[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G11B 20/10 (2006.01)
G11B 20/12 (2006.01)

[12] 发明专利说明书

专利号 ZL 200410090519.X

[45] 授权公告日 2009 年 9 月 30 日

[11] 授权公告号 CN 100545932C

[22] 申请日 2004.7.30
[21] 申请号 200410090519.X
[30] 优先权
[32] 2003.7.30 [33] JP [31] 282336/03
[73] 专利权人 索尼株式会社
地址 日本东京都
[72] 发明人 浅野智之 村松克美 木谷聪
高岛芳和 米满润
[56] 参考文献
US6530025B1 2003.3.4
JP2001-44984A 2001.2.16
US6101422A 2000.8.8
审查员 董泽华

[74] 专利代理机构 北京市柳沈律师事务所
代理人 吕晓章 马 莹

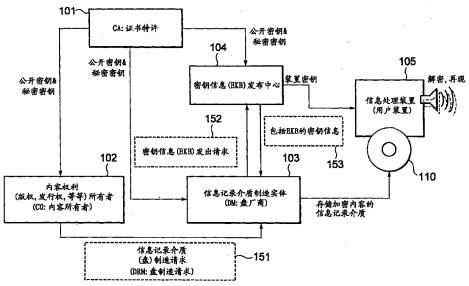
权利要求书 6 页 说明书 28 页 附图 13 页

[54] 发明名称

信息记录介质制造控制系统、信息处理装置与方法

[57] 摘要

一种用于防止未经授权制造和发行包含内容的信息记录介质的系统、装置和方法，其中信息记录介质制造实体发送根据由内容权利所有者所发出的信息记录介质制造请求所产生的密钥信息发出请求，验证所发出请求的可靠性，并且根据作为这种验证的结果所证实的合法性，发出用于把所述内容存储到信息记录介质中的密钥信息。至于通过非法手段获取的内容，不能获取所述密钥信息，因而避免了制造包含未经授权而获取内容的盘或介质。



1.一种信息记录介质制造控制系统，包括:

一具有一内容的版权或发行权的内容权利所有装置;

一信息记录介质制造装置，用于从所述内容权利所有装置接收信息记录介质制造请求数据，该信息记录介质制造请求数据用于执行存储加密内容的信息记录介质的制造处理；和

一密钥信息发出装置，用于响应来自所述信息记录介质制造装置的密钥信息发出请求数据向所述信息记录介质制造装置提供密钥信息块，用于获取解密所述加密内容的密钥信息；其中

所述密钥信息发出装置验证来自所述信息记录介质制造装置的密钥信息发出请求数据是否包括对应于来自所述内容权利所有装置的信息记录介质制造请求数据的已授权的请求数据，并在验证了所述已授权的请求数据的基础上，向所述信息记录介质制造装置提供所述密钥信息块;

所述信息记录介质制造请求数据和所述密钥信息发出请求数据都包括信息记录介质制造数量数据；和

所述信息记录介质制造装置制造存储加密内容的信息记录介质，其中所述加密内容是通过对从内容权利所有装置接收的内容和从所述密钥信息发出装置接收的密钥信息块执行加密而得到的。

2.根据权利要求 1 所述的信息记录介质制造控制系统，其中，所述密钥信息块存储只需要在存储在具有已被授予内容使用权的用户装置中的密钥的基础上利用解密处理即可获得的密钥信息，并可从所述密钥信息块中获得的所述密钥信息包括对存储在所述信息记录介质上的加密内容执行解密处理过程中需要的密钥信息。

3.根据权利要求 2 所述的信息记录介质制造控制系统，其中，所述密钥信息块包括使能密钥块，其只用解密处理来获取密钥信息，所述解密处理应用从设置为树结构中的叶的多个用户装置中选择的用户装置的存储密钥。

4.根据权利要求 1 所述的信息记录介质制造控制系统，其中，在包括在来自所述信息记录介质制造装置的密钥信息发出请求数据中的所述内容权利所有装置的签名验证处理的基础上，所述密钥信息发出装置对所述密钥信息发出请求数据是否包括对应于信息记录介质制造请求数据的已授权的请

求数据执行验证。

5.根据权利要求 1 所述的信息记录介质制造控制系统，其中，在所述内容权利所有装置、所述信息记录介质制造装置和密钥信息发出装置当中所执行的数据发送和接收中，执行相互授权处理，在满足所述授权的条件下执行数据通信，并对发送数据执行加密处理。

6.根据权利要求 1 所述信息记录介质制造控制系统，其中，在所述内容权利所有装置和所述信息记录介质制造装置之间的信息发送通过记录介质来执行。

7.根据权利要求 1 的所述信息记录介质制造控制系统，其中：

所述内容权利所有装置、所述信息记录介质制造装置和所述密钥信息发出装置具有一对应于由一证书特许机关发出的公开密钥证书的公开密钥和一秘密密钥；和

在所述内容权利所有装置、所述信息记录介质制造装置和所述密钥信息发出装置之间的通信是利用公开密钥加密方法通过相互授权来执行。

8.根据权利要求 1 所述的信息记录介质制造控制系统，其中，所述信息记录介质制造请求数据和所述密钥信息发出请求数据包括所述内容权利所有装置和所述信息记录介质制造装置的识别信息。

9.根据权利要求 1 所述的信息记录介质制造控制系统，其中：

所述密钥信息发出请求数据包括所述内容权利所有装置的公开密钥证书；和

所述密钥信息发出装置将一吊销状态验证为所述内容权利所有装置的所述公开密钥证书的无效状态，并在验证为没有吊销所述公开密钥证书的条件下，执行向所述信息记录介质制造装置提供所述密钥信息块的处理。

10.根据权利要求 1 的所述信息记录介质制造控制系统，其中，所述密钥信息发出请求数据包括将要存储在信息记录介质上的内容或对应于所述内容的散列值。

11.根据权利要求 1 所述的信息记录介质制造控制系统，其中，所述信息记录介质制造装置具有一被所述信息记录介质制造控制系统的控制装置许可的数据写入装置；并且在从所述控制实体接收到写入许可信息的条件下，利用所述数据写入装置在所述信息记录介质上执行数据写入处理。

12.一种信息处理装置，包括用于创建信息记录介质制造请求数据的装

置，该信息记录介质制造请求数据配备有与数据相关的数字签名，并且该信息记录介质制造请求数据包括:

内容;

用于每个内容权利所有装置和信息记录介质制造装置的识别数据；和

信息记录介质制造数量数据。

13.一种信息处理装置，包括一个创建装置，用于创建对应于从所述内容权利所有装置接收的信息记录介质制造请求数据的密钥信息发出请求数据，其中，所述密钥信息发出请求数据包括:

至少是内容或基于所述内容的一散列值;

用于所述内容权利所有装置和信息记录介质制造装置的每一个的识别数据;

信息记录介质制造数量数据；和

每个所述数据的所述内容权利所有装置的数字签名。

14.一种信息处理装置，用于响应来自所述信息记录介质制造装置的密钥信息发出请求数据向信息记录介质制造装置提供密钥信息块，用于获取用于解密存储在信息记录介质上的加密内容的密钥信息，所述装置包括:

验证装置，用于处理包括在所述密钥信息发出请求数据内的内容权利所有装置的签名；和

发送装置，用于在验证所述密钥信息发出请求数据是一个对应于由所述内容权利所有装置所发出的信息记录介质制造请求数据的已授权的密钥信息发出请求数据的条件下，在由所述验证装置验证的签名的基础上，将所述密钥信息块发送给所述信息记录介质制造装置。

15.一种信息记录介质制造控制方法，包括步骤:

从对内容拥有版权或发行权的内容权利所有装置向执行制造存储加密内容的信息记录介质的处理的信息记录介质制造装置发送信息记录介质制造请求数据;

从所述信息记录介质制造装置向一密钥信息发出装置发送密钥信息发出请求数据;

利用所述密钥信息发出装置验证所述密钥信息发出请求数据是否是对应于来自所述内容权利所有装置的信息记录介质制造请求数据的已授权的请求数据;

作为在所述验证步骤中的所述验证处理的结果，在验证所述密钥信息发出请求数据是对应于信息记录介质制造请求数据的已授权的请求数据的条件下，从所述密钥信息发出装置向所述信息记录介质制造装置提供密钥信息块，用于获取密钥信息，所述密钥信息被用于解密所述加密内容；和

通过加密从所述内容权利所有装置接收到的内容和从所述密钥信息发出装置收到的所述密钥信息块制造存储加密内容的信息记录介质，

其中，所述信息记录介质制造请求数据和所述密钥信息发出请求数据都包括信息记录介质制造数量数据。

16.根据权利要求 15 的所述信息记录介质制造控制方法，其中，所述密钥信息块存储只需在存储在具有已被授予内容使用权的用户装置中的密钥的基础上利用解密处理就可获得的密钥信息，并且从所述密钥信息块中可获得的所述密钥信息包括解密存储在所述信息记录介质上的加密内容过程中所需的密钥信息。

17.根据权利要求 16 所述的信息记录介质制造控制方法，其中，所述密钥信息块包括使能密钥块，其只用解密处理来取密钥信息，所述解密处理应用从设置为树结构中的叶的多个用户装置中选择的用户装置的存储密钥。

18.根据权利要求 15 所述的信息记录介质制造控制方法，其中，所述验证步骤包括如下步骤：在包括在来自所述信息记录介质制造装置的密钥信息发出请求数据内的所述内容权利所有装置的签名验证处理的基础上，验证所述密钥信息发出请求数据是否包括对应于信息记录介质制造请求数据的已授权的请求数据。

19.根据权利要求 15 所述的信息记录介质制造控制方法，其中，在满足相互授权处理的授权的条件下 ，在所述内容权利所有装置、所述信息记录介质制造装置和所述密钥信息发出装置当中执行作为数据通信处理的数据通信，并且还包括发送数据的加密处理。

20.根据权利要求 15 所述信息记录介质制造控制方法，其中，在所述内容权利所有装置和所述信息记录介质制造装置之间的信息发送通过记录介质来执行。

21.根据权利要求 15 的所述信息记录介质制造控制方法，其中：

所述内容权利所有装置、所述信息记录介质制造装置和所述密钥信息发出装置都具有一对应于由证书特许机关所发出的公开密钥证书的公开密钥

和一秘密密钥；和

在所述内容权利所有装置、所述信息记录介质制造装置和所述密钥信息发出装置之间的通信是利用一公开密钥加密方法通过相互授权执行的。

22.根据权利要求 15 所述的信息记录介质制造控制方法，其中，所述信息记录介质制造请求数据和所述密钥信息发出请求数据包括所述内容权利所有装置和所述信息记录介质制造装置的识别信息。

23.根据权利要求 15 所述的信息记录介质制造控制方法，其中：

所述密钥信息发出请求数据包括所述内容权利所有装置的公开密钥证书；和

所述密钥信息发出装置将一吊销状态验证为所述内容权利所有装置的所述公开密钥证书的无效状态，并在验证为没有吊销所述公开密钥证书的条件下，执行向所述信息记录介质制造装置提供所述密钥信息块的处理。

24.根据权利要求 15 的所述信息记录介质制造控制方法，其中，所述密钥信息发出请求数据包括将要存储在信息记录介质上的内容或对应于所述内容的散列值。

25.根据权利要求 15 所述的信息记录介质制造控制方法，其中，所述信息记录介质制造装置具有被所述信息记录介质制造控制系统的控制装置许可的数据写入装置；和

在从所述控制装置接收写入许可信息的条件下，所述信息记录介质制造步骤使用所述数据写入装置对所述信息记录介质执行数据写入处理。

26.一种信息处理方法，用于创建被提供有与数据相关的数字签名的信息记录介质制造请求数据，其中该信息记录介质制造请求数据包括：

内容；

用于每个内容权利所有装置和信息记录介质制造装置的识别数据；和

信息记录介质制造数量数据。

27.一种信息处理方法，用于创建对应于从内容权利所有装置接收的信息记录介质制造请求数据的密钥信息发出请求数据，其中，所述密钥信息发出请求数据包括：

至少一内容或基于该内容的一散列值；

用于所述内容权利所有装置和信息记录介质制造装置的每一个的识别数据；

信息记录介质制造数量数据；和

每个所述数据的所述内容权利所有装置的数字签名。

28.一种信息处理方法，用于响应来自所述信息记录介质制造装置的密钥信息发出请求数据向信息记录介质制造装置提供密钥信息块，用于获取用于解密存储在信息记录介质上的加密内容的密钥信息，所述方法包括：

处理包括在所述密钥信息发出请求数据内的内容权利所有装置的签名；和

在验证所述密钥信息发出请求数据是一个对应于由所述内容权利所有装置发出的信息记录介质制造请求数据的已授权密钥信息发出请求数据的条件下，在由验证装置的签名的验证的基础上，将所述密钥信息块发送给所述信息记录介质制造装置。

信息记录介质制造控制系统、信息处理装置与方法

技术领域

本发明涉及一种信息记录介质制造控制系统、一种信息处理装置和方法和一种计算机程序。具体地说，本发明涉及一种信息记录介质制造控制系统，该系统能够避免其上记录有内容的信息记录介质的未经授权的拷贝的制作和发布和未经授权复制内容的使用,本发明还涉及一种信息处理装置和方法和一种计算机程序。

背景技术

诸如音乐的音频数据、诸如电影的图像数据、游戏程序和各种应用程序的各种软件数据(这些在下面称之为内容)可以作为数字数据被存在诸如DVD（数字化视频盘）、MD (小型盘)和 CD (密致盘)的记录介质中。另外，近年来，例如已经研制出能通过使用蓝色激光来高密度记录的盘,并且数字内容被存储在这些各种信息记录介质(记录介质)中和提供给用户。用户在再现装置中执行再现和使用该内容，例如在自己的 PC（个人计算机）和盘播放器中。

对于诸如音乐数据和图像数据的多种内容来说，它们的创作者或销售者通常拥有发行权等。因此，在这些内容的发行中，通常使用一种带有某种使用限制的配置。换句话说,只允许正规用户使用该内容以防止未经授权的复制等。

根据数字数据的记录/再现处理，可以重复执行记录和再现而不降低图像和音频的质量，于是出现了所谓盗版盘的发行问题，其中内容被复制在诸如CD -R 的可记录数据的介质上。

尤其是，诸如 DVD 的相对大容量记录介质或使用能够更大容量记录的蓝色激光记录方法的记录介质可以在单个介质上记录例如一个或多个电影的数据。由于可以用这样的方式很容易地把内容记录成数字信息，所以未经授权的复制的流通问题时常发生，从而使得避免版权所有者和发行权所有者的利益受到损害的问题变得重要。根据这样的当前形势，如何防止未经授权

的复制以保护版权所有者和发行权所有者的利益成了一个重要议题。

当制造用于存储内容的诸如CD、DVD或蓝色激光记录介质的信息记录时，内容所有者拥有该内容的权利。换句话说，该内容的所述版权或发行权向盘(信息记录介质)制造厂提供所述内容,和所述盘工厂在盘上记录从所述内容所有者收到的所述内容并经过诸如商店的经销商提供给用户。

拥有所述内容权利的内容所有者和所述盘制造者通常作为独立的实体而存在。对内容所有者或所述盘制造者中的一个执行内容控制是不够的，必须对这两个实体都执行适当的控制。

然而,现在很难说在用于存储内容的信息记录介质的制造过程中实现了一种用于全面、高效地执行内容控制和密钥信息控制的合理配置，并且具有未经授权复制内容的记录介质很可能在市场上流通。

特别是，在诸如使用诸如DVD的记录介质的电影的内容传送业务中出现了下述情形，即盗版制造者大量地制造盗版盘并且把它们经销到市场上，从而导致本应给予内容所有者的利益被不适当地减少的问题。当发生这种情形中的一个情节时,诸如未经授权复制内容的所偷盗的内容就被运送的盘工厂并被用于制造盗版盘。

很难在由从内容所有者接收一请求的内容编辑者发行到市场中或由盘制造者自身制造偷盗内容的作为偷盗行为结果的介质和正规产品之间进行鉴定，并且，未经授权介质向市场的发行正在引起更加严重的状态。

具体地说，发生了盘制造者自己大量地制造未经授权复制内容的情况。考虑到当前这种形势，甚至不能完全信任被提供有由内容所有者提供的内容并制造存有该内容的盘的盘制造者，必须形成一种对这种盘制造实体执行控制的系统以抑制制造这种存储未经授权内容的记录介质。

发明内容

本发明从上述问题的角度出发进行了考虑，和本发明的目的是提供一种能够在诸如DVD、CD和兰色激光记录介质的各种信息记录介质上存储和提供内容的一配置中抑制存储未经授权内容的信息记录介质的制造并避免存储未经授权内容的记录介质的制造、发行和使用的信息记录介质制造控制系统；一种信息处理装置和方法；和一种计算机程序。

本发明被配置如下：当诸如盘工厂的信息记录介质制造者制造一存加密

内容的信息记录介质时，其从密钥信息(EKB)发出中心接收用于获得解密存储在所述信息记录介质上的加密内容的密钥的密钥信息(EKB: 使能密钥块)，作为所述信息记录介质制造者得到来自所述密钥信息(EKB)发出中心的密钥信息(EKB)的条件，所述信息记录介质制造者表明其从内容权利所有装置收到了授权信息记录介质制造请求数据。 提供了所述信息记录介质制造控制系统、信息处理装置和方法和计算机程序，其中即使所述信息记录介质制造者诸如盘工厂没有从所述内容权利所有装置收到盘制造请求数据而获取了非法获得的内容，也不能从所述密钥信息(EKB)发出中心接收所述密钥信息(EKB)，并且可以避免用于非法获得的内容的盘制造。

本发明的第一方面包括一信息记录介质制造控制系统，该系统具有：一具有一内容的版权或发行权的内容权利所有装置；一信息记录介质制造者，用于从所述内容权利所有装置接收信息记录介质制造请求数据，以便执行存储加密内容的信息记录介质的制造处理；和一密钥信息发出装置，用于响应来自所述信息记录介质制造者的密钥信息发出请求数据向所述信息记录介质制造者提供能够获取解密所述加密内容的密钥信息的密钥信息块；其中所述密钥信息发出装置验证来自所述信息记录介质制造者的密钥信息发出请求数据是否包括对应于来自所述内容权利所有装置的信息记录介质制造请求数据的已授权的请求数据，并在验证了所述已授权的请求数据的基础上，向所述信息记录介质制造者提供所述密钥信息块；所述信息记录介质制造请求数据和所述密钥信息发出请求数据都包括信息记录介质制造数量数据；和 所述信息记录介质制造者包括一种配置，该配置能够制造存储加密内容的信息记录介质，其中所述加密内容是通过对从内容权利所有装置接收的内容和从所述密钥信息发出装置接收的密钥信息块执行加密而得到的。

此外，所述密钥信息块可以存储只需要在存储在具有已被授予内容使用权的用户装置中的密钥的基础上利用解密处理即可获得的密钥信息，并可从所述密钥信息块中获得的所述密钥信息包括对存储在所述信息记录介质上的加密内容执行解密处理过程中需要的密钥信息。

所述密钥信息块最好包括一 EKB (使能密钥块)，所述 EKB 能够只用解密处理来获取密钥信息，所述解密处理应用从设置为树结构中的叶的多个用户装置中选出的用户装置的存储密钥。

另外，密钥信息发出装置最好在包括在来自信息记录介质制造者的密钥

信息发出请求数据内的所述内容权利所有装置的签名验证处理的基础上执行一验证处理，以验证所述密钥信息发出请求数据是否包括对应于信息记录介质制造请求数据的已授权的请求数据。

同样，根据本发明优选实施例的所述信息记录介质制造控制系统最好还包括一种结构，在该结构中，在所述内容权利所有装置、所述信息记录介质制造者和密钥信息发出装置当中所执行的数据发送和接收中，执行相互授权处理，在满足所述授权的条件下执行数据通信，并对发送数据执行加密处理。

同样地，根据本发明一个优选实施例的所述信息记录介质制造控制系统最好进一步包括一种结构，在该结构中，在所述内容权利所有装置和所述信息记录介质制造者之间的信息发送通过记录介质来执行。

此外，所述内容权利所有装置、所述信息记录介质制造者和所述密钥信息发出装置拥有一对应于由证书特许机关发出的公开密钥证书的公开密钥和一秘密密钥；在所述实体之间的通信利用一公开密钥加密方法通过相互授权来执行。

同样地，根据本发明一个优选实施例的所述信息记录介质制造控制系统最好还具有所述信息记录介质制造请求数据和包括内容权利所有装置和信息记录介质制造者的识别信息的密钥信息发出请求数据。

最好，根据本发明一个优选实施例的信息记录介质制造控制系统还包括具有所述内容权利所有装置的公开密钥证书的密钥信息发出请求数据； 并且所述密钥信息发出装置验证作为所述内容权利所有装置的公开密钥证书的无效状态的吊销状态，并且，在验证其没有被吊销的条件下，执行向所述信息记录介质制造者提供所述密钥信息的处理。

同样地，根据本发明一个优选实施例的信息记录介质制造控制系统，所述密钥信息发出请求数据最好包括将要存储在信息记录介质的内容或一个对应于所述内容的散列值。

另外，信息记录介质制造者最好执行信息记录介质制造处理，其应用一信息记录介质制造装置执行制造数量记录处理。

此外，信息记录介质制造者拥有由所述信息记录介质制造控制系统的控制实体许可的数据写入机制；并且在从所述控制实体接收到写入许可信息的条件下，利用所述数据写入机制在所述信息记录介质上执行写入处理。

本发明另一优选实施例提供一种信息处理装置，用于执行创建被提供有

与包括内容、用于每个内容权利所有装置和信息记录介质制造者的识别数据和信息记录介质制造数量数据的数据相关的数字签名的信息记录介质制造请求数据的处理。

本发明的又一个优选实施例提供了一种信息处理装置，其包括一个用于创建对应于从内容权利所有装置接收的信息记录介质制造请求数据的密钥信息发出请求数据的创建机制，其中，所述密钥信息发出请求数据包括：至少一内容或基于所述内容的一散列值；用于所述内容权利所有装置和所述信息记录介质制造者中每一个的识别数据；信息记录介质制造数量数据；和每个所述数据的所述内容权利所有装置的数字签名。

本发明又一个优选实施例提供一种信息处理装置，用于响应来自所述信息记录介质制造者的密钥信息发出请求数据向信息记录介质制造者提供能够获取用于解密存储在信息记录介质上加密内容的密钥信息的密钥信息块的信息处理装置，所述装置包括：一验证机制，其处理包括在所述密钥信息发出请求数据内的内容权利所有装置的签名；和一发送机制，在验证密钥信息发出请求数据是对应于由所述内容权利所有装置发出的信息记录制造请求数据的已授权的密钥信息的条件下，在由所述验证机制验证的基础上，将所述密钥信息块发送给信息记录介质制造者。

另外，根据本发明又一个优选实施例提供了一种信息记录介质方法，其包括步骤：从对内容具有版权和发行权的内容权利所有装置向执行制造存储加密内容的信息记录介质的信息记录介质制造者发送一信息记录介质制造请求数据；从所述信息记录介质制造者向密钥信息发出装置发送一密钥信息发出请求数据；利用所述密钥信息发出装置验证所述密钥信息发出请求数据是否是已授权的、对应于来自所述内容权利所有装置的信息记录介质制造请求数据的请求数据；作为在所述验证步骤中的验证处理的结果，在验证所述密钥信息发出请求数据是对应于所述信息记录介质制造请求数据的已授权的请求数据的条件下，提供能够获取密钥信息的密钥信息块，所述密钥信息应用于从所述密钥信息发出装置到所述信息记录介质制造者的加密内容的解密；并制造一种存储加密内容的信息记录介质，所述加密内容利用从所述内容权利所有装置接收的内容和从所述密钥信息发出装置接收的密钥信息块执行加密，其中所述信息记录介质制造请求数据和所述密钥信息发出请求数据都包括信息记录介质制造数量数据。

在这种信息记录介质制造控制方法中，所述密钥信息块最好包括存储只需在存储在具有授予内容使用权的用户装置中的密钥的基础上通过解密处理就可获得的密钥信息，并且可从所述密钥信息块中获得的所述密钥信息包括在对存于所述信息记录介质上的加密内容执行解密处理中所需要的密钥信息。

此外，所述密钥信息块最好包括一 EKB (使能密钥块)，所述 EKB 能够只用解密处理来获取密钥信息，所述解密处理应用从设置为树结构的叶的多个用户装置中选择的用户装置的所存储的密钥。

同样地，所述验证步骤最好包括下述步骤，即根据包括在来自所述信息记录介质制造者的密钥信息发出请求数据内的内容权利所有装置的签名验证处理，验证所述密钥信息发出请求数据是否包括对应于一信息记录介质制造请求数据的已授权的请求数据。

此外，在满足了相互授权处理的授权的条件下，在所述内容权利所有装置、信息记录介质制造者和密钥信息发出装置当中执行作为数据通信处理的数据通信，并且还包括发送数据的加密处理。

另外，最好在内容权利所有装置和信息记录介质制造者之间执行作为经由一记录介质的处理的信息发送处理。

此外，所述内容权利所有装置、所述信息记录介质制造者和所述密钥信息发出装置都可以具有一对应于由证书特许机关所发出的公开密钥证书的公开密钥及一秘密密钥；在所述实体之间的通信利用一公开密钥加密方法通过相互授权来执行。

此外，信息记录介质制造请求数据和密钥信息发出请求数据可以包括内容权利所有装置和信息记录介质制造者的识别信息。

另外，密钥信息发出请求数据可以包括内容权利所有装置的公开密钥证书；并且密钥信息发出装置验证作为所述内容权利所有装置的公开密钥证书的无效状态的吊销状态，并且，在验证其没有被吊销的条件下，执行向信息记录介质制造者提供所述密钥信息的处理。

此外，密钥信息发出请求数据包括将要存储在信息记录介质上的内容或对应于所述内容的散列值。

再有，所述信息记录介质制造步骤执行信息记录介质制造处理，该处理应用一信息记录介质制造装置执行所制造数量的记录处理。

另外，所述信息记录介质制造者具有被所述信息记录介质制造控制系统的控制实体许可的一数据写入机制；和在从所述控制实体接收到写入许可信息的条加下，所述信息记录介质制造步骤使用所述数据写入机制在所述信息记录介质上执行数据写入处理。

另外，根据本发明又一个优选实施例，提供了一种信息处理方法，用于执行创建被提供有与包括内容的数据相关的数字签名的信息记录介质制造请求数据、用于每个内容权利所有装置和信息记录介质制造者的识别数据和信息记录制造数量数据的处理。

根据本发明的又一个优选实施例，提供了一种信息处理方法，用于创建对应于从内容权利所有装置接收的信息记录介质制造请求数据的密钥信息发出请求数据，其中，所述密钥信息发出请求数据包括： 至少一内容或基于所述内容的一个散列值；用于每个所述内容权利所有装置的识别数据和一信息记录介质制造者；信息记录介质制造数量数据和每个所述数据的所述内容权利所有装置的数字签名。

根据本发明又一个优选实施例，提供了一种信息处理方法，用于响应来自所述信息记录介质制造者的密钥信息发出请求数据向信息记录介质制造者提供能够获取用于解密存储在信息记录介质上的加密内容的密钥信息的密钥信息块，所述方法包括： 处理包括在所述密钥信息发出请求数据内的内容权利所有装置的签名；和在验证密钥信息发出请求数据是对应于由内容权利所有装置所发出的信息记录介质制造请求数据的已授权的密钥信息的条件下，在由所述验证机制验证签名的基础上，将所述密钥信息块发送给所述信息记录介质制造者。

根据本发明的又一优选实施例，提供一计算机可读程序，用于使一计算机执行创建被提供有与包括内容的数据相关的数字签名的信息记录介质制造请求数据、用于每个内容权利所有装置和信息记录介质制造者的识别数据和信息记录制造数量数据的处理。

另外，本发明的又一个优选实施例提供了计算机可读程序，用于使计算机执行一种信息处理方法的处理，该方法用于创建对应于从内容权利所有装置接收的信息记录介质制造请求数据的密钥信息发出请求数据，其中所述密钥信息发出请求数据包括：至少一内容或基于所述内容的一个散列值；用于所述内容权利所有装置和信息记录介质制造者中每一个的识别数据；信息记

录介质制造数量数据和每个所述数据的所述内容权利所有装置的数字签名。

根据本发明的又一个优选实施例，提供了一种计算机可读程序，用于使一计算机执行一种信息处理方法的处理，所述信息处理方法用于响应来自所述信息记录介质制造者的密钥信息发出请求数据，向信息记录介质制造者提供能够获取用于解密存储在一信息记录介质上的加密内容的密钥信息的密钥信息块，所述方法包括:

对包括在所述密钥信息发出请求数据内的内容权利所有装置的签名进行处理；和

在验证密钥信息发出请求数据是对应于由所述内容权利所有装置所发出的信息记录制造请求数据的已授权的密钥信息发出请求数据的条件下，在由所述验证机制验证的签名基础上，将所述密钥信息块发送给所述信息记录介质制造者。

应该注意，本发明的计算机程序是能够用于可执行各种程序码的计算机系统的经由以计算机可读形式提供的存储介质、例如诸如 CD、FDH、MO 的记录介质的通信介质、或诸如网络的通信介质所提供的计算机程序。以计算机可读形式提供所述程序以根据计算机系统中的所述程序来实现处理。

应该注意到，说明书中的所述系统是一种多个装置的逻辑组合结构，并且各个结构的所述装置并不限于在同一或单个外壳内提供。

根据本发明的所述结构，信息记录介质制造者(DM:盘制造者) 被构造成发送密钥信息(EKB)发出请求数据到密钥信息(EKB)发出中心，其中所述密钥信息(EKB)发出请求数据是根据由内容权利所有者(CO:内容所有者)所发出的信息记录介质（盘)制造请求数据(DMR :盘制造请求)创建的，在所述密钥信息(EKB)发出中心验证所述密钥信息(EKB)发出请求数据。换句话说，验证密钥信息(EKB)发出请求数据是否是对应于已授权信息记录介质(盘)制造请求数据(DMR :盘制造请求)的已授权请求数据，并且如果满足了该验证，就发出将要存储在信息记录介质上的所述密钥信息(EKB)的密钥信息。因此，对于从非法途径获取的内容来说，从密钥信息(EKB)发出中心获取密钥信息(EKB)是不可能的，存储对应于将要存储在所述信息记录介质上的加密内容的密钥信息(EKB)是不可能的，并且预防了制造存有非法获取的内容的盘。

另外，根据本发明的所述结构，对于从非法途径获取的、没有由内容权利所有者(CO:内容所有者) 所发出的正式的信息记录介质(盘)制造请求数据

(DMR:盘制造请求) 的内容来说，不能获取来自密钥信息(EKB)发出中心的密钥信息(EKB)，并不可能制造存储所述密钥信息(EKB)的信息记录介质。

在本发明的所述结构中，作为验证所述密钥信息 EKB）发出请求数据是否是对应于已经授权的信息记录介质（盘）制造请求数据 DMRP: 盘制造请求）的已经授权的请求数据的处理，所述密钥信息(EKB)发出中心执行包括在从信息记录介质制造者(DM:盘制造者)接收的所述密钥信息(EKB)发出请求数据内的所述内容权利所有者(CO:内容所有者)的签名验证处理。由此，不可能在信息记录介质制造者(DM :盘制造者)处伪造，并且可以可靠地判断所述密钥信息(EKB)是否对应于所述已授权的信息记录介质(盘)制造请求数据(DMR:盘制造请求)。

附图说明

通过下面结合附图的详细描述说明，本发明优选具体实施例的上述及其他目的和特征对于本领域普通技术人员来说将变得更加明显，其中：

图 1 用于解释根据本发明的信息记录介质控制结构；

图 2 用于解释存储在信息记录介质上的数据结构；

图 3 用于解释用于对各种密钥和数据进行加密处理和分配处理的分级型树状结构；

图 4 简要示出了一个分配的例子和一使用内容密钥的使能密钥块(EKB)进行解密处理的例子；

图 5 示出了用于解释信息记录介质制造请求数据和 EKB 发出请求数据的数据结构；

图 6 示出了用于解释信息记录介质制造请求数据和 EKB 发出请求数据的数据结构。

图 7 示出了用于解释在每一实体中的信息处理装置的结构实例子；

图 8 示出用于解释内容权利所有者(CO: 内容所有者)的处理顺序流程；

图 9 示出了用于解释信息记录介质制造实体(DM: 盘制造者)的处理顺序的流程；

图 10 示出了用于解释所述信息记录介质制造实体(DM: 盘制造者)的盘制造过程顺序的流程；

图 11 示出了用于解释密钥信息(EKB)发出中心的处理顺序的流程；

图 12 用于解释根据本发明的信息记录介质控制结构;

图 13 示出了用于解释所述信息记录介质制造实体(DM: 盘制造者)的盘制造顺序的流程。

具体实施方式

在下文中，参照所述附图详细描述了一种信息记录介质制造控制系统、一种信息处理装置和方法和一种计算机程序。应该注意到，所述描述是按下述顺序进行的。

1.信息记录介质的制造过程概要

2. EKB 的结构和密钥获取处理

3.信息记录介质的制造控制处理的细节

4.每一实体的信息处理装置结构

5.每一实体的处理顺序

6.通过许可装置的数据写入

1.信息记录介质的制造过程概要

首先，参照图 1 和后面的内容来描述信息记录介质的制造过程概要。在所述信息记录介质中，诸如音乐、图像和程序的各种内容被存储并提供给用户。具有一内容的版权或发行权内容权利所有者(CO: 内容所有者)102 在一预定程序的基础上向信息记录介质(盘)制造实体(DM：盘制造者) 103 提供所述内容，并且所述信息记录介质(盘)制造实体 103 在盘上存储所述收到的内容以制造一信息记录介质 110 并通过经销商（未示出）把其提供给用户。用户把信息记录介质加载到诸如数据记录/再现装置和 PC (个人计算机)的一信息处理装置(用户装置) 105 上，以执行所述内容的再现和使用。

所述内容权利所有者 102 是内容所有者，其拥有诸如所述内容的版权或发行权的复制和提供所述内容的权利。例如，它由诸如电影公司之类的内容所有者组成。所述内容权利所有者 102 根据诸如原创内容来创建一编辑内容，并把所述编辑内容提供给所述信息记录介质制造实体 103，其中该编辑内容将存储在诸如 CD 和 DVD 之类的信息记录介质上。 然后，所述信息记录介质制造实体 103 大量地转录(重复) CD、DVD 等，作为在某种程序下根据所收到的内容而向用户提供的介质以向用户提供并制造所述信息记录介质 110。

在本发明的内容存储信息记录介质的制造控制结构中，除了所述内容权利所有者 102 和信息记录介质制造实体 103 之外，还有 CA (证书特许机关)101 和密钥信息(EKB)发出中心 104。下面将对各实体的功能和角色执行描述。

在根据信用调查了每个实体之后，所述 CA(证书特许机关)101 向各实体发出基于公开密钥加密的公开密钥、秘密密钥和用于保证所述公开密钥有效的公开密钥证书。此外，当需要时，它还发出作为无效信息的具有已发出的公开密钥证书的吊销证书清单并将其提供给么实体。

所述密钥信息(EKB)发出中心 104 是一发出密钥信息(EKB)的机构。 所述 EKB 是一使能密钥块并且是存储用于解密例如内容的某些机密信息的密钥信息的密钥信息块。例如，它是一个能够在存储在特定装置中的装置密钥的基础上仅需经过解密处理就能够获取机密信息的密钥信息块。例如，它被形成为一密钥信息块，该块能够在存储在一具有有效许可的用户信息处理装置中的装置密钥的基础上，经处理（解密）获取解密内容所需的密钥信息。

所述 EKB 被形成为一种密钥信息块，它能够通过仅对所施加的从被设置成树结构的叶结构的多个用户装置中选择一用户装置的被存储密钥进行解密处理获取密钥信息。

所述EKB是一种能够仅靠存储于具有有效许可的用户装置中的装置密钥就可以得到密钥的密钥信息块。用被作废(吊销处理)了的用户装置中所存的装置密钥，不能处理(解密)和获取密钥。当对用户装置的许可的有效性方式变化时，所述密钥信息(EKB)发出中心 104 可以执行所述 EKB 的结构变化，以创建一种只利用存储在特定用户装置中的装置密钥就能够执行解密的 EKB。所述 EKB 连同内容一起记录在信息记录介质 110 上，所述信息记录介质 110 存储了所述加密内容并提供给用户。稍后详细描述所述 EKB 的结构和密钥获取处理。

内容权利所有者(CO: 内容所有者)102 是一个具有诸如对内容的版权或发行权的对内容进行复制和提供的实体。具体地说，其由电影公司和唱片公司等等组成。所述内容权利所有者(CO: 内容所有者)102 可以有其自己的内容编辑 (创作)机制，以执行内容的编辑，或可以请求一个作为单独实体的创作工作室来编辑(创作)一内容。所述内容权利所有者(CO: 内容所有

者)102 在编辑(创作)完之后，至少拥有复制和提供内容的权利。

所述信息记录介质制造实体(DM:盘制造者)103 是一个制造信息记录介质的实体，所述信息记录介质存储了根据所述内容权利所有者(CO: 内容所有者)102 的请求从所述内容权利所有者(CO:内容所有者)102 所收到内容。例如，其拥有 CD 和 DVD 等的盘制造装置并且用其来制造存储从所述内容权利所有者(CO:内容所有者)102 收到的内容的信息记录介质。

如图 2 所示，在由所述信息记录介质制造实体(DM: 盘制造者)103 制造的信息记录介质 110 中，存储有用于获取所述加密内容 201 的解密处理所需的密钥信息的一密钥信息(EKB)202 和一加密内容 201。

用户使用先前存储在所述信息处理装置 105 中的装置密钥在所述信息处理装置 105 中执行所述密钥信息(EKB) 202 的解密，以便获取解密所述加密内容 201 的处理所需的密钥信息，并根据所获取的信息执行所述加密内容 201 的解密处理，以执行再现和使用所述内容。应该注意，通过所述密钥信息(EKB)202 的解密而获取的密钥信息，可以作为所述加密内容的解密密钥而被直接应用或用于所述加密内容的解密密钥可以通过基于其他信息的加密处理获取。无论如何，拥有能够解密所述密钥信息(EKB)202 的装置密钥的用户装置只是拥有已授权的许可证的用户装置。

可以只使用存储在具有有效许可的用户的信息处理装置中的装置密钥处理(解密)所述密钥信息(EKB)202，而不能使用存储在作废(吊销处理)了的用户装置中的装置密钥处理。根据所谓的分级型树结构，使用一信息传送方法来向用户装置(信息处理装置)提供这些。

2.EKB 的结构和密钥获取处理

参照附图描述所述 EKB 的结构和密钥获取处理。在图 3 中最低一级处的数字 0 到 15 是作为执行例如内容使用的信息处理装置的用户装置。换句话说，在图 3 中分级型树结构所示的每片叶结构都是一个装置。

0 到 15 中的每个装置都在一存储器中存储了一密钥集(装置密钥 DNK：装置节点密钥))，其由在所述分级树结构中分配给从其自己的叶到根的节点的密钥(节点密钥)和在制造或装运或其之后的时候的每个叶的叶密钥形成。在图 3 最低一级处示出的 K0000 到 K1111 分别是分配给 0 到 15 的各个装置的叶密钥，而从最高一级处的 KR (根密钥)到来自最低一级的第二节点

所描述的密钥 KR-K111 是节点密钥。

在图 3 示出的树结构中，例如所述装置 0 拥有叶密钥 K00000 和所述节点密钥 K0000、K00、K0、KR 作为装置密钥。装置 5 拥有 K0101、K010、K01、K0、KR。装置 15 拥有 K1111、K111、K11、K1、KR。 应该注意到，在图 3 中的所述树中只描述了从 0 到 15 的 16 个装置，并且所述树结构被示为一种四级结构的平衡对称的结构，但是在所述树中还有可能有更多装置形成，并在所述树的每个部分都提供了一种配置和不同的级数。

此外，包括在图 3 中的树结构内的所述各个装置，包括使用各种记录介质的装置的各种类型，例如，嵌入式存储器或诸如 DVD、CD、MD、闪速存储器等等可随意拆卸的介质。并且，可以同时存在各种应用服务程序。 是图 3 所示内容或密钥分配配置的分级树结构被应用于这种不同装置和不同应用程序的共存结构。

在一系统中，这些各种装置和应用程序共存，例如图 3 中由虚线所包围的部分。换句话说，所述装置 0、1、 2、3 被设为一组。例如，只有包括在由虚线所包围的该组内的装置才拥有存储在所述信息记录介质上的所述加密内容的已经授权的使用权，即，所述许可证。在这种情况下，只有装置 0、1、2、3 将所述 KEB 设置成能够获取应用于内容解密的密钥以把其存储在存储所述加密内容的所述信息记录介质上。

如从图 3 可看出的，包括在一组内的所述 0、1、2、3 三个装置拥有公用密钥 K0K00、K0、KR 作为存储在所述各个装置中的 DNK (装置节点密钥)。

在这种情况下，只允许装置 0、1、2 获取用于内容解密的内容密钥 Kcon 的所述 EKB 的结构例如是在图 4 中所示出的结构。具体地说，所述 EKB 被设置为

索引	加密数据
000	Enc (K0000, Kcon)
0010	Enc (K0010, Kcon)。

应该注意到，Enc (Kx, Ky)指的是利用密钥 Kx 加密数据 Ky 获得的加密数据。在这种情况下，所述装置 0、1 可以使用其拥有的装置密钥[K000]解密索引[000]的加密数据，并且装置 2 可以使用装置密钥[K0010]解密前述 EKB 的索引[0010]的加密数据，和所述内容密钥 Knon 可以通过各个已加密数据的解密处理来获取。其它的装置并未拥有装置密钥[K0000]、

[K0010]中的任一个，并且即使是当其接收到具有图 4 所示配置 EKB 时，也不能通过解密所述 EKB 来获取内容密钥。

利用这样的方式，所述 EKB 被配置为一种密钥信息块，其只能够向一特定装置提供诸如一内容密钥的机密信息，所述内容密钥可以根据拥有许可证的装置通过设置为结构数据而只在一任意所选的装置中被处理。所述密钥信息(EKB)发出中心 104，创建可以只在允许使用所述内容的装置中处理的所述 EKB，并把其提供给所述信息记录介质制造实体 103。所述信息记录介质制造实体 103 把该 EKB 连同所述已加密内容存储在信息记录介质 110 上并把其提供给用户。

3.信息记录介质的制造控制处理细节

回到图 1，描述在制造信息记录介质过程中的所述控制结构。 假设所述内容权利所有者(CO: 内容所有者)102 在编辑(创作)之后拥有一内容用以存储在一信息记录介质上。所述内容权利所有者(CO: 内容所有者) 102 发送一信息记录介质(盘)制造请求(DMR: 盘制造请求)151 给所述介质制造实体 103。

图 5 示出了所述信息记录介质(盘)制造请求(DMR: 盘制造请求) 151 的数据格式的一个例子。在图 5 中示出的所述信息记录介质(盘)制造请求(DMR: 盘制造请求)151 的数据包括下列数据:

(1) 需要存储在盘上的内容

(2) 内容权利所有者(CM: 内容所有者)的 ID (识别符)

(3) 信息记录制造实体(DM: 盘制造者)的 ID (识别符)

(4) 信息记录介质(盘)的制造的请求量(定购数)，所述定购数指出了所述内容权利所有者(CO: 内容所有者)允许使用其所提供的内容制造多少盘。

此外，作为用于上述数据(1)到(4)的电子签名信息，还包括一通过利用内容权利所有者(CO: 内容所有者)的秘密密钥所创建的数字签名(签名)和一存储所述内容权利所有者(CO: 内容所有者)的公开密钥的公开密钥证书(内容所有者的证书)。应当注意，在一个例子中，如果所述信息记录介质制造实体存储了所述内容权利所有者(CO: 内容所有者)的公开密钥证书(内容所有者的证书)，那么，所述内容权利所有者(CO: 内容所有者)的公开密钥证书

(内容所有者的证书)就不必被在第二请求或其后的请求中发送以减少所述负荷。

所述数字签名是一种可以仅仅由用于某一数据(诸如就计算量而言另一实体难于创建的数据)的一特定实体创建的数据,并且根据一预定顺序执行签名验证处理以允许确定是否存在经过签名的数据的伪造。

作为用于数字签名的方法,DSA(数字签名算法)、省略DSA(elliptical DSA)、或根据RSA加密方法的方法都是合适的。例如在由Okamoto Tatsuaki、Yamamoto Hirosuke所著、由Sangyo Tosho所出版的"流加密(Current Encryption)"介绍了所述DSA和RSA方法,并且所述省略DSA还在当前的IEEE-P1363标准的考虑中。

应该注意到,除了前述(1)到(4)数据以外的信息,也可以被包括在所述信息记录介质(盘)制造请求(DMR:盘制造请求)151内。例如,可以包括诸如所述内容的复制控制信息这样的信息和诸如提供所述内容的再现的数量/时间的所述内容的使用许可信息(使用规则)。通过利用所述内容权利所有者(CO:内容所有者)的秘密密钥所创建的数字签名(签名),是为包括该附加信息的所述数据而创建的。因此,预防了另外的实体或用户的伪造数据。此外,作为一个例子,所述信息记录介质(盘)制造请求(DMR)可以包括单个DMR的识别信息,诸如序号、发行所述DMR的时间信息等等。通过这样做,有可能预防重复使用某一信息记录介质(盘)制造请求(DMR)。

该信息是连同在所述信息记录介质上的所述内容一起存储的,并且在对装置端的内容再现过程中,在内容使用处理程序的控制下执行内容使用,所述内容处理程序根据复制控制信息和所允许的内容再现的数量/时间执行处理,借此以根据所述附加信息允许所述内容的使用。

接收具有图5所示数据结构的信息记录介质(盘)制造请求(DMR:盘制造请求)151的信息记录介质制造实体(DM:盘制造者)103使用所述CA的认证密码(所述公开密钥)验证包括在信息记录介质(盘)制造请求(DMR)151内的所述公开密钥证书(内容所有者的证书)。如果验证失败,就不执行后续处理。如果验证成功,就从该证书中取出内容权利所有者(CO:内容所有者)102的公开密钥,并且,所取出的公开密钥被用于执行所述数字签名(签名)的验证处理,其中,所述数字签名包括在所述信息记录介质(盘)制造请求(DMR)151内。利用所述数字签名(签名)的验证处理,验证了上述(1)到(4)的数据

是已经授权的数据而不是伪造的。

应当注意，验证是否是内容权利所有者(CO:内容所有者)102的识别符(ID)是在由所述CA（证书特许机关）101发出的公开密钥证书吊销(无效的)清单中描述的，并且如果在所述清单中有描述，则因为所述内容权利所有者(CO:内容所有者)102是一个被确定为无效实体的实体，而把所述验证设置为失败，并且收不到所述信息记录介质(盘)制造请求(DMR)151。

当内容权利所有者(CO:内容所有者)102的识别符(ID)没有被描述在由CA（证书特许机关)101发出的所述公开密钥证书吊销(无效)清单中和前述公开密钥证书和所述信息记录介质(盘)制造请求(DMR:盘制造请求)显示前述公开密钥证书和所述信息记录介质(盘)制造请求(DMR:盘制造请求)的数据(1)到(4)是已经授权的数据而不是伪造的时，所述信息记录介质制造实体(DM:盘制造者）103将密钥信息(EKB)发出请求152传送给密钥信息(EKB)发出中心104。

所述密钥信息(EKB)发出请求152包括与参照图5描述的信息记录介质(盘)制造请求(DMR:盘制造请求)151的格式相同的数据。

最好，在从信息记录介质制造实体(DM：盘制造者）103向密钥信息(EKB)发出中心104发送密钥信息(EKB)发出请求152之前，信息记录介质制造实体(DM:盘制造者)103和密钥信息(EKB)发出中心104两者都执行相互授权和会话密钥共享处理，以检查两者的有效性，并共享一用于通信数据的加密会话密钥以加密并发送所述通信数据。换句话说，所述密钥信息(EKB)发出请求152具有所述会话密钥。

应当注意，作为所述相互授权和会话密钥共享处理，基于一种利用共有的秘密密钥和公开密钥证书的公开密钥加密方法的相互授权处理(例如，ISO9798-3)是合适的。

此外，有可能使用一种配置，在该配置中，增加了信息记录介质制造实体(DM:盘制造者）103的数字签名并且信息记录介质制造实体(DM:盘制造者)103的公开密钥证书被从用于发送的信息记录介质制造中心(DM:盘制造者)103附着到用于密钥信息EKB)发出中心104的密钥信息EKB)发出请求152上。使用信息记录介质制造实体(DM：盘制造者）103的秘密密钥经过对用于密钥信息(EKB)发出请求152的所述结构数据的加密处理创建所述数字签名。

所述密钥信息(EKB)发出中心104使用所述CA的验证密钥(公开密钥)验证包括在密钥信息(EKB)发出请求152内的内容权利所有者(CO:内容所有者)102的公开密钥证书(内容所有者的证书)。如果验证失败，就不执行后续处理。而如果验证成功，就从该证书中取出所述内容权利所有者(CO:内容所有者)102的公开密钥，并且所取出的公开密钥被用于执行包括在所述密钥信息(EKB)发出请求152内的所述内容权利所有者(CO:内容所有者)102的所述数字签名(签名)的验证处理。利用所述数字签名(签名)的验证处理，所述密钥信息(EKB)发出中心104检查包括在所述密钥信息(EKB)发出请求152内的所述数据是否为这样一种请求，其对应于一已经授权的、由所述内容权利所有者(CO:内容所有者)102所发出的信息记录(盘)制造请求DMR 151。

此外，密钥信息(EKB)发出中心104验证包括在密钥信息(EKB)发出请求152内的内容权利所有者(CO:内容所有者)102的所述公开密钥证书(内容所有者的证书)的吊销状态，并在检查出其没有被吊销之后执行签名验证。如果其被吊销了，则停止所述密钥信息(EKB)发出处理。

应当注意，当密钥信息(EKB)发出请求152包括信息记录介质制造实体(DM:盘制造者)103的数字签名(签名)和一公开密钥证书(盘制造者的证书)时，密钥信息(EKB)发出中心104就使用所述CA的验证密钥(公开密钥)来验证信息记录介质制造实体(DM:盘制造者)103的所述公开密钥证书。如果验证失败，就不执行后续处理。而如果验证成功，就从该证书中取出信息记录介质制造实体(DM:盘制造者)103的公开密钥，然后所取出的公开密钥就被用于执行包括在密钥信息(EKB)发出请求152内的信息记录介质制造实体(DM:盘制造者)103的数字签名(签名)的验证处理，利用所述数字签名(签名)的验证处理，其执行对所述密钥信息(EKB)发出请求152本身是否为已经授权的数据而不是伪造的数据的检查处理。应当注意，在这种情况下，密钥信息(EKB)发出中心104执行下述检查，即信息记录介质制造实体(DM:盘制造者)103的公开密钥证书(盘制造的证书)是否被吊销。如果其被吊销了，则停止所述密钥信息(EKB)发出处理。

当密钥信息(EKB)发出中心104检查密钥信息(EKB)发出请求152的有效性时，换句话说，当包括在密钥信息(EKB)发出请求152内的数据是用于由内容权利所有者(CO:内容所有者)102通过上述处理所发出的已授权信息记录介质(盘)制造请求(DMR)151的请求时，作为对该请求的应答，其将包括

EKB 的密钥信息 153 发送给信息记录介质制造实体(DM: 盘制造者) 103。应当注意，在这种数据发送中，最好在发送之前执行基于会话密钥的加密处理。

应当注意，有可能利用这样一种结构，其中密钥信息(EKB)发出中心 104 以该结构创建存于密钥信息(EKB)中的所述密钥信息和用于所述内容的加密的密钥，然后把它们发送给信息记录介质制造实体(DM: 盘制造者) 103，还有可能使用这样一种结构，其中在信息记录介质制造实体(DM: 盘制造者)103 一端，以该结构创建用于所述内容的加密处理的密钥，所创建的密钥被发送给密钥信息(EKB)发出中心 104，然后密钥信息(EKB)发出中心 104 创建存储所创建密钥的密钥信息(EKB)并将其传送给信息记录介质制造实体(DM: 盘制造者) 103。

当信息记录介质制造实体(DM: 盘制造者)103 从密钥信息(EKB)发出中心 104 接收到包括所述 EKB 的密钥信息 153 时，其使用对应于这些密钥信息的密钥执行对从内容权利所有者(CO: 内容所有者)102 接收的内容的加密处理，创建将被存储在信息记录介质上的加密内容，并制造存储所创建的加密内容和所述密钥信息(EKB)的信息记录介质。所制造的信息记录介质的数量对应于内容权利所有者(CO: 内容所有者)102 所要求制造的数量。

应当注意，信息记录介质制造实体(DM ：盘制造者)103 所使用的信息记录介质制造装置最好被形成为具有一种配置，该配置例如执行存储对应于一具体 EKB 的制造盘数量的存储处理以便将存储数据存储在存储器中。当需要时，这些数据对由密钥信息（EKB）发出中心 104 或内容权利所有者（CO: 内容所有者）102 进行的验证进行监控。此外，有可能使用这样一种配置，其中，诸如密钥信息(EKB)发出中心 104 和内容权利所有者(CO: 内容所有者) 102 的信息处理装置可以与信息记录介质制造实体(DM: 盘制造者) 103 所使用的信息记录介质制造装置执行通信，该配置被如此构成以致使每个实体都能够与信息记录介质制造实体(DM: 盘制造者)103 所用的信息记录介质制造装置进行通信，以便在需要时执行存储数据的验证。

如上所述，根据本发明的所述配置，信息记录介质制造实体(DM ：盘制造者)103 被构造成发送密钥信息(EKB)发出请求 152 给密钥信息(EKB)发出中心 104，其中所述密钥信息(EKB)发出请求 152 是根据由内容权利所有者(CO: 内容所有者)102 所发出的信息记录介质(盘)制造请求(DMR: 盘制造请求) 151 创建的。换句话说，验证密钥信息(EKB)发出请求 152 是否是对应于已

授权信息记录介质(盘)制造请求(DMR:盘制造请求) 151的已授权请求数据，并且如果满足了所述验证，就发出包括将要存储在信息记录介质110上的所述密钥信息(EKB)的密钥信息153。因此，对于从未经授权途径获取的内容来说，从密钥信息(EKB)发出中心104获取包括所述密钥信息(EKB)的密钥信息153是不可能的，存储对应于将要存储在所述信息记录介质上的加密内容的密钥信息(EKB)是不可能的，并且预防了制造存有非法获取的内容的盘。

如上所述，根据本发明的所述配置，对于从未经授权径获取的没有经内容权利所有者(CO:内容所有者)102发出的正式信息记录介质(盘)制造请求(DMR:盘制造请求) 151的内容，不能获取包括来自密钥信息(EKB)发出中心104的密钥信息(EKB)的密钥信息153，并且不可能制造存储所述密钥信息(EKB)的信息记录介质110。

应当注意，作为验证所述密钥信息（EKB）发出请求152是否是对应于已授权的信息记录介质（盘）制造请求（DMR: 盘制造请求）的已授权请求数据的处理，所述密钥信息(EKB)发出中心104执行该处理以作为从信息记录介质制造实体(DM:盘制造者)103接收到的包括在密钥信息(EKB)发出请求151内的内容权利所有者(CO:内容所有者)102的签名验证处理。因此，在信息记录介质制造实体(DM:盘制造者)103中的伪造是不可能的，并且密钥信息(EKB)发出中心104能可靠地确定密钥信息(EKB)发出请求152是否对应于已授权的信息记录介质(盘)制造请求(DM:盘制造请求)151。

另外，尽管上面的描述已经假设从信息记录介质制造实体(DM：盘制造者) 103发送给密钥信息(EKB)发出中心104的密钥信息(EKB)发出请求152包括全部包括在将要从内容权利所有者(CO:内容所有者)发送给信息记录介质制造实体(DM:盘制造者)103的信息记录介质(盘)制造请求(DMR:盘制造请求)151内的所述数据，换句话说，包括所述内容数据本身，但还是存在下述问题，即如果所述内容数据的容量越大，则发送的负荷就越大。

必须在从内容权利所有者(CO:内容所有者)102发送给信息记录介质制造实体(DM:盘制造者)103的信息记录介质(盘)制造请求(DMR:盘制造请求)中包括所述内容，但是没有必要把全部内容都包括在从信息记录介质制造实体(DM:盘制造者) 103发送给密钥信息(EKB)发出中心104的密钥信息(EKB)发出请求152内，所以，如图6所示，所述密钥信息(EKB)发出中心152可以被配置成不包括所述内容。

然而，为允许检查密钥信息(EKB)发出中心104中的内容，在内容数据的基础上创建一散列值，在信息记录介质制造实体(DM:盘制造者) 103的所述秘密密钥的基础上创建一签名，以用于包括所述散列值并包括在密钥信息(EKB)发出请求152中的数据。

如图6所示，内容权利所有者(CO:内容所有者)102在内容数据311的基础上创建一作为散列值的内容散列值312并将基于内容权利所有者(CO：内容所有者)102的所述秘密密钥的签名添加到包括内容散列值312的所述数据上，以创建信息记录介质(盘)制造请求(DMR：盘制造请求)数据301。

此外，信息记录介质制造实体(DM:盘制造者)103把基于信息记录介质制造实体(DM:盘制造者)103的秘密密钥的一个签名313添加到除内容311以外的数据上，附上存储信息记录介质制造实体(DM:盘制造者)103的公开密钥的公开密钥证书314，并把其作为密钥信息(EKB)发出请求数据312发送给密钥信息(EKB)发出中心104。

利用这种数据结构，能够显著地减少密钥信息(EKB)发出请求152的数据量。如果以后发生争执，当信息记录介质制造实体(DMR:盘制造者)103能够提供对应于所述散列值的内容数据时，也可以保证信息记录介质制造实体(DM:盘制造者)103已经执行了正确的处理。

应当注意，作为向散列函数H输入所述内容数据的结果，所述散列值被配置为一固定长度的数据(例如，160位)。所述散列函数H是这样一种函数，在该函数中，很容易为任意长度范围的数据x计算输出y = H（x)，而很难在给定y时确定满足y = H（x′）的x′（其不能与x相同)的计算量。例如，作为输出长度为160位的散列函数，在FIP180-1和180-2中定义了SHA-1。

4.用于每个实体的信息处理装置的结构

图1所示的内容权利所有者(CO:内容所有者) 102、信息记录介质制造实体(DM:盘制造者)103和密钥信息(EKB)发出中心104中的每一个都执行相互发送和接收的数据的所述数据的发送/接收处理。换句话说，从内容权利所有者(CO:内容所有者)102发送给信息记录介质制造实体(DM：盘制造者)103的信息记录介质(盘)制造请求(DMR:盘制造请求) 151、从信息记录介质制造实体DM:盘制造者)103所发送的密钥信息(EKB)发出中心152、包括从密钥信息(EKB)发出中心104发送给信息记录介质制造实体(DM:盘制造者)

103 的密钥信息 153 等，也执行发送数据的创建和接收数据的验证处理等。

因此，图 1 所示的内容权利所有者(CO: 内容所有者) 102、信息记录介质制造实体(DM: 盘制造者)103 和密钥信息(EKB)发出中心 104 中的每一个都必须具有一信息处理装置，用于执行需要发送数据的创建处理、数据发送/接收处理和数据验证处理等。

图 7 示出了由这些实体中的每一个所拥有的所述信息处理装置的结构例。如图 7 所示，所述信息处理装置具有控制器 501、运算单元 502、输入/输出接口 503、保密存储单元 504、主存储单元 505、网络接口 506 和介质接口 507。

例如，控制器 501 由 CPU 构成,其具有根据计算机程序执行数据处理的控制单元的作用。运算单元 502 提供专用于创建加密密钥、创建随机数和加密处理的运算函数。输入/输出接口 503 是支持从诸如键盘和鼠标等的输入装置的数据输入和到诸如显示器等的输出设备的数据输出处理。例如，保密存储器单元 504 是一种存储单元，用于存储需要被安全或保密保持的数据，诸如是加密密钥和各种 ID。主存储单元 505 是一个存储区域，用于例如在控制器 501 中执行的数据处理程序和一暂存处理参数，也可以是用于执行程序的工作区，等等。保密存储单元 504 和主存储单元 505 可以由诸如 RAM（随机存取存储器）、ROM（只读存储器）等存储器构成。

网络接口 506 是一连接到因特网的网络接口或一专用线路等，并被用于与外部实体的通信处理。介质接口 507 提供从/向诸如 CD、DVD 和 MD 的介质进行读/写的功能。

5.每个实体的处理顺序

接下来，描述内容权利所有者(CO: 内容所有者)102、信息记录介质制造实体(DM ：盘制造者) 103 和密钥信息(EKB)发出中心 104 中每一个的处理顺序。

首先，参照图 8 描述内容权利所有者(CO: 内容所有者)102 所执行处理的顺序。

在步骤 S101，内容权利所有者(CO: 内容所有者)102 创建将被发送给介质制造实体(DM: 盘制造者)103 的信息记录介质(盘)制造请求(DMR: 盘制造请求) 151。如参照图 5 和图 6 所描述的，信息记录介质(盘)制造请求(DMR:

盘制造请求)是包括将被存储在所述信息记录介质上的内容、内容权利所有者 ID、盘制造实体 ID、所请求制造的数量、所述内容权利所有者签名和所述内容权利所有者的公开密钥证书的数据。

在步骤S102,内容权利所有者(CO:内容所有者) 102 将信息记录介质(盘)制造请求(DMR: 盘制造请求) 151 发送给介质制造实体(DM :盘制造者)103。

应当注意,当通过网络执行通信从内容权利所有者(CO:内容所有者)102 发送信息记录介质(盘)制造请求(DM:盘制造者)时,在发送信息记录介质(盘)制造请求(DMR:盘制造请求)之前,在内容权利所有者(CO:内容所有者)102 和信息记录介质制造实体(DM: 盘制造者) 103 之间执行相互授权和会话密钥共享处理,并且在所述通信伙伴被验证的条件下,进行数据通信。换句话说,利用会话密钥加密信息记录介质(盘)制造请求(DM:盘制造请求)并发送。另外,作为一个例子,可以利用作为通信信道的诸如 CD-R 的记录介质发送信息记录介质(盘)制造请求(DM:盘制造请求),并且可以使用记录介质作为通信信道发送大容量数据的内容数据而其他数据则经过网络来发送。

接下来,参照图 9 描述由信息记录介质制造实体(DM:盘制造者) 103 所执行的处理顺序。

在步骤 S201,信息记录介质制造实体(DM:盘制造者)103 从内容权利所有者(CO:内容所有者)102 接收信息记录介质(盘)制造请求(DMR :盘制造请求)。

在步骤 S202,信息记录介质制造实体(DM:盘制造者) 103 执行信息记录介质(盘)制造请求(DMR:盘制造请求)的验证处理。具体地说,信息记录介质制造实体(DM: 盘制造者) 103 使用 CA 的所述验证密钥(公开密钥)对包括在信息记录介质(盘)制造请求(DMR)内的所述公开密钥证书(内容所有者证书)执行验证。如果验证失败,就不执行后续处理。如果验证成功,就从该证书中取出内容权利所有者(CO:内容所有者)102 的公开密钥,并且所取出的公开密钥被用于执行所述签名的验证处理,其中所述签名包括在所述信息记录介质(盘)制造请求(DMR)内。当发生签名验证错误时,其确定信息记录介质(DMC)制造请求(DMR)是例如伪造的未经授权的数据,并结束所述处理而不再执行后续处理。

应当注意,如上所述的,验证所述内容权利所有者(CO:内容所有者)102 的识别符(ID)是否是在由所述 CA (证书特许机关)101 发出的公开密钥证书

吊销(无效的)清单中被进行了描述，如果在所述清单中有描述，则内容权利所有者(CO:内容所有者) 102是一个被确定为无效实体的实体，以致所述验证失败，并且不能接收道所述信息记录介质(盘)制造请求(DMR)151。

利用所述签名验证，确定信息记录介质(盘)制造请求(DMR)是已授权的数据，前进到步骤S203，在这里，信息记录介质制造实体(DM:盘制造者)103将所述密钥信息(EKB)发出请求传送给密钥信息(EKB)发出中心104。

如参照图5和图6所执行的描述，各种数据结构中的任一种都可以被用于所述密钥信息(EKB)发出请求，诸如作为所述信息记录介质（盘）制造请求（DM: 盘制造请求）的一种格式由相同数据形成的数据格式，或由包括所述内容的散列值的数据和包括信息记录介质制造请求（M: 盘制造请求）103和公开密钥证书的结构形成的数据格式。

在从信息记录介质制造实体(DM:盘制造者)103向密钥信息(EKB)发出中心104发送所述密钥信息(EKB)发出请求之前,信息记录介质制造实体(DM:盘制造者)103和密钥信息(EKB)发出中心104两者都执行相互授权和会话密钥共享处理，以检查两者的有效性，并共享用于通信数据加密数据的所述会话密钥以加密所述通信数据。换句话说，密钥信息(EKB)发出请求152具有用于发送的所述会话密钥。

在步骤S204,信息记录介质制造实体(DM:盘制造者)103从密钥信息(EKB)发出中心104接收包括所述EKB的密钥信息，并在步骤S205使用包括在从密钥信息(EKB)发出中心104接收到的所述密钥信息内的密钥，以对从内容权利所有者(CO:内容所有者)102处收到的所述内容执行加密并写入所述盘以执行盘制造处理。

图10示出了信息记录介质制造实体(DM:盘制造者)103执行盘制造处理的详细顺序。在步骤S301，信息记录介质制造实体(DM:盘制造者)103使用包括在从密钥信息(EKB)发出中心104接收的密钥信息内的所述密钥，对从内容权利所有者(CO:内容所有者)102接收的内容执行加密。在步骤S302，所述加密内容被存储在所述信息记录介质(盘)中。

在步骤S303，信息记录介质制造实体(DM:盘制造者)103把从密钥信息(EKB)发出中心104接收的所述EKB存储在所述信息记录介质(盘)上。

应当注意，图10所示的流程是原版盘的制造处理流程，利用该处理流程所制造的原版盘用来制造多个盘。制造的数量是所要求制造的数量，其包

括在从内容权利所有者(CO:内容所有者)102接收的所述信息记录介质(盘)制造请求(DMR :盘制造请求)内。

接下来，参照图11描述所述密钥信息(EKB)发出中心104的处理顺序。

在步骤S401,密钥信息(EKB)发出中心104从信息记录介质制造实体(DM:盘制造者)103接收密钥信息(EKB)发出请求。

在步骤S402，密钥信息(EKB)发出中心104执行所述密钥信息(EKB)发出请求的验证处理。密钥信息(EKB)发出中心104使用所述验证密钥(公开密钥)验证包括在所述密钥信息(EKB)发出请求中的所述内容权利所有者(CO:内容所有者)102的公开密钥证书(内容所有者的证书)。如果验证失败，就不执行后续处理。如果验证成功，就从该证书中取出所述内容权利所有者(CO:内容所有者)102的公开密钥,并且所取出的公开密钥被用于执行包括在密钥信息(EKB)中的内容权利所有者(CO:内容所有者)102的数字签名(签名)的验证处理。利用所述数字签名(签名)的验证处理，密钥信息(EKB)发出中心104确定包括在所述密钥信息(EKB)发出请求内的所述数据是一个对应于由内容权利所有者（CO: 内容所有者）102发出的已授权信息记录介质（盘）制造请求（DMR）的请求。

应当注意，当所述密钥信息(EKB)发出请求包括信息记录介质制造实体(DM:盘制造者)103 的数字签名(签名)和所述公开密钥证书(盘制造者的证书)时，密钥信息(EKB)发出中心104使用所述CA的验证密钥(公开密钥)，来验证信息记录介质制造实体(DM :盘制造者)103的公开密钥证书(盘制造的证书)。如果验证失败，就不再执行后续处理。而如果验证成功，就从该证书中取出信息记录介质制造实体(DM :盘制造者)103的公开密钥，然后利用所取出的公开密钥执行包括在密钥信息(EKB)发出请求152内的所述数字签名(签名)的验证处理，和利用所述数字签名(签名)的验证处理，可以确保所述密钥信息(EKB)发出请求本身不是伪造的有效数据。

当在前述签名验证处理中即使有一个导致错误时，可以确定所述信息（EKB）发布请求例如是一伪造的未经授权数据，由此，处理结束而不执行后续处理。

当在所述签名验证的基础上验证所述密钥信息(EKB)发出请求是一对应于由内容权利所有者(CO:内容所有者)102发出的有效信息记录介质(盘)制造请求(DMR)的一合法的请求时，密钥信息(EKB)发出中心104将包括EKB的

所述密钥信息发送给信息记录介质制造实体(DM:盘制造者)103作为对所述密钥信息(EKB)发出请求的应答。应该注意，这些数据最好是作为在所述会话密钥基础上的经加密处理的数据进行发送。

应该注意,如上所述,由于可以使用一种配置，在该配置中，密钥信息(EKB)发出中心104创建存储在密钥信息(EKB)中的所述密钥信息和在加密所述内容中使用的密钥，然后将它们发送给信息记录介质制造实体(DM:盘制造者)103，用于所述内容加密处理的密钥是在信息记录介质制造实体(DM:盘制造者)103一端被创建的，所创建的密钥被发送给密钥信息(EKB)发出中心104，存储所创建密钥的密钥信息(EKB)由密钥信息(EKB)发出中心104创建的并被送给信息记录介质制造实体(DM:盘制造者)103。

6.由许可装置写入的数据

接下来，借助于一个从执行内容控制的控制中心接收许可证并使用一能够执行特定数据写入处理的数据写入装置执行写入数据处理的装置的结构例来描述由所述信息记录介质制造实体(DM：盘制造者)执行的信息记录介质的制造处理。

参照图12描述本发明一优选实施例的一个例子的处理结构。在图12中，一CA（证书特许机关)601在对每个实体的信用进行调查之后，向各实体发出一基于公开密钥加密的公开密钥、秘密密钥和用于保证所述公开密钥有效性的公开密钥证书。内容权利所有者(CO:内容所有者)602是一个具有诸如对所述内容的版权和发行权的对所述内容进行复制和提供的实体。

信息记录介质制造实体(DM:盘制造者)603是一个在来自内容权利所有者(CO:内容所有者)602的请求的基础上制造存储从所述内容权利所有者(CO：内容所有者）602接收的所述内容的信息记录介质的实体。所述信息记录介质制造实体具有一个接收控制中心611的许可证的数据写入机制612。能够执行特定数据写入处理的数据写入机制612例如是一个能够使用盘内建立的坑状中的细微差别嵌入特定数据的装置，也可以是一种能够利用不同于一般的数据写入处理来写诸如一个内容的数据的装置。

控制中心611具有一密钥信息(EKB)发出中心604，作为一种工具，它能够发出密钥信息(EKB)并将数据写入机制612出租给被许可的信息记录介质制造实体(DM:盘制造者)603的机制。

应该注意，在本发明优选实施例的该例子中，对控制中心 611 具有密钥信息(EKB)发出中心 604 的结构执行了描述，虽然这些实体可以作为单独的独立实体而形成。

为了制造盘，首先，从内容权利所有者(CO: 内容所有者)602 向信息记录介质制造实体(DM：盘制造者)603 发送一信息记录介质(盘)制造请求(DM：盘制造请求) 651。所述数据格式与先前具体实施例中的相同并具有参照图 5 和图 6 所描述的数据结构。

在验证信息记录介质(盘)制造请求(DMR：盘制造请求) 651 之后，信息记录介质制造实体(DM 盘制造者)603 向密钥信息(EKB)发出中心 604 发送一密钥信息(EKB)发出请求 652。密钥信息(EKB)发出中心 652 具有和先前具体实施例(见图 5 和图 6)中相同的数据结构。

在验证信息记录介质(盘)制造请求(DMR：盘制造请求) 651 的有效性时，密钥信息(EKB)发出中心 604 向信息记录介质制造实体(DM：盘制造者) 603 发送包括所述 EKB 的密钥信息 653 以作为对所述请求的应答。此外，具有一密钥信息(EKB)发出中心 604 的控制中心 611 发送一数据写入许可信息 654 作为数据写入机制 612 的使用许可信息，其中该数据写入许可信息被发送给具有所述许可证的信息记录介质制造实体(DM: 盘制造者)603。

当信息记录介质制造实体(DM: 盘制造者)603 从密钥信息(EKB)发出中心 604 接收到包括所述 EKB 的密钥信息并从控制中心 611 接收到数据写入许可信息 654 时，其应用基于包括所述 EKB 的密钥信息 653 而获取的加密密钥对从内容权利所有者(CO: 内容所有者)602 接收的所述内容执行加密处理，以产生将要被存储在一信息记录介质上的所述加密内容，并制造存储所产生的加密内容和所述密钥信息(EKB)的信息记录介质。此外，信息记录介质制造实体(DM: 盘制造者)603 利用数据机制 612 根据来自控制中心 611 的数据写入许可信息 654 执行特定数据的写入。

应该注意，使用数据写入机制 612 写入的信息例如是对存储在信息记录介质上的加密内容进行解密处理所需要的加密密钥、或加密密钥创建信息、或诸如声明（dick）、内容、实体等的识别数据。

在参照图 13 所描述的实施例中，描述了信息记录介质制造实体(DM: 盘制造者)603 所执行的盘制造处理的详细顺序。

信息记录介质制造实体(DM: 盘制造者)603 在步骤 S501 对包括来自密钥

信息(EKB)发出中心 604 的所述 EKB 的密钥信息执行接收检查，并在步骤 S502 检查来自控制中心 611 的所述数据写入信息的接收。如果没有收到所述信息，就不执行所述盘制造。

在步骤 S503，在包括从密钥信息(EKB)发出中心 604 接收的所述 EKB 的密钥信息的基础上，获取一内容加密密钥，以便对从内容权利所有者(CO: 内容所有者)602 接收的所述内容执行加密。在步骤 S504，所述加密内容被存储在所述信息记录介质(盘)中。

在步骤 S505，信息记录介质制造实体(DM：盘制造者)603 把从密钥信息(EKB)发出中心 604 接收的所述 EKB 存储在所述信息记录介质(盘)上。此外，在步骤 S506，信息记录介质制造实体(DM ：盘制造者)603 使用数据机制 612 在来自控制中心 611 的数据写入许可信息 654 的基础上执行特定数据的写入。

例如，具有来自控制中心 611 的许可证的信息记录介质制造实体(DM ：盘制造者)603 可用的数据写入机制 612 具有一种结构，该结构例如执行存储对应于一具体 EKB 的制造盘数量的处理并将所述存储数据存储在一存储器中。

当需要时，控制中心 611 执行一检查，以验证与存储在数据写入机制 612 中的所制造盘的数量相关的数据。此外，它披露在对密钥信息(EKB)发出中心 604 和内容权利所有者(CO 内容所有者)602 进行检查过程中获得的与制造盘数量相关的数据。

另外，可以使用这样一种结构，在该结构中，数据写入机制 612 被配置得能够连续或间歇地与控制中心 611 或其它实体极性通信，以允许对下述情况执行监视，诸如是否按照规则执行盘制造或是否在制造比内容权利所有者(CO: 内容所有者)602 所要求更多数量的盘。

已经在上面参照优选实施例的具体例子描述了本发明。然而，显然本领域普通技术人员可以对所述具体实施例执行修改、替换、变更、组合或再组合而不脱离本发明的所述范围。换句话说，本发明已经以举例说明的形式公开了，并且不应该被解释为是对确定本发明的范围的限制。

应该注意，在本说明书中所描述的一系列处理都可以通过硬件或软件或两者的组合结构来执行。当用软件执行所述处理时，记录所述处理顺序的程序有可能被安装在结合进专用硬件的计算机存储器中以备执行，或者在能够

执行各种类型的处理的通用计算机中安装程序以备执行。

例如，所述程序可以被预先存储在作为记录介质的硬件或者 ROM（只读存储器）中。作为选择，所述程序可以被临时或者永久地存储（记录）在诸如是软磁盘、CD-ROM（密致盘只读存储器）、MO（磁光）盘、DVD（数字化视频盘）、磁盘和/或半导体存储器或者存储装置的可拆卸的记录介质内。可以在所谓的软件包内提供这种可拆卸记录介质。

应该注意到，如上所述从可拆卸记录介质安装到一计算机上，所述程序可以无线地从一下载站点发送给计算机、或利用线路经过诸如 LAN（局域网）和因特网之类的网络发送给计算机，并且计算机可以接收如此发送的所述程序并把其安装在诸如内置的硬盘等的记录介质上。

同样地，在所述说明书中描述的各种类型的处理，不仅可以根据描述按照时间序列被执行，而且可以并行或独立地根据执行所述处理的装置的处理性能或按要求执行。此外，在说明书中，所述系统是一种多个装置的逻辑设置结构，并且各个结构的装置并不限于相同的外壳。

如上所述，根据本发明的所述结构，信息记录介质制造实体（DM：盘制造者）103 被结构成向密钥信息（EKB）发出中心发送密钥信息（EKB）发出请求，其中所述密钥信息（EKB）发出请求是根据由内容权利所有者（CO：内容所有者）102 所发出的信息记录介质（盘）制造请求（DMR：盘制造请求）创建的，在所述密钥信息（EKB）发出中心验证所述密钥信息（EKB）发出请求。换句话说，验证密钥信息（EKB）发出请求是否是对应于已授权信息记录介质（盘）制造请求（DMR：盘制造请求）的已授权请求数据，并且如果满足了该验证，就发出将要存储在信息记录介质上的所述密钥信息（EKB）的密钥信息。因此，对于从非法途径获取的内容来说，不可能从所述密钥信息（EKB）发出中心获取密钥信息（EKB），不可能存储对应于将要存储在所述信息记录介质上的加密内容的密钥信息（EKB），并且预防了制造存储非法获取的内容的盘，从而使该应用能够作为一种在信息记录介质的制造处理中的控制系统和方法，其中所述信息记录介质把内容作为数字数据来记录，诸如基于 CD、DVD、MD 或蓝色激光执行数据记录处理的盘装置。单个处理过程，可以应用在内容存储信息记录介质的制造和控制中所涉及的每个实体的信息处理装置中，诸如内容提供实体、信息记录介质的制造实体、并提供密钥信息的实体。

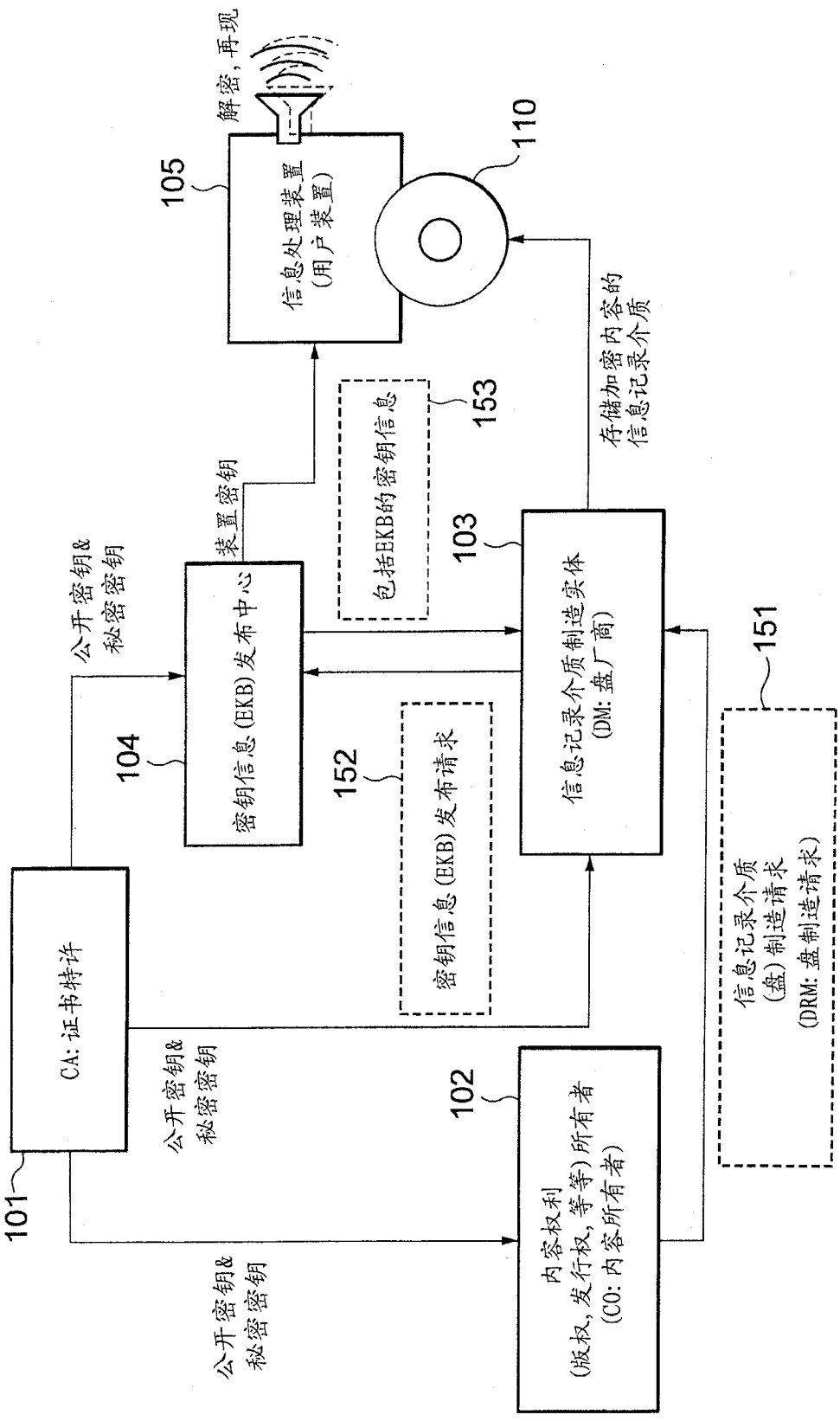

CA: 证书特许
101
公开密钥&
秘密密钥
公开密钥&
秘密密钥
104
密钥信息(EKB)发布中心
装置密钥
公开密钥&
秘密密钥
102
内容权利
(版权,发行权,等等)所有者
(CO: 内容所有者)
密钥信息(EKB)发布请求
152
包括EKB的密钥信息
153
103
信息记录介质制造实体
(DM: 盘厂商)
存储加密内容的
信息记录介质
151
信息记录介质
(盘)制造请求
(DRM: 盘制造请求)
110
105
信息处理装置
(用户装置)
解密,再现

图 1

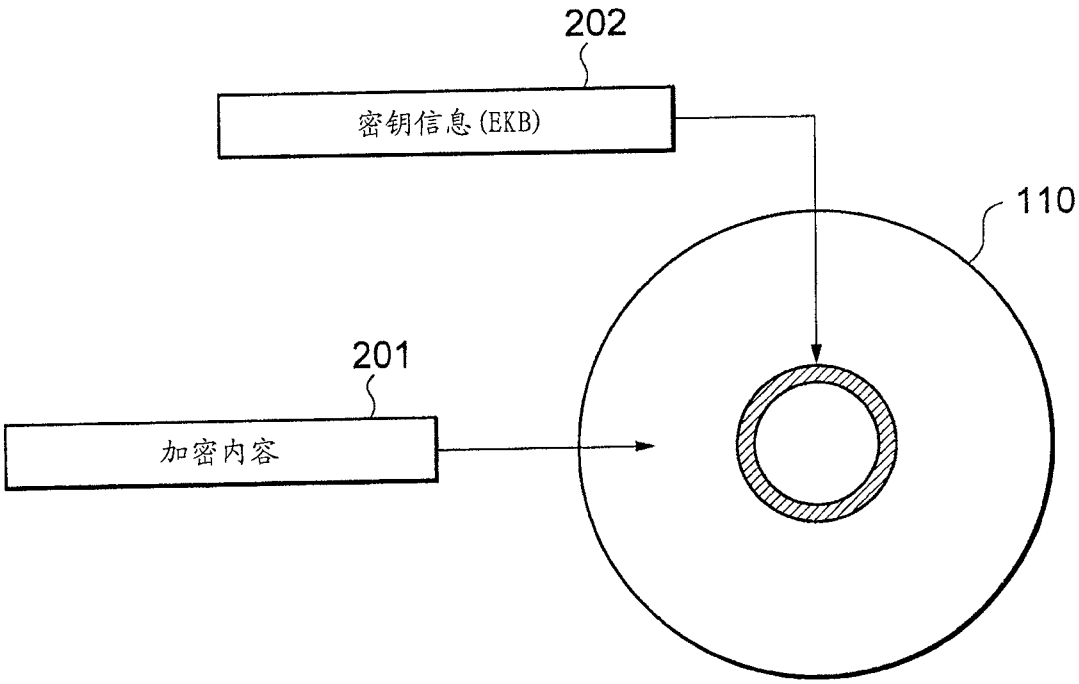


图 2

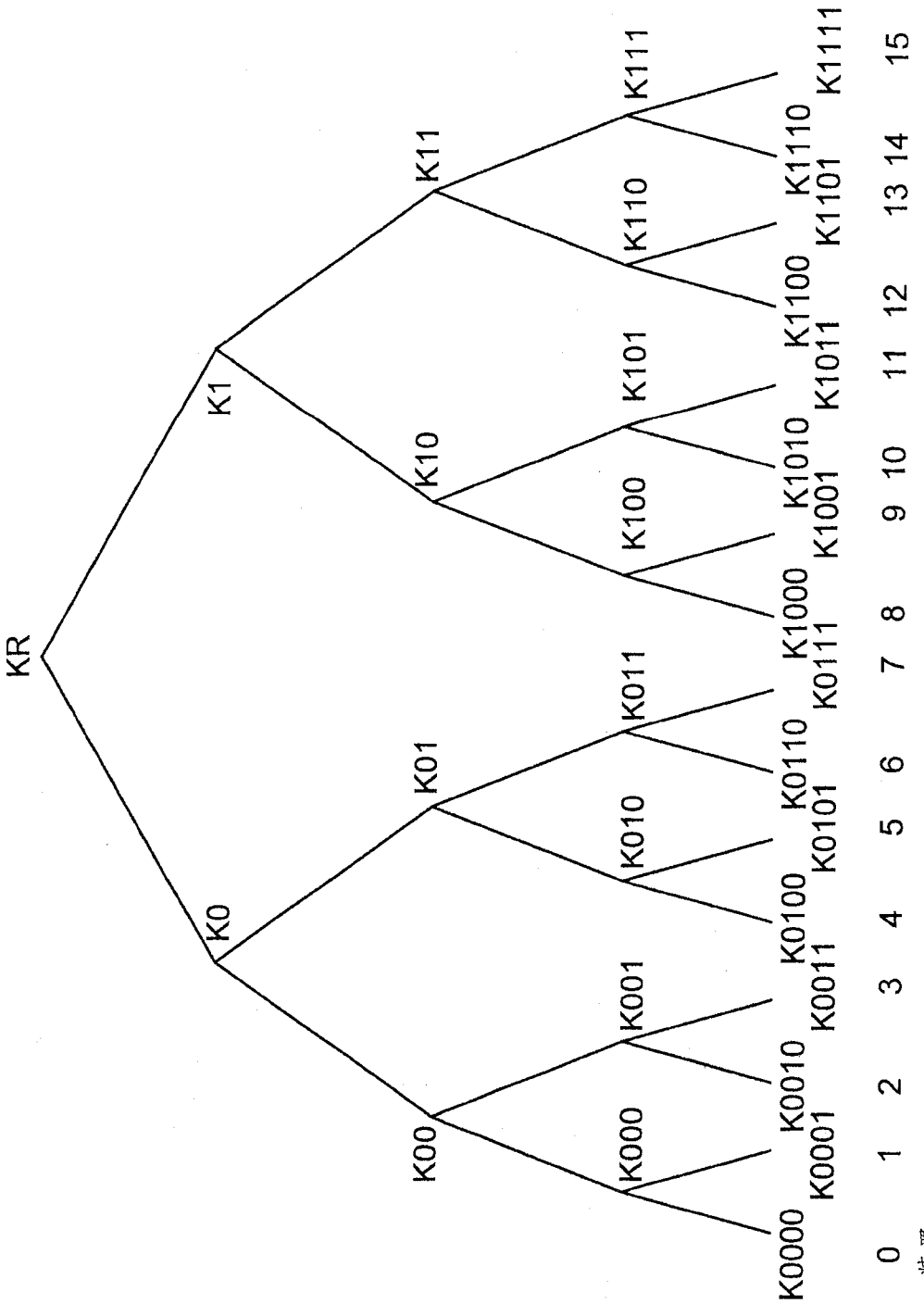

KR
K0
K1
K00
K01
K10
K11
K000
K001
K010
K011
K100
K101
K110
K111
K0000
K0001
K0010
K0011
K0100
K0101
K0110
K0111
K1000
K1001
K1010
K1011
K1100
K1101
K1110
K1111
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
装置

图 3

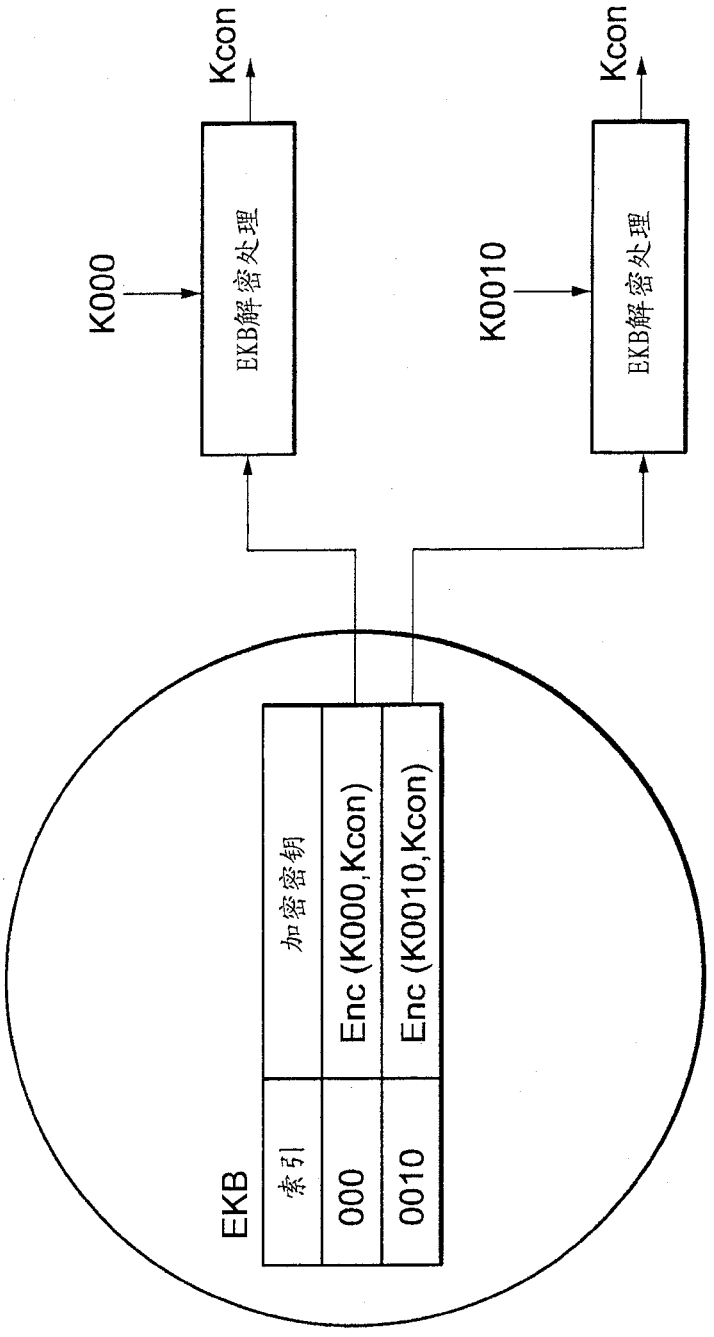

Kcon
Kcon
K000
K0010
EKB解密处理
EKB解密处理
EKB
索引
加密密钥
000
Enc (K000,Kcon)
0010
Enc (K0010,Kcon)
记录介质

图 4

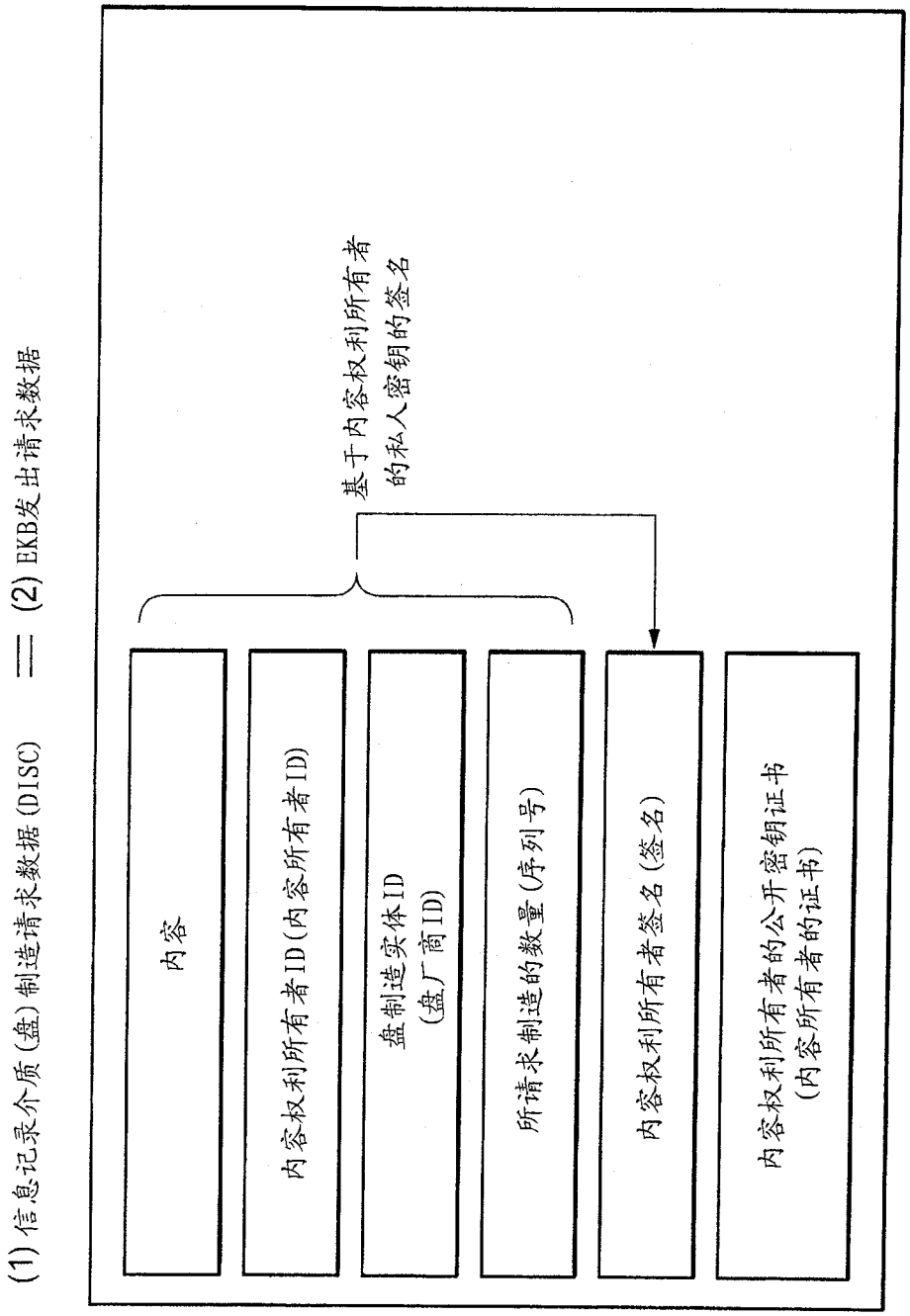

(1) 信息记录介质(盘)制造请求数据(DISC)
(2) EKB发出请求数据
内容
内容权利所有者ID(内容所有者ID)
盘制造实体ID
(盘厂商ID)
所请求制造的数量(序列号)
内容权利所有者签名(签名)
内容权利所有者的公开密钥证书
(内容所有者的证书)
基于内容权利所有者
的私人密钥的签名

图 5

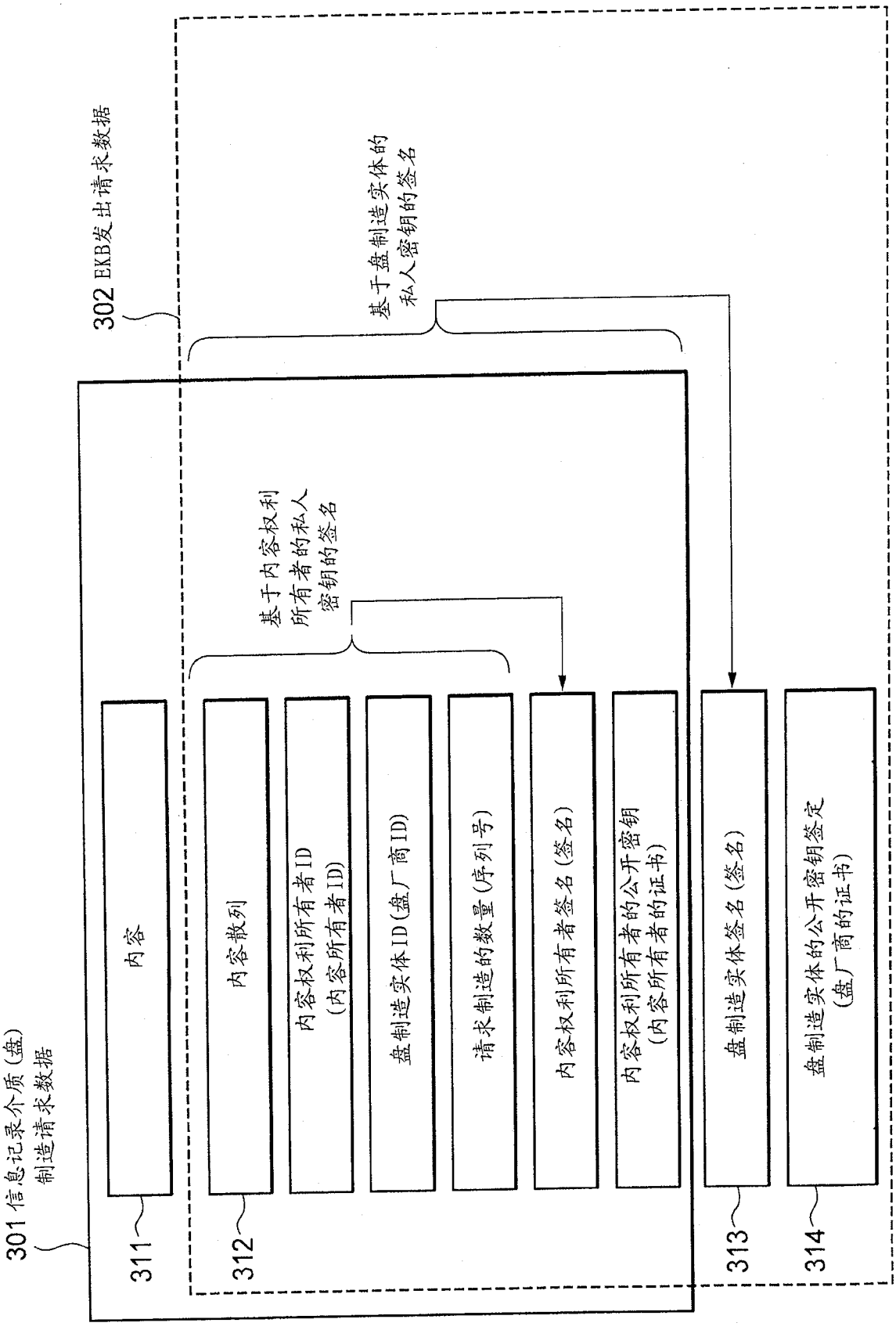

301 信息记录介质(盘)
制造请求数据
302 EKB发出请求数据
基于盘制造实体的
私人密钥的签名
基于内容权利
所有者的私人
密钥的签名
311
内容
312
内容散列
内容权利所有者ID
(内容所有者ID)
盘制造实体ID(盘厂商ID)
请求制造的数量(序列号)
内容权利所有者签名(签名)
内容权利所有者的公开密钥
(内容所有者的证书)
313
盘制造实体签名(签名)
314
盘制造实体的公开密钥签定
(盘厂商的证书)

图 6

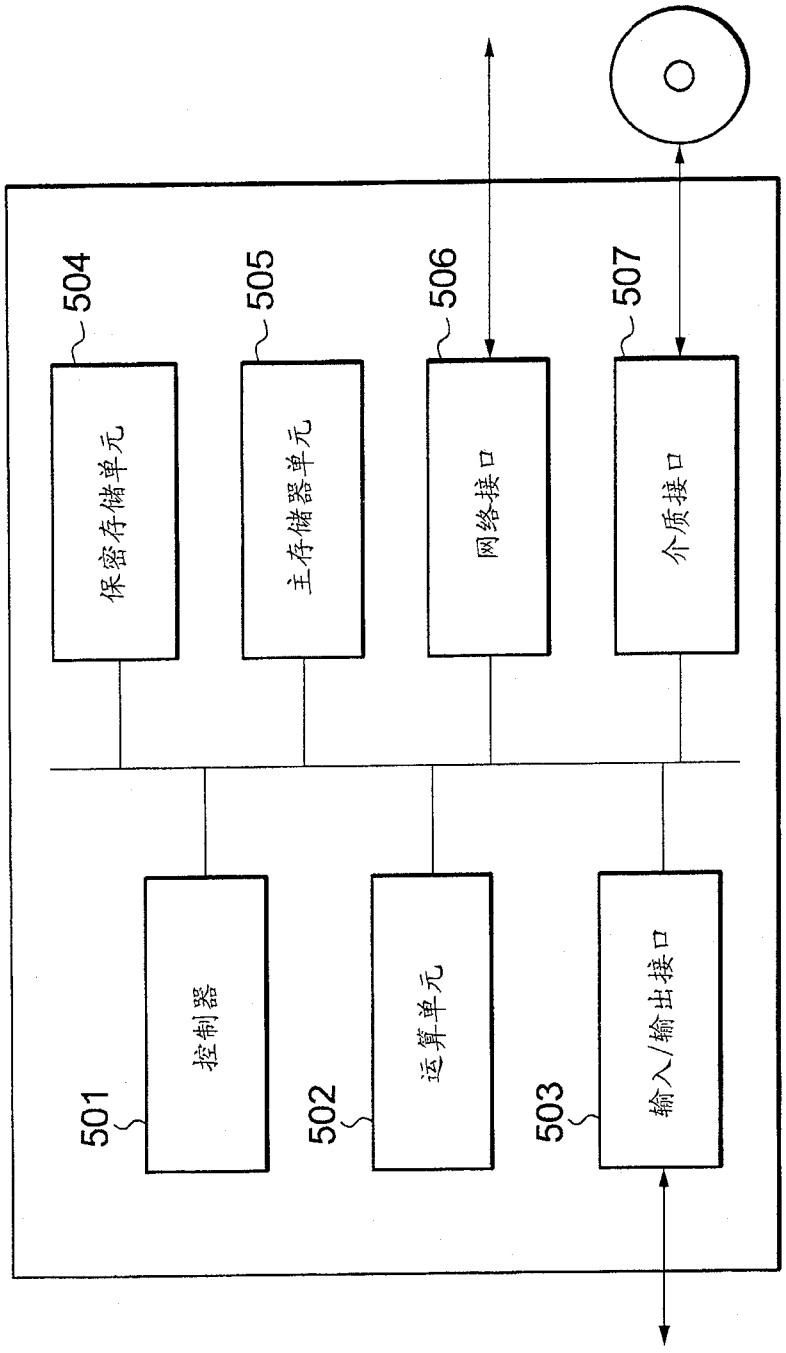

504
505
506
507
保密存储单元
主存储器单元
网络接口
介质接口
501
502
503
控制器
运算单元
输入/输出接口

图 7

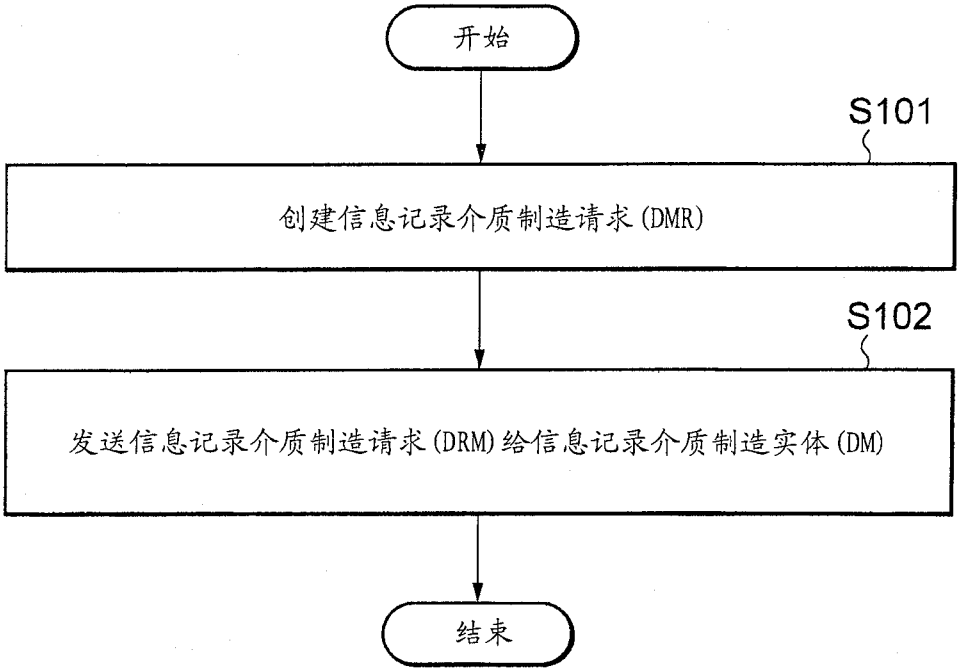

开始
S101
创建信息记录介质制造请求(DMR)
S102
发送信息记录介质制造请求(DRM)给信息记录介质制造实体(DM)
结束

图 8

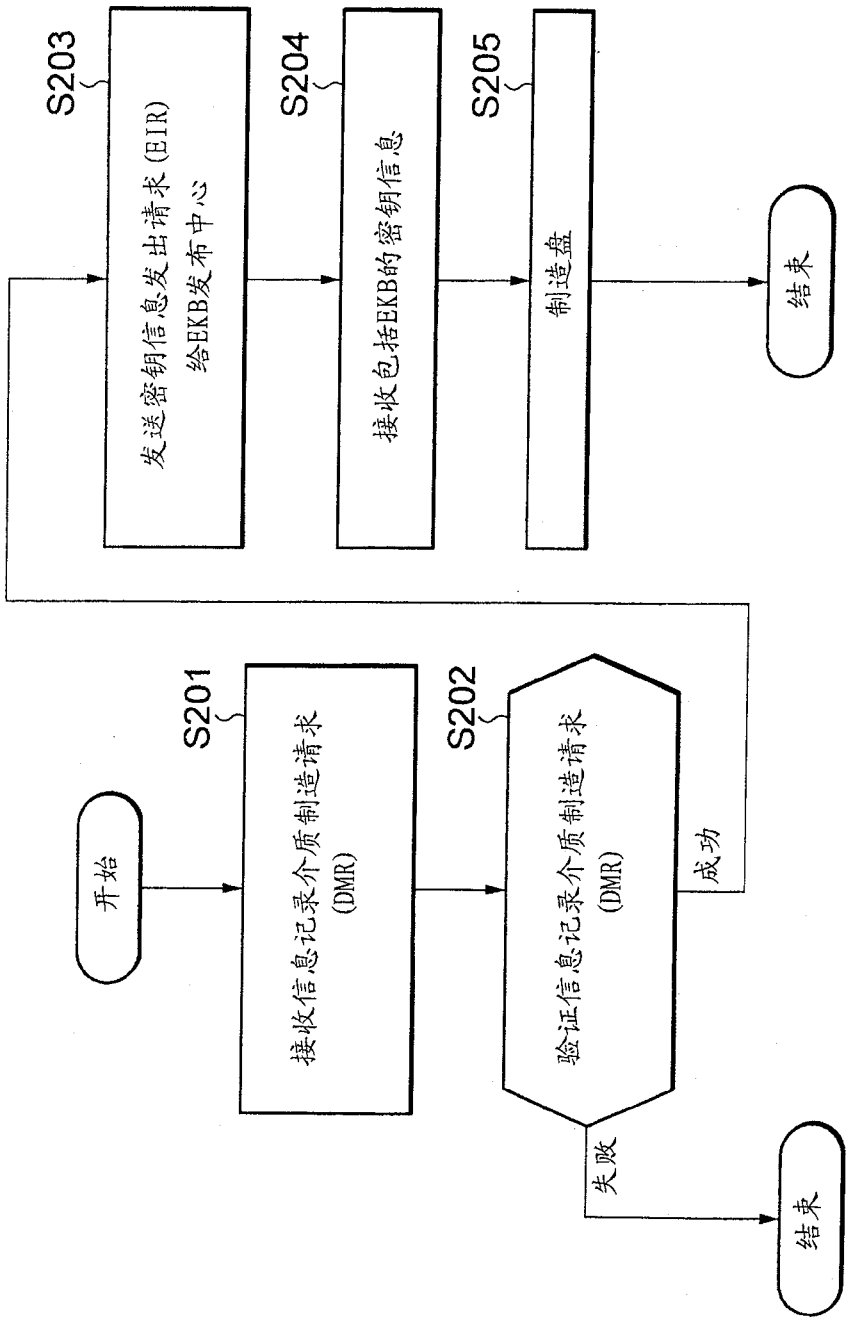

开始
S201
接收信息记录介质制造请求
(DMR)
S202
验证信息记录介质制造请求
(DMR)
失败
成功
结束
S203
发送密钥信息发出请求(EIR)
给EKB发布中心
S204
接收包括EKB的密钥信息
S205
制造盘
结束

图 9

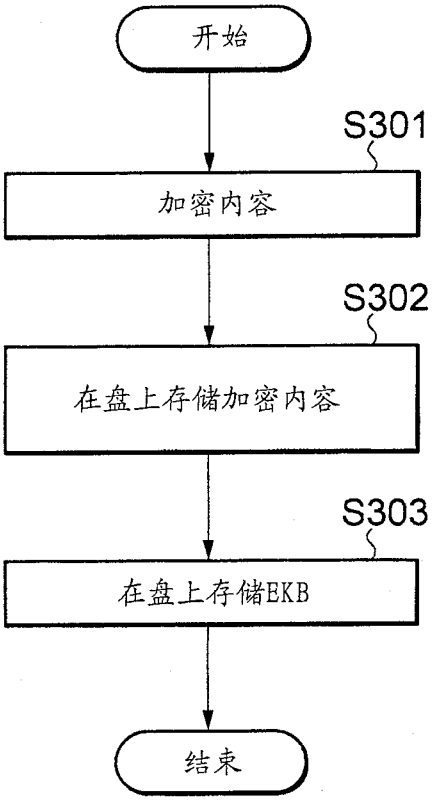


图 10

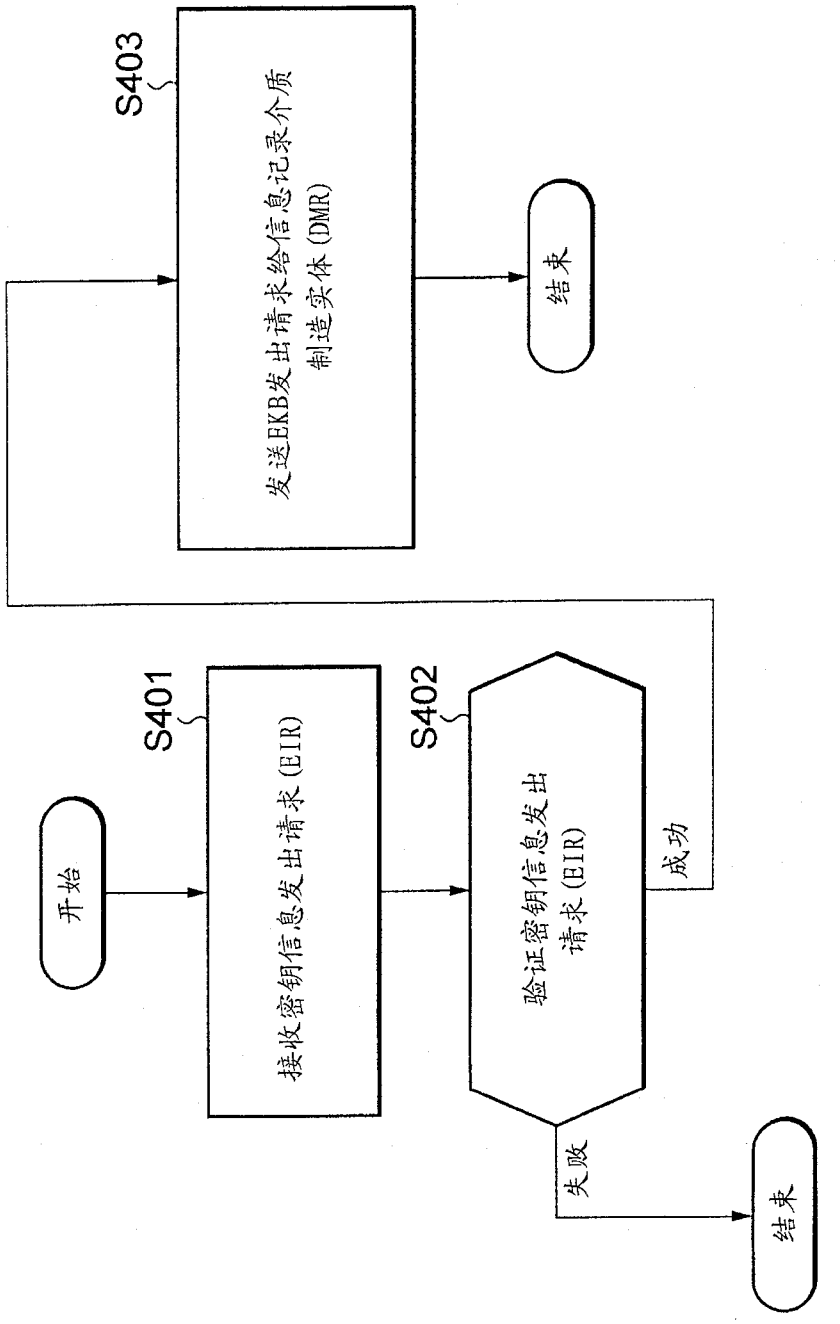

开始
S401
接收密钥信息发出请求 (EIR)
S402
验证密钥信息发出请求 (EIR)
成功
失败
结束
S403
发送EKB发出请求给信息记录介质制造实体 (DMR)
结束

图 11

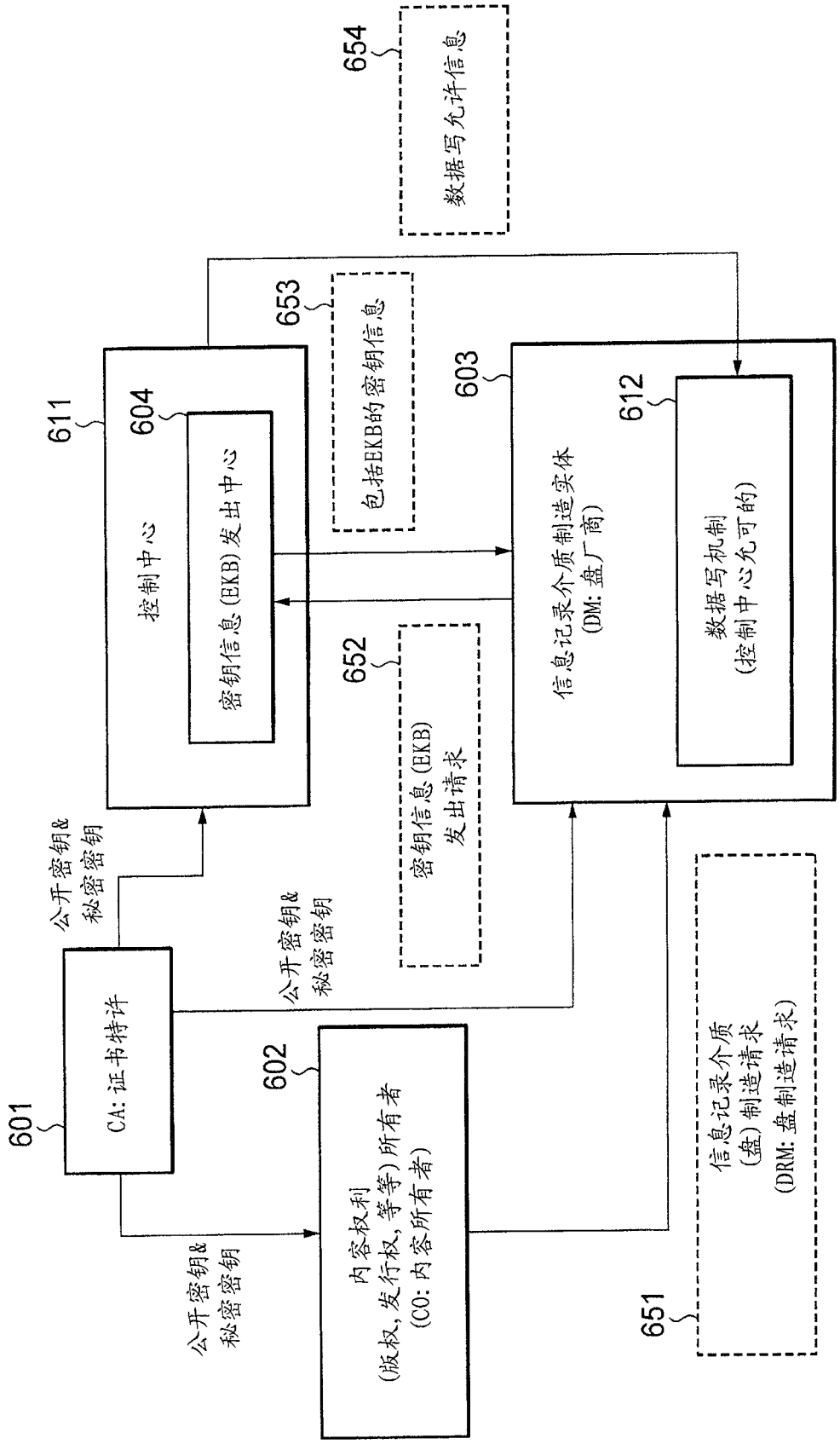

654
数据写允许信息
653
包括EKB的密钥信息
611
604
控制中心
密钥信息(EKB)发出中心
603
612
信息记录介质制造实体
(DM:盘厂商)
数据写机制
(控制中心允可的)
652
密钥信息(EKB)
发出请求
公开密钥&
秘密密钥
601
CA:证书特许
602
内容权利
(版权,发行权,等等)所有者
(CO:内容所有者)
651
信息记录介质
(盘)制造请求
(DRM:盘制造请求)

图 12

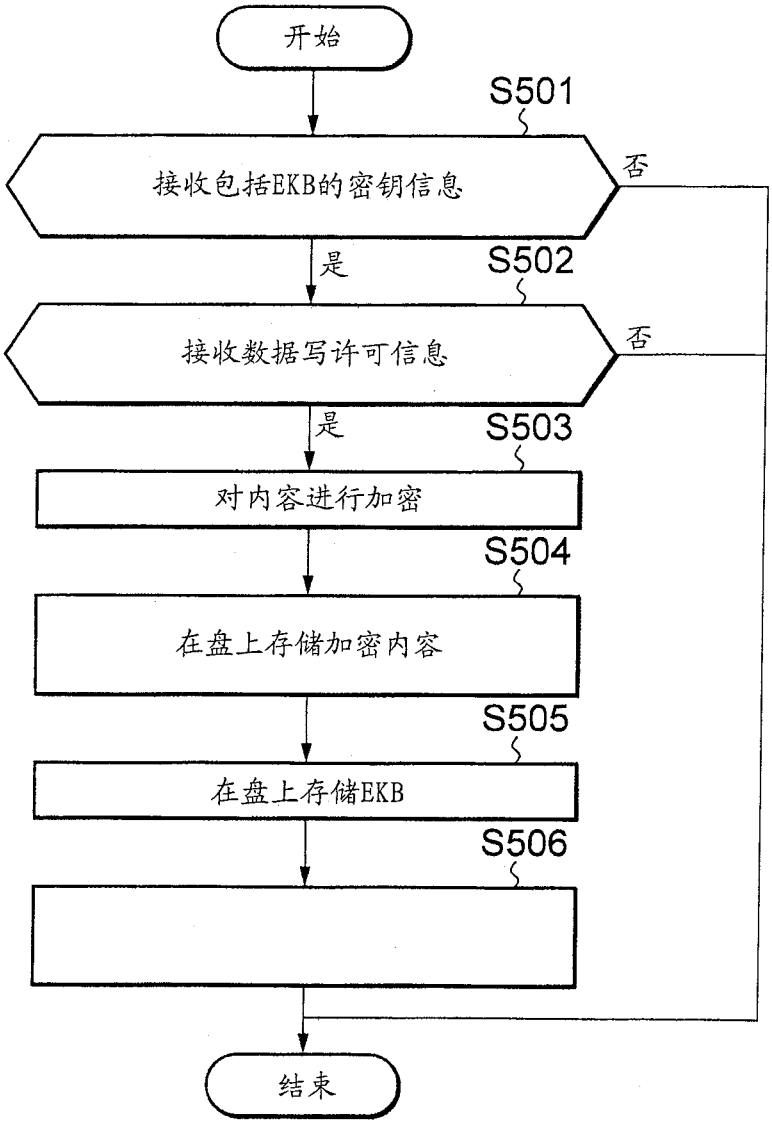

开始
S501
接收包括EKB的密钥信息
否
是
S502
接收数据写许可信息
否
是
S503
对内容进行加密
S504
在盘上存储加密内容
S505
在盘上存储EKB
S506
结束

图 13