[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 12/14 (2006.01)
G06F 15/00 (2006.01)
G11B 20/10 (2006.01)
H04L 9/32 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200580004138.8

[43] 公开日 2007 年 2 月 21 日

[11] 公开号 CN 1918553A

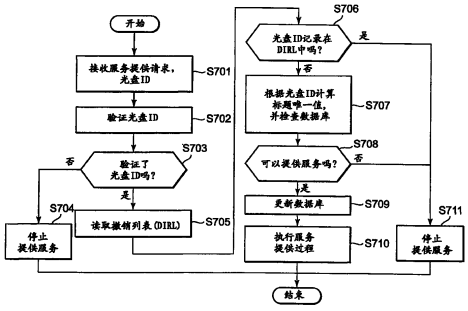
[22] 申请日 2005.1.17
[21] 申请号 200580004138.8
[30] 优先权
[32] 2004. 2. 4 [33] JP [31] 027940/2004
[86] 国际申请 PCT/JP2005/000497 2005.1.17
[87] 国际公布 WO2005/076142 日 2005.8.18
[85] 进入国家阶段日期 2006.8.4
[71] 申请人 索尼株式会社
地址 日本东京
[72] 发明人 浅野智之
[74] 专利代理机构 中国国际贸易促进委员会专利商标事务所
代理人 付建军
权利要求书 6 页 说明书 30 页 附图 17 页

[54] 发明名称

服务提供服务器、信息处理设备、数据处理方法，以及计算机程序

[57] 摘要

提供了能使对应于存储在信息记录介质中的内容的服务只能提供到具有有效信息记录介质的设备的设备和方法。 在其中提供存储在信息记录介质中的内容，并且从联网的服务提供服务器执行服务提供过程的配置中，服务提供服务器验证从用户设备传输给它的信息记录介质 ID，并根据每一个信息记录介质 ID 的服务提供情况数据判断是否可以提供服务，并提供服务。 只有在传输了服务请求的信息处理设备是读取了有效信息记录介质 ID 的信息处理设备的情况下才提供服务，并根据服务提供情况数据，允许提供服务。



1. 用于响应来自信息处理设备的服务提供请求执行服务提供过程的服务提供服务器，其特征在于具有：

数据接收部分，用于从信息处理设备接收伴有信息记录介质 ID 和服务 ID 的服务请求；

存储部分，用于存储每一个信息记录介质 ID 的服务提供情况数据，作为对应于存储在信息记录介质上的内容的标题的每一个标题唯一值的服务管理数据；以及

数据处理部分，用于执行验证通过数据接收部分接收到的信息记录介质 ID 的过程，在验证了信息记录介质 ID 的条件下，根据信息记录介质 ID 获取标题唯一值，从存储部分获取对应于标题唯一值的服务提供情况数据，以判断是否可以提供由信息记录介质 ID 和服务 ID 指定的服务，并在判断可以提供服务的条件下执行服务提供过程。

2. 根据权利要求 1 所述的服务提供服务器，其特征在于：

数据处理部分被配置为作为验证信息记录介质 ID 中包含的签名数据的过程，执行验证信息记录介质 ID 的过程，并根据信息记录介质 ID 中包含的标题唯一值，或通过基于信息记录介质 ID 中包含的数据执行计算而计算出的标题唯一值，执行从存储部分获取对应于标题唯一值的服务提供情况数据的过程。

3. 根据权利要求 1 所述的服务提供服务器，其特征在于：

服务提供服务器具有存储部分，用于存储撤销列表，所述撤销列表是未经授权的信息记录介质 ID 的列表；以及

数据处理部分中的验证信息记录介质 ID 的过程是作为将从信息处理设备接收到的信息记录介质 ID 与记录在撤销列表中的 ID 进行比较的过程来执行的。

4. 根据权利要求 1 所述的服务提供服务器，其特征在于：

信息记录介质 ID 被配置为包括对应于存储在信息记录介质中的内容的标题的标题唯一值，以及根据管理设备的秘密密钥生成的签

名数据，并且所述信息记录介质 ID 对于每一个信息记录介质都是不同的；以及

数据处理部分被配置为作为生成向消息应用管理设备的公钥的消息的过程，执行验证信息记录介质 ID 的过程，用于与信息记录介质 ID 中包含的签名数据进行比较，还执行从存储部分获取对应于信息记录介质 ID 中包含的标题唯一值的服务提供情况数据的过程。

5. 根据权利要求 1 所述的服务提供服务器，其特征在于：

信息记录介质 ID 包括：

响应制造的信息记录介质的数量 w 中的每一个设置的素数 p(w)；以及

由基于素数 p(w) 和标题唯一值的计算而计算出的数据 IDKey(w)；以及

数据处理部分被配置为作为 ID 验证过程，执行判断信息记录介质 ID 中包含的数据是否为素数的过程，还根据信息记录介质 ID 中包含的数据 IDKey(w) 计算标题唯一值，从存储部分获取对应于计算出的标题唯一值的服务提供情况数据。

6. 用于执行发往服务提供服务器的服务提供请求的信息处理设备，其特征在于具有：

记录介质接口，该接口执行访问信息记录介质的过程；以及

数据处理部分，用于执行验证通过记录介质接口从信息记录介质读取的信息记录介质 ID 的过程，并在验证了信息记录介质 ID 的条件下，执行向服务提供服务器传输信息记录介质 ID 的过程。

7. 根据权利要求 6 所述的信息处理设备，其特征在于：

数据处理部分被配置为作为验证信息记录介质 ID 中包含的签名数据的过程，执行验证信息记录介质 ID 的过程。

8. 根据权利要求 6 所述的信息处理设备，其特征在于：

数据处理部分中的验证信息记录介质 ID 的过程被配置为从存储部分或信息记录介质中获取撤销列表的过程，所述撤销列表是未经授权的信息记录介质 ID 的列表，以及将从信息处理设备接收到的信

息记录介质 ID 与记录在所获取的撤销列表中的 ID 进行比较的过程。

9. 根据权利要求 6 所述的信息处理设备，其特征在于:

信息记录介质 ID 包括对应于存储在信息记录介质中的内容的标题的标题唯一值，以及根据管理设备的秘密密钥生成的签名数据，并且所述信息记录介质 ID 对于每一个信息记录介质都是不同的；以及

数据处理部分被配置为作为生成向消息应用管理设备的公钥的消息的过程，执行验证信息记录介质 ID 的过程，用于与信息记录介质 ID 中包含的签名数据进行比较。

10. 根据权利要求 6 所述的信息处理设备，其特征在于:

信息记录介质 ID 包括:

响应制造的信息记录介质的数量 w 中的每一个设置的素数 p(w)；以及

由基于素数 p(w) 和标题唯一值的计算而计算出的数据 IDKey(w)；以及

数据处理部分被配置为作为 ID 验证过程，执行判断信息记录介质 ID 中包含的数据是否为素数的过程。

11. 用于响应来自信息处理设备的服务提供请求执行服务提供过程的数据处理方法，其特征在于具有:

数据接收步骤，从信息处理设备接收伴有信息记录介质 ID 和服务 ID 的服务请求；以及

数据处理步骤，执行验证接收到的信息记录介质 ID 的过程，在验证了信息记录介质 ID 的条件下，根据信息记录介质 ID 获取标题唯一值，从存储部分获取对应于所获取的标题唯一值的服务提供情况数据，判断是否可以提供由信息记录介质 ID 和服务 ID 指定的服务，并在判断可以提供服务的条件下执行服务提供过程，所述存储部分存储每一个信息记录介质 ID 的服务提供情况数据，作为对应于存储在信息记录介质上的内容的标题的每一个标题唯一值的服务管理

数据。

12. 根据权利要求 11 所述的数据处理方法，其特征在于：

数据处理步骤被配置为包括下列步骤：作为验证信息记录介质 ID 中包含的签名数据的过程，执行验证信息记录介质 ID 的过程，并根据信息记录介质 ID 中包含的标题唯一值，或通过基于信息记录介质 ID 中包含的数据执行计算而计算出的标题唯一值，执行从存储部分获取对应于标题唯一值的服务提供情况数据的过程。

13. 根据权利要求 11 所述的数据处理方法，其特征在于：

数据处理步骤中的验证信息记录介质 ID 的过程被配置为包括作为将从信息处理设备接收到的信息记录介质 ID 与记录在撤销列表中的 ID 进行比较的过程来执行的步骤，所述撤销列表是未经授权的信息记录介质 ID 的列表。

14. 根据权利要求 11 所述的数据处理方法，其特征在于：

信息记录介质 ID 被配置为包括对应于存储在信息记录介质中的内容的标题的标题唯一值，以及根据管理设备的秘密密钥生成的签名数据，并且所述信息记录介质 ID 对于每一个信息记录介质都是不同的；以及

数据处理步骤被配置为包括下列步骤：作为生成向消息应用管理设备的公钥的消息的过程，执行验证信息记录介质 ID 的过程，用于与信息记录介质 ID 中包含的签名数据进行比较，还执行从存储部分获取对应于信息记录介质 ID 中包含的标题唯一值的服务提供情况数据的过程。

15. 根据权利要求 11 所述的数据处理方法，其特征在于：

信息记录介质 ID 包括：

响应制造的信息记录介质的数量 w 中的每一个设置的素数 p(w)；以及

由基于素数 p(w) 和标题唯一值的计算而计算出的数据 IDKey(w)；以及

数据处理步骤被配置为包括下列步骤：作为 ID 验证过程，执

行判断信息记录介质 ID 中包含的数据是否为素数的过程，还根据信息记录介质 ID 中包含的数据 IDKey(w) 计算标题唯一值，从存储部分获取对应于计算出的标题唯一值的服务提供情况数据。

16. 用于执行发往服务提供服务器的服务提供请求的数据处理方法，其特征在于具有：

记录介质访问步骤，执行通过记录介质接口访问信息记录介质的过程；以及

数据处理步骤，执行验证通过记录介质接口从信息记录介质读取的信息记录介质 ID 的过程，并在验证了信息记录介质 ID 的条件下，执行向服务提供服务器传输信息记录介质 ID 的过程。

17. 根据权利要求 16 所述的数据处理方法，其特征在于：

数据处理步骤被配置为作为验证信息记录介质 ID 中包含的签名数据的过程，执行验证信息记录介质 ID 的过程。

18. 根据权利要求 16 所述的数据处理方法，其特征在于：

数据处理步骤中的验证信息记录介质 ID 的过程被配置为包括下列步骤：从存储部分或信息记录介质中获取撤销列表，所述撤销列表是未经授权的信息记录介质 ID 的列表，以及将从信息处理设备接收到的信息记录介质 ID 与记录在所获取的撤销列表中的 ID 进行比较。

19. 根据权利要求 16 所述的数据处理方法，其特征在于：

信息记录介质 ID 被配置为包括对应于存储在信息记录介质中的内容的标题的标题唯一值，以及根据管理设备的秘密密钥生成的签名数据，并且所述信息记录介质 ID 对于每一个信息记录介质都是不同的；以及

数据处理步骤被配置为包括下列步骤：作为生成向消息应用管理设备的公钥的消息的过程，执行验证信息记录介质 ID 的过程，用于与信息记录介质 ID 中包含的签名数据进行比较。

20. 根据权利要求 16 所述的数据处理方法，其特征在于：

信息记录介质 ID 包括：

响应制造的信息记录介质的数量 w 中的每一个设置的素数 p(w)；以及

由基于素数 p(w) 和标题唯一值的计算而计算出的数据 IDKey(w)；以及

数据处理步骤被配置为包括下列步骤：作为 ID 验证过程，执行判断信息记录介质 ID 中包含的数据是否为素数的过程。

21. 用于响应来自信息处理设备的服务提供请求执行服务提供过程的计算机程序，其特征在于具有：

数据接收步骤，从信息处理设备接收伴有信息记录介质 ID 和服务 ID 的服务请求；以及

数据处理步骤，执行验证接收到的信息记录介质 ID 的过程，在验证了信息记录介质 ID 的条件下，根据信息记录介质 ID 获取标题唯一值，从存储部分获取对应于所获取的标题唯一值的服务提供情况数据，判断是否可以提供由信息记录介质 ID 和服务 ID 指定的服务，并在判断可以提供服务的条件下执行服务提供过程，所述存储部分存储每一个信息记录介质 ID 的服务提供情况数据，作为对应于存储在信息记录介质上的内容的标题的每一个标题唯一值的服务管理数据。

22. 用于执行发往服务提供服务器的服务提供请求的计算机程序，其特征在于具有：

记录介质访问步骤，执行通过记录介质接口访问信息记录介质的过程；以及

数据处理步骤，执行验证通过记录介质接口从信息记录介质读取的信息记录介质 ID 的过程，并在验证了信息记录介质 ID 的条件下，执行向服务提供服务器传输信息记录介质 ID 的过程。

服务提供服务器、信息处理设备、数据处理方法，以及计算机程序

技术领域

本发明涉及服务提供服务器、信息处理设备、数据处理方法，以及计算机程序。具体来说，本发明指向服务提供服务器、信息处理设备、数据处理方法，以及计算机程序，它们都向用户设备提供与内容相关的服务，而用户设备执行播放诸如其中存储了内容的光盘之类的信息记录介质的过程。

背景技术

各种软件数据（以下简称为“内容”），如包括音乐的音频数据、包括电影的图像数据，游戏程序和各种应用程序，在存储在诸如 DVD（数字通用光盘）、MD（小型光盘）、CD（压缩光盘）或使用蓝色激光（Blu-ray 光盘）的高密度可记录光盘之类的信息记录介质的情况下，可以提供给用户。用户可以在包括 PC（个人计算机）、光盘播放器的用户设备中（即，在播放设备中）播放内容。

此外，近年来，提供服务的配置也得到广泛的使用，在这种配置中，从与用户设备联网的服务器提供与存储在诸如光盘之类的信息记录介质中的内容相关的各种服务。

例如，当存储在光盘中的内容是外语电影时，从通过网络连接的服务器向诸如 PC 之类的用户设备提供各种与内容相关的服务，包括小标题或其音频的配音数据，或内容的续集的购买光盘折扣票。

如何从服务器提供服务的方式可以采用各种形式。某些服务可能对访问没有限制，而某些其他服务可能要符合某种条件，例如，对于在其上记录了与服务相关的内容每一个光盘，这些服务最多只能提供一次。

分发存储在光盘中的内容（即，诸如音乐数据和图像数据之类的

各种内容）的权限等等，一般由它们的创作者或它们的经销商所有。因此，在分发这样的内容时，一般采用了设置某一受限访问的配置，即，只有被授权的用户才被允许使用内容，以便防止未授权使用。

因此，对于提供的与内容相关的服务，希望确定一个系统，其中，在验证了某一使用权的条件下才允许提供服务，即，已经执行验证用户是正版光盘的购买者的过程。

发明内容

[本发明解决的问题]

本发明是在考虑到上文所提及的问题的背景下作出的，其目标是提供服务提供服务器、信息处理设备、数据处理方法，以及计算机程序，在提供存储在包括 DVD、CD、蓝色激光记录介质的各种信息记录介质上的内容，并且，联网的服务提供服务器执行服务提供过程的配置中，通过验证服务的使用权，它们所有的都能使未授权使用服务的情况排除。

[解决问题的手段]

本发明的第一个方面是：

用于根据来自信息处理设备的服务提供请求执行服务提供过程的服务提供服务器，其特征在于具有：

数据接收部分，用于从信息处理设备接收伴有信息记录介质 ID 和服务 ID 的服务请求；

存储部分，用于存储每一个信息记录介质 ID 的服务提供情况数据，作为对应于存储在信息记录介质上的内容的标题的每一个标题唯一值的服务管理数据；以及

数据处理部分，用于执行验证通过数据接收部分接收到的信息记录介质 ID 的过程，在验证了信息记录介质 ID 的条件下，根据信息记录介质 ID 获取标题唯一值，从存储部分获取对应于标题唯一值的服务提供情况数据，以判断被否可以提供由信息记录介质 ID 和服务 ID 指定的服务，并在判断可以提供服务的条件下执行服务提供过程。

此外，在本发明的服务提供服务器的一个实施例中，数据处理部

分的特征在于，被配置为作为验证信息记录介质 ID 中包含的签名数据的过程，执行验证信息记录介质 ID 的过程，并根据信息记录介质 ID 中包含的标题唯一值，或通过基于信息记录介质 ID 中包含的数据执行计算而计算出的标题唯一值，执行从存储部分获取对应于标题唯一值的服务提供情况数据的过程。

此外，在本发明的服务提供服务器的一个实施例中，服务提供服务器的特征在于，具有存储部分，用于存储撤销列表，所述撤销列表是未经授权的信息记录介质 ID 的列表，数据处理部分中的验证信息记录介质 ID 的过程的特征在于是作为将从信息处理设备接收到的信息记录介质 ID 与记录在撤销列表中的 ID 进行比较的过程来执行的。

此外，在本发明的服务提供服务器的一个实施例中，信息记录介质 ID 的特征在于，被配置为包括对应于存储在信息记录介质中的内容的标题的标题唯一值，以及根据管理设备的秘密密钥生成的签名数据，并且所述信息记录介质 ID 对于每一个信息记录介质都是不同的，数据处理部分的特征在于，被配置为作为生成向消息应用管理设备的公钥的消息的过程，执行验证信息记录介质 ID 的过程，用于与信息记录介质 ID 中包含的签名数据进行比较，还执行从存储部分获取对应于信息记录介质 ID 中包含的标题唯一值的服务提供情况数据的过程。

此外，在本发明的服务提供服务器的一个实施例中，信息记录介质 ID 的特征在于，被配置为包括响应制造的信息记录介质的数量 w 设置的素数 p(w)，以及由基于素数 p(w) 和标题唯一值的计算而计算出的数据 IDKey(w)，数据处理部分的特征在于，被配置为，作为 ID 验证过程，执行判断信息记录介质 ID 中包含的数据是否为素数的过程，还根据信息记录介质 ID 中包含的数据 IDKey(w) 计算标题唯一值，从存储部分获取对应于计算出的标题唯一值的服务提供情况数据。

此外，本发明的第二个方面是：

用于执行发往服务提供服务器的服务提供请求的信息处理设备，其特征在于具有：

记录介质接口，用于执行访问信息记录介质的过程；以及

数据处理部分，用于执行验证通过记录介质接口从信息记录介质读取的信息记录介质 ID 的过程，并被验证了信息记录介质 ID 的条件下，执行向服务提供服务器传输信息记录介质 ID 的过程。

此外，在本发明的信息处理设备的一个实施例中，数据处理部分的特征在于，被配置为作为验证信息记录介质 ID 中包含的签名数据的过程，执行验证信息记录介质 ID 的过程。

此外，在本发明的信息处理设备的一个实施例中，数据处理部分中的验证信息记录介质 ID 的过程的特征在于，被配置为从存储部分或信息记录介质中获取撤销列表的过程，所述撤销列表是未经授权的信息记录介质 ID 的列表，以及将从信息处理设备接收到的信息记录介质 ID 与记录在所获取的撤销列表中的 ID 进行比较的过程。

在本发明的信息处理设备的一个实施例中，信息记录介质 ID 的特征在于，被配置为包括对应于存储在信息记录介质中的内容的标题的标题唯一值，以及根据管理设备的秘密密钥生成的签名数据，并且所述信息记录介质 ID 对于每一个信息记录介质都是不同的；数据处理部分的特征在于，被配置为作为生成向消息应用管理设备的公钥的消息的过程，执行验证信息记录介质 ID 的过程，用于与信息记录介质 ID 中包含的签名数据进行比较。

此外，在本发明的信息处理设备的一个实施例中，信息记录介质 ID 的特征在于，被配置为包括响应制造的信息记录介质的数量 w 中的每一个设置的素数 p(w)，以及由基于素数 p(w) 和标题唯一值的计算而计算出的数据 IDKey(w)，数据处理部分被配置为，作为 ID 验证过程，执行判断信息记录介质 ID 中包含的数据是否为素数的过程。

此外，本发明的第三方面是：

用于根据来自信息处理设备的服务提供请求执行服务提供过程

的数据处理方法，其特征在于具有：

数据接收步骤，从信息处理设备接收伴有信息记录介质 ID 和服务 ID 的服务请求；以及

数据处理步骤，执行验证接收到的信息记录介质 ID 的过程，在验证了信息记录介质 ID 的条件下，根据信息记录介质 ID 获取标题唯一值，从存储部分获取对应于所获取的标题唯一值的服务提供情况数据，判断被否可以提供由信息记录介质 ID 和服务 ID 指定的服务，并在判断可以提供服务的条件下执行服务提供过程，所述存储部分存储每一个信息记录介质 ID 的服务提供情况数据，作为对应于存储在信息记录介质上的内容的标题的每一个标题唯一值的服务管理数据。

此外，在本发明的数据处理方法的一个实施例中，数据处理步骤的特征在于包括下列步骤：作为验证信息记录介质 ID 中包含的签名数据的过程，执行验证信息记录介质 ID 的过程，并根据信息记录介质 ID 中包含的标题唯一值，或通过基于信息记录介质 ID 中包含的数据执行计算而计算出的标题唯一值，执行从存储部分获取对应于标题唯一值的服务提供情况数据的过程。

此外，在本发明的数据处理方法的一个实施例中，数据处理步骤中的验证信息记录介质 ID 的过程的特征在于包括作为将从信息处理设备接收到的信息记录介质 ID 与记录在撤销列表中的 ID 进行比较的过程来执行的步骤，所述撤销列表是未经授权的信息记录介质 ID 的列表。

此外，在本发明的数据处理方法的一个实施例中，信息记录介质 ID 的特征在于，被配置为包括对应于存储在信息记录介质中的内容的标题的标题唯一值，以及根据管理设备的秘密密钥生成的签名数据，并且所述信息记录介质 ID 对于每一个信息记录介质都是不同的，数据处理步骤的特征在于包括下列步骤：作为生成向消息应用管理设备的公钥的消息的过程，执行验证信息记录介质 ID 的过程，用于与信息记录介质 ID 中包含的签名数据进行比较，还执行从存储部分获

取对应于信息记录介质 ID 中包含的标题唯一值的服务提供情况数据的过程。

此外，在本发明的数据处理方法的一个实施例中，信息记录介质 ID 的特征在于，包括响应制造的信息记录介质的数量 w 中的每一个设置的素数 p(w)，以及由基于素数 p(w) 和标题唯一值的计算而计算出的数据 IDKey(w)，数据处理步骤的特征在于包括下列步骤：作为 ID 验证过程，执行判断信息记录介质 ID 中包含的数据是否为素数的过程，还根据信息记录介质 ID 中包含的数据 IDKey(w) 计算标题唯一值，从存储部分获取对应于计算出的标题唯一值的服务提供情况数据。

本发明的第四方面是：

用于执行发往服务提供服务器的服务提供请求的数据处理方法，其特征在于具有：

记录介质访问步骤，执行通过记录介质接口访问信息记录介质的过程；以及

数据处理步骤，执行验证通过记录介质接口从信息记录介质读取的信息记录介质 ID 的过程，并被验证了信息记录介质 ID 的条件下，执行向服务提供服务器传输信息记录介质 ID 的过程。

此外，在本发明的数据处理方法的一个实施例中，数据处理步骤的特征在于，作为验证信息记录介质 ID 中包含的签名数据的过程，执行验证信息记录介质 ID 的过程。

此外，在本发明的数据处理方法的一个实施例中，数据处理步骤中的验证信息记录介质 ID 的过程的特征在于包括下列步骤：从存储部分或信息记录介质中获取撤销列表，所述撤销列表是未经授权的信息记录介质 ID 的列表，以及将从信息处理设备接收到的信息记录介质 ID 与记录在所获取的撤销列表中的 ID 进行比较。

此外，在本发明的数据处理方法的一个实施例中，信息记录介质 ID 的特征在于，包括对应于存储在信息记录介质中的内容的标题的标题唯一值，以及根据管理设备的秘密密钥生成的签名数据，并且所

述信息记录介质 ID 对于每一个信息记录介质都是不同的，数据处理步骤的特征在于包括下列步骤：作为生成向消息应用管理设备的公钥的消息的过程，执行验证信息记录介质 ID 的过程，用于与信息记录介质 ID 中包含的签名数据进行比较。

此外，在本发明的数据处理方法的一个实施例中，信息记录介质 ID 的特征在于，包括响应制造的信息记录介质的数量 w 中的每一个设置的素数 p(w)，以及由基于素数 p(w) 和标题唯一值的计算而计算出的数据 IDKey(w)，数据处理步骤的特征在于包括下列步骤：作为 ID 验证过程，执行判断信息记录介质 ID 中包含的数据是否为素数的过程。

本发明的第五方面是：

用于根据来自信息处理设备的服务提供请求执行服务提供过程的计算机程序，其特征在于具有：

数据接收步骤，从信息处理设备接收伴有信息记录介质 ID 和服务 ID 的服务请求；以及

数据处理步骤，执行验证接收到的信息记录介质 ID 的过程，在验证了信息记录介质 ID 的条件下，根据信息记录介质 ID 获取标题唯一值，从存储部分，获取对应于所获取的标题唯一值的服务提供情况数据，判断被否可以提供由信息记录介质 ID 和服务 ID 指定的服务，并在判断可以提供服务的条件下执行服务提供过程，所述存储部分存储每一个信息记录介质 ID 的服务提供情况数据，作为对应于存储在信息记录介质上的内容的标题的每一个标题唯一值的服务管理数据。

本发明的第六方面是：

用于执行发往服务提供服务器的服务提供请求的计算机程序，其特征在于具有：

记录介质访问步骤，执行通过记录介质接口访问信息记录介质的过程；以及

数据处理步骤，执行验证通过记录介质接口从信息记录介质读取

的信息记录介质 ID 的过程，并被验证了信息记录介质 ID 的条件下，执行向服务提供服务器传输信息记录介质 ID 的过程。

注意，本发明的计算机程序是可以通过存储介质、通信介质，例如，诸如 CD 或 FD、MO 之类的存储介质，或诸如网络之类的通信介质提供的计算机程序，以计算机可读的形式提供到可以执行各种程序代码的通用计算机系统。通过以计算机可读的形式提供这样的程序，可以在计算机系统上实现根据程序的过程。

通过比较详细描述，本发明的其他目标、特点和优点将变得显而易见，详细描述是基于稍后描述的本发明的实施例和附图进行的。注意，本说明书中所使用的系统表示多个设备逻辑设置配置，不仅限于其中具有其自己的配置的每一个设备都组合在同一个外壳内的情况。

[本发明的效果]

根据本发明的配置，在这样的配置中，即提供存储在包括 DVD、CD、蓝色激光记录介质之类的各种信息记录介质中的内容，并且从联网的服务提供服务器执行服务提供过程，服务提供服务器验证从信息处理设备（用户设备）传输给它的信息记录介质 ID，并根据每一个信息记录介质 ID 的服务提供情况数据来提供服务。因此，只有在传输了服务请求的信息处理设备是从信息记录介质中读取了有效信息记录介质 ID 的信息处理设备的情况下，并且只有在根据服务提供情况数据验证了可以提供服务的情况下，才提供服务。

此外，根据本发明的配置，存储在信息记录介质上的信息记录介质 ID 包括可以检查其有效性的数据，如管理设备的签名数据，还可以具有标题唯一值或者包括可以用来计算标题唯一值的数据。因此，服务提供服务器可以基于信息记录介质 ID 中包括的数据检查有效性，另外，还可以获取标题唯一值，从而，服务器可以指定服务提供情况数据集，以便对应于标题唯一值。

附图说明

[图 1] 它是用于说明存储在信息记录介质中的数据的图表。

[图 2] 它是用于说明撤销列表的配置的图表。

[图 3] 它是用于说明当使用 MAC(消息验证代码)时 MAC 生成/验证过程的图表。

[图 4] 它是用于说明应用于加密和分发各种密钥和数据的过程的分层树形结构的图表。

[图 5] 它是显示了使用 EKB(启用密钥块)分发内容密钥并对其进行解密的示例的图表。

[图 6] 它是用于说明制造、管理信息记录介质的配置的图表。

[图 7] 它是用于说明服务提供服务器的配置示例的图表。

[图 8] 它是用于说明服务提供服务器持有的服务提供情况数据的图表。

[图 9] 它是用于说明信息处理设备(用户设备)的配置示例的图表。

[图 10] 它是用于说明光盘 ID 设置示例的图表。

[图 11] 它是用于说明信息处理设备(用户设备)执行的过程的流程图。

[图 12] 它是用于说明信息处理设备(用户设备)执行的光盘 ID 验证序列的流程图。

[图 13] 它是用于说明信息处理设备(用户设备)执行的光盘 ID 验证序列的流程图。

[图 14] 它是用于说明信息处理设备(用户设备)执行的光盘 ID 验证序列的流程图。

[图 15] 它是用于说明信息处理设备(用户设备)执行的光盘 ID 验证序列的流程图。

[图 16] 它是用于说明信息处理设备从服务提供服务器接收服务的过程的图表。

[图 17] 它是用于说明服务提供服务器执行的过程的流程图。

具体实施方式

下面,将参考图形描述根据本发明的服务提供服务器、信息处理设备、数据处理方法、以及计算机程序的详细信息。注意,将按照下

列项目进行描述:

1. 存储在信息记录介质中的数据

2. 用于提供存储了内容的信息记录介质以及使用它们/对它们进行管理的配置

3. 包括服务提供服务器和用户设备的信息处理设备的配置

4. 用户设备中的处理的详细信息

5. 服务提供服务器中的处理的详细信息

[1. 存储在信息记录介质中的数据]

图 1 显示了记录在信息记录介质中的数据的配置示例。图 1 是用于说明存储在包括 CD（压缩光盘）、DVD（数字通用光盘）、MD（小型光盘）、蓝色激光光盘（Blu-ray 光盘）、闪速存储器的各种信息记录介质 100 中的数据的图表。尽管图 1 中作为示例显示了盘状的介质，但是，本发明不仅适用于这样的盘状的介质，而且还适用于包括闪速存储器的各种信息记录介质。

在信息记录介质 100 上，存储了图 1 所示的信息，即，光盘 ID 101、内容 102、光盘 ID 撤销列表 (DIRL) 103、加密密钥信息（EKB: 启用密钥块）104。

光盘 ID 101 可以是光盘所特有的标识符，其存储方式应该很难擦除或改写。注意，光盘 ID 101 包括对应于存储在信息记录介质 100 上的内容 102 的每一个标题的唯一值（标题唯一值）、每一个信息记录介质 100 的唯一值（光盘唯一值），以及表示其有效性的信息，例如，诸如签名之类的信息（有效性验证值）。稍后将描述光盘 ID 的详细信息。

注意，由于在下面描述的实施例中显示了盘状的介质作为存储了内容的信息记录介质，因此，其标识符被描述为光盘 ID。如果使用诸如闪速存储器之类的任何其他信息记录介质作为存储了内容的信息记录介质，则设置对应于光盘 ID 的信息记录介质 ID。

内容 102 也存储在信息记录介质 100 上。内容是作为加密的内容来存储的。在加密的内容的情况下，用于对内容进行解密的密钥信

息要么存储在信息记录介质 100 中，要么通过网络提供。

光盘 ID 撤销列表 (DIRL) 103 也存储在信息记录介质 100 上。光盘 ID 撤销列表 (DIRL) 103 是这样的数据，当在市场上发现了被认为是未经授权复制的任何光盘，例如，存储了未经授权的复制的内容的 CD-R，则提取并列出未经授权的 CD-R 上复制的光盘 ID 以及内容。由中心机构 (CA) 执行光盘 ID 撤销列表 (DIRL) 103 的生成和管理，并将列表信息提供给光盘制造商等等。

下面将参考图 2 描述光盘 ID 撤销列表 (DIRL) 的数据配置。如图 2 所示，光盘 ID 撤销列表 (DIRL) 150 包括随着创建列表的时间单调地增大的版本号 151、枚举了光盘的光盘 ID 以便排除的被撤销光盘 ID 列表 152，以及作为版本号 151 和被撤销光盘 ID 列表 152 的窜改验证值 153 的验证器。窜改验证值 153 是用于判断用于验证的数据（即，在此情况下，版本号 151 和被撤销光盘 ID 列表 152）是否被窜改的数据。使用公钥加密技术的数字签名，以及使用对称密钥加密技术的消息验证代码 (MAC) 也适用。

如果是使用公钥加密技术的数字签名被用作窜改验证值 153，则播放设备获取可靠的实体（例如，上文所提及的中心机构 (CA)）的签名验证密钥（公钥），并使用每一个播放机获取的签名验证密钥（公钥）来验证利用中心机构 (CA) 签名生成密钥（秘密密钥）创建的签名，从而判断版本号 151 和被撤销光盘 ID 列表 152 是否已经被窜改。

下面将参考图 3 描述使用 MAC 作为窜改验证值 153 的消息验证代码 (MAC) 生成/验证过程。生成消息验证代码 (MAC) 作为窜改验证的数据。尽管有各种模式可用于 MAC 生成/验证过程，但是，图 3 显示了使用 DES 加密过程配置生成 MAC 值的示例。

如图 3 所示，用于处理的消息，即，在此情况下，版本号 151 和被撤销光盘 ID 列表 152，被分成 8 字节块（被划分的消息以下简称为 M1、M2，...，MN）。首先，将初始值（以下简称为 IV）与 M1 进行异或运算（结果是 I1）。接下来，将 I1 输入到使用密钥（以下

简称为 K1）的 DES 加密部分（其输出是 E1）。再接下来，将 E1 与 M2 进行异或运算，并将其输出 I2 输入到使用密钥 K1 的 DES 加密部分（输出是 E2）。此后，重复此过程，以对所有消息进行加密。最后一个输出 EN 是消息验证代码 (MAC)。

一旦其生成元数据已经改变，MAC 值使用不同的值。如此，如果根据用于验证的数据（消息）生成的 MAC 和记录的 MAC 之间的比较表明两者一致，则证明了用于验证的数据（消息）没有被改变或窜改。

返回到图 1，下面将继续描述存储在信息记录介质 100 中的数据。加密密钥信息（EKB: 启用密钥块）104 也存储在信息记录介质 100 中。

下面将参考图形描述用于使用加密密钥信息 (EKB) 提供机密信息的配置。图 4 的最下层所显示的编号 0-15 是作为使用内容的信息处理设备的用户设备。即，图 4 所示的分层树形结构中的叶子分别对应于设备。

每一个设备 0-15 都在其制造或装运时或此后将密钥集（设备密钥（DNK: 设备节点密钥））存储在存储器中。密钥集 (DNK) 包括分配给分层树形结构中的从其自己的叶子到根的路径中的节点的密钥（节点密钥），以及其自己的叶子的叶子密钥。图 4 中的最下层所显示的符号 K0000-K1111 是分别分配给设备 0-15 的叶子密钥，从最上层的 KR（根密钥）到下面的倒数第二层中的节点表示的密钥 KR-K111 是节点密钥。

例如，在图 4 所示的树形结构中，设备 0 拥有叶子密钥 K0000，以及节点密钥 K000、K00、K0、KR 作为设备密钥。设备 5 拥有 K0101、K010、K01、K0、KR。设备 15 拥有 K1111、K111、K11、K1、KR。注意，在图 4 的树中只显示了十六个设备 0-15，树形结构是具有四层的对称结构。然而，在树内包括更多设备的其他配置，在树的某些部分具有不同的层也是适用的。

此外，图 4 的树形结构中的设备还包括各种记录介质，如，

DVD、CD、MD、嵌入在设备中或可从设备中取出的闪速存储器。此外，各种应用程序服务也可以共存。它位于这样的配置中，其中，不同设备和不同应用程序共存，其中，应用了图 4 所示的分层树形结构（内容或密钥分发配置）。

在这样的各种设备和应用程序共存的系统中，图 4 中的虚线包围起来的部分中的设备，即，设备 0、1、2、3 被分为一组。例如，只有由虚线包围起来的并包括在该组中这些设备才拥有授权的权限，即，使用存储在信息记录介质上的加密内容的许可证。在此情况下，设置了 EKB，以便只有设备 0、1、2、3 才可以获取用于对内容进行解密的密钥，设置的 EKB 存储在其中存储了加密内容的信息记录介质中。

从图 4 可以看出，包括在同一个组中的三个设备 0、1、2、3 拥有共享的密钥 K00、K0、KR 作为存储在它们的设备中的设备密钥（DNK: 设备节点密钥）。

如此，在图 5 中显示了只允许设备 0、1、2 获取用于对内容进行解密的内容密钥 Kcon 的 EKB 配置。即，按如下方式设置 EKB:

索引	加密数据
000	Enc (K000, Kcon)
0010	Enc (K0010, Kcon)

注意，Enc (Kx, Ky) 表示用密钥 Kx 加密的数据 Ky。如此，设备 0、1 可以使用它们所拥有的设备密钥 [K000] 对索引为 [000] 的加密数据进行解密，设备 2 也可以使用它所拥有的设备密钥 [K0010] 对 EKB 中的索引为 [0010] 的加密数据进行解密。它们可以通过它们的对相应的加密数据进行解密的过程获取内容密钥 Kcon。另一个设备没有设备密钥 [K000]、[K0010] 中的任何一个，如此，不能通过对 EKB 进行解密来获取内容密钥，即使接收到了如图 5 所示的如此配置的 EKB。

如此，EKB 被设置为具有对应于被授权的设备的配置的数据，从而，EKB 被配置为仅仅可以由任何所选择的设备处理的密钥信息

块，通过该密钥信息块，诸如内容密钥之类的机密信息只能提供给特定设备。密钥信息 (EKB) 颁发中心 104 生成仅仅可以由它允许使用其内容的设备处理的 EKB，并将该 EKB 提供到信息记录介质制造实体 103。信息记录介质制造实体 103 将 EKB 连同加密内容存储在信息记录介质 110 中，并将介质提供给用户。

[2. 用于提供存储了内容的信息记录介质以及使用它们/对它们进行管理的配置]

图 6 是说明用于提供存储了上文所提及的各种数据的信息记录介质 200 以及使用它们/对它们进行管理的配置。

如图 6 所示，在提供内容并对内容进行管理的配置中，有供中心机构 (CA) 使用的管理设备 201、供内容提供商使用的内容提供设备 203、供光盘制造商使用的光盘制造设备 202、供用户用于执行内容播放过程的信息处理设备（用户设备）400、以及服务提供服务器 300，用于对于信息处理设备（用户设备）400 执行提供对应于存储在信息记录介质 200 上的内容的服务（例如，小标题）的过程。

管理设备 201 生成如前所述的光盘 ID 和光盘 ID 撤销列表 (DIRL)，并将它们提供到光盘制造设备 202。此外，内容提供设备 203 还向光盘制造设备 202 提供加密内容和启用密钥块 (EKB)。

光盘制造设备 202 制造信息记录介质 200，在该介质 200 中，记录了从管理设备 201 接收到的光盘 ID 和光盘 ID 撤销列表 (DIRL) 以及从内容提供设备 203 接收到的加密内容数据和启用密钥块 (EKB)。

用户购买了信息记录介质 200，并将它放置到信息处理设备（用户设备）400 中。信息处理设备（用户设备）400 可以验证记录在信息记录介质 200 中的光盘 ID 是否有效，检查在撤销列表 DIRL 中没有发现该光盘 ID，并根据其自己的设备节点密钥数据 DNK 从启用密钥块 EKB 获取适当的内容密钥数据，从而，他/她可以对加密内容数据进行解密，并播放该内容数据。

此外，信息处理设备（用户设备）400 将记录在信息记录介质 200

上的光盘 ID 和作为服务标识符的服务 ID 传输到服务提供服务器 300。然后，在服务提供服务器 300 中，验证光盘 ID 的有效性，并进一步，根据服务提供服务器 300 所拥有的服务提供情况数据判断是否可以提供服务。如果根据服务提供情况数据判断光盘 ID 是有效的并且可以提供服务，则服务器 300 为信息处理设备（用户设备）400 执行其服务提供过程。

[3. 包括服务提供服务器和用户设备的信息处理设备的配置]

接下来，描述作为服务提供服务器和用户设备的信息处理设备的配置。

图 7 是显示了图 6 所示的服务提供服务器的配置的图表。如图 7 所示，服务提供服务器 300 具有包括 CPU 的控制器 302、用于执行各种计算过程的计算单元 303、输入/输出接口 (I/F) 304，作为从数据输入设备输入数据以及向输出数据设备输出数据的接口，以及通过网络输入/输出数据的接口，安全存储器 305、主存储器 306。这些组件通过总线 301 互连在一起。

主存储器 306 存储了用于由计算单元 303 和控制器 302 进行的处理的各种数据中的低安全性级别的数据。安全存储器 305 存储了用于由计算单元 303 和控制器 302 进行的处理的各种数据中的高安全性级别的数据。例如，安全存储器 305 存储了从图 6 所示的管理设备 201 接收到的光盘 ID 等等。

输入/输出接口 304 连接到控制装置或网络（未显示），并从图 6 所示的管理设备 201 和内容提供设备 203 接收各种数据。接口 304 进一步与将接收服务的信息处理设备（用户设备）400 进行通信，以便提供服务。

计算单元 303 根据控制器 302 的控制，执行各种计算，包括生成签名数据的验证数据。控制器 302 执行各种程序，如，关于是否可以向用户设备提供服务的检查程序，服务提供程序。

服务提供服务器 300 定期或对于每一个事件通过输入/输出接口 (I/F) 304 从管理设备 201、内容提供设备 203 或其他设备接收光

盘 ID 撤销列表，并不断地将最新的版本存储在安全存储器 305 中。

此外，服务器 300 还通过输入/输出接口 (I/F) 304 从内容提供设备 203 或其他设备接收基于标题的标题唯一值和用于识别待提供的服务的服务标识信息，并将其中管理了基于标题的服务提供情况信息的服务提供情况数据库存储在安全存储器 305 中。

“标题”表示对应于存储在被放置于信息处理设备(用户设备)400 中的信息记录介质 200 上的内容的标题。

图 8 显示了服务提供情况数据库的数据配置的示例。如图 8 所示，服务提供情况数据库包括，关于对应于服务提供服务器 300 所提供的服务的内容的标题标识信息，关于为每一个标题唯一值设置的服务的并对应于存储了具有该标题的内容的光盘的光盘 ID 的服务提供情况。

例如，图 8(a) 中所显示的服务提供情况数据是关于如下情况的服务提供情况数据:

标题标识信息: aaaa; 以及

标题唯一值: bbbb,

并是基于分别具有光盘 ID 1 和光盘 ID 2 的光盘，到目前为止响应服务提供请求，提供的与对应于此标题的内容关联的服务 1 和服务 2 的次数的记录。

注意，在图 8(a) 中所显示的服务提供情况数据中，

服务 1 是规定只能向光盘 ID 1 提供一次的服务，以及

服务 2 是规定最多可以向光盘 ID 2 提供 5 次的服务。

服务提供服务器 300 将图 8 所显示的服务提供情况数据存储在安全存储器 305 中，并将它们保存在那里，并响应来自信息处理设备(用户设备)400 的伴有光盘 ID 的服务提供请求，检查发出了服务提供请求的设备是否基于有效光盘 ID 发出服务提供请求，并根据图 8 中所显示的服务提供情况数据，只有在没有到达可以提供服务的上限的情况下才提供服务。

当从信息处理设备(用户设备)400 接收到伴有光盘 ID 的服

务提供请求时，服务提供服务器 300 验证从信息处理设备（用户设备）400 传输给它的光盘 ID，还检查在服务提供服务器 300 所持有的撤销列表中没有撤销从信息处理设备（用户设备）400 传输给它的光盘 ID。

此外，服务提供服务器 300 还执行诸如基于经过验证的光盘 ID 检查或提取标题唯一值，提取光盘唯一值之类的处理。然后，服务器 300 根据所获取的标题唯一值，通过参考存储了图 8 中所显示的服务提供情况数据的数据库，指定关于对应的标题的服务提供情况数据，并根据指定的数据，检查服务器 300 是否可以提供服务。即，根据图 8 中所显示的服务提供情况数据，只有在没有到达可以提供服务的上限的情况下服务器 300 才提供服务。

注意，在图 8 中所显示的服务提供情况数据的配置示例中，为每一个光盘 ID 存储了服务提供情况数据。然而，也可以采用其他配置，其中，使用用于识别单个光盘的光盘唯一值来代替光盘 ID。

注意，当向信息处理设备（用户设备）400 提供了服务时，服务提供服务器 300 更新图 8 中所显示的服务提供情况数据。

下面请参看图 9，将描述信息处理设备（用户设备）400 的配置。

如图 9 所示，信息处理设备（用户设备）400 具有输入/输出接口 402、编解码器 403，用于执行生成诸如 MPEG（活动图像专家组）之类的各种编码数据并对其进行解码，拥有 A/D 和 D/A 转换器 405 的输入/输出接口 404、加密处理部分 406、ROM（只读存储器）407、控制器 408、存储器 409，以及用于访问信息记录介质 200 的记录介质接口。这些组件互连到总线 401。

输入/输出接口 402 接收从诸如网络之类的外部源提供的数字信号，以便输出到总线 401 中，也可以接收总线 401 上的数字信号，以便输出到外部源。

编解码器 403 对通过总线 401 提供的 MPEG 编码数据进行解码，以便输出到输入/输出接口 404，还对从输入/输出接口 404 提供的数字信号进行编码，以便输出到总线 401 中。

输入/输出接口 404 包括了 A/D 和 D/A 转换器 405。输入/输出接口 404 接收从外部源提供的模拟信号，并使用 A/D 和 D/A 转换器 405 对该信号进行模拟-数字转换处理，以便作为数字信号输出到编解码器 403，还使用 A/D 和 D/A 转换器 405 对来自编解码器 403 的数字信号进行数字-模拟转换处理，以便作为模拟信号输出到外部源。

加密处理部分 406 可以由单芯片 LSI 制成，具有用于对数字信号（如通过总线 401 提供给它的内容）进行加密或进行解密的配置，以便输出到总线 401 中。注意，加密处理部分 406 不仅限于单芯片 LSI，而可以通过其中组合了各种软件或硬件的配置来实现。

ROM 407 存储了叶子密钥数据，该数据要么是作为用户设备的每一个信息处理设备所特有的设备密钥，要么是包含多个信息处理设备（用户设备）的每一个组所特有的设备密钥，以及节点密钥数据，该数据是在多个播放设备或者多个组之间共享的设备密钥数据。 这些数据用于对作为加密密钥信息的如前所述的启用密钥块 (EKB) 进行解密的过程。

控制器 408 包括用于执行存储在存储器 409 中的程序的 CPU。控制器 408 集中地控制对信息处理设备（用户设备）400 的处理。即，通过由控制器 408 执行的程序来调节信息处理设备（用户设备）400 的功能（处理）。

存储器 409 从信息记录介质 200 中读取上文所提及的光盘 ID 撤销列表 (DIRL) 以便进行安全的存储。例如，优选情况下，通过根据为每一个信息处理设备（用户设备）400 设置的 ID，作为加密形式将数据存储在存储器中来保留抗窜改数据。如此，这样存储光盘 ID 撤销列表 (DIRL)，以便它不会轻松地从外部被擦除、窜改或替换为任何旧的版本。记录介质接口 410 被用来访问信息记录介质 200。

[4. 用户设备中的处理的详细信息]

接下来，描述当作为用户设备的信息处理设备 400 在从服务提

供服务器 300 接收到服务时执行的处理的详细信息。

图 10 是用于说明其中装入了信息记录介质的图 9 所示的信息处理设备（用户设备）400 在从服务提供服务器接收到服务时执行处理的序列的流程图。

在步骤 S101 中，在将信息记录介质 200 置于信息处理设备的预先确定的访问位置时，信息处理设备（用户设备）400 通过记录介质接口 410 从信息处理介质 200 读取光盘 ID，并将它存储在存储器 409 中。

在步骤 S102 中，信息处理设备（用户设备）400 的 控制器 408 读取存储在存储器 409 中的光盘 ID，以验证它是否被窜改以及它是否有效。稍后将描述此验证过程。

在步骤 S103 中，在控制器 408 在 S102 步骤中判断了上述光盘 ID 是有效的情况下，进入步骤 S105；否则，控制器 408 进入步骤 S104。在步骤 S104 中，控制器 408 停止（禁止）记录在信息记录介质 200 上的加密内容的解密和播放。

如果已经判断光盘 ID 是有效的，则控制器 408 在步骤 S105 中通过记录介质接口 410 从信息记录介质 200 中读取光盘 ID 撤销列表 (DIRL)。如果使用公钥加密技术的数字签名被作为读取的撤销列表的窜改验证值，则控制器 408 使用签名验证密钥（公钥）对列表 DIRL 进行验证。如果消息验证代码 MAC 被作为窜改验证值，则执行早先参考图 3 所描述的 MAC 验证过程。

在判断光盘 ID 撤销列表 (DIRL) 未被窜改的条件下，控制器 408 将该光盘 ID 撤销列表 (DIRL) 的版本和已经存储在存储器 409 中的光盘 ID 撤销列表 (DIRL) 的版本进行比较。

如果读取的光盘 ID 撤销列表 (DIRL) 的版本比已经存储在存储器 409 中的光盘 ID 撤销列表 (DIRL) 的版本新，则控制器 408 用读取的光盘 ID 撤销列表 (DIRL) 更新存储器 409 中的撤销列表 DIRL。

在步骤 S106 中，控制器 408 判断在步骤 S101 中读取的光盘

ID 是否存在于撤销列表 DIRL 中，当判断它存在时，进入步骤 S107；否则，进入步骤 S108。在步骤 S107 中，控制器 408 停止（禁止）记录在信息记录介质 200 上的加密内容的解密和播放。

如果光盘 ID 不存在于撤销列表中，则控制器 408 在进入步骤 S108 之后，将在步骤 S101 中读入的光盘 ID 传输到服务提供服务器，进一步，在步骤 S109 中，从服务提供服务器接收服务。注意，服务提供服务器验证在步骤 S108 中从信息处理设备（用户设备）400 接收到的光盘 ID，并且只有在光盘 ID 被验证的情况下才执行服务提供过程。

下面将描述在步骤 S102 中执行的光盘 ID 验证过程。存储在信息记录介质中的光盘 ID 被设置为高度抗仿造的标识信息。图 11 显示了一个光盘 ID 格式示例。

图 11 显示了六种光盘 ID 设置示例，每一种都指出了作为信息记录介质标识符的信息记录介质 ID（光盘 ID），标题唯一值（是被设置为存储在信息记录介质上的内容的标题的唯一值），以及被设置为信息记录介质的唯一值的光盘唯一值之间的对应关系。注意，光盘 ID 和光盘唯一值都是由管理设备 201 生成的。标题唯一值 M 可以是构成了存储在信息记录介质上的内容的信息的一部分也可以被配置为由管理设备 201、内容提供设备 203 生成。标题唯一值 S 是由管理设备 201 根据标题唯一值 M 生成的。

图 11 所示符号具有下列含义：

M：对应于存储在信息记录介质上的内容的标题的唯一值；

w：$w = 1, 2, ..., W$，其中，W 是要制造的信息记录介质的数量；

Sig(w)：基于管理设备的秘密密钥（例如，根据公钥加密技术设置的秘密密钥）的签名数据，它是根据要制造的信息记录介质的数量 W 生成的，如此，对于每一个信息记录介质是不同的。Sig(w) 表示光盘的签名被设置为 Sig(1), Sig(2), ..., Sig(W)；

p(w)：被设置对应于要制造的信息记录介质的数量 W 的素数。为根据要制造的信息记录介质的数量 w 生成的每一个信息记录介质

设置了不同的素数数据；以及

S：对应于存储在信息记录介质上的内容的标题的唯一值，并且 $S = K^T \bmod M$，其中，T 是由下列公式给出的值：

[数学式 1]

$$T = \prod_{w=1}^{W} p_w$$

IDKey(w)：$IDKey(w) = K^{T/p(w)} \bmod M$

其中，K 是被设置到每一个标题的值，并满足 $K \in Z'_M$（K 是循环群 $K \in Z'_M$ 的生成元。注意，对于每一个 $X \in Z'_M$，以整数存在元素 $X^{-1} \in Z'_M$ modulo x，x 是 1 到 X－1）。

e(w)：对应于要制造的光盘数量 W 的不同的值，满足 $e(w) \in Z'_M$，其中，e(w) 和 λ(M) 是不相交的，即，e(w) 和 λ(M) 的最大公约数是 1。注意，λ(M) 是素数 (q1 - 1) 和 (q2 - 1) 的最小公倍数，其中，q1、q2 是足够大，可以应用于 RSA 加密的素数。

I (w)：$I(w) = S^{d(w)} \bmod M$

其中，d(w) 是 e(w) modulo λ(M) 的倒数。

Σw：通过对消息 M(w) 进行加密而获得的数据，消息 M(w) 是通过将数据 S 和数据 e(w) 与管理设备 (CA) 201 的秘密密钥连接在一起而获得的连接数据。

下面将描述对应于图 11 所示的六个不同光盘 ID 设置示例的信息处理设备（用户设备）400 中的光盘 ID 验证处理序列。

下面请参看图 12，描述对应于设置示例 1 的信息处理设备（用户设备）400 中的光盘 ID 验证处理序列。

在设置示例 1 中，

设置了

光盘 ID = M，Sig(w)，

标题唯一值 = M，以及

光盘唯一值 = Sig(w)

在步骤 S201 中，信息记录设备（用户设备）400 的控制器 408 提取光盘 ID(w) 中的签名数据 SIG(w)。注意，光盘 ID 被表示为光

盘 ID(w)，因为它取每一个单个光盘 (w) 所特定的值，其中，w＝1, 2, ... W，假设要制造的光盘数量是 W。

在步骤 S202 中，控制器 408 根据管理设备 12（中心机构，CA）的公钥和发布的参数，从在步骤 S201 中读取的签名数据 SIG(w) 生成 M(w)'。还可以类似于光盘 ID(w) 地表示消息。消息 M(w) 表示，使消息对应于每一个光盘。

在步骤 S203 中，控制器 408 将光盘 ID(w) 中包含的消息 M(w) 与在步骤 S202 中生成的消息 M(w)' 进行比较。

在步骤 S204 中，当在步骤 S203 中的比较过程中判断两者一致时，控制器 408 进入步骤 S205；否则，它进入步骤 S206。

在步骤 S205 中，控制器 408 判断在步骤 S201 中提取的光盘 ID(w) 有效。在步骤 S206 中，控制器 408 判断在步骤 S201 中提取的光盘 ID(w) 无效。

在设置示例 2 中，

设置了

光盘 ID = S, Sig(w),

标题唯一值 ＝S，以及

光盘唯一值 ＝Sig(w)

此设置示例 2 与设置示例 1 的不同之处只在于标题唯一值 S 代替了 M。如此，信息处理设备（用户设备）400 中的其光盘 ID 验证处理序列类似于设置示例 1 中的光盘 ID 验证处理序列，只是在步骤 S202 中从签名数据生成的数据是消息 S'(w)，用于在步骤 S203 中进行比较的数据是光盘 ID 中包含的数据 S(w)。

下面请参看图 13，描述对应于设置示例 3 的信息处理设备（用户设备）300 中的光盘 ID 验证处理序列。

在设置示例 3 中，

设置了

光盘 ID = p(w)，IDKey(w)，

标题唯一值 ＝S，以及

光盘唯一值 = p(w) 或 IDKey(w)

在步骤 S301 中，信息处理设备（用户设备）400 的控制器 408 提取从信息记录介质 200 中读取的光盘 ID(w) 中的数据 p(w)。

在步骤 S302 中，控制器 408 判断在步骤 S302 中提取的数据 p(w) 是否为素数。当判断数据 p(w) 是素数时，控制器 408 进入步骤 S303; otherwise，它进入步骤 S304。

在步骤 S303 中，控制器 408 判断在步骤 S301 中提取的光盘 ID(w) 有效。在步骤 S304 中，控制器 408 判断在步骤 S301 中提取的光盘 ID(w) 无效。

下面请参看图 14，描述对应于设置示例 4 的信息处理设备（用户设备）400 中的光盘 ID 验证处理序列。

在设置示例 4 中，

设置了

光盘 ID = e(w)，I(w)，

标题唯一值 = S，以及

光盘唯一值 = e(w) 或 I(w)

在步骤 S401 中，信息处理设备（用户设备）400 在将信息记录介质 200 置于预先确定的访问位置时，通过记录介质接口 410 从信息记录介质 200 读取光盘 ID，并将它存储在存储器 409 中。

在步骤 S402 中，信息处理设备（用户设备）400 的控制器 408 使用记录在存储器 409 中的光盘 ID 中的数据 e(w) 和 I(w) 计算 $I(w)^{e(w)} \bmod M$，并将结果设置数据 S'。即，

$$S' = I(w)^{e(w)} \bmod M$$

在步骤 S403 中，控制器 408 通过记录介质接口 410 从信息记录介质 200 中读取光盘 ID 撤销列表 (DIRL)。在使用公钥加密技术的数字签名被作为读取的撤销列表的窜改验证值的情况下，则控制器 408 使用签名验证密钥（公钥）对列表 DIRL 进行验证。在消息验证代码 MAC 被作为窜改验证值的情况下，执行早先参考图 3 所描述的 MAC 验证过程。

在判断光盘 ID 撤销列表 (DIRL) 未被窜改的条件下，控制器 408 将该光盘 ID 撤销列表 (DIRL) 的版本和已经存储在存储器 409 中的光盘 ID 撤销列表 (DIRL) 的版本进行比较。在读取的光盘 ID 撤销列表 (DIRL) 的版本比已经存储在存储器 409 中的光盘 ID 撤销列表 (DIRL) 的版本新，则控制器 408 用读取的光盘 ID 撤销列表 (DIRL) 更新存储器 409 中的撤销列表 DIRL。

在步骤 S404 中，控制器 408 判断在步骤 S401 中读入的光盘 ID 是否存在于撤销列表中，当判断它存在时，进入步骤 S405; 否则，进入步骤 S406。

在步骤 S405 中，控制器 408 停止（禁止）记录在信息记录介质 200c 上的加密内容的解密和播放。在步骤 S406 中，控制器 408 将在步骤 S401 中读取的光盘 ID 传输到服务提供服务器，此外，在步骤 S407 中，从服务提供服务器中接收服务。注意，服务提供服务器验证在步骤 S406 中从信息处理设备（用户设备）400 接收到的光盘 ID，并且只有在光盘 ID 被验证的情况下才执行服务提供过程。

下面请参看图 15，描述对应于设置示例 5 的信息处理设备（用户设备）400 中的光盘 ID 验证处理序列。

在设置示例 5 中，

设置了

光盘 ID = Σw，

标题唯一值 = S，以及

光盘唯一值 = e(w)

在步骤 S501 中，信息处理设备（用户设备）400 的控制器 408 根据管理设备 201（中心机构，CA）的公钥数据，对从信息记录介质 200 读取的光盘 ID(w) 进行解密，以生成消息 M(w)。如前所述，消息 M(w) 是其中数据 S 和数据 e(w) 连接在一起的数据。

在步骤 S502 中，信息处理设备（用户设备）400，根据管理设备 201 发布的大小 |S|、大小 |e(w)|，以及数据 S 和数据 e(w) 的组合模式,从在步骤 S501 中解密的消息 M(w) 提取数据 S。

在图 15 所示的上文所提及的过程之后，信息处理设备（用户设备）400 执行图 10 所示的步骤 S105-S109。在此情况下，在图 10 所示的步骤 S105、S106 中的与撤销列表进行的光盘 ID 比较过程中，信息处理设备（用户设备）400 使用在步骤 S501 中从信息记录介质 200 中读取的光盘 ID(w) 作为光盘 ID。

信息处理设备（用户设备）400 使用在步骤 S502 中提取的数据 S 作为内容密钥数据，对内容数据进行解密。因此，在不能通过步骤 S501、S502 的上述过程获取适当的数据 S 的情况下，不能适当地对内容数据进行解密。

在设置示例 6 中，设置了

光盘 ID = p(w)，IDKey(w)，

标题唯一值 = S，以及

光盘唯一值 = p(w)

这具有类似于设置示例 3 中的光盘 ID 配置，如此，执行类似于早先参考图 13 所描述的过程的光盘 ID 验证过程。

[5. 服务提供服务器中的处理的详细信息]

接下来，描述了当服务提供服务器 300 从信息处理设备（用户设备）400 接收到服务提供请求时服务提供服务器 300 执行的过程。

如图 16 所示，服务提供服务器 300 从信息处理设备（用户设备）400 接收光盘 ID。此光盘 ID 是通过信息处理设备（用户设备）400 中的验证过程而验证了其有效性的光盘 ID，信息处理设备（用户设备）400 在其中装入了信息记录介质 200 之后执行了从信息记录介质 200 中读取光盘 ID 的过程。

服务提供服务器 300 在从信息处理设备（用户设备）400 接收到光盘 ID 以及服务提供请求之后，验证光盘 ID 的有效性，此后，在验证了光盘 ID 的条件下提供服务。

注意，信息处理设备（用户设备）400 传输作为服务标识符的服务 ID，连同光盘 ID，以及服务提供请求。

服务提供服务器 300 定期或对于每一个事件通过图 7 所示的

输入/输出接口 (I/F) 304 从管理设备 201、内容提供设备 203 或其他设备接收光盘 ID 撤销列表，并执行不断地将最新的版本存储在安全存储器 305 中的过程。此外，服务器 300 还通过输入/输出接口 (I/F) 304 从内容提供设备 203 或其他设备接收基于标题的标题唯一值和用于标识服务器 300 提供的服务的服务标识信息，并将其中管理了基于标题的服务提供情况信息的早先参考图 8 所描述的服务提供情况数据库存储在安全存储器 305 中。

服务提供服务器 300 将图 8 中所显示的服务提供情况数据存储并保存在安全存储器 305 中，并响应来自信息处理设备（用户设备）400 的伴有光盘 ID 的服务提供请求，检查发出了服务提供请求的设备是否基于有效光盘 ID 发出服务提供请求，并根据图 8 中所显示的服务提供情况数据，只有在没有到达可以提供服务的上限的情况下才提供服务。

下面将参考图 17 描述了当服务提供服务器 300 从信息处理设备（用户设备）400 接收到服务提供请求时服务提供服务器 300 执行的处理序列。

在步骤 S701 中，服务提供服务器 300 通过图 7 所示的输入/输出接口 (I/F) 304 从信息处理设备（用户设备）400 接收服务提供请求。此来自信息处理设备（用户设备）400 的服务提供请求包括信息处理设备（用户设备）400 从信息记录介质 200 获取的光盘 ID，以及被请求的服务的标识符（服务标识符）。光盘 ID 是早先参考图 11 描述的设置示例 1-6 中的任何一个光盘 ID。

在步骤 S702 中，服务提供服务器 300 执行验证接收到的光盘 ID 的过程。根据类似于在信息处理设备（用户设备）400 中执行的验证过程的验证序列的验证序列，即，根据参考图 12-15 描述的光盘 ID 设置示例 1-6 中的任何一个的验证序列，来执行此验证过程。

当在步骤 S703 中按照光盘 ID 验证过程验证光盘 ID 时，过程进入步骤 S705。当判断光盘 ID 是无效的时，过程进入步骤 S704，以停止提供服务。注意，对于此停止过程，可以向信息处理设备（用

户设备）400 传输说明停止服务提供过程的消息。

在验证了光盘 ID 并且过程进入步骤 S705 的情况下，服务器 300 读取存储在安全存储器 305 中的光盘 ID 撤销列表 (DIRL)(参见图 7）。

在步骤 S706 中，服务器 300 判断接收到的被验证了的光盘 ID 是否记录在撤销列表中。

在接收到的光盘 ID 记录在撤销列表中，服务器 300 判断光盘 ID 是无效的情况下，过程进入步骤 S711，以停止服务提供过程。注意，对于此停止过程，可以向信息处理设备（用户设备）400 传输说明停止服务提供过程的消息。

在接收到的光盘 ID 没有记录在撤销列表中的情况下，那么，在步骤 S707 中，服务器 300 根据光盘 ID 计算标题唯一值。光盘 ID 被配置为包含标题唯一值 M 或 S 的数据或可以用来计算标题唯一值 M 或 S 的数据，如早先参考图 11 所描述的。服务提供服务器 300 获取包含在接收到的光盘 ID 中的标题唯一值 M 或 S，或从由计算单元 303 执行的计算过程而得到的光盘 ID 计算标题唯一值 M 或 S。此获取、计算标题唯一值 M 或 S 的过程是作为不同于早先参考图 11 描述的设置示例 1-6 的过程来执行的。

在步骤 S707 中，服务器进一步可以根据从光盘 ID 获取的标题唯一值 M 或 S，从数据库中获取对应于标题的服务提供情况数据。即，这是参考图 8 所描述的服务提供情况数据，是其中设置了对应于光盘 ID 的各种服务提供情况的数据。

在步骤 S707 中，服务器 300 从服务提供情况数据中提取对应于从信息处理设备（用户设备）400 中接收到的光盘 ID 和服务标识符的数据，并检查是否可以提供服务。

下面将使用图 8 中所显示的服务提供情况数据作为示例来进行描述。例如，在从信息处理设备(用户设备)400 接收到的光盘 ID 是（光盘 ID 1），以及服务标识符是（服务 1）的情况下，判断服务是可以提供的，因为对于服务 1，上限被设置为一次，其服务提供情

况显示“未提供”。

当在步骤 S708 中根据服务提供情况数据判断可以提供服务，过程进入步骤 S709，而当在步骤 S708 中根据服务提供情况数据判断不可以提供服务，过程进入步骤 S711。

在步骤 S711 中，服务器 300 停止其服务提供过程。注意，对于此停止过程，可以向信息处理设备（用户设备）400 传输说明停止服务提供过程的消息。

如果根据服务提供情况数据判断可以提供服务，则服务器在步骤 S709 中更新数据库。

下面将再次使用图 8 中所显示的服务提供情况数据作为示例来进行描述。例如，在从信息处理设备（用户设备）400 接收到的光盘 ID 是（光盘 ID 1），以及服务标识符是（服务 1）的情况下，是“未提供”的服务提供情况被更改为“提供了一次”。

在步骤 S710 中，服务提供服务器 300 执行向传输了服务提供请求的信息处理设备（用户设备）400 服务提供过程。

例如，当存储在光盘中的内容是外语电影时，通过网络从服务提供服务器 300 向信息处理设备（用户设备）400 提供各种与内容相关的服务，包括小标题或其音频的配音数据，或内容的续集的购买光盘折扣票。

注意，优选情况下，信息处理设备（用户设备）400 和服务提供服务器 300 之间的通信是通过建立安全的通信通道来实现的，在该安全通信通道中，可以使用加密来进行相互的身份验证，并共享会话密钥。

此外，在上文所提及的示例中，每次接收到服务提供请求时，在步骤 S705、S706 中服务器 300 检查光盘 ID 撤销列表 (DIRL)。然而，可以这样配置，以便预先定期检查光盘 ID 撤销列表，以对于那里列出的任何光盘 ID，使数据库保持更新，以便停止提供涉及该光盘 ID 的服务。在这样的配置中，可以省略在接收到服务提供请求时检查光盘 ID 撤销列表 (DIRL) 的过程，以缩短提供服务的时间。

此外，在上文所提及的实施例中，所描述的光盘 ID 是彼此不同的。然而，光盘 ID 可以对诸如 10 个光盘、100 个光盘或 1,000 光盘组成的单位通用，可以在考虑到一组中的光盘数量的情况下确定为单个光盘 ID 设置的服务提供限制。

上文是参考特定的实施例对本发明进行详细描述的。然而，显然，在不偏离本发明的范围和精神的情况下，那些精通本技术的人可以对实施例作出各种修改和替换。即，是通过示例来说明本发明的，如此，不应该作出限制性的解释。为了判断本发明的范围和精神，应该考虑到在开始处阐述的权利要求。

注意，本说明书中所描述的一系列过程可以通过硬件、软件或其中组合了两者的配置来执行。在执行基于软件的进程的情况下，通过将其中记录了处理序列的程序安装在集成到专用硬件中的计算机内的存储器中，或通过将程序安装在可以执行各种进程的通用计算机中，来执行各种进程。

例如，程序可以预先记录在作为记录介质的硬盘或 ROM（只读存储器）上。或者，程序也可以临时或永久地存储（记录）在可移动记录介质上，如软磁盘、CD-ROM（压缩光盘只读存储器）、MO（磁光）光盘、DVD（数字通用光盘）、磁盘、半导体存储器。可以作为所谓的“程序包软件”提供这样的可移动记录介质。

注意，不仅可以从诸如上文所提及的可移动记录介质中将程序安装在计算机中，而且也可以从下载站点以无线方式传输到计算机，通过诸如局域网、因特网之类的网络以有线方式传输到计算机，以允许计算机接收如此传输的程序，以便安装在诸如那里的硬盘之类的存储介质中。

注意，说明书中所描述的各种过程不仅可以根据描述按时间顺序执行，而且也可以根据分配用于执行过程的设备的处理能力或根据需要并行地或分别地执行。此外，本说明书中所使用的系统表示多个设备逻辑设置配置，不仅限于其中具有其自己的配置的每一个设备都组合在同一个外壳内的情况。

[工业实用性]

如前所述，根据本发明的配置，在其中提供存储在包括 DVD、CD、蓝色激光记录介质之类的各种信息记录介质中的内容，并且从联网的服务提供服务器执行服务提供过程的配置中，服务提供服务器验证从信息处理设备（用户设备）传输给它的信息记录介质 ID，并根据每一个信息记录介质 ID 的服务提供情况数据来提供服务。因此，只有在传输了服务请求的信息处理设备是从信息记录介质中读取了有效信息记录介质 ID 的信息处理设备，并且根据服务提供情况数据验证了可以提供服务的情况下，才提供服务。如此，在一个从服务器提供对应于内容的服务信息（如，当存储在光盘上的内容是外语电影时，各种与内容关联的服务，包括小标题或配音数据）的系统中，本发明的配置允许在严格检查服务接收器并且检查他/她具有授予的权限之后提供对应于内容的各种服务信息。

此外，根据本发明的配置，存储在信息记录介质上的信息记录介质 ID 包括可以检查其有效性的数据，如管理设备的签名数据，还可以具有标题唯一值或者包括可以用来计算标题唯一值的数据。因此，服务提供服务器可以基于信息记录介质 ID 中包括的数据检查有效性，另外，还可以获取标题唯一值，从而，服务器可以指定服务提供情况数据集，以便对应于标题唯一值。因此，在严格检查服务接收器并且检查他/她具有授予的权限之后提供对应于内容的各种服务信息。

图1

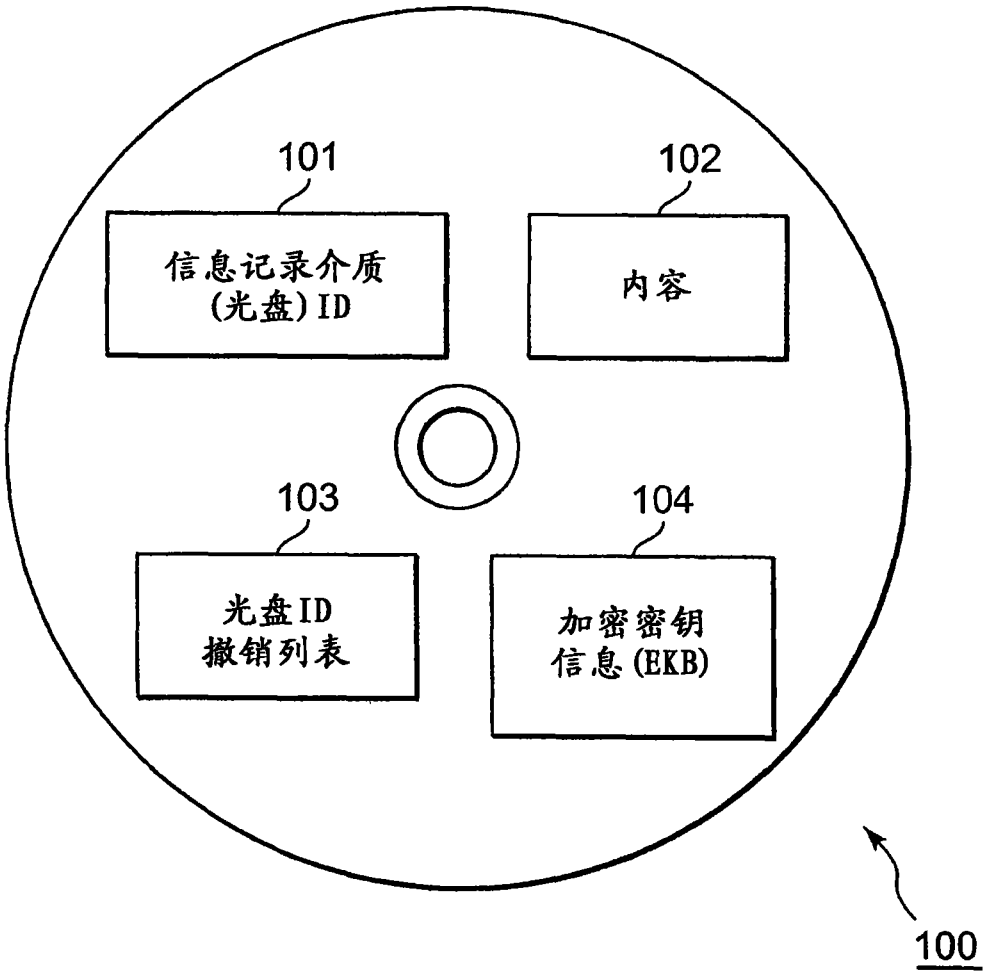


图2

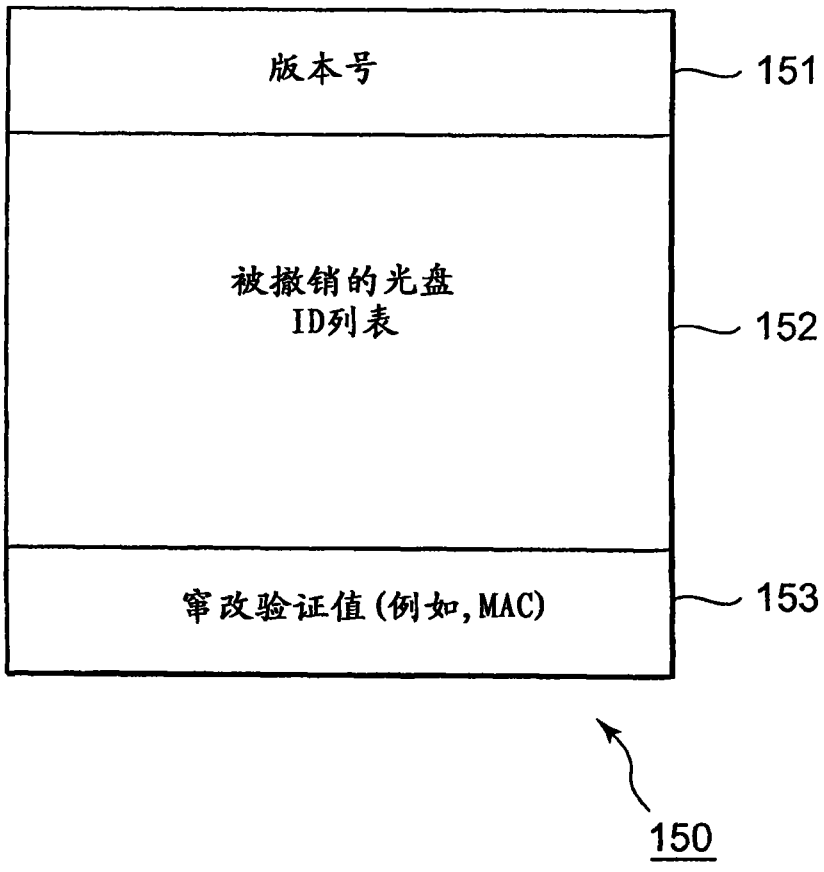


图3

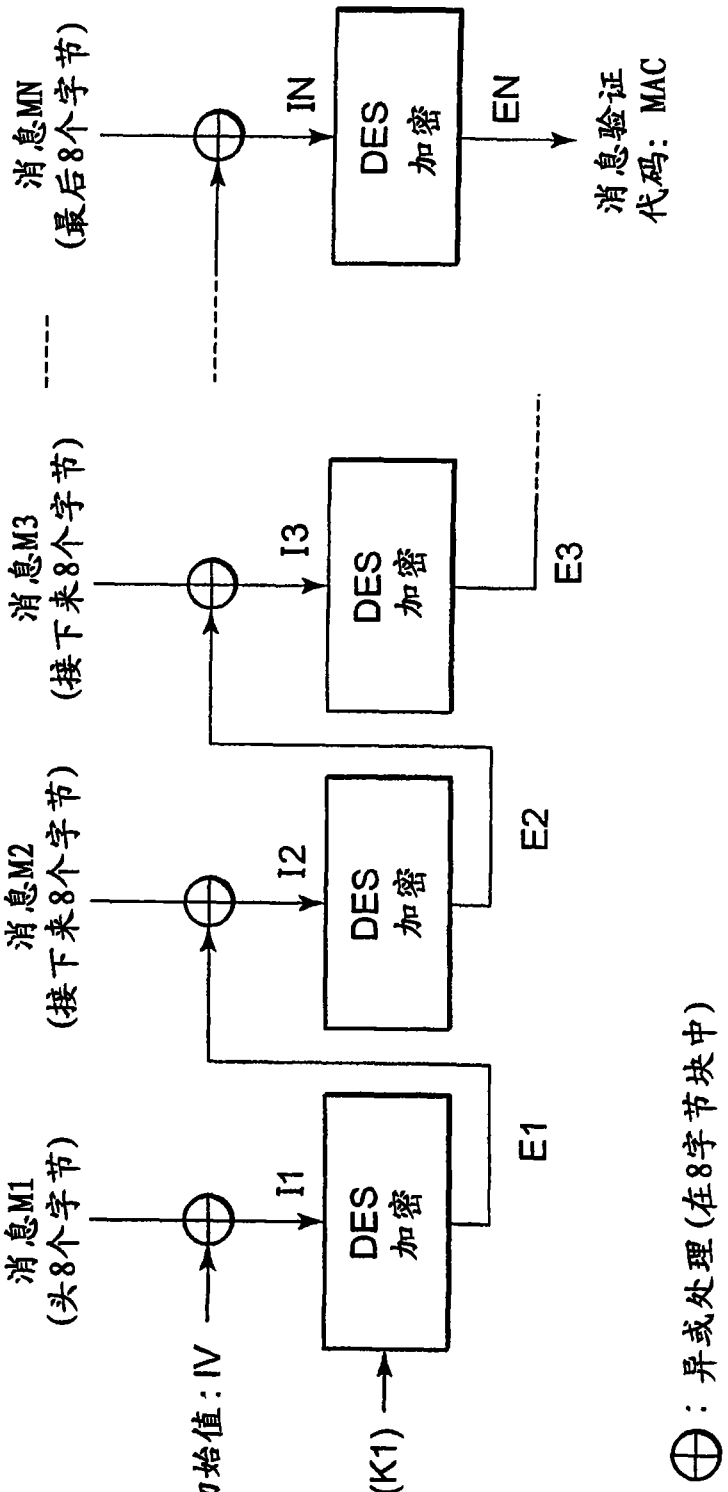

消息M1
(头8个字节)
消息M2
(接下来8个字节)
消息M3
(接下来8个字节)
消息MN
(最后8个字节)
初始值：IV
密钥(K1)
I1
I2
I3
IN
DES
加密
E1
E2
E3
EN
消息验证
代码：MAC
⊕：异或处理(在8字节块中)

图4

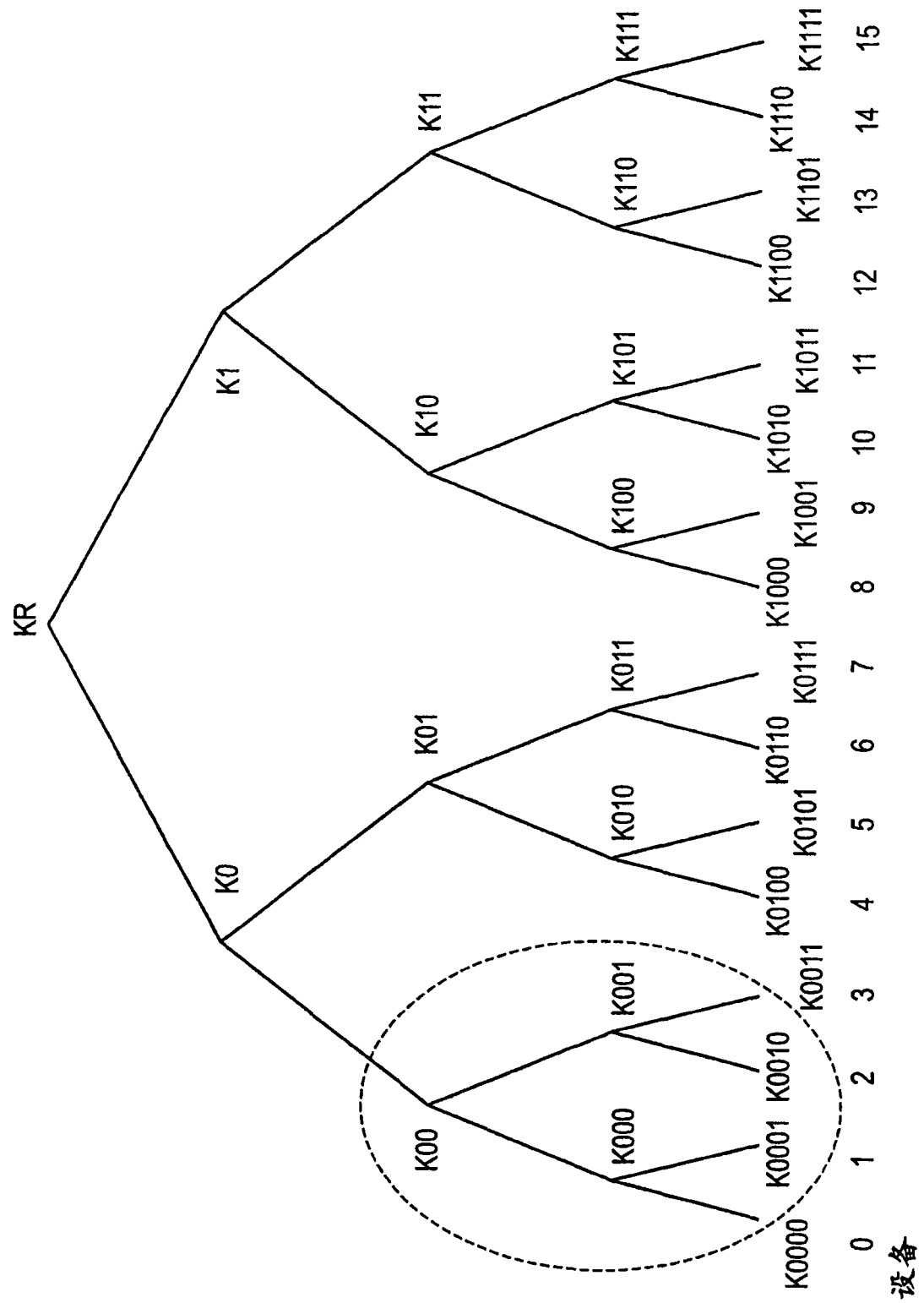

KR
K0
K1
K00
K01
K10
K11
K000
K001
K010
K011
K100
K101
K110
K111
K0000
K0001
K0010
K0011
K0100
K0101
K0110
K0111
K1000
K1001
K1010
K1011
K1100
K1101
K1110
K1111
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
设备

图5

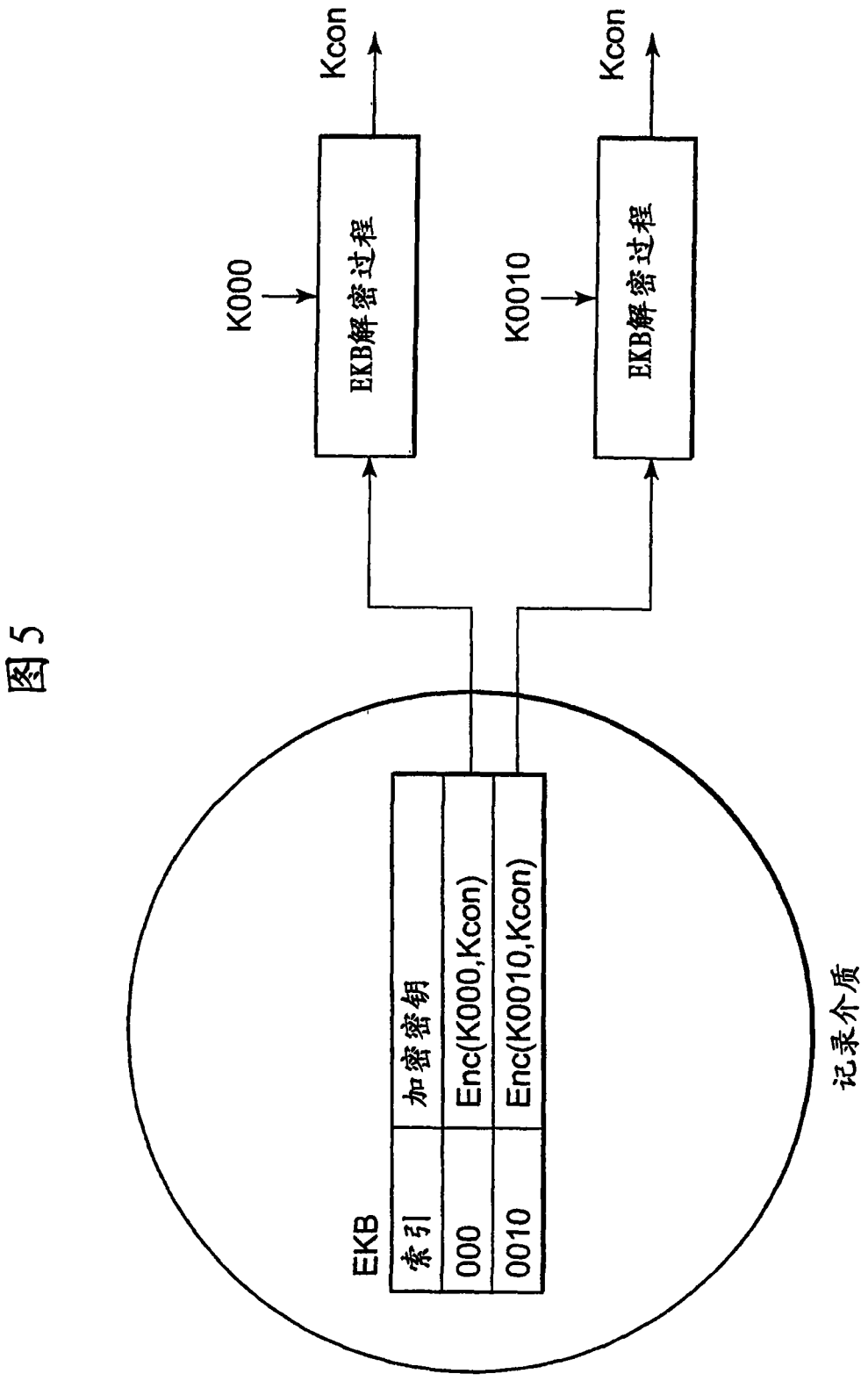

K000
EKB解密过程
Kcon
K0010
EKB解密过程
Kcon
EKB
索引
加密密钥
000
Enc(K000,Kcon)
0010
Enc(K0010,Kcon)
记录介质

图6

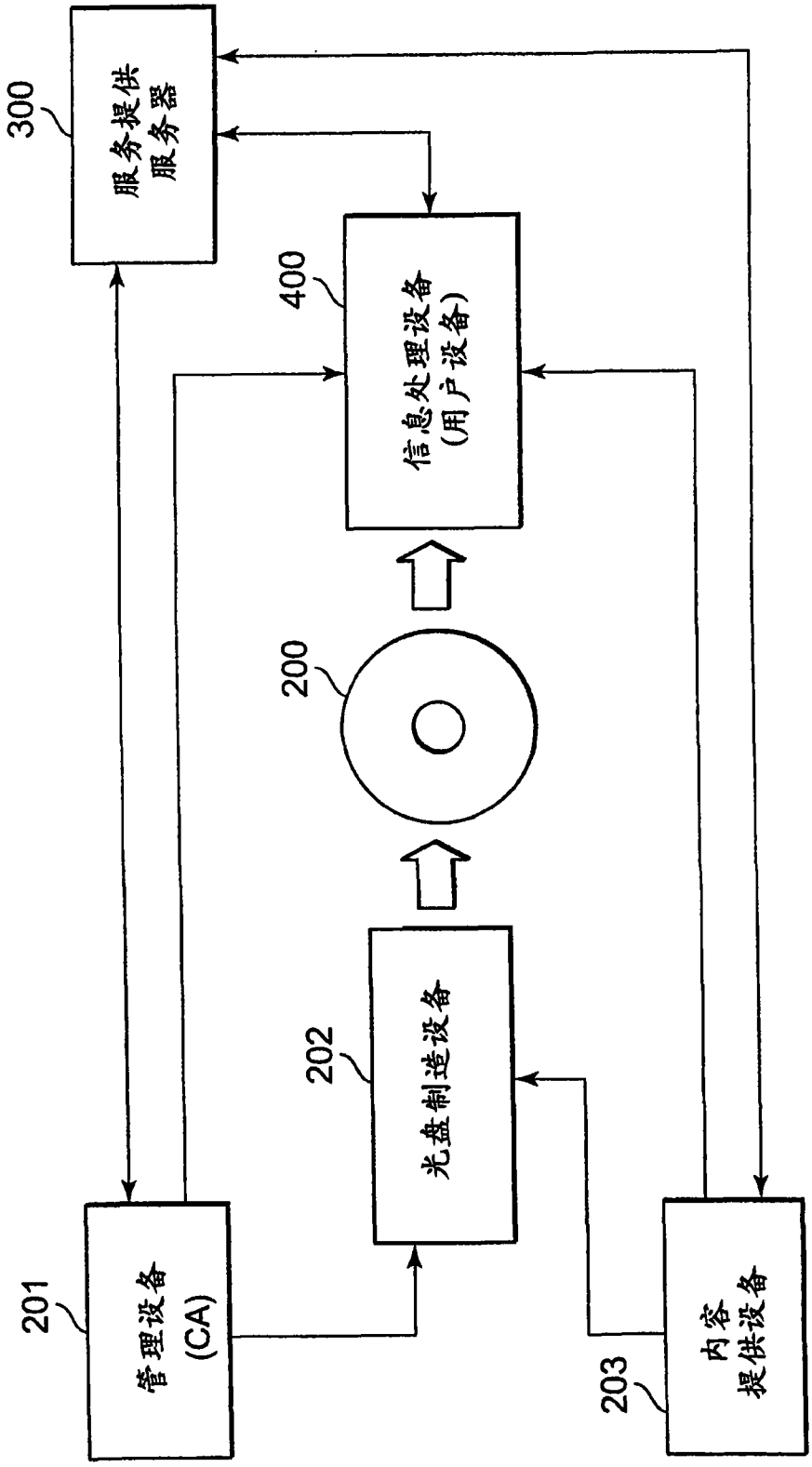

300
服务提供
服务器
400
信息处理设备
(用户设备)
200
202
光盘制造设备
201
管理设备
(CA)
203
内容
提供设备

图7

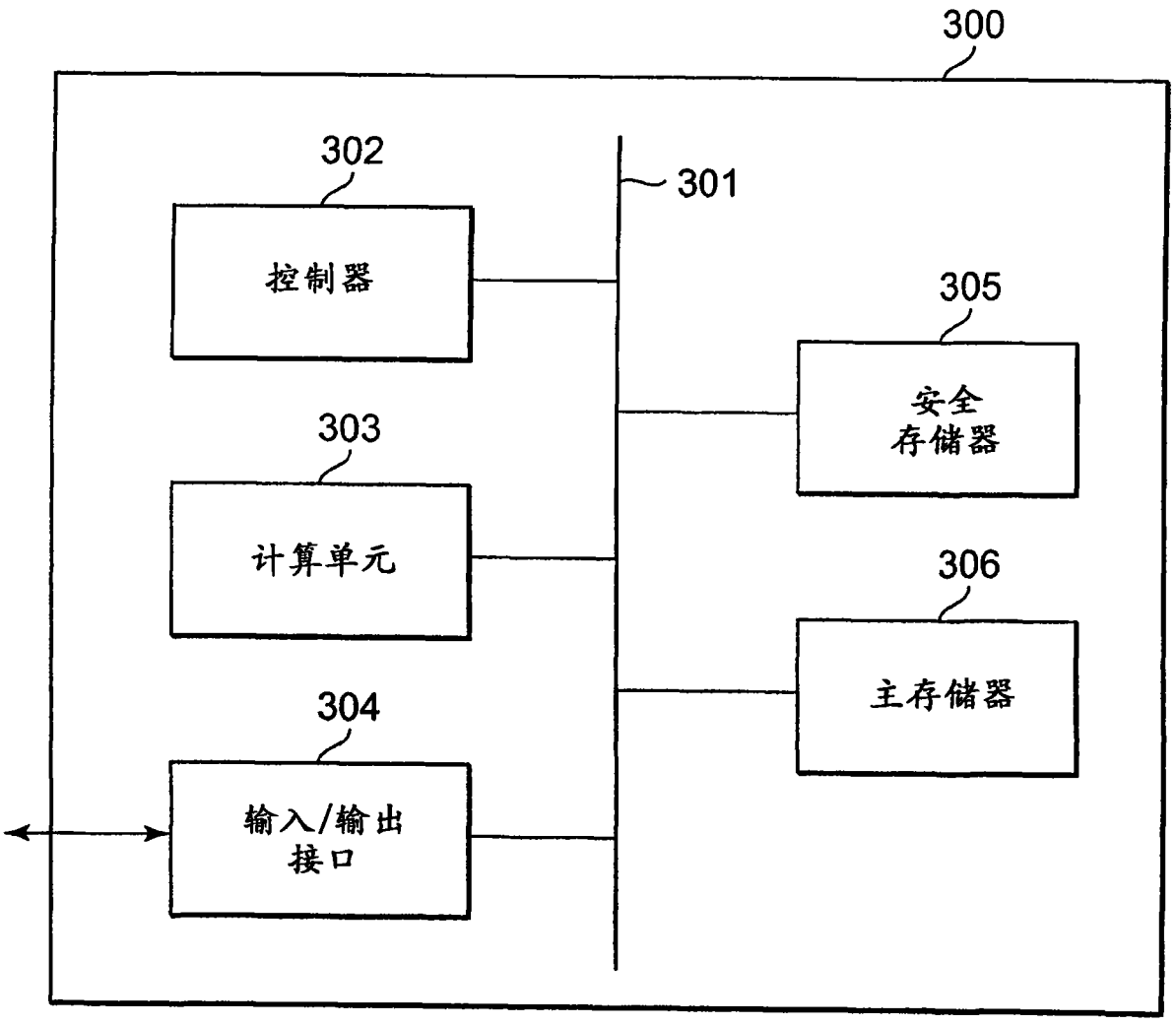


图8

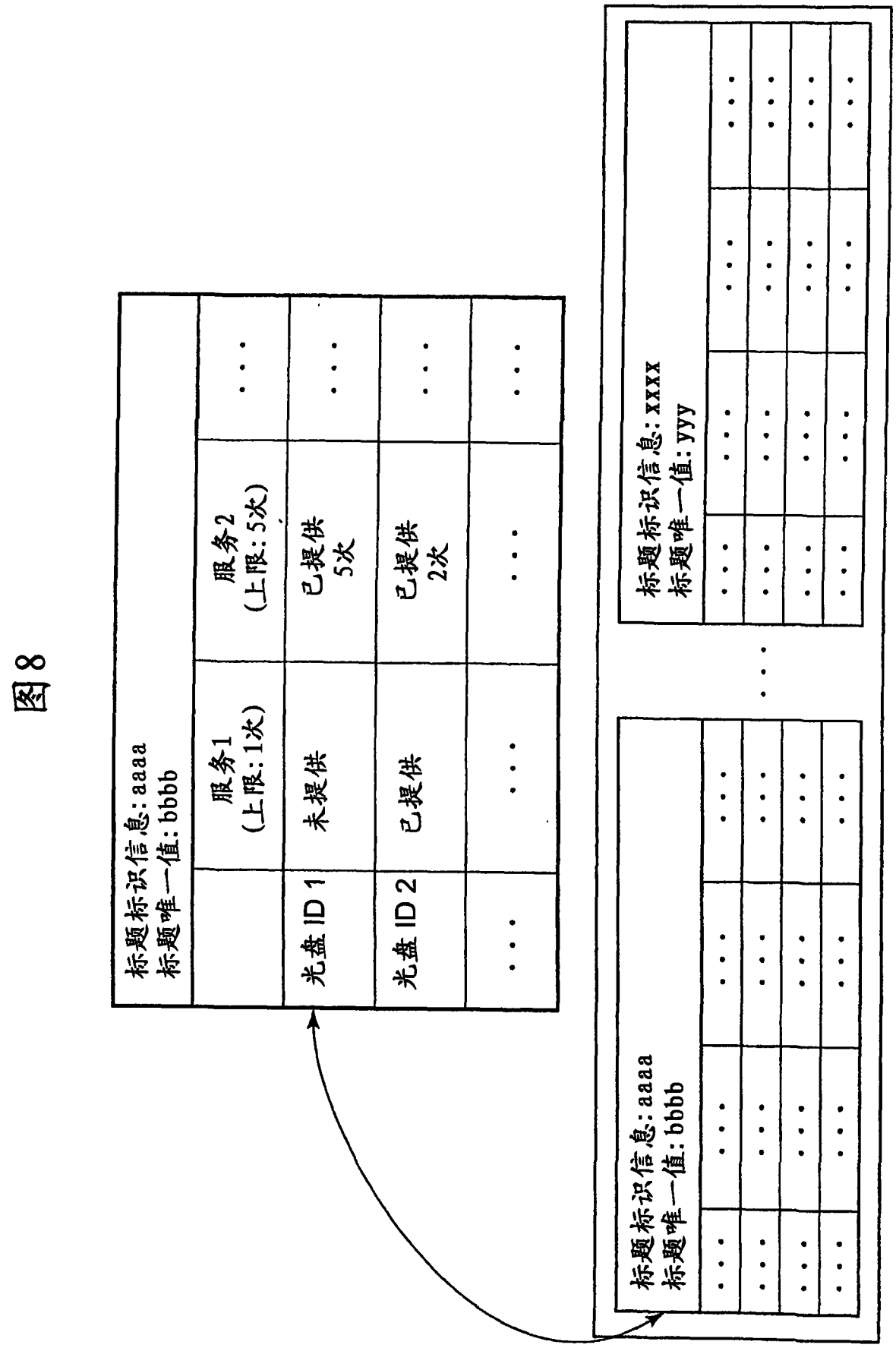

标题标识信息:aaaa
标题唯一值:bbbb
服务1
(上限:1次)
服务2
(上限:5次)
光盘ID 1
未提供
已提供
5次
光盘ID 2
已提供
已提供
2次
标题标识信息:aaaa
标题唯一值:bbbb
标题标识信息:xxxx
标题唯一值:yyy

图 9

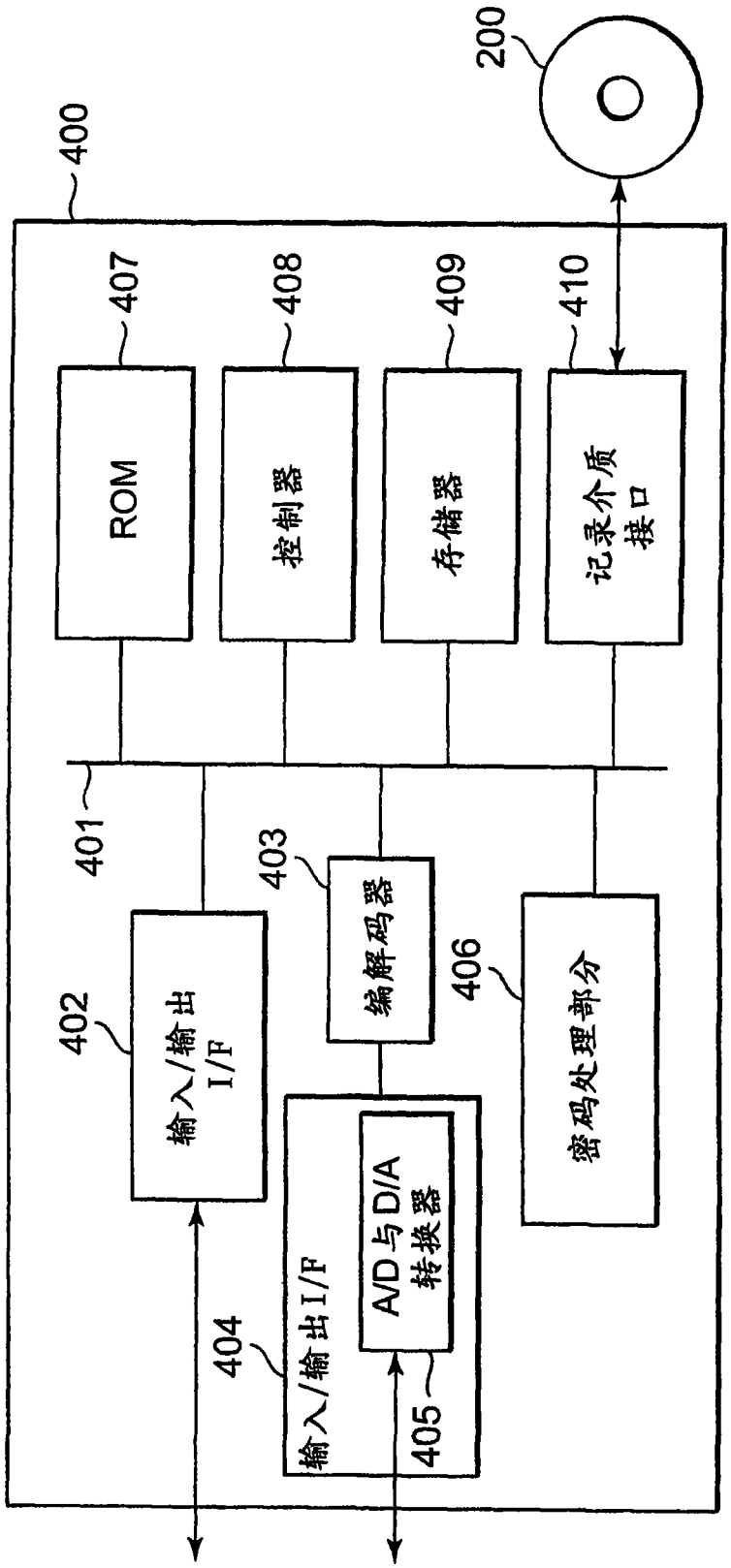

200
400
407
408
409
410
ROM
控制器
存储器
记录介质接口
401
403
402
输入/输出 I/F
编解码器
406
密码处理部分
404
输入/输出 I/F
A/D 与 D/A 转换器
405

图10

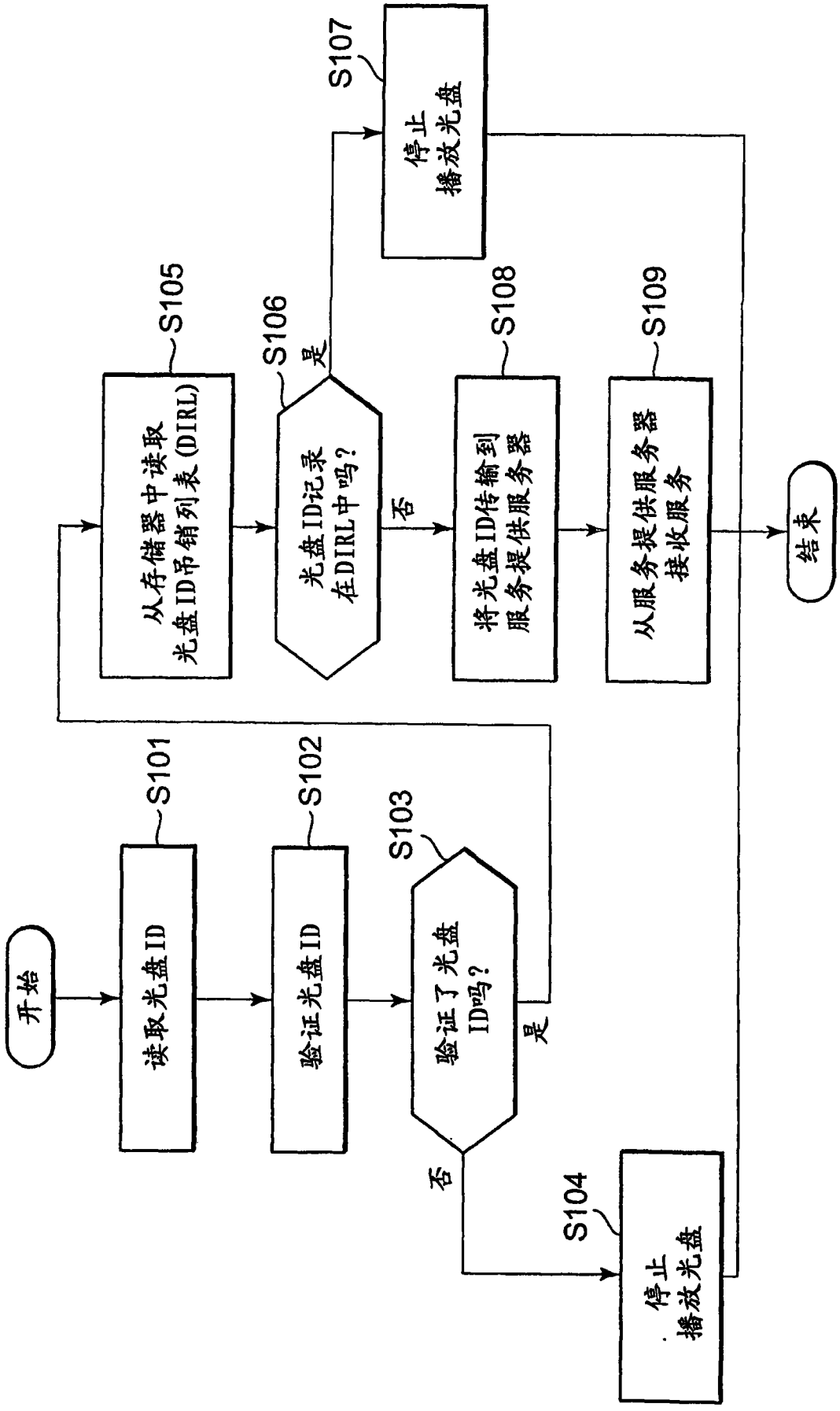

开始
读取光盘ID
S101
验证光盘ID
S102
验证了光盘ID吗?
S103
是
否
停止播放光盘
S104
从存储器中读取光盘ID吊销列表(DIRL)
S105
光盘ID记录在DIRL中吗?
S106
是
否
停止播放光盘
S107
将光盘ID传输到服务提供服务器
S108
从服务提供服务器接收服务
S109
结束

图11

	光盘ID	标题唯一值	光盘唯一值
光盘ID 设置示例 1	M, Sig(w)	M	Sig(w)
光盘ID 设置示例 2	S, Sig(w)	S	Sig(w)
光盘ID 设置示例 3	p(w), IDKey(w)	S	p(w) OR IDKey(w)
光盘ID 设置示例 4	e(w), I(w)	S	e(w) OR I(w)
光盘ID 设置示例 5	Σ w	S	e(w)
光盘ID 设置示例 6	p(w), IDKey(w)	S	p(w)

图12

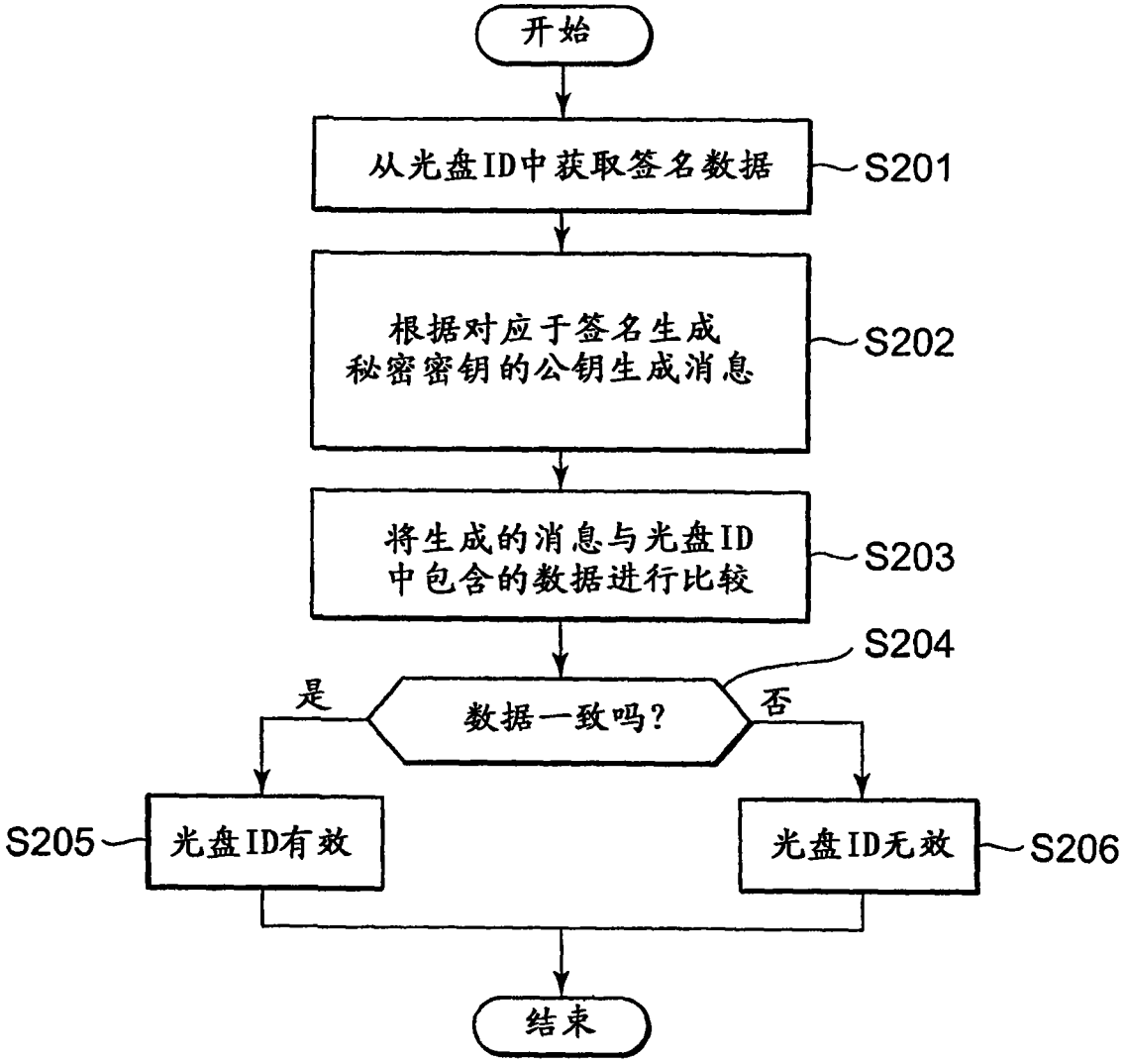

开始
从光盘ID中获取签名数据
S201
根据对应于签名生成
秘密密钥的公钥生成消息
S202
将生成的消息与光盘ID
中包含的数据进行比较
S203
S204
数据一致吗?
是
否
S205
光盘ID有效
光盘ID无效
S206
结束

图13

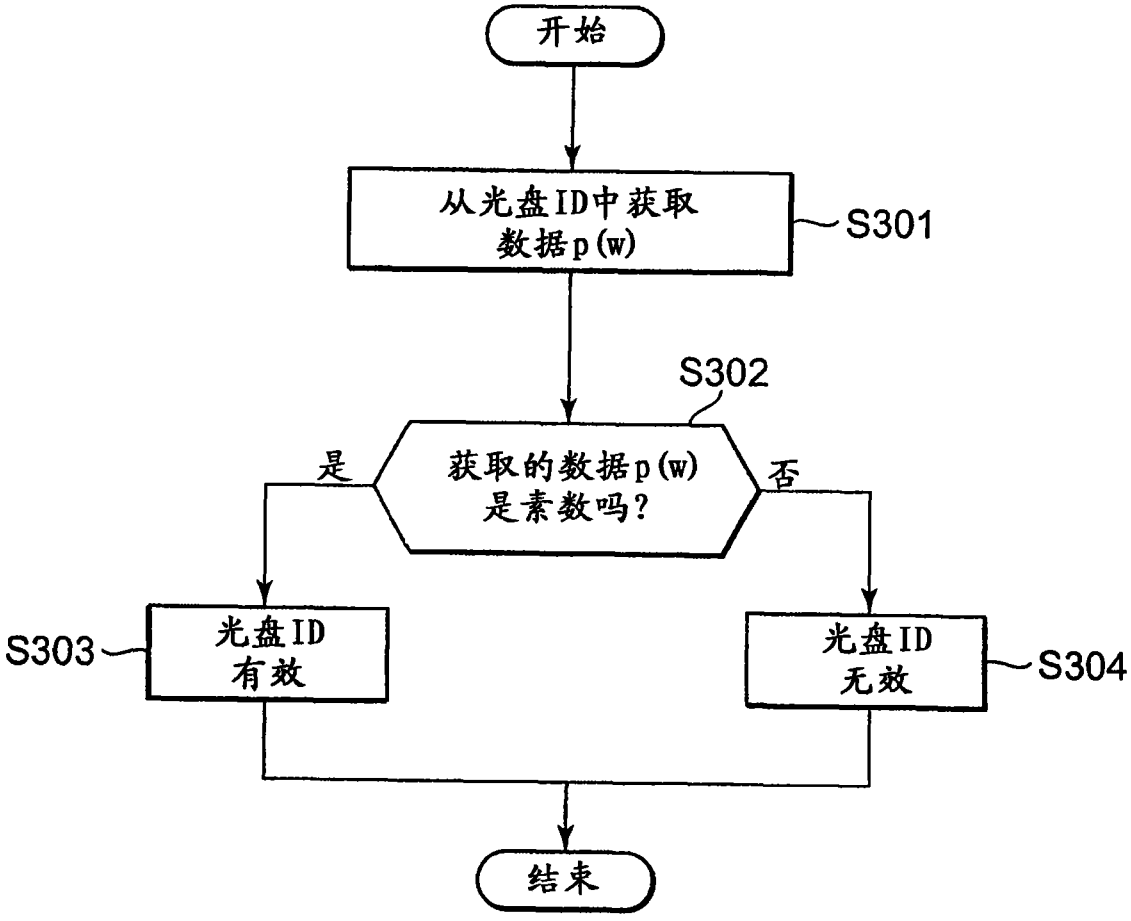

开始
从光盘ID中获取
数据p(w)
S301
S302
获取的数据p(w)
是素数吗?
是
否
S303
光盘ID
有效
光盘ID
无效
S304
结束

图14

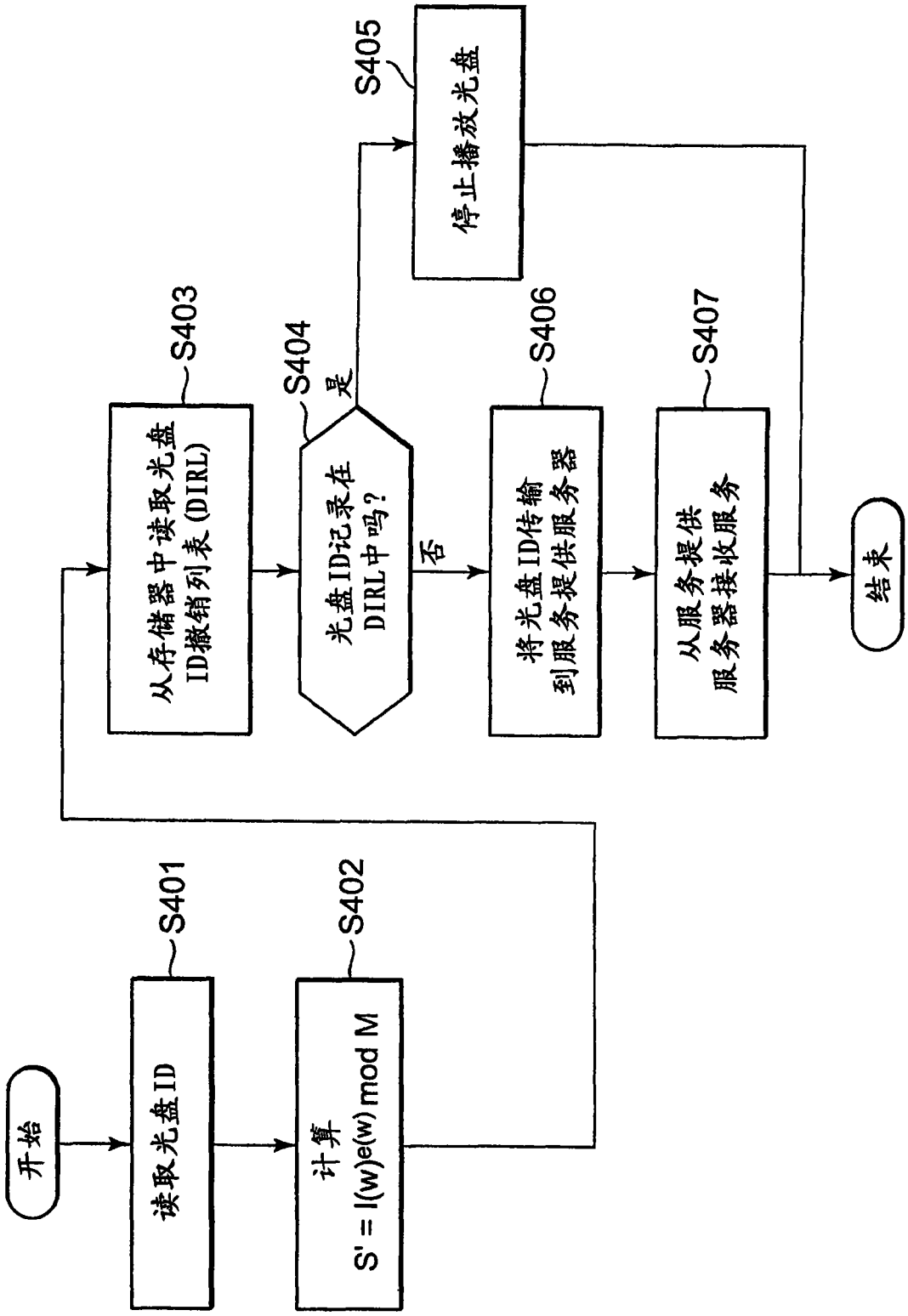

开始
读取光盘ID
S401
计算
S' = I(w)e(w) mod M
S402
从存储器中读取光盘
ID撤销列表(DIRL)
S403
光盘ID记录在
DIRL中吗?
S404
是
否
停止播放光盘
S405
将光盘ID传输
到服务提供服务器
S406
从服务提供
服务器接收服务
S407
结束

图15

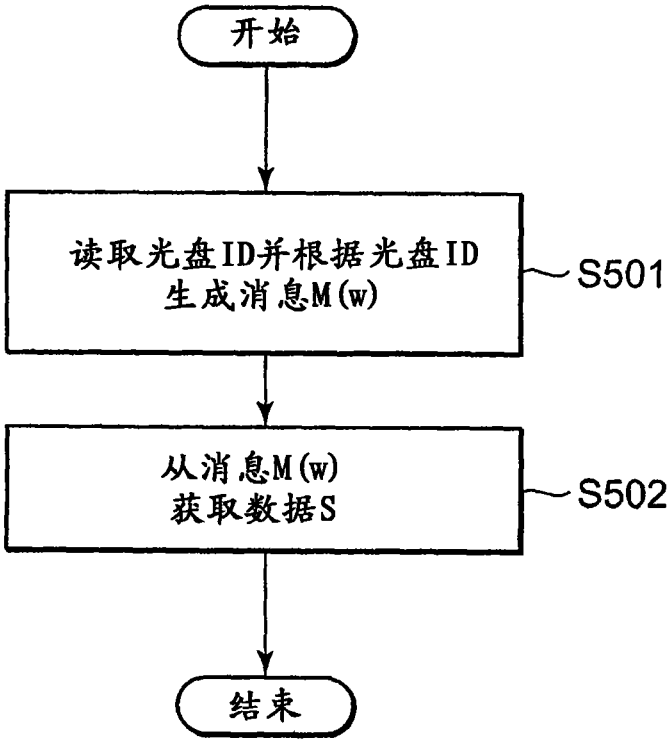


图16

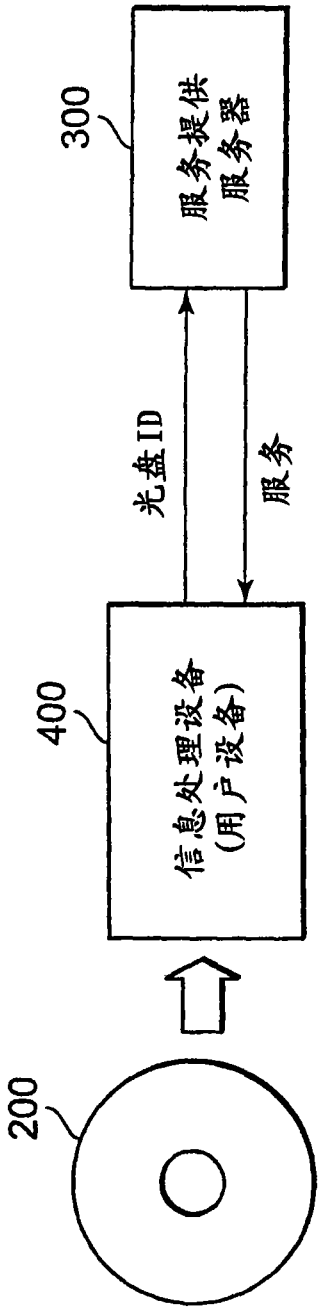
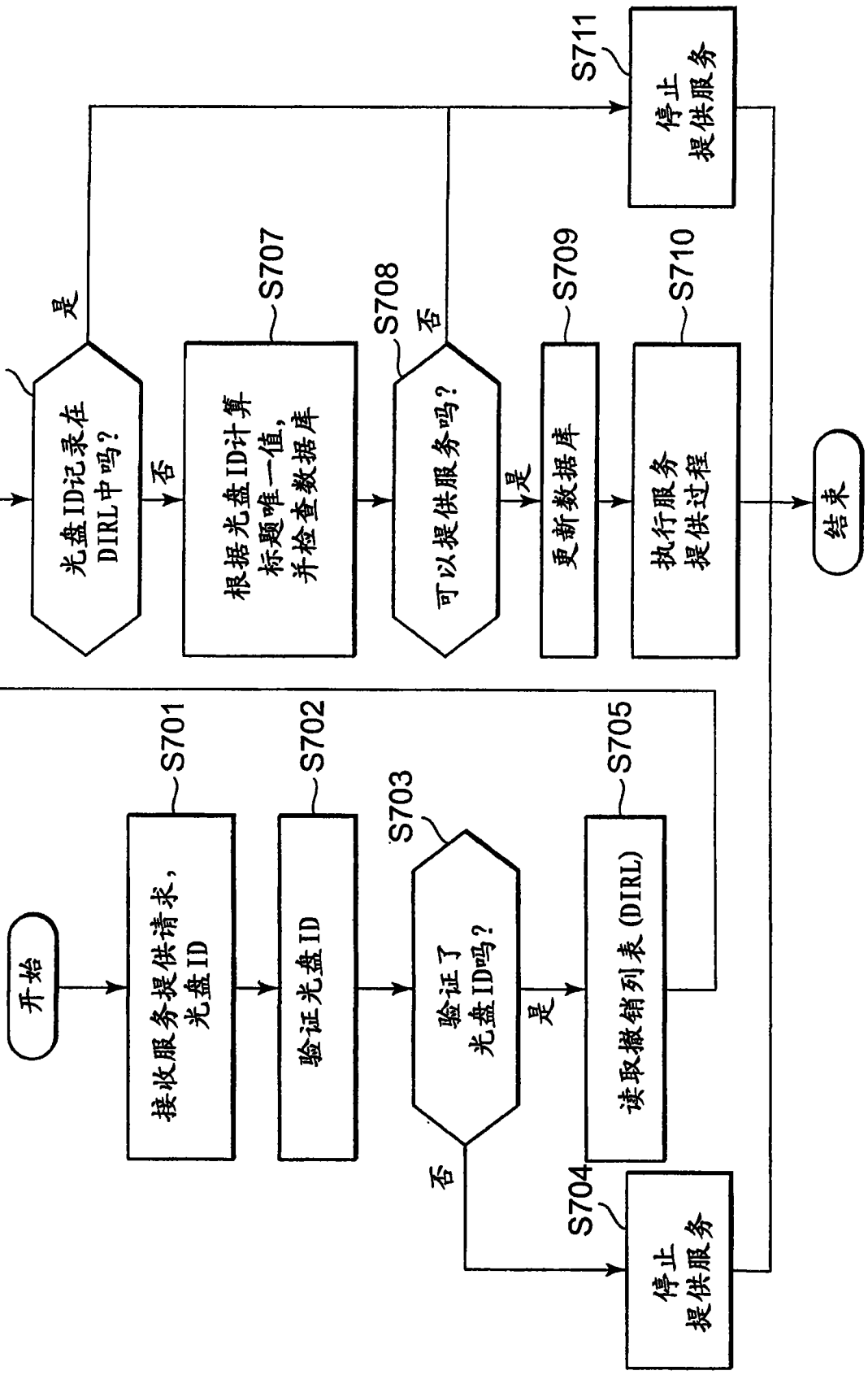


图17


开始
S701
接收服务提供请求，光盘ID
S702
验证光盘ID
S703
验证了光盘ID吗？
是
否
S704
停止提供服务
S705
读取撤销列表(DIRL)
S706
光盘ID记录在DIRL中吗？
是
否
S707
根据光盘ID计算标题唯一值，并检查数据库
S708
可以提供服务吗？
是
否
S709
更新数据库
S710
执行服务提供过程
S711
停止提供服务
结束