(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101208747 B
(45)授权公告日 2011.04.13

(21)申请号 200680016939.0

(22)申请日 2006.06.28

(30)优先权数据
189053/2005 2005.06.28 JP

(85)PCT申请进入国家阶段日
2007.11.16

(86)PCT申请的申请数据
PCT/JP2006/313347 2006.06.28

(87)PCT申请的公布数据
WO2007/001087 EN 2007.01.04

(73)专利权人 株式会社东芝
地址 日本东京都
专利权人 东芝解决方案株式会社

(72)发明人 矶崎宏 松川伸一 石原淳
加藤拓

(74)专利代理机构 永新专利商标代理有限公司
72002
代理人 王英

(51)Int.Cl.
G11B 20/00(2006.01)

(56)对比文件
JP 2001216727 A,2001.08.10, 全文 .
CN 1505029 A,2004.06.16, 全文 .
US 2005038997 A1,2005.02.17, 全文 .

审查员 胡文娟

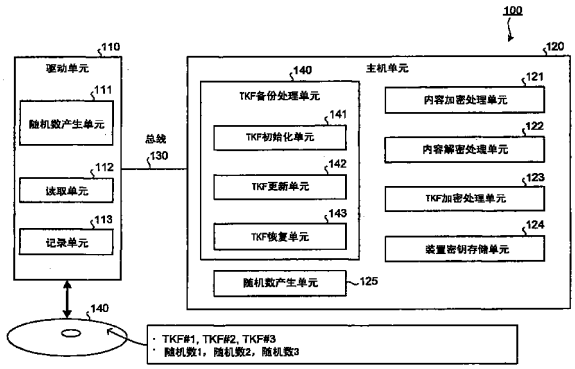
权利要求书 5 页 说明书 19 页 附图 19 页

(54)发明名称

用于记录和再生内容的装置和方法

(57)摘要

内容记录和再生装置执行记录介质的记录和再生处理，该记录介质存储在其中登记了至少一个标题密钥的标题密钥文件和通过该标题密钥加密的标题内容，该标题密钥加密对应于节目视频或声音的多个标题内容中的每一个。该内容记录和再生装置包括：TKF初始化单元，其产生标题密钥文件并将其记录在该记录介质中；随机数产生单元，其产生对应于多个标题密钥文件中的每一个的随机数；和记录单元，其在DVD介质中记录多个标题密钥文件。该TKF初始化单元登记随机数、对应于该标题密钥文件的TKF随机数和加密标题密钥。



CN 101208747 B

1. 一种内容记录和再生装置，包括：

记录和再生单元，其执行记录介质的记录和再生，其中，所述记录介质记录有在其中登记了至少一个标题密钥的标题密钥文件和通过所述标题密钥加密的标题内容，所述标题密钥加密对应于节目视频或声音的多个标题内容中的每一个；

密钥文件产生单元，其产生多个标题密钥文件，并且在所述多个标题密钥文件的每一个中登记所述至少一个标题密钥；

第一随机数产生单元，其产生第一随机数，该第一随机数是与所述多个标题密钥文件中的每一个对应的一个随机数；以及

第二随机数产生单元，其产生第二随机数，该第二随机数是不同于所述第一随机数的一个随机数，该第二随机数与所述多个标题密钥文件中的每一个对应并且用于加密与所述多个标题密钥文件中的每一个相关联的另一标题密钥文件，

其中，所述密钥文件产生单元在所述多个标题密钥文件的每一个中登记对应于所述多个标题密钥文件中每一个的所述第一随机数、对应于所述多个标题密钥文件中每一个的所述第二随机数以及加密的标题密钥，其中，通过利用在所述多个标题密钥文件的每一个中登记的所述第一随机数和在除了登记有所述第一随机数的该标题密钥文件之外的、与所述多个标题密钥文件中的每一个相关联的另一标题密钥文件中登记的第二随机数来加密所述标题密钥，从而形成所述加密的标题密钥，

并且所述记录和再生单元在所述记录介质中记录所述多个标题密钥文件。

2. 如权利要求 1 所述的装置，其中，第一标题密钥文件与第三标题密钥文件相关联，第二标题密钥文件与所述第一标题密钥文件相关联，所述第三标题密钥文件与所述第二标题密钥文件相关联，以及

所述密钥文件产生单元还：

在所述第一标题密钥文件中登记对应于所述第一标题密钥文件的第一加密标题密钥、对应于所述第一标题密钥文件的所述第一随机数和对应于所述第一标题密钥文件的所述第二随机数，其中，通过利用在所述第一标题密钥文件中登记的第一随机数和在所述第三标题密钥文件中登记的第二随机数来加密所述标题密钥，从而形成所述第一加密标题密钥；

在所述第二标题密钥文件中登记对应于所述第二标题密钥文件的第二加密标题密钥、对应于所述第二标题密钥文件的所述第一随机数和对应于所述第二标题密钥文件的所述第二随机数，其中，通过利用在所述第二标题密钥文件中登记的第一随机数和在所述第一标题密钥文件中登记的第二随机数来加密所述标题密钥，从而形成所述第二加密标题密钥；并且

在所述第三标题密钥文件中登记对应于所述第三标题密钥文件的第三加密标题密钥、对应于所述第三标题密钥文件的所述第一随机数和对应于所述第三标题密钥文件的所述第二随机数，其中，通过利用在所述第三标题密钥文件中登记的第一随机数和在所述第二标题密钥文件中登记的第二随机数来加密所述标题密钥，从而形成所述第三加密标题密钥。

3. 如权利要求 1 所述的装置，其中，第一标题密钥文件与第二标题密钥文件相关联，所述第二标题密钥文件与所述第一标题密钥文件相关联，并且

所述密钥文件产生单元还：

在所述第一标题密钥文件中登记对应于所述第一标题密钥文件的第一加密标题密钥、对应于所述第一标题密钥文件的所述第一随机数和对应于所述第一标题密钥文件的所述第二随机数，其中通过利用在所述第一标题密钥文件中登记的第一随机数和在所述第二标题密钥文件中登记的第二随机数来加密所述标题密钥，从而形成所述第一加密标题密钥；并且

在所述第二标题密钥文件中登记对应于所述第二标题密钥文件的第二加密标题密钥、对应于所述第二标题密钥文件的所述第一随机数和对应于所述第二标题密钥文件的所述第二随机数，其中通过利用在所述第二标题密钥文件中登记的第一随机数和在所述第一标题密钥文件中登记的第二随机数来加密所述标题密钥，从而形成所述第二加密标题密钥。

4. 如权利要求 1 所述的装置，还包括：

解密单元，当将新的标题密钥添加到所述记录介质时，或者当从所述记录介质删除任意标题密钥时，所述解密单元通过利用由所述记录和再生单元读取的所述多个标题密钥文件的每一个中所登记的所述第一随机数以及在与所述多个标题密钥文件的每一个相关联的另一标题密钥文件中登记的第二随机数来解密在所述多个标题密钥文件的每一个中登记的加密的标题密钥；

重新加密单元，其通过利用新的第一随机数和与所述另一标题密钥文件相关联的新的第二随机数来加密经解密的标题密钥，从而产生新的加密的标题密钥；以及

更新单元，其通过在所述多个标题密钥文件中登记所述新的加密的标题密钥、所述新的第一随机数和所述新的第二随机数来更新所述多个标题密钥文件，

其中，所述第一随机数产生单元产生与所述多个标题密钥文件中的每一个相关联的所述新的第一随机数，

所述第二随机数产生单元产生与所述新的第一随机数不同的所述新的第二随机数，所述新的第二随机数与所述多个标题密钥文件中的每一个相关联，并且

所述记录和再生单元在所述记录介质中记录通过所述更新单元而更新的所述多个标题密钥文件。

5. 如权利要求 4 所述的装置，其中，第一标题密钥文件与第三标题密钥文件相关联，第二标题密钥文件与所述第一标题密钥文件相关联，所述第三标题密钥文件与所述第二标题密钥文件相关联，以及

当将新的标题密钥添加到所述记录介质时，或者当从所述记录介质删除任意标题密钥时，所述解密单元还通过利用由所述记录和再生单元读取的所述第一标题密钥文件中所登记的所述第一随机数和在所述第三标题密钥文件中登记的所述第二随机数来解密在所述第一标题密钥文件中登记的加密的标题密钥，以及

所述重新加密单元：

通过利用对应于所述第一标题密钥文件的所述新的第一随机数和对应于所述第三标题密钥文件的所述新的第二随机数来加密在所解密的标题密钥文件中登记的标题密钥，从而产生所述第一标题密钥文件中的所述新的加密的标题密钥；

通过利用对应于所述第二标题密钥文件的所述新的第一随机数和对应于所述第一标

题密钥文件的所述新的第二随机数来加密在所解密的标题密钥文件中登记的所述标题密钥，从而产生所述第二标题密钥文件中的所述新的加密的标题密钥；并且

通过利用对应于所述第三标题密钥文件的所述新的第一随机数和对应于所述第二标题密钥文件的所述新的第二随机数来加密在所解密的标题密钥文件中登记的标题密钥，从而产生所述第三标题密钥文件中的所述新的加密的标题密钥。

6. 如权利要求 4 所述的装置，其中，第一标题密钥文件与第二标题密钥文件相关联，所述第二标题密钥文件与所述第一标题密钥文件相关联，以及

当将新的标题密钥添加到所述记录介质时，或者当从所述记录介质删除任意标题密钥时，所述解密单元还通过利用由所述记录和再生单元读取的所述第一标题密钥文件中所登记的第一随机数和在所述第二标题密钥文件中登记的第二随机数来解密在所述第一标题密钥文件中登记的所述加密的标题密钥，以及

所述重新加密单元：

通过利用对应于所述第一标题密钥文件的所述新的第一随机数和对应于所述第二标题密钥文件的所述新的第二随机数来加密在所解密的标题密钥文件中登记的所述标题密钥，从而产生所述第一标题密钥文件中的所述新的加密标题密钥；以及

通过利用对应于所述第二标题密钥文件的所述新的第一随机数和对应于所述第一标题密钥文件的所述新的第二随机数来加密在所解密的标题密钥文件中登记的所述标题密钥，从而产生所述第二标题密钥文件中的所述新的加密标题密钥。

7. 如权利要求 4 所述的装置，其中，所述标题密钥文件还登记指示所述标题密钥的版本的世代，以及

当由所述记录和再生单元读取的所述多个标题密钥文件的所有世代彼此一致时，所述更新单元更新所述多个标题密钥文件。

8. 如权利要求 4 所述的装置，其中，当在所述记录介质中记录的所述多个标题密钥文件中一个任意标题密钥文件不存在或被破坏时，所述解密单元通过利用在与该任意标题密钥文件相关联的第一另一标题密钥文件中所登记的第一随机数和与该第一另一标题密钥文件相关联的第二另一标题密钥文件中所登记的第二随机数来解密在该第一另一标题密钥文件中登记的所述加密的标题密钥，

所述记录和再生单元还包括恢复单元，其通过将由所述重新加密单元加密的所述新的加密的标题密钥、由所述第一随机数产生单元产生的所述新的第一随机数和由所述第二随机数产生单元产生的所述新的第二随机数登记到所述多个标题密钥文件中，来恢复所述多个标题密钥文件，以及

所述记录和再生单元在所述记录介质中记录通过所述恢复单元恢复的所述多个标题密钥文件。

9. 如权利要求 8 所述的装置，其中，第一标题密钥文件与第三标题密钥文件相关联，第二标题密钥文件与所述第一标题密钥文件相关联，所述第三标题密钥文件与所述第二标题密钥文件相关联，以及

当在所述记录介质中不存在所述第一标题密钥或所述第一标题密钥被破坏时，所述解密单元通过利用存在于所述记录介质中的所述第三标题密钥文件中所登记的第一随机数和在所述第二标题密钥文件中登记的第二随机数来解密在所述第三标题密钥文件中登

记的所述加密的标题密钥，以及

所述重新加密单元：

通过利用对应于所述第一标题密钥文件的所述新的第一随机数和对应于所述第三标题密钥文件的所述新的第二随机数来加密在所解密的第三标题密钥文件中登记的标题密钥，从而产生所述第一标题密钥文件中的所述新的加密的标题密钥；

通过利用对应于所述第二标题密钥文件的所述新的第一随机数和对应于所述第一标题密钥文件的所述新的第二随机数来加密在所解密的第三标题密钥文件中登记的标题密钥，从而产生所述第二标题密钥文件中的所述新的加密的标题密钥；并且

通过利用对应于所述第三标题密钥文件的所述新的第一随机数和对应于所述第二标题密钥文件的所述新的第二随机数来加密在所解密的第三标题密钥文件中登记的所述标题密钥，从而产生所述第三标题密钥文件中的所述新的加密的标题密钥。

10. 如权利要求 8 所述的装置，其中，第一标题密钥文件与第二标题密钥文件相关联，所述第二标题密钥文件与所述第一标题密钥文件相关联，以及

当在所述记录介质中不存在所述第一标题密钥文件或所述第一标题密钥文件被破坏时，所述解密单元通过利用存在于所述记录介质中的所述第二标题密钥文件中所登记的第一随机数和在所述第一标题密钥文件中登记的第二随机数来解密在所述第二标题密钥文件中登记的所述加密的标题密钥，以及

所述重新加密单元：

通过利用对应于所述第一标题密钥文件的所述新的第一随机数和对应于所述第二标题密钥文件的所述新的第二随机数来加密在所解密的第二标题密钥文件中所登记的所述标题密钥，从而产生所述第一标题密钥文件中的所述新的加密的标题密钥；以及

通过利用对应于所述第二标题密钥文件的所述新的第一随机数和对应于所述第一标题密钥文件的所述新的第二随机数来加密在所解密的第二标题密钥文件中登记的所述标题密钥，从而产生所述第二标题密钥文件中的所述新的加密的标题密钥。

11. 如权利要求 8 所述的装置，其中，所述标题密钥文件还登记指示所述标题密钥的版本的世代，以及

当由所述记录和再生单元读取的所述多个标题密钥文件的世代中的任何一个彼此不一致时，所述恢复单元恢复所述多个标题密钥文件。

12. 如权利要求 8 所述的装置，其中，所述记录介质包括不能在其中写入任意值的受保护区域和可以通过任意应用程序在其中记录任意值的用户区域，

所述记录和再生单元在所述受保护区域中记录所述标题密钥文件的第一随机数，在所述用户区域中记录所述第二随机数，并且当记录除所述标题密钥文件之外的文件时，将指示不正确记录的不正确信息作为第一随机数记录在所述受保护区域中，以及

当解密所述加密的标题密钥时，所述恢复单元确定所述不正确信息是否记录在所述第一随机数中，并且当记录了所述不正确信息时不恢复所述多个标题密钥文件。

13. 一种记录和再生内容的方法，包括：

执行记录介质的记录和再生，其中，所述记录介质记录在其中登记了至少一个标题密钥的标题密钥文件以及利用所述标题密钥加密的标题内容，所述标题密钥加密对应于节目视频或声音的多个标题内容中的每一个；

产生多个标题密钥文件，并在所述多个标题密钥文件的每一个中登记所述至少一个标题密钥；

产生第一随机数，该第一随机数是与所述多个标题密钥文件中的每一个相对应的一个随机数；

产生第二随机数，该第二随机数是不同于所述第一随机数的一个随机数，该第二随机数与所述多个标题密钥文件中的每一个相对应并且用于加密与所述多个标题密钥文件的每一个相关联的另一标题密钥文件；

在所述多个标题密钥文件的每一个中登记对应于所述多个标题密钥文件中每一个的第一随机数、对应于所述多个标题密钥文件中每一个的第二随机数和加密的标题密钥，其中，通过利用对应于所述多个标题密钥文件中每一个的第一随机数和对应于除了登记有所述第一随机数的该标题密钥文件之外的、与所述多个标题密钥文件中每一个相关联的另一标题密钥文件的第二随机数来加密所述标题密钥，从而形成所述加密的标题密钥；以及

在所述记录介质中记录所述多个标题密钥文件。

用于记录和再生内容的装置和方法

技术领域

[0001] 本发明涉及用于记录和再生记录介质的内容记录和再生装置、内容记录和再生方法以及内容记录和再生程序产品，其中，该记录介质记录在其中登记了至少一个标题密钥的标题密钥文件和通过该标题密钥加密的标题内容，该标题密钥将对应于节目视频或声音的多个标题内容中的每一个进行加密。

[0002] 背景技术

[0003] 如非专利文档 1 中所披露的，为了防止未经授权对记录在诸如 DVD（数字多功能光盘）的记录介质中的内容进行拷贝，传统地存在一种公知技术，其中，利用不同的标题密钥对作为节目视频或者声音的内容的多个标题内容的每一个执行加密处理，并在 DVD 介质中记录所加密的标题内容。

[0004] 在非专利文档 1 所披露的技术中，利用设备密钥和随机数对多个标题密钥的每一个进行加密，并将所加密的标题密钥和随机数登记在该标题密钥文件中且记录在 DVD 介质中。 在正确记录并再生内容的每一个记录和再生装置诸如 DVD 刻录机中告知设备密钥。 该随机数被随机产生。 在再生标题内容的情形下，利用该随机数和用于再生的记录和再生装置的设备密钥对在该标题密钥文件中登记的所加密的标题密钥进行解密，并利用所解密的标题密钥来解密所述标题内容，以再生所述标题内容。

[0005] 在可重写的 DVD 介质中删除所述标题内容的一部分的情形下，更新该标题密钥文件。 特别地，一旦该标题密钥文件被解密，则最新产生随机数，使用利用该新的随机数和该设备密钥被再次加密的设备密钥删除该标题密钥文件，并在该 DVD 介质中记录该标题密钥文件，其中，该标题密钥对应于从该 DVD 介质删除的标题内容。 因此，可以防止以下攻击，其中：对应于所删除的标题内容的该标题密钥被预先拷贝，并且利用所拷贝的标题密钥不适当地再生所删除的标题内容。

[0006] 类似利用标题密钥的此内容保护是用于防止未经授权地使用 DVD 介质中的内容的有效技术。 然而，在由于 DVD 介质内的瑕疵和裂纹导致无法读取区域部分并从而无法读取该标题密钥文件的情形下，或在用户由于错误操作删除了该标题密钥文件的情形下，将无法解密所述标题内容，并无法执行再生操作。 因此，在 DVD 介质中将该标题密钥文件的拷贝记录为备份文件，并在由于该标题密钥文件破损或类似原因而无法读取该标题密钥文件时将该备份文件用作该标题密钥文件。

[0007] [非专利文档 1：Advanced Access Content System（AACS）Recordable Video Book Revision 0.90]

发明内容

[0008] 本发明需要解决的问题

[0009] 然而，仅当在该 DVD 介质中记录该标题密钥文件的简单备份文件时，才允许未经授权的再生所述内容。 例如，假定攻击者先前在另一个介质中拷贝了该标题密钥文件的备份文件。 在此情形下，当以一般的方式将标题内容的部分移到另一个介质中时，更

新标题密钥文件，其中删除对应于所移动的标题内容的标题密钥。 在这点上，该攻击者自该 DVD 介质删除该标题密钥文件，并且该攻击者在该 DVD 介质中恢复在另一个介质中拷贝的备份文件。 因为在该 DVD 介质中不存在原始的标题密钥文件，因此根据该备份文件该记录和再生装置恢复该标题密钥文件。 由于该备份文件是在更新之前产生的标题密钥文件，因此将错误地恢复对应于应该自该 DVD 介质删除的标题内容的标题密钥。

[0010] 考虑以上描述，本发明的目的是提供内容记录和再生装置、内容记录和再生方法以及内容记录和再生程序产品，在安全地恢复该标题密钥文件时，其可以防止恶意的第三方不正确地恢复内容。

[0011] 用于解决问题的方式

[0012] 根据本发明的一个方面，内容记录和再生装置包括：记录和再生单元，其执行记录介质的记录和再生，其中，所述记录介质记录有在其中登记了至少一个标题密钥的标题密钥文件和通过所述标题密钥加密的标题内容，所述标题密钥加密对应于节目视频或声音的多个标题内容中的每一个：密钥文件产生单元，其产生至少一个标题密钥文件，并且在所产生的标题密钥文件中登记至少一个标题密钥；随机数产生单元，其产生与所述多个标题密钥文件中的每一个对应的随机数；以及 TKF 随机数产生单元，其产生用于加密与所述标题密钥文件相关联的其它标题密钥文件的 TKF 随机数，其中，所述记录和再生单元在所述记录介质中记录一组所产生的标题密钥文件和所述随机数，以及所述密钥文件产生单元登记对应于所述标题密钥文件的所述随机数、对应于所述标题密钥文件的所述 TKF 随机数以及加密的标题密钥，其中，通过利用在所述标题密钥文件中登记的随机数和在所述其它标题密钥文件中登记的 TKF 随机数来加密所述标题密钥，从而形成所述加密的标题密钥。

[0013] 根据本发明的另一个方面，一种记录和再生内容的方法包括：执行记录介质的记录和再生，其中，所述记录介质记录在其中登记了至少一个标题密钥的标题密钥文件以及利用所述标题密钥加密的标题内容，所述标题密钥加密对应于节目视频或声音的多个标题内容中的每一个；产生至少一个标题密钥文件，并在所产生的标题密钥文件中登记至少一个所述标题密钥；产生对应于所述多个标题密钥文件中的每一个的随机数；产生用于加密其它标题密钥文件的 TKF 随机数；在所述记录介质中记录一组所产生的标题密钥文件和所述随机数；以及登记对应于所述标题密钥文件的随机数、对应于所述标题密钥文件的 TKF 随机数和加密的标题密钥，其中，通过利用对应于所述标题密钥文件的随机数和对应于所述其它标题密钥文件的 TKF 随机数来加密所述标题密钥，从而形成所述加密的标题密钥。

[0014] 仍根据本发明的另一个方面的计算机程序产品使得计算机执行根据本发明的方法。

附图说明

[0015] 图 1 是示出根据第一实施例的内容记录和再生装置的配置的框图；

[0016] 图 2 是示出扇区结构的说明图；

[0017] 图 3 是示出在 DVD 介质中写入随机数的处理的过程的顺序图；

[0018] 图 4A 是示出第一实施例的标题密钥文件和备份文件的结构的说明图；

[0019] 图 4B 是示出加密的密钥文件的数据结构的说明图；

[0020] 图 5 是示出初始化标题密钥文件（TKF）备份的处理的过程的流程图；

[0021] 图 6A 是示出更新该标题密钥文件（TKF）备份的处理的过程的流程图；

[0022] 图 6B 是示出在通过重新产生的随机数 1 解密和加密标题密钥文件 TKF#1 之后，在该 DVD 介质中写入标题密钥文件 TKF#1 和重新产生的随机数 1 的过程的顺序图；

[0023] 图 7 是示出恢复该标题密钥文件（TKF）备份的处理的整个过程的流程图；

[0024] 图 8 是示出通过备份文件 TKF#3 执行的恢复处理的过程的流程图；

[0025] 图 9 是示出通过备份文件 TKF#1 执行的恢复处理的过程的流程图；

[0026] 图 10 是示出通过备份文件 TKF#2 执行的恢复处理的过程的流程图；

[0027] 图 11 是示出在每次更新世代时产生随机数的情形下初始化标题密钥文件（TKF）备份的处理的整个过程的流程图；

[0028] 图 12 是示出第二实施例的标题密钥文件和备份文件的结构的说明图；

[0029] 图 13 是示出初始化该标题密钥文件（TKF）备份的处理的过程的流程图；

[0030] 图 14 是示出更新第二实施例的标题密钥文件（TKF）备份的处理的过程的流程图；

[0031] 图 15 是示出恢复第二实施例的标题密钥文件（TKF#1）的处理的整个过程的流程图；

[0032] 图 16 是示出通过第二实施例的备份文件 TKF#2 和 TKF#3 执行的恢复处理的过程的流程图；

[0033] 图 17 是示出通过第二实施例的标题密钥文件 TKF#1 和备份文件 TKF#3 执行的恢复处理的过程的流程图；

[0034] 图 18 是示出通过第二实施例的标题密钥文件 TKF#1 和备份文件 TKF#2 执行的恢复处理的过程的流程图；以及

[0035] 图 19 是示出内容记录和再生装置的配置的框图，其中，通过以内部总线连接驱动单元和主机单元来整体形成该驱动单元和主机单元。

具体实施方式

[0036] 参考附图，将详细描述内容记录和再生装置、内容记录和再生方法以及内容记录和再生程序产品的最佳模式。

[0037] （第一实施例）

[0038] 图 1 是示出根据第一实施例的内容记录和再生装置 100 的配置的框图。 在此，可以将执行 DVD 介质的记录和再生的 DVD 刻录机例示成该内容记录和再生装置 100 的例子。 如图 1 所示，在根据第一实施例的内容记录和再生装置 100 的配置中，驱动单元 110 和主机单元 120 通过总线 130 连接。 该驱动单元 110 在可重写的 DVD 介质 140 中记录数据，并且该驱动单元 110 从该 DVD 介质 140 中读取数据。 该主机单元 120 将该标题内容进行加密和解码，并且该主机单元 120 执行标题密钥文件（TKF）的备份处理。

[0039] 如图 1 所示，在该 DVD 介质 140 中记录标题密钥文件（TKF#1）、TKF#2 和 TKF#3 以及随机数 1 至 3。 TKF#2 和 TKF#3 是该标题密钥文件的备份文件。 随后将描述该标题密钥文件（TKF#1）、TKF#2 和 TKF#3 以及随机数 1 至 3。

[0040] 符合 HD-DVD（高密度数字多功能光盘）视频记录标准的 DVD 介质是用于第一实施例的内容记录和再生装置 100 中的 DVD 介质 140 的目标格式。 然而，该 DVD 介质 140 并不总是限于符合该 HD-DVD 视频记录标准的 DVD 介质。

[0041] 该驱动单元 110 主要包括随机数产生单元 111、读出单元 112 和记录单元 113。该随机数产生单元 111 随机地产生随机数，该读出单元 112 直接从该 DVD 介质 140 读取数据，而该记录单元 113 直接在该 DVD 介质 140 中记录数据。

[0042] 如图 1 所示，该主机单元 120 主要包括内容加密处理单元 121、内容解密处理单元 122、 TKF 加密处理单元 123、设备密钥存储单元 124、备份处理单元 140 和随机数产生单元 125。

[0043] 该内容加密处理单元 121 是利用该标题密钥来加密标题内容的处理单元。 该内容解密处理单元 122 是利用该标题密钥来解密所加密的标题内容的处理单元。

[0044] 如此处所使用的，标题内容表示一组视频或声音内容诸如过程。 例如，一个电影的内容变成一个标题内容。 该标题密钥是用于加密标题内容的密钥。 在每一个情形下，将不同的标题密钥用于所述标题内容。 通过相同的标题密钥可以加密多个标题。

[0045] 该 TKF 加密处理单元 123 是加密该标题密钥文件 (TKF) 的处理单元。 如此处所使用的，该标题密钥文件 (TKF) 表示通过随机数和由该内容记录和再生装置 100 持有的设备密钥加密的一组至少一个标题密钥，并且用于加密的该组标题密钥和随机数是所登记的文件。 在该标题密钥文件中登记随后提及的随机数、TKF 随机数和至少一个标题密钥，并且在该 DVD 介质 140 中记录该标题密钥文件。 该 TKF 随机数产生除了该标题密钥文件本身之外的文件或备份文件的加密的标题密钥。 参考图 4A 和图 4B，随后将详细描述该详细的标题密钥文件。

[0046] 返回图 1，该设备密钥存储单元 124 是在其中存储设备密钥的记录介质诸如存储器。 如此处所使用的，该设备密钥表示先前被给予该形式内容记录和再生装置 100 的密钥，并且该设备密钥还表示用于加 密和解密该标题密钥文件的标题密钥的密钥。

[0047] 该 TKF 备份处理单元 140 是为在该 DVD 介质 140 中记录的标题密钥文件 (TKF) 执行备份处理的处理单元。 该 TKF 备份处理单元 140 主要包括 TKF 初始化单元 141、TKF 更新单元 142 和 TKF 恢复单元 143。

[0048] 该 TKF 初始化单元 141 是用于产生标题密钥文件 (TKF#1) 和标题密钥文件 TKF#2 以及 TKF#3 的处理单元。 在该 DVD 介质 140 中记录该标题密钥文件 (TKF#1)，而该标题密钥文件 TKF#2 和 TKF#3 是备份文件。

[0049] 当通过删除或增加该 DVD 介质 140 中的一部分标题内容来改变标题密钥列表时，更新该标题密钥文件。 该 TKF 更新单元 142 是用于重新产生并更新该标题密钥文件 TKF#1 和作为备份文件的标题密钥文件 TKF#2 及 TKF#3 的处理单元。

[0050] 该 TKF 恢复单元 143 是用于在该标题密钥文件 TKF#1 和作为备份文件的标题密钥文件 TKF#2 及 TKF#3 的一个在该 DVD 介质 140 中被破坏的情形下，或在该标题密钥文件 TKF#1 和作为备份文件的标题密钥文件 TKF#2 及 TKF#3 的一个不存在于该 DVD 介质 140 中的情形下，根据该标题密钥文件 TKF#1 和作为备份文件的标题密钥文件 TKF#2 及 TKF#3 的一个来再生标题密钥，以恢复该标题密钥文件和作为备份文件的标题密钥文件的处理单元。 该随机数产生单元 125 是用于产生随后提及的 TKF 随机数的处理单元。

[0051] 以下将描述该 DVD 介质 140 的扇区结构组成数据。 在该 DVD 介质 140 中记录该数据，同时将该数据分成称作为扇区的具有固定长度的片数据。 该 DVD 介质 140 上的任一片数据以扇区单元进行读取和写入。 图 2 是示出扇区结构的说明图。 如图 2 所示，一个扇区包括具有 M 字节固定长度的管理扇区报头和具有 N 字节的数据。 将该数据记录在可以以任意应用程序读取和写入的用户区域中，将该扇区报头的部分记录在无法从外部写入任意值的受保护的区域中。 可以将图 3 所示的协议用作致使无法从外部写入任意值的机制。 图 3 是示出在该 DVD 介质 140 中写入随机数的处理的过程的顺序图。

[0052] 首先，将随机数产生命令从该主机单元 120 传输到该驱动单元 110（步骤 S301）。在接收该随机数产生命令的驱动单元 110 中，该随机数产生单元 111 产生该随机数（步骤 S302），并将所产生的随机数暂时存储在该随机数产生单元 111 中。 该主机单元 120 将随机数写入命令传输给该驱动单元 110（步骤 S303）。 在此点上，随机数的值不包括在该随机数写入命令中。 在接收该随机数写入命令的驱动单元 110 中，该记录单元 113 在该 DVD 介质 140 中写入暂时存储的随机数（步骤 S304）。 因为该随机数不包括在该随机数写入命令中，因此可以防止将除了通过该驱动单元 110 产生的值之外的值写入该 DVD 介质 140 中。

[0053] 以下将描述第一实施例的标题密钥文件备份。 图 4A 是示出第一实施例的标题密钥文件和是备份文件的标题密钥文件的结构的说明图。 在以下描述中，出于简便的目的，将是备份文件的标题密钥文件 TKF#2 和 TKF#3 简单称作为备份文件 TKF#2 和 TKF#3。 在第一实施例中，该 TKF 初始化单元 141 将在该 DVD 介质 140 中记录的标题密钥文件 (TKF#1) 的备份文件产生为 TKF#2 和 TKF#3，并且该驱动单元 110 的记录单元 113 在该 DVD 介质 140 中存储这三个文件 TKF#1、TKF#2 和 TKF#3。

[0054] 标题密钥文件 (TKF#1) 和备份文件 TKF#2 及 TKF#3 的每一个具有在其中登记随机数 1 至 3(BN1、BN2 和 BN3)、世代 (generation)、TKF 随机数 1 至 3 和加密的标题密钥 (ETK1 至 3) 的配置。 该驱动单元 110 的随机数产生单元 111 通过接收主机单元 120 的要求而随机产生随机数 1 至 3(BN1、BN2 和 BN3)，该驱动单元 110 的记录单元 113 在该 DVD 介质 140 中记录所述随机数 1 至 3(BN1、BN2 和 BN3)。 该世代表示该标题密钥文件 (TKF#1) 和备份文件 TKF#2 及 TKF#3 的改变次数。

[0055] TKF 随机数 1 至 3(TKFN1、 TKFN2 和 TKFN3) 是分别计算除了本身文件的除 TKF 随机数 1 至 3(TKFN1、 TKFN2 和 TKFN3) 之外的文件或备份文件的加密的标题密钥 (ETK1、ETK2 和 ETK3) 的随机数。 该驱动单元 110 的随机数产生单元 125 产生所述 TKF 随机 数 1 至 3。

[0056] 加密的标题密钥 (ETK1、 ETK2 和 ETK3) 是利用在该标题密钥文件或备份文件中登记的随机数 1 至 3(BN1、BN2 和 BN3) 或利用在另一个文件中登记的相关的 TKF 随机数 1 至 3(TKFN1、TKFN2 和 TKFN3) 进行加密的标题密钥文件的所有标题密钥的数据。图 4B 是示出加密的标题密钥 (ETK1、 ETK2 和 ETK3) 的结构的说明图。 如图 4 所示，每一个加密的标题密钥 (ETK1、 ETK2 和 ETK3) 是被加密的每一个标题密钥 1 至 n 中的一个。 通过公式 (1) 至 (3) 表示所加密的标题密钥 (ETK1、ETK2 和 ETK3)。

[0057] $ETK1 = f(TK, BN1, TKFN3)$ (1)

[0058] $ETK2 = f(TK, BN2, TKFN1)$ (2)

[0059] ETK3 = f(TK, BN3, TKFN2) (3)

[0060] 其中 TK 指示纯文本的标题密钥，而 f 指示利用作为加密密钥的第二参数 (BN1 至 BN3) 和第三参数 (TKFN1 至 TKFN3) 对第一参数 (TK) 执行加密处理。 可以将众所周知的加密算法诸如 AES(高级加密标准) 用于该加密处理 f。

[0061] TKF#1 与 TKF#3 相关，以随机数 1(BN1) 和相关的 TKF#3 的 TKF 随机数 3(TKFN3) 加密该标题密钥 (TK)。 TKF#2 与 TKF#1 相关，以随机数 2(BN2) 和该相关的 TKF#1 的 TKF 随机数 1(TKFN1) 加密该标题密钥 (TK)。 TKF#3 与 TKF#2 相关，以随机数 3(BN3) 和该相关的 TKF#2 的 TKF 随机数 2(TKFN2) 加密该标题密钥 (TK)。

[0062] 因此，该标题密钥文件 TKF#1 和备份文件 TKF#2 及 TKF#3 与其它文件彼此相关，并且该加密标题密钥 (ETK1、 ETK2 和 ETK3) 变成该标题密钥，其中，以在本身文件中登记的随机数 1 至 3(BN1、 BN2 和 BN3) 的每一个和在其它相关文件中登记的 TKF 随机数 1 至 3(TKFN1、 TKFN2 和 TKFN3) 的每一个加密该标题密钥 (TK)，从而即使当恶意的第三方拷贝备份文件之一时，仍无法重新该标题密钥 (TK)。

[0063] 标题密钥文件与备份文件的其它文件的 TKF 随机数的相关性并不限于公式 (1) 至 (3)，但利用除了公式 (1) 至 (3) 之外的其它 模式可以使该标题密钥文件与备份文件的 TKF 随机数相关。

[0064] 在此，将该随机数 1 至 3(BN1、 BN2 和 BN3) 记录在扇区在图 3 中所示的受保护的区域中，在此记录该标题密钥文件 TKF#1 和所述备份文件 TKF#2 和 TKF#3。 另一方面，将该 TKF 随机数 1 至 3(TKFN1、 TKFN2 和 TKFN3) 记录在用户区域中，在此记录该标题密钥文件 TKF#1 和所述备份文件 TKF#2 和 TKF#3。 因此，虽然用户无法将任意值记录在随机数 1 至 3(BN1、 BN2 和 BN3) 中，但有时通过应用程序诸如编辑程序可以将任意值写入 TKF 随机数 1 至 3(TKFN1、TKFN2 和 TKFN3)，其中不执行密钥管理处理。 在第一实施例中，在通过密钥管理处理不被执行的一般应用程序对该标题密钥文件 TKF#1 和备份文件 TKF#2 及 TKF#3 执行编辑 (写入) 操作的情形下，该记录单元 113 适用于在随机数 1 至 3 中写入不正确信息 “0”。 例如，在通过密钥管理处理不被执行的应用程序将值写入 TKF#1 的 TKFN1 的情形下，该记录单元 113 将 BN1 设定为 “0”。 对于 TKF#2 和 TKF#3 保持相同。

[0065] 接着，下文将描述由具有上述配置的第一实施例的该内容记录和再生装置 100 执行的标题密钥文件备份处理。 首先，将描述用于初始化标题密钥文件 (TKF) 备份的处理。 图 5 是示出用于初始化该标题密钥文件 (TKF) 备份的处理的过程的流程图。

[0066] 首先，该主机单元 120 产生该标题密钥 (TK)。 该 TKF 初始化单元 141 使得该随机数产生单元 125 随机产生所述 TKF 随机数 1 至 3(TKFN1、TKFN2 和 TKFN3)(步骤 S501)，并随机产生该世代 (步骤 S502)。

[0067] 接着，该 TKF 初始化单元 141 获得保留在该驱动单元 110 中的随机数 1(BN1)(步骤 S503)。 产生并获得该随机数 1 通过图 3 所示的方法执行。 根据公式 (1) 以随机数 1(BN1) 和相关的 TKF 随机数 3(TKFN3) 加密所产生的标题密钥，以产生所加密的标题密钥 (ETK1)(步骤 S504)。 根据该随机数 1(BN1)、该 TKF 随机数 1(TKFN1)、该世代和所产生的加密的标题密钥 (ETK1)，该 TKF 初始化单元 141 产生该标题密钥文件 TKF#1(步骤 S505)。 该 TKF 初 始化单元 141 将所产生的标题密钥文件 TKF#1 传输给该

驱动单元 110，并且该记录单元 113 在该 DVD 介质 140 中记录该标题密钥文件 TKF#1（步骤 S506）。

[0068] 接着，该 TKF 初始化单元 141 获得保留在该驱动单元 110 中的随机数 2（BN2）（步骤 S507）。产生并获得随机数 2 的处理由图 3 所示的方法执行。根据公式 (2) 以随机数 2（BN2）和相关的 TKF 随机数 1（TKFN1）加密该标题密钥 (TK)，用以产生加密的标题密钥 (ETK2)（步骤 S508）。根据该随机数 2（BN2）、该 TKF 随机数 2（TKFN2）、该世代和所产生的加密的标题密钥 (ETK2)，该 TKF 初始化单元 141 产生备份文件 TKF#2（步骤 S509）。该 TKF 初始化单元 141 将所产生的备份文件 TKF#2 传输给该驱动单元 110，并且该记录单元 113 在该 DVD 介质 140 中记录该备份文件 TKF#2（步骤 S510）。

[0069] 接着，该 TKF 初始化单元 141 获得保留在该驱动单元 110 中的随机数 3（BN3）（步骤 S511）。产生并获得随机数 3 的处理由图 3 所示的方法执行。根据公式 (3) 以随机数 3（BN3）和相关的 TKF 随机数 2（TKFN2）加密该标题密钥 (TK)，用以产生加密的标题密钥 (ETK3)（步骤 S512）。根据该随机数 3（BN3）、该 TKF 随机数 3（TKFN3）、该世代和所产生的加密的标题密钥 (ETK3)，该 TKF 初始化单元 141 产生备份文件 TKF#3（步骤 S513）。该 TKF 初始化单元 141 将所产生的备份文件 TKF#3 传输给该驱动单元 110，并且该记录单元 113 在该 DVD 介质 140 中记录该备份文件 TKF#3（步骤 S514）。因此，将该 DVD 介质 140 上的标题密钥存储在这三个文件中。

[0070] 以下将描述用于更新该标题密钥文件 (TKF) 备份的处理。图 6A 是示出用于更新该标题密钥文件 (TKF) 备份的处理的过程的流程图。在通过删除或增加该 DVD 介质 140 的标题内容来更新标题密钥 (TK) 列表的情形下，执行该备份文件更新处理。同时，该读出单元 112 从该 DVD 介质 140 读取该标题密钥 (TKF#1) 和两个备份文件 TKF#2 及 TKF#3。检查该标题密钥文件 (TKF#1) 和两个备份文件 TKF#2 及 TKF#3 的所有世代的域值是否彼此相符。当该世代的域值彼此不相符时，执行随后提及的恢复处理。当该世代的域值彼此相符时，继 续以下处理。该 TKF 更新单元 142 从该驱动单元 110 的读出单元 112 获得在该 DVD 介质 140 上记录的随机数 1（BN1）（步骤 S601）。根据公式 (1) 以该随机数 1（BN1）和相关的 TKF 随机数 #3 解码该标题密钥文件 TKF#1 的加密的标题密钥 (ETK1)（步骤 S602），以获得该标题密钥 (TK)。该 TKF 更新单元 142 随机产生新的 TKF 随机数 1 至 3（TKFN1、TKFN2 和 TKFN3）（步骤 S603），并且该 TKF 更新单元 142 通过对该世代加 1 而更新该世代（步骤 S604）。

[0071] 该 TKF 更新单元 142 请求该驱动单元 110 产生随机数，并且该 TKF 更新单元 142 从该驱动单元 110 获得通过该随机数产生单元 111 重新产生的新的随机数 1（BN1）（步骤 S605）。根据公式 (1)，该 TKF 更新单元 142 以该新的随机数 1（BN1）和该最新相关的 TKF 随机数 3（TKFN3）加密该标题密钥 (TK)，用以产生加密的标题密钥 (ETK1)（步骤 S606）。根据该新的随机数 1（BN1）、该新的 TKF 随机数 1（TKFN1）、所更新的世代和所产生的加密的标题密钥 (ETK1)，该 TKF 更新单元 142 产生该标题密钥文件 TKF#1（步骤 S607），以更新 TKF#1。该 TKF 更新单元 142 将所更新的标题密钥文件 TKF#1 传输给该驱动单元 110，并且该记录单元 113 在该 DVD 介质 140 中记录该标题密钥文件 TKF#1（步骤 S608）。

[0072] 在聚焦该主机单元 120 和该驱动单元 110 之间的数据传输和接收的同时将描述从

步骤 S601 到 S607 的处理。 图 6B 是示出在通过重新产生的随机数 1 解密和加密该标题密钥文件 TKF#1 之后，在该 DVD 介质中写入该标题密钥文件 TKF#1 和重新产生的随机数 1 的过程的顺序图。 该主机单元 120 将随机数读取命令传输给该驱动单元 110（步骤 S621）。 当该驱动单元 110 接收到该随机数读取命令时，该驱动单元 110 使得该读出单元 112 从该 DVD 介质 140 读取该随机数 1（步骤 S622）。 该驱动单元 110 将自该 DVD 介质 140 读取的该随机数 1 传输给该主机单元 120（步骤 S623）。 接收该随机数 1 的该主机单元 120 执行 TKF#1 解密处理（步骤 S624）。

[0073] 接着，该主机单元 120 将该随机数产生命令传输给该驱动单元 110（步骤 S625）。当该驱动单元 110 接收到该随机数产生命令时， 该驱动单元 110 使得该随机数产生单元 111 重新产生随机数 1（步骤 S626），并且将该重新产生的随机数 1 暂时存储在该驱动单元 110 中。 当该主机单元 120 将该随机数读取命令传输给该驱动单元 110 时（步骤 S627），该驱动单元 110 将该暂时存储的随机数 1 传输给该主机单元 120（步骤 S628）。

[0074] 接收该重新产生的随机数 1 的该主机单元 120 利用该重新产生的随机数 1 执行 TKF#1 加密处理（步骤 S629）。 当该 TKF#1 加密处理结束时，该主机单元 120 将随机数写入命令 (ETK1) 传输给该驱动单元 110（步骤 S630）。 当该驱动单元 110 接收到该随机数写入命令时，该记录单元 113 在该 DVD 介质 140 中写入该随机数 1 和 ETK1（步骤 S630）。

[0075] 当将 TKF#1 和该随机数 1 写入该 DVD 介质 140 时，流程返回图 6A。 该 TKF 更新单元 142 请求该驱动单元 110 产生随机数，并且该 TKF 更新单元 142 从该驱动单元 110 获得通过该随机数产生单元 111 重新产生的新的随机数 2(BN2)（步骤 S609）。 根据公式 (2)，该 TKF 更新单元 142 以新的随机数 2(BN2) 和最新相关的 TKF 随机数 1(TKFN1) 加密该标题密钥 (TK)，用以产生加密的标题密钥 (ETK2)（步骤 S610）。 根据该新的随机数 2(BN2)、新的 TKF 随机数 2(TKFN2)、更新的世代和所产生的加密的标题密钥 (ETK2)，该 TKF 更新单元 142 产生备份密钥文件 TKF#2（步骤 S611）以更新 TKF#2。 该 TKF 更新单元 142 将所更新的标题密钥文件 TKF#2 传输给该驱动单元 110，并且该记录单元 113 在该 DVD 介质 140 中记录该标题密钥文件 TKF#2（步骤 S612）。

[0076] 接着，该 TKF 更新单元 142 请求该驱动单元 110 产生随机数，并且该 TKF 更新单元 142 从该驱动单元 110 获得通过该随机数产生单元 111 重新产生的新的随机数 3(BN3)（步骤 S613）。 根据公式 (3)，该 TKF 更新单元 142 以新的随机数 3(BN3) 和最新相关的 TKF 随机数 2(TKFN2) 加密该标题密钥 (TK)，用以产生加密的标题密钥 (ETK3)（步骤 S614）。 根据该新的随机数 3(BN2)、新的 TKF 随机数 3(TKFN3)、更新的世代和所产生的加密的标题密钥 (ETK3)， 该 TKF 更新单元 142 产生备份文件 TKF#3（步骤 S615）以更新 TKF#3。 该 TKF 更新单元 142 将所更新的备份文件 TKF#3 传输给该驱动单元 110，并且该记录单元 113 在该 DVD 介质 140 中记录该标题密钥文件 TKF#3（步骤 S616）。 因此，更新了该标题密钥文件 TKF#1 和备份文件 TKF#2 及 TKF#3，并且在该 DVD 介质 140 中顺序写入 TKF#1、 TKF#2 和 TKF#3。 以上述次序将该标题密钥文件和备份文件写入该 DVD 介质 140 中，这允许通过世代之间的一致和不一致来确定是否需要备份文件恢复。

[0077] 以下将描述用于标题密钥文件 (TKF#1) 和备份文件 (TKF#2 和 TKF#3) 的备份恢

复处理。图 7 是示出用于恢复标题密钥文件 (TKF#1) 备份的处理的整个过程的流程图。

[0078] 在该标题密钥文件 TKF#1 和备份文件 TKF#2 及 TKF#3 之一不存在于该 DVD 介质 140 中的情形下，或在该标题密钥文件 TKF#1 和备份文件 TKF#2 及 TKF#3 之一被破坏的情形下，或在三个文件 TKF#1、TKF#2 和 TKF#3 的世代彼此不相符的情形下，执行备份文件恢复处理。特别地，通过以下确定来执行该备份文件恢复处理。

[0079] 该读出单元 112 从该 DVD 介质 140 读取该标题密钥文件 TKF#1 和备份文件 TKF#2 及 TKF#3，并且该 TKF 恢复单元 143 检查该标题密钥文件 TKF#1 是否不存在或该标题密钥文件 TKF#1 是否被破坏（步骤 S701）。当该标题密钥文件 TKF#1 不存在或被破坏时（步骤 S701 中的不存在或被破坏），通过该备份文件 TKF#3 执行恢复处理（步骤 S708）。

[0080] 另一方面，在步骤 S701，当该标题密钥文件 TKF#1 存在且未被破坏时（步骤 S701 中的存在且未被破坏），该 TKF 恢复单元 143 检查是否不存在备份文件 TKF#2 或该备份文件 TKF#2 是否被破坏（步骤 S702）。当该备份文件 TKF#2 不存在或被破坏时（步骤 S702 中的不存在或被破坏），通过该标题密钥文件 TKF#1 执行恢复处理（步骤 S706）。

[0081] 另一方面，在步骤 S702 中，当该备份文件 TKF#2 存在且未被破坏时（步骤 S702 中的存在且未被破坏），该 TKF 恢复单元 143 检查 是否不存在该备份文件 TKF#3 或该备份文件 TKF#3 是否被破坏（步骤 S703）。当该备份文件 TKF#3 不存在或被破坏时（步骤 S703 中的不存在或被破坏），通过该标题密钥文件 TKF#2 执行该恢复处理（步骤 S707）。

[0082] 另一方面，在步骤 S703 中，当该备份文件 TKF#3 存在且未被破坏时（步骤 S703 中的存在且未被破坏），该 TKF 恢复单元 143 检查 TKF#1 的世代是否大于 TKF#2 的世代（步骤 S704）。当 TKF#1 的世代大于 TKF#2 的世代（＝ TKF#3 的世代）时（步骤 S704 中：是），该 TKF 恢复单元 143 确定由于该内容记录和再生装置 100 的关机使得在更新 TKF#1 之后并且在更新 TKF#2 之前中断该更新处理，并且该 TKF 恢复单元 143 利用 TKF#3 执行该恢复处理（步骤 S708）。

[0083] 另一方面，在步骤 S704 中，当该 TKF#1 的世代不大于该 TKF#2 的世代（＝ TKF#3 的世代）时（步骤 S704 中的否），该 TKF 恢复单元 143 检查该 TKF#3 的世代是否小于该 TKF#2 的世代（＝ TKF#1 的世代）（步骤 S705）。当该 TKF#3 的世代小于 TKF#2 的世代（＝ TKF#1 的世代）（步骤 S704 中：是）时，该 TKF 恢复单元 143 确定由于该内容记录和再生装置 1 00 的关机操作，使得在更新 TKF#2 之后在更新 TKF#3 之前中断更新处理，并且该 TKF 恢复单元 143 利用 TKF#2 执行恢复处理（步骤 S707）。

[0084] 另一方面，在步骤 S705，当 TKF#3 的世代不小于 TKF#2 的世代（＝ TKF#1 的世代）时（步骤 S705 中的否），存在备份文件且没有被破坏，并且在更新期间不中断该更新处理。因此，该 TKF 恢复单元 143 确定不必恢复该备份文件，并且在不执行恢复处理的情形下结束流程。

[0085] 以下将描述在步骤 S708 中通过备份文件 TKF#3 执行的恢复处理。图 8 是示出通过该备份文件 TKF#3 执行的恢复处理的过程的流程图。

[0086] 在不存在 TKF#1 或其被破坏的情形下，或在 TKF#1 的世代大于 TKF#2 和 TKF#3 的世代的情形下，该 TKF 恢复单元 143 根据公式 (3) 以 TKF#3 解密所加密的标题密钥 (ETK3)，用以获得该标题密钥 (TK)，并且该 TKF 恢复单元 143 根据该标题密钥 (TK) 执

行 TKF#1、TKF#2 和 TKF#3 的恢复处理。

[0087] 因此，首先，该 TKF 恢复单元 143 检查是否在存储 TKF#2 的随机数 2(BN2) 的受保护的区域中设定了不正确信息“0”(步骤 S801)。当例如在 TKF#2 的随机数 2(BN2) 中设定“0”时(步骤 S801：是)，存储在 TKF#2 的用户区域中的 TKFN2 的值通过应用程序诸如编辑程序改变。在此情形下，因为存在不正确的更新，因此该 TKF 恢复单元 143 执行错误处理(步骤 S818)，并且在不执行恢复处理的情形下结束该流程。

[0088] 另一方面，在步骤 S801，当在存储 TKF#2 的随机数 2(BN2) 的受保护的区域中没有设定“0”时(步骤 S801 的否)，该 TKF 恢复单元 143 确定 TKF#2 是正确的，并且该 TKF 恢复单元 143 继续以下的恢复处理。

[0089] 该 TKF 恢复单元 143 从该驱动单元 110 获得记录在该 DVD 介质 140 上的随机数 3(BN3) 和 TKF#2 及 TKF#3(步骤 S802)。该 TKF 恢复单元 143 根据公式 (3) 以随机数 3(BN3) 和相关的 TKF 随机数 2(TKFN2) 解密该备份文件 TKF#3 的加密的标题密钥 (ETK3)(步骤 S803)，以获得该标题密钥 (TK)。该 TKF 更新单元 142 随机产生新的 TKF 随机数 1 至 3(TKFN1、TKFN2 和 TKFN3)(步骤 S804)，并且通过对世代加 1，该 TKF 更新单元 142 更新该世代(步骤 S805)。

[0090] 接着，该 TKF 恢复单元 143 请求该驱动单元 110 产生随机数，并且该 TKF 恢复单元 143 从该驱动单元 110 获得通过该随机数产生单元 111 重新产生的新的随机数 1(BN1)(步骤 S806)。该 TKF 恢复单元 143 根据公式 (1) 以该新的随机数 1(BN1) 和该最新相关的 TKF 随机数 3(TKFN3) 加密该标题密钥 (TK)，以产生加密的标题密钥 (ETK1)(步骤 S807)。该 TKF 恢复单元 143 根据该新的随机数 1(BN1)、该新的 TKF 随机数 1(TKFN1)、所更新的世代和所产生的加密的标题密钥 (ETK1) 来产生该标题密钥文件 TKF#1(步骤 S808) 以恢复 TKF#1。该 TKF 恢复单元 143 将所恢复的标题密钥文件 TKF#1 传输给该驱动单元 110，并且该记录单元 113 在该 DVD 介质 140 中记录该标题密钥文件 TKF#1 和该随机数 1(BN1)(步骤 S809)。

[0091] 接着，该 TKF 恢复单元 143 请求该驱动单元 110 产生随机数，并且该 TKF 恢复单元 143 从该驱动单元 110 获得通过该随机数产生单元 111 重新产生的新的随机数 2(BN2)(步骤 S810)。该 TKF 恢复单元 143 根据公式 (2) 以该新的随机数 2(BN2) 和该最新相关的 TKF 随机数 1(TKFN1) 加密该标题密钥 (TK)，以产生加密的标题密钥 (ETK2)(步骤 S811)。该 TKF 恢复单元 143 根据该新的随机数 2(BN2)、该新的 TKF 随机数 2(TKFN2)、所更新的世代和所产生的加密的标题密钥 (ETK2) 来产生备份文件 TKF#2(步骤 S812)，以恢复 TKF#2。该 TKF 恢复单元 143 将所恢复的备份文件 TKF#2 传输给该驱动单元 110，并且该记录单元 113 在该 DVD 介质 140 中记录该标题密钥文件 TKF#2 和该随机数 2(BN2)(步骤 S813)。

[0092] 接着，该 TKF 恢复单元 143 请求该驱动单元 110 产生随机数，并且该 TKF 恢复单元 143 从该驱动单元 110 获得通过该随机数产生单元 111 重新产生的新的随机数 3(BN3)(步骤 S814)。该 TKF 恢复单元 143 根据公式 (3) 以该新的随机数 3(BN3) 和该最新相关的 TKF 随机数 2(TKFN2) 加密该标题密钥 (TK)，以产生加密的标题密钥 (ETK3)(步骤 S815)。该 TKF 恢复单元 143 根据该新的随机数 3(BN3)、该新的 TKF 随机数 3(TKFN3)、所更新的世代和所产生的加密的标题密钥 (ETK3) 产生备份文件 TKF#3(步

骤 S816) 以恢复 TKF#3。 该 TKF 恢复单元 143 将所恢复的备份文件 TKF#3 传输给该驱动单元 110，并且该记录单元 113 在该 DVD 介质 140 中记录该备份文件 TKF#3 和该随机数 3(BN3)(步骤 S817)。 因此，利用 TKF#3 恢复所有的备份文件。

[0093] 以下将描述通过该标题密钥文件 TKF#1 执行的步骤 S706 中的恢复处理。 图 9 是示出通过该标题密钥文件 TKF#1 执行的恢复处理的过程的流程图。

[0094] 当 TKF#2 不存在或被破坏时，该 TKF 恢复单元 143 以 TKF#1 解密该加密的标题密钥 (ETK1)，以获得该标题密钥 (TK)，并且该 TKF 恢复单元 143 根据 TK 执行 TKF#1、TKF#2 和 TKF#3 的恢复处 理。

[0095] 因此，首先，该 TKF 恢复单元 143 检查是否将是不正确信息的 “0” 设定给 TKF#3 的随机数 3(BN3)(步骤 S901)。 例如，当在 TKF#3 的随机数 3(BN2) 中设定 “0” 时 (步骤 S901 ：是)，通过应用程序诸如编辑程序改变存储在 TKF#3 的用户区域中的 TKFN3 的值。 在此情形下，因为存在不正确的更新，因此该 TKF 恢复单元 143 执行错误处理 (步骤 S918)，并且在不执行恢复处理的情形下结束流程。

[0096] 另一方面，在步骤 S901，当 “0” 没有被设定给 TKF#3 的随机数 3(BN3) 时 (步骤 S901 中 ：否)，该 TKF 恢复单元 143 确定 TKF#3 是正确的，并且该 TKF 恢复单元 143 继续以下的恢复处理。

[0097] 该 TKF 恢复单元 143 从该驱动单元 110 获得记录在该 DVD 介质 140 上的随机数 1(BN1) 和 TKF#1 及 TKF#3(步骤 S902)。 该 TKF 恢复单元 143 根据公式 (1) 以该随机数 1(BN1) 和该相关的 TKF 随机数 3(TKFN3) 解密该标题密钥文件 TKF#1 的加密的标题密钥 (ETK1)(步骤 S903)，以获得该标题密钥 (TK)。 该 TKF 更新单元 142 随机产生新的 TKF 随机数 1 至 3(TKFN1、TKFN2 和 TKFN3)(步骤 S904)，并且通过对世代增加 1，该 TKF 更新单元 142 更新该世代 (步骤 S905)。

[0098] 从步骤 S906 到步骤 S917 的 TKF#1、TKF#2 和 TKF#3 恢复处理类似于图 8 所示的从步骤 S906 到步骤 S917 的处理。 因此，利用 TKF#1 恢复所有的备份文件。

[0099] 以下将描述通过备份文件 TKF#2 执行的步骤 S707 中的恢复处理。 图 10 是示出通过该备份文件 TKF#2 执行的恢复处理的过程的流程图。

[0100] 当 TKF#3 不存在或被破坏时，或当 TKF#3 的世代小于 TKF#2 和 TKF#1 的世代时，该 TKF 恢复单元 143 以 TKF#2 解密该加密的标题密钥 (ETK2)，以获得该标题密钥文件 (TKF)，并且该 TKF 恢复单元 143 根据 TKF 执行 TKF#1、TKF#2 和 TKF#3 的恢复处理。

[0101] 因此，首先，该 TKF 恢复单元 143 检查为不正确信息的 “0” 是 否被设定给 TKF#1 的随机数 1(BN1)(步骤 S1001)。 例如，当在 TKF#1 的随机数 1(BN1) 中设定 “0” 时 (步骤 S1001 ：是)，通过应用程序诸如编辑程序改变存储在 TKF#1 的用户区域中的 TKFN1 的值。 在此情形下，因为存在不正确的更新，因此该 TKF 恢复单元 143 执行错误处理 (步骤 S1018)，并且在没有执行恢复处理的情形下结束流程。

[0102] 另一方面，在步骤 S1001，当 “0” 不被设定给 TKF#1 的随机数 1(BN1) 时 (步骤 S1001 ：否)，该 TKF 恢复单元 143 确定 TKF#1 是正确的，并且该 TKF 恢复单元 143 继续以下的恢复处理。

[0103] 该 TKF 恢复单元 143 从该驱动单元 110 获得记录在该 DVD 介质 140 上的随机数

2(BN2) 和 TKF#2 及 TKF#1(步骤 S1002)。 该 TKF 恢复单元 143 根据公式 (2) 以该随机数 2(BN2) 和该相关的 TKF 随机数 1(TKFN1) 解密该备份文件 TKF#2 的加密的标题密钥 (ETK2)(步骤 S1003),以获得标题密钥 (TK)。 该 TKF 更新单元 142 随机产生新的 TKF 随机数 1 至 3(TKFN1、TKFN2 和 TKFN3)(步骤 S1004),并且该 TKF 更新单元 142 通过将世代增加 1 来更新该世代(步骤 S1005)。

[0104] 步骤 S1006 和 S1017 中的 TKF#1、TKF#2 和 TKF#3 恢复处理类似于图 8 所示的步骤 S906 和 S917 的处理。 因此,利用 TKF#2 恢复所有的备份文件。

[0105] 如上所述,在第一实施例中,准备该标题密钥 (TK) 的三个加密文件,并且根据公式 (1) 至 (3) 的每一个利用本身的随机数和与本身的随机数相关的另一个文件的 TKF 随机数来加密每一个加密的标题密钥。 例如,攻击者先前在另一个介质中拷贝一个备份文件,该攻击者将标题内容的部分移至另一个介质,以一般过程更新该标题密钥文件,该攻击者从该 DVD 介质中删除该标题密钥文件,以在该 DVD 介质中恢复在另一个介质中拷贝的备份文件。 即使在此情形下,当存在至少两个文件时,根据公式 (1) 至 (3) 无法解密该标题密钥。 此外,通过该更新处理更新另外的两个文件。 因此,无法恢复该标题密钥。 因此,可以防止不正确地恢复从该 DVD 介质中删除的标题内 容的标题密钥,并且可以防止未被授权地使用所述标题内容。

[0106] 例如,即使在攻击者先前重新命名一个备份文件以在该 DVD 介质中存储该备份文件的情形下,当除了用于产生该标题密钥文件的应用程序之外的应用程序编辑该标题密钥文件时,为不正确信息的 “0” 被设定给记录在受保护区域中的随机数 1 至 3。 因此,不执行不正确的备份文件恢复处理,并且无法恢复该标题密钥。 因此,可以防止未经授权地使用所述标题内容。

[0107] (变形)

[0108] 在第一实施例中,标题密钥文件 TKF#1 和备份文件 TKF#2 及 TKF#3 的世代在初始化处理中随机产生,并且在每次通过删除或增加标题内容来改变标题密钥列表时,将世代增加 1 作为更新处理的部分。 然而,本发明并不限于第一实施例,而可以在每次更新处理中随机产生该世代。 图 11 是示出在每次更新该世代时产生随机数的情形下,初始化标题密钥文件 (TKF) 备份的处理的整个过程的流程图。

[0109] 图 11 所示的整个备份恢复处理仅在步骤 S1104 和 S1105 不同于图 7 所示的整个处理。 也就是说,在步骤 S1104,虽然 TKF#2 和 TKF#3 的世代值彼此相符,但确定 TKF#2 和 TKF#3 的世代值是否与 TKF#1 的世代值相符。 在步骤 S1105,虽然 TKF#1 和 TKF#2 的世代值彼此相符,但确定 TKF#1 和 TKF#2 的世代值是否与 TKF#3 的世代值相符。 这是因为在变更的每一个更新处理中随机产生该世代。

[0110] (第二实施例)

[0111] 如图 4A 所示,在第一实施例中,该标题密钥文件 TKF#1 和所述备份文件 TKF#2 及 TKF#3 具有相同的结构。 然而在第二实施例中,在结构上,该备份文件 TKF#3 不同于该标题密钥文件 TKF#1 和该备份文件 TKF#2。

[0112] 第二实施例的记录和再生装置具有与参照图 1 描述的第一实施例的记录和再生装置相同的配置。

[0113] 图 12 是示出第二实施例的标题密钥文件和备份文件的结构的说明图。 在第二

实施例中，该备份文件 TKF#3 不具有加密的标题密钥和 TKF 随机数 3，但该备份文件 TKF#3 具有 TKF 随机数 1(TKFN1) 和 TKF 随机数 2(TKFN2)。 此外，第二实施例在计算该标题密钥文件 TKF#1 的加密的标题密钥 (ETK1) 和该备份文件 TKF#2 的加密的标题密钥 (ETK2) 的方法上不同于第一实施例。

[0114] 类似于第一实施例的 TKF#1 和 TKF#2，该标题密钥文件 TKF#1 和该备份文件 TKF#2 分别包括随机数 1 和 2(BN1 和 BN2)、所述世代、 TKF 随机数 1 和 2(TKFN1 和 TKFN2) 以及加密的标题密钥 (ETK1 和 ETK2)。 TKF#1 的该 TKF 随机数 1(TKFN1) 是用于计算除了本身的 TKF#1 之外的备份文件 TKF#2 的加密的标题密钥 (ETK2) 的随机数。 TKF#2 的 TKF 随机数 2(TKFN2) 是用于计算除了本身的 TKF#2 之外的备份文件 TKF#1 的加密的标题密钥 (ETK1) 的随机数。

[0115] 该备份文件 TKF#3 具有不同于 TKF#1 和 TKF#2 的结构，并且该备份文件 TKF#3 包括该随机数 3(BN3)、该世代、该 TKF 随机数 1(TKFN1) 和该 TKF 随机数 2(TKFN2)。 在 TKF#3 的 TKF 随机数中，在 TKFN1 中记录与该标题密钥文件 TKF#1 的 TKF 随机数 1(TKFN1) 相同的值，而在 TKFN2 中记录与该备份文件 TKF#2 的 TKF 随机数 2(TKFN2) 相同的值。

[0116] 所述加密的标题密钥 (ETK1 和 ETK2) 是以下数据，其中：以在该标题密钥文件 TKF#1 或备份文件 TKF#2 及 TKF#3 中登记的随机数 (BN1 和 BN2) 和在另一个文件中登记的相关 TKF 随机数 (TKFN1 和 TKFN2) 加密该标题密钥文件的所有标题密钥。 通过公式 (4) 和 (5) 来表示所述加密的标题密钥 (ETK1 和 ETK2)。

[0117] $ETK1 = f(TK, BN1, TKFN2)$ (4)

[0118] $ETK2 = f(TK, BN2, TKFN1)$ (5)

[0119] 其中， TK 表示标题密钥，而 f 表示利用第二参数 (BN1、 BN2) 和第三参数 (TKFN1、TKFN2) 作为加密的密钥对第一参数 (TK) 执行加密处理。 可以将公知的加密算法诸如高级加密标准 (AES) 用于加密处理 f。

[0120] 以下将描述具有上述配置的第二实施例的内容记录和再生装置 100 执行的标题密钥文件备份处理。

[0121] 以下将描述初始化该标题密钥文件 (TKF) 备份的处理。图 13 是示出初始化该标题密钥文件 (TKF) 备份处理的过程的流程图。 在第二实施例的备份文件初始化处理中，如图 13 所示，该备份文件 TKF#3 的结构不同于 TKF#1 和 TKF#2 的结构，并且通过公式 (4) 和 (5) 来确定所述加密的标题密钥 (ETK1 和 ETK2)。 因此，在产生该标题密钥文件 TKF#1 的加密的标题密钥 (ETK1) 的处理中，在产生该标题密钥文件 TKF#1 的处理中，以及在产生该备份文件 TKF#3 的处理中，第二实施例的备份文件初始化处理不同于图 5 的第一实施例的备份文件初始化处理。

[0122] 首先，该主机单元 120 产生该标题密钥 (TK)。 该 TKF 初始化单元 141 使得该随机数产生单元 125 随机产生所述 TKF 随机数 1 和 2(TKFN1 和 TKFN2)(步骤 S1301)，并且该随机数产生单元 125 还随机产生该世代 (步骤 S1302)。

[0123] 接着，该 TKF 初始化单元 141 获得保留在该驱动单元 110 中的随机数 1(BN1)(步骤 S503)。 通过图 3 所示的方法执行产生并获得随机数 1 的处理。 根据公式 (4) 以该随机数 1(BN1) 和相关的 TKF 随机数 2(TKFN2) 加密所产生的标题密钥，以产生加密

的标题密钥 (ETK1)(步骤 S1304)。 根据该随机数 1(BN1)、该 TKF 随机数 1(TKFN1)、该世代和所产生的加密的标题密钥 (ETK1)，该 TKF 初始化单元 141 产生该标题密钥文件 TKF#1(步骤 S1305)。 该 TKF 初始化单元 141 将所产生的标题密钥文件 TKF#1 传输给该驱动单元 110，并且该记录单元 113 在该 DVD 介质 140 中记录该标题密钥文件 TKF#1(步骤 S1306)。

[0124] 接着，该 TKF 初始化单元 141 获得保留在该驱动单元 110 中的随机数 2(BN2)(步骤 S507)。 通过图 3 所示的方法来执行产生并获得该随机数 2 的处理。 根据公式 (5) 以该随机数 2(BN2) 和该相关的 TKF 随机数 1(TKFN1) 加密该标题密钥 (TK)，以产生该加密的标题密钥 (ETK2)(步骤 S1308)。 该 TKF 初始化单元 141 根据该随机数 2(BN2)、该 TKF 随机数 2(TKFN2)、该世代和所产生的加密的标题密钥 (ETK2) 来产生备份文件 TKF#2(步骤 S1309)。 该 TKF 初始化单元 141 将所产生的备份文件 TKF#2 传输给该驱动单元 110， 并且该记录单元 113 在该 DVD 介质 140 中记录该备份文件 TKF#2(步骤 S1310)。

[0125] 接着，该 TKF 初始化单元 141 获得保留在该驱动单元 110 中的随机数 3(BN3)(步骤 S1311)。 通过图 3 所示的方法来执行产生并获得随机数 1 的处理。 根据该随机数 3(BN3)、该 TKF 随机数 1(TKFN1)、 TKF 随机数 2(TKFN2) 和该世代来产生具有图 12 所示结构的备份文件 TKF#3(步骤 S1312)。 该 TKF 初始化单元 141 将所产生的备份文件 TKF#3 传输给该驱动单元 110，并且该记录单元 113 在该 DVD 介质 140 中记录该备份文件 TKF#3(步骤 S1313)。 通过上述处理产生图 12 所示的标题密钥文件 TKF#1 和备份文件 TKF#2 及 TKF#3。

[0126] 以下将描述用于更新该标题密钥文件 (TKF) 备份的处理。 图 14 是示出在第二实施例中更新该标题密钥文件 (TKF) 备份的处理的过程的流程图。 在第二实施例中，图 12 中所示的备份文件 TKF#3 的结构不同于 TKF#1 和 TKF#2 的结构，并且通过公式 (4) 和 (5) 确定加密的标题密钥 (ETK1 和 ETK2)。 因此，在解密该标题密钥文件 (TKF#1) 的处理中、在产生该标题密钥文件 TKF#1 的加密的标题密钥 (ETK1) 的处理中、在产生该标题密钥文件 TKF#1 的处理中以及在产生该备份文件 TKF#3 的处理中，第二实施例的备份更新处理不同于图 6A 的第一实施例的备份文件更新处理。

[0127] 在第二实施例中，在通过删除或增加该 DVD 介质 140 的标题内容来更新该列标题密钥 (TK) 的情形下，执行该备份文件更新处理。 同时，该读出单元 112 从该 DVD 介质 140 读取该标题密钥 (TKF#1) 和所述两个备份文件 TKF#2 及 TKF#3。 该 TKF 更新单元 142 从该驱动单元 110 的该读出单元 112 获得在该 DVD 介质 140 上记录的随机数 1(BN1)(步骤 S1401)。 根据公式 (4) 以该随机数 1(BN1) 和该相关的 TKF 随机数 #2 解密该标题密钥文件 TKF#1 的加密的标题密钥 (ETK1)(步骤 S1402)，以获得该标题密钥 (TK)。该 TKF 更新单元 142 随机产生新的 TKF 随机数 1(TKFN1) 和 TKF 随机数 2(TKFN2)(步骤 S1403)，并且该 TKF 更新单元 142 通过对世代增 加 1 来更新该世代 (步骤 S1404)。

[0128] 该 TKF 更新单元 142 请求该驱动单元 110 产生随机数，并且该 TKF 更新单元 142 从该驱动单元 110 获得通过该随机数产生单元 111 重新产生的新的随机数 1(BN1)(步骤 S1405)。 根据公式 (4)，该 TKF 更新单元 142 以该新的随机数 1(BN1) 和该最新相关的 TKF 随机数 2(TKFN2) 加密该标题密钥 (TK)，以产生该加密的标题密钥 (ETK1)(步骤

S1406)。根据该新的随机数 1(BN1)、该新的 TKF 随机数 1(TKFN1)、所更新的世代和所产生的加密的标题密钥 (ETK1)，该 TKF 更新单元 142 产生该标题密钥文件 TKF#1(步骤 S1407) 以更新 TKF#1。该 TKF 更新单元 142 将所更新的标题密钥文件 TKF#1 传输给该驱动单元 110，并且该记录单元 113 在该 DVD 介质 140 中记录该标题密钥文件 TKF#1(步骤 S1408)。

[0129] 接着，该 TKF 更新单元 142 请求该驱动单元 110 产生随机数，并且该 TKF 更新单元 142 从该驱动单元 110 获得通过该随机数产生单元 111 重新产生的新的随机数 2(BN2)(步骤 S1409)。根据公式 (5)，该 TKF 更新单元 142 以该新的随机数 2(BN2) 和该最新相关的 TKF 随机数 1(TKFN1) 加密该标题密钥 (TK)，以产生该加密的标题密钥 (ETK2)(步骤 S1410)。该 TKF 更新单元 142 根据该新的随机数 2(BN2)、该新的 TKF 随机数 2(TKFN2)、所更新的世代和所产生的加密的标题密钥 (ETK2) 来产生该备份文件 TKF#2(步骤 S1411) 以更新 TKF#2。该 TKF 更新单元 142 将所更新的备份文件 TKF#2 传输给该驱动单元 110，并且该记录单元 113 在该 DVD 介质 140 中记录该备份文件 TKF#2(步骤 S1412)。

[0130] 接着，该 TKF 更新单元 142 请求该驱动单元 110 产生随机数，并且该 TKF 更新单元 142 从该驱动单元 110 获得通过该随机数产生单元 111 重新产生的新的随机数 3(BN3)(步骤 S1413)。该 TKF 更新单元 142 根据该新的随机数 3(BN3)、所更新的世代、该新的 TKF 随机数 1(TKFN1) 和该新的 TKF 随机数 2(TKFN2) 来产生图 12 所示结构的备份文件 TKF#3(步骤 S1414) 以更新 TKF#3。该 TKF 更新单元 142 将所更新的备份文件 TKF#3 传输给该驱动单元 110，，并且该记录单元 113 在该 DVD 介质 140 中记录该备份文件 TKF#3(步骤 S1415)。因此，更新该标题密钥文件 TKF#1 和所述备份文件 TKF#2 及 TKF#3，并且将 TKF#1、TKF#2 和 TKF#3 顺序写入该 DVD 介质 140 中。

[0131] 以下将描述该标题密钥文件 (TKF#1) 和备份文件 (TKF#2 和 TKF#3) 的备份的恢复处理。图 15 是示出恢复该标题密钥文件 (TKF#1) 的处理的整个过程的流程图。在第二实施例中，图 12 中所示的备份文件 TKF#3 的结构不同于 TKF#1 和 TKF#2 的结构，并且通过公式 (4) 和 (5) 来确定加密的标题密钥 (ETK1 和 ETK2)。因此，第二实施例的恢复处理不同于第一实施例的恢复处理。

[0132] 也就是说，从步骤 S1501 至步骤 S1505 的确定处理类似于图 7 中解释的步骤 S701 至步骤 S705 的处理。在第二实施例中，当在步骤 S1502 中不存在 TKF#2 或其被破坏时，以 TKF#1 和 TKF#3 执行该恢复处理 (步骤 S1506)。当在步骤 1503 中不存在 TKF#3 或其被破坏时，或当在步骤 S1505 中 TKF#3 的世代小于 TKF#1 和 TKF#2 的世代时，以 TKF#1 和 TKF#2 执行恢复处理 (步骤 S1507)。当在步骤 1501 中不存在 TKF#1 或其被破坏时，或当在步骤 S1504 中 TKF#1 的世代大于 TKF#2 和 TKF#3 的世代时，以 TKF#2 和 TKF#3 执行该恢复处理 (步骤 S1508)。

[0133] 以下将描述在步骤 S1508 中通过解密备份文件 TKF#2 的加密的标题密钥 (ETK2) 来执行的恢复处理。图 16 是示出利用备份文件 TKF#2 和 TKF#3 执行的恢复处理的过程的流程图。第二实施例的恢复处理不同于图 8 的第一实施例的恢复处理，其中利用备份文件 TKF#2、用于解密该备份文件 TKF#2 的加密的标题密钥 (ETK2) 的处理、产生该标题密钥文件 TKF#1 的加密的标题密钥 (ETK1) 的处理、产生该标题密钥文件 TKF#1 的处

理和产生该备份文件 TKF#3 的处理，来检查是否将是不正确信息的 “0” 设定给该备份文件 TKF#3 的随机数 3。

[0134] 首先，该 TKF 恢复单元 143 检查是否在 TKF#3 的随机数 3(BN3) 所存储的受保护区域中设定是不正确信息的 “0”（步骤 S1601）。 例如，当 “0” 被设定给 TKF#3 的随机数 3(BN3) 时（步骤 S1601 ：是），存储在 TKF#3 的用户区域中的 TKFN1 和 TKFN2 的值通过应用程序诸如编辑程序改变。 在此情形下，因为存在不正确的更新，因此该 TKF 恢复单元 143 执行错误处理（步骤 S1617），并且在没有执行恢复处理的情形下结束流程。

[0135] 另一方面，在步骤 S1601 中，当没有在 TKF#3 的随机数 3(BN3) 所存储的受保护区域中设定 “0” 时（步骤 S1601 的否），该 TKF 恢复单元 143 确定 TKF#3 是正确的，并且该 TKF 恢复单元 143 继续以下的恢复处理。

[0136] 该 TKF 恢复单元 143 从该驱动单元 110 获得记录在该 DVD 介质 140 上的随机数 2(BN2)、 TKF#2 和 TKF#3（步骤 S1602）。 根据公式 (5)，该 TKF 恢复单元 143 以存储在 TKF#3 中的随机数 2(BN2) 和 TKF 随机数 1(TKFN1) 解密该备份文件 TKF#2 的加密的标题密钥 (ETK2)（步骤 S1603），以获得该标题密钥 (TK)。 该 TKF 更新单元 142 随机产生新的 TKF 随机数 1 和 2(TKFN1 和 TKFN2)（步骤 S1604），并且该 TKF 更新单元 142 通过对世代增加 1 来更新该世代（步骤 S1605）。

[0137] 接着，该 TKF 恢复单元 143 请求该驱动单元 110 产生随机数，并且该 TKF 恢复单元 143 从该驱动单元 110 获得通过该随机数产生单元 111 重新产生的新的随机数 1(BN1)（步骤 S1606）。 根据公式 (4)，该 TKF 恢复单元 143 以该新的随机数 1(BN1) 和最新相关的 TKF 随机数 2(TKFN2) 加密该标题密钥 (TK)，以产生加密的标题密钥 (ETK1)（步骤 S1607）。 该 TKF 恢复单元 143 根据该新的随机数 1(BN1)、该新的 TKF 随机数 1(TKFN1)、更新的世代和所产生的加密的标题密钥 (ETK1) 来产生该标题密钥文件 TKF#1（步骤 S1608），以恢复 TKF#1。 该 TKF 恢复单元 143 将所恢复的标题密钥文件 TKF#1 传输给该驱动单元 110，并且该记录单元 113 在该 DVD 介质 140 中记录该标题密钥文件 TKF#1 和该随机数 1(BN1)（步骤 S1609）。

[0138] 接着，该 TKF 恢复单元 143 请求该驱动单元 110 产生随机数， 并且该 TKF 恢复单元 143 从该驱动单元 110 获得通过该随机数产生单元 111 重新产生的新的随机数 2(BN2)（步骤 S1610）。 根据公式 (5)，该 TKF 恢复单元 143 以该新的随机数 2(BN2) 和最新相关的 TKF 随机数 1(TKFN1) 加密该标题密钥 (TK)，以产生加密的标题密钥 (ETK2)（步骤 S1611）。 该 TKF 恢复单元 143 根据该新的随机数 2(BN2)、该新的 TKF 随机数 2(TKFN2)、所更新的世代和所产生的加密的标题密钥 (ETK2) 来产生备份文件 TKF#2（步骤 S1612），以恢复 TKF#2。 该 TKF 恢复单元 143 将所恢复的备份文件 TKF#2 传输给该驱动单元 110，并且该记录单元 113 在该 DVD 介质 140 中记录该备份文件 TKF#2 和随机数 2(BN2)（步骤 S1613）。

[0139] 接着，该 TKF 恢复单元 143 请求该驱动单元 110 产生随机数，并且该 TKF 恢复单元 143 从该驱动单元 110 获得通过该随机数产生单元 111 重新产生的新的随机数 3(BN3)（步骤 S1614）。 根据该新的随机数 3(BN3)、新的 TKF 随机数 1(TKFN1)、新的 TKF 随机数 2(TKFN2) 和更新的世代，该 TKF 恢复单元 143 产生具有图 12 所示结构的备份文件 TKF#3（步骤 S1615），以恢复 TKF#3。 该 TKF 恢复单元 143 将所恢复的备份文件

TKF#3 传输给该驱动单元 110，并且该记录单元 113 在该 DVD 介质 140 中记录该备份文件 TKF#3 和随机数 3(BN3)（步骤 S1616）。 因此，利用 TKF#2 和 TKF#3 恢复所有的备份文件。

[0140] 以下将描述利用该标题密钥文件 TKF#1 和该备份文件 TKF#3 执行的恢复处理。图 17 是示出利用该标题密钥文件 TKF#1 和该备份文件 TKF#3 执行的恢复处理的过程的流程图。 在解密该标题密钥文件 TKF#1 的加密的标题密钥 (ETK1) 的处理中、在产生该标题密钥文件 TKF#1 的加密的标题密钥 (ETK1) 的处理中、在产生该标题密钥文件 TKF#1 的处理中以及在产生该备份文件 TKF#3 的处理中，第二实施例的恢复处理不同于图 9 的第一实施例中利用 TKF#1 执行的恢复处理。

[0141] 首先，该 TKF 恢复单元 143 检查是否在 TKF#3 的随机数 3(BN3) 所存储的受保护区域中设定是不正确信息的 “0”（步骤 S1601）。 例如，当将 “0” 设定给 TKF#3 的随机数 3(BN3) 时（步骤 S1701 ：是），存储在 TKF#3 的用户区域中的 TKFN1 和 TKFN2 的值通过应用程序诸如编辑程序而改变。 在此情形下，因为存在不正确的更新，因此该 TKF 恢复单元 143 执行错误处理（步骤 S1717），并且在没有执行恢复处理的情形下结束流程。

[0142] 另一方面，在步骤 S1701 中，当在 TKF#3 的随机数 3(BN3) 所存储的受保护区域中没有设定 “0” 时（步骤 S1701 的否），该 TKF 恢复单元 143 确定 TKF#3 是正确的，并且该 TKF 恢复单元 143 继续以下的恢复处理。

[0143] 该 TKF 恢复单元 143 从该驱动单元 110 获得在该 DVD 介质 140 上记录的随机数 1(BN1) 和 TKF#1 及 TKF#3（步骤 S1702）。 根据公式 (4)，该 TKF 恢复单元 143 以存储在 TKF#3 中的随机数 1(BN1) 和 TKF 随机数 2(TKFN2) 来解密备份文件 TKF#1 的加密的标题密钥 (ETK1)（步骤 S1703) 以获得该标题密钥 (TK)。 该 TKF 更新单元 142 随机产生新的 TKF 随机数 1 和 2(TKFN1 和 TKFN2)（步骤 S1704），并且该 TKF 更新单元 142 通过对该世代增加 1 来更新该世代（步骤 S1705）。

[0144] 随后从步骤 S1706 到步骤 S1716 的 TKF#1、TKF#2 和 TKF#3 的恢复处理类似于图 16 从步骤 S1606 到步骤 S1616 的处理。 因此，利用 TKF#1 和 TKF#3 来恢复所有的备份文件。

[0145] 接着，以下将描述利用该标题密钥文件 TKF#1 和该备份文件 TKF#2 执行的恢复处理。 图 18 是示出通过该标题密钥文件 TKF#1 和该备份文件 TKF#2 执行的恢复处理的过程的流程图。 当 TKF#3 不存在或被破坏时，或当 TKF#3 的世代小于 TKF#2 和 TKF#1 的世代时，该 TKF 恢复单元 143 利用 TKF#1 和 TKF#2 执行 TKF#3 的恢复处理。

[0146] 因此，该 TKF 恢复单元 143 检查是否将是不正确信息的 “0” 设定给 TKF#1 的随机数 1(BN1) 和 TKF#2 的随机数 2(BN2)（步骤 S1801）。 例如，当 “0” 被设定给 TKF#1 的随机数 1(BN1) 和 TKF#2 的随机数 2(BN2) 时（步骤 S1801 ：是），存储在该标题密钥文件 TKF#1 的用户区域中的 TKFN2 值或存储在该备份文件 TKF#2 的用户 区域中的 TKFN1 通过应用程序诸如编辑程序而改变。 在此情形下，因为可能存在不正确的更新，因此该 TKF 恢复单元 143 执行错误处理（步骤 S1805），并且在没有执行该恢复处理的情形下结束流程。

[0147] 另一方面，在步骤 S1801 中，当 “0” 没有被设定给 TKF#1 的随机数 1(BN1) 和

TKF#2 的随机数 2(BN2) 时（步骤 S1801 的否），该 TKF 恢复单元 143 确定 TKF 是正确的，并且该 TKF 恢复单元 143 继续以下的恢复处理。

[0148] 该 TKF 恢复单元 143 从该驱动单元 110 获得在该 DVD 介质 140 上记录的随机数 3(BN3)、TKF#1 和 TKF#2。该 TKF 恢复单元 143 根据 TKF#1 读取 TKF 随机数 1(TKFN1) 和世代，该 TKF 恢复单元 143 根据 TKF#2 读取 TKF 随机数 2(TKFN2) 和世代，并且该 TKF 恢复单元 143 根据该新的随机数 3(BN3)、该世代、该 TKF 随机数 1(TKFN1) 和该 TKF 随机数 2(TKFN2) 产生具有图 12 所示结构的备份文件 TKF#3（步骤 S1803）以恢复 TKF#3。该 TKF 恢复单元 143 将所恢复的备份文件 TKF#3 传输给该驱动单元 110，并且该记录单元 113 在该 DVD 介质 140 中记录该备份文件 TKF#3 和该随机数 3(BN3)（步骤 S1804）。因此，利用 TKF#1 和 TKF#2 来恢复该备份文件 TKF#3。

[0149] 如上所述，在第二实施例中，准备标题密钥 (TK) 的两个加密的文件 TKF#1 和 TKF#2，TKF#3 包括随机数 3、TKF 随机数 2、TKF 随机数 3 和世代，并且如公式 (4) 和 (5) 所示，利用本身的随机数和彼此的 TKF 随机数来加密该加密的标题密钥 TKF#1 和 TKF#2。因此，类似于第一实施例，可以防止不正确地恢复从 DVD 介质中删除的标题内容的标题密钥，并且可以防止未经授权地使用标题内容。

[0150] （第二变形）

[0151] 在第一和第二实施例中，该内容记录和再生装置 100 具有如下配置，其中：该驱动单元 110 和该主机单元 120 经由总线 30 彼此连接。

[0152] 然而，通过以内部总线连接该驱动单元 110 和该主机单元 120，可以整体形成该驱动单元 110 和该主机单元 120。图 19 是示出内容记录和再生装置 1900 的配置的框图，其中，通过以内部总线 1930 连接该 驱动单元 110 和该主机单元 120，整体形成该驱动单元 110 和该主机单元 120。

[0153] 如图 19 所示，包括在该驱动单元 110 中的单元类似于第一和第二实施例的那些单元。然而，主机单元 1920 不包括随机数产生单元。在图 19 的配置中，驱动单元 110 中的随机数产生单元 111 适用于由该主机单元 1920 和驱动单元 110 共同使用。

[0154] 在图 19 中，将该随机数产生单元 111 包括在该驱动单元 110 中。可选择地，该随机数产生单元不包括在该驱动单元 110 中，而仅是该主机单元 1920 可以包括该随机数产生单元。可选择地，该随机数产生单元不是直接包括在该驱动单元 110 和该主机单元 1920 中，但除了该驱动单元 110 和该主机单元 120 之外的装置中的其它单元可以包括该随机数产生单元。

[0155] 在先前并进 ROM 或类似物中时，提供在第一和第二实施例的内容记录和再生装置中执行的内容记录和再生程序。

[0156] 通过在计算机可读取的记录介质诸如 CD-ROM、软驱 (FD)、CD-R 和 DVD 中记录该内容记录和再生程序，可以将在第一和第二实施例的内容记录和再生装置中执行的内容记录和再生程序提供成具有可安装的格式或可执行的格式的文件。

[0157] 通过在连接到网络诸如因特网的计算机中存储程序并通过经由网络下载程序，可以提供在第一和第二实施例的内容记录和再生装置中执行的内容记录和再生程序。通过网络诸如因特网可以提供或分配在第一和第二实施例的内容记录和再生装置中执行的内容记录和再生程序。

[0158] 在第一和第二实施例的内容记录和再生装置中执行的内容记录和再生程序具有包括上述单元（内容加密处理单元 121、内容解密处理单元 122、TKF 加密处理单元 123 和备份处理单元 140）的模块结构。在实际的硬件中，CPU（处理器）从 ROM 读取内容记录和再生程序以执行该内容记录和再生程序，这允许将每一个单元加载到主存储装置上，以在该主存储装置上产生该内容加密处理单元 121、该内容解密处理单元 122、该 TKF 加密处理单元 123 和该备份处理单元 140。

[0159] 代替内置式装置诸如 DVD 刻录机，第一和第二实施例的内容记录和再生装置可以使用一般的计算机，同时包括控制装置诸如 CPU、存储装置诸如只读存储器（ROM）和 RAM、外部存储装置诸如 HDD 和 CD 驱动器、显示装置和输入装置诸如键盘和鼠标。在此情形下，例如，可以将 USB 用作连接该主机单元 120 和该驱动单元 110 的总线。

[0160] 本发明并不限于上述实施例。在实现阶段，可以做出各种变更和修改而不脱离本发明的精神和范围。

[0161] 工业实用性

[0162] 如上所述，根据本发明的内容记录和再生装置、内容记录和再生方法以及内容记录和再生程序产品对于 DVD 记录和再生装置、DVD 记录和再生方法和 DVD 记录和再生程序产品是有用的，其中将内容记录在 DVD 介质中或从 DVD 介质中再生该内容。特别地，本发明适用于 DVD 记录和再生装置、DVD 记录和再生方法以及 DVD 记录和再生程序产品，其中在加密的同时记录该内容。

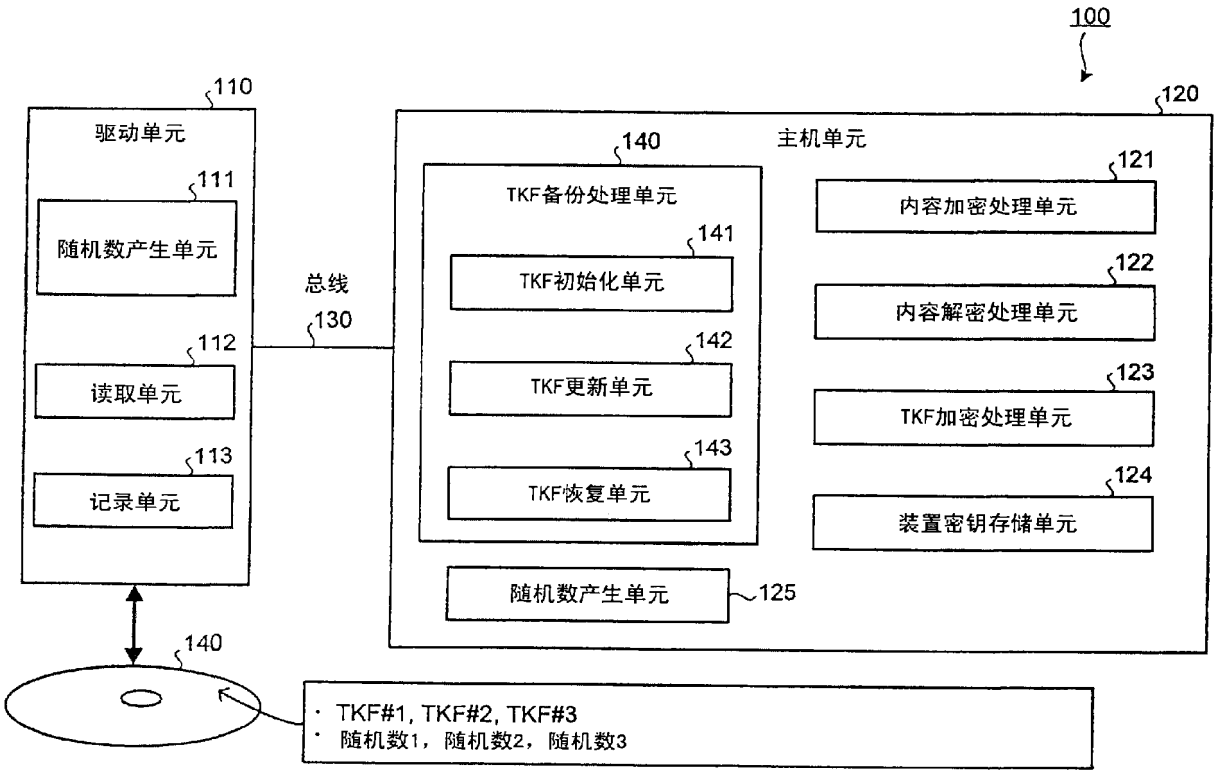

100
110
驱动单元
111
随机数产生单元
112
读取单元
113
记录单元
总线
130
120
主机单元
140
TKF备份处理单元
141
TKF初始化单元
142
TKF更新单元
143
TKF恢复单元
随机数产生单元
125
121
内容加密处理单元
122
内容解密处理单元
123
TKF加密处理单元
124
装置密钥存储单元
140
· TKF#1, TKF#2, TKF#3
· 随机数1，随机数2，随机数3

图1

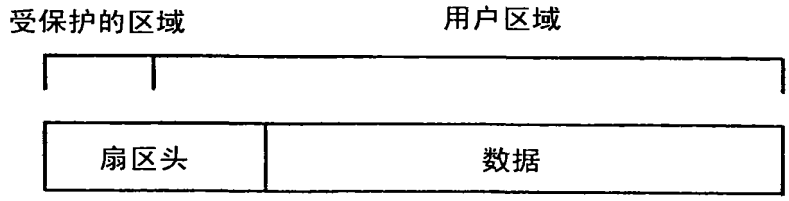

受保护的区域
用户区域
扇区头
数据

图2

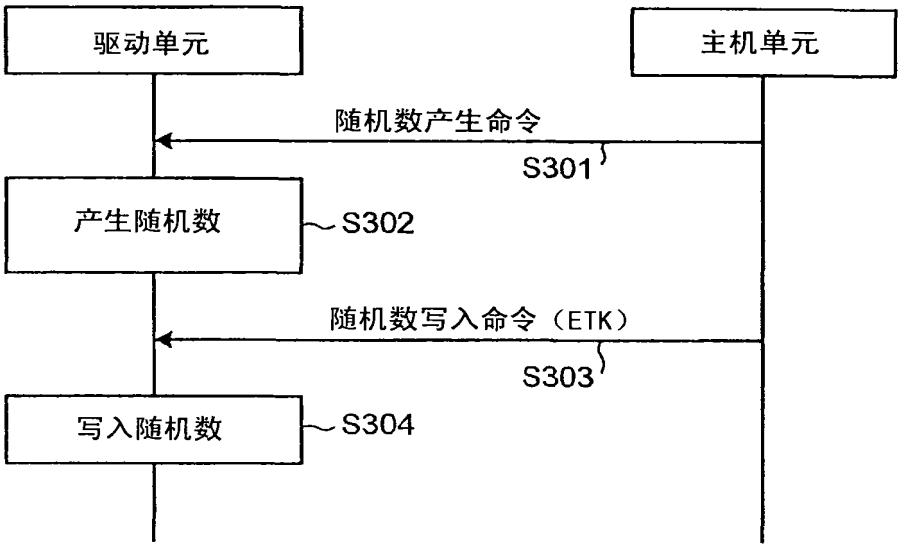
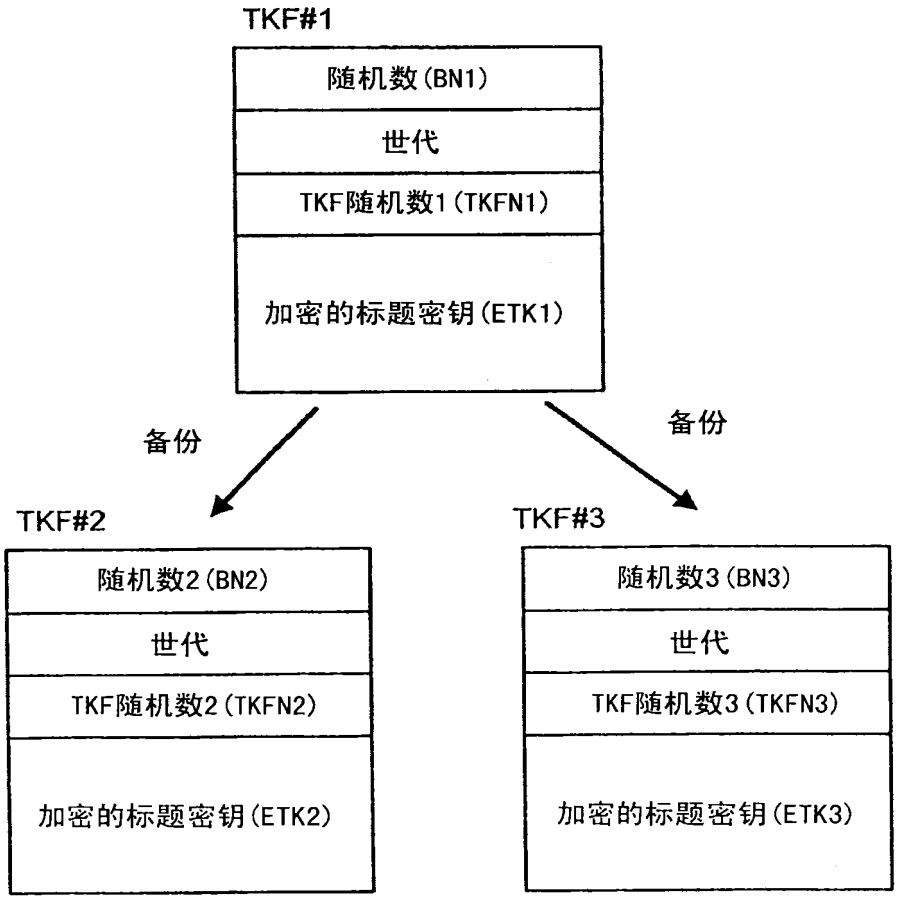

驱动单元
主机单元
随机数产生命令
S301
产生随机数
S302
随机数写入命令（ETK）
S303
写入随机数
S304

图3



ETK1 = f (TK, BN1, TKFN3)
ETK2 = f (TK, BN2, TKFN1)
ETK3 = f (TK, BN3, TKFN2)

图4A

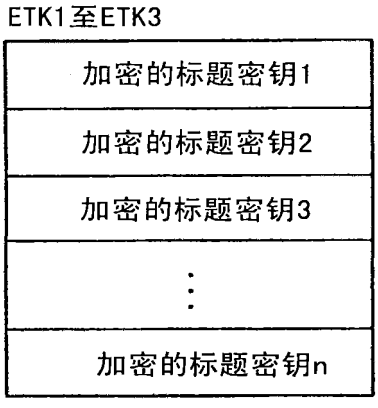


图4B

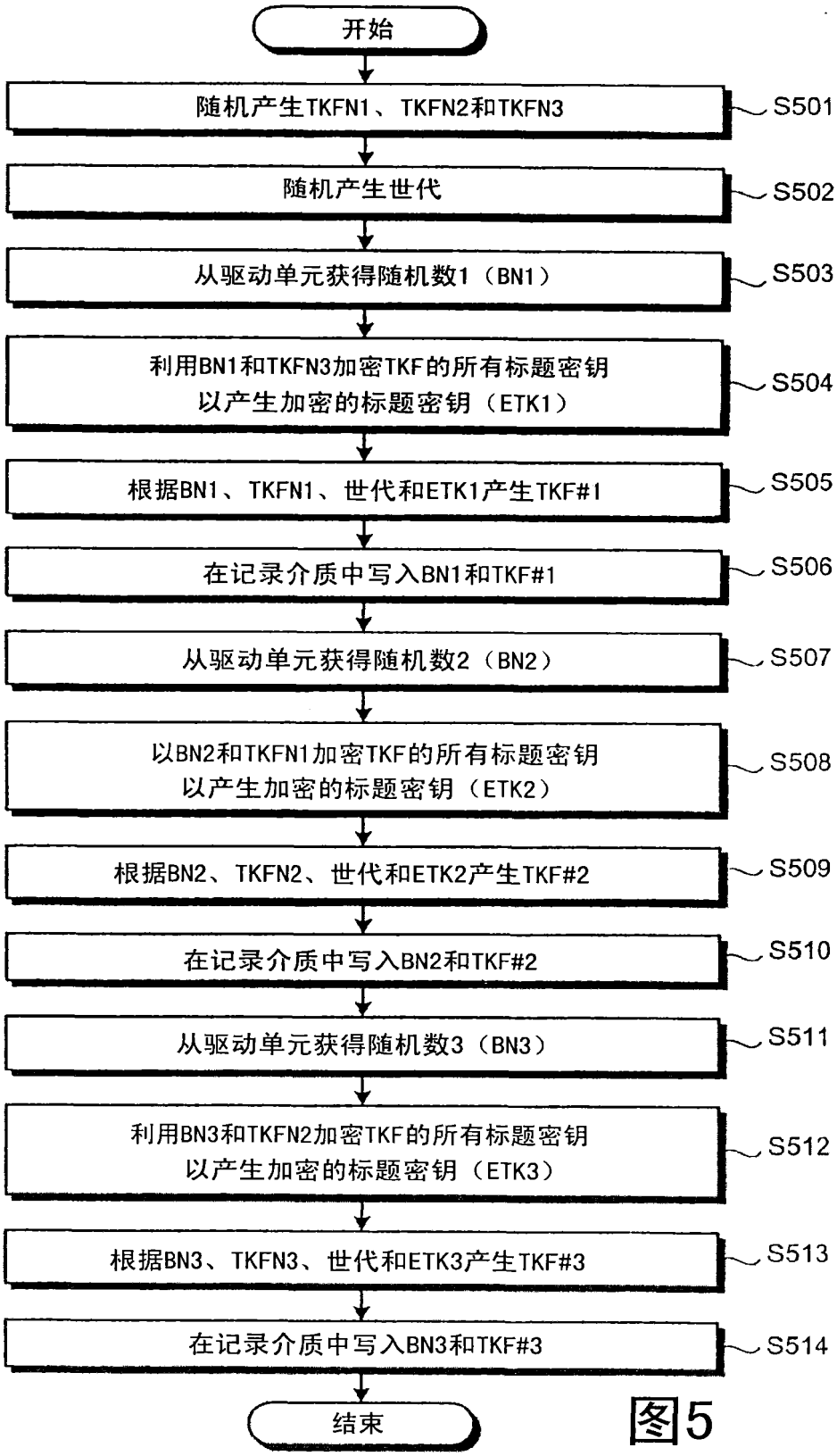

开始
随机产生TKFN1、TKFN2和TKFN3
S501
随机产生世代
S502
从驱动单元获得随机数1（BN1）
S503
利用BN1和TKFN3加密TKF的所有标题密钥
以产生加密的标题密钥（ETK1）
S504
根据BN1、TKFN1、世代和ETK1产生TKF#1
S505
在记录介质中写入BN1和TKF#1
S506
从驱动单元获得随机数2（BN2）
S507
以BN2和TKFN1加密TKF的所有标题密钥
以产生加密的标题密钥（ETK2）
S508
根据BN2、TKFN2、世代和ETK2产生TKF#2
S509
在记录介质中写入BN2和TKF#2
S510
从驱动单元获得随机数3（BN3）
S511
利用BN3和TKFN2加密TKF的所有标题密钥
以产生加密的标题密钥（ETK3）
S512
根据BN3、TKFN3、世代和ETK3产生TKF#3
S513
在记录介质中写入BN3和TKF#3
S514
结束

图5

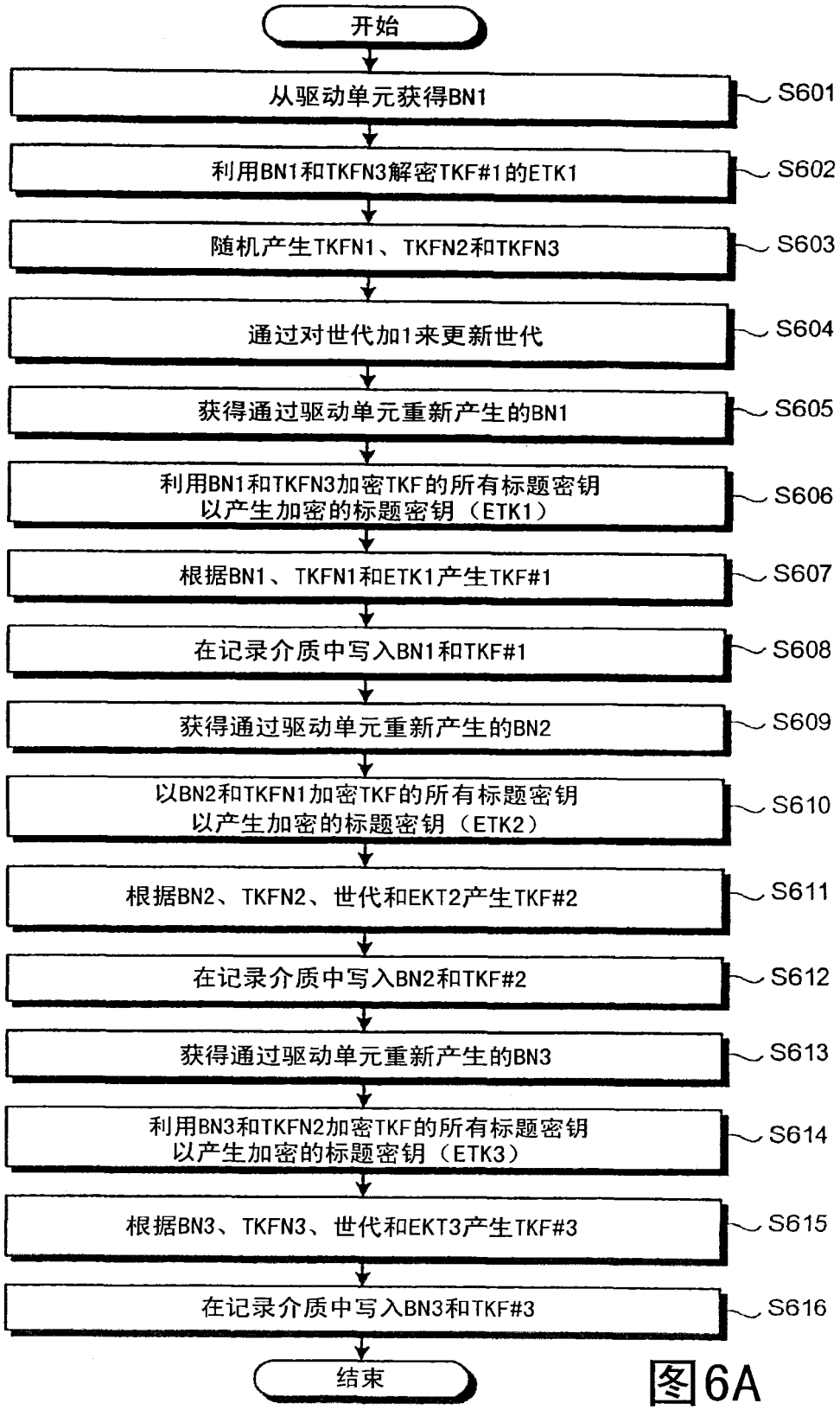

开始
从驱动单元获得BN1
S601
利用BN1和TKFN3解密TKF#1的ETK1
S602
随机产生TKFN1、TKFN2和TKFN3
S603
通过对世代加1来更新世代
S604
获得通过驱动单元重新产生的BN1
S605
利用BN1和TKFN3加密TKF的所有标题密钥
以产生加密的标题密钥（ETK1）
S606
根据BN1、TKFN1和ETK1产生TKF#1
S607
在记录介质中写入BN1和TKF#1
S608
获得通过驱动单元重新产生的BN2
S609
以BN2和TKFN1加密TKF的所有标题密钥
以产生加密的标题密钥（ETK2）
S610
根据BN2、TKFN2、世代和EKT2产生TKF#2
S611
在记录介质中写入BN2和TKF#2
S612
获得通过驱动单元重新产生的BN3
S613
利用BN3和TKFN2加密TKF的所有标题密钥
以产生加密的标题密钥（ETK3）
S614
根据BN3、TKFN3、世代和EKT3产生TKF#3
S615
在记录介质中写入BN3和TKF#3
S616
结束

图6A

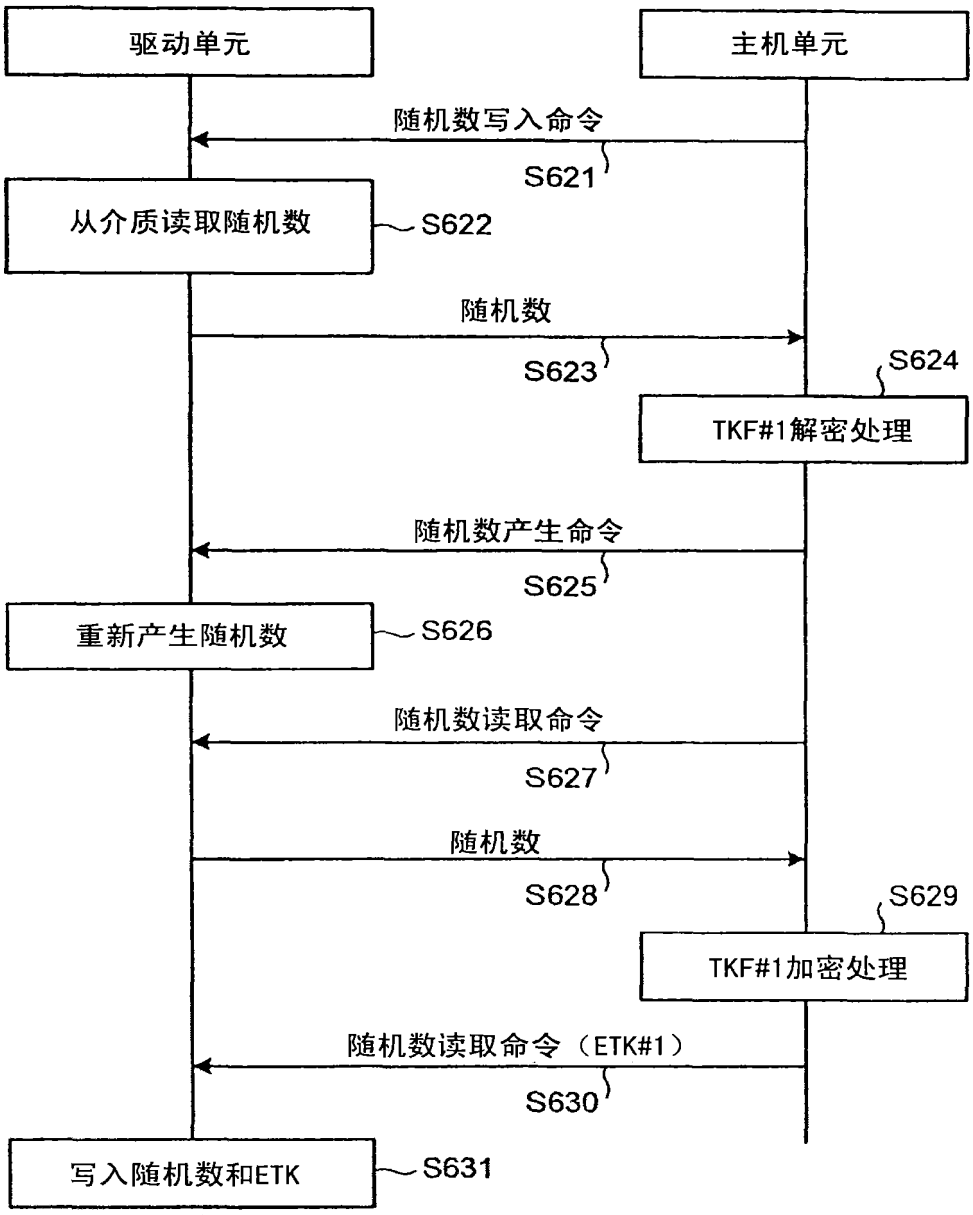

驱动单元
主机单元
随机数写入命令
S621
从介质读取随机数
S622
随机数
S623
S624
TKF#1解密处理
随机数产生命令
S625
重新产生随机数
S626
随机数读取命令
S627
随机数
S628
S629
TKF#1加密处理
随机数读取命令（ETK#1）
S630
写入随机数和ETK
S631

图6B

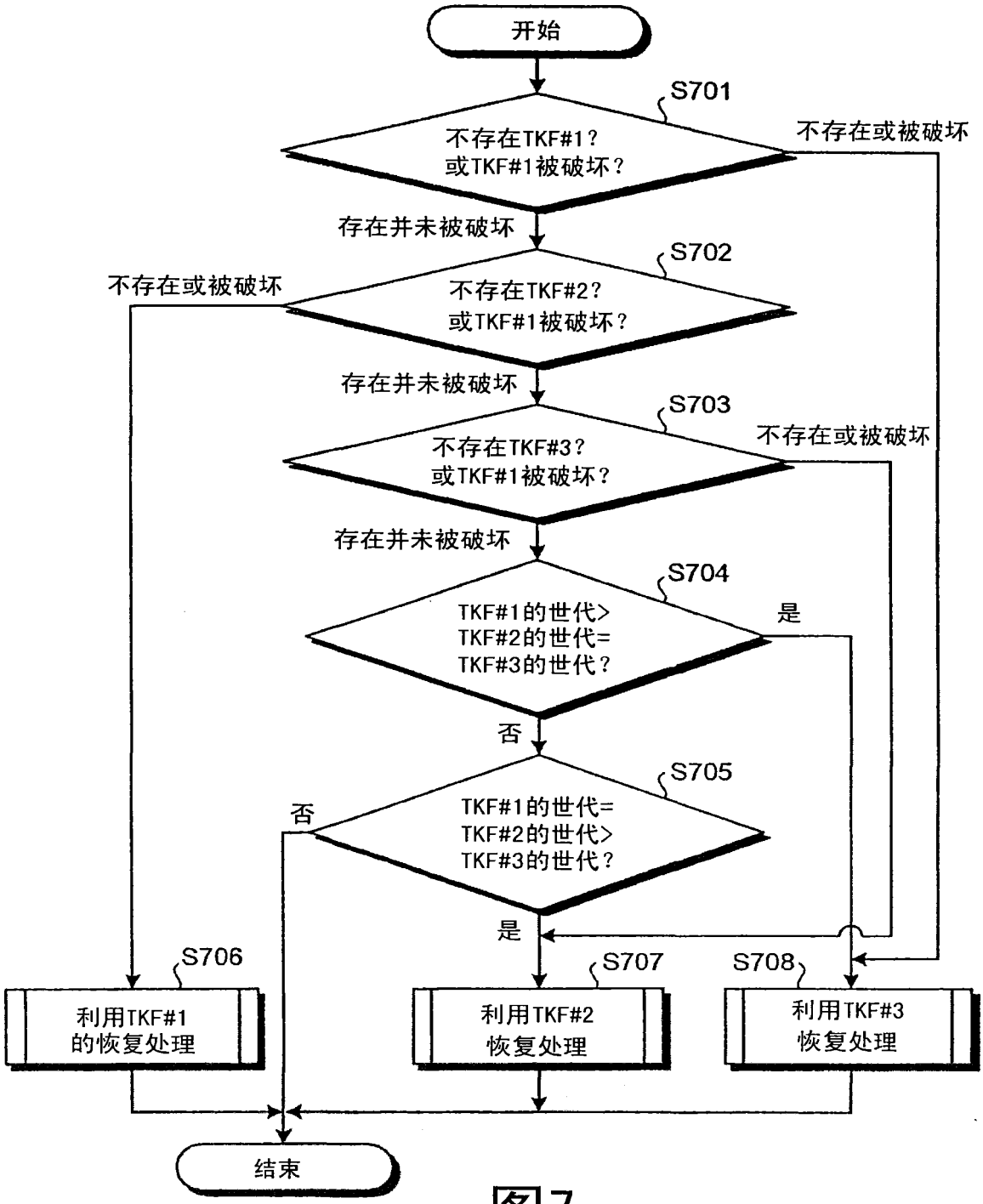

开始
S701
不存在TKF#1？
或TKF#1被破坏？
不存在或被破坏
存在并未被破坏
S702
不存在TKF#2？
或TKF#1被破坏？
不存在或被破坏
存在并未被破坏
S703
不存在TKF#3？
或TKF#1被破坏？
不存在或被破坏
存在并未被破坏
S704
TKF#1的世代>
TKF#2的世代=
TKF#3的世代？
是
否
S705
TKF#1的世代=
TKF#2的世代>
TKF#3的世代？
否
是
S706
利用TKF#1
的恢复处理
S707
利用TKF#2
恢复处理
S708
利用TKF#3
恢复处理
结束

图7

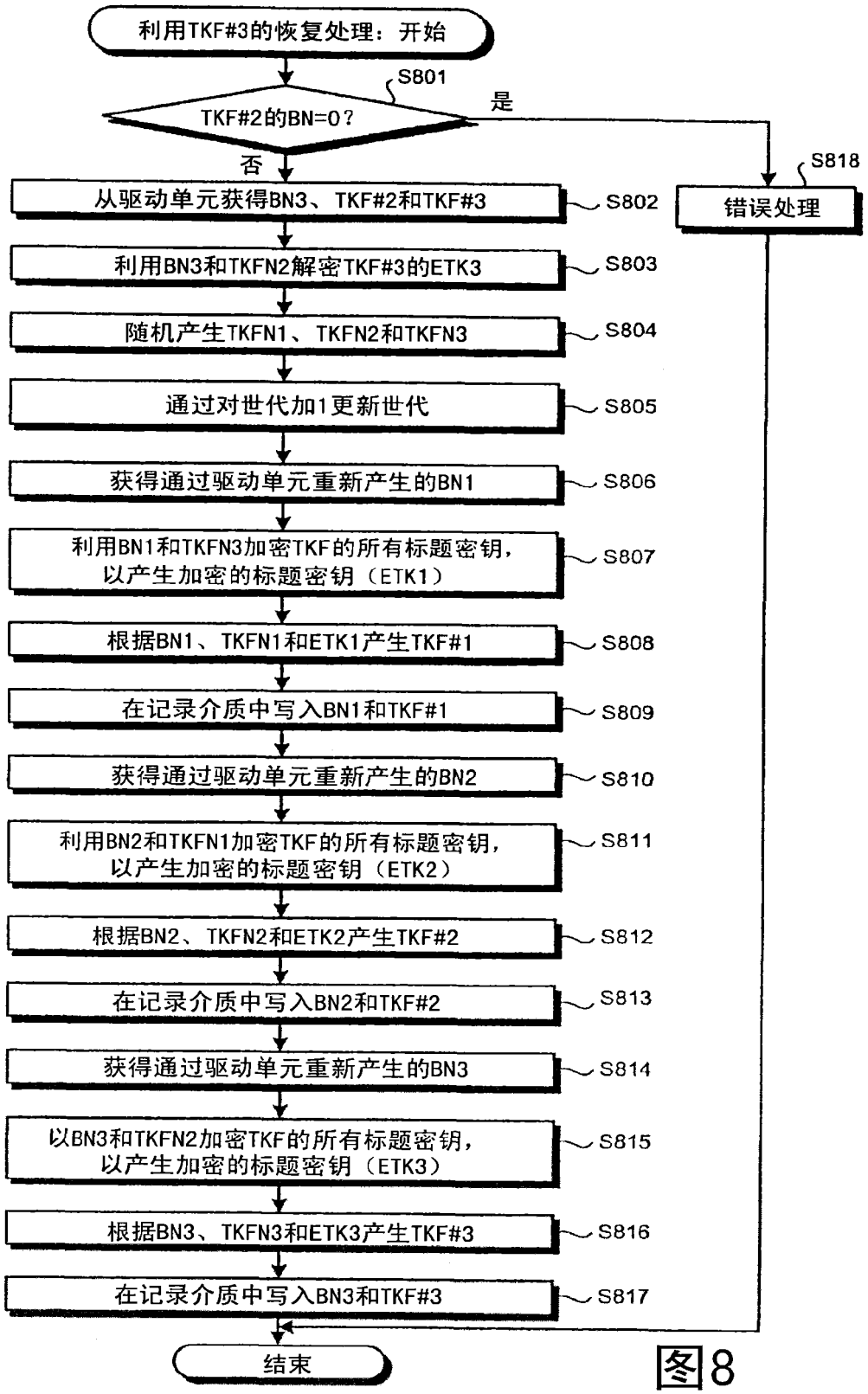

利用TKF#3的恢复处理：开始
S801
TKF#2的BN=0？
是
否
S818
错误处理
从驱动单元获得BN3、TKF#2和TKF#3
S802
利用BN3和TKFN2解密TKF#3的ETK3
S803
随机产生TKFN1、TKFN2和TKFN3
S804
通过对世代加1更新世代
S805
获得通过驱动单元重新产生的BN1
S806
利用BN1和TKFN3加密TKF的所有标题密钥，以产生加密的标题密钥（ETK1）
S807
根据BN1、TKFN1和ETK1产生TKF#1
S808
在记录介质中写入BN1和TKF#1
S809
获得通过驱动单元重新产生的BN2
S810
利用BN2和TKFN1加密TKF的所有标题密钥，以产生加密的标题密钥（ETK2）
S811
根据BN2、TKFN2和ETK2产生TKF#2
S812
在记录介质中写入BN2和TKF#2
S813
获得通过驱动单元重新产生的BN3
S814
以BN3和TKFN2加密TKF的所有标题密钥，以产生加密的标题密钥（ETK3）
S815
根据BN3、TKFN3和ETK3产生TKF#3
S816
在记录介质中写入BN3和TKF#3
S817
结束

图8

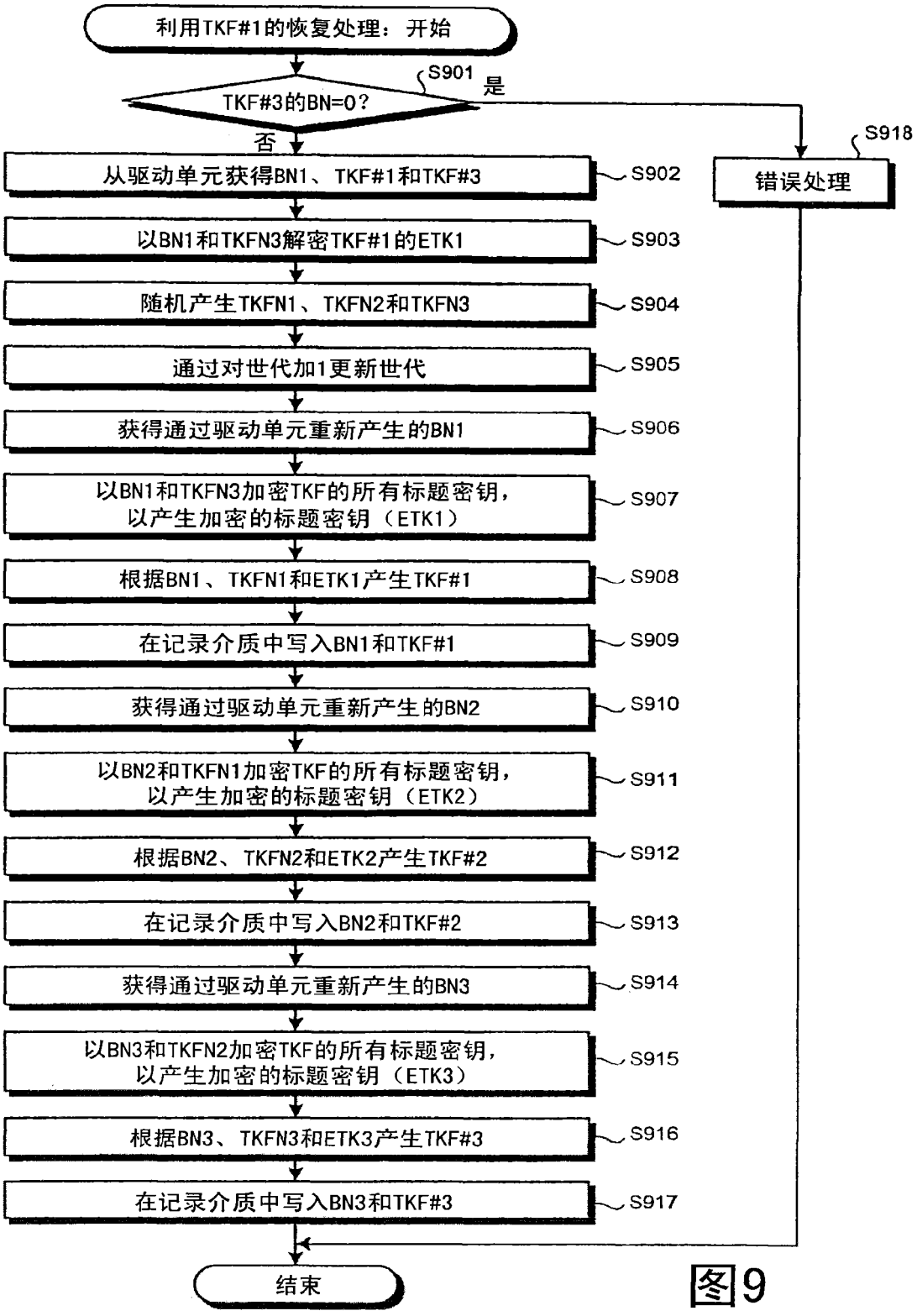

利用TKF#1的恢复处理：开始
S901
TKF#3的BN=0？
是
否
S918
错误处理
从驱动单元获得BN1、TKF#1和TKF#3
S902
以BN1和TKFN3解密TKF#1的ETK1
S903
随机产生TKFN1、TKFN2和TKFN3
S904
通过对世代加1更新世代
S905
获得通过驱动单元重新产生的BN1
S906
以BN1和TKFN3加密TKF的所有标题密钥，以产生加密的标题密钥（ETK1）
S907
根据BN1、TKFN1和ETK1产生TKF#1
S908
在记录介质中写入BN1和TKF#1
S909
获得通过驱动单元重新产生的BN2
S910
以BN2和TKFN1加密TKF的所有标题密钥，以产生加密的标题密钥（ETK2）
S911
根据BN2、TKFN2和ETK2产生TKF#2
S912
在记录介质中写入BN2和TKF#2
S913
获得通过驱动单元重新产生的BN3
S914
以BN3和TKFN2加密TKF的所有标题密钥，以产生加密的标题密钥（ETK3）
S915
根据BN3、TKFN3和ETK3产生TKF#3
S916
在记录介质中写入BN3和TKF#3
S917
结束

图9

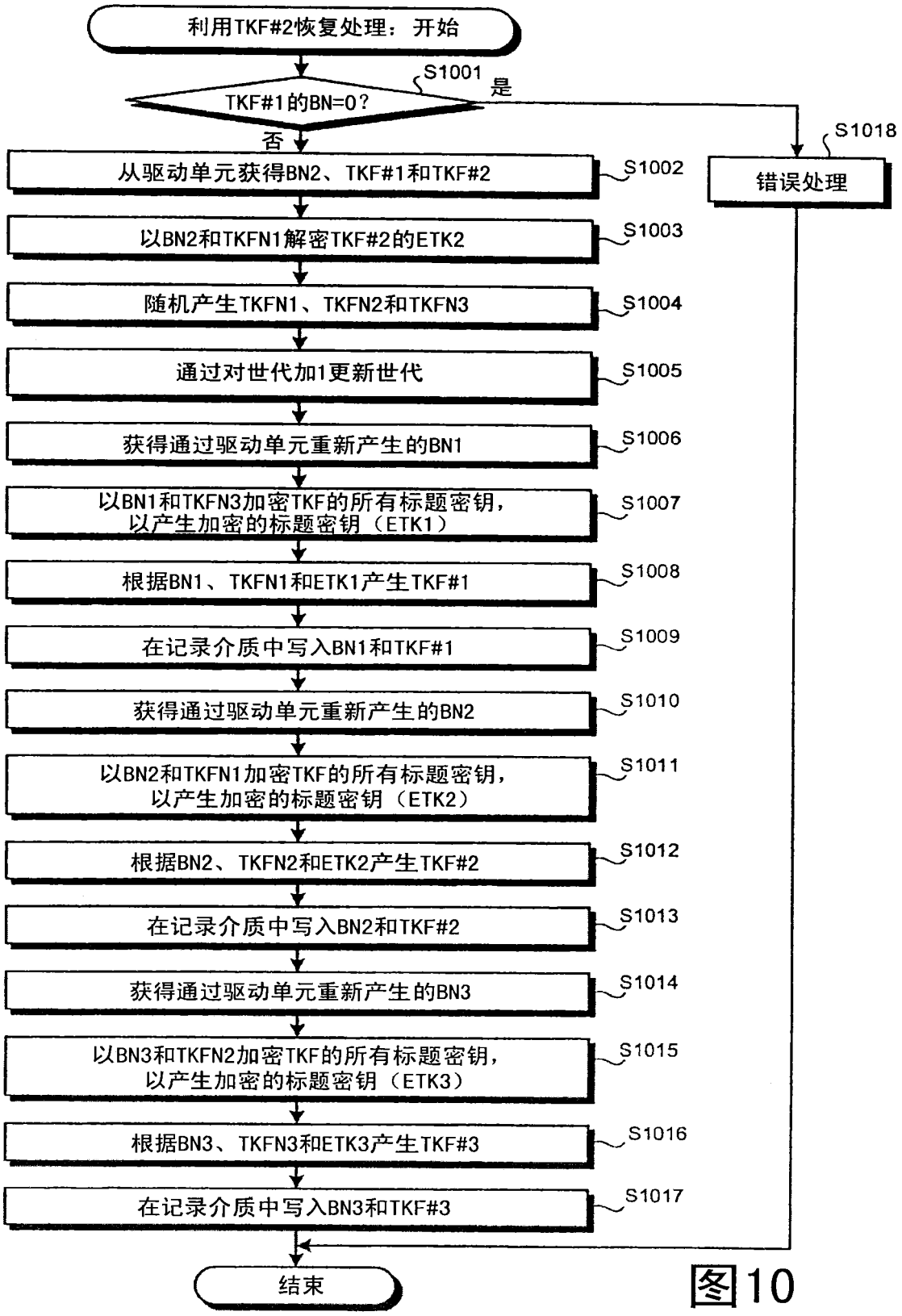

利用TKF#2恢复处理：开始
S1001
TKF#1的BN=0？
是
否
S1018
错误处理
从驱动单元获得BN2、TKF#1和TKF#2
S1002
以BN2和TKFN1解密TKF#2的ETK2
S1003
随机产生TKFN1、TKFN2和TKFN3
S1004
通过对世代加1更新世代
S1005
获得通过驱动单元重新产生的BN1
S1006
以BN1和TKFN3加密TKF的所有标题密钥，以产生加密的标题密钥（ETK1）
S1007
根据BN1、TKFN1和ETK1产生TKF#1
S1008
在记录介质中写入BN1和TKF#1
S1009
获得通过驱动单元重新产生的BN2
S1010
以BN2和TKFN1加密TKF的所有标题密钥，以产生加密的标题密钥（ETK2）
S1011
根据BN2、TKFN2和ETK2产生TKF#2
S1012
在记录介质中写入BN2和TKF#2
S1013
获得通过驱动单元重新产生的BN3
S1014
以BN3和TKFN2加密TKF的所有标题密钥，以产生加密的标题密钥（ETK3）
S1015
根据BN3、TKFN3和ETK3产生TKF#3
S1016
在记录介质中写入BN3和TKF#3
S1017
结束

图10

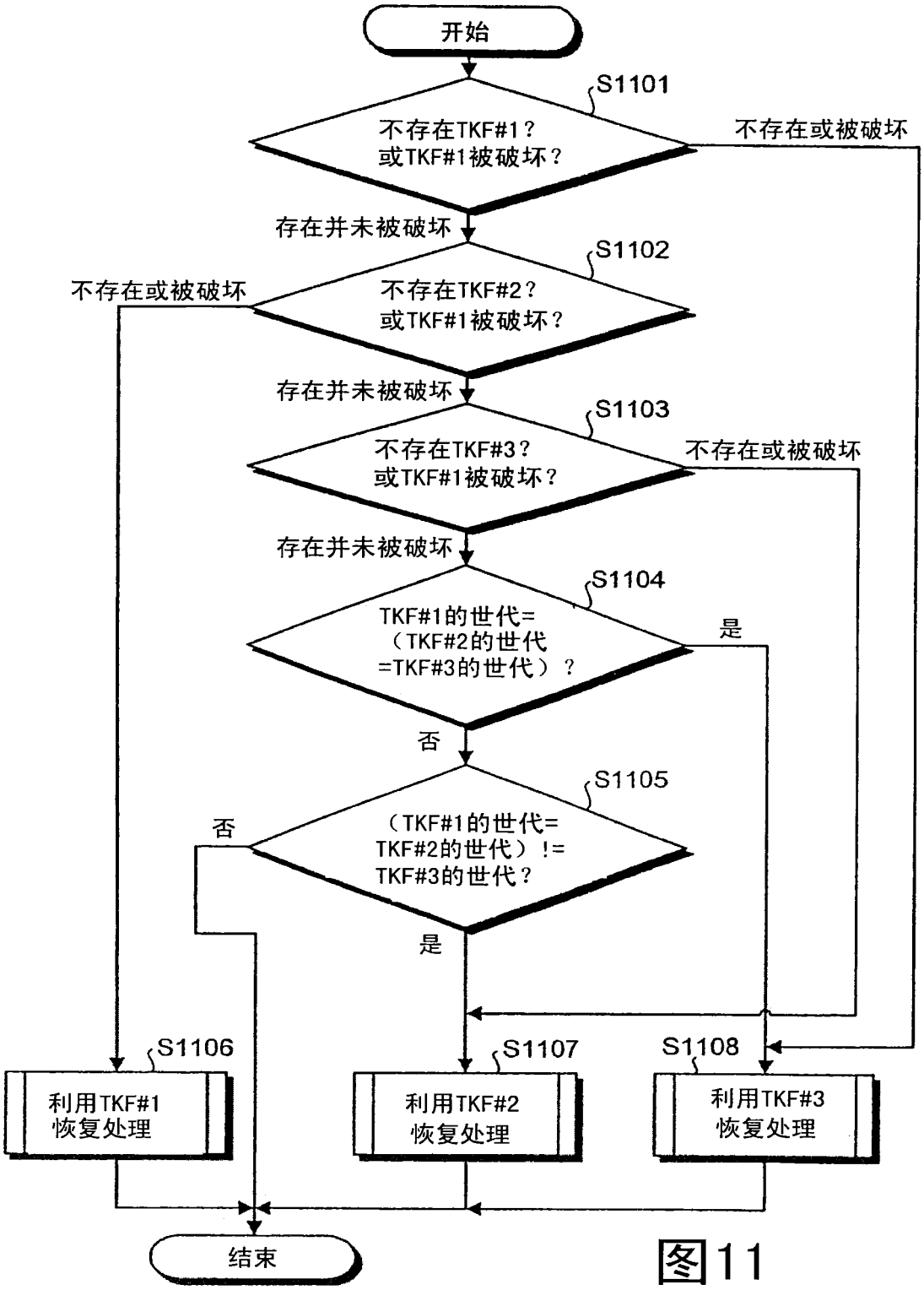

开始
S1101
不存在TKF#1？
或TKF#1被破坏？
不存在或被破坏
存在并未被破坏
S1102
不存在TKF#2？
或TKF#1被破坏？
不存在或被破坏
存在并未被破坏
S1103
不存在TKF#3？
或TKF#1被破坏？
不存在或被破坏
存在并未被破坏
S1104
TKF#1的世代=
（TKF#2的世代
=TKF#3的世代）？
是
否
S1105
（TKF#1的世代=
TKF#2的世代）!=
TKF#3的世代？
否
是
S1106
利用TKF#1
恢复处理
S1107
利用TKF#2
恢复处理
S1108
利用TKF#3
恢复处理
结束

图11

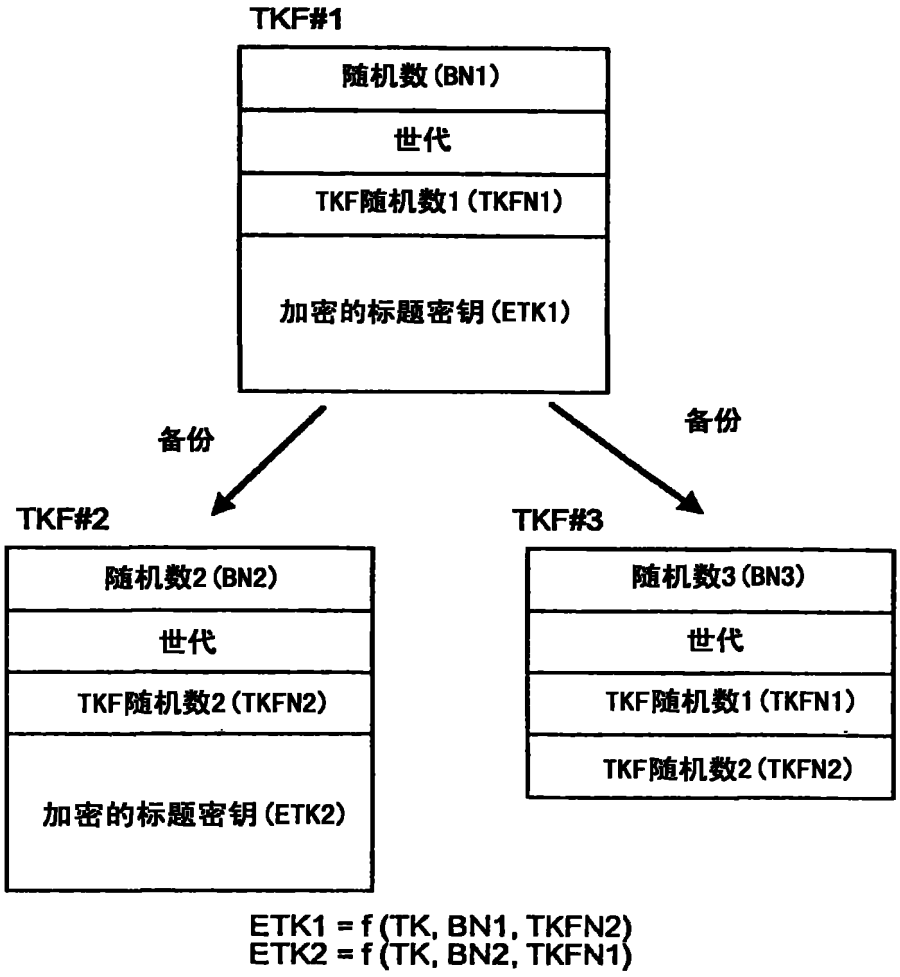

TKF#1
随机数(BN1)
世代
TKF随机数1(TKFN1)
加密的标题密钥(ETK1)
备份
备份
TKF#2
随机数2(BN2)
世代
TKF随机数2(TKFN2)
加密的标题密钥(ETK2)
TKF#3
随机数3(BN3)
世代
TKF随机数1(TKFN1)
TKF随机数2(TKFN2)
ETK1 = f(TK, BN1, TKFN2)
ETK2 = f(TK, BN2, TKFN1)

图12


开始
随机产生TKFN1和TKFN2
S1301
随机产生世代
S1302
从驱动单元获得随机数1（BN1）
S1303
以BN1和TKFN2加密TKF的所有标题密钥，
以产生加密的标题密钥（ETK1）
S1304
根据BN1、TFKN1、世代和ETK1产生TKF#1
S1305
在记录介质中写入BN1和TKF#1
S1306
从驱动单元获得随机数2（BN2）
S1307
以BN2和TKFN1加密TKF的所有标题密钥，
以产生加密的标题密钥（ETK2）
S1308
根据BN2、TFKN2、世代和ETK2产生TKF#2
S1309
在记录介质中写入BN2和TKF#2
S1310
从驱动单元获得随机数3（BN3）
S1311
根据BN3、世代、TKFN1和TKFN2产生TKF#3
S1312
在记录介质中写入BN3和TKF#3
S1313
结束

图13


开始
从驱动单元获得BN1
S1401
以BN1和TKFN2解密TKF#1的ETK1
S1402
随机产生TKFN1和TKFN2
S1403
通过对世代加1更新世代
S1404
获得通过驱动单元重新产生的BN1
S1405
以BN1和TKFN2加密TKF的所有标题密钥，
以产生加密的标题密钥（ETK1）
S1406
根据BN1、世代、TFKN1和ETK1产生TKF#1
S1407
在记录介质中写入BN1和TKF#1
S1408
获得通过驱动单元重新产生的BN2
S1409
以BN2和TKFN1加密TKF的所有标题密钥，
以产生加密的标题密钥（ETK2）
S1410
根据BN2、TKFN2、世代和ETK2产生TKF#2
S1411
在记录介质中写入BN2和TKF#2
S1412
获得通过驱动单元重新产生的BN3
S1413
根据BN3、世代、TKFN1和TKFN2 产生TKF#3
S1414
在记录介质中写入BN3和TKF#3
S1415
结束

图14

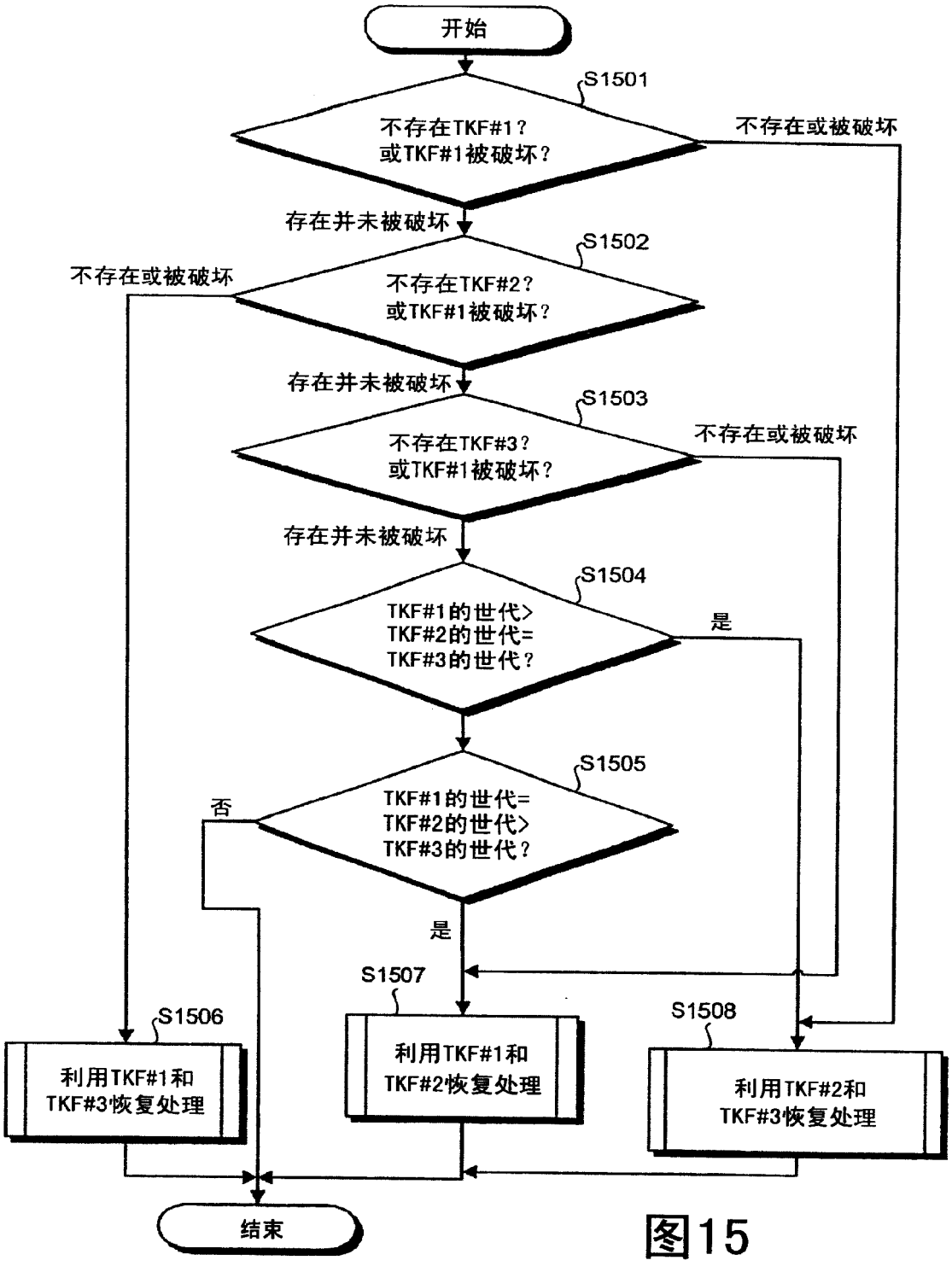

开始
S1501
不存在TKF#1？
或TKF#1被破坏？
不存在或被破坏
存在并未被破坏
S1502
不存在TKF#2？
或TKF#1被破坏？
不存在或被破坏
存在并未被破坏
S1503
不存在TKF#3？
或TKF#1被破坏？
不存在或被破坏
存在并未被破坏
S1504
TKF#1的世代>
TKF#2的世代=
TKF#3的世代？
是
S1505
TKF#1的世代=
TKF#2的世代>
TKF#3的世代？
否
是
S1507
利用TKF#1和
TKF#2恢复处理
S1506
利用TKF#1和
TKF#3恢复处理
S1508
利用TKF#2和
TKF#3恢复处理
结束

图15

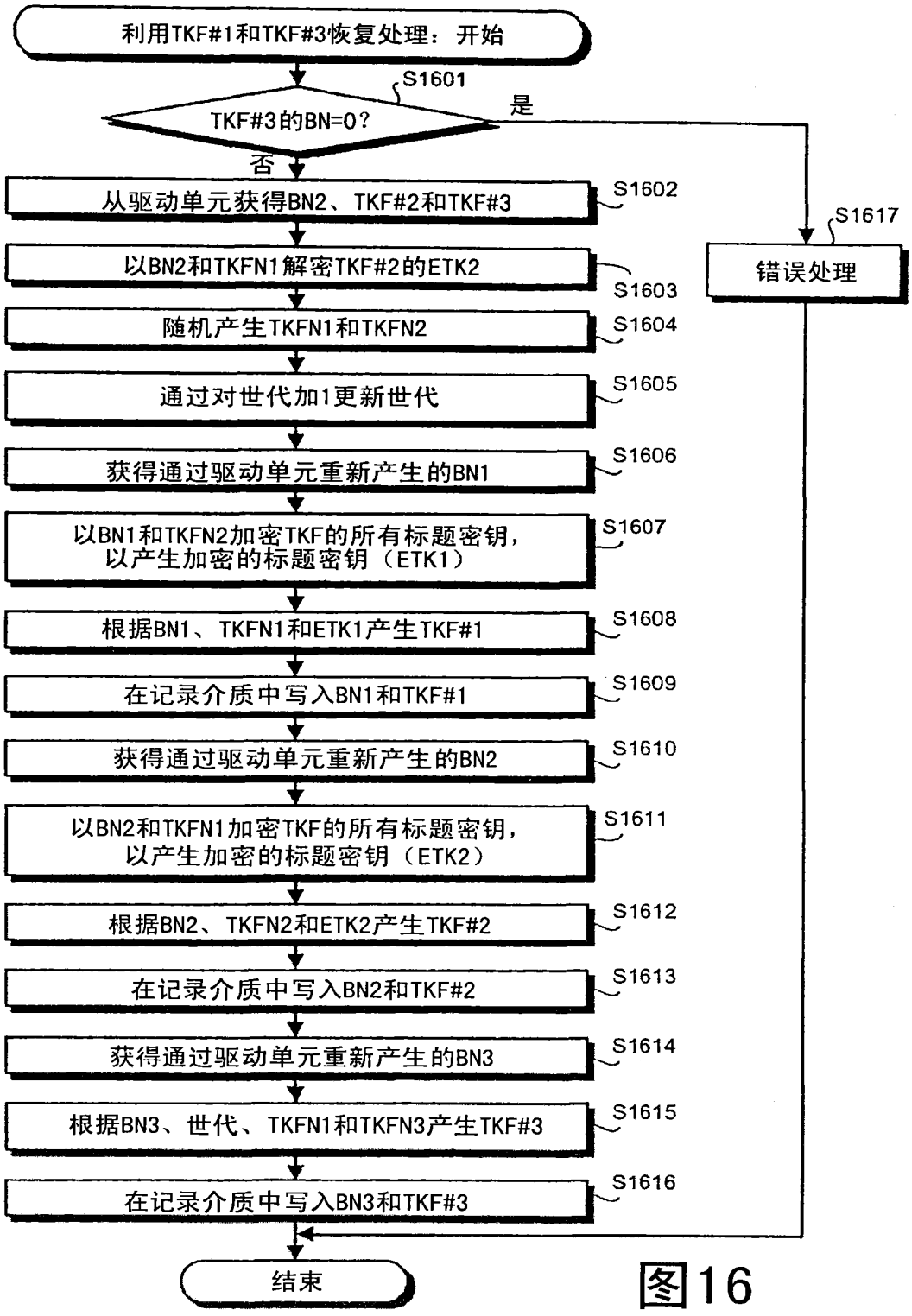

利用TKF#1和TKF#3恢复处理：开始
S1601
TKF#3的BN=0？
是
否
S1617
错误处理
从驱动单元获得BN2、TKF#2和TKF#3
S1602
以BN2和TKFN1解密TKF#2的ETK2
S1603
随机产生TKFN1和TKFN2
S1604
通过对世代加1更新世代
S1605
获得通过驱动单元重新产生的BN1
S1606
以BN1和TKFN2加密TKF的所有标题密钥，
以产生加密的标题密钥（ETK1）
S1607
根据BN1、TKFN1和ETK1产生TKF#1
S1608
在记录介质中写入BN1和TKF#1
S1609
获得通过驱动单元重新产生的BN2
S1610
以BN2和TKFN1加密TKF的所有标题密钥，
以产生加密的标题密钥（ETK2）
S1611
根据BN2、TKFN2和ETK2产生TKF#2
S1612
在记录介质中写入BN2和TKF#2
S1613
获得通过驱动单元重新产生的BN3
S1614
根据BN3、世代、TKFN1和TKFN3产生TKF#3
S1615
在记录介质中写入BN3和TKF#3
S1616
结束

图16

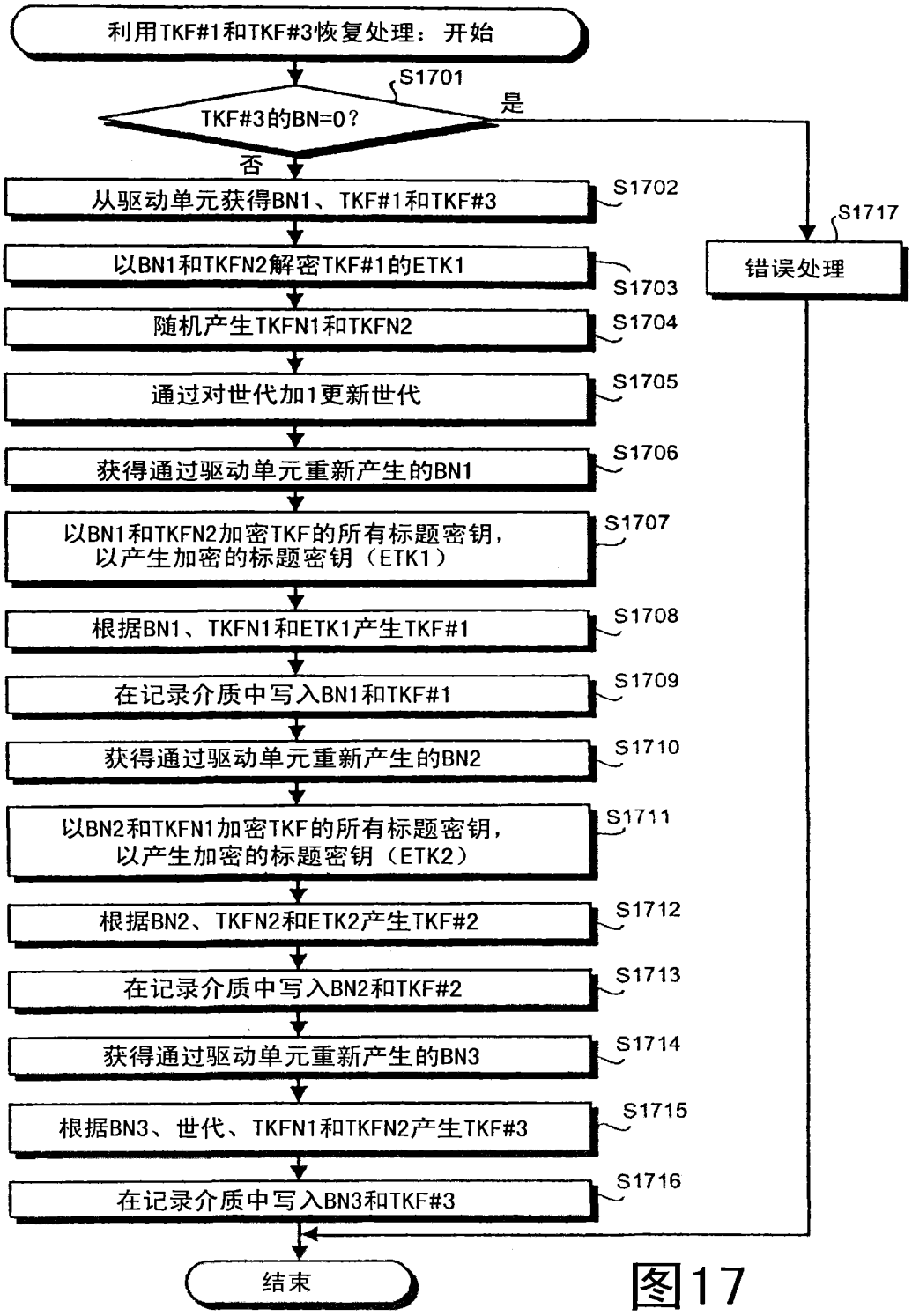

利用TKF#1和TKF#3恢复处理：开始
S1701
TKF#3的BN=0？
是
否
S1717
错误处理
从驱动单元获得BN1、TKF#1和TKF#3
S1702
以BN1和TKFN2解密TKF#1的ETK1
S1703
随机产生TKFN1和TKFN2
S1704
通过对世代加1更新世代
S1705
获得通过驱动单元重新产生的BN1
S1706
以BN1和TKFN2加密TKF的所有标题密钥，
以产生加密的标题密钥（ETK1）
S1707
根据BN1、TKFN1和ETK1产生TKF#1
S1708
在记录介质中写入BN1和TKF#1
S1709
获得通过驱动单元重新产生的BN2
S1710
以BN2和TKFN1加密TKF的所有标题密钥，
以产生加密的标题密钥（ETK2）
S1711
根据BN2、TKFN2和ETK2产生TKF#2
S1712
在记录介质中写入BN2和TKF#2
S1713
获得通过驱动单元重新产生的BN3
S1714
根据BN3、世代、TKFN1和TKFN2产生TKF#3
S1715
在记录介质中写入BN3和TKF#3
S1716
结束

图17

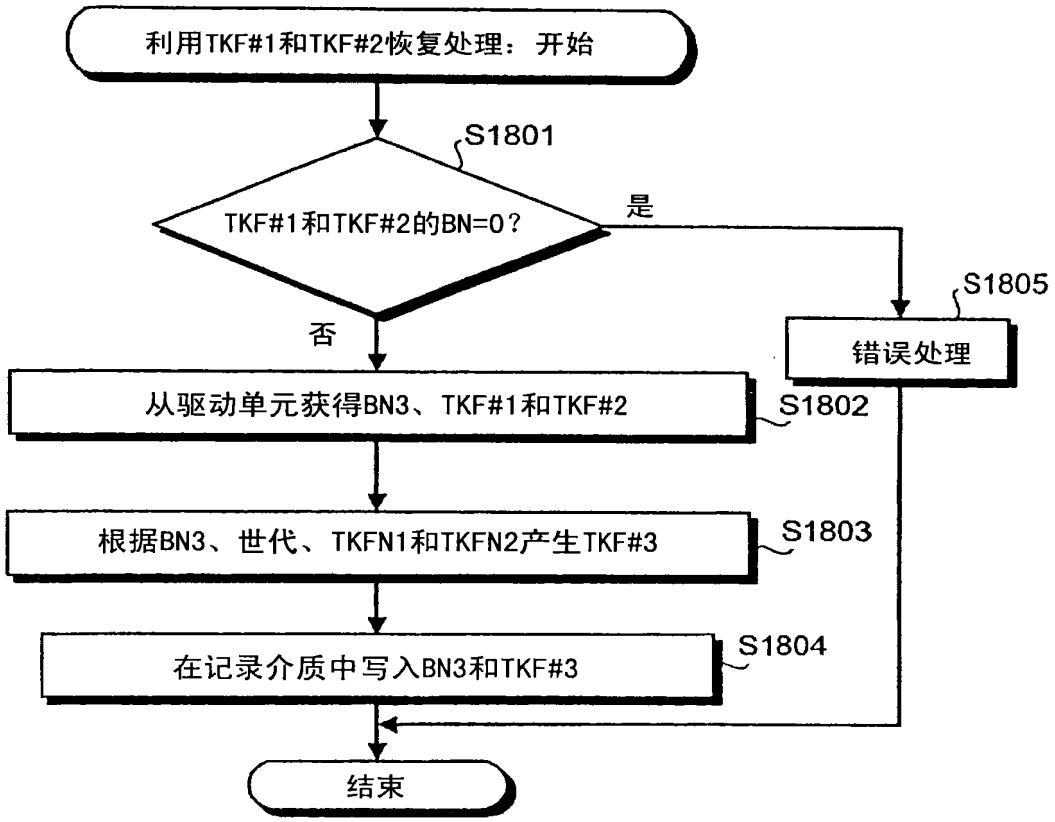

利用TKF#1和TKF#2恢复处理：开始
S1801
TKF#1和TKF#2的BN=0？
是
否
S1805
错误处理
从驱动单元获得BN3、TKF#1和TKF#2
S1802
根据BN3、世代、TKFN1和TKFN2产生TKF#3
S1803
在记录介质中写入BN3和TKF#3
S1804
结束

图18

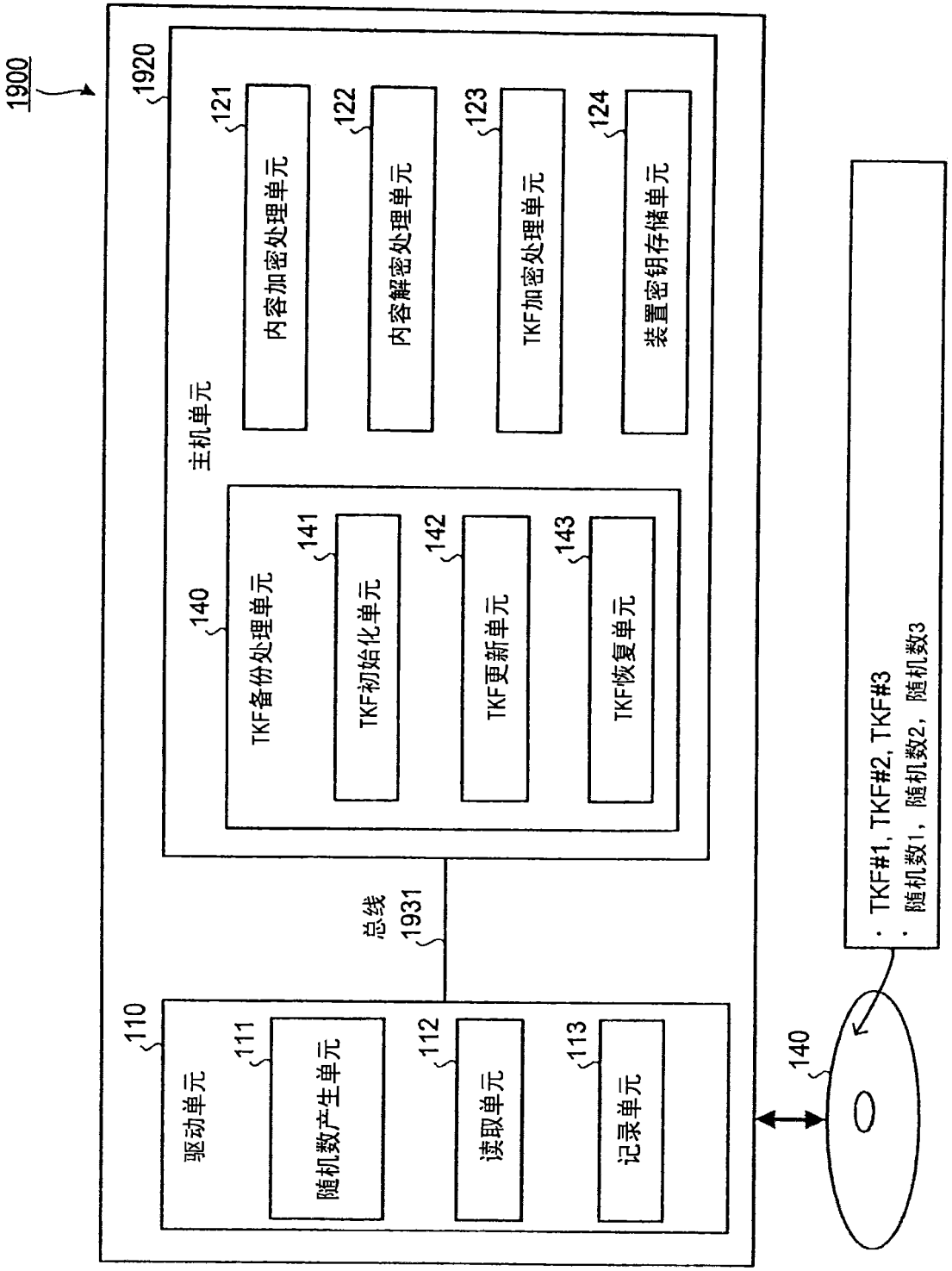

1900
1920
主机单元
121
内容加密处理单元
122
内容解密处理单元
123
TKF加密处理单元
124
装置密钥存储单元
140
TKF备份处理单元
141
TKF初始化单元
142
TKF更新单元
143
TKF恢复单元
总线
1931
110
驱动单元
111
随机数产生单元
112
读取单元
113
记录单元
140
· TKF#1, TKF#2, TKF#3
· 随机数1，随机数2，随机数3

图19