象定位和路由）”，IFIP/ACM，国际会议 *Distributed Systems Platforms(Middleware)*，2001中描述；以及

• Tapestry，由B.Y.Zhao、J.Kubiatowicz和A.D.Joseph在“Tapestry：An Infrastructure for Falut-tolerant Wide-Area Location and Routing（Tapestry：一种用于故障容许广域定位和路由的基础结构）”，技术报告编号UCB/CSD-01-1141，加利福尼亚大学，伯克利中描述。

对等网络可提供各种特征，如冗余和故障容许。当由对等网络的节点复制内

容时，储存在对等网络中的内容可逐渐传播。例如，内容 110 可由内容发行器 102 提供以与网络 106 的其它节点，即客户机装置 104 和多个许可证授权机构 108(h)共享。内容 110 可由网络 106 的每一节点访问，并由相应的节点储存。例如，每一许可证授权机构 108(h)可分别储存内容 112(h)。因此，客户机装置 104 可访问来自多个许可证授权机构 108(h)的内容 112(h)和/或来自内容发行器 102 和/或网络 106 中的其它节点的内容 110。客户机装置 104 也可提供内容 114 用于通过网络 106 分发。例如，内容 114 可从客户机装置 104 起源以跨网络分发。另外，内容 114 可由客户机装置 104 从由网络 106 的任一其它节点，如许可证授权机构 108(h)和/或内容发行器 102 储存的内容复制。由此，内容在对等网络中可变得高度冗余，会导致数据的增加的可靠性和可用性。这可以有效地降低由内容发行器 102 提供内容的操作成本，并由此可以由各种各样的用户使用，如各种各样的内容发行器和/或客户机装置。

内容发行器 102 包括由内容发行器 102 执行来提供数字权限管理的许可证模块 116。该许可证模块 116 可用于生成对应于由内容发行器 102 为在网络 106 上分发而发行的内容 110 的正式许可证。正式许可证令对应于该正式许可证的内容可被访问。例如，正式许可证可包括用于访问该内容的解密密钥和访问规则，如由内容提供者许可的访问和/或对消费者可用的访问。

每一许可证授权机构 108(h)也包括相应的许可证模块 118(h)，也用于提供 DRM 系统 100 中的数字权限管理。例如，内容发行器 102 的许可证模块 116 可用于向每一许可证授权机构 108(h)提供数据，使得其每一相应的许可证模块 118(h)可分别提供一个或多个部分许可证 120(b)。部分许可证 120(b)可用于形成用于提供对内容的访问的一个或多个正式许可证。提供部分许可证的许可证授权机构 108(h)的配置的进一步描述可以在图 3 和 5 中找到。

客户机装置 104 包括输出内容，如储存在客户机装置 104 上的内容 114、从相应的许可证授权机构 108(h)获取的内容 112(h)以及从内容发行器 102 获取的内容 112 的内容播放器 122。当由客户机装置 104 执行时，内容播放器 122 可获取一个或多个部分许可证 120(b)来形成正式许可证。通过在 DRM 系统 100 中分布部分许可证的供应，可提供各种功能。例如，可令 DRM 系统 100 变得故障容许，使得即使一个或多个许可证授权机构 108(h)变得不可用时也可以形成正式许可证。另外，DRM 系统 100 可以是入侵容许的，没有单个易受攻击点被攻击来获取正式许可证，

如参考图 7 更详细描述的。

图 2 所示是在其中更详细地示出了图 1 的客户机装置 104、内容发行器 102 和许可证授权机构 108(h)的一个示例性实现。内容发行器 102 包括处理器 202 和存储器 204。示出许可证模块 116 在处理器 202 上执行，并可储存在存储器 204 中。示出存储器 204 储存内容 110 和对应于内容 110 的正式许可证 206。正式许可证 206 提供使内容 110 可以被输出的信息，如解密密钥和访问规则。访问规则可指定内容发行器允许的访问权限和/或客户机专用访问规则。例如，内容发行器可基于不同的付款数量指定用于访问内容的不同的持续时间。因此，消费者的访问规则可取决于购买的持续时间。正式许可证 106 可由内容发行器 102 以各种方式提供。例如，可通过许可证模块 116 的执行自动生成正式许可证 206。另外，可由内容的开发者指定正式许可证 206，如由开发者书写并连同内容 110 一起上传到内容发行器 102。

许可证模块 116 可在内容发行器 102 的处理器 202 上执行，以创建可由许可证授权机构 108(h)的许可证模块 118(h)用于提供多个部分许可证 120(1)-120(B)的数据。在一个实现中，由内容发行器 102 向许可证授权机构 108(h)提供一个或多个部分许可证 120(1)-120(B)，即，数据是实际的部分许可证 120(1)-120(B)。部分许可证 120(1)-120(B)然后如图所示地储存在存储器 210 中。

在另一实现中，向许可证授权机构 108(h)提供数据，许可证授权机构 108(h)可从该数据生成一个或多个部分许可证 120(1)-120(B)。例如，示出许可证授权机构 108(h)的许可证模块 118(h)在处理器 208 上执行，并可储存在存储器 210 中。当在处理器 208 上执行许可证模块 118(h)时，许可证模块 118(h)响应于对一个或多个部分许可证 120(1)-120(B)的请求，生成多个部分许可证 120(1)-120(B)的一个或多个。部分许可证的生成参考图 6 有更详细的描述。

客户机装置 104 包括输出内容 114 的内容播放器 122。示出内容播放器 122 在处理器 212 上执行，并可储存在存储器 214 中。当执行时，内容播放器 122 可输出各种内容，如歌曲、影片、图片、文档等等。

示出内容播放器 122 包括 DRM 模块 216。当在处理器 212 上执行时，DRM 模块 216 从图 1 的多个部分许可证 120(b)的两个或多个生成正式许可证。然后可由内容播放器 122 读取正式许可证来输出内容 114。由 DRM 模块 216 形成正式许可证相对图 4 和 6 有更详细的描述。DRM 模块 216 可被配置成安全且防篡改的一个或多个软件模块。例如，尽管内容播放器 122 可与 DRM 模块 216 进行交互，DRM

模块 216 可不被内容播放器 122 修改。

为获取图 1 的多个部分许可证 120(b)的一个或多个，内容 114 可包括许可证授权机构 108(h)的网络地址 218，许可证授权机构 108(h)储存了用于形成正式许可证的部分许可证。例如，内容发行器 102 可包装内容 114 来包括图 1 的许可证授权机构 108(h)的地址 218，许可证授权机构 108(h)具备部分许可证和/或生成部分许可证的数据。包括地址 218 的内容 114 可通过网络 106 分发，然后如图所示由客户机装置 104 获取。为输出内容，内容播放器 122 启动 DRM 模块 216 来形成正式许可证以输出内容 114。DRM 模块 216 可获取图 1 的许可证授权机构 108(h)的地址 218，这些许可证授权机构分别提供了来自内容 114 的部分许可证 120(b)。由 DRM 模块形成正式许可证的更多的示例可以在图 4 和 6 中找到。

通过在相应的许可证授权机构 108(h)中分布图 1 的部分许可证 120(b)的供应，保护了正式许可证免受攻击。然而，给予足够长的时间，攻击者最终攻克用于形成正式许可证的足够多的许可证授权机构 108(h)。为阻止这一攻击，可以用提前的机密共享模式通过执行一个或多个更新模块 220、222 来更新图 1 的部分许可证 120(b)。例如，许可证授权机构 108(h)和/或内容发行器 102 的每一个可包括更新模块 220、222 之一。示出更新模块 220、222 在相应的处理器 202、208 上执行，并可储存在相应的存储器 204、210 中。当执行时，更新模块 220、222 可周期性地在两个或多个许可证授权机构 108(h)中更新图 1 的部分许可证 120(b)的排列。通过更新排列，图 1 的不同的相应许可证授权机构 108(h)可以被配置成提供部分许可证 120(b)。另外，部分许可证 120(b)还可以被划分并储存在不同的许可证授权机构 108(h)上，使得需要不同的部分许可证来形成正式许可证。因此，攻击者必须在更新部分许可证之前攻克足够数量的生成正式许可证的许可证授权机构 108(h)。否则，攻击者被迫重新开始攻击。更新模式的进一步讨论可以在图 8 和 9 中找到。

在分布式 DRM 系统中生成并形成正式许可证

图 3 所示是示例性实现的过程 300 的流程图，其中，DRM 系统中多个许可证授权机构被配置成提供可用于形成正式许可证的部分许可证。在块 302，通过执行内容发行器 102 上的许可证模块 116 生成用于内容 110 的正式许可证 206。正式许可证 206 适合图 2 的客户机装置 104 用于输出内容 110。例如，正式许可证 206 可包括访问规则 304、解密密钥 306 和其它信息 308。访问规则 304 可指定访问内容

110 的规则和消费者具有的权限，和/或内容发行器 104 允许访问内容 110 的规则和权限。解密密钥 306 可用于对内容 110 进行解密。

在块 310，从正式许可证生成适合提供部分许可证 312、314、316 的数据。在一个实现中，数据是实际的部分许可证 312、314、316，它们可组合来形成正式许可证 206。在另一实现中，数据可由每一许可证授权机构 108(1)、108(h)用于通过执行各自的许可证模块 118(1)、118(h)生成部分许可证 312-316。

在块 318，每一许可证授权机构 108(1)、108(h)被配置成提供部分许可证 312-316 的一个或多个。例如，当由内容发行器执行时，许可证模块 116 可形成包括块 310 生成的数据的一个或多个传输。许可证授权机构 108(1)、108(h)可使用该传输来通过执行各自的许可证模块 118(1)、118(h)生成相应的部分许可证 312-316。例如，许可证授权机构 108(1)可执行许可证模块 118(1)，以从在传输中从内容发行器 102 处接收的数据生成部分许可证 312。同样，许可证授权机构 108(h)可执行许可证模块 118(h)，以从由内容发行器 102 处接收的数据生成部分许可证 314、316。由此，一个或多个传输可用于配置许可证授权机构 108(1)、108(h)来生成部分许可证 312-316。部分许可证 312-316 可组合来形成正式许可证 206，这在图 4 中有更详细的描述。

在块 320，许可证模块 116 由内容发行器 102 执行来包装内容 110 以包括获取部分许可证处的地址 322，即网络地址。例如，地址 322 可包括用于查找每一许可证授权机构 108(1)、108(h)的代理的一个或多个网络地址。在另一实现中，地址 322 包括用于查找每一许可证授权机构 108(1)、108(h)的网络地址。包装的内容然后可以使用各种方式，如通过图 1 的网络 106 在计算机可读媒质上分发等等。

图 4 是描述示例性实现的过程 400 的流程图，其中，从图 3 的部分许可证 312-316 形成正式许可证来输出内容 110。在块 402，接收播放内容 110 的请求。例如，内容 110 可由客户机装置 104 通过图 1 的网络 106 从内容发行器 102 接收。客户机装置 104 执行内容播放器 122 来输出内容 110，如播放歌曲、显示图片、显示影片等等。内容播放器 122 可提供一用户接口以从用户接收命令，如播放内容、选择内容、控制内容的输出（如，快进、暂停和倒带）等等。

当内容播放器 122 接收输出内容 110 的请求时，由内容播放器 122 启动 DRM 模块 216 来提供对内容的访问。DRM 模块 216 是提供内容 110 的数字权限管理的 PLI 的一部分。内容 110 的数字权限在图 3 的正式许可证 206 中提供。因此，为提

供对内容 110 的访问，当由客户机装置 104 执行时，DRM 模块 216 形成正式许可证，使内容播放器 122 可以输出内容 110。

例如，在块 404，DRM 模块 216 由客户机装置执行以从多个许可证授权机构 108(1)、108(h)获取部分许可证 312-316。例如，DRM 模块 216 可首先检查内容 110 以找出提供部分许可证 312-316 的许可证授权机构 108(1)、108(h)的地址 322。DRM 模块然后可以请求每一许可证授权机构 108(1)、108(h)提供相应的部分许可证 312-316。部分许可证 312-316 可由相应的许可证授权机构 108(1)、108(h)以各种方式提供。例如，许可证授权机构 108(1)可储存部分许可证 314，并在请求时提供部分许可证 314。在另一示例中，许可证授权机构 108(h)可从在图 3 的块 318 提供给许可证授权机构 108(h)的数据生成部分许可证 316、318。

在块 406，执行 DRM 模块 216 以从多个部分许可证 312-316 形成正式许可证 206。正式许可证 206 可由 DRM 模块 216 通过组合多个部分许可证 312-316 形成。在一个实现中，每一部分许可证 312-316 提供正式许可证 206 的一部分。在另一实现中，可通过使用用于划分并恢复正式许可证 206 的(k, m)阈值机密共享模式提供每一部分许可证。使用(k, m)阈值机密共享模式，即使可组合 k 个部分许可证来形成正式许可证，这些部分许可证即使当组合 k-1 个或更少的部分许可证时也不揭露关于正式许可证的信息。在块 408，将正式许可证绑定到客户机装置，使得可由客户机装置 104 单独使用该正式许可证。因此，进一步保护了正式许可证免受非授权形成，如图 5-7 中更详细描述的。

如图 3 和 4 所示，在客户机装置 104、许可证授权机构 108(1)、108(h)和内容发行器 102 之间有许多通信会话。为保护通信的安全性，可使用安全套接层（SSL）来确保通信安全性。另外，许可证授权机构 108(1)、108(h)也可使用证书来保护许可证授权机构 108(h)免受攻击者的模仿。例如，证书可用于核实许可证授权机构 108(1)、108(h)的凭证，如通过使用许可证授权机构的标识符（ID）、签发证书授权机构的数字签名等等。

使用(k, m)阈值机密共享模式的示例性实现

在先前的实现中，从一分布式数字权限管理（DRM）系统获取部分许可证。部分许可证用于形成正式许可证以向消费者提供对受保护的内容，即，加密的和/或具有正式许可证中指定的访问权限的内容的访问。为进一步增加 DRM 系统的效

率和故障容许，可采用(*k*, *m*)阈值机密共享模式来分布并形成部分许可证。

在一个实现中，DRM 系统采用一(*k*, *m*)阈值机密共享模式，其中，将正式许可证划分成 *m* 个部分许可证。划分正式许可证使得可使用任意 *k* 个或更多的部分许可证的知识来形成正式许可证。另外，不可使用任意 *k*-1 个或更少的部分许可证的知识来形成包括在正式许可证中的信息，即，*k*-1 个部分许可证的所有可能值为等可能的，并由此具有 *k*-1 个部分许可证的任何人完全不能确定正式许可证。

图 5 所示是一个示例性实现的过程 500 的流程图，其中，DRM 系统采用(*k*, *m*)阈值机密共享模式，使得多个许可证授权机构被配置成提供可用于形成正式许可证的部分许可证。本实现的数字权限管理系统可包括图 1 所示的内容发行器和多个许可证授权机构。在块 502，由内容发行器对内容加密。可以采用各种加密算法来加密该内容。可使用的加密算法的一个示例是先进加密标准（AES），它是对称加密算法。对称加密算法使用单个密钥来加密和解密数据。

在块 504，对内容生成正式证书，它可由消费者用于播放加密的内容。正式许可证包含对块 502 的加密内容解锁的解密密钥以及消费者，即正式许可证的拥有者所具有的与内容进行交互的访问规则。访问规则可包括对特定消费者的访问权限，如可访问内容的持续时间、可访问内容的方式等等。访问规则可在正式许可证中使用各种语言来表示，如 XRML（可扩充权限标记语言）、XACML（可扩充访问控制标记语言）、ODRL（开放数字权限语言）等等。

在块 506，从块 504 的正式许可证生成预许可证。预许可证可包含与内容发行器允许的访问规则关联的解密密钥。预许可证可用于生成部分许可证，然后使用部分许可证来形成正式许可证，如参考图 6 更详细讨论的。

例如，在块 508，通过使用非对称加密算法、对称加密算法等从正式许可证生成预许可证，下文的公式中被表示为 *prel*。非对称加密算法在公钥密码学中使用。公钥密码学采用了一对“密钥”，被称为私钥和公钥。公钥密码学在加密和解密过程的不同步骤使用公钥或私钥。例如，公钥密码学可使用非对称加密算法来加密数据，并使用非对称解密算法来解密所加密的数据。非对称加密算法使用公钥和要加密的原始数据来形成加密的数据，如密文。非对称解密算法使用私钥连同加密数据一起生成原始数据。在使用对称加密算法来生成预许可证的另外的实现中，对加密和解密使用单个密钥。非对称加密和解密的一个示例由首字母缩写词“RSA”（Rivest、Shamir 和 Adleman）可知。在下文示出的公式（1）中，使用公钥加密

正式许可证来生成预许可证。正式许可证、预许可证和公钥在公式（1）中分别被表示为“*license*”、“*prel*”和“*PK*”。

$$prel = (license)^{pk} \quad (1)$$

在块 510，对应的“机密”私钥，被表示为 *SK*，使用(*k, m*)阈值机密共享模式划分成 *m* 个共享，在该模式中，私钥 *SK* 被划分成 *m* 个部分机密共享，其任意 *k* 个可组合来生成该机密。例如，可生成共享多项式 *f(x)*，在公式（2）中示出如下：

$$f(x) = a_0 + a_1 x + \ldots + a_{k-1} x^{k-1} \quad (2)$$

内容发行器生成共享多项式 *f(x)*，其中，$a_0 = SK$。尽管描述了多项式内插，也可以使用其它函数集。然后可使用如下所示的公式（3）计算每一部分机密共享 S_i：

$$S_i = f(id_i) \bmod \phi(N) \quad (3)$$

其中，*N* 是 RSA 模块，$\phi(N)$是欧拉 ϕ 函数。

在块 512，内容发行器选择 *m* 个许可证授权机构，在以下公式中由 id_i 标识，其中，$i = 1, \ldots, m$，并向每一选择的许可证授权机构上传表示为 S_i 的部分机密共享之一以及块 508 生成的预许可证 *prel* 和许可证 ID。许可证 ID 可用于查找部分机密共享和预许可证。例如，许可证授权机构可被配置成提供多个部分许可证以生成不同的相应的许可证。因此，许可证授权机构可基于许可证 ID 标识一具体的部分许可证。尽管描述了向不同的许可证授权机构上传部分机密共享的每一个（如，部分机密共享的数量等于许可证授权机构的数量），然而可采用各种分布模式来选择许可证授权机构。例如，可向单个许可证授权机构上传一个以上机密共享，可选择 *m* 个许可证授权机构来提升冗余度等等，如参考图 7 更详细描述的。

为提升 DRM 系统的完整性，尤其是每一许可证授权机构所接收的部分机密共享的完整性，可结合(*k, m*)阈值机密共享模式使用可核实机密共享（VSS）模式。例如，VSS 模式可使每一接收部分机密共享的许可证授权机构能够核实所接收的部分机密共享的有效性，其示例在块 514 和 516 中示出。

例如，在块 514，内容发行器可广播共享多项式系数的 *k* 个公共证据，表示为 $\{g^{a_0}, \cdots, g^{a_{k-1}}\}$，其中，$g \in z_N^*$。在广播之后，内容发行器可毁坏该多项式。在块 516，每一许可证授权机构 id_i 核实接收的部分机密共享的有效性。可通过使用在块 514 广播的共享多项式的系数确定如下所示的公式（4）是否适用接收的部分机密共享 S_i，来检查有效性：

$$g^{S_i} = g^{a_0} \cdot (g^{a_1})^{id_i} \cdot \ldots \cdot (g^{a_{k-1}})^{id_i^{k-1}} \bmod N \quad (4)$$

以这一方式，每一许可证授权机构 id_i 可核实接收的部分机密共享 S_i 的有效性，而不展现或知道该机密，即私钥 SK。

在块 518，包装来自块 502 的加密内容。包装的内容包括储存了部分机密共享、预许可证和许可证 ID 的所选择的许可证授权机构的地址。通过在加密内容内提供所选择的许可证授权机构地址，当在客户机装置上执行时，内容播放器可查找所选择的许可证授权机构来形成块 504 的正式许可证以访问该内容。通过执行内容播放器形成正式许可证的示例参考图 6 讨论。

在块 520，分发包装的内容。可以各种方式分发包装的内容。例如，包装的内容可储存在向消费者售出的计算机可读媒质中、可通过图 1 所示的网络令其可用等等。例如，在对等网络中，内容发行器 102 可将包装的内容发送到图 1 的对等网络 106。包装的内容由网络 106 的节点复制以向消费者，即客户机装置、其它内容发行者等等提供内容。消费者可使用网络 106 中提供的搜索机制来查找并检索期望的内容。

图 6 是一个示例性实现中过程 600 的流程图，其中，由客户机装置形成正式许可证来播放图 5 的内容。在块 602，接收由内容播放器播放内容的请求。例如，该请求可由用户通过执行图 2 的内容播放器 122 来提供。在接收请求之后，在块 604，由内容播放器启动 DRM 模块来检查用于请求的内容的有效正式许可证。如上所述，提供了正式许可证以使内容播放器能够输出该内容。如果有有效的正式许可证可用，则在块 606，DRM 模块检查访问规则并播放该内容。如果没有有效的正式许可证可用，则在块 608，DRM 模块启动形成正式许可证的过程。

在块 610，DRM 模块检查该内容来找出用于该内容的许可证授权机构的地址。例如，如参考图 5 的块 518 所讨论的，可包装内容以包括能够生成部分许可证的许可证授权机构的地址。执行内容播放器的网络的节点 p，如客户机装置，检索许可证授权机构的地址列表。许可证授权机构的列表标识了网络的哪些节点被配置成能够提供一个或多个部分许可证的许可证授权机构，这些部分许可证可由内容播放器使用来为请求的内容形成正式许可证。

在块 612，通过执行 DRM 模块，客户机装置从许可证授权机构的至少一个子集请求部分许可证，使得提供 k 个部分许可证。例如，包括在内容内的地址可提供许可证授权机构的列表，这些许可证授权机构提供了比需要用来形成正式许可证更多的部分许可证，如 k+1 个。因此，DRM 模块可向许可证授权机构传递请求，使

得获取 k 个部分许可证。在另一实现中，DRM 模块可向包装的内容内标识的每一许可证授权机构传递请求。因此，如果许可证授权机构之一不能成功地提供对应的部分许可证，则仍可从其它许可证授权机构获取 k 个部分许可证，如参考图 7 更详细描述的。

在块 614，一个或多个联系的许可证授权机构可从消费者请求另外的信息。例如，可向消费者要求用于注册目的的信息、付款信息等等。例如，付款信息可由一个或多个许可证授权机构处理以授予对内容的访问权限。一旦处理了付款信息，许可证授权机构可生成用于形成正式许可证以访问内容的部分许可证。由此，许可证授权机构可在启用正式许可证的形成之前提供付款信息的处理。

在块 616，每一许可证授权机构生成一部分许可证，它是在图 5 的块 512 上传到许可证授权机构的部分机密共享和预许可证的结果。通过生成部分许可证，不揭露预许可证和部分机密共享，由此提高了 DRM 系统的安全性。例如，每一部分许可证可用于完成正式许可证。在接收了 k 个部分许可证之后，可形成正式许可证，而不需要任一许可证授权机构学到其它部分机密。由此，可维护并重新使用私钥 SK 的保密性。

例如，每一许可证授权机构 id_i 可使用公式（5）从其相应的部分机密共享 S_i 和预许可证 $prel$ 计算部分许可证 $prel_i$，公式（5）示出如下：

$$prel_i = (prel)^{S_i} \bmod N \qquad (5)$$

为使客户机装置能够核实部分机密共享，生成一随机数 u 并用于计算 $A_1=g^u$，$A_2=prel^u$，$r=u-c*S_i$，以及公式（6）：

$$c = hash(g^{S_i}, prel_i, A_1, A_2) \qquad (6)$$

在块 618，每一许可证授权机构通过向请求节点 p，即客户机装置安全地传递部分许可证 $prel_i$、A_1、A_2 和 r 来响应。

在块 620，当由客户机装置执行时，内容播放器通过确认每一部分许可证确定是否接收了 k 个正确的部分许可证。部分许可证可如下确认。首先，节点 p 从共享多项式系数的公共证据计算，

$$g^{S_i} = g^{a_0} \cdot (g^{a_1})^{id_1} \cdot \ldots \cdot (g^{a_{k-1}})^{id_i^{k-1}} \bmod N \qquad (7)$$

如参考图 5 的块 516 和公式（4）所讨论的。然后向 g^{S_i} 和接收的部分许可证 $prel_i$、A_1 和 A_2 应用公式（6）来计算 c。通过检查以下公式是否成立来核实接收的部分许可证 $prel_i$：$g^r \cdot (g^{S_i})^c = A_1$ 和 $prel^r \cdot (prel_i)^c = A_2$。重复以上步骤直到节点 p 获

得 k 个有效的部分许可证。如果不能获得 k 个有效的部分许可证，则正式许可证的生成失败（块 622）。

如果获得了 k 个有效的部分许可证，则在块 624，内容播放器组合部分许可证来形成正式许可证。例如，节点 p 使用 k 个有效的部分结果以使用公式（8）计算正式许可证：

$$license = \prod_i (prel_i)^{l_{id_i}(0)} = (prel)^{\sum_i s_i \cdot l_{id_i}(0)} \quad (8)$$

$$= (prel)^{SK} = ((license)^{PK})^{SK} \bmod N,$$

其中，$l_{id_i}(x) = \prod_{j=1, j\neq i}^{k} \frac{x - id_j}{id_i - id_j}$。

在块 626，将正式许可证绑定到执行该内容播放器的客户机装置。例如，可使用与生成正式许可证的节点 p 的具体硬件有关的密钥加密该正式许可证，密钥如网络接入卡的全局唯一标识符（GUID）。由此，该正式许可证是一仅可由节点 p，即客户机装置使用的个性化许可证。正式许可证可储存在客户机装置中用于将来的访问，使得不需要在每次由内容播放器输出内容时都生成正式许可证。在块 606，DRM 模块检查正式许可证中的访问规则并播放该内容。

尽管在本实现中，描述正式许可证由内容播放器内的 DRM 模块形成，然而，也可以由专用模块，如参考图 2-4 示出的 DRM 模块 216 生成正式许可证。例如，由客户机装置执行的步骤可由在内容播放器之内和/或耦合到其上的“黑箱”DRM 模块执行。“黑箱”DRM 模块可以是安全且防篡改的，使得尽管内容播放器可与 DRM 模块交互，内容播放器和客户机装置的软件模块都不能改变 DRM 模块。

由客户机装置从部分许可证形成的正式许可证也可以是客户机专用的，使得可以修改访问规则来反映不同消费者的不同访问权限。例如，内容发行器可在图 5 的块 504 生成正式许可证，该块描述了用于访问内容的所支持的各种选项，如用于输出具有对应的付款时间表的内容的不同的时间段。在图 6 的块 614，许可证授权机构可从消费者请求另外的信息，如选择期望的输出持续时间。作为响应，消费者可提供付款信息并选择期望的选项。内容发行器然后配置部分许可证来提供反映该选项的正式许可证。由此，由内容提供者生成的正式许可证可担当用于形成客户机专用正式许可证的模板。

图 7 所示是一个示例性实现，它示出了使用(k, m)阈值机密共享模式来提供用于生成正式许可证的部分许可证的 DRM 系统 700 中的冗余。通过在 DRM 系统中

提供部分许可证的分布式生成，其中，任意 k 个部分许可证的集合可用于形成正式许可证，可由 DRM 系统 700 提供各种功能。

万一一个或多个许可证授权机构变得不可用，(k, m)阈值机密共享模式可通过分布部分许可证的生成来提供冗余。例如，可以以(2, 3)阈值机密共享模式提供部分许可证，其中，一组三个部分许可证 702、704、706 中的任意两个部分许可证就足够形成正式许可证 708。部分许可证 702、704 和 706 的每一个可在多个许可证授权机构 710、712、714 的相应的一个上生成。如上所述，客户机装置 716 可接收通过内容播放器 718 输出内容的请求，并因此执行 DRM 模块 720 来形成正式许可证 708。客户机装置 716 从相应的许可证授权机构 710、712、714 请求部分许可证 702、704、706。

然而，许可证授权机构 712 可能无法提供其相应的部分许可证 704，如由于软件错误、硬件错误和/或网络错误。即使部分许可证 704 对客户机装置 716 不可用，客户机装置 716 仍可从部分许可证 702、706 形成正式许可证，部分许可证 702、706 分别由许可证授权机构 710、714 生成。由此，DRM 系统 700 可分布 k+1 个部分许可证的生成来为正式许可证 708 的形成提供冗余。

(k, m)阈值机密共享模式也可通过分布部分许可证的生成提供对攻击的安全性。当采用(k, m)阈值机密共享模式时，k-1 个部分许可证的知识不足以形成正式许可证。因此，当采用$(k, m$ 阈值机密共享模式时，DRM 系统 700 还可保护免受非授权内容的使用。例如，假定 DRM 系统 700 的一个攻击者获取了 k-1 个部分许可证。即使组合，该 k-1 个部分许可证不揭露包括在正式许可证中的任何信息。因此，攻击者必须攻克足够数量的许可证授权机构来获取 k 个部分许可证。为进一步提高安全性，可采用一种参考图 8 所更详细描述的更新模式。

(k, m)阈值机密共享模式也可提供部分许可证的供应的各种分布。例如，可在 DRM 系统中基于各种考虑，如安全性、负载共享、网络可用性、可用硬件和/软件资源等排列部分许可证的集合，如表格。例如，可向可靠和/或具有相当高的安全保护的第一许可证授权机构给予生成两个部分许可证的能力，而向不具备与第一许可证授权机构一样广泛的安全保护的第二许可证授权机构提供生成单个部分许可证的能力。以这一方式，可以在 DRM 系统内分别基于每一许可证授权机构所提供的安全级别排列许可证授权机构对部分许可证的生成。

此外，可以在不改变正式许可证的情况下改变部分许可证。例如，可对同一

自由项使用新的多项式$f_{new}(x)$。该类型的频繁改变可增强安全性，因为从安全缺口中获取的部分许可证不能组合，除非所有的部分许可证是f(x)多项式，即$f_{new}(x)$的同一版本的值，如参考图8更详细描述的。

图8所示是一个示例实现中过程800的流程图，其中，在采用(k, m)阈值机密共享模式的DRM系统中使用了一种更新模式。在先前的实现所描述的机密共享模式中，通过在许可证授权机构之中分布部分机密共享来保护该机密。然而，给予足够长的时间，攻击者最终可攻克k个部分机密共享来推断出该“机密”，即私钥SK。为阻止这一攻击，可使用提前的机密共享模式周期性地更新该部分机密共享。因此，攻击者必须在部分机密被更新之前攻克k个部分机密。否则，攻击者将被迫重新开始攻击。可使用各种提前机密共享更新算法来使用机密共享的新版本创建许可证授权机构的配置。

例如，以周期性的间隔，许可证授权机构可通过执行图2的各自的更新模块222更新其各自的私钥SK的共享。在块802，每一许可证授权机构i使用一随机更新多项式$f_{i,update}(x)$生成一机密0的随机(k, m)共享，如公式（9）所示：

$$f_{i,update}(x)\ b_{i,1}x \ldots b_{i,k\,1}x^{k\,1} \qquad (9)$$

在块804，每一许可证授权机构i计算子共享$S_{i,j}=f_{i,update}(j)$，$j=1, \ldots, m$。

在块806，每一许可证授权机构i向许可证授权机构j分发子共享$S_{i,j}$，其中，$j=1, \ldots, m$。因此，每一许可证授权机构i具有m个子共享$S_{i,j}$，其中，$j=1, \ldots, m$。可向原始共享S_i添加子共享，结果是新的更新的共享，如公式（10）所示：

$$S_i' = S_i + \sum_{j=1}^{m} S_{j,i} \qquad (10)$$

对应的新机密共享多项式$f_{new}(x)$是原始多项式$f(x)$和每一随机生成的多项式$f_{i,update}(x)$之和。如以下证明中所示出的，S_i'是从$f_{new}(x)$生成的部分机密共享。

证明：

$$f_{new}(x) \equiv f(x) + \sum_{j=1}^{m} f_{j,update}(x) = a_0 + (a_1 + \sum_{j=1}^{m} b_{j,1})x + \ldots + (a_{k-1} + \sum_{j=1}^{m} b_{j,k-1})x$$

$$S_i' = S_i + \sum_{j=1}^{m} S_{i,j} = f(i) + \sum_{j=1}^{m} f_{j,update}(i) = f_{new}(i)$$

图9示出了示例性更新模式900的一个示例，其中，通过使用子共享来更新部分机密。尽管描述了在每一许可证授权机构上执行图2的更新模块222，也可以使用集中式更新模块。例如，可由图2的内容发行器102执行更新模块220来更新部分许可证如何由图1的每一许可证授权机构108(h)提供。

总结

讨论了一种可用于构建分布式 DRM 许可证服务系统的公共许可证基础结构（PLI）和许可证授权机构。基于该 PLI 和许可证授权机构，描述了一种可在对等网络中使用的分布式 DRM 系统。描述的 DRM 系统可使用一种(*k*, *m*)阈值机密共享模式，一种可核实的机密共享模式和一种提前共享更新模式。阈值机密共享模式和 PLI 令 DRM 系统变得入侵容许、故障容许、灵活、可伸缩、可靠和高度可用。由此，通过使用多个许可证授权机构，不再需要常规 DRM 系统中的复杂且集中式许可证服务器。

尽管以对结构化特征和/或方法行动特定的语言描述了本发明，可以理解，所附权利要求书中定义的本发明不必局限在描述的具体特征和行动上。相反，揭示了具体的特征和行动作为实现所要求权利的发明的示例性形式。

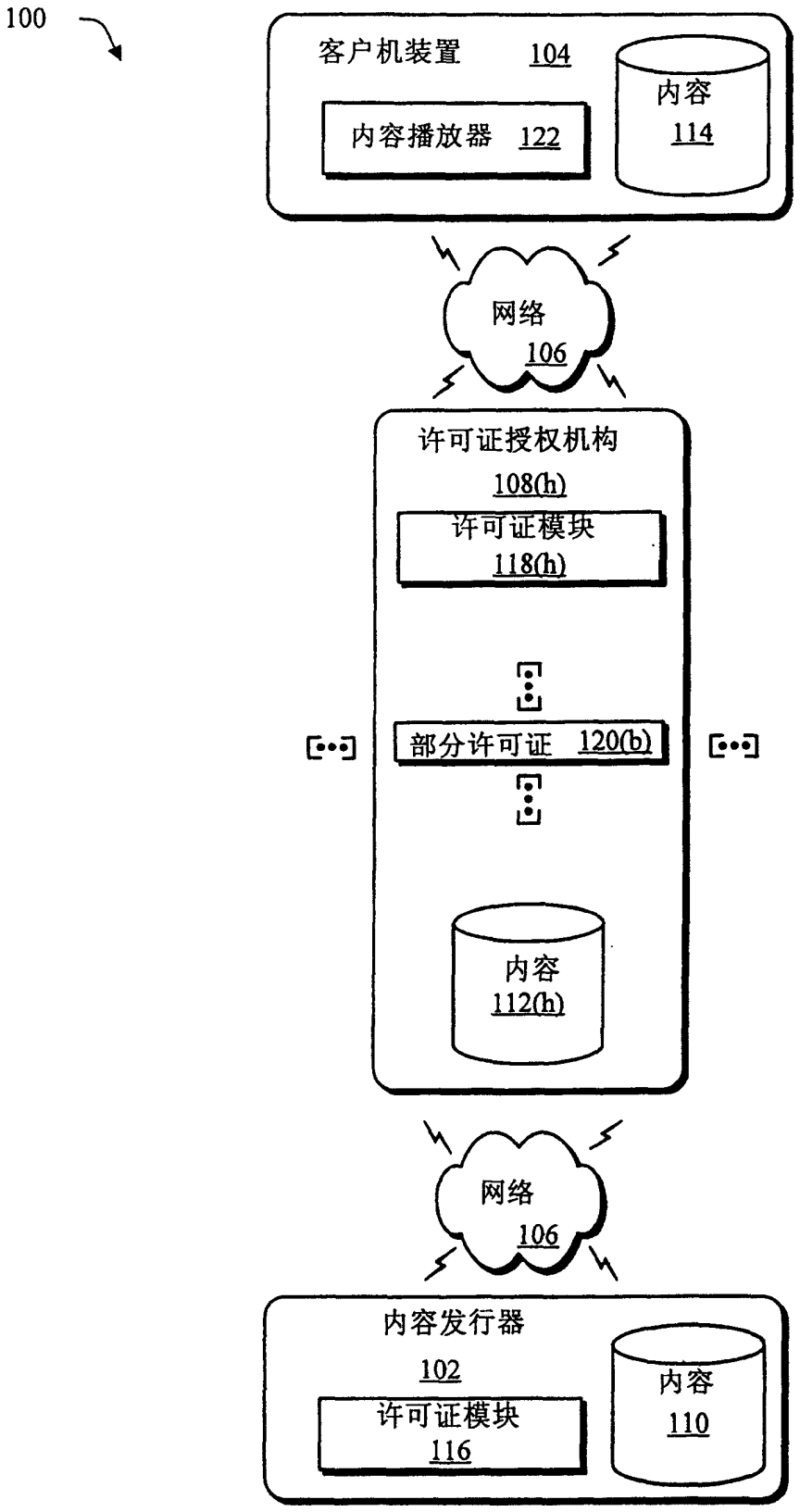

100
客户机装置 104
内容播放器 122
内容 114
网络 106
许可证授权机构 108(h)
许可证模块 118(h)
部分许可证 120(b)
内容 112(h)
网络 106
内容发行器 102
许可证模块 116
内容 110

图 1

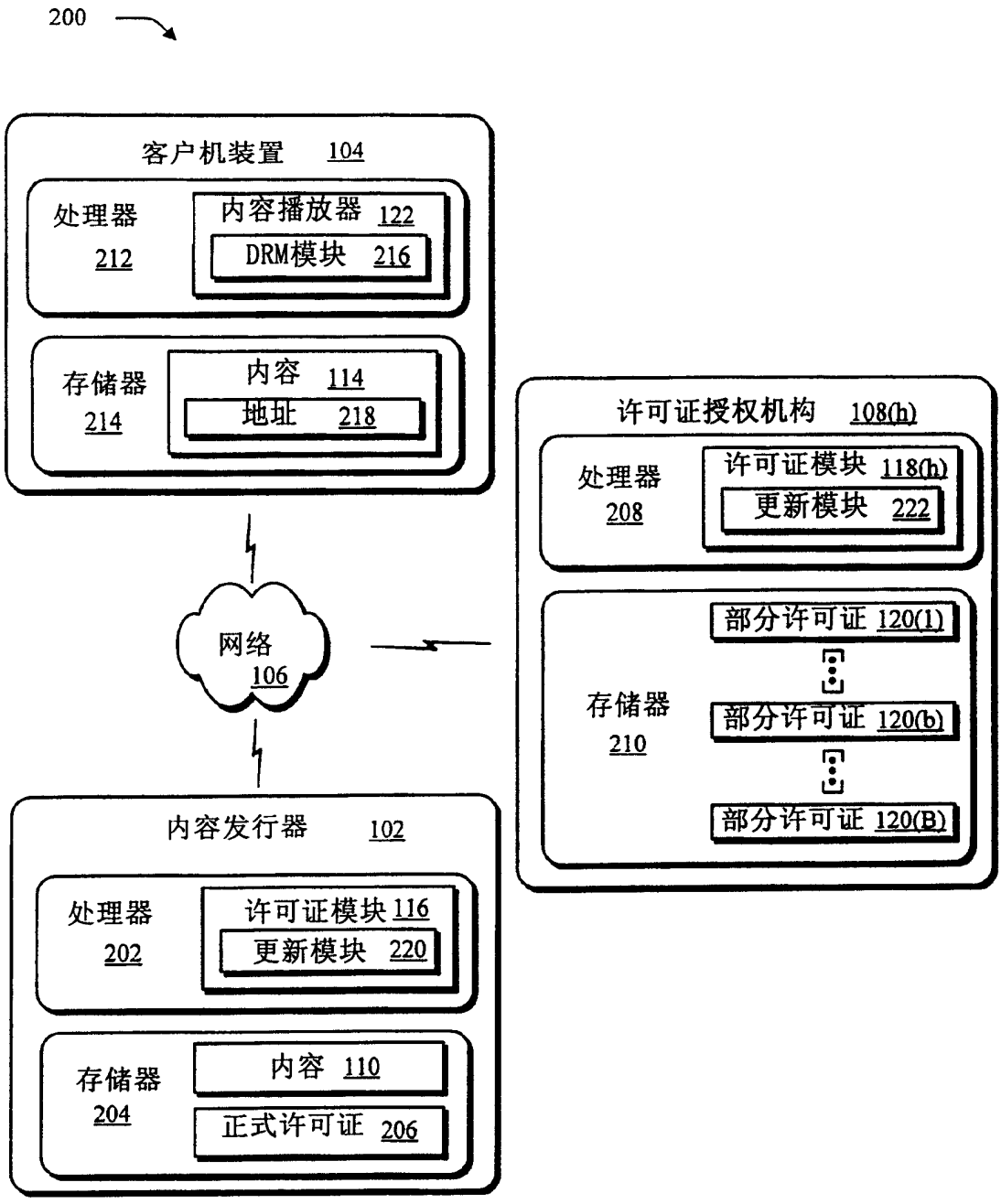

200
客户机装置 104
处理器 212
内容播放器 122
DRM模块 216
存储器 214
内容 114
地址 218
网络 106
内容发行器 102
处理器 202
许可证模块 116
更新模块 220
存储器 204
内容 110
正式许可证 206
许可证授权机构 108(h)
处理器 208
许可证模块 118(h)
更新模块 222
存储器 210
部分许可证 120(1)
部分许可证 120(b)
部分许可证 120(B)

图 2

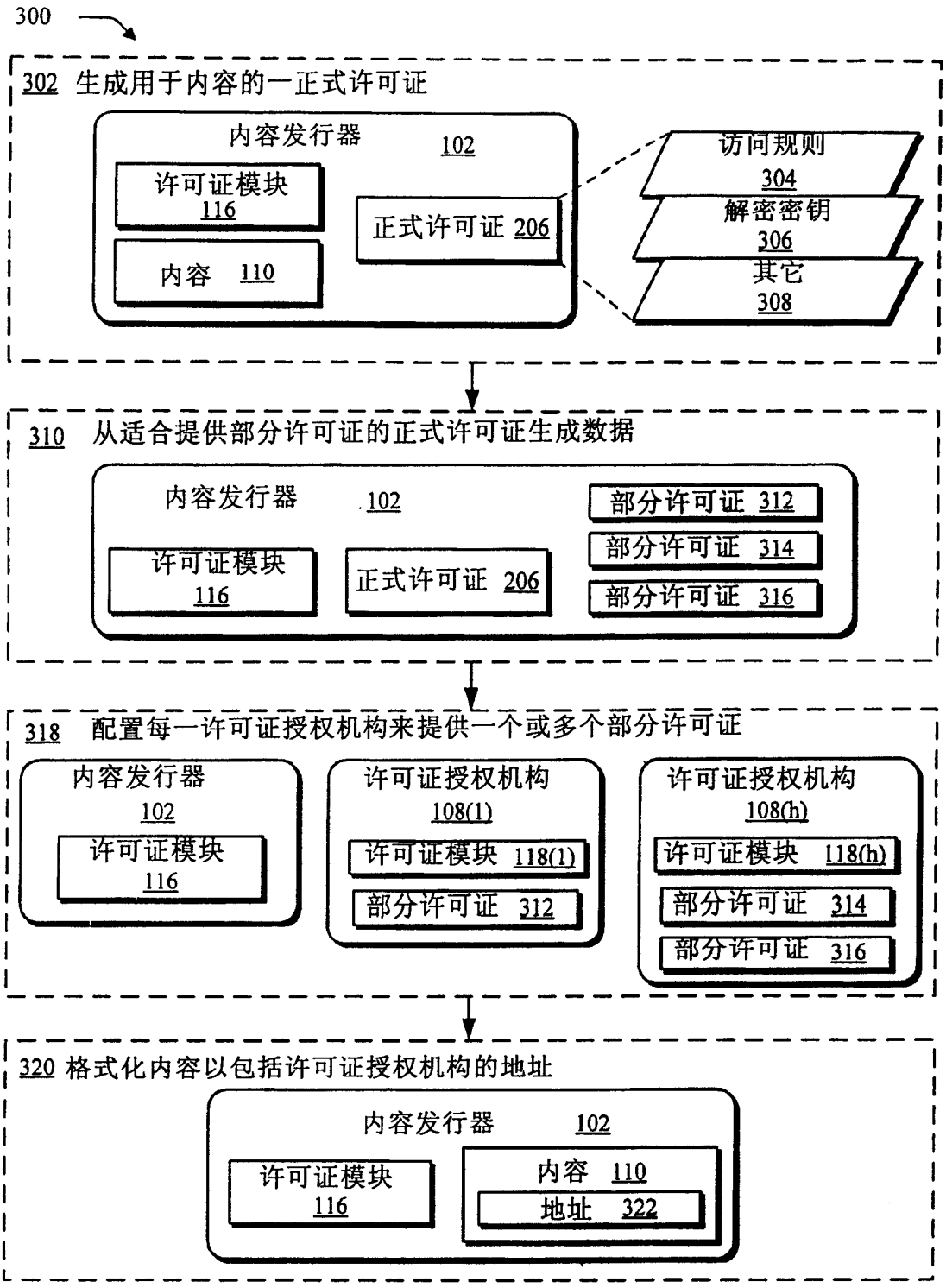

300
302 生成用于内容的一正式许可证
内容发行器 102
许可证模块 116
内容 110
正式许可证 206
访问规则 304
解密密钥 306
其它 308
310 从适合提供部分许可证的正式许可证生成数据
内容发行器 102
许可证模块 116
正式许可证 206
部分许可证 312
部分许可证 314
部分许可证 316
318 配置每一许可证授权机构来提供一个或多个部分许可证
内容发行器 102
许可证模块 116
许可证授权机构 108(1)
许可证模块 118(1)
部分许可证 312
许可证授权机构 108(h)
许可证模块 118(h)
部分许可证 314
部分许可证 316
320 格式化内容以包括许可证授权机构的地址
内容发行器 102
许可证模块 116
内容 110
地址 322

图 3

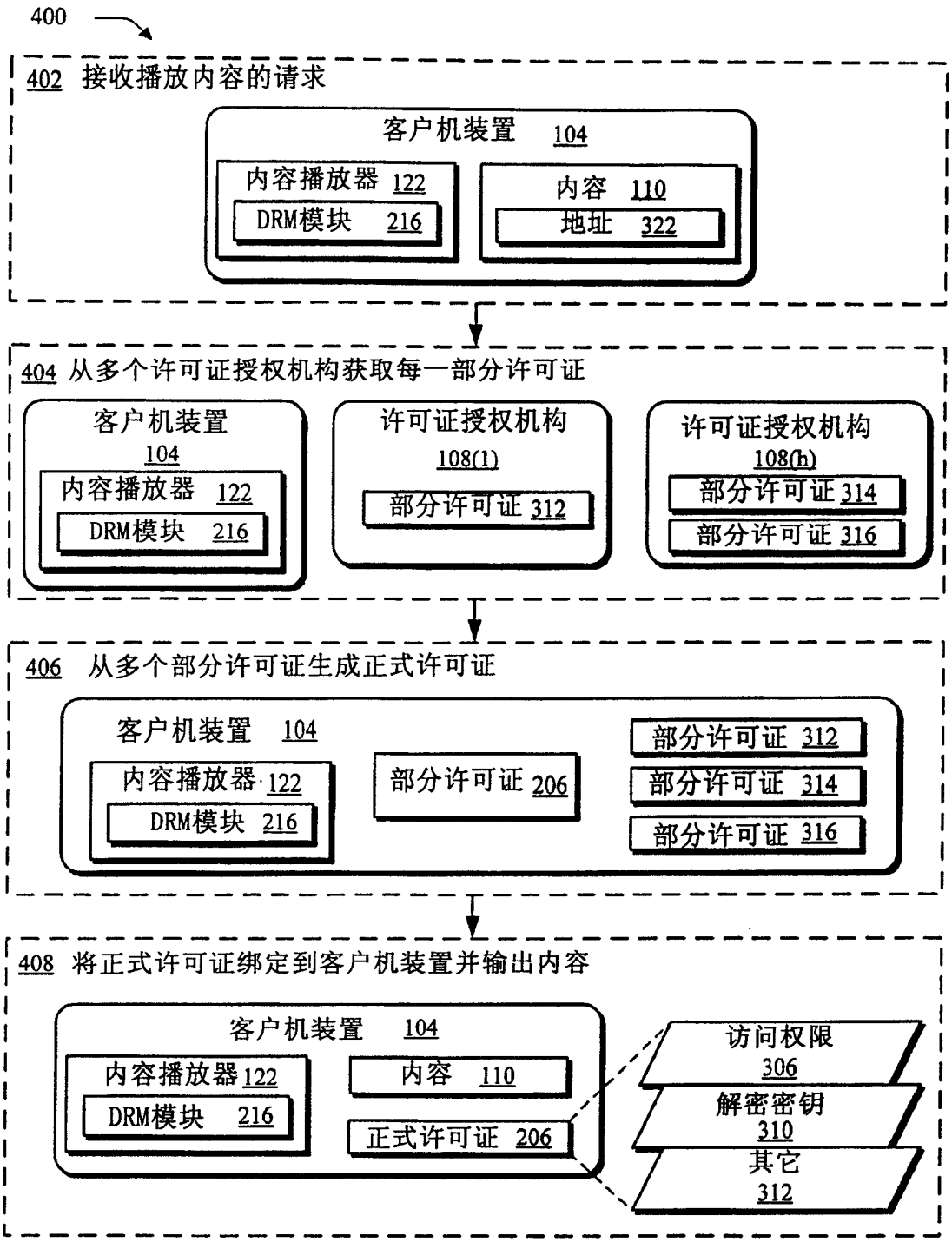

400
402 接收播放内容的请求
客户机装置 104
内容播放器 122
DRM模块 216
内容 110
地址 322
404 从多个许可证授权机构获取每一部分许可证
客户机装置 104
内容播放器 122
DRM模块 216
许可证授权机构 108(1)
部分许可证 312
许可证授权机构 108(h)
部分许可证 314
部分许可证 316
406 从多个部分许可证生成正式许可证
客户机装置 104
内容播放器 122
DRM模块 216
部分许可证 206
部分许可证 312
部分许可证 314
部分许可证 316
408 将正式许可证绑定到客户机装置并输出内容
客户机装置 104
内容播放器 122
DRM模块 216
内容 110
正式许可证 206
访问权限 306
解密密钥 310
其它 312

图 4

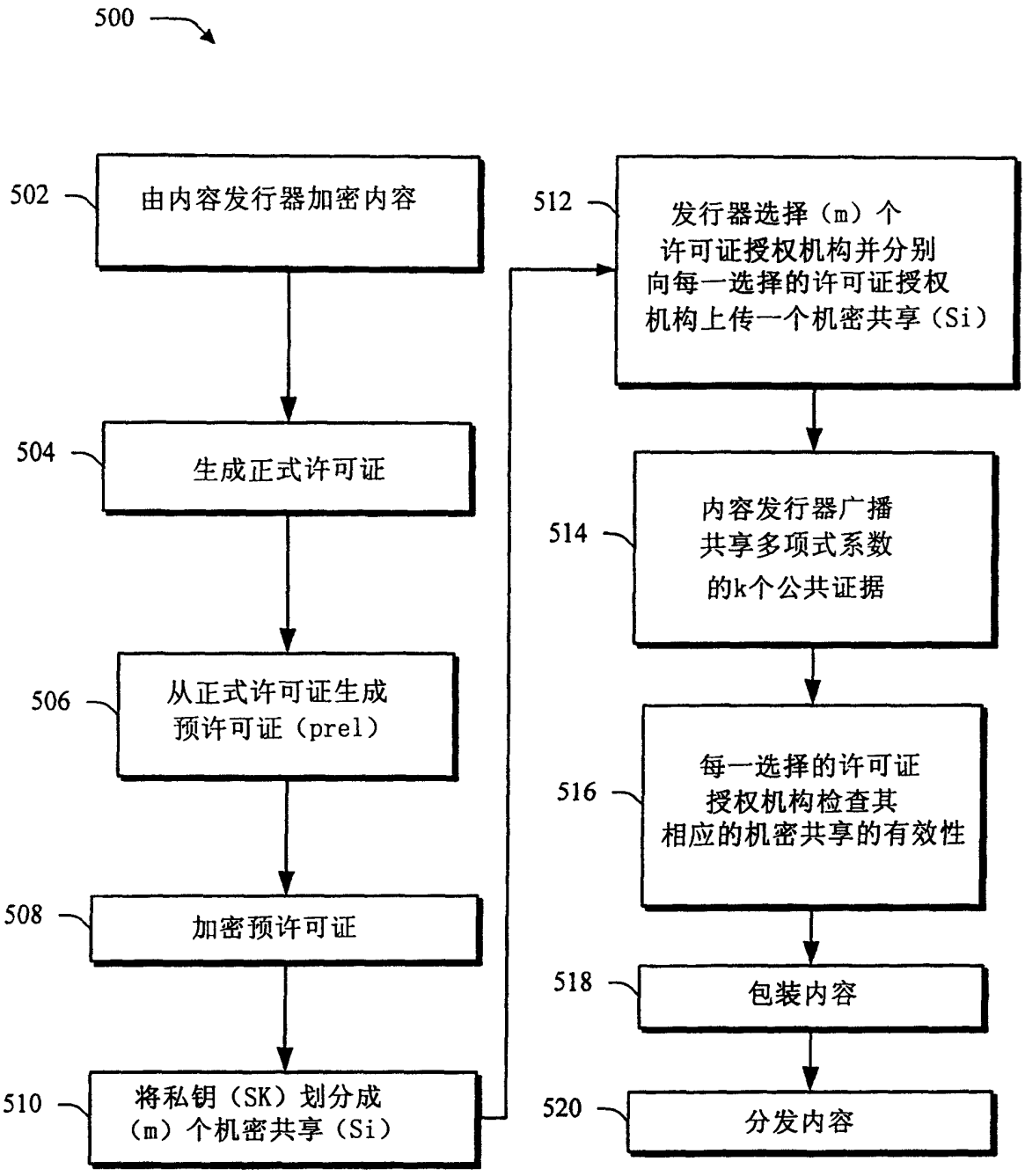

500
502
由内容发行器加密内容
504
生成正式许可证
506
从正式许可证生成
预许可证（prel）
508
加密预许可证
510
将私钥（SK）划分成
（m）个机密共享（Si）
512
发行器选择（m）个
许可证授权机构并分别
向每一选择的许可证授权
机构上传一个机密共享（Si）
514
内容发行器广播
共享多项式系数
的k个公共证据
516
每一选择的许可证
授权机构检查其
相应的机密共享的有效性
518
包装内容
520
分发内容

图 5

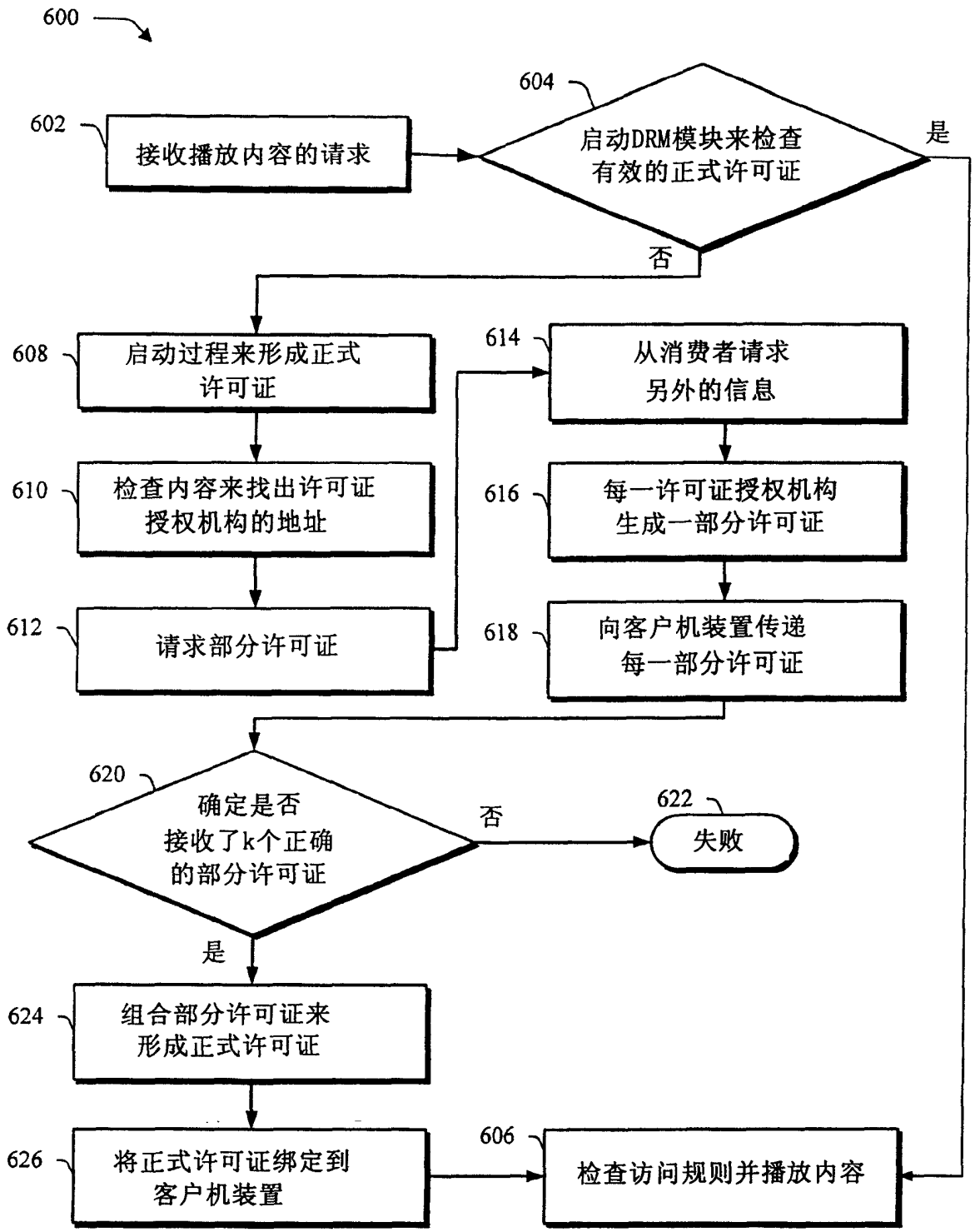

600
602
接收播放内容的请求
604
启动DRM模块来检查
有效的正式许可证
是
否
608
启动过程来形成正式
许可证
610
检查内容来找出许可证
授权机构的地址
612
请求部分许可证
614
从消费者请求
另外的信息
616
每一许可证授权机构
生成一部分许可证
618
向客户机装置传递
每一部分许可证
620
确定是否
接收了k个正确
的部分许可证
否
622
失败
是
624
组合部分许可证来
形成正式许可证
626
将正式许可证绑定到
客户机装置
606
检查访问规则并播放内容

图 6

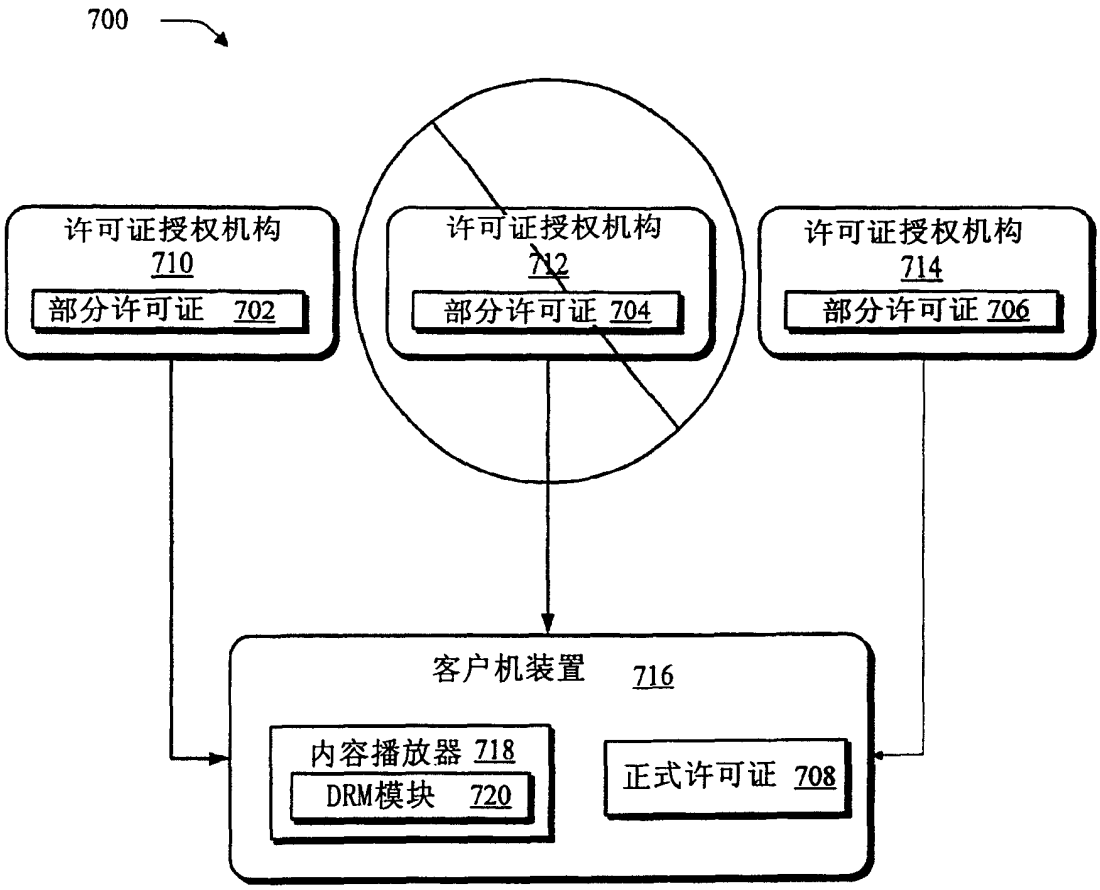

700
许可证授权机构
710
部分许可证 702
许可证授权机构
712
部分许可证 704
许可证授权机构
714
部分许可证 706
客户机装置 716
内容播放器 718
DRM模块 720
正式许可证 708

图 7

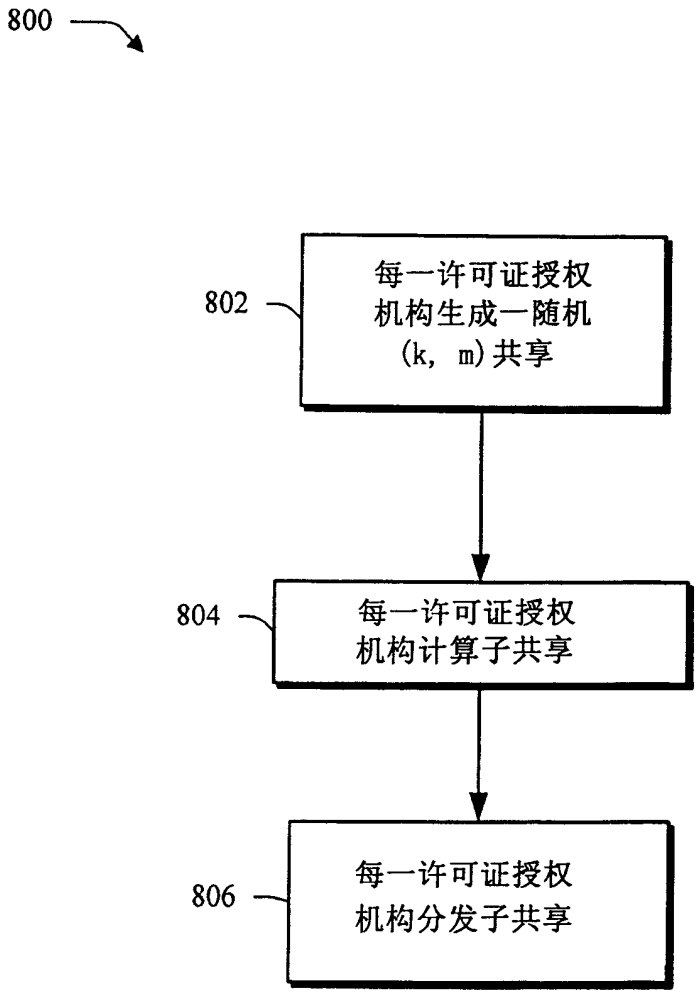

800
802
每一许可证授权机构生成一随机(k, m)共享
804
每一许可证授权机构计算子共享
806
每一许可证授权机构分发子共享

图 8

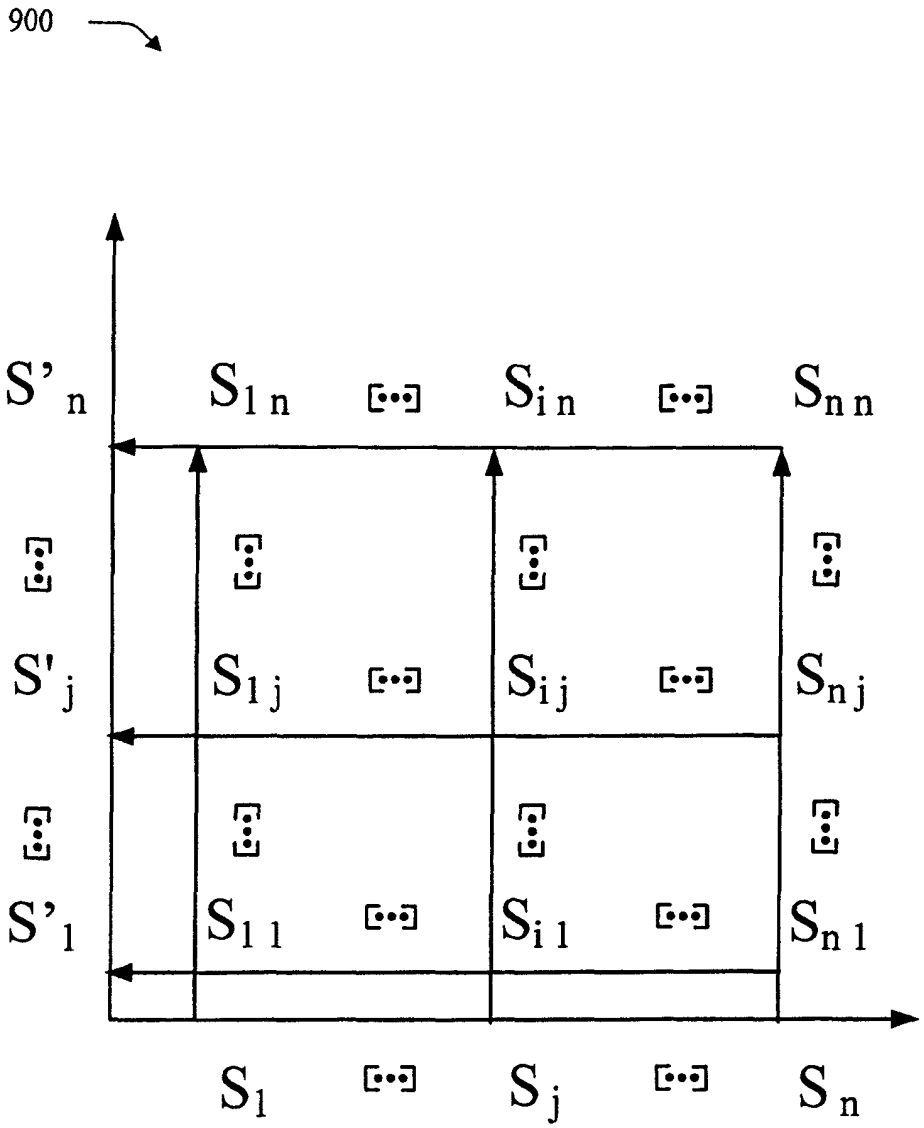


图 9