[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/08 (2006.01)

[12] 发明专利申请公开说明书

[21] 申请号 200480006660.5

[43] 公开日 2006 年 4 月 12 日

[11] 公开号 CN 1759559A

[22] 申请日 2004.3.11
[21] 申请号 200480006660.5
[30] 优先权
[32] 2003. 3.11 [33] JP [31] 065591/2003
[32] 2003. 6. 4 [33] JP [31] 158927/2003
[86] 国际申请 PCT/JP2004/003161 2004.3.11
[87] 国际公布 WO2004/082203 日 2004.9.23
[85] 进入国家阶段日期 2005.9.12
[71] 申请人 松下电器产业株式会社
地址 日本大阪府
[72] 发明人 山道将人(死亡) 中野稔久
布田裕一 大森基司 馆林诚
原田俊治 村濑薰
[74] 专利代理机构 永新专利商标代理有限公司
代理人 王 英

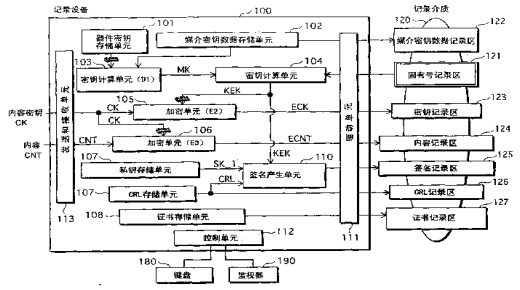
权利要求书 21 页 说明书 84 页 附图 20 页

[54] 发明名称

数字作品的保护系统、记录设备、再现设备及记录介质

[57] 摘要

本发明提供能够阻止非法使用内容的记录设备和再现设备。 记录介质在其中的不可重写区中存储介质固有号。 记录设备将媒介密钥数据和加密内容写到记录介质上。 媒介密钥数据包括通过(i)分别对每一个未失效的再现设备，利用未失效的再现设备的器件密钥来对媒介密钥加密，和(ii)分别对每一个失效的再现设备，利用失效的再现设备的器件密钥来对预定的探测信息加密而产生的加密媒介密钥。 再现设备利用器件密钥对加密媒介密钥解密以产生解密媒介密钥，判断解密媒介密钥是否为探测信息，且在判断为肯定时阻止记录在记录介质上的加密内容被解密。



1、一种数字作品保护系统，该系统包括一记录设备和多个再现设备，该记录设备可被操作以对内容进行加密并将加密内容写到记录介质上，而该多个再现设备各自可被操作以试图对记录在该记录介质上的加密内容进行解密，其中

所述多个再现设备中的一个或多个失效，

该记录介质具有：(i)预存储该记录介质固有的介质固有号的只读不可重写区；和(ii)可以向其写入并从其中读取数据的可重写区，并且

该记录设备包括：

存储单元，在其中存储包含多个加密媒介密钥的媒介密钥数据块，该多个加密媒介密钥是通过(i)对每一个未失效的再现设备，分别利用该未失效的再现设备的器件密钥来对媒介密钥进行加密，和(ii)对每一个失效的再现设备，分别利用该失效的再现设备的器件密钥来对预定的探测信息进行加密而产生的；

读取单元，可被操作以从所述记录介质的不可重写区中读取所述介质固有号；

产生单元，可被操作以根据所读取的介质固有号和所述媒介密钥来产生加密密钥；

加密单元，可被操作以根据所产生的加密密钥对作为数字数据块的所述内容进行加密，以产生所述加密内容；

读取单元，可被操作以从所述存储单元中读取所述媒介密钥数据块；以及

写入单元，可被操作以将所读取的媒介密钥数据块和所产生的加

密内容写入所述记录介质的可重写区，且

每一再现设备包括：

读取单元，可被操作以从记录在所述记录介质的可重写区中的所述媒介密钥数据块中读取与该再现设备相对应的加密媒介密钥；

解密单元，可被操作以利用所述再现设备的器件密钥来对所读取的加密媒介密钥进行解密，以产生解密媒介密钥；

控制单元，可被操作以判断所产生的解密媒介密钥是否为该探测信息，当判断为肯定时阻止对所述加密内容进行解密，且当判断为否定时允许对所述加密内容进行解密；以及

解密单元，在允许对所述加密内容进行解密时，可被操作以从所述记录介质中读取该加密内容，并根据所产生的解密媒介密钥来对所读取的加密内容进行解密，以产生被解密的内容。

2、一种记录设备，该记录设备可操作对内容进行加密并将加密内容写到第一记录介质上，并用于包括该记录设备和多个再现设备的数字作品保护系统中，每一再现设备可被操作以试图对记录在该第一记录介质上的所述加密内容进行解密，其中

所述多个再现设备中的一个或多个失效，

第一记录介质具有：(i)预存储第一记录介质固有的介质固有号的只读不可重写区；和（ii）可以向其写入并从其中读取数据的可重写区，并且

该记录设备包括：

存储单元，在其中存储包含多个加密媒介密钥的媒介密钥数据块，该多个加密媒介密钥是通过（i）对每一个未失效的再现设备，分别利用该未失效的再现设备的器件密钥来对媒介密钥进行加密，和

（ii）对每一个失效的再现设备，分别利用该失效的再现设备的器件密钥来对预定的探测信息进行加密而产生的；

第一读取单元，可被操作以从该不可重写区中读取所述介质固有号；

产生单元，可被操作以根据所读取的介质固有号和所述媒介密钥来产生加密密钥；

加密单元，可被操作以根据所产生的加密密钥对作为数字数据块的所述内容进行加密，以产生所述加密内容；

第二读取单元，可被操作以从所述存储单元中读取所述第一媒介密钥数据块；以及

写入单元，可被操作以将所读取的第一媒介密钥数据块和所产生的加密内容写入所述可重写区中。

3、根据权利要求 2 的记录设备，其中

第二记录介质在其中存储包含另一组加密媒介密钥的第二媒介密钥数据块，该另一组加密媒介密钥是通过（i）对每一个未失效的再现设备，分别利用该未失效的再现设备的器件密钥来对该媒介密钥进行加密，和（ii）对每一个失效的再现设备，分别利用该失效的再现设备的器件密钥来对预定的探测信息进行加密而产生的，且

该记录设备还包括：

比较单元，可被操作以将记录在所述第二记录介质上的所述第二媒介密钥数据块与存储在该存储单元中的所述第一媒介密钥数据块进行比较，以判断哪一个较新；和

更新单元，当判断所述第二媒介密钥数据块较新时，可被操作以从所述第二记录介质中读取所述第二媒介密钥数据块，并使用所述第

二媒介密钥数据块来覆盖存储在该存储单元中的所述第一媒介密钥数据块，以及

所述第二读取单元，从该存储单元中读取所述第二媒介密钥数据块而不是所述第一媒介密钥数据块；和

所述写入单元将所述第二媒介密钥数据块而不是所述第一媒介密钥数据块写入所述可重写区。

4、根据权利要求 3 的记录设备，其中

存储在该存储单元中的所述第一媒介密钥数据块包括表示所述第一媒介密钥数据块的产生的第一版本信息块，

记录在所述第二记录介质上的所述第二媒介密钥数据块包括表示所述第二媒介密钥数据块的产生的第二版本信息块，和

比较单元，通过比较所述第一版本信息块与所述第二版本信息块，从而判断所述第一媒介密钥数据块和所述第二媒介密钥数据块中哪一个更新。

5、根据权利要求 3 的记录设备，其中

存储在所述存储单元中的所述第一媒介密钥数据块包括表示所述第一媒介密钥数据块产生的日期和时间的第一日期和时间信息块，

记录在所述第二记录介质上的所述第二媒介密钥数据块包括表示所述第二媒介密钥数据块产生的日期和时间的第二日期和时间信息块，并且

所述比较单元通过比较所述第一日期和时间信息块与所述第二日期和时间信息块，从而判断所述第一媒介密钥数据块和所述第二媒介密钥数据块中哪一个更新。

6、根据权利要求 2 的记录设备，其中

所述存储单元还在其中存储失效数据块，该失效数据块表示分配给该记录设备和多个再现设备的一个或多个公钥失效，

所述记录设备还包括签名产生单元，该签名产生单元可被操作以对所述失效数据块应用数字签名功能，以产生验证信息块；且

该写入单元还将所产生的验证信息块写入所述第一记录介质的所述可重写区中。

7、根据权利要求 6 的记录设备，其中

该签名产生单元对所述失效数据块应用具有附录的数字签名，以产生签名数据块，从而根据所产生的签名数据块和所述失效数据块来产生所述验证信息块，和

该写入单元将该验证信息块写入。

8、根据权利要求 6 的记录设备，其中

该签名产生单元对所述失效数据块应用具有消息恢复的数字签名，以产生所述验证信息块。

9、根据权利要求 6 的记录设备，其中

所述存储单元还在其中存储所述记录设备的私钥和公钥证书，

所述签名产生单元利用所存储的私钥来应用所述数字签名功能，

所述第二读取单元还从所述存储单元中读取该公钥证书，以及

所述写入单元将所读取的公钥证书写入到所述第一记录介质的可重写区中。

10、根据权利要求 2 的记录设备，其中

所述存储单元还在其中存储所述记录设备的公钥证书，

所述第二读取单元从所述存储单元中读取该公钥证书，以及

所述写入单元将所读取的公钥证书写入所述第一记录介质的可重写区中。

11、根据权利要求 2 的记录设备，其中

所述存储单元还在其中存储失效数据块，该失效数据块表示分配给所述记录设备和所述多个再现设备的一个或多个公钥失效，

所述记录设备还包括签名产生单元，该签名产生单元可被操作以对所述失效数据块应用数字签名功能，以产生验证信息块；而且所述写入单元还将所产生的验证信息块写到所述第二记录介质上。

12、根据权利要求 2 的记录设备，其中

所述存储单元还在其中存储失效数据块，该失效数据块表示分配给所述记录设备和所述多个再现设备的一个或多个公钥失效，

所述第二读取单元还从所述存储单元中读取该失效数据块，以及

所述写入单元将所读取的失效数据块写到所述第二记录介质上。

13、根据权利要求 2 的记录设备，其中

所述存储单元还在其中存储所述记录设备的公钥证书，

所述第二读取单元还从所述存储单元中读取该公钥证书，而且

所述写入单元将所读取的公钥证书写到所述第二记录介质上。

14、根据权利要求 2 的记录设备，其中

所述存储单元还在其中存储识别所述记录设备的设备识别符，

所述记录设备还包括：嵌入单元，可被操作以读取该设备识别符，并将所读取的设备识别符作为电子水印嵌入到所述内容中；并且

所述加密单元对其中嵌入有该设备识别符的所述内容进行加密。

15、根据权利要求 2 的记录设备，其中

存储于所述存储单元中的第一媒介密钥数据块还包括识别所述第一媒介密钥数据块的第一数据识别符，

所述写入单元（i）将第一数据识别符和该加密内容以如此方式写入所述第一记录介质的可重写区中，使得所述第一数据识别符和所述加密内容彼此相应，并且（ii）将包含所述第一数据识别符的所述第一媒介密钥数据块写入所述可重写区。

16、根据权利要求 15 的记录设备，其中

所述第一记录介质还在其中存储包括另一组加密媒介密钥的第二媒介密钥数据块，该另一组加密媒介密钥是通过（i）对每一个未失效的再现设备，分别利用该未失效的再现设备的器件密钥来对媒介密钥进行加密，和（ii）对每一个失效的再现设备，分别利用该失效的再现设备的器件密钥来对预定的探测信息进行加密而产生的，

所述第二媒介密钥数据块包括识别该第二媒介密钥数据块的第二数据识别符；且

所述记录设备还包括分配单元，该分配单元可被操作以向存储在所述存储单元中的第一媒介密钥数据块分配与所述第二数据识别符不同的所述第一数据识别符。

17、根据权利要求 15 的记录设备，还包括：

比较单元，可被操作以将存储在所述存储单元中的所述第一媒介密钥数据块与记录在所述第二记录介质上的所述第二媒介密钥数据块进行比较，以判断哪一个更新；和

分配单元，在判断所述第一媒介密钥数据块更新时，可被操作以向所述第一媒介密钥数据块分配所述第一数据识别符。

18、根据权利要求 17 的记录设备，其中

存储在所述存储单元中的所述第一媒介密钥数据块包括表示该第一媒介密钥数据块产生的日期和时间的第一日期和时间信息块，

存储在所述第一记录介质中的所述第二媒介密钥数据块包括表示该第二媒介密钥数据块产生的日期和时间的第二日期和时间信息块，和

所述比较单元通过比较所述第一日期和时间信息块与所述第二日期和时间信息块，从而判断所述第一媒介密钥数据块和所述第二媒介密钥数据块中哪一个更新。

19、一种再现设备，包含在至少由多个再现设备和一个记录设备构成的数字作品保护系统中，该记录设备可被操作以对内容进行加密并将加密内容写到第一记录介质上，该多个再现设备的每一个可被操作以试图对记录在所述第一记录介质上的加密内容进行解密，其中

该多个再现设备中的一个或多个失效，

所述第一记录介质具有：(i)预存储所述第一记录介质固有的介质固有号的只读不可重写区；和（ii）可以向其写入并从其中读取数据的可重写区，

所述记录设备在其中存储包含多个加密媒介密钥的媒介密钥数

据块，该多个加密媒介密钥是通过（i）对每一个未失效的再现设备，分别利用该未失效的再现设备的器件密钥来对媒介密钥进行加密，和（ii）对每一个失效的再现设备，分别利用该失效的再现设备的器件密钥来对预定的探测信息进行加密而产生的；

所述记录设备（i）从所述第一记录介质的不可重写区中读取所述介质固有号，(ii)根据所读取的介质固有号和所述媒介密钥来产生加密密钥，（iii）根据所产生的加密密钥对作为数字数据块的所述内容进行加密以产生加密内容，（iv）从所述存储单元中读取所述媒介密钥数据块，并（v）将所读取的媒介密钥数据块和所产生的加密内容写入所述第一记录介质的可重写区中，并且

该再现设备包括：

读取单元，可被操作以从记录在所述可重写区中的所述媒介密钥数据块中读取与该再现设备相对应的一个加密媒介密钥；

第一解密单元，可被操作以利用所述再现设备的器件密钥来对所读取的加密媒介密钥进行解密，以产生解密密钥；

控制单元，可被操作以判断所产生的解密媒介密钥是否为所述检测信息，以当判断为肯定时阻止对该加密内容进行解密，且当判断为否定时允许对该加密内容进行解密；以及

第二解密单元，在允许对该加密内容进行解密时，可被操作以从所述第一记录介质中读取该加密内容，并根据所产生的解密媒介密钥来对所读取的加密内容进行解密，以产生被解密的内容。

20、根据权利要求 19 的再现设备，其中

所述记录设备还在其中存储失效数据块，该失效数据块表示分配给该记录设备和多个再现设备的一个或多个公钥失效，对该失效数据

块应用数字签名功能以产生验证信息块，并将所产生的验证信息块写入所述第一记录介质的可重写区，

所述读取单元还读取记录在所述可重写区中的验证信息块，

所述再现设备还包括验证单元，该验证单元可被操作以根据所读取的验证信息块来执行签名验证，并输出表示验证成功或验证失败的验证结果，并且

在该验证结果表示验证失败时，该控制单元还阻止对所述加密内容进行解密，而在该验证结果表示验证成功时允许对所述加密内容进行解密。

21、根据权利要求 20 的再现设备，其中

所述记录设备（i）对该失效数据块应用具有附录的数字签名以产生签名数据块，（ii)根据所产生的签名数据块和所述失效数据块来产生验证信息块，（iii）写入所产生的验证信息块，并且

所述验证单元根据包含在所述验证信息块中的签名数据块来执行所述签名验证。

22、根据权利要求 20 的再现设备，其中

所述记录设备对所述失效数据块应用具有消息恢复的数字签名以产生验证信息块，并且

在所述验证结果表示验证成功时，所述验证单元根据该验证信息块产生所述失效数据块。

23、根据权利要求 20 的再现设备，其中

所述记录设备还在其中存储所述记录设备的私钥和公钥证书，

所述记录设备（i）利用所存储的私钥应用数字签名功能，（ii）读取所述公钥证书，并且（iii）将所读取的公钥证书写入所述第一记录介质的可重写区中，并且

所述验证单元从所述第一记录介质中读取所述公钥证书，从所读取的公钥证书中提取公钥，并利用所提取的公钥执行所述签名验证。

24、根据权利要求 20 的再现设备，其中

所述记录设备在其中存储失效数据块，对该失效数据块应用数字签名功能以进一步产生另一验证信息块，并将所产生的验证信息块写入所述第二记录介质，

所述读取单元从所述第二记录介质中而不是从所述第一记录介质中读取另一验证信息块，和

所述验证单元，根据从所述第二记录介质中读取的所述另一验证信息块来执行所述签名验证。

25、根据权利要求 19 的再现设备，其中

所述记录设备还在其中存储该记录设备的公钥证书，读取该公钥证书，并将所读取的公钥证书写入所述第一记录介质的可重写区中，

该再现设备还包括：

存储单元，在其中存储第一失效数据块，该第一失效数据块表示分配给该记录设备和多个再现设备的一个或多个公钥失效；

证书读取单元，可被操作以从所述第一记录介质中读取所述公钥证书；以及

公钥验证单元，可被操作以根据所述第一验证数据块来检验包含在所读取的公钥证书中的公钥是否失效，且

在所述公钥失效时，所述控制单元进一步阻止对该加密内容进行解密，而在所述公钥没有失效时，允许对该加密内容进行解密。

26、根据权利要求 25 的再现设备，其中

第二记录介质在其中存储第二失效数据块，该第二失效数据块表示分配给该记录设备和多个再现设备的一个或多个公钥失效，

该再现设备还包括：

比较单元，可被操作以将记录在所述第二记录介质上的第二失效数据块与存储于所述存储单元中的第一失效数据块比较，以判断哪一个较新，和

更新单元，当判断所述第二失效数据块较新时，可被操作以从所述第二记录介质中读取所述第二失效数据块，并使用所读取的第二失效数据块来覆盖所述存储单元中的第一失效数据块。

27、根据权利要求 26 的再现设备，其中

所述比较单元通过比较所述第一和第二失效数据块的长度来判断所述第一失效数据块和第二失效数据块中哪一个更新。

28、根据权利要求 26 的再现设备，其中

所述比较单元通过比较由所述第一和第二失效数据块所表示的失效的公钥的数量来判断所述第一失效数据块和第二失效数据块中哪一个更新。

29、根据权利要求 26 的再现设备，其中

存储在所述存储单元中的第一失效数据块包括表示第一失效数据块的产生的第一版本信息块，

记录在所述第二记录介质上的第二失效数据块包括表示第二失效数据块产生的第二版本信息块，并且

所述比较单元通过比较所述第一与第二版本信息块来判断所述第一失效数据块和第二失效数据块中哪一个更新。

30、根据权利要求 26 的再现设备，其中

存储在所述存储单元中的第一失效数据块包括表示第一失效数据块产生的日期和时间的第一日期和时间信息块，

记录在所述第二记录介质上的第二失效数据块包括表示第二失效数据块产生的日期和时间的第二日期和时间信息块，并且

所述比较单元通过比较所述第一与第二日期和时间信息块来判断所述第一失效数据块和第二失效数据块中哪一个更新。

31、根据权利要求 25 的再现设备，其中

所述记录设备还在其中存储第二失效数据块，该第二失效数据块表示分配给该记录设备和多个再现设备的一个或多个公钥失效，

所述记录设备读取所述第二失效数据块，并将所读取的第二失效数据块写入所述第二记录介质，并且

所述公钥验证单元从所述第二记录介质中读取所述第二失效数据块而不是所述第一失效数据块，并根据所述第二失效数据块来验证该公钥是否失效。

32、根据权利要求 25 的再现设备，其中

所述记录设备还在其中存储所述记录设备的公钥证书，

所述记录设备读取公钥证书并将所读取的公钥证书写到所述第

二记录介质上，以及

所述证书读取单元从所述第二记录介质而不是从所述第一记录介质上读取该公钥证书。

33、根据权利要求 19 的再现设备，还包括：

存储单元，在其中存储识别所述再现设备的设备识别符，和

嵌入单元，在允许对所述加密内容进行解密时，可被操作以从所述存储单元中读取所述设备识别符，并将所读取的设备识别符作为电子水印嵌入到所述加密内容中；和

写入单元，可被操作以将其中嵌入有所述设备识别符的加密内容写到所述第一记录介质上。

34、根据权利要求 19 的再现设备，其中

存储在所述记录设备中的媒介密钥数据块还包括识别该媒介密钥数据块的数据识别符，

所述记录设备将该数据识别符和该加密内容以如此方式写入该可重写区，使得该数据识别符和该加密内容彼此相应，并将包含该数据识别符的媒介密钥数据块写入该可重写区，而且

该再现设备还包括：

接收单元，可被操作以接收记录在所述第一记录介质上的该加密内容的说明书；

第一读取单元，可被操作以从所述第一记录介质中读取与所接收的说明书中的加密内容相应的数据识别符；和

第二读取单元，可被操作以从所述第一记录介质中读取包含该数据识别符的该媒介密钥数据块，而且

该控制单元根据所读取的媒介密钥数据块来判断是阻止对所述加密内容进行解密还是允许对所述加密内容进行解密。

35、一种由记录设备使用的记录方法，该记录设备可被操作以对内容进行加密并将加密内容写到记录介质上，且其包含于至少由该记录设备和多个再现设备构成的数字制品保护系统中，而该多个再现设备的每一个可被操作以试图对记录在该记录介质上的加密内容进行解密，其中

该多个再现设备中的一个或多个失效，

该记录介质具有：(i)预存储该记录介质固有的介质固有号的只读不可重写区；和（ii）可以向其写入并从其中读取数据的可重写区，并且

该记录设备包括：

存储单元，在其中存储包含多个加密媒介密钥的媒介密钥数据块，该多个加密媒介密钥是通过（i）对每一个未失效的再现设备，分别利用该未失效的再现设备的器件密钥来对媒介密钥进行加密，和（ii）对每一个失效的再现设备，分别利用该失效的再现设备的器件密钥来对预定的探测信息进行加密而产生的；而且

该记录方法包括：

第一读取步骤，从所述记录介质的不可重写区中读取所述介质固有号；

产生步骤，根据所读取的介质固有号和该媒介密钥产生加密密钥；

加密步骤，根据所产生的加密密钥对作为数字数据块的所述内容进行加密，以产生加密内容；

第二读取步骤，从所述存储单元中读取所述媒介密钥数据；和

写入步骤，将所读取的媒介密钥数据块和所产生的加密内容写入所述记录介质的可重写区中。

36、一种由记录设备使用的用于记录目的的计算机程序，该记录设备可被操作以对内容加密并将加密内容写到记录介质上，且其包含于至少由该记录设备和多个再现设备构成的数字作品保护系统中，而该多个再现设备的每一个可被操作以试图对记录在所述记录介质上的加密内容进行解密，其中

该多个再现设备中的一个或多个失效，

该记录介质具有：(i)预存储该记录介质固有的介质固有号的只读不可重写区；和（ii）可以向其写入并从其中读取数据的可重写区，并且

该记录设备包括：

存储单元，在其中存储包含多个加密媒介密钥的媒介密钥数据块，该多个加密媒介密钥是通过（i）对每一个未失效的再现设备，分别利用该未失效的再现设备的器件密钥来对媒介密钥进行加密，和（ii）对每一个失效的再现设备，分别利用该失效的再现设备的器件密钥来对预定的探测信息进行加密而产生的；并且

该用于记录目的的计算机程序包括：

第一读取步骤，从该记录介质的不可重写区中读取该所述介质固有号；

产生步骤，根据所读取的介质固有号和该媒介密钥产生加密密钥；

加密步骤，根据所产生的加密密钥对作为数字数据块的所述内

容进行加密，以产生加密内容；

第二读取步骤，从该存储单元中读取该媒介密钥数据；和

写入步骤，将所读取的媒介密钥数据块和所产生的加密内容写入该记录介质的可重写区中。

37、根据权利要求36的用于记录目的的计算机程序，被记录在计算机可读记录介质中。

38、一种由包含于数字作品保护系统中的每一个再现设备使用的再现方法，该数字制品保护系统由至少该再现设备和记录设备构成，该记录设备可被操作以对内容进行加密并将加密内容写到记录介质上，该再现设备各自可被操作以试图对记录在该记录介质上的加密内容进行解密，其中

该多个再现设备中的一个或多个失效，

该记录介质具有：(i)预存储该记录介质固有的介质固有号的只读不可重写区；和(ii)可以向其写入并从其中读取数据的可重写区，和

该记录设备在其中存储包含多个加密媒介密钥的媒介密钥数据块，该多个加密媒介密钥是通过(i)对每一个未失效的再现设备，分别利用该未失效的再现设备的器件密钥来对媒介密钥进行加密，和(ii)对每一个失效的再现设备，分别利用该失效的再现设备的器件密钥来对预定的探测信息进行加密而产生的；

该记录设备(i)从该记录介质的不可重写区中读取该所述介质固有号，(ii)根据所读取的介质固有号和媒介密钥来产生加密密钥，(iii)根据所产生的加密密钥对作为数字数据块的所述内容进行加密

以产生加密内容，（v）从该存储单元中读取媒介密钥数据块，并且（vi）将所读取的媒介密钥数据块和所产生的加密内容写入该记录介质的可重写区中，并且

该再现方法包括：

读取步骤，从记录在该记录介质的可重写区中的媒介密钥数据块中读取与该再现设备相应的一个加密媒介密钥；

第一解密步骤，利用该再现设备的器件密钥对所读取的加密媒介密钥进行解密，以产生解密媒介密钥；

控制步骤，判断所产生的解密媒介密钥是否为所述探测信息，当判断为肯定时阻止对所述加密内容进行解密，而当判断为否定时允许对所述加密内容进行解密；和

第二解密步骤，当允许对所述加密内容进行解密时，从所述记录介质中读取所述加密内容，并根据所产生的解密媒介密钥对所读取的加密内容进行解密，以产生解密内容。

39、一种由包含于数字作品保护系统中的每一个再现设备使用的用于再现目的的计算机程序，该数字作品保护系统至少由该多个再现设备和记录设备构成，该记录设备可被操作以对内容进行加密并将加密内容写到记录介质上，该再现设备各自可被操作以试图对记录在记录介质上的加密内容进行解密，其中

该多个再现设备中的一个或多个失效，

该记录介质具有：（i）预存储该记录介质固有的介质固有号的只读不可重写区；和（ii）可以向其写入并从其中读取数据的可重写区，并且

该记录设备存储包含多个加密媒介密钥的媒介密钥数据块，该

多个加密媒介密钥是通过（i）对每一个未失效的再现设备，分别利用该未失效的再现设备的器件密钥来对媒介密钥进行加密，和（ii）对每一个失效的再现设备，分别利用该失效的再现设备的器件密钥来对预定的探测信息进行加密而产生的；

该记录设备（i）从该记录介质的不可重写区中读取该介质固有号，（ii）根据所读取的介质固有号和该媒介密钥来产生加密密钥，（iii）根据所产生的加密密钥对作为数字数据块的所述内容进行加密以产生加密内容，（v）从该存储单元中读取媒介密钥数据块，并且（vi）将所读取的媒介密钥数据块和所产生的加密内容写入该记录介质的可重写区中，并且

该用于再现目的的计算机程序包括：

读取步骤，从记录在该记录介质的可重写区中的媒介密钥数据块中读取与该再现设备相应的一个加密媒介密钥；

第一解密步骤，利用该再现设备的器件密钥对所读取的加密媒介密钥进行解密，以产生解密媒介密钥；

控制步骤，判断所产生的解密媒介密钥是否为所述探测信息，当判断为肯定时阻止对该加密内容进行解密，而当判断为否定时允许对该加密内容进行解密；和

第二解密步骤，当允许对该加密内容进行解密时，从该记录介质中读取该加密内容，并根据所产生的解密媒介密钥对所读取的加密内容进行解密，以产生解密内容。

40、根据权利要求 39 的用于再现目的的计算机程序，被记录在计算机可读记录介质中。

41、一种计算机可读记录介质，包括（i）只读不可重写区和可以向其写入并从其中读出数据的可重写区，其中

将该记录介质固有的介质固有号预存储在该不可重写区中，

将媒介密钥数据块和加密内容记录在可重写区中，

该媒介密钥数据块包括多个加密媒介密钥，该多个加密媒介密钥是通过（i）对每一个未失效的再现设备，分别利用该未失效的再现设备的器件密钥来对媒介密钥进行加密，和（ii）对每一个失效的再现设备，分别利用该失效的再现设备的器件密钥来对预定的探测信息进行加密而产生的；

通过根据加密密钥对作为数字数据块的内容进行加密来产生该加密内容，和

根据记录在该记录介质的不可重写区中的该介质固有号和该媒介密钥来产生该加密密钥。

42、一种计算机可读记录介质，包括（i）只读不可重写区和可以向其写入并从其中读出数据的可重写区，其中

将该记录介质固有的介质固有号预存储在不可重写区中，

将媒介密钥数据块和加密内容记录在可重写区中，

该媒介密钥数据块包括多个加密媒介密钥，该多个加密媒介密钥是通过（i）对每一个未失效的再现设备，分别利用该未失效的再现设备的器件密钥来对媒介密钥进行加密，和（ii）对每一个失效的再现设备，分别利用该失效的再现设备的器件密钥来对预定的探测信息进行加密而产生的，并且还包括识别该媒介密钥数据块的数据识别符；

通过根据加密密钥对作为数字数据块的内容进行加密来产生该

加密内容，且该加密内容包括该数据识别符，并且

根据记录在该记录介质的不可重写区中的该介质固有号和媒介密钥来产生该加密密钥。

数字作品的保护系统、记录设备、再现设备及记录介质

技术领域

本发明涉及在大容量记录介质上记录和再现数字数据的技术，特别涉及防止利用非法设备来非法记录和再现内容的技术。

背景技术

近些年来，由于已经发展了涉及多媒体的技术且已经可利用大容量的记录介质，所以开始流行这样一种系统，在该系统中产生了由视频、音频等构成的数字内容（下文中简称为“内容”），这些内容通过被存储在诸如光盘的大容量记录介质中或经由网络而被分配。

使用计算机、再现设备等来读取所分配的内容，以便于可以再现或复制它们。

一般而言，为了保护内容的版权，换句话说，为了防止非法使用诸如非法再现和非法复制的内容，而使用加密技术。更为具体地，记录设备在将内容记录到诸如光盘记录介质上，并且记录介质被分配之前，使用加密密钥对内容加密。仅各自具有相应于加密密钥的解密密钥的再现设备能够使用该解密密钥对从记录介质中读取的加密内容解密，并执行包括内容再现的操作。

应该注意的是，当内容被加密并被记录在记录介质上时，可以使用不同的方法，诸如（i）使用相应于存储于再现设备中的解密密钥的加密密钥来对内容加密然后将其记录，以及（ii）使用密钥对内容加密并将其记录，然后，与该密钥相应的解密密钥被通过使用与存储在再现设备中的解密密钥相应的加密密钥来加密并将其记录。

在这种情况下，需要严格地管理存储于再现设备中的解密密钥，使得不将其泄露到外界。当非法用户非法分析再现设备内部时，存在该解密密钥会被泄露出去的危险。一旦非法用户发现解密密钥，则存在该非法用户为了非法利用内容并非法出售这些设备而制造记录设备或再现设备，或者为了非法利用内容来制造计算机程序并经由网络等来分配该程序的可能性。

在这种情形下，版权所有人想要确保一旦泄漏的解密密钥不能处理将来所提供的内容。实现该目的的技术被称作密钥失效技术。专利文献 1 公开了实现密钥失效的系统。

在常规的密钥失效技术中，在记录介质的不可重写的区域中预先存储表示使存储在该设备中的密钥失效的密钥失效信息块。该设备使用记录在记录介质上的密钥失效信息块来判断存储于该设备中的密钥是否是失效的。当设备具有失效的密钥时，其被设置成以至于该设备不能使用记录介质。同样，当密钥再度被失效时，更新密钥失效信息块，且将所更新的密钥失效信息块记录于在密钥的新近失效之后制造的各记录介质上。这样，提供了其中不能利用具有失效密钥的新记录介质的机制。

另一方面，一般而言，使用被称为光盘驱动器的一种个人计算机的外围设备来从和向诸如光盘的记录介质中读取和写入内容。为了获得器件的兼容性，用于输入和输出内容数据的方法被标准化为公共信息，且通常不保密制作。因此，能够利用个人计算机等来容易地读取记录在记录介质上的内容，且还能够将所读取的数据写入另一记录介质上。因此，为了具有保护内容版权的系统，需要该系统包含防止用户读取记录在记录介质上的数据以便于将该数据写入另一记录介质上的有效功能，这是任何用户能够执行的一种常规动作。用于防止

从记录介质上读取数据被写入另一记录介质上的技术被称作为媒介绑定（media bind）技术。专利文献 2 公开了实现一种形式的媒介绑定的机制。

为了利用常规的媒介绑定技术来获取版权保护，在记录介质的不可重写区域中预存储识别该记录介质的介质识别符，并根据该介质识别符来对在记录介质上记录的加密内容加密。因此，当在第二记录介质上仅复制该加密内容时，由于第二记录介质具有在其上记录的另一介质识别符，所以不能正确地根据这另一介质识别符来对加密的内容解密。

然而，为了防止内容的非法使用被传播，需求实现各种用于防止非法使用的技术。

专利文献 **1**

日本未审专利申请公开 No.2002-281013

专利文献 2

日本专利公开 No.3073590

专利文献 **3**

日本未审专利申请公开 No.09-160492

发明内容

为了满足上述需求，本发明的目的是提供数字作品保护系统、记录设备、记录方法、再现设备、再现方法、计算机程序以及记录介质，其中每一个能够防止非法使用内容。

为了获得该目的，本发明提供一种数字作品保护系统，该系统包括记录设备和多个再现设备，记录设备可被操作以对内容加密并将加密内容写入在记录介质上，而多个再现设备各自可被操作以尝试对记

录在记录介质上的加密内容解密。在该系统中，多个再现设备中的一个或多个被失效。

该记录介质具有：（i）只读不可重写区，其中预存储该记录介质固有的介质固有号；和（ii）可以向其写入并从其中读取数据的可重写区。

该记录设备包括：存储单元，在其中存储包含多个加密媒介密钥的媒介密钥数据块，该加密媒介密钥是通过（i）对每一个未失效的再现设备，分别利用未失效的再现设备的器件密钥来对媒介密钥加密，和（ii）对每一个失效的再现设备，分别利用该失效的再现设备的器件密钥来对预定的探测信息加密而产生的；读取单元，可被操作以从记录介质的不可重写区中读取介质固有号；产生单元，可被操作以根据读取的介质固有号和媒介密钥来产生加密密钥；加密单元，可被操作以根据所产生的加密密钥对作为数字数据块的内容加密，以便于产生加密内容；读取单元，可被操作以从存储单元中读取媒介密钥数据块；以及写入单元，可被操作以将所读取的媒介密钥数据块和所产生的加密内容写入记录介质的可重写区。

每一再现设备包括：读取单元，可被操作以从记录在记录介质的可重写区中的媒介密钥数据块中读取与再现设备相应的加密媒介密钥；解密单元，可被操作以利用再现设备的器件密钥来对所读取的加密媒介密钥解密，以便于产生解密介质密钥；控制单元，可被操作以判断所产生的解密媒介密钥是否为探测信息，以当判断为肯定时阻止加密内容被解密，且当判断为否定时允许加密内容被解密；以及解密单元，在允许加密内容被解密时，可被操作以从记录介质中读取加密内容并根据所产生的解密媒介密钥来对所读取的加密内容解密，以便于产生解密内容。

根据本发明的方案，该记录设备，（i）将包含多个加密媒介密钥的媒介密钥数据块写到记录介质上，该多个加密媒介密钥是通过（a）对每一个未失效的再现设备，分别利用该未失效的再现设备的器件密钥来对媒介密钥加密，和（b）对每一个失效的再现设备，分别利用该失效的再现设备的器件密钥来对预定的探测信息加密而产生的；（ii）根据所读取的介质固有号和媒介密钥来产生加密密钥；和（iii）将根据所产生的加密密钥而产生的加密内容写到记录介质上。再现设备利用器件密钥来对加密媒介密钥解密以便于产生解密媒介密钥，并在所产生的解密媒介密钥为探测信息时阻止记录在记录介质上的加密内容被解密。

采用该方案，能够排除一个或多个失效的再现设备。

这里，可采取这样一种方案，其中，第二记录介质在其中存储包含另一组加密媒介密钥的第二媒介密钥数据块，该另一组加密媒介密钥是通过（i）对每一个未失效的再现设备，分别利用该未失效的再现设备的器件密钥来对媒介密钥加密，和（ii）对每一个失效的再现设备，分别利用该失效的再现设备的器件密钥来对预定的探测信息加密，而产生的；且记录设备还包括：比较单元，可被操作以将记录在第二记录介质上的第二媒介密钥数据块与存储在该存储单元中的第一媒介密钥数据块比较，以便于判断哪一个较新；和更新单元，当判断第二媒介密钥数据块较新时，可被操作以从第二记录介质中读取第二媒介密钥数据块，并使用第二媒介密钥数据块来覆盖存储在该存储单元中的第一媒介密钥数据块，并且第二读取单元从该存储单元中读取第二媒介密钥数据块而不是第一媒介密钥数据块；而写入单元将取代第一媒介密钥数据块的第二媒介密钥数据块写入可重写区。

采用该方案，记录介质能够使用从第二记录介质中获得的另一加

密媒介密钥来更新存储在本记录介质中的媒介密钥数据块。

这里，可接采取这样一种方案，其中，存储单元还在其中存储表示分配给该记录设备和多个再现设备的一个或多个公钥失效的失效数据块，该记录设备还包括信号签名（signature）产生单元，该单元可被操作以对失效数据块应用数字签名功能，以产生验证信息块；而写入单元还将所产生的验证信息块写入第一记录介质的可重写区中。另外，可采用这样一种方案，其中，记录设备还在其中存储表示分配给记录设备和多个再现设备的一个或多个公钥被失效的失效数据块，对失效数据块应用数字签名功能以产生验证信息块，并将所产生的验证信息块写入第一记录介质的可重写区，读取单元还读取记录在可重写区中的验证信息块，再现设备还包括验证单元，该验证单元可被操作以根据所读取的验证信息块来执行签名验证，并输出表示验证成功或验证失败的验证结果，而控制单元还在验证结果表示验证失败时阻止加密内容被解密，而在验证结果表示验证成功时允许加密内容被解密。

采用该方案，记录设备还将使用数字签名功能而产生的验证信息块写入记录介质，因此，能够通过在再现设备处检验验证信息块来排除非法再现设备。

这里，可采取这样一种方案，其中，存储单元在其中存储记录设备的公钥证书，第二读取单元从该存储单元中读取公钥证书，而写入单元将所读取的公钥证书写入第一记录介质的可重写区中。此外，可采取这样一种方案，其中，记录设备还在其中存储该记录设备的公钥证书，读取公钥证书，并将所读取的公钥证书写入第一记录介质的可重写区中，再现设备还包括：存储单元，在其中存储表示分配于该记录设备和多个再现设备的一个或多个公钥被失效的第一失效数据块；

证书读取单元，可被操作以从第一记录介质中读取公钥证书；以及公钥验证单元，可被操作以根据第一验证数据块来检验包含在所读取的公钥证书中的公钥是否被失效，且控制单元在公钥被失效时阻止加密内容被解密，而在公钥没有被失效时允许加密内容被解密。

采用这种方案，记录设备将公钥证书写入记录介质上，而再现设备从记录介质中读取公钥证书。因此，当公钥被失效时，能够阻止加密内容被解密。

这里，可采取这样一种方案，其中第二记录介质在其中存储表示分配于记录设备和多个再现设备的一个或多个公钥被失效的第二失效数据块，再现设备还包括：比较单元，可被操作以将记录在第二记录介质上的第二失效数据块与存储于该存储单元中的第一失效数据块比较以便于判断哪一个较新，和更新单元，当判断第二失效数据块较新时，可被操作以从第二记录介质中读取第二失效数据块，并使用所读取的第二失效数据块来覆盖存储单元中的第一失效数据块。

采用该方案，再现设备能够更新失效数据以便于其处于最新状态。

这里，可采取这样一种方案元，其中，存储单元还在其中存储识别记录设备的设备识别符，记录设备还包括：嵌入单元，可被操作以读取设备识别符并将所读取的设备识别符作为电子水印嵌入到内容中；并且加密单元对其中嵌入有设备识别符的内容加密。此外，再现设备还可以包括：存储单元，在其中存储识别再现设备的设备识别符；和嵌入单元，在允许加密内容被解密时，可被操作以从存储单元中读取设备识别符，并将所读取的设备识别符作为电子水印嵌入到加密的内容中，以及写入单元，可被操作以将其中嵌入有设备识别符的加密内容写到第一记录介质上。

采用该方案，记录设备和再现设备各自能够将其中嵌入有设备识别符的内容写到记录介质上，因此，在其中以非法方式分配内容的情况下，能够通过从内容中提取嵌入的设备识别符来识别用于记录该内容的记录设备和再现设备。

这里，可采取这样一种方案，其中，存储于存储单元中的第一媒介密钥数据块还包括识别第一媒介密钥数据块的第一数据识别符，写入单元（i）将第一数据识别符和加密内容以如此方式写入第一记录介质的可重写区中，使得第一数据识别符和加密内容彼此相应，并(ii)将包含第一数据识别符的第一媒介密钥数据块写入该可重写区。此外，可采取这样一种方案，其中存储在记录设备中的媒介密钥数据块还包括识别媒介密钥数据块的数据识别符，该记录设备将数据识别符和加密内容以如此方式写入可重写区，使得数据识别符和加密内容彼此相应，并将包含数据识别符的媒介密钥数据块写入可重写区，而再现设备还包括：接收单元，可被操作以接收记录在第一记录介质上的加密内容的说明（specification）；第一读取单元，可被操作以从第一记录介质中读取与所接收的说明中的加密内容相应的数据识别符；和第二读取单元，可被操作以从第一记录介质中读取包含数据识别符的媒介密钥数据块，而控制单元根据所读取的媒介密钥数据块来判断是阻止加密内容被解密还是允许被解密。

采用该方案，记录设备将数据识别符和加密内容以如此方式写在记录介质上，使得它们彼此相对应，并将包含数据识别符的媒介密钥数据写在记录介质上，因此，再现设备能够获得通过数据识别符与加密内容相应的媒介密钥数据块，并根据所获得的媒介密钥数据块来判断是否允许加密内容被解密。

附图的简要描述

图 1 是示出内容供给系统 10 的结构的结构示意图；

图 2 是示出记录设备 100 的结构的方框图；

图 3 是示出记录在记录介质 120 上的数据结构的数据结构示意图；

图 4 是示出再现设备 200 的结构的方框图；

图 5 是示出通过记录设备 100 执行的将数据写到记录介质 120 上的操作的流程图；

图 6 是示出通过再现设备 200 执行的再现记录介质 120 上的数据的操作的流程图（在图 7 中继续）；

图 7 是示出通过再现设备 200 执行的再现记录介质 120 上的数据的操作的流程图（接图 6）；

图 8 是示出在第一实施例的修改实例中记录在 n 块记录媒介上的数据的结构的数据结构示意图；

图 9 是示出在第一实施例的修改实例中记录在记录介质上的数据的结构的数据结构示意图；

图 10 是示出内容供给系统 20 的结构的结构示意图；

图 11 是示出记录设备 1100 的结构的方框图；

图 12 是示出记录在记录介质 1300 上的数据的结构的数据结构示意图；

图 13 是示出再现设备 1200 的结构的方框图；

图 14 是示出记录在记录介质 1300a 上的数据的结构的数据结构示意图；

图 15 是示出记录在记录介质 1300b 上的数据的结构的数据结构示意图；

图 16 是通过记录设备 1100 执行的将数据写入记录介质 1300 上的操作的流程图，将在图 17 中继续；

图 17 是通过记录设备 1100 执行的将数据写入记录介质 1300 上的操作的流程图，将在图 18 中继续；

图 18（接图 17）是通过记录设备 1100 执行的将数据写入记录介质 1300 上的操作的流程图；

图 19 是通过再现设备 1200 执行的再现记录在记录介质 1300 上的数据的操作的流程图，将在图 20 中继续；和

图 20（接图 19）是通过再现设备 1200 执行的再现记录在记录介质 1300 上的数据的操作的流程图。

执行本发明的最佳方式

1. 第一实施例

下面将描述作为本发明实施例的内容供给系统 10。

1.1 内容供给系统 10 的结构

如图 1 中所示，内容供给系统 10 包括：内容服务器设备 500，记录设备 100 和再现设备 200a、200b、200c、200d、200e 等。记录设备 100 和再现设备 200a、200b、200c、200d、200e…的总数量为 n。将设备号“1”分配给记录设备 100。将设备号“2”、“3”、“4”…“n”分别分配给再现设备 200a、200b、200c、200d、200e…。使用设备号来识别分配了设备号的各设备。

在这 n 个设备中，再现设备 200b 和再现设备 200c 已经被失效，因为它们被非法第三方非法侵袭且泄漏了应该保密的密钥。

提供音乐和电影内容的公司拥有经由专用线 30 彼此连接的内容服务器设备 500 和记录设备 100。内容服务器设备 500 具有内容和用

于内容加密的内容密钥。响应于来自记录设备 100 的请求，内容服务器设备 500 经由专用线 30 向记录设备 100 发送内容和相应的内容密钥。

记录设备 100 经由专用线 30 接收来自内容服务器设备 500 的内容和相应的内容密钥，对所接收的内容和内容密钥加密，并将加密内容、加密内容密钥以及其它相关信息写到记录介质 120 上。

其上记录有加密内容、加密内容密钥以及相关信息的记录介质 120 在商店被售出，且用户购买该记录介质 120。

当安装记录介质 120 时，用户拥有的再现设备 200a 从记录介质 120 中读取加密内容、加密内容密钥以及相关信息。再现设备 200a 由所读取相关信息判断对该内容解密是否可行。当判断解密可行时，再现设备 200a 从加密内容密钥中产生解密内容密钥，利用解密内容密钥产生解密内容，并将来自所产生的解密内容中的电影或音乐输出。

1.2 内容服务器设备 500

内容服务器设备 500 包括信息存储单元 501、控制单元 502、输入单元 503、显示单元 504 以及发送和接收单元 505（未在附图中示出）。

更为具体地，内容服务器设备 500 为一计算机系统，该计算机系统包括微处理器、ROM、RAM、硬盘单元、通信单元、显示单元、键盘、鼠标等。RAM 和硬盘单元各自在其中存储计算机程序。在微处理器根据计算机程序操作时，内容服务器设备 500 的构件实现它们的功能。

发送和接收单元 505 经由专用线 30 连接于记录设备 100 并在记

录设备 100 与控制单元 502 之间执行信息的发送和接收。

信息存储单元 501 在其中预存储多组内容和内容密钥，该内容是通过压缩编码（compression-coding）视频信息和音频信息而产生，而内容密钥为在内容加密中使用的密钥。

控制单元 502 接收用于经由专用线 30 以及发送和接收单元 505 来从记录设备 100 中得到获取一个内容的请求。当接受请求时，控制单元从信息存储单元 501 中读取请求中指出的内容和相应的内容密钥，并将所读取的内容和内容密钥经由发送和接收单元 505 以及专用线 30 发送到记录设备 100。

输入单元503从内容服务器设备500的用户接收指令并将所接收的指令输出到控制单元 502。

显示单元 504 在控制单元 502 的控制下显示各种信息。

1.3 记录设备 100

如图 2 中所示，记录设备 100 包括器件密钥存储单元 101、媒介密钥数据存储单元 102、密钥计算单元 103、密钥计算单元 104、加密单元 105、加密单元 106、私钥存储单元 107、证书存储单元 108、CRL 存储单元 109、签名产生单元 110、驱动单元 111、控制单元 112 以及发送和接收单元 113。

更为具体地，同内容服务器设备 500 相同，记录设备 100 为一计算机系统，该计算机系统包括微处理器、ROM、RAM、硬盘单元等。RAM 和硬盘单元各自在其中存储计算机程序。在微处理器根据计算机程序操作时记录设备 100 实现其功能。

（1）器件密钥存储单元 101

器件密钥存储单元 101 在其中以如此方式秘密地存储器件密钥

DK_1 以便于器件密钥 DK_1 不能被外部设备访问。器件密钥 DK_1 为对于记录设备 100 唯一的密钥。应该注意的是，在本发明的该说明书中，将存储于设备 m 中的器件密钥表达为 DK_m。

（2）媒介密钥数据存储单元 102

媒介密钥数据存储单元 102 在其中存储媒介密钥数据 MDATA。媒介密钥数据 MDATA 包括 n 组加密媒介密钥和设备号。在各组中，加密媒介密钥和设备号彼此相应。如前所述，n 为记录设备 100 和再现设备 200a、200b…等的总数量。

在这 n 组中，第一组由第一加密媒介密钥和设备号“1”构成。设备号“1”为识别记录设备 100 的识别信息。通过利用分配给用设备号“1”来识别的设备即记录设备 100 的器件密钥 DK_1 对媒介密钥 MK 实施加密算法 E1 而产生第一加密媒介密钥。

第一加密媒介密钥 ＝E1（DK_1，MK）

这里，加密算法 1 是以，例如，DES（数据加密标准）为依据的。E（A，B）表示通过利用密钥 A 对纯文本 B 执行加密算法 E 所获得的加密文本。

作为附加信息，媒介密钥 MK 为对于记录介质 120 唯一的密钥。

在这 n 组中，第二组由第二加密媒介密钥和设备号“2”构成。设备号“2”表示再现设备 200a。通过利用分配给用设备号“2”来识别的设备即再现设备 200a 的器件密钥 DK_2 对媒介密钥 MK 执行加密算法 E1 而产生第二加密媒介密钥。

第二加密媒介密钥 ＝E1（DK_2，MK）

在这 n 组中，第三组和第四组分别由第三加密媒介密钥和设备号“3”以及第四加密媒介密钥和设备号“4”构成。设备号“3”和“4”分别表示再现设备 200b、200c。分别通过利用分配给用设备号“3”

和“4”来识别的设备即再现设备 200b 和 200c 的器件密钥 DK_3 和 DK_4 对数值 0 而不是媒介密钥 MK 执行加密算法 E1 而产生第三和第四加密媒介密钥。

第三加密媒介密钥 ＝E1（DK_3，MK）

第四加密媒介密钥 ＝E1（DK_4，MK）

这里，数值“0”为完全与媒介密钥 MK 不相关的数据块。之所以使用值“0”来替换媒介密钥 MK 的原因是分别相应于第三和第四加密媒介密钥的再现设备 200b 和 200c 被失效了。数值“0”用作探测再现设备 200b 和 200c 已经被失效的探测信息。

当通过利用失效设备的器件密钥对完全与媒介密钥 MK 无关的值“0”加密来为失效的设备产生加密媒介密钥时，能够允许在除失效设备之外的所有设备中共享媒介密钥 MK。同样，能够从该系统中排除失效设备。

虽然这里使用值“0”，也可以使用与媒介密钥 MK 无关的另一种数据。例如，能够使用另一固定值“0xFFFF”，或表示产生该加密媒介密钥的日期或时间的信息，或者失效设备的器件密钥。

应该注意的是，可以使用其他失效方法来使设备失效。例如，专利文献 1 公开了使用树结构的失效方法。

在这 n 组中，第五至第 n 组分别由第五加密媒介密钥和设备号“5”、…以及第 n 加密媒介密钥和设备号“n”组成。设备号“5”至“n”分别标示再现设备 200d、200e、…。分别通过利用分配给用设备号“5”至“n”来识别的设备即再现设备 200d、200e、…的器件密钥 DK_5 之 DK_n 对媒介密钥 MK 执行加密算法 E1 而产生第五至第 n 加密媒介密钥。

第五加密媒介密钥 ＝E1（DK_5，MK）

……

第 n 加密媒介密钥 ＝E1（DK_n，MK）

（3）密钥计算单元 103

密钥计算单元 103 在其中预存储分配给记录设备 100 的设备号“1”。

密钥计算单元 103 从包含于存储在媒介密钥数据存储单元 102 中的媒介密钥数据 MDATA 的 n 组中搜索并读取包括预存储设备号“1”的组。然后密钥计算单元 103 从所读取的组中提取与设备号“1”相应的加密媒介密钥 E1（DK_1，MK）。

接着，密钥计算单元 103 从器件密钥存储单元 101 中读取器件密钥 DK_1，并利用所读取的器件密钥 DK_1 来对所提取的加密媒介密钥 E1（DK_1，MK）执行解密算法 D1，以便于产生媒介密钥 MK。

媒介密钥 MK＝D1（DK_1，E1（DK_1，MK））

这里，解密算法 D1 为用于对通过执行加密算法 E1 而产生的加密文本解密的算法，并且，例如，以 DES 为依据。D（A，B）表示通过利用密钥 A 对加密文本 B 执行解密算法而获得的解密文本。

接着，密钥计算单元 103 向密钥计算单元 104 输出所产生的媒介密钥 MK。

应该注意的是，在图 2 中，表示记录设备 100 的构件的方框经由连接线与其他方框相互连接，然而，附图中省略了一些连接线。这里，连接线表示通过其发送信号和信息的路径。同样，在这些连接于表示密钥计算单元 103 的方框的连接线中，标记有密钥符号的连接线为在其上向计算单元 103 发送作为密钥的信息的路径。这同样适用于表示其它构件的其它方框。这同样适用于其他附图。

（4）密钥计算单元 104

密钥计算单元 104 接收来自密钥计算单元 103 的媒介密钥 MK 并经由驱动单元 111 从记录介质 120 的固有号记录区 121 读取介质固有号 MID。

接着，密钥计算单元 104 将所接收的媒介密钥 MK 与所读取的介质固有号 MID 按照以上顺序合并，从而产生合并的值（MK||MID）。这里，“A||B”表示数据 A 和数据 B 按照以上顺序的位的合并。然后密钥计算单元 104 对所产生的合并值（MK||MID）执行散列函数 SHA-1，以便于获得散列值 H=SHA-1（MK||MID）。密钥计算单元 104 将所获得的散列值 H 作为密钥加密密钥 KEK 并向加密单元 105 和信号签名产生单元 110 输出密钥加密密钥 KEK。

这里，SHA-1（A）表示通过对信息 A 执行散列函数 SHA-1 而获得的散列值。

应该注意的是，密钥计算单元 104 将通过执行散列函数 SHA-1 所获得的散列值作为密钥加密密钥 KEK，然而，本发明不限于此。将所获得的散列值的一部分作为密钥加密密钥 KEK 也是可行的。

应该注意的是，由于散列函数 SHA-1 为公知的，所以省略其解释。使用其它种类的散列函数也是可接受的。

（5）加密单元 105

加密单元 105 经由发送和接收单元 113 接收来自内容服务器设备 500 的内容密钥 CK，并接收来自密钥计算单元 104 的密钥加密密钥 KEK.

接着，加密单元 105 利用所接收的密钥加密密钥 KEK 来对所接收的内容密钥 CK 执行加密算法 E2，以便于产生加密内容密钥 ECK。

加密内容密钥 ECK = E2（KEK，CK）

这里，加密算法 E2，例如，以 DES 为依据。

然后加密单元105通过驱动单元111在记录介质120上保留密钥记录区123，并通过驱动单元111将所产生的加密内容密钥ECK写入记录介质120的密钥记录区123中。

（6）加密单元106

加密单元106经由发送和接收单元113接收来自内容服务器设备500的内容密钥CK和内容CNT，并利用所接收的内容密钥CK对所接收的内容CNT执行加密算法E3，以便于产生加密内容ECNT。

加密内容ECNT＝E3（CK，CNT）

这里，加密算法E3，例如，以DES依据。

接着，加密单元106经由驱动单元111在记录介质120上保留内容记录区124，并经由驱动单元111将所产生的加密内容ECNT写入记录介质120的内容记录区124中。

（7）私钥存储单元107

私钥存储单元107在其中以如此方式存储用于记录设备100的私钥SK_1，使得该私钥SK_1不可被外部设备访问。私钥SK_1与公钥加密方法一致。这里，使用的公钥加密方法例如为RSA（Rivest Shamir Adleman）加密方法。

（8）证书存储单元108

证书存储单元108在其中存储公钥证书PKC。公钥证书PKC如此构造以便于包括证书识别符ID_1、公钥PK_1和签名数据Sig_1。

证书识别符ID_1为唯一识别公钥证书PKC的识别信息。公钥PK_1为与存储在私钥存储单元107中的私钥SK_1相应的公钥。通过利用认证中心CA的私钥SK_CA对证书识别符ID_1和公钥PK_1的合并值（ID_1||PK_1）使用数字签名功能Sig来产生签名数据Sig_1。

签名数据Sig_1=Sig（SK_CA，ID_1||PK_1）

这里，Sig（A，B）表示通过利用密钥 A 来对数据 B 使用数字签名功能 Sig 而获得的签名数据块。数字签名功能 Sig 的一个实例为使用了具有散列函数 SHA-1 的 RSA 的数字签名。

（9）CRL 存储单元 109

CRL 存储单元 109 具有记录在其上的公钥证书失效列表（下文中，称之为失效列表“CRL”），其表示在第一时间点失效的一个或多个公钥证书。

失效列表 CRL 包括一个或多个证书识别符以及签名数据 SigID 和版本号。

每一个证书识别符为识别失效的公钥证书的识别信息。

通过利用认证中心的私钥 SK_CA 对包含于失效列表 CRL 中的所有证书识别符（或在失效列表 CRL 中包含一个证书识别符的情况下，对该证书识别符使用数字签名功能 Sig）的合并值使用数字签名功能 Sig 来产生签名数据 SigID。

签名数据 SigID=Sig（SK_CA，所有证书识别符的合并值）

例如，当使用证书识别符 ID_3 和 ID_4 来识别的公钥证书被失效时，失效列表 CRL 包括证书识别符 ID_3、ID_4，签名数据 SigID=Sig（SK_CA，（ID_3||ID_4））以及版本号。

版本号为表示失效列表 CRL 版本的信息，并示出实效列表 CRL 是基于第一时间点。公钥证书失效列表的版本越新，版本号的值越大。

（10）签名产生单元 110

签名产生单元 110 从私钥存储单元 107 中读取私钥 SK_1，从 CRL 存储单元 109 中读取失效列表 CRL，并接收来自密钥计算单元 104 的密钥加密密钥 KEK。

然后签名产生单元 110 将所接收的密钥加密密钥 KEK 与所读取

的失效列表 CRL 按照上述顺序合并，以产生合并值（KEK||CRL）。签名产生单元 110 还利用所读取的私钥 SK_1 来对所产生的合并值（KEK||CRL）使用数字签名功能 Sig，以产生签名数据 SigCRL。

签名数据 SigCRL=Sig（SK_1，（KEK||CRL））

接着，签名产生单元 110 经由驱动单元 111 在记录介质 120 上保留签名记录区 125，并经由驱动单元 111 将所产生的签名数据 SigCRL 写入记录介质 120 的签名记录区 125 中。

（11）控制单元 112

控制单元 112 经由发送和接收单元 113 向内容服务器设备 500 发送用于获取内容的请求。

控制单元 112 还从证书存储单元 108 中读取公钥证书 PKC，经由驱动单元 111 在记录介质 120 上保留证书记录区 127，并经由驱动单元 111 将所读取的公钥证书 PKC 写入记录介质 120 的证书记录区 127 中。

另外，控制单元 112 从媒介密钥数据存储单元 102 中读取媒介密钥数据 MDATA，经由驱动单元 111 在记录介质 120 上保留媒介密钥数据记录区 122，且然后经由驱动单元 111 将所读取的媒介密钥数据 MDATA 写入记录介质 120 的媒介密钥数据记录区 122 中。

此外，控制单元 112 从 CRL 存储单元 109 中读取失效列表 CRL，经由驱动单元 111 在记录介质 120 上保留 CRL 记录区 126，且然后经由驱动单元 111 将所读取的失效列表 CRL 写入记录介质 120 的 CRL 记录区 126 中。

控制单元 112 根据记录设备 100 的操作者发出的操作指令来接收来自键盘 180 的指令信息，并根据指令信息操作。控制单元 112 还控制记录设备 100 的其它构件的操作。

（12）发送和接收单元 113

发送和接收单元 113 经由专用线 30 与内容服务器设备 500 连接，并在内容服务器设备 500 与控制单元 112 之间执行信息的发送与接收。在控制单元 112 的控制下，发送和接收单元 113 还在内容服务器设备 500 与加密单元 105 之间以及内容服务器设备 500 与加密单元 106 之间执行信息的发送与接收。

（13）驱动单元 111

在控制单元 112 的控制下，驱动单元 111 从记录介质 120 的固有号记录区 121 中读取介质固有号 MID，并将所读取的介质固有号 MID 输出到密钥计算单元 104。

同样，在控制单元 112 的控制下，驱动单元 111 接收来自加密单元 105、加密单元 106 和签名产生单元 110 的信息块，在记录介质 120 上保留用于将上述信息块写入其中的若干区域，然后将信息块写入该区域。

另外，驱动单元 111 接收来自控制单元 112 的信息，在记录介质 120 上保留要将该信息写入其中的区域，然后将信息写入该区域。

（14）键盘 180 和监视器 190

键盘 180 接收由记录设备 100 的操作者发出的操作指令，并将与所接收的操作指令相应的指令信息输出到控制单元 112。

监视器 190 在控制单元 112 的控制下显示各种信息。

1.4 记录介质 120

记录介质 120 为光盘介质，且，如图 3 中所示，包括固有号记录区 121 和普通区 129。

在固有号记录区 121 中，预存储作为识别记录介质 120 的固有号

的介质固有号 MID。固有号记录区 121 为不能向其中写入其它信息且在其中不能重写介质固有号 MID 的不可重写区。将介质固有号 MID 表达为，例如，八个字符的十六进制数，且为“0x00000006”。应该注意的是，在本说明书中，“0x”意味着其后的表达式为十六进制数。

普通区 129 为能够向其写入其它信息的区。最初，没有信息写入普通区 129。

在由记录设备 100 执行上述操作之后，如图 3 中所示，在普通区 129 中保留媒介密钥数据记录区 122、密钥记录区 123、内容记录区 124，签名记录区 125、CRL 记录区 126 及证书记录区 127。

如前所述，在第一实施例中，记录设备 100 和再现设备 200a、200b、200c、200d、200e…的总数量为 n。在这些设备中，再现设备 200b 和再现设备 200c 被失效。假设这 n 个设备中的每一个仅拥有各自唯一的器件密钥。根据该假设，在记录介质 120 的普通记录区 129 的区域内记录作为具体实例的各类数据。

媒介密钥数据记录区 **122**

媒介密钥数据记录区 122 具有记录在其中的媒介密钥数据 MDATA。媒介密钥数据 MDATA 包括 n 组加密媒介密钥和设备号。

每一设备号为识别一个设备的识别信息。

通过利用分配给由相应的设备号“m”识别的设备“m”的器件密钥 DK_m 来对媒介密钥 MK 执行加密算法 E1 来产生每一加密媒介密钥。这里，在其中设备 m 被失效的情况下，使用值“0”。相反，在其中设备 m 未被失效的情况下，使用媒介密钥 MK。

加密媒介密钥=E1（DK_m，MK）

或加密媒介密钥=E1（DK_m，0）

密钥记录区 **123**

密钥记录区 123 具有记录在其中的加密内容密钥 ECK。通过利用密钥加密密钥 KEK 对内容密钥 CK 执行加密算法 E2 来产生加密内容密钥 ECK。

加密内容密钥 ECK=E2（KEK，CK）

这里，在输入值为媒介密钥 MK 与介质固有号 MID 的合并值时，密钥加密密钥 KEK 为利用散列函数的输出值计算的密钥。

密钥加密密钥 KEK=SHA-1（MK||MID）

内容记录区 **124**

内容记录区 124 具有在其中记录的加密内容 ECNT。通过利用内容密钥 CK 对内容执行加密算法 E3 来产生加密内容 ECNT。

加密内容 ECNT=E3（CK，CNT）

签名记录区 **125**

签名记录区 125 具有在其中记录的签名数据 SigCRL。

签名数据 SigCRL 是通过利用私钥 SK_1 对密钥加密密钥 KEK 和失效列表 CRL 的合并值（KEK||CRL）使用数字签名功能 Sig 来产生的。

签名数据 SigCRL=Sig（SK_1，（KEK||CRL））

CRL 记录区 **126**

CRL 记录区 126 具有记录在其中的失效列表 CRL。失效列表 CRL 示出要被失效的证书的 ID。失效列表 CRL 包括，例如，证书识别符

ID_3、ID_4、签名数据 SigID 以及版本号。

证书识别符 ID_3 和 ID_4 各自为识别被失效的公钥证书的识别信息块。签名数据 SigID 是通过利用认证中心 CA 的私钥 SK_CA 对包含于失效列表 CRL 中的所有证书识别符的合并值使用数字签名功能 Sig（或者在其中失效列表 CRL 中包含有一个证书识别符的情况下，对该证书识别符使用数字签名功能 Sig）来产生的。

签名数据 SigID=Sig（SK_CA，所有证书识别符的合并值）

包含了认证中心 CA 的签名数据，因而可以保证失效列表 CRL 被认证。

版本号为表示失效列表 CRL 版本的信息。

CRL 的格式可以是公知的一种。或者， CRL 的格式可以是专用于一个系统。

证书记录区 **127**

证书记录区 127 具有在其中记录的公钥证书 PKC。公钥证书 PKC 包括证书识别符 ID_1、公钥 PK_1 以及签名数据 Sig_1。

证书识别符 ID_1 为识别公钥证书 PKC 的识别信息。公钥 PK_1 与一个公钥加密方法一致，并对应于私钥 SK_1。

签名数据 Sig_1 是通过利用认证中心 CA 的私钥 SK_CA 对证书识别符 ID_1 和公钥 PK_1 的合并值（ID_1||PK_1）使用数字签名功能 Sig 而产生的。

签名数据 Sig_1=Sig（SK_CA，（ID_1||PK_1））

在认证中心 CA 中包括了签名数据，从而可以保证公钥证书的认证。

公钥证书的格式可以是公知的一种。或者，公钥证书的格式为专

用于一种系统。

1.5 再现设备 200

由于再现设备 200a、200b、200c…具有相同的结构，所以这里对再现设备 200 进行阐释。

如图 4 中所示，再现设备 200 包括：器件密钥存储单元 201、密钥计算单元 202、密钥计算单元 203、解密单元 204、解密单元 205、CA 公钥存储单元 206、证书验证单元 207、CRL 存储单元 208、CRL 验证单元 209、CRL 比较更新单元 210、证书判断单元 211、签名验证单元 212、开关 213、再现单元 214、控制单元 215、输入单元 216、显示单元 217 和驱动单元 218。

更为具体地，与内容服务器设备 500 相同，再现设备 200 为一计算机系统，该系统包括微处理器、ROM、RAM、硬盘单元等。RAM 和硬盘单元各自在其中存储计算机程序。在微处理器根据计算机程序操作时再现设备 200 实现其功能。

（1）器件密钥存储单元 201

器件密钥存储单元 201 在其中以如此方式保密地存储器件密钥 DK_x，使得器件密钥 DK_x 不被外部设备访问。器件密钥 DK_x 为对于再现设备 200 唯一的密钥。

对于再现设备 200a、200b、200c、200d、200e…的每一个，存储在器件密钥存储单元 201 中的器件密钥 DK_x 各不同。再现设备 200a、200b、200c、200d、200e…的器件密钥存储单元 201 分别在其中存储器件密钥 DK_2、DK_3、DK_4、DK_5、DK_6…。

（2）密钥计算单元 202

密钥计算单元 202 在其中预存储分配给再现设备 200 的设备号“x”。对于再现设备 200a、200b、200c、200d、200e…的每一个，

存储在密钥计算单元202中的设备号“x”各不同。再现设备200a、200b、200c、200d、200e…的密钥计算单元202分别在其中存储设备号“2”、“3”、“4”、“5”、“6”…。

密钥计算单元202经由驱动单元218从记录介质120的媒介密钥数据记录区 122 中顺序地读取包含于媒介密钥数据 MDATA 中的 n 组。然后密钥计算单元202从所读取的组中搜索包括所存储的设备号“x”的组。当发现包含设备号“x”的组时，密钥计算单元202从所发现的组中提取相应于设备号“x”的加密媒介密钥E1（DK_x，y）。这里，当再现设备200为再现设备200b或再现设备200c时，y的值为 “0”。当再现设备200为除再现设备200b和200c之外的再现设备时，y为媒介密钥MK。

接着，密钥计算单元202从器件密钥存储单元201中读取器件密钥DK_x，并利用所读取的器件密钥DK_x对所提取的加密媒介密钥E1（DK_x，y）执行解密算法D1，以便于产生解密媒介密钥y。

解密媒介密钥y=D1（DK_x，E1（DK_x，y））

这里，解密媒介密钥y为媒介密钥MK或者值“0”。

接着，密钥计算单元202向密钥计算单元203输出所产生的解密媒介密钥y。

（3）密钥计算单元203

密钥计算单元203以与密钥计算单元104相同的方式操作。

密钥计算单元 203 接收来自密钥计算单元 202 的解密媒介密钥y，并经由驱动单元218从记录介质120的固有号记录区121中读取媒介固有号MID。

接着，密钥计算单元203将所接收的解密媒介密钥y与所读取的介质固有号MID按照上述顺序合并，以便于产生合并值（y||MID）。

然后密钥计算单元 203 对所产生的合并值（y||MID）执行散列函数 SHA-1，以便于获得散列值 H'=SHA-1（y||MID）。密钥计算单元 203 将所获得的散列值 H'作为密钥解密密钥 KDK，并将密钥解密密钥 KDK 输出到解密单元 204 和签名验证单元 212。

如上所述，当密钥计算单元 104 将所获得的散列值的一部分作为密钥加密密钥 KEK 时，密钥计算单元 203 也将所获得的散列值的相同部分作为密钥解密密钥 KDK。

（4）解密单元 204

解密单元 204 经由驱动单元 218 从记录介质 120 的密钥记录区 123 中读取加密内容密钥 ECK，并接收来自密钥计算单元 203 的密钥解密密钥 KDK。

接着，解密单元 204 利用所接收的密钥解密密钥 KDK 对所读取的加密内容密钥 ECK 执行解密算法 D2，以便于产生解密内容密钥 DCK。

解密内容密钥 DCK=D2（KDK，ECK）

这里，解密算法 D2 为用于对通过执行加密算法 E2 所产生的加密文本解密的算法，且解密算法 D2 以，例如，DES 为依据。

接着，解密单元 204 向解密单元 205 输出所产生的解密内容密钥 DCK。

（5）解密单元 205

解密单元 205 经由驱动单元 218 从记录介质 120 的内容记录区 124 中读取加密内容 ECNT，并接收来自解密单元 204 的解密内容密钥 DCK。

接着，解密单元 205 利用所接收的解密内容密钥 DCK 对所读取的加密内容 ECNT 执行解密算法 D3，以便于产生解密内容 DCNT。

解密内容 DCNT=D3（DCK，ECNT）

这里，解密算法 D3 为对通过执行加密算法 E3 而产生的加密文本解密的算法，并且以，例如，DES 为依据。

接着，解密单元 205 向开关 213 输出所产生的解密内容 DCNT。

（6）CA 公钥存储单元 206

CA 公钥存储单元 206 在其中预存储认证中心 CA 的公钥 PK_CA。

（7）证书验证单元 207

证书验证单元 207 经由驱动单元 218 从 CA 公钥存储单元 206 中读取公钥 PK_CA，并从记录介质 120 的证书记录区 127 中读取公钥证书 PKC。

接着，证书验证单元 207 从所读取的公钥证书 PKC 中提取证书识别符 ID_1、公钥 PK_1 和签名数据 Sig_1，并将所提取的证书识别符 ID_1 与公钥 PK_1 按照上述顺序合并，以便于产生合并值（ID_1||PK_1）。

然后证书验证单元 207 利用所读取的公钥 PK_CA 对所提取的签名数据 Sig_1 和所产生的合并值（ID_1||PK_1）执行签名验证算法 Vrfy，以便于获得验证结果 RSL2。验证结果 RSL2 为表示验证成功或验证失败的信息。

这里，签名验证算法 Vrfy 为用于验证使用数字签名功能 Sig 而产生的签名数据块的算法。

接着，证书验证单元 207 向开关 213 输出验证结果 RSl2。

（8）CRL 存储单元 208

CRL 存储单元 208 具有在其上记录的公钥证书失效列表（下面称之为所存储的失效列表“CRL_ST”），其表示在第二时间点被失效

的一个或多个公钥证书。

与表示在第一时间点被失效的公钥证书的失效列表 CRL 相同，所存储的失效列表 CRL_ST 包括一个或多个证书识别符以及签名数据 SigID 和版本号。

关于证书识别符和签名数据 SigID，它们与前面所述的相同。

版本号为表示所存储的失效列表 CRL_ST 的产生的信息，且示出所存储的失效列表 CRL_ST 是基于第二时间点的。所存储的失效列表的版本越新，版本号的值越大。

（9）CRL 验证单元 209

CRL 验证单元 209 经由驱动单元 218 从 CA 公钥存储单元 206 中读取公钥 PK_CA 并从记录介质 120 的 CRL 记录区 126 中读取失效列表 CRL。

接着，CRL 验证单元 209 从所读取的失效列表 CRL 中提取一个或多个证书识别符和签名数据 SigID。这里，当提取多个证书识别符时，按照它们在失效列表 CRL 中布置的顺序合并，以产生合并值。当仅提取一个证书识别符时，将该证书识别符作为合并值。

接着 CRL 验证单元 209 利用所读取的公钥 PK_CA 对所提取的签名数据 SigID 和所产生的合并值执行签名验证算法 Vrfy，以便于获得验证结果 RSL3。验证结果 RSL3 表示验证成功或验证失败。

当验证结果 RSL3 示出验证成功，CRL 验证单元 209 向签名验证单元 212 和 CRL 比较更新单元 210 输出所读取的失效列表 CRL。

（10）CRL 比较更新单元 210

CRL 比较更新单元 210 接收来自 CRL 验证单元 209 的失效列表 CRL。

一旦接收失效列表 CRL，CRL 比较更新单元 210 从所接收的失

效列表 CRL 中提取版本号，从 CRL 存储单元 208 中读取所存储的失效列表 CRL_ST，并从所读取的所存储的失效列表 CRL_ST 中提取版本号。接着，CRL 比较更新单元 210 判断从失效列表 CRL 中提取的版本号是否大于从所存储的失效列表 CRL_ST 中提取的版本号。

一旦判断从失效列表 CRL 中提取的版本号大于从所存储的失效列表 CRL_ST 中提取的版本号，则 CRL 比较更新单元 210 认为失效列表 CRL 的版本比所存储的失效列表 CRL_ST 的版本新，并用该失效列表 CRL 覆盖 CRL 存储单元 208 中所存储的失效列表 CRL_ST，该失效列表 CRL 充当所存储的是失效列表 CRL_ST。

一旦判断从失效列表 CRL 中提取的版本号小于或等于从所存储的失效列表 CRL_ST 中提取的版本号，则 CRL 比较更新单元 210 认为失效列表 CRL 的版本比所存储的失效列表 CRL_ST 的版本旧或相等，则不执行上述覆盖。

（11）证书判断单元 211

证书判断单元 211 从 CRL 存储单元 208 中读取所存储的失效列表 CRL_ST。这里，存储在 CRL 存储单元 208 中的所存储的失效列表 CRL_ST 已经被 CRL 比较更新单元 210 更新为最新的。证书判断单元 211 经由驱动单元 218 从记录介质 120 的证书记录区 127 中读取公钥证书 PKC。

接着证书判断单元 211 从所读取的公钥证书 PKC 中提取证书识别符 ID_1，并判断所提取的证书识别符 ID_1 是否包含在所存储的失效列表 CRL_ST 中。然后证书判断单元 211 向开关 213 输出判断结果 JDG。这里，判断结果 JDG 是表明证书识别符 ID_1 是否包含在所存储的失效列表 CRL_ST 中的信息。

（12）签名验证单元 212

签名验证单元 212 接收来自密钥计算单元 203 的密钥解密密钥 KDK。同样，签名验证单元 212 经由驱动单元 218 从记录介质 120 的签名记录区 125 中读取签名数据 SigCRL，并经由驱动单元 218 从记录介质 120 的证书记录区 127 中读取公钥证书 PKC。签名验证单元 212 还接收来自 CRL 验证单元 209 的失效列表 CRL。

接着，签名验证单元 212 从所读取的公钥证书 PKC 中提取公钥 PK_1，并将所接收的密钥解密密钥 KDK 与所接收的失效列表 CRL 合并，以产生合并值（KDK||CRL）。签名验证单元 212 还利用所提取的公钥 PK_1 对所读取的签名数据 SigCRL 和所产生的合并值（KDK||CRL）执行签名验证算法 Vrfy，以获得验证结果 RSL1。

验证结果 RSL1 为表明验证成功或验证失败的信息。

接着，签名验证单元 212 向开关 213 输出验证结果 RSL1。

（13）开关 213

开关 213 接收来自解密单元 205 的解密内容 DCNT。开关 213 还接收来自证书判断单元 211 的判断结果 JDG，接收来自证书验证单元 207 的验证结果 RSL2，并接收来自签名验证单元 212 的验证结果 RSL1。

当满足下列所有条件时，开关 213 向再现单元 214 输出所接收的解密内容 DCNT：（i）所接收的验证结果 RSL1 表明验证成功；（ii）所接收的验证结果 RSL2 表明验证成功；且（iii）所接收的判断结果 JDG 表明证书识别符 ID_1 不包含在所存储的失效列表 CRL_ST 中。当满足下列条件中的至少一个时，开关 213 不向再现单元 214 输出所接收的解密内容 DCNT：（i）所接收的验证结果 RSL1 表明验证失败；（ii）所接收的验证结果 RSL2 表明验证失败；以及（iii）所接收的判断结果 JDG 表明证书识别符 ID_1 包含在所存储的失效列表

CRL_ST 中。

（14）再现单元 214

再现单元 214 接收来自开关 213 的解密内容 DCNT，由所接收的解密内容 DCNT 产生视频信息和音频信息，并将所产生的视频信息和音频信息转换为模拟视频信号和模拟音频信号，以便于向监视器 290 输出模拟视频和音频信号。

（15）控制单元 215、输入单元 216、显示单元 217、驱动单元 218、监视器 290 和遥控器 280

控制单元 215 控制再现设备 200 的各构件的操作。

遥控器 280 包括各种按钮，并根据操作者在按钮上的操作来产生操作指令，以便于以红外线方式输出所产生的操作指令信息。

输入单元 216 接收来自遥控器 280 的包括操作指令信息的红外线，从所接收的红外线中提取操作指令信息，并将所提取的操作指令信息输出到控制单元 215。

显示单元 217 在控制单元 215 的控制下显示各种信息。

驱动单元 218 从记录介质 120 中读取信息。

监视器 290 包括 CRT 和扬声器，并接收来自再现单元 214 的模拟视频信号和模拟音频信号，以便于根据视频信号显示图像并根据音频信号输出声音。

1.6 内容供给系统 10 的操作

下面描述内容供给系统 10 的操作，特别地，描述通过记录设备 100 执行的向记录介质 120 上写数据的操作,和通过再现设备 200 执行的再现记录在记录介质 120 上的数据的操作。

（1）由记录设备 100 执行的写数据的操作

下面参考图5种的流程图描述通过记录设备100执行的向记录介质120上写数据的操作。

密钥计算单元103分别从器件密钥存储单元101和媒介密钥数据存储单元102中读取器件密钥DK_1和媒介密钥数据MDATA（步骤S301）。然后密钥计算单元103利用所读取的器件密钥DK_1和媒介密钥数据MDATA来产生媒介密钥MK（步骤S302）。

接着，密钥计算单元104从记录介质120的固有号记录区121中读取介质固有号MID（步骤S303），并利用所产生的媒介密钥MK和所读取的介质固有号MID来计算密钥加密密钥KEK（步骤S304）。

然后，加密单元105利用所计算的密钥加密密钥KEK对从内容服务器设备500所获得的内容密钥CK加密，以产生加密内容密钥ECK（步骤S305）。

接着，加密单元106利用从内容服务器设备500获得的内容密钥CK对从内容服务器500获得的内容CNT加密，以产生加密内容ECNT（步骤S306）。

然后签名产生单元110从私钥存储单元107中读取私钥SK_1（步骤S307），并利用所读取的私钥SK_1来产生用于密钥加密密钥KEK和失效列表CRL的签名数据SigCRL（步骤S308）。

接着，记录设备100经由驱动单元111在记录介质上记录媒介密钥数据MDATA、加密内容密钥ECK、加密内容ECNT、签名数据SigCRL、失效列表CRL和公钥证书PKC（步骤S309）。

（2）由再现设备200执行的再现数据的操作

下面参考图6和7中的流程图，来描述通过再现设备200执行的再现记录在记录介质120上的数据的操作。

再现设备200从记录介质120上读取媒介密钥数据MDATA、介

质固有号 MID、加密内容密钥 ECK、加密内容 ECNT、签名数据 SigCRL、失效列表 CRL 和公钥证书 PKC（步骤 S401）。

接着，密钥计算单元 202 从器件密钥存储单元 201 中读取器件密钥 DK_x（步骤 S402），并利用所读取的媒介密钥数据 MDATA 和器件密钥 DK_x 来获得解密媒介密钥 y（步骤 S403）。

然后密钥计算单元 203 根据所读取的介质固有号 MID 和所获得的解密媒介密钥 y 来计算密钥解密密钥 KDK（步骤 S404）。

然后解密单元 204 利用所计算的密钥解密密钥 KDK 对所读取的解密内容密钥 ECK 解密，以获得解密内容密钥 DCK（步骤 S405）。

接着，解密单元 205 利用所获得的解密内容密钥 DCK 对所读取的加密内容 ECNT 解密，以获得解密内容 DCNT（步骤 S406）。

然后证书验证单元 217 从 CA 公钥存储单元 206 中读取认证中心 CA 的公钥 PK_CA（步骤 S407），并利用所读取的认证中心 CA 的公钥 PK_CA 来验证所读取的公钥证书 PKC 的有效性（步骤 S408）。

当公钥证书 PKC 的有效性验证失败（步骤 S409）时，控制转移到步骤 S422。当公钥证书 PKC 的有效性验证成功（步骤 S409）时，CRL 验证单元 209 利用认证中心 CA 的公钥 PK_CA 来验证所读取的失效列表 CRL 的有效性（步骤 S410）。

当失效列表 CRL 的有效性验证失败（步骤 S411）时，控制专利到步骤 S422。当失效列表 CRL 的有效性验证成功（步骤 S411）时，CRL 比较更新单元 210 从 CRL 存储单元 208 中读取所存储的失效列表 CRL_ST（步骤 S412），并将从记录介质 120 中读取的失效列表 CRL 与从 CRL 存储单元 208 中读取的所存储的失效列表 CRL_ST 相比较，以判断哪一个更新（步骤 S413）。

作为比较结果，当判断失效列表 CRL 比所存储的失效列表

CRL_ST 更新时（步骤 S414），CRL 比较更新单元 210 使用已经被判断为更新的失效列表 CRL 覆盖 CRL 存储单元 208 中所存储的失效列表 CRL_ST，并且该失效列表 CRL 充当所存储的失效列表 CRL_ST（步骤 S415）。当判断失效列表 CRL 比所存储的失效列表 CRL_ST 更旧时（步骤 S414），控制转移到步骤 S416。

接着，证书判断单元 211 从 CRL 存储单元 208 中读取所存储的失效列表 CRL_ST（步骤 S416），并通过判断从所读取的公钥证书 PKC 提取的证书识别符 ID_1 是否包含在所存储的失效列表 CRL_ST 中，来判断公钥证书 PKC 是否记录在所读取的所存储的失效列表 CRL_ST 中（步骤 S417）。

当判断结果为公钥证书被记录（步骤 S418）时，控制转移到步骤 S422。当判断结果为没有记录公钥证书（步骤 S418）时，签名验证单元 212 利用密钥解密密钥 KDK、公钥证书 PKC 和失效列表 CRL 来验证签名数据 SigCRL 的有效性（步骤 S419）。

当签名数据 SigCRL 的有效性验证失败时（步骤 S420），开关 213 被断开，从而不使该内容再现（步骤 S422）。由此，由再现设备 200 执行的再现操作结束。

相反地，当签名数据 SigCRL 的有效性验证成功时（步骤 S420），开关 213 被连通，且将解密内容 DCNT 输出到再现单元 214 以便于再现单元 214 再现解密内容 DCNT（步骤 S421）。由此，由再现设备 200 执行的再现操作完成。

1.7 其它修改实例

（1）在第一实施例中，为了实现其中经由记录介质传送失效列表 CRL 的机制，记录设备产生用于作为签名的标的的失效列表 CRL

的签名数据 SigCRL，并将所产生的签名数据 SigCRL 写道记录介质上；然而，本发明不限于此方案。

例如，可采取这样一种方案，其中，记录设备计算失效列表 CRL 的散列值，并产生该散列值的签名数据。

签名数据=Sig（SK_1，HASH（CRL））

这里 HASH（A）为通过对数据 A 执行散列函数 HASH 而获得的散列值。

或者，也可以采用一种方案，其中记录设备计算失效列表 CRL 的散列值，并对该散列值和媒介密钥执行 XOR（异或）操作，以产生作为操作的结果的签名数据。

签名数据=Sig（SK_1，（HASH（CRL）XOR（MK））

这样，记录设备产生用于失效列表 CRL 和所述内容的签名数据，或者产生用于失效列表 CRL 和各种密钥数据的签名数据。结果，由于将所产生的签名数据写入记录介质，所以能够防止对记录在记录介质上的失效列表的伪造和删除。

另外，在这些情况下，再现设备利用每种情况下相应的数据来执行签名验证。

（2）在第一实施例中，当将从外部获得的失效列表 CRL 与存储在设备内的失效列表 CRL 相比较以判断哪一个更新时，比较版本号；然而，本发明不限于该方案。

例如，在这样一个前提下，当失效列表 CRL 被更新时，失效列表 CRL 只是尺寸增加，可以判断尺寸较大的 CRL 较新。

以相似的方式，在这样的前提下，在失效列表 CRL 被更新时，失效设备的数量简单增加，通过比较所包含的失效设备的数量，可以判断具有较大数量的失效设备的 CRL 更新。

如上所述，可以采用任何方案，只要该方案能够从 CRL 中获得为了比较和判断哪一列表更新的信息。

（3）可以采用一种方案，其中，将最新版本的媒介密钥数据经由第二记录介质传送到记录设备。

将最新版本的媒介密钥数据记录在第二记录介质上。

记录设备在其中预存储媒介密钥数据块。当将其上记录有媒介密钥数据块的第二记录介质安装在记录设备上时，记录设备将存储在记录设备中的媒介密钥数据块与记录在第二记录介质上的媒介密钥数据块相比较，以判断哪一个更新。当记录在第二记录介质上的媒介密钥数据块比存储在记录设备中的媒介密钥数据块更新时，记录设备用记录在第二记录介质上的媒介密钥数据块覆盖存储在记录设备中的媒介密钥数据块。

这里，将表示版本的版本号附加于每一媒介密钥数据块。记录设备使用该版本号来比较各媒介密钥数据块，并判断哪一个更新。

还可以采用一种方案，其中，根据媒介密钥数据块计算的媒介密钥的一部分为版本号，且使用随机号来产生媒介密钥的剩余部分。记录设备从每一媒介密钥数据块中提取作为媒介密钥一部分的版本号，并使用所提取的版本号来比较各媒介密钥数据块并判断哪一个更新。

此外，在这样一个前提下，即，当媒介密钥数据块更新时，媒介密钥数据块中的失效设备的数量简单增加，换句话说，其中加密了值“0”而不是媒介密钥 MK 的加密媒介密钥的数量简单增加，则记录设备可使用包含于每一媒介密钥数据块中的失效设备的数量来比较媒介密钥数据块并判断哪一个更新。

此外，可以采用一种方案，其中，将示出媒介密钥数据块何时产生的时间信息（年、月、日、小时、分钟、秒）贴附于每一媒介密钥

数据块，且记录设备使用该时间信息以比较各媒介密钥数据块并判断哪一个更新。

如到目前为止所述的，可以采用任何方案，只要该方案能够比较各媒介密钥数据块以正确判断哪一个更新。

另外，可以采用一种方案，其中，将认证中心 CA 的签名贴附到每一媒介密钥数据块以便于防止伪造。记录设备通过验证该签名来验证每一媒介密钥数据块的有效性。

（4）可以采用一种方案，其中，当另外将第二加密内容写到其上已经记录有媒介密钥数据块、加密内容等的记录介质上时，记录设备通过根据存储在记录介质上的媒介密钥数据块或根据记录在记录介质上的媒介密钥数据块对从外部（例如内容服务器设备）获取的内容加密，来产生第二加密内容，并将所产生的第二加密内容写到记录介质上。

在这种情况下，有可能在记录介质上存在多个媒介密钥数据块、多个公钥证书和多个失效列表 CRL。

此外，可以采用一种方案，其中，记录设备将记录在记录介质上的媒介密钥数据块与存储在记录设备中的媒介密钥数据块相比较以判断哪一个更新，且当存储在记录设备中的媒介密钥数据块较新时，记录设备通过对记录在记录介质上的加密内容解密而产生解密内容，以及通过根据存储在记录介质中较新的媒介密钥来对所产生的解密内容加密而产生再加密内容，使得将所产生的再加密内容写到记录介质上。此时，可以删除记录在记录介质上的加密内容。

（5）在第一实施例中，通过对密钥加密密钥 KEK 使用数字签名功能来产生签名数据块，然而，本发明并不限于此方案。

例如，可以采用一种方案，其中通过对用于内容 CNT 整体的散

列值使用数字签名功能来产生签名数据块。

签名数据=Sig（SK_1，HASH（CNT））

更为具体地，采用签名的目的是验证记录内容的记录设备的有效性；因此，作为签名的目标的数据可以是任何信息，只要该数据为涉及该内容或涉及在加密中所使用的密钥的信息。

（6）在第一实施例中，如图 2 中所示，将记录设备 100 构造成为一个主体，该主体包括：器件密钥存储单元 101、媒介密钥数据存储单元 102、密钥计算单元 103、密钥计算单元 104、加密单元 105、加密单元 106、私钥存储单元 107、证书存储单元 108、CRL 存储单元 109、签名产生单元 110、驱动单元 111、控制单元 112、以及发送和接收单元 113；然而，本发明不限于此。

例如，记录设备可以由驱动设备和处理设备构成，驱动设备作为一个主体包括器件密钥存储单元 101、媒介密钥数据存储单元 102、密钥计算单元 103、密钥计算单元 104、加密单元 105、加密单元 106、私钥存储单元 107、证书存储单元 108、CRL 存储单元 109、签名产生单元 110、驱动单元 111 和控制单元 112 的一部分；而处理设备作为一个主体包括控制单元 112 的另一部分与发送和接收单元 113。在该方案中，将记录设备分成（i）执行在记录媒介写和读数据以及加密的驱动设备与（ii）执行其它处理的处理设备。

可以采用一种方案，其中，器件密钥存储单元 101、媒介密钥数据存储单元 102、私钥存储单元 107、证书存储单元 108 和 CRL 存储单元 109 处于外部记录设备的记录区中。这里，外部记录设备的一个实例为便携式安全存储卡。

此外，在第一实施例中，如图 4 中所示，再现设备 200 被构造成为一个主体，该主体包括：器件密钥存储单元 201、密钥计算单元 202、

密钥计算单元 203、解密单元 204、解密单元 205、CA 公钥存储单元 206、证书验证单元 207、CRL 存储单元 208、CRL 验证单元 209、CRL 比较更新单元 210、证书判断单元 211、签名验证单元 212、开关 213、再现单元 214、控制单元 215、输入单元 216、显示单元 217 和驱动单元 218；然而本发明不限于该方案。

再现设备可以由驱动设备和处理设备构成，驱动设备作为一个主体包括器件密钥存储单元 201、密钥计算单元 202、密钥计算单元 203、解密单元 204、解密单元 205、CA 公钥存储单元 206、证书验证单元 207、CRL 存储单元 208、CRL 验证单元 209、CRL 比较更新单元 210、证书判断单元 211、签名验证单元 212、开关 213 和驱动单元 218；而处理设备作为一个主体包括：再现单元 214、控制单元 215、输入单元 216 和显示单元 217。在该方案中，将再现设备分为（i）执行在记录媒介写和读数据以及加密的驱动设备与（ii）执行其它处理的处理设备。

可以采用一种方案，其中，器件密钥存储单元 201，CA 公钥存储单元 206 和 CRL 存储单元 208 处于外部记录设备的记录区中。这里，外部记录设备的一个实例为便携式安全存储卡。

到此为止的阐述表明，以下方案是可以接收的，记录设备和再现设备各自分别用彼此分离的数据读/写设备和处理设备构成，而不是构造成一个主体。在这种情况下，数据读/写设备执行加密是可行的。或者，处理设备执行加密也是可行的。

（7）在第一实施例中，存在一种方案，其中，媒介密钥数据 MDATA、加密内容密钥 ECK、加密内容 ECNT、签名数据 SigCRL、失效列表 CRL 和公钥证书 PKC 都被记录在一个记录介质上；然而，本发明不限于此方案。

例如，可以采用一种方案，其中，记录设备 100 将部分数据，如签名数据 SigCRL、失效列表 CRL 和公钥证书 PKC，记录在不同于记录介质 120 的记录介质上，并且记录介质 120 和其它记录介质都被分配。

此外，可以采用一种方案，其中，记录设备 100 通过因特网连接于网络，这样经由网络来分配一部分数据。再现设备 200 也连接于网络，以便于经由网络从记录设备 100 获得这部分数据。

如上所述，可以采用一种方案，其中，媒介密钥数据 MDATA、加密内容密钥 ECK、加密内容 ECNT、签名数据 SigCRL、失效列表 CRL 和公钥证书 PKC 被记录在一个或多个记录媒介上并被分配，或者记录在一个或多个记录媒介上并由网络分配。

（8）在第一实施例中，内容被加密并根据器件密钥来对加密内容解密；然而，本发明不限于该方案。

例如，可以采用一种方案，其中，记录设备和再现设备各自获得一个使用条件，并根据该使用条件来控制记录和再现。这里，使用条件为内容附带的管理信息，例如日期、时间以及所允许的对该内容记录和再现的次数。

（9）在第一实施例中，再现设备从 CRL 存储单元中读取失效列表 CRL 用于进行比较以判断较新的列表，将较新的失效列表 CRL 存储到 CRL 存储单元中，并且在需要检验是否公钥证书被登记时再次读取失效列表 CRL；然而，本发明不限于该方案。

例如，可以采用一种方案，其中，再现设备不比较失效列表 CRL 以判断哪一个较新，且不将被判断为较新的失效列表 CRL 存储到 CRL 存储单元中，而在判断在失效列表 CRL 中是否登记有公钥证书之后，将从记录介质 120 中读取的失效列表 CRL 存储到 CRL 存储单

元中。

其中执行签名验证、CRL 验证和公钥证书判断的顺序不限于在第一实施例中所描述的顺序。再现设备可以以各种顺序执行签名验证、CRL 验证和公钥证书判断以控制内容的再现。

（10）下面的方案是可接受的，记录设备和再现设备各自具有电子水印处理单元，该单元可被操作以产生和嵌入电子水印。

例如，记录设备可以在其中存储识别该记录设备的设备 ID，且当记录设备将内容记录在记录介质上时，记录设备将设备 ID 作为电子水印嵌入该内容中。

在这种情况下，如果向其中嵌入作为电子水印的设备 ID 的内容非法进入流通，则通过从该内容中提取被嵌入的设备 ID，能够识别记录该内容的记录设备。

此外，以相同的方法，在再现工艺期间，再现设备将该再现设备的设备 ID 作为电子水印嵌入记录在记录介质上的内容中也是可行的。在这种情况下，如果向其中嵌入作为电子水印的设备 ID 的内容非法进入流通，则通过从内容中提取被嵌入的设备 ID，能够识别再现该内容的再现设备。

（11）可以采用一种方案，其中，内容供给系统包括器件密钥发现设备，在发现包含被公开的器件密钥的非法设备时，该设备可被操作以识别存储在其中的器件密钥。该非法设备具有与再现设备 200 相同的结构。

如图 8 中所示，器件密钥发现设备产生 n 个记录媒介块，诸如 MD1、MD2、MD3、…和 MDn。应该注意的是，在图 8 中，从图中省略除媒介密钥数据块之外的数据。

记录媒介块 MD1、MD2、MD3、…MDn 各自具有记录在其上的

数据，除了下述方面之外，该数据与图 3 中示出的记录在记录介质 120 上的数据相同：

（a）在记录于各记录媒介 MD1、MD2、MD3、…MDn 上的失效列表中没有记录失效公钥证书。换句话说，失效列表 CRL 不包含公钥证书的识别符。

（b）记录于记录媒介 MD1、MD2、MD3、…MDn 上的媒介密钥数据块与记录在记录介质 120 上的媒介密钥数据块不同。图 8 中示出记录于记录媒介 MD1、MD2、MD3、…MDn 上的媒介密钥数据块的实例。

（b-1）记录于记录媒介 MD1 上的媒介密钥数据块包括 n 组加密媒介密钥和设备号。该设备号与第一实施中所描述的相同。

通过利用器件密钥 DK_1 对媒介密钥 MK 执行加密算法 E1 来产生第一加密媒介密钥。

通过分别利用器件密钥 DK_2、DK_3、…DK_n 对值“0”执行加密算法 E1 来产生第二、第三、…第 n 个加密媒介密钥。

（b-2）记录在记录介质 MD2 上的媒介密钥数据块包括 n 组加密媒介密钥和设备号。设备号与在第一实施例中描述的相同。

通过利用器件密钥 DK_1 对值“0”执行加密算法 E1 来产生第一加密媒介密钥。

通过利用器件密钥 DK_2 对媒介密钥 MK 执行加密算法 E1 来产生第二加密媒介密钥。

通过分别利用器件密钥 DK_3、…、DK_n 对值“0”执行加密算法 E1 来产生第三、…、第 n 加密媒介密钥。

（b-3）这同样适用于记录媒介 MD3、…、MDn。

记录在记录介质 Mdi 上的媒介密钥数据块包括 n 组加密媒介密

钥和一个设备号，其中 i 为满足 1≤i≤n 的整数。设备号与在第一实施例中描述的相同。

通过利用器件密钥 DK_i 对值“0”执行加密算法 E1 来产生第 i 加密媒介密钥。

其它加密媒介密钥的每一个是通过利用相应的器件密钥对媒介密钥 MK 执行加密算法 E1 来产生的。

接着，操作者依序将记录媒介 MD1、MD2、MD3、…、MDn 一个接一个地安装在非法设备上，并命令非法设备再现内容。

这样，这 n 个记录媒介块的每一个在非法设备上被试着再现。

当非法设备正确地再现内容时，从所安装的记录介质来判断，能够识别期望被存储在非法设备中的器件密钥。

例如，当记录介质 MD1 被安装时，如果非法设备正确再现内容，则存储在该非法设备中的器件密钥为 DK_1。

一般而言，当记录介质 MDi 被安装时，如果非法设备正确再现内容，则存储在非法设备中的器件密钥为 DK_i。

非法设备具有与再现设备 200 相同的结构，且如图 6 和 7 中所示操作。因此，仅当记录媒介 MD1、MD2、MD3、…、MDn 中的一个被安装时，非法设备正确再现内容。

（12）在第一实施例中，作为产生签名的算法，使用具有附录的签名。具有附录的签名意味着将签名附属到作为签名目标的数据块上；然而，本发明不限于该方案。

例如，使用具有信息还原的签名来代替具有附录的签名是可行的。应该注意的是，在专利文献 3 中公开了具有信息还原的签名。

当使用具有信息还原的签名时，签名器能够将保密信息嵌入将要产生的签名中，且验证器能够在验证签名之后获得该保密信息。通过

使用该技术特征，记录设备对保密信息和密钥数据（例如内容密钥）执行 XOR（异或）操作，并通过对操作结果使用具有信息还原的签名来产生签名数据块。在这种情况下，再现设备执行签名验证，且当验证成功时，再现设备获得该操作结果，并对存储在再现设备中的保密信息和操作结果执行 XOR（异或）操作以获得密钥数据（例如，内容密钥）。

应该注意的是，要对保密信息和密钥数据执行的操作不必限定为 XOR 操作。也可以执行其它操作，或者通过将其中合并有保密信息和密要数据的数据块作为输入值来使用散列函数值的输出。

另外，保密信息作用于其上的信息不必为内容密钥。如果该信息为诸如密钥加密密钥的另一类密钥也是可接受的。

如上所述，可以采用任何方案，只要该方案就阻止内容再现，除非可以得到作为签名验证结果而能够被得到的保密信息。

当如此使用具有信息还原的签名时，有必要采用签名验证，以便于再现内容。

（13）在第一实施例中，从记录设备的外部资源获得内容密钥和内容；然而，本发明不限于该方案。

例如，可以采用一种方案，其中，将内容密钥和内容以如此方式预存储在内容记录设备中，使它们彼此相应。或者，可以采用一种方案，其中每当需要使用内容密钥时在记录设备中产生内容密钥。

（14）在第一实施例中，根据各种验证和判断的结果来被控制的开关 213 设置在解密单元 205 和再现单元 214 之间，且可被操作以控制再现单元 214 以将解密内容输出或不输出；然而，本发明并不限于该方案。

例如，可以采用一种方案，其中，开关 213 设置在解密单元 204

和解密单元 205 之间，且可被操作以控制解密单元 205 以使解密内容密钥输出或不输出。

或者，也可以采用一种方案，其中，该开关设置在密钥计算单元 203 和解密单元 204 之间，且可被操作以控制解密单元 204，使得密钥解密密钥 KDK 被输出或不被输出。

如上所述，可以采用任何一种方案，只要该方案能够根据验证结果来最终控制内容的再现。此外，开关 213 不一定是物理开关。开关 213 由软件构成也是可行的，只要它能够控制再现。

此外，可以采用一种方案，其中，密钥计算单元 202 判断所产生的作为探测信息的解密媒介密钥 y 是否为值“0”，且当判断解密媒介密钥 y 为值“0”时，密钥计算单元 202 命令开关 213 不向再现单元 214 输出解密内容 DCNT。

还可以采用一种方案，其中，当判断解密媒介密钥 y 为值“0”时，密钥计算单元 202 命令密钥计算单元 203、解密单元 204 和解密单元 205 的全部或一部分不产生密钥解密密钥、不产生解密内容密钥、或不产生解密内容。

此外，可以采用一种方案，其中，当判断解密媒介密钥 y 为值“0”时，密钥计算单元 202 通知控制单元 215 解密媒介密钥 y 为值“0”，以便于已经接收到该信息的控制单元 215 命令再现设备 200 的其它构件停止对加密内容的解密和再现。

（15）在第一实施例中，使用由诸如媒介密钥、密钥加密密钥和内容密钥的三个分级层构成的加密系统；然而，本发明不限于该方案。

例如，可以采用一种方案，其中，省略内容密钥，并直接使用密钥加密密钥对内容加密。或者，可以采用一种方案，其中，引入另一密钥以便于增加一分级层。

（16）可以采用一种方案，其中，记录设备或再现设备通过由因特网表示的网络来获得最新版本的媒介密钥数据和失效列表 CRL，从而更新存储在记录设备或再现设备中的数据。

（17）在第一实施例中，记录设备将失效列表 CRL 记录在记录介质上；然而，本发明不限于该方案。

例如，可以采用一种方案，其中再现设备通过网络获得失效列表 CRL，而记录设备不将失效列表 CRL 记录到记录介质上。

（18）在第一实施例中，记录设备对要记录到记录介质上的内容或涉及内容的信息产生签名数据块，然后将所产生的签名数据块记录到记录介质上；然而，本发明不限于该方案。

例如，记录设备不产生签名也是可行的。在这种情况下，可以采用一种方案，其中，记录设备根据存储在记录设备中的媒介密钥数据块和介质固有号来对内容加密，然后将在加密中使用的媒介密钥数据块和所加密的内容记录到记录介质上。在这种情况下，再现设备从记录介质中读取媒介密钥数据块、介质固有号和加密内容，然后根据媒介密钥数据块和介质固有号来对内容解密。

（19）在第一实施例中，记录设备通过根据媒介密钥和介质固有号产生密钥加密密要来实现媒介绑定（media bind）；然而，本发明不限于该方案。

例如，可以采用一种方案，其中记录设备根据媒介密钥和介质固有号来产生认证符，并将所产生的认证符记录到记录介质上从而实现媒介绑定。在这种情况下，再现设备以相似的方式根据媒介密钥和介质固有号来产生认证符，并判断记录在记录介质上的认证符是否与所产生的认证符相匹配，以便于控制内容的再现。

例如，上面产生认证符的方法如下：

对媒介密钥、介质固有号和加密内容密钥的合并值执行散列函数；并将所获得的散列值或散列值的特定部分作为认证符。

（20）在第一实施例中，一个记录介质与一个内容供给系统相对应；然而，本发明不限于该方案。下述方案也是可能的：

存在多个内容供给系统，例如，其中之一为用于供给电影内容的系统；另一内容供给系统为用于供给计算机软件的系统，而又一内容供给系统为供给音乐的系统。这样，取决于要被供给的内容的种类来使用不同的内容供给系统中的每一个。

或者，下面的方案是可能的：一个内容供给系统为用于供给来自电影提供公司 A 的电影内容的系统。另一内容供给系统为用于供给来自电影提供公司 B 的电影内容的系统。再一内容供给系统为用于供给来自电影提供公司 C 的电影内容的系统。这样，取决于内容的提供着来使用不同内容供给系统的每一个。

下面描述其中在各自不同的多个内容供给系统中使用一个记录介质的机制。

在记录介质的不可重写区中，除了记录介质固有的介质固有号之外，预存储密钥失效数据块。在这种情况下，第一内容供给系统通过利用预存储在不可重写区中的密钥失效数据块来实现数字作品保护的机制。第二内容供给系统通过如第一实施例所描述的方案来实现数字作品保护的机制。

图 9 示出记录在记录介质上的这种数据的实例。

记录介质 700 具有不可重写区 710 和可重写区 720。不可重写区 710 包括用于第一内容供给系统的密钥失效数据记录区 711 和固有号记录区 712。可重写区 720 包括用于第二内容供给系统的密钥失效数据记录区 721、第一加密内容密钥记录区 722、第二加密内容密钥记

录区 723 和其它加密内容密钥记录区（未在附图中示出）。

这里，用于第二内容供给系统的密钥失效数据记录区 721 相应于第一实施例中的媒介密钥数据记录区 122。此外，将基于用于第一内容供给系统的密钥失效数据块而被加密的数据记录在第一加密内容密钥记录区 722 中。以相同的方式，将基于用于第二内容供给系统的密钥失效数据块而被加密的数据记录在第二加密内容密钥记录区 723 中。

如到此为止所述，在其中一个记录介质支持多个内容供给系统的情况下，不需要每一系统具有介质固有号。对于一个记录介质，一个介质固有号是充足的。多个内容供给系统共同使用一个介质固有号或一个介质固有号的一部分是可行的。

这里，“使用一个介质固有号的一部分”意味着，例如，在 128 位介质固有号的情况下，（i）使用后 96 位作为介质固有号，而不使用前 32 位；或（ii）用零全部替换介质固有号的前 32 位并使用该结果作为 128 位介质固有号。

如上所述，通过共预存储在多个内容供给系统中的记录介质上的介质固有号，可以实现一个系统，即使对已经被出售和使用且在其上仅记录介质固有号的记录介质，该系统也能够保护数字作品版权。另外，由于不需要对每一系统记录介质固有号，所以能够减小不可重写区的大小。

如上所述，本发明为一种数字作品保护系统，该系统对至少第一和第二内容供给系统提供用于保护数字作品的机制。

记录介质包括只读不可重写区和允许数据的读和写的可重写区。将记录介质固有的介质固有号和用于第一内容供给系统的密钥失效数据块预存储在不可重写区中。

第一内容供给系统由记录设备和多个再现设备构成，记录设备可被操作以对内容加密并将加密内容写到记录介质上，而每一再现设备可被操作以试图对记录在记录介质上的加密内容解密。多个再现设备中的一个或多个被失效。记录在记录介质的不可重写区中的密钥失效数据块表示一个或多个被失效的再现设备的各自的密钥。

记录设备包括：加密单元，可被操作以利用记录在不可重写区中的失效数据块对内容加密；和写入单元，可被操作以将所产生的加密内容写入记录介质的可重写区中。

再现设备的每一个包括：读取单元，可被操作以读取记录在记录介质中的不可重写区的密钥失效数据块和记录在记录介质上的加密内容；判断单元，可被操作以利用所读取的密钥失效数据块判断是否允许对加密内容解密；和解密单元，当不允许解密时可被操作以阻止加密内容被解密，而当允许解密时对加密内容解密以产生解密内容。

此外，第二内容供给系统由记录设备和多个再现设备构成，记录设备可被操作以对内容加密并将加密内容写到记录介质上，而每一再现设备可被操作以对记录在记录介质上的加密内容解密。多个再现设备中的一个或多个被失效。

记录设备包括：存储单元，在其中存储包含多个加密媒介密钥的媒介密钥数据块，该媒介密钥数据块是通过（i）对每一未失效的再现设备，分别利用未失效的再现设备的器件密钥对媒介密钥加密，和（ii）对每一失效的再现设备，分别利用失效的再现设备的器件密钥对预定的探测信息加密而产生的；读取单元，可被操作以从记录介质的不可重写区中读取介质固有号；产生单元，可被操作以根据所读取的介质固有号和媒介密钥来产生加密密钥；加密单元，可被操作以根据所产生的加密密钥对作为数字数据块的内容加密，以便于产生加密

内容；读取单元，可被操作以从存储单元中读取媒介密钥数据块；和写入单元，可被操作以将所读取的媒介密钥数据块和所产生的加密内容写入记录介质的可重写区中。

每一再现设备包括：读取单元，可被操作以从记录在记录介质的可重写区中的媒介密钥数据块中读取与再现设备相应的一个加密媒介密钥；第一解密单元，可被操作以利用再现设备的器件密钥对所读取的加密媒介密钥解密，以便于产生解密媒介密钥；控制单元，可被操作以判断所产生的解密媒介密钥是否为探测信息，且当所产生的解密媒介密钥为探测信息时，阻止记录在记录介质上的加密内容被解密，而当所产生的解密媒介密钥不是探测信息时，允许该加密内容被解密；和第二解密单元，当允许解密加密内容时，从记录介质中读取加密内容，并根据所产生的解密媒介密钥来对所读取的加密内容解密，以便于产生解密内容。

1.8 概要

如上所述，本发明提供一种数字作品保护系统，该系统包括：记录设备，可被操作以对内容加密并记录加密内容；记录介质，在其上记录加密内容；和再现设备，可被操作以从记录介质中读取加密内容并对加密内容解密。

记录设备在其中存储失效数据块，用于失效存储在特定设备中的密钥，根据该失效数据块对内容加密，将失效数据块和加密内容记录到记录介质上，且还为该内容和涉及内容加密的数据产生签名，并将所产生的签名记录到记录介质上。

记录介质具有用于唯一识别记录介质的识别号，该识别号存储在不能由用户重写的区中，且还具有记录在其上的失效数据块、加密内

容和所产生的签名。

可以采用一种方案，其中，再现设备从记录介质中读取失效数据块、加密内容和签名，根据失效数据块对内容解密，并根据签名的有效性验证的结果来控制解密内容的再现。

这里，在该数字作品保护系统中，可以采用一种方案，其中，记录介质具有记录在其上的失效数据块和加密内容；而通过除该记录介质之外的另一记录介质或通信介质来分配签名。

这里，在该数字作品保护系统中，可以采取这样的方案，即，记录设备通过一组两个或多个设备执行这种处理，且这些设备各自分担一部分处理。

同样，在该数字作品保护系统中，可以采取这样的方案，再现设备通过一组两个或多个设备来执行这种处理，且这些设备各自分担部分处理。

此外，在该数字作品保护系统，记录设备根据内容使用的条件来记录内容是可行的。

此外，在该数字作品保护系统中，再现设备根据内容使用条件来再现内容是可行的。

此外，在该数字作品保护系统中，可以采取这样的方案，记录设备在其中存储唯一识别该记录设备的设备识别号，并且在记录内容时将设备识别号作为电子水印嵌入内容中。

而且，在该数字作品保护系统中，可以采取这样的方案，再现设备在其中存储唯一识别该再现设备的设备识别号，并且在再现内容时将设备识别号作为电子水印嵌入内容中。

这里，这样的方案是可接受的，数字作品保护系统包括：密钥发现设备，在发现非法设备时，该设备可被操作以判断在非法设备中存

储何类密钥。

本发明还提供记录设备，该设备可被操作以对内容加密并记录加密内容，其中，记录设备在其中存储用于失效存储在特定设备中的密钥的失效数据块，根据失效数据块对内容加密，将失效数据块和加密内容记录在记录介质上，且还产生用于该内容或涉及内容加密的数据的签名，并将所产生的签名记录到记录介质上。

这里，记录设备除根据失效数据块之外还根据唯一识别记录介质的识别号来加密内容是可行的。

这里，记录设备将相应于在产生签名中使用的私钥的公钥记录到记录介质上是可行的。

而且，记录设备产生用于公钥失效列表的签名是可行的，该公钥失效列表是该签名的目标。

而且，以下方案是可行的，在失效数据块存在于在其上记录有内容的记录介质上的情况下，记录设备可被操作以将存储在记录设备中的失效数据块与存在于记录介质上的失效数据块相比较，以确定哪一个更新，并在其中存储较新的失效数据块。

而且，以下方案是可行的，记录设备通过比较失效数据块的尺寸并将尺寸较大的失效数据块判定为较新的数据块，来比较失效数据块以确定哪一个更新。

此外，以下方案是可行的，记录设备通过比较已经被失效的密钥数量并将失效密钥数量较大的失效数据块判定为较新的数据块，来比较失效数据块以确定哪一个较新。

还可以接受这样的方案，记录设备通过比较失效数据块产生的日期或版本号来比较失效数据块以确定哪一个更新，并且该产生日期和版本号被保护以防止伪造。

这里，可以采用一种方案，其中，在（i）失效数据块和加密内容都存在于其上记录有内容的记录介质上；(ii)存储在记录设备中的另一失效数据块比记录在记录介质上的失效数据块新的情况下，记录设备一旦以相同的方式根据记录在记录介质上的失效数据块对记录在记录介质上的加密内容解密，怎根据存储在记录设备中的失效数据块对解密内容再加密。

这里，以下方案是可接受的，记录设备在记录设备内产生保密信息，根据保密信息和失效数据块对内容加密，并且，将该保密信息作为要嵌入到签名中的信息来产生签名。

此外，本发明提供再现设备，该设备可被操作以从记录介质中读取加密内容并对加密内容解密，其中，再现设备从记录介质中读取失效数据块、加密内容以及签名，根据失效数据块对内容解密，并根据签名的有效性验证的结果来控制解密内容的再现。

这里，以下方案是可接受的，再现设备除根据失效数据块之外还根据唯一识别记录介质的识别号来对加密内容解密。

这里，以下方案也是可接受的，再现设备在其中存储公钥失效列表，判断用于签名的真实性验证的公钥是否记录在公钥失效列表中，并根据判断结果控制解密内容的再现。

这里，以下方案是可接受的，在失效列表存在于记录介质上的情况下，再现设备可被操作以将存储在再现设备中的失效列表与存在于记录介质上的失效列表相比较，以确定哪一个较新，且在其中存储较新的失效列表。

此外，以下方案是可接受的，再现设备通过比较失效列表的尺寸并将尺寸较大的失效列表判定为较新的失效列，来比较失效列表以确定哪一个较新。

此外，以下方案是可接受的，再现设备通过比较已经失效的公钥的数量并将失效公钥数量较大的失效列表判定为较新的失效列，来比较失效列表以确定哪一个较新。

以下方案也是可接受的，再现设备通过验证签名的有效性来获得保密信息，并根据所获得的保密信息和失效数据块来对加密内容解密。

本发明还提供记录介质，该记录介质可被操作以在其上记录加密内容，其中，该记录介质具有用于唯一识别该记录介质的识别号，该识别号存储在该记录介质中的用户不可重写区中，且还具有记录在其上的失效数据块、加密内容和签名。

这里，以下方案是可接受的，记录介质在其上记录内容，根据失效数据块和识别号该内容被加密。

这里，还可接受的是，记录介质具有记录在其上的与在签名产生中使用的私钥相对应的公钥。

还可以采用一种方案，其中，在两个或多个记录设备向记录介质上写入数据的情况下，记录介质具有记录在其上的两个或多个失效数据块和两个或多个公钥。

如上所述，在第一实施例中，由于记录设备基于根据媒介密钥数据块计算的媒介密钥来对内容加密，并将加密内容与记录设备的公钥证书和所产生的签名一起记录，所以即使密钥失效信息没有记录在记录介质的不可重写区中，也能够获得密钥失效和媒介绑定，并实现对由于使用非法设备记录和再现内容而引起的数字作品侵权的阻止。

更为具体地，在存在合法记录设备和非法再现设备的情况下，合法记录设备根据表示非法再现设备被失效的媒介密钥数据块对内容加密，并将加密内容记录在记录介质上。插入记录介质的非法再现设

备不能对来自记录在记录介质上的媒介密钥数据块的媒介密钥解密。因此，能够防止非法再现设备再现内容。

此外，在存在非法记录设备和合法再现设备的情况下，非法记录设备根据旧的媒介密钥数据块对内容加密，并将加密内容记录到记录介质上，根据该媒介密钥数据，记录设备不被失效。此时，记录介质还记录记录设备的公钥证书和所产生的签名数据块。插入了记录介质的合法再现设备能够对来自所记录的媒介密钥数据块的媒介密钥解密；然而，由于在再现内容之前再现设备判断记录设备的公钥证书是否记录在失效列表 CRL 中，所以如果该内容是由记录在失效列表 CRL 中非法记录设备记录的，则再现设备能够阻止内容再现。

2. 第二实施例

下面描述作为本发明另一实施例的内容供给系统 20。

2.1 内容供给系统 **20** 的结构

内容供给系统 20 的结构与内容供给系统 10 的结构相似，且，如图 10 中所示，包括分配位置设备（distributing station apparatus）1400、内容服务器设备 1500、记录设备 1100 和再现设备 1200a、1200b、1200c、1200d、1200e、…。

与第一实施例相同，已经失效一个或多个再现设备。

2.2 分配位置设备 **1400**

分配位置设备 1400 包括信息存储单元 1401、控制单元 1402、输入单元 1403、显示单元 1404、以及发送和接收单元 1405（未在附图中示出）。

更为具体地，与第一实施例中的内容服务器设备 500 相同，分配

位置设备 1400 为一计算机系统，该系统包括微处理器、ROM、RAM、硬盘单元、通信单元、显示单元、键盘、鼠标等。RAM 和硬盘单元各自在其中存储计算机程序。在微处理器根据计算机程序操作时分配位置设备 1400 的各构件实现它们的功能。

发送和接收单元 1405 通过因特网 40 连接于记录设备 1100，并在记录设备 1100 与控制单元 1402 之间执行信息的发送和接收。

信息存储单元 1401 在其中以如此方式预存储密钥失效数据 RDATA 和版本号 VR 以使它们彼此对应。

密钥失效数据 RDATA 与第一实施例中的媒介密钥数据 MDATA 相同。因此省略详细阐述。

版本号 VR 为表示与版本号 VR 相应的密钥失效数据的产生的信息。

控制单元 1402 经由因特网 40 与发送和接收单元 1405 从记录设备 1100 接收控制单元 1402 应该获得密钥失效数据 RDATA 的请求。一旦接收该请求，控制单元 1402 从信息存储单元 1401 中读取密钥失效数据 RDATA 和版本号 VR，并将所读取的密钥失效数据 RDATA 和版本号 VR 经由发送和接收单元 1405 以及因特网 40 发送到记录设备 1100。

输入单元 1403 接收来自分配位置设备 1400 的操作者的指令，并将所接受的指令输出到控制单元 1402。

显示单元 1404 在控制单元 1402 的控制显示各种信息。

2.3 内容服务器设备 1500

内容服务器设备 1500 具有与第一实施例的内容服务器设备 500 相同的结构。因此省略描述。

2.4 记录设备 1100

如图 11 中所示，记录设备 1100 包括：器件密钥存储单元 1101、失效数据存储单元 1102、密钥计算单元 1103、加密单元 1105、加密单元 1106、认证符产生单元 1104、分配单元 1107、比较单元 1108、控制单元 1109、驱动单元 1110 以及发送和接收单元 1111。

更为具体地，与记录设备 100 相同，记录设备 1100 为一计算机系统，该系统包括微处理器、ROM、RAM、硬盘单元等。RAM 和硬盘单元各自在其中存储计算机程序。在微处理器根据计算机程序操作时记录设备 1100 实现其功能。

（1）器件密钥存储单元 1101

器件密钥存储单元 1101 在其中以如此方式保密地存储器件密钥 DK_1 以使得器件密钥 DK_1 不被外部设备访问。器件密钥 DK_1 为对于记录设备 1100 唯一的密钥。

（2）失效数据存储单元 1102

失效数据存储单元 1102 具有用于存储从分配位置设备 1400 中获取的密钥失效数据 RDATA 和版本号的区域。

（3）密钥计算单元 1103

密钥计算单元 1103 具有与第一实施例中的密钥计算单元 193 相同的结构。

密钥计算单元 1103 从密钥数据存储单元 1102 中读取密钥失效数据 RDATA，并从器件密钥存储单元 1101 中读取器件密钥 DK_1。然后，同密钥计算单元 103 一样，密钥计算单元 1103 利用所读取得器件密钥 DK_1 对所读取的密钥失效数据 RDATA 执行解密算法 D1，以便于产生媒介密钥 MK，并将所产生的媒介密钥 MK 输出到认证符产生单元 1104 和加密单元 1105。

（4）加密单元 1105

加密单元 1105 经由发送和接收单元 1111 接收来自内容服务器设备 1500 的内容密钥 CK，并接收来自密钥计算单元 1103 的媒介密钥 MK。

接着，加密单元 1105 利用所接收的媒介密钥 MK 对所接收的内容密钥 CK 执行加密算法 E2，以便于产生加密内容密钥 ECK。

加密内容密钥 ECK=E2（MK，CK）

然后加密单元 1105 通过驱动单元 1110 在记录介质 1300 上的加密内容文件 1320 内保留密钥记录单元 1323，并且还将所产生的加密内容密钥 ECK 经由驱动单元 1110 写入密钥记录单元 1323。

加密单元 1105 还向认证符产生单元 1104 输出所产生的加密内容密钥 ECK。

（5）加密单元 1106

加密单元 1106 经由发送和接收单元 1111 接收来自内容服务器设备 1500 的内容密钥 CK 和内容 CNT，并利用所接收的内容密钥 CK 对所接收的内容 CNT 进行加密算法 E3，以便于产生加密内容 ECNT。

加密内容 ECNT=E3（CK，CNT）

然后加密单元 1106 通过驱动单元 1110 在记录介质 1300 上的加密内容文件 1320 内保留内容记录单元 1324，且还将所产生的加密内容 ECNT 经由驱动单元 1110 写入内容记录单元 1324。

（6）认证符产生单元 1104

认证符产生单元 1104 接收来自密钥计算单元 1103 的媒介密钥 MK，接收来自加密单元 1105 的加密内容密钥 ECK，并从记录介质 1300 上的介质固有号记录区 1301 中读取介质固有号 MID。

接着，认证符产生单元 1104 将所接收的媒介密钥 MK、所读取

的介质固有号 MID、所接收的加密内容密钥 ECK 按照上述顺序合并，以便于产生合并数据块，并通过对所产生的合并数据块执行单向函数 F 来产生认证符 MAC（信息认证码）。

MAC=F（MK||ECK||MID）

这里，F（A）表示通过对数据 A 执行单向函数 F 而获得的值。单向函数 F 的一个实例为散列函数 SHA-1。

接着，认证符产生单元 1104 通过驱动单元 1110 在记录介质 1300 上的加密内容文件 1320 内保留认证符记录单元 1322，并通过驱动单元 1110 将所产生的认证符 MAC 写入认证符记录单元 1322。

当再现设备 1200 判断内容的真实性时，使用如上产生的认证符 MAC。

（7）分配单元 1107

对于记录在记录介质 1300 上的密钥失效数据 RDATA，分配单元 1107 产生唯一识别记录介质 1300 上的密钥失效数据 RDATA 的密钥失效数据识别符 RID。分配单元 1107 通过驱动单元 1110 在记录介质上的加密内容文件 1320 内保留识别符记录单元 1321，并通过驱动单元 1110 将所产生的密钥失效数据识别符 RID 写入识别符记录单元 1321 中。

应该注意的是，稍后将描述由分配单元 1107 使用的用于分配密钥失效数据识别符 RID 的具体方法。

（8）比较单元 1108

比较单元 1108 根据控制单元 1109 的指令来通过驱动器 1110 检验密钥失效数据文件是否存在于记录介质 1300 上。比较单元 1108 还接收来自驱动单元 1110 的表示密钥数据文件是否存在的存在信息。

当存在信息表明没有密钥失效文件存在于记录介质 1300 上时，比较单元 1108 命令分配单元 1107 产生密钥失效数据识别符 RID，并命令驱动单元 1110 将密钥失效数据文件写到记录介质 1300 上，密钥失效数据文件如此构造以包括记录在失效数据存储单元 1102 中的密钥失效数据 RDATA、其版本号 VR、以及由分配单元 1107 产生的密钥失效数据识别符 RID。

当存在信息表示一个或多个密钥失效文件存在于记录介质 1300 上时，比较单元 1108 经由驱动单元 1110 从记录介质上的各密钥失效数据文件中读取包含于密钥失效数据 RDATA 中的版本号 VF。此时，读取一个或多个版本号 VF。比较单元 1108 还从失效数据存储单元 1102 中读取与密钥失效数据 RDATA 相应的版本号 VR。

接着，比较单元 1108 判断在于所读取的一个或多个版本号 VF 中是否存在与所读取的版本号 VR 相同的版本号。当判断结果为否定时，与上述相同，比较单元 1108 命令分配单元 1107 产生密钥失效数据识别符 RID，并命令驱动单元 1110 将密钥失效数据文件写到记录介质 1300 上，密钥失效数据文件如此构造以包括记录在失效数据存储单元 1102 中的密钥失效数据 RDATA、其版本号 VR、以及由分配单元 1107 产生的密钥失效数据识别符 RID。

当判断结果为肯定时，比较单元 1108 向控制单元 1109 输出表示存在等同于所读取的版本号 VR 的版本号的信息。

（9）控制单元 1109

控制单元 1109 经由发送和接收单元 1111 与因特网 40 向分配位置设备 1400 发送分配位置设备 1400 应该获得密钥失效数据 RDATA 的请求。控制单元 1109 还经由发送和接收单元 1111 向内容服务器设备 1500 发送内容服务器设备 1500 应该获得内容的请求。

控制单元 1109 命令比较单元 1108 检验在记录介质 1300 上是否存在一个或多个密钥失效文件。

当从比较单元 1108 中接收表示存在等同于版本号 VR 的版本号的信息时，控制单元 1109 命令驱动单元 1110 从记录介质 1300 上的包括等同于版本号 VR 的版本号的密钥失效数据文件中读取密钥失效数据识别符 RID，且还接收来自驱动单元 1110 的密钥失效数据识别符 RID。

接着，控制单元 1109，（i）命令密钥计算单元 1103 读取器件密钥 DK_1 和密钥失效数据 RDATA 以便于产生媒介密钥 MK，（ii）命令加密单元 1105 对内容密钥 CK 加密，（iii）命令识别符产生单元 1104 读取介质固有号 MID 并产生认证符 MAC，（iv）命令加密单元 1106 对内容 CNT 加密，（v）命令驱动单元 1110 在记录介质 1300 上保留加密内容文件，（vi）命令认证符产生单元 1104、加密单元 1105 和加密单元 1106 分别将所产生的认证符 MAC、所产生的加密内容密钥 ECK 和所产生的加密内容 ECNT 写入记录介质 1300 上的加密内容文件中。同样，控制单元 1109 命令驱动单元 1110（i）在记录介质 1300 上的加密内容文件内保留识别符记录单元 1303 和（ii）将通过分配单元 1107 产生的或从驱动单元 1110 接收的密钥失效数据识别符 RID 写到识别符记录单元 1303 上。

（10）发送和接收单元 1111

发送和接收单元 1111 经由因特网 40 连接于分配位置设备 1400，并经由专用线 30 连接于内容服务器设备 1500。

发送和接收单元 1111 经由因特网 40 接收来自分配位置设备 1400 的密钥失效数据 RDATA 和版本号 VR。已经接收密钥失效数据 RDATA 和版本号 VR 后，发送和接收单元 1111 将它们以如此方式写

到失效数据存储单元 1102 上以使它们彼此相对应。

发送和接收单元 1111 经由专用线 30 接收来自内容服务器设备 1500 的内容密钥 CK 和内容 CNT，向加密单元 1106 输出所接收的内容密钥 CK 和内容 CNT，向加密单元 1105 输出所接收的内容密钥 CK。

（11）驱动单元 1110

驱动单元 1110 根据记录设备 1100 的构件的指令来从记录介质 1300 中读取信息，并向作为指令源的构件输出所读取的信息。

驱动单元 1110 根据记录设备 1110 的构件的指令来在记录介质 1300 上保留区域，从该构件中接收信息块，并将所接收的信息块写到所保留的区域中。

（12）键盘 1180 和监视器 1190

键盘 1180 接收来自记录设备 1100 的操作者的操作指令，并将相应于所接收的操作指令的指令信息输出到控制单元 1109。

监视器 1190 在控制单元 1109 的控制下显示各种信息。

2.5 记录介质 1300

与记录介质 120 相同，记录介质 1300 为光盘介质，且具有不可重写区 1308 和可重写区 1309，如图 12 中所示。

不可重写区 1308 包括固有号记录区 1301，如图 12 中所示。在记录介质 1300 的制造工艺期间，记录介质 1300 所固有的介质固有号 MID 被记录在固有号记录区 1301 中。此时，可重写区 1309 中没有记录任何东西。在附图的实例中，介质固有号 MID 被表达为八个字符的十六进制数，且实际为“5”。

稍后，在记录设备 1100 如上所述将信息写到记录介质 1300 上之后，记录设备 1100 在可重写区 1309 中保留记录区 1305 和记录区 1306，以便于将一个或多个密钥失效数据文件记录到记录区 1305 中，

并将一个或多个加密内容文件记录到记录区 1306 中。

例如，如图 12 中所示，将密钥失效数据文件 1310 记录到记录区 1305 中，并将加密内容文件 1320 记录到记录区 1306 中。应该注意的是，如图 12 中所示，仅作为举例，在记录介质 1300 上仅记录一个密钥失效数据文件和一个加密内容文件；然而，也可以将不止一个密钥失效数据文件和不止一个加密内容文件记录到记录介质上。

如图 12 中所示，密钥失效数据文件 1310 包括版本号记录单元 1311、识别符记录单元 1312 和数据记录单元 1313。

将表示密钥失效数据 RDATA 的产生的版本号记录到版本号记录单元 1311；将由记录设备 1100 的分配单元 1107 分配的密钥失效数据识别符 RID 记录到识别符记录单元 1312 中；并将密钥失效数据 RDATA 记录到数据记录单元 1313 中。

这里，版本号、密钥失效数据识别符 RID 和密钥失效数据 RDATA 如上所述。

在图 12 中，版本号被表达为四个字符的十六进制数，且实际为“3”。在第二实施例中，密钥失效数据块的版本号由分配位置设备 1400 来分配。

在图 12 中，密钥失效数据识别符被表达为四个字符的十六进制数，且实际为“1”。

如图 12 中所示，加密内容文件 1320 包括识别符记录单元 1321、认证符记录单元 1322、密钥记录单元 1323 和内容记录单元 1324。同样，将识别包含于加密内容文件 1320 中的加密内容的内容号附加到加密内容文件 1320 上（附图中未示出）。

将密钥失效数据识别符 RID 记录到识别符记录单元 1321 中。密钥失效数据识别符 RID 已经被分配给密钥失效数据块，该密钥失效

数据块在由记录单元 1100 的分配单元 1107 执行的内容加密中使用。

将认证符 MAC 记录在认证符记录单元 1322 中。认证符 MAC 由记录设备 1100 的认证符产生单元 1104 产生。

通过记录设备 1100 的加密单元 1105 将所产生的加密内容密钥 ECK 记录到密钥记录单元 1323 中。

通过记录设备 1100 的加密单元 1106 将所产成的加密内容 ECNT 记录到内容记录单元 1324 中。

2.6 再现设备 1200

由于再现设备 1200a、1200b、1200c…具有相同的结构，所以这里对再现设备 1200 进行阐释。

如图 13 中所示，再现设备 1200 包括：器件密钥存储单元 1201、密钥计算单元 1202、认证符产生单元 1203、解密单元 1204、解密单元 1205、比较单元 206、规格接收单元 1207、获取单元 1208、搜索单元 1209、开关 1211、驱动单元 1213、再现单元 1214、控制单元 1215、输入单元 1216 和显示单元 1217。

更为具体地，与再现设备 200 相同，再现设备 1200 为一计算机系统，该系统包括微处理器、ROM、RAM、硬盘单元等。RAM 和硬盘单元各自在其中存储计算机程序。在微处理器根据计算机程序操作时再现设备 1200 实现其功能。

（1）说明接收单元 1207

说明接收单元 1207 经由遥控器 1280 和输入单元 1216 接收来自用户的要被再现的内容的说明，并将所接收的说明书中识别该内容的内容号输出到获取单元 1208 和认证符产生单元 1203。

（2）获取单元 1208

获取单元 1208 接收来自说明接收单元 1207 的内容号，并经由驱动单元 1213 从记录介质 1300 的记录区 1305 中找到所接收的内容号被附加其中的加密内容文件 1320。然后获取单元 1208 从已经找到的加密内容文件 1320 的识别符记录单元 1321 中读取密钥失效数据识别符 RID，并将所读取的密钥失效数据识别符 RID 输出到搜索单元 1209。

（3）搜索单元 1209

搜索单元 1209 接收来自获取单元 1208 的密钥失效数据识别符 RID。一旦接收密钥失效数据识别符 RID，搜索单元 1209 经由驱动单元 1213，在记录在记录介质 1300 的记录区 1305 上的一个或多个密钥失效数据文件中，查找其识别符记录单元包括等同于所接收的密钥失效数据识别符 RID 的密钥失效数据识别符的密钥失效数据文件，并从已经被查找到的该密钥失效数据文件的数据记录单元中读取密钥失效数据 RDATA。

然后，搜索单元 1209 向密钥计算单元 1202 输出所读取的密钥失效数据 RDATA。

（4）器件密钥存储单元 1201

与器件密钥存储单元 201 相同，器件密钥存储单元 1201 在其中以如此方式保密地存储器件密钥 DK_x 使得器件密钥 DK_x 不能被外部设备访问。器件密钥 DK_x 为对于再现设备 1200 唯一的密钥。

（5）密钥计算单元 1202

密钥计算单元 1202 接收来自搜索单元 1209 的密钥失效数据 RDATA，并从器件密钥存储单元 1201 中读取器件密钥 DK_x。

接着，与密钥计算单元 202 相同，密钥计算单元 1202 利用所读取的器件密钥 DK_x 对所接收的密钥失效数据 RDATA 执行解密算法

D1，以产生解密媒介密钥 y。

这里，解密媒介密钥 y 为媒介密钥 MK 或者值“0”。

接着，密钥计算单元 1202 向认证符产生单元 1203 和开关 1211 输出所产生的解密媒介密钥 y。

（6）认证符产生单元 1203

认证符产生单元 1203 接收来自密钥计算单元 1202 的解密媒介密钥 y，并通过驱动单元 1213 从记录介质 1300 的固有号记录区 1301 中读取介质固有号 MID。认证符产生单元 1203 还接收来自说明接收单元 1207 的内容号，并通过驱动单元 1213 在记录介质 1300 上指定附加了所接收的内容号的加密内容文件 1320，并从所指定的加密内容文件 1320 的密钥记录单元 1323 中读取加密内容密钥 ECK。

接着，认证符产生单元 1203 将所接收的解密媒介密钥 y、所读取的加密内容密钥 ECK、所读取的介质固有号 MID 按照上述顺序合并，以产生合并数据块，并对所产生的合并数据块执行单向函数 F，以产生解密认证符 DMAC。

DMAC=F（y||ECK||MID）

接着，认证符产生单元 1203 向比较单元 1206 输出所产生的解密认证符 DMAC。

（7）比较单元 1206

比较单元 1206 接收来自认证符产生单元 1203 的解密认证符 DMAC。比较单元 1206 还接收来自说明接收单元 1207 的内容号，并经由驱动单元 1213 在记录介质 1300 上指定附加了所接收的内容号的加密内容文件 1320，并读取记录在该指定加密内容文件 1320 的认证符记录单元 1322 中的认证符 MAC。

接着，比较单元 1206 判断所接收的解密认证符 DMAC 是否与所

读取的认证符 MAC 相匹配。当判断结果为肯定时，比较单元 1206 向开关 1211 输出开关 1211 应该闭合的指令。当判断结果为否定时，比较单元 1206 向开关 1211 输出开关 1211 应该断开的指令。

（8）开关 1211

根据来自比较单元 1206 的指令来控制开关 1211 的断开和闭合。当从比较单元 1206 中接收开关应该闭合的指令时开关 1211 闭合，而当从比较单元 1206 中接收开关应该断开的指令时开关 1211 断开。

开关 1211 接收来自密钥计算单元 1202 的解密媒介密钥 y。当开关 1211 接收开关应该闭合的指令时，开关 1211 向解密单元 1204 输出所接收的解密媒介密钥 y。当开关 1211 接收开关应该断开的指令时，不将解密媒介密钥 y 输出到外部。

（9）解密单元 1204

解密单元 1204 接收来自开关 1211 的解密媒介密钥 y。解密单元 1204 还接收来自说明接收单元 1207 的内容号，并通过驱动单元 1213 在记录介质 1300 上指定附加了所接收的内容号的加密内容文件 1320。然后解密单元 1204 读取记录在所指定的加密内容文件 1320 的密钥记录单元 1323 中的加密内容密钥 ECK，并利用所接收的解密媒介密钥 y 对所读取的加密内容密钥 ECK 执行解密算法 D2，以产生解密内容密钥 DCK。解密单元 1204 还向解密单元 1205 输出所产生的解密内容密钥 DCK。

（10）解密单元 1205

杰密单元 1205 接收来自解密单元 1204 的解密内容密钥 DCK。解密单元 1205 还接收来自说明接收单元 1207 的内容号，并经由驱动单元 1213 在记录介质 1300 上指定附加了所接收的内容号的加密内容文件 1320。解密单元 1205 还读取记录在所指定的加密内容文件 1320

的内容记录单元 1324 中的加密内容 ECNT，并利用所接收的解密内容密钥 DCK 对所读取的加密内容 ECNT 执行解密算法 D3，以产生解密内容 DCNT。解密单元 1205 还向再现单元 1214 输出所产生的解密内容 DCNT。

（11）再现单元 1214

再现单元 1214 接收来自解密单元 1205 的解密内容 DCNT，根据所接收的解密内容 DCNT 产生视频信息和音频信息，并将所产生的视频和音频信息转换为模拟视频信号和模拟音频信号，以便于向监视器 1290 输出模拟视频和音频信号。

（12）控制单元 1215、输入单元 1216、显示单元 1217、驱动单元 1213、监视器 129、遥控器 1280

控制单元 1215 控制再现设备 1200 的构件的操作。

遥控器 1280 包括各种按钮，并根据操作者在按钮上的操作来产生操作指令信息，以便于以红外线形式输出所产生的操作指令信息。输入单元 1216 从遥控器 1280 接收包括操作者指令信息的红外线，从所接收的红外线中提取操作者指令信息，并将所提取的操作者指令信息输出到控制单元 1215 或说明接收单元 1207。

显示单元 1217 在控制单元 1215 的控制下显示各种信息。

驱动单元 1213 从记录介质 1300 中读取信息。

监视器 1290 包括 CRT 和扬声器，并从再现单元 1214 接收模拟视频信号和模拟音频信号，以便于根据视频信号显示图像并根据音频信号输出声音。

2.7 在记录介质上记录的数据的结构和相关处理

（1）版本号

在图 12 种，版本号被表达为四个字符的十六进制数且实际为“3”。在第二实施例中，从分配位置设备 1400 分配密钥失效数据块的版本号。

更为具体地，将版本号“1”分配给最先发行的密钥失效数据块，其后，将版本号“2”、“3”、…分配给所发行的密钥失效数据块。

当密钥失效时，发行新的密钥失效数据块，且此时将新的版本号附加其上。应该注意的是，发行新的密钥失效数据块的时间并不限于密钥失效时。例如，考虑到安全问题，可以采用一种方案，在每个预定时间段发行一次新的密钥失效数据块。

（2）密钥失效数据识别符

在图 12 中，记录在识别符记录单元 1312 中的密钥失效数据识别符被表达为四个字符的十六进制数，密钥失效数据识别附 RID 为“1”。

这里，密钥失效识别符 RID 为唯一识别记录在各记录介质上的密钥失效数据块的信息。结果，能够根据独立设置的系统对每一记录介质分配密钥失效数据识别符。

对于由记录设备 1100 的分配单元 1107 分配密钥失效数据识别符 RID 的具体方法，分配单元 1107 分配一个值，该值不同于分配给已经记录到记录介质上的密钥失效数据块的密钥失效数据识别符。

在图 14 中示出的实例中，密钥失效数据文件 1 和密钥失效数据文件 2 已经被记录在记录介质 1300a 上，且其密钥失效数据识别符分别为“1”和“2”。

在这种情况下，当将密钥失效数据文件 3 再被记录到记录介质 1300a 上时，分配单元分配除了“1”和“2”之外的值“3”作为密钥失效数据识别符 RID。

（3）器件密钥和媒介密钥

在图 12 中，将加密媒介密钥 E（DK_i，MK）记录到数据记录单元 1313 上，通过利用 n 个器件密钥 DK_i（其中 i=1、2、…n）的每一个对媒介密钥加密而分别获得加密媒介密钥 E。

在图 12 中，存储在设备 n 中的器件密钥被表达为器件密钥_n。在图 12 中示出的实例中，由于设备 3 和设备 4 已经被失效，所以存储在其中的器件密钥 DK_3 和 DK_4 分别用于对和媒介密钥 MK 完全无关的数据块“0”加密。

通过这样产生这些密钥失效数据块，例如，在其中存储器件密钥 DK_1 的设备 1 能够通过使用器件密钥 DK_1 对密钥失效数据 E（DK_1，MK）解密来获得媒介密钥 MK；然而，在其中存储器件密钥 DK_3 的设备 3 即使通过使用器件密钥 DK_3 对密钥失效数据 E（DK_3，0）解密也不能获得媒介密钥 MK。

因此，在图 12 中示出的实例中，仅除设备 3 和 4 之外的设备都能共同地具有正确的媒介密钥 MK。设备 3 和 4 不能获得正确的媒介密钥 MK。因此，能够从系统中排除失效的设备 3 和 4。

应该注意的是，能够使用其它失效方法来失效设备。例如，专利文献 1 公开了其中使用树结构的失效方法。

（4）加密内容文件

如图 12 中所示，加密内容文件 1320 包括识别符记录单元 1321、认证符记录单元 1322、密钥记录单元 1323、以及内容记录单元 1324。

在图 12 中，记录在识别符记录单元 1321 中的密钥失效数据识别符被表达为四个字符的十六进制数，且该密钥失效数据识别符 RID 实际为“1”。

使用密钥失效数据识别符 RID，以便于从记录介质 1300 中获得密钥失效数据文件 1310，该密钥失效数据文件 1310 在对要在再现设

备 1200 上再现的加密内容解密中使用。

更为具体地，当记录在记录介质 1300 上的加密内容被解密并在再现设备 1200 上再现时，则再现设备 1200 从记录介质 1300 中获得密钥失效数据文件 1310，该密钥失效数据文件 1310 的识别符记录单元 1312 包括和记录在要被再现的加密内容文件 1320 的识别符记录单元 1321 中的密钥失效数据识别符 RID 相同的密钥失效数据识别符的。

这里，参考图 15 提供详细的阐述。如图 15 中所示，将密钥失效数据文件 1、密钥失效数据文件 2、加密内容文件 A、加密内容文件 B 和加密内容文件 C 记录在记录介质 1300b 上。

如图 15 中所示，密钥失效数据文件 1 和密钥失效数据文件 2 的密钥失效数据识别符分别为“1”和“2”。加密内容文件 A、加密内容文件 B 和加密内容文件 C 的密钥失效数据识别符分别为“1”、“1”和“2”。

这意味着，在记录设备 1100 上，当产生并记录加密内容文件 A 时，使用密钥失效数据文件 1 中的密钥失效数据块。当产生并记录加密内容文件 B 时，使用密钥失效数据文件 1 中的密钥失效数据块。当产生并记录加密内容文件 C 时，使用密钥失效数据文件 2 中的密钥失效数据块。

在这种情况下，例如，当再现设备 1200 解密并再现图 15 中示出的记录介质 1300b 上的加密内容文件 B 时，由于，加密内容文件 B 的密钥失效数据识别符为“1”，所以再现设备 1200 获得其密钥失效数据识别符为“1”的密钥失效数据文件 1，并利用包含于所获得的密钥失效数据文件 1 中的密钥失效数据块对存储在加密内容文件 B 中的加密内容解密。

2.8 内容供给系统 **20** 的操作

下面描述内容供给系统20的操作，特别地，描述由记录设备1100执行的将数据写到记录介质1300上的操作和由再现设备1200执行的再现记录在记录介质1300上的数据的操作。

（1）由记录设备1100执行的写数据的操作

下面参考图16、17和18的流程图来描述由记录设备1100执行的将数据写到记录介质1300上的操作。

记录设备1100的发送和接收单元1111经由因特网40接收来自分配位置设备1400的密钥失效数据RDATA和版本号VR，并将所接收的密钥失效数据RDATA和版本号VR以如此方式存储到失效数据存储单元1102中以使它们彼此相对应（步骤S1501）。

在步骤S1501中接收密钥失效数据RDATA和版本号VR的时间为分配位置设备1400发行新密钥失效数据RDATA的时候。如前面所述，将表示它们发行顺序的版本号VR附加到密钥失效数据块RDATA。根据版本号VR记录设备1100来检验所接收的密钥失效数据块RDATA是否为新的。

例如，在记录设备1100的失效数据存储单元1102在其中存储附加有版本号“1”的密钥失效数据块的情况下，假设从分配位置设备1400中接收附加有版本号“2”的密钥失效数据块，记录设备1100的控制单元1109将附加到所接收的密钥失效数据块的版本号“2”与附加到存储在失效数据存储单元1102中的密钥失效数据块的版本号“1”相比较。由于附加到所接收的密钥失效数据块的版本号“2”更新，所以控制单元1109认为所接收的密钥失效数据块较新，并命令发送和接收单元1111将所接收的密钥失效数据块和版本号“2”存储到失效数据存储单元1102中。这里，版本号越大，附加有该版本号

的数据越新。

这里，提供在使用版本号比较密钥失效数据块以确定哪一个较新的情况下的解释；然而，本发明不限于该方法。可以采用一种方案，其中，例如，向每一密钥失效数据块，附加发行该密钥失效数据块的日期和时间，来取代版本号，使得根据发行日期和时间来比较密钥失效数据块，以判断哪一个较新。

此外，这里，从分配位置设备 1400 获得密钥失效数据块，然而，获得密钥失效数据块的方法不限于此。可以采用一种方案，其中，例如，分配在其上记录密钥失效数据块和版本号的记录介质以使记录设备 1100 从该记录介质中读取密钥失效数据块和版本号。

接着，记录设备 1100 的比较单元 1108 通过驱动单元 1110 检验密钥失效数据文件是否存在于记录介质 1300 的记录区 1305 中。当确定没有密钥失效数据文件存在（步骤 S1502）时，程序前进到步骤 S1505a，该步骤在下面描述。

当确定存在密钥失效数据文件 1310（步骤 S1502）时，比较单元 1108 检验，在被记录在所有现存的密钥失效数据文件的版本号记录单元中的版本号中是否存在与附加到步骤 S1501 中获得的密钥失效数据块的版本号相同的版本号。

当在步骤 S1503 中没有满足上述条件的版本号（步骤 S1504）时，程序前进到步骤 S1505a，该步骤将在下面描述。

在步骤 S1504，当存在满足上述条件的版本号（步骤 S1504）时，控制单元 1109 通过驱动单元 1110 从包括满足所述条件的版本号的密钥失效数据文件 1310 的识别符记录单元 1312 中读取密钥失效数据识别符 RID（步骤 S1505）。

密钥计算单元 1103 从器件密钥存储单元 1101 中读取器件密钥，

并从失效数据存储单元 1102 中读取密钥失效数据块（步骤 S1506），然后通过利用所读取的器件密钥对所读取的密钥失效数据块解密来计算媒介密钥 MK（步骤 S1507）。

然后加密单元 1105 利用所计算的媒介密钥对从内容服务器设备 500 接收的内容密钥 CK 加密，以产生加密内容密钥 ECK（步骤 S1508）。

认证符产生单元 1104 从记录介质 1300 的固有号记录区 1301 中读取介质固有号 MID（步骤 S1509），并通过将（i）由密钥计算单元 1103 计算的媒介密钥 MK、（ii）由加密单元 1105 产生的加密内容密钥 ECK、以及（iii）所读取的介质固有号 MID 的合并值作为散列函数的输入值来产生作为输出值的认证符 MAC（步骤 S1510）。应该注意的是，这里使用的散列函数可以利用公知技术获得。例如，可以使用 SHA-1 作为散列函数；然而本发明不限于 SHA-1。

接着，加密单元 1106 以相似的方式利用从内容服务器设备 1500 接收的内容密钥 CK 对所接收的内容 CNT 加密（步骤 S1511）。

记录设备 1100 将加密内容文件记录到记录介质 1300 的记录区 1305 中（步骤 S1512），以完成该工序，加密内容文件包括：在步骤 S1505 中获得的或在步骤 S1505a 中分配的密钥失效数据识别符 RID、在步骤 S1510 产生的认证符 MAC、在步骤 S1508 中产生的加密内容密钥、以及在步骤 S1511 中产生的加密内容。

当确认密钥失效数据文件 1310 不存在于记录介质 1300 上（步骤 S1502）时，且当在步骤 S1503 中不存在满足所述条件的版本号（步骤 S1504）时，分配单元 1107 将作为密钥失效数据识别符的值分配给在步骤 1501 中获得的密钥失效数据块，该值与分配给记录在记录介质 1300 的记录区 1305 中的所有密钥失效数据文件的任何密钥失效

数据识别符 RID 不同（步骤 S1505a）。

例如，当没有密钥失效数据文件存在于记录介质 1300 上时，分配单元 1107 分配任意值，例如“1”。如图 14 中示出的实例，当其密钥失效数据识别符分别为“1”和“2”的密钥失效数据文件 1 和 2 存在于记录介质 1300a 上时，分配单元 1107 分配与“1”和“2”不同的值（例如“3”）。

接着，记录设备 1100 的驱动单元 1110 将在步骤 S1501 中获得的密钥失效数据块、密钥失效数据块的版本号、具有在步骤 S1505a 中分配的密钥失效数据识别符的密钥失效数据文件记录到记录介质 1300 上的密钥失效数据文件 1302 中（步骤 S1505b）。此时，驱动单元 1110 将密钥失效数据块、版本数量和密钥失效数据识别符 RID 分别记录到密钥失效数据文件 1310 的数据记录单元 1313、版本号记录单元 1311 以及识别符记录单元 1312。然后控制该程序前进到步骤 S1506，以便于其后执行从步骤 S1506 至步骤 S1512 的前述程序序。

（2）由再现设备 1200 执行的再现操作

下面参考图 19 和 20 的流程图来描述由再现设备 1200 执行的再现记录在记录介质 1300 上的数据的操作。

再现设备 1200 的说明接收单元 1207 接收要被再现的内容的说明（步骤 S1601）。

获取单元 1208 从记录介质 1300 的记录区 1305 中发现与在步骤 S1601 中指定的内容相对应的加密内容文件（步骤 S1602）。

关于由说明接收单元 1207 使用的用于指定要再现的内容的方法和用于发现相应于指定内容的加密内容文件的方法，例如，再现设备 1200 在再现设备 1200 的显示单元 1217 上显示，表示记录在记录介质 1300 的记录区 1305 中的所有加密内容文件的属性（例如，加密内

容的文件名、内容标题、内容记录的日期和时间、内容的概要信息、内容的缩图、表示内容的图标等）的信息列表，并且使用户从列表中选择他/她希望再现的内容，使得可以接收要被再现的内容的说明。再现设备 1200 从指定内容的属性信息中找出其中存储有该指定内容的加密内容文件的文件名，并从记录介质 1300 的记录区 1305 中发现具有特定文件名的加密内容文件。

关于用于发现加密内容文件的方法，本发明不限于上述方法；可以使用其他方法。

获取单元 1208 从在步骤 S1602 中发现的加密内容文件 1320 的识别符记录单元 1321 中读取密钥失效数据识别符（步骤 S1603）。

搜索单元 1209 从记录介质 1300 的记录区 1305 中发现其识别符记录单元 1312 在其中存储等同于在步骤 S1603 中读取的密钥失效数据识别符 RID 的值的密钥失效数据文件 1310（步骤 S1604）。然后搜索单元 1209 获取在步骤 S1604 中发现的密钥失效数据文件 1310（步骤 S1605）。

密钥计算单元 1202 从器件密钥存储单元 1201 中读取器件密钥，并从搜索单元 1209 中接收密钥失效数据块（步骤 S1606）。

密钥计算单元 1202 通过利用器件密钥对在步骤 S1606 中接收的密钥失效数据块解密来计算解密媒介密钥 y（步骤 S1607）。

认证符产生单元 1203 从记录介质 1300 的固有号记录区 1301 中读取介质固有号 MID（步骤 S1608），从在步骤 S1602 中发现的加密内容文件 1320 的密钥记录单元 1323 中读取加密内容密钥 ECK，并通过将(i)在步骤 S1607 中获得的解密媒介密钥 y、(ii)在步骤 S1609 中读取的加密内容密钥 ECK 以及（iii）在步骤 S1608 中获得的介质固有号 MID 的合并值作为散列函数的输入值来产生作为输出值的解

密认证符 DMAC（步骤 S1610）。这里使用的散列函数为与记录设备 1100 使用的散列函数相同的散列函数 SHA-1。

比较单元 1206 从在步骤 S1602 中发现的加密内容文件 1320 的认证符记录单元 1322 中读取认证符 MAC（步骤 S1611），并检验在步骤 S1610 种计算的解密认证符 DMAC 是否与在步骤 S1611 中读取的认证符 MAC 相匹配（步骤 S1612）。

当解密认证符DMAC与所述认证符MAC不相匹配(步骤S1613)时，结束该再现操作。

当该解密认证符DMAC与所述认证符MAC相匹配(步骤S1613)时，解密单元 1204 利用在步骤 S1607 计算的解密媒介密钥 y 来对加密内容密钥解密，以获得解密内容密钥 DCK（步骤 S1614）。

解密单元 1205 从在步骤 S1602 中发现的加密内容文件 1320 的内容记录单元 1324 中读取加密内容（步骤 S1615），并利用在步骤 S1614 中被解密的解密内容密钥 DCK 对在步骤 S1615 中读取的加密内容解密，以获得解密内容。再现单元 1214 再现该解密内容（步骤 S1616）。

2.9 其它修改实例

可以采用下述方案：

（1）在第二实施例中，将表示密钥失效数据块产生的版本号和识别密钥失效数据块的密钥失效数据识别符分别记录到密钥失效数据文件的版本号记录单元和识别符记录单元；然而，本发明不限于该方法。

例如，可以采用这样的方案，识别密钥失效数据文件的文件名包括密钥失效数据块的版本号和密钥失效数据识别符的其中之一或两

者。更为具体地，可以将密钥失效数据文件的文件名设定为“KRD_n_m”。这里，“n”为版本号，而“m”为密钥失效数据识别符。在这种情况下，例如，当使用文件名“KRD_0001_0002”识别（identified with）密钥失效数据文件时，其版本号为“1”，而密钥失效数据识别符 RID 为“2”。

采用其中文件名包括版本号和密钥失效数据识别符的其中之一或两者的这种方案，再现设备通过参考文件名能够找出密钥失效数据文件的版本号和密钥失效数据识别符 RID。因此，具有能够减少由再现设备执行的文件搜索所需的处理的有利效果。

（2）在第二实施例中，将密钥失效数据识别符记录到加密内容文件的识别符记录单元中；然而本发明并不限于该方法。

例如，可以采用一种方法，其中，识别加密内容文件的文件名包括密钥失效数据识别符。更为具体地，可以使识别加密内容文件的文件名为“ECNT_m”。这里，“m”为密钥失效数据识别符。例如，当加密内容文件的文件名为“ECNT_0002”时，密钥失效数据识别符 RID 为“2”。

采用其中文件名包括密钥失效数据识别符的方案，再现设备通过查阅文件名能够找出密钥失效数据识别符。因此，具有能够减少由再现设备执行的获取密钥失效数据识别符所需的处理的有利效果。

（3）在第二实施例中，为了将密钥失效数据与密钥失效数据识别符相关联，以及为了将加密内容与密钥失效数据识别符 RID 相关联，进行能够进行这样的布置以使得，密钥失效数据文件 1310 包括分别用于在其中记录版本号和密钥失效数据识别符的版本号记录单元 1311 和识别符记录单元 1312。同样，加密内容文件 1320 包括用于记录密钥失效数据识别符的识别符记录单元 1321。然而，本发明

不限于这些方案。

例如，可以采用一种方案，其中，记录设备在记录介质 1300 上记录一个或多个密钥失效数据文件、一个或多个加密内容文件以及一个密钥失效数据管理文件。对于每一个密钥失效数据文件，密钥失效数据管理文件包括密钥失效数据块的版本号、密钥失效数据识别符、用于唯一识别记录介质上的密钥失效数据文件的信息块（例如，示出在何处记录密钥失效数据文件的目录名或文件名）、在记录介质上，用于唯一识别使用该密钥失效数据文件加密的加密内容文件的信息块（例如，示出在何处记录加密内容文件的目录名或文件名）等。再现设备基于记录在密钥失效数据管理文件上的这些信息块来获取关于被指定进行再现的加密内容的密钥失效数据文件。

此外，还可以将该实施例的方案与其中提供了密钥失效数据管理文件的方案相结合。

（4）在第二实施例中，使用密钥失效数据块的版本号和密钥失效数据识别符两者；然而，本发明不限于该方案。也可以仅使用密钥失效数据识别符。

（5）在第二实施例中，阐述了采用密钥失效技术的方案，在该方案中，记录于记录介质的可重写区中的密钥失效数据块包括：（i）利用存储在未失效的设备中的器件密钥加密的媒介密钥和（ii）利用存储在失效的设备中的器件密钥加密的与媒介密钥无关的值（例如“0”），且要记录到记录介质的可重写区中的加密内容为基于该媒介密钥加密的内容；然而，本发明不限于该方案。

例如，可以采用任何一种方案，只要满足下述条件：对于记录在记录介质的可重写区中的密钥失效数据块和加密内容来说，未失效的设备能够基于密钥失效数据块来解密并再现加密内容；而失效设备不

能基于密钥失效数据块来解密并再现加密内容。

（6）在第二实施例中，提供作为媒介绑定技术的方案，其中，在记录设备 1100 处，利用介质固有号 MID 产生认证符 MAC，并在再现设备 1200 处，比较认证符 MAC；然而，本发明不限于该方案。

例如，可以采用一种方案，其中，在记录设备 1100 处，利用介质固有号 MID 对内容加密并将其记录到记录介质上，且在再现设备 1200 处，利用介质固有号 MID 对加密内容解密。

（7）在第二实施例中，当分配了密钥失效数据识别符时，作为密钥失效识别符被分配的值不是被分配给已经记录在记录设备 1100 上的密钥失效数据块的值；然而，本发明不限于该方案。

例如，可以采用这样的方案，记录设备 1100 在其中存储已经被分配的密钥失效数据识别符和介质固有号 MID，以使记录设备 1100 基于存储在其中的该信息分配其它密钥失效数据识别符。

2.10 总述

从上面的描述可以看出，本发明提供记录设备，该设备包括：密钥失效数据存储单元，在其中存储用于失效存储在指定设备中的密钥的密钥失效数据块；内容加密单元，可被操作以根据密钥失效数据块来对内容加密；分配单元，可被操作以向该密钥失效数据块分配唯一识别记录介质上的密钥失效数据块的密钥失效数据识别信息；密钥失效数据记录单元，可被操作以将密钥失效数据块以如此方式记录到记录介质上，使得它与密钥失效数据识别信息相对应；以及内容记录单元，可被操作从而以如此方式记录加密内容，使得它与密钥失效数据识别信息相对应。

此外，分配单元将与已经分配给记录在记录介质上的密钥失效数

据块的密钥失效数据识别信息不同的值作为密钥失效数据识别信息分配。

此外，分配单元将记录在记录介质上的密钥失效数据块与存储在密钥失效数据存储单元中的密钥失效数据块相比较，并且仅当判断存储在密钥失效数据存储单元中的密钥失效数据块较新时，分配密钥失效数据识别信息。

另外，分配单元根据关于产生密钥失效数据块的日期和时间的信息或关于产生密钥失效数据块的顺序的信息，来判断记录在记录介质上的密钥失效数据块和存储在密钥失效数据存储单元中的密钥失效数据块中的哪一个较新。

本发明还提供再现设备，该设备包括：内容读取单元，可被操作以从记录介质中读取加密内容以及与加密内容相对应记录的密钥失效数据识别信息；密钥失效数据读取单元，可被操作以从记录介质中读取密钥失效数据块，与由内容读取单元所读取的密钥失效数据识别信息块相同的密钥失效数据识别信息块与该读取的密钥失效数据块相对应；以及内容解密单元，可被操作以根据由密钥失效数据读取单元读取的密钥失效数据块对由内容读取单元读取的加密内容解密。

本发明提供记录介质，该介质包括：密钥失效数据存储单元，其以如此方式记录密钥失效数据块，以使其与唯一识别记录介质上的密钥失效数据块的密钥失效数据识别信息块相对应；和内容存储单元，可被操作从而以如此方式记录根据密钥失效数据块加密的加密内容，以使其与失效数据识别信息块相对应。

本发明还提供记录介质，该记录介质还包括与每一密钥失效数据块相对应的表示哪一个密钥失效数据块较新的信息。

本发明还提供数字作品保护系统，该系统至少由记录设备、记录

介质和再现设备构成，其中，记录设备包括：密钥失效数据存储单元，在其中存储用于失效存储在指定设备中的密钥的密钥失效数据块；内容加密单元，可被操作以根据密钥失效数块对内容加密；分配单元，可被操作以向密钥失效数据块分配唯一识别记录介质上的密钥失效数据块的密钥失效数据识别信息；密钥失效数据记录单元，可被操作以将密钥失效数据块以如此方式记录到记录介质上，使得它与密钥失效数据识别信息相对应；以及内容记录单元，可被操作从而以如此方式记录加密内容以使它与密钥失效数据识别信息相对应，而记录介质包括：密钥失效数据存储单元，其以如此方式记录密钥失效数据块，以使其与密钥失效数据识别信息块相对应；和内容存储单元，可被操作从而以如此方式记录加密内容，以使其与失效数据识别信息块相对应，以及再现设备包括：内容读取单元，可被操作以从记录介质中读取加密内容以及与加密内容相对应记录的密钥失效数据识别信息；密钥失效数据读取单元，可被操作以从记录介质中读取密钥失效数据块，与由内容读取单元所读取的密钥失效数据识别信息块相同的密钥失效数据识别信息块与该读取的密钥失效数据块相对应；以及内容解密单元，可被操作以根据由密钥失效数据读取单元读取的密钥失效数据块对由内容读取单元读取的加密内容解密。

采用如上所述的根据第二实施例的该记录设备、记录介质、再现设备和数字作品保护系统，(i)将密钥失效数据识别符分配给要记录在记录介质上的密钥失效数据块，以使得密钥失效数据识别符唯一识别记录介质上的密钥失效数据块，(ii)与将要记录到记录介质上的密钥失效数据块相对应地将密钥失效数据识别符作为密钥失效数据文件来记录；以及（iii）将与利用密钥失效数据块加密的内容相对应的密钥失效数据识别符作为加密内容文件记录。因此，当再现设备解密

并再现加密内容时，即使在记录介质上记录多个加密内容文件和多个密钥失效数据文件，也能够搜索到并获取包含等同于在特定加密内容文件中包含的密钥失效数据识别符的密钥失效数据识别符的密钥失效数据文件，且因此能够利用所获得的密钥失效数据文件来解密并再现加密内容文件。

3. 其它修改实例

到此为止，根据实施例阐述了本发明；然而，务须说明，本发明不限于这些实施例。下述实例也包含在本发明中：

（1）在这些实施例中，所述内容为这样的数据，其中视频数据和音频数据被有效被压缩编码；然而，本发明不限于此。例如，可以采用这样的方案，所述内容为计算机数据，其中小说、静态图像、视频等被数字化。

此外，还可接受这样的方案，例如，所述内容为由用于控制包含于计算机中的微处理器的操作的指令构成的计算机程序。或者，可接受这样的方案，所述内容为使用电子指标（spreadsheet）软件产生的表格数据。还可接受这样的方案，所述内容为使用数据库软件产生的数据库。

（2）前述设备中的每一个具体是包括微处理器、ROM、RAM、硬盘单元、现实单元、键盘、鼠标等的计算机系统。RAM 和硬盘单元各自在其中存储计算机程序。在微处理器根据计算机程序操作时每一个设备实现其功能。

（3）将本发明看作为如上所述的方法也是可接受的。将本发明看作为利用计算机来实现这种方法的计算机程序，或看作为由该计算机程序转换的数字信号也是可接受的。

另外，可以认为本发明提供在其上记录这种计算机程序或这种数字信号的计算机可读记录介质，例如软盘、硬盘、CD-ROM、MO、DVD、DVD-ROM、DVD-RAM、BD（蓝光盘）和半导体存储器，或可以认为本发明提供记录在这种介质上的这种计算机程序或这种数字信号。

此外，可以认为本发明使得能够通过电信线、无线或电缆通信网络、由因特网代表的网络、数字广播等来发送这种计算机程序或这种数字信号。

此外，可以认为本发明提供包括微处理器和存储器的计算机系统，其中存储器存储计算机程序，而微处理器根据计算机程序操作。

此外，另一个独立的计算机系统执行发送到该记录媒介上的程序或数字信号，或者经由上述网络执行该程序或数字信号。

（4）将一些所述实施例和修改实例组合起来也是可接受的。

工业应用

在制造内容并供给它们的内容供给工业中，可操作地、连续地并重复地使用本发明的设备和记录介质。在电子制造工业中，还能够可操作地、连续地且重复地制造和出售本发明的设备和记录介质。

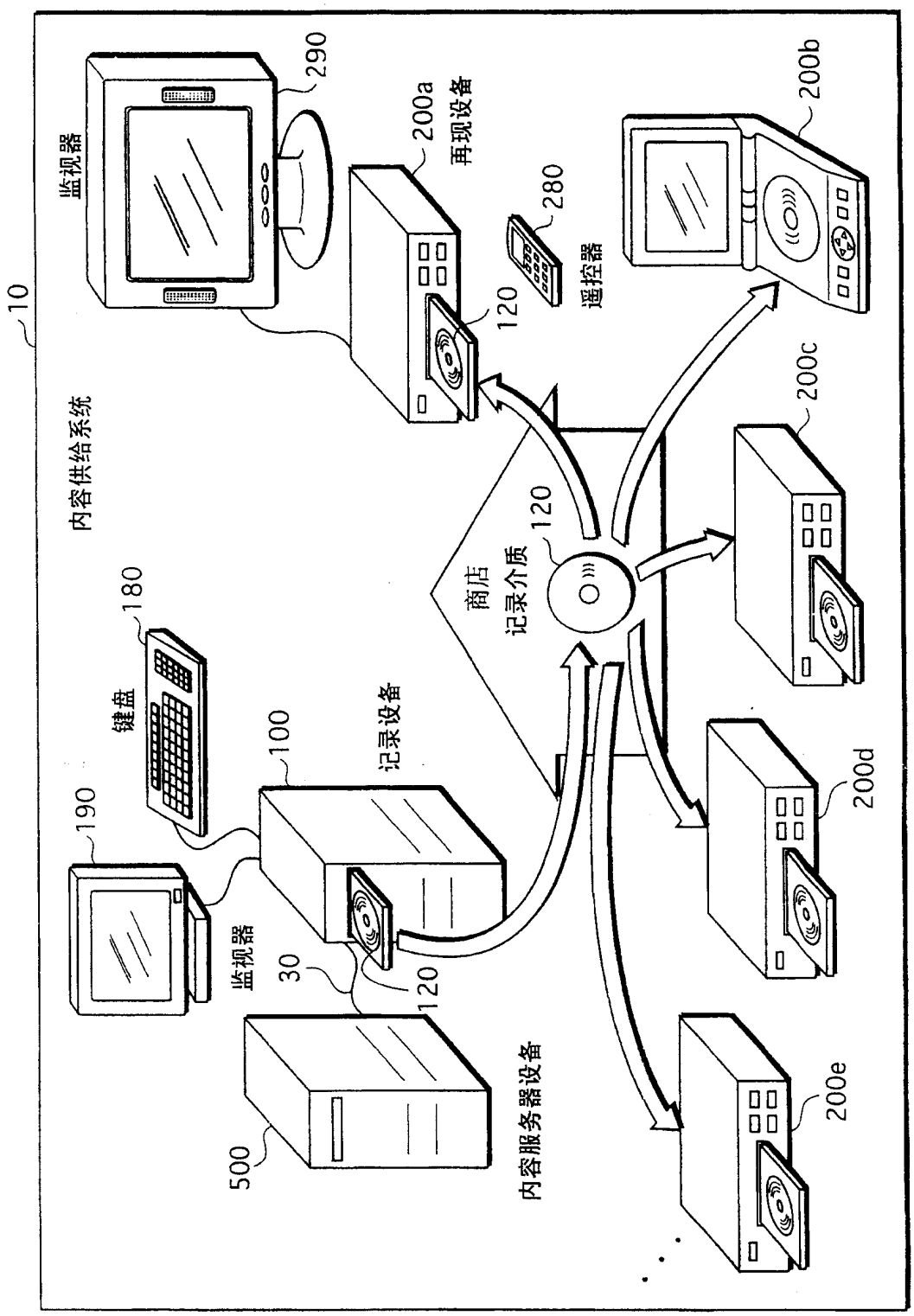

10
内容供给系统
监视器
290
200a
再现设备
280
遥控器
120
200b
200c
商店
记录介质
120
键盘
180
100
记录设备
190
监视器
30
120
200d
500
内容服务器设备
200e

图1

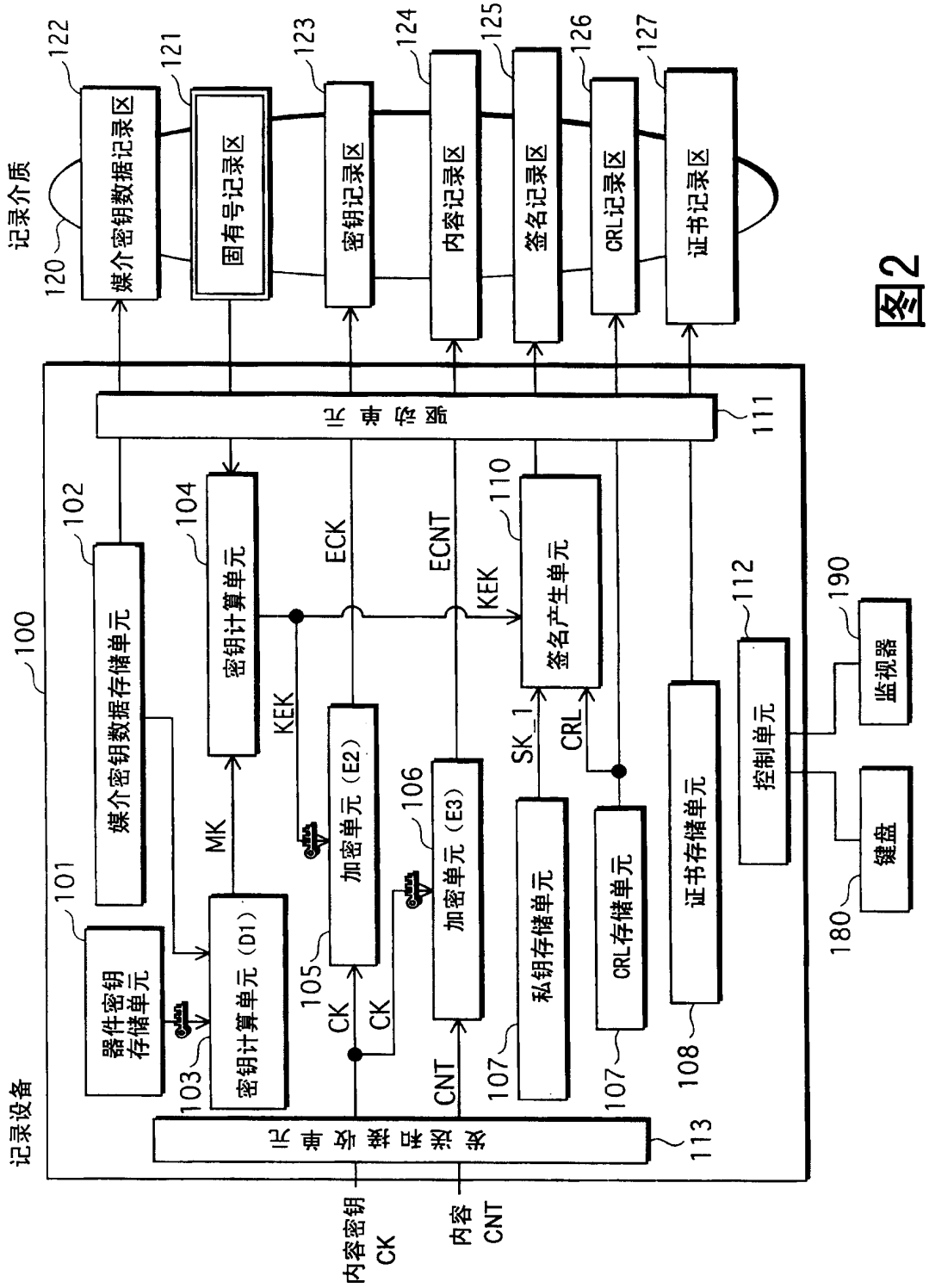

记录介质
120
媒介密钥数据记录区
122
121
固有号记录区
123
密钥记录区
124
内容记录区
125
签名记录区
126
CRL记录区
127
证书记录区
驱动单元
111
100
102
媒介密钥数据存储单元
104
密钥计算单元
ECK
ECNT
110
KEK
签名产生单元
112
190
监视器
101
器件密钥存储单元
MK
密钥计算单元（D1）
103
KEK
105
加密单元（E2）
106
加密单元（E3）
SK_1
CRL
私钥存储单元
CRL存储单元
证书存储单元
控制单元
键盘
180
CK
CK
CNT
107
107
108
113
记录设备
数据接收单元
内容密钥
CK
内容
CNT

图2

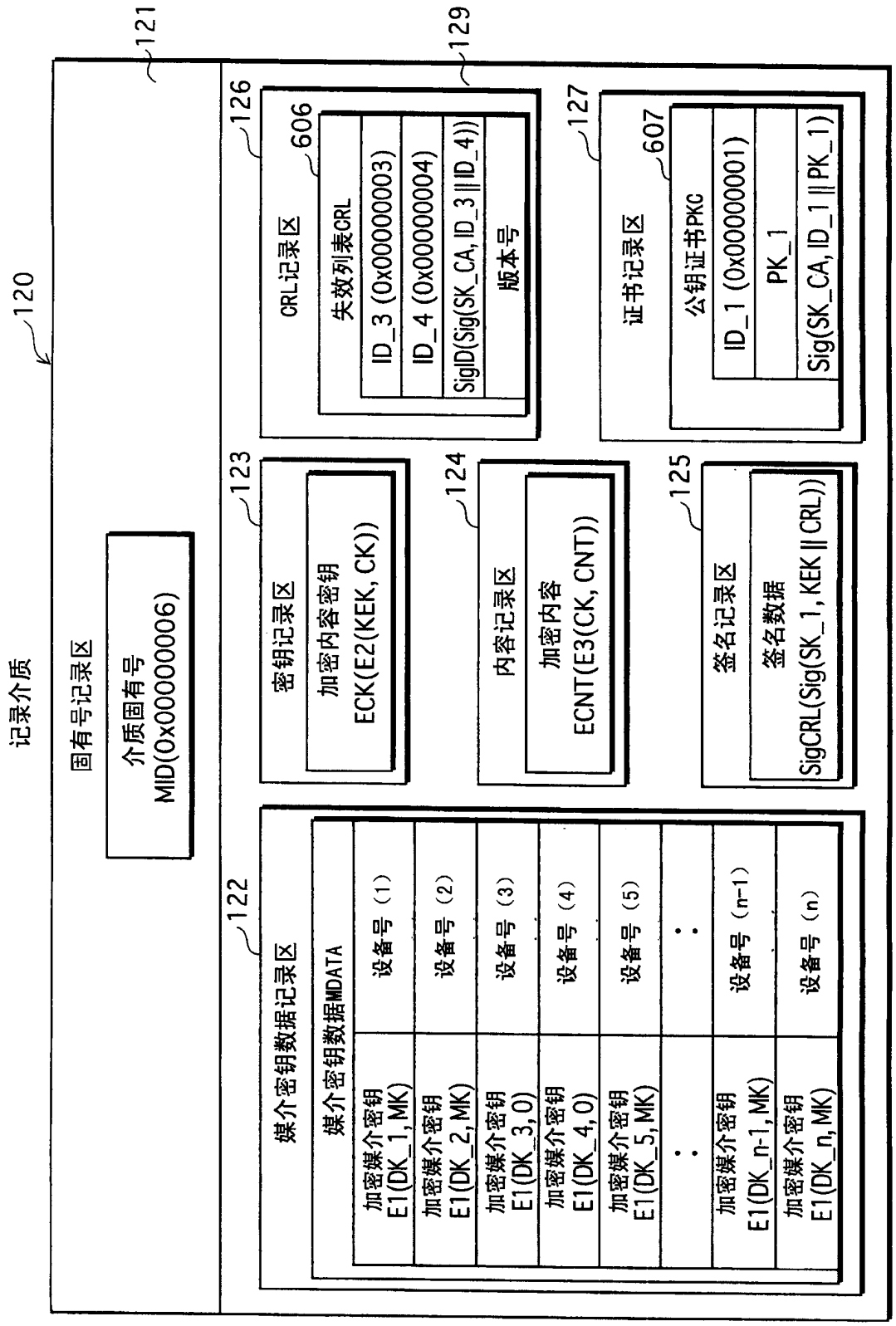

记录介质
120
121
固有号记录区
介质固有号
MID(0x00000006)
媒介密钥数据记录区
122
媒介密钥数据MDATA
加密媒介密钥 E1(DK_1,MK)
设备号（1）
加密媒介密钥 E1(DK_2,MK)
设备号（2）
加密媒介密钥 E1(DK_3,0)
设备号（3）
加密媒介密钥 E1(DK_4,0)
设备号（4）
加密媒介密钥 E1(DK_5,MK)
设备号（5）
加密媒介密钥 E1(DK_n-1,MK)
设备号（n-1）
加密媒介密钥 E1(DK_n,MK)
设备号（n）
密钥记录区
123
加密内容密钥
ECK(E2(KEK, CK))
内容记录区
124
加密内容
ECNT(E3(CK, CNT))
签名记录区
125
签名数据
SigCRL(Sig(SK_1, KEK || CRL))
CRL记录区
126
129
失效列表CRL
606
ID_3 (0x00000003)
ID_4 (0x00000004)
SigID(Sig(SK_CA, ID_3 || ID_4))
版本号
证书记录区
127
公钥证书PKC
607
ID_1 (0x00000001)
PK_1
Sig(SK_CA, ID_1 || PK_1)

图3

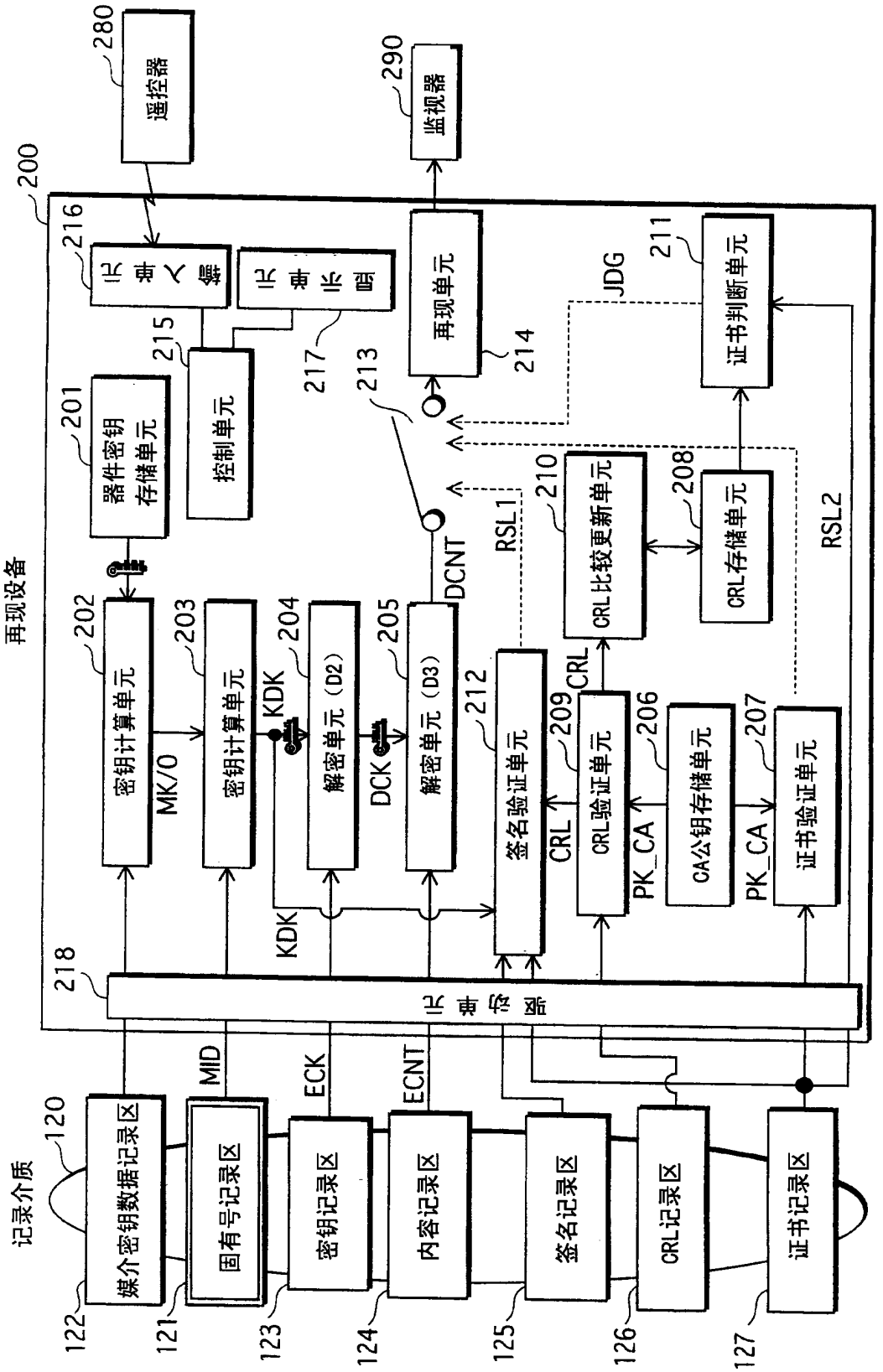

再现设备
200
记录介质
120
媒介密钥数据记录区
122
固有号记录区
121
密钥记录区
123
内容记录区
124
签名记录区
125
CRL记录区
126
证书记录区
127
MID
ECK
ECNT
驱动单元
218
密钥计算单元
202
密钥计算单元
203
解密单元（D2）
204
解密单元（D3）
205
签名验证单元
212
CRL验证单元
209
CA公钥存储单元
206
证书验证单元
207
CRL比较更新单元
210
CRL存储单元
208
证书判断单元
211
再现单元
214
器件密钥存储单元
201
控制单元
215
输入单元
216
显示单元
217
遥控器
280
监视器
290
MK/O
KDK
DCK
DCNT
CRL
PK_CA
RSL1
RSL2
JDG
213

图4

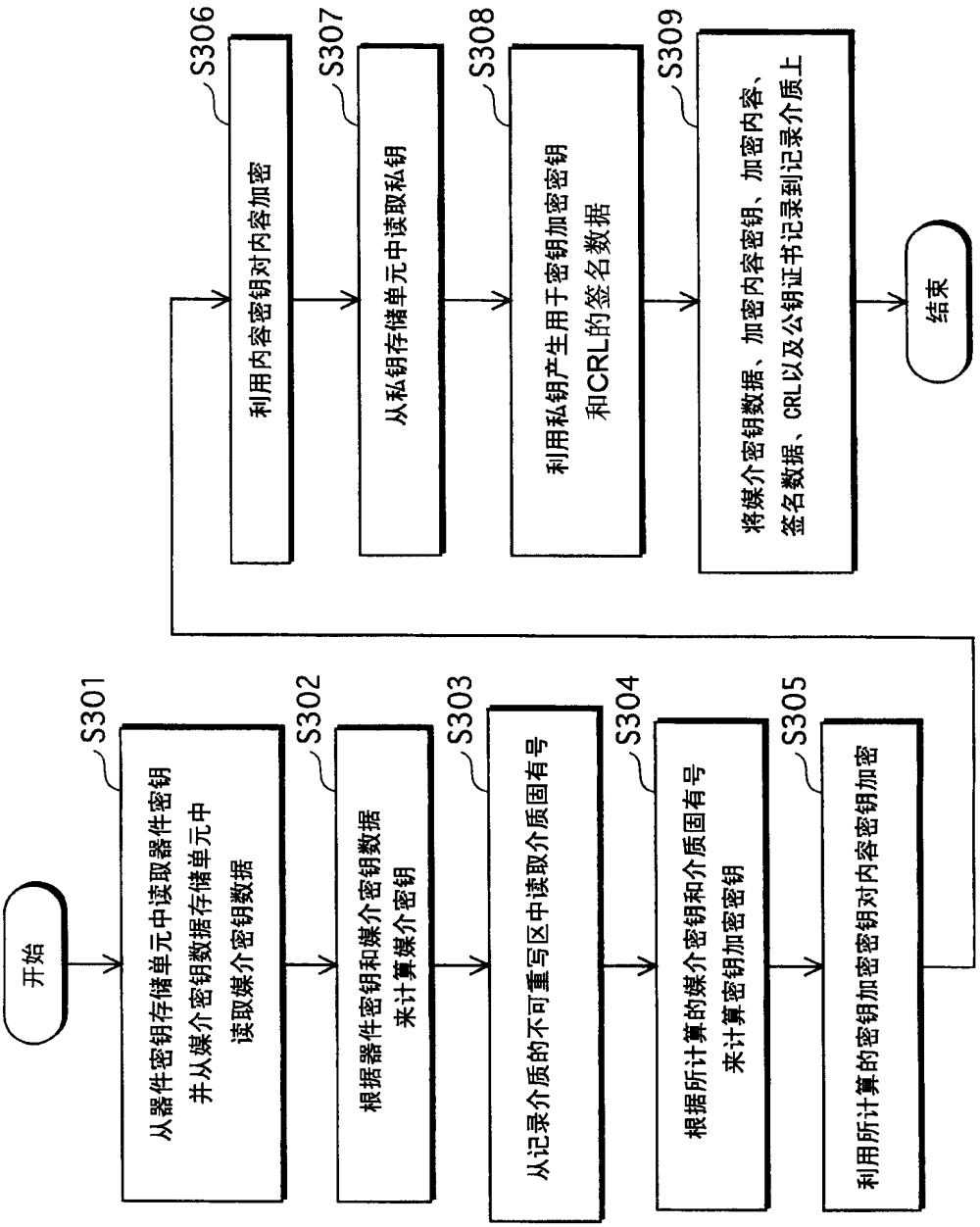

开始
S301
从器件密钥存储单元中读取器件密钥
并从媒介密钥数据存储单元中
读取媒介密钥数据
S302
根据器件密钥和媒介密钥数据
来计算媒介密钥
S303
从记录介质的不可重写区中读取介质固有号
S304
根据所计算的媒介密钥和介质固有号
来计算密钥加密密钥
S305
利用所计算的密钥加密密钥对内容密钥加密
S306
利用内容密钥对内容加密
S307
从私钥存储单元中读取私钥
S308
利用私钥产生用于密钥加密密钥
和CRL的签名数据
S309
将媒介密钥数据、加密内容密钥、加密内容、
签名数据、CRL以及公钥证书记录到记录介质上
结束

图5

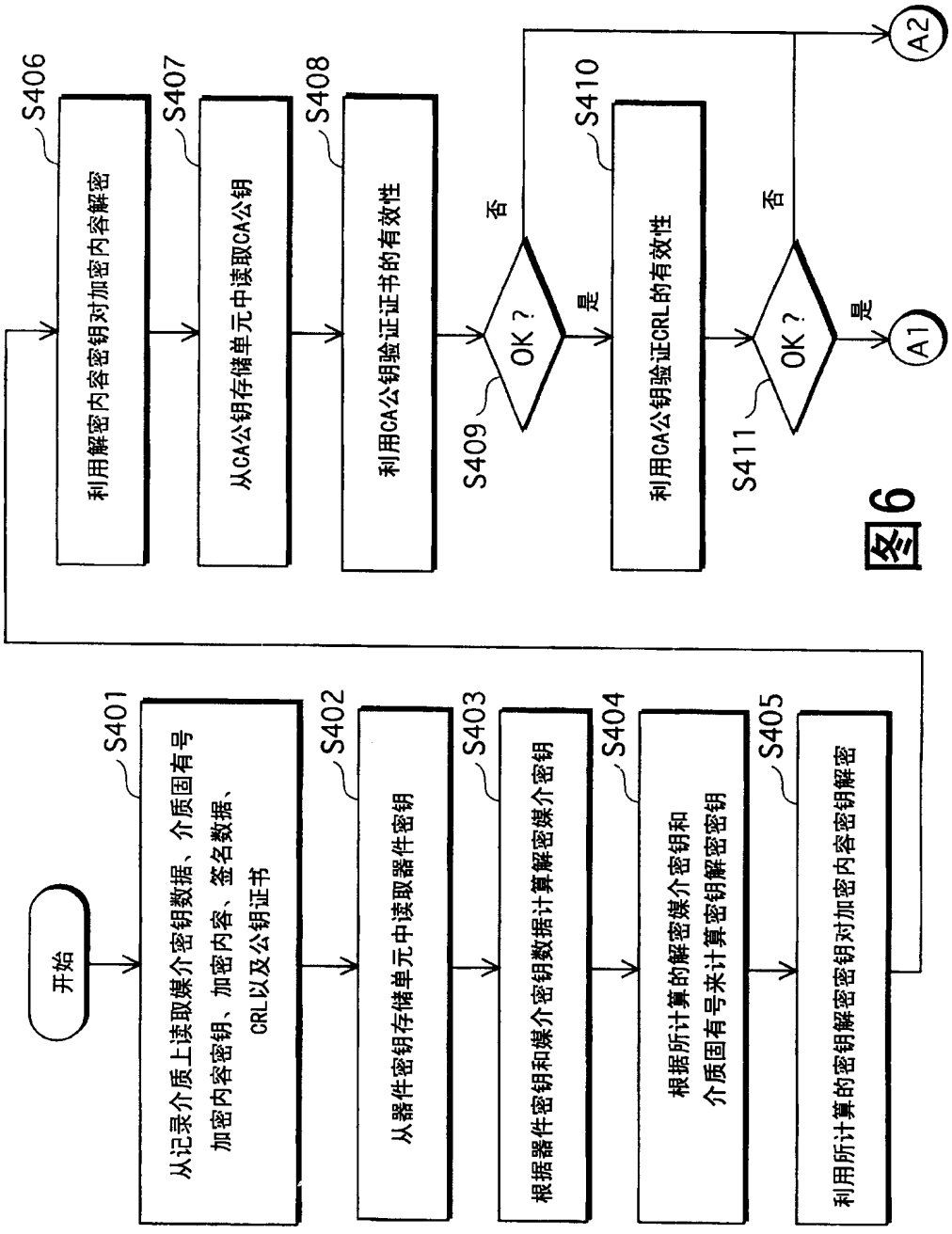

开始
S401
从记录介质上读取媒介密钥数据、介质固有号
加密内容密钥、加密内容、签名数据、
CRL以及公钥证书
S402
从器件密钥存储单元中读取器件密钥
S403
根据器件密钥和媒介密钥数据计算解密媒介密钥
S404
根据所计算的解密媒介密钥和
介质固有号来计算密钥解密密钥
S405
利用所计算的密钥解密密钥对加密内容密钥解密
S406
利用解密内容密钥对加密内容解密
S407
从CA公钥存储单元中读取CA公钥
S408
利用CA公钥验证证书的有效性
S409
OK ?
否
是
S410
利用CA公钥验证CRL的有效性
S411
OK ?
否
是
A1
A2

图6

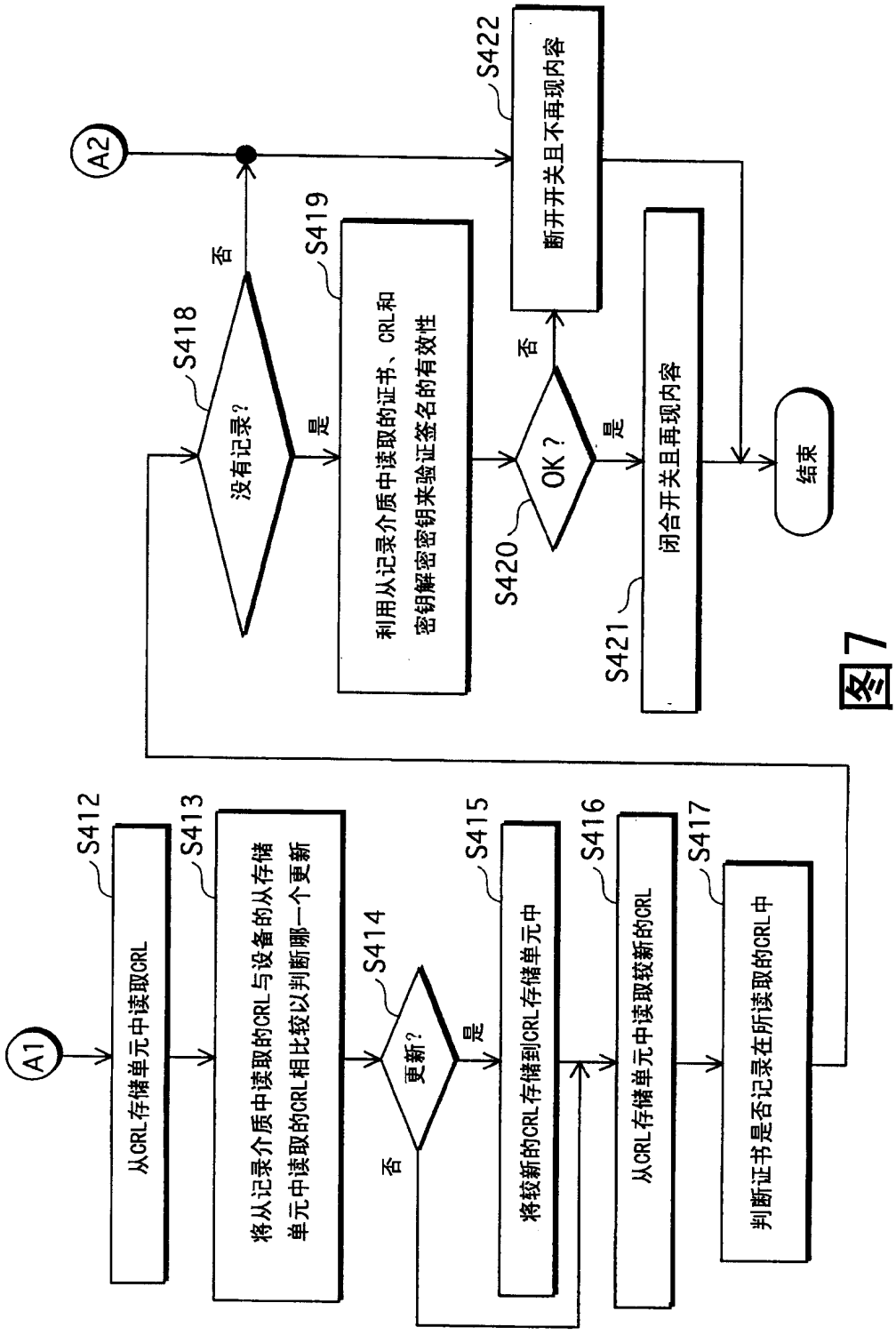

A1
S412
从CRL存储单元中读取CRL
S413
将从记录介质中读取的CRL与设备的从存储单元中读取的CRL相比较以判断哪一个更新
S414
更新?
否
是
S415
将较新的CRL存储到CRL存储单元中
S416
从CRL存储单元中读取较新的CRL
S417
判断证书是否记录在所读取的CRL中
A2
S418
没有记录?
否
是
S419
利用从记录介质中读取的证书、CRL和密钥解密密钥来验证签名的有效性
S420
OK ?
否
是
S421
闭合开关且再现内容
S422
断开开关且不再现内容
结束

图7

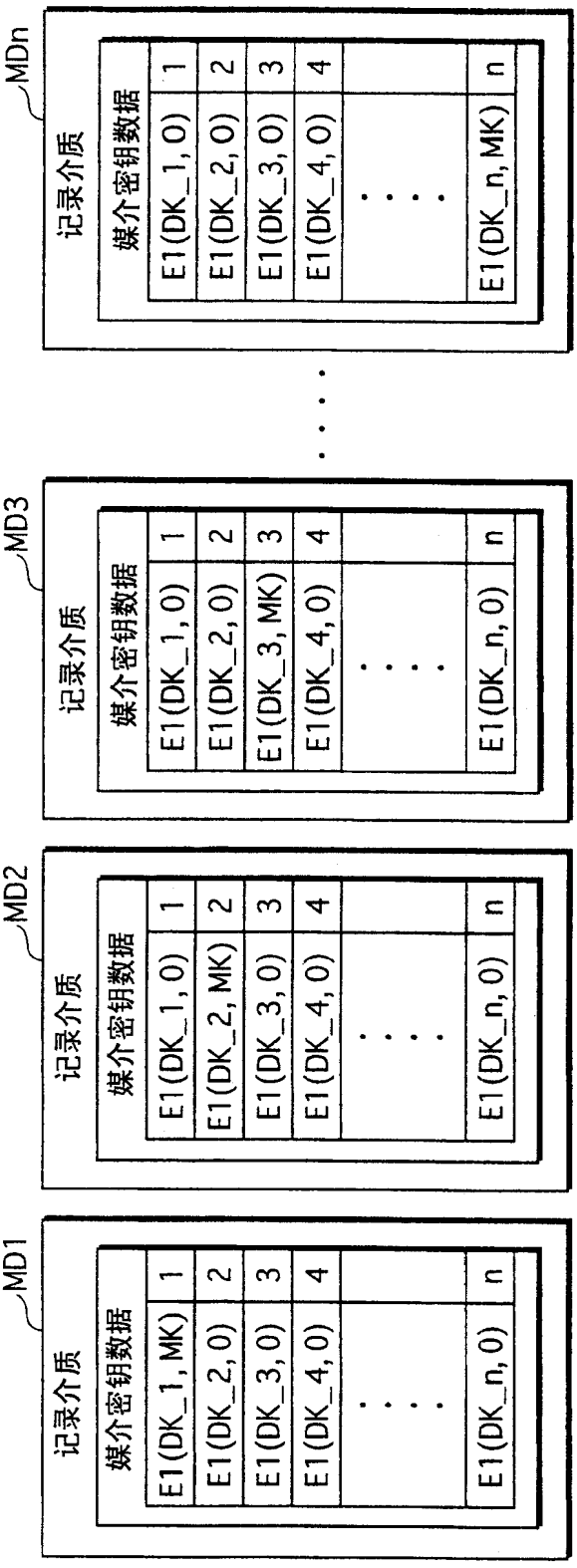

MD1
记录介质
媒介密钥数据
E1(DK_1, MK) 1
E1(DK_2, 0) 2
E1(DK_3, 0) 3
E1(DK_4, 0) 4
E1(DK_n, 0) n
MD2
记录介质
媒介密钥数据
E1(DK_1, 0) 1
E1(DK_2, MK) 2
E1(DK_3, 0) 3
E1(DK_4, 0) 4
E1(DK_n, 0) n
MD3
记录介质
媒介密钥数据
E1(DK_1, 0) 1
E1(DK_2, 0) 2
E1(DK_3, MK) 3
E1(DK_4, 0) 4
E1(DK_n, 0) n
MDn
记录介质
媒介密钥数据
E1(DK_1, 0) 1
E1(DK_2, 0) 2
E1(DK_3, 0) 3
E1(DK_4, 0) 4
E1(DK_n, MK) n

图8

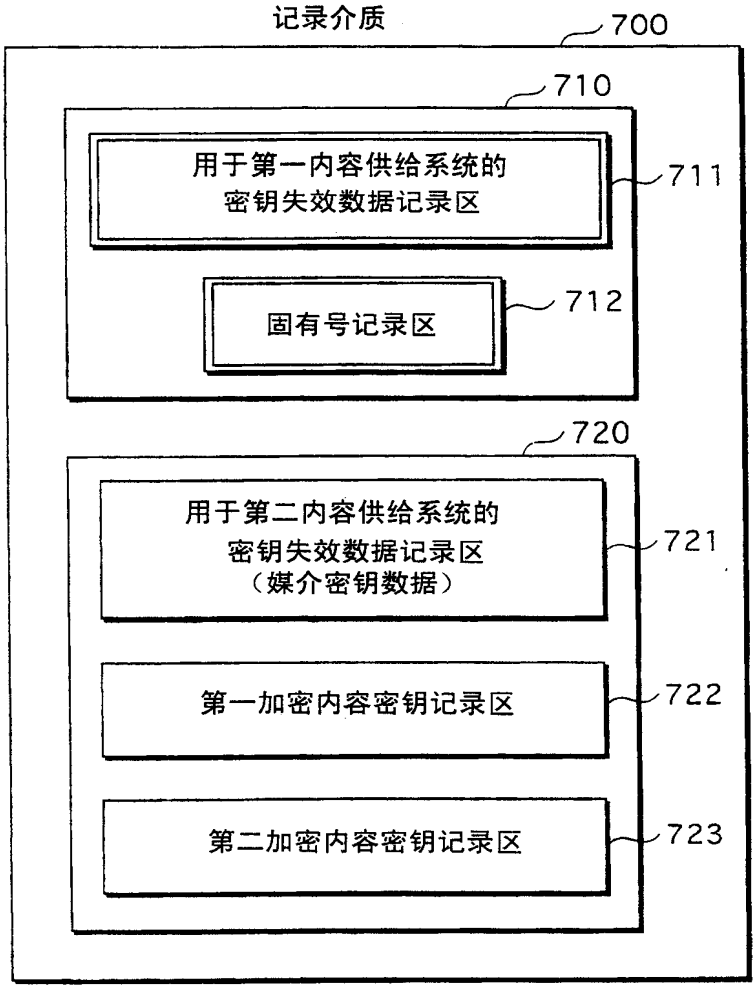

记录介质
700
710
用于第一内容供给系统的
密钥失效数据记录区
711
固有号记录区
712
720
用于第二内容供给系统的
密钥失效数据记录区
（媒介密钥数据）
721
第一加密内容密钥记录区
722
第二加密内容密钥记录区
723

图9

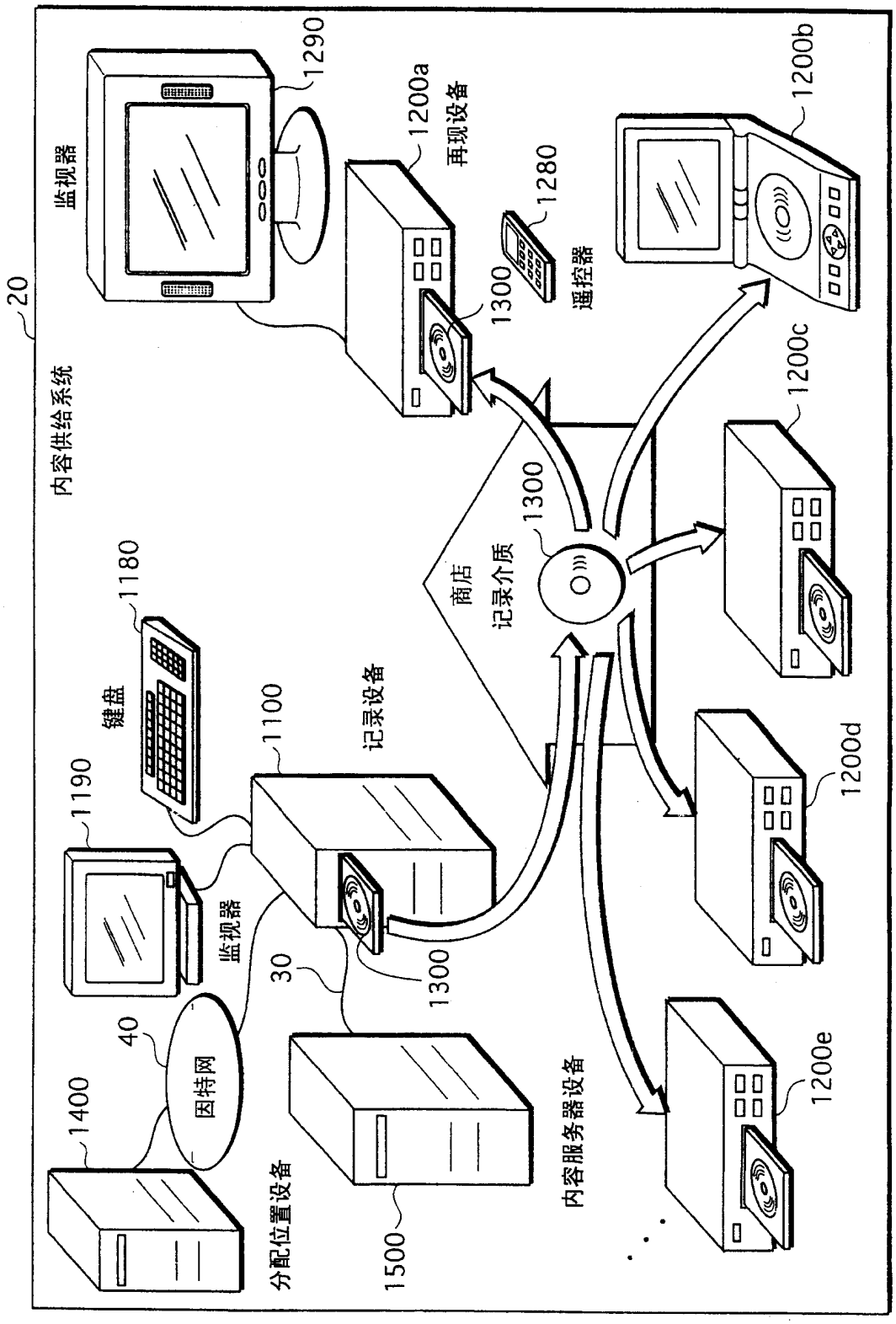

20
内容供给系统
监视器
1290
1200a
再现设备
1280
1300
遥控器
1200b
1200c
商店
记录介质
1300
1180
键盘
1100
记录设备
1190
监视器
30
1300
1200d
40
因特网
1400
分配位置设备
1500
内容服务器设备
1200e

图10

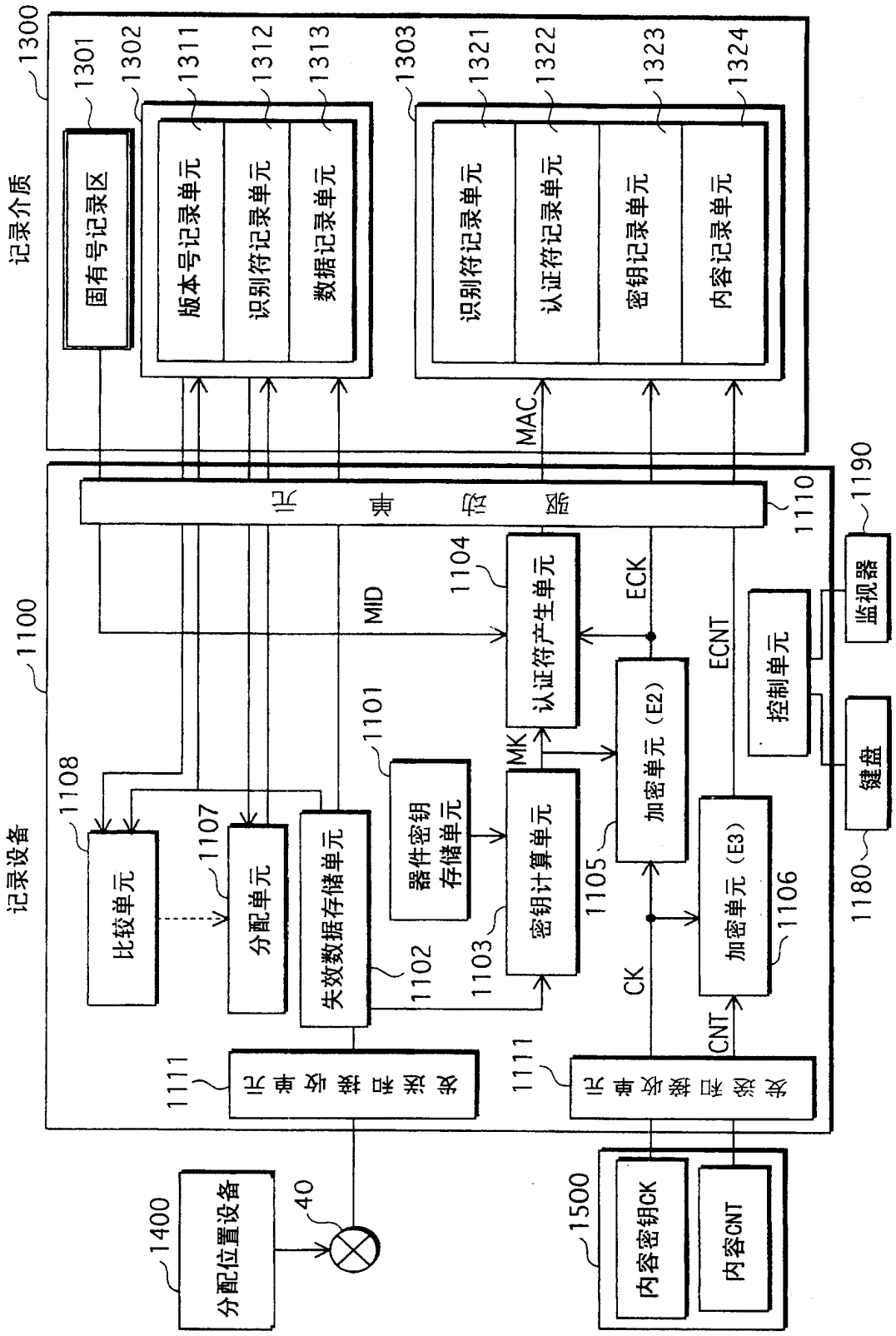

记录介质
1300
固有号记录区
1301
版本号记录单元
1311
识别符记录单元
1312
数据记录单元
1313
识别符记录单元
1321
认证符记录单元
1322
密钥记录单元
1323
内容记录单元
1324
1302
1303
MAC
记录设备
1100
驱动单元
1110
比较单元
1108
分配单元
1107
失效数据存储单元
1101
器件密钥存储单元
1102
密钥计算单元
1103
认证符产生单元
1104
加密单元（E2）
1105
加密单元（E3）
1106
控制单元
监视器
1190
键盘
1180
MID
MK
ECK
ECNT
CK
CNT
发送和接收单元
1111
发送和接收单元
1111
分配位置设备
1400
40
内容密钥CK
内容CNT
1500

图11

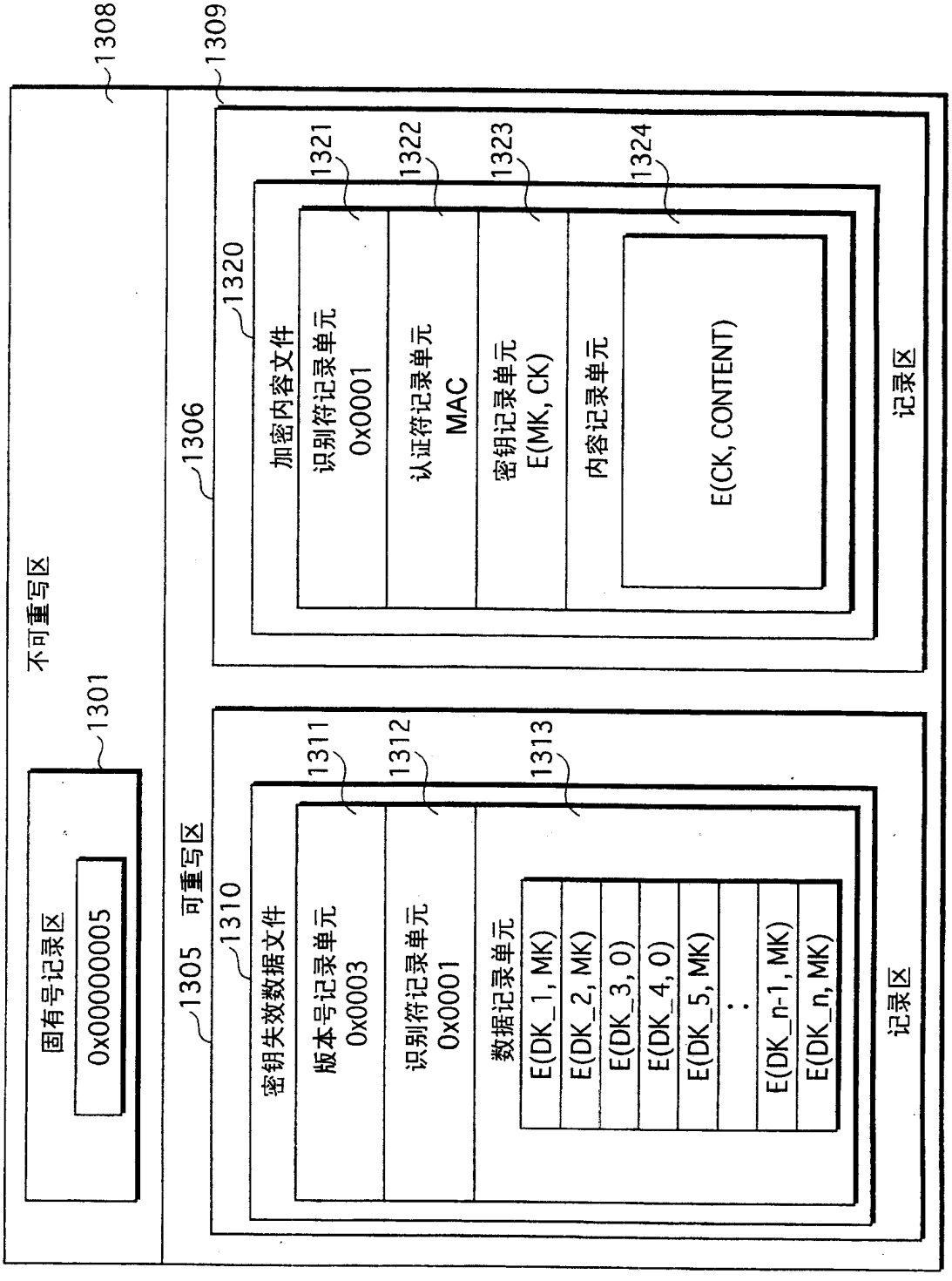

1308
1309
不可重写区
固有号记录区
1301
0x00000005
1305 可重写区
1306
1310
密钥失效数据文件
1311
版本号记录单元
0x0003
1312
识别符记录单元
0x0001
1313
数据记录单元
E(DK_1, MK)
E(DK_2, MK)
E(DK_3, 0)
E(DK_4, 0)
E(DK_5, MK)
E(DK_n-1, MK)
E(DK_n, MK)
记录区
1320
加密内容文件
1321
识别符记录单元
0x0001
1322
认证符记录单元
MAC
1323
密钥记录单元
E(MK, CK)
1324
内容记录单元
E(CK, CONTENT)
记录区

图12

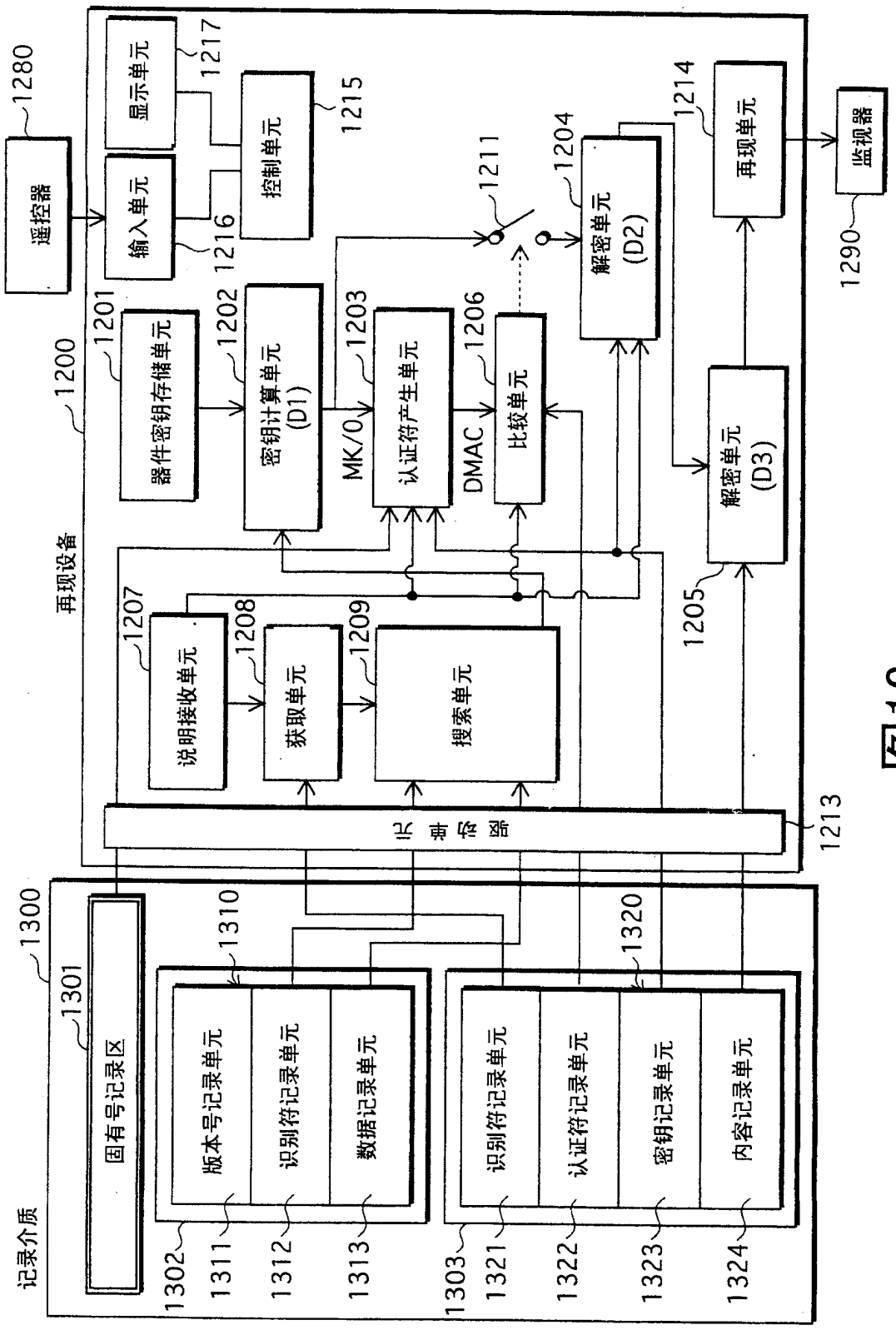

记录介质
1300
固有号记录区
1301
1310
版本号记录单元
识别符记录单元
数据记录单元
1311
1312
1313
1302
1320
识别符记录单元
认证符记录单元
密钥记录单元
内容记录单元
1321
1322
1323
1324
1303
再现设备
1200
1201
器件密钥存储单元
1202
密钥计算单元 (D1)
MK/0
1203
认证符产生单元
DMAC
1206
比较单元
1211
1204
解密单元 (D2)
1214
再现单元
1290
监视器
1205
解密单元 (D3)
1207
说明接收单元
1208
获取单元
1209
搜索单元
1213
1280
遥控器
输入单元
1216
显示单元
1217
控制单元
1215

图13

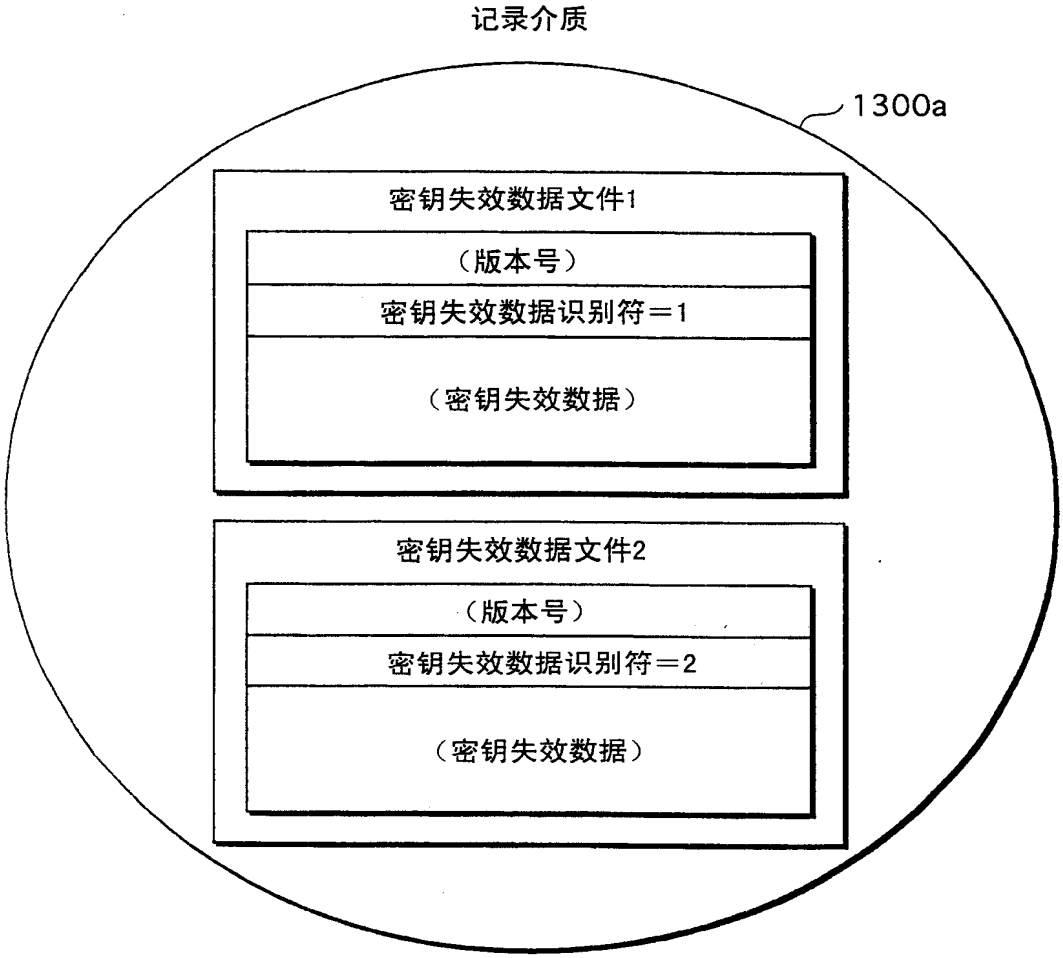

记录介质
1300a
密钥失效数据文件1
（版本号）
密钥失效数据识别符＝1
（密钥失效数据）
密钥失效数据文件2
（版本号）
密钥失效数据识别符＝2
（密钥失效数据）

图14

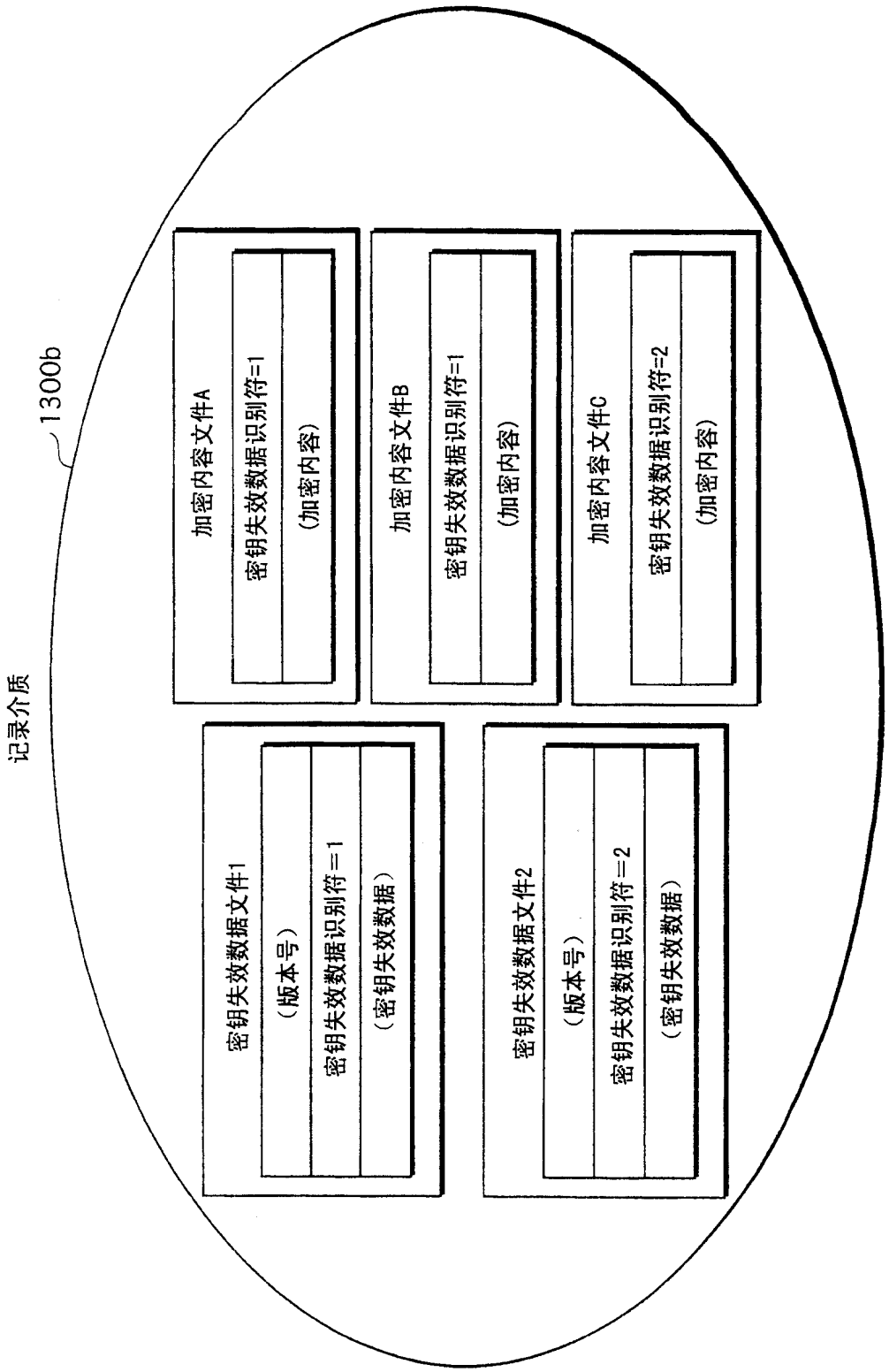

记录介质
1300b
加密内容文件A
密钥失效数据识别符=1
(加密内容)
加密内容文件B
密钥失效数据识别符=1
(加密内容)
加密内容文件C
密钥失效数据识别符=2
(加密内容)
密钥失效数据文件1
(版本号)
密钥失效数据识别符=1
(密钥失效数据)
密钥失效数据文件2
(版本号)
密钥失效数据识别符=2
(密钥失效数据)

图15

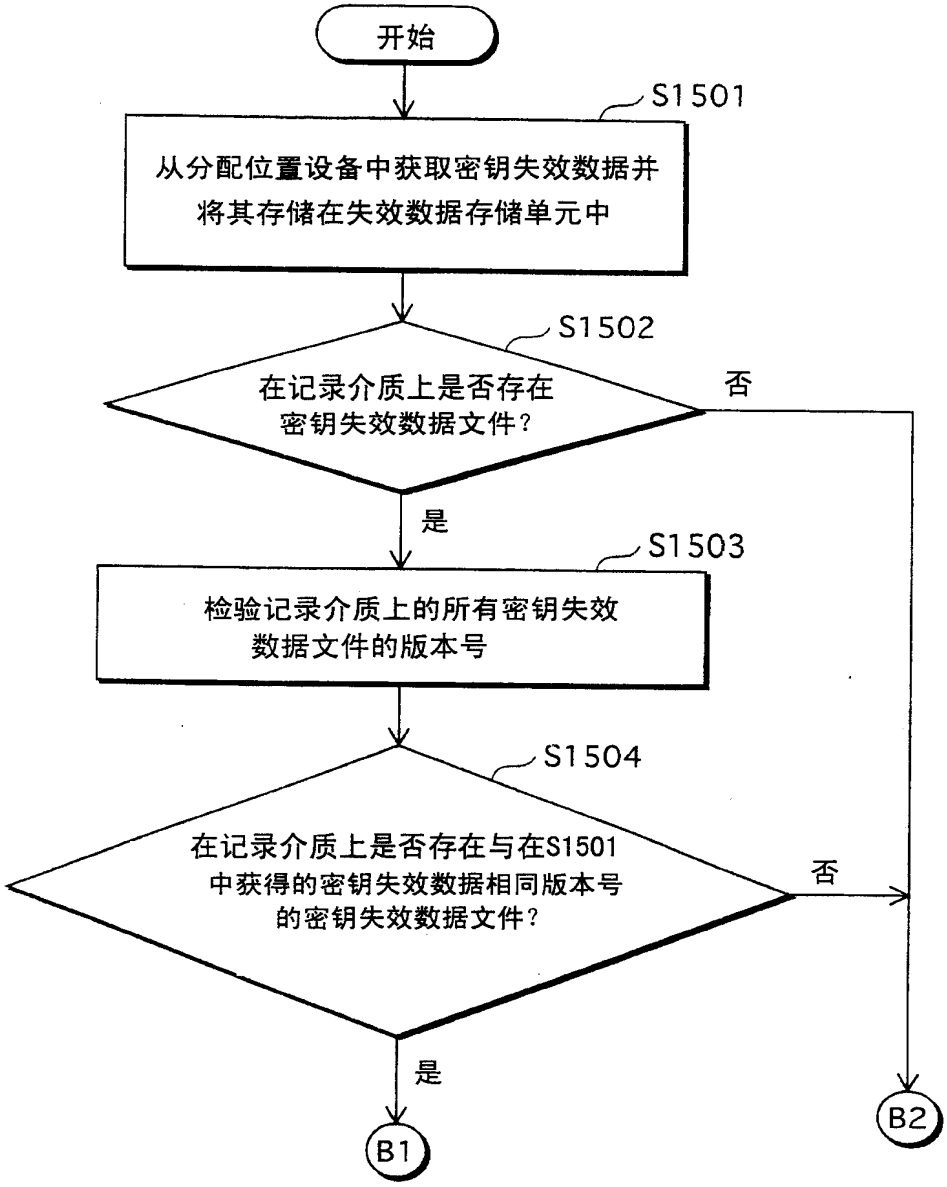

开始
S1501
从分配位置设备中获取密钥失效数据并
将其存储在失效数据存储单元中
S1502
在记录介质上是否存在
密钥失效数据文件？
否
是
S1503
检验记录介质上的所有密钥失效
数据文件的版本号
S1504
在记录介质上是否存在与在S1501
中获得的密钥失效数据相同版本号
的密钥失效数据文件？
否
是
B1
B2

图16

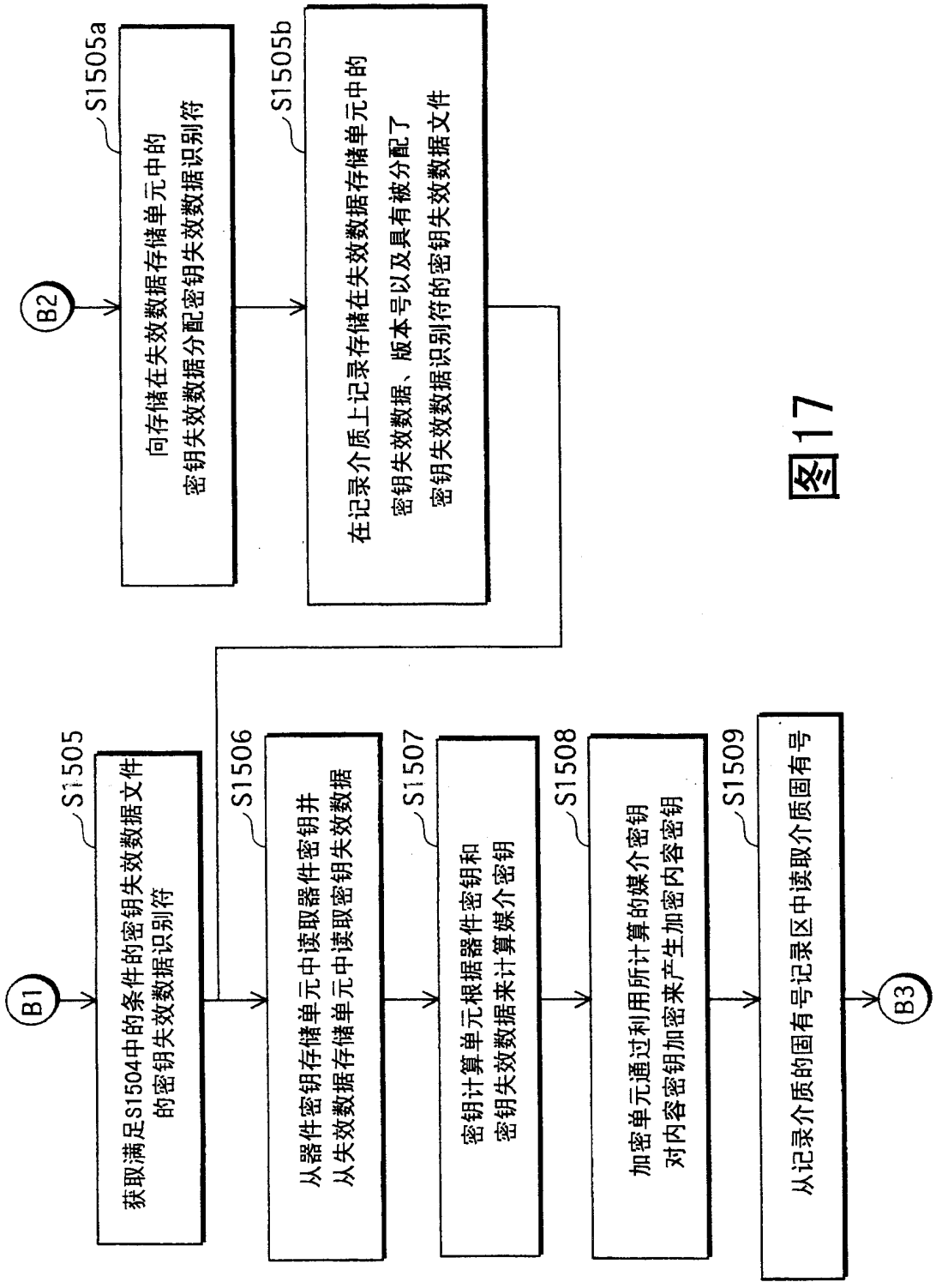

B1
S1505
获取满足S1504中的条件的密钥失效数据文件的密钥失效数据识别符
S1506
从器件密钥存储单元中读取器件密钥并从失效数据存储单元中读取密钥失效数据
S1507
密钥计算单元根据器件密钥和密钥失效数据来计算媒介密钥
S1508
加密单元通过利用所计算的媒介密钥对内容密钥加密来产生加密内容密钥
S1509
从记录介质的固有号记录区中读取介质固有号
B3
B2
S1505a
向存储在失效数据存储单元中的密钥失效数据分配密钥失效数据识别符
S1505b
在记录介质上记录存储在失效数据存储单元中的密钥失效数据、版本号以及具有被分配了密钥失效数据识别符的密钥失效数据文件

图17

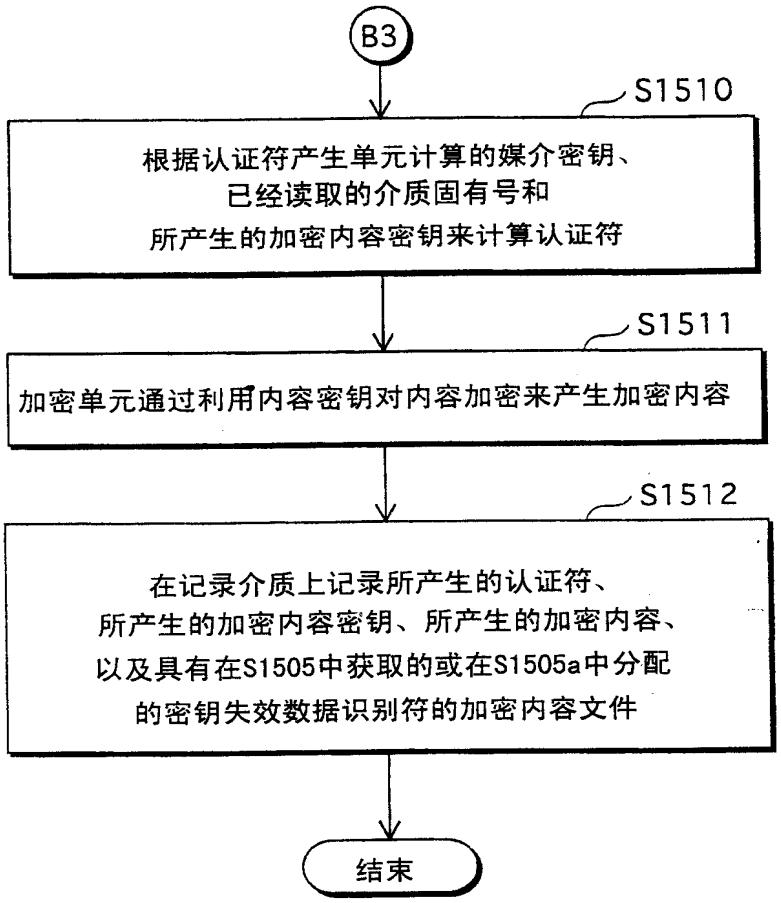

B3
S1510
根据认证符产生单元计算的媒介密钥、
已经读取的介质固有号和
所产生的加密内容密钥来计算认证符
S1511
加密单元通过利用内容密钥对内容加密来产生加密内容
S1512
在记录介质上记录所产生的认证符、
所产生的加密内容密钥、所产生的加密内容、
以及具有在S1505中获取的或在S1505a中分配
的密钥失效数据识别符的加密内容文件
结束

图18

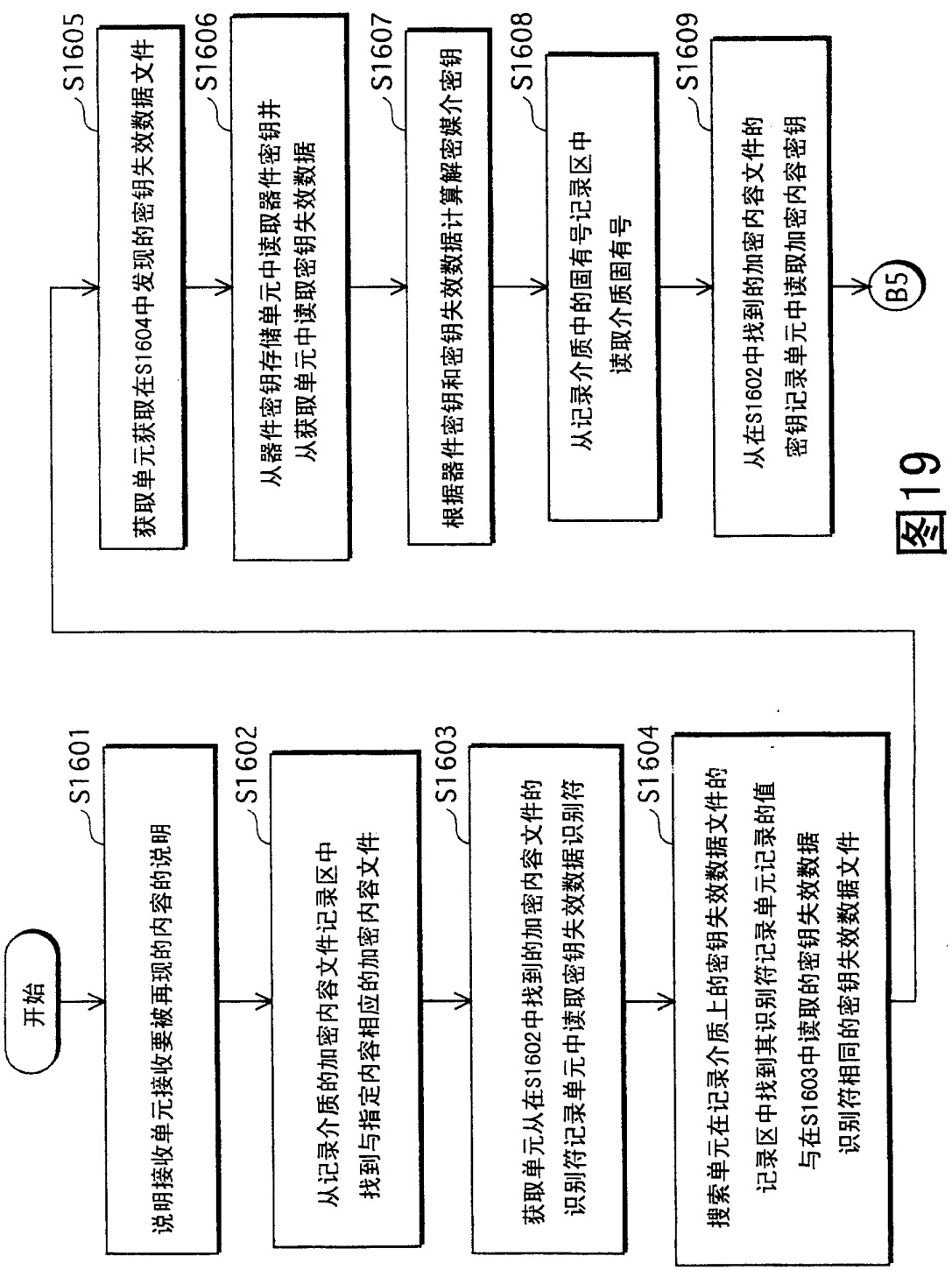

开始
S1601
说明接收单元接收要被再现的内容的说明
S1602
从记录介质的加密内容文件记录区中
找到与指定内容相应的加密内容文件
S1603
获取单元从在S1602中找到的加密内容文件的
识别符记录单元中读取密钥失效数据识别符
S1604
搜索单元在记录介质上的密钥失效数据文件的
记录区中找到其识别符记录单元记录的值
与在S1603中读取的密钥失效数据
识别符相同的密钥失效数据文件
S1605
获取单元获取在S1604中发现的密钥失效数据文件
S1606
从器件密钥存储单元中读取器件密钥并
从获取单元中读取密钥失效数据
S1607
根据器件密钥和密钥失效数据计算解密媒介密钥
S1608
从记录介质中的固有号记录区中
读取介质固有号
S1609
从在S1602中找到的加密内容文件的
密钥记录单元中读取加密内容密钥
B5

图19

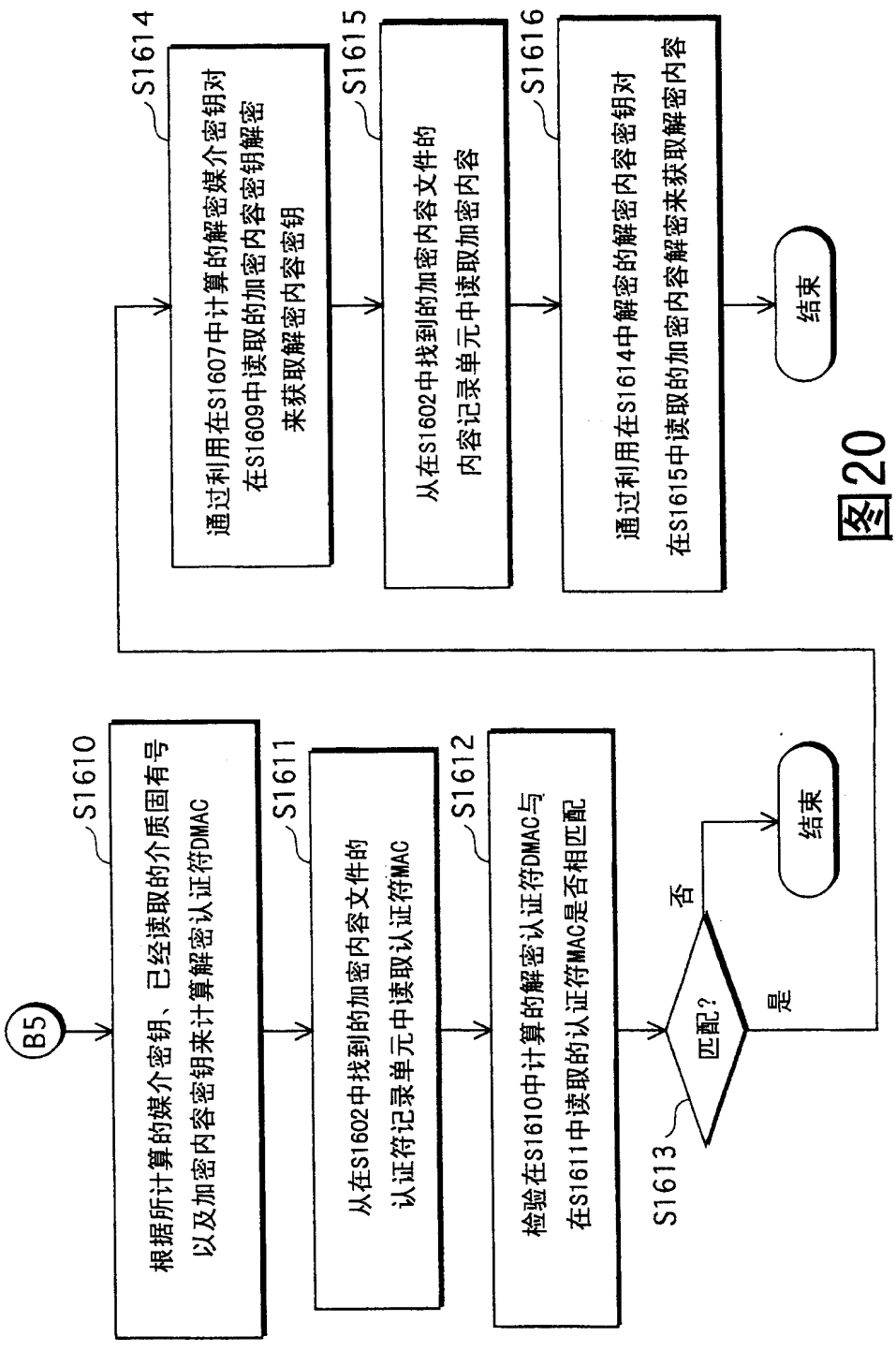

B5
S1610
根据所计算的媒介密钥、已经读取的介质固有号以及加密内容密钥来计算解密认证符DMAC
S1611
从在S1602中找到的加密内容文件的认证符记录单元中读取认证符MAC
S1612
检验在S1610中计算的解密认证符DMAC与在S1611中读取的认证符MAC是否相匹配
S1613
匹配?
否
是
结束
S1614
通过利用在S1607中计算的解密媒介密钥对在S1609中读取的加密内容密钥解密来获取解密内容密钥
S1615
从在S1602中找到的加密内容文件的内容记录单元中读取加密内容
S1616
通过利用在S1614中解密的解密内容密钥对在S1615中读取的加密内容解密来获取解密内容
结束

图20