[19] 中华人民共和国国家知识产权局

[12] 发明专利说明书

专利号 ZL 00806868.2

[51] Int. Cl.
G11B 20/00 (2006.01)
G11B 7/007 (2006.01)
G11B 23/28 (2006.01)
G06F 1/00 (2006.01)

[45] 授权公告日 2007 年 12 月 26 日

[11] 授权公告号 CN 100358034C

[22] 申请日 2000.4.27 [21] 申请号 00806868.2

[30] 优先权

[32] 1999. 4.28 [33] JP [31] 122104/99

[32] 1999. 5.10 [33] JP [31] 128197/99

[32] 1999.10.21 [33] JP [31] 299635/99

[86] 国际申请 PCT/JP2000/002750 2000.4.27

[87] 国际公布 WO2000/067257 英 2000.11.9

[85] 进入国家阶段日期 2001.10.29

[73] 专利权人 松下电器产业株式会社

地址 日本大阪府

[72] 发明人 永井隆弘 石原秀志 高木裕司
弓场隆司 东海林卫 大嶋光昭
大原俊次 伊藤基志 石田隆
中村敦史 谢花正司 中田浩平

[56] 参考文献

WO9858368A1 1998.12.23

CN1166223A 1997.11.26

审查员 庞 娜

[74] 专利代理机构 中科专利商标代理有限责任公司

代理人 刘晓峰

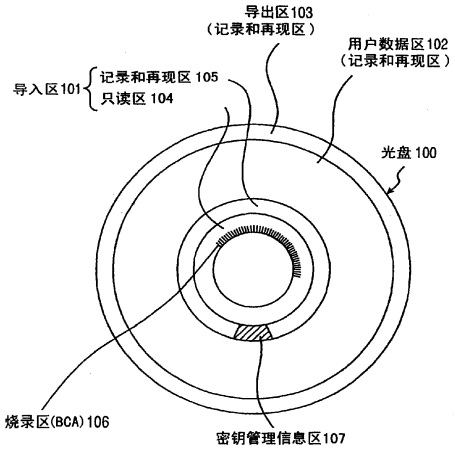
权利要求书 2 页 说明书 62 页 附图 36 页

[54] 发明名称

光盘记录和再现装置以及光盘记录和再现方法

[57] 摘要

本发明提供了一种可记录数据的记录型光盘，所述光盘包括数据记录和再现区，用于在其上记录数据并从其上再现数据；和只读盘识别信息区，用于在其中记录识别光盘的盘识别信息。 在光盘中，盘识别信息通过以带状形状除去形成在光盘上的反射膜而形成。 盘识别信息包括用于每个光盘的固有盘标识符。 数据记录和再现区包括用于在其中记录利用包括识别光盘的盘识别信息的信息作为密钥来加密的已加密数据的区域。



1．一种用于光盘的光盘记录装置，所述的光盘包含第一区和第二区，所述的第一区是沿着圆周方向以条纹形式形成，所述的第一区包括可以得到间歇性的反射光量较低的信号的区；

其中，所述的第一区形成于离所述的第二区有一定的径向间距之处，

作为只读数据记录在所述的第一区内的数据也被记录在所述的第一区和第二区之间的区域内，

所述的光盘记录装置包含记录部件，用于通过使用形成在所述第一区中的作为密钥的信号加密用户数据并通过光束照射所述的第二区将加密的用户数据记录到所述第二区上。

2．一种用于在包含第一区和第二区的光盘内的光盘记录方法，所述的第一区沿着圆周方向以条纹状形成，所述的第一区包含可以得到间歇性的反射光量较低的信号的区，

其中，所述的第一区形成于离所述的第二区有一定的径向间距之处，

作为只读数据记录在所述的第一区内的数据也被记录在所述的第一区和第二区之间的区域内，

所述的光盘记录方法包含通过使用形成在所述第一区中的作为密钥的信号加密用户数据并通过光束照射所述的第二区将加密的用户数据记录到所述第二区上的步骤。

3．一种用于光盘的光盘再现装置，所述的光盘包含第一区和第二区，所述的第一区是沿着圆周方向以条纹形式形成，所述的第一区包括可以得到间歇性的反射光量较低的信号的区；

其中，所述的第一区形成于离所述的第二区有一定的径向间距之处，

作为只读数据记录在所述的第一区内的数据也被记录在所述的第一区和第二区之间的区域内，

所述的光盘再现装置包含：

用于再现所述的第一区的第一再现部件；

用于再现作为只读数据记录在第一区和第二区之间的数据的第二再现装置；和

第三再现装置，用于再现记录在所述第二区域中的用户数据，并通过使用形成在所述第一区中的作为密钥的信号作为钥匙而解密被再现的用户数据。

4．一种用于在包含第一区和第二区的光盘内的光盘再现方法，所述的第一区沿着圆周方向以条纹状形成，所述的第一区包含可以得到间歇性的反射光量较低的信号的区，

其中，所述的第一区形成于离所述的第二区有一定的径向间距之处，

作为只读数据记录在所述的第一区内的数据也被记录在所述的第一区和第二区之间的区域内，

所述的光盘再现方法包含如下步骤：

再现所述的第一区；

再现作为只读数据记录在所述的第一区和第二区之间的数据；和再现记录在所述的第二区内的数据，并通过使用形成在所述第一区中的作为密钥的信号而解密被再现的用户数据。

光盘记录和再现装置以及光盘记录和再现方法

技术领域

本发明涉及光盘、光盘记录和再现设备以及在光盘上记录、再现和删除数据的方法和信息处理系统。本发明尤其涉及这样一种光盘、光盘记录和再现设备以及在光盘上记录、再现和删除数据的方法和信息处理系统，其可阻止从一个光盘向另一个记录介质如另一种记录类型的光盘等进行非法的数字复制，原光盘上记录了例如包括具有版权保护的电影图像数据和音乐声音数据等 AV 数据（音频和视频数据）的数据。

背景技术

光盘在随机存取性方面优于常规的磁带介质，并且由于能够采用激光非接触地记录和再现，因此具有减少由于重复使用造成的品质恶化的优点。另外，光盘还具有这样的优点，即可以通过光盘制造商的进行的母盘制造（mastering），以低价格进行批量生产，并且随着高质量的数字音频替代常规留声机的模拟记录，CD（紧致盘）变得普遍。另外，近年来数字记录高质量图像数据的 DVD（数字视盘或数字通用盘）已商品化，而且预计在不久的将来光盘将进一步发展为用于 AV 数据的数字记录介质。

另一方面，除了由光盘制造商事先以预制凹坑（pre-pit）的形式在其上记录数据的只读光盘，如音乐 CD、CD-ROM、DVD-ROM 等之外，用户可在家中记录 AV 数据的记录型光盘，如 CD-R、CD-RW、MO、MD、DVD-RAM 等近年来也得到了发展和广泛的传播。

此外，在电视广播中，已经引入了允许多通道或各种服务的数字系统来替代传统的模拟系统，并且在不久的将来这种趋势将广泛漫延。特别是，将记录型的光盘作为通过数字广播或通讯传递的内容的记录介质，

以记录主要出于时间转换应用目的的 AV 数据，而在时间转换应用中，当内容在传输时被累积之后，执行节目选择并且收听或收看所选择的内容。

传统地，已主要用于计算机的记录型光盘被用于存储由用户自己创建的数据，并且记录型光盘没有任何阻止在记录型光盘之间进行复制的手段。当广泛使用记录型光盘时，普通用户把光盘记录数据不合法地照原样复制到另一个记录型的光盘，以致得到非法再现而不支付要向该 AV 数据的作者或著者支付的版权费成为可能，并且由于记录型光盘是数字可记录的，因此不会降低声音品质和图像品质，这变成了阻碍高质量内容传播的一个因素。关于在其上数字记录音乐等的 MD，已经引入了执行限制复制次数的生成管理方法，与生成管理数据相结合的数据被记录在光盘上并且复制次数受到生成管理数据的限制。

此外，为了阻止 CD-ROM 或 DVD-ROM 的非法复制，例如国际专利申请公开 No.WO 97/14144 中提出了一种方法，形成一个烧录区（Burst Cutting Area）（以后称为 BCA），这是一个一次写入区，用于覆盖光盘凹点部分上的条形码，并用于在 BCA 上记录 ID，在生产光盘时针对每个光盘的 ID 彼此不同。根据该方法，因为口令针对每个盘的 ID 是不同是，所以一个口令只能解密一个盘上的密码，因此即使当内容被非法复制时，也会由于没有盘的 ID 信息不能对内容进行解密。

图 39 是表示传统 DVD-ROM 的用户数据区结构和用于对来自用户数据区的数据中已加密的内容进行解密的光盘再现设备的配置图。如图 39 所示，在 DVD-ROM 中，对记录在盘上的内容数据进行加密。

参考图 39，DVD-ROM 的用户数据区由扇区头部区 3201、主数据区 3202 和检错码 3203 组成。在这种情况中，在扇区头部区 3201 上记录扇区地址 3204、版权控制信息 3205 和解密密钥 3206，其中扇区地址 3204 指示扇区的位置，在版权控制信息 3205 中记录了关于记录在主数据区 3202 上的数据的版权控制信息（例如，加扰标志、复制控制信息等），解密密钥 3206 用于在对记录于主数据区 3202 上的数据执行加密时对该密码进行解密。此外，对主要为版权保护所需要的 AV 数据等加密，并将其记录在主数据区 3202 上。

在再现这种用户数据区的时候，首先获得从扇区头部区域3201再现已加密的内容所需的解密密钥 3206。把获得的解密密钥 3206 输入到密钥解密装置 3207 中，该装置通过利用预定的光盘密钥将输入的解密密钥 3206 解密为内容解密密钥，并且把内容解密密钥输出到解密装置 3208。接下来，解密装置 3208 根据存储在对应于主数据区 3202 的扇区头部区 3201 中的版权控制信息 3205，利用已解密的内容解密密钥对主数据区 3202 的已加密内容进行解密，并且能够获得可再现数据的已解密内容。

在根据图 39 所示结构的光盘中，可以通过个人计算机等驱动设备执行从主数据区 3202 的读取。但是，通过形成这样的光盘能够防止非法再现或盗版生产，因为具有正规认证功能的光盘再现设备只能读出记录有解密密钥 3206 的区域。

但是，对于使用生成管理数据的非法复制防止方法，不可避免地要在复制时改变生成管理数据（从“可以复制一次”改变到“不可以复制”）。另一方面，存在着这样的问题，通过复制光盘上的数据和生成管理数据而不改变生成管理数据，或通过计算机等更改生成管理数据并将其记录在光盘上，则不能充分地防止非法复制。另外，因为根据先前与内容一起记录的生成管理数据来限定复制次数，所以存在这样一个问题，即甚至当交付了正规的版权费时，也根本不允许向另一个光盘复制已经制有“不可复制”的数据，并且用户必须等待从内容提供者处提供内容数据。两个问题都是由于内容提供者不能充分地管理由用户执行的向记录型光盘上复制的内容而引起的。

近来，个人计算机在性能上有了进一步的改进并且还连接到网络，以致于可以由多个个人计算机高速进行密码解密。为了进一步提高密码抵抗这种解密的鲁棒性，延长密码所使用的密钥的密钥长度成为必须。但是，在传统上提出的在扇区头部记录解密密钥的密钥管理方法中，存在这样一个问题，即，只记录具有预定长度大小（解密密钥区的大小）或更小长度的解密密钥，不可以为提高密码在未来的鲁棒性的目的而延长密钥的长度。

发明内容

本发明的第一个目的在于提供一种光盘、光盘记录设备、光盘再现设备、光盘记录和再现设备、在光盘上记录和再现数据的方法、在光盘上记录数据的方法、在光盘上再现数据的方法、删除光盘上的数据的方法，和信息处理系统，其可以防止内容提供者不能管理的非法数字复制。

另外本发明的第二目的在于提供一种光盘、一种光盘记录设备、一种光盘再现设备、一种光盘记录和再现设备、在光盘上记录和再现的方法、在光盘上记录的方法、在光盘上再现的方法、删除光盘上的数据的方法，和信息处理系统，其能够提高解密需要版权保护的数据所需的解密密钥的可靠性。

另外，本发明的第三目的在于提供一种光盘、一种光盘记录设备、光盘再现设备、光盘记录和再现设备、在光盘上记录和再现数据的方法、在光盘上记录数据的方法、在光盘上再现数据的方法、删除光盘上的数据的方法，和一种信息处理系统，其能够根据将要被记录的内容的版权保护等级来设置密码的鲁棒水平。

为实现上述目的，根据本发明的一个方面，一种可记录数据的记录型光盘，包括：

数据记录和再现区，用于在其中记录数据并从其再现数据；和

只读盘识别信息区，用于在其中记录用于识别光盘的盘识别信息。

在上述光盘中，盘识别信息最好通过以带状形状除去形成在光盘上的反射膜而形成。

在上述光盘中，盘识别信息最好包括用于每个光盘的固有盘标识符。

在上述光盘中，数据记录和再现区最好包括用于在其中记录利用包括识别光盘的盘识别信息的信息作为密钥来加密的已加密数据的区域。

在上述光盘中，已加密数据最好包括内容数据，该数据至少是图像数据和音乐数据之一。

在上述光盘中，已加密数据最好包括解扰密钥，用于对已经执行到内容数据上的密码解密。

在上述光盘中，已加密数据最好包括：

（a）解扰密钥，用于对已经执行到内容数据上的密码解密，和

（b）检错码，用于检测解扰密钥中的错误。

根据本发明的另一方面，提供一种在其上可记录数据的记录型光盘，

其中光盘包括数据记录和再现区，用于在其中记录数据并从其中再现数据，和

其中数据记录和再现区包括在其中记录内容数据和解扰密钥的区域，其中内容数据至少是已加密图像数据和已加密音乐数据之一，解扰密钥用于对已经执行到内容数据上的密码解密。

根据本发明的另一方面，提供一种可在其上记录数据的记录型光盘，包括：

只读盘识别信息区，用于在其中记录识别光盘用的盘识别信息；

数据记录和再现区，用于在其中记录和从其中再现至少包括已加密图像数据和已加密音乐数据之一的内容数据；和

密钥管理信息区，用于在其中记录再现内容数据时所使用的密钥信息和利用盘识别信息作为密钥加密的解扰密钥。

根据本发明的另一方面，提供一种用于至少控制下列操作之一的光盘记录和再现设备：

（a）在可记录数据的记录型光盘的数据记录和再现区中记录数据的记录操作，和

（b）从数据记录和再现区中再现数据的再现操作，

其中光盘包括盘识别信息区，用于在其中记录识别光盘用的盘识别信息，并且

其中光盘记录和再现设备包括：

再现装置，用于从盘识别信息区再现盘识别信息；和

控制装置，用于判断是否根据再现的盘识别信息执行记录操作和再现操作中的至少一个，并且用于控制光盘记录和再现设备，响应于判断结果执行记录操作和再现操作中的至少一项操作。

根据本发明的另一方面，提供一种光盘记录设备，用于在可记录数据的记录型光盘上记录内容数据，

其中光盘包括用于记录识别光盘的盘识别信息区，并且

其中光盘记录设备包括：

再现装置，用于从盘识别信息区再现盘识别信息；和

记录装置，利用再现的盘识别信息作为密钥在光盘上记录至少部分已加密的数据。

根据本发明的另一方面，提供一种光盘再现设备，用于从可记录数据的记录型光盘上再现内容数据，

其中光盘包括盘识别信息区，用于在其中记录识别光盘用的盘识别信息，并且

其中光盘再现设备包括：

再现装置，用于从盘识别信息区再现盘识别信息，和

解密装置，在从光盘中再现了至少部分已加密的数据之后，利用再现的盘识别信息作为密钥，对至少部分已加密的数据解密。

根据本发明的另一方面，提供一种用于至少控制下列操作之一的光盘记录和再现方法：

（a）在可记录数据的记录型光盘的数据记录和再现区中记录数据的记录操作，和

（b）从数据记录和再现区中再现数据的再现操作，

其中光盘包括盘识别信息区，用于在其中记录识别光盘用的盘识别信息，并且

其中所述方法包括下述步骤：

从盘识别信息区再现盘识别信息；和

根据再现的盘识别信息判断是否执行记录操作和再现操作中的至少一个，并且控制记录操作和再现操作，根据判断结果执行记录操作和再现操作中的至少一项操作。

根据本发明的另一方面，提供一种在可记录数据的记录型光盘上记录内容数据的方法，

其中光盘包括用于在其中记录识别光盘所用的盘识别信息的盘识别信息区，并且

其中该方法包括下述步骤：

从盘识别信息区再现盘识别信息；和

利用再现的盘识别信息作为密钥在光盘上记录至少部分已加密的数据。

根据本发明的另一方面，提供一种光盘再现方法，用于从可记录数据的记录型光盘上再现内容数据，

其中光盘包括盘识别信息区，用于在其中记录识别光盘用的盘识别信息，并且

其中该方法包括下述步骤：

从盘识别信息区再现盘识别信息；和

在从光盘中再现了至少部分已加密的数据之后，利用再现的盘识别信息作为密钥，对至少部分已加密的数据解密。

根据本发明的另一方面，提供一种可记录数据的记录型光盘，包括：

第一信息区，用于在其中记录第一盘信息；

第二信息区，用于在其中记录识别每个光盘用的第二盘信息；和

用户数据区，用于通过向用户数据区上照射光束而记录信息数据。

根据本发明的另一方面，提供一种可记录数据的记录型光盘，

其中光盘具有包括多个扇区的扇区结构，

其中每个扇区包括扇区头部区和用于在其中记录已加密数据的主数据区，

其中扇区头部区包括解密密钥信息区，用于在其中记录解密已加密数据所需要的至少一个解密密钥，和

其中解密密钥信息区的大小小于每个解密密钥。

根据本发明的另一方面，提供一种可记录数据的记录型光盘，

其中光盘包括用于在其中记录数据的主数据区，

其中主数据区包括用于记录非加密状态数据的非加密区，和用于记录加密状态数据的加密区，

其中非加密区包括解密密钥转换数据，该数据用于对数据进行解密的解密密钥的转换，和

其中加密区中的数据被利用解密密钥加密，所述解密密钥被使用解密密钥转换数据转换。

根据本发明的另一方面，提供一种在可记录数据的记录型光盘上记录数据的光盘记录方法，包括步骤：

读出记录在光盘上的解密密钥状态，并根据读出的解密密钥状态判

断是否有用于解密密钥的空区；

当判定存在用于解密密钥的空区时保留解密密钥区并在解密密钥区中记录解密密钥；

至少在文件单元和扩展单元之一中设置版权控制信息和解密密钥索引；

利用解密密钥对数据加密，并在光盘的文件单元和扩展单元的至少一个中记录已加密数据；和

在光盘上记录用于管理记录在光盘上的数据的光盘文件管理信息。

根据本发明的另一方面，提供一种用于从可记录数据的记录型光盘上再现数据的光盘再现方法，包括步骤：

从在文件单元或扩展单元中记录了将要被再现的数据的数据记录区再现并获得解密密钥索引；

再现并获得对应于获得的解密密钥索引的解密密钥；和

在文件单元或扩展单元中再现利用解密密钥加密的数据。

根据本发明的另一方面，提供一种光盘删除方法，用于从可记录数据的记录型光盘中删除数据，该方法包括：

从在文件单元或扩展单元中记录了将要被删除的数据的数据记录区再现并获得解密密钥索引；

更新对应于获得的解密密钥索引并指示解密密钥的记录状态的解密密钥状态，并释放解密密钥；和

通过删除对应于将要从文件管理信息中删除的数据的文件条目，更新用于管理记录在光盘上的数据的文件管理信息。

根据本发明的另一方面，提供一种信息处理系统，包括：

数据加密设备，利用密码密钥对数据加密；

光盘记录和再现设备，用于在记录型光盘上记录用于解密数据所需的解密密钥，并且再现已记录的解密密钥；和

连接到光盘记录和再现设备以及数据加密设备的控制装置，

其中光盘记录和再现设备包括：

第一记录和再现装置，用于在光盘上记录解密密钥表，并从光盘上再现解密密钥表；

加密和解密装置，用于对解密密钥加密，传送加密的解密密钥，从控制装置接收加密的解密密钥并对加密的解密密钥解密；和

第二记录和再现装置，用于在光盘上记录指示解密密钥的记录状态的解密密钥状态表，并从光盘上再现解密密钥状态表；

其中数据加密设备包括：

加密装置，用于对解密密钥加密，并把加密的解密密钥传送给控制设备；和

其中控制设备包括：

从数据加密设备的加密装置接收已加密的解密密钥的接收装置；和

分配装置，用于根据再现的解密密钥状态表，为解密密钥搜索空区，把接收并加密的解密密钥分配给搜索到的空区，并把分配并加密的解密密钥传送给光盘记录和再现设备，和

其中光盘记录和再现设备的加密和解密装置从控制设备的分配装置接收分配并加密的解密密钥，并对接收到的加密的解密密钥解密。

根据本发明的另一方面，提供一种用于再现记录数据的只读型光盘，包括：

用于在其中记录数据的数据再现区；和

用于在其中记录识别光盘用的盘识别信息的只读盘识别信息区，

其中数据再现区包括记录数据的区域，其中该数据被利用包括识别光盘用的盘识别信息的信息作为密钥加密。

附图说明

通过下面参考附图对优选实施例的描述，本发明的各种目的和特征将变得更加清晰，在全文中相似的部件用相同的标号表示，其中：

图 1 是表示根据本发明第一优选实施例的记录型光盘 100 的数据记录区平面图；

图 2A 表示用于形成图 1 所示光盘 100 的 BCA 106 的设备结构的框图和截面图；

图 2B 表示在形成图 1 所示光盘 100 的 BCA 106 之后的光盘 100 的截面图和水平方向上反射光的强度曲线；

图 3 表示图 1 所示 BCA 106 的记录格式示意图；

图 4 表示图 1 所示的用户数据区 102 内扇区数据 401 的扇区结构示图；

图 5 表示图 1 所示密钥管理信息区 107 的结构示图；

图 6A 是根据第一优选实施例的改型的优选实施例，在图 1 所示扇区数据 401 中记录解扰密钥和 AV 数据的记录方法的框图；

图 6B 是根据第一优选实施例，在图 1 所示扇区数据 401 中记录解扰密钥的密钥索引和 AV 数据的记录方法的框图；

图 7 是根据本发明第二优选实施例的光盘介质和再现设备的结构框图；

图 8 是表示由图 7 所示的光盘记录和再现设备的控制 CPU 710 执行的 AV 数据记录处理的流程图；

图 9 是表示由图 7 所示的光盘记录和再现设备的控制 CPU 710 执行的密钥管理信息区的分配处理的流程图；

图 10 是表示由图 7 所示的光盘记录和再现设备的控制 CPU 710 执行的解扰密钥的记录处理的流程图；

图 11 是表示由图 7 所示的光盘记录和再现设备的控制 CPU 710 执行的 AV 数据再现处理的流程图；

图 12 是表示由图 7 所示的光盘记录和再现设备的控制 CPU 710 执行的解扰密钥的获取处理的流程图；

图 13 是按照第一优选实施例的改型优选实施例，根据加密的解扰密钥判断解扰密钥是否正常的方法的框图；

图 14 是按照第一优选实施例的改型优选实施例的解扰区管理表的结构示图；

图 15A 是表示在第一优选实施例中、在记录内容时记录区域标识符的情况下，是否可以在相同区域或不同区域内复制或再现内容的示意图；

图 15B 是表示在第一优选实施例中、在装运光盘时先记录区域标识符的情况下，是否可以在相同区域或不同区域内复制或再现内容的示意图；

图 16 是根据本发明第三优选实施例的光盘 1101 的数据记录区的平

面图；

图 17 是表示根据第三优选实施例的 BCA 再现电路 1401 中再现的信号 1201 和再现的二值化信号 1207 的信号波形的信号波形图；

图 18 是表示根据第三优选实施例的 BCA 再现电路 1401 结构的框图；

图 19 是根据第三优选实施例的光盘记录和再现系统的结构框图；

图 20 是根据第四优选实施例的光盘记录和再现系统的结构框图；

图 21 是根据本发明第五实施例的光盘 1601 的数据记录区的平面图；

图 22 是根据第五优选实施例的光盘记录和再现系统的结构框图；

图 23 表示根据第五优选实施例的 ID 附加表结构的表；

图 24 是根据第三优选实施例的改型优选实施例的光盘 1101a 的数据记录区的平面图；

图 25 是根据第五优选实施例的改型优选实施例的光盘 1601a 的数据记录区的平面图；

图 26 是表示根据本发明的第六优选实施例，光盘上用户数据区的结构、用于从用户数据区的数据中解密加密的内容的光盘再现设备结构的框图；

图 27 是表示在根据第六优选实施例的光盘中，把版权控制信息和解密密钥布置到用户数据区，并把加密的内容布置到主数据区的框图；

图 28 是表示在根据第六优选实施例的光盘中，把纠错单元应用于光盘中多个扇区的情况下的布局框图；

图 29 是表示根据本发明第七优选实施例的光盘中导入区 2401 和用户数据区 2402 的结构、以及用于从存储在导入区 2401 和用户数据区 2402 的数据中解密加密的内容的光盘再现设备的结构框图；

图 30A 是表示在根据第七优选实施例的光盘中，导入区的主数据区中通过解密密钥的初始值指示未记录状态的情形中数据结构的框图；

图 30B 是表示在根据第七优选实施例的光盘中，导入区的主数据区中通过解密密钥的状态表指示记录状态的情形中数据结构的框图；

图 31 是表示根据第七优选实施例的光盘中解密密钥的布局框图；

图 32 是表示由本发明第八优选实施例的文件管理系统管理光盘数据

的数据结构框图；

图 33 是表示根据第八优选实施例由文件管理系统执行的、记录需要版权保护的内容的处理的流程图；

图 34 是表示根据第八优选实施例由文件管理系统执行的内容再现处理的流程图；

图 35 是表示根据第八优选实施例由文件管理系统执行的内容删除处理的流程图；

图 36 是表示根据本发明第九优选实施例的光盘系统的结构框图；

图 37 是表示根据本发明第十优选实施例的光盘中用户数据区的结构、在用户数据区中加密并记录内容的光盘记录设备的结构，和从存储在用户数据区的数据中对加密的内容解密的光盘再现设备的框图；

图 38 是表示根据本发明的第十一优选实施例中用户数据区的结构、在用户数据区中加密并记录内容的光盘记录设备的结构，和从用户数据区的数据中解密加密的内容的光盘再现设备的结构框图；和

图 39 是表示现有的 DVD-ROM 的用户数据区的结构、用于从用户数据区的数据中解密加密的内容的光盘再现设备的结构框图。

具体实施方式

下面将参考附图对本发明的优选实施例进行描述。

第一优选实施例

图 1 表示根据本发明第一优选实施例的记录型光盘 100 的数据记录区平面图。此记录型光盘 100 是一种能够记录数字数据的记录介质，包括一次写入型非可重写光盘和可重写光盘。

参见图 1，101 表示导入区，用于在其中记录对光盘 100 的管理信息，102 表示用户数据区，用于在其中记录需要版权保护的数字数据，如（a）至少包括图像数据（包括静态画面图像和动态画面图像）如电影等和语言声音数据如音乐等其中之一的 AV 数据内容；和（b）计算机软件。103 表示导出区，用于在其中记录缺陷管理信息等。导入区 101 由在其中以预制凹坑的形式记录数据的只读区 104 和记录及再现区 105 构成，记录及再现区 105 是具有导槽的可重写区。在这种情况下，在只读区 104 中，

由制造者以预制凹坑的形式记录描述光盘 100 的物理特征的控制区等。在导出区 103 和可重写区 105 中，由光盘记录设备记录由光盘记录设备执行的写入测试的数据和管理光盘 100 上的缺陷的管理信息。另外，在导入区 101 中的只读区 104 的内周侧，当已经记录了内容的光盘 100 完成之后，通过下列已知的方法在光盘 100 上一次写入形成为盘专用信息的 BCA 106。

图 2A 表示在形成图 1 所示光盘 100 的 BCA 106 时的设备结构的框图和截面图。图 2B 表示在形成图 1 所示光盘 100 的 BCA 106 之后的光盘 100 的截面图和水平方向上反射光的强度曲线。

参见图 2A 和 2B，图中示出了双面记录型光盘 100 的一个实例，构成光盘 100，使得记录层 202、反射层 203、粘结层 204、反射层 205 和记录层 206 位于两片基底 201 和 207 之间。

当 BCA 记录在光盘 100 上时，如图 2A 所示，以带状形式记录相位编码调制后的数据，从而通过以脉冲的形式从高功率激光源 211 通过聚焦透镜 212 向例如光盘 100 的反射层 205 照射激光束重叠在凹点上，消除或除去反射层 205 的一部分。再现信号时，如图 2B 所示，由来自消除或去除了反射层 205 的部分的较低反射光量而产生的信号被间歇地再现。再现的信号被二值化后经过相位编码解调而再现。由此记录系统形成的 BCA 可以记录盘标识符，该标识符是对于每个光盘 100 的特定信息，并且 BCA 还有使已记录的数据不能被篡改的特点。

图 3 表示图 1 所示 BCA 106 的记录格式。如图 3 所示，在 BCA 106 中，记录同步码 301、检错码 302、纠错码 303 等以提高 BCA 数据 304 的读出因子。通过连接多个 BCA 数据 304，构成盘识别信息 305。在盘识别信息 305 中，有可以记录在用户数据区中的数据的类型和可以从用户数据区中再现的数据的类型。不能篡改 BCA 106 的数据，并且因此用户可以通过在制作光盘 100 时记录的盘识别信息将盘的使用限制在某个程度。

图 4 是图 1 所示的用户数据区 102 中扇区数据 401 的扇区结构。参见图 4，图 1 中所示的用户数据区 102 具有能以特定数量为单位进行存取的扇区结构，并且扇区数据 401 由头部 402、主数据 403 和检错码 404

构成。

主数据 403 是其中记录 AV 数据、计算机数据等的区域。在头部 402 中，记录数据 ID（数据标识符）405、ID 检错码 406、加扰控制信息 407、密钥信息 408 等。在数据 ID 405 中，记录用于识别扇区的逻辑地址等，并且提供 ID 检错码 406 以检测数据 ID 中的错误。加扰控制信息 407 是用于显示主数据是否被加扰的标志，以及在密钥信息 408 中，记录关于对主数据解扰的密钥的信息。作为关于密钥的信息，记录解扰密钥本身（在第一优选实施例的改型优选实施例中）或密钥索引（在第一优选实施例中），密钥索引是对于记录在光盘 100 另一区上的解扰密钥的指针。图 4 的实例表示记录密钥索引用于参考图 1 所示的密钥管理信息区 107 中记录的解扰密钥的的情形，它是光盘 100 的另一个区。

图 5 表示图 1 所示的密钥管理信息区 107 的结构。参见图 5，密钥管理信息区 107 由密钥信息区 501、内容信息区 502 和密钥索引列表区 503 构成。

在密钥信息区 501 中记录所记录的密钥区 504 的个数，并且密钥信息区 501 包括（a）解扰密钥区 505，该区是用于记录解扰密钥的区域，解扰密钥对已加扰的 AV 数据等进行解扰，和（b）密钥状态区 506，用于在其中记录解扰密钥区 505 中记录的解扰密钥的记录状态（表示未使用、区保留、被记录等）。在解扰密钥区 505 中记录多个解扰密钥，并且在密钥索引列表区 503 中记录表示解扰密钥区 505 中的存储位置的密钥索引。上述的多个解扰密钥可以通过该密钥索引查阅。在密钥状态区 506 中，把表示解扰密钥的记录状态的状态信息存储到可以由密钥索引查到的位置。

需要版权保护时，在内容信息区 502 中登记记录在光盘 100 上的内容，并且登记关于用于该内容的密钥的信息。在内容信息区 502 中，记录登记在密钥索引列表区 503 的内容 507 的个数和关于内容编号的内容信息 508。另外，在内容信息 508 中记录用于识别内容的内容 ID、用于该内容的解扰密钥的个数和对记录已使用的密钥的密钥索引列表 509 的指针。密钥索引列表区 503 是以内容单元的形式记录查阅用于内容所用的密钥的索引的区域。在密钥索引列表区 503 中记录用于查阅内容所用

的解扰密钥的整个记录区的密钥索引。

以这种方式构成的记录型光盘 100 能够根据内容所持有的版权的保护等级或利用等级，通过在盘识别信息上记录代表盘使用条件或状态的信息并通过用光盘和再现装置检测这种信息而控制记录操作和再现操作，其中盘识别信息是难于重写的信息，如区域标识符、数据类别标识符和制造时的盘标识符。因为记录数据使得其难于重写，以致于用户不能够改变数据，甚至在版权保护的内容被复制到另一个光盘时，盘识别信息不可以被复制，同时保持能够复制用户数据区。因此，因为存在不能在具有不同盘识别信息的光盘中解扰的用户数据区，通过在光盘上记录利用盘识别信息加扰的数据，可以防止正确的再现。

图 15A 是表示在第一优选实施例中、在记录内容时记录区域标识符的情况下，是否可以在相同区域或不同区域内复制或再现内容的示意图。图 15B 是表示在第一优选实施例中、在装运光盘时提前记录区域标识符的情况下，是否可以在相同区域或不同区域内复制或再现内容的示意图。

例如，如图 15A 所示，在装运光盘时不记录区域识别码、并且在记录和再现区中记录代表记录内容时可获得内容的区域的区域标识符的情形中，可以防止在另一个区域中使用。但是，内容可以记录在能够在另一个区域中使用的盘中（图 15A 所示的区域 RC2），并且可以正确地再现内容。在其中可以数字复制内容的记录介质配置有征税系统，保护版权持有者的利益，当光盘卖出时汇集附加费。但是，附加费根据国家而不同，并且不正当地使用要用在另一个国家中的记录介质时，存在版权持有者不能分享适当的利润的可能性。

如图 15B 所示，通过在装运之前以区域标识符不能篡改的方式提前记录，可以防止向在另一个区域中使用的光盘复制或再现内容。按照与上述类似的方式，在数据列表标识符记录为盘识别信息的情况下，可以通过记录数据所具有的类别标识符之间的比较，限制向可记录并可再现数据的盘上复制或再现内容。在把每个光盘的固有盘标识符记录为盘识别信息的情形中，记录的数据只能通过以盘标识符加密已记录的数据通过光盘获得。

在本优选实施例中，由盘识别信息加扰的数据可以是 AV 数据或是

需要版权保护的计算机数据，或者可以是用于对已加扰 AV 数据或计算机数据解扰的解扰密钥。

图 13 是按照第一优选实施例的改型优选实施例，根据加密的解扰密钥判断解扰密钥是否是正常的解扰密钥的方法的框图。如图 13 所示，通过给解扰密钥附加用于检测解扰密钥中的错误的检错码所获得的数据可以被利用盘识别信息进行加扰，从而计算可能记录在光盘上的加密的解扰密钥。在光盘再现设备中，加密的解扰密钥被解密成解扰密钥和检错码，从而通过根据解密的检错码中的奇偶校验检测错误，来判断解密的解扰密钥是否是正常的解扰密钥。例如，在利用不同的盘识别信息解扰的情况下，产生错误的解扰密钥，使得可以通过校验检错码来检测非正常的复制，其中检错码用于判断错误的解扰密钥不是正常解扰密钥。

作为记录盘识别信息的另一种方法，通过制备由多种类型的盘识别信息以预制凹坑的形式形成的模子（stamper）并通过用每个模子形成光盘，可以对由不同模子形成的各种光盘给出不同的使用限制。另外，通过利用秘密密钥对盘识别信息加扰，并通过在光盘上记录已加扰的识别信息，使用户不知道盘识别信息中描述的版权保护，能够进一步提高版权保护。

下面将参考图 6A 和图 6B 描述解扰密钥本身被记录为关于图 4 中（第一优选实施例的改型优选实施例）描述的密钥的信息的情形以及记录密钥索引的情形（第一优选实施例中），其中密钥索引是对记录在盘的另一个区中的解扰密钥的指针。图 6A 是根据第一优选实施例的改型的优选实施例，在图 1 所示扇区数据 401 中记录解扰密钥和 AV 数据的记录方法的框图。图 6B 是根据第一优选实施例，在图 1 所示扇区数据 401 中记录解扰密钥的密钥索引和 AV 数据的记录方法框图。

在图 6A 的情况下，在相同的扇区数据 401 中记录主数据 403 和解扰密钥，其中解扰密钥是对主数据 403 解扰所需的密钥信息 408a。因而，需要获得在记录 AV 数据时解扰所需的解扰密钥。也就是说，在记录 AV 数据时获得或购买密钥本身是不可避免的。

另一方面，在图 6B 的情况下，在相同的扇区数据 401 中记录主数据 403 和密钥索引，密钥索引是用于查阅记录解扰主数据 403 所必须的

信息的解扰密钥区的密钥信息 408，并且解扰密钥记录在由密钥索引指示的区域中。当记录 AV 数据时获得密钥 ID，该密钥 ID 指示对用于记录内容的密钥当中哪一个密钥进行解扰，并且还获得密钥信息 408，该信息是对应于来自密钥索引列表的密钥 ID 的密钥索引，密钥索引列表包含在内容信息中，它与主数据 403 一起被记录。当获得将要被记录在由密钥索引表示的解扰密钥区中的解扰密钥时，执行对解扰密钥的记录，其中密钥索引对应于密钥 ID。结果，可以独立地记录 AV 数据和对应于 AV 数据的解扰密钥。也就是说，可以独立地执行 AV 数据的记录和密钥的获取或购买，以致于当记录 AV 数据时，不必获取或购买密钥。用户可以使用记录内容并在实际再现时获取密钥的方法。

图 14 是根据第一优选实施例的改型优选实施例的解扰区管理表的结构示意图。在上述优选实施例中，为了使加密的内容与用于对其密码解扰的解扰密钥相关联，描述了记录密钥索引以对相同的扇区数据 401 查阅解扰密钥的情形，但是也可以使用图 14 中所示的解扰区管理表，该表管理记录加密内容的扇区的地址范围和解扰密钥之间的对应关系。此解扰区管理表以起始地址和结束地址表示记录加密内容的扇区的地址范围，并且当再现扇区的数据时查阅解扰密钥，然后解扰加密的内容。

为了获得记录的内容和用于记录的内容的解扰密钥，利用使内容可识别的内容 ID。如图 5 中所示，在记录于光盘上记录的内容信息区 502 内的内容管理列表中的内容信息中，记录内容 ID 和用于内容的解扰密钥的列表。通过具有这样的列表结构，即多个解扰密钥可以用于一条内容，可以得到这样的服务，即可以出售内容的一部分或软件的一部分。

在参考图 13 的上述改型的优选实施例中，当把数据不正当地复制到另一张盘上时，其中，在盘识别信息中对附加有诸如校验和或循环冗余校验码这样的检错码的解扰密钥进行加扰，通过用不同的盘识别信息解扰，将其检测为错误。在这种情况下，还可以获得通过记录在光盘上的盘识别信息加扰的解扰密钥，并且通过以所获得的解扰密钥替换该解扰密钥，形成能够正确再现的盘。

图 1 中所示的密钥管理信息区 107 被记录在可重写的导入区 101 中。一般地，用户数据区 102 包括可以从个人计算机的驱动设备存取的用户

区和关于光盘上的缺陷扇区的空余区，并且对于传统的 READ 命令和 WRITE 命令，只有用户区可以作为逻辑连续区进行存取。通过把密钥管理信息放入到导入区 101 中，可以防止直接从个人计算机的驱动设备等进行存取，以致于可以使得不能从个人计算机获得用于解扰已加扰的 AV 数据等的密钥。

第二优选实施例

图 7 是根据本发明第二优选实施例的光盘介质和再现设备的结构框图。提供此光盘记录和再现设备用于针对根据第一优选实施例的光盘 100，记录如图像数据或音乐数据这样需要版权保护的 AV 数据的内容。

参见图 7，701 表示第一优选实施例的光盘，702 表示光学头，它是由半导体激光器和光学元件构成的光学拾取器，703 表示用于控制半导体激光器的工作并将再现的信号二值化的记录和再现控制电路。704 表示调制和解调电路，用于数字调制要被记录的数字数据并数字解调二值化的再现信号，705 表示检错和纠错电路，用于对由光盘 701 上的划痕、尘埃等导致的错误进行检错和纠错处理，并用于执行检错和纠错处理所需的纠错码产生处理。706 表示用于工作存储器的 RAM 的缓冲存储器和检错和纠错电路 705 的数据缓冲存储器，707 表示对已加扰的记录 AV 数据进行解扰的解扰电路，708 表示用于扩展压缩记录动态图像数据等的 MPEG 解码电路。709 表示用于 D/A 转换扩展图像数据以产生并输出视频信号和音频信号的输出电路，710 表示用于控制光盘记录和再现设备的整体操作的控制 CPU，711 表示用于获取对设置在内容中的密码解扰的解扰密钥的通讯电路。712 表示数据接收电路，用于从如机顶盒等通讯终端设备接收如图像数据和音乐数据等加密内容的数字数据。

下面将描述如上所述构成的图 7 的光盘记录和再现设备的数据记录操作。在通过数据接收电路 712 进行接收之后，将从如机顶盒或 MPEG 编码器等通信终端设备传输过来的如图像数据或音乐数据等已加密内容的数字数据暂时存储在缓冲存储器 706 中。检错和纠错电路 705 产生检错和纠错处理所需的检错和纠错码以重新构建数字数据，其中错误是由于光盘 701 上的划痕或尘埃等而在存储内容的数字数据中产生的。对于

检错和纠错码，使用如公知的 Reed-Solomn 这样的码。在这种情况下，重新构成的记录数据包括内容的数字数据和检错和纠错码。调制和解调电路 704 在记录时利用调制系统（例如 8/16 调制系统）并数字调制记录数据。另外，记录和再现控制电路 703 根据数字调制的记录数据调制从光学头 702 输出的激光束的功率强度，使得激光照射到光盘 701 上，把记录数据记录到光盘 701 上。

图 8 是表示由图 7 所示的光盘记录和再现设备的控制 CPU 710 执行的 AV 数据记录处理的流程图。

参见图 8，首先，在步骤 S801 中，在 AV 数据的记录之前从光盘 701 上再现导入区 101 的盘识别信息，然后在步骤 S802 中，根据记录在盘识别信息中的用户数据区 102 中的可记录数据的类型或种类，判断是否能够记录目前要记录的内容的数字数据。在步骤 S802 为肯定的情况下，流程继续到步骤 S803，而在否定的情况下，记录操作在步骤 S810 停止，并且 AV 数据的记录过程结束。

在步骤 S803 中，再现密钥管理信息记录在导入区 101 的扇区数据，并且在步骤 S804，判断是否为在再现的密钥管理信息中记录内容所需的密钥信息分配一个区域。在步骤 S804 为否定的情况下，在为把密钥信息记录到密钥管理信息区 107 而分配一个区域之后，流程继续到步骤 S806。另一方面，在步骤 S804 为肯定的情况下，程序流程直接进行到步骤 S806。

在记录内容的情况下，光盘记录和再现设备的控制 CPU 710 通过数据接收电路 712 从通讯终端设备接收加密内容的记录数据和与用于解扰密码的解扰密钥有关的信息。在这种情况下，与密钥有关的信息是用于内容的密钥本身，或是指示它对应于整个内容中采用的密钥中的哪一个密钥的密钥 ID。在接收到密钥 ID 的情况下，在步骤 S806 中，接收到的密钥 ID 被转换成密钥索引，该密钥索引是用于指示记录了对应于密钥 ID 的解扰密钥的区域的指针，并且把转换后的解扰密钥放置到扇区的头部区，在该头部区中记录了用解扰密钥解密的内容的数据。然后，在步骤 S807 中，控制 CPU 710 通过控制记录和再现控制电路 703、调制和解调电路 704 以及检错和纠错电路 705 执行下列记录数据处理。在此处理过程中，把检错和纠错码附加到希望被记录的扇区数据上，并且再利用调

制系统，如公知的 8/16 调制系统，数字调制附加了这些码的扇区数据，从而控制光学头 702，使其位于预定的记录位置，并且根据数字调制的记录数据调制激光束的强度。通过这样，把记录数据记录到光盘 701 上，并且另外，在步骤 S808 中，判断内容的记录是否完成，并且在否定的情况下，流程返回到步骤 S806，重复上述处理。在步骤 S808 为肯定的情况下，在步骤 S809 中把更新后的密钥管理信息记录在光盘 701 上的密钥管理信息区 107 中，然后结束 AV 数据的记录过程。

图 9 是表示由图 7 所示的光盘记录和再现设备的控制 CPU 710 执行的密钥管理信息区的分配处理的流程图。提供此过程为在记录内容数据之前分配用于记录解扰密钥的区域。

参见图 9，在步骤 S901 中，获得例如关于从电子节目指南等记录的内容密钥的信息（包括所使用的解扰密钥的个数），然后在步骤 S902 中，再现记录于光盘 701 的密钥管理信息区 107 内的密钥管理信息。然后在步骤 S903 中，从密钥状态区 506 中搜索解扰密钥区 505 的空区，从而判断是否可以记录用于要被记录的内容的解扰密钥。在步骤 S903 为否定的情况下，记录操作在步骤 S907 停止，并且结束分配过程。另一方面，在步骤 S903 为肯定的情况下，将要被记录的内容登记到内容信息区 502 之内的内容列表中，通过在对应的密钥状态区中设置区域保留标志，分配记录区，以便保留在步骤 S905 中在解扰密钥区 505 中记录解扰密钥所需的区域。另外，在步骤 S906 中，指示用于记录解扰密钥的分配区的密钥索引形成为密钥列表，并且在分配了设置为内容信息的指针之后，结束分配过程。

图 10 是表示由图 7 所示的光盘记录和再现装置的控制 CPU 710 执行的解扰密钥的记录处理的流程图。提供此记录过程用于记录从光盘 701 中的密钥管理中心所获得的解扰密钥。

参见图 10，首先，在步骤 S1001 中，当光盘 701 上导入区 101 的盘识别信息被再现之后，盘识别信息和用于识别解扰期望的内容所需密钥的密钥 ID 通过通讯电路 711 传送给密钥管理中心，以便在步骤 S1002 从密钥管理中心获得解扰密钥。在密钥管理中心，选择解扰来自给定的密钥 ID 的内容所需的解扰密钥，从而利用如传送的盘识别信息等信息对解

扰密钥进行加密，并将其返回。

在步骤 S1003 中通过通讯电路 711 从密钥管理中心获得对应于密钥 ID 的解扰密钥之后，再现密钥管理信息区 107 的数据，使得在步骤 S1004 中从再现的密钥管理信息区 107 内的数据中，由密钥 ID 指示的密钥索引列表中获得指示用于记录解扰密钥的区域的密钥索引。然后在步骤 S1005，把以上获得的解扰密钥分配到由密钥索引指示的解扰密钥区，并且设置用于指示在对应的密钥状态区 506 获得的密钥的获得标志。另外，在步骤 S1006 中，判断是否完成了所有密钥的获取，并且在否定的情况下通过返回到步骤 S1003 而重复上述处理。另一方面，在步骤 S1006 为肯定的情况下，在步骤 S1007 中在密钥管理信息区 107 中记录更新后的密钥管理信息，并且结束解扰密钥记录过程。

接下来，将参考图 7 对本实施例的光盘记录和再现设备的数据再现操作进行描述。记录在光盘 701 上的数字数据按下列方式再现。来自半导体激光器的激光束从光学头 702 照射到光盘 701 上，使得此时光盘 701 上反射的反射光通过光学头 702 进入到记录和再现控制电路 703 中。在光电转换进入的反射光之后，记录和再现控制电路 703 通过执行放大和二值化处理，产生并输出所产生的再现二值化信号给调制和解调电路 704。调制和解调电路 704 通过利用诸如公知的 8/16 调制系统之类的调制系统在记录时把数字调制信号数字解调成数字信号，然后把所得的数字信号输出给检错和纠错电路 705。然后，检错和纠错电路 705 利用缓冲存储器 706 作为工作存储器，执行对光盘 701 上由于划痕或尘埃导致的检错和纠错处理。此检错和纠错处理通过解码例如公知的 Reed-Solomn 码执行。

被进行了检错和纠错处理的再现数据被输出给解扰电路 707 以执行解扰处理。解扰电路 707 事先使用在数据再现之前再现的密钥管理信息区 107 的解扰密钥，并且对再现的数据执行解扰处理，然后输出给 MPEG 解码电路 708。然后，MPEG 解码电路 708 扩展压缩的动态图像数据和音乐数据，并且再把扩展的数据输出给输出电路 709。另外，输出电路 709 把输入的扩展数据 D/A 转换成视频和音频数据，并且把所得的视频和音频信号输出给上层设备，如电视机、音响设备等。

图 11 是表示由图 7 所示的光盘记录和再现装置的控制 CPU 710 执行的 AV 数据再现处理的流程图。

参见图 11，首先，在步骤 S1101 中，在向光盘 710 中记录 AV 数据之前再现导入区 101 内的盘识别信息，并且在步骤 S1102，根据记录于盘识别信息中的可再现数据的类型，判断是否能够再现希望当前被再现的内容。在步骤 S1102 为否定的情况下，再现操作在步骤 S1112 停止，并且然后结束 AV 数据的再现处理。另一方面，在步骤 S1102 为肯定的情况下，密钥管理信息被记录于导入区 101 的密钥管理信息区 107 内的扇区中的数据被再现，并且在步骤 S1104 判断再现内容所需的密钥信息是否被记录在密钥管理信息中。在步骤 S1104 为肯定的情况下，程序流程直接进行到步骤 S1106。另一方面，在步骤 S1104 为否定的情况下，在步骤 S1105 中，通过通讯电路 711 从管理密钥的密钥管理中心获得解扰密钥，并且记录到光盘 701 上的密钥管理信息区 107，然后，程序流程进行到步骤 S1106。

然后，在步骤 S1106 中，控制 CPU 710 使得光学头 702 移动到光盘 701 的用户数据区，并且控制记录和再现控制电路 703、调制和解调电路 704 以及检错和纠错电路 705，使得 AV 数据被再现。然后，在步骤 S1107 中，从包含在再现扇区的头部中的密钥索引所指示的解扰密钥区 505 中获得解扰扇区数据所需的解扰密钥，然后，在步骤 S1108 中，通过利用盘识别信息的解扰对解扰密钥的加扰信息进行解码。另外，在步骤 S1108 中，通过检查附加到解扰密钥的检错码，判断解扰密钥中是否有错误。在步骤 S1108 为肯定的情况下，将内容判断为非法获得的（或不合法地复制了内容），再现操作在步骤 S1112 停止，并且结束 AV 数据的再现处理。

另一方面，在步骤 S1108 为否定的情况下，内容的数据在步骤 S1109 通过解扰密钥解扰，并且在步骤 S1110 把解扰后的 AV 数据输出给 MPEG 解码电路 708。然后，控制 CPU 710 通过控制 MPEG 解码电路 708 和输出电路 709，通过预定的 MPEG 系统，对解扰后的 AV 数据进行 MPEG 扩展，并且 MPEG 扩展后的 AV 数据被 A/D 转换成视频信号和音频信号，输出给上层设备，如电视机和音响设备等。然后，在步骤 S1111 中，判

断是否完成了内容的再现，并且在否定的情况下，程序流程返回到步骤S1106，重复上述处理。另一方面，在步骤 S1111 为肯定的情况下，结束AV 数据的再现处理。

在步骤 S1109 中检测到错误的情况下，内容被认为是不合法地获得的，例如内容被认为是不合法地复制的，再现操作停止。但是，可以通过通讯电路 711 从管理密钥的密钥管理中心获得密钥信息，并通过与未记录任何密钥的情形相同的方式执行步骤 S1105 的处理，将其记录到光盘 701 的密钥管理信息区 107 中。通过这样，通过以合法的程序获得密钥，即使是复制的 AV 数据也是可再现的。

图 12 是表示由图 7 所示的光盘记录和再现装置的控制 CPU 710 执行的解扰密钥的获取处理的流程图。此处理提供用于从再现的密钥索引中再现解扰密钥，并且此处理在图 11 所示的 AV 数据再现处理之前执行。

参见图 12，首先在步骤 S1201，判断在再现的扇区中的数据是否被加扰控制信息加扰，并且在否定的情况下，程序流程进行到步骤 S1206。另一方面，在步骤 S1201 为肯定的情况下，在步骤 S1202 中，通过再现记录于与上述扇区相同的扇区中的密钥信息获得密钥索引，并且然后，在步骤 S1203 中，从解扰密钥区 505 中获得由上述密钥索引指示的解扰密钥，之后，在步骤 S1204，通过利用盘识别信息解扰所获得的解扰密钥，并且通过检查检错码，判断在解扰密钥中是否存在错误。在步骤 S1204 为肯定的情况下，再现操作在步骤 S1205 停止，并且结束解扰密钥的获取处理。另一方面，在步骤 S1204 为否定的情况下，程序流程进行到步骤 S1206。当再现的扇区未被加扰或作为通过盘识别信息对解扰密钥解扰的结果、没有发现任何错误时，允许在步骤 S1206 的再现操作，再现扇区的数据被输出，并且结束解扰密钥的获取处理。

如上所述，在根据本发明优选实施例的光盘以及光盘记录和再现设备中，可以由用户使用在盘制造阶段制作的只读的盘识别信息控制记录和再现操作。另外，通过利用上述盘识别信息对一部分数据进行加扰，可以防止正常再现用户数据区被物理复制的盘上数据。另外，通过在不同于数据区的区域中分配数据解扰所需的解扰密钥，可以独立地执行内容的记录和解扰密钥的记录。因而，如果需要，通过记录内容并通过获

取解扰密钥，例如当再现内容数据时，可以将内容保持为可再现的状态。此时，通过用盘识别信息对解扰密钥进行加扰，可以按照与以上相同的方式明确地防止通过物理复制的不合法使用。除此之外，通过从密钥管理中心合法地获得用光盘的盘识别信息加扰的解扰密钥，并通过在光盘中记录所获得的解扰密钥，非法复制的盘可以变成能够被正常再现的光盘。

虽然以上描述的是将已加密数据输入到光盘记录和再现设备中，但通过提供用于在光盘记录和再现设备中加密内容的电路，可以通过加密输入内容的数据和在光盘上记录该数据而获得相同的效果。

虽然在本优选实施例中通过利用盘识别信息只对解密已加密内容所需的解扰密钥进行加密，防止了具有不同盘识别信息的盘之间的复制，可以通过利用盘识别信息对内容本身进行加密而防止复制。另外，通过利用秘密密钥对盘识别信息进行加密，可以使对记录在盘上的内容的非法解密更加困难。

第一和第二优选实施例的优越效果

本发明优选实施例的光盘将执行每个光盘的用户数据区的记录操作和再现操作的盘识别信息记录在不可重写的只读区中，因此光盘可以通过用户利用制作光盘时记录的信息控制内容向光盘上的记录操作和内容从光盘再现的操作。

根据本发明优选实施例的光盘可以防止盘识别信息被复制，以便甚至在由用户通过在光盘的用户数据区中记录加密的数据把用户数据区信息复制到不同的记录型光盘上的情况下，不能正确解码和再现数据，其中加密的数据是利用不可能被重写的只读型盘识别信息的密钥加密的。

根据本发明优选实施例的光盘使得能够独立地执行下列操作：（a）获得需要版权保护的数据如电影、音乐；和（b）通过在不同的扇区内记录加密的数据和用于对加密的内容解扰的解扰密钥获得对加密的内容解密的解扰密钥。另外，通过用盘识别信息的密钥加密并记录解扰密钥，甚至在用户数据区信息被用户复制到另一记录型光盘上时，盘识别信息也不能被复制，并且不可能正确地解码和再现数据，并且通过获取并记

录已加密的解扰密钥，其中该解扰密钥以被复制的光盘上的盘识别信息为密钥进行加密，使得不能正确解码并再现数据。

第三优选实施例

接下来，将参考附图对本发明的第三优选实施例的加密内容记录和再现方法进行描述。图 16 是本发明第三优选实施例的光盘 1101 的数据记录区的平面图。

参见图 16，1101 表示可以记录数字数据的记录介质，它是记录型光盘，如可重写或不可重写的光盘，1102 表示控制用户数据区，在其中以微小凹凸凹坑的形式记录盘信息，1103 表示用户数据区，用户通过向光盘照射激光束而记录数据。1104 表示其中记录盘 ID 的 BCA。在 BCA 1104 中，控制用户数据区 1102 内周圆部分中微小的凹凸凹坑上的记录膜通过用脉冲激光器，如 YAG 激光器等，局部地照射到记录膜上而被修整，使得在径向形成多个伸长形状的修整区 1105，由此记录盘 ID，该盘 ID 是已解扰的识别信息。

图 17 是表示根据第三优选实施例的 BCA 再现电路 1401 中再现的信号 1201 和再现的二值化信号 1207 的信号波形的信号波形图，图 18 是表示根据第三优选实施例的 BCA 再现电路 1401 结构的框图。图 17 表示再现 BCA 1104 的数据时的再现信号 1201。在图 18 中，1301 表示个光学拾取器，1302 表示前置放大器，1303 表示低通滤波器（LPF），1304 表示二值化电路，1305 表示解调电路。

参见图 18，从光学拾取器 1301 输出的激光束照射到光盘 1101 的 BCA 1104，并且反射光被光学拾取器 1301 光电转换，并且之后，已经被光电转换的电信号被前置放大器 1302 放大以获得再现信号 1201。在这种情况下，图 17 所示的再现信号 1201 具有对应于控制用户数据区 1102 的凹凸凹坑的电平，并且在此再现信号 1201 中，1202、1203 和 1204 中的每一个均表示修整部分，当记录膜通过脉冲激光的修整处理而被除去时，发出凹凸凹坑形式的信号。此修整处理由光盘制造商执行。

参见图 18 进行描述，再现的信号 1201 被输入给低通滤波器 1303，低通滤波器 1303 除去由凹凸凹坑形成的调制信号，并且之后向二值化电

路 1304 输出所得的信号。输入到二值化电路 1304 的再现信号被利用限幅电平 1206 二值化，该电平是显著低于取代正常限幅电平 1205 的电平，限幅电平 1205 二值化控制用户数据区 1102 的信号，获得再现的二值化信号 1207。从二值化电路 1304 输出的再现的二值化信号 1207 被解调电路 1305 解调，获得盘 ID 信号 1306。

如上所述，通过增加用于识别光盘的盘识别信息，可以很容易地执行光盘的管理。另外，通过记录以凹凸凹坑形式记录 BCA 1104，可以防止 BCA 1104 中用于识别光盘的信息被很容易地篡改。另外，因为图 16 所示的控制用户数据区 1102 和 BCA 1104 彼此相邻，所以当控制用户数据区 1102 的数据被再现时，可以连续地再现 BCA 1104 的数据，或者当 BCA 1104 的数据被再现时，可以连续地再现控制用户数据区 1102 的数据，并且因此可以加速获得 BCA 1104 的信息的处理，其中 BCA 1104 的信息用于例如当光盘被启动时 CPU 快速识别光盘，并记录加密的内容。

虽然形成优选实施例的 BCA 1104 以修整控制用户数据区 1102 的内周边部分中凹凸凹坑形式的记录膜，但构成记录型光盘的记录膜与形成在只读光盘上的反射膜相比很容易受到热的影响，其中记录型光盘是可重写光盘或非可重写光盘。通过修整控制用户数据区 1102 的内周边部分，与修整外周边的情形相比，可以保护用户数据区 1103 免受修整时发出的热的影响。另外，在控制用户数据区 1102 的内周侧形成 BCA 1104 的原因在于在激光束的光斑直径由于激光器设备的聚焦伺服电路的不稳定性而改变的情况下应该考虑一定的余量。

修整之前记录在 BCA 1104 中的数据可以记录在控制用户数据区 1102。记录在 BCA 1104 中的数据也可以记录在控制用户数据区 1102 中，并且这导致可以保护控制用户数据区 1102 的以上数据免于修整。另外，当记录在 BCA 1104 中的数据被从 BCA 1104 连续并反复地记录到控制用户数据区 1102 时，可以通过找到控制用户数据区 1102 的以上数据而预测 BCA 1104 的位置。

接下来，将描述通过网络在具有上述 BCA 1104 的光盘 1101 上记录由盘 ID 加密的内容的过程。在第三至第五实施例中，网络表示如因特网、公共电话线或其它通讯线，如导线或电路。图 19 是根据第三优选实施例

的光盘记录和再现系统的结构框图，它表示用于在记录型光盘 1101 上记录加密内容的设备结构，它可以是具有上述 BCA 1104 的可重写光盘或非可重写光盘。

参见图 19，光盘记录和再现系统由通过如因特网等网络 1405 彼此相连的光盘记录和再现设备 1410 和加密部分 1406 构成。光盘记录和再现设备 1410 包括光学拾取器 1301、BCA 再现电路 1401，因特网 403、记录电路 1411、数据再现部分 1412 和加密解码器 413。另外，加密部分 1406 包括接口 1404、内容存储器 1407 和加密编码器 1408。

首先，从光学拾取器 1301 输出的激光束照射例如 RAM 型光盘 1101 的 BCA 1104，并且在反射光被光学拾取器 1301 光电转换之后，已经被光电转换的再现信号被输入到 BCA 再现电路 1401。BCA 再现电路 1401 根据输入的再现信号再现 BCA 内的盘 ID 信号 1402，把再现的盘 ID 信号 1402 输出给加密解码器 1413，并且同时还把相同的盘 ID 信号 1402 经接口 1403 和 1404 以及网络 1405 输出给加密部分 1406 的加密编码器 1408。加密编码器 1408 对内容的数据加密或对图像和语音的内容数据加扰，使得盘 ID 信号 1402 变为对光盘 1101 上的加密内容进行解密的解密密钥，其中将内容存储器 1407 中的内容数据记录在光盘 1101 上。

在本优选实施例中，利用盘 ID 信号 1402 作为密码密钥来加密内容 1407 的处理与加密处理表示相同的含义。另外，在本优选实施例中，加密和解密被认为是锁和钥匙的关系，以致于用钥匙进行锁定被称作加密，用钥匙进行开锁被称作解密。因此，加密和解密在实际操作中彼此不同，但是，用于加密和解密的钥匙却彼此相同。内容 1407 由 C 表示，盘 ID 信号 1402 由 BCAS 表示，加密的内容 1409 由 C[BCAS]表示，并且加密处理的操作由*表示。下列方程可以表示为：

$$C*BCAS=C[BCAS] \qquad (1)$$

由加密部分 1406 加密的内容 1409 经接口 1403 和 1404 以及网络 1405 发送给记录和再现设备 1410 的记录电路 1411。记录电路 1411 以预定的方式数字调制输入内容的数据，并通过调制与数字调制的数据相对应的

从光学拾取器 1301 发出的激光束的强度和把激光束照射到光盘 1101 上把内容的数据记录到光盘 1101 上。

接下来，当再现被加密并记录到光盘 1101 上的内容时，从光学拾取器 1301 输出的激光束照射到记录上述用户数据区 1103 的加密内容的区域，并且在反射光被光学拾取器 1301 光电转换之后，将被光电转换的再现信号输入到数据再现部分 1412。数据再现部分 1412 把输入的再现信号 A/D 转换成数字数据，并且把数字数据输出给加密解码器 1413。另一方面，从光学拾取器 1301 发出的激光束照射到光盘 1301 的 BCA 1104 上，并且在反射光被光学拾取器 1301 光电转换之后，将已经被光电转换的再现信号输入 BCA 再现电路 1401。BCA 再现电路 1401 A/D 转换输入的再现信号，以产生盘 ID 信号 1402，并再把盘 ID 信号 1402 输出给加密解码器 1413。

加密解码器 1413 把输入的盘 ID 信号 1402 用作对加密内容的数据解密的密钥。此时，当把内容合法地记录到光盘 1101 上时，用于对记录在光盘 1101 上的加密内容解密的密钥是光盘 1101 的盘 ID 信号 1402，并且再现时从 BCA 再现电路 1401 输出的盘 ID 信号 1402 也是光盘 1101 的盘 ID 信号（BCAS）。因此，被解密或解扰的内容从加密解码器 1413 输出，作为输出信号 1414。当解码处理的操作用#表示时，下列方程可以表示为：

$$C[BCAS]\#BCAS=C \qquad (2)$$

在这种情况下，当内容的数据是图像数据时，扩展诸如 MPEG 信号之类的图像数据，以获得图像信号的数据。

如上所述，本优选实施例的加密具有盘 ID，作为密钥，并且因为对应于一个光盘只存在一个盘 ID，所以有这样一个有益的效果，即只能在该光盘上记录相同的加密内容。也就是说，当试图从具有盘 ID 为 ID1 的合法光盘向具有另一盘 ID 为 ID2 的光盘上复制并再现以上描述的内容 1407 时，从 BCA 再现电路 401 输出 ID2 作为盘 ID 信号 1402。但是，加密的内容是用 ID1 的盘 ID 信号进行加密的，因此，加密解码器 1413

不能对加密的内容解码。

加密编码器 1408 不位于内容的供应源处，而是位于网络中记录和再现设备侧，可以以其上安装有加密解码器的 IC 卡等形式形成。另外，因为上述光盘 1101 只利用盘 ID 进行加密，所以可以用任意的具有 BCA 再现电路 1401 和加密解码器 1413 的光盘记录和再现设备再现数据。

第四优选实施例

接下来，参见附图对根据本发明第四优选实施例的加密内容记录方法进行描述。图 20 是根据第四优选实施例的光盘记录和再现系统的结构框图，表示用于在作为具有 BCA 的可重写光盘或非可重写光盘的记录型光盘上记录加密内容的设备结构。在第四优选实施例中，省去对与第三优选实施例共用元件的描述。

参见图 20，根据第四优选实施例的光盘记录和再现系统包括 CATV 公司设备 1501、密钥发行中心设备 1507、CATV 解码器 1506、光盘记录和再现设备 1514 和电视机 1530。在这种情况下，CATV 公司设备 1501 包括用于存储如电影软件等内容的数据的内容存储器 1502、用于存储第一加密密钥的第一加密密钥存储器 1503 和第一密码编码器 1504。另外，密钥发布中心设备 1507 包括用于控制设备 1507 的操作的控制部分 1507a、用于存储时限信息的时限信息存储器 1510 和用于存储限定容许码的记录容许码存储器 1511。另外，CATV 解码器 1506 包括用于存储 CATV 解码器 1506 的系统 ID 的系统 ID 存储器 1508、第一密码解码器 1513、第二密码编码器 1516 和设置在 IC 卡 1522 中的公司识别信号存储器 1523。另外，光盘记录和再现设备 1514 包括记录电路 1518、数据再现部分 1519、BCA 再现电路 1521、第二密码解码器 1520 和设置在 IC 卡 1524 中的公司识别信号存储器 1526。

首先，CATV 公司设备 1501 的第一密码编码器 1504 利用存储在第一加密密钥存储器 1503 中的第一加密密钥对存储在内容存储器 1502 中的诸如电影软件之类的内容数据加密，由此产生第一加密内容 1505。然后，通过网络为每个用户把产生的第一加密内容 1505 传递给 CATV 解码器 1506 的第一密码解码器 1513。当存储在内容存储器 1502 中的数据由

C 表示，第一加密密钥 1503 由 FK 表示，并且第一加密内容 1505 由 C[FK] 表示时，下列方程表示为：

$$C*FK=C[FK] \qquad (3)$$

CATV 解码器 1506 通过网络把下列内容传送到密钥发布中心设备 1507，

（a）存储在系统 ID 存储器 1508 中的 CATV 解码器 1506 的系统 ID；和

（b）例如利用 CATV 解码器 1506 的键盘（未示出）输入的标题码 1509，它被事先附加到将被记录到音频型或 RAM 型光盘 1101 上的上述内容中。在这种情况下，标题码 1509 可以通过根据 TV 屏幕的选择输入，或可以利用键盘直接输入，也可以从遥控器等输入。因此，可以通过用户以其自己的方式的采集获得标题码 1509，或者可以与第一加密内容 1505 一起输入给 CATV 解码器 1506。标题码 1509 可以事先在不同于第一加密内容 1505 的时间以诸如节目指南之类的形式发送。

根据 CATV 解码器 1506 的系统 ID 和上述内容的标题码 1509，密钥发布中心设备 1507 的控制部分 1507a 查阅存储在时限信息存储器 1510 中的时限信息和存储在记录容许码存储器 511 中的记录容许码，并与记录容许码和时限码一起通过网络向 CATV 解码器 1506 的第一密码解码器 1513 发射对应于记录容许码和时限码的这些数据的密钥（K）1512。时限信息使得能够在不同时间多次广播相同内容的情况下区分相同的内容。当第一解密密钥由 FK 表示、CATV 解码器 1506 的系统 ID 由 DID 表示、时限信息由 TIME 表示、记录容许码由 COPY 表示，并且内容的标题码 1509 由 T 表示时，密钥（K）满足下列方程表示的关系：

$$FK=K*T*DID*TIME*COPY \qquad (4)$$

根据例如当 CATV 公司设备 1501 判断广播内容是否是新任务或旧任务时的判断结果，判断存储在记录容许码存储器 1511 中的记录容许码

是只针对观看和收听，还是针对观看、收听和记录。

当第一解密密钥（FK）、密钥（K）1512、上述内容的标题码 1509、系统 ID、记录许可码和时限信息满足上述关系、并且从时钟电路 1527 输出的目前时间信息满足时限信息的条件时，CATV 解码器 1506 的第一密码解码器 1513 对第一加密内容 1505 进行解密。在这种情况下，当上述加密内容是图像信号时，将解扰后的图像信号从第一密码解码器 1513 输出到电视机 1530，然后，用户可以观看图像信号的图像，收听对应于图像信号的音频信号。在这种情况下，第一密码解码器 1513 的解密处理由下列方程表示：

$$C[FK]\#(K*T*DID*TIME*COPY)$$
$$=C[FK]\#FK$$
$$=C \qquad (5)$$

当记录许可码只允许观看和收听时，内容数据可以记录在光盘 1101 上，但是，当观看和收听以及记录都允许时，可以把内容数据记录在光盘 1101 上。因此，此方法描述如下。

光盘记录和再现设备 1514 的 BCA 再现电路 1521 再现光盘 1101 的 BCA 1104 的数据，获得盘 ID 信号 1515，并把盘 ID 信号输出给 CATV 解码器 1506 的第二密码编码器 1516。CATV 解码器 1506 的第二密码编码器 1516 利用盘 ID 信号 1515 作为第二加密密钥对从第一密码解码器 1513 输出的内容数据加密，以产生第二加密内容 1517，并把产生的第二加密内容 1517 输出到光盘记录和再现设备 1514 的记录电路 1518。应该注意，第二密码解码器 1516 的上述加密被限定在第一加密内容被解密并从第一密码解码器 1513 输出的时间。作为来自第一密码解码器 1513 的输出信号的内容由 C 表示，作为第二加密密钥的盘 ID 信号 1515 由 BCAS 表示，并且第二加密内容 1517 由 C[BCAS]表示，则能够表示成下面的方程：

$$C*BCAS=C[BCAS] \qquad (6)$$

发送到光盘记录和再现设备 1514 的记录电路 1518 的第二加密内容 1517 利用例如公知的 8/16 调制系统调制到记录电路 1518，并且调制后的信号由光学拾取器（未示出）记录在光盘 1101 上的用户数据区 1103 中。当再现上述被加密并记录在光盘 1101 上的内容时，从光学拾取器输出的激光束照射到光盘 1101 上的记录了上述加密内容的区域上，以致于反射光进入到光学拾取器。上述光学拾取器把进入的反射光光电转换成再现的电信号，并把已经被光电转换的再现信号输出到数据再现部分 1519。数据再现部分 1519 把输入的再现信号 A/D 转换成数字再现信号，并且数字再现信号被输出到第二密码解码器 1520。

另一方面，从光学拾取器输出的激光束照射到光盘 1101 的 BCA 1104 上，以致于反射光进入到光学拾取器。上述光学拾取器把进入的反射光光电转换成再现的电信号，并再把已经被光电转换的电信号输出给 BCA 再现电路 1521。BCA 再现电路 1521 根据输入的再现信号产生盘 ID 信号 1515，并且把产生的盘 ID 信号输出给第二密码解码器 1520。响应于盘 ID 信号，第二密码解码器 1520 利用输入的盘 ID 信号 1515 作为密钥对来自数据再现部分 1519 的再现加密内容解密。此时，在内容被非法地记录到光盘 1101 上的情况下，用于对记录在光盘 1101 上的加密内容解密的密钥是光盘 1101 的盘 ID，并且从 BCA 再现电路 1521 输出的盘 ID 信号也是光盘 1101 的盘 ID 信号（BCAS），因此，第二密码解码器 1520 可以正常地执行解密处理。因此，解密的或解扰的内容数据被作为输出信号 1525 从第二密码解码器 1520 中输出。在这种情况下，第二密码解码器 1520 的解密处理可以表达成下列方程。当数据内容是图像信号时，第二密码解码器 1520 扩展例如 MPEG 信号，再现原始图像信号，并输出图像信号。

$$C[BCAS]\#BCAS=C \qquad (7)$$

只利用盘 ID 信号（BCAX）1515 对上述光盘解密 1101，并且因此可以通过任意的包括 BCA 再现电路 1521 和第二密码解码器 1520 的光学

记录和再现设备再现内容。虽然在上述叙述中加密编码器 1504 和 1516 执行加密并且加密解码器 1513 和 1520 执行解密，但加密和解密可以通过这样一种结构执行，即在由 CPU 执行的程序中包括用于加密算法的程序和用于解密算法的程序，其中 CPU 是每个设备 1501、1506 和 1514 的控制部分。

虽然在本优选实施例中，CATV 解码器 1506 的第二密码编码器 1516 利用盘 ID 信号 1515 作为第二密码密钥对内容加密，但是也可以按照下列方式对内容加密。例如，可以把为每个 CATV 公司设备 1501 准备的 IC 卡 1522 安装到 CATV 解码器 1506 上，并且 IC 卡 1522 的公司识别信息存储器 1523 内记录的公司识别信号和由 BCA 再现电路 1521 再现的盘 ID 信号（BCAS）可以合并成第二密码密钥，用于通过第二密码编码器 1516 对内容加密。来自第一密码解码器 1513 的输出信号的内容用 C 表示，作为第一密码密钥的盘 ID 信号 1515 用 BCAS 表示，作为第二密码密钥的公司识别信号 1523 用 CK 表示，并且第二加密内容 1517 用 C[BCAS,CK] 表示。于是，第二密码编码器 1516 的加密处理由下列方程表示：

$$C*BCAS*CK=C[BCAS,CK] \qquad (8)$$

接下来，当再现加密并记录在光盘 1101 上的内容时，从光学拾取器输出的激光束照射到光盘 1101 上记录了上述加密内容的区域上，以致于反射光进入到光学拾取器。光学拾取器把进入的反射光光电转换成再现的信号，并在把已经被光电转换的再现信号输出到数据再现部分 1519。数据再现部分 1519 把输入的再现信号 A/D 转换成数字再现信号，并且再被输出到第二密码解码器 1520。另一方面，从光学拾取器输出的激光束照射到光盘 1101 的 BCA 1104 上，以致于反射光进入到光学拾取器。光学拾取器把进入的反射光光电转换成再现的信号，并输出给 BCA 再现电路 1521。BCA 再现电路 1521 根据输入的再现信号再现盘 ID 信号 1515，并且把该盘 ID 信号 1515 输出给第二密码编码器 1516 和第二密码解码器 1520。

另外，把存储在 IC 卡 1524 的公司识别信号存储器 1526 中的公司识

别信号输入给第二密码解码器 1520，其中 IC 卡 1524 安装在光盘记录和再现设备 1514 上。公司识别信号并不记录在 IC 卡 1524 的公司识别信号存储器 1526 中，例如在安装光盘记录和再现设备 1514 的记录程序时，公司识别信号可以记录在与光盘记录和再现设备 1514 的控制部分的 CPU 相连的存储器（未示出）中。或者，可以利用光盘记录和再现设备 1514 的键盘（未示出）输入公司识别信号。

第二密码解码器 1520 利用输入的盘 ID 信号 1515 以及公司识别信号作为解密密钥对加密的内容解密。此时，在 CATV 解码器 1506 的用户与具有 CATV 公司设备 1502 的特定 CATV 公司正式签约、并且内容 1502 被合法地记录到光盘 1101 上的情况下，用于被加密并记录在光盘 1101 上的加密内容的第一解密密钥正是在该时刻将被精确再现的光盘 1101 的盘 ID 信号（BCAS）,并且第二密码密钥是公司识别信号（CK），该信号存储在由签约的 CATV 公司提供的 IC 卡 1524 的公司识别信号存储器 1526 中。因此，解码或解扰内容的输出信号 1525 被从第二密码解码器 1520 中输出。在这种情况下，第二密码解码器 1520 的解密处理被表达成下列方程。当内容例如是图像信号时，MPEG 信号被第二密码解码器 1502 扩展，并且图像信号的输出信号 1525 被输出。

$$C[BCAS,CK]\#(BCAS*CK)=C \qquad (9)$$

因为上述光盘 1101 的内容被利用盘 ID 信号 1515 和公司识别信号加密，所以如果与提供上述内容的 CATV 公司签约，则能够通过包括 BCA 再现电路 1521 和第二密码解码器 1520 的任意光盘记录和再现设备执行再现。相反，如果未与上述 CATV 公司签约，则不能获得公司识别信号，并且不能再现内容，这使其能够区分签约用户和非签约用户。

另外，因为在本优选实施例中每个用户从光盘记录和再现设备 1514 向位于他们自己家中的 CATV 解码器 1506 发送盘 ID 信号以对图像数据等加密，所以不需要 CATV 设备 1501 改变分别输送给每个用户的加密内容，因此，可以简化广播系统，低成本地向大量受众提供相同的内容。另外，根据本优选实施例，只允许具有 CATV 解码器 1506 的每个用户在

一张 RAM 型光盘上进行记录。

虽然在本优选实施例中，描述了从有线电视系统的头端广播内容的情形，但本发明并不限于此，本发明可以应用到使用无线电波的广播。

第五优选实施例

下面将参考附图对根据本发明第五优选实施例的记录和再现加密内容的方法进行描述。图 21 是本发明第五实施例的光盘 1601 的数据记录区的平面图，图 22 是根据第五优选实施例的光盘记录和再现系统的结构框图。在第五优选实施例中，省去对与第三和第四优选实施例共用元件的描述。

参见图 21，1601 表示记录型光盘，是可重写型或非可重写型光盘，1602 表示控制用户数据区，盘信息以凹凸凹坑的形式记录在其中，1603 表示用户数据区，用户通过把激光器发出的光束照射到光盘上而在其中记录数据，1604 表示 BCA，在其中记录盘 ID。

在 BCA 1604 中，通过利用如 YAG 等脉冲激光器局部修整控制用户数据区内周边部分中凹凸凹坑上的记录膜而形成在径向具有伸长形状的多个修整区 1606。修整由盘制造商执行。另外，通过把盘 ID 附加到记录在 BCA 1604 中的数据，可以很容易地执行光盘的管理。另外，通过在凹凸凹坑上记录 BCA 1604 数据，可以防止记录 BCA 1604 中的用于识别光盘的信息被篡改。

此外，通过布置控制用户数据区 1602 和 BCA 1604 使其彼此相邻，当控制用户数据区的数据被再现时可以连续地再现 BCA 1604 的数据，或者当再现 BCA 1604 的数据时可以连续地再现控制用户数据区的数据，因此使加速获得或取得 BCA 1604 的信息的处理成为可能，从而例如当光盘被启动时，由 CPU 迅速识别光盘并记录加密的内容。

虽然本发明优选实施例的 BCA 1604 是通过修整在控制用户数据区 1602 内周边部分中的凹凸凹坑上的记录膜而形成的，但构成可重写或不可重写的记录型光盘的记录膜与形成在只读光盘上的记录膜相比，很容易受热影响。与修整外周边时相比，通过修整控制用户数据区 1602 的内周边部分，可以保护用户数据区 1603 的记录数据不受修整时产生的热的

影响。BCA 1604 形成在控制用户数据区 1602 内周边侧的原因在于考虑到当来自激光束的光斑的直径由于激光器装置聚焦伺服电路的不稳定性而发生波动时留有一定余量。修整之前记录在 BCA 1604 中的数据可以被记录在控制用户数据区 1602 中。记录在 BCA 1604 中的数据可以被记录在控制用户数据区 1602 中，使得在修整时控制用户数据区 1602 的上述数据可以得到保护。

另外，当上述数据被连续且反复地从 BCA 1604 记录到控制用户数据区 1602 时，可以通过在控制用户数据区 1602 中找出上述数据来预测 BCA 1604 的位置。另外，通过以与用户数据区 1603 相同的方式照射光束而记录密钥信息记录区 1605 中的数据。

以类似于本优选实施例的方式，通过布置控制用户数据区 1602 和密钥信息记录区 1605 使其彼此相邻，可以当再现控制用户数据区 1602 的数据时连续再现密钥信息记录区 1605 中的数据，或当再现密钥信息记录区 1605 的数据时能够连续地再现控制用户数据区 1602 的数据，因此，使加速获得或取得 BCA 1604 的信息的过程成为可能，从而例如当光盘被启动时由 CPU 迅速识别光盘并再现加密的内容。

参见图 22，根据第五优选实施例的光盘记录和再现系统包括 CATV 公司设备 1701、密钥发行中心设备 1707、CATV 解码器 1706、光盘记录和再现设备 1714 和电视机 1730。在这种情况下，CATV 公司设备 1701 包括用于存储诸如电影软件之类的内容的内容存储器 1702、用于存储第一密码密钥的第一密码密钥存储器 1703 和第一密码编码器 1704。另外，CATV 解码器 1706 包括系统 ID 存储器 1708，第一密码解码器 1713，和用于输出目前时间信息的时钟电路 1725。此外，密钥发布中心设备 1707 包括用于控制设备 1707 的操作的控制部分 1707a、和时限信息存储器 1710。另外，光盘记录和再现设备 1714 包括记录电路 1717、密钥信息记录电路 1719、BCA 再现电路 1720、数据再现部分 1721、第二密码解码器 1722 和密钥信息再现部分 1723。

首先，CATV 公司设备 1701 的第一密码编码器 1704 利用第一密码密钥 1703 对存储在内容存储器 1702 中的诸如电影软件之类的内容数据加密，由此产生第一加密内容 1705，并通过网络向每个用户的 CATV 解

码器 1706 的第一密码解码器 1713 传送所产生的第一加密内容 1705。存储在内容存储器 1702 中的内容由 C 表示，存储在第一密码密钥存储器 1703 中的第一密码密钥 1703 由 FK 表示，并且第一加密内容 1705 由 C[FK] 表示，则能够表示下列方程：

$$C*FK=C[FK] \qquad (10)$$

CATV 解码器 1706 通过网络向密钥发布中心设备 1707 的控制部分 1707a 传送：存储在 CATV 解码器 1706 的系统 ID 存储器 1708 中的系统 ID，和利用例如键盘（未示出）输入的用户想观看并收听的上述内容的标题码 1709。上述标题码 1709 可以根据电视机 1730 屏幕通过选择输入，或可以利用键盘直接输入，也可以从遥控器等输入。因此，可以由用户以其自己的方式获得标题码，或者可以与第一加密内容 1705 一起从 CATV 解码器 1706 发送，或者可以事先在不同于第一加密内容的时间以节目指南等的形式发送。

根据 CATV 解码器 1706 的系统 ID 和上述内容的标题码 1709，密钥发行中心设备 1707 的控制部分 1707a 查阅存储在时限信息存储器 1710 中的对应时限信息，产生对应的密钥（K）1712，并把产生的密钥（K）1712 通过网络向 CATV 解码器 1706 的第一密码解码器 1713 传送。时限信息使得能够在不同时间多次广播相同内容的情况下进行区分。第一解密密钥由 FK 表示、CATV 解码器 1706 的系统 ID 由 DID 表示、时限信息由 TIME 表示，并且内容的标题码由 T 表示，密钥（K）1712 满足由下列方程表示的关系：

$$FK=K*T*DID*TIME \qquad (11)$$

如果第一解密密钥（FK）、上述从密钥发行中心设备 1701 传送的密钥（K）1712、上述内容的标题码、系统 ID 和时限信息满足上述关系，并且时限信息满足来自时钟电路 1725 的当前时间信息的条件，则第一密码解码器 1713 可以对第一加密内容 1705 解密。在这种情况下，当第一

加密内容 1705 是图像信号时，将解扰后的图像信号从第一解密解码器 1713 输出给电视机 1730，使得用户可以在电视机 1730 上观看和收听该内容。在这种情况下，第一密码解码器 1713 的解密处理表示如下：

$$C[FK]\#(K*T*DID*TIME)$$
$$=C[FK]\#FK$$
$$=C \qquad (12)$$

下面将描述在光盘 601 上记录上述内容的方法。当内容记录在光盘 1601 上时，将未被 CATV 解码器 1706 解密的第一加密内容 1705 从 CATV 公司设备 1701 的第一密码编码器 1740 传送给光盘记录和再现设备 1714 的记录电路 1717。记录电路 1717 利用诸如公知的 8/16 调制系统之类的调制系统数字调制接收到的第一加密内容 1705 的数据，并且调制的数字数据被光学拾取器（未示出）记录在光盘 1601 上。因此，需要对第一加密内容 1705 解密，以便再现上述加密并记录在光盘 1601 上的内容。

光盘记录和再现设备 1714 通过网络向密钥发布中心设备 1707 的控制部分 1707 传送由 BCA 再现电路 1720 再现的光盘 1601 的盘 ID 信号 1715 和利用例如键盘（未示出）输入的观众想再现的上述内容的标题码 1716。至于发送盘 ID 的计时，可以在访问密钥发行中心设备 1707 时发送盘 ID，或者可以在收听和观看内容时与标题码一起发送盘 ID。

虽然作为发送盘 ID 的方法描述了通过再现图 22 所示光盘 1601 的 BCA 1604 从 BCA 再现电路 1720 直接向密钥发行中心设备 1707 发送输出信号的方法，但本发明并不局限于此，也可以采用下列方法。例如，当启动光盘时，在访问密钥发行中心设备 1707 之前再现 BCA 1604 的数据，并且把 BCA 1604 的数据存储在光盘记录和再现设备 1714 或 CATV 解码器 1706 的存储器（未示出）中，然后以上述计时传送到密钥发行中心设备 1707 的控制部分 1707a。另外，当可以视觉识别一些形式如标签等的盘 ID 时，可以用键盘输入盘 ID。当标签是条形码时，条形码阅读器可以用于读取盘 ID。

密钥发行中心设备 1707 的控制部分 1707a 产生对应于光盘 1601 的

盘 ID 信号 1715 和内容的标题码 1716 的密钥（DK）1718，并把产生的密钥（DK）1718 传送给光盘记录和再现设备 1714 的密钥信息记录电路 1719。在这种情况下，第一解密密钥由 FK 表示、光盘 1601 的盘 ID 信号 1715 由 BCAS 表示、内容的标题码 1716 由 T 表示，则密钥（DK）满足下列关系式：

$$FK=DK*BCA*T \qquad (13)$$

利用诸如公知的 8/16 调制系统等之类的调制系统数字调制输入到光盘记录和再现设备 1714 的密钥信息记录电路 1719 的密钥（DK），并再通过光学拾取器（未示出）把调制的数字数据记录到光盘 1601 上的密钥信息记录区 1605 中。在密钥信息记录区 1605 中可以多次记录密钥(KD)。通过多次记录相同的密钥，可以当密钥信息记录区 1605 的记录膜退化或光盘 1601 被划痕时保护密钥（KD），使得只有当任一密钥（DK）的数据可以被再现时就能对内容解密。

虽然在本优选实施例中密钥信息记录区 1605 设置在用户数据区 1603 的内周边侧，但也可以设置在用户数据区 1603 的外周边侧，或设置在内周边和外周边两侧。通过在外周边侧设置密钥信息记录区 1605，可以记录更多的密钥（DK）。另外，通过分散地设置多个密钥信息记录区，即使在一个密钥信息记录区不能再现的情况下，密钥（DK）可以受到其它密钥信息记录区的保护。

另一方面，从光学拾取器输出的激光束照射到光盘 1601 上记录了上述内容的区域上，使得反射光进入到光学拾取器中。光学拾取器把进入的反射光光电转换成再现的电信号，并且把已经被光电转换的再现信号输出到数据再现部分 1721。响应于此，数据再现部分 1721 把输入的再现信号 A/D 转换成加密的数字数据，输出给第二密码解码器 1722。另外，从光学拾取器输出的激光束照射到光盘 1601 的 BCA 604 上，并且反射的光进入到光学拾取器。光学拾取器把进入的反射光光电转换成再现的电信号，并且把已经被光电转换的再现信号输出到 BCA 再现电路 1720。响应于此，BCA 再现电路 1720 根据输入的再现信号再现盘 ID 信

号 1715，并输出到加密解码器 1722。另外，从光学拾取器输出的激光束照射到光盘 1601 的密钥信息记录区 1605，使得反射光进入到光学拾取器。光学拾取器把进入的反射光光电转换成再现的电信号，并把再现的信号输出给密钥信息再现部分 1723。响应于此，密钥信息再现部分 1723 根据输入的再现信号产生密钥（DK）的数据，并输出到第二密码解码器 1722。

当访问密钥发行中心设备 1707 之后立即再现内容时，密钥信息记录电路 1719 可以在向密钥信息记录区 1605 中记录相同的密钥（DK）之前，把密钥（DK）直接输入到第二密码解码器 1722。这样，可以缩短直到再现开始之前的时间。密码解码器 1722 利用包括输入的盘 ID 信号 1715、密钥（DK）和上述内容的标题码 1716 的解密密钥，对加密的内容解密。第二密码解码器 1722 的解密处理由下列方程表示。当内容是图像信号时，例如，扩展 MPEG 信号，使得图像信号的输出信号 1724 从第二密码解码器 1722 输出。

$$
\begin{aligned}
&C[FK]\#（DK*BCA*T） \\
&=C[FK]\#FK \\
&=C \qquad\qquad\qquad\qquad\qquad\qquad （14）
\end{aligned}
$$

在本优选实施例中，当从密钥发行中心设备 1707 的控制部分 1707a 接收到密钥信号时，征收用户费用，收听并观看内容和第一次再现记录在光盘 1601 上的内容时单独收费，避免只在向光盘 1601 上记录内容数据时收费。因此，与一次性征收收听或观看和在光盘 1601 上进行记录的费用的情况相比，可以对下列情况降低所付费用：

（a）希望收听并观看内容，但不需要把内容记录在光盘 1601 上的用户，或

（b）希望在光盘 1601 上记录内容数据但不需要在广播时收听和观看内容的用户。

另外，因为不只对在光盘 1601 上进行记录征收费用，所以用户可以

判断用户是否接收到用于在收听并观看之后、再现光盘 1601 以再次收听并观看的密钥。虽然在上述优选实施例中使用通过网络从密钥发行中心设备 1707 的控制部分 1701a 接收密钥（DK）的方法，但本发明并不局限于此，内容的标题和盘 ID 号可以口头地输送到电话上，并且在口头接收之后利用键盘输入。

接下来，将描述在访问密钥发行中心设备 1707 之后再现在密钥信息记录区 1605 中记录了密钥（DK）的光盘 1601 的情况。首先，从光学拾取器输出的激光束照射到光盘 1601 上记录了上述内容的区域，并且再经执行光电转换的光学拾取器把反射光输入到数据再现部分 1721。响应于此，数据再现部分 1721 把加密内容的数据输出给第二密码解码器 1722。另一方面，从光学拾取器输出的激光束被照射到光盘 1601 的 BCA 1604 上，使得反射光经执行光电转换的光学拾取器输入到 BCA 再现电路 1720。响应于此，BCA 再现电路 1720 根据输入的再现信号产生盘 ID 信号 1715，并输出到第二密码解码器 1722。

另外，从光学拾取器输出的激光束照射到光盘 1601 的密钥信息记录区 1605，使得反射光经执行光电转换的光学拾取器输入密钥信息再现部分 1723。响应于此，密钥信息再现部分 1723 根据输入的再现信号产生密钥（DK）的数据，并输出到第二密码解码器 1722。第二密码解码器 1722 利用包括输入的盘 ID 信号 1755、密钥（DK）和上述内容的标题码 1716 的解密密钥对从再现部分 1721 输出的加密内容解密。第二密码解码器 1722 的解密处理表达成下列方程。当内容是图像信号时，例如，扩展 MPEG 信号，并且把扩展的 MPEG 信号从第二密码解码器 1722 输出。

$$C[FK]\#（DK*BCA*T）$$
$$=C[FK]\#FK$$
$$=C \qquad （15）$$

通过在密钥信息记录区 1605 中一次记录密钥（DK）的数据，可以总是无需对密钥发行中心设备 1707 进行任何访问而再现上述加密的内容。另外，因为解密处理所需的所有解密密钥都被记录在光盘 1601 上，

所以可以通过任一包括 BCA 再现电路 1720、密钥信息再现部分 1723 和第二密码解码器 1722 的光盘记录和再现设备再现上述光盘 1601。

另外，在把上述加密的内容复制到具有不同盘 ID 的光盘 1601 上之后又试图再现的情况下，从 BCA 再现电路 1720 输出不同于上述光盘 1601 的盘 ID 信号，因此，加密的内容不能被解密，这样防止了内容被复制后再现。但是，即使在这种情况下，通过把内容的标题和盘 ID 经网络或口头输送给密钥发行中心，可以在付费之后接收到解密密钥。通过这种方式，即使加密内容被复制到另一张光盘 1601 上，也不能非法地再现任何内容，并且当再现复制有加密内容的光盘 1601 时总要付费，这导致对内容的版权保护。

图 23 是根据第五优选实施例的带有 ID 的表结构的表，以重新排列的形式表示输入到第一密码解码器 1713 的密钥（K）和输入到密钥信息记录电路 1719 的密钥（DK），是对于不同的系统 ID 和不同的盘 ID 的。

参见图 23，T1,T2 和 T3 表示对于不同内容的标题码，FK1,FK2 和 FK3 表示用于对分别具有 T1,T2 和 T3 标题码的加密内容进行解密的解密密钥。DID1、DID2 和 DID3 表示对于不同 CATV 解码器 1706 的系统 ID，BCAS1、BCAS2 和 BCAS3 表示对于不同光盘 1601 的盘 ID。在这种情况下，确定输入到 CATV 解码器 1706 中的密钥（Kmn）以满足下列方程：

$$FKn = Kmn * Tn * DID * TIMEn \qquad (16)$$

另外，确定输入到光盘记录和再现设备 1714 的密钥（DKmn）以满足下列方程：

$$FKn = DKmn * BCAm * Tn \qquad (17)$$

如图 23 所示，不仅在不同内容的情况下，而且在相同内容的情况下，从密钥发行中心设备 1707 获得的对于每个不同 CATV 解码器 1706、对于每个不同的光盘和对于每个不同广播时间的密钥信息被设置得彼此不同，并由此导致对版权的详尽保护。以同样的方式，因为甚至对于同样

的内容，系统 ID、盘 ID 和时间信息彼此不同时，密钥信息也不同，所以 CATV 公司设备 1701 不需要改变对每个用户的加密内容，因此，为一项内容准备一个加密内容。于是，可以简化广播系统，并且能够低成本地为大量受众提供内容。

虽然在本优选实施例中描述了从有线电视的头端广播内容的情形，但本发明可以用于采用无线电波的广播。

第三至第五优选实施例的有益效果

根据本优选实施例的光盘包括（a）用于在其中记录第一盘信息的第一信息区，（b）用于在其中记录识别个体用的第二盘信息的第二信息区，和（c）可以通过把光束照射到用户数据区而记录信息的用户数据区。因此，通过对根据现有技术的光盘附加用于识别光盘的上述信息，可以很容易地执行光盘的管理。在这种情况下，上述第二信息区最好记录在上述第一信息区中，并且可以通过用于再现上述第一信息区的光学拾取器再现。在上述第二信息区中，第二信息的数据通过部分消除或去除上述第一信息区内的记录膜来记录，使得形成在径向具有伸长形状的多个修整区，并且可以防止上述第二盘信息被很容易地篡改。

根据本优选实施例的记录加密内容的方法，当内容数据被记录在光盘的用户数据区上时，其中光盘包括：（a）用于在其中记录第一盘信息的第一信息区，（b）用于在其中记录识别各个盘用的第二盘信息的第二信息区，和（c）可以通过把光束照射到用户数据区而记录信息的用户数据区，内容的数据被加密并且记录加密的数据，使得内容的数据可以通过使用至少上述第二盘信息的操作或计算来解密和再现。因此，通过利用只存在于一个特定光盘中的光盘识别信息对内容进行加密，可以有这样的有益效果，即可以防止对内容的非法复制，从而保护版权。

根据本优选实施例的光盘在用户数据区内具有用于记录对加密并记录的内容解密的密钥信息的密钥信息记录区。因此，在需要用于对加密并记录的内容解密的密钥信息的系统中，有这样具体的有益效果，即一旦在密钥信息记录区中记录密钥信息之后，不需要每次再现时都输入密钥信息。

另外，根据本优选实施例的记录加密内容的方法，当内容被记录到光盘的用户数据区中时，其中光盘包括：（a）用于在其中记录第一盘信息的第一信息区，（b）用于在其中记录识别各个用的第二盘信息的第二信息区，（c）可以通过把光束照射到用户数据区而记录信息的用户数据区，和（d）密钥信息记录区，用于在其中记录密钥信息，该密钥信息用于对用户数据区内加密并记录的内容的数据进行解密，对内容数据加密并记录加密的内容，使得内容的数据可以通过至少利用上述第二盘信息和上述密钥信息的操作来解密并再现。因此，即使加密的内容数据被复制到另一张光盘上，其数据也不能被非法地再现，并且无论何时再现复制有加密内容的光盘时都要付费，这导致对版权的保护。

在这种情况下，第一盘信息最好以微凹凸凹坑的形式形成，并且在凹凸凹坑上记录用于识别光盘的第二盘信息。因此，可以容易地防止第二盘信息被篡改。而且，优选的是彼此相邻地形成所述第一盘信息和第二盘信息。在这种情况下，当再现上述第一盘信息时，可以连续地再现第二盘信息，或者当再现第二盘信息时可以连续地再现第一盘信息，因此可以加速在获得第二盘信息之后记录加密内容的处理，其中第二盘信息用于例如在启动光盘时由 CPU 迅速识别光盘。

根据本发明优选实施例记录加密数据的方法，因为甚至对于相同的内容，对于每个不同的系统 ID、每个盘 ID 和每个时间信息，密钥信息不同，所以不需要 CATV 公司设备 701 为每个用户改变加密的内容，并且 CATV 公司设备 701 可以为一个内容只准备一个加密的内容。这导致广播系统能够被简化，并且可以以低成本向大量受众提供内容。

第三和第五优选实施例的改型优选实施例

虽然在如图 16 和 21 所示的上述第三和第五优选实施例中修整区 1105 和 1606 分别形成在位于控制用户数据区 1102 和 1602 之内的内周边部分的 BCA 1104 和 1604 中，但本发明并不局限于此。如图 24 和 25 所示，图中分别表示根据第三和第五优选实施例的改型优选实施例的光盘 1101a 和 1601a 的数据记录区，修整区 1105a 和 1606a 可以通过修整记录膜、从而使其从控制用户数据区 1102 和 1602 伸向光盘的内周边侧

来形成。也就是说，BCA 1104a 和 1604a 并不被分别包含在控制用户数据区 1102 和 1602 中，但形成并分配成从控制用户数据区 1102 和 1602 的内周部分突出或伸向控制用户数据区 1102 和 1602 的内侧。在这些改型的优选实施例中，以这种方式形成 BCA 1104 和 1604 的原因在于在激光束的光斑直径由于激光器设备的聚焦伺服电路的不稳定性而改变的情况下应该考虑一定的余量。在本改型的优选实施例中，用户数据区 1103 和 1603 存在于控制用户数据区 1102 和 1602 的外部，因此分配并形成修整区 1105a 和 1606a，保护记录在那些用户数据区 1103 和 1602 中的数据免受损害。

第六优选实施例

图 26 是表示根据本发明的第六实施例的光盘上的用户数据区的结构、和用于对来自用户数据区中的数据的加密内容解密的光盘再现设备的结构的框图。在本优选实施例中，光盘例如是一种诸如 DVD-RAM 之类的记录型光盘。

如图 26 所示，用户数据区 2150 包括扇区头部区 2101、主数据区 2102 和检错码 2103。在扇区头部区 2101 中，记录用于指示扇区位置的扇区地址 2104，和用于记录关于记录在主数据区 2102 中的数据的版权控制信息的版权控制信息 2105（包括加扰标志、复制控制信息等）。扇区头部区 2101 包括解密密钥区 2106，用于在其被嵌入或加密到主数据区 2102 的数据中时对加密信息解密。另外，主数据区 2102 被分成记录非加密内容 2107 的区域和记录加密内容 2108 的区域，非加密内容 2107 包括对于诸如 MPEG 中的同步模式之类的后续数据的控制信息，，或所有类型的控制信息。另外，加密内容 2108 包括主要为已经加密的诸如 AV 数据等之类的版权保护所需的内容数据。

再现下列主数据区 2102 的解密密钥被以预定的大小分成多个分支解密密钥（以下被称作分支解密密钥），然后登记到解密密钥区 2106 中。例如，在一个解密密钥区为 4 字节、解密密钥为 8 字节的情况下，8 字节的解密密钥被分成两个各为 4 字节的分支解密密钥，使得在 8 字节的解密密钥被分成各为 4 字节的分支解密密钥之后，两个分支解密密钥被

记录在两个逻辑连续扇区的解密密钥区 2106 和 2109 中。当再现这种用户数据区的数据时，从逻辑连续的多个扇区（由于跳过缺陷而不可用的每个扇区）的解密密钥区 2106 和 2109 中获得多个分支解密密钥，并且所需数量的获得的分支解密密钥被数据链接设备 2111 链接或连接，获得再现所需的已加密的解密密钥（8 字节）。根据版权控制信息 2105 的每个单元的内容，对记录在扇区的主数据区 2102 中的数据执行解密处理，而在该扇区处可以通过解密设备 2114 获得已加密的解密密钥（8 字节）。

另外，为了进一步提高加密的强度，可以对解密密钥加密，或通过将作为数据中的信息的解密密钥转换数据添加到密钥上，从而具有加密的恒定结果，甚至对相同的加密密钥，也可以提供不同的加密结果。更具体地说，如图 26 所示，从数据链接设备 2111 输出的已加密的解密密钥被输入给密钥解密设备 2112，并且利用预定的盘密钥，密钥解密设备 2112 把输入的已加密的解密密钥解密成作为伪数据的填充数据（1 字节）和解密密钥（7 字节），然后输出给密钥转换器 2113。在这种情况下，由盘密钥解密设备（未示出）利用作为预定的万能密钥（master key）的秘密密钥对记录在光盘中的加密盘密钥解密，获得盘密钥。另外，密钥转换器 2113 通过预定的转换操作，诸如利用乘、除或预定加权系数之类的操作，利用从上述密钥解密设备 2112 输出的解密密钥，转换从主数据区 2102 读出的解密密钥转换数据 2110 的数据，并产生和输出内容解密密钥（7 字节）给解密设备 2114。然后，解密设备 2114 利用从上述密钥转换器 2113 输出的内容解密密钥（7 字节），通过解密从主数据区 2102 读出的内容的数据来产生并输出解密内容的数据。作为解密密钥转换数据 2110，最好利用这样的数据，如可以立即检测诸如篡改复制生成管理信息或模拟宏观控制标志等之类对数据的非法使用。

图 27 是表示根据第六优选实施例的光盘，用户数据区中布置版权控制信息和解密密钥，和在光盘的主数据区分配加密的内容的框图。在图 27 所示的用户数据区 2150 的实例中，按照将解密密钥区分成具有 4 字节的分支解密密钥的第一解密密钥区 2201 和具有 4 字节的分支解密密钥的第二解密密钥区 2202 的方式来安排解密密钥区。因此，与记录在两个扇区中的加密内容的大小无关，可利用多个扇区（图 27 中的 2 个扇区）。

在这种情况下，将伪数据记录在未使用的区中作为补充数据。在图 27 所示的实例中，在只有一个扇区存在加密内容 2204 的情况下，记录一个扇区的补充数据 2203。

图 28 是表示在根据第六优选实施例的光盘中，把纠错单元位于多个扇区上的情况下的布局框图。例如，在光盘是 DVD 的情况下，通过利用 16 个扇区的纠错码的单元块（以下称作 ECC 块）提高纠错能力。因此，当执行数据记录和再现时，需要利用 ECC 块单元执行记录处理。在解密密钥被分成随后被记录的任意个数的分支解密密钥的情况下，可能导致在多个纠错块中记录一个解密密钥的情况。当再现同样内容时，需要再现所有的多个分支解密密钥，因此，还需要不仅再现用于记录加密内容的数据的扇区中的数据，而且还要再现刚好在记录解密密钥之前的 ECC 块中的数据。图 28 的实例的特征在于将在分割解密密钥时的分支个数设置为 ECC 块的扇区个数的量度或因子。这导致不能记录多个分支解密密钥，以便位于多个 ECC 块之上。另外，作为用在一个 ECC 块中的解密密钥，只采用一种类型的解密密钥，并且在记录的 AV 数据对于一个 ECC 块不足时，可以通过设置补充数据和补充扇区，而防止从光盘中读出再现时不必要的扇区数据。

第七优选实施例

图 29 是表示根据本发明第七优选实施例的光盘中导入区 2401 和用户数据区 2402 的结构、以及用于对来自导入区 2401 和用户数据区 2402 的数据的加密内容进行解密的光盘再现设备的结构框图。

参见图 29，以与图 26 的第六优选实施例相同的方式，导入区 2401 和用户数据区 2402 中的每一个由具有扇区头部区 2101、主数据区 2102 和检错码 2103 的扇区构成。在扇区头部区 2101 中，记录用于指示扇区位置的扇区地址 2104 和用于记录关于记录在主数据区 2102 中的数据的版权控制信息的版权控制信息 2105（包括加扰标志、复制控制信息等），扇区头部区 2101 还包括用于记录指示解密密钥的记录位置（即主数据区 2102 内解密密钥表 2404 中存储位置的记录位置）的密钥索引的密钥索引区 2403，在主数据区 2102 的数据被加密的情况下，用于查阅用于解

密的解密密钥。用于对记录在用户数据区 2402 中的加密内容进行解密的解密密钥被以解密密钥表 2404 的形式记录在导入区 2401 中，该导入区可以以表的形式重写。记录在导入区 2401 中的解密密钥通过记录在密钥索引区 2403 中的密钥索引来查阅。在与图 26 所示的第六优选实施例相同的方式下，以上的解密密钥被密钥解密设备 2112 使用预定的盘密钥解密成填充数据和解密密钥（或标题密钥），此后，上述被解密的解密密钥（或标题密钥）通过密钥转换器 2113 利用解密密钥转换数据，转换成内容解密密钥，并且再把转换的内容解密密钥输出给解密设备 2114。解密设备 2114 利用内容解密密钥对加密的内容数据解密，然后产生并输出解密内容的数据。

在以上构成的第七优选实施例的光盘记录和再现设备中，通过在扇区头部区 2101 内的密钥索引区 2403 中记录查阅用的密钥索引，能够独立于密钥索引区 2403 的大小来分配解密密钥表 2404 的解密密钥的大小。另外，分配解密密钥表 2404 的大小之后，通过连续利用来自由密钥索引区 2403 内的密钥索引指示的解密密钥表 2404 的多个解密密钥，可以使用任意或自由大小的解密密钥。

图 30A 是表示在根据第七优选实施例的光盘中，解密密钥的初始值表示导入区 2401 的主数据区 2102 中未记录状态的情形下数据结构的框图。参见图 30A，作为格式化光盘等时记录的解密密钥的初始值，记录处于未被记录状态 2501 的数据，以及已知的不用作密钥的固定值（例如，全为零的数据），由此指示解密密钥的未被记录的状态。

图 30B 是表示在根据第七优选实施例的光盘中，导入区的主数据区中通过解密密钥状态表表示记录状态的情形下的数据结构的框图。参见图 30B，在与图 30A 所示解密密钥相同的方式下，在导入区 2401 中以可通过索引查阅的表的形式布置解密密钥状态表 2502，解密密钥的记录状态如下描述成记录状态数据 2503：

（1）0x00：未使用

（2）0x01：区域保留；

（3）0x03：密钥记录；和

（4）其它：保留。

在这种情况下，0x 指示下列符号或数字的十六进制表示。

图 31 是表示根据第七优选实施例的光盘中解密密钥的布局框图。在图 31 的例子中，设计盘的解密密钥区的分配，以提高解密密钥的可靠性。通常，在用户数据区 2602 中执行缺陷管理，并且，在发生写入失败的情况下，执行对被替换区的替换处理。但是在导入区 2601 中，不执行如上所述的缺陷管理。因此，由于写入失败、读出失败等情况的发生，为产生 AV 数据所需的解密密钥可以转换成不可使用的状态，并且可能有光盘本身可以被转换成不可使用的状态的情况。因此，希望在多个不同的 ECC 块上记录总的多个解密密钥。在多个解密密钥被记录于彼此相邻的区域中的情况下，由于划痕或尘埃，可能读不出已经记录的所有多个解密密钥。因此，如图 31 所示，最好按照布局中的不同位置进行记录，如分别在光盘的内周侧和外周侧，例如，在导入区 2601 和导出区 2603 中。

在图 29 的优选实施例中，将解密密钥区分配在导入区 2401 和 2601 中。这是因为考虑到用户数据区 2602 是通过常规的读命令和写命令可访问的区域，要从个人计算机的驱动单元等发生访问时的安全性考虑。因此，可以通过在用户数据区 2602 中的分配获得相同的有益效果。

第八优选实施例

图 32 是表示由本发明第八优选实施例的文件管理系统管理光盘数据的数据结构的框图。在图 32 的实例中，根据文件系统的结构管理用于存储所需文件的扇区地址。

在国际标准化组织的 ISO 13346 中所规定的文件系统的结构中，利用被称作文件条目的信息管理文件的记录位置，以使用可重写型光盘。如图 32 所示，例如，文件（1）2703 的记录位置的数据存储为文件管理信息区 2751 中的文件条目（1）2701，文件（2）2704 的记录位置的数据被存储为文件条目（2）2702。每个文件由用于管理多个扇区的扩展名 2705 和 2706 组成，多个扇区连续地位于光盘上。如第七优选实施例中示出的加密内容记录在由光盘上的文件条目指示的主数据区 2102 中，并且解密密钥记录在导入区 2601 内的解密密钥表 2707 中。在记录加密内容的用户数据区 2602 的扇区头部区 2101 中，在密钥索引区 2708 中记录

指示记录位置的指针，用于查阅解密所需的解密密钥。虽然在本优选实施例中利用文件单元、扩展单元管理并记录解密密钥，但本发明并不局限于此。可以利用至少文件单元或扩展单元之一管理并记录解密密钥。

如上所述，在通过文件系统管理的光盘中，将参考图 33 对版权保护所需的内容的记录操作进行描述。图 33 示出由根据第八优选实施例的文件管理系统执行的版权保护所需的内容记录处理。

当记录加密内容时，首先，在步骤 S2801，读出图 30B 所示的解密密钥状态表 2502 以检查解密密钥表 2707 的空区。接下来，在步骤 S2802，判断是否存在解密密钥状态表 2502 的任何空区，并且在否定的情况下，通过在步骤 S2807 中停止记录操作，结束内容的记录过程，因为不能记录用于加密内容的解密密钥。另一方面，在步骤 S2802 为肯定的情况下，记录获得的解密密钥（或标题密钥），并且在不能获得解密密钥的情况下，保留解密密钥区。接下来，在步骤 S2804 中，设置记录内容的版权控制信息（包括关于是否执行了加密的信息、用于指示加密的类型或种类的信息等）和将被记录在密钥索引区 2708 中的密钥索引，此后，在步骤 S2805 中对内容加密，然后利用扩展单元把加密的内容以文件的形式记录到光盘上。在这种情况下，可以利用文件单元，使用相同的版权控制信息和密钥索引；或者可以利用扩展单元，对其进行切换。也就是说，在步骤 S2804 和 S2805 中，被处理的单元至少是文件单元或扩展单元之一。最后，在步骤 S2806 中，根据关于记录内容的信息，在更新了用于管理上述记录数据的文件管理信息之后，结束内容的记录处理。

图 34 是表示由根据第八优选实施例的文件管理系统执行的内容再现处理的流程图。图 34 表示通过图 33 所示的方法从光盘上再现以文件形式记录的内容的处理。

当执行对文件的再现操作时，对于由文件管理信息区 2751 内的文件条目所示的区域，获得密钥索引，以便找出或知道由再现的文件利用的解密密钥表中的区域。更具体地说，步骤 S2901 中，在通过读取和再现获得从文件管理信息 2751 再现的文件的文件条目之后，在步骤 S2902 中读出密钥索引区的值，然后从由获得的文件条目所示的区域的扇区头部区 2102 中再现。在使用扩展单元进行不同方式的加密时，读出每个扩展

单元的扇区头部中的密钥索引区。然后，在步骤 S2903 中，读出解密密钥，并再现，以从由获得的解密密钥指示的解密密钥表 2707 的解密密钥区获得解密密钥。另外，在步骤 S2904 中，从文件条目所示的区域中读出并再现文件内的内容数据，然后对再现内的数据解密。在这种情况下，当结束内容文件的再现和解密时，结束内容的再现处理。

图 35 是表示由根据第八优选实施例的文件管理系统执行的内容删除处理的流程图，并且图 35 示出了通过图 33 所示的方法删除以文件形式记录的内容数据的操作。

当执行文件的删除操作时，获得关于由文件条目表示的区域的密钥索引，从而找出或知道删除文件所使用的解密密钥表 2707 的区域。更具体地说，步骤 S3001 中，在从文件管理信息区 2751 内的文件管理信息中获得删除文件的文件条目之后，在步骤 S3002 中，从由文件条目指示的区域的扇区头部获得密钥索引区的值。在这种情况下，当利用扩展单元进行不同方式的加密时，读出每个扩展单元的扇区头部中密钥索引区中的数据。然后，在步骤 S3003 中，从由获得的密钥索引指示的解密密钥表 2707 的解密密钥区打开或释放解密密钥（这里的释放或打开解密密钥意味着从表中删除解密密钥），并且在步骤 S3004 中，从文件管理信息中删除用于指示删除文件的写入位置的文件条目，然后结束内容的删除处理。虽然在常规的文件系统中，删除文件时只删除文件条目，但不能删除记录在另一区中的解密密钥，因为加密内容的解密密钥和记录扇区被记录在分离的区域中。在上述优选实施例中，通过从解密密钥表 2707 删除用于指示扇区头部区中的密钥索引的解密密钥来执行对光盘上解密密钥的管理。

第九优选实施例

图 36 是表示根据本发明第九优选实施例的光盘系统的结构框图，并且此光盘系统是一个信息处理系统，用于在光盘 3100 上记录和再现需要版权保护的内容。光盘系统包括编码设备 3101，光盘设备 3102，解码设备 3103 和个人计算机 3104。

编码设备 3101 包括用于存储内容数据的内容存储器 3131，用于以

MPEG 形式对上述的内容数据进行编码的编码电路 3132，用于存储密码密钥的密码密钥存储器 3133，用于利用密码密钥对编码的内容数据进行加密、产生解密密钥并将其存储在解密密钥存储器 3111 中的加密电路 3134，用于存储解密密钥的解密密钥存储器 3111，用于对解密密钥进行总线加密的总线加密电路 3112 和通过 PCI 总线 3151 连接到个人计算机 3104 的接口 3122 的接口 3124，其中接口 3124 传输加密内容和解密密钥。另外，光盘设备 3102 包括用于在其中存储多个解密密钥的解密密钥表存储器 3113，总线加密和解密电路 3114，用于在光盘 3100 上记录数据并从光盘 3100 上读出和再现数据的记录和再现电路 3119，和经 SCSI 总线 3152 连接到个人计算机 3104 的接口 3121 的接口 3120，其中接口 3120 执行诸如数据或信号的传送和接收以及信号的转换和协议转换等处理。SCSI 总线 3152 可以优选地为 ATAPI 总线。在这种情况下，总线加密和总线解密分别意味着密码加密处理和解密处理，用于对密码密钥或解密密钥加密，并且在 PCI 总线 3151 或 SCSI 总线 3152 上传送和接收相同的密钥。

另外，个人计算机 3104 包括用于控制个人计算机 3104 的操作的控制部分 3130，用于在其中存储多个总线加密解密密钥的总线加密解密密钥表存储器 3115，用于存储多个对应于上述多个总线加密解密密钥的解密密钥状态的数据（指示多个解密密钥状态的记录状态或条件，更具体地讲，指示非利用或未使用，区域保留、记录的密钥或保留等）的解密密钥状态表存储器 3116，经 SCSI 总线 3152 连接到接口 3120 或光盘设备 3102 的接口 3121，接口 3121 执行诸如发送和接收数据和信号以及信号转换和协议转换等处理，还包括经 PCI 总线 3151 连接到解码设备 3103 的接口 3123 以及编码设备 3101 的接口 3124 的接口 3122，其中接口 3122 执行诸如数据或信号的发送和接收以及信号转换和协议转换等处理。另外，解码设备 3103 包括与个人计算机 3104 的接口 3122 相连的接口 3123，其中接口 3123 执行诸如数据或信号的发送和接收以及信号转换和协议转换等处理，还包括用于对由接口 3123 接收到的加密解密密钥进行总线解密或总线解码的总线解密电路 3117，用于在其中存储解密密钥的解密密钥存储器 3118，和用于利用解密密钥存储器 3118 的解密密钥对接口 3123

接收的加密内容的数据进行解密或编码以及通过执行 MPEG 格式的解码处理产生图像信号或语音信号的解密电路 3141，其中产生的图像信号和语音信号输出给显示设备 3105。

在此光盘系统的编码设备 3101 中，编码电路 3132 对以 MPEG 格式的形式存储或输入到内容存储器 3131 的诸如 AV 数据之类的内容数据进行编码，并且加密电路 3134 利用加密密钥存储器 3133 内的密码密钥对上述编码内容的数据加密，产生密码密钥是为了避免了在个人计算机 3104 上对所述内容的非法使用，然后，经过接口 3124 和个人计算机 3104 把编码的内容数据发送给光盘设备 3102。在这种情况下，加密的内容数据经 PCI 总线 3151、个人计算机 3104 的接口 3122 和接口 3121 以及光盘设备 3102 的接口 3120 从编码设备 3101 的接口 3124 传送给记录和再现电路 3119。然后，加密内容的数据通过光盘设备 3102 的记录和再现电路 3119 被记录到光盘 3100 上。另外，光盘设备 3102 的记录和再现电路 3119 再现被记录在光盘 3100 上的加密内容的数据，然后，经个人计算机的接口 3120、接口 3121 和接口 3122 以及解码器设备 3103 的接口 3123 把再现的加密内容的数据传送给解密电路 3141。解码设备 3103 的解密电路 3141 对加密内容数据的加密进行解密，并且执行 MPEG 格式的解码处理，然后分别把解码内容的图像信号和语音信号输出给显示设备 3105 和扬声器设备（未示出）。

编码设备 3101 的加密电路 3134 利用密码密钥存储器 3133 内的密码密钥对以 MPEG 格式编码的内容数据进行加密，并且同时产生并存储再现时所需的解密密钥在解密密钥存储器 3111 中。虽然需要在光盘 3100 上记录加密内容的数据和解密密钥，但是在解密密钥在个人计算机 3104 上被按照明文文本处理的情况下，存在着这样的可能性，即加密内容的数据解码通过从光盘 3100 上读出解密密钥而变得容易。为了避免这种在编码设备 3101 和光盘设备 3102 之间进行互相授权，利用相互共享的总线密钥执行总线加密。

更具体地说，也就是存储在解密密钥存储器 3111 中的解密密钥由编码设备 3101 的总线加密电路 3112 加密，此后，把加密的解密密钥经接口 3124、PCI 总线 3151 和接口 3122 存储到个人计算机 3104 的总线加密

解密密钥表存储器 3115 中。另一方面，在光盘设备 3102 的总线加密和解密电路 3114 中，对加密的解密密钥进行解码，该解密密钥由记录和再现电路 3119 从光盘 3100 再现，此后，把已经解密或解码的解密密钥存储到解密密钥表存储器 3113。另外，总线加密和解密电路 3114 经接口 3121、SCSI 总线 3152 和接口 3120 从总线加密解密密钥表存储器 3115 中接收，并对例如更新后并进行了总线加密的解密密钥进行总线解密，并在解密密钥表存储器 3113 中存储进行了总线解密的解密密钥。之后，由记录和再现电路 3119 在光盘 3100 上记录进行了总线解密的解密密钥。

在通过记录和再现电路 3119 从光盘 3100 再现解密密钥状态表之后，解密密钥状态表通过解密 3120、SCSI 总线 3152 和接口 3121 传送并存储到解密密钥状态表存储器 3116 中。另外，被个人计算机 3104 更新的解密密钥状态表被从解密密钥状态表存储器 3116 中读出，然后经接口 3121、SCSI 总线 3152 和接口 3120 传送到记录和再现电路 3119。之后，记录和再现电路 3119 把接收的解密密钥状态表记录到光盘 3100 上。因此，在位于中间的个人计算机 3104 上利用加密解密密钥表 3115 和解密密钥状态表存储器 3116，只处理加密的解密密钥，并将导致建立更高的安全性。

在光盘设备 3102 和解码设备 3103 之间以同样的方式执行解密密钥的总线加密导致建立更高的安全性。这就是说，解码设备 3103 的总线解密电路 3117 对从个人计算机 3104 经接口 3123 接收到的加密的解密密钥进行总线解密或总线解码，并且把进行了总线解密的解密密钥存储到解密密钥存储器 3118 中。解密电路 3141 利用存储在解密密钥存储器 3118 中的解密密钥对加密内容的数据进行解密。

如上述第七优选实施例所示，在用于对光盘 3100 上加密的内容数据进行解密的解密密钥被以表的形式记录的情况下，被光盘设备 3102 再现的解密密钥表被总线加密和解密电路 3114 进行总线加密，此后，总线加密的解密密钥表的数据被经接口 3120 传送到个人计算机 3104 的总线加密的解密密钥表存储器 3115，并且存储在其中。当记录内容的数据时，个人计算机 3104 通过从以明文文本的形式记录于光盘 3100 中的解密密钥状态表中寻找解密密钥状态表的空区而进行搜索，然后，把从编码设

备 3101 传送的经总线加密的解密密钥分配给搜索到的空区。在这种情况下，当这种利用解密密钥单元作为总线加密而结束加密时（例如利用以解密密钥长度为单位的块加密），不需要在分配给解密密钥块时解密并重新加密解密密钥。

因为解密密钥表和解密密钥状态表在光盘设备 3100 之间传送并存储，所以光盘设备 3102 和个人计算机 3104 分别是一个块数据，可以称作块数据。

在再现内容的情况下，只检索对希望从光盘设备 3102 中再现的解密密钥块再现的内容进行解密所需的解密密钥，并从总线加密的解密密钥表存储器 3115 中取出，并再把取出的解密密钥经个人计算机 3104 和解码设备 3103 的总线解密电路 3117 传送并存储到解密密钥存储器 3118。然后，解密电路 3141 经个人计算机 3104 和接口 3123 接收由光盘设备 3102 的记录和再现电路 3119 从光盘 3100 再现的加密 AV 数据，此后，利用解密密钥存储器 3118 内的解密密钥对接收到的加密 AV 数据进行解密，并且把解密的数据输出为图像信号和语音信号。在这种情况下，按照与上述情况相同的方式，当记录内容时，在解密密钥单位作为总线加密而完成这种加密的情况下（例如，以解密密钥长度为单位的块加密），在从解密密钥块取出解密密钥时，不需要对解密密钥解密和重新加密。另外，当扩大解密密钥的大小时，在个人计算机 3104 上可以很容易和安全地执行诸如分配多个解密密钥之类的解密密钥区的扩展，而不改变光盘设备 3102 的任何结构。

第十优选实施例

图 37 是表示根据本发明第十实施例的光盘中用户数据区的结构、在用户数据区中加密并记录加密的内容的光盘记录设备的结构，和对来自用户数据区中的数据的加密内容进行解密的光盘再现设备的结构的框图。所述第十优选实施例的特征在于把光盘记录设备的结构增加到第六优选实施例上，下面将详细描述该结构。

在光盘记录设备中，为了提高加密的强度从而没有恒定的加密结果，在密钥转换器 2119 利用作为内容中的信息的解密密钥转换数据，通过对

输入的密码密钥执行诸如乘，除之类的预定密钥转换或利用预定加权系数进行操作（计算），获得或取得内容解密密钥之后，利用内容解密密钥对内容数据进行加密。

也就是说，当记录内容时，把内容数据和用于对内容数据加密的密码密钥输入到光盘记录设备。在这种情况下，把内容数据输入到密钥转换器 2119 和加密设备 2120，并且把密码密钥输入到密钥加密设备 2118 和密钥转换器 2119。密钥转换器 2119 利用第一和第二解密密钥转换数据 2115 和 2116 对上述输入的密码密钥执行预定的密钥转换操作或计算，第一和第二解密密钥转换数据 2115 和 2116 分别是内容中的部分信息，然后，产生并输出内容解密密钥到加密设备 2120。然后，加密设备 2120 利用上述内容解密密钥对上述输入的内容的数据进行加密，并且再在光盘上的用户数据区 2150 内的 AV 数据记录扇区 2152 中记录加密的内容。

在这种情况下，作为用在光盘再现设备中的解密密钥转换数据，使用作为 AV 数据中的信息的、并且在扇区单元中通常不同的第二解密密钥转换数据 2116，包括在记录有控制信息的扇区中的复制生成管理信息，和作为包括模拟宏观控制标志的复制控制信息的第一解密密钥转换数据 2115。通过利用第二解密密钥转换数据，可以恢复内容解密密钥，用于根据第二解密密钥转换数据的内容通过密钥转换器 2113 对每个扇区的内容数据加密。另外，因为第一解密密钥转换数据是一种篡改时容易被检测到非法利用的数据，所以可以得到这样的有益效果，即，易于防止内容数据在第一解密密钥转换数据被篡改时被解密。更具体地说，通过将用于记录用于 AV 数据的再现控制的再现控制信息的再现控制记录扇区中的数据作为第一解密密钥转换数据的预定转换操作，将密码密钥转换为解密密钥，并将转换后的解密密钥用作加密设备 2120 中的内容解密密钥。另外，通过利用两个解密密钥转换数据对加密密钥执行预定的转换操作或计算，其中两个解密密钥转换数据包括作为再现控制记录扇区中的数据的第一解密密钥转换数据，和作为用于在其中记录加密的内容的扇区中的非加密内容的一部分的第二解密密钥转换数据，计算另一内容解密密钥，该密钥可以用作加密设备 2120 中的内容解密密钥。

另一方面，密钥加密设备 2118 利用以与光盘再现设备相同的方式输

入的盘密钥对上述输入的加密密钥加密，并产生加密的解密密钥。与这种加密的解密密钥的大小相比，扇区头部区中的每个解密密钥区 2106 和 2109 较小。因此，数据分隔器 2121 把加密的解密密钥分成多个分支解密密钥，然后，把各个分支解密密钥记录到不同的解密密钥区 2106 和 2109。在图 37 的实例中，加密的解密密钥被分成两个加密的分支解密密钥，然后被记录到两个连续扇区的解密密钥区 2106 和 2109 中。在这种情况下，因为由密钥加密设备 2118 对密码密钥的解密密钥进行加密，所以可以提高对加密密钥加密的安全强度。

再现内容时，密钥转换器 2113 利用上述第一解密密钥转换数据 2115 和第二解密密钥转换数据 2116 的信息对来自密钥解密设备 2112 的解密密钥执行预定的密钥转换操作或计算，产生内容解密密钥，然后输出给解密设备 2114。另外，解密设备 2114 利用此内容解密密钥对加密的内容数据进行解密，以获得解密的内容。在这种情况下，密钥转换器 2113 可以只利用第一解密密钥数据 2115 的信息对来自密钥解密设备 2112 的解密密钥执行预定的密钥转换操作或计算。

第十一优选实施例

图 38 是表示根据本发明的第十一优选实施例中光盘上的用户数据区的结构、在对内容加密并记录加密的内容记录在用户数据区中的光盘记录设备的结构，和对来自用户数据区的数据的加密内容进行解密的光盘再现设备的结构发框图。此第十一优选实施例的特征在于把光盘记录设备的结构增加到第七优选实施例上，下面将详细描述该结构。

参见图 38，光盘记录设备包括密钥加密设备 2118，利用预定的盘密钥按照与图 37 所示的第十优选实施例相同的方式对密码密钥加密；密钥转换器 2119，通过利用内容中的第一和第二解密密钥转换数据 2115 和 2116 对密码密钥执行的预定密钥转换操作从而对内容解密密钥执行操作或计算；和加密设备 2120，利用上述的内容解密密钥对内容执行加密。在这种情况下，将从密钥加密设备 2118 输出的解密密钥记录到导入区 2401 内的主数据区 2102 中。另一方面，光盘再现设备按照与图 29 所示的第七优选实施例相同的方式包括密钥解密设备 2112，密钥转换器

2113，和密钥解密设备 2114。在这种情况下，记录在导入区 2401 内的主数据区 2102 中的解密密钥被读出并输入到密钥解密设备 2112 中，然后利用预定的盘密钥对解密密钥进行解密，并输出解密后的解密密钥给密钥转换器 2113。另外，密钥转换器 2113 利用第一和第二解密密钥转换数据 2115 和 2116 对来自密钥解密设备 2112 的解密密钥执行预定的密钥转换操作或计算，以计算内容解密密钥，并输出给解密设备 2114。

第六至第九优选实施例的有益效果

如上所述，根据本优选实施例的记录型光盘把解密密钥分隔成具有分布在扇区头部区中的预定大小的解密密钥区的解密密钥，并记录分隔的解密密钥，或在由分布于扇区头部区中的密钥索引指示的解密密钥区中记录具有可变长度的解密密钥，于是，能够提供一种记录型光盘，其中该光盘利用任意或自由长度的解密密钥，而与扇区头部区中规定大小的解密密钥区无关。因此，根据对记录内容的版权保护等级，可以采用任意密钥长度的加密。

改型的优选实施例

在上述优选实施例中，上述盘识别信息最好由不可重写的预制凹坑构成，并且上述盘识别信息最好有区域标识符，用于代表光盘被使用的区域。另外，上述盘识别信息最好具有数据类别标识符，代表光盘上可被记录和再现的内容的类型、级别或种类。另外，上述盘识别信息最好利用秘密密钥加密，并且在制造时被记录到盘识别信息区。再者，上述盘识别信息最好包括用于代表可以记录到数据记录和再现区中的数据的类型、级别和种类，或可以从数据记录和再现区中再现的数据的类型、级别和种类的数据。

在上述优选实施例中，上述光盘最好有在其中记录内容数据的扇区区和用于管理与解扰密钥的对应关系的解扰区管理表。密钥管理信息区最好包括解扰密钥区，用于记录利用盘识别信息作为密钥加密的解扰密钥；具有解扰密钥状态区的密钥信息区，用于代表解扰密钥的记录状态或状况；内容信息区，用于在其中记录再现盘上记录的内容时使用的密

钥信息；和密钥索引区，用于在其中记录指针，该指针用于查阅再现内容所需的解扰密钥。另外，在记录内容数据的扇区中，最好记录有上述内容的数据，和用于指示在其中记录解扰密钥的区域的指针。

在上述优选实施例中，光盘记录和再现设备的盘识别信息的再现电路最好包括用于对已经利用秘密密钥加密的盘识别信息进行解密的电路。另外，在光盘记录和再现设备中，利用盘识别信息作为密钥加密的数据最好是诸如图像数据和音乐数据这样内容的数据。另外，盘识别信息最好代表可记录在数据记录和再现区中的数据的类型、级别或种类，并且盘识别信息的再现电路通过上述数据的类型，级别和种类判断该数据是否是可记录的数据。另外，利用盘识别信息作为密钥解密的数据最好是诸如图像数据或音乐数据这样的内容数据。另外，盘识别信息最好代表可以从记录和再现区再现的数据的类型、级别和种类，并且再现电路根据上述数据的类型、级别和种类判断该数据是否是可再现的内容。

在上述优选实施例中，内容的记录电路最好在相同的扇区中记录诸如加密的图像数据和音乐数据等之类的内容数据以及用于对上述内容的数据的加密进行解码或解密的解扰密钥。另外，内容的再现电路最好从相同的扇区中再现诸如加密的图像数据和音乐数据等之类内容数据以及用于对上述内容的数据的加密进行解码或解密的解扰密钥。

在上述优选实施例中，用于分配密钥区的电路或方法最好在代表解扰密钥的记录状态的解扰密钥状态区中设置用于保留区的标志，记录关于再现内容数据时使用的密钥的信息，并记录代表分配给该内容数据的解扰密钥的记录区的密钥索引。另外，设置解扰密钥的电路或方法最好从内容信息区中再现内容中使用的解扰密钥区的索引，把解扰密钥布置到由对应于记录的解扰密钥的密钥索引所指示的解扰密钥区中，并在由对应于记录的解扰密钥的密钥索引所指示的解扰密钥状态区中设置记录信息的标志。

在上述优选实施例中，光盘再现设备最好再现盘识别信息，搜索内容是否可以再现，再现密钥管理信息，再现其中已经记录了诸如图像数据或音乐数据这样的内容数据的扇区，并从再现的扇区获得解扰密钥。另外，再现内容的数据最好通过解扰密钥进行解扰，并且输出解扰后的

数据。

在上述优选实施例中，记录内容数据的方法最好记录加密的内容，使得当在具有用于在其中记录第一盘信息的第一信息区、用于在其中记录识别各个盘的第二盘信息的第二信息区、和用于通过在用户数据区上照射光束而记录信息的用户数据区的光盘的用户数据区中记录内容时，能够通过至少利用上述第二盘信息的操作或计算进行解码和再现。

在上述优选实施例中，记录内容数据的方法最好加密并记录信息，使得当在具有用于在其中记录第一盘信息的第一信息区、用于在其中记录识别各个盘的第二盘信息的第二信息区、用于通过在用户数据区上照射光束而记录信息的用户数据区、和用于在用户数据区内记录对加密并记录的内容解码或解密的密钥信息的密钥信息记录区的光盘的用户数据区中记录内容时，能够通过至少利用上述第二盘信息和密钥信息的操作或计算进行解码和再现。

在上述优选实施例中，把伪数据记录在具有解密密钥区的光盘的扇区中，其中解密密钥区用于在多个连续的扇区中记录多个分支解密密钥，最好把伪数据记录在主数据区中，在所述主数据区中，包括 AV 数据的数据大小小于（主数据大小）×（分支解密密钥的个数）。另外，在 ECC 块中，将具有解密密钥区的扇区记录（ECC 块单元）/（分支解密密钥的个数）次，其中解密密钥区用于记录被划分到多个连续扇区中的分支脱密密钥，并且把伪数据记录在主数据区中，在所述主数据区中，包括 AV 数据的数据大小小于（主数据大小）×（ECC 块单元）。

在上述优选实施例中，最好把用于对已经对包括 AV 数据的数据执行的加密进行解密的解密密钥分成具有预定大小的多个分支解密密钥，并且把多个分支解密密钥记录到其中解密密钥表连续的多个解密密钥区中。另外，最好把上述解密密钥表记录在可重写导入区内的主数据区中。另外，最好把用于代表解密密钥表的记录状态或状况的信息记录在解密密钥表的每个解密密钥区中，作为固定值。另外，将解密密钥表多次记录在设置在光盘的内外周的上述不同的 ECC 块内。

在上述优选实施例中，数据加密设备的编码设备 3101 和光盘记录和再现设备的光盘设备 3102 最好共享互相授权系统中的总线密钥。另外，

数据解码设备的解码设备 3103 和光盘记录和再现设备的光盘设备 3102 最好共享交叉授权系统中的总线密钥。

虽然在上述优选实施例中，描述了可记录数据并且是一次写入型或包括 RAM 型的可重写型、或不可重写型的记录型光盘，但是本发明并不局限于此。本发明可以应用于只读型光盘，可以读出并再现先前记录的数据但不能重新记录数据。在只读型光盘的情况下，可以用读出并再现数据的数据再现区代替数据记录和再现区，并且在制造时先记录内容数据或其它各种控制信息的数据。在这种情况下，记录型光盘包括 CD-R、CD-RW、MO、MD、DVD-RAM 等。只读型光盘包括音乐 CD、CD-ROM、DVD-ROM 等。

工业实用性

如上面的详细描述，根据本发明的光盘，把对每个光盘执行记录操作和再现操作所使用的盘识别信息记录在不可重写的只用于生产的区域（produce-only area），对光盘的内容记录操作和内容再现操作可以由用户利用制造光盘时所记录的信息进行控制。

另外，根据本发明的光盘，把已经利用不可重写的只读盘识别信息作为密钥进行了加密的数据记录到光盘的用户数据区，因此，甚至在用户把用户数据区复制到另一张记录型光盘的情况下，也不能复制盘识别信息，以致于不能进行数据的正确解密和再现。

另外，根据本发明的光盘，加密数据和用于对加密进行解密的解扰密钥被记录在彼此不同的扇区中，并且可以获得如电影和音乐这样需要版权保护的数据，并获得用于对加密进行独立解扰的解扰密钥。而且，通过利用盘识别信息作为密钥加密并记录解扰密钥，不能复制盘识别信息，这使得即使用户数据区被用户复制到另一张记录型光盘上，也不可能正确地记录和再现数据。通过获得并记录已经利用其上复制了数据的光盘的盘识别信息作为密钥进行了加密的解扰密钥，使其能够正确地记录和再现数据。

而且，根据本发明的光盘包括：用于在其中记录第一盘信息的第一信息区，用于记录识别各个盘的第二盘信息的第二信息区，和通过照射

光束而在用户数据区上记录信息的用户数据区。因此，通过根据现有技术给光盘上附加用于识别上述光盘的信息，可以很容易地执行光盘的管理。在这种情况下，上述第二信息区最好记录在上述第一信息区中，并且第二信息区的数据可以被用于再现上述第一信息区的光学拾取器再现。另外，上述第二信息区通过部分地消除或去除上述第一信息区内的记录膜而被记录，以致于形成多个具有径向伸长形状的修整区，并且这样就可以防止上述第二盘信息被很容易地篡改。

另外，根据本发明的光盘，解密密钥被分成多个分支解密密钥，该多个分支解密密钥被分配在各具有预定大小的、设置在扇区头部区中的多个解密密钥区中，或者解密密钥被记录在由设置在扇区头部区中的密钥索引区指示的解密密钥区中。这样可以提供一种记录型光盘，该盘可以独立于扇区头部区中的、具有规定大小的解密密钥区，利用具有任意或自由长度的解密密钥。因此，能够根据被记录内容的版权保护等级，利用任意的密钥长度进行加密。

虽然以上已参考附图结合优选实施例对本发明做了详细的描述，但应注意到，对本领域普通技术人员而言，各种变化和改型是显而易见的。这种变化和改型应理解为包括在本发明由权利要求限定的范围之内。

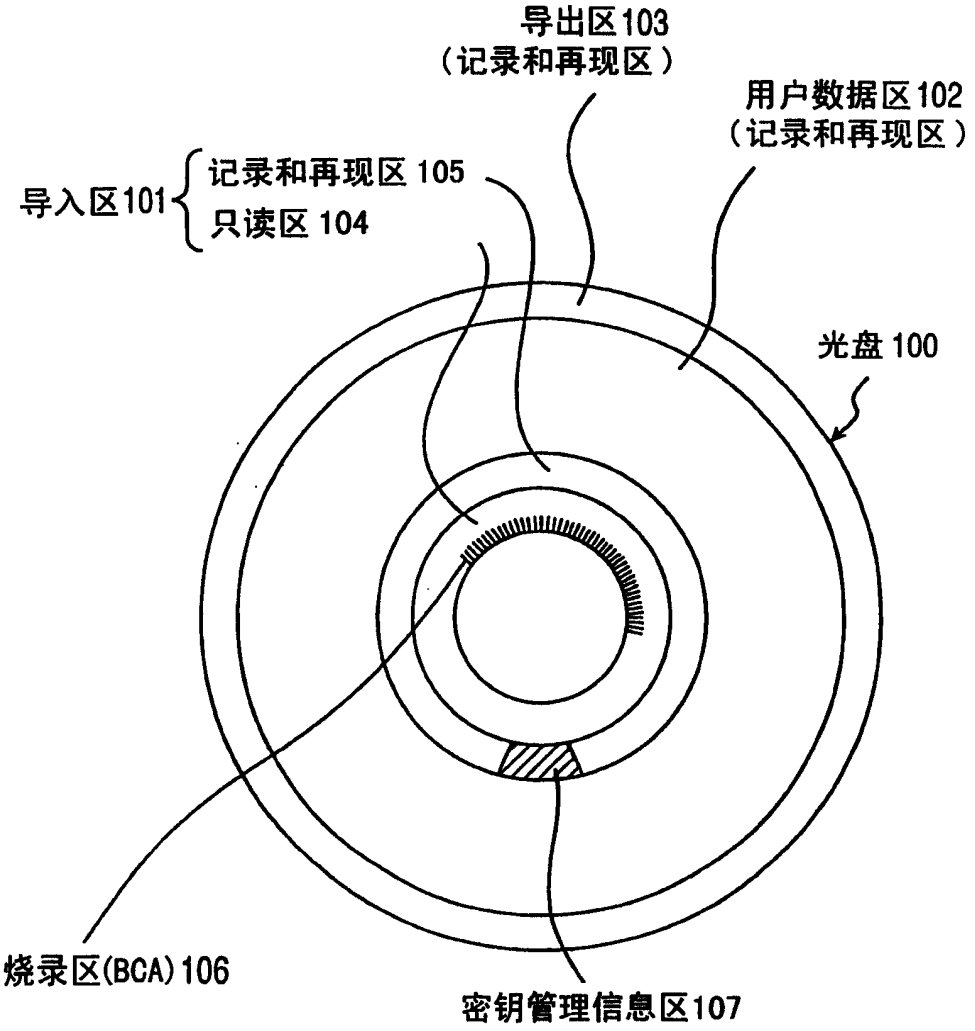

导出区103
（记录和再现区）
用户数据区102
（记录和再现区）
导入区101
记录和再现区 105
只读区 104
光盘 100
烧录区(BCA)106
密钥管理信息区107

图 1

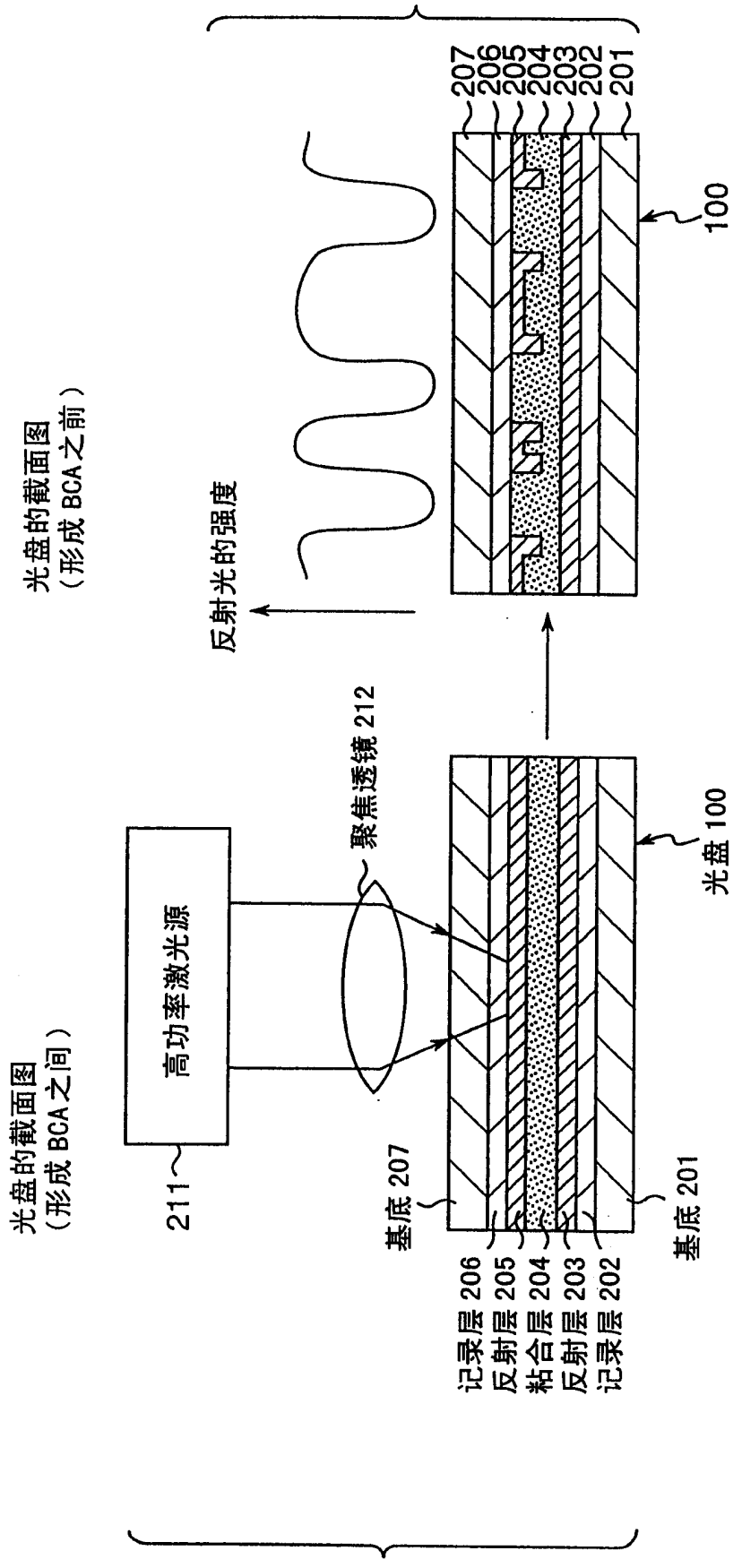

光盘的截面图
（形成 BCA 之前）
高功率激光源
211
聚焦透镜 212
光盘的截面图
（形成 BCA 之间）
基底 207
记录层 206
反射层 205
粘合层 204
反射层 203
记录层 202
基底 201
光盘 100
反射光的强度
207
206
205
204
203
202
201
100

图 2A

图 2B

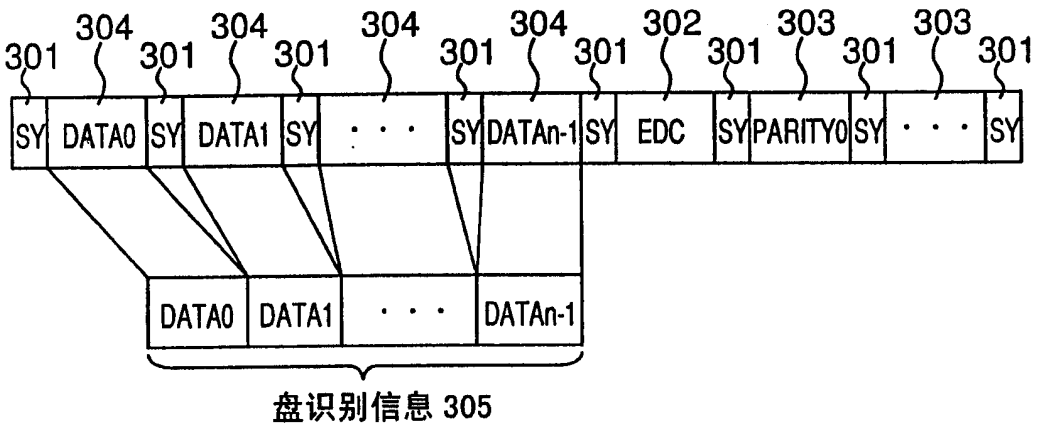

BCA的记录格式106
301
304
302
303
SY
DATA0
DATA1
DATAn-1
EDC
PARITY0
DATA0
DATA1
DATAn-1
盘识别信息 305

图 3

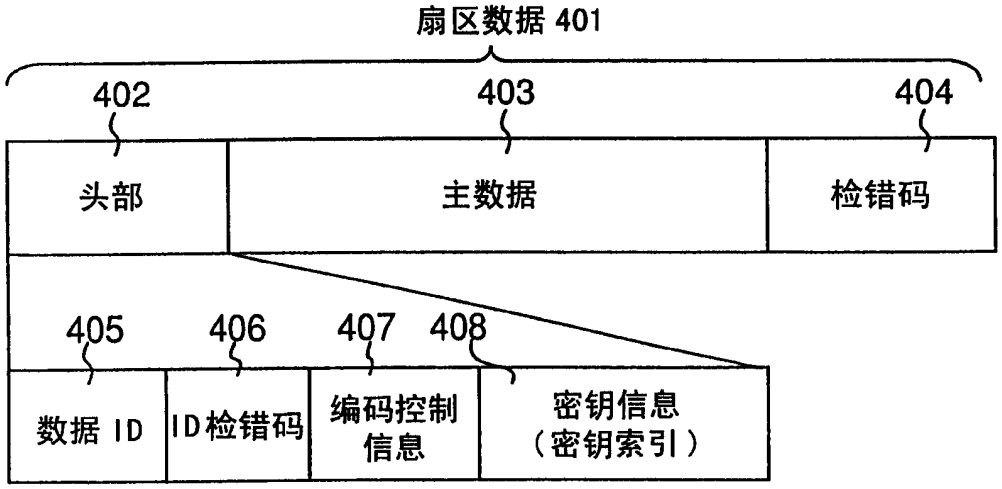

用户数据区 102 中的扇区 401 的扇区结构
扇区数据 401
402
403
404
头部
主数据
检错码
405
406
407
408
数据 ID
ID检错码
编码控制信息
密钥信息（密钥索引）

图 4

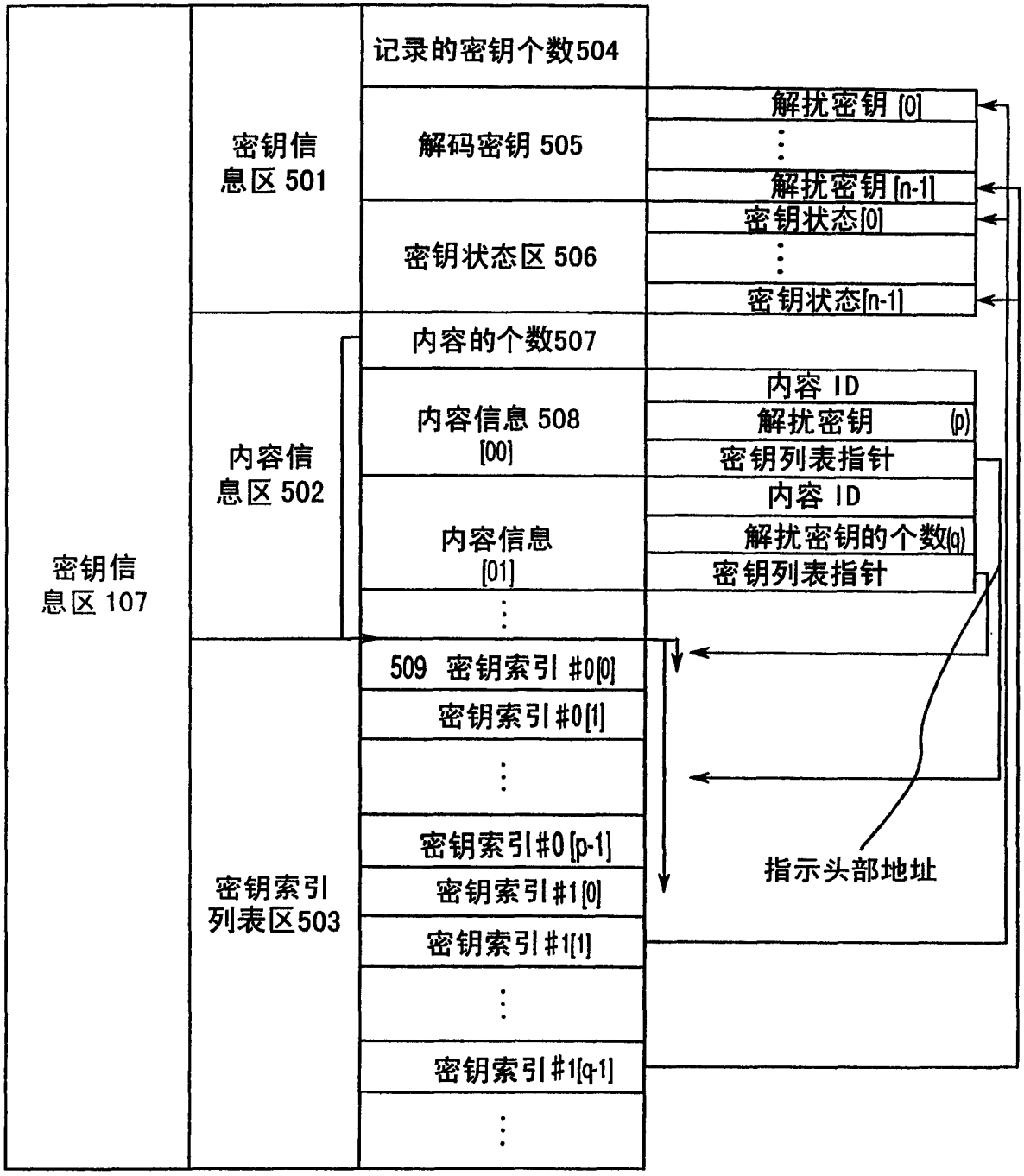
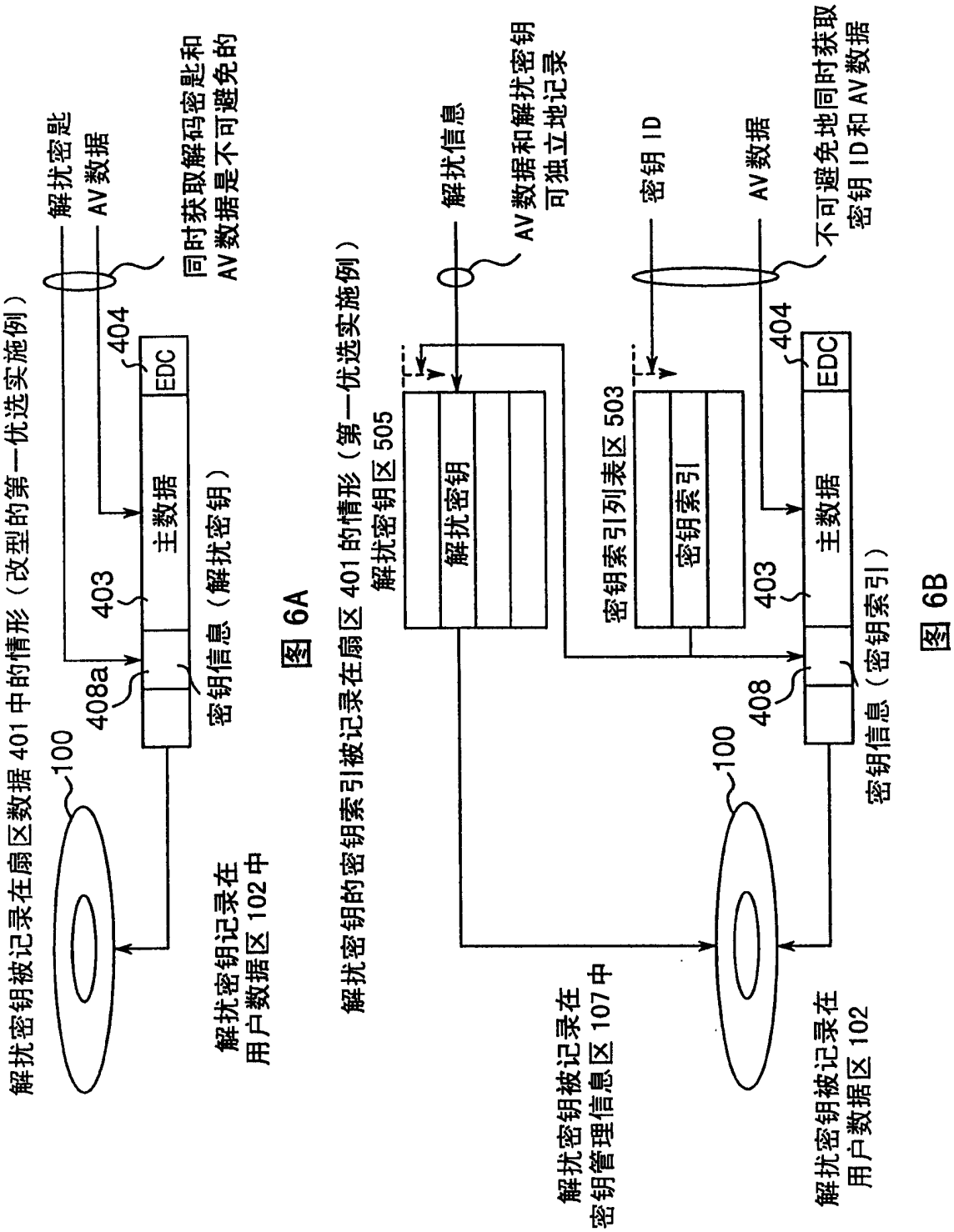

密钥信息区 107
密钥信息区 501
内容信息区 502
密钥索引列表区503
记录的密钥个数504
解码密钥 505
密钥状态区 506
内容的个数507
内容信息 508 [00]
内容信息 [01]
509 密钥索引 #0[0]
密钥索引#0[1]
密钥索引#0[p-1]
密钥索引#1[0]
密钥索引#1[1]
密钥索引#1[q-1]
解扰密钥 [0]
解扰密钥 [n-1]
密钥状态[0]
密钥状态[n-1]
内容 ID
解扰密钥 (p)
密钥列表指针
内容 ID
解扰密钥的个数(q)
密钥列表指针
指示头部地址

图 5


解扰密钥被记录在扇区数据 401 中的情形（改型的第一优选实施例）
100
408a
403
404
EDC
解扰密匙
AV数据
主数据
密钥信息（解扰密钥）
同时获取解码密匙和
AV数据是不可避免的
解扰密钥记录在
用户数据区 102 中
图 6A
解扰密钥的密钥索引被记录在扇区 401 的情形（第一优选实施例）
解扰密钥区 505
解扰信息
AV数据和解扰密钥
可独立地记录
密钥索引列表区 503
密钥 ID
AV数据
不可避免地同时获取
密钥 ID 和 AV 数据
解扰密钥
密钥索引
主数据
EDC
403
404
408
100
密钥信息（密钥索引）
解扰密钥被记录在
密钥管理信息区 107 中
解扰密钥被记录在
用户数据区 102
图 6B

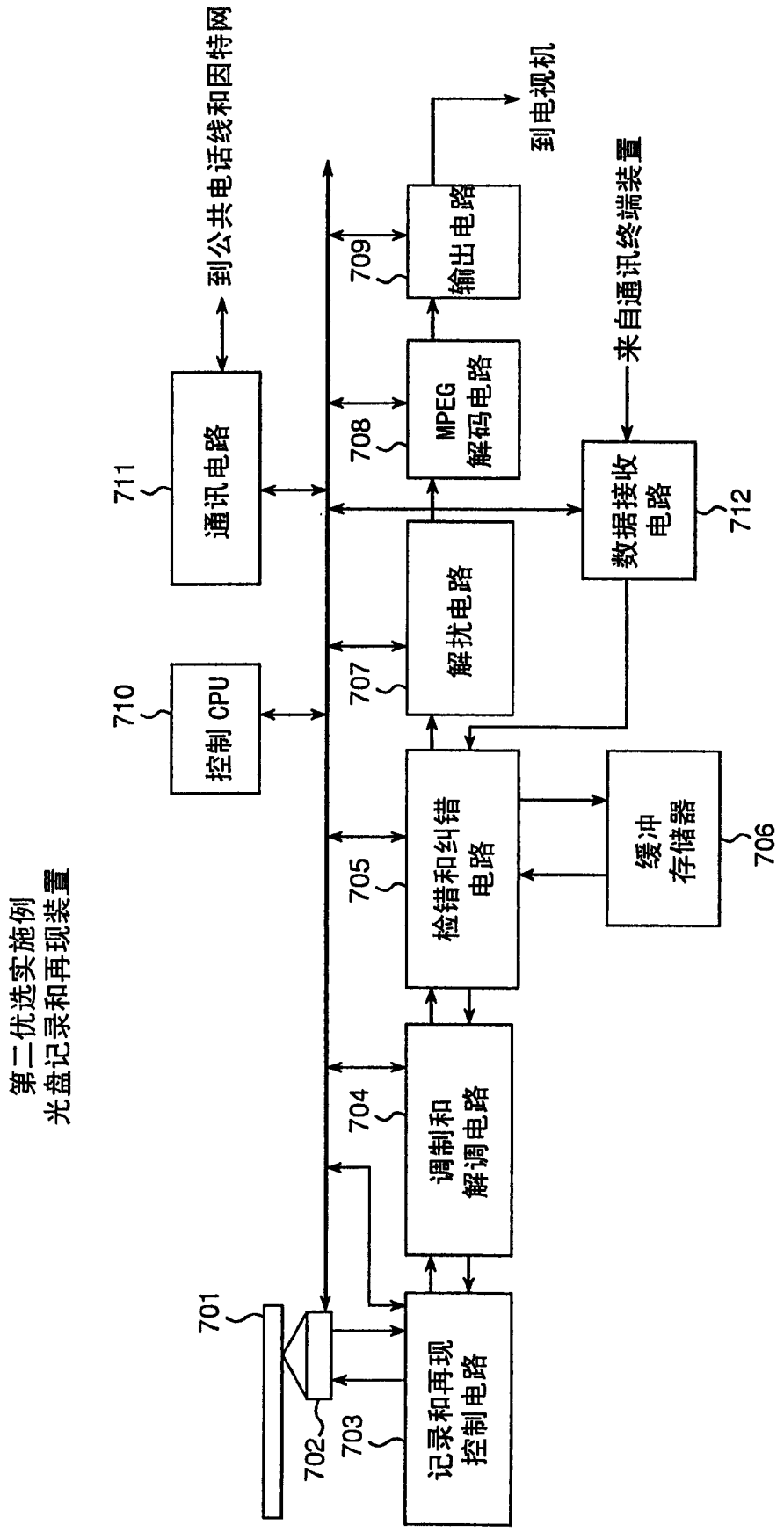

第二优选实施例
光盘记录和再现装置
701
702
703
记录和再现
控制电路
704
调制和
解调电路
705
检错和纠错
电路
706
缓冲
存储器
707
解扰电路
708
MPEG
解码电路
709
输出电路
到电视机
来自通讯终端装置
数据接收
电路
712
710
控制 CPU
711
通讯电路
到公共电话线和因特网

图 7

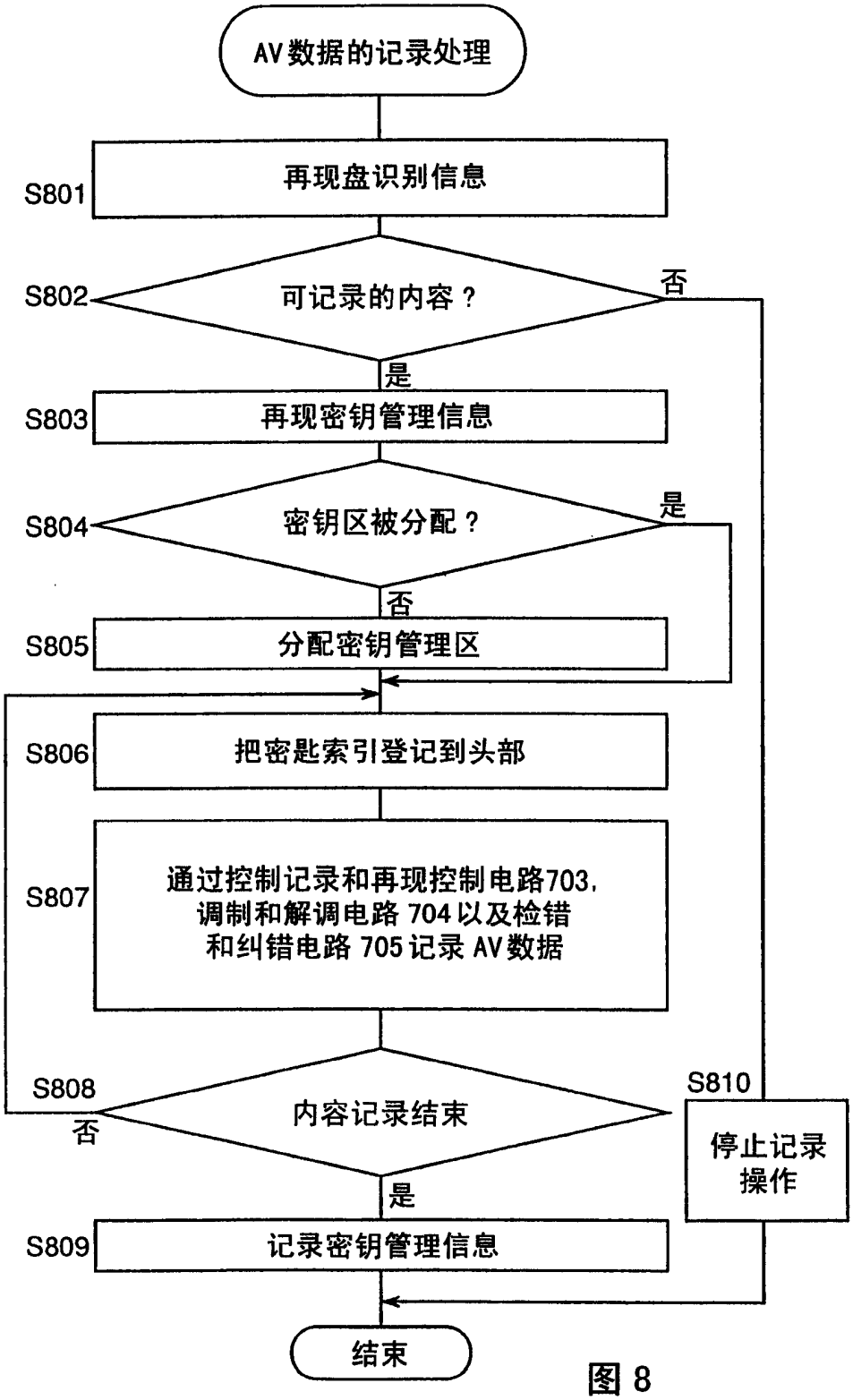

AV数据的记录处理
S801
再现盘识别信息
S802
可记录的内容？
否
是
S803
再现密钥管理信息
S804
密钥区被分配？
是
否
S805
分配密钥管理区
S806
把密匙索引登记到头部
S807
通过控制记录和再现控制电路703，
调制和解调电路 704 以及检错
和纠错电路 705 记录 AV数据
S808
内容记录结束
否
S810
停止记录
操作
是
S809
记录密钥管理信息
结束

图 8

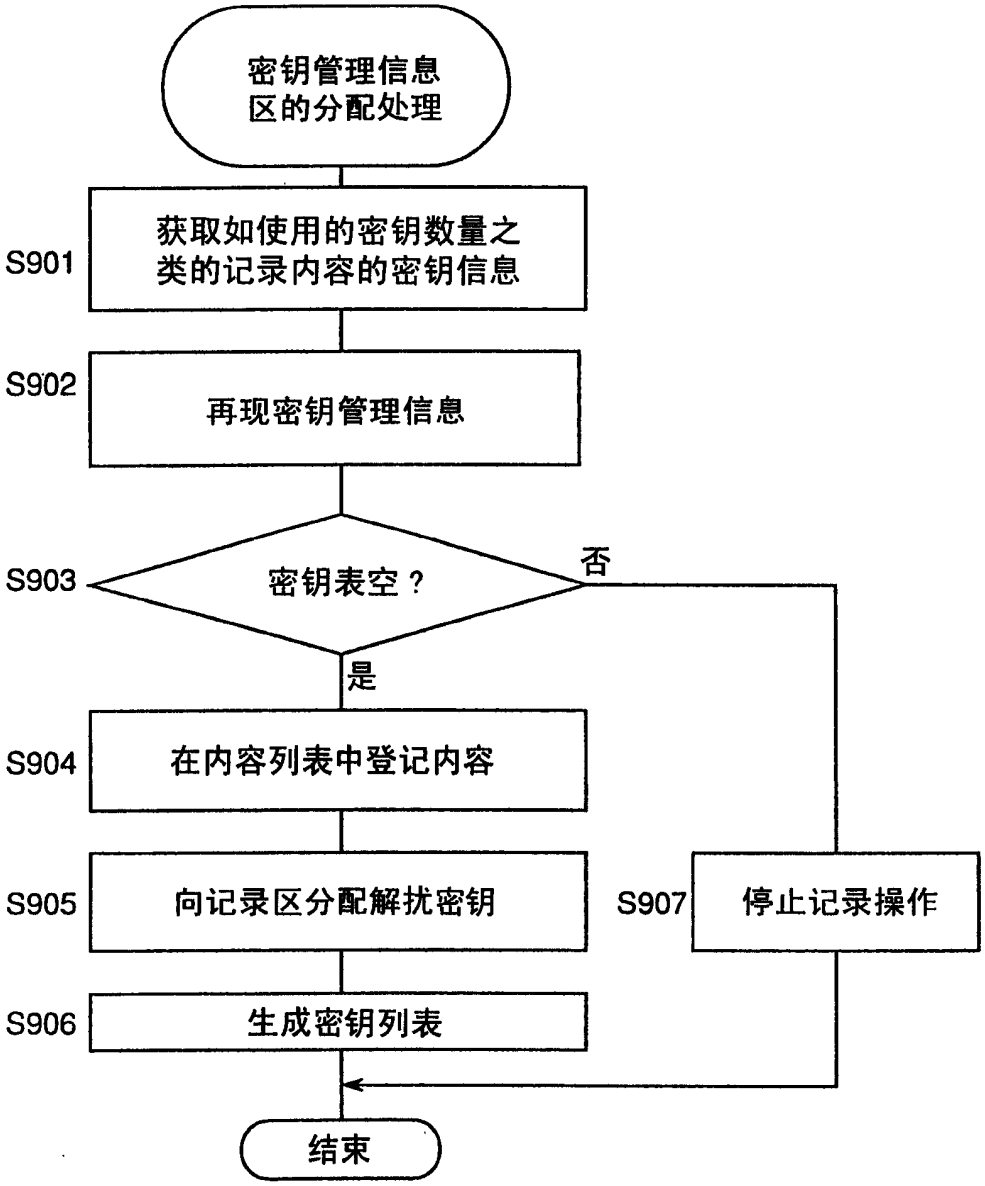

密钥管理信息
区的分配处理
S901
获取如使用的密钥数量之
类的记录内容的密钥信息
S902
再现密钥管理信息
S903
密钥表空？
否
是
S904
在内容列表中登记内容
S905
向记录区分配解扰密钥
S907
停止记录操作
S906
生成密钥列表
结束

图 9

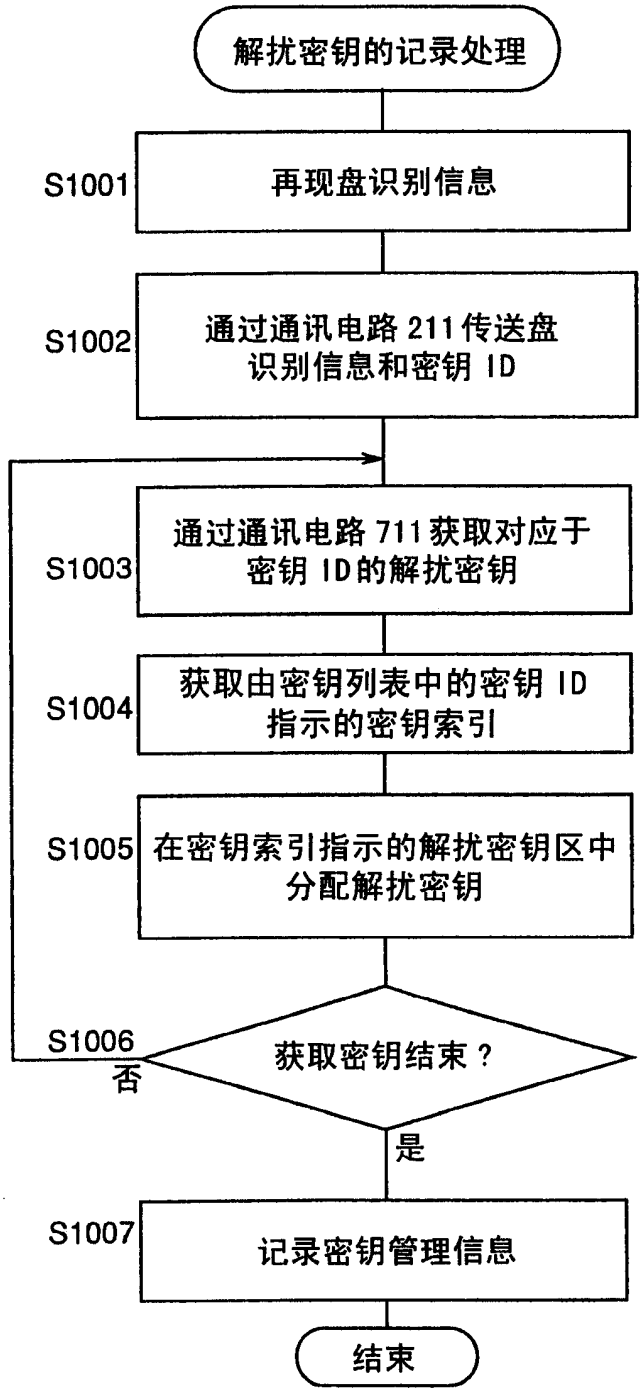

解扰密钥的记录处理
S1001
再现盘识别信息
S1002
通过通讯电路 211 传送盘识别信息和密钥 ID
S1003
通过通讯电路 711 获取对应于密钥 ID 的解扰密钥
S1004
获取由密钥列表中的密钥 ID 指示的密钥索引
S1005
在密钥索引指示的解扰密钥区中分配解扰密钥
S1006
获取密钥结束？
否
是
S1007
记录密钥管理信息
结束

图 10

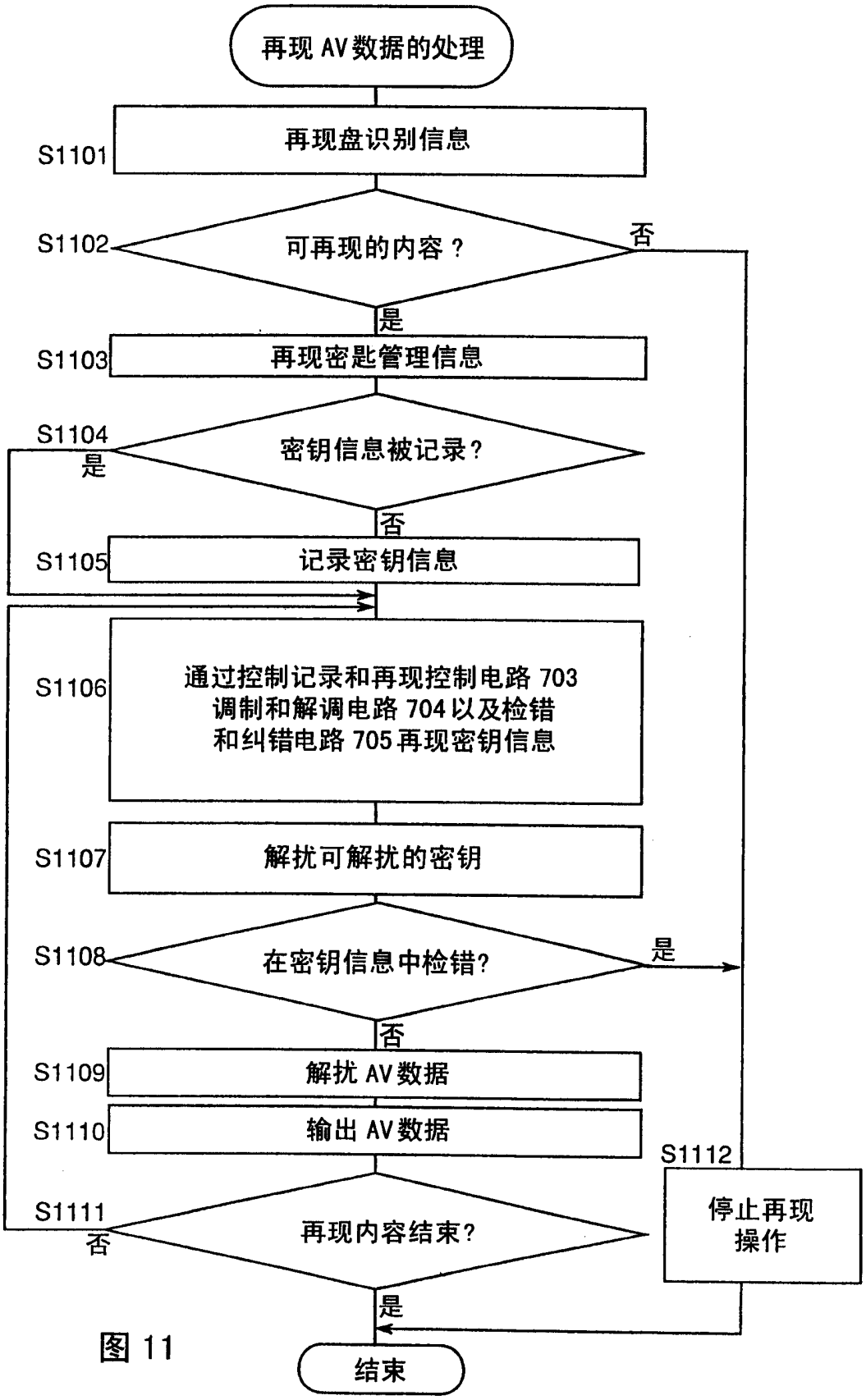

再现 AV数据的处理
S1101
再现盘识别信息
S1102
可再现的内容？
否
是
S1103
再现密匙管理信息
S1104
密钥信息被记录？
是
否
S1105
记录密钥信息
S1106
通过控制记录和再现控制电路 703
调制和解调电路 704 以及检错
和纠错电路 705 再现密钥信息
S1107
解扰可解扰的密钥
S1108
在密钥信息中检错？
是
否
S1109
解扰 AV数据
S1110
输出 AV数据
S1111
再现内容结束？
否
是
S1112
停止再现
操作
结束

图 11

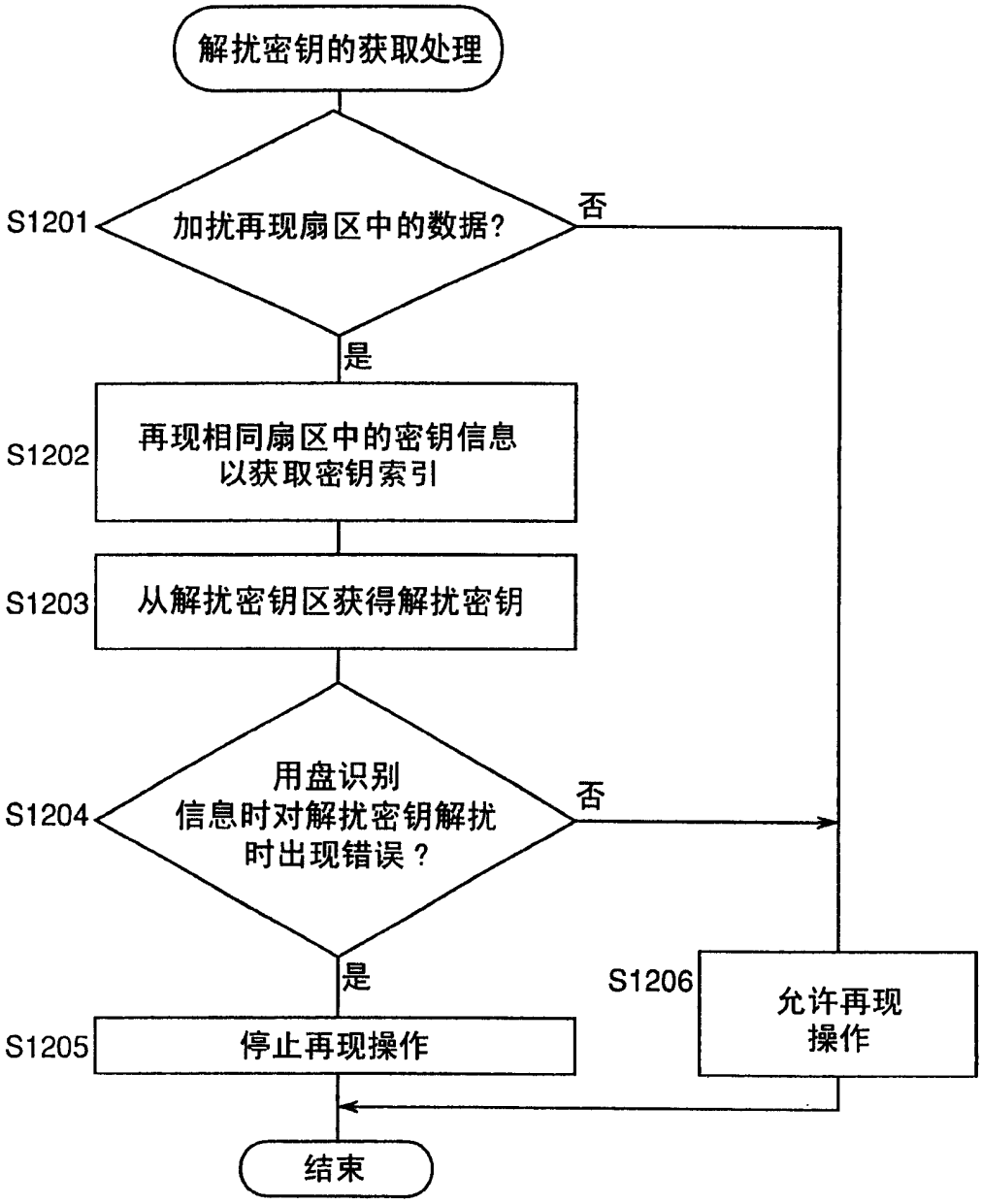

解扰密钥的获取处理
S1201
加扰再现扇区中的数据?
否
是
S1202
再现相同扇区中的密钥信息
以获取密钥索引
S1203
从解扰密钥区获得解扰密钥
S1204
用盘识别
信息时对解扰密钥解扰
时出现错误？
否
是
S1206
允许再现
操作
S1205
停止再现操作
结束

图 12

改型的第一优选实施例

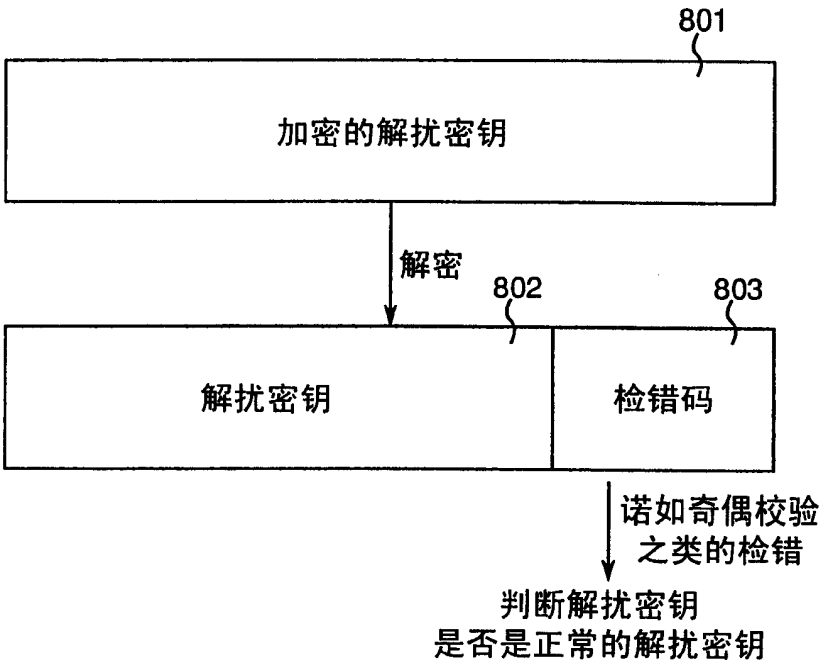


图 13

改型的第一优选实施例

解扰区管理表

1	起始地址 1	结束地址 1	解扰密钥 1
2	起始地址 2	结束地址 2	解扰密钥 2
⋮	⋮	⋮	⋮
n	起始地址 n	结束地址 n	解扰密钥 n

图 14

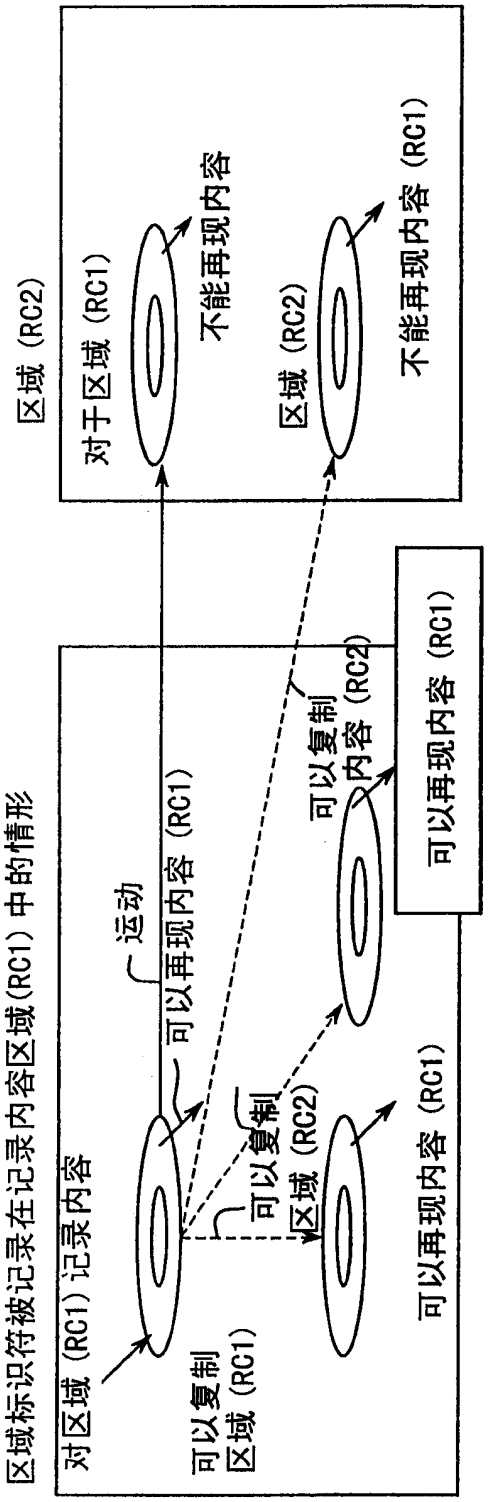

区域标识符被记录在记录内容区域(RC1)中的情形
对区域(RC1)记录内容
运动
可以再现内容(RC1)
可以复制区域(RC1)
可以复制区域(RC2)
可以复制内容(RC2)
可以再现内容(RC1)
可以再现内容(RC1)
区域(RC2)
对于区域(RC1)
不能再现内容
区域(RC2)
不能再现内容(RC1)

图 15A

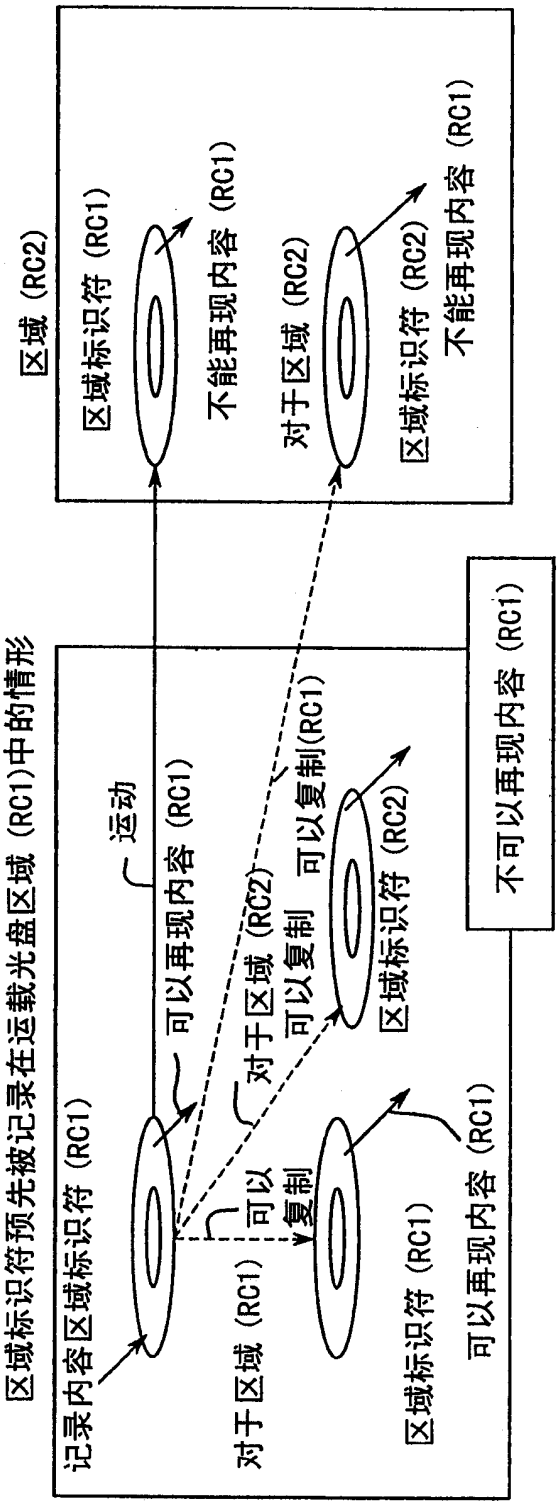

区域标识符预先被记录在运载光盘区域(RC1)中的情形
记录内容区域标识符(RC1)
运动
可以再现内容(RC1)
对于区域(RC1)
可以复制
对于区域(RC2)
可以复制(RC1)
区域标识符(RC1)
区域标识符(RC2)
可以再现内容(RC1)
不可以再现内容(RC1)
区域(RC2)
区域标识符(RC1)
不能再现内容(RC1)
对于区域(RC2)
区域标识符(RC2)
不能再现内容(RC1)

图 15B

第三优选实施例

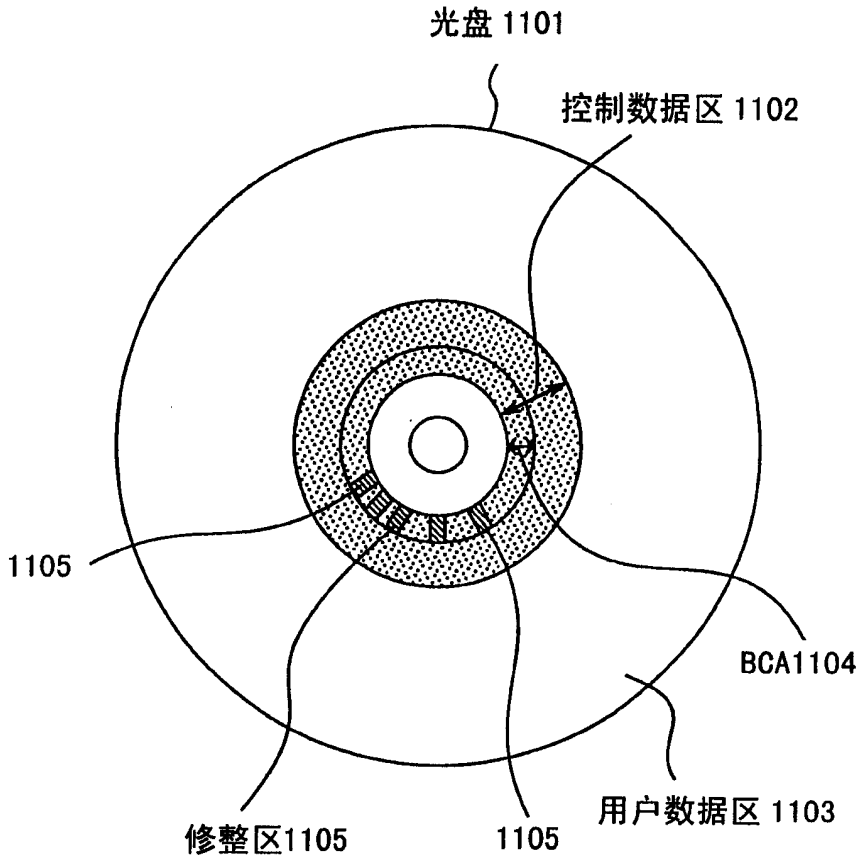


图 16

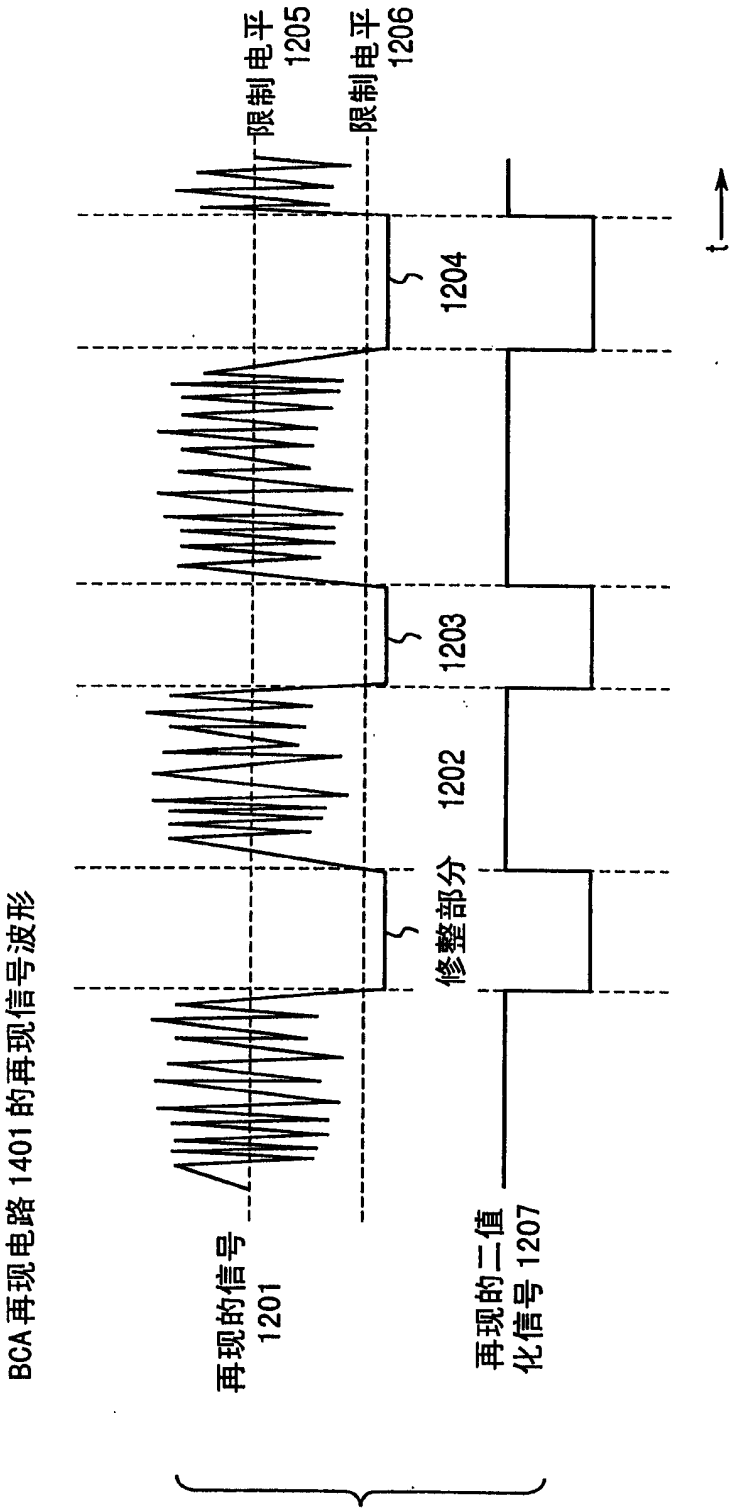

BCA再现电路1401的再现信号波形
再现的信号 1201
限制电平 1205
限制电平 1206
修整部分 1202
1203
1204
再现的二值化信号 1207
t

图 17

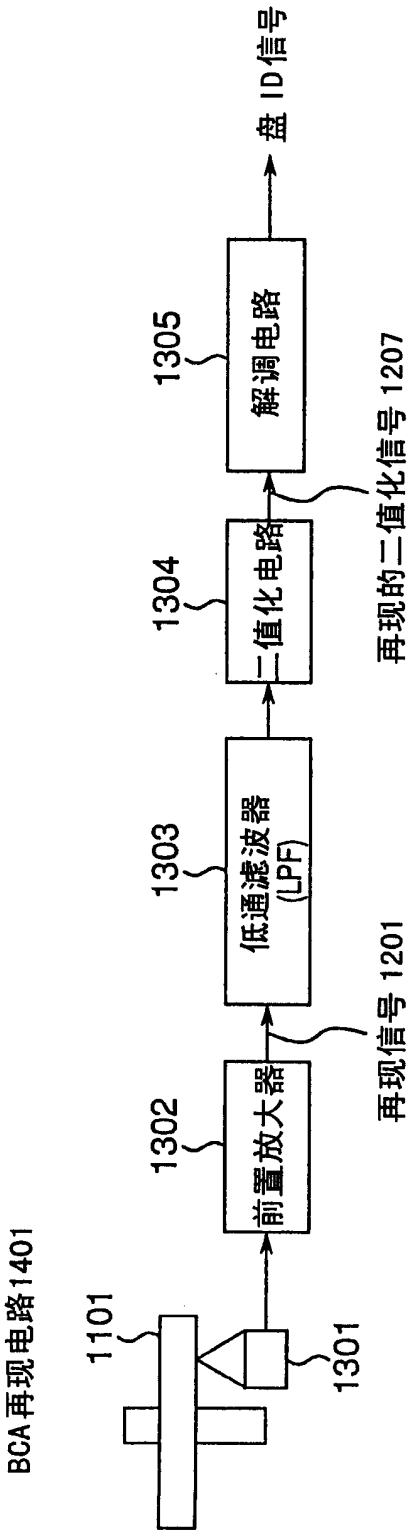

BCA再现电路1401
1101
1301
1302
前置放大器
再现信号 1201
1303
低通滤波器
(LPF)
1304
二值化电路
再现的二值化信号 1207
1305
解调电路
盘 ID信号

图 18

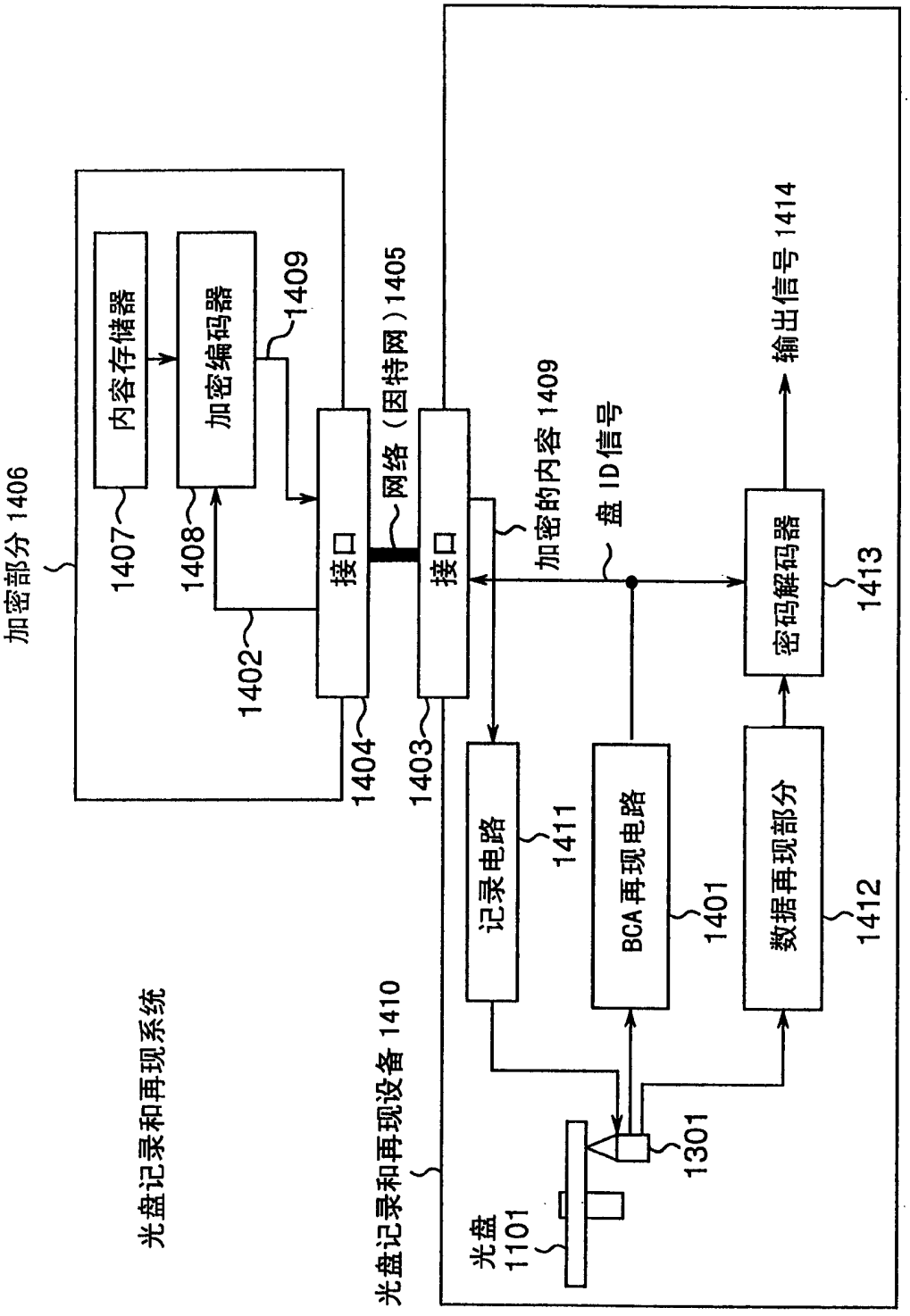

光盘记录和再现系统
加密部分 1406
内容存储器
1407
加密编码器
1408
1409
1402
接口
1404
网络（因特网）1405
接口
1403
光盘记录和再现设备 1410
光盘
1101
1301
记录电路
1411
BCA再现电路
1401
数据再现部分
1412
加密的内容 1409
盘 ID信号
密码解码器
1413
输出信号 1414

图 19

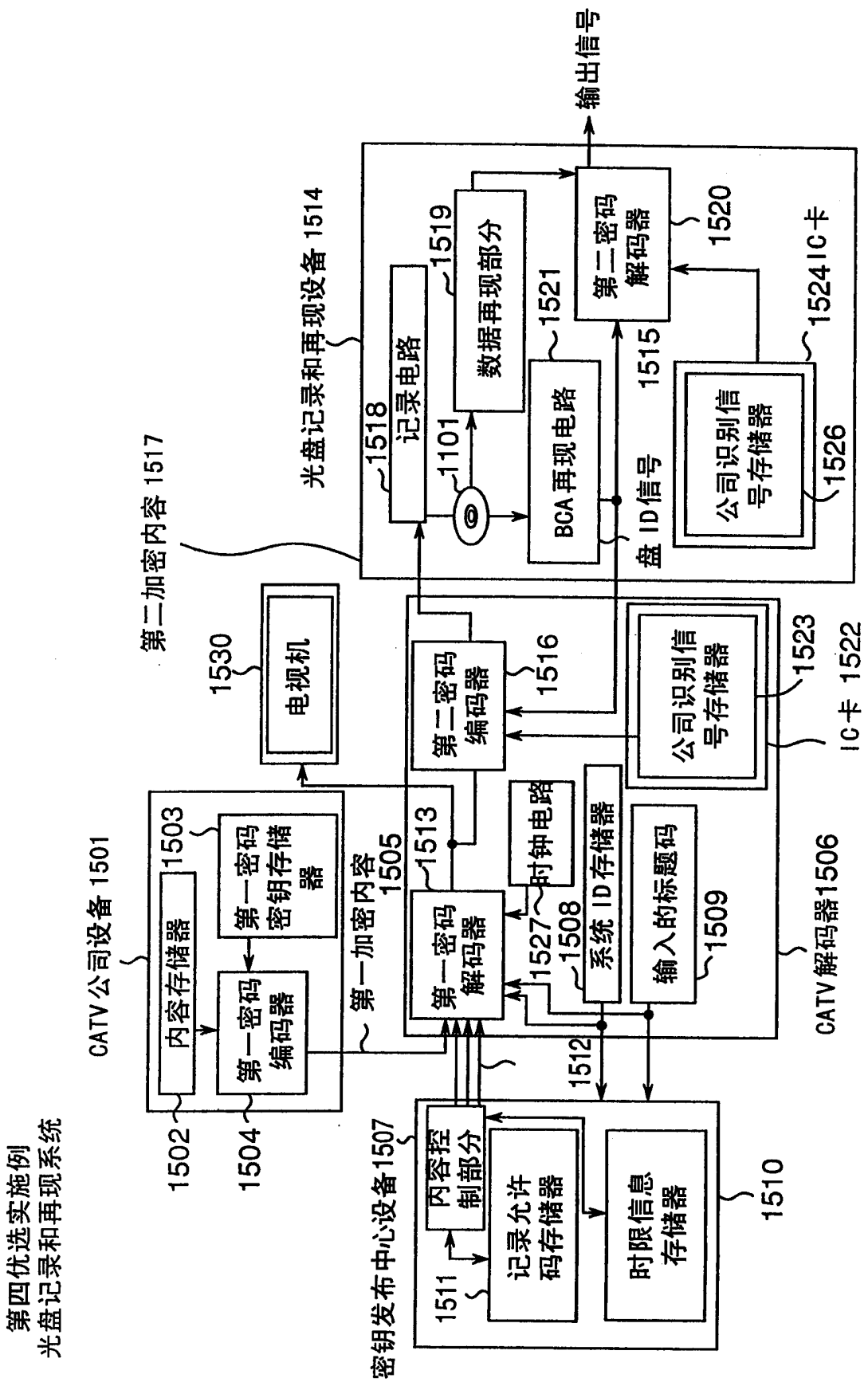

第四优选实施例
光盘记录和再现系统
CATV公司设备 1501
内容存储器
1502
第一密码编码器
1504
第一密码密钥存储器
1503
第一加密内容
1505
密钥发布中心设备1507
内容控制部分
1511
记录允许码存储器
时限信息存储器
1510
1512
第一密码解码器
1527
1508
时钟电路
系统ID存储器
输入的标题码
1509
CATV解码器1506
第二密码编码器
1516
第二加密内容 1517
1530
电视机
公司识别信号存储器
1523
IC卡 1522
光盘记录和再现设备 1514
1518
记录电路
1101
1519
数据再现部分
1521
BCA再现电路
盘ID信号
1515
第二密码解码器
1520
1524IC卡
公司识别信号存储器
1526
输出信号

图 20

第五优选实施例

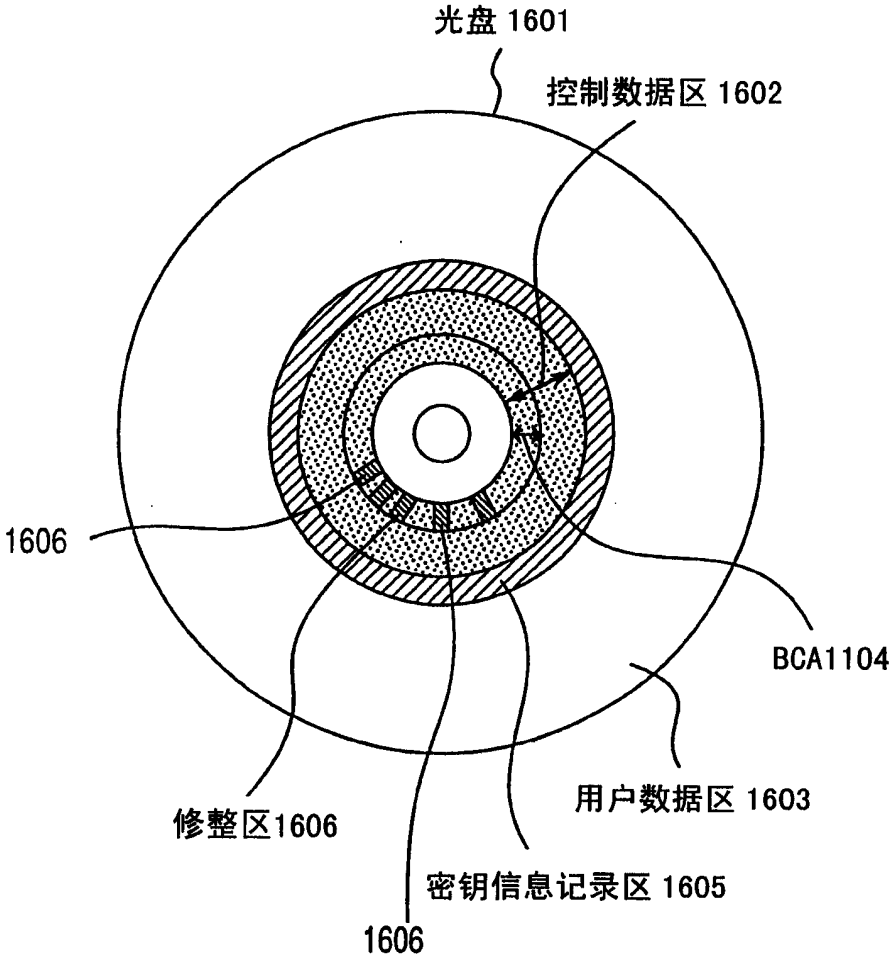

光盘 1601
控制数据区 1602
1606
BCA1104
用户数据区 1603
修整区1606
密钥信息记录区 1605
1606

图 21

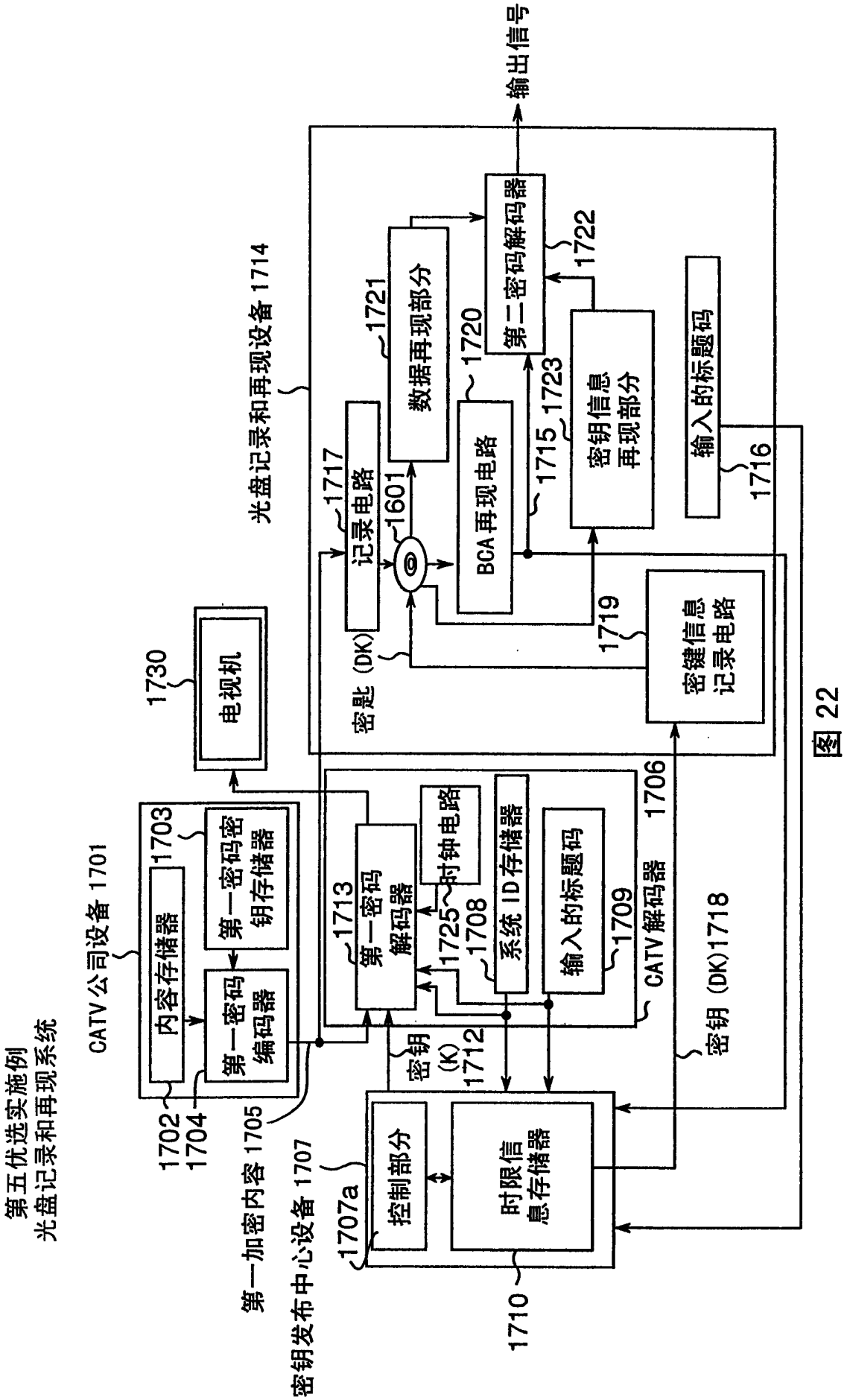

第五优选实施例
光盘记录和再现系统
CATV公司设备 1701
内容存储器
1703
第一密码密钥存储器
第一密码编码器
1702
1704
第一加密内容 1705
密钥发布中心设备 1707
1707a
控制部分
时限信息存储器
1710
密钥 (K) 1712
第一密码解码器
1713
时钟电路
1725
1708
系统 ID存储器
输入的标题码
1709
CATV解码器 1706
密钥 (DK)1718
光盘记录和再现设备 1714
记录电路
1717
1601
密匙 (DK)
1730
电视机
数据再现部分
1721
BCA 再现电路
1720
第二密码解码器
1722
密钥信息再现部分
1715
1723
1719
密键信息记录电路
输入的标题码
1716
输出信号

图 22

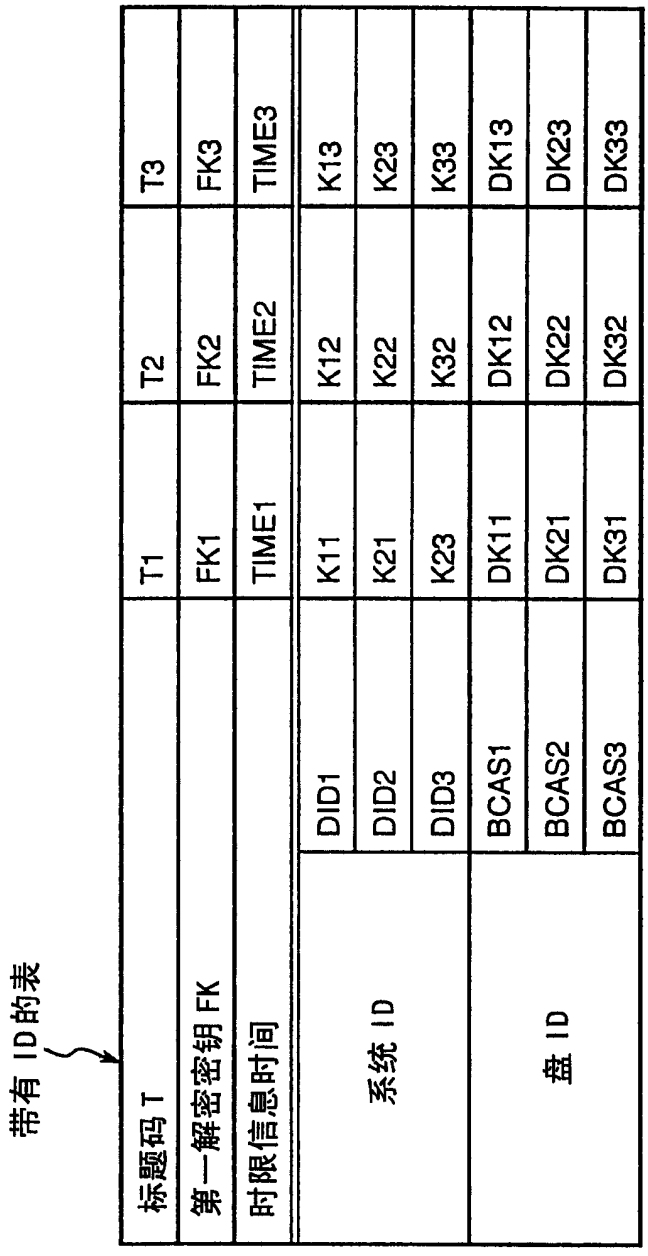

带有 ID 的表
标题码 T
T1
T2
T3
第一解密密钥 FK
FK1
FK2
FK3
时限信息时间
TIME1
TIME2
TIME3
系统 ID
DID1
K11
K12
K13
DID2
K21
K22
K23
DID3
K23
K32
K33
盘 ID
BCAS1
DK11
DK12
DK13
BCAS2
DK21
DK22
DK23
BCAS3
DK31
DK32
DK33

图 23

改型的第三优选实施例

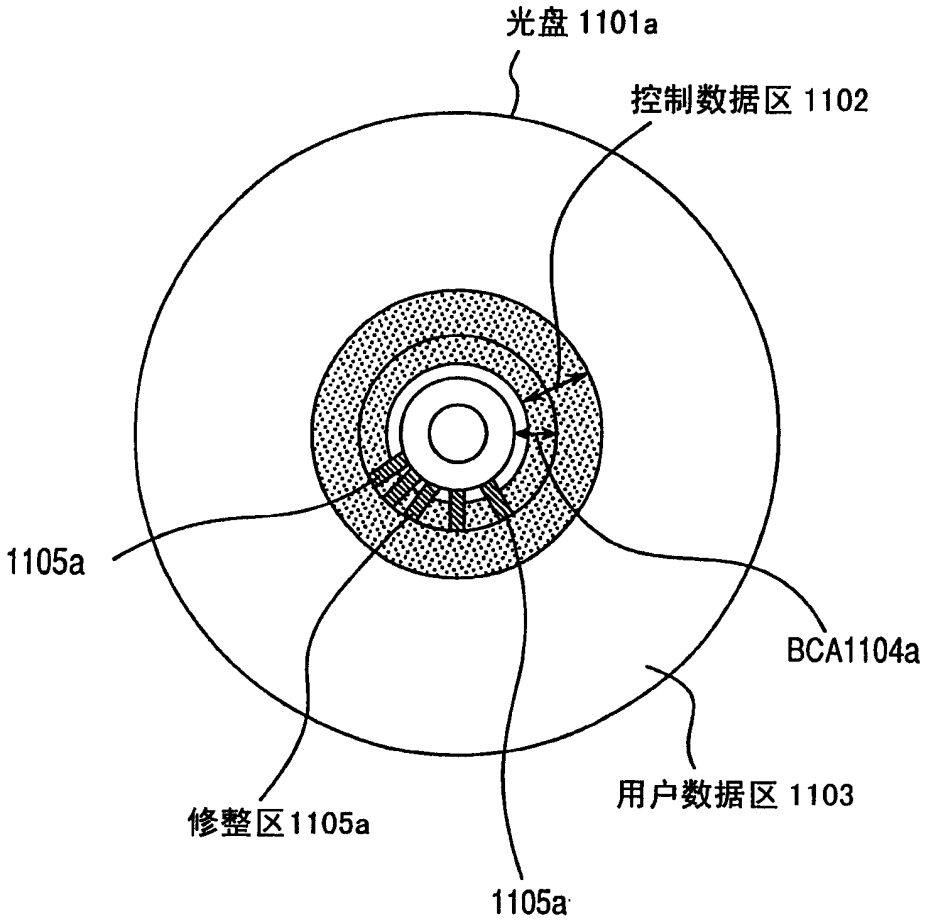


图 24

改型的第五优选实施例

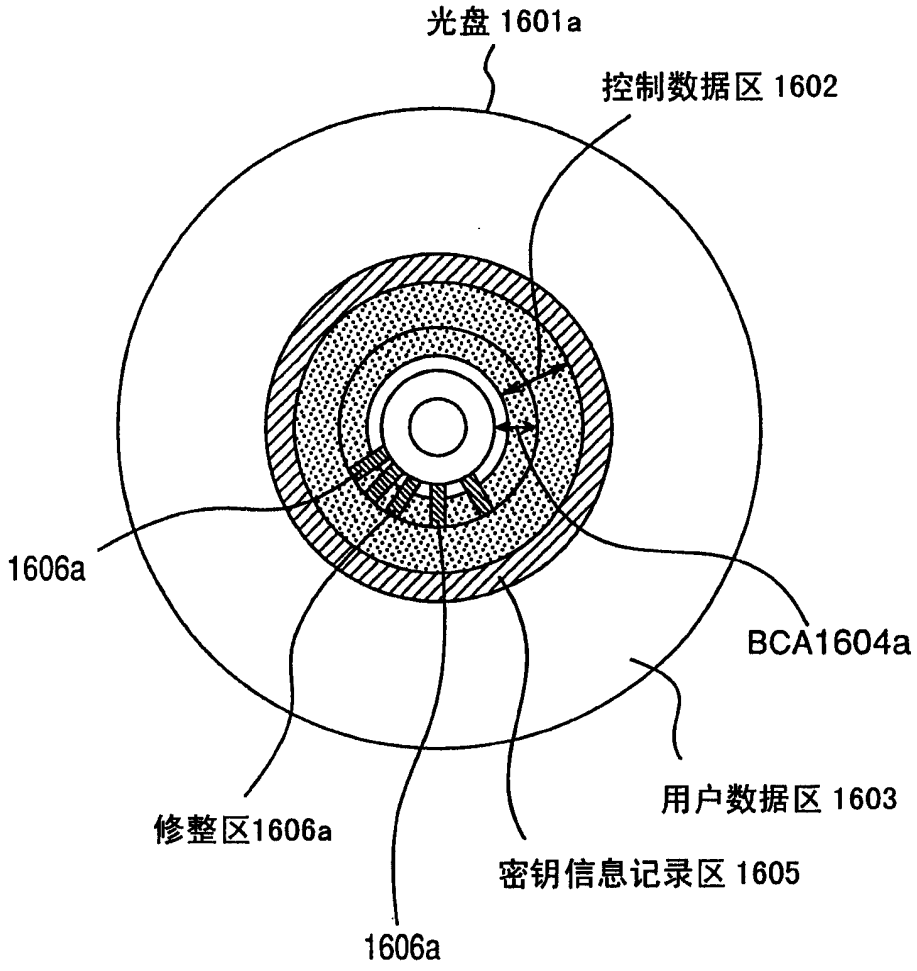


图 25

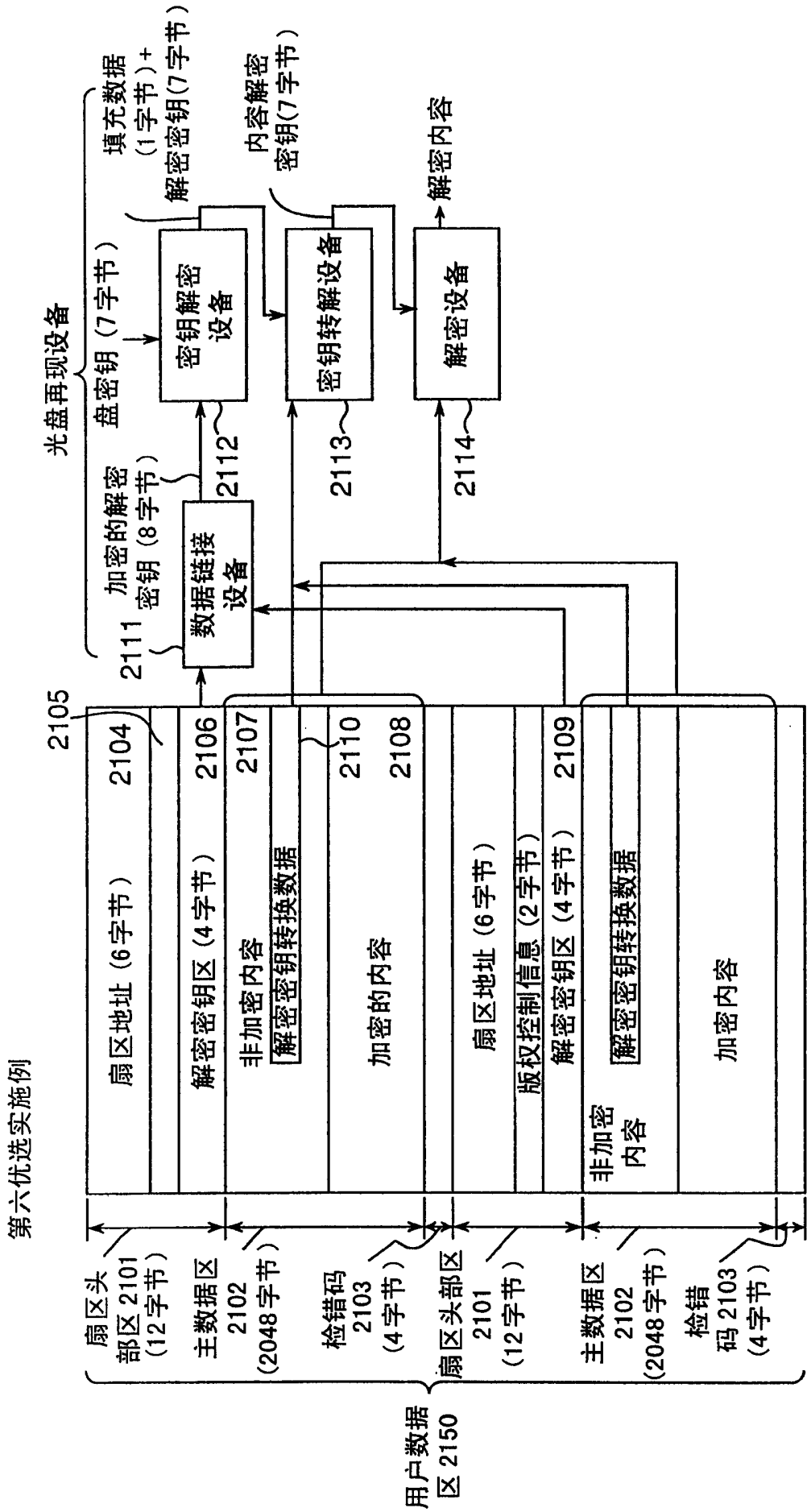

第六优选实施例
光盘再现设备
盘密钥（7字节）
加密的解密密钥（8字节）
2111
数据链接设备
密钥解密设备
2112
密钥转解设备
2113
解密设备
2114
填充数据（1字节）+解密密钥(7字节)
内容解密密钥(7字节)
解密内容
2105
扇区地址（6字节）
2104
解密密钥区（4字节）
2106
非加密内容
2107
解密密钥转换数据
2110
加密的内容
2108
扇区地址（6字节）
版权控制信息（2字节）
解密密钥区（4字节）
2109
非加密内容
解密密钥转换数据
加密内容
扇区头部区2101（12字节）
主数据区2102（2048字节）
检错码2103（4字节）
扇区头部区2101（12字节）
主数据区2102（2048字节）
检错码2103（4字节）
用户数据区2150

图 26

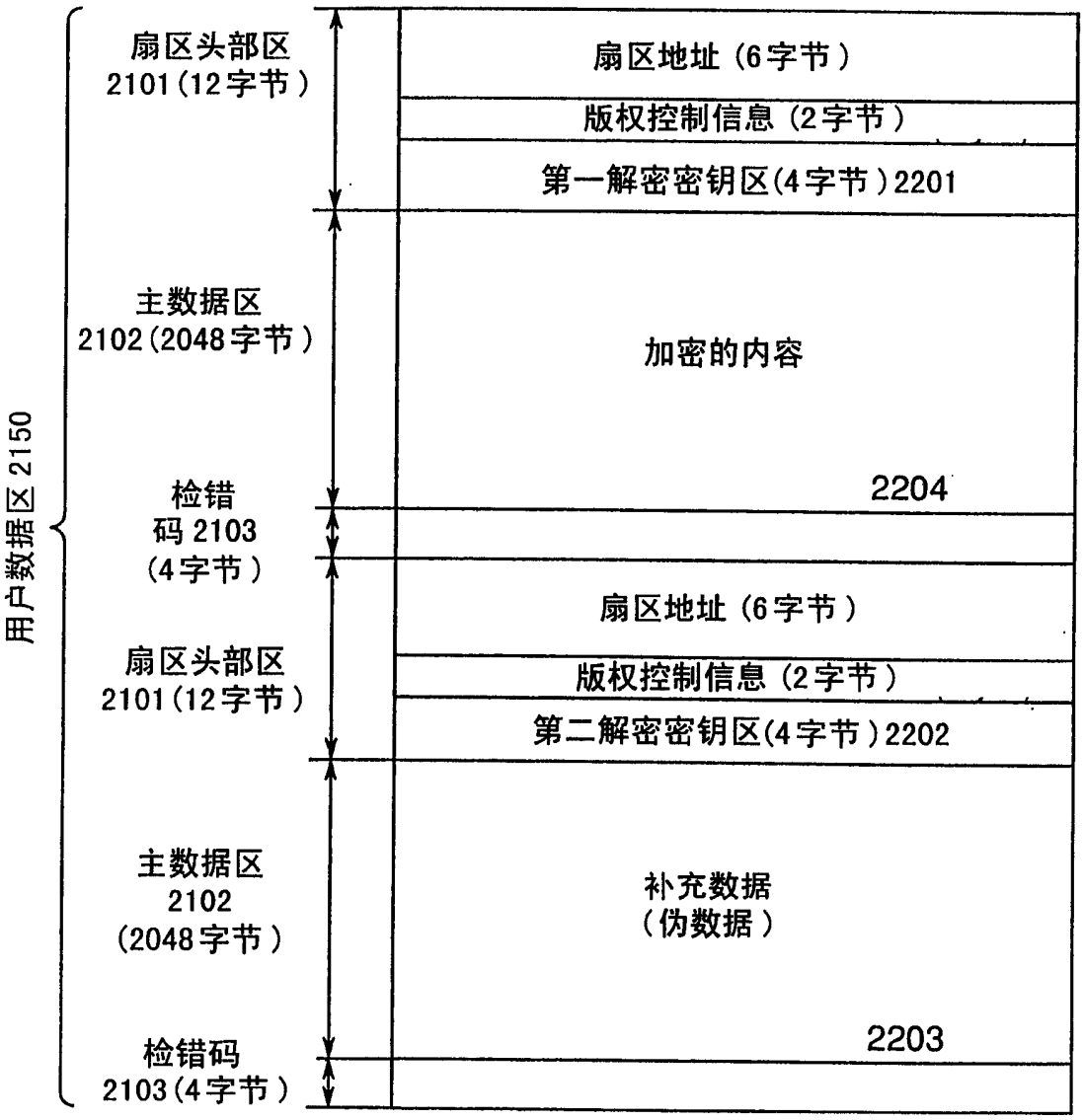

用户数据区 2150
扇区头部区
2101(12字节)
主数据区
2102(2048字节)
检错
码 2103
(4字节)
扇区头部区
2101(12字节)
主数据区
2102
(2048字节)
检错码
2103(4字节)
扇区地址(6字节)
版权控制信息(2字节)
第一解密密钥区(4字节)2201
加密的内容
2204
扇区地址(6字节)
版权控制信息(2字节)
第二解密密钥区(4字节)2202
补充数据
(伪数据)
2203

图 27

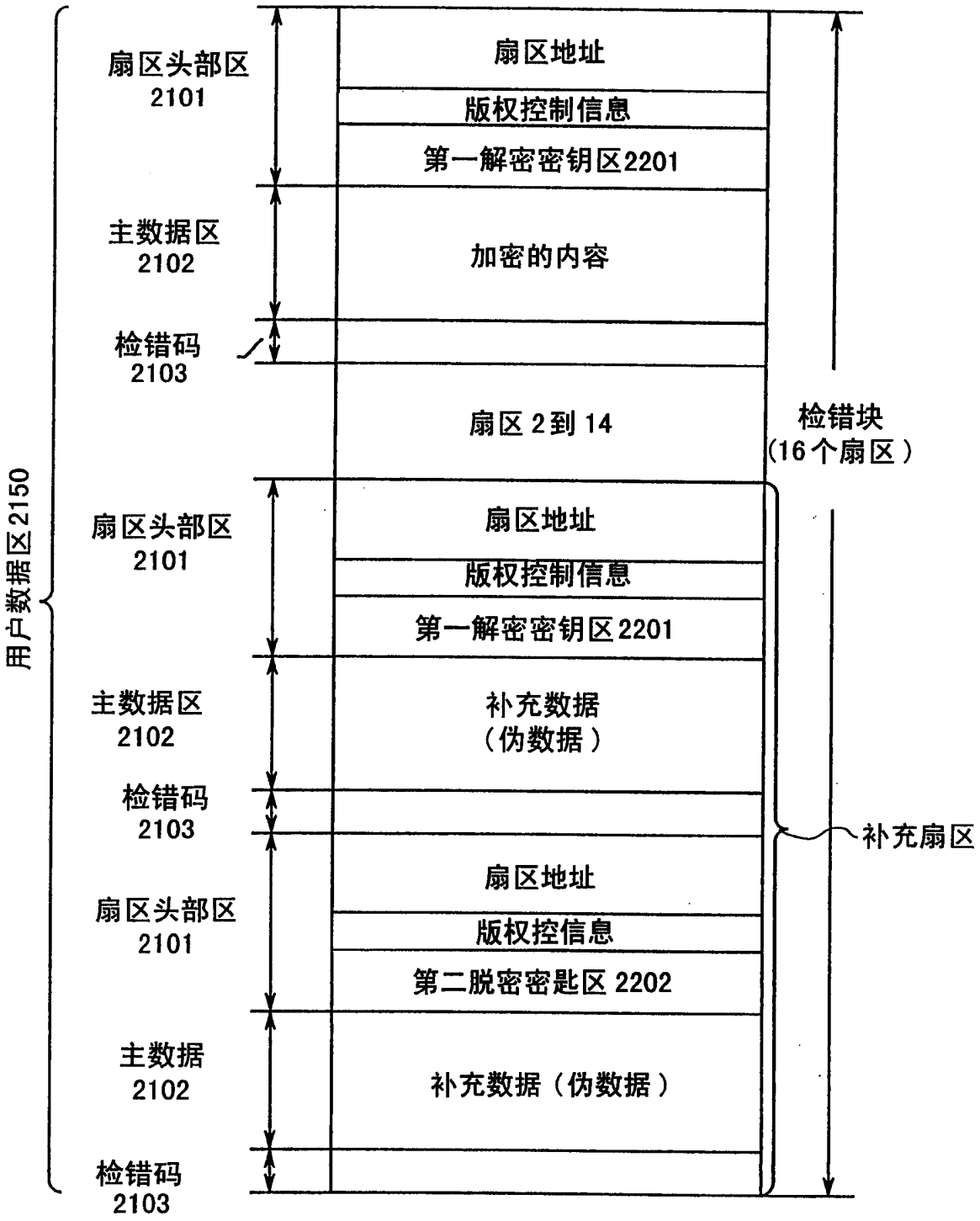

用户数据区2150
扇区头部区
2101
扇区地址
版权控制信息
第一解密密钥区2201
主数据区
2102
加密的内容
检错码
2103
扇区 2到 14
检错块
(16个扇区)
扇区头部区
2101
扇区地址
版权控制信息
第一解密密钥区2201
主数据区
2102
补充数据
(伪数据)
检错码
2103
补充扇区
扇区头部区
2101
扇区地址
版权控信息
第二脱密密匙区 2202
主数据
2102
补充数据(伪数据)
检错码
2103

图 28

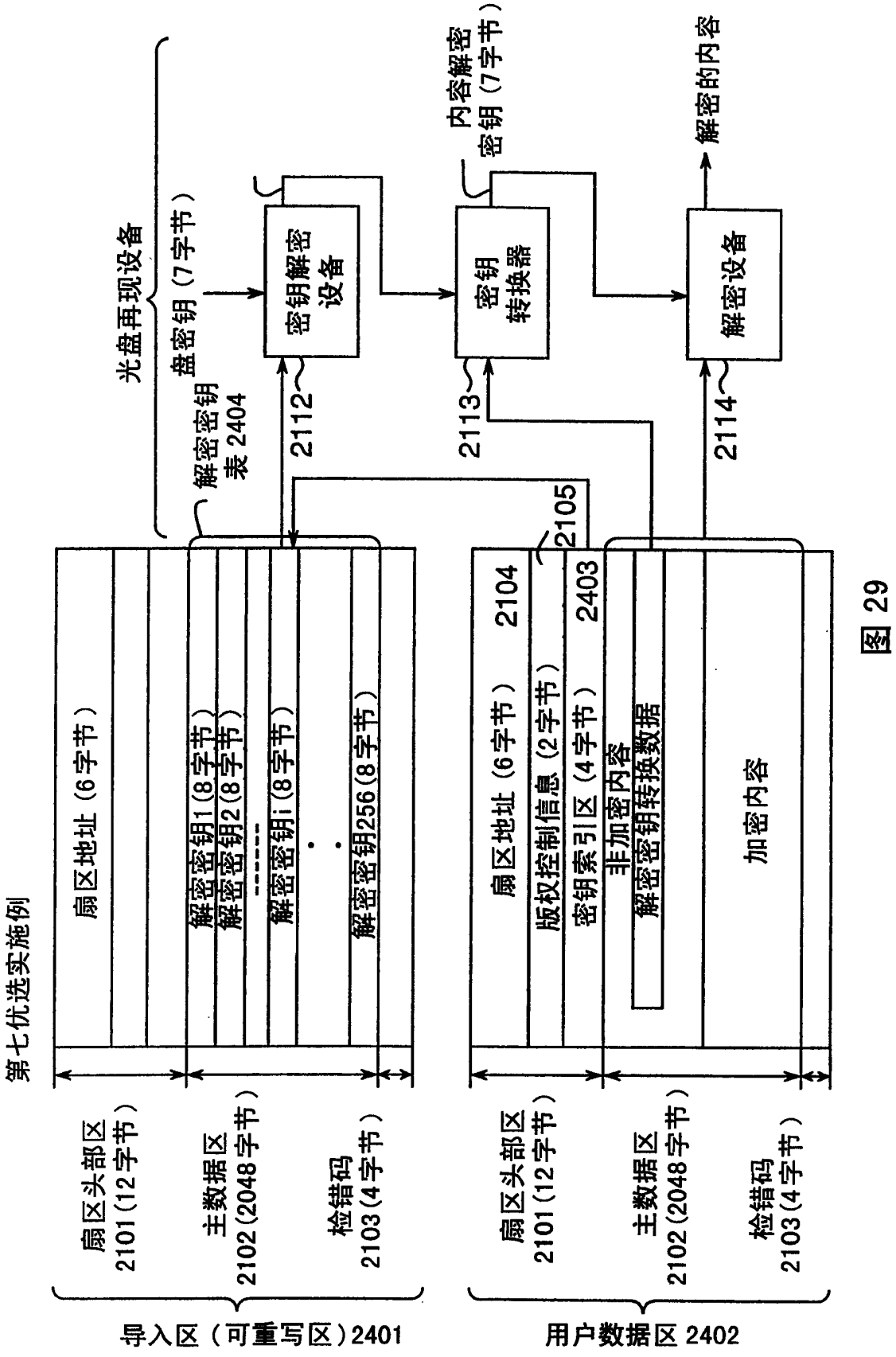

第七优选实施例
光盘再现设备
盘密钥（7字节）
解密密钥表 2404
密钥解密设备
2112
内容解密密钥（7字节）
密钥转换器
2113
解密设备
2114
解密的内容
2105
扇区地址（6字节）
解密密钥1(8字节)
解密密钥2(8字节)
解密密钥i(8字节)
解密密钥256(8字节)
扇区地址（6字节）
2104
版权控制信息（2字节）
密钥索引区（4字节）
2403
非加密内容
解密密钥转换数据
加密内容
扇区头部区 2101(12字节)
主数据区 2102(2048字节)
检错码 2103(4字节)
扇区头部区 2101(12字节)
主数据区 2102(2048字节)
检错码 2103(4字节)
导入区（可重写区）2401
用户数据区 2402

图 29

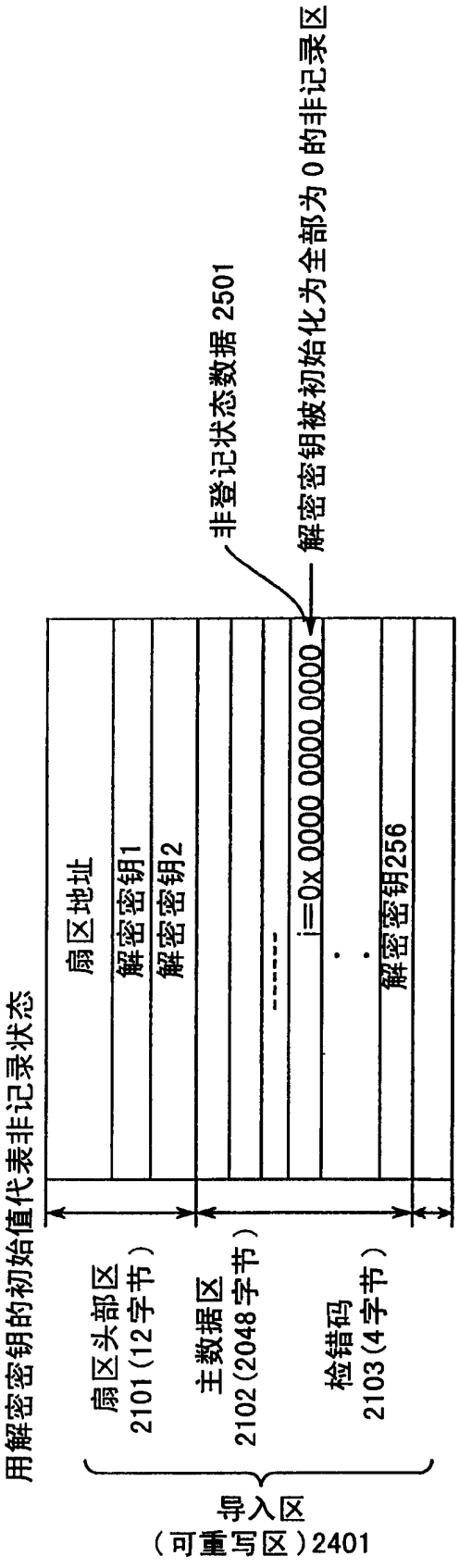

用解密密钥的初始值代表非记录状态
扇区地址
解密密钥1
解密密钥2
非登记状态数据 2501
解密密钥被初始化为全部为 0 的非记录区
i=0x 0000 0000 0000
解密密钥256
扇区头部区
2101(12字节)
主数据区
2102(2048字节)
检错码
2103(4字节)
导入区
(可重写区)2401

图 30A

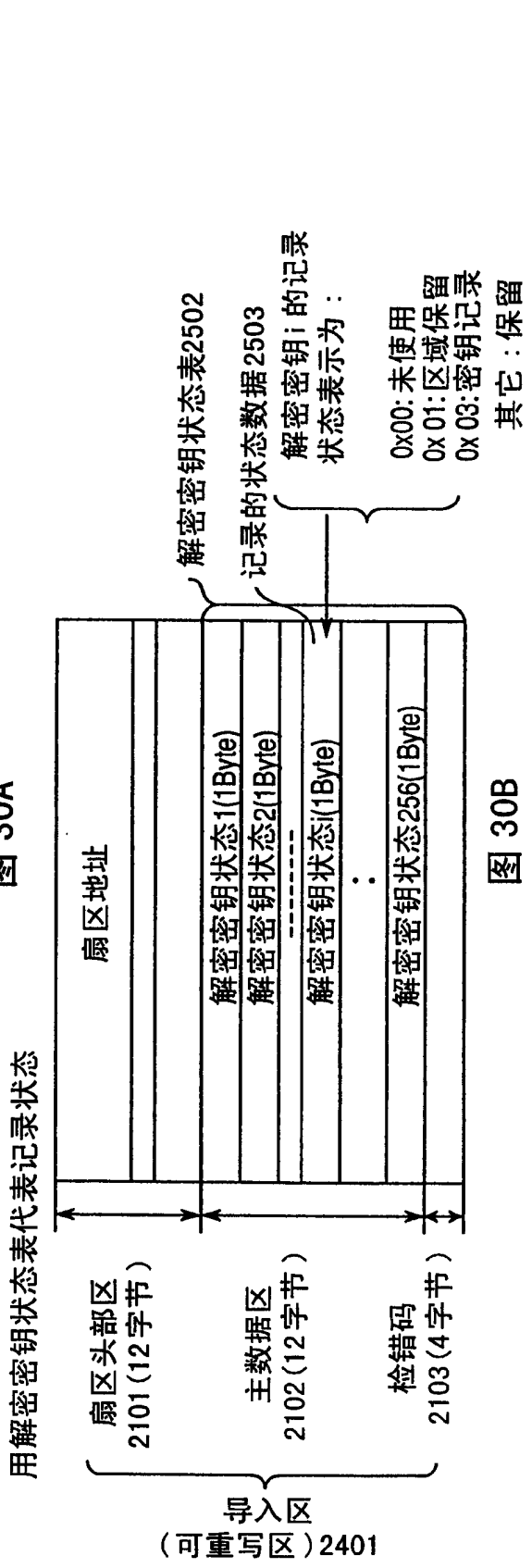

用解密密钥状态表代表记录状态
扇区地址
解密密钥状态表2502
记录的状态数据2503
解密密钥状态1(1Byte)
解密密钥状态2(1Byte)
解密密钥状态i(1Byte)
解密密钥状态256(1Byte)
解密密钥i的记录状态表示为：
0x00:未使用
0x 01:区域保留
0x 03:密钥记录
其它：保留
扇区头部区
2101(12字节)
主数据区
2102(12字节)
检错码
2103(4字节)
导入区
(可重写区)2401

图 30B

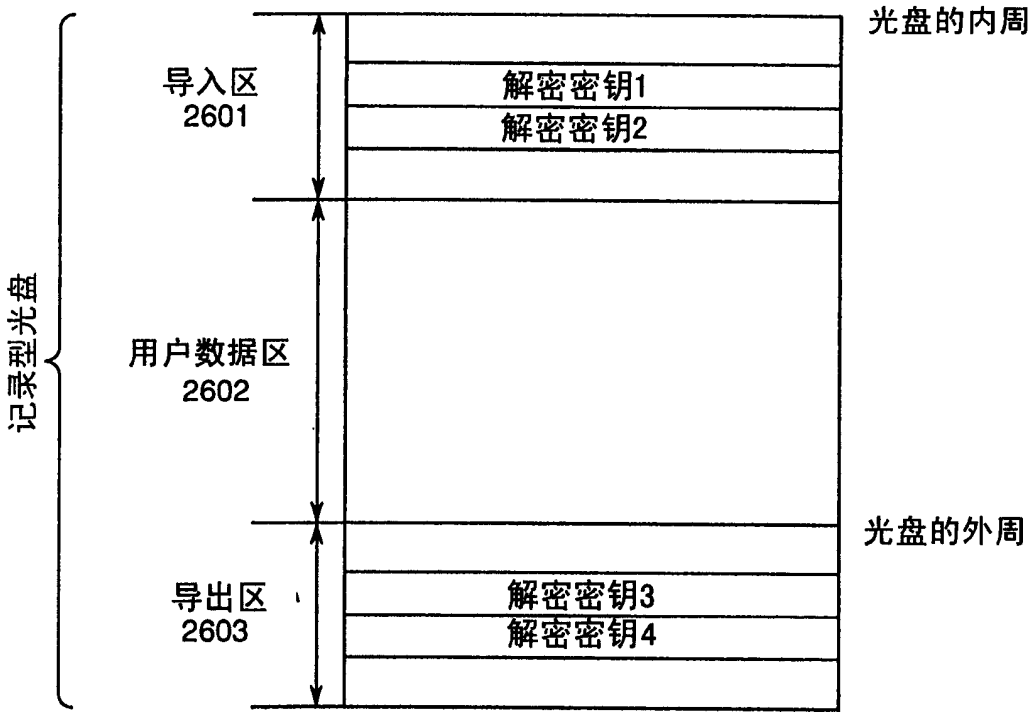

光盘的内周
导入区
2601
解密密钥1
解密密钥2
记录型光盘
用户数据区
2602
光盘的外周
导出区
2603
解密密钥3
解密密钥4

图 31

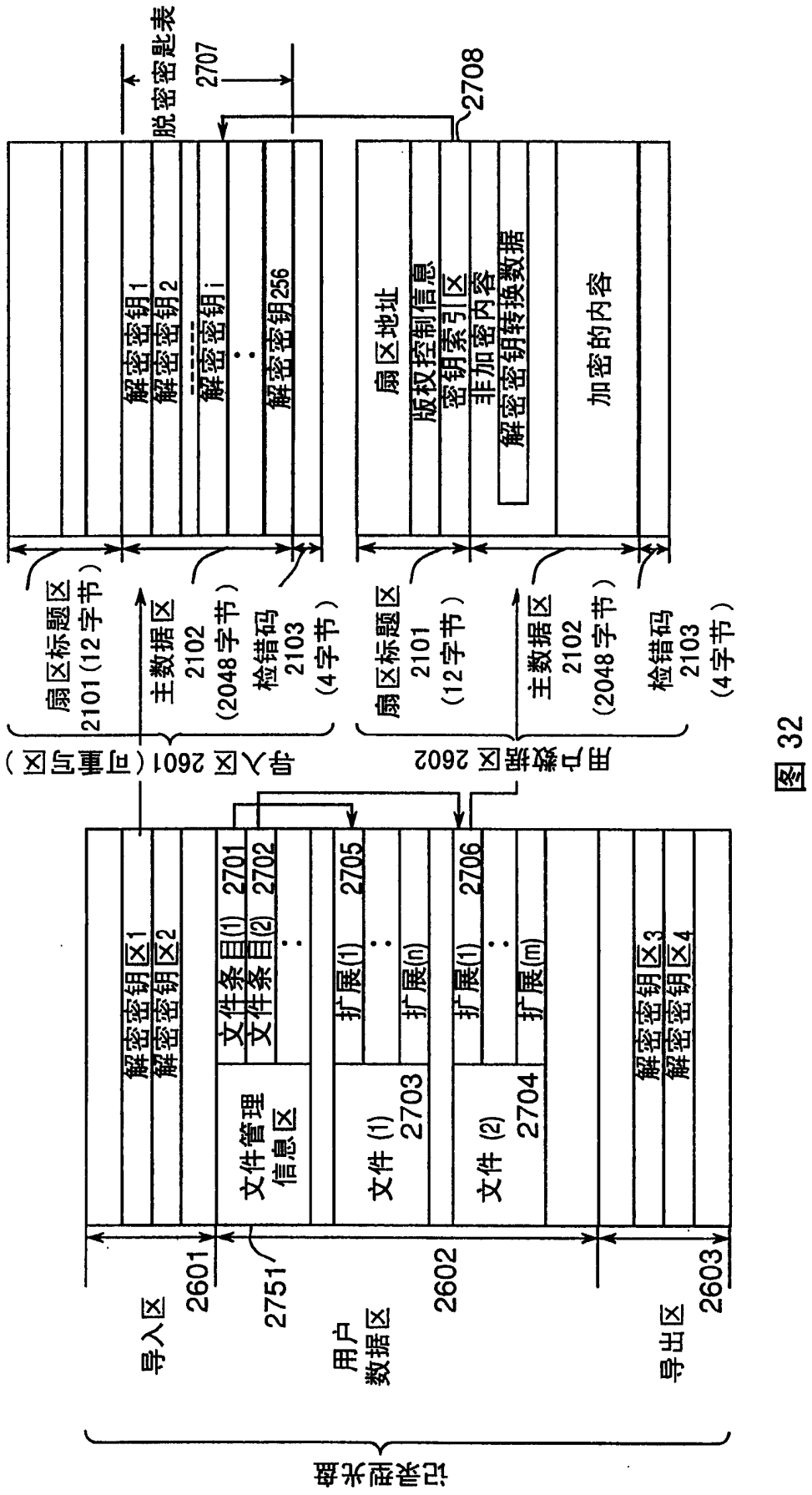

记录型光盘
导入区
2601
用户数据区
2751
2602
导出区
2603
解密密钥区1
解密密钥区2
文件管理信息区
文件条目(1) 2701
文件条目(2) 2702
扩展(1) 2705
扩展(n)
文件 (1) 2703
扩展(1) 2706
扩展(m)
文件 (2) 2704
解密密钥区3
解密密钥区4
导入区 2601（可重写区）
用户数据区 2602
扇区标题区 2101 (12字节)
主数据区 2102 (2048字节)
检错码 2103 (4字节)
脱密密匙表
2707
2708
解密密钥1
解密密钥2
解密密钥i
解密密钥256
扇区地址
版权控制信息
密钥索引区
非加密内容
解密密钥转换数据
加密的内容
扇区标题区 2101 (12字节)
主数据区 2102 (2048字节)
检错码 2103 (4字节)

图 32

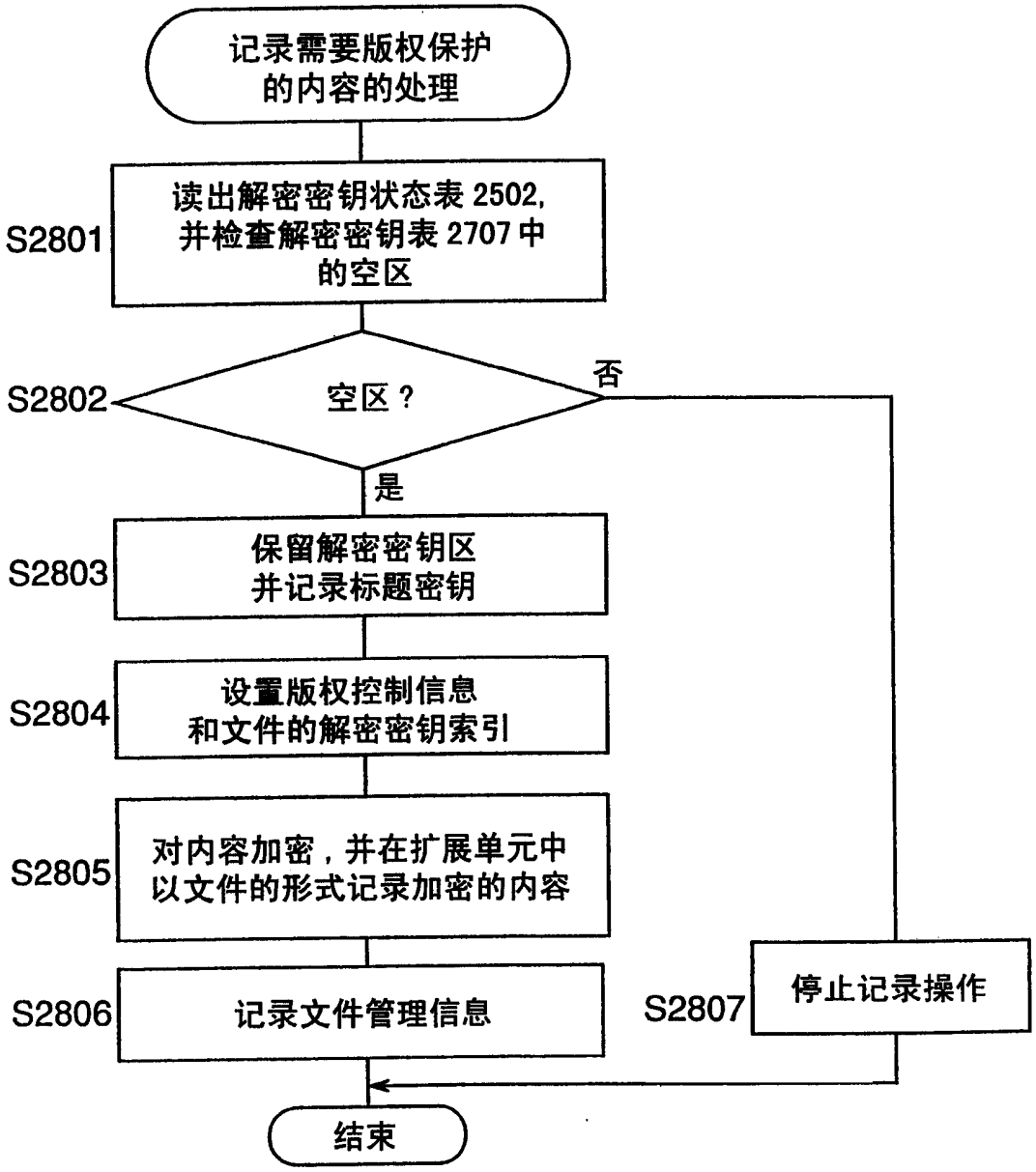

记录需要版权保护
的内容的处理
S2801
读出解密密钥状态表 2502,
并检查解密密钥表 2707 中
的空区
S2802
空区？
否
是
S2803
保留解密密钥区
并记录标题密钥
S2804
设置版权控制信息
和文件的解密密钥索引
S2805
对内容加密，并在扩展单元中
以文件的形式记录加密的内容
S2806
记录文件管理信息
S2807
停止记录操作
结束

图 33

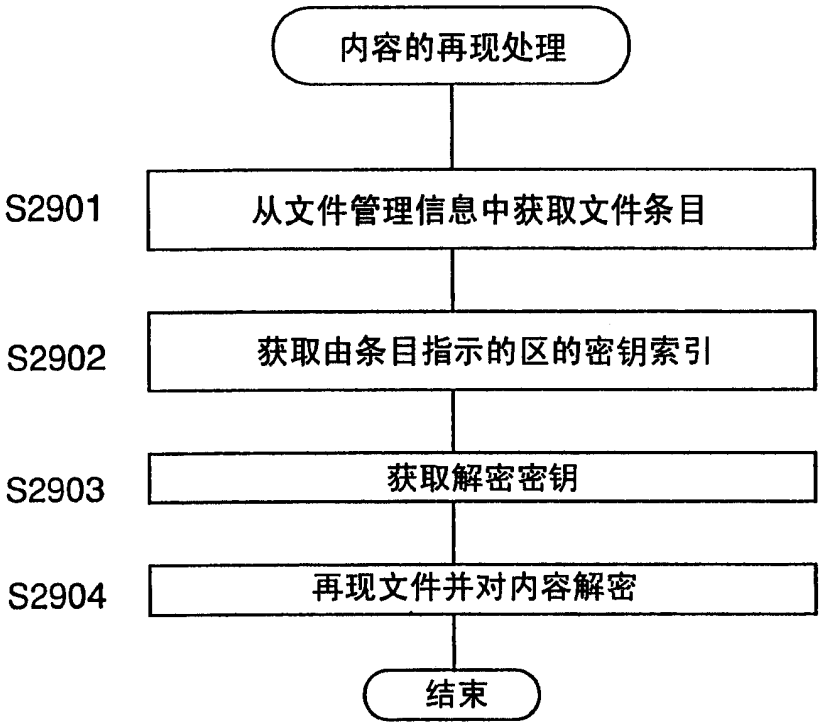

内容的再现处理
S2901
从文件管理信息中获取文件条目
S2902
获取由条目指示的区的密钥索引
S2903
获取解密密钥
S2904
再现文件并对内容解密
结束

图 34

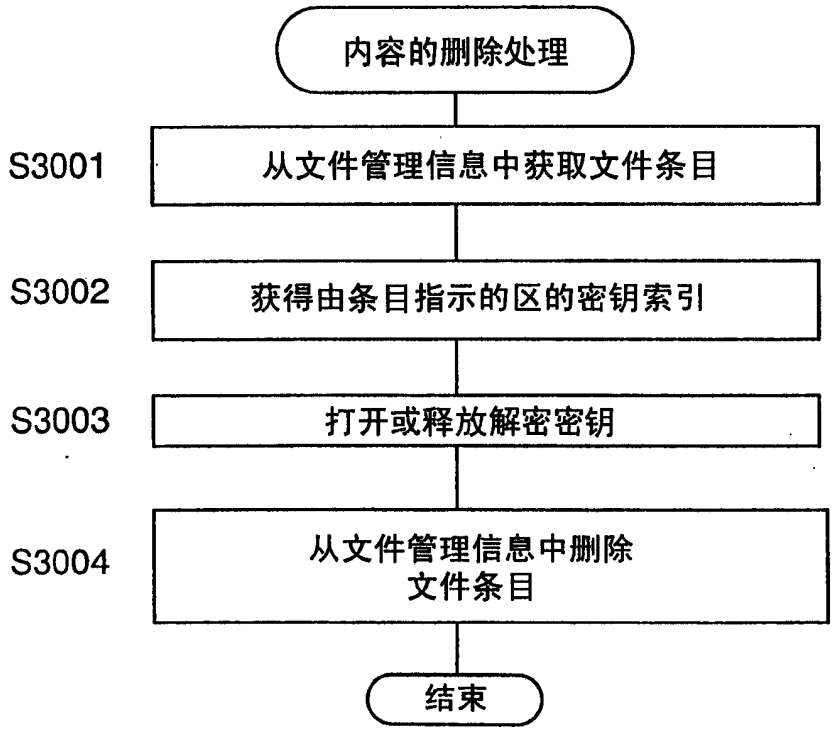

内容的删除处理
S3001
从文件管理信息中获取文件条目
S3002
获得由条目指示的区的密钥索引
S3003
打开或释放解密密钥
S3004
从文件管理信息中删除
文件条目
结束

图 35

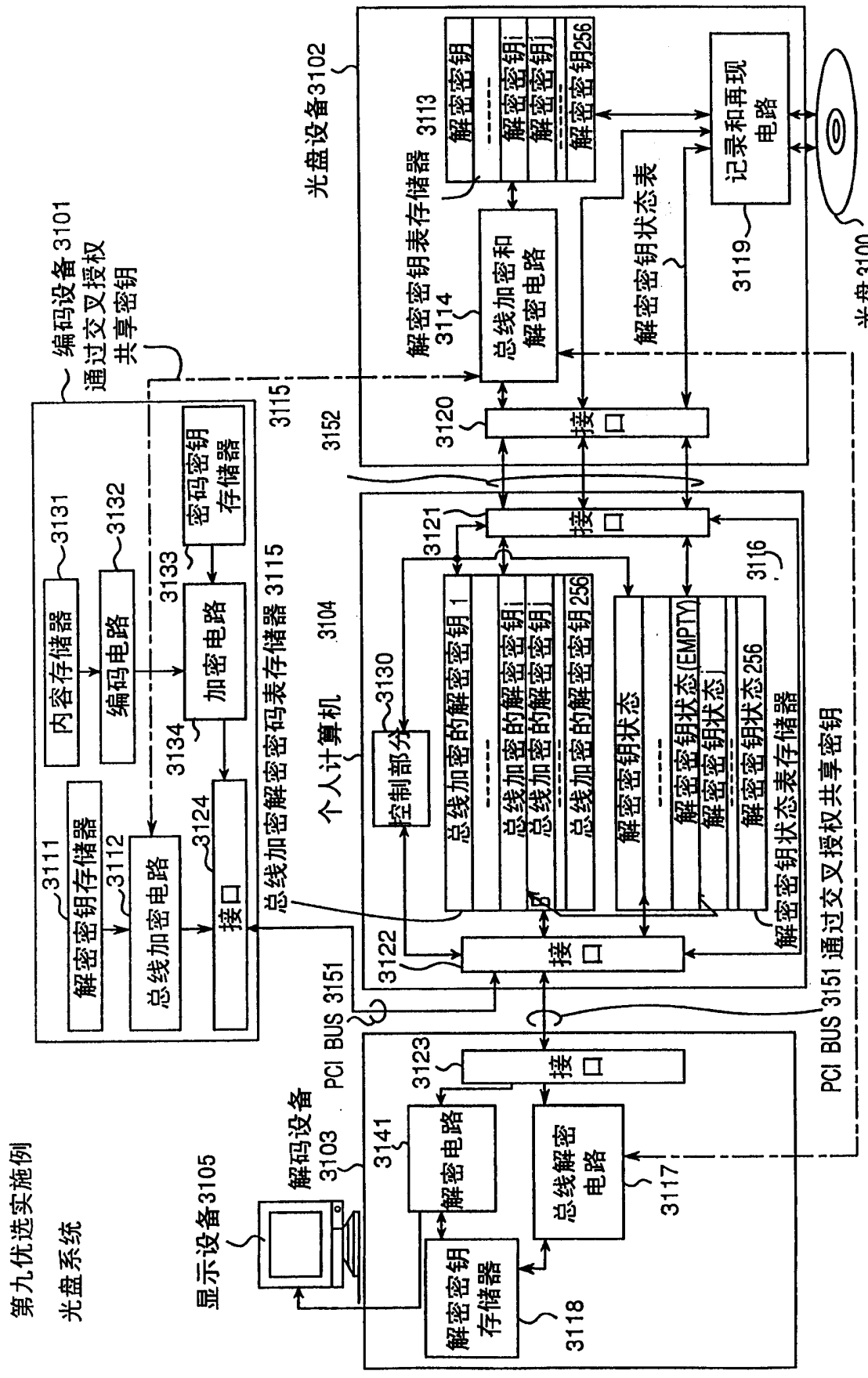

第九优选实施例
光盘系统
编码设备3101
通过交叉授权
共享密钥
光盘设备3102
光盘3100
内容存储器
3131
编码电路
3132
密码密钥
存储器
3133
加密电路
3134
解密密钥存储器
3111
总线加密电路
3112
接口
3124
总线加密解密密码表存储器3115
3115
3152
3120
接口
解密密钥表存储器
3113
解密密钥
解密密钥i
解密密钥j
解密密钥256
总线加密和
解密电路
3114
解密密钥状态表
记录和再现
电路
3119
个人计算机
3104
控制部分
3130
3121
接口
总线加密的解密密钥 1
总线加密的解密密钥i
总线加密的解密密钥j
总线加密的解密密钥256
解密密钥状态
解密密钥状态(EMPTY)
解密密钥状态i
解密密钥状态256
3116
解密密钥状态表存储器
3122
接口
PCI BUS 3151
PCI BUS 3151 通过交叉授权共享密钥
3123
接口
解码设备
3103
3141
解密电路
总线解密
电路
3117
显示设备3105
解密密钥
存储器
3118

图 36

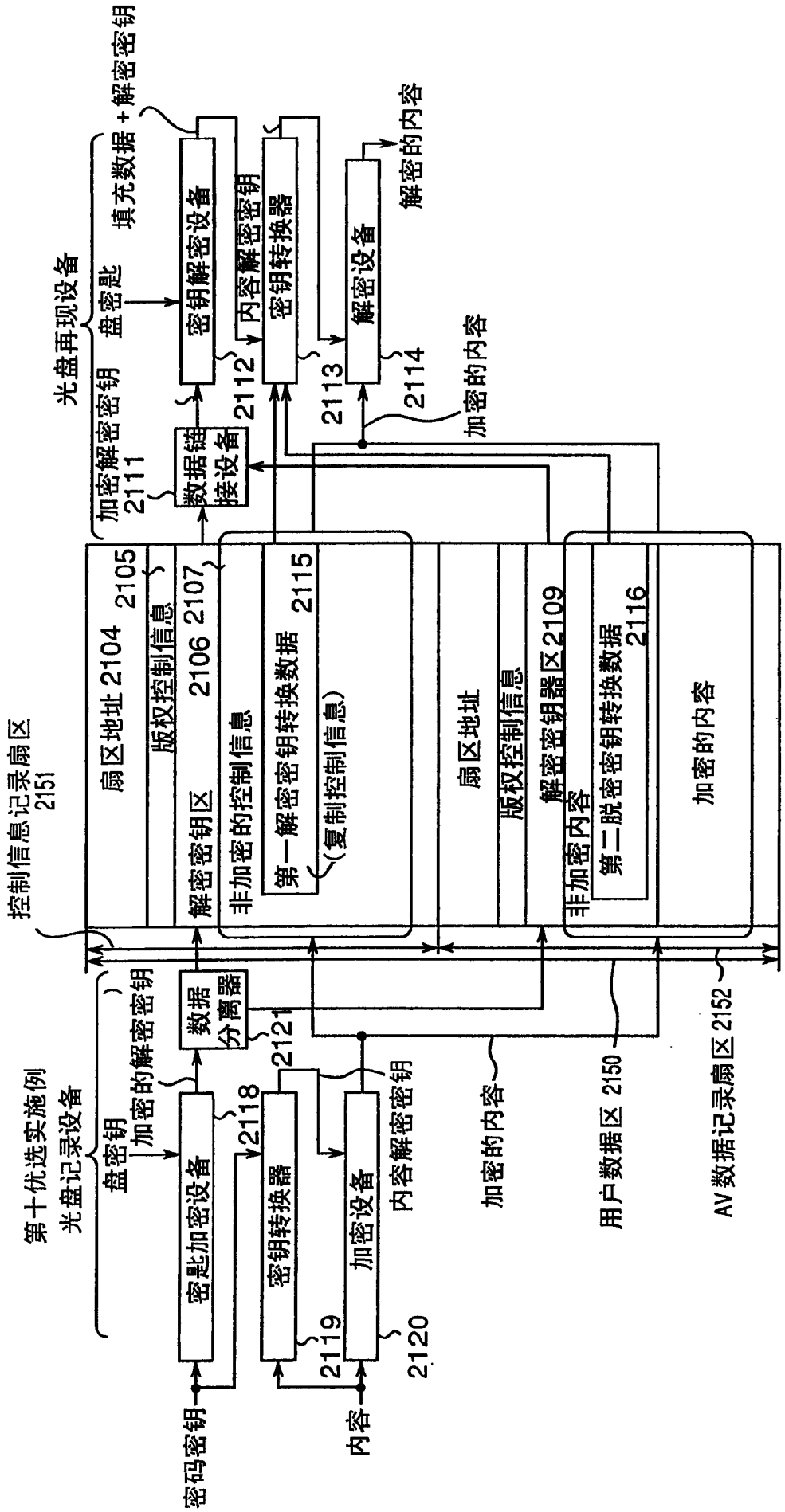

第十优选实施例
光盘记录设备
密码密钥
盘密钥
密钥加密设备
2118
加密的解密密钥
数据分离器
2121
内容
密钥转换器
2119
加密设备
2120
内容解密密钥
控制信息记录扇区 2151
扇区地址 2104
2105
版权控制信息
2106
解密密钥区
2107
非加密的控制信息
第一解密密钥转换数据
2115
(复制控制信息)
扇区地址
版权控制信息
解密密钥器区2109
非加密内容
第二脱密密钥转换数据
2116
加密的内容
加密的内容
用户数据区 2150
AV数据记录扇区 2152
光盘再现设备
盘密匙
填充数据 + 解密密钥
加密解密密钥
2111
数据链接设备
密钥解密设备
2112
内容解密密钥
密钥转换器
2113
解密设备
2114
解密的内容
加密的内容

图 37

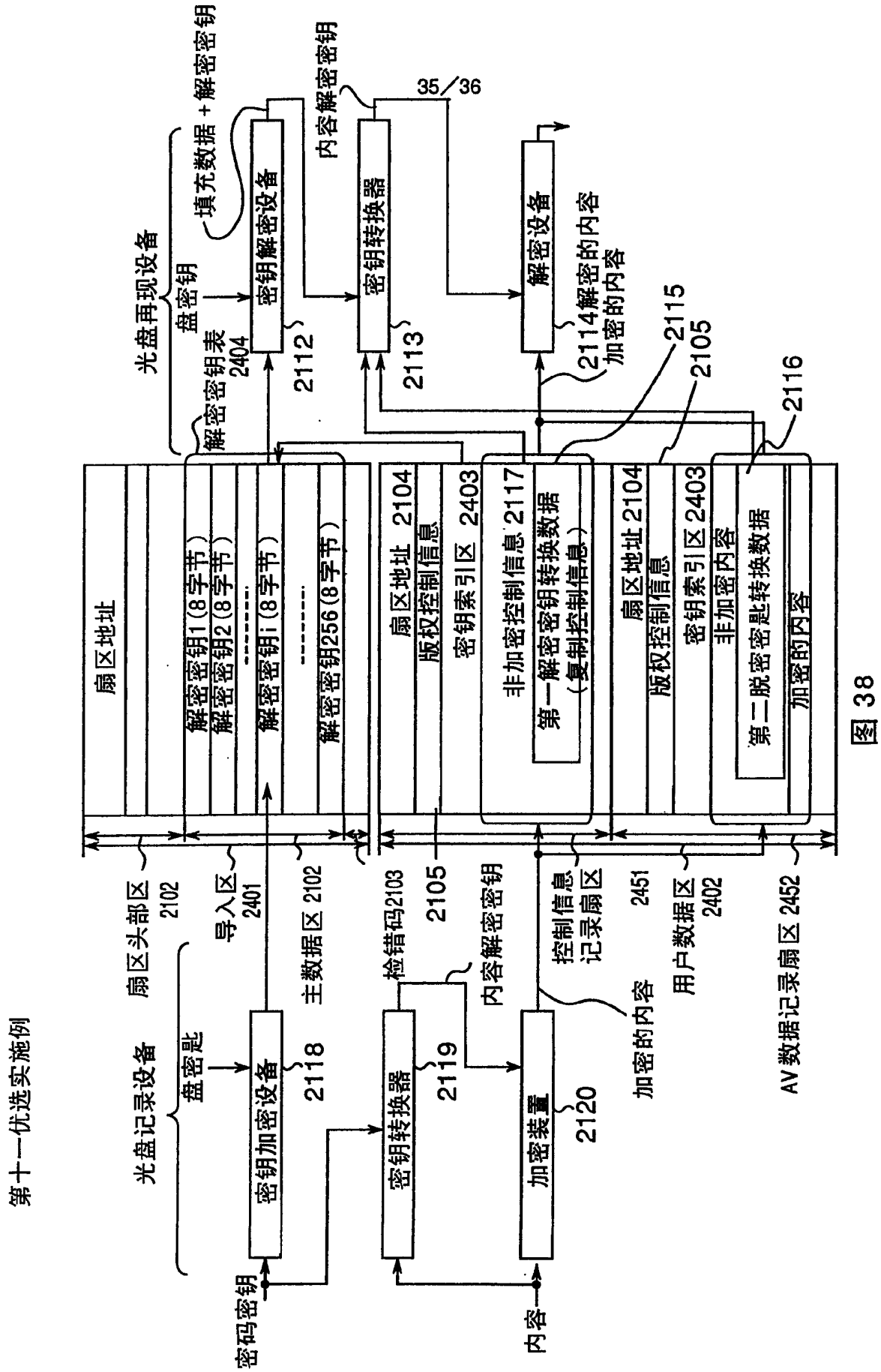

第十一优选实施例
光盘记录设备
盘密匙
密钥加密设备
2118
密码密钥
扇区头部区 2102
导入区 2401
主数据区 2102
检错码2103
2105
密钥转换器
2119
内容解密密钥
加密装置
2120
内容
控制信息记录扇区 2451
加密的内容
用户数据区 2402
AV数据记录扇区 2452
光盘再现设备
盘密钥
解密密钥表 2404
填充数据 + 解密密钥
密钥解密设备
2112
内容解密密钥
密钥转换器
2113
35/36
解密设备
2114解密的内容
加密的内容
2115
2105
2116
扇区地址
解密密钥1(8字节)
解密密钥2(8字节)
解密密钥i(8字节)
解密密钥256(8字节)
扇区地址 2104
版权控制信息
密钥索引区 2403
非加密控制信息 2117
第一解密密钥转换数据
(复制控制信息)
扇区地址 2104
版权控制信息
密钥索引区 2403
非加密内容
第二脱密密匙转换数据
加密的内容

图 38

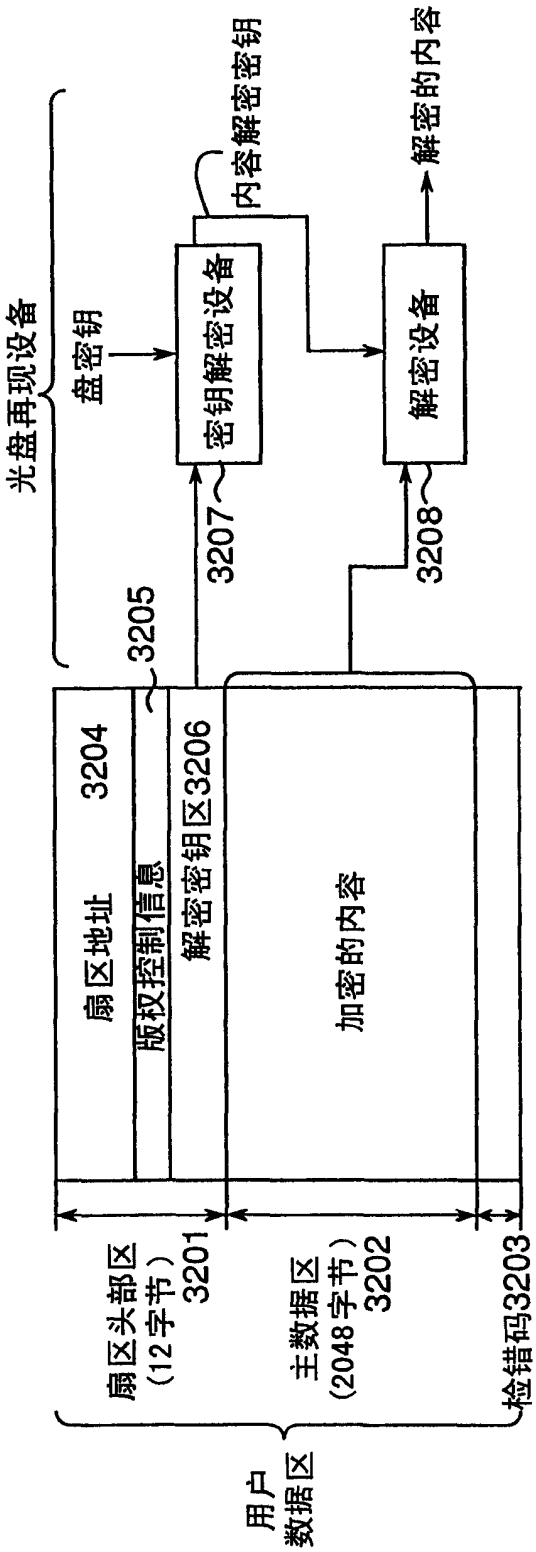

光盘再现设备
盘密钥
密钥解密设备
内容解密密钥
解密设备
解密的内容
3207
3208
3205
扇区地址
3204
版权控制信息
解密密钥区3206
加密的内容
扇区头部区
(12字节)
3201
主数据区
(2048字节)
3202
检错码3203
用户
数据区

图 39