[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
*G11B 20/10* (2006.01)
*H04L 9/08* (2006.01)
*G06F 12/14* (2006.01)

[12] 发明专利说明书

专利号 ZL 02803093.1

[45] 授权公告日 2008 年 5 月 28 日

[11] 授权公告号 CN 100390892C

[22] 申请日 2002.9.3 [21] 申请号 02803093.1

[30] 优先权

[32] 2001.9.14 [33] JP [31] 280191/2001

[86] 国际申请 PCT/JP2002/008918 2002.9.3

[87] 国际公布 WO2003/025930 日 2003.3.27

[85] 进入国家阶段日期 2003.5.30

[73] 专利权人 索尼株式会社

地址 日本东京

[72] 发明人 佐古曜一郎 古川俊介 猪口达也

[56] 参考文献

JP2001-223654A 2001.8.17

JP7-245740A 1995.9.19

JP2001-216727A 2001.8.10

审查员 李 冰

[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 李德山

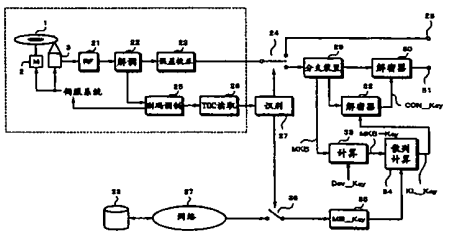
权利要求书 6 页 说明书 16 页 附图 6 页

[54] 发明名称

# 记录媒体的再现方法和设备及记录媒体的记录方法和设备

[57] 摘要

本发明公开了一种记录媒体的再现方法和设备及记录媒体的记录方法和设备。判断从记录媒体中已经读取的内容数据是否是加密的内容数据。在从记录媒体中已经读取的内容数据是加密的内容数据时以至少第一密钥数据(媒体结合密钥数据)和从记录媒体中已经读取的第二密钥数据(媒体密钥块)产生用于对从记录媒体中已经读取的经加密的内容密钥数据进行解密的第三密钥数据(密钥箱密钥数据)。以通过第三密钥数据已经解密的内容密钥数据对从记录媒体中已经读取的经加密的内容数据进行解密。



1. 一种记录媒体的再现方法，包括如下的步骤：

判断从记录媒体中已经读取的内容数据是否是经加密的内容数据；

在从记录媒体中已经读取的内容数据是经加密的内容数据时，以至少第一密钥数据、即媒体结合密钥数据和从记录媒体中已经读取的第二密钥数据、即媒体密钥数据，产生用于对从记录媒体中已经读取的经加密的内容密钥数据进行解密的第三密钥数据、即密钥箱密钥数据；以及

以通过第三密钥数据已经解密的内容密钥数据对从记录媒体中已经读取的经加密的内容数据进行解密。

2. 如权利要求1所述的记录媒体的再现方法，

其中通过如下的步骤执行第三密钥产生步骤：

以第二密钥数据和再现装置唯一的密钥数据、即装置密钥数据产生进一步的密钥数据（MKB_Key）；和

对所产生的进一步的密钥数据和第一密钥数据执行计算处理。

3. 如权利要求2所述的记录媒体的再现方法，

其中第一密钥数据是通过常规再现装置能够从记录媒体中读取的密钥数据。

4. 如权利要求2所述的记录媒体的再现方法，

其中第一密钥数据是通过常规再现装置不能够读取的密钥数据。

5. 如权利要求1所述的记录媒体的再现方法，进一步包括如下的步骤：

在第一密钥数据还没有通过再现装置从记录媒体中读取时通过网络从外部获得第一密钥数据。

6. 如权利要求1所述的记录媒体的再现方法，

其中将内容数据识别为经加密的内容数据的识别数据已经记录在记录媒体上，并且

其中该方法进一步包括如下的步骤;

根据从记录媒体中已经读取的识别数据判断从记录媒体中已经读取的内容数据是否是经加密的数据。

7. 如权利要求1所述的记录媒体的再现方法，进一步包括如下的步骤:

根据版权管理数据控制解密的内容数据的输出。

8. 如权利要求1所述的记录媒体的再现方法，进一步包括如下的步骤:

对从记录媒体已经读取的数据执行再现信号处理并在从记录媒体中已经读取的内容数据是非加密的内容数据时输出结果信号。

9. 一种记录媒体的再现设备，包括:

用于从记录媒体中读取数据的头部部分，在该记录媒体上至少已经记录了数据和将该数据识别为经加密的数据的识别数据;

再现信号处理部分，其用于对头部部分的输出数据执行再现信号处理;

判断部分，其用于根据识别数据判断从记录媒体中已经读取的数据是否是经加密的数据;

解密处理部分，其用于接收再现信号处理部分的输出数据;以至少第一密钥数据、即媒体密钥块和从记录媒体中已经读取的第二密钥数据、即媒体结合密钥数据，产生用于对从记录媒体中已经读取的经加密的内容密钥数据进行解密的第三密钥数据、即密钥箱密钥数据;以及以通过第三密钥数据已经解密的内容密钥数据对从记录媒体中已经读取的经加密的内容数据进行解密。

10. 如权利要求9所述的记录媒体的再现设备，

其中解密处理部分被构造成以第二密钥数据和再现装置唯一的密钥数据、即装置密钥数据产生进一步的密钥数据（MKB_Key），并且对所产生的进一步的密钥数据和第一密钥数据执行计算处理以产生第三密钥数据。

11. 如权利要求9所述的记录媒体的再现设备，

其中第一密钥数据是通过常规再现装置能够从记录媒体中读取的密钥数据。

12. 如权利要求 9 所述的记录媒体的再现设备，

其中第一密钥数据是通过常规再现装置不能够读取的密钥数据。

13. 如权利要求 9 所述的记录媒体的再现设备，

其中在第一密钥数据还没有通过再现装置从记录媒体中读取时通过网络从外部获得第一密钥数据。

14. 如权利要求 9 所述的记录媒体的再现设备，

其中解密处理部分被构造成根据版权管理数据控制解密的内容数据的输出。

15. 如权利要求 9 所述的记录媒体的再现设备，进一步包括：

输出端，

其中在判断部分已经判断已经从记录媒体中读取的内容数据是非加密的内容数据时，将再现信号处理部分的输出数据输送给输出端。

16. 如权利要求 9 所述的记录媒体的再现设备，进一步包括：

输出端，和

根据判断部分的判断结果来控制的开关电路，

其中在判断部分已经判断已经从记录媒体中读取的内容数据是经加密的内容数据时，操作开关电路以使再现信号处理部分的输出数据输送给解密处理部分，并且

其中在判断部分已经判断已经从记录媒体中读取的内容数据是非加密的内容数据时，操作开关电路以使再现信号处理部分的输出数据输送给输出端。

17. 一种记录媒体的记录方法，包括如下的步骤：

判断所提供的内容数据是否是需要加密的内容数据，并在该判断结果表示所提供的内容数据是需要加密的内容数据时，通过内容密钥数据加密所提供的内容数据；

以至少以第一密钥数据（MB_Key）和记录在记录媒体中的第二密钥数据（MKB）产生的第三密钥数据（KL_Key）对内容密钥数据

进行加密；和

记录经加密的内容数据、经加密的内容密钥数据和用于将内容数据识别为经加密的内容数据的识别数据。

18. 如权利要求 17 所述的记录媒体的记录方法，进一步包括如下的步骤：

以第二密钥数据和记录媒体的再现装置唯一的密钥数据、即装置密钥数据产生进一步的密钥数据（MKB_Key），并对进一步的密钥数据和第一密钥数据执行计算处理以产生第三密钥数据。

19. 如权利要求 17 所述的记录媒体的记录方法，

其中第一密钥数据是通过常规的记录媒体再现装置能够从记录媒体中读取的密钥数据。

20. 如权利要求 17 所述的记录媒体的记录方法，

其中第一密钥数据是通过常规的记录媒体再现装置不能够从记录媒体读取的密钥数据。

21. 如权利要求 17 所述的记录媒体的记录方法，进一步包括如下的步骤：

通过网络从外部获得第一密钥数据。

22. 如权利要求 17 所述的记录媒体的记录方法，进一步包括如下的步骤：

对用于将记录在记录媒体上的内容数据识别为非加密的数据的识别数据和所提供的内容数据执行信号处理，并在判断结果表示所提供的内容数据是不需要加密的内容数据时将结果信号记录在记录媒体上。

23. 一种记录媒体的记录设备，包括：

判断部分，其用于判断所提供的内容数据是否是需要加密的内容数据；

加密处理部分，其用于在该判断部分已经判断所提供的内容数据是需要加密的内容数据时，以内容密钥数据对所提供的内容数据进行加密，并以至少以第一密钥数据（MB_Key）和记录在记录媒体中的

第二密钥数据（MKB）产生的第三密钥数据（KL_Key）对内容密钥数据进行加密；和

记录部分，其用于对从加密处理部分中已经输出的经加密的内容数据、经加密的内容密钥数据和用于将内容数据识别为经加密的内容数据的识别数据执行信号处理，并将结果信号记录在记录媒体上。

24. 如权利要求 23 所述的记录媒体的记录设备，

其中加密处理部分被构造成以第二密钥数据和记录媒体的再现装置唯一的密钥数据、即装置密钥数据产生进一步的密钥数据（MKB_Key），并对所产生的进一步的密钥数据和第一密钥数据执行计算处理以产生第三密钥数据。

25. 如权利要求 23 所述的记录媒体的记录设备，

其中第一密钥数据是通过常规的再现装置能够从记录媒体中读取的密钥数据。

26. 如权利要求 23 所述的记录媒体的记录设备，

其中第一密钥数据是通过常规再现装置不能够读取的密钥数据。

27. 如权利要求 23 所述的记录媒体的记录设备，

其中加密处理部分被构造成通过网络从外部获得第一密钥数据。

28. 如权利要求 23 所述的记录媒体的记录设备，

其中记录部分被构造成在该判断部分已经判断所提供的内容数据是不需要加密的内容数据时，对用于将记录在记录媒体上的内容数据识别为非加密的内容数据的识别数据和所提供的内容数据执行信号处理，并将结果信号记录在记录媒体上。

29. 一种记录媒体的再现方法，包括如下的步骤：

以至少第一密钥数据、即媒体结合密钥数据和从记录媒体中已经读取的第二密钥数据、即媒体密钥块产生用于对从记录媒体中已经读取的经加密的内容密钥数据进行解密的第三密钥数据、即密钥箱密钥数据；以及

通过以第三密钥数据已经解密的内容密钥数据对从记录媒体中已经读取的经加密的内容数据进行解密。

30. 如权利要求 29 所述的记录媒体的再现方法，

其中以第二密钥数据和再现装置唯一的密钥数据、即装置密钥数据产生进一步的密钥数据（MKB_Key），并对所产生的进一步的密钥数据和第一密钥数据执行计算处理以产生第三密钥数据。

31. 如权利要求 30 所述的记录媒体的再现方法，

其中第一密钥数据是通过常规的再现装置能够从记录媒体中读取的密钥数据。

32. 如权利要求 30 所述的记录媒体的再现方法，

其中第一密钥数据是通过常规再现装置不能够读取的密钥数据。

# 记录媒体的再现方法和设备及记录媒体的记录方法和设备

## 技术领域

本发明涉及允许使用加密保持安全性的记录媒体的再现方法和再现设备和记录媒体的记录方法和记录设备。

## 背景技术

根据 MP3（MPEG1 声频层 III）已经压缩的记录在 CD（光盘）上的音乐信息的数字数据的内容发布在因特网上。从 CD 中读取的数据拷贝到 CD-R（可记录的 CD）盘上。 此外，已经广泛地使用由 Napster（一家美国公司）提供的对等式音乐文件交换服务。结果，近年来，版权保护（在下文中有时称为安全性）的问题已经引起了人们的注意。因此，在近年来已经提出的新型媒体（比如对应于 SACD（超音频 CD）和 DVD（数字通用盘或数字视频盘）声频标准的光盘、存储器卡等）中，对内容数据进行加密以保持内容的安全性。例如，存储器卡使用快速存储器并可连接到设备和从该设备取下。在试图将加密的音乐数据记录在存储器卡中时，该设备和存储器卡彼此进行验证。仅在它们彼此成功地验证了时，才可以将经加密的数据记录到存储器卡中。

为防止非法地获取或拷贝记录在 CD 上的数据，已经设计出了与常规的 CD 具有相同的物理结构并使用拷贝保护装置的新型媒体。在这种新型的媒体中，将结合在该媒体中的隐藏密钥数据记录在其中以便防止数据不被按位拷贝。

只有那些能够处理新型媒体的设备才可以读取密钥数据。因此，虽然充分地保持了数据的安全性（版权保护），但是由于许多常规的 CD 播放器不能读取密钥数据，因此它们不能从新型媒体中再现内容

数据。因此，为使用这种新型的媒体，用户必须购买处理新型媒体的记录器/播放器。因此，给用户添加了包括经济负担的新负担。这种负担阻碍了新型媒体的广泛使用。

因此，本发明的一个目的是提供一种记录媒体的再现方法和再现设备和记录媒体的记录方法和记录设备，它们允许使用结合在媒体中的密钥具有全面安全性功能的新型媒体、驱动器等容易引入。

发明内容

为实现前述的目的，本发明的技术方案1是一种记录媒体的再现方法，包括如下的步骤：

判断从记录媒体中已经读取的内容数据是否是经加密的内容数据；

在从记录媒体中已经读取的内容数据是经加密的内容数据时，以至少第一密钥数据（媒体结合密钥数据）和从记录媒体中已经读取的第二密钥数据（媒体密钥数据），产生用于对从记录媒体中已经读取的经加密的内容密钥数据进行解密的第三密钥数据（密钥箱密钥数据）；以及

以通过第三密钥数据已经解密的内容密钥数据对从记录媒体中已经读取的经加密的内容数据进行解密。

本发明的技术方案9是一种记录媒体的再现设备，包括：

用于从记录媒体中读取数据的头部部分，在该记录媒体上至少已经记录了数据和将该数据识别为经加密的数据的识别数据；

再现信号处理部分，其用于对头部部分的输出数据执行再现信号处理；

判断部分，其用于根据识别数据判断从记录媒体中已经读取的数据是否是经加密的数据；

解密处理部分，其用于接收再现信号处理部分的输出数据；以至少第一密钥数据（媒体密钥块）和从记录媒体中已经读取的第二密钥数据（媒体结合密钥数据），产生用于对从记录媒体中已经读取的经

加密的内容密钥数据进行解密的第三密钥数据（密钥箱密钥数据）；以及以通过第三密钥数据已经解密的内容密钥数据对从记录媒体中已经读取的经加密的内容数据进行解密。

本发明的技术方案 17 是一种记录媒体的记录方法，包括如下的步骤：

判断所提供的内容数据是否是需要加密的内容数据，并在该判断结果表示所提供的内容数据是需要加密的内容数据时，通过内容密钥数据对所提供的内容数据进行加密；

以至少以第一密钥数据（MB_Key）和记录在记录媒体中的第二密钥数据（MKB）产生的第三密钥数据（KL_Key）对内容密钥数据进行加密；和

记录经加密的内容数据、经加密的内容密钥数据和用于将内容数据识别为经加密的内容数据的识别数据。

本发明的技术方案 23 是一种记录媒体的记录设备，包括：

判断部分，其用于判断所提供的内容数据是否是需要加密的内容数据；

加密处理部分，其用于在该判断部分已经判断所提供的内容数据是需要加密的内容数据时，以内容密钥数据对所提供的内容数据进行加密，并以至少以第一密钥数据（MB_Key）和记录在记录媒体中的第二密钥数据（MKB）产生的第三密钥数据（KL_Key）对内容密钥数据进行加密；和

记录部分，其用于对从加密处理部分中已经输出的经加密的内容数据、经加密的内容密钥数据和用于将内容数据识别为经加密的内容数据的识别数据执行信号处理，并将结果信号记录在记录媒体上。

本发明的技术方案 29 是一种记录媒体的再现方法，包括如下的步骤：

以至少第一密钥数据（媒体结合密钥数据）和从记录媒体中已经读取的第二密钥数据（媒体密钥块）产生用于对从记录媒体中已经读取的经加密的内容密钥数据进行解密的第三密钥数据（密钥箱密钥数据）；以及

通过以第三密钥数据已经解密的内容密钥数据对从记录媒体中已经读取的经加密的内容数据进行解密。

附图说明

附图1所示为简要解释根据本发明的加密系统的示意图;

附图2所示为说明根据本发明的一种实施例的记录设备的结构的实例的方块图;

附图3所示为说明根据本发明的实施例的记录操作的过程的流程图;

附图4所示为说明根据本发明的实施例的再现设备的结构的实例的方块图; 以及

附图5所示为说明根据本发明的实施例的再现操作的过程的流程图。

具体实施方式

接着, 描述本发明的一种实施例。该实施例是本发明用于新型光盘的一种实例。接着, 参考附图1, 简要地描述光盘D的安全性(版权保护)系统。在包括尺寸的物理标准方面该光盘与市场上可购买的CD几乎相同。因此, 通过常规的再现设备比如CD播放器可以光学地读取记录在光盘D上的数据。但是, 与CD不同的是, 经加密的内容数据已经记录在光盘D上。经加密的内容数据例如是对应于例如CD-ROM格式或CD-DA(数字声频)格式或图形的已经加密的声频数据。作为加密的方法, 可以使用DES(数据加密标准)等。在需要时, 根据ATRAC(自适应变换声编码)、MP3(MPEG1声频层III)、TwinVQ(变换域加权隔行矢量量化)等已经对作为内容数据的声频数据进行压缩和编码。

除了经加密的内容数据、内容密钥数据、关于DRM(数字权利管理)的数据、媒体结合密钥数据MB_Key和媒体密钥块数据MKB已经记录在光盘D上。关于DRM的数据是指定如何处理内容数据、

已经拷贝了内容数据多少次、是否再现或拷贝了内容数据的管理数据以及拷贝的内容数据的产生的管理数据。内容密钥数据和关于 DRM 的数据已经加密并记录在光盘 D 上。

通过解密器 51 以内容密钥数据 CON_Key 对通过光学拾取器(未示)从光盘 D 中读取的经加密的内容数据进行解密。经解密的内容数据从解密器 51 中输出。在通过解密器 51 对经加密的内容数据进行解密时，抽取关于 DRM 的数据。与关于 DRM 的数据相对应，控制从解密器 51 中输出的经解密的内容数据。结果，限制经解密的内容数据的再现和拷贝。通过光学拾取器（未示）从光盘 D 中读取的内容密钥数据和关于 DRM 的数据输送给解密器 52。解密器 52 使用密钥箱密钥数据 KL_Key 对内容数据和关于 DRM 的数据进行解密并获得作为输出数据的内容密钥数据 CON_Key。

散列（hash）计算部分 53 使用媒体结合密钥数据 MB_Key、媒体密钥块数据 MKB 和装置密钥数据 DEV_Key 产生密钥箱密钥数据 KL_Key。装置密钥数据 DEV_Key 是将内容数据记录到光盘 D 或从光盘 D 再现内容数据的记录和/或再现设备唯一的或者安装到从光盘 D 中再现内容数据的个人计算机的应用软件唯一的密钥数据。处理光盘 D 的记录和/或再现设备具有装置密钥数据 DEV_Key。装置密钥数据 DEV_Key 是输出到该设备的外面并传输给另一设备的密钥数据。

媒体结合密钥数据 MB_Key 是常规的 CD 播放器、常规的 CD 驱动器或常规的应用软件不能再现的密钥数据。媒体结合密钥数据 MB_Key 具有预定的位长。媒体结合密钥数据 MB_Key 意味着以结合在其中的方式记录在光盘 D 上的密钥数据。媒体结合密钥数据 MB_Key 已经嵌入在光盘 D 上以使在 CD 驱动器等从光盘 D 再现内容数据时 CD 驱动器等不能从光盘 D 中读取媒体结合密钥数据 MB_Key。相反，前述的能够将内容数据记录到光盘 D 或从光盘 D 再现内容数据的记录和/或再现设备等能够从光盘 D 中读取媒体结合密钥数据 MB_Key。在实际中，以形成在光盘 D 上的凹坑的变形表示的密钥数据、以凹坑的摆动表示的密钥数据或者以 EFM 调制的组合位（三位）

表示的密钥数据是媒体结合密钥数据 MB_Key。

通过光学拾取器（未示）已经从光盘 D 中读取的媒体结合密钥数据 MB_Key 输送给散列计算部分 53。同样地，已经从光盘 D 中读取的媒体密钥块数据 MKB 输送给计算部分 54。与媒体结合密钥数据 MB_Key 不同的是，通过常规的 CD 驱动器等能够从光盘 D 中读取媒体密钥块数据 MKB。存储在该设备的控制器等中的装置密钥数据 DEV_Key 输送给计算部分 54。计算部分 54 计算媒体密钥块数据 MKB 和装置密钥数据 DEV_Key 并产生密钥数据 MKB_Key。将内容数据记录到光盘 D 并从光盘 D 再现内容数据的不同的记录和/或再现设备产生相同的密钥数据 MKB_Key。散列计算部分 53 获得媒体结合密钥数据 MB_Key 和密钥数据 MKB_Key 的散列值作为密钥箱密钥数据 KL_Key。散列计算部分 53 将密钥箱密钥数据 KL_Key 输送给解密器 52。应用密钥箱密钥数据 KL_Key，解密器 52 对内容密钥数据和关于 DRM 的数据假像解密并获得内容密钥数据 CON_Key。

光盘 D 的实例有只读（ROM）型、写一次型和可重写型光盘 D。在附图 1 中，光盘 D 是多对话（multi-session）型光盘。在光盘 D 的径向方向上将光盘 D 的记录区域划分为两部分。这两部分的内周边侧是在其中可以记录非加密的内容数据（即明码内容数据）和加密的数据中的一种的第一话路 P1。这两部分的外周边侧是在其中可以记录在第一话路 P2 中没有记录的非加密的内容数据（明码内容数据）或经加密的数据的第二话路 P2。每个话路由导入区、程序区和导出区构成。在导入区中，记录了在节目区中记录的内容数据的管理数据、识别光盘 D 的类型的标识符数据等。在程序区中记录内容数据。导出区设置在程序区的外周边侧上。

附图 2 所示为根据本发明的记录设备的实例。在附图 2 中所示的记录设备并不限于专用的硬件。可替换的是，该记录设备可以通过已经安装了专用软件的个人计算机实现。在附图 2 中，通过虚线包围的块由硬件（它是用于常规的 CD-R 光盘记录和再现设备或常规的 CD-R/W 光盘记录和再现设备的光盘驱动器）构成。其余的部分由通

过控制器比如 CPU 执行的软件实现。软件可以包含装置密钥数据 DEV_Key 和媒体密钥块数据 MKB。

在附图 2 中，参考标号 1 表示可记录的光盘比如 CD-RW 或者 CD-R 光盘。已经从常规的记录媒体比如 CD-DA 或者 CD-ROM 中再现的内容数据或者已经从光盘 D（它是前述新型类型的媒体）中再现的内容数据记录到光盘 1 中。换句话说，在附图 2 中所示的记录设备可以用于形成已经从常规的记录媒体比如 CD 或者前述的光盘 D 中读取的数据的拷贝。

在附图2中所示的记录设备可以将已经从光盘D中读取的数据记录到用于常规的光盘的记录和再现设备（即光盘驱动器）中。换句话说，能够处理新型光盘 D 的记录设备或者由应用软件构成并能够处理光盘 D 的驱动器将媒体结合密钥数据 MB_Key 记录在光盘 D 上以使媒体结合密钥数据 MB_Key 结合在其中。相反，常规的记录设备或者常规的驱动器不能将媒体结合密钥数据MB_Key记录在光盘D上以使该媒体结合密钥数据 MB_Key 结合在其中。因此，正如下文所描述，常规的记录设备或常规的驱动器通过网络接收媒体结合密钥数据 MB_Key。

主轴马达 2 以恒定的线速度或恒定的角速度旋转并驱动光盘 1。为将数据记录到光盘 1 和并从其中读取数据，设置光学拾取器 3。通过使用进给马达（未示）的行进机构在光盘 1 的径向方向上使光学拾取器 3 行进。

根据本实施例，光盘 1 是相变型光盘，通过具有可记录的输出等级的激光辐射到光盘 1 来记录数据并通过检测从光盘 1 反射的激光的光量的变化再现数据。由相变型记录材料构成的记录膜涂敷在由聚碳酸酯构成的衬底上。通过注射模制的聚碳酸酯，轨道导向槽已经形成在衬底上。该轨道导向槽也称为预制槽，因为它们事先已经形成。形成在槽之间的部分称为脊面。通常，从在衬底上的读激光的入射侧看，附近的侧面是脊面，而远处的侧面是槽。从内周边到外周边连续地并成螺旋地形成槽。只要光盘 1 是可记录的光盘，则除了相变型光盘以

外，本发明还可以用于使用由此色料作为记录材料的磁光盘或者只写一次光盘。

槽在光盘的径向方向上摆动以便控制光盘1的旋转并获得记录数据的参考信号。数据记录在槽和脊面中。此外，槽按照与作为地址信息的绝对时间信息相对应的在光盘的径向方向上的摆动信息摆动以连续地记录数据。在CD-R盘和CD-RW盘中，参考作为根据槽的摆动信息获得的地址信息的绝对时间信息，在光盘1上寻找所需的写位置。光学拾取器3行进到所需的写位置并从光学拾取器3中将激光辐射到光盘1。结果，数据写到光盘。

以如下的方式产生具有摆动槽的光盘。在母版制作设备中，激光辐射到涂敷在盘形玻璃衬底上的光致抗蚀剂膜上。此外，激光在径向方向上偏转或摆动。换句话说，显示激光。结果，形成了在光盘的径向方向上摆动的槽（即摆动槽）。对已经以激光辐射过的光致抗蚀剂膜进行显影。结果，形成了母盘。电铸显影的母盘。由此，形成了模板。应用该模板，执行注模过程。由此形成了具有摆动槽的盘衬底。通过溅射法等方法在盘衬底上涂敷相变型记录材料。由此形成了光盘。

参考附图2，例如要记录的声频和/或视频数据的内容数据Din从输入端4输送到内容判断部分5。内容数据Din是需要加密的内容数据或者不需要加密的内容数据。需要加密的内容数据是例如从前述的光盘D中已经再现的内容数据。不需要加密的内容数据是例如已经从常规的CD中再现的内容数据。内容判断部分5判断内容数据Din是不需要加密的内容数据还是需要加密的内容数据以对例如包含在输入内容数据中的信息进行格式化。内容判断部分5输出表示识别的结果的标识符信号Sid、不需要加密的内容数据SCD1和需要加密的内容数据SCD2。

不需要加密的内容数据SCD1从内容判断部分5输出并输送给误差校正码编码器6。误差校正码编码器6对内容数据SCD1执行误差校正码编码。误差校正码编码器6的输出数据输送给调制部分7。调制部分7执行调制过程例如EFM调制过程。调制部分7的输出数据

输送给记录电路 8。此外，标识符信号 Sid 输送给记录电路 8。记录电路 8 执行将帧同步信号、地址数据等相加的过程以从调制部分 7 输出数据。记录电路 8 的激光驱动电路部分产生使半导体激光器件输出具有预定等级的激光的驱动信号以使记录数据记录在光盘 1 中。激光驱动电路部分的驱动信号输送给作为光学拾取器 3 的光源的半导体激光器件。对应于从半导体激光器件输送的驱动信号调制的激光辐射到光盘 1。结果，数据记录在光盘 1 中。

识别记录在光盘 1 上的内容作为不需要加密的明码内容/内容数据或者需要加密并已经加密的内容/内容数据的标识符信号 Sid 输送给记录电路 8.记录电路 8 给光学拾取器 3 输出标识符信号 Sid 以使标识符信号 Sid 作为 TOC 数据记录到预定的位置例如光盘 1 的导入区中。

在内容数据 Din 是需要加密的内容数据时，内容数据 SCD2 从内容判断部分 5 中输出。加密器 11 以内容密钥数据 CON_Key 对内容数据 SCD2 进行加密。经加密的数据输送给选择器 12。除了加密器 11 的输出数据以外，加密器 13 的输出数据、媒体密钥块数据 MKB 和媒体结合密钥数据 MB_Key 都输送给选择器 12。加密器 13 以密钥箱密钥数据 KL_Key 对内容密钥数据 CON_Key 进行加密。经加密的内容密钥数据输送给选择器 12。关于 DRM 的数据加入到内容密钥数据 CON_Key。

密钥箱密钥数据 KL_Key 是通过散列计算部分 14 计算的数据。媒体密钥块数据 MKB 和装置密钥数据 DEV_Key 都通过计算部分 15 计算。计算部分 15 的输出输送给散列计算部分 14。存储存储部分 16 中的媒体结合密钥数据 MB_Key 输送给散列计算部分 14。散列计算部分 14 产生媒体结合密钥数据 MB_Key 和密钥数据 MKB_Key 的散列值（即密钥箱密钥数据 KL_Key）。除了媒体结合密钥数据 MB_Key 以外前述的加密所需的密钥数据包含在光盘 D 的再现数据中并通过应用软件从再现数据中抽取。媒体结合密钥数据 MB_Key 被隐藏起来但不包含在光盘 D 的再现输出数据中。

等效于媒体结合密钥数据 MB_Key 的密钥数据从 WEB（WEB

站点）19通过开关17和网络18下载到存储部分16。由于下载的密钥数据还没有结合到记录媒体中，严格地说，密钥数据不同于光盘D的媒体结合密钥数据MB_Key。但是，由于它们在它们的功能上相同，因此下载的密钥数据也称为媒体结合密钥数据MB_Key。在除了光盘驱动器以外的结构都由个人计算机的应用软件实现时，使用个人计算机的通信功能通过网络18实现媒体结合密钥数据MB_Key。开关17在对应于标识符信号Sid的接通状态和切断状态之间操作。只有在需要加密的内容数据记录在光盘1上时，开关17才操作在接通状态。

为通过网络18获得媒体结合密钥数据MB_Key，如在附图2中所示的服务器19和记录设备都应该彼此成功地验证。在如附图2中所示的记录设备由例如应用软件、个人计算机和驱动器构成时，个人计算机将用户ID数据、软件唯一的号码、口令等输入到服务器19。只有在这些输入内容都正确时，才可以从服务器19中获得媒体结合密钥数据MB_Key。网络18例如是因特网。由于安全性的原因，在对光盘1已经执行了一次记录操作之后，已经下载到存储部分16的媒体结合密钥数据MB_Key被擦除。可替换的是，在已经下载了媒体结合密钥数据MB_Key之后的预定时间内，都可以擦除它。

选择器12将以内容密钥数据CON_Key加密的内容数据、以密钥箱密钥数据KL_Key加密的内容密钥数据CON_Key、媒体密钥块数据MKB和媒体结合密钥数据MB_Key以预定的时序输出给在光盘驱动器中由虚线所包围的误差校正码编码器6。经加密的内容数据通过光盘驱动器作为主数据处理。光盘驱动器处理内容密钥数据CON_Key、媒体密钥块数据MKB和媒体结合密钥数据MB_Key以使它们共存于主数据中。例如，这些数据作为不同于主数据的文件的文件记录。可替换的是，内容密钥数据CON_Key、媒体密钥块数据MKB和媒体结合密钥数据MB_Key都可以作为副码数据处理或记录在导入区中。误差校正码编码器6的输出数据通过调制部分7调制。经调制的数据通过记录电路8输送给光学拾取器3。光学拾取器3将经调制的数据记录在光盘1上。标识符信号Sid记录到预定位置上，例如光

盘1的导入区。

在这种方式中，媒体结合密钥数据MB_Key通过网络18从服务器19中下载。因此，与将内容数据记录到光盘D上并从光盘D再现内容数据的记录和/或再现设备相同的环境可以通过常规的光盘等实现。结果，常规的光盘等可以将经加密的内容数据记录到与光盘D类似的光盘1中。

附图3所示为将内容数据记录到的的应用软件的处理。在步骤S1中，输入需要加密的内容数据。在步骤S2中，光盘驱动器判断媒体结合密钥数据MB_Key是否已经写入到媒体中以使媒体结合密钥数据MB_Key结合到其中。光盘D记录和再现设备可以将媒体结合密钥数据MB_Key写入到媒体中以使媒体结合密钥数据MB_Key结合在其中，流程进行到步骤S3中。在步骤S3中，媒体结合密钥数据MB_Key记录到光盘1以使仅仅光盘D的记录和/或再现设备能够读取媒体结合密钥数据MB_Key（即媒体结合密钥数据MB_Key被结合到该媒体中）。

由于根据本实施例的常规的光盘驱动器等不能将媒体结合密钥数据MB_Key写入到媒体中以使该媒体结合密钥数据MB_Key结合到其中，因此在步骤S2中的判断结果为否。在步骤S4中，判断光盘驱动器是否连接到服务器19中。在服务器19和作为记录设备的光盘驱动器已经彼此成功地验证时，光盘驱动器连接到服务器19。在步骤S4中的判断结果表示光盘驱动器和服务器19还没有连接时，流程进行到步骤S5。在步骤S5中，提示信息比如“将光盘驱动器连接到WEB服务器！”显示在光盘驱动器的显示部分上。在预定的时间周期中在光盘驱动器还没有连接到服务器19时，产生超时错误并执行错误处理（未示）。

在步骤S4中的判断结果表示光盘驱动器已经连接到服务器19（即光盘驱动器和服务器19已经彼此成功地验证并且已经从服务器19下载媒体结合密钥数据MB_Key）时，流程进行到步骤S6。在步骤S6中，光盘驱动器将媒体结合密钥数据MB_Key记录到光盘1以使常

规的光盘驱动器能够读取媒体结合密钥数据 MB_Key。为改善媒体结合密钥数据 MB_Key 的安全性，可以不将它记录在光盘 1 上。在这种情况下，与下文描述的再现设备一样，通过网络可以获得媒体结合密钥数据 MB_Key。通过媒体结合密钥数据 MB_Key，可以对经加密的内容数据进行再现。

附图 4 所示为作为常规的光盘驱动器等并能够再现需要加密并已经加密的内容数据的再现设备的实例。该再现设备由如在附图 4 中所示的虚线包围的硬件的驱动器、CD-ROM 光盘再现设备、CD-R 光盘记录和再现设备、CD-RW 光盘记录和再现设备等以及应用软件构成。当然再现设备可以只由硬件构成。在附图 4 中所示的光盘 1 是在其上通过前述的设备已经记录明码或经加密的内容数据的光盘。明码或经加密的内容数据是从 CD 或前述的光盘 D 中已经读取的数据的拷贝。但是，光盘 1 并不限于这些。可替换的是，光盘 1 可以是在其上已经记录了通过例如 EMD(电子音乐发布设备)已经发布的内容数据的盘。可替换的是，光盘 1 可以是在其上已经记录了经加密的内容数据的只读光盘。

光学拾取器 3 将再现内容数据所需的激光辐射到光盘 1 上。设置在光学拾取器 3 上的四分区的光电检测器检测由光盘 1 反射的激光。通过光电检测器检测的信号输送给 RF 处理块 21。在 RF 处理块 21 中，矩阵放大器计算光电检测器的检测信号并产生再现（RF）信号、跟踪误差信号和聚焦误差信号。在时钟信号和地址数据已经作为摆动槽的信息记录在光盘 1 上时，摆动检测信号从 RF 处理块 21 中输出。RF 信号输送给解调部分 22。解调部分 22 执行例如 EFM 解调。解调部分 22 的输出数据输送给误差校正电路 23。误差校正电路 23 执行误差校正处理。误差校正电路 23 的输出数据输送给开关 24。

跟踪误差信号和聚焦误差信号从 RF 处理块 21 输送给伺服电路（未示）以控制主轴马达 2 的旋转和从光学拾取器 3 辐射的激光的跟踪和聚焦。伺服电路对光学拾取器 3 执行跟踪伺服和聚焦伺服和对主轴马达 2 执行主轴伺服和螺纹伺服。

解调部分 22 输出再现的副码数据。副码数据输送给副码解调部分 25。副码解调部分 25 对包含在副码数据中的时间数据（时间数据是对应于在盘上的位置的地址数据）进行解调。应用这种时间数据，伺服电路运行。时间数据输送给系统控制器（未示）。应用这种时间数据，控制光学拾取器 3 的位置以从光盘 1 中读取所需的数据。在初始状态中在光盘 1 装载到在附图 4 中所示的光盘驱动器中时，光学拾取器 3 读取光盘 1 中的导入区。光学拾取器 3 读取记录在光盘 1 的导入区中的 TOC 数据。将该 TOC 数据输送给 TOC 读取部分 26。

从 TOC 读取部分 26 中输出的数据包含标识符信号 Sid。判断部分 27 根据从 TOC 读取部分 26 的输出数据中抽取的标识符信号 Sid 执行判断操作。根据判断部分 27 的识别结果控制开关 24。换句话说，在已经从光盘 1 中读取的数据是还没有加密的明码内容数据时，开关 24 操作以使误差校正电路 23 的输出数据输送给输出终端 28。相反，在已经从光盘 1 中读取的数据是已经加密的内容数据时，开关 24 操作以使误差校正电路 23 的输出数据输送给分流装置 29。

分流装置 29 使以内容密钥数据 CON_Key 加密的内容密钥数据、以密钥箱密钥数据 KL_Key 加密的内容密钥数据 CON_Key 和媒体密钥块数据 MKB 分开。经加密的内容数据输送给解密器 30。解密器 30 对以内容密钥数据 CON_Key 加密的内容数据进行解密并将经解密的数据输出给输出终端 31。解密器 32 输出内容密钥数据 CON_Key。

从分流装置 29 中输出的媒体密钥块数据 MKB 输送给计算部分 33。再现设备或应用软件唯一的装置密钥数据 DEV_Key 输送给计算部分 33。计算部分 33 产生密钥数据 MKB_Key。从存储部分 35 中输送的密钥数据 MKB_Key 和媒体结合密钥数据 MB_Key 输送给散列计算部分 34。散列计算部分 34 计算媒体结合密钥数据 MB_Key 和密钥数据 MKB_Key 的散列值并获得密钥箱密钥数据 KL_Key 并将所获得的数据输送给解密器 32。解密器 32 对已经加密的内容密钥数据和关于 DRM 的数据进行解密并获得内容密钥数据 CON_Key。

常规的光盘驱动器等不能读取的媒体结合密钥数据 MB_Key 通

过开关36和网络37从WEB（WEB站点）38下载到存储部分35。在除了在附图4中所示的以虚线包围的驱动器以外的结构都由个人计算机的应用软件实现时，使用个人计算机的通信功能实现媒体结合密钥数据MB_Key。根据识别的结果控制开关36。只有在再现经加密的内容数据时，开关36才接通。

为通过网络37获得媒体结合密钥数据MB_Key，如在附图4中所示的再现设备和WEB服务器38都应该彼此成功地验证。在再现设备由应用软件、个人计算机和驱动器构成时，个人计算机输入关于用户的ID数据、软件唯一的号码、口令等。只有在输入内容和输入数据都正确时，再现设备（即光盘驱动器）才可以从WEB服务器38中获得媒体结合密钥数据MB_Key。网络37例如是因特网。由于安全性的原因，在对光盘的数据或内容数据已经再现了一次之后，已经下载到存储部分35的媒体结合密钥数据MB_Key被擦除。可替换的是，在已经下载了媒体结合密钥数据MB_Key之后的预定时间内，都可以擦除它。从WEB服务器38中获得媒体结合密钥数据MB_Key的方法与用于前述的记录设备的方法相同。

由于通过网络37从WEB服务器38下载媒体结合密钥数据MB_Key，通过常规的光盘驱动器等可以实现与用于光盘D的记录和/或再现设备相同的环境。结果，常规的光盘驱动器等可以从光盘D中读并再现经加密的内容数据。

在通过网络将媒体结合密钥数据MB_Key发送给光盘驱动器等时，再现设备（再现应用软件）侧或服务器侧可以管理关于DRM的数据（数字权利管理）比如关于内容数据的拷贝次数的限制。在服务器侧管理内容数据的拷贝次数时，再现设备、驱动器和应用软件每个都管理媒体结合密钥数据MB_Key的下载历史。在这种情况下，在请求下载密钥数据时，光盘的标识符信息或内容数据也发送给WEB服务器38。WEB服务器38监测每个盘的密钥数据或每种内容数据已经下载的次数。结果，WEB服务器38可以掌握盘或内容数据的拷贝或再现次数。结果，WEB服务器38可以限制盘或内容数据的拷贝或再

现。

附图5所示为从光盘D中再现内容数据的应用软件的过程。步骤S11中，输入通过再现设备的驱动器已经读取并再现的经加密的内容数据。在步骤S12中，判断驱动器是否已经读取媒体结合密钥数据MB_Key。在驱动器是从光盘D中能够再现内容数据的前述再现设备等时，由于驱动器可以读取媒体结合密钥数据MB_Key，流程进行到步骤S13。在步骤S13中，执行对从光盘1中已经读取的经加密的内容数据进行解密的解密过程。

由于常规的光盘驱动器等不能读取媒体结合密钥数据MB_Key，在步骤S12中的判断的结果为否。此后，流程进行到步骤S14。在步骤S14中，判断驱动器是否已经连接到WEB服务器38。在WEB服务器38和再现设备已经成功彼此验证时，该设备连接到WEB服务器38。在步骤S14的判断结果表示该设备还没有连接到WEB服务器38时，流程进行到步骤S15。在步骤S15中，提示信息比如“将设备连接到WEB服务器！！”显示在再现设备的显示部分（未示）上。在预定的时间周期中该设备还没有连接到WEB服务器38时，产生超时错误并终止在附图5中所示的处理。

在步骤S14中的判断结果表示该设备已经连接到WEB服务器38时，WEB服务器38和记录设备已经彼此成功地验证。因此，为下载媒体结合密钥数据MB_Key，流程进行到步骤S16。在步骤S16中，从WEB服务器38下载媒体结合密钥数据MB_Key并将其存储到存储部分35。应用所获得的媒体结合密钥数据MB_Key，对经加密的内容数据进行解密（在步骤S13中）。

虽然参考本发明的最佳实施例已经示出并描述了本发明，但是在本领域的普通技术人员应该理解的是，在不脱离本发明的精神和范围的前提下可以对前述的实施例在细节方面作出各种改变、省略和增加。例如，除了个人计算机以外，前述的应用软件可以安装到网络家用电子设备比如置顶盒。在根据本发明的记录方法应用于只读光盘时，在附图2中的记录设备可以应用于母版制作设备。此外，本发明也可以

应用于其它的数据记录媒体比如除了光盘以外的存储器卡。

本发明提供了在新型驱动器等还没有普及的阶段中与全面安全性功能的兼容性，该新型驱动器等使用与媒体结合的媒体结合密钥实现全面安全性功能。在实现了安全性功能时，可以平稳地引入新型驱动器等。在引入与媒体结合的密钥时，能够防止非法地拷贝。应用不能处理与媒体结合的密钥的常规驱动器，为获得等效于与媒体结合的密钥的密钥，驱动器和 WEB 服务器应该成功地相互验证。因此，可以确保安全性。

图1

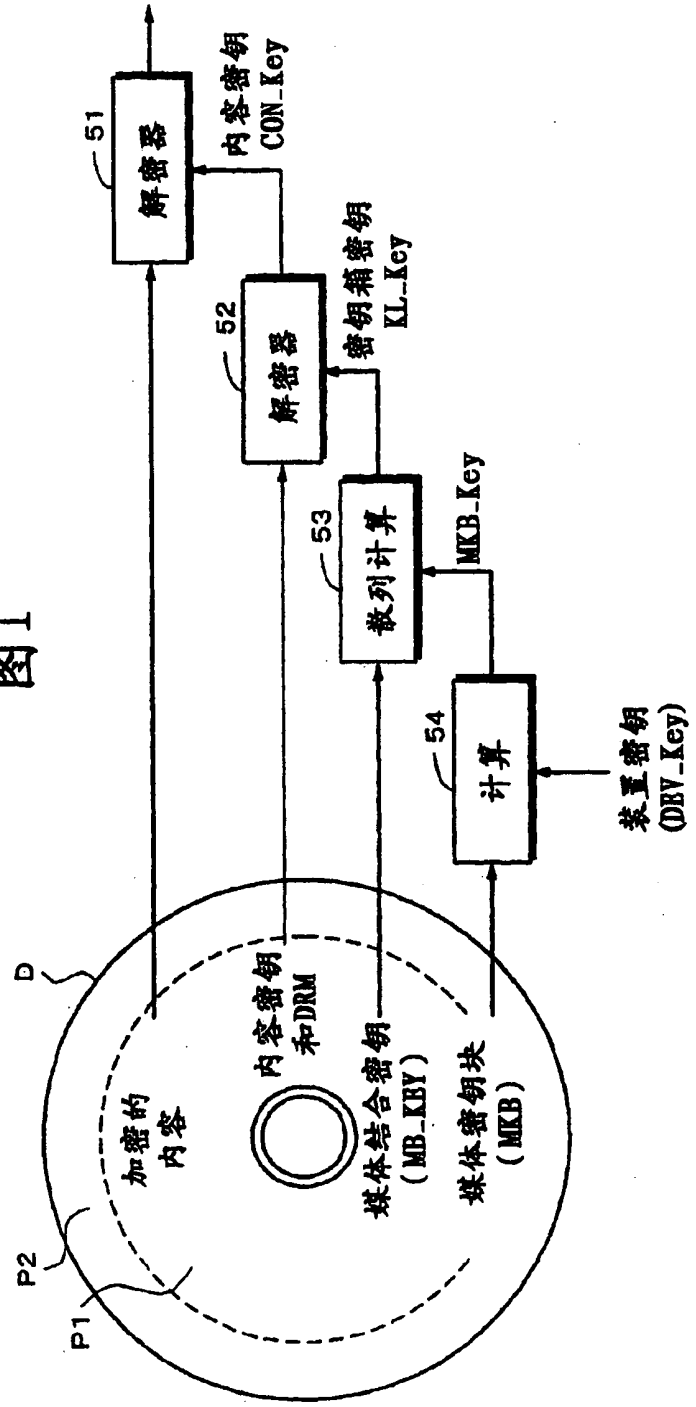

51
解密器
内容密钥
CON_Key
52
解密器
密钥箱密钥
KL_Key
53
散列计算
MKB_Key
54
计算
装置密钥
(DEV_Key)
D
加密的
内容
内容密钥
和DRM
媒体结合密钥
(MB_KEY)
媒体密钥块
(MKB)
P2
P1

图2

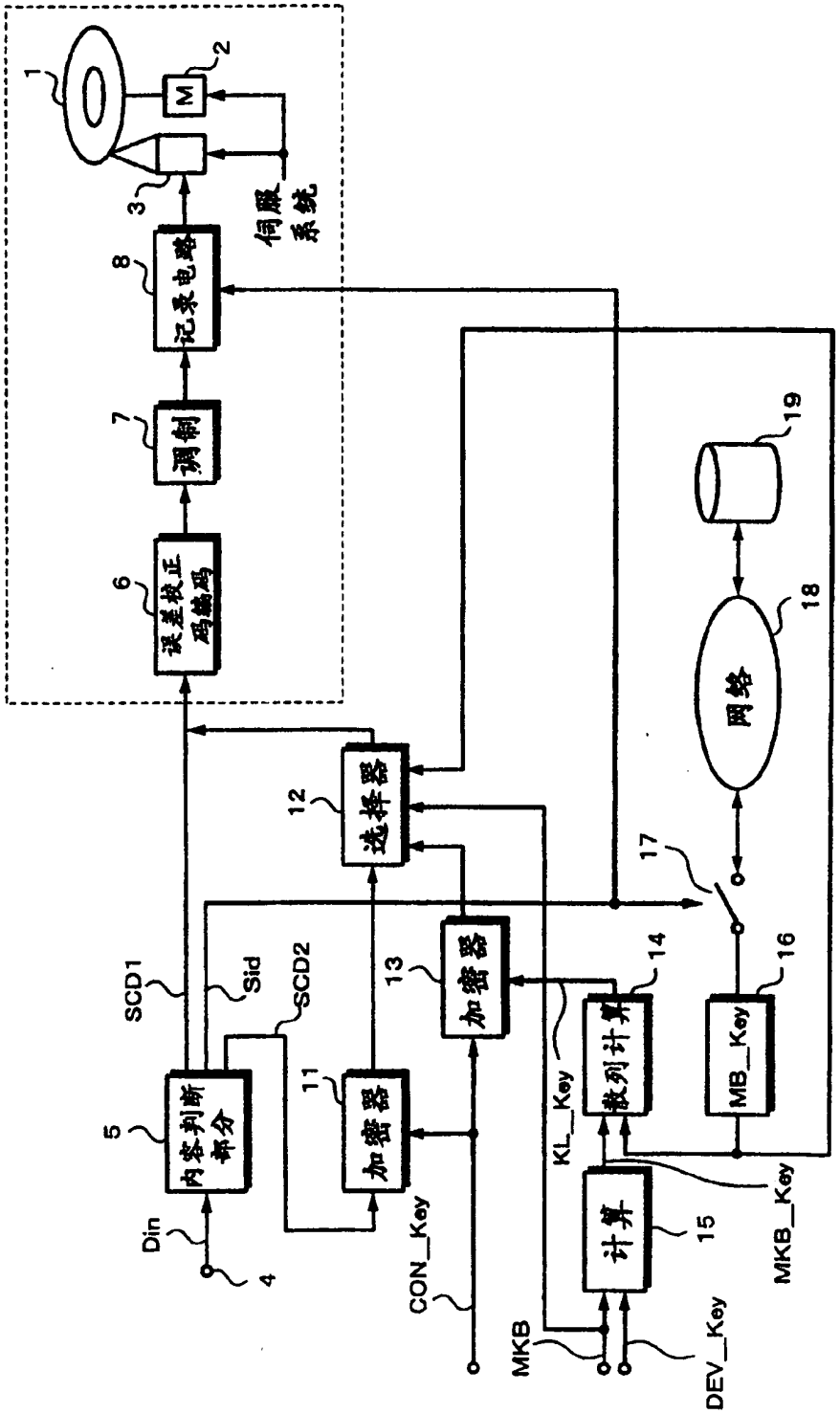

伺服系统
记录电路
调制
误差校正码编码
内容判断部分
加密器
选择器
加密器
散列计算
计算
网络
MB_Key
SCD1
SId
SCD2
Din
CON_Key
KL_Key
MKB
DEV_Key
MKB_Key

图3

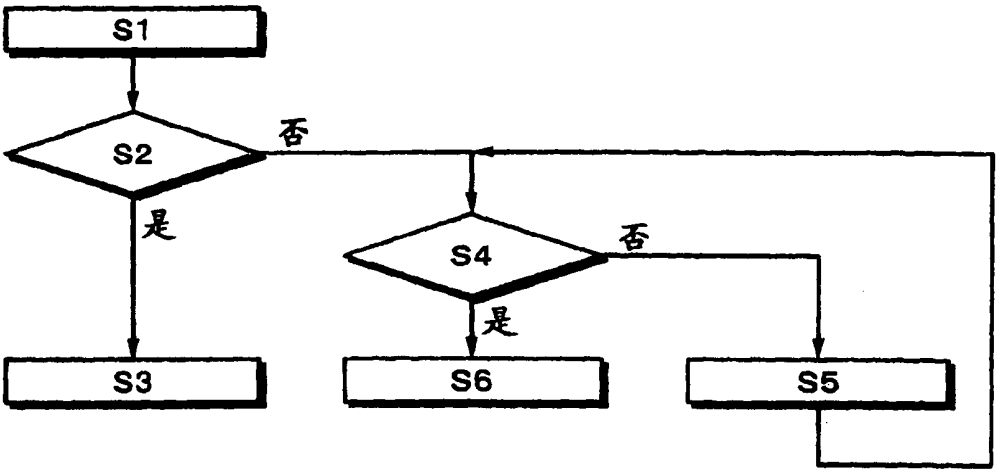


图 4

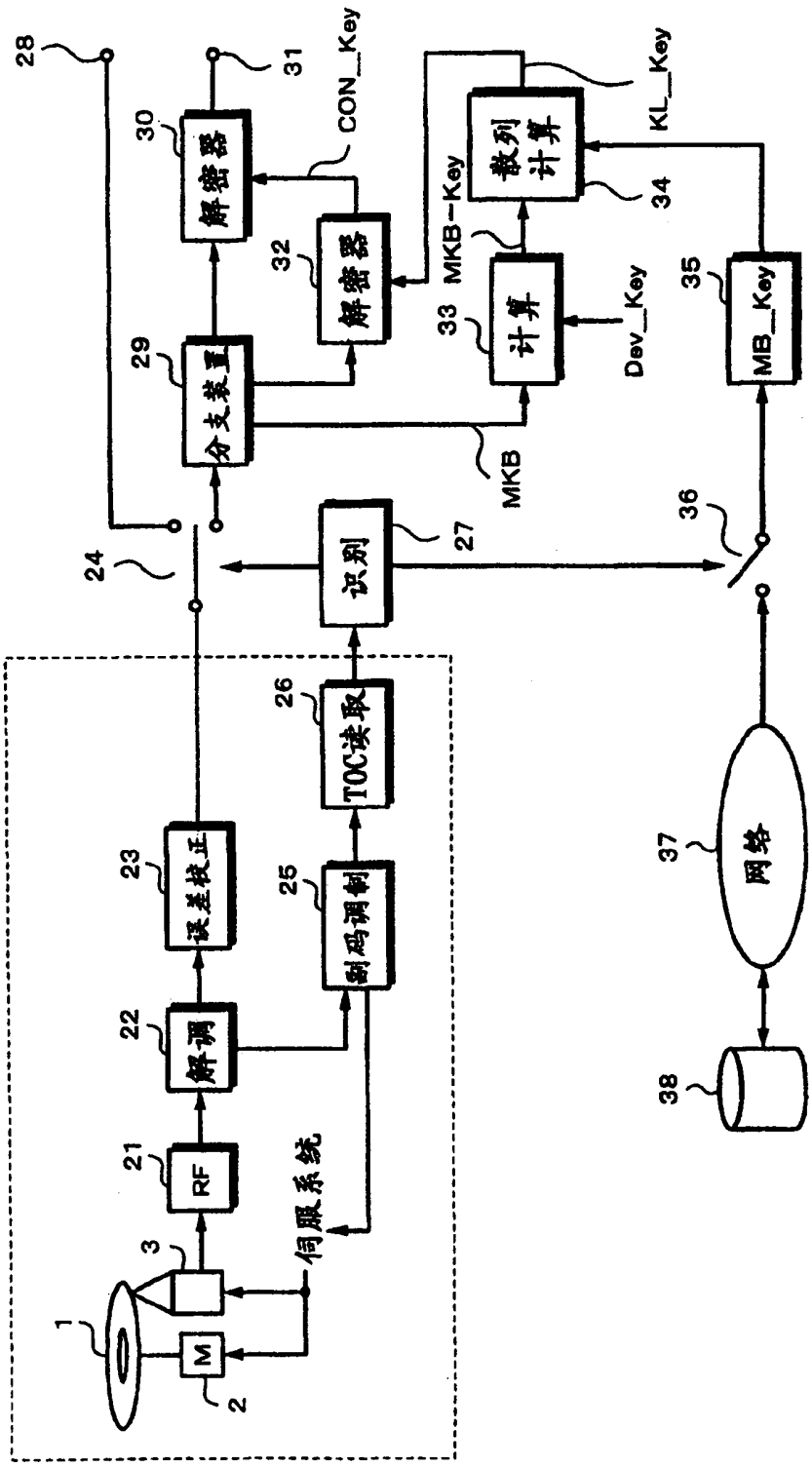
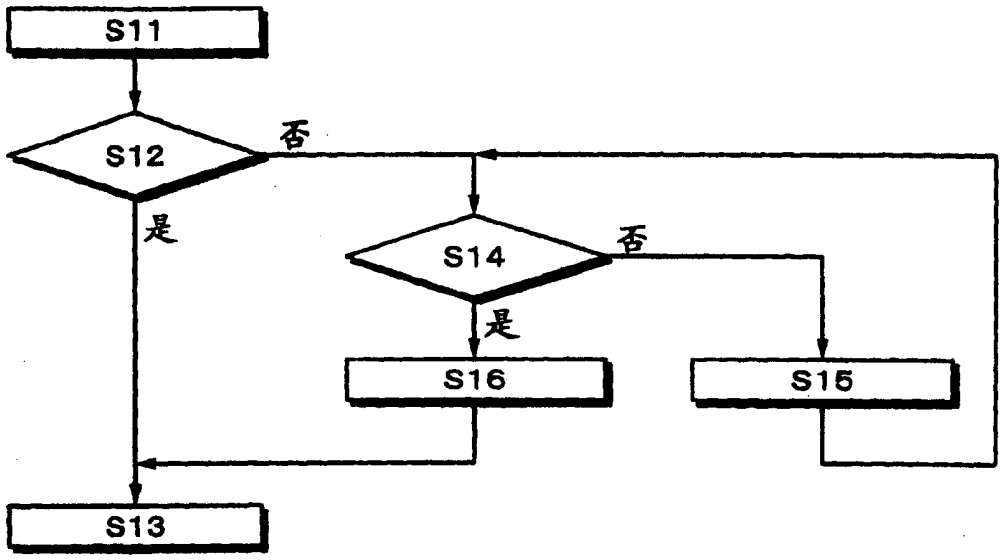

28
31
CON_Key
30
解密器
32
解密器
MKB-Key
散列计算
KL_Key
34
33
计算
Dev_Key
35
MB_Key
29
分支装置
MKB
36
24
识别
27
26
TOC读取
23
误差校正
25
制码调制
22
解调
21
RF
3
伺服系统
1
M
2
37
网络
38

图5



# 参考标号说明

| | |
|---|---|
| 1 | 光盘 |
| 3 | 光学拾取器 |
| 5 | 内容判断部分 |
| 11，13 | 加密器 |
| 16 | 媒体结合密钥的存储部分 |
| 18 | 网络 |
| 19 | 网络服务器 |
| 30，32 | 解密器 |
| 35 | 媒体结合密钥的存储部分 |
| 37 | 网络 |
| S1 | 输入内容 |
| S2 | MB_Key能被写入？ |
| S3 | 记录MB_Key以使仅以新型式读取 |
| S4 | 设备已连接到网络？ |
| S5 | 显示提示信息 |
| S6 | 记录等效于MB_Key的密钥以使能以常规型式读取 |
| S11 | 输入内容 |
| S12 | MB_Key能被读取？ |
| S13 | 执行解密过程 |
| S14 | 设备已连接到网络？ |
| S15 | 显示提示信息 |
| S16 | 获得MB_Key |